命令手册

RG-NBR 系列出口网关

NBR_RGOS 11.9(4)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

- 锐捷睿易官方网站：http://www.ruijiery.com/
- 锐捷睿易在线客服：http://ocs.ruijie.com.cn/?p=smb
- 锐捷网络官方网站服务与支持版块：http://www.ruijie.com.cn/service.aspx
- 7 天无休技术服务热线：4001-000-078
- 锐捷睿易技术论坛：http://bbs.ruijiery.com/
- 常见问题搜索：http://www.ruijie.com.cn/service/know.aspx
- 锐捷睿易技术支持与反馈信箱：4001000078@ruijie.com.cn
- 锐捷网络服务公众号：【锐捷服务】扫码关注

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。

命令参考-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. 基础配置管理
3. LINE
4. PASSWORD-POLICY
5. File System
6. LICENSING
7. PKG_MGMT
8. CWMP
9. 系统日志
10. LED
11. 异常告警
12. HTTP
13. PATCH-UPGRADE
14. WEB-UPGRADE

1 命令行界面

1.1 alias

配置一条命令的别名。
alias *mode command-alias original-command*

删除自定义的命令别名，对于存在默认别名的命令，可恢复缺省配置。
no alias *mode* [*command-alias*]

对于存在默认别名的命令，还可以通过 **default** 恢复缺省配置。
default alias *mode* [*command-alias*]

【参数说明】

参数	描述
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语法。

【缺省配置】 在普通或特权用户模式下，部分命令存在默认的别名。

【命令模式】 全局配置模式

【缺省级别】 14

【使用指导】 普通或特权用户模式下默认的命令别名为 h、p、s、u、un 的实际命名分别为 **help**、**ping**、**show**、**undebug**、**undebug**。
默认的命令别名不能通过 **no alias exec** 命令删除。
通过配置命令别名，可以用一个单词来代替一条命令。例如，创建一个别名来代表一条命令的前一部分，然后可以继续输入后面的部分。
别名所代表的命令所处的命令模式是当前系统中存在的命令模式，在全局配置模式下，输入 **alias** ?可以列出当前可以配置别名的全部命令模式：

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

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

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

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

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

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

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

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

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

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

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

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

命令别名在使用时必须完整输入，否则不能被识别。

使用 **show aliases** 命令可以查看系统中的别名设置。

【配置举例】 1：设置全局配置模式下，使用命令别名"def-route"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 def-route ip route 0.0.0.0 0.0.0.0 192.168.1.1
Ruijie(config)#def-route?
*def-route="ip route 0.0.0.0 0.0.0.0 192.168.1.1"
Ruijie(config)#end
Ruijie#show aliases config
globle configure mode alias:
def-route            ip route 0.0.0.0 0.0.0.0 192.168.1.1
```

【检验方法】 在命令行编辑界面上，配置用一个单词作为一条命令的别名。输入这个的单词，如果可以来代替这条命令，即说明该别名配置有效。

【提示信息】 命令别名长度不能超过 19 个字符，如果超过这个限制则会出现以下提示信息：

```
% Overly long alias name truncated after 19 characters.
```

别名所代表的实际命令语法字符串长度不能超过 255 个字符，如果超过这个限制则会出现以下提示信息：

```
% Command alias string too long.
```

每个命令模式下支持的最多的别名个数为 100 个，如果超过这个限制则会出现以下提示信息：

```
% Can't add more than 100 command aliases in single mode.
```

因为各种意外原因（例如内存不足等），添加别名失败时，则会出现以下提示信息：

```
% Adding command alias fail.
```

【常见错误】 -

【平台说明】 -

1.2 privilege

配置一条命令的执行权限授予一个命令级别。
privilege *mode* [**all**] {**level** *level* **| reset**} *command-string*

恢复缺省配置。
no privilege *mode* [**all**] [**level** *level*] *command-string*

【参数说明】

参数	描述
mode	要授权的命令所属的 CLI 命令模式
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*	指定命令或子命令的运行权限级别，级别的范围 0-15
reset	将命令的执行权限恢复为默认级别
command-string	要授权的命令字符串

【缺省配置】 -

【命令模式】 全局配置模式

【缺省级别】 15

【使用指导】 下表显示一部分在 **privilege** 命令中可进行授权的 CLI 命令模式关键字，不同的设备，可授权的命令模式数量可能会发生变化，在全局配置模式下，可以使用 **privilege ?**列出当前所有可授权的 CLI 命令模式。

模式	说明
config	全局配置模式
exec	特权模式
interface	接口配置模式
ip-dhcp-pool	DHCP 地址池配置模式
keychain	KeyChain 配置模式
keychain-key	KeyChain-key 配置模式
time-range	Time-Range 配置模式

【配置举例】 1：设置 CLI 级别 1 的口令为”test”，并设置执行 **reload** 命令的权限，可以复位设备。

```
Ruijie(config)#privilege exec level 1 reload
```

此时，使用级别 1 进入 CLI 界面，发现可以使用 **reload** 命令：

```
Ruijie>reload ?
LINE    Reason for reload
<cr>
```

如果要将 **reload** 的全部子命令都授权给级别 1 的用户，则可以使用 **all** 关键字：

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

此时，使用级别 1 进入 CLI 界面，发现可以使用 **reload** 的全部子命令：

```
Ruijie>reload ?
LINE    Reason for reload
at                      reload at a specific time/date
cancel                 cancel pending reload scheme
in                      reload after a time interval
```

【检验方法】 选择一条在高级别（例如 14 级）支持而低级别（例如 1 级）不支持的命令，然后将该命令授权给低级别。切换到低级别后，如果该命令可以被执行，则表明授权有效。

【提示信息】 -

【常见错误】 -

【平台说明】 -

1.3 show aliases

显示所有的命令别名或特定命令模式下的命令别名。

show aliases [*mode*]

【参数说明】

参数	描述
mode	别名所代表的命令所处的命令模式

【命令模式】 特权用户模式

【缺省级别】 14

【使用指导】 如果没有输入命令模式，则显示所有的命令别名设置。

【配置举例】 1：显示 EXEC 模式下的命令别名。

```
Ruijie#show aliases exec
exec mode alias:
h                   help
p                   ping
```

s	show
u	undebug
un	undebug

【提示信息】 -

【平台说明】 -

2 基础配置管理

2.1 <1-99>

恢复已经建立的 Telnet Client 会话连接。
<1-99>

【参数说明】

参数	描述
-	-

【缺省配置】 -

【命令模式】 普通用户模式

【缺省级别】 1

【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，可以使用数字键**<1-99>**命令进行恢复。同时，如果连接已建立，可以使用 **show session** 命令查看已建立的连接信息。

【配置举例】 1：恢复已经建立的 Telnet Client 会话连接。

```
Ruijie# 1
```

【检验方法】 -

【提示信息】 -

【常见错误】 -

【平台说明】 -

2.2 banner exec

定制用户登录 line 线路进入普通用户模式前的提示欢迎信息
banner exec *c message c*

取消提示欢迎信息的配置
no banner exec

【参数说明】

参数	描述
c	提示欢迎信息的分隔符，提示欢迎信息内容中间不允许出现间隔符。
message	配置提示欢迎信息内容。

【缺省配置】 -

【命令模式】 全局配置模式

【缺省级别】 14

【使用指导】 使用该命令可以配置提示欢迎信息，如果键入结束的分隔符后仍然输入字符，则这些字符将被系统丢弃。
当用户登录设备时，MOTD（**banner motd**）首先显示，然后将显示 LOGIN 的提示信息（**banner login**），用户成功登录设备以后 ,将根据连接类型出现 EXEC(**banner exec**)的提示信息或 incoming(**banner incoming** ）的提示信息。如果是反向 Telnet 则出现 incoming 提示信息，其他连接则出现 EXEC 提示信息。
该命令配置的提示信息是针对所有的 line 线路，如果要在某条线路上禁止 EXEC 提示信息，可以在具体的 line 线路上配置 **no exec-banner**。

【配置举例】 1：下面的示例进行提示欢迎信息的设置：

```
Ruijie(config)# banner exec $ 欢迎使用锐捷设备 $
```

【检验方法】 配置后，用户登录 line 线路进入普通用户模式，可显示所配置的信息。

【提示信息】 -

【常见错误】 -

【平台说明】 -

2.3 banner incoming

配置建立反向 Telnet 连接的提示信息
banner incoming *c message c*

取消反向 telnet 连接的提示信息的配置
no banner incoming

【参数说明】

参数	描述
c	反向 Telnet 连接的提示信息的分隔符，提示信息内容中间不允许出现间隔符。
message	配置反向 Telnet 连接的提示信息内容。

【缺省配置】 -

【命令模式】 全局配置模式

【缺省级别】 14

【使用指导】 使用该命令可以配置反向 Telnet 连接的提示信息，如果键入结束的分隔符后仍然输入字符，则这些字符将被系统丢弃。
当用户登录设备，MOTD（**banner motd**）首先显示，然后将显示 LOGIN 的提示信息（**banner login**），用户成功登录设备以后，将根据连接类型出现 EXEC（**banner exec**）的提示信息或 incoming（**banner incoming**）的提示信息。如果是反向 Telnet 则出现 incoming 提示信息，其他连接则出现 EXEC 提示信息。

【配置举例】 1：下面的示例进行反向 Telnet 连接信息的设置：

```
Ruijie(config)# banner incoming $ 欢迎使用锐捷设备 $
```

【检验方法】 配置后，反向 Telnet 连接用户登录 line 线路进入普通用户模式，可显示所配置的信息。

【提示信息】 -

【常见错误】 -

【平台说明】 -

2.4 banner login

配置登录标题信息
banner login *c message c*

取消登录标题信息的配置
no banner login

【参数说明】

参数	描述
c	登录标题信息的分隔符，登录标题信息内容中间不允许出现间隔符。
message	配置登录标题信息内容。

【缺省配置】 -

【命令模式】 全局配置模式

【缺省级别】 14

【使用指导】 使用该命令可以配置登录标题信息，如果键入结束的分隔符后仍然输入字符，则这些字符将被系统丢弃。
当用户登录路由器，MOTD（**banner motd**）首先显示，然后将显示 LOGIN 的提示信息（**banner login**），用户成功登录设备以后 ,将根据连接类型出现 EXEC(**banner exec**)的提示信息或 incoming(**banner incoming** ）的提示信息。如果是反向 Telnet 则出现 incoming 提示信息，其他连接则出现 EXEC 提示信息。

【配置举例】 1：下面的示例进行登录标题信息的设置：

```
Ruijie(config)# banner login $ enter your password $
```

【检验方法】 配置后，用户登录系统，可显示所配置的信息。

【提示信息】 -

【常见错误】 -

【平台说明】 -

2.5 banner motd

配置每日通知信息 MOTD（message of the day）
banner [**motd**] *c message c*

取消每日通知的配置信息
no banner [**motd**]

【参数说明】

参数	描述
c	每日通知信息的分隔符，每日通知信息内容中间不允许出现间隔符。
message	配置的每日通知信息内容。

【缺省配置】 -

【命令模式】 全局配置模式

【缺省级别】 14

【使用指导】 使用该命令可以配置每日通知信息，如果键入结束的分隔符后仍然输入字符，则这些字符将被系统丢弃。
当用户登录设备时，MOTD（**banner motd**）首先显示，然后将显示 LOGIN 的提示信息（**banner login**），用户成功登录设备以后 ,将根据连接类型出现 EXEC(**banner exec**)的提示信息或 incoming(**banner incoming** ）的提示信息。如果是反向 Telnet 则出现 incoming 提示信息，其他连接则出现 EXEC 提示信息。
该命令配置的提示信息是针对所有的 line 线路，如果要在某条线路上禁止 MOTD 提示信息，可以在具体的 line 线路上配置 **no motd-banner**。

【配置举例】 1：下面的示例进行每日通知信息的设置：

```
Ruijie(config)# banner motd $ hello,world $
```

【检验方法】 配置后，用户登录系统，可显示所配置的信息。

【提示信息】 -

【常见错误】 -

【平台说明】 -

2.6 banner prompt-timeout

定制用户登录认证超时的提示信息
banner prompt-timeout *c message c*

取消用户登录认证超时的提示欢迎信息配置
no banner prompt-timeout

【参数说明】

参数	描述
c	提示用户登录认证超时信息的分隔符 ,提示信息内容中间不允许出现间隔符。
message	配置提示用户登录认证超时信息内容。

【缺省配置】 -

【命令模式】 全局配置模式

【缺省级别】 14

【使用指导】 使用该命令可以配置提示用户登录认证超时信息，如果键入结束的分隔符后仍然输入字符，则这些字符将被系统丢弃。
当用户进行登录认证超时时，显示 prompt-timeout 的提示信息（**banner prompt-timeout**）。

【配置举例】 1：下面的示例进行登录认证超时提示信息的设置：

```
Ruijie(config)# banner exec $ 登录认证超时 $
```

【检验方法】 配置后，用户登录 line 线路但不进行登录认证，可显示所配置的信息。

【提示信息】 -

【常见错误】 -

【平台说明】 -

2.7 banner slip-ppp

定制 SLIP/PPP 线路连接提示信息

banner slip-ppp *c message c*

取消 SLIP/PPP 线路连接的提示信息

no banner slip-pp

【参数说明】

参数	描述
c	提示信息的分隔符，提示信息内容中间不允许出现间隔符。
message	配置提示信息内容。

【缺省配置】 -

【命令模式】 全局配置模式

【缺省级别】 14

【使用指导】 使用该命令可以配置提示欢迎信息，如果键入结束的分隔符后仍然输入字符，则这些字符将被系统丢弃。

通过 SLIP/PPP 线路连接（例如路由器拨号连接）时，对应终端会显示 slip-ppp 提示信息（**banner slip-ppp**）。

【配置举例】 1：下面的示例进行 SLIP/PPP 提示信息的设置：

```
Ruijie(config)# banner slip-ppp $ 欢迎使用锐捷设备 $
```

【检验方法】 -

【提示信息】 -

【常见错误】 -

【平台说明】 -

2.8 configure

进入全局配置模式。

configure [**terminal**]

【参数说明】

参数	描述
-	-

【缺省配置】 -

【命令模式】 特权用户模式

【缺省级别】 14

【使用指导】 -

【配置举例】 1：进入全局配置模式

```
Ruijie# configure
Ruijie(config)#
```

【检验方法】 -

【提示信息】 -

【常见错误】 -

【平台说明】 -

2.9 disable

降低当前用户所在的级别。

disable [*privilege-level*]

【参数说明】

参数	描述
privilege-level	权限等级

【缺省配置】 -

【命令模式】 普通用户模式

【缺省级别】 0

【使用指导】 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。

【配置举例】 1：如下的示例配置设备将当前权限等级降低到第 10 级：

```
Ruijie# disable 10
```

【检验方法】 通过 **show privilege** 命令查看当前用户所在的级别

【提示信息】 -

【常见错误】 -

【平台说明】 -

2.10 disconnect

断开挂起的 Telnet Client 连接。

disconnect *session-id*

【参数说明】

参数	描述
session-id	挂起的 Telnet Client 连接会话号

【缺省配置】 -

【命令模式】 普通用户模式

【缺省级别】 1

【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。

【配置举例】 1：输入指定的 Telnet Client 连接会话号，断开指定的 Telnet Client 连接。

```
Ruijie# disconnect 1
```

【检验方法】 1：使用 **show sessions** 命令，可以查看指定的 Telnet Client 连接是否已经被断开。

【提示信息】 -

【常见错误】 -

【平台说明】 -

2.11 do telnet

登录到 Telnet 服务器。

do telnet [**oob**] *host* [*port*] [**/source** { **ip** *A.B.C.D* **| ipv6** *X:X:X:X::X* **| interface** *interface-name* }]

【参数说明】

参数	描述
oob	通过带外通信（一般指通过 MGMT 接口）远程连接到 Telnet 服务器，只有在设备具备 MGMT 管理口的时候才会有该选项
host	Telnet 服务器的 IPV4 地址、IPV6 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
ipv6 *X:X:X:X::X*	指定 Telnet 客户端使用的源 IPV6 地址
interface *interface-name*	指定 Telnet 客户端使用的源接口

【缺省配置】 -

【命令模式】 普通用户模式|特权模式|接口模式

【缺省级别】 1

【使用指导】 -

【配置举例】 **-**

【检验方法】 -

【提示信息】 -

【常见错误】 -

【平台说明】 NBR6205-E、NBR6135-E、NBR6210-E、NBR6215-E 支持 MGMT 口；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 MGMT 口。

2.12 enable

进入特权用户模式。

enable [*privilege-level*]

【参数说明】

参数	描述
privilege-level	权限等级

【缺省配置】 -

【命令模式】 普通用户模式

【缺省级别】 0

【使用指导】 使用该命令从普通用户模式进入到特权用户模式。如果加上权限等级，则将当前权限等级提升到指定的权限等级。

【配置举例】 1：如下的示例配置设备将当前权限等级降低到第 14 级：

```
Ruijie> enable 14

Password:
```

【检验方法】 通过 **show privilege** 命令查看当前用户所在的级别

【提示信息】 -

【常见错误】 -

【平台说明】 -

2.13 enable password

配置不同权限级别的口令。
enable password [**level** *level*] { [**0**] *password* | **7** *encrypted-password* }

删除指定级别的口令。
no enable password [**level** *level*]

【参数说明】

参数	描述
level	用户的权限级别
0	（可选）指定明文口令字符串
password	用户进入特权 EXEC 配置层的口令明文，字符串长度范围：1~126
7 encrypted-password	表示输入的口令字符串为密文字符串

【缺省配置】 -

【命令模式】 全局配置模式

【缺省级别】 15

【使用指导】 通常无须输入加密类型。一般情况下，只有当复制并粘贴由设备加密过的口令时，才需要输入加密类型。
有效口令定义如下：
必须包含 1 到 26 个大小写字母和数字字符。
口令前面可以有前导空格，但被忽略。中间及结尾的空格则作为口令的一部分。

⚠ 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。

【配置举例】 1：下面的示例设置口令为 pw10：

```
Ruijie(config)# enable password pw10
```

【检验方法】 -

【提示信息】 -

【常见错误】 -

【平台说明】 -

2.14 enable secret

配置不同权限级别的安全的口令。
enable secret [**level** *level*] { [**0**] *password* | **5** *encrypted-secret* }

删除指定级别的口令。
no enable secret [**level** *level*]

【参数说明】

参数	描述
level	用户的级别
0	（可选）指定明文口令字符串
password	用户进入特权 EXEC 配置层的口令明文，字符串长度范围：1~126
5 *encrypted-password*	用于指定已经过 MD5 不可逆加密的口令文本，配置后将作为加密后的口令进行保存

【缺省配置】 -

【命令模式】 全局配置模式

【缺省级别】 15

【使用指导】 Enable 认证口令分为 password 和 security 口令两种：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。

【配置举例】 1：下面的示例设置安全口令为 pw10：

```
Ruijie(config)# enable secret 0 pw10
```

【检验方法】 -

【提示信息】 -

【常见错误】 -

【平台说明】 -

2.15 enable service

打开与关闭指定的服务（SSH Server/Telnet Server/Web Server/Snmp Agent）。

enable service { **ssh-server** | **telnet-server** | **web-server** [**http | https | all**] | **snmp-agent** }

【参数说明】

参数	描述
ssh-server	打开与关闭 SSH Server。
telnet-server	打开与关闭 Telnet Server。
web-server [**http	https	all**]	打开与关闭 Web Server。
snmp-agent	打开与关闭 Snmp Agent。

【缺省配置】 默认 telnet-server、snmp-agent 和 web-server 是打开的，ssh-server 是关闭的。

【命令模式】 全局配置模式

【缺省级别】 14

【使用指导】 该命令用于打开与关闭指定的服务。使用 **no enable service** 命令关闭指定的服务。

enable service web-server 命令后面有 3 个可选关键字 [http | https | all]。如果执行该命令时后面不跟任

何关键字，或跟 all 关键字，则表示同时打开 http 服务和 https 服务；如果跟 http 关键字，则表示只打开 http 服务；如果跟 https 关键字，则表示只打开 https 服务。

【配置举例】 1：下面的示例命令 **enable service ssh-server** 打开 SSH Server 功能：

```
Ruijie(Config)# enable service ssh-server
```

【检验方法】 通过 **show service** 命令查看服务的开启或关闭情况

【提示信息】 -

【常见错误】 -

【平台说明】 -

2.16 end

从配置模式退出到特权模式

end

【参数说明】

参数	描述
-	-

【缺省配置】 -

【命令模式】 所有非特权模式

【缺省级别】 0

【使用指导】 在任何非特权模式下只要执行 end 命令即可退出到特权模式

【配置举例】 1：下面的示例命令 **end** 退出到特权模式：

```
Ruijie#con
Enter configuration commands, one per line.  End with CNTL/Z.
Ruijie(config)#line vty 0
Ruijie(config-line)#end
*May 20 09:49:38: %SYS-5-CONFIG_I: Configured from console by console
Ruijie#
```

【检验方法】 -

【提示信息】 -

【常见错误】 -

【平台说明】 -

2.17 exec-banner

在指定的 line 线路上重新激活显示 EXEC 提示信息
exec-banner

禁止在指定的 line 线路上显示 EXEC 提示信息
no exec-banner

【参数说明】

参数	描述
-	-

【缺省配置】 所有线路上激活 EXEC 提示信息

【命令模式】 LINE 配置模式

【缺省级别】 14

【使用指导】 配置了 **banner exec** 和 **banner motd**，则默认情况下，将在所有 line 线路上显示 EXEC 和 MOTD 提示信息。如果想在某条具体的 line 线路上关闭 EXEC 和 MOTD 提示信息，可以使用该命令的 **no** 形式在指定线路上关闭 EXEC 和 MOTD 的提示信息。

⚠ 该命令对 **banner incoming** 不起作用，即如果配置了 **banner incoming**，则在全部线路的反向 Telnet 连接中显示 incoming 提示信息，无法在指定线路上关闭 incoming 提示信息。

【配置举例】 1：下面的示例进行对 line 1 线路禁止提示欢迎信息的显示：

```
Ruijie(config)# line vty 1
Ruijie(config-line)no exec-banner
```

【检验方法】 配置后，用户登录系统，不显示所配置的信息。

【提示信息】 -

【常见错误】 -

【平台说明】 -

2.18 exec-timeout

配置 LINE 下的到此设备的连接超时时间。
exec-timeout *minutes* [*seconds*]

取消 LINE 下的连接超时，连接永不超时。
no exec-timeout

【参数说明】

参数	描述
minutes	指定的超时时间的分钟数，取值范围为 0-35791。
seconds	（可选）指定的超时时间的秒数，取值范围为 0-2147483。

【缺省配置】 缺省的超时时间为 10 min

【命令模式】 LINE 配置模式

【缺省级别】 14

【使用指导】 如果在指定的时间内，此连接没有任何输入输出信息，将中断此连接，并恢复此 LINE 为空闲可用状态。

【配置举例】 1：下面的示例指定 line vty 0 的连接超时时间为 5 分 30 秒：

```
Ruijie(config-line)# exec-timeout 5 30
```

【检验方法】 -

【提示信息】 -

【常见错误】 -

【平台说明】 -

2.19 exit

从配置模式退出到上级模式或者从特权模式退出 CLI 界面
exit

【参数说明】

参数	描述
-	-

【缺省配置】 -

【命令模式】 所有模式

【缺省级别】 0

【使用指导】 -

【配置举例】 1：下面的示例命令 **exit** 退出到上级模式：

```
Ruijie#con
Enter configuration commands, one per line.  End with CNTL/Z.
Ruijie(config)#line vty 0
Ruijie(config-line)#end
*May 20 09:49:38: %SYS-5-CONFIG_I: Configured from console by console
Ruijie#con
Enter configuration commands, one per line.  End with CNTL/Z.
Ruijie(config)#line vty 0
Ruijie(config-line)#exit
Ruijie(config)#exit
*May 20 09:51:48: %SYS-5-CONFIG_I: Configured from console by console
Ruijie#exit

Press RETURN to get started
```

【检验方法】 -

【提示信息】 -

【常见错误】 -

【平台说明】 -

2.20 help

查看帮助系统的一些简要信息。

help

【参数说明】

参数	描述
-	-

【缺省配置】 -

【命令模式】 任何配置模式

【缺省级别】 1

【使用指导】 使用该命令可以查看帮助系统的一些简要说明，在具体配置过程中，可以通"?"来查看当前配置模式下的所有命令或某个命令后所跟参数类型。

【配置举例】 1：下面的示例只显示一些帮助系统简要信息：

```
Ruijie#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?'.)
```

2：下面的示例显示接口配置模式下能运行的所有命令：

```
Ruijie(config-if-GigabitEthernet 0/0)#?
Interface configuration commands:
  arp              ARP interface subcommands
  bandwidth        Set bandwidth informational parameter
  carrier-delay    Specify delay for interface transitions
  dampening        Enable event dampening
  default          Set a command to its defaults
  description      Interface specific description
  dldp             Exec data link detection command
  duplex           Configure duplex operation
  efm              Config efm for an interface
  end              Exit from interface configuration mode
  exit             Exit from interface configuration mode
  expert           Expert extended ACL
  flowcontrol      Set the flow-control value for an interface
  full-duplex      Force full duplex operation
  global           Global ACL
  gvrp             GVRP configure command
  half-duplex      Force half duplex operation
```

```
  help             Description of the interactive help system
  ip               Interface Internet Protocol config commands
  l2               Config L2 attribute
  label-switching  Enable interface process mpls packet
  lldp             Link Layer Discovery Protocol
  load-interval    Specify interval for load calculation for an interface
  mac              Mac extended ACL
  mac-address      Set mac-address
  mpls             Multi-Protocol Label Switching
  mtu              Set the interface Maximum Transmission Unit (MTU)
  no               Negate a command or set its defaults
  ntp              Configure NTP
  port-group       Aggregateport/port bundling configuration
  redirect         Redirect packets
  rmon             Rmon command
  security         Configure the Security
  show             Show running system information
  shutdown         Shutdown the selected interface
  snmp             Modify SNMP interface parameters
  speed            Configure speed operation
  switchport       Set switching mode characteristics
  vrrp             VRRP interface subcommands
  xconnect         Xconnect commands
```

3：下面的示例显示命令后面所跟的参数类型：

```
Ruijie(config)#access-list 1 permit ?
  A.B.C.D  Source address
  any      Any source host
  host     A single source host
```

【检验方法】 -

【提示信息】 -

【常见错误】 -

【平台说明】 -

2.21 hostname

指定或修改设备的主机名。

hostname *name*

【参数说明】

参数	描述
name	设备的主机名，只能使用字符串、数字以及连接符。最大长度为 63 个字符。

【缺省配置】 缺省的主机名为 Ruijie。

【命令模式】 全局配置模式

【缺省级别】 14

【使用指导】 主机名主要用于识别设备以及在拨号和 CHAP 认证中作为本地设备的用户名。

【配置举例】 1：下面的示例指定设备的主机名为 BeiJing_Ruijie：

```
Ruijie(config)# hostname BeiJing_Ruijie
BeiJing_Ruijie(config)#
```

【检验方法】 -

【提示信息】 -

【常见错误】 -

【平台说明】 -

2.22 ip telnet source-interface

指定接口上的 IP 地址作为 Telnet 连接的源地址。

ip telnet source-interface *interface-name*

【参数说明】

参数	描述
interface-name	指定该接口上配置的 IP 地址作为 Telnet 连接的源地址，接口类型包括 AP 口、Gi 口、Loopback 口、null 口、VLAN 口。

【缺省配置】 -

【命令模式】 全局配置模式

【缺省级别】 14

【使用指导】 该命令用于指定接口上的 IP 地址作为全局 Telnet 连接的源地址。在使用 telnet 命令登录连接一台 Telnet 服务

器的时候，如果没有为该连接单独指定源接口或源地址，将使用该全局设置。
使用 **no ip telnet source-interface** 命令将设置恢复为默认值。

【配置举例】 1：下面的示例命令，指定 Loopback 1 接口上的 IP 地址作为全局 Telnet 连接的源地址：

```
Ruijie(config)# ip telnet source-interface Loopback 1
```

【检验方法】 -

【提示信息】 -

【常见错误】 -

【平台说明】 -

2.23 lock

在终端上设置一个暂时的口令。
lock

【参数说明】

参数	描述
-	-

【缺省配置】 -

【命令模式】 普通用户模式

【缺省级别】 1

【使用指导】 用户通过设置临时口令的方式，在保持连接会话的同时，锁住终端界面以防止访问。通过以下步骤锁住终端界面：

- 第一点：输入 **lock** 命令，系统会提示输入口令；
- 第二点：输入口令，可以是任意字符串。输入后，系统会提示确认输入的口令，然后，系统会清除屏幕，并显示“Locked”信息；
- 要想重新进入终端，需要输入设置的临时口令。

要在终端上使用锁住终端的功能，你需要通过在 line 配置模式下执行 **lockable** 命令，在相应的 line 上打开支持锁住终端的特性。

【配置举例】 1：下面的示例为锁住一个终端界面：

```
Ruijie(config-line)# lockable
Ruijie(config-line)# end
Ruijie# lock
```

```
Password: <password>
Again: <password>
Locked
Password: <password>
```

【检验方法】 -

【提示信息】 -

【常见错误】 -

【平台说明】 -

2.24 lockable

允许用户锁住当前线路所连接的终端。
lockable

取消设置。
no lockable

【参数说明】

参数	描述
-	-

【缺省配置】 终端在缺省情况下不支持 **lock** 命令。

【命令模式】 LINE 配置模式

【缺省级别】 1

【使用指导】 该命令用于在相应线路上支持锁住终端的特性，要锁住终端可以通过在 EXEC 模式下执行 **lock** 命令。
如果用户要执行 **lock** 命令来锁住当前线路连接的终端，就必须先使用命令 **lockable** 设置当前线路允许用户锁住当前线路连接的终端。

【配置举例】 1：下面的示例在控制台口上打开锁住终端的功能，并锁住控制台：

```
Ruijie(config)# line console 0
Ruijie(config-line)# lockable
Ruijie(config-line)# end
Ruijie# lock
Password: <password>
Again: <password>
```

```
Locked
Password: <password>
```

【检验方法】 -

【提示信息】 -

【常见错误】 -

【平台说明】 -

2.25 login

在 AAA 关闭的情况下，在 LINE 线路上配置简单的登录口令校验。
login

取消登录口令校验。
no login

【参数说明】

参数	描述
-	-

【缺省配置】 控制台默认关闭 login 功能， VTY 终端默认打开 login 功能。

【命令模式】 LINE 配置模式

【缺省级别】 14

【使用指导】 如果没有启用 AAA 安全服务 ,则该命令用于登录认证时作简单的口令校验。这里的口令是是指 VTY 或 console 接口中配置的口令。

【配置举例】 1：下面的示例演示在 VTY 上设置登录口令校验。

```
Ruijie(config)# no aaa new-model
Ruijie(config)# line vty 0
Ruijie(config-line)# password 0 normatest
Ruijie(config-line)# login
```

【检验方法】 -

【提示信息】 -

【常见错误】 -

【平台说明】 -

2.26 login access non-aaa

在 AAA 打开的情况下，配置该命令，在 LINE 线路上可以选择采用非 AAA 服务来进行认证。
login access non-aaa

禁止在 AAA 打开的情况下使用非 AAA 服务来进行认证。
no login access non-aaa

【参数说明】

参数	描述
-	-

【缺省配置】 默认关闭该功能。

【命令模式】 全局配置模式

【缺省级别】 14

【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。

【配置举例】 1：下面的示例演示在打开 AAA 安全服务的时候，在 VTY 上设置本地用户认证。

```
Ruijie(config)#log access non-aaa
Ruijie(config)#aaa new-model
Ruijie(config)#line vty 0 4
Ruijie(config-line)#login local
Ruijie(config-line)#
```

【检验方法】 -

【提示信息】 -

【常见错误】 -

【平台说明】 -

2.27 login authentication

在 AAA 打开的情况下，在 LINE 线路上配置 AAA 登录认证方法列表。
login authentication { **default** | *list-name* }

删除登录认证方法列表。
no login authentication { **default** | *list-name* }

【参数说明】

参数	描述
default	默认的认证方法列表名
list-name	可选的方法列表名

【缺省配置】 AAA 打开的情况下，默认使用 **default** 认证方法。

【命令模式】 LINE 配置模式

【缺省级别】 14

【使用指导】 -

【配置举例】 1：下面的示例演示在 VTY 上关联方法列表并用 radius 进行登录认证。

```
Ruijie(config)# aaa new-model
Ruijie(config)# aaa authentication login default group radius
Ruijie(config)# line vty 0
Ruijie(config-line)# login authentication default
```

【检验方法】 -

【提示信息】 -

【常见错误】 -

【平台说明】 -

2.28 login local

在 AAA 关闭的情况下，在 LINE 线路上配置本地用户认证。
login local

取消登录本地用户认证。

no login local

【参数说明】

参数	描述
-	-

【缺省配置】 -

【命令模式】 LINE 配置模式

【缺省级别】 14

【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。

【配置举例】 1：下面的示例演示在 VTY 上设置登录本地认证。

```
Ruijie(config)# no aaa new-model
Ruijie(config)# username test password 0 test
Ruijie(config)# line vty 0
Ruijie(config-line)# login local
```

【检验方法】 -

【提示信息】 -

【常见错误】 -

【平台说明】 -

2.29 motd-banner

在指定的 line 线路上重新激活显示 MOTD 提示信息
motd-banner

禁止在指定的 line 线路上显示 MOTD 提示信息
no motd-banner

【参数说明】

参数	描述
-	-

【缺省配置】 所有线路上激活 MOTD 提示信息。

【命令模式】 LINE 配置模式

【缺省级别】 14

【使用指导】 配置了 **banner exec** 和 **banner motd**，则默认情况下，将在所有 line 线路上显示 EXEC 和 MOTD 提示信息。如果想在某条具体的 line 线路上关闭 EXEC 和 MOTD 提示信息 ,可以使用该命令的 **no** 形式在指定线路上关闭 EXEC 和 MOTD 的提示信息。

⚠ 该命令对 **banner incoming** 不起作用，即如果配置了 **banner incoming**，则在全部线路的反向 Telnet 连接中显示 incoming 提示信息，无法在指定线路上关闭 incoming 提示信息。

【配置举例】 1：下面的示例进行对 Vty1 线路禁止提示 MOTD 信息的显示：

```
Ruijie(config)# line vty 1
Ruijie(config-line)no motd-banner
```

【检验方法】 配置后，用户登录系统，不显示所配置的信息。

【提示信息】 -

【常见错误】 -

【平台说明】 -

2.30 password

配置 line 线路登录口令。

password { [**0**] *password* | ***7*** *encrypted-password* }

删除 line 登录口令。

no password

【参数说明】

参数	描述
0	（可选）指定明文口令字符串
password	指定远程用户 line 线路的口令明文，字符串长度范围：1~25
7 *encrypted-password*	表示输入的口令字符串为密文字符串

【缺省配置】 -

【命令模式】 LINE 配置模式

【缺省级别】 14

【使用指导】 -

【配置举例】 1：下面的示例指定 line 登录口令为 red：

```
Ruijie(config)# line vty 0
Ruijie(config-line)# password red
```

【检验方法】 -

【提示信息】 -

【常见错误】 -

【平台说明】 -

2.31 prompt

配置用户命令接口（CLI）的提示。
prompt *string*

取消用户命令接口（CLI）提示符的配置。
no prompt

【参数说明】

参数	描述
string	命令提示符字符串，最长可以配置 32 个字符

【缺省配置】 -

【命令模式】 全局配置模式

【缺省级别】 14

【使用指导】 如果你没有配置命令接口（CLI）的提示符，则以系统名称作为提示符，提示符将随着系统名称的变化而变化。
命令接口（CLI）提示符只对 EXEC 模式有效。

【配置举例】 1：下面的示例将配置命令提示符为 RGOS：

```
Ruijie(config)# prompt RGOS
Ruijie(config)# end
RGOS
```

【检验方法】 -

【提示信息】 -

【常见错误】 -

【平台说明】 -

2.32 secret

配置 line 线路登录 MD5 不可逆加密口令。
secret { [**0**] *password* | **5** *encrypted-secret* }

删除 line 线路登录 MD5 不可逆加密口令。
no secret

【参数说明】

0	（可选）指定明文口令文本，配置后将进行 MD5 不可逆加密
password	指定远程用户 line 线路的口令明文，字符串长度：1~25
5 *encrypted-secret*	用于指定已经过 MD5 不可逆加密的口令文本，配置后将作为加密后的口令进行保存

【缺省配置】 -

【命令模式】 line 配置模式

【缺省级别】 14

【使用指导】 该命令用于配置对远程用户试图登录 line 线路进行认证的 MD5 不可逆加密口令。

⚠ 如果指定加密类型为 5，则输入的合法密文长度必须为 24，并且口令文本的第 1、3、8 个字符必须是"$"字符。

⚠ 通常无须指定加密类型为 5。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 5。

⚠ line 下可以同时配置 password 和 secret 口令，当系统上配置了 password 和 secret 两种口令时，用户登录时输入口令，会优先匹配 secret 口令，若 secret 口令匹配失败时，会继续匹配 password 口令，当两种口令都匹配失败的情况下，用户登录失败。

【配置举例】 下面的示例指定 line 登录 MD5 不可逆加密口令为 vty0：

```
Ruijie(config)# line vty 0
```

```
Ruijie(config-line)# secret vty0
```

配置此口令之后，vty0 将进行 MD5 不可逆加密，show 出来的效果如下所示：

```
secret 5 $1$X834$wvx6y794uAD8svzD
```

【检验方法】 -

【提示信息】 -

【常见错误】 -

【平台说明】 -

2.33 session-timeout

配置当前 LINE 上已经建立的到远程终端的会话的超时时间。
session-timeout *minutes* [**output**]

取消 LINE 下到远程终端的会话的超时时间，会话永不超时。
no session-timeout

【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

【缺省配置】 缺省的超时时间为 0 min，代表永不超时。

【命令模式】 LINE 配置模式

【缺省级别】 14

【使用指导】 如果在指定的时间内，从当前 LINE 上已经建立的到远程终端的会话，没有任何输入输出信息，将中断此连接，并恢复此 LINE 为空闲可用状态。

【配置举例】 1：下面的示例指定 line vty 0 的会话超时时间为 5 分钟：

```
Ruijie(config-line)# session-timeout 5 output
```

【检验方法】 -

【提示信息】 -

【常见错误】 -

【平台说明】 -

2.34 show debugging

显示当前设备的调试开关打开信息。

show debugging

【参数说明】

参数	描述
-	-

【命令模式】 特权用户模式

【缺省级别】 15

【使用指导】 -

【配置举例】 1：下面的示例是执行 **show debugging** 命令的一个示例：

```
Ruijie#show debugging


debug fw-group detect intf-state
```

【提示信息】 -

【平台说明】 -

2.35 show hostname

显示当前设备的主机名称信息。

show hostname

【参数说明】

参数	描述
-	-

【命令模式】 特权用户模式

【缺省级别】 15

【使用指导】 -

【配置举例】 1：下面的示例是执行 **show hostname** 命令的一个示例，示例显示该设备的主机名称为 Ruijie：

```
Ruijie#show hostname
Ruijie
Ruijie#
```

【提示信息】 -

【平台说明】 -

2.36 show line

查看线路的配置信息。

show line { **console** *line-num* | **vty** *line-num* **|** *line-num* }

【参数说明】

参数	描述
console	查看控制台线路的配置信息。
vty	查看虚终端线路的配置信息。
line-num	查看的 line 线路。

【命令模式】 特权用户模式

【缺省级别】 14

【使用指导】 -

【配置举例】 1：查看 console 口的配置信息。

```
Ruijie# show line console 0
CON     Type    speed   Overruns
* 0     CON     9600    45927
Line 0, Location: "", Type: "vt100"
Length: 24 lines, Width: 79 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: 53564 bytes
Total output:  395756 bytes
Data overflow:  27697 bytes
stop rx interrupt:  0 times
```

字段解释：

字段	说明
CON	终端类型，CON 表示为控制台。0 表示为终端线路编号，编号前面加*号表示当前正在使用的终端。
Type	终端类型，包括 CON、VTY 等。
speed	异步速率。
Overruns	驱动接收的 overrun 错误数量统计值。
Line 0	终端线路编号。
Location: ""	线路 location 设置。
Type: "vt100"	线路兼容终端标准。
Special Chars	终端特殊字符，包括 Escape 字符、Disconnect 字符和 Activation 字符。
Timeouts	终端超时时间，never 表示永不超时。
History	历史命令记录开关以及最大条目数。
Total input	从驱动接收的数据量统计值。
Total output	发送到驱动的数据量统计值。
Data overflow	接收溢出的数据量统计值。
stop rx interrupt	驱动 RX 中断数量统计值。

【提示信息】 -

【平台说明】 -

2.37 show reload

查看系统的重新启动设置。

show reload

【参数说明】

参数	描述
-	-

【命令模式】 特权用户模式

【缺省级别】 1

【使用指导】

【配置举例】 1：下面的示例查看系统重新启动的设置：

```
Ruijie# show reload
System reload state: Warm
```

字段解释：

字段	说明
System reload state	系统重机的状态

【提示信息】 -

【平台说明】 -

2.38 show running-config

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 running-config [**interface** *interface*]

【参数说明】

参数	描述
-	-

【命令模式】 特权用户模式

【缺省级别】 14

【使用指导】 -

【配置举例】 -

【提示信息】 -

【平台说明】 -

2.39 show service

查看当前服务的开启或关闭情况。

show service

【参数说明】

参数	描述
-	-

【命令模式】 特权用户模式

【缺省级别】 1

【使用指导】 -

【配置举例】 1：查看当前服务的开启或关闭情况。

```
Ruijie# show service
web-server   : disabled
web-server(https): disabled
snmp-agent    : enabled
ssh-server    : enabled
telnet-server : disabled
```

【提示信息】 -

【平台说明】 -

2.40 show sessions

显示已经建立的 Telnet Client 实例的每个实例信息。

show sessions

【参数说明】

参数	描述
-	-

【命令模式】 普通用户模式

【缺省级别】 1

【使用指导】 显示已经建立的 Telnet Client 实例的每个实例信息，包括：连接所占用的 VTY 号、服务器地址。

【配置举例】 1：显示已建立的 Telnet Client 会话连接信息。

```
Ruijie#show sessions
Conn  Address
*1    127.0.0.1
*2    192.168.21.122
```

【提示信息】 -

【平台说明】 -

2.41 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 startup-config

【参数说明】

参数	描述
-	-

【命令模式】 特权用户模式

【缺省级别】 14

【使用指导】 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。

在锐捷设备上，startup-config 指的是保存于设备内置 Flash 中的默认配置文件“/config.text”中的配置信息。

【配置举例】 -

【提示信息】 -

【平台说明】 -

2.42 show this

查看系统当前模式下生效的配置信息。

show this

【参数说明】

参数	描述
-	-

【命令模式】 所有配置模式

【缺省级别】 14

【使用指导】 在 range 模式下可以显示当前模式的配置。包括：

1. 通过 **line** *first-line last-line* 命令指定配置一个范围的线路，并进入 LINE 配置模式；
2. 通过 **vlan range** 命令指定配置多个 VLAN，并进入 vlan range 配置模式；
3. 通过 **interface range** 命令指定配置多个接口，并进入 interface range 配置模式；

在上述情况下，使用该命令将可以显示当前模式下生效的配置信息。

在 **vlan range** 或者 **interface range** 模式下，如果操作的 vlan 或者 interface 数量超过 50 个，则执行该命令只会显示前 50 个 vlan 或者 interface 的配置。

【配置举例】 1：下面的示例查看 interface fastEthernet 0/1 下生效的配置信息

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

2：下面的示例查看 interface range vlan 1-3 下生效的配置信息

```
Ruijie(config-if-range)#show this

Building configuration...
!
interface VLAN 1
 ip address dhcp
interface VLAN 2
 ip address 1.1.1.1 255.255.255.0
interface VLAN 3
 ip address 3.3.3.3 255.255.255.0
!
end
Ruijie(config-if-range)#
```

【提示信息】 -

【平台说明】 -

2.43 speed

配置终端设备的速率。

speed *speed*

恢复终端设备速率的默认配置。

no speed

【参数说明】

参数	描述
speed	终端设备的传输速率，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。

【缺省配置】 缺省的速率是 9600

【命令模式】 LINE 配置模式

【缺省级别】 14

【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】 1: 下面的示例将串口速率设置为 57600 bps：

```
Ruijie(config)# line console 0
Ruijie(config-line)# speed 57600
```

【检验方法】 通过 **show line** 命令查看 LINE 线路所配置的速率。

【提示信息】 -

【常见错误】 -

【平台说明】 -

2.44 telnet

登录到 Telnet 服务器。

telnet [**oob**] *host* [*port*] [**/source** { **ip** *A.B.C.D* **| ipv6** *X:X:X:X::X* **| interface** *interface-name }*]

【参数说明】

参数	描述
oob	通过带外通信（一般指通过 MGMT 接口）远程连接到 Telnet 服务器，只有在设备具备 MGMT 管理口的时候才会有该选项
host	Telnet 服务器的 IPV4 地址、IPV6 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
ipv6 *X:X:X:X::X*	指定 Telnet 客户端使用的源 IPV6 地址
interface *interface-name*	指定 Telnet 客户端使用的源接口

【缺省配置】 -

【命令模式】 普通用户模式

【缺省级别】 1

【使用指导】 -

【配置举例】 -

【检验方法】 -

【提示信息】 -

【常见错误】 -

【平台说明】 NBR6205-E、NBR6135-E、NBR6210-E、NBR6215-E 支持 MGMT 口；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 MGMT 口。

2.45 username

配置本地用户账号以及可选的授权信息。
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*]

删除本地用户。
no username *name*

【参数说明】

参数	描述
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。

【缺省配置】 -

【命令模式】 全局配置模式

【缺省级别】 15

【使用指导】 该命令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。

【配置举例】 1：下面的示例配置一个用户名和口令，并绑定用户级别为 15 级：

```
Ruijie(config)# username test privilege 15 password 0 pw15
```

2：下面的示例配置给 web 认证专用的用户名和口令：

```
Ruijie(config)# username user1 web-auth password 0 pw
```

3：下面的示例配置用户 test 具有所有文件和目录的读写权限：

```
Ruijie(config)# username test permission rw /
```

4：下面的示例配置用户 test 除了 config.text 文件，其它文件和目录具有读、写、执行权限：

```
Ruijie(config)# username test permission n /config.text
Ruijie(config)# username test permission rwx /
```

【检验方法】 -

【提示信息】 -

【常见错误】 -

【平台说明】 -

2.46 username export

把用户信息导出到文件。

username export *filename*

【参数说明】

参数	描述
filename	文件名

【缺省配置】 -

【命令模式】 特权用户模式

【缺省级别】 1

【使用指导】 该命令用于把用户信息导出到文件。

【配置举例】 1：下面的示例配置导入用户信息:

```
Ruijie# username export user.csv
```

【检验方法】 -

【提示信息】 -

【常见错误】 -

【平台说明】 -

2.47 username import

从文件导入用户信息。

username import *filename*

【参数说明】

参数	描述
filename	文件名

【缺省配置】 -

【命令模式】 特权用户模式

【缺省级别】 1

【使用指导】 该命令用于从外部导入用户信息。

【配置举例】 1：下面的示例配置导入用户信息:

```
Ruijie# username import user.csv
```

【检验方法】 -

【提示信息】 -

【常见错误】 -

【平台说明】 -

2.48 write

将系统配置（running-config）保存到指定位置。

write [**memory** | **terminal**]

【参数说明】

参数	描述
memory	将系统配置写入 NVRAM，等同于 **copy running-config startup-config。**
terminal	显示系统配置，等同于 show running-config。

【缺省配置】 -

【命令模式】 特权用户模式

【缺省级别】 14

【使用指导】 该命令虽然有替代命令，但由于其广泛的使用和被大家认可，所以依然保留下来方便用户使用。
如果该文件所处的设备存在，系统将自动创建指定文件并写入系统配置；如果该文件所处的设备不存在（可能的情况为：启动配置文件被指定在如 U 盘之类的可移动存储设备上，而在执行 **write** [**memory**]命令时该设备尚未被加载），则系统将询问是否要将当前配置保存于默认启动配置文件“/config.text”中，并根据用户的回答执行相应的操作。

【配置举例】 1：以下示范如何在设备上保存系统配置：

```
Ruijie# write
Building configuration...
[OK]
```

【检验方法】 -

【提示信息】 -

【常见错误】 -

【平台说明】 -

3 LINE

3.1 access-class

通过 ACL 过滤（IPv4）控制终端登录。

access-class { *access-list-number* | *access-list-name* } { **in** | **out** }

取消 ACL 过滤（IPV4）控制终端登录。

no access-class { *access-list-number* | *access-list-name* } { **in** | **out** }

【参数说明】

参数	描述
access-list-number	ACL 编号 ,可配范围 :IP 标准 ACL(1-99 ,1300-1999) ;IP 扩展 ACL(100-199，2000-2699)。
access-list-name	ACL 名称。
in	过滤进来的连接。
out	过滤外出的连接。

【缺省配置】 -

【命令模式】 LINE 配置模式

【缺省级别】 14

【使用指导】 -

【配置举例】 1：配置对编号范围为 0-5 的 VTY 进来的连接进行编号为 20 的 ACL 过滤。

```
Ruijie(config)# line vty 0 5
Ruijie(config-line)#access-class 20 in
```

2：配置对编号范围为 6-7 的 VTY 出去的连接进行 ACL 名称为 test 的 ACL 过滤。

```
Ruijie(config)# line vty 6 7
Ruijie(config-line)#access-class test out
```

【检验方法】 -

【提示信息】 -

【常见错误】 -

【平台说明】 -

3.2 accounting commands

开启 line 线路上命令活动记账功能。

accounting commands *level* { **default** | *list-name* }

取消命令活动记账功能。

no accounting commands *level*

【参数说明】

参数	描述
level	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	默认的认证方法列表名。
list-name	可选的方法列表名。

【缺省配置】 关闭线路上的记账功能。

【命令模式】 LINE 配置模式

【缺省级别】 14

【使用指导】 与 AAA 认证结合使用，先配置 AAA 命令记账方法后，再应用在需要进行命令记账的终端线路上。

【配置举例】 1：开启 Vty 1 线路上的命令活动记账功能，要求记账的命令级别为 15 级。

```
Ruijie(config)# aaa new-model
Ruijie(config)# aaa accounting commands 15 default start-stop group tacacs+
Ruijie(config)# line vty 1
Ruijie(config-line)# accounting commands 15 default
```

【检验方法】 -

【提示信息】 -

【常见错误】 -

【平台说明】 -

3.3 accounting exec

开启 line 线路上的用户访问活动记账功能。

accounting exec { **default** | *list-name* }

取消 Exec 记账功能。
no accounting exec

【参数说明】

参数	描述
default	默认的认证方法列表名。
list-name	可选的方法列表名。

【缺省配置】 关闭线路上的记账功能

【命令模式】 LINE 配置模式

【缺省级别】 14

【使用指导】 与 AAA 认证结合使用，先配置 AAA Exec 记账方法后，再应用在需要进行 Exec 记账的终端线路上。

【配置举例】 1：开启 Vty 1 线路用户访问活动记账功能。

```
Ruijie(config)# aaa new-model
Ruijie(config)# aaa accounting exec default start-stop group radius
Ruijie(config)# line vty 1
Ruijie(config-line)# accounting exec default
```

【检验方法】 -

【提示信息】 -

【常见错误】 -

【平台说明】 -

3.4 authorization commands

开启线路上的命令授权功能。
authorization commands *level* { **default** | *list-name* }

取消命令授权功能。
no authorization commands *level*

【参数说明】

参数	描述
level	要进行授权的命令级别，范围 0~15，决定哪个级别的命令需要授权通过后才能执行。

default	默认的认证方法列表名。
list-name	可选的方法列表名。

【缺省配置】 关闭命令授权功能。

【命令模式】 LINE 配置模式

【缺省级别】 14

【使用指导】 与 AAA 认证结合使用，先配置 AAA 命令授权方法后，再应用在需要进行命令授权的终端线路上。

【配置举例】 1：对 Vty 1 线路上用户执行的 15 级命令进行授权。

```
Ruijie(config)# aaa new-model
Ruijie(config)# aaa authorization commands 15 default group tacacs+
Ruijie(config)# line vty 1
Ruijie(config-line)# authorization commands 15 default
```

【检验方法】 -

【提示信息】 -

【常见错误】 -

【平台说明】 -

3.5 authorization exec

开启线路上的 Exec 授权功能。
authorization exec { **default** | *list-name* }

取消 Exec 授权功能。
no authorization exec

【参数说明】

参数	描述
default	默认的认证方法列表名。
list-name	可选的方法列表名。

【缺省配置】 关闭 Exec 授权功能。

【命令模式】 LINE 配置模式

【缺省级别】 14

【使用指导】 与 AAA 认证结合使用，先配置 AAA Exc 授权方法后，再应用在需要进行 Exec 授权的终端线路上。

【配置举例】 1：对 Vty 1 线路进行 Exec 授权。

```
Ruijie(config)# aaa new-model
Ruijie(config)# aaa authorization exec default group radius
Ruijie(config)# line vty 1
Ruijie(config-line)# authorization exec default
```

【检验方法】 -

【提示信息】 -

【常见错误】 -

【平台说明】 -

3.6 clear line

清除线路的连接状态。

clear line { **console** *line-num* | **vty** *line-num* **|** *line-num* }

【参数说明】

参数	描述
console	清除控制台线路的连接状态。
vty	清除虚终端线路的连接状态。
line-num	清除的 line 线路。

【命令模式】 特权用户模式

【缺省级别】 14

【使用指导】 使用 **clear line** 命令清除线路的连接状态，将会强制断开已经连接上的终端。并将线路恢复到未占用状态，可以重新建立终端连接。

【配置举例】 1：清除 LINE VTY 13 的连接状态，如果该 VTY 上已经有客户端（例如 Telnet、SSH 等）连接会话，则会立刻断开连接。

```
Ruijie# clear line vty 13
```

【检验方法】 -

【提示信息】 -

【常见错误】 -

【平台说明】 -

3.7 disconnect-character

设置断开终端服务连接的热键。
disconnect-character *ascii-value*

恢复默认缺省设置。
no disconnect-character

【参数说明】

参数	描述
ascii-value	断开终端服务连接的热键的 ASCII 码对应的十进制值，取值范围为 0-255。

【缺省配置】 缺省情况下，系统设置终端服务连接断开的热键为 **Ctrl+D**，也就是 0x04 对应的组合键。

【命令模式】 LINE 配置模式

【缺省级别】 14

【使用指导】 本命令设置的是终端服务连接断开的热键，用户可以根据需要设置断开终端服务连接的热键。终端服务连接断开热键不能是常用 ASCII 码(如‘a’～‘z’，‘A’～‘Z’以及‘0’～‘9’等等)，否则将导致终端服务不能正常通讯。

【配置举例】 1：设置在 Vty0-5 上断开终端服务连接的热键为 Ctrl+E(其 ASCII 值为 0x05)。

```
Ruijie(config)# line vty 0 5
Ruijie(config-line)# disconnect-character 5
```

【检验方法】 -

【提示信息】 -

【常见错误】 -

【平台说明】 -

3.8 escape-character

设置线路上退出字符。
escape-character *escape-value*

恢复系统缺省设置。
no escape-character

【参数说明】

参数	描述
escape-value	用户自定义的退出字符的 ASCII 码对应的十进制值，取值范围为 0-255。

【缺省配置】 缺省情况下 ,线路上已经设置退出字符并且其 *escape-value* 值为 30 ,也就是 **Ctrl+^**(组合键为 **Ctrl+Shift+6**)。

【命令模式】 LINE 配置模式

【缺省级别】 14

【使用指导】 如果设置了 **escape-character** *escape-value* 命令 ,用户就可以使用 *escape-value* 对应的组合键然后紧接着键入“**x** ”，就可以中断当前会话回到创建该会话的原始会话上去。

【配置举例】 1：设置 Vty 0 线路上的退出字符为 23(对应的组合键为(**Ctrl+w**))。

```
Ruijie(config)# line vty 0
Ruijie(config-line)# escape-character 23
```

【检验方法】 -

【提示信息】 -

【常见错误】 -

【平台说明】 -

3.9 exec

允许 line 线路进入命令行界面。
exec

限制 line 线路进入命令行界面。
no exec

【参数说明】

参数	描述
-	-

【缺省配置】 缺省允许线路进入命令行界面。

【命令模式】 LINE 配置模式

【缺省级别】 14

【使用指导】 若不允许 line 线路进入命令行界面，可以配置 no exec，则用户登录时不能通过所配置的线路进入命令行界面，而是通过其他未限制线路进入命令行界面。

【配置举例】 1：限制 1 线路进入命令行界面。

```
Ruijie(config)# line vty 1
Ruijie(config-line)# no exec
Ruijie# show users
Line             User         Host(s)              Idle       Location
---------------- ------------ -------------------- ---------- -------------------
*  0 con 0       ---          idle                 00:00:00   ---
   1 vty 0       ---          idle                 00:01:03   20.1.1.2
   3 vty 2       ---          idle                 00:00:13   20.1.1.2
```

【检验方法】 -

【提示信息】 -

【常见错误】 -

【平台说明】 -

3.10 history

开启 line 线路历史命令记录功能，或者配置 line 线路历史命令记录的条目数。
history [**size** *size*]

取消 line 线路历史命令记录功能。
no history

恢复 line 线路历史命令记录的条目数
no history size

【参数说明】

参数	描述
size *size*	条目数，取值范围：0~256。

【缺省配置】 缺省情况下开启历史命令记录功能，最大历史命令记录的条目数为 10

【命令模式】 LINE 配置模式

【缺省级别】 14

【使用指导】 -

【配置举例】 1：配置 0-5 的 line 线路的历史记录条目数为 20。

```
Ruijie(config)# line vty 0 5
Ruijie(config-line)# history size 20
```

2：关闭 0-5 的 line 线路的历史记录功能。

```
Ruijie(config)# line vty 0 5
Ruijie(config-line)# no history
```

【检验方法】 -

【提示信息】 -

【常见错误】 -

【平台说明】 -

3.11 length

设置指定的线路终端上的单屏最大行数。
length *screen-length*

恢复缺省设置。
no length

【参数说明】

参数	描述
screen-ength	行高值，取值范围为 0-512。

【缺省配置】 缺省情况下，单屏最大行数为 24 行。

【命令模式】 LINE 配置模式

【缺省级别】 14

【使用指导】 -

【配置举例】 1：设置指定线路的单屏最大行数为 10 行。

```
Ruijie(config-line)# length 10
```

【检验方法】 -

【提示信息】 -

【常见错误】 -

【平台说明】 -

3.12 line

进入到指定的 LINE 模式。

line [**console** | **vty**] *first-line* [*last-line*]

【参数说明】

参数	描述
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。

【缺省配置】 -

【命令模式】 全局配置模式

【缺省级别】 14

【使用指导】 -

【配置举例】 1：进入到 LINE VTY 1 到 3 的 LINE 模式。

```
Ruijie(config)# line vty 1 3
```

【检验方法】 -

【提示信息】 -

【常见错误】 -

【平台说明】 -

3.13 line vty

增加当前可以使用的 VTY 连接数目。
line vty *line-number*

减少当前可以使用的 VTY 连接数目。
no line vty *line-number*

【参数说明】

参数	描述
line-number	VTY 连接数目，范围：0~35。

【缺省配置】 -

【命令模式】 全局配置模式

【缺省级别】 14

【使用指导】 -

【配置举例】 1：将可用的 VTY 连接数目增加到 20，可用 VTY 编号范围为 0-19。

```
Ruijie(config)# line vty 19
```

2：将可用的 VTY 连接数目减少到 10，可用 VTY 编号范围为 0-9。

```
Ruijie(config)# no line vty 10
```

【检验方法】 -

【提示信息】 -

【常见错误】 -

【平台说明】 -

3.14 location

设置指定线路的位置描述。
location *location*

恢复系统缺省设置。
no location

【参数说明】

参数	描述
location	当前线路的位置描述。

【缺省配置】 -

【命令模式】 LINE 配置模式

【缺省级别】 14

【使用指导】 -

【配置举例】 1：设置指定线路的位置描述为 Swtich’s Line Vty 0。

```
Ruijie(config)# line vty 0
Ruijie(config-line)# location Swtich’s Line Vty 0
```

【检验方法】 -

【提示信息】 -

【常见错误】 -

【平台说明】 -

3.15 monitor

支持在终端上打开日志显示。
monitor

取消在终端上打开日志显示。
no monitor

【参数说明】

参数	描述

-	-

【缺省配置】 -

【命令模式】 LINE 配置模式

【缺省级别】 14

【使用指导】 -

【配置举例】 1：支持 0-5 的 line 线路上终端打印日志。

```
Ruijie(config)# line vty 0 5
Ruijie(config-line)# monitor
```

【检验方法】 -

【提示信息】 -

【常见错误】 -

【平台说明】 -

3.16 privilege level

配置 line 线路登录级别。
privilege level *level*

恢复 line 线路登录级别。
no privilege level

【参数说明】

参数	描述
level	权限级别，取值范围为 0-15。

【缺省配置】 缺省情况下，privilege level 为 1。

【命令模式】 LINE 配置模式

【缺省级别】 14

【使用指导】 -

【配置举例】 1：将 0-4 的 VTY line 线路的登录权限级别设置为 14。

```
Ruijie(config)# line vty 0 4
Ruijie(config-line)#privilege level 14
```

【检验方法】 -

【提示信息】 -

【常见错误】 -

【平台说明】 -

3.17 refuse-message

配置 line 线路拒绝登录提示信息。
refuse-message [*c message c*]

取消 line 线路拒绝登录提示信息。
no refuse-message

【参数说明】

参数	描述
c	拒绝登录提示信息的分隔符 ,拒绝登录提示信息内容中间不允许出现间隔符。
message	拒绝登录提示信息。

【缺省配置】 -

【命令模式】 LINE 配置模式

【缺省级别】 14

【使用指导】 使用该命令可以配置退出登录提示信息，如果键入结束的分隔符后仍然输入字符，则这些字符将被系统丢弃。当用户被拒绝登录设备时，窗口会提示当前线路拒绝用户登录的提示信息。

【配置举例】 1：配置 line 线路退出登录提示信息为非法用户限制登录锐捷设备。

```
Ruijie(config-line)#refuse-message @ 非法用户限制登录锐捷设备 @
```

【检验方法】 -

【提示信息】 -

【常见错误】 -

【平台说明】 -

3.18 show history

显示当前 line 线路的历史记录命令。

show history

【参数说明】

参数	描述
-	-

【命令模式】 特权用户模式

【缺省级别】 14

【使用指导】 -

【配置举例】 显示当前 line 线路记录的历史命令。

```
Ruijie# show history
exec:
sh privilege
sh run
show user
sh user all
show history
```

【检验方法】 -

【提示信息】 -

【常见错误】 -

【平台说明】 -

3.19 show line

查看线路的配置信息。

show line { **console** *line-num* | **vty** *line-num* **|** *line-num* }

【参数说明】

参数	描述

console	查看控制台线路的配置信息。
vty	查看虚终端线路的配置信息。
line-num	查看的 line 线路。

【命令模式】 特权用户模式

【缺省级别】 14

【使用指导】 -

【配置举例】 1：查看 console 口的配置信息。

```
Ruijie# show line console 0
CON     Type    speed   Overruns
* 0     CON     9600    45927
Line 0, Location: "", Type: "vt100"
Length: 24 lines, Width: 79 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: 53564 bytes
Total output:  395756 bytes
Data overflow:  27697 bytes
stop rx interrupt:  0 times
```

字段解释：

字段	说明
CON	终端类型，CON 表示为控制台。0 表示为终端线路编号，编号前面加*号表示当前正在使用的终端。
Type	终端类型，包括 CON、VTY 等。
speed	异步速率。
Overruns	驱动接收的 overrun 错误数量统计值。
Line 0	终端线路编号。
Location: ""	线路 location 设置。
Type: "vt100"	线路兼容终端标准。
Special Chars	终端特殊字符，包括 Escape 字符、Disconnect 字符和 Activation 字符。
Timeouts	终端超时时间，never 表示永不超时。
History	历史命令记录开关以及最大条目数。
Total input	从驱动接收的数据量统计值。
Total output	发送到驱动的数据量统计值。
Data overflow	接收溢出的数据量统计值。

stop rx interrupt	驱动 RX 中断数量统计值。

【提示信息】 -

【平台说明】 -

3.20 show privilege

显示当前 line 线路权限级别。

show privilege

【参数说明】

参数	描述
-	-

【命令模式】 特权用户模式

【缺省级别】 1

【使用指导】 -

【配置举例】 显示当前 line 线路权限级别。

```
Ruijie# show privilege
Current privilege level is 10
```

【提示信息】 -

【平台说明】 -

3.21 show users

显示线路登录用户信息。

show users [**all**]

【参数说明】

参数	描述
all	显示所有可登录的线路用户信息，包含当前已登录的线路用户信息，以及未登录的线路用户信息。

【命令模式】 特权用户模式

【缺省级别】 14

【使用指导】 -

【配置举例】 1：显示当前已登录的线路用户信息。

```
Ruijie# show users
Line             User         Host(s)              Idle       Location
---------------- ------------ -------------------- ---------- -------------------
   0 con 0       ---          idle                 00:00:46   ---
   1 vty 0       ---          idle                 00:00:29   20.1.1.2
*  2 vty 1       ---          idle                 00:00:00   20.1.1.2
```

2：显示所有的线路用户信息。

```
Ruijie(config)# show users all
Line             User         Host(s)              Idle       Location
---------------- ------------ -------------------- ---------- -------------------
   0 con 0       ---          idle                 00:00:49   ---
   1 vty 0       ---          idle                 00:00:32   20.1.1.2
*  2 vty 1       ---          idle                 00:00:00   20.1.1.2
   3 vty 2       ---                               00:00:00   ---
   4 vty 3       ---                               00:00:00   ---
   5 vty 4       ---                               00:00:00   ---
   6 vty 5       ---                               00:00:00   ---
```

【提示信息】 -

【平台说明】 -

3.22 speed

设置指定的线路终端上的波特率。

speed *baudrate*

恢复缺省设置。

no speed

【参数说明】

参数	描述
baudrate	波特率值，取值范围为 9600-115200。

【缺省配置】 缺省情况下，波特率为 9600。

【命令模式】 LINE 配置模式

【缺省级别】 14

【使用指导】 -

【配置举例】 1：设置指定线路的波特率为 115200。

```
Ruijie(config-line)# speed 115200
```

【检验方法】 -

【提示信息】 -

【常见错误】 -

【平台说明】 -

3.23 terminal escape-character

设置当前终端的退出字符。

terminal escape-character *escape-value*

恢复当前终端的系统缺省设置。

terminal no escape-character

【参数说明】

参数	描述
escape-value	用户自定义的退出字符的 ASCII 码对应的十进制值，取值范围为 0-255。

【缺省配置】 缺省情况下 ,线路上已经设置退出字符并且其 *escape-value* 值为 30 ,也就是 **Ctrl+^**(组合键为 **Ctrl+Shift+6**)。

【命令模式】 特权用户模式

【缺省级别】 14

【使用指导】 如果设置了 **escape-character** *escape-value* 命令 ,用户就可以使用 *escape-value* 对应的组合键然后紧接着键入“**x** ” ，就可以中断当前会话回到创建该会话的原始会话上去。

【配置举例】 1：设置当前终端的退出字符为 23(对应的组合键为(**Ctrl+w**))。

```
Ruijie# terminal escape-character 23
```

【检验方法】 -

【提示信息】 -

【常见错误】 -

【平台说明】 -

3.24 terminal history

在当前终端开启 line 线路历史命令记录功能，或者配置 line 线路历史命令记录的条目数。
terminal history [**size** *size*]

在当前终端取消 line 线路历史命令记录功能。
terminal no history

在当前终端恢复 line 线路历史命令记录的条目数
terminal no history size

【参数说明】

参数	描述
size *size*	条目数，取值范围：0~256。

【缺省配置】 缺省情况下开启历史命令记录功能，最大历史命令记录的条目数为 10

【命令模式】 特权用户模式

【缺省级别】 14

【使用指导】 -

【配置举例】 1：设置当前终端的 line 线路的历史记录条目数为 20。

```
Ruijie# terminal history size 20
```

2：关闭当前终端的 line 线路的历史记录功能。

```
Ruijie# terminal no history
```

【检验方法】 -

【提示信息】 -

【常见错误】 -

【平台说明】 -

3.25 terminal length

设置当前终端上的单屏最大行数。
terminal length *screen-length*

恢复当前终端的缺省设置。
terminal no length

【参数说明】

参数	描述
screen-ength	行高值，取值范围为 0-512。

【缺省配置】 缺省情况下，单屏最大行数为 24 行。

【命令模式】 特权用户模式

【缺省级别】 14

【使用指导】 -

【配置举例】 1：设置当前终端的单屏最大行数为 10 行。

```
Ruijie# terminal length 10
```

【检验方法】 -

【提示信息】 -

【常见错误】 -

【平台说明】 -

3.26 terminal location

设置当前终端的位置描述。
terminal location *location*

恢复当前终端的系统缺省设置。
terminal no location

【参数说明】

参数	描述
location	当前线路的位置描述。

【缺省配置】 -

【命令模式】 特权用户模式

【缺省级别】 14

【使用指导】 -

【配置举例】 1：设置当前终端的位置描述为 Swtich’s Line Vty 0。

```
Ruijie# terminal location Swtich’s Line Vty 0
```

【检验方法】 -

【提示信息】 -

【常见错误】 -

【平台说明】 -

3.27 terminal speed

设置当前终端上的波特率。

terminal speed *baudrate*

恢复缺省设置。

terminal no speed

【参数说明】

参数	描述
baudrate	波特率值，取值范围为 9600-115200。

【缺省配置】 缺省情况下，波特率为 9600。

【命令模式】 特权用户模式

【缺省级别】 14

【使用指导】 -

【配置举例】 1：设置当前终端的波特率为 115200。

```
Ruijie# terminal speed 115200
```

【检验方法】 -

【提示信息】 -

【常见错误】 -

【平台说明】 -

3.28 terminal width

配置当前终端上的单行最大列数，即一行的宽度。
terminal width *screen-width*

恢复当前终端的行宽。
terminal no width

【参数说明】

参数	描述
screen-width	行宽值，取值范围为 0-256。

【缺省配置】 缺省情况下，单行最大列数为 79 列。

【命令模式】 特权用户模式

【缺省级别】 14

【使用指导】 -

【配置举例】 1：设置当前终端的单行最大列数为 10 列。

```
Ruijie# terminal width 10
```

【检验方法】 -

【提示信息】 -

【常见错误】 -

【平台说明】 -

3.29 timeout login

设置 line 线路登录认证超时时间。

timeout login response *seconds*

恢复默认 line 线路登录认证时间。

no timeout login response

【参数说明】

参数	描述
response	Line 线路等待用户输入任何信息的时间。
seconds	超时时间，取值范围 1-300，单位为秒。

【缺省配置】 认证等待用户输入的超时时间，默认 30 秒

【命令模式】 LINE 配置模式

【缺省级别】 14

【使用指导】 -

【配置举例】 配置 0-5 的 line Vty 线路的登录认证超时间为 300 秒。

```
Ruijie(config)# line vty 0 5
Ruijie(config-line)#timeout login response 300
```

【检验方法】 -

【提示信息】 -

【常见错误】 -

【平台说明】 -

3.30 transport input

指定 line 线路下可以通讯的协议。

transport input { **all** | **ssh** | **telnet** | **none** }

恢复 line 线路下可以通讯的协议。

no transport input { **all** | **ssh** | **telnet** | **none** }

【参数说明】

参数	描述
all	允许所有协议。
ssh	允许 ssh 协议。
telenet	允许 telnet 协议。
none	任何协议都不允许。

【缺省配置】 缺省情况下，可以通讯的协议为 all，即 ssh 和 telnet 协议都可以。

【命令模式】 LINE 配置模式

【缺省级别】 14

【使用指导】 -

【配置举例】 配置 0-4 的 VTY line 线路只允许 telnet 通讯协议。

```
Ruijie(config)# line vty 0 5
Ruijie(config-line)#transport input ssh
```

【检验方法】 -

【提示信息】 -

【常见错误】 -

【平台说明】 -

3.31 vacant-message

配置 line 线路退出登录提示信息。

vacant-message [*c message c*]

取消 line 线路退出登录提示信息。

no vacant-message

【参数说明】

参数	描述
c	退出登录提示信息的分隔符 ,退出登录提示信息内容中间不允许出现间隔符。
message	退出登录提示信息。

【缺省配置】 -

【命令模式】 LINE 配置模式

【缺省级别】 14

【使用指导】 使用该命令可以配置退出登录提示信息，如果键入结束的分隔符后仍然输入字符，则这些字符将被系统丢弃。当用户退出登录设备时，窗口会提示当前线路退出登录的提示信息。

【配置举例】 1：配置 line 线路退出登录提示信息为退出锐捷设备。

```
Ruijie(config-line)#vacant-message @ 退出锐捷设备 @
```

【检验方法】 -

【提示信息】 -

【常见错误】 -

【平台说明】 -

3.32 width

配置指定线路终端上的单行最大列数，即一行的宽度。
width *screen-width*

恢复指定线路的行宽。
no width

【参数说明】

参数	描述
screen-width	行宽值，取值范围为 0-256。

【缺省配置】 缺省情况下，单行最大列数为 79 列。

【命令模式】 LINE 配置模式

【缺省级别】 14

【使用指导】 -

【配置举例】 1：设置指定线路的单行最大列数为 10 列。

```
Ruijie(config-line)# width 10
```

【检验方法】 -

【提示信息】 -

【常见错误】 -

【平台说明】 -

4 PASSWORD-POLICY

4.1 password policy life-cycle

设置口令生存周期。
password policy life-cycle *days*

删除口令生存周期设置。
no password policy life-cycle

【参数说明】

参数	描述
days	口令生存周期，单位：天，范围：1~65535。

【缺省配置】 不限制口令的生存周期。

【命令模式】 全局配置模式

【缺省级别】 14

【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。

配置了此功能后，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。

【配置举例】 1：下面的示例配置口令生存周期为 90 天：

```
Ruijie(config)# password policy life-cycle 90
```

【检验方法】 1：使用 **show password policy** 命令，可以查看是否设置口令的生存周期及生存周期的大小。

【提示信息】 -

【常见错误】 -

【平台说明】 -

4.2 password policy min-size

限制用户口令的最小长度。
password policy min-size *length*

删除限制用户口令的最小长度。
no password policy min-size

【参数说明】

参数	描述
length	指定口令最小长度，范围：1~31。

【缺省配置】 关闭口令最小长度限制，不进行口令最小长度限制。

【命令模式】 全局配置模式

【缺省级别】 14

【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。

配置了此功能后，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。

【配置举例】 1：下面的示例配置口令最小长度为 8：

```
Ruijie(config)# password policy min-size 8
```

【检验方法】 1：使用 **show password policy** 命令，可以查看是否限制口令最小长度及限制的口令最小长度。

【提示信息】 -

【常见错误】 -

【平台说明】 -

4.3 password policy no-repeat-times

限制重复使用最近几次已配置过的口令。
password policy no-repeat-times *times*

删除限制重复使用最近几次已配置过的口令。

no password policy no-repeat-times

【参数说明】

参数	描述
times	最近几次已配置过的口令，范围：1~31。

【缺省配置】 不限制重复使用最近几次使用过的口令。

【命令模式】 全局配置模式

【缺省级别】 14

【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。

> 配置了此功能后，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。

【配置举例】 1：下面的示例配置限制重复使用最近 5 次已配置过的口令：

```
Ruijie(config)# password policy no-repeat-times 5
```

【检验方法】 1：使用 **show password policy** 命令，可以查看是否限制重复使用最近几次已配置过的口令及口令历史记录最大条数。

【提示信息】 -

【常见错误】 -

【平台说明】 -

4.4 password policy strong

打开强口令检测功能。
password policy strong

关闭强口令检测功能。
no password policy strong

【参数说明】

参数	描述
-	-

【缺省配置】 关闭强口令检测，用户设置口令时不进行强口令检测。

【命令模式】 全局配置模式

【缺省级别】 14

【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。

配置了此功能后，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。

【配置举例】 1：下面的示例配置强口令检查：

```
Ruijie(config)# password policy strong
```

【检验方法】 1：使用 **show password policy** 命令，可以查看是否开启强口令检测功能。

【提示信息】 -

【常见错误】 -

【平台说明】 -

4.5 service password-encryption

设置口令加密存储。
service password-encryption

删除口令加密存储设置。
no service password-encryption

【参数说明】

参数	描述
-	-

【缺省配置】 不对口令进行加密存储。

【命令模式】 全局配置模式

【缺省级别】 14

【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。

【配置举例】 1：下面的示例设置对口令进行加密存储：

```
Ruijie(config)# service password-encryption
```

【检验方法】 1：使用 **show password policy** 命令，可以查看是否开启口令加密存储功能。

【提示信息】 -

【常见错误】 -

【平台说明】 -

4.6 show password policy

查看用户设置的口令安全策略信息。

show password policy

【参数说明】

参数	描述
-	-

【命令模式】 特权模式

【缺省级别】 1

【使用指导】 使用该命令可以查看设备上设置的口令安全策略信息。

【配置举例】 1：查看用户设置的口令安全策略信息

```
Ruijie#show password policy
Global password policy configurations:
 Password encryption:                Enabled
 Password strong-check:              Enabled
 Password secret-dictionary-check:   Enabled
 Password min-size:                  Enabled (6 characters)
 Password life-cycle:                Enabled (90 days)
 Password no-repeat-times:           Enabled (max history record: 5)
```

字段解释：

字段	说明

Password encryption	口令是否加密存储
Password strong-check	是否打开强口令检查
Password secret-dictionary-check	是否打开密码字典检查
Password min-size	限制口令最小长度
Password life-cycle	限制口令生存周期
Password no-repeat-times	限制重复使用最近几次使用过的口令

【提示信息】 -

【平台说明】 -

5 File System

5.1 cd

更改当前路径或者文件系统。

cd [*filesystem*:] [*directory*]

【参数说明】

参数	描述
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:**。
directory	路径名，如果是以“/”开头，则表示绝对路径，否则表示相对路径。

【缺省配置】 默认的文件系统是 **flash:**，如果路径名没有指定，则表示该文件系统的根路径。

【命令模式】 特权模式

【缺省级别】 1

【使用指导】 -

【配置举例】 1：使用 **cd** 命令进入 sata 硬盘：

```
Ruijie#pwd
flash:/
Ruijie#cd sata:
Ruijie#pwd
sata:/
```

【检验方法】 通过 **cd** 和 **pwd** 命令来改变和查看当前工作路径。

【提示信息】 -

【常见错误】 -

【平台说明】 NBR2500D-E、NBR3000D-E、NBR3000D-UE 出厂带 SATA 硬盘。NBR108G-P 、NBR800G、NBR950G、NBR1500G、NBR2000G、NBR1000G-C、NBR2000G-C、NBR3000G-S、NBR1000G-E、NBR6120-E、NBR1300G-E、NBR1700G-E、NBR2100G-E、NBR6205-E、NBR6135-E、NBR6210-E、NBR6215-E 出厂无 SATA 硬盘。其中 NBR6205-E、NBR6135-E、NBR6210-E、NBR6215-E 可自行购买 SATA 硬盘使用。

5.2 copy

在文件系统间拷贝文件。

copy *src-url dst-url*

【参数说明】

参数	描述
src-url	拷贝动作的源文件的 URL。源文件可以在本地或者在远程。
dst-url	拷贝动作的目的文件的 URL。目的文件可以在本地或远程。

【缺省配置】 -

【命令模式】 特权模式

【缺省级别】 1

【使用指导】

⚠ 当要拷贝的文件在目标 URL 上已经存在时，由目标文件系统决定如何操作，如报错，覆盖，或让用户选择。

url 可以用如下格式：

参数	描述
running-config	当前正在跑的配置文件
startup-config	用于初始化的配置文件
flash:	本地 flash 文件系统
tftp:	TFTP 网络服务器的 URL，语法如下所示： **tftp**:[[//location]/directory]**/filename**

【配置举例】 1：拷贝 192.168.64.2 设备上的文件 netconfig 到 flash 磁盘的 netconfig，本地的 netconfig 已经存在：

```
Ruijie#copy tftp://192.168.64.2/netconfig flash:/netconfig
The file [flash:/netconfig] exits,override it? [Y/N]: y
Copying: !!!!!!!!

Accessing tftp://192.168.64.2/netconfig finished, 2399bytes prepared
Flushing data to flash:/netconfig...
Flush data done
```

【检验方法】 通过 **copy** 和 **dir** 命令来拷贝和显示文件信息。

【提示信息】 -

【常见错误】 所指定的拷贝的源文件是目录，目录是无法拷贝的。

【平台说明】 -

5.3 delete

删除一个文件。

delete [*filesystem***:**] *file-url* [**/force** | **/recursive**]

【参数说明】

参数	描述
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	带路径的文件名字，如果是以“/”开头，则表示绝对路径，否则表示相对路径。
/force	强制删除文件，不等待用户确认
/recursive	递归删除一个目录的所有文件，包括目录本身

【缺省配置】 默认的文件系统是 **flash**:。

【命令模式】 特权模式

【缺省级别】 1

【使用指导】 -

【配置举例】 1：删除 flash 磁盘上的文件 fstab：

```
Ruijie#pwd
flash:/
Ruijie#dir
Directory of flash:/
1   -rw-        336   Jan 03 2012 18:53:42  fstab
2   -rw-       4096   Jan 03 2012 12:32:09  rc.d
3   -rw-   10485760   Jan 03 2012 18:13:37  rpmdb
3 files, 0 directories
10,490,192 bytes total (13,192,656 bytes free)
Ruijie#delete flash:/fstab
Ruijie#dir
Directory of flash:/
1   -rw-       4096   Jan 03 2012 12:32:09  rc.d
2   -rw-   10485760   Jan 03 2012 18:13:37  rpmdb
2 files, 0 directories
10,489,856 bytes total (13,192,992 bytes free)
```

2：递归删除 flash 磁盘上的非空文件夹 file：

```
Ruijie#pwd
flash:/
Ruijie#dir
Directory of flash:/
   1 drwx             0  Thu Jan  1 02:02:25 1970  file
   2 -rw-        610019  Tue Aug 14 02:21:13 2012  file-5.11.tar.gz
1 file, 1 directory
58,720,256 bytes total (28,577,792 bytes free)
Ruijie#delete /recursive flash:/file
Ruijie#dir
Directory of flash:/
   1 -rw-        610019  Tue Aug 14 02:21:13 2012  file-5.11.tar.gz
1 file, 0 directories
58,720,256 bytes total (31,358,976 bytes free)
```

【检验方法】 通过 **delete** 和 **dir** 命令来删除文件，显示文件信息。

【提示信息】 -

【常见错误】 -

【平台说明】 NBR2500D-E、NBR3000D-E、NBR3000D-UE 出厂带 SATA 硬盘。NBR108G-P 、NBR800G、NBR950G、NBR1500G、NBR2000G、NBR1000G-C、NBR2000G-C、NBR3000G-S、NBR1000G-E、NBR6120-E、NBR1300G-E、NBR1700G-E、NBR2100G-E、NBR6205-E、NBR6135-E、NBR6210-E、NBR6215-E 出厂无 SATA 硬盘。其中 NBR6205-E、NBR6135-E、NBR6210-E、NBR6215-E 可自行购买 SATA 硬盘使用。

5.4 dir

显示一个文件系统上的文件列表。

dir [*filesystem*:] [*file-url*]

【参数说明】

参数	描述
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。

【缺省配置】 默认的文件系统是 **flash:**，如果路径名没有指定，则表示该文件系统的根路径。

【命令模式】 特权模式

【缺省级别】 1

【使用指导】 -

【配置举例】 1：显示 flash 磁盘的根目录的文件列表：

```
Ruijie#dir flash:/
Directory of flash:/
1   -rw-        336   Jan 03 2012 18:53:42  fstab
2   -rw-       4096   Jan 03 2012 12:32:09  rc.d
3   -rw-   10485760   Jan 03 2012 18:13:37  rpmdb
3 files, 0 directories
10,490,192 bytes total (13,192,656 bytes free)
```

字段解释：

字段	说明
1、2、3.。。。	索引号
-rw-	权限，一个文件可以有下面的任意项： ● d ：表明这是一个目录 ● r ：可读 ● w ： 可写 ● x ： 可执行
10485760	文件大小
rpmdb	文件名
files	文件数目统计
directories	目录数目统计
total	总大小
free	剩余可用空间

【检验方法】 -

【提示信息】 -

【常见错误】 -

【平台说明】 NBR2500D-E、NBR3000D-E、NBR3000D-UE 出厂带 SATA 硬盘。NBR108G-P 、NBR800G、NBR950G、NBR1500G、NBR2000G、NBR1000G-C、NBR2000G-C、NBR3000G-S、NBR1000G-E、NBR6120-E、NBR1300G-E、NBR1700G-E、NBR2100G-E、NBR6205-E、NBR6135-E、NBR6210-E、NBR6215-E 出厂无 SATA 硬盘。其中 NBR6205-E、NBR6135-E、NBR6210-E、NBR6215-E 可自行购买 SATA 硬盘使用。

5.5 erase

擦除没有文件系统的设备或文件。

erase *filesystem*:

【参数说明】

参数	描述
filesystem:	文件系统名称，后面跟一个冒号，例如：usb0:。

【缺省配置】

【命令模式】 特权模式

【缺省级别】 1

【使用指导】 -

【配置举例】 1：擦除 usb 文件系统：

```
Ruijie#erase usb0:
Sure to erase usb0:? [Y/N] y
Erasing disk usb0 …
Erase disk usb0 done!
```

【检验方法】 **erase** 之后用 **dir** 命令查看文件信息

【提示信息】 -

【常见错误】 -

【平台说明】 -

5.6 file

显示一个文件的信息。

file [*filesystem*:] *file-url*

【参数说明】

参数	描述
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	带路径的文件名字，如果是以“/”开头，则表示绝对路径，否则表示相对路径。

【缺省配置】 默认的文件系统是 flash:。

【命令模式】 特权模式

【缺省级别】 1

【使用指导】 -

【配置举例】 1：显示 gcc 可执行文件的信息：

```
Ruijie#file flash:/gcc
/usr/bin/gcc-4.6: ELF 32-bit LSB executable, Intel 80386, version 1 (SYSV), dynamically linked (uses shared libs), for GNU/Linux 2.6.15, stripped
```

【检验方法】 -

【提示信息】 -

【常见错误】 -

【平台说明】 NBR2500D-E、NBR3000D-E、NBR3000D-UE 出厂带 SATA 硬盘。NBR108G-P 、NBR800G、NBR950G、NBR1500G、NBR2000G、NBR1000G-C、NBR2000G-C、NBR3000G-S、NBR1000G-E、NBR6120-E、NBR1300G-E、NBR1700G-E、NBR2100G-E、NBR6205-E、NBR6135-E、NBR6210-E、NBR6215-E 出厂无 SATA 硬盘。其中 NBR6205-E、NBR6135-E、NBR6210-E、NBR6215-E 可自行购买 SATA 硬盘使用。

5.7 file prompt

指定提示的级别。

file prompt [**noisy** | **quiet**]

【参数说明】

参数	描述
noisy	为所有的文件操作进行确认
quiet	极少提示

【缺省配置】 **noisy**

【命令模式】 特权模式

【缺省级别】 1

【使用指导】 -

【配置举例】 1：修改文件提示级别为 noisy 模式：

```
Ruijie#file prompt noisy
```

【检验方法】 -

【提示信息】 -

【常见错误】 -

【平台说明】 -

5.8 mkdir

创建一个新目录。

mkdir [*filesystem*:] *directory*

【参数说明】

参数	描述
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:**。
directory	路径名，如果是以“/”开头，则表示绝对路径，否则表示相对路径。

【缺省配置】 -默认的文件系统是 **flash:**，如果路径名没有指定，则表示该文件系统的根路径。

【命令模式】 特权模式

【缺省级别】 1

【使用指导】 -

【配置举例】 1：创建一个名为 newdir 的目录：

```
Ruijie#dir
Directory of flash:/
1   -rw-        336   Jan 03 2012 18:53:42  fstab
2   -rw-       4096   Jan 03 2012 12:32:09  rc.d
3   -rw-   10485760   Jan 03 2012 18:13:37  rpmdb
3 files, 0 directories
10,490,132 bytes total (13,192,656 bytes free)
Ruijie#mkdir newdir
Created dir flash:/newdir
Ruijie#dir
Directory of flash:/
1   -rw-        336   Jan 03 2012 18:53:42  fstab
2   -rw-       4096   Jan 03 2012 12:32:09  rc.d
3   -rw-   10485760   Jan 03 2012 18:13:37  rpmdb
4   drw-       4096   Jan 03 2012 18:13:37  newdir
3 files, 1 directories
10,494,228 bytes total (13,188,560 bytes free)
```

【检验方法】 -

【提示信息】 -

【常见错误】 -

【平台说明】 NBR2500D-E、NBR3000D-E、NBR3000D-UE 出厂带 SATA 硬盘。NBR108G-P 、NBR800G、NBR950G、NBR1500G、NBR2000G、NBR1000G-C、NBR2000G-C、NBR3000G-S、NBR1000G-E、NBR6120-E、NBR1300G-E、NBR1700G-E、NBR2100G-E、NBR6205-E、NBR6135-E、NBR6210-E、NBR6215-E 出厂无 SATA 硬盘。其中 NBR6205-E、NBR6135-E、NBR6210-E、NBR6215-E 可自行购买 SATA 硬盘使用。

5.9 more

显示一个文件的内容。

more [**/ascii** | **/binary**] [*filesystem*:] *file-url*

【参数说明】

参数	描述
/ascii	以 ASCII 的格式显示文件内容
/binary	以 16 进制/文本的格式显示文件内容
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。

【缺省配置】 缺省以文件的原有格式来显示

【命令模式】 特权模式

【缺省级别】 1

【使用指导】 -

【配置举例】 1：显示 flash 磁盘根目录下的 netconfig 文件的内容：

```
Ruijie#more flash:/netconfig
#
# The network configuration file. This file is currently only used in
# conjunction with the TI-RPC code in the libtirpc library.
#
# Entries consist of:
#
#       <network_id> <semantics> <flags> <protofamily> <protoname> \
#               <device> <nametoaddr_libs>
#
```

```
# The <device> and <nametoaddr_libs> fields are always empty in this
# implementation.
#
udp        tpi_clts      v     inet     udp     -       -
tcp        tpi_cots_ord  v     inet     tcp     -       -
udp6       tpi_clts      v     inet6    udp     -       -
tcp6       tpi_cots_ord  v     inet6    tcp     -       -
rawip      tpi_raw       -     inet      -      -       -
local      tpi_cots_ord  -     loopback  -      -       -
```

【检验方法】 -

【提示信息】 -

【常见错误】 -

【平台说明】 NBR2500D-E、NBR3000D-E、NBR3000D-UE 出厂带 SATA 硬盘。NBR108G-P 、NBR800G、NBR950G、NBR1500G、NBR2000G、NBR1000G-C、NBR2000G-C、NBR3000G-S、NBR1000G-E、NBR6120-E、NBR1300G-E、NBR1700G-E、NBR2100G-E、NBR6205-E、NBR6135-E、NBR6210-E、NBR6215-E 出厂无 SATA 硬盘。其中 NBR6205-E、NBR6135-E、NBR6210-E、NBR6215-E 可自行购买 SATA 硬盘使用。

5.10 pwd

显示用户当前工作目录的完整路径。

pwd

【参数说明】

参数	描述
-	-

【缺省配置】 -

【命令模式】 特权模式

【缺省级别】 1

【使用指导】 -

【配置举例】 1：显示工作目录从 flash:切换到 sata:的过程

```
Ruijie#pwd
flash:/
Ruijie#cd sata:/
```

```
Ruijie#pwd
sata:/
```

【检验方法】 -

【提示信息】 -

【常见错误】 -

【平台说明】 NBR2500D-E、NBR3000D-E、NBR3000D-UE 出厂带 SATA 硬盘。NBR108G-P 、NBR800G、NBR950G、NBR1500G、NBR2000G、NBR1000G-C、NBR2000G-C、NBR3000G-S、NBR1000G-E、NBR6120-E、NBR1300G-E、NBR1700G-E、NBR2100G-E、NBR6205-E、NBR6135-E、NBR6210-E、NBR6215-E 出厂无 SATA 硬盘。其中 NBR6205-E、NBR6135-E、NBR6210-E、NBR6215-E 可自行购买 SATA 硬盘使用。

5.11 rename

移动一个现有文件或文件夹。

rename *src-url dst-url*

【参数说明】

参数	描述
src-url	待移动的路径和文件名
dst-url	接收文件的路径和文件名

【缺省配置】 -

【命令模式】 特权模式

【缺省级别】 1

【使用指导】 -

【配置举例】 1：将 flash 磁盘根目录下的 fstab 文件重命名为 new-fstab：

```
Ruijie#dir
Directory of flash:/
1   -rw-        336   Jan 03 2012 18:53:42  fstab
2   -rw-       4096   Jan 03 2012 12:32:09  rc.d
3   -rw-   10485760   Jan 03 2012 18:13:37  rpmdb
3 files, 0 directories
10,490,192 bytes total (13,192,656 bytes free)
Ruijie#rename flash:/fstab flash:/new-fstab
Renamed file flash:/new-fstab
```

```
Ruijie#dir
Directory of flash:/
1   -rw-        336   Jan 03 2012 18:53:42  new-fstab
2   -rw-       4096   Jan 03 2012 12:32:09  rc.d
3   -rw-   10485760   Jan 03 2012 18:13:37  rpmdb
3 files, 0 directories
10,490,192 bytes total (13,192,656 bytes free)
```

【检验方法】 -

【提示信息】 -

【常见错误】 -

【平台说明】 -

5.12 rmdir

删除一个现有的空目录。

rmdir [*filesystem***:**] *directory*

【参数说明】

参数	描述
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:**。
directory	

【缺省配置】 默认的文件系统是 **flash:**。

【命令模式】 特权模式

【缺省级别】 1

【使用指导】 -

【配置举例】 1：**rmdir** 命令删除现有的 test 的空目录：

```
Ruijie#mkdir newdir
Ruijie#dir
Directory of flash:/
1   -rw-        336   Jan 03 2012 18:53:42  fstab
2   -rw-       4096   Jan 03 2012 12:32:09  rc.d
3   -rw-   10485760   Jan 03 2012 18:13:37  rpmdb
```

```
4   drw-       4096   Jan 03 2012 18:13:37  newdir
3 files, 1 directories
10,494,228 bytes total (13,188,560 bytes free)
Ruijie#rmdir newdir
removed dir flash:/newdir
Ruijie#dir
Directory of flash:/
1   -rw-        336   Jan 03 2012 18:53:42  fstab
2   -rw-       4096   Jan 03 2012 12:32:09  rc.d
3   -rw-   10485760   Jan 03 2012 18:13:37  rpmdb
3 files, 0 directories
10,490,132 bytes total (13,192,656 bytes free)
```

【检验方法】 -

【提示信息】 -

【常见错误】 -

【平台说明】 NBR2500D-E、NBR3000D-E、NBR3000D-UE 出厂带 SATA 硬盘。NBR108G-P 、NBR800G、NBR950G、NBR1500G、NBR2000G、NBR1000G-C、NBR2000G-C、NBR3000G-S、NBR1000G-E、NBR6120-E、NBR1300G-E、NBR1700G-E、NBR2100G-E、NBR6205-E、NBR6135-E、NBR6210-E、NBR6215-E 出厂无 SATA 硬盘。其中 NBR6205-E、NBR6135-E、NBR6210-E、NBR6215-E 可自行购买 SATA 硬盘使用。

5.13 show disk

获取 sata/usb 信息

show disk sata/usb/flash

【参数说明】

参数	描述
sata	获取硬盘信息
usb	获取 usb 信息
flash	获取 flash 信息

【命令模式】 特权模式

【缺省级别】 1

【使用指导】

【配置举例】 1：查看 sata 信息：

```
Ruijie#show disk sata
```

```
Disk /dev/sda: 160.0 GB, 160039272960 bytes
255 heads, 63 sectors/track, 19457 cylinders
```

Units = cylinders of 16065 * 512 = 8225280 bytes

2：查看 usb 信息：

```
Ruijie#show disk usb
Disk /dev/sdb: 8159 MB, 8159477760 bytes
252 heads, 62 sectors/track, 1020 cylinders
Units = cylinders of 15624 * 512 = 7999488 bytes
```

3：查看 flash 信息：

Ruijie#show disk flash

Nand flash size: 512MB

Nor flash size: 1MB

【检验方法】 -

【提示信息】 -

【常见错误】 -

【平台说明】 NBR2500D-E、NBR3000D-E、NBR3000D-UE 出厂带 SATA 硬盘。NBR108G-P 、NBR800G、NBR950G、NBR1500G、NBR2000G、NBR1000G-C、NBR2000G-C、NBR3000G-S、NBR1000G-E、NBR6120-E、NBR1300G-E、NBR1700G-E、NBR2100G-E、NBR6205-E、NBR6135-E、NBR6210-E、NBR6215-E 出厂无 SATA 硬盘。其中 NBR6205-E、NBR6135-E、NBR6210-E、NBR6215-E 可自行购买 SATA 硬盘使用。

5.14 show file systems

显示文件系统的相关信息。

show file systems

【参数说明】

参数	描述
-	-

【命令模式】

【缺省级别】 1

【使用指导】 -

【配置举例】 1：显示所有已挂载的文件系统的信息：

```
Ruijie#show file systems
  Size(KB)       Free(KB)     Type   Flags  Prefixes
        NA             NA       ram     rw  tmp:
```

```
          NA            NA   network     rw  tftp:
        8192          2416      disk     rw  flash:
   167772160     147772160      disk     rw  sata0:
     1048576        548576      disk     rw  usb0:
```

字段解释：

字段	说明
Size(KB)	文件系统的空间大小，单位 KB。
Free(KB)	文件系统的剩余空间，单位 KB。
Type	文件系统类型
Flags	文件系统的权限，有如下几种： ● ro：只读 ● wo: 只写 ● rw: 可读写
Prefixes	文件系统前缀

【提示信息】 -

【平台说明】 NBR2500D-E、NBR3000D-E、NBR3000D-UE 出厂带 SATA 硬盘。NBR108G-P 、NBR800G、NBR950G、NBR1500G、NBR2000G、NBR1000G-C、NBR2000G-C、NBR3000G-S、NBR1000G-E、NBR6120-E、NBR1300G-E、NBR1700G-E、NBR2100G-E、NBR6205-E、NBR6135-E、NBR6210-E、NBR6215-E 出厂无 SATA 硬盘。其中 NBR6205-E、NBR6135-E、NBR6210-E、NBR6215-E 可自行购买 SATA 硬盘使用。

5.15 show mount

显示系统挂载信息。

show mount

【参数说明】

参数	描述
-	-

【命令模式】 特权模式

【缺省级别】 1

【使用指导】 -

【配置举例】 1：显示系统挂载信息：

```
Ruijie#show mount
/dev/sda1 on / type ext4 (rw,errors=remount-ro,commit=0)
proc on /proc type proc (rw,noexec,nosuid,nodev)
sysfs on /sys type sysfs (rw,noexec,nosuid,nodev)
```

```
fusectl on /sys/fs/fuse/connections type fusectl (rw)
none on /sys/kernel/debug type debugfs (rw)
none on /sys/kernel/security type securityfs (rw)
udev on /dev type devtmpfs (rw,mode=0755)
devpts on /dev/pts type devpts (rw,noexec,nosuid,gid=5,mode=0620)
tmpfs on /run type tmpfs (rw,noexec,nosuid,size=10%,mode=0755)
none on /run/lock type tmpfs (rw,noexec,nosuid,nodev,size=5242880)
none on /run/shm type tmpfs (rw,nosuid,nodev)
/dev/sda3 on /hao-share type ext3 (rw,commit=0)
binfmt_misc on /proc/sys/fs/binfmt_misc type binfmt_misc (rw,noexec,nosuid,nodev)
```

字段解释，以第一行为例：

字段	说明
proc	挂载的源地址
on	-
/proc	挂载的目的地址
type	-
proc	挂载的类型
(rw,noexec,nosuid,nodev)	挂载的属性

【提示信息】 -

【平台说明】 -

5.16 tftp-client source

TFTP Client 可以绑定客户端源 IP 或源接口地址，使用源接口 IP 或指定 IP 地址与服务器端 IP 地址进行通信。

tftp-client source {**ip** *ip-address* | *interface*}

取消对客户端源 IP 地址绑定。

no tftp-client source {**ip** *ip-address* | *interface*}

恢复缺省配置.。

default tftp-client source {**ip** *ip-address* | *interface*}

【参数说明】

参数	描述
ip-address	指定 IPv4 源地址
interface	指定源接口

【缺省配置】 缺省情况下，客户端不进行本地源地址/源接口绑定，由路由进行选择。

【命令模式】 全局配置模式

【缺省级别】 14

【使用指导】 -

【配置举例】 1：配置 TFTP Client 绑定客户端源 IP 为 192.168.23.236 地址。

```
Ruijie(config)# tftp-client source ip 192.168.23.236
```

2：配置 TFTP Client 绑定客户端源 IP 为接口 gigabitEthernet 0/0 地址。

```
Ruijie(config)# tftp-client source gigabitEthernet 0/0
```

3：no 命令取消对客户端源 IP 地址绑定。

```
Ruijie(config)# no tftp-client source ip 192.168.23.236
```

4：TFTP Client 恢复为缺省配置。

```
Ruijie(config)# default tftp-client source ip 192.168.23.236
```

【检验方法】 1：使用 show run 命令，可以查看 tftp-client source ip192.168.23.236 配置。
2：使用 show run 命令，可以查看 tftp-client source gigabitEthernet 0/0 配置。

【提示信息】 1：如果配置的 ip 地址或者接口不是本地地址，则会提示错误；如果是，则配置成功，不会出现任何提示。
2：一定配置成功，不会出现任何提示。

【常见错误】 -

【平台说明】 -

5.17 tree

显示一个现有的目录的文件树。

tree [*filesystem*:] [*directory*]

【参数说明】

参数	描述
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:**。
directory	路径名，如果是以“/”开头，则表示绝对路径，否则表示相对路径。

【缺省配置】 -默认的文件系统是 **flash:**。

【命令模式】 特权模式

【缺省级别】 1

【使用指导】 -

【配置举例】 1：显示 flash:/echo 下面的文件树：

```
Ruijie#tree flash:/echo
+-- client_module
+-- client_userspace
+-- echo_cli.c
+-- echo_client.c
+-- echo_client.h
+-- echo_client.o
+-- echo_cli.o
+-- echo_flag.h
+-- echo.h
+-- echo.ko
+-- echo_server.h
+-- exec_set_echo.h
+-- exec_show_echo.h
+-- Makefile
+-- module
¦   +-- echo.ko
¦   +-- echo.mod.c
¦   +-- echo.mod.o
¦   +-- echo_module.c
¦   +-- echo_module.o
¦   +-- echo.o
¦   +-- echo_server.c
¦   +-- echo_server.o
¦   +-- echo_sysfs.c
¦   +-- echo_sysfs.h
¦   +-- echo_sysfs.o
¦   +-- Makefile
¦   +-- modules.order
¦   +-- Module.symvers
¦   +-- msg_fd.c
¦   +-- msg_fd.o
+-- readme
+-- server_module
+-- server_userspace
+-- sys_rgos.ko
```

```
+-- user_space
    +-- echo_server.c
    +-- echo_server.o
    +-- Makefile
    +-- msg_fd.c
    +-- msg_fd.o 10,490,132 bytes total (13,192,656 bytes free)
```

【检验方法】 -

【提示信息】 -

【常见错误】 -

【平台说明】 NBR2500D-E、NBR3000D-E、NBR3000D-UE 出厂带 SATA 硬盘。NBR108G-P 、NBR800G、NBR950G、NBR1500G、NBR2000G、NBR1000G-C、NBR2000G-C、NBR3000G-S、NBR1000G-E、NBR6120-E、NBR1300G-E、NBR1700G-E、NBR2100G-E、NBR6205-E、NBR6135-E、NBR6210-E、NBR6215-E 出厂无 SATA 硬盘。其中 NBR6205-E、NBR6135-E、NBR6210-E、NBR6215-E 可自行购买 SATA 硬盘使用。

5.18 verify

计算、显示、校验文件 md5 信息

verify [**/md5** *md5-value*] *filesystem***:** [*file-url*]

【参数说明】

参数	描述
/md5	计算并显示文件的 MD5 值
md5-value	文件的 md5 值，将会和计算出的 md5 值进行比较
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。

【缺省配置】 默认的文件系统是 **flash:**。

【命令模式】 特权模式

【缺省级别】 1

【使用指导】 -

【配置举例】 1：计算 flash:/gcc 的 md5 信息：

```
Ruijie#verify flash:/gcc
8b072de7db7affd8b2ef824e7e4d716c
```

2：计算 flash:/gcc 的 md5 信息并进行比较：

```
Ruijie#verify /md5 8b072de7db7affd8b2ef824e7e4d716c flash:/gcc
%SUCCESS verifying /mnt/flash/gcc = 8b072de7db7affd8b2ef824e7e4d716c
Ruijie#verify /md5 8b072de7db7affd8b2ef824e7e4d71 flash:/gcc
%Error verifying flash:/gcc
Computed signature = 8b072de7db7affd8b2ef824e7e4d716c
Submitted signature = 8b072de7db7affd8b2ef824e7e4d71
```

【检验方法】 -

【提示信息】 -

【常见错误】 -

【平台说明】 NBR2500D-E、NBR3000D-E、NBR3000D-UE 出厂带 SATA 硬盘。NBR108G-P 、NBR800G、NBR950G、NBR1500G、NBR2000G、NBR1000G-C、NBR2000G-C、NBR3000G-S、NBR1000G-E、NBR6120-E、NBR1300G-E、NBR1700G-E、NBR2100G-E、NBR6205-E、NBR6135-E、NBR6210-E、NBR6215-E 出厂无 SATA 硬盘。其中 NBR6205-E、NBR6135-E、NBR6210-E、NBR6215-E 可自行购买 SATA 硬盘使用。

6 LICENSING

6.1 license copy

备份授权文件。

license { **copy-all** | **copy-file** *filename* } { **flash: | usb0:** } [*target-filename*]

【参数说明】

参数	描述
copy-all	备份系统上的所有永久授权
copy-file	备份授权上由 *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* 为特性名时，就备份该特性下所有已安装的授权文件
filename	系统已安装的授权文件名或特性名
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
target-filename	指定授权文件名字

【缺省配置】 -

【命令模式】 特权模式

【缺省级别】 4

【使用指导】 当备份系统中所有授权文件时，生成的是 tar 文件。此命令不需要授权。
copy-file 可以备份单个授权文件，也可以备份某个特性的所有授权文件。

【配置举例】 备份系统上所有的授权到 u 盘的 rg-license-lics 路径（该路径必须存在）下，授权压缩包命名为 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。

【提示信息】 1：当备份所有授权时，系统上不存在可备份的授权

```
Copy failed, there's no permanent license in the system.
```

2：成功备份系统所有授权

```
Success to copy all permanent license.
```

3：如果设备上没有指定的特性或授权文件，则提示错误。

```
Copy failed, there's no such service or license installed in the system.
```

4：如果指定的授权是时效性的，则提示失败。

```
Copy failed, the license is temporary.
```

5：成功备份指定授权

```
Success to copy license vsd.lic.
```

【常见错误】
1. 系统上不存在指定授权或指定文件
2. 指定要备份的授权是临时的，不能备份

【平台说明】 -

6.2 license grace-period

设置授权失效的提前告警时间。
license grace-peroid *license days*

关闭失效前警告。
no license grace-peroid *filename*

恢复缺省配置。
default license grace-peroid *filename*

【参数说明】

参数	描述
filename	授权特性名字
days	失效前警告限发点。

【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

【缺省级别】 4

【使用指导】 当一项授权超时时限小于友好周期警告值时，每天产生一次警告；在授权失效的前一天，会每小时产生一次警告。警告以日志或 SNMP TRAP 形式发送。

此命令不需要授权。

评估授权才能设置提前告警时间，永久授权不需要设置。

【配置举例】 -

【检验方法】 -

【提示信息】 1：系统中不存在指定授权

```
There's no license abc in the system.
```

【常见错误】 系统中不存在指定授权

【平台说明】 -

6.3 license install

安装一个授权。

license install { **flash: | usb0:** } *filename*

【参数说明】

参数	描述
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

【缺省级别】 4

【使用指导】 授权文件名可修改。此命令不需要授权。

在 VSU 环境下，**CM** 管理板上使用 **license install** 命令，其他各板也都安装了该授权；非 cm 管理板上使用 **license install** 命令，只在自己本地执行安装。

【配置举例】 -

【检验方法】 使用 **show license all-license**，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。

【提示信息】 1：授权文件不存在：

```
Install failed: no such file or directory.
```

2：授权文件检查不合法：

```
Install failed: the install license may be wrong.
```

3：系统内已存在一个比要安装的授权文件更新的授权：

```
Install failed: the system already has a same license which is newer.
```

4：重复安装授权文件：

```
Install failed: the license has been installed before.
```

5：该授权是临时授权，系统中已存在相同的永久授权

```
Install failed: The system already has a same permanent license.
```

【常见错误】
1. 不存在指定的授权文件
2. 授权文件不合法
3. 授权文件 sn 码与设备不匹配
4. 预安装的授权比系统已有的更旧
5. 重复安装同一个授权文件
6. 预安装临时授权，而系统已安装有永久授权

【平台说明】 -

6.4 license unbind

解除绑定一个授权。

license unbind *pak*

【参数说明】

参数	描述
pak	指定授权码

【缺省配置】 -

【命令模式】 特权模式

【缺省级别】 4

【使用指导】 此命令不需要授权

该命令的作用就是解除某个授权文件和对应设备的绑定关系。用户在网页上解除绑定之前，必须先在要设备上用该命令解除绑定。

成功解除绑定之后，会获得一串验证码。该验证码在网页上解除绑定时需要。

【配置举例】 解除绑定授权码为 LIC-FCOE00000012268888 的授权

```
Ruijie#license unbind LIC-FCOE00000012268888
Success to unbind license LIC-FCOE00000012268888.
The verification string is 775719468737BA269825589557F558657575B5D5D5D5D785782598859765A8355855.
```

【检验方法】 可使用 **show license** 命令，查看是否还有指定授权码对应的授权。

-

【提示信息】 1：系统中不存在匹配的授权：

```
Unbind failed: not match license found.
```

【常见错误】 系统中不存在匹配的授权

【平台说明】 -

6.5 license uninstall

卸载授权。

license uninstall { **all** | *license* [*filename*] }

【参数说明】

参数	描述
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

【缺省级别】 4

【使用指导】 此命令不需要授权

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

【配置举例】 -

【检验方法】 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。

【提示信息】 1：错误提示：设备上没有指定授权（本例中指定授权名为 defd）

```
Uninstall failed: there's no license defd in the system.
```

2：错误提示：设备上没有指定特性的指定授权文件（本例中指定特性为 LIC-WLAN-AP-32，指定授权文件名为 123.lic）。

```
Uninstall failed: there's no license 123.lic of service LIC-WLAN-AP-32 in the system..
```

3：错误提示：卸载单实例授权特性的单个授权文件。

```
Uninstall failed: single instance license does not support license based uninstalling.
```

4．某授权中单个文件卸载成功（本例中 LIC-WLAN-AP-32 为授权特性名，AP32_1.lic 为单个授权文件）：

```
Uninstall license AP32_1.lic of service LIC-WLAN-AP-32 success.
```

【常见错误】
1. 设备上还未安装指定授权特性的授权
2. 设备上指定授权特性下不存在指定的授权文件
3. 预卸载单实例特性下的某个授权文件（单实例授权不支持单个文件的卸载）

【平台说明】 -

6.6 license update

更新一个授权。

license update { **flash: | usb0:** } *filename*

【参数说明】

参数	描述
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

【缺省级别】 4

【使用指导】 此命令不需要授权，授权文件名可修改。

【配置举例】 -

【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。
-

【提示信息】 1：授权文件不存在：

```
Update failed: No such file or directory.
```

2：授权文件检查不合法：

```
Update failed: the update license may be wrong.
```

3：预安装的授权文件比系统中存在的更旧：

```
Update failed: the new installed license is older than the system one
```

4：该授权之前已被安装过：

```
Update failed: the license has been installed before.
```

5：临时授权不能代替永久授权：

```
Update failed: the period license cannot replace permanent license.
```

6：预安装授权对应的授权特性之前未安装任何授权，请先安装：

```
Update failed: now the system does not have the license.
               Try "license install" instead.
```

【常见错误】
1. 授权文件不是本设备的
2. 预用较旧的授权替代较新的授权
3. 更新的授权就之前已经安装过
4. 预用临时授权代替永久授权
5. 更新授权时，对应的授权特性未安装任何授权

【平台说明】 -

6.7 show license

查看设备的授权情况。

show license { **all-license | dev-license | file** [*license*] }

【参数说明】

参数	描述
all-license	显示设备中所有已安装授权文件的列表

dev-license	显示环境中各个设备上的授权文件列表
file *filename*	显示一个指定授权名的信息

【命令模式】 特权模式

【缺省级别】 2

【使用指导】 该命令不需要授权，用于显示系统中的授权信息

【配置举例】

1 显示系统里所有已安装的授权信息

```
Ruijie#show  license all-license
Searching license in the system...
1. Service name: LIC-AP-64
    Attribute: Releasable
    [Permanent licenses]     [Licensed serial number]
    19880966.lic             LIC-AP-6400000012264966
    19880988.lic             LIC-AP-6400000012264988

    [Temporary license]      [Licensed serial number]
    19880900.lic             LIC-AP-6400000012264900
    (63 days left)
```

3. 显示系统里各个设备上已安装的授权信息

```
Ruijie#show  license dev-license
Searching license in the system...

Dev 1:
1. Service name: LIC-AP-64
    Attribute: Releasable
    [Permanent licenses]     [Licensed serial number]
    19880966.lic             LIC-AP-6400000012264966
    19880988.lic             LIC-AP-6400000012264988

    [Temporary license]      [Licensed serial number]
    19880900.lic             LIC-AP-6400000012264900
    (63 days left)

Dev 2:
 1. Service name: LIC-FC-BLADE-S
    Attribute: Temporary, Releasable
```

```
   Left days: 99
   Licensed serial number: LIC-FC-BLADE-S 00000001884686

2. Service name: LIC-AP
   Attribute: Permanent, Releasable
   [Installed licenses]     [Licensed serial number]
   19880921.lic             LIC-AP00000012265001
   19880922.lic             LIC-AP00000012265002
```

字段解释：

字段	说明
Service name	授权的特性名称
Attribute	该授权的一些属性
Left days	授权期限剩余天数
Installed license	已安装的授权文件
Licensed serial number	授权码

【提示信息】 -

【平台说明】 -

6.8 show license hostid

显示用于授权的主机号。

show license hostid

【参数说明】

参数	描述
-	-

【命令模式】 特权模式

【缺省级别】 2

【使用指导】 此命令不需要授权，该序列号用于唯一标识一台设备。

【配置举例】 1：查看某台设备的 hostid

```
Ruijie#show license hostid
1234942570021
```

【提示信息】 -

【平台说明】 -

6.9 show license unbind-code

查看本设备已解除绑定授权的验证码

show license unbind-code

【参数说明】

参数	描述
-	-

【命令模式】 特权模式

【缺省级别】 2

【使用指导】 此命令不需要授权

【配置举例】 -

【提示信息】 -

【平台说明】 -

6.10 show license usage

查看系统当前授权使用情况。

show license usage

【参数说明】

参数	描述
-	-

【命令模式】 特权模式

【缺省级别】 2

【使用指导】 此命令不需要授权

【配置举例】 1：查看授权信息

```
Ruijie#show license usage
Searching license in the system...
1. Service name: LIC-AP-64
```

```
  Attribute: Releasable
  [Permanent licenses]     [Licensed serial number]
  19880966.lic             LIC-AP-6400000012264966
  19880988.lic             LIC-AP-6400000012264988

  [Temporary license]      [Licensed serial number]
  19880900.lic             LIC-AP-6400000012264900
  (63 days left)
```

字段解释：

字段	说明
Service name	授权的特性名称
Attribute	该授权的一些属性
Left days	授权期限剩余天数

【提示信息】 -

【平台说明】 -

7 PKG_MGMT

7.1 clear storage

清除本地安装包。

clear storage [*url*]

【参数说明】

参数	描述
url	安装包存放的本地 *url* 目录或全路径名

【缺省配置】 -

【命令模式】 特权模式

【缺省级别】 2

【使用指导】 该命令可以指定清除某个安装包或某个目录下的所有安装包，默认清除本地所有安装包。

【配置举例】

```
Ruijie#clear storage
Remove the whole storage directory?[y/n]y
Ruijie#clear storage usb0
Remove the file or directory usb0 from the storage?[y/n]y
Ruijie#
```

【检验方法】 查看指定 *url*

【提示信息】 -

【常见错误】 -

【平台说明】 -

7.2 patch active

激活补丁，使补丁作用生效。

patch active

【参数说明】

参数	描述

-	-

【缺省配置】 -

【命令模式】 特权模式

【缺省级别】 2

【使用指导】 补丁安装成功后才能执行激活操作，激活后补丁才真正被系统使用，该命令用于临时激活热补丁，设备重启后补丁失效。

【配置举例】 1．盒式设备激活补丁。

```
Ruijie#patch active
 Active the patch package success
```

【检验方法】 使用 **show patch** 查看补丁信息。

【提示信息】 1．执行成功提示：

```
Active the patch package success
```

2．执行失败提示错误，补丁包未安装，需先安装热补丁包：

```
Patch not installed
```

3．补丁包已经被激活，无需执行该命令：

```
The patch status is already active or running
```

4．补丁包自身问题，请联系客服：

```
Cannot find the package's scripts file
```

【常见错误】
- 当前设备还未安装热补丁
- 当前设备的热补丁已经处于激活状态

【平台说明】 -

7.3 patch deactive

使补丁作用失效。

patch deactive

【参数说明】

参数	描述

-	-

【缺省配置】 -

【命令模式】 特权模式

【缺省级别】 2

【使用指导】 只有处于激活状态的补丁才能执行该操作，该操作使补丁作用失效。

【配置举例】 1．盒式设备使补丁失效。

```
Ruijie#patch deactive
 Deactive the patch package success
```

【检验方法】 使用 **show patch** 查看补丁信息

【提示信息】 1．执行成功提示：

```
Deactive the patch package success；
```

2．执行失败提示错误，补丁包未安装，需先安装热补丁包：

```
Patch not installed
```

3．补丁包功能已经失效，无需执行该命令：

```
The patch is not in active or running status
```

4．补丁包自身问题，请联系客服：

```
Cannot find the package's scripts file
```

【常见错误】
- 当前设备还未安装热补丁
- 当前设备的热补丁已经失效

【平台说明】 -

7.4 patch delete

删除补丁。

patch delete

【参数说明】

参数	描述
-	-

【缺省配置】 -

【命令模式】 特权模式

【缺省级别】 2

【使用指导】 此命令用于清除设备上已存在的热补丁包

【配置举例】 1．盒式设备清除已安装的热补丁包。

```
Ruijie# patch delete
 Clear the patch patch_bridge success
 Clear the patch success
```

【检验方法】 使用 **show patch** 查看补丁信息。

【提示信息】 1．执行成功提示：

```
Clear the patch success
```

2．补丁包未安装，需先安装热补丁包：

```
Patch not installed
```

【常见错误】
- 当前设备还未安装热补丁

【平台说明】 -

7.5 patch running

使补丁作用永久生效。

patch running

【参数说明】

参数	描述
-	-

【缺省配置】 -

【命令模式】 特权模式

【缺省级别】 2

【使用指导】 补丁安装成功后才能执行激活操作，激活后补丁才真正被系统使用，该命令用于永久激活热补丁。

【配置举例】 1．盒式设备激活补丁。

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

【检验方法】 使用 **show patch** 查看补丁信息。

【提示信息】 1．执行成功提示：

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

2．执行失败提示错误，补丁包未安装，需先安装热补丁包：

```
Patch not installed
```

3．补丁包功能已经失效，无需执行该命令：

```
The patch is not in active or running status
```

4．补丁包自身问题，请联系客服：

```
Cannot find the package's scripts file
```

【常见错误】
- 当前设备还未安装热补丁
- 当前设备的热补丁已经处于激活状态

【平台说明】 -

7.6 show component

显示当前设备已安装所有组件及各组件信息。

show component

【参数说明】

参数	描述
-	-

【命令模式】 特权模式

【缺省级别】 2

【使用指导】 该命令包含两种形式，带 *component_name* 参数和不带该参数。用户在升级，卸载组件前往往需要了解当前设备所有已安装的组件及组件版本信息，此时应使用不带参数的 **show component** 命令。当用户需要详细了解组件时要使用带参数的 **show component** 命令，可获取对应组件的详细信息。通过这些信息用户可以方便的了解组件的工作状态，判断组件内容是否被人为破坏，在排除功能故障，确保组件安全，可靠的运行方面有重要意义。

某些组件使用过程中会修改自身默认的配置文件，尽管这是正常情况，不属于恶意破坏，但 **show component** 命令只能判断组件文件在使用过程中发生了改变，无法区分是否属于恶意破坏，用户必须进一步自行判断。

【配置举例】 1．**盒式设备**显示当前已安装所有组件及各组件信息。

```
Ruijie# show component
Package  :sysmonit
     Version:1.0.1.23cd34aa      Build time: Wed Dec  7 00:58:56 2013
     Size:12877    Install time :Wed  Mar 5 14:23:12 2012
     Description: this is a system monit package
     Required packages: None
------------------------------------------------------------------
Package:bridge
     Version:2.0.1.37cd5cda      Build time: Wed Dec  7 00:54:56 2013
     Size:23245    Install time :Wed  Mar 5 14:30:12 2012
     Description: this is a bridge package
     Required packages: None
------------------------------------------------------------------
```

使用该命令形式，可以获取设备内已安装的所有组件及组件基本信息，这些信息为用户决定是否需要升级，卸载组件提供了依据。

字段	说明
Package	组件名称
Version	组件版本号
Build time	组件在服务器上编译完成的时间
Size	组件包含内容的大小
Install time	设备安装该组件的时间
Description	组件功能的简单描述
Required packages	依赖哪些组件

盒式设备显示当前设备已安装的特定组件信息。

```
Ruijie# show component bridge
package:bridge
     Version: 2.3.1.1252ea       Build time: Wed Dec  7 00:54:56 2013
     Size:26945    Install time : Wed Mar 19:23:15 2012
     Description:this is a bridge package
     Required packages: None
     Package files:
        /lib64
        /lib64/libbridge.so
        /sbin
        /sbin/bridge
```

```
    Package file validate: [OK]
    Required relationship verify: [OK]
```

除了组件基本信息外还包括：

字段	说明
Package file validate	校验组件包含文件的完整性。如果所有组件文件都正常则显示结果[OK]；如果部分文件丢失或文件被修改，则显示结果[ERR]，并明确指出哪个文件丢失或被修改。
Required package	列举该组件的所有依赖组件，若依赖组件已经安装则标注“[OK]”；若依赖组件还未安装则标注“[ERR]”并且详细说明哪个依赖组件还没有安装及依赖组件的版本信息
Package files	列出包内包含的所有文件

【提示信息】 执行成功显示设备内各组件信息：

```
Package  :sysmonit
     Version:1.0.1.23cd34aa      Build time: Wed Dec  7 00:58:56 2013
     Size:12877    Install time :Wed  Mar 5 14:23:12 2012
     Description: this is a system monit package
     Required packages: None
------------------------------------------------------------------
Package:bridge
     Version:2.0.1.37cd5cda      Build time: Wed Dec  7 00:54:56 2013
     Size:23245    Install time :Wed  Mar 5 14:30:12 2012
     Description: this is a bridge package
     Required packages: None
------------------------------------------------------------------
```

【平台说明】 -

7.7 show patch

显示设备中已安装的热补丁包的相关信息。

show patch [*patch _name*]

【参数说明】

参数	描述
patch _name	补丁名称。 当不存在此参数值时：命令用于显示设备中所有已安装的补丁及各补丁的基本信息。 当存在此参数值时：命令用于显示对应补丁的详细信息，补丁内容，校验组件内容是否完整等。

【命令模式】 特权模式

【缺省级别】 2

【使用指导】 该命令可以查看已安装的补丁，以及补丁信息

【配置举例】 1．盒式设备显示当前已安装所有补丁。

```
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
```

使用该命令形式，可以获取设备内已安装的所有补丁基本信息。

字段	说
Package	补丁名称
status	补丁状态
Version	组件补丁版本信息
Build time	补丁在服务器上编译完成的时间
Size	补丁包含内容的大小
Install time	设备安装该补丁的时间
Description	补丁功能的简单描述

盒式设备显示当前设备已安装的特定补丁信息。

```
Ruijie# show component bridge
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
     Package files:
        /lib64
        /lib64/libbridge.so
        /sbin
        /sbin/bridge

    Package file validate: [OK]
```

除了补丁基本信息外还包括：

字段	说明
Package file validate	校验补丁包含文件的完整性。如果所有文件都正常则显示结果[OK]；如果部分文件丢失或文件被修改，则显示结果[ERR]，并明确指出哪个文件丢失或被修改。
Package files	列出补丁包内包含的所有文件

【提示信息】 执行后显示设备存在的补丁信息。

```
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
```

【平台说明】 -

7.8 show upgrade file

显示存放在设备文件系统中的安装包文件信息。

show upgrade file *url*

【参数说明】

参数	描述
url	安装包文件存放的本地 *url* 路径。

【命令模式】 特权模式

【缺省级别】 2

【使用指导】 下载安装包文件到本地文件系统后可使用该命令预先查看安装包的主要信息。

【配置举例】 1．显示安装包文件信息。

```
Ruijie# show upgrade file flash://bridge_eg1000m_2.3.1.1252ea-1.mips.rpm
Name : bridge
Version:1.0.1.23cd34aa
Package type      : common component
Support target    : eg1000m
Size              : 26945
Build time        : Wed Dec  7 00:54:56 2013
Install date      : (not installed)
Description       : this is a bridge package
```

```
Package files :
    Package files:
       /lib64
       /lib64/libbridge.so
       /sbin
       /sbin/bridge
```

使用该命令可以获取包内信息。

字段	说明
Name	包名称
Version	包发布版本信息
Package type	包类型
Support target	包支持的产品说明
Size	包含内容的大小
Build time	包编译时间
Install date	包安装日期
Description	包描述信息
Package files	包内包含的所有内容

【提示信息】 执行显示安装包信息。

```
Name : bridge
Version:1.0.1.23cd34aa
Package type      : common component
Support target    : eg1000m
Size              : 26945
Build time        : Wed Dec  7 00:54:56 2013
Install date      : (not installed)
Description       : this is a bridge package
Package files :
    Package files:
       /lib64
       /lib64/libbridge.so
       /sbin
       /sbin/bridge
```

【平台说明】 -

7.9 show upgrade history

显示升级历史信息。

show upgrade history

【参数说明】

参数	描述
-	-

【命令模式】 特权模式

【缺省级别】 2

【使用指导】 -

【配置举例】 -

【提示信息】

```
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
```

【平台说明】 -

7.10 upgrade

安装，升级本地文件系统内安装包。

upgrade *url* [**force**]

【参数说明】

参数	描述
url	*url* 为安装包存放的本地路径。该命令用于升级设备内存放的安装包。
force	**force** 表示强制升级

【缺省配置】 -

【命令模式】 特权模式

【缺省级别】 2

【使用指导】 该命令支持各子系统组件安装包，功能组件安装包，热补丁包。使用该命令前，先使用 copy 命令将功能包拷入设备文件系统内。

当使用该命令、不指定范围参数时，升级功能将按照自动同步配置，对匹配到的系统部件进行升级。

【配置举例】 1．设备升级 main 包。

```
Ruijie#upgrade usb0:/eg1000m_main_1.0.0.0f328e91.bin
 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!
```

【检验方法】

1. 使用 **show version detail** 查看子系统组件是否升级成功。
2. 使用 **show component** 查看功能组件是否升级成功。
3. 使用 **show patch** 查看热补丁是否安装成功。

【提示信息】 1．升级成功提示：

```
Upgrade info [OK]
```

2．安装包无效或被损坏重新获取安装包并执行升级命令：

```
Invalid package file
```

3．设备不支持该安装包，重新获取安装包并执行升级命令

```
Device don't support
```

4．设备无需升级：

```
The version in device is newer or the same
```

5．升级空间不足，检查设备附带的 U 盘是否完好：

```
No enough space for decompress
```

6．出现严重问题，系统损坏，联系客服处理：

```
No enough space,rootfs been destroyed. Please upgrade in uboot
```

7．系统中已存在补丁包，需先卸旧补丁包

```
Already exist patch, please uninstall before upgrade
```

8．补丁包不适用于该系统，更换补丁包：

```
Patch compatibility err
```

9．该设备无法使用此补丁包升级，重新获取补丁包：

```
some origin cmpnt has change
```

【常见错误】 -

【平台说明】 -

7.11 upgrade auto

一键安装升级包，对于 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。

upgrade auto *url* [**force**]

【参数说明】

参数	描述
url	系统自动升级时，所使用的升级包的路径
force	**force** 表示强制升级

【命令模式】 特权模式

【缺省级别】 2

【使用指导】

执行该命令对 VSU 系统进行自动升级。

使用该命令前须将新版本的软件下载到设备上（例如通过 copy tftp 命令）。

在同一次升级过程中，请勿将 **upgrade auto** 命令与其它升级命令（如 **upgrade**）同时使用；如果自动升级过程执行失败退出，请按系统提示执行版本恢复过程。

自动升级过程中，请勿重复执行更新系统安装包（包括 copy tftp 和 U 盘拷备方式）或升级相关操作（upgrade /upgrade auto 等）。

在自动升级过程中，请勿执行板卡插拔、热备切换、机箱下电、VSU 软硬件配置变更等操作。

【配置举例】

1．设备升级 main 包。

```
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】

4. 使用 **show version detail** 查看子系统组件是否升级成功。
5. 使用 **show component** 查看功能组件是否升级成功。
6. 使用 **show patch** 查看热补丁是否安装成功。

【提示信息】

1．升级成功提示：

```
Upgrade info [OK]
```

2．安装包无效或被损坏重新获取安装包并执行升级命令：

```
Invalid package file
```

3．设备不支持该安装包，重新获取安装包并执行升级命令

```
Device don't support
```

4．设备无需升级：

```
The version in device is newer or the same
```

5．升级空间不足，检查设备附带的 U 盘是否完好：

```
No enough space for decompress
```

6．出现严重问题，系统损坏，联系客服处理：

```
No enough space,rootfs been destroyed. Please upgrade in uboot
```

	7．系统中已存在补丁包，需先卸旧补丁包
	`Already exist patch, please uninstall before upgrade`
	8．补丁包不适用于该系统，更换补丁包：
	`Patch compatibility err`
	9．该设备无法使用此补丁包升级，重新获取补丁包：
	`some origin cmpnt has change`

【常见错误】	-
【平台说明】	-

7.12 upgrade download tftp

下载并安装，升级 tftp 服务器上的安装包。

upgrade download tftp:/*path* [**force**]

【参数说明】

参数	描述
path	*path* 为 tftp 服务器上安装包的路径，该命令自动从服务器上下载安装包，并自动升级。
force	表示强制升级

【缺省配置】 -

【命令模式】 特权模式

【缺省级别】 2

【使用指导】 该命令支持各子系统组件安装包，功能组件安装包，热补丁包。使用该命令自动完成安装文件拷贝操作并升级。

【配置举例】 1．升级 main 包。

```
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 to take effect!
```

【检验方法】

7. 使用 **show version detail** 查看子系统组件是否升级成功。
8. 使用 **show component** 查看功能组件是否升级成功。
9. 使用 **show patch** 查看热补丁是否安装成功。

【提示信息】

1．升级成功提示：

```
Upgrade info [OK]；
```

2．安装包无效或被损坏重新获取安装包并执行升级命令：

```
Invalid package file
```

3．设备不支持该安装包，重新获取安装包并执行升级命令：

```
Device don't support
```

4．设备无需升级：

```
The version in device is newer or the same
```

5．升级空间不足，检查设备附带的 U 盘是否完好：

```
No enough space for decompress
```

6．出现严重问题，系统损坏，联系客服处理：

```
No enough space, rootfs been destroyed. Please upgrade in uboot
```

7．系统中已存在补丁包，需先卸旧补丁包：

```
Already exist patch, please uninstall before upgrade
```

8．补丁包不适用于该系统，更换补丁包：

```
Patch compatibility err
```

9．该设备无法使用此补丁包升级，重新获取补丁包：

```
Some origin component has change
```

【常见错误】 -

【平台说明】 -

7.13 upgrade rollback

使子系统回滚到升级前的版本。

upgrade rollback

【参数说明】

参数	描述
-	-

【缺省配置】 -

【命令模式】 特权模式

【缺省级别】 2

【使用指导】 若升级子系统后设备不能正常工作，则可采用此命令，仅当上次成功的升级了子系统组件，该命令才能生效。

设备重启后命令生效，无法通过连续执行此命令实现递归回滚。

【配置举例】 1．盒式设备使子系统回滚到升级前的版本。

```
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!
```

【检验方法】 重启设备后，使用 **show version detail** 查看子系统组件是否成功回滚

【提示信息】 1．成功提示：

```
 Rollback success!
 Restart to take effect !
```

2．上次并没有升级子系统组件，因此子系统组件无法回滚：

```
Not subsys package last upgrade
```

3．上次升级并未成功，因此不回滚：

```
Last upgrade err or skip
```

4．未执行过升级命令，或者已经执行过回滚操作：

```
Monitor file lost
```

【常见错误】
- 上一次并非针对子系统组件升级，而是功能组件包，热补丁包等
- 已经执行过子系统回滚操作。

【平台说明】 -

8 CWMP

8.1 acs password

配置 CPE 连接 ACS 时用于认证的密码。

acs password {*password* | *encryption-type encrypted-password*}

恢复缺省配置

no acs password

【参数说明】

参数	描述
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。

【缺省配置】 encryption-type 默认为 0，encrypted-password 默认为空。

【命令模式】 cwmp 配置模式

【缺省级别】 1

【使用指导】 配置 CPE 连接 ACS 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：

- 密码必须为英文字母或数字。
- 密码中间及结尾的空格则作为密码的一部分。

【配置举例】 1：配置 CPE 连接 ACS 时用于认证的密码为“123”。

```
Ruijie#config
Enter configuration commands, one per line.  End with CNTL/Z.
Ruijie(config)#cwmp
Ruijie(config-cwmp)#acs password 123
Ruijie(config-cwmp)#
```

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

【提示信息】 1: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，则提示错误

```
%%Error: Invalid Encrypted Password
```

2:如果用户输入密码类型为明文，密码长度超过 100,则提示错误.

```
%%Error: The Length of ACS's Password is Too Long
```

3:如果用户输入密码类型为明文，并且包含非法字符,则提示错误

```
%%Error: Password String Include Invalid Characters!
```

【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。
- 如果用户输入密码类型为明文，密码长度超过 100。
- 如果用户输入密码类型为明文，并且包含非法字符。

【平台说明】 -

8.2 acs url

配置 CPE 连接 ACS 的 URL。

acs url *url*

恢复缺省配置。

no acs url

【参数说明】

参数	描述
url	ACS 的 URL。

【缺省配置】 为空。

【命令模式】 cwmp 配置模式

【缺省级别】 1

【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 格式必须为：http://host[:port]/path（或是 https://host[:port]/path）的格式。
- ACS URL 的最大长度为 256 个字符。

【配置举例】 1：配置 CPE 要连接 ACS 的 URL 为“http://10.10.10.1:8080/acs”。

```
Ruijie#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Ruijie(config)#cwmp
Ruijie(config-cwmp)#acs url http://10.10.10.1:8080/acs
Ruijie(config-cwmp)#
```

2：配置 CPE 要连接 ACS 的 URL 为“http://www.test.com/service/tr069servlet”。

```
Ruijie#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Ruijie(config)#cwmp
Ruijie(config-cwmp)#acs url http://www.test.com/service/tr069servlet
```

```
Ruijie(config-cwmp)#
```

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

【提示信息】 1：如果 ACS URL 地址为 NULL，则提示错误。

```
input acs attribute parameter is null
```

【常见错误】
- ACS URL 没按要求的格式输入。
- ACS URL 的长度超过 256 个字符。

【平台说明】 -

8.3 acs username

配置 CPE 连接 ACS 时用于认证的用户名。

acs username *username*

恢复缺省配置。

no acs username

【参数说明】

参数	描述
- *username*	CPE 连接 ACS 用于认证的用户名。

【缺省配置】 为空。

【命令模式】 cwmp 配置模式

【缺省级别】 1

【使用指导】 配置 CPE 连接 ACS 时用于认证的用户名。

【配置举例】 1：配置 CPE 连接 ACS 时用于认证的用户名为“admin”

```
Ruijie#config
Enter configuration commands, one per line.  End with CNTL/Z.
Ruijie(config)#cwmp
Ruijie(config-cwmp)#acs username admin
Ruijie(config-cwmp)#
```

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

【提示信息】 1：如果用户输入用户名为 NULL，则提示错误。

```
input acs attribute parameter is null
```

【常见错误】 无。

【平台说明】 -

8.4 cpe back-up

配置 CPE 主程序/配置备份恢复功能。
cpe back-up [**delay-time** *seconds*]
关闭 CPE 的主程序/配置备份恢复功能
no cpe back-up

【参数说明】

参数	描述
seconds	CPE 主程序/配置备份恢复的延迟时间 ,单位为秒 ,取值范围 30~10000。

【缺省配置】 默认值为 60 秒。

【命令模式】 cwmp 配置模式

【缺省级别】 1

【使用指导】 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。

【配置举例】 1：关闭 CPE 主程序/配置备份恢复功能。

```
Ruijie#config
Enter configuration commands, one per line.  End with CNTL/Z.
Ruijie(config)#cwmp
Ruijie(config-cwmp)#no cpe back-up
Ruijie(config-cwmp)#
```

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

【提示信息】 -

【常见错误】 无。

【平台说明】 -

8.5 cpe inform

配置 CPE 周期性 INFORM 通告功能。

cpe inform [**interval** *seconds*] [**starttime** *time*]

恢复缺省配置

no cpe inform

【参数说明】

参数	描述
seconds	配置 CPE 周期性 INFORM 通告时间间隔。单位为秒，取值范围 30～3600。
time	开始周期性 INFORM 的日期时间，格式为 yyyy-mm-ddThh:mm:ss

【缺省配置】 默认值为 600 秒。

【命令模式】 cwmp 配置模式

【缺省级别】 1

【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。

CPE 周期性 INFORM 通告时间间隔越短，ACS 就越能及时地跟踪 CPE 的最新状态，同时 CPE 与 ACS 的会话也越频繁，所耗 CPE 与 ACS 的资源就越多，用户需要根据当前的网络状况以及 ACS 的性能配置合适的时间间隔。

【配置举例】 1：配置 CPE 周期 INFORM 通告时间间隔为 60 秒。

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

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

【提示信息】 -

【常见错误】 无。

【平台说明】 -

8.6 cpe password

配置 ACS 连接 CPE 时用于认证的密码，该命令的 no 形式恢复缺省配置。

cpe password {*password* **|** *encryption-type encrypted-password***}**

恢复缺省配置

no cpe password

【参数说明】

参数	描述
password	ACS 连接 CPE 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。

【缺省配置】 encryption-type 默认为 0，encrypted-password 默认为空。

【命令模式】 cwmp 配置模式

【缺省级别】 1

【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：

- 由英文字母及数字组成。
- 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。

【配置举例】 1：配置 ACS 连接 CPE 时用于认证的密码为“123”。

```
Ruijie#config
Enter configuration commands, one per line.  End with CNTL/Z.
Ruijie(config)#cwmp
Ruijie(config-cwmp)#cpe password 123
Ruijie(config-cwmp)#
```

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

【提示信息】 1: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，则提示错误

```
%%Error: Invalid Encrypted Password
```

2:如果用户输入密码类型为明文，密码长度超过 100,则提示错误.

```
%%Error: The Length of ACS's Password is Too Long
```

3:如果用户输入密码类型为明文，并且包含非法字符,则提示错误

```
%%Error: Password String Include Invalid Characters!
```

4:如果用户输入密码类型为密文，并且包含非法字符（合法字符只能是：数字 0~9、字符 a~f、A~F），则提示错误。

```
%%Error: Invalid Encrypted Password
```

【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。
- 如果用户输入密码类型为明文，密码长度超过 100。
- 如果用户输入密码类型为明文，并且包含非法字符。
- 如果用户输入密码类型为密文，并且包含非法字符（合法字符只能是：数字 0~9、字符 a~f、A~F）。

【平台说明】 -

8.7 cpe url

配置 ACS 连接 CPE 的 URL。

cpe url *url*

恢复缺省配置

no cpe url

【参数说明】

参数	描述
url	CPE 的 URL。

【命令模式】 cwmp 配置模式

【缺省配置】 为空。

【缺省级别】 1

【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】 1：配置 ACS 要连接 CPE 的 URL 为“http://10.10.10.1:7547/”。

```
Ruijie#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Ruijie(config)#cwmp
Ruijie(config-cwmp)#cpe url http://10.10.10.1:7547/
Ruijie(config-cwmp)#
```

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

【提示信息】 1：如果 CPE 的 URL 地址为 NULL，则提示错误。

```
input CPE attribute parameter is null
```

【常见错误】
- CPE URL 没按要求的格式输入。
- CPE URL 的长度超过 256 个字符。

【平台说明】 -

8.8 cpe username

配置 ACS 连接 CPE 时用于认证的用户名。

cpe username *username*

恢复缺省配置。

no cpe username

【参数说明】

参数	描述
username	配置 ACS 连接 CPE 用于认证的用户名

【命令模式】 cwmp 配置模式

【缺省配置】 为空。

【缺省级别】 1

【使用指导】 配置 ACS 连接 CPE 时用于认证的用户名。

【配置举例】 1：配置 ACS 连接 CPE 时用于认证的用户名为“admin”

```
Ruijie#config
Enter configuration commands, one per line.  End with CNTL/Z.
Ruijie(config)#cwmp
Ruijie(config-cwmp)#cpe username admin
Ruijie(config-cwmp)#
```

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

【提示信息】 1：如果用户输入用户名为 NULL，则提示错误。

```
input acs attribute parameter is null
```

【常见错误】 无。

【平台说明】 -

8.9 cwmp

配置开启/关闭 CWMP 功能。

cwmp

关闭 CWMP 功能。

no cwmp

【参数说明】

参数	描述

【命令模式】 全局配置模式

【缺省级别】 1

【使用指导】 配置 CWMP 的功能状态。

【配置举例】 1：关闭 CWMP 功能。

```
Ruijie#config
Enter configuration commands, one per line.  End with CNTL/Z.
Ruijie(config)#no cwmp
Ruijie(config)#
```

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

【提示信息】 -

【常见错误】 无。

【平台说明】 -

8.10 disable download

配置关闭从 ACS 下载主程序和配置文件的功能。

disable download

恢复缺省配置

no disable download

【参数说明】

参数	描述

【命令模式】 cwmp 配置模式

【缺省级别】 1

【缺省配置】 CPE 文件下载功能为开启（**no disable download**）。

【使用指导】 配置关闭从 ACS 下载主程序和配置文件的功能。

- 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。

【配置举例】 1：配置关闭从 ACS 下载主程序和配置文件的功能。

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

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

【提示信息】 -

【常见错误】 无。

【平台说明】 -

8.11 disable upload

配置关闭向 ACS 上传配置文件和日志文件的功能。

disable upload

恢复缺省配置

no disable upload

【参数说明】

参数	描述

【命令模式】 cwmp 配置模式

【缺省配置】 CPE 文件上传功能为开启（**no disable upload**）。

【缺省级别】 1

【使用指导】 配置关闭向 ACS 上传配置文件和日志文件的功能

【配置举例】 1：配置关闭向 ACS 上传配置文件和日志文件的功能。

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

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

【提示信息】 -

【常见错误】 无。

【平台说明】 -

8.12 show cwmp configuration

显示 CWMP 功能的当前配置

show cwmp configuration

【参数说明】

参数	描述

【命令模式】 特权模式

【缺省级别】 1

【使用指导】

【配置举例】 1：显示 CWMP 功能的当前配置。

```
Ruijie(config-cwmp)#show cwmp configuration
CWMP Status                    : enable
ACS URL                        : http://www.ruijie.com.cn/acs
ACS username                   : admin
ACS password                   : ******
CPE URL                        : http://10.10.10.2:7547/
```

```
CPE username                    : ruijie
CPE password                    : ******
CPE inform status               : disable
CPE inform interval             : 60s
CPE inform start time           : 0:0:0 0 0 0
CPE wait timeout                : 50s
CPE download status             : enable
CPE upload status               : enable
CPE back up status              : enable
CPE back up delay time          : 60s
```

字段解释：

字段	说明
CWMP Status	CWMP 功能的使能状态。
ACS URL	CPE 连接 ACS 的 URL。
ACS username	CPE 连接 ACS 的用户名。
ACS password	CPE 连接 ACS 的密码。
CPE URL	ACS 连接 CPE 的 URL。
CPE username	ACS 连接 CPE 的用户名。
CPE password	ACS 连接 CPE 的密码。
CPE inform status	CPE 的周期性 INFORM 通告状态。
CPE inform interval	CPE 周期性 INFORM 通告时间间隔。
CPE wait timeout	CPE 会话超时时间
CPE inform start time	CPE 周期性 INFORM 开始通告日期时间。
CPE download status	是否接受从 ACS 下载主程序和配置文件。
CPE upload status	是否向 ACS 上传配置文件和日志文件
CPE back up status	是否开启主程序/配置恢复的功能状态
CPE back up delay time	主程序/配置恢复的等待延迟时间

【提示信息】 -

【平台说明】 -

8.13 show cwmp status

显示 CWMP 的当前运行状态

show cwmp status

【参数说明】

参数	描述

【命令模式】 特权模式

【缺省级别】 1

【使用指导】

【配置举例】 1：显示 CWMP 的当前运行状态。

```
Ruijie(config-cwmp)#show cwmp status
CWMP Status                     : enable
Session status                  : Close
Last success session            : Unknown
Last success session time       : Thu Jan  1 00:00:00 1970
Last fail session               : Unknown
Last fail session time          : Thu Jan  1 00:00:00 1970
Session retry times             : 0
```

字段解释：

字段	说明
CWMP Status	CWMP 功能的使能状态。
Session status	CPE 与 ACS 的当前会话状态。
Last success session	最后一次成功会话的类型。
Last success session time	最后一次成功会话结束时间
Last fail session	最后一次失败会话的类型
Last fail session time	最后一次失败会话结束时间
Session retry times	当前会话重试次数。

【提示信息】 -

【平台说明】 -

8.14 timer cpe-timeout

配置 ACS 无响应 CPE 超时时间。

timer cpe- timeout *seconds*

恢复缺省配置

no timer cpe-timeout

【参数说明】

参数	描述
seconds	超时时间。单位为秒，取值范围 10～600。

【命令模式】 cwmp 配置模式。

【缺省配置】 默认值为 30 秒。

【缺省级别】 1

【使用指导】 配置 ACS 无响应 CPE 超时时间。

- 由于一些异常情况（如网络断开连接）无法收到 ACS 的响应时会话等待的最大时延

【配置举例】 1：配置 ACS 无响应 CPE 超时时间为 50 秒。

```
Ruijie#config
Enter configuration commands, one per line.  End with CNTL/Z.
Ruijie(config)#cwmp
Ruijie(config-cwmp)#timer cpe-timeout 50
Ruijie(config-cwmp)#
```

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

【提示信息】 -

【常见错误】 无。

【平台说明】 -

9 系统日志

9.1 clear logging

清除内存缓冲区中的日志信息。
clear logging

【参数说明】

参数	描述
-	-

【命令模式】 特权用户模式

【缺省级别】 1

【使用指导】 该命令只清除内存缓冲区中日志报文内容。不能清除日志报文的统计信息。

【配置举例】 1：下面示例清除内存缓冲区中日志报文内容。

```
Ruijie# clear logging
```

【提示信息】 -

【平台说明】 -

9.2 logging

将日志记录到指定的 Syslog Server。
logging { *ip-address* } [**udp-port** *port*]

删除 Syslog Server 列表中的指定地址的 Syslog Server。
no logging { *ip-address* }

恢复日志发送 Syslog Server 的默认端口号（514）。
no logging { *ip-address* } **udp-port**

【参数说明】

参数	描述
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）

【缺省配置】 默认不向任何 Syslog Server 发送日志信息

【命令模式】 全局配置模式

【缺省级别】 14

【使用指导】 该命令指定一个 Syslog server 来接收设备的日志信息。用户可以配置多达 5 个 Syslog Server。日志信息将同时发给配置的所有 Syslog Server。

【配置举例】 1：下面的示例指定一个地址为 202.101.11.1 的 syslog server：

```
Ruijie(config)# logging 202.101.11.1
```

2：下面的示例指定一个地址为 202.101.11.1，端口号为 8099 的 syslog server：

```
Ruijie(config)# logging 202.101.11.1 udp-port 8099
```

【检验方法】 1：使用 **show logging** 命令，可以查看设置的日志服务器地址。

【提示信息】 1：如果设备上已经配置的 Syslog Server 超过 5 个，则提示错误。

```
%%Warning: Can not configure more than 5 syslog servers!
```

【常见错误】 -

【平台说明】 -

9.3 logging buffered

设置记录日志信息的内存缓冲区参数（日志信息严重性、缓冲区大小）。
logging buffered [*buffer-size*] [*level*]

禁止在内存缓冲区中记录日志信息。
no logging buffered

将把内存缓冲区大小恢复为缺省值。
default logging buffered

【参数说明】

参数	描述
buffer-size	缓冲区大小，与具体设备类型有关： 核心/汇聚交换机取值范围从 4K 到 10M Bytes。 接入交换机取值范围从 4K 到 1M Bytes。

	其他设备取值范围从 4K 到 128K Bytes。
level	日志信息的严重性，从 0 到 7。可以使用级别名称，也可以直接使用数字。

【缺省配置】

缓冲区默认大小与具体设备类型有关：

核心交换机默认为 1M Bytes。

汇聚交换机默认为 256K Bytes。

接入交换机默认为 128K Bytes。

其他设备默认为 4K Bytes。

日志信息严重性默认为 7。

【命令模式】 全局配置模式

【缺省级别】 14

【使用指导】 内存缓冲区空间是循环使用的，如果指定大小的内存区被写满，则最早的日志信息将被覆盖。要查看内存缓冲区的日志信息，请使用特权用户命令 **show logging**。

内存缓冲区中的日志信息是临时性的，设备重启或者执行特权用户命令 **clear logging**，缓冲区中的日志信息将被清除。如果要跟踪问题，应该将日志写到扩展 FLASH 或者发送给 Syslog Server。

日志信息分为以下 8 个级别：

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

值越小，级别越高，即 0 级别的信息是最高级别的信息。

当指定设备允许显示的日志信息级别以后，等于或低于所设置值级别的日志信息将被允许显示。

在系统运行较长时间以后，此时修改日志缓冲大小，特别是较大缓冲的时候，可能不会成功，会提示失败信息。这一般是因为系统运行时间较长，可供分配的连续内存空间不足所致。建议在系统刚启动时修改日志缓冲大小。

【配置举例】 1：下面示例设置只允许级别为 6 以及低于 6 的日志信息记录在大小为 10000 字节的内存缓冲区中：

```
Ruijie(config)# logging buffered 10000 6
```

【检验方法】 1：使用 **show logging** 命令，可以查看设置的日志内存缓冲区的参数。

【提示信息】 -

【常见错误】 -

【平台说明】 -

9.4 logging console

设置允许在控制台上显示的日志信息级别
logging console [*level*]

禁止在控制台上打印日志报文。
no logging console

【参数说明】

参数	描述
level	日志报文的严重性，范围从 0 到 7。可以使用级别名称，也可以直接使用数字。关于日志信息严重性的详细说明，请参照如下【使用指导】。

【缺省配置】 7（Debugging，调试信息)

【命令模式】 全局配置模式

【缺省级别】 14

【使用指导】 设置一个日志严重性以后，在数值上等于或低于该严重性级别的日志报文将被显示在控制台上。
通过 **show logging** 命令可以查看日志设置的相关参数和统计。
日志信息分为以下 8 个级别：

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

【配置举例】 1：下面示例设置允许在控制台显示的日志信息级别为 6：

```
Ruijie(config)# logging console informational
```

【检验方法】 1:使用 **show logging** 命令,可以查看设置的允许在控制台上显示的日志信息级别和已经输出到控制台上面的日志条目。

【提示信息】 -

【常见错误】 -

【平台说明】 -

9.5 logging count

打开日志统计功能。
logging count

清除日志统计数据并关闭日志统计功能。
no logging count

【参数说明】

参数	描述
-	-

【缺省配置】 日志统计功能关闭。

【命令模式】 全局配置模式

【缺省级别】 14

【使用指导】 通过此命令打开日志统计功能。从命令打开时开始统计。执行 **no logging count** 命令时，统计功能被关闭，并且统计数据被清除。

【配置举例】 1：打开日志统计功能：

```
Ruijie(config)# logging count
```

【检验方法】 1：使用 **show logging** 命令，可以查看是否打开日志统计功能。

【提示信息】 -

【常见错误】 -

【平台说明】 -

9.6 logging delay-send file

配置延迟上送时缓存在设备本地的日志文件名。
logging delay-send file flash:*filename*

恢复延迟上送时缓存在设备本地的日志文件名为默认值。
no logging delay-send file

【参数说明】

参数	描述
flash:*filename*	延迟上送的日志文件名

【缺省配置】 默认发送到远端服务器的日志文件名格式为：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。

【命令模式】 全局配置模式

【缺省级别】 14

【使用指导】 通过此命令可以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。

【配置举例】 1：配置延迟上送的日志文件名为 log_server：

```
Ruijie(config)# logging delay-send file flash:log_server
```

【检验方法】 1：使用 **show logging** 命令，可以查看延迟上送时缓存在设备本地的日志文件名。

【提示信息】 -

【常见错误】 -

【平台说明】 -

9.7 logging delay-send interval

配置日志延迟上送给服务器的时间间隔。
logging delay-send interval *seconds*

恢复日志延迟上送给服务器的时间间隔成默认值。
no logging delay-send interval

【参数说明】

参数	描述
seconds	日志延迟上送的时间间隔（单位为秒）

【缺省配置】 默认时间间隔是 3600 秒（1 小时）。

【命令模式】 全局配置模式

【缺省级别】 14

【使用指导】 通过此命令设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。

【配置举例】 1：配置日志延迟上送的时间间隔是 600 秒（1 分钟）：

```
Ruijie(config)# logging delay-send interval 600
```

【检验方法】 1：使用 **show logging** 命令，可以查看日志延迟上送的时间间隔。

【提示信息】 -

【常见错误】 -

【平台说明】 -

9.8 logging delay-send server

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

删除日志延迟上送给服务器的地址和上报方式。
no logging delay-send server { *ip-address* }

【参数说明】

参数	描述

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

【缺省配置】 默认不向任何 FTP 或者 TFTP Server 发送日志信息。

【命令模式】 全局配置模式

【缺省级别】 14

【使用指导】 该命令指定一个 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】 1：下面的示例指定一个地址为 192.168.23.12、用户名 admin、密码 admin 的 FTP Server：

```
Ruijie(config)# logging delay-send server 192.168.23.12 mode ftp user admin password admin
```

【检验方法】 1：使用 **show logging** 命令，可以查看日志延迟上送服务器的地址和上报方式。

【提示信息】 -

【常见错误】 -

【平台说明】 -

9.9 logging delay-send terminal

打开延时上送日志输出到控制台和远程终端。
logging delay-send terminal

关闭延时上送日志输出到控制台和远程终端。
no logging delay-send terminal

【参数说明】

参数	描述
-	-

【缺省配置】 缺省情况下关闭延时上送的日志输出到控制台和远程终端。

【命令模式】 全局配置模式

【缺省级别】 14

【使用指导】 可以使用此命令打开延时上送的日志输出到控制台和远程终端。

【配置举例】 1：下面的示例打开延时上送的日志输出到控制台和远程终端：

```
Ruijie(config)# logging delay-send terminal
```

【检验方法】 1：使用 **show logging** 命令，可以查看日志输出到控制台和远程终端的开关状态。

【提示信息】 -

【常见错误】 -

【平台说明】 -

9.10 logging facility

设置日志信息的设备值
logging facility *facility-type*

恢复设备值为默认值(23)。
no logging facility

【参数说明】

参数	描述
facility-type	Syslog 设备值，具体的设置值请参考使用指导。

【缺省配置】 在开启 RFC5424 日志格式的情况下，设备值缺省为 16（Local0，Local use）；
在没有开启 RFC5424 日志格式的情况下，设备值缺省为 23（Local7，Local use）。

【命令模式】 全局配置模式

【缺省级别】 14

【使用指导】 日志信息的设备值用于构造日志信息的优先级，具体的计算公式为：
priority（优先级） = Facility（设备值） * 8 + serverity（日志等级）。
计算出来后的日志优先级，将作为日志报文的一部分发送给日志服务器，日志服务器可以用于标志不同的日志来源，查找、过滤对应日志源的日志。
下表是 Syslog 可能的设备值：

Numerical Code	Facility

0 (kern)	Kernel messages
1 (user)	User-level messages
2 (mail)	Mail system
3 (daemon)	System daemons
4 (auth1)	security/authorization message
5 (syslog)	Messages generated internally by syslogd
6 (lpr)	Line printer system
7 (news)	USENET news
8 (uucp)	Unix-to-Unix copy system
9 (clock1)	Clock daemon
10 (auth2)	security/authorization message
11 (ftp)	FTP daemon
12 (ntp)	NTP daemon
13 (logaudit)	Log audit
14 (logalert)	Log alert
15 (clock2)	Clock daemon
16 (local0)	Local use
17 (local1)	Local use
18 (local2)	Local use
19 (local3)	Local use
20 (local4)	Local use
21 (local5)	Local use
22 (local6)	Local use
23 (local7)	Local use

默认设备值为(local7)23。

【配置举例】 1：下面的设置 Syslog 设备值为 kernel：

```
Ruijie(config)# logging facility kern
```

【检验方法】 -

【提示信息】 -

【常见错误】 -

【平台说明】 -

9.11 logging file

将日志信息保存在文件中，日志文件可以保存在硬盘、扩展 FLASH、USB 中的一种。

logging file { **sata0:***filename* | **flash:***filename* } [*max-file-size*] [*level*]

取消在扩展 FLASH 中记录日志信息。

no logging file

【参数说明】

参数	描述
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
filename	日志文件名。不带文件类型，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	允许被记录到日志文件中的日志信息级别。可以使用级别名称，也可以直接使用数字。缺省写到扩展 FLASH 的中日志级别为 6。关于日志信息的级别，请参考【使用指导】。

【缺省配置】 不能将日志信息记录到扩展 FLASH 中。

【命令模式】 全局配置模式

【缺省级别】 14

【使用指导】 如果没有 Syslog Server，或者基于各种安全考虑不希望在网络中传输日志信息，可以选择将日志信息直接保存在扩展 FLASH 中。

日志文件后缀为固定为 txt，配置文件后缀名将被拒绝。

将日志信息记录到扩展 FLASH，必须另外采购扩展 FLASH，如果没有采购扩展 FLASH，logging file flash 将被自动隐藏，不允许进行配置。

日志信息分为以下 8 个级别：

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

【配置举例】 1：下面示例将日志信息记录在扩展 FLASH 中，文件名为 syslog.txt，文件大小为 128K，日志信息级别为 6。

```
Ruijie(config)# logging file flash:syslog
```

【检验方法】 1：使用 **show logging** 命令，可以查看设置的日志信息保存在扩展 FLASH 中的相关参数。

【提示信息】 1：如果配置的时候日志文件名长度超过 20 个字符，假如配置时文件名长度为 21，则提示错误。

```
%Error: The file length must not be longer then 20, Current file length 21.
```

【常见错误】 -

【平台说明】 NBR2500D-E、NBR3000D-E、NBR3000D-UE 出厂带 SATA 硬盘。NBR108G-P 、NBR800G、NBR950G、NBR1500G、NBR2000G、NBR1000G-C、NBR2000G-C、NBR3000G-S、NBR1000G-E、NBR6120-E、NBR1300G-E、NBR1700G-E、NBR2100G-E、NBR6205-E、NBR6135-E、NBR6210-E、NBR6215-E 出厂无 SATA 硬盘。其中 NBR6205-E、NBR6135-E、NBR6210-E、NBR6215-E 可自行购买 SATA 硬盘使用。

9.12 logging file numbers

配置系统日志信息写入扩展 FLASH 中的文件个数。
logging file numbers *numbers*

取消配置日志文件的个数，恢复为默认值。
no logging file numbers

【参数说明】

参数	描述
numbers	日志文件的个数，范围：2~32，单位：个

【缺省配置】 日志文件的个数默认为 16 个。

【命令模式】 全局配置模式

【缺省级别】 14

【使用指导】 通过此命令设置日志文件的个数。可以通过 **no logging file numbers** 命令，将日志文件的个数恢复为默认值 16 个。
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。

【配置举例】 1：下面示例配置日志文件的个数为 8 个。

```
Ruijie(config)# logging file numbers 8
```

【检验方法】 1：使用 **show run** 命令，可以查看设置的日志文件个数。

【提示信息】 -

【常见错误】 -

【平台说明】 -

9.13 logging filter direction

将往某个方向的日志信息过滤掉。
logging filter direction { **all** | **buffer | file** | **server | terminal** }

清除对往某个方向的日志信息的过滤操作。
no logging filter direction { **all** | **buffer | file** | **server | terminal** }

【参数说明】

参数	描述
all	过滤往所有方向的日志信息（包括：Console 方向、VTY 终端、日志缓冲区、日志文件、日志服务器）
buffer	过滤往日志缓冲区的日志信息（即 show logging 命令显示出来的日志信息）
file	过滤往日志文件的日志信息
server	过滤往日志服务器的日志信息
terminal	过滤往控制台和 VTY 终端（包括 Telnet/SSH 等）的日志信息

【缺省配置】 过滤往所有方向的日志信息，即为 all

【命令模式】 全局配置模式

【缺省级别】 14

【使用指导】 用户配置了日志过滤功能后，通常情况下，会想要将匹配过滤规则后的日志信息，在所有方向上都过滤掉（包括：Console 方向、VTY 终端、日志缓冲区、日志文件、日志服务器），而某些情况下，用户可能只想过滤往特定方向的日志信息，比如：过滤掉的日志信息不需要到终端界面，但需要写入到日志文件，或发送给日志信息器，只需要配置过滤往 **terminal** 方向的日志信息。

【配置举例】 1：下面的例子配置过滤往 **terminal** 方向（包括：console 和 VTY 终端等）的日志信息：

```
Ruijie(config)# logging filter direction terminal
```

【检验方法】 -

【提示信息】 -

【常见错误】 -

【平台说明】 -

9.14 logging filter rule

配置日志信息的过滤规则。

logging filter rule { **exact-match module** *module-name* **mnemonic** *mnemonic-name* **level** *level* | **single-match** [**level** *level* | **mnemonic** *mnemonic-name* | **module** *module-name*] }

删除日志信息的“精确匹配”过滤规则。

no logging filter rule exact-match [**module** *module-name* **mnemonic** *mnemonic-name* **level** *level*]

删除日志信息的“单个匹配”过滤规则。

no logging filter rule single-match [**level** *level* | **mnemonic** *mnemonic-name* | **module** *module-name*]

【参数说明】

参数	描述
exact-match	精确匹配，若选择精确匹配，则后面的三个过滤选项都需要填写。
single-match	单个匹配，若选择单个匹配，则后面的三个过滤选项只需要填写其中的一个。
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*	日志信息等级，即填写要过滤的日志信息等级。

【缺省配置】 无日志信息过滤规则，不进行日志过滤

【命令模式】 全局配置模式

【缺省级别】 14

【使用指导】 1.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，在配置时，需要指定具体的模块名、助记符名称、日志等级。

2.某些情况下，用户可能想过滤掉某些类型的日志信息，则可以使用“单个匹配”规则，在配置时，只需要指定模块名、日志等级、助记符名称当中的一种。

⚠ 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。

【配置举例】 1：配置日志信息过滤规则为精确匹配，模块名为 LOGIN、日志等级为 5、助记符名称为 LOGOUT：

```
Ruijie(config)# logging filter rule exact-match module LOGIN mnemonic LOGOUT level 5
```

2：配置日志信息的过滤规则为单个匹配，模块名为 SYS：

```
Ruijie(config)# logging filter rule single-match module SYS
```

【检验方法】 -

【提示信息】 -

【常见错误】 -

【平台说明】 -

9.15 logging filter type

配置日志信息的过滤类型。

logging filter type { **contains-only** | **filter-only** }

恢复日志信息的过滤类型。

no logging filter type

【参数说明】

参数	描述
contains-only	“只包含”，代表：只输出包含了过滤规则里面的关键字信息的日志，其它没有包含过滤规则里面的日志不会输出。
filter-only	“只过滤”，代表：将过滤掉包含了过滤规则里面的关键字信息的日志，不会输出这些过滤掉的日志信息。

【缺省配置】 缺省的过滤类型为“只过滤”

【命令模式】 全局配置模式

【缺省级别】 14

【使用指导】 1.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，将刷屏的日志信息过滤掉。

2.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。

⚠ 在实际应用过程中，“只包含”和“只过滤”这两种过滤类型互斥，即同一时刻只能配置一种过滤类型。

⚠ 在配置过程中，若只配置了过滤方向、过滤类型，但是没有配置过滤规则，那么配置不会生效，即不会进行日志过滤操作。

【配置举例】 1：下面的例子配置日志信息过滤类型为“只包含”：

```
Ruijie(config)# logging filter type contains-only
```

【检验方法】 -

【提示信息】 -

【常见错误】 -

【平台说明】 -

9.16 logging flash flush

将系统缓冲区中的日志信息立即写入到 FLASH 文件中。

logging flash flush

【参数说明】

参数	描述
-	-

【缺省配置】 -

【命令模式】 全局配置模式

【缺省级别】 14

【使用指导】 在系统开启日志信息写 FLASH 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 FLASH 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 FLASH 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 FLASH 文件中

【配置举例】 1：下面示例将系统缓冲区中的日志信息立即写入到 FLASH 文件中。

```
Ruijie(config)# logging flash flush
```

【检验方法】 1：使用 **dir** 命令，可以查看写入到 FLASH 当中的日志文件。

【提示信息】 -

【常见错误】 -

【平台说明】 -

9.17 logging flash interval

配置系统日志信息写入扩展 FLASH 中的时间间隔。
logging flash interval *seconds*

取消配置日志信息写 FLASH 的时间间隔，恢复为默认值。
no logging flash interval

【参数说明】

参数	描述
interval *seconds*	日志信息写入到 FLASH 文件的时间间隔，范围：1~51840，单位：秒

【缺省配置】 日志信息写入 FLASH 文件的时间间隔默认为 3600s，即：1 个小时。

【命令模式】 全局配置模式

【缺省级别】 14

【使用指导】 通过此命令设置日志信息保存到 FLASH 文件中的时间间隔，且从命令配置后开始计时。可以通过 no logging flash interval 命令，将日志信息写 FLASH 文件的时间间隔恢复为默认值 3600s。

⚠ 为了避免系统太过频繁去写 FALSH 文件，时间间隔不要配置得太小。

【配置举例】 1：下面示例配置日志信息写 FLASH 文件的时间间隔为 5 分钟（300s）。

```
Ruijie(config)# logging flash interval 300
```

【检验方法】 1：使用 **show logging** 命令，可以查看设置的时间间隔相关参数。

【提示信息】 -

【常见错误】 -

【平台说明】 -

9.18 logging life-time

配置扩展 FLASH 中的日志文件的保存时间。
logging life-time level *level days*

取消配置日志的保存时间。
no logging life-time level *level*

【参数说明】

参数	描述
level	指定日志信息级别，可以使用级别名称，也可以直接使用数字。
days	日志信息级别对应的日志文件保存天数。

【缺省配置】 缺省不对日志文件的保存时间进行限制，日志文件的保存时间受限于用户配置的日志文件的大小。

【命令模式】 全局配置模式

【缺省级别】 14

【使用指导】 考虑到扩展 FLASH 的大小和不同级别日志信息的重要性程度不同，可以针对不同级别的日志信息指定不同的保存天数。

⚠ 当用户开启了基于时间的日志保存功能，则原本基于文件大小的日志保存功能将失效，且日志信息文件统一存放在扩展 FLASH 的 syslog/目录下。

【配置举例】 1：下面示例配置日志信息级别为 6 的日志信息，保存天数为 10 天：

```
Ruijie(config)# logging life-time level 6 10
```

【检验方法】 -

【提示信息】 -

【常见错误】 -

【平台说明】 -

9.19 logging monitor

设置允许在 VTY 窗口（Telnet 窗口、SSH 窗口等）上显示的日志信息级别。
logging monitor [*level*]

禁止在 VTY 窗口上打印日志报文。
no logging monitor

【参数说明】

参数	描述
level	日志报文的严重性。可以使用级别名称，也可以直接使用数字。关于日志信息严重性的详细说明，请参考【使用指导】。

【缺省配置】 允许在 VTY 窗口上显示的日志信息级别为 7（Debugging，调试信息）

【命令模式】 全局配置模式

【缺省级别】 14

【使用指导】 要在 VTY 窗口上打印日志信息，首先执行特权用户命令 **terminal monitor**，允许在当前 VTY 窗口打印日志信息。然后可以执行全局配置模式命令 **logging monitor** 来定义显示到 VTY 窗口上面的日志信息级别。
日志信息分为以下 8 个级别：

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

【配置举例】 1：下面示例配置允许在 VTY 窗口上打印的日志信息级别为 6：

```
Ruijie(config)# logging monitor informational
```

【检验方法】 -

【提示信息】 -

【常见错误】 -

【平台说明】 -

9.20 logging on

允许日志信息在不同设备上的显示。
logging on

禁止日志信息的显示。
no logging on

【参数说明】

参数	描述
-	-

【缺省配置】 允许日志信息在不同设备上显示。

【命令模式】 全局配置模式

【缺省级别】 14

【使用指导】 日志信息不仅可以显示在 Console 窗口、VTY 窗口上 ,也可以记录在不同的设备上 :内存缓冲区、扩展 FLASH、Syslog Server。该命令为日志总开关，如果关闭日志开关，所有日志信息将不被显示或记录，除了严重性级别为大于 1 的 Log。

【配置举例】 1：下面的示例在设备上关闭日志开关：

```
Ruijie(config)# no logging on
```

【检验方法】 1：使用 **show logging** 命令，可以查看是否允许日志信息在设备上显示。

【提示信息】 -

【常见错误】 -

【平台说明】 -

9.21 logging policy

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

删除一条日志分级上报的分级策略。
no logging policy module *module-name* [**not-lesser-than**] *level* **direction** { **all** | **server** | **file** | **console** | **monitor** | **buffer** }

删除所有日志分级上报的分级策略。
no logging policy

【参数说明】

参数	描述
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

【缺省配置】 缺省情况下，不实行日志分级策略。

【命令模式】 全局配置模式

【缺省级别】 14

【使用指导】 此命令用于配置按模块和严重级别将日志输出到不同目的地。

【配置举例】 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，级别小于等于 3 级的日志只往缓冲区方向输出：

```
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】 -

【提示信息】 -

【常见错误】 -

【平台说明】 -

9.22 logging rate-limit

打开日志速率限制功能，限制每秒内允许输出的日志信息。

logging rate-limit { *number* | **all** *number* | **console** { *number* | **all** *number* } } [**except** [*severity*]]

关闭日志速率限制功能。

no logging rate-limit

【参数说明】

参数	描述
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	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。
severity	日志信息严重性级别，级别越小，严重性越高，范围为 0~7。

【缺省配置】 不进行速率控制。

【命令模式】 全局配置模式

【缺省级别】 14

【使用指导】 此命令控制系统的日志信息输出。使用此命令，可以防止大量的日志信息输出。

【配置举例】 1：设置每秒钟内允许处理的所有日志信息（包括 debug）为 10 条，但是对 warning 及更严重级别不进行控制：

```
Ruijie(config)#logging rate-limit all 10 except warnings
```

【检验方法】 -

【提示信息】 -

【常见错误】 -

【平台说明】 -

9.23 logging server

将日志记录到指定的 Syslog Server。
logging server [**oob**] { *ip-address* | **ipv6** *ipv6-address* } [**udp-port** *port*]

删除 Syslog Server 列表中的指定地址的 Syslog Server。
no logging server [**oob**] { *ip-address* | **ipv6** *ipv6-address* }

恢复日志发送 Syslog Server 的默认端口号（514）。
no logging server { *ip-address* | **ipv6** *ipv6-address* } **udp-port**

【参数说明】

参数	描述
oob	将日志服务器指定为带外通信（一般指通过 MGMT 口发往日志服务器），只有在设备具备 MGMT 管理口的时候才会有该选项
ip-address	接收日志信息的主机 IP 地址
ipv6-address	指定接收日志信息的主机 IPV6 地址
udp-port *port*	指定日志主机的端口号（默认端口号为 514）

【缺省配置】 默认不向任何 Syslog Server 发送日志信息

【命令模式】 全局配置模式

【缺省级别】 14

【使用指导】 该命令指定一个 Syslog server 来接收设备的日志信息。用户可以配置多达 5 个 Syslog Server。日志信息将同时发给配置的所有 Syslog Server。

【配置举例】 1：下面的示例指定一个地址为 202.101.11.1 的 syslog server：

```
Ruijie(config)# logging server 202.101.11.1
```

2：下面的示例指定一个地址为 202.101.11.1，端口号为 8099 的 syslog server：

```
Ruijie(config)# logging server 202.101.11.1 udp-port 8099
```

【检验方法】 1：使用 **show logging** 命令，可以查看设置的日志服务器地址。

【提示信息】 1：如果设备上已经配置的 Syslog Server 超过 5 个，则提示错误。

```
%%Warning: Can not configure more than 5 syslog servers!
```

【常见错误】 -

【平台说明】 NBR6205-E、NBR6135-E、NBR6210-E、NBR6215-E 支持 MGMT 口；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 MGMT 口。

9.24 logging source interface

设置日志报文的源接口。
logging source [**interface**] *interface-type interface-number*

取消指定报文的源接口设置。
no logging source [**interface**]

【参数说明】

参数	描述
interface-type	接口类型
interface-number	接口编号

【缺省配置】 默认没有设置日志源地址

【命令模式】 全局配置模式

【缺省级别】 14

【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。

【配置举例】 1：下面的示例指定 Loopback 0 的地址为 Syslog 报文的源地址：

```
Ruijie(config)# logging source interface loopback 0
```

【检验方法】 -

【提示信息】 -

【常见错误】 -

【平台说明】 -

9.25 logging source ip

设置日志报文的源 IP 地址。
logging source { **ip** *ip-address* }

取消指定报文的源 IP 地址设置。
no logging source { **ip** }

【参数说明】

参数	描述
ip-address	指定向 IPV4 日志主机发送日志报文的源 IPV4 地址

【缺省配置】 默认没有设置日志源地址

【命令模式】 全局配置模式

【缺省级别】 14

【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】 1：下面的示例指定地址 192.168.1.1 为 Syslog 报文的源地址：

```
Ruijie(config)# logging source ip 192.168.1.1
```

【检验方法】 -

【提示信息】 -

【常见错误】 -

【平台说明】 -

9.26 logging statistic enable

打开日志定时上送功能。
logging statistic enable

关闭日志定时上送功能。
no logging statistic enable

【参数说明】

参数	描述
-	-

【缺省配置】 默认是关闭日志定时上送功能。

【命令模式】 全局配置模式

【缺省级别】 14

【使用指导】 可以使用此命令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。

【配置举例】 1：下面的示例打开日志定时上送的功能：

```
Ruijie(config)# logging statistic enable
```

【检验方法】 1：使用 **show logging** 命令，可以查看日志定时上送功能的开关状态。

【提示信息】 -

【常见错误】 -

【平台说明】 -

9.27 logging statistic interval

配置日志定时上送的时间间隔。
logging statistic mnemonic *mnemonic* **interval** *minutes*

恢复默认的日志定时上送时间间隔。
no logging statistic mnemonic *mnemonic*

【参数说明】

参数	描述
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

【缺省配置】 默认的定时上送时间间隔为 15 分钟。

【命令模式】 全局配置模式

【缺省级别】 14

【使用指导】 可以使用此命令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】 -

【检验方法】 -

【提示信息】 -

【常见错误】 -

【平台说明】 -

9.28 logging statistic terminal

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。
logging statistic terminal

关闭定时上送日志输出到控制台和远程终端。
no logging statistic terminal

【参数说明】

参数	描述
-	-

【缺省配置】 缺省情况下关闭定时上送的日志输出到控制台和远程终端。

【命令模式】 全局配置模式

【缺省级别】 14

【使用指导】 可以使用此命令打开定时上送的日志输出到控制台和远程终端。

【配置举例】 1：下面的示例打开定时上送的日志输出到控制台和远程终端：

```
Ruijie(config)# logging statistic terminal
```

【检验方法】 1：使用 **show logging** 命令，可以查看定时上送日志输出到控制台和远程终端的开关状态。

【提示信息】 -

【常见错误】 -

【平台说明】 -

9.29 logging synchronous

打开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。
logging synchronous

关闭用户输入与日志信息输出同步功能。
no logging synchronous

【参数说明】

参数	描述
-	-

【缺省配置】 用户输入与日志信息输出同步功能关闭

【命令模式】 线路配置模式

【缺省级别】 14

【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，如下面的使用情况：

如果正在输入命令时，打印端口 UP-DOWN 日志信息，则输入的命令会重新输出：

```
Ruijie# configure terminal
Oct  9 23:40:55 %LINK-5-CHANGED: Interface GigabitEthernet 0/1, changed state to down
Oct  9 23:40:55 %LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet 0/1, changed state to DOWN
Ruijie# configure terminal          //用户输入的命令重新输出，而不被打断
```

【配置举例】 1：如下命令打开控制台上面的用户输入与日志信息输出同步功能：

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

【检验方法】 -

【提示信息】 -

【常见错误】 -

【平台说明】 -

9.30 logging trap

设置允许发送给 Syslog Server 的日志信息级别。
logging trap [*level*]

禁止将日志报文发送给 Syslog Server。
no logging trap

【参数说明】

参数	描述
level	日志报文的严重性。可以使用级别名称，也可以直接使用数字。关于日志信息严重性的详细说明，请参考【使用指导】。

【缺省配置】 6（Informational，说明性的信息）

【命令模式】 全局配置模式

【缺省级别】 14

【使用指导】 要将日志信息发送给 Syslog Server，首先要使用全局配置命令 **logging** 配置 Syslog Server。然后，使用 **logging trap** 指定发送给日志信息的严重性级别。
通过 **show logging** 命令可以查看日志设置的相关参数和统计。
日志信息分为以下 8 个级别：

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

【配置举例】 1：下面的例子配置将级别为 6 的日志信息发送给地址为 202.101.11.22 的 Syslog Server：

```
Ruijie(config)# logging server 202.101.11.22
Ruijie(config)# logging trap informational
```

【检验方法】 1：使用 **show logging** 命令，可以查看设置的允许发送给 Syslog Server 的日志信息级别。

【提示信息】 -

【常见错误】 -

【平台说明】 -

9.31 logging userinfo

开启记录用户登录/退出的 Log 信息。
logging userinfo

关闭记录用户登录/退出的 Log 信息。
no logging userinfo

【参数说明】

参数	描述
-	-

【缺省配置】 用户登录/退出设备的时候，设备是不会记录相关的 Log 信息。

【命令模式】 全局配置模式

【缺省级别】 14

【使用指导】 开启记录用户登录/退出设备的 Log 信息后，当有用户连接到设备时，就会打出相应的 Log 信息提醒设备管理

员，日志格式如下：

```
Mar 22 14:05:45 %LOGIN-5-LOGIN_SUCCESS: User login from vty0 (192.168.23.68) OK.
```

【配置举例】 1：下面的例子配置打开记录用户登录/退出设备的 Log 信息功能：

```
Ruijie(config)# logging user-info
```

【检验方法】 -

【提示信息】 -

【常见错误】 -

【平台说明】 -

9.32 logging userinfo command-log

开启记录用户操作的 Log 信息。
logging userinfo command-log

关闭记录用户操作的 Log 信息。
no logging userinfo command-log

【参数说明】

参数	描述
-	-

【缺省配置】 设备不会记录相关操作的 Log 信息。

【命令模式】 全局配置模式

【缺省级别】 14

【使用指导】 开启记录用户操作的 Log 信息后，当有用户修改设备配置时，就会打出相应的 Log 信息提醒设备管理员，日志格式如下：

```
Mar 22 14:10:40 %CLI-5-EXEC_CMD: Configured from vty0 (192.168.23.68) command-log: logging server 192.168.23.68.
```

【配置举例】 1：下面的例子配置打开记录用户操作的 Log 信息功能：

```
Ruijie(config)# logging user-info command-log
```

【检验方法】 -

【提示信息】 -

【常见错误】 -

【平台说明】 -

9.33 service log-format rfc5424

切换到 RFC5424 日志格式。
service log-format rfc5424

切换到旧日志格式。
no service log-format rfc5424

【参数说明】

参数	描述
-	-

【缺省配置】 缺省情况下，使用旧的日志格式（即 RFC3164 日志格式）。

【命令模式】 全局配置模式

【缺省级别】 14

【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前后，**show logging** 和 **show logging config** 的命令的显示内容也会有所变化。

【配置举例】 1：下面示例配置日志格式为 RFC5424 日志格式：

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

【检验方法】 -

【提示信息】 -

【常见错误】 -

【平台说明】 -

9.34 service private-syslog

将日志格式调整成私有的日志显示格式。
service private-syslog

取消私有的日志显示格式，并采用默认的日志格式进行显示。
no service private-syslog

【参数说明】

参数	描述
-	-

【缺省配置】 日志信息采用默认日志格式进行显示。

【命令模式】 全局配置模式

【缺省级别】 14

【使用指导】 默认情况下，设备上面的日志信息显示格式如下：
*timestamp: %facility-severity-mnemonic: description
依次是：*时间戳：%模块名-严重性级别-助记符信息：详细日志信息
例子如：

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

若打开私有日志格式显示功能，设备上面的日志信息显示格式如下：
timestamp facility-severity-mnemonic: description
依次是：时间戳 模块名-严重性级别-助记符信息：详细日志信息
例子如：

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

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

【配置举例】 1：下面示例配置将日志格式调整成私有日志格式

```
Ruijie(config)# service private-syslog
```

【检验方法】 1：使用 **show logging** 命令，可以查看日志显示格式是否调整为私有格式。

【提示信息】 -

【常见错误】 -

【平台说明】 -

9.35 service sequence-numbers

在日志信息中加上序号
service sequence-numbers

取消在日志信息中的序号。
no service sequence-numbers

【参数说明】

参数	描述
-	-

【缺省配置】 日志信息中不带序号。

【命令模式】 全局配置模式

【缺省级别】 14

【使用指导】 除了在日志信息中加上时间戳信息以外，还可以在日志信息中加上序号，序号从 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。

【配置举例】 1：下面示例配置在日志信息中加上序号：

```
Ruijie(config)# service sequence-numbers
```

【检验方法】 1：使用 **show logging** 命令，可以查看日志格式是否有添加上序号。

【提示信息】 -

【常见错误】 -

【平台说明】 -

9.36 service standard-syslog

将日志格式调整成标准 RFC3164 中所定义的日志格式。
service standard-syslog

取消标准 RFC3164 中所定义的日志格式，并采用默认的日志格式进行显示。
no service standard-syslog

【参数说明】

参数	描述

-	-

【缺省配置】 日志信息采用默认日志格式进行显示。

【命令模式】 全局配置模式

【缺省级别】 14

【使用指导】 默认情况下，设备上面的日志信息显示格式如下：
*timestamp: %facility-severity-mnemonic: description
依次是：*时间戳：%模块名-严重性级别-助记符信息：详细日志信息
例子如：

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

若打开标准日志格式显示功能，设备上面的日志信息显示格式如下：
timestamp %facility-severity-mnemonic: description
依次是：时间戳 %模块名-严重性级别-助记符信息：详细日志信息
例子如：

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

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

【配置举例】 1：下面示例配置将日志格式调整成标准日志格式

```
Ruijie(config)# service standard-syslog
```

【检验方法】 1：使用 **show logging** 命令，可以查看日志显示格式是否调整为标准格式。

【提示信息】 -

【常见错误】 -

【平台说明】 -

9.37 service sysname

在日志信息中加上系统名。
service sysname

取消在日志信息中的系统名。
no service sysname

【参数说明】

参数	描述
-	-

【缺省配置】 日志信息中不带系统名。

【命令模式】 全局配置模式

【缺省级别】 14

【使用指导】 除了在日志信息中加上时间戳信息以外，还可以在日志信息中系统名。加上系统名以后，日志发送服务器后，在服务器上，可以清楚地知道日志信息来自哪个设备。

【配置举例】 1：下面示例配置在日志信息中加上系统名：

```
Mar 22 15:28:02 %SYS-5-CONFIG: Configured from console by console
Ruijie# config terminal
Enter configuration commands, one per line. End with CNTL/Z.
Ruijie(config)# service sysname
Ruijie(config)# end
Mar 22 15:35:57 Ruijie %SYS-5-CONFIG: Configured from console by console
```

【检验方法】 1：使用 **show logging** 命令，可以查看日志格式是否有添加上系统名。

【提示信息】 -

【常见错误】 -

【平台说明】 -

9.38 service timestamps

在日志信息中加上时间戳信息。
service timestamps [*message-type* [**uptime** | **datetime** [**msec** | **year**]]]

取消在日志信息中打上时间戳信息。
no service timestamps [**message-type**]

恢复日志信息的时间戳为默认值。
default service timestamps [**message-type**]

【参数说明】

参数	描述

message-type	日志类型，有两种 log 和 debug。log 信息是指在严重性级别在 0 - 6 之间的日志信息，debug 信息是严重性级别为 7 的日志信息。
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，格式：月 日期 时:分:秒.毫秒 例：Jul 27 16:53:07.299
year	当前设备日期支持年份显示，格式：年 月 日期 时：分：秒 例：2007 Jul 27 16:53:07

【缺省配置】 日志信息中的时间戳，为当前设备时间。如果设备没有 RTC，则自动调整为设备启动时间。

【命令模式】 全局配置模式

【缺省级别】 14

【使用指导】 使用 Uptime 选项的时间格式是设备自从上次启动到目前的运行时间，单位为秒。使用 Datetime 选项的时间格式为当前设备的日期， 年 - 月 - 日 小时：分钟：秒。

【配置举例】 1：下面示例配置启用 Log 信息和 Debug 信息的时间戳，格式为 Datetime：，并且支持毫秒显示：

```
Ruijie(config)# service timestamps debug datetime msec
Ruijie(config)# service timestamps log datetime msec
Ruijie(config)# end
Oct 8 23:04:58.301 %SYS-5-CONFIG_I: Configured from console by console
```

【检验方法】 1：使用 **show logging** 命令，可以查看日志时间戳格式类型。

【提示信息】 -

【常见错误】 -

【平台说明】 -

9.39 show logging

查看日志配置的参数、统计信息，以及内存缓冲区中的日志报文。日志信息按照时间戳从旧到新的顺序显示。

show logging

【参数说明】

参数	描述
-	-

【命令模式】 特权用户模式

【缺省级别】 1

【使用指导】 -

【配置举例】 1：下面示例是在没有开启 RFC5424 日志格式的情况下，执行 **show logging** 的一个结果：

```
Ruijie# show logging
Syslog logging: enabled
  Console logging: level debugging, 15495 messages logged
  Monitor logging: level debugging, 0 messages logged
  Buffer logging: level debugging, 15496 messages logged
  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, 15242 message lines logged,0 fail
    logging to  202.101.11.22
    logging to  192.168.200.112
Log Buffer (Total 131072 Bytes): have written 1336,
015487: *Sep 19 02:46:13: Ruijie %LINK-3-UPDOWN: Interface FastEthernet 0/24, changed state to up.
015488: *Sep 19 02:46:13: Ruijie %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet 0/24,
changed state to up.
015489: *Sep 19 02:46:26: Ruijie %LINK-3-UPDOWN: Interface FastEthernet 0/24, changed state to down.
015490: *Sep 19 02:46:26: Ruijie %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet 0/24,
changed state to down.
015491: *Sep 19 02:46:28: Ruijie %LINK-3-UPDOWN: Interface FastEthernet 0/24, changed state to up.
015492: *Sep 19 02:46:28: Ruijie %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet 0/24,
changed state to up.
```

字段解释：

字段	说明
Syslog logging	日志开关：打开显示 enabled,关闭显示 disabled
Console logging	打印在控制台上日志信息的级别，以及统计
Monitor logging	打印在 VTY 窗口上日志信息的级别，以及统计
Buffer logging	记录在内存缓冲区中日志信息的级别，以及统计
Standard format	标准日志格式
Timestamp debug messages	Debug 信息时间戳格式
Timestamp log messages	Log 信息时间戳格式
Sequence-number log messages	序号开关

Sysname log messages	日志信息中加上系统名
Count log messages	日志统计功能
Trap logging	发送给 Syslog Server 日志信息的级别，以及统计
Log Buffer	记录在内存缓冲区中的日志报文

2：下面示例是在开启 RFC5424 日志格式的情况下，执行 **show logging** 的一个结果：

```
Ruijie# show logging
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
Log Buffer (Total 4096 Bytes): have written 4096, Overwritten 3292
<135>1 2013-07-24T12:19:33.130290Z ruijie - 7 - - Please config the IP address for capwap.
<132>1 2013-07-24T12:20:02.80313Z ruijie CAPWAP 4 NO_IP_ADDR - No ip address for capwap.
<135>1 2013-07-24T12:20:02.80343Z ruijie - 7 - - Please config the IP address for capwap.
<132>1 2013-07-24T12:20:32.250265Z ruijie CAPWAP 4 NO_IP_ADDR - No ip address for capwap.
<134>1 2013-07-24T12:29:33.410123Z ruijie SYS 6 SHELL_LOGIN [USER@4881 name="" type="" from="console"] user login success.
<134>1 2013-07-24T12:29:34.343763Z ruijie SYS 6 SHELL_CMD [USER@4881 name=""][CMD@4881 task="rl_con" cmd="enable"]
```

字段解释：

字段	说明
Syslog logging	日志开关：打开显示 enabled,关闭显示 disabled
Console logging	打印在控制台上日志信息的级别，以及统计

Monitor logging	打印在 VTY 窗口上日志信息的级别，以及统计
Buffer logging	记录在内存缓冲区中日志信息的级别，以及统计
Count log messages	日志统计功能
Statistic log messages	日志定时上送功能的总开关
Statistic log messages to terminal	日志定时上送输出控制台和远程终端的开关
Delay-send file name	日志延迟上送缓存在设备本地的文件名、当前写入的文件索引以及延迟上送的的时间间隔
Trap logging	发送给 Syslog Server 日志信息的级别，以及统计
Delay-send logging	日志延迟上送给服务器的地址和上送的方式，以及统计
Log Buffer	记录在内存缓冲区中的日志报文

【提示信息】 -

【平台说明】 -

9.40 show logging config

查看日志配置的参数、统计信息。

show logging config

【参数说明】

参数	描述
-	-

【命令模式】 特权用户模式

【缺省级别】 1

【使用指导】 -

【配置举例】 1：下面示例是在没有开启 RFC5424 日志格式的情况下，执行 **show logging config** 的一个结果：

```
Ruijie# show logging config
Syslog logging: enabled
  Console logging: level debugging, 15495 messages logged
  Monitor logging: level debugging, 0 messages logged
  Buffer logging: level debugging, 15496 messages logged
  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, 15242 message lines logged,0 fail
    logging to  202.101.11.22
    logging to  192.168.200.112
```

字段解释：

字段	说明
Syslog logging	日志开关：打开显示 enabled,关闭显示 disabled
Console logging	打印在控制台上日志信息的级别，以及统计
Monitor logging	打印在 VTY 窗口上日志信息的级别，以及统计
Buffer logging	记录在内存缓冲区中日志信息的级别，以及统计
Standard format	标准日志格式
Timestamp debug messages	Debug 信息时间戳格式
Timestamp log messages	Log 信息时间戳格式
Sequence-number log messages	序号开关
Sysname log messages	日志信息中加上系统名
Count log messages	日志统计功能
Trap logging	发送给 Syslog Server 日志信息的级别，以及统计

2：下面示例是在开启 RFC5424 日志格式的情况下，执行 **show logging config** 的一个结果：

```
Ruijie# show logging
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
```

字段解释：

字段	说明

Syslog logging	日志开关：打开显示 enabled,关闭显示 disabled
Console logging	打印在控制台上日志信息的级别，以及统计
Monitor logging	打印在 VTY 窗口上日志信息的级别，以及统计
Buffer logging	记录在内存缓冲区中日志信息的级别，以及统计
Count log messages	日志统计功能
Statistic log messages	日志定时上送功能的总开关
Statistic log messages to terminal	日志定时上送输出控制台和远程终端的开关
Delay-send file name	日志延迟上送缓存在设备本地的文件名、当前写入的文件索引以及延迟上送的时间间隔
Trap logging	发送给 Syslog Server 日志信息的级别，以及统计
Delay-send logging	日志延迟上送给服务器的地址和上送的方式，以及统计

【提示信息】 -

【平台说明】 -

9.41 show logging count

查看系统中各模块日志信息产生的次数，以及最后产生的时间等统计信息。

show logging count

【参数说明】

参数	描述
-	-

【命令模式】 特权用户模式

【缺省级别】 1

【使用指导】 为了使用日志报文统计功能，需要在全局配置模式下，执行 **logging count** 命令。启用了日志报文统计功能后，将对系统中输出的日志报文进行分类统计，统计的结果可以通过命令 **show logging count** 进行查看。

【配置举例】 1：下面示例是执行 **show logging count** 的结果：

```
Ruijie# show logging count
Module Name   Message Name Sev Occur      Last Time
==================================================SYS           CONFIG_I         5   1
Jul 6 10:29:57
------------------------------------------SYS       TOTAL      1
```

字段解释：

字段	说明
Module Name	日志模块名

Message Name	日志助记符名称
Sev	日志级别
Occur	自打开 logging count 以来统计到的该类日志条目
Last Time	最后一次产生此类日志的时间

【提示信息】 -

【平台说明】 -

9.42 show logging reverse

查看日志配置的参数、统计信息，以及内存缓冲区中的日志报文。日志信息按照时间戳从新到旧的顺序显示。

show logging reverse

【参数说明】

参数	描述
-	-

【命令模式】 特权用户模式

【缺省级别】 1

【使用指导】 -

【配置举例】 1：下面示例是在没有开启 RFC5424 日志格式的情况下，执行 **show logging reverse** 的一个结果：

```
Ruijie# show logging reverse
Syslog logging: enabled
  Console logging: level debugging, 15495 messages logged
  Monitor logging: level debugging, 0 messages logged
  Buffer logging: level debugging, 15496 messages logged
  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, 15242 message lines logged,0 fail
    logging to  202.101.11.22
    logging to  192.168.200.112
Log Buffer (Total 131072 Bytes): have written 1336,
015492: *Sep 19 02:46:28: Ruijie %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet 0/24,
```

```
changed state to up.
015491: *Sep 19 02:46:28: Ruijie %LINK-3-UPDOWN: Interface FastEthernet 0/24, changed state to up.
015490: *Sep 19 02:46:26: Ruijie %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet 0/24, changed state to down.
015489: *Sep 19 02:46:26: Ruijie %LINK-3-UPDOWN: Interface FastEthernet 0/24, changed state to down.
015488: *Sep 19 02:46:13: Ruijie %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet 0/24, changed state to up.
015487: *Sep 19 02:46:13: Ruijie %LINK-3-UPDOWN: Interface FastEthernet 0/24, changed state to up.
```

字段解释：

字段	说明
Syslog logging	日志开关：打开显示 enabled,关闭显示 disabled
Console logging	打印在控制台上日志信息的级别，以及统计
Monitor logging	打印在 VTY 窗口上日志信息的级别，以及统计
Buffer logging	记录在内存缓冲区中日志信息的级别，以及统计
Standard format	标准日志格式
Timestamp debug messages	Debug 信息时间戳格式
Timestamp log messages	Log 信息时间戳格式
Sequence-number log messages	序号开关
Sysname log messages	日志信息中加上系统名
Count log messages	日志统计功能
Trap logging	发送给 Syslog Server 日志信息的级别，以及统计
Log Buffer	记录在内存缓冲区中的日志报文

2：下面示例是在开启 RFC5424 日志格式的情况下，执行 **show logging reverse** 的一个结果：

```
Ruijie# show logging reverse
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

Log Buffer (Total 4096 Bytes): have written 4096, Overwritten 3292

<134>1 2013-07-24T12:29:34.343763Z ruijie SYS 6 SHELL_CMD [USER@4881 name=""][CMD@4881
task="rl_con" cmd="enable"]

<134>1 2013-07-24T12:29:33.410123Z ruijie SYS 6 SHELL_LOGIN [USER@4881 name="" type=""
from="console"] user login success.

<132>1 2013-07-24T12:20:32.250265Z ruijie CAPWAP 4 NO_IP_ADDR - No ip address for capwap.

<135>1 2013-07-24T12:20:02.80343Z ruijie - 7 - - Please config the IP address for capwap.

<132>1 2013-07-24T12:20:02.80313Z ruijie CAPWAP 4 NO_IP_ADDR - No ip address for capwap.

<135>1 2013-07-24T12:19:33.130290Z ruijie - 7 - - Please config the IP address for capwap.
```

字段解释：

字段	说明
Syslog logging	日志开关：打开显示 enabled,关闭显示 disabled
Console logging	打印在控制台上日志信息的级别，以及统计
Monitor logging	打印在 VTY 窗口上日志信息的级别，以及统计
Buffer logging	记录在内存缓冲区中日志信息的级别，以及统计
Count log messages	日志统计功能
Statistic log messages	日志定时上送功能的总开关
Statistic log messages to terminal	日志定时上送输出控制台和远程终端的开关
Delay-send file name	日志延迟上送缓存在设备本地的文件名、当前写入的文件索引以及延迟上送的的时间间隔
Trap logging	发送给 Syslog Server 日志信息的级别，以及统计
Delay-send logging	日志延迟上送给服务器的地址和上送的方式，以及统计
Log Buffer	记录在内存缓冲区中的日志报文

【提示信息】 -

【平台说明】 -

9.43 terminal monitor

允许在当前 VTY 窗口上显示日志信息。

terminal monitor

关闭在当前 VTY 窗口上显示日志信息。

terminal no monitor

【参数说明】

参数	描述
-	-

【缺省配置】 在 VTY 窗口上不允许显示日志信息。

【命令模式】 特权用户模式

【缺省级别】 14

【使用指导】 本命令只是设置当前 VTY 的临时属性。作为临时属性设置，它不会被永久保存。在 VTY 终端会话结束后，系统将采用默认设置而该临时属性设置将失效。控制台上也可以执行该命令，但不起作用。

【配置举例】 1：下面示例，设置当前 VTY 窗口允许打印日志信息。

```
Ruijie# terminal monitor
```

【检验方法】 -

【提示信息】 -

【常见错误】 -

【平台说明】 -

9.44 logging language

配置系统日志语言。

logging language { **Chinese** | **English** }

恢复默认日志语言。

no logging language

【参数说明】

参数	描述
Chinese	中文
English	英文

【缺省配置】 缺省配置为中文

【缺省配置】 缺省配置为英文

【命令模式】 全局配置模式

【缺省级别】 NA

【使用指导】 本命令用于设置系统日志语言。

【配置举例】 1：下面示例，设置系统日志语言为英文。

```
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
```

【配置举例】 1：下面示例，设置系统日志语言为中文。

```
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
logging language Chinese
 login local
```

【提示信息】 -

【常见错误】 -

【平台说明】 -

10 LED

10.1 led on

打开 AP 定位灯
led on

关闭 AP 定位灯
no led on

【参数说明】

参数	描述
-	

【缺省配置】 缺省是关闭的

【命令模式】 AP 配置模式

【缺省级别】 14

【使用指导】 此命令用来打开 AP 定位灯，以便于定位 AP 的位置。

【配置举例】 1：打开 AP 定位灯

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

2：关闭 AP 定位灯

```
Ruijie(config)#ap-config 00d0.f822.33bc
Ruijie(config-ap)#no led on
```

【检验方法】 观察 AP 定位 LED 灯是否生效

【提示信息】 -

【常见错误】 -

【平台说明】 -

10.2 quiet-mode session

配置 LED 灯为静默模式

quiet-mode session *session-num*

关闭 LED 的静默模式

no quiet-mode session *session-num*

【参数说明】

参数	描述
session-num	Session id

【缺省配置】 缺省是关闭的

【命令模式】 AP 配置模式

【缺省级别】 14

【使用指导】 配置此命令可以关闭 AP 上所有的 LED 灯

【配置举例】 1：将 LED 配置为 23:00 到第二天 7:00 进入静默状态

```
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
```

2：关闭 LED 的静默模式。

```
Ruijie(config)#ap-config 00d0.f822.33bc
Ruijie(config-ap)#no quiet-mode session 1
```

【检验方法】 系统时间配置的时间段时，所有 LED 灯都熄灭

【提示信息】 -

【常见错误】 当配置的 Session id 不存在的时候，会提示如下错误信息：

```
Ruijie(config-ap)#quiet-mode session 1
invalid session!
```

【平台说明】 -

11 异常告警

11.1 feedback frequency

配置邮件发送频率

feedback frequency *min*

恢复缺省配置

no feedback frequency

【参数说明】

参数	描述
frequency *min*	发送频率。单位为分钟，默认 60。可配置范围：5-10080

【缺省配置】 60

【命令模式】 全局模式

【缺省级别】 15

【使用指导】 如果希望有异常尽快收到邮件，该值应该尽量小；值越小越能及时收到异常告警邮件。但是如果异常信息较多，会频繁收到邮件。

如果不想频繁收到邮件，可以将该值设置大一点，如一天。那么一天内的异常信息，只发送一次邮件，很可能在发生异常后，不能马上收到邮件。

请根据需要设置邮件发送频率。

【配置举例】 1：设置邮件发送频率为 2 小时。

```
Ruijie(config)# feedback frequency 120
```

【检验方法】 1：使用 **show run** 命令，查看配置。

【提示信息】 -

【常见错误】 -

【平台说明】 -

11.2 feedback ignore item

设置忽略的告警选项 id

feedback ignore-item *item-id*

删除配置

no feedback ignore-item *item-id*

【参数说明】

参数	描述
ignore-item *item-id*	设置忽略的选项 id。范围 0-8

【缺省配置】 -

【命令模式】 全局模式

【缺省级别】 15

【使用指导】

⚠ 配置忽略后，该项即使异常也不发送邮件。

【配置举例】 1：设置邮件发送频率为 2 小时。

```
Ruijie(config)# feedback frequency 120
```

【检验方法】 1：使用 **show run** 命令，查看配置。

【提示信息】 配置的 id 超过范围，提示命令输入错误。

【常见错误】 配置的 id 不支持，提示命令输入错误。

【平台说明】 -

11.3 feedback subscriber

设置接收信息的邮件地址

feedback subscriber *mail-addr*

删除配置

no feedback subscriber *mail-addr*

【参数说明】

参数	描述
subscriber *mail-addr*	设置接收信息的邮件地址。可多次配置，最多支持 6 个。

【缺省配置】 -

【命令模式】 全局模式

【缺省级别】 15

【使用指导】 如果需要发送到多个人的邮箱，则重复执行该命令。

【配置举例】 1：设置收件人。

```
Ruijie(config)# feedback subscriber ruijie@sina.com.cn
```

【检验方法】 1：使用 **show run** 命令，查看配置。

【提示信息】 -

【常见错误】 配置的邮箱地址不可达。命令不检查格式和可达性，需要用户自己检查。

【平台说明】 -

11.4 feedback user enable

开启异常告警功能。

feedback user enable

关闭异常告警功能

no feedback user enable

【参数说明】

参数	描述
-	-

【缺省配置】 关闭

【命令模式】 全局模式

【缺省级别】 15

【使用指导】 使用异常告警功能必须开启。

需要同时配置以下功能才能正常使用：

1、 开启邮件服务
2、 配置 smtp 服务器
3、 配置发送的帐号、密码
4、 配置收件人地址

【配置举例】 1：开启异常告警功能。

```
Ruijie(config)# feedback user enable
```

【检验方法】 1：使用 **show run** 命令，查看配置。

【提示信息】 -

【常见错误】 -

【平台说明】 -

11.5 mail-client check

检查邮件相关配置生效
mail-client check

【参数说明】

参数	描述
-	-

【缺省配置】 -

【命令模式】 特权模式

【缺省级别】 15

【使用指导】 配置 smtp 服务器和邮箱的帐号、密码后，使用该命令检查配置是否成功。
如果配置成功，则邮箱会收到一封测试邮件。

【配置举例】 1：检查邮件配置。

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

【检验方法】 使用浏览器登录邮箱，查看是否收到测试邮件。

【提示信息】 1：验证成功。

```
Connect to smtp server. OK！
Login to smtp server. OK!
Send a test mail. OK!
Check OK！
```

2：未配置 SMTP 服务器或帐号。

```
Check failed！
```

3：smtp 服务器配置错误，或未配置 dns。

```
Connect to smtp server. Failed!
```

4：用户名或密码错误。

```
Send a test mail. Failed！
```

【常见错误】 1、 smtp 服务器配置错误
2、 邮箱帐号或密码错误

【平台说明】 -

11.6 mail-client smtp server

检查邮件相关配置生效
mail-client smtp server *addr* [**port** *value*]

删除配置
no mail-client smtp server

【参数说明】

参数	描述
addr	smtp 服务器地址
value	smtp 服务器端口号，取值范围：1-65535

【缺省配置】 -

【命令模式】 全局模式

【缺省级别】 15

【使用指导】 要发送异常告警邮件必须配置。
smtp 服务器地址可以从对应的网站上查找到，如：smtp.qq.com，smtp.126.com

另外，有些邮箱（如 QQ 邮箱）smtp 服务是默认关闭的，使用浏览器登录邮箱后，在设置选项中找到该项并设置为开启。

【配置举例】 1：设置 SMTP 服务器

```
Ruijie(config)# mail-client server smtp.126.com
```

【检验方法】 使用浏览器登录邮箱，查看是否收到测试邮件。

【提示信息】 -

【常见错误】 1、 smtp 服务未开启
2、 smtp 服务器地址错误
3、 设备未配置 dns

【平台说明】 -

11.7 mail-client username

配置邮箱的帐号密码
mail-client username *mail-addr* **password** *pw-string*

删除配置
no mail-client username *mail-addr* **password** *pw-string*

【参数说明】

参数	描述
username *mail-addr*	邮箱帐号，格式一般为 xxx@yyy。该命令没有对格式进行检查。
password *pw-string*	邮箱密码。

【缺省配置】 -

【命令模式】 全局模式

【缺省级别】 15

【使用指导】 请确认一下几个步骤：
1：使用的是常用邮箱网站上申请的邮箱帐号。目前经过验证可以用的有 163、126、139、sina、qq、tom。其它邮箱帐号有可能也能用，但未经过验证。
2：邮箱支持 smtp 服务。上述邮箱都支持。
3：使用浏览器登录邮箱，查看是否开启 smtp 服务
4：登录邮箱网站，查看 smtp 服务器地址。

【配置举例】 1：配置邮箱的帐号和密码

```
Ruijie(config)# mail-client username ruijie@qq.com password ******
```

【检验方法】 1：使用 show run 命令查看是否配置成功。

【提示信息】 1：删除失败。邮箱帐号输入错误或失败。

```
%error: please input right account_name(nabi@126.com) to delete！
```

2：删除邮箱帐号成功。

```
%notice: account_name(nabi@126.com) has been deleted
```

【常见错误】 1：输入的邮箱帐号不支持 smtp
2：邮箱未开启 smtp 服务
3：输入的邮箱帐号，没有通过网站申请

【平台说明】 -

11.8 mail-service enable

开启邮件服务
mail-service enable

关闭邮件服务
no mail-service enable

【参数说明】

参数	描述
-	-

【缺省配置】 开启

【命令模式】 全局模式

【缺省级别】 15

【使用指导】 与发送邮件相关的功能，都需要开启邮件服务。

【配置举例】 1：开启邮件服务。

```
Ruijie(config)# mail-service enable
```

【检验方法】 1：使用 show run 命令查看是否配置成功。

【提示信息】 -

【常见错误】 -

【平台说明】 -

11.9 mail-service source

配置邮件服务源 IP

mail-service source *ip*

删除邮件服务源 IP

no mail-service source

【参数说明】

参数	描述
ip	源 IP 地址

【缺省配置】 无

【命令模式】 全局模式

【缺省级别】 15

【使用指导】 公网模式下需要配置，一般为内网口 IP。

【配置举例】 1：配置邮件服务源 ip 为 1.1.1.1。

```
Ruijie(config)# mail-service source 1.1.1.1
```

【检验方法】 1：使用 show run 命令查看是否配置成功。

【提示信息】 -

【常见错误】 -

【平台说明】 -

11.10 show feedback items

查看异常告警选项。

show feedback items

【参数说明】

参数	描述
-	-

【命令模式】 特权模式、全局模式、接口模式

【缺省级别】 15

【使用指导】 使用该命令可以查看设备支持的各告警选项。

【配置举例】 1：查看当前支持的告警选项。

```
Ruijie#show feedback items
no.  name                          ignore
-------------------------------------------
4,   cpu 温度过高,                  NO
5,   设备受攻击,                   NO
6,   总带宽超过限制,               NO
7,   流控异常,                     NO
8,   主板温度过高,                 NO
```

字段解释：

字段	说明
no.	选项 id
name	选项描述
ignore	是否配置为忽略

【提示信息】 1：如果 feedback 模版载入失败，则无显示。

【平台说明】 -

12 HTTP

12.1 enable service web-server

打开 HTTP 服务功能。
enable service web-server [**http** | **https** | **all**]

关闭 HTTP 服务功能。
{ no | **default } enable service web-server** [**http** | **https** | **all**]

【参数说明】

参数	描述
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。

【缺省配置】 HTTP 服务和 HTTPS 服务功能关闭。

【命令模式】 全局模式

【缺省级别】 14

【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，则表示同时关闭 HTTP 服务和 HTTPS 服务。

【配置举例】 1：同时打开 HTTP 和 HTTPS 服务功能。

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

【检验方法】

【提示信息】

【常见错误】 1、如果端口被其他模块占用了，可能会出现打开 Web 服务失败。

【平台说明】 -

12.2 http check-version

检测 HTTP 服务器中可升级的文件信息。

http check-version

【参数说明】

参数	描述
-	-

【缺省配置】 检测 HTTP 服务器中可升级的文件版本信息。

【命令模式】 特权模式

【缺省级别】 14

【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。

【配置举例】 1：检测 HTTP 升级版本。

```
Ruijie# http check-version
Business modules need to be updated: character-db, route-db
app name:web
    app-name            version           filename
--------------- -------------------- ------------------------
character-db     2014.02.09.14.02.09 app_sub_1.exe
character-db     2014.02.09.14.02.09 app_file_list.txt
character-db     2014.02.09.14.02.09 app_sub_3.exe
character-db     2014.02.09.14.02.09 app_sub_2.exe
route-db         2013.12.01.00       route-choose.db
```

【检验方法】 -

【提示信息】 1：如果当前没有业务模块注册到升级模块中。

```
%notice: No bussiness modules registration.
```

2：如果无法与服务器建立连接或者与服务器通信失败，给出以下提示信息。

```
%notice: Communicate with the server failed.
```

3：如果设备申请内存不足。

```
%warning: Out of memory, application memory failure.
```

4：如果服务器应答报文格式不对。

```
%notice: The server response message format is wrong.
```

5：如果业务模块正在升级或者没有注册版本号。

```
%notice: Suspend, some business modules are upgrading or haven't registered release.
```

6：如果全部业务模块版本已经是最新的。

```
%notice: All bussiness modules are the latest versions.
```

【常见错误】 1、执行该命令提示与服务器通信失败，可能是网络不通或者没有开启 DNS 服务。

【平台说明】 -

12.3 http update

手动升级文件。

http update { **all** | *string* }

【参数说明】

参数	描述
all	升级所有的业务模块
string	需要升级的业务模块名称，可以输入多个，名称之间通过空格分割。

【缺省配置】 -

【命令模式】 特权模式

【缺省级别】 14

【使用指导】 用户通过本命令手动升级指定的业务模块。

【配置举例】 1：手动下载升级远程服务器中最新的 route-db 与 url-db。

```
Ruijie# http update route-db
Downloading updated files, please wait...
Press Ctrl+C to quit
route-db: download and notify successfully.
```

【检验方法】 1：使用 **http check-version** 命令，可以检测 HTTP 服务器中可升级的文件信息。

【提示信息】 1：如果当前没有业务模块注册到升级模块中。

```
%notice: No bussiness modules registration.
```

2：如果指定业务模块没有注册，给出以下提示信息。

```
%notice: The bussiness modules haven't registered.
```

3：如果当前升级模块正在升级中，给出如下提示信息。

```
%notice: There are business modules in the upgrading, please wait for a moment.
```

4：如果无法与服务器建立连接或者与服务器通信失败，给出以下提示信息。

```
%notice: Communicate with the server failed.
```

5：如果设备申请内存不足。

```
%warning: Out of memory, application memory failure.
```

6：如果服务器应答报文格式不对。

```
%notice: The server response message format is wrong.
```

7：如果业务模块正在升级或者没有注册版本号。

```
%notice: Suspend, some business modules are upgrading or haven't registered release.
```

8：如果全部业务模块版本已经是最新的。

```
%notice: All bussiness modules are the latest versions.
```

【常见错误】 1、执行该命令提示与服务器通信失败，可能是网络不通或者没有开启 DNS 服务。

【平台说明】 -

12.4 http update mode

配置 HTTP 升级模式为手动升级模式。

http update mode manual

恢复为自动升级模式。

no http update mode

【参数说明】

参数	描述
manual	手动升级模式。

【缺省配置】 默认是自动升级模式。

【命令模式】 全局模式

【缺省级别】 14

【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。。

【配置举例】 1：将 HTTP 升级模式设置为手动检测模式。

```
Ruijie(config)# http update mode manual
```

【检验方法】 -

【提示信息】 -

【常见错误】 -

【平台说明】 -

12.5 http update server

配置 HTTP 升级的服务器地址和端口号。

http update server { *host-name* | *ip-address* } [**port** *port-number*]

删除配置的 HTTP 升级的服务器，恢复缺省值。

no http update server

【参数说明】

参数	描述
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。

【缺省配置】 默认服务器地址是 0.0.0.0，端口号是 80。

【命令模式】 全局模式

【缺省级别】 14

【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。

【配置举例】 1：配置 HTTP 升级服务器的地址为 10.83.132.1，端口号为 90。

```
Ruijie(config)# http update server 10.83.132.1 port 90
```

【检验方法】 -

【提示信息】

```
-
```

【常见错误】 -

【平台说明】 -

12.6 http update set oob

配置 HTTP 从 MGMT 口升级。
http update set oob

配置 HTTP 从普通口升级，恢复缺省配置。
no http update set oob

【参数说明】

参数	描述
-	-

【缺省配置】 默认从普通口升级。

【命令模式】 全局模式

【缺省级别】 14

【使用指导】 通过本命令配置 HTTP 从 MGMT 口升级。
执行该命令的 **no** 形式，HTTP 从普通口升级。
仅支持 MGMT 口的设备支持该参数。

【配置举例】 1：配置 HTTP 从 MGMT 口升级。

```
Ruijie(config)# http update set oob
```

【检验方法】 -

【提示信息】

```
-
```

【常见错误】 -

【平台说明】 NBR6205-E、NBR6135-E、NBR6210-E、NBR6215-E 支持 MGMT 口；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 MGMT 口。

12.7 http update time

配置 HTTP 自动检测时间。
http update time daily *hh*:*mm*

删除配置的 HTTP 自动检测时间，恢复缺省配置。
no http update time

【参数说明】

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

【缺省配置】 默认自动检测时间是随机的。

【命令模式】 全局模式

【缺省级别】 14

【使用指导】 通过本命令配置 HTTP 自动检测时间，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，设备检测时间是随机。

【配置举例】 1：配置 HTTP 自动检测时间为 23:40。

```
Ruijie(config)# http update time daily 23:40
```

【检验方法】 -

【提示信息】 -

【常见错误】 -

【平台说明】 -

12.8 ip http port

设置 HTTP 服务的端口。
ip http port *port-number*

恢复缺省端口。
no ip http port

【参数说明】

参数	描述
port-number	设置 HTTP 服务端口，取值范围为 80 及 1025-65535。

【缺省配置】 默认端口号为 80。

【命令模式】 全局模式

【缺省级别】 14

【使用指导】 使用该命令设置 HTTP 服务的端口。

【配置举例】 1：设置 HTTP 的服务端口是 8080。

```
Ruijie(config)# ip http port 8080
```

【检验方法】 使用 **show web-service** 命令，查看 Web 服务器状态。

【提示信息】 -

【常见错误】 -

【平台说明】 -

12.9 ip http secure-port

设置 HTTPS 服务的端口。

ip http secure-port *port-number*

恢复缺省端口。

no ip http secure-port

【参数说明】

参数	描述
port-number	设置 HTTPS 服务端口，取值范围为 443 及 1025-65535。

【缺省配置】 默认端口号为 4430。

【命令模式】 全局模式

【缺省级别】 14

【使用指导】 使用该命令设置 HTTPS 服务的端口。

【配置举例】 1：设置 HTTPS 的服务端口是 4443。

```
Ruijie(config)# ip http secure-port 4443
```

【检验方法】 使用 **show web-service** 命令，查看 Web 服务器状态。

【提示信息】 -

【常见错误】 -

【平台说明】 -

12.10 show web-service

查看 Web 服务配置信息和状态。

show web-service

【参数说明】

参数	描述
-	-

【命令模式】 特权模式

【缺省级别】 14

【使用指导】 使用该命令可以查看 Web 服务配置信息和状态。

【配置举例】 1：查看 Web 服务配置信息和状态。

```
Ruijie# show web-service
webservice:
  http      : enable
            : port(80)
  https     : enable
            : port(4430)
```

【提示信息】 -

【平台说明】 -

13 PATCH-UPGRADE

13.1 patch-upgrade

设置补丁升级模块的模式，自动升级模式或手动升级模式。
patch-upgrade set-mode { **auto** | **manual**}

设置补丁升级模块补丁自动加载时间段。
patch-upgrade set-active-time start *hh:mm* **end** *hh:mm*

设置补丁升级模块执行手动升级
patch-upgrade manual-active

设置补丁升级模块执行卸载并删除补丁包。
patch-upgrade delete

【参数说明】

参数	描述
hh:mm	小时分钟

【缺省配置】 缺省为自动升级状态，缺省补丁自动加载时间段为 03:00-04:00

【命令模式】 特权模式

【缺省级别】 14

【使用指导】 1：设置为自动升级模式后，补丁包会自动被安装，加载。
2：当前设备上已下载并安装了补丁包后，才可执行手动升级

【配置举例】 1：配置为自动升级模式。

```
Ruijie# patch-upgrade set-mode auto
```

2：关闭应用控制审计的优化阻断功能。

```
Ruijie# patch-upgrade set-active-time start 12:00 end 13:00
```

【检验方法】 使用 show patch-upgrade state 命令可以查看配置状态。

【提示信息】 -

【常见错误】 -

【平台说明】 MSC 产品不支持，其他网关系列产品均支持

13.2 show patch-upgrade state

查询补丁升级模块配置和状态。

show patch-upgrade state

【参数说明】

参数	描述

【命令模式】 特权模式

【缺省级别】 14

【使用指导】 使用该命令可以查询补丁升级模块状态和配置信息。

【配置举例】 1：查询补丁升级模块状态和配置信息。

```
Ruijie# showpatch-upgrade state
 show patch update info:
----------------------------
mode            :auto
patch state     :uninstall
next state      :
outer state     :
active time     :NULL
check start     :03:00
check end       :04:00
check quiet     :5
need reboot     :0
version         :notpatch
per version     :notpatch
----------------------------
```

【提示信息】

【平台说明】

13.3 show patch-upgrade log

查询补丁升级模块的日志信息。

show patch-upgrade log

【参数说明】

参数	描述

【命令模式】 特权模式

【缺省级别】 14

【使用指导】 使用该命令可以查询补丁升级模块日志信息。

【配置举例】 1：查询补丁升级模块日志信息。

```
Ruijie# show patch-upgrade log
show patch log info
2017-08-16 11:49:32, [auto] patch install success
2017-08-16 12:00:03, [auto] patch active success
2017-08-16 14:04:43, [manual] patch running success
2017-08-16 17:12:33, [manual] patch install fail
2017-08-16 17:16:53, [manual] patch install success
2017-08-16 17:16:53, [manual] patch active success
2017-08-16 17:16:54, [manual] patch running success
2017-08-16 17:21:43, [manual] patch install fail
2017-08-16 17:31:37, [manual] patch install fail
2017-08-16 17:35:56, [manual] patch install fail
...
```

【提示信息】

【平台说明】

14 WEB-UPGRADE

命令	作用
web-upgrade	WEB 包升级。
show web-upgrade	显示当前 WEB 包信息。

14.1 web-upgrade

安装，升级本地文件系统内 WEB 包。

web-upgrade *url* [force]

【参数说明】

参数	描述
url	url 为 WEB 包存放的本地路径。
force	忽略版本比较，强制升级

【缺省配置】 -

【命令模式】 特权模式

【缺省级别】 14

【使用指导】 该命令支持 WEB 包本地升级。

使用该命令前，需先将 WEB 包拷入设备文件系统指定目录中。

当使用该命令时，将在根据输入的路径查找 WEB 包，并进行升级。

url 可以用如下格式：

参数	描述
tmp:*url*	路径/tmp/vsd/0/
path *url*	自定义本地文件路径

默认相同版本不进行升级，如果需要忽略版本比较，可以带上参数 force

无

【配置举例】 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.
```

【验证方法】 通过 show web-upgrade 查看当前 web 包信息，确认升级成功

【提示信息】

【常见错误】 WEB 包文件路径或文件名不正确

【平台说明】 -

14.2 show web-upgrade

显示当前 WEB 包的版本信息。

show web-upgrade

【参数说明】

参数	描述
-	-

【命令模式】 特权模式，配置模式，接口模式

【缺省级别】 -

【使用指导】 -

【配置举例】 1：显示当前 WEB 包的版本信息

```
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
```

使用该命令可以获取包内信息。

字段	说明
Version	包的版本信息
Md5	包 MD5
Size	包大小
Build	包编译生成时间
Compatible	包支持的产品型号
Incompatible	包不支持的产品型号

【提示信息】 -

【平台说明】 -

命令参考-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. PPP
8. Aggregate Port
9. VLAN-TERMINAL

1 接口

1.1 bandwidth

在接口配置模式下设置接口的带宽参数。
bandwidth *kilobits*

恢复带宽参数的缺省值。
no bandwidth

【参数说明】

参数	描述
kilobits	每秒钟带宽，以每秒 K 比特为单位

【缺省配置】 当该接口中没有设置 **bandwidth** 命令参数时，在特权用户模式下用 **show interface** 命令来显示其缺省值。

【命令模式】 接口配置模式

【缺省级别】 14

【使用指导】 **bandwidth** 命令不能实际影响某个接口的带宽，只是让用户告诉系统该接口的带宽指标，默认情况下，以太网接口的带宽是根据实际端口 Link 的速率决定的，如果有需要可以自己指定，Bandwidth 只是个路由参数，不会影响物理链路的接口的真正带宽。

【配置举例】 1：以下的例子示范配置接口带宽参数为 64Kbps：

```
Ruijie(config)#interface gigabitEthernet 0/1
Ruijie(config-if-GigabitEthernet 0/1)# bandwidth 64
```

【检验方法】 -

【提示信息】 -

【常见错误】 -

【平台说明】 -

1.2 carrier-delay

在接口配置模式下使用命令 **carrier-delay** 在接口设置载波时延。

carrier-delay {[**milliseconds**] *num* | **up** [**milliseconds**] *num* **down** [**milliseconds**] *num*}

恢复缺省值。

no carrier-delay

【参数说明】

参数	描述
num	可选参数，默认以秒为单位，范围 0～60 秒。
milliseconds	可选参数，加上此关键字，num 数值以毫秒为单位，范围 0~60000 毫秒
up	可选参数，设置载波检测信号 DCD 从 Down 状态到 Up 状态的时间延时
down	可选参数，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】 载波时延缺省值是 2 秒。

【命令模式】 接口模式。

【缺省级别】 14

【使用指导】 载波延迟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 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的状态的变化而不至于上层的数据链路层重新协商。

如果 DCD 载波中断时间比较长，那么将该参数设长些，可以尽快加速路由汇聚，以便路由表可以较快地收敛。

如果相反，DCD 载波中断时间小于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路由震荡。

【配置举例】 1：配置接口的载波时延为 5 秒。

```
Ruijie(config)# interface GigabitEthernet 1/1
Ruijie(config-if-GigabitEthernet 1/1)# carrier-delay 5
```

2：配置接口的载波时延为 100 毫秒。

```
Ruijie(config)# interface GigabitEthernet 1/1
Ruijie(config-if-GigabitEthernet 1/1)#carrier-delay milliseconds 100
```

3：配置接口链路的载波检测信号 DCD 从 Down 状态到 Up 状态的时间延迟为 100 毫秒，从 Up 状态到 Down 的时间延迟为 200 毫秒

```
Ruijie(config)# interface GigabitEthernet 1/1
Ruijie(config-if-GigabitEthernet 1/1)# carrier-delay up milliseconds 100 down milliseconds 200
```

【检验方法】 1：使用 **show interfaces** 命令，可以查看接口的载波时延。

【提示信息】 -

【常见错误】 -

【平台说明】 -

1.3 clear counters

清除接口计数器。

clear counters [*interface-type interface-number*]

【参数说明】

参数	描述
interface-type interface-number	接口类型和接口号。

【命令模式】 特权模式。

【缺省级别】 14

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

【配置举例】 1：清除接口 GigabitEthernet 1/1 的计数器。

```
Ruijie# clear counters GigabitEthernet 1/1
```

【提示信息】 -

【平台说明】 -

1.4 clear interface

接口硬件复位。

clear interface *interface-type interface-number*

【参数说明】

参数	描述
interface-type interface-number	接口类型和接口号。

【命令模式】 特权模式。

【缺省级别】 14

【使用指导】 该命令只对交换端口，二层聚合端口的成员端口，路由端口和三层聚合端口的成员端口有效。执行该命令相当于对接口绑定执行 **shutdown** 和 **no shutdown** 命令。

【配置举例】 1：对接口 GigabitEthernet 1/1 进行硬件复位。

```
Ruijie# clear interface GigabitEthernet 1/1
```

【提示信息】 -

【平台说明】 -

1.5 description

设置接口的别名。
description *string*

恢复成缺省值。
no description

【参数说明】

参数	描述
string	接口的别名。

【缺省配置】 缺省没有别名。

【命令模式】 接口配置模式

【缺省级别】 14

【使用指导】 使用 **show interfaces** 命令查看接口信息，包括别名。

【配置举例】 1：给接口 GigabitEthernet 1/1 配置别名 GBIC-1。

```
Ruijie(config)# interface GigabitEthernet 1/1
Ruijie(config-if-GigabitEthernet 1/1)# description GBIC-1
```

【检验方法】 1：使用 **show interfaces** 命令，可以查看接口的别名。
2：使用 **show interfaces description** 命令，可以查看接口的别名。

【提示信息】 1：如果别名长度超过 80，则提示错误。

```
% The length of description is up to 80!
```

【常见错误】 -

【平台说明】 -

1.6 duplex

设置接口的双工模式。

duplex { **auto** | **full** | **half** }

恢复成缺省值。

no duplex

【参数说明】

参数	描述
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】 全双工和半双工自适应。

【命令模式】 接口模式

【缺省级别】 14

【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。

【配置举例】 1：把接口 GigabitEthernet 1/1 的双工模式配置成全双工。

```
Ruijie(config)# interface GigabitEthernet 1/1
Ruijie(config-if-GigabitEthernet 1/1)# duplex full
```

【检验方法】 1：使用 **show interfaces** 命令，可以查看接口的双工模式。

【提示信息】 -

【常见错误】 -

【平台说明】 -

1.7 interface

该命令是模式导航命令，进入接口配置模式。

interface *interface-type interface-number*

【参数说明】

参数	描述
interface-type	接口类型
interface-number	接口编号

【缺省配置】 -

【命令模式】 接口模式

【缺省级别】 14

【使用指导】 该命令进入接口配置模式，下一步就可以修改接口的配置。

【配置举例】 1：进入 Aggregateport 1 的配置模式。

```
Ruijie(config)# interface Aggregateport 1
Ruijie(config-if-Aggregateport 1)#
```

2：进入 GigabitEthernet 1/2 的配置模式。

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

3：进入 VLAN 1 的配置模式。

```
Ruijie(config)# interface vlan 1
Ruijie(config-if-VLAN 1)#
```

【检验方法】 -

【提示信息】 -

【常见错误】 -

【平台说明】 -

1.8 interface range

在全局配置模式下使用 **interface** 命令进入接口配置模式。

Interface range { *port-range* | **macro** *macro_name* }

以上命令中的宏名使用 **define interface-range** 来定义。

define interface-range *macro_name*

【参数说明】

参数	描述
port-range	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、Loopback 口等，输入形式为 *interface-type slot-number/interface-number*。
macro *macro_name*	选择输入定义宏来表示接口范围，macro_name 为宏名字。

【缺省配置】 缺省情况下，不使用该功能

【命令模式】 全局配置模式。

【缺省级别】 14

【使用指导】 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。

【配置举例】 1：直接输入端口范围批量配置接口配置。

```
Ruijie(config)# interface range gigabitEthernet 0/0, 0/2
Ruijie(config-if-range)# bandwidth 100
```

2：输入宏名批量配置接口配置。

```
Ruijie(config)# define interface-range route1 gigabitEthernet 0/0-2
Ruijie(config)# interface range macro route1
Ruijie(config-if-range)# bandwidth 100
```

【检验方法】 -

【提示信息】 -

【常见错误】 -

【平台说明】 -

1.9 load-interval

在接口配置模式下指定一个接口的负载计算的间隔时间。
load-interval *seconds*

恢复缺省配置。
no load-interval

【参数说明】

参数	描述
seconds	单位秒，取值范围 5 到 600

【缺省配置】 10 秒。

【命令模式】 接口配置模式

【缺省级别】 14

【使用指导】 1：在接口中用此命令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 秒计算一次每秒中输入输出的报文数和比特数。举个例子，如果在接口 GigabitEthernet 0/1 中将此参数更改成 180 秒，用 show interface gigabitEthernet 0/1 可以看到：

```
3 minutes input rate 15 bits/sec, 0 packets/sec
3 minutes output rate 14 bits/sec, 0 packets/sec
```

【配置举例】 1：以下的例子示范在以太网口 GigabitEthernet 0/1 中设置负载计算的间隔时间成 180 秒

```
Ruijie(config)# interface gigabitEthernet 0/1
Ruijie(config-if-GigabitEthernet 0/1)# load-interval 180
```

【检验方法】 -

【提示信息】 -

【常见错误】 -

【平台说明】 -

1.10 logging

配置打印接口相关信息。

logging [link-updown | error-frame | link-dither]

【参数说明】

参数	描述
link-updown	打印接口状态发生改变时的信息
error-frame	打印接口收到错误帧时的信息
link-dither	打印接口发生震荡时的信息

【缺省配置】 该功能开启。

【命令模式】 全局模式

【缺省级别】 14

【使用指导】 由用户自行决定是否开启打印接口相关信息。默认情况下为开启，当接口状态发生改变、接口收到错误帧或接口发生震荡时，打印提示信息。配置 no logging [link-updown | error-frame | link-dither]后，则不会打印提示信息。

【配置举例】 1：配置打印接口状态改变信息。

```
Ruijie(config)# logging link-updown
Ruijie(config)# logging error-frame
```

```
Ruijie(config)# logging link-dither
```

【检验方法】 -

【提示信息】 -接口状态发生改变时提示信息：
%LINK-3-UPDOWN: Interface GigabitEthernet 0/0, changed state to up.
%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet 0/0, changed state to up.
接口收到错误帧时提示信息：
%PORT-3-ERR_FRAME: Received error frames on interface GigabitEthernet 0/0. Please check the physical link.
接口发生震荡时提示信息：
%LINK-4-DITHER: The state of Interface GigabitEthernet 0/1 is astable. Please check the physical link.
%LINK-4-DITHER: The state of interface GigabitEthernet 0/1 is astable and the interface will be shutdown.Please check the physical link

【常见错误】 -

【平台说明】 -

1.11 medium-type

选择接口的介质类型。
medium-type { **auto-select** [**prefer** [**fiber | copper**]] **| fiber | copper** }

恢复成缺省值。
no medium-type

【参数说明】

参数	描述
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】 缺省是电口。

【命令模式】 接口配置模式（物理端口）

【缺省级别】 14

【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。

【配置举例】 1：端口 GigabitEthernet 1/1 是光电口，把介质类型设置成电口。

```
Ruijie(config)# interface GigabitEthernet 1/1
Ruijie(config-if-GigabitEthernet 1/1)# medium-type copper
```

【检验方法】 1：使用 **show interfaces** 命令，可以查看接口的介质类型。

【提示信息】 -

【常见错误】 -

【平台说明】 -

1.12 mtu

设置接口的 MTU

mtu *num*

【参数说明】

参数	描述
num	64 - ?(不同产品的最大值不同，由芯片决定)

【缺省配置】 缺省为 1500。

【命令模式】 接口模式

【缺省级别】 14

【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的 MTU。

【配置举例】 1：把端口 GigabitEthernet 1/1 的 MTU 设置为 9000。

```
Ruijie(config)# interface GigabitEthernet 1/1
Ruijie(config-if-GigabitEthernet)# mtu 9000
```

【检验方法】 1：使用 **show interfaces** 命令，可以查看接口的 MTU。

【提示信息】 -

【常见错误】 -

【平台说明】 -

1.13 physical-port dither protect

配置接口震荡保护。
physical-port dither protect

【参数说明】

参数	描述
-	-

【缺省配置】 该功能开启。

【命令模式】 全局模式

【缺省级别】 14

【使用指导】 端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，即 **physical-port dither protect，**当接口发生震荡时并超过一定规定次数时，将 shutdown 端口，起到保护端口的作用；配置 **no physical-port dither protect** 命令后，只打印提示信息，不关闭接口。
说明：
接口每 2s 或 10s 检测一次震荡，如果检测到接口 2s 震荡 6 次，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 shutdown 接口。 对于 10s 检测一次震荡，震荡次数超过 10 次，则打印提示信息，不关闭接口.。

【配置举例】 1：开启保护接口震荡功能。

```
Ruijie(config)# physical-port dither protect
```

【检验方法】 -

【提示信息】 -接口发送震荡时提示信息：
接口每 2s 内检测到 6 次震荡或者 10s 内检测 10 次震荡提示如下信息：
%LINK-4-DITHER: The state of Interface GigabitEthernet 0/1 is astable. Please check the physical link.
接口在 20s 内发送 10 次震荡，最后一次震荡提示信息为：
%LINK-4-DITHER: The state of interface GigabitEthernet 0/1 is astable and the interface will be shutdown.Please check the physical link.

【常见错误】 -

【平台说明】 -

1.14 show interfaces

查看接口设置信息。

show interfaces [*interface-type interface-number*] [**description**]

【参数说明】

参数	描述
interface-type *interface-number*	接口类型和接口编号。
description	接口的描述符信息，包括 link 状态。

【命令模式】 特权模式

【缺省级别】 14

【使用指导】 如果不加参数，则显示接口的基本信息。

【配置举例】 1：当 GigabitEthernet 0/1 为 Trunk 端口时，查看接口信息。

```
SwitchA#show interfaces GigabitEthernet 0/1
Index(dec):1 (hex):1
GigabitEthernet 0/1 is DOWN  , line protocol is DOWN
  Hardware is Broadcom 5464 GigabitEthernet, address is 00d0.f865.de9b (bia 00d0.f865.de9b)
  Interface address is: no ip address
  MTU 1500 bytes, BW 1000000 Kbit
  Encapsulation protocol is Ethernet-II, loopback not set
  Keepalive interval is 10 sec , set
  Carrier delay is 2 sec
  Ethernet attributes:
    Last link state change time: 2012-12-22 14:00:48
    Time duration since last link state change: 3 days, 2 hours, 50 minutes, 50 seconds
    Priority is 0
    Medium-type is Copper
    Admin duplex mode is AUTO, oper duplex is Unknown
    Admin speed is AUTO, oper speed is Unknown
    Flow receive control admin status is OFF,flow send control admin status is OFF
    Flow receive control oper status is Unknown,flow send control oper status is Unknown
    Storm Control: Broadcast is OFF, Multicast is OFF, Unicast is OFF
  Bridge attributes:
    Port-type: trunk
    Native vlan:1
    Allowed vlan lists:1-4094                    //Trunk 口的许可 VLAN 列表
    Active vlan lists:1, 3-4  //实际生效的 vlan（即该设备上仅创建了 VLAN1、3 和 4）
```

```
  Queueing strategy: FIFO
    Output queue 0/0, 0 drops;
    Input queue 0/75, 0 drops
  Rxload is 1/255,Txload is 1/255
  5 minutes input rate 0 bits/sec, 0 packets/sec
  5 minutes output rate 0 bits/sec, 0 packets/sec
    0 packets input, 0 bytes, 0 no buffer, 0 dropped
    Received 0 broadcasts, 0 runts, 0 giants
    0 input errors, 0 CRC, 0 frame, 0 overrun, 0 abort
    0 packets output, 0 bytes, 0 underruns , 0 dropped
    0 output errors, 0 collisions, 0 interface resets
```

2：当 GigabitEthernet 0/1 为 Access 端口时，查看接口信息。

```
SwitchA#show interfaces GigabitEthernet 0/1
Index(dec):1 (hex):1
GigabitEthernet 0/1 is DOWN  , line protocol is DOWN
  Hardware is Broadcom 5464 GigabitEthernet, address is 00d0.f865.de9b (bia 00d0.f865.de9b)
  Interface address is: no ip address
  MTU 1500 bytes, BW 1000000 Kbit
  Encapsulation protocol is Ethernet-II, loopback not set
  Keepalive interval is 10 sec , set
  Carrier delay is 2 sec
  Ethernet attributes:
    Last link state change time: 2012-12-22 14:00:48
    Time duration since last link state change: 3 days, 2 hours, 50 minutes, 50 seconds
    Lastchange time:0 Day: 0 Hour: 0 Minute:13 Second
    Priority is 0
    Medium-type is Copper
    Admin duplex mode is AUTO, oper duplex is Unknown
    Admin speed is AUTO, oper speed is Unknown
    Flow receive control admin status is OFF,flow send control admin status is OFF
    Flow receive control oper status is Unknown,flow send control oper status is Unknown
    Storm Control: Broadcast is OFF, Multicast is OFF, Unicast is OFF
  Bridge attributes:
    Port-type: access
    Vlan id : 2                          //Access 口的所属 VLAN ID
  Queueing strategy: FIFO
    Output queue 0/0, 0 drops;
    Input queue 0/75, 0 drops
  Rxload is 1/255, Txload is 1/255
  5 minutes input rate 0 bits/sec, 0 packets/sec
```

```
  5 minutes output rate 0 bits/sec, 0 packets/sec
    0 packets input, 0 bytes, 0 no buffer, 0 dropped
    Received 0 broadcasts, 0 runts, 0 giants
    0 input errors, 0 CRC, 0 frame, 0 overrun, 0 abort
    0 packets output, 0 bytes, 0 underruns , 0 dropped
    0 output errors, 0 collisions, 0 interface resets
```

3：当 GigabitEthernet 0/1 为 Hybrid 端口时，查看接口二层信息。

```
SwitchA#show interfaces GigabitEthernet 0/1
Index(dec):1 (hex):1
GigabitEthernet 0/1 is DOWN  , line protocol is DOWN
  Hardware is Broadcom 5464 GigabitEthernet
  Interface address is: no ip address
  MTU 1500 bytes, BW 1000000 Kbit
  Encapsulation protocol is 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
    Lastchange time:0 Day: 0 Hour: 0 Minute:13 Second
    Priority is 0
    Medium-type is Copper
    Admin duplex mode is AUTO, oper duplex is Unknown
    Admin speed is AUTO, oper speed is Unknown
    Flow receive control admin status is OFF,flow send control admin status is OFF
    Flow receive control oper status is Unknown,flow send control oper status is Unknown
    Storm Control: Broadcast is OFF, Multicast is OFF, Unicast is OFF
  Bridge attributes:
    Port-type: hybrid
    Tagged vlan id:2                          //打标记的 VLAN ID
    Untagged vlan id:none                     //不打标记的 VLAN ID
  Queueing strategy: FIFO
    Output queue 0/0, 0 drops;
    Input queue 0/75, 0 drops
  Rxload is 1/255 ,Txload is 1/255
  5 minutes input rate 0 bits/sec, 0 packets/sec
  5 minutes output rate 0 bits/sec, 0 packets/sec
    0 packets input, 0 bytes, 0 no buffer, 0 dropped
    Received 0 broadcasts, 0 runts, 0 giants
    0 input errors, 0 CRC, 0 frame, 0 overrun, 0 abort
```

```
    0 packets output, 0 bytes, 0 underruns , 0 dropped
    0 output errors, 0 collisions, 0 interface resets
```

4：查看 GigabitEthernet 0/1 的二层信息。

```
Ruijie# show interfaces GigabitEthernet 0/1 switchport
Interface                Switchport Mode      Access Native Protected VLAN lists
------------------------ ---------- --------- ------ ------ --------- ----------
GigabitEthernet 0/1      enabled    ACCESS    2      1      Disabled  ALL
```

【提示信息】 -

【平台说明】 -

1.15 show interfaces link-state-change statistics

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**

【参数说明】

参数	描述
interface-type interface-number	接口类型和接口编号。

【命令模式】 特权模式

【缺省级别】 14

【使用指导】 如果不指定接口名称，则显示所有接口的链路状态变化信息。

【配置举例】 1：显示接口 GigabitEthernet 0/1 的链路状态变化信息。

```
Ruijie# show interfaces GigabitEthernet 0/1 link-state-change statistics
Interface     Link state     Link state change times      Last change time
------------  ---------      -----------------------      -------------------
Gi 0/1        down           100                          2012-12-24 15:00:00
```

Interface	接口信息
Link state	当前链路状态
Link state change times	链路状态变化次数
Last change time	上一次链路状态变化的时间

【提示信息】 -

【平台说明】 -

1.16 show interfaces status

查看接口的状态信息。

show interfaces [*interface-type interface-number*] **status**

【参数说明】

参数	描述
interface-type interface-number	接口类型和接口编号。
status	查看接口的各种状态信息，包括速率和双工等。

【命令模式】 特权模式

【缺省级别】 14

【使用指导】 如果不指定接口名称，则显示所有接口的状态信息。

【配置举例】 1：显示接口 GigabitEthernet 0/1 的状态信息。

```
Ruijie#show interfaces GigabitEthernet 0/1 status
Interface              Status       Vlan     Duplex  Speed   Type
---------------------  ----------   ------   ------  ------  ------
GigabitEthernet 0/1    up           1        Full    1000M   copper
```

【提示信息】 -

【平台说明】 -

1.17 show interfaces usage

查看接口带宽利用率。

show interfaces [*interface-type interface-number*] **usage** [*up* | *down*]

【参数说明】

参数	描述
interface-type interface-number	可选参数，接口类型和接口编号，不选则显示所有接口。
up	可选参数，显示接口状态为 up 的带宽利用率
down	可选参数，显示接口状态为 down 的带宽利用率

【命令模式】 所有 CLI 用户模式

【缺省级别】 14

【使用指导】 如果不指定接口名称，则显示所有接口的带宽利用率信息。这里的带宽指的是实际链路带宽，而不是接口下的

bandwidth 配置值。

【配置举例】 1：显示接口 GigabitEthernet 0/1 的端口带宽利用率信息。

```
Interface                 Bandwidth     Average Usage      Output Usage      Input Usage
------------------------- ------------ ------------------ ------------------ ------------------
GigabitEthernet 0/0       1000 Mbit     0.002822759%       0.001183280%       0.004462237%
```

说明：Bandwidth 是接口链路带宽，也就是 Link 的最大速率，Average UsageBandwidth Usage 是当前带宽利用率。，Output Usage 是发送带宽利用率，Input Usage 是接收带宽利用率。

【提示信息】 -

【平台说明】 -

1.18 shutdown

在接口配置模式中，使用该命令关闭接口。

shutdown

打开接口。

no shutdown

【参数说明】

参数	描述
-	-

【缺省配置】 接口的管理状态是 UP。

【命令模式】 接口模式

【缺省级别】 14

【使用指导】 对于接口（以太网端口、聚合端口和交换虚拟接口），该命令关闭接口，接口的其它配置仍然存在，但是不起作用。使用 **show interfaces** 命令查看接口状态。

若使用脚本频繁快速做 **no shutdown** 接口操作，可能会发生接口状态翻转提示信息。

【配置举例】 1：关闭聚合端口 1。

```
Ruijie(config)# interface Aggregateport 1
Ruijie(config-if-Aggregateport 1)# shutdown
```

2：打开聚合端口 1。

```
Ruijie(config)# interface Aggregateport 1
```

```
Ruijie(config-if-Aggregateport 1)# no shutdown
```

【检验方法】 1：使用 **show interfaces** 命令，可以查看接口的状态。

【提示信息】 -

【常见错误】 -

【平台说明】 -

1.19 snmp trap link-status

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

snmp trap link-status

关闭该功能，SNMP 将不发出 LinkTrap。

no snmp trap link-status

【参数说明】

参数	描述
-	-

【缺省配置】 缺省情况下，该功能打开。

【命令模式】 接口模式。

【缺省级别】 14

【使用指导】 对于接口（以太网端口、聚合端口和交换虚拟接口），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。

【配置举例】 1：下面的例子配置接口不发送 LinkTrap。

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

2：下面的例子配置接口发送 LinkTrap。

```
Ruijie(config)# interface GigabitEthernet 1/1
Ruijie(config-if-GigabitEthernet 1/1)# snmp trap link-status
```

【检验方法】 -

【提示信息】 -

【常见错误】 -

【平台说明】 -

1.20 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。

snmp-server if-index persist

【参数说明】

参数	描述
-	-

【缺省配置】 该功能关闭。

【命令模式】 全局模式

【缺省级别】 14

【使用指导】 执行命令“**snmp-server if-index persist**”以后，保存配置时将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。注意重启前必须保证配置。

【配置举例】 1：开启接口索引永久化功能。

```
Ruijie(config)# snmp-server if-index persist
```

【检验方法】 -

【提示信息】 -

【常见错误】 -

【平台说明】 -

1.21 speed

设置接口的速率。

speed [**10 | 100 | 1000 | auto**]

恢复成缺省值。

no speed

【参数说明】

参数	描述
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】 速率缺省是自适应的。

【命令模式】 接口模式

【缺省级别】 14

【使用指导】 如果接口是聚合端口的成员，则该接口的速率由聚合端口的速率决定。接口退出聚合端口时使用自己的速率设置。使用 **show interfaces** 命令查看设置。接口类型不同，允许设置的速率类型也会有所不同，如 SFP 类型的接口就不允许把速率设为 10M。

【配置举例】 1：把端口 GigabitEthernet 1/1 的速率设置成 100Mbps。

```
Ruijie(config)# interface GigabitEthernet 1/1
Ruijie(config-if-GigabitEthernet 1/1)# speed 100
```

【检验方法】 1：使用 **show interfaces** 命令，可以查看接口的速率。

【提示信息】 -

【常见错误】 -

【平台说明】 -

2 模式管理

2.1 bridge-map

进入桥接映射表命令模式层。

bridge-map *bridge-num*

【参数说明】

参数	描述
bridge-map *bridge-num*	桥接映射表索引号。该索引号的取值取决于设备上网络接口的数量，桥的配置需要一个内网接口和一个外网接口组成一对桥，因此设备有几对内外网接口，就有几个桥接映射表。不支持子接口配置桥，因此子接口的内外网对数不计算在内。 例如：设备最多有三对内外网接口，则桥接映射表索引参数范围为 0~2 。

【缺省配置】 无。

【命令模式】 全局模式

【缺省级别】 14

【使用指导】 通过配置本命令，进入桥接映射表命令模式层。在桥接映射表命令模式层中，可以指定内外网接口的桥接映射关系和工作模式。

⚠ 必须切换到非网关模式才能配置，非网关模式的切换命令详见 sys-mode 命令。

⚠ 桥接映射表命令模式层不允许被 no 掉。

【配置举例】 1：进入桥接映射表命令模式层。

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

【检验方法】 1：使用 **show bridge-map** 命令，可以查看当前桥设备支持的桥映射表信息。

【提示信息】 1：输入的参数合法，则进入桥映射命令模式层。

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

```
Ruijie(config-bridge-map)#
```

2：输入的参数不合法，则提示当前桥映射不存在。

```
Ruijie#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Ruijie(config)#bridge-map 5
%% Bridge 5 not exist!
```

3：no 掉一个已存在的桥映射，则提示不允许。

```
Ruijie#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Ruijie(config)#no bridge-map 5
%% Removal of bridge-map is not permitted
```

【常见错误】 -

【平台说明】 所有网关系列产品均支持，必须工作在网桥模式下。

2.2 lan-ip

配置 receive-only 模式下的内网网段 IP 与掩码。
lan-ip *ip_address subnet_mask*

取消配置 receive-only 模式下的内网网段 IP 与掩码。
no lan-ip *ip_address subnet_mask*

【参数说明】

参数	描述
ip_address	内网网段 IP
subnet_mask	子网掩码

【缺省配置】 无。

【命令模式】 桥接映射表命令层配置模式

【缺省级别】 14

【使用指导】 用户在设置桥工作在单臂模式时，可根据实际内网网段情况配置。

必须切换到非网关模式才能配置，非网关模式的切换命令详见 sys-mode 命令。

单臂模式下需要用户正确配置内网 IP 段，该工作模式下的业务才可以正确运行。

最多可以配置 100 个网段。两个单臂模式下可配置相同的内网网段。

【配置举例】 1：配置桥接映射表 0 工作在 receive-only 模式；当前网络内网网段为：192.168.1.0/24 和 10.10.10.0/24。

```
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 0/0 GigabitEthernet 0/1 receive-only
Ruijie(config-bridge-map)# lan-ip 192.168.1.0 255.255.255.0
Ruijie(config-bridge-map)# lan-ip 10.10.10.0 255.255.255.0
```

【检验方法】 1：使用 **show bridge-map** *bridge-num* **lan-ip** 命令，可以查看指定桥的内网网段配置。

【提示信息】 1：非单臂模式下配置内网 IP 段，提示不允许配置。

```
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 0/0 GigabitEthernet 0/1 forward
Ruijie(config-bridge-map)# lan-ip 192.168.1.0 255.255.255.0
it's not receive_only mode!
```

2：配置第 101 个内网段，提示内网 IP 段已满。

```
Ruijie#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Ruijie(config)#bridge-map 0
Ruijie(config-bridge-map)# lan-ip 192.168.101.0 255.255.255.0
lan ip net is full!
```

【常见错误】 同上

【平台说明】 所有网关系列产品均支持，必须工作在网桥模式下。

2.3 link-mode

配置桥映射及工作模式。

link-mode *interface-name1 interface-name2* { **forward** | **sniffer** | **bypass** | **receive-only** }

取消已设置的内外网接口的桥接映射关系和转发工作模式。

no link-mode *interface-name1 interface-name2* { **forward** | **sniffer** | **bypass** | **receive-only** }

【参数说明】

参数	描述
interface-name1	桥接映射的内网网络接口，该参数不能配置外网网络接口.
interface-name2	桥接映射的外网网络接口，该参数不能配置内网网络接口。
forward	该桥接映射表对应的内外网接口工作在 forward 工作模式，可以对转发报文进行流量识别，流量阻断，流量控制，流量审计。
sniffer	该桥接映射表对应的内外网接口工作在 sniffer 工作模式，可以对转发报文进行流量识别，流量审计。
bypass	该桥接映射表对应的内外网接口工作在软件 bypass 工作模式，转发报文只进行接口报文收发统计后就直接转发。
receive-only	该桥接模式表对应的内外网口工作在 *receive-only* 工作模式，可以对转发报文进行流量识别等操作，但是只接收报文，不转发报文。

【缺省配置】 无。

【命令模式】 桥接映射表命令层配置模式

【缺省级别】 14

【使用指导】 不支持子接口配置桥接工作模式。
用户应根据实际需要，在设备桥模式下选择适当的工作模式。

必须切换到非网关模式才能配置，非网关模式的切换命令详见 sys-mode 命令。

【配置举例】 1：配置内网口 GigabitEthernet 0/0 和外网口 GigabitEthernet 0/1 工作在 forward 工作模式下。

```
Ruijie(config)#bridge-map 0
Ruijie(config-bridge-map)#link-mode GigabitEthernet 0/0 GigabitEthernet 0/1 forward
```

【检验方法】 1：使用 **show bridge-map** 命令，可以查看当前桥配置情况。

【提示信息】 1：配置桥映射的工作模式为 bypass 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 0/0 GigabitEthernet 0/1 bypass
```

2：如果重复配置此命令，则新配置覆盖原有配置。

```
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 0/0 GigabitEthernet 0/1 forward
```

3：如果第一个接口不是内网口，或者第二个接口不是外网口，或者两个接口一样，都会出现提示。此处假设 Gi0/0 和 Gi0/2 是内网口，Gi0/1 是外网口。

```
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 0/1 GigabitEthernet 0/0 forward
%% Wan interface is not suitable for bridge-map inside interface, please use lan interface instead.

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 0/0 GigabitEthernet 0/2 forward
%% Lan interface is not suitable for bridge-map ouside interface, please use wan interface instead.

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 0/0 GigabitEthernet 0/0 forward
%% Inside interface can't be the same as outside interface.
```

4：如果指定的接口已在其他的桥映射表中，则会出现提示。

```
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 0/0 GigabitEthernet 0/1 forward
%% Lan interface has configured on other bridge map.

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 0/2 GigabitEthernet 0/1 forward
%% Wan interface has configured on other bridge map.
```

【常见错误】 1：没有选择正确的属性的接口组成桥。

2：配置单臂模式后，没有配置其内网 IP 段。

【平台说明】 其他网关系列产品只支持 forward、sniffer、软件 bypass、单臂模式四种工作模式，必须工作在网桥模式下。

2.4 native-vlan

设置桥接映射表的 native-vlan id 值。
native-vlan *vlan-id*

取消设置桥接映射表的 native-vlan id 值。
no native-vlan

恢复缺省配置。
default native-vlan

【参数说明】

参数	描述
native-vlan *vlan-id*	Vlan id 值，参数允许范围为 1~4094
default	缺省的 native-vlan 编号为 1

【缺省配置】 缺省的 native-vlan 编号为 1。

【命令模式】 桥接映射表命令层配置模式

【缺省级别】 14

【使用指导】 在实际网络环境，如果这个桥收到的报文没有带 vlan tag，则该报文将被识别为当前配置的 vlan id 对应的 vlan 分类对象；如果有带 vlan tag，则识别为该 tag 对应的 vlan 分类对象。

必须切换到非网关模式才能配置，非网关模式的切换命令详见 sys-mode 命令。

【配置举例】 1：配置桥接映射表 1 的 native-vlan id 为 100。

```
Ruijie(config)#bridge-map 1
Ruijie(config-bridge-map)#native-vlan 100
```

【检验方法】 1：使用 **show bridge-map** 命令，可以查看当前的 native-vlan 配置。

【提示信息】 1：配置桥映射表的 native-vlan id 为 100，配置成功无提示，可以用新配置覆盖原有配置。

```
Ruijie#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Ruijie(config)#bridge-map 1
Ruijie(config-bridge-map)#native-vlan 100
```

2：如果指定的 id 超过 4094，则命令无法配置下去。

【常见错误】 -

【平台说明】 所有网关系列产品均支持，必须工作在网桥模式下。

2.5 show bridge-map

显示桥接映射表的相关信息。

show bridge-map *bridge-num* [**lan-ip**]

【参数说明】

参数	描述
bridge-map *bridge-num*	桥接映射表索引号。

【命令模式】 特权模式、全局模式、接口模式

【缺省级别】 14

【使用指导】 通过指定桥接映射表索引号，来显示相关桥接映射表的信息。

不指定桥接映射表索引，则显示所有桥接映射表的信息。

带上 lan-ip 参数，可以显示单臂模式的内网 IP 段配置

必须切换到非网关模式才能配置，非网关模式的切换命令详见 sys-mode 命令。

【配置举例】 1：查看所有桥映射表的的详细信息

```
Ruijie# show bridge-map
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

BRIDGE MAP 1,STATE is DOWN
  Inside interface is NULL,Outside interface is NULL
  Working mode is null
  Native vlan is 1

BRIDGE MAP 2,STATE is DOWN
  Inside interface is NULL,Outside interface is NULL
  Working mode is null
  Native vlan is 1
```

字段解释：

字段	说明

Inside interface	组成桥的内网接口
Outside interface	组成桥的外网接口
Working mode	当前桥映射的工作模式 ,有 forward、sniffer、bypass、receive-only 四种。
Native vlan	当桥桥映射的 native-vlan 编号

2：查看单臂模式下内网 IP 段配置情况

```
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
```

字段解释：

字段	说明
IP add	内网 IP 地址
mask add	内网 IP 段掩码

【提示信息】 -

【平台说明】 所有网关系列产品均支持，必须工作在网桥模式下。

2.6 show sys-mode

查看系统模式，接口内外网属性的相关信息。

show sys-mode

【参数说明】

参数	描述
-	-

【命令模式】 特权模式、全局模式、接口模式

【缺省级别】 14

【使用指导】 -

【配置举例】 1：查看详细信息

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

字段解释：

字段	说明
System	系统模式
LAN	具备内网属性的接口列表
WAN	具备外网属性的接口列表

【提示信息】 -

【平台说明】 -

2.7 specify interface

设置接口的内外网属性。
specify interface *interface-name* { **lan** | **wan** }

取消设置接口的内外网属性。
no specify interface *interface-name*

【参数说明】

参数	描述
interface *interface-name*	要配置的接口名称。
lan	设置为内网接口。
wan	设置为外网接口。

【缺省配置】 网络接口的缺省内外网属性在不同的设备型号上有所不同。

【命令模式】 全局模式

【缺省级别】 14

【使用指导】 在全局配置模式下，配置接口的内外网属性，no 命令恢复接口属性到默认值。可支持物理接口。
聚合口具备内外网属性，其内外网属性由加入其中的接口成员的属性决定，不支持手动切换。
部分子接口也具有内外网属性：以太口的子接口，dialer 口的子接口。其内外网属性不支持手工配置。
这类子接口创建时从主接口继承内外网属性，主接口在修改内外网配置后重启生效，然后同步给子接口。
内外网属性的修改，需要保存配置重启生效。

【配置举例】 1：配置 GigabitEthernet 0/0 为内网接口。

```
Ruijie(config)#specify interface GigabitEthernet 0/0 lan
```

【检验方法】 1：使用 **show sys-mode** 命令，可以查看所有网络接口的内外网属性。

【提示信息】 1：配置成功或重复配置，无提示。

2：配置聚合口为外网口，提示不允许。

```
Ruijie#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Ruijie(config)#specify interface Aggregateport 0 wan
Converting interface attribute to wan is not supported on AP member.
```

【常见错误】 1：输入的接口名称不正确。

【平台说明】 -

2.8 sys-mode gateway

设置系统模式为网关模式。

sys-mode gateway

【参数说明】 -

【缺省配置】 缺省为网关模式。

【命令模式】 全局模式

【缺省级别】 14

【使用指导】 该命令用于指定系统工作在网关模式下。

系统工作在网关模式下时，根据路由表来转发报文，可以进行 NAT 转换，此时的网络接口为三层口，可以配置 IP 地址。

【配置举例】 1：配置系统工作模式为网关模式。

```
Ruijie(config)# sys-mode gateway
```

【检验方法】 1：使用 **show sys-mode** 命令，可以查看当前系统模式状态。

【提示信息】 -

【常见错误】 -

【平台说明】 -

2.9 xaui-mode

设置接口工作在万兆模式。
xaui-mode slot *slot-num*

取消设置，切换到 4 个千兆口模式。
no xaui-mode slot *slot-num*

【参数说明】

参数	描述
slot-num	万兆口槽号，范围为[2,3]

【缺省配置】 无配置。

【命令模式】 全局配置模式

【缺省级别】 14

【使用指导】 1、4 个千兆口与一个万兆口之间切换。
2、命令需保存配置，重启生效。

【配置举例】 例 1：配置将第一个万兆口启用：

```
Ruijie(config)#xaui-mode slot 2
```

【检验方法】 1：设备重启后，使用 **show running-config** 命令，可以查看当前的万兆口配置情况。
2：设备重启后，**show interface**，会生成一个万兆口（slot 2 对应 TenGigabitEthernet 0/2，slot 3 对应 TenGigabitEthernet 0/3）

【提示信息】 配置成功提示：

```
Please save the config, and reload system to take effect!
```

其余以“error:”开头的提示为错误提示。

【常见错误】 同上

【平台说明】

2.10 write-db enable

开启日志信息不保存本地硬盘功能。
no write-db enable

关闭日志信息不保存本地硬盘功能。
write-db enable

【参数说明】 -

【缺省配置】 EG2000X/XE/UE、ACE3000E 缺省开启日志信息不保存本地硬盘功能，EG2000G/GE、ACE2000E 缺省关闭。

【命令模式】 全局模式

【缺省级别】 14

【使用指导】 该命令用于开启或关闭日志信息不保存本地硬盘功能。需要保存配置后重启才能生效。
开启日志信息不保存本地硬盘功能，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本地硬盘。

【配置举例】 1：配置开启日志信息不保存本地硬盘功能。

```
Ruijie(config)#no write-db enable
```

【检验方法】 1：使用 **show write-db** 命令，可以查看当前设备是否开启日志信息不保存本地硬盘功能。

【提示信息】 -

【常见错误】 1：修改日志信息是否保存本地硬盘配置，提示重启后生效。

```
Ruijie#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Ruijie(config)# no write-db enable
Write-db status has changed, you must save config and reload the system.
```

【平台说明】 -

3 DLDP

3.1 clear dldp

清除 DLDP 各个监测点中关于 up/down 次数的统计信息，并重新开始进行统计。

clear dldp [**interface** *interface-name* [*ip-address*]]

【参数说明】

参数	描述
interface-name	三层接口名称
ip-address	对端设备的 IP 地址

【命令模式】 特权模式

【缺省级别】 2

【命令模式】 特权模式

【使用指导】 DLDP 有记录链路 up/down 次数的统计信息 通过执行本命令可以清除指定监测点的 up/down 统计次数，并且重新开始统计。通过指定三层接口或设备 IP 地址，可以清除指定三层接口上所有监测点或某一监测点的 up/down 统计次数。当未指定三层接口和设备 IP 地址时，表示清除所有监测点的 up/down 统计次数。

【配置举例】 1：清除所有监测点的 up/down 统计次数：

```
Ruijie#clear dldp
```

2：清除 interface GigabitEthernet 0/0 接口上所有监测点的 up/down 统计次数：

```
Ruijie#clear dldp interface GigabitEthernet 0/0
```

3：清除 interface GigabitEthernet 0/0 接口上关于对端设备 10.83.132.1 的 up/down 统计次数：

```
Ruijie# clear dldp interface GigabitEthernet 0/0 10.83.132.1
```

【提示信息】 -

【平台说明】 -

3.2 dldp

开启 DLDP 检测功能。用户可以使用该命令的 no 选项关闭指定 IP 的 DLDP 检测功能。

dldp *ip-address* [*next-hop-ip*] [**mac-address** mac-addr] [**interval** *tick* | **retry** *retry-num* | **resume** *resume-num*]

no dldp *ip-address*

【参数说明】

参数	描述
ip-address	被检测对端设备的 IP 地址。
next-hop-ip	若被检测对端设备处于跨网段，用以指定下一跳 IP 地址。
mac-address mac-addr	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。
interval *tick*	探测间隔时间。取值范围 5~6000，单位为 tick，必须为 5 的整数倍。（1tick=10ms）
retry *retry-num*	重传次数，该参数范围 1~3600。
resume *resume-num*	对应被检测对端设备的链路恢复次数，该次数设置链路从 DOWN 状态变为 UP 前，需要收到连续的 DLDP 检测报文个数，该参数范围 1~200。

【缺省配置】 tick 为 10tick（100ms），retry-num 为 3 次，resume-num 为 3 个。

【命令模式】 接口配置模式。

【缺省级别】 14

【使用指导】 通过配置本命令启动 DLDP 检测功能，可以实现对以太网链路故障的快速检测。
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。

【配置举例】 例 1：开启对设备 10.83.132.10 的 DLDP 检测功能：

```
Ruijie(config)#int gi0/0
Ruijie(config-if-GigabitEthernet 0/0)#ip address 10.83.132.1 24
Ruijie(config-if-GigabitEthernet 0/0)#dldp 10.83.132.10
Ruijie(config-if-GigabitEthernet 0/0)#
```

例 2：开启对跨网段设备 10.83.131.10 的 DLDP 检测功能：

```
Ruijie#config
Ruijie(config)# int gi0/0
Ruijie(config-if-GigabitEthernet 0/0)#ip address 10.83.132.1 255.255.255.0
Ruijie(config-if-GigabitEthernet 0/0)#dldp 10.83.131.10 10.83.132.2
```

例 3：关闭对设备 10.83.132.10 的 DLDP 检测功能：

```
Ruijie#config
Ruijie(config)# int gi0/0
Ruijie(config-if-GigabitEthernet 0/0)#no dldp 10.83.132.10
```

【提示信息】 -

【常见错误】 -

【平台说明】 -

3.3 dldp interval

设置所有 DLDP 检测的探测间隔时间。用户可以使用该命令的 no 选项恢复缺省检测模式。

dldp interval *tick*

no dldp interval

【参数说明】

参数	描述
tick	探测间隔时间。取值范围 5~6000 ,单位为 tick ,必须为 5 的整数倍。(1tick= 10ms)

【缺省配置】 tick 为 10（100ms）

【命令模式】 全局配置模式

【缺省级别】 14

【使用指导】 在实际应用中，如果需要对所有 DLDP 检测的探测间隔时间进行设置，则可使用该命令快速生效。

当网络设备在“检测报文的发送间隔”×“重传次数”的时间周期内没有收到对端的应答报文，则认为三层接口 DOWN（实际物理链路还是连通的）。一旦恢复正常通讯，则三层接口 UP。

【配置举例】 配置 DLDP 检测的探测间隔时间：

```
Ruijie#config
Ruijie(config)#dldp interval 20
```

【提示信息】 -

【常见错误】 -

【平台说明】 -

3.4 dldp passive

设置 DLDP 检测模式为被动模式。用户可以使用该命令的 no 选项恢复缺省检测模式。

dldp passive

no dldp passive

【参数说明】

参数	描述
-	-

【缺省配置】 主动模式

【命令模式】 接口配置模式

【缺省级别】 14

【使用指导】 实际网络中，如果两端设备都打开 DLDP，通过两端互发 ICMP Echo 来实现通路检测，这中方式存在多余重复的报文。实际中只要有一端设备使用 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，就可以实现双方设备检测链路通路的效果，并且也节省了带宽资源和设备 CPU 资源的消耗。因此可以将主动发 ICMP Echo 的设备配置为主动模式，而将被动接收 ICMP Echo 的设备配置成被动模式。

启动被动模式时，需要确保对端设备的时间参数配置与本设备完全一致，以便同步链路状态效果的检测。否则在被动模式中可能因对端发包的不同步而引起链路状态误判。

【配置举例】 配置 DLDP 的检测模式为被动模式：

```
Ruijie#config
Ruijie(config)#interface gi0/0
Ruijie(config-if-GigabitEthernet 0/0)#ip address 10.83.132.1 255.255.255.0
Ruijie(config-if-GigabitEthernet 0/0)#dldp passive
```

【提示信息】 -

【常见错误】 -

【平台说明】 -

3.5 dldp resume

设置所有 DLDP 检测的链路恢复次数。用户可以使用该命令的 no 选项恢复缺省检测模式。

dldp resume *resume-num*

no dldp resume

【参数说明】

参数	描述
resume-num	对应被检测对端设备的链路恢复次数 ,该次数设置链路从 DOWN 状态变为 UP 前，需要收到连续的 DLDP 检测报文个数，该参数范围 1~200。

【缺省配置】 resume-num 为 3 个。

【命令模式】 全局配置模式

【缺省级别】 14

【使用指导】 在实际应用中，如果需要对所有 DLDP 检测的链路恢复次数进行设置，则可使用该命令快速生效。

【配置举例】 配置 DLDP 检测的探测间隔时间：

```
Ruijie#config
Ruijie(config)#dldp resume 4
```

【提示信息】 -

【常见错误】 -

【平台说明】

3.6 dldp retry

设置所有 DLDP 检测的重传次数。用户可以使用该命令的 no 选项恢复缺省检测模式。

dldp retry *retry-num*

no dldp retry

【参数说明】

参数	描述
retry-num	重传次数，该参数范围 1~3600。

【缺省配置】 retry-num 为 3 次

【命令模式】 全局配置模式

【缺省级别】 14

【使用指导】 在实际应用中，如果需要对所有 DLDP 检测的重传次数进行设置，则可使用该命令快速生效。

【配置举例】 配置 DLDP 检测的探测间隔时间：

```
Ruijie#config
Ruijie(config)#dldp retry 4
```

【提示信息】 -

【常见错误】 -

【平台说明】 -

3.7 show dldp

显示 DLDP 中各个监测点的配置或统计信息。

show dldp [**statistic**] [**interface** *interface-name*]

【参数说明】

参数	描述
interface-name	三层接口名称
statistic	统计信息

【缺省配置】 -

【命令模式】 特权模式

【缺省级别】 2

【使用指导】 通过指定 statistic 关键字来显示所有监测点或指定三层接口上所有监测点的统计信息。指定三层接口名称，用以显示特定三层接口上所有监测点的配置和统计信息。

【配置举例】 例 1：显示所有监测点的配置信息：

```
Ruijie#show dldp
Interface  Type         Ip          Next-hop    Interval  Retry  Resume  State
---------  -------  ----------  ----------  --------  -----  ------  ------
Gi0/0      Passive  192.168.6.3  192.168.2.2  10        5      3       Up
Gi0/1      Passive  192.168.7.3              10        5      3       Up
Gi0/2      Passive  192.168.3.3  192.168.4.2  10        5      3       Up
```

例 2：显示三层接口 gigabitEthernet 0/0 上所有监测点的配置信息：

```
Ruijie#show dldp intface gigabitEthernet 0/0
Interface  Type         Ip          Next-hop    Interval  Retry  Resume  State
---------  -------  ----------  ----------  --------  -----  ------  ------
```

```
Gi0/0       Passive   192.168.6.3   192.168.2.2   10          5       3         Up
```

例 3：显示所有监测点的统计信息：

```
Ruijie#show dldp statistic
Interface   Type          Ip        record-time   Up-count   Down-count
---------   -------   -----------   -----------   --------   ----------
Gi0/0       Passive   192.168.6.3   2h34m5s       10         9
Gi0/1       Passive   192.168.3.3   1d2h3m52s     10         9
```

例 4：显示三层接口 gigabitEthernet 0/0 上所有监测点的统计信息：

```
Ruijie#show dldp statistic interface gigabitEthernet 0/0
Interface   Type          Ip        record-time   Up-count   Down-count
---------   -------   -----------   -----------   --------   ----------
Gi0/0       Passive   192.168.6.3   2h34m5s       10         9
```

字段	说明
record-time	该信息表示用于统计 up/down 次数的时间段长度。对应时间长的显示格式为 *y***d**h**m**s，这里的 y 表示年，d 表示天，h 表示小时，m 表示分钟，s 表示秒。结合后面的 Up-count Down-count 参数，即说明在这段时间内，up/down 了多少次。
Up-count	对应监测点记录的协议状态 up 次数。
Down-count	对应监测点记录的协议状态 down 次数。

【提示信息】 -

【平台说明】 -

4 PCAP

4.1 packet capture file

指定保存的文件名。

packet capture file *filename* **[buffer-size** *buf-size***] [packet-num** *pkt-num***]**

删除保存文件，恢复为输出 log

clear packet capture file

【参数说明】

参数	描述
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。

【命令模式】 特权模式

【缺省级别】 14

【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。

【配置举例】 例 1：指定保存的文件名为 capture.pcap，抓取 100 个报文

```
Ruijie# packet capture file flash:capture.pcap packet-num 100
```

【检验方法】 执行该命令以后，用户可通过 show packet capture status 检查配置是否成功。

【提示信息】 -

【常见错误】 -

【平台说明】 -

4.2 packet capture point

创建抓包点。

packet capture point *capture-point-name* **rule** *rule-name* **location {interface** *interface-name* | **vlan** *vlan-id* |

control-plane} {in | out | both}

删除抓包点。

clear packet capture point *capture-point-name*

【参数说明】

参数	描述
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

【缺省级别】 14

【使用指导】 1、根据需要，用户可以在同一位置定义多个（目前支持 4 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。

【配置举例】 例 1：创建抓取 Gi0/1 接口的 CPU 报文的抓包点

```
Ruijie# packet capture point cap-1 rule tcp location interface gi0/1 both
```

【检验方法】 执行该命令以后，用户可通过 show packet capture status 检查配置是否成功。

【提示信息】 -

【常见错误】 -

【平台说明】 -

4.3 packet capture rule

定义抓包匹配规则。

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***]**

删除抓包匹配规则。

clear packet capture rule *rule-name*

【参数说明】

参数	描述

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

【命令模式】 特权模式

【缺省级别】 14

【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。

【配置举例】 例 1：定义 tcp 协议抓包匹配规则

```
Ruijie# packet capture rule tcp etype ip protocol tcp
```

【检验方法】 执行该命令以后，用户可通过 show packet capture status 检查配置是否成功。

【提示信息】 -

【常见错误】 -

【平台说明】 -

4.4 packet capture start

开始抓包。
packet capture start

停止抓包。
packet capture stop

【参数说明】

参数	描述

start	开始抓包
stop	停止抓包

【命令模式】 特权模式

【缺省级别】 14

【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。

【配置举例】 例 1：开始抓包

```
Ruijie# packet capture start
```

【检验方法】 执行该命令以后，用户可通过 show packet capture status 检查配置是否成功。

【提示信息】 -

【常见错误】 -

【平台说明】 -

4.5 show packet capture status

查看抓包信息。

show packet capture status

【参数说明】

参数	描述
-	

【命令模式】 特权用户模式

【缺省级别】 14

【使用指导】 执行本命令可以查看抓包信息。

【配置举例】 -

【提示信息】 例 1：查看抓包信息显示如下：

```
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#
```

字段解释：

字段	说明
Capture rule	抓包规则名称
etype	二层协议类型
source MAC	源 MAC
destination MAC	目的 MAC
protocol	三层协议类型
source IP	源 IP

destination IP	目的 IP
source port	源端口
destination port	目的端口
Capture point	抓包点名称
location	抓包位置
direction	抓包方向
buffer size	buffer 大小
packets limit	抓包数目限制
filename	输出文件名称
status	抓包状态
packets captured	已捕获的报文数量

【平台说明】 -

5 PPPOE-CLIENT

5.1 clear dialer

清除拨号接口的统计信息。

clear dialer

【参数说明】

参数	描述
-	-

【命令模式】 特权模式

【缺省级别】 14

【使用指导】 此命令用来清除拨号接口的统计信息。

【配置举例】 1：清除拨号接口的统计信息。

```
R1# clear dialer
```

【提示信息】 -

【平台说明】 -

5.2 clear pppoe tunnel

清除所有 PPPoE 隧道。

clear pppoe tunnel

【参数说明】

参数	描述
-	-

【命令模式】 特权模式

【缺省级别】 14

【使用指导】 此命令用来清除所有 PPPoE 隧道。

【配置举例】 1：清除所有 PPPoE 隧道。

```
R1# clear pppoe tunnel
```

【提示信息】 -

【平台说明】 -

5.3 dialer enable-timeout

配置线路无效时间。
dialer enable-timeout *seconds*

恢复线路无效时间缺省值。
no dialer enable-timeout

【参数说明】

参数	描述
Seconds	线路无效时间（秒）。

【缺省配置】 15 秒。

【命令模式】 接口模式

【缺省级别】 14

【使用指导】 线路无效时间是线路切断或拨号失败后至可以拨号之前接口的等待时间，即接口再次拨号前的等待时间。

【配置举例】 1：配置 dialer 1 口线路无效时间为 20 秒。

```
R1(config)# interface dialer 1
R1(config-if-dialer 1)# dialer enable-timeout 20
```

2：恢复 dialer 1 口线路无效时间为缺省值。

```
R1(config)# interface dialer 1
R1(config-if-dialer 1)# no dialer enable-timeout
```

【检验方法】 1：使用 **show running-config interface dialer** *1* 命令，查看配置是否存在。

【提示信息】 -

【常见错误】 -

【平台说明】 -

5.4 dialer hold-queue

配置接口的保持队列。

dialer hold-queue *packets* [**timeout** *seconds*]

关闭保持队列。

no dialer hold-queue [*packets* [**timeout** *seconds*]]

【参数说明】

参数	描述
Packets	队列中保持的报文分组数，取值 0 到 100。
timeout *seconds*	分组保持在队列的时间（秒），缺省是 45 秒。

【缺省配置】 关闭保持队列。

【命令模式】 接口模式

【缺省级别】 14

【使用指导】 设备使用 MODEM 拨号进行连接需要一段协商时间，在此期间会丢弃报文。但如果配置了保持队列，则可以让配备刺激拨号规则的报文保存在设备上，连接建立以后，立即发送。

【配置举例】 1：配置 dialer 1 口的保持队列为 50 个报文分组。

```
R1(config)# interface dialer 1
R1(config-if-dialer 1)# dialer hold-queue 50
```

2：关闭 dialer 1 口的保持队列。

```
R1(config)# interface dialer 1
R1(config-if-dialer 1)# no dialer hold-queue
```

【检验方法】 1：使用 **show running-config interface dialer** *1* 命令，查看配置是否存在。

【提示信息】 -

【常见错误】 -

【平台说明】 -

5.5 dialer idle-timeout

配置线路空闲时间。

dialer idle-timeout *seconds*

恢复线路空闲时间缺省值。
no dialer idle-timeout

【参数说明】

参数	描述
Seconds	线路空闲时间（秒）。

【缺省配置】 120 秒。

【命令模式】 接口模式

【缺省级别】 14

【使用指导】 线路空闲时间指定拨号线路在没有数据通信多长时间切断线路，期间收到一个到目的地址的报文，将重新复位线路空闲时间。

【配置举例】 1：配置 dialer 1 口线路空闲时间为 60 秒。

```
R1(config)# interface dialer 1
R1(config-if-dialer 1)# dialer idle-timeout 60
```

2：恢复 dialer 1 口线路空闲时间为缺省值。

```
R1(config)# interface dialer 1
R1(config-if-dialer 1)# no dialer idle-timeout
```

【检验方法】 1：使用 **show running-config interface dialer** *1* 命令，查看配置是否存在。

【提示信息】 -

【常见错误】 -

【平台说明】 -

5.6 dialer pool

配置逻辑口关联的拨号池。
dialer pool *number*

取消逻辑口关联的拨号池。
no dialer pool *number*

【参数说明】

参数	描述
number	物理拨号池的编号，有效值为 1~255 之间的整数。

【缺省配置】 不关联拨号池。

【命令模式】 接口模式

【缺省级别】 14

【使用指导】 在高级拨号中，逻辑接口必须关联具体物理口才能进行实际拨号。为了建立逻辑接口和物理接口的关联，使用了拨号池。首先，将具体物理接口加入一个或多个拨号池，然后，在逻辑接口上关联其中一个拨号池，从而实现逻辑接口和物理接口的关联。一个物理接口可以属于多个拨号池，但一个逻辑接口只能关联一个拨号池，逻辑接口在进行具体拨号的时候，随机选择拨号池中空闲的接口进行拨号。

【配置举例】 1：配置 dialer 1 口关联的拨号池 1。

```
R1(config)# interface dialer 1
R1(config-if-dialer 1)# dialer pool 1
```

2：取消 dialer 1 口关联的地址池。

```
R1(config)# interface dialer 1
R1(config-if-dialer 1)# no dialer pool
```

【检验方法】 1：使用 **show running-config interface dialer** *1* 命令，查看配置是否存在。

【提示信息】 -

【常见错误】 -

【平台说明】 -

5.7 dialer-group

关联接口刺激拨号的规则。
dialer-group *group-number*

删除拨号口关联的拨号刺激规则。
no dialer-group

【参数说明】

参数	描述
group-number	刺激拨号规则的编号。

【缺省配置】 没有关联拨号规则。

【命令模式】 接口模式

【缺省级别】 14

【使用指导】 一个接口如果试图拨号，首先必须确定什么报文可以刺激拨号，刺激拨号规则有全局配置命令 **dialer-list** 指定，然后，在接口上关联其中一条拨号规则。

【配置举例】 1：将 dialer 1 口关联接口刺激拨号的规则 1。

```
R1(config)# interface dialer 1
R1(config-if-dialer 1)# dialer-group 1
```

2：删除 dialer 1 口关联的刺激拨号规则。

```
R1(config)# interface dialer 1
R1(config-if-dialer 1)# no dialer-group
```

【检验方法】 1：使用 **show running-config interface dialer** *1* 命令，查看配置是否存在。

【提示信息】 -

【常见错误】 -

【平台说明】 -

5.8 dialer-list

定义刺激拨号的规则。

dialer-list *dialer-group* **protocol** *protocol-name* **ip** { **permit** | **deny** | **list** *access-list-number* }

删除指定的刺激拨号规则。

no dialer-list *dialer-group* [**protocol** *protocol-name* **ip** { **permit** | **deny** | **list** *access-list-number* }]

【参数说明】

参数	描述
dialer-group	刺激拨号规则的编号。
protocol *protocol-name*	协议名称。
Ip	允许的是 IP 协议
Permit	允许整个 IP 协议。
Deny	拒绝整个 IP 协议。
List	使用访问列表而不是整个协议来定义刺激拨号规则。
access-list-number	访问列表的编号。

【缺省配置】 不定义刺激拨号规则。

【命令模式】 全局模式

【缺省级别】 14

【使用指导】 该命令在全局配置模式下定义一条或多条刺激拨号规则 ,然后用 **dialer-group** 将拨号规则应用于具体的接口拨号。属于拨出必须配置的命令之一。

【配置举例】 1：配置拨号刺激规则 1 为允许 IP 协议报文。

```
R1(config)# dialer-list 1 protocol ip permit
```

2：删除拨号刺激规则 1。

```
R1(config)# no dialer-list 1
```

【检验方法】 1：使用 **show running-config | include dialer-list** *1* 命令，查看配置是否存在。

【提示信息】 -

【常见错误】 -

【平台说明】 -

5.9 ip address

配置接口 IP 策略。

ip address { **negotiate |** *ip-addr subnet-mask* }

删除接口 IP 策略。

no ip address

【参数说明】

参数	描述
negotiate	配置接口通过 PPP 协商获得 IP 地址。
ip-addr	指定接口 IP
subnet-mask	指定接口掩码

【缺省配置】 没有缺省值。

【命令模式】 接口模式

【缺省级别】 14

【使用指导】 该命令主要用于指定逻辑接口 IP 的获得方式。
如果选择通过 PPP 协商获得地址，则逻辑接口的 IP 由服务器端分配。
如果手工指定逻辑接口的 IP，需要在协商过程中得到服务器端的同意，所指定的 IP 才能生效。

【配置举例】 1：配置 dialer 1 口的 IP 获得方式为 PPP 协商获得。

```
R1(config)# interface dialer 1
R1(config-if-dialer 1)# ip address negotiate
```

2：删除 dialer 1 口的 IP 策略。

```
R1(config)# interface dialer 1
R1(config-if-dialer 1)# no ip address
```

【检验方法】 1：使用 **show running-config interface dialer** *1* 命令，查看配置是否存在。
2：使用 **show ip interface brief | in dialer** *1* 命令，查看配置是否协商到 IP 且已经协议 UP。

【提示信息】 -

【常见错误】 -

【平台说明】 -

5.10 ppp max-bad-auth

指定 PPP 认证的重试次数。
ppp max-bad-auth *number*

恢复 PPP 认证重试次数为默认值。
no ppp max-bad-auth

【参数说明】

参数	描述
number	PPP 认证重试次数，取值范围为 1-255。

【缺省配置】 不进行重试。

【命令模式】 接口模式

【缺省级别】 14

【使用指导】 重试次数包含第一次的认证，即如果配置重试次数为 3，第一次认证失败以后，还能重新认证 2 次。最后一次

认证失败以后，线路被挂断（复位）。

【配置举例】 1：配置 dialer 1 口的 PPP 认证的重试次数为 3。

```
R1(config)# interface dialer 1
R1(config-if-dialer 1)# ppp max-bad-auth 3
```

2：恢复 PPP 认证重试次数为默认值。

```
R1(config)# interface dialer 1
R1(config-if-dialer 1)# no ppp max-bad-auth
```

【检验方法】 1：使用 **show running-config interface dialer** *1* 命令，查看配置是否存在。

【提示信息】 -

【常见错误】 -

【平台说明】 -

5.11 pppoe enable

启用接口的 PPPoE 功能。
pppoe enable

关闭接口的 PPPoE client 功能。
no pppoe enable

【参数说明】

参数	描述
-	-

【缺省配置】 接口的 PPPoE 功能关闭。

【命令模式】 接口模式

【缺省级别】 14

【使用指导】 必须要在 WAN 属性的物理口或者 WAN 属性的聚合口上才能配置。如果接口是 LAN 属性，命令不显示。

【配置举例】 1：启用 GigabitEthernet 0/5 口的 PPPoE client 功能。

```
R1(config)# interface GigabitEthernet 0/5
R1(config-if- GigabitEthernet 0/5)# pppoe enable
```

2：关闭 GigabitEthernet 0/5 口的 PPPoE client 功能。

```
R1(config)# interface GigabitEthernet 0/5
R1(config-if- GigabitEthernet 0/5)# no pppoe enable
```

【检验方法】 1：使用 **show running-config interface GigabitEthernet** *0/5* 命令，查看配置是否存在。

【提示信息】 -

【常见错误】 -

【平台说明】 -

5.12 pppoe multi-dial enable

开启设备的 PPPoE Client 多拨功能。即在一个物理口上可以配置多路 pppoe 拨号，如果不启用，那么在每个物理口上只能启用一路 pppoe 拨号。

pppoe multi-dial enable

关闭设备的 PPPoE Client 多拨功能。

no pppoe multi-dial enable

【参数说明】

参数	描述
-	-

【缺省配置】 设备上的 PPPoE Client 多拨功能默认关闭。

【命令模式】 全局模式

【缺省级别】 14

【使用指导】 该命令用来开启 PPPOE 的多拨功能，默认是关闭的。

【配置举例】 1：在全局模式下启用设备的 PPPoE Client 多拨功能

```
R1(config)# pppoe multi-dial enable
```

2：关闭设备的 PPPoE Client 多拨功能。

```
R1(config)# no pppoe multi-dial enable
```

【检验方法】 1：使用 **show running-config** 命令，查看配置是否存在。

【提示信息】 -

【常见错误】 -

【平台说明】 -

5.13 pppoe session mac-address

配置接口上 pppoe 会话的 mac 地址。
pppoe session mac-address *H.H.H*

删除接口上配置的 pppoe 会话的 mac 地址。
no pppoe session mac-address

【参数说明】

参数	描述
H.H.H	mac 地址

【缺省配置】 关闭。

【命令模式】 接口模式

【缺省级别】 14

【使用指导】 使用该命令可以指定 pppoe 拨号会话的 mac 地址，该配置可以在接口下配置，但是仅仅在子接口下才能配置生效。在子接口上配置会话的 mac 地址之前必须使能该接口的 pppoe 功能。

【配置举例】 1：配置 GigabitEthernet 0/5.1 的 pppoe 会话的 mac 地址为 00d0.f822.33f3。

```
Ruijie (config)# interface GigabitEthernet 0/5.1
Ruijie(config-subif-GigabitEthernet 0/5.1)#pppoe enable
Ruijie(config-subif-GigabitEthernet 0/5.1)#encapsulation dot1Q 1
Ruijie(config-subif-GigabitEthernet 0/5.1)#pppoe sessiom mac-address 00d0.f822.33f3
```

2：删除 GigabitEthernet 0/5.1 接口上配置的 pppoe 会话的 mac 地址。

```
Ruijie (config)# interface GigabitEthernet 0/5.1
Ruijie(config-subif-GigabitEthernet 0/5.1)#no pppoe sessiom mac-address
```

【检验方法】 1：使用 **show running-config interface GigabitEthernet** *0/5.1* 命令，查看配置是否存在。

【提示信息】 1：接口需要先启用 PPPoE 功能。
PPPoE: must enable PPPoE firstly.

【常见错误】 -

【平台说明】 -

5.14 pppoe-client dial-pool-number

将以太口加入拨号池，并配置拨号类型。
pppoe-client dial-pool-number *number* **no-ddr**

将以太口从拨号池中取出，并删除其拨号策略。
no pppoe-client dial-pool-number *number*

【参数说明】

参数	描述
number	拨号池编号。

【缺省配置】 关闭。

【命令模式】 接口模式

【缺省级别】 14

【使用指导】 使用该命令将以太网口绑定到指定一个拨号池，逻辑接口使用指定拨号池，从而为以太网口和逻辑接口建立关联，实现拨号。配置该命令前，接口必须先配置 pppoe enable。

【配置举例】 1：配置 GigabitEthernet 0/5 口加入拨号池 1。

```
R1(config)# interface GigabitEthernet 0/5
R1(config-if- GigabitEthernet 0/5)# pppoe-client dial-pool-number 1 no-ddr
```

2：配置 GigabitEthernet 0/5 口从拨号池 1 中取出。

```
R1(config)# interface GigabitEthernet 0/5
R1(config-if- GigabitEthernet 0/5)# no pppoe-client dial-pool-number 1
```

【检验方法】 1：使用 **show running-config interface GigabitEthernet** *0/5* 命令，查看配置是否存在。

【提示信息】 1：接口需要先启用 PPPoE 功能。
PPPoE: must enable PPPoE firstly.

【常见错误】 -

【平台说明】 -

5.15 show pppoe

查看 PPPoE 会话的相关信息。

show pppoe { **ref** | **session** | **tunnel** }

【参数说明】

参数	描述
Ref	显示所有 PPPoE 会话的快转信息
Session	显示所有 PPPoE 会话信息
Tunnel	显示所有 PPPoE 隧道信息

【命令模式】 特权模式、全局模式、接口模式

【缺省级别】 14

【使用指导】 用于显示 PPPoE 会话的相关信息，通过指定关键字可显示不同形式的 PPPoE 会话信息。

【配置举例】 1：显示所有 PPPoE 会话的快转信息。

```
R1# show pppoe ref

 GigabitEthernet 0/6 Virtual-pppoe 2 dialer 1
  Protocol UP dialer-group 1 last_time 164235070 ms
  Ether Header: 00 60 4F 67 02 50 00 D0 F8 22 33 43 88 64
  PPPoE Header: 11 00 00 7F 00 50
  PPP Header  : 00 21
  DstMac 0060.4f67.0250, SrcMAC 00d0.f822.3343, SessionID 127
  Input Err : 0 MAC, 0 PPPoE Header
  Input Info: 0 Normal, 0 Drop, 345 Reserve, 0 Lost
  Output Err : 0 SessionState, 0 no ref, 0 length
  Output Info: 0 Normal, 0 Drop, 0 Reserve, 0 Lost

 There is 1 pppoe session in System
```

字段解释：因为信息本身已经描述的很清楚了，这里不再重复。

2：显示所有 PPPoE 会话信息。

```
R1# show pppoe session
state is SESSION ,my mac is 00.D0.F8.22.33.43 , peer mac is 00.60.4F.67.02.50
   Timer is running: 59750
```

字段解释：因为信息本身已经描述的很清楚了，这里不再重复。

3：显示所有 PPPoE 隧道信息。

```
R1# show pppoe tunnel
state is SESSION ,my mac is 00.D0.F8.22.33.43 , peer mac is 00.60.4F.67.02.50
   Timer is running: 59003
```

字段解释：因为信息本身已经描述的很清楚了，这里不再重复。

【提示信息】 -

【平台说明】 -

6 PPPoE-SERVER

6.1 ac-cookie enable

要启用 ac-cookie 功能，请在 bba-group 组中配置 ac-cookie enable 命令，该命令的 no 形式恢复到缺省状态。
ac-cookie enable

关闭 ac-cookie。
no ac-cookie enable

恢复缺省配置。
no ac-cookie enable

【参数说明】

参数	描述
-	-

【缺省配置】 关闭 ac-cookie。

【命令模式】 bba-group

【缺省级别】 14

【使用指导】 该命令用于在配置的 bba-group pppoe 组中使能 ac-cookie 功能。

【配置举例】

例 1：下面的示例将使能 ac-cookie 功能：

```
Ruijie(config)# bba-group pppoe pppoe_server_group
Ruijie(config-bba-group)# ac-cookie enable
```

【检验方法】 1：使用 **show run** 命令，可以查看 ac-cookie 是开启还是关闭。

【提示信息】 -

【常见错误】 -

【平台说明】 -

6.2 bba-group pppoe

要设置 bba-group pppoe 拨号组，请在全局配置模式下执行 bba-group pppoe 命令，该命令的 no 形式删除掉指定的 bba group 。

bba-group pppoe *bba-group-name*

删除 bba-group

no bba-group pppoe *bba-group-name*

恢复缺省配置。

default bba-group pppoe *bba-group-name*

【参数说明】

参数	描述
bba-group-name	设置的 bba-group 的名称。

【缺省配置】 缺省未配置 bba-group。

【命令模式】 全局模式。

【缺省级别】 14

【使用指导】 该命令用于配置 bba-group pppoe 组，用于 pppoe-server 端的拨号。

⚠ bba-group-name 最大只能配置 32 个字符。

【配置举例】 例 1：下面的示例将配置一个 bba-group：

```
Ruijie(config)# bba-group pppoe pppoe_server_group
```

【检验方法】 1：使用 **show run** 命令，可以查看 bba-group 的配置。

【提示信息】 -

【常见错误】 -

【平台说明】 -

6.3 pppoe-server enable group

要在接口上启用 pppoe server 功能，请执行 pppoe-server enable group 命令，该命令的 no 形式关闭该接口上的 pppoe server 功能。

pppoe-server enable group *group-name*

关闭 pppoe server 功能。
no pppoe-server enable

恢复缺省配置。
default pppoe-server enable group

【参数说明】

参数	描述
group *group-name*	该接口关联的 bba-group 拨号组

【缺省配置】 缺省情况下，接口上未启用 pppoe-server 的功能。

【命令模式】 接口配置模式

【缺省级别】 14

【使用指导】 要在接口上启用 pppoe-server 的功能，请在接口模式下执行该命令。group-name 最大支持 32 个字符。改命令可以使能在三层物理口或者三层子接口以及 SVI 口上。
在无线产品上，仅支持 SVI 口。

【配置举例】 例 1：以下的例子示范在 vlan 3 上启用 pppoe server 功能。

```
Ruijie(config)# interface vlan 3
Ruijie(config-if-VLAN 3)# pppoe-server enable group pppoe_server_group
```

【检验方法】 1：使用 **show run 或 show interface** 命令可以查看接口是否有开启 pppoe-server。

【提示信息】 -

【常见错误】 -

【平台说明】 -

6.4 sessions local-mac limit

要配置当前 bba-group 组关联的接口所允许本端同一 mac 地址所能接受呼入的最大会话数目，请在指定的 bba-group 组下配置 sessions local-mac limit 命令，该命令的 no 形式恢复至缺省值。
sessions local-mac limit *limit-count*

恢复缺省值。
no sessions local-mac limit

恢复缺省配置。

default sessions local-mac limit

【参数说明】

参数	描述
limit-count	设置的允许本端同一 mac 地址接受的最大会话数目，配置范围为 0-1000。

【缺省配置】 缺省情况下，本端同一 mac 地址所能接受的最大会话数目为 1000。

【命令模式】 bba-group

【缺省级别】 14

【使用指导】 要设置允许本端同一 mac 地址接受的会话数目时，在对应的 bba-group 组下执行该命令。
修改该参数不影响已经建立的会话，对下一条拨入的会话有效。
配置为 0 表示当前接口不允许接受 pppoe 的呼入。

【配置举例】 例 1：设置名为 pppoe_server_group 的 ppoe 拨号组所允许本端 mac 地址接受的会话数目为 50。

```
Ruijie(config)# bba-group pppoe pppoe_server_group
Ruijie(config-bba-group)# sessions local-mac limit 50
```

【检验方法】 1：使用 **show run** 命令，可以查看 bba-group 下的 sessions per-mac 个数。

【提示信息】 -

【常见错误】 -

【平台说明】 -

6.5 sessions max limit

要配置当前系统允许接入的最大会话数目，在 bba-group 模式下配置 sessions max limit 命令，该命令的 no 形式恢复至缺省值。

sessions max limit *limit-count*

恢复缺省值。

no sessions max limit

恢复缺省配置。

no sessions max limit

【参数说明】

参数	描述
limit-count	设置当前系统允许接入的最大会话数目，配置范围为 0-1000。

【缺省配置】 缺省情况下，系统所能接受的最大会话数目为 1000。

【命令模式】 bba-group

【缺省级别】 14

【使用指导】 要设置允许本端系统接受的最大会话数目时，在对应的 bba-group 组下执行该命令。
修改该参数不影响已经建立的会话，对下一条拨入的会话有效。
配置为 0 表示当前接口不允许接受 pppoe 的呼入。
在某一个 bba-group 下设置该值对当前配置的所有 bba-group 有效，同时修改后的值会在所有的 bba-group 组下显示出来。
系统当前所允许接入的会话数目以最后一次配置的该命令为准。

【配置举例】 例 1：设置当前系统所允许的最大会话数目为 500。

```
Ruijie(config)# bba-group pppoe pppoe_server_group
Ruijie(config-bba-group)# sessions max limit 500
```

【检验方法】 1：使用 **show run** 命令，可以查看 bba-group 的 sessions max limit 的配置。

【提示信息】 -

【常见错误】 -

【平台说明】 -

6.6 sessions per-mac limit

要配置当前 bba-group 组关联的接口所允许对端同一 mac 地址所能呼入的最大会话数目，请在指定的 bba-group 组下配置 sessions per-mac limit 命令，该命令的 no 形式恢复至缺省值。
sessions per-mac limit *limit-count*

恢复缺省值。
no sessions per-mac limit

恢复缺省配置。
no sessions per-mac limit

【参数说明】

参数	描述
limit-count	允许对端同一 mac 地址发起的最大会话数目，配置范围为 0-500。

【缺省配置】 缺省情况下，对端同一 mac 地址所能发起的最大会话数目为 100。

【命令模式】 bba-group

【缺省级别】 14

【使用指导】 要设置允许对端同一 mac 地址发起的会话数目时，在对应的 bba-group 组下执行该命令。
修改该参数不影响已经建立的会话，对下一条拨入的会话有效。
配置为 0 表示当前接口不允许接受 pppoe 的呼入。

【配置举例】 例 1：设置名为 pppoe_server_group 的 ppoe 拨号组所允许对端同一 mac 地址发起的会话数目为 50 。

```
Ruijie(config)# bba-group pppoe pppoe_server_group
Ruijie(config-if)# sessions per-mac limit 50
```

【检验方法】 1：使用 **show run** 命令，可以查看 sessions per-mac limit 的配置

【提示信息】 -

【常见错误】 -

【平台说明】 -

6.7 virtual-template

要指定当前 bba-group pppoe 组关联的 virtual-template 接口 ,请在 bba-group pppoe 组下执行 virtual-template 命令，该命令的 no 形式去掉关联
virtual-template *interface-number*

删除 virtual-template。
no virtual-template *interface-number*

恢复缺省配置。
default virtual-template *interface-number*

【参数说明】

参数	描述
interface-number	接口编号。

【缺省配置】 缺省情况下，未关联 virtual-template 接口。

【命令模式】 bba-group

【缺省级别】 14

【使用指导】 要在指定的 bba-group 组下关联 virtual-template 接口，请在 bba-group pppoe 模式下执行该命令。

【配置举例】 例 1：以下的例子指定在 关联 virtual-template 接口 5：

```
Ruijie(config)# bba-group pppoe pppoe_server_group
Ruijie(config-bba-group)# virtual-template 5
```

【检验方法】 1：使用 **show run** 命令，可以查看 bba-group 下的配置。

【提示信息】 -

【常见错误】 -

【平台说明】 -

6.8 show pppoe-server

要查看 PPPOE SERVER 的状态信息，请执行特权用户模式命令 show pppoe-server 命令。

show pppoe-server { ref | session | tunnel } [session-id *sid* **]**

【参数说明】

参数	描述
ref	查看数据面所有的 Session 信息
session	显示 PPPOE Session 的信息
tunnel	显示 PPPOE tunnel 的信息
session-id	显示指定 session-id 的相关信息
sid	session-id 的值

【命令模式】 特权模式、全局模式、接口模式

【缺省级别】 14

【使用指导】 该命令的 session 和 tunnel 状态信息一样。

【配置举例】 例 1：下面是 show pppoe-server ref 的一个执行结果

```
Ruijie#show pppoe-server  ref
PPPOE Server ref current sessions count : 4
Sid: 2,In Intf:virtual-access 1,Out Intf:CAPWAP-Tunnel 1
```

```
LocalMAC:00-1A-A9-7C-B2-DD,RemoteMAC: C8-3A-35-C3-01-AC
             Input Info: 13 Normal, 0 Drop, 16 Reserve, 0 Lost
             Output Info: 0 Normal, 0 Drop, 0 Reserve, 0 Lost

Sid: 3,In Intf:virtual-access 2,Out Intf:CAPWAP-Tunnel 1
LocalMAC:00-1A-A9-7C-B2-DD,RemoteMAC: D8-5D-4C-7F-10-0A
             Input Info: 2 Normal, 0 Drop, 13 Reserve, 0 Lost
             Output Info: 0 Normal, 0 Drop, 0 Reserve, 0 Lost

Sid: 4,In Intf:virtual-access 0,Out Intf:CAPWAP-Tunnel 1
LocalMAC:00-1A-A9-7C-B2-DD,RemoteMAC: C8-3A-35-C0-B4-FC
             Input Info: 7 Normal, 0 Drop, 7 Reserve, 0 Lost
             Output Info: 0 Normal, 0 Drop, 0 Reserve, 0 Lost
```

各字段解释如下：

字段	描述
PPPOE Server ref current sessions count	数据面建立的 session 总数
Sid	Session id
In Intf	当前 session 对应的接收报文的虚拟接口
Out Intf	当前 session 传输报文的物理接口
LocalMAC	本地接口的 mac 地址
RemoteMAC	Session 远端接口 mac 地址
Input Info	入方向的报文统计
Normal	正常接收的报文个数
Drop	丢弃的接收到的异常报文个数
Reserve	接收的送控制面的报文个数
Lost	接收的丢失的报文个数
Output Info	出方向的报文统计
Normal	正常发送的报文个数
Drop	丢弃的发送异常报文个数
Reserve	送控制面的发送报文个数
Lost	丢失的发送报文个数

例 2：下面的示例是 show pppoe-server session 的一个执行结果

```
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
```

各字段解释如下：:

字段	描述
PPPOE Server current sessions count t	控制面建立的 session 总数
Sid	Session id
State	STATE_SENT_IDLE 空闲 STATE_SENT_PADI 发送 PADI STATE_RECEIVED_PADI 收到 PADI STATE_SEND_PADO 发送 PADO STATE_RECEIVED_PADO 收到 PADO STATE_SENT_PADR 发送 PADR STATE_RECEIVED_PADR 收到 PADR STATE_SEND_PADS 发送 PADS STATE_SESSION 进入 SESSION 阶段 STATE_TERMINATED SESSION 终结
intf	当前 session 对应的接口
External vid	封装的 vlan id
Inner vid	QINQ 场景下的内层 vlan id，目前不支持 QINQ 终结，所以总是为 0。
PeerIP	为 pppoe client 分配的 ip 地址
LocalMAC	本地接口的 mac 地址
RemoteMAC	Session 远端接口 mac 地址
online time	当前 session 的在线时长

【提示信息】 -

【平台说明】 -

7 PPP

7.1 ppp accm

配置 PPP 协商的 ACCM(异步字符转换掩码)选项
ppp accm *value*

恢复默认值
no ppp accm

【参数说明】

参数	描述
value	ACCM 选项的值，取值范围 0-0xffffffff。

【命令模式】 接口配置模式下

【缺省配置】 默认取值为 0x000A0000

【缺省级别】 14

【使用指导】 此命令用来配置 PPP 协商阶段 ACCM 选项的值，取值范围是 0-0xffffffff，默认值为 0x000A0000。

【配置举例】 1：配置 PPP 协商阶段 ACCM 选项的值。

```
Ruijie(config-if-Virtual-ppp 1)#ppp accm 0x0000000f
Ruijie(config-if-Virtual-ppp 1)#
```

【检验方法】 Show Running-config 可查看接口下配置的 ppp 协商的 accm 的值。

【提示信息】 -

【平台说明】 -

7.2 ppp accounting

配置 PPP 的记账方式
ppp accounting { default | *list_name* **}**

删除 PPP 的记账列表
no ppp accounting

【参数说明】

参数	描述
default	默认的记账列表
list_name	aaa 记账 list 名称

【命令模式】 接口配置模式下

【缺省级别】 14

【使用指导】 此命令用来配置 PPP 的记账方式，可以设置记账方式为默认的 default list，也可以指定记账的 list 的名称，此命令的配置必须使能 AAA 模块的功能开关才能配置，否则命令不可见。

【配置举例】 1：配置 PPP 的记账方式。

```
Ruijie#conf
Enter configuration commands, one per line.  End with CNTL/Z.
Ruijie(config)#aaa new-model
Ruijie(config)#int virtual-ppp 1
Ruijie(config-if-Virtual-ppp 1)#ppp accounting default
Ruijie(config-if-Virtual-ppp 1)#
```

【检验方法】 Show Running-config 可查看接口下配置的 ppp 的记账列表的名称。

【提示信息】 -

【平台说明】 -

7.3 ppp authentication

配置 PPP 认证方式。

ppp authentication { { **pap | chap** } [**callin** | { **chap | pap** } | **default** | *list_name*] }

删除 PPP 的认证方式

no ppp authentication { { **pap | chap** } [**callin** | { **chap** | **pap** } | **default** | *list_name*] }

【参数说明】

参数	描述
pap	配置认证方式为 PAP
callin	仅仅认证进来的请求报文
chap	配置认证方式为 CHAP
default	无论是 PAP 还是 CHAP 认证，使用默认的认证列表
list_name	配置认证时的认证列表名称

【命令模式】 接口配置模式下

【缺省级别】 14

【使用指导】 此命令用来配置 PPP 的认证方式，包括 PAP 认证，CHAP 认证。

【配置举例】 1：配置 PPP 的认证方式。

```
Ruijie(config-if-Virtual-ppp 1)#ppp authentication pap
Ruijie(config-if-Virtual-ppp 1)#ppp authentication chap
Ruijie(config-if-Virtual-ppp 1)#ppp authentication pap chap callin default
Ruijie(config-if-Virtual-ppp 1)#ppp authentication pap chap test_list
Ruijie(config-if-Virtual-ppp 1)#
```

【检验方法】 1：使用 **show running-config** 命令，查看接口下是否配置了 PPP 的认证方式。

【提示信息】 -

【常见错误】 -

【平台说明】 -

7.4 ppp authorization

配置 PPP aaa 认证的授权列表。
ppp authorization { **default** | *list_name* }

删除 PPP aaa 认证的授权列表。
no ppp authorization

【参数说明】

参数	描述
default	默认的 aaa 认证的授权列表。
list_name	PPP aaa 认证的授权列表。

【命令模式】 接口配置模式下

【缺省级别】 14

【使用指导】 配置 PPP AAA 认证的列表，用来在 PPP 的认证阶段使用 AAA 的授权列表来进行 AAA 的认证，该命令必须在开启 AAA 模块的前提下才可见。

【配置举例】 1：将 Virtual-PPP 1 口下的 PPP 认证的授权列表设置为 auth_list。

```
Ruijie(config)#
Ruijie(config)#aaa new-model
Ruijie(config)#int virtual-ppp 1
Ruijie(config-if-Virtual-ppp 1)#ppp authorization default
Ruijie(config-if-Virtual-ppp 1)#
```

【检验方法】 1：使用 **show running-config** 命令，查看接口下配置的 PPP 的授权列表。

【提示信息】 -

【常见错误】 -

【平台说明】 -

7.5 ppp chap

配置 PPP chap 认证的用户名和密码。
ppp chap hostname *name*
ppp chap password *password*

删除配置的 PPP 的用户名和密码。
no ppp chap hostname

【参数说明】

参数	描述
name	chap 认证的用户名
password	chap 认证的密码

【命令模式】 接口配置模式下

【缺省级别】 14

【使用指导】 VPDN 和 PPPOE 拨号等都需要用到 PPP 的协商，协商的第二阶段就是用户名密码的认证，本命令主要用来配置 CHAP 认证的用户名和密码。

【配置举例】 1：在 Virtual-PPP 1 口上配置 CHAP 认证的用户名和密码。

```
Ruijie(config-if-Virtual-ppp 1)#ppp chap hostname 111
Ruijie(config-if-Virtual-ppp 1)#ppp chap password 111
Ruijie(config-if-Virtual-ppp 1)#no ppp chap hostname
Ruijie(config-if-Virtual-ppp 1)#
```

【检验方法】 1：使用 **show running-config** 命令，查看接口下配置的 CHAP 认证的用户名和密码。

【提示信息】 -

【常见错误】 -

【平台说明】 -

7.6 ppp ipcp dns

配置 PPP 协商 IPCP 阶段的 DNS 选项的值。

ppp ipcp dns { *A.B.C.D* [*A.B.C.D*] [**accept**] **| accept** | **request** | **reject** }

删除配置的 DNS 选项的值。

no ppp ipcp dns { *A.B.C.D* [*A.B.C.D*] [**accept**] | **accept** | **request** | **reject** }

【参数说明】

参数	描述
accept	接收所有非 0 的 DNS 地址
request	从对端服务器请求 DNS 地址
reject	拒绝和对端协商 DNS 选项
A.B.C.D	DNS 地址

【缺省配置】 默认不配置 DNS 选项的值。

【命令模式】 接口配置模式下

【缺省级别】 14

【使用指导】 该命令用来配置 IPCP 协商阶段 DNS 选项的值。

【配置举例】 1：配置 IPCP 协商阶段的 DNS 选项的值。

```
Ruijie(config-if-Virtual-ppp 1)#ppp ipcp dns accept
Ruijie(config-if-Virtual-ppp 1)#ppp ipcp dns reject
Ruijie(config-if-Virtual-ppp 1)#ppp ipcp dns request
Ruijie(config-if-Virtual-ppp 1)#ppp ipcp dns 1.1.1.1 2.2.2.2
Ruijie(config-if-Virtual-ppp 1)#no ppp ipcp dns
Ruijie(config-if-Virtual-ppp 1)#
```

【检验方法】 1：使用 **show running-config** 命令，查看接口下的配置是否存在。

【提示信息】 -

【常见错误】 -

【平台说明】 -

7.7 ppp lcp mru negotiate

配置 PPP 协商的 MRU(最大接收单元)选项自动协商。
ppp lcp mru negotiate

取消配置 PPP 自动协商 MRU
no ppp lcp mru

【参数说明】

参数	描述
-	-

【命令模式】 接口模式

【缺省级别】 14

【使用指导】 MRU 选项是在 PPP 协商过程中的一个较为常见的选项，表示最大可接收单元，双方在协商的过程中会携带该选项，从而进行协商通过，确定整个链路中应该传输的报文的大小。

【配置举例】 1：配置 Virtual-ppp 1 口上 MRU 自动协商。

```
Ruijie(config-if-Virtual-ppp 1)#ppp lcp mru negotiate
Ruijie(config-if-Virtual-ppp 1)#
```

【检验方法】 1：使用 **show running-config** 命令，查看配置是否存在。

【提示信息】 -

【常见错误】 -

【平台说明】 -

7.8 ppp max-bad-auth

指定 PPP 认证的重试次数。
ppp max-bad-auth *number*

恢复 PPP 认证重试次数为默认值。

no ppp max-bad-auth

【参数说明】

参数	描述
number	PPP 认证重试次数，取值范围为 1-255。

【缺省配置】 默认值为 1。

【命令模式】 接口配置模式下

【缺省级别】 14

【使用指导】 重试次数包含第一次的认证，即如果配置重试次数为 3，第一次认证失败以后，还能重新认证 2 次。最后一次认证失败以后，线路被挂断（复位）。

【配置举例】 1：配置 virtual-ppp1 口的 PPP 认证的重试次数为 3。

```
Ruijie(config-if-Virtual-ppp 1)# ppp max-bad-auth 3
```

2：恢复 PPP 认证重试次数为默认值。

```
Ruijie(config-if-Virtual-ppp 1)# no ppp max-bad-auth
```

【检验方法】 1：使用 **show running-config interface virtual-ppp** *1* 命令，查看配置是否存在。

【提示信息】 -

【常见错误】 -

【平台说明】 -

7.9 ppp negotiation-timeout

指定 PPP 协商的最大超时时间。

ppp negotiation-timeout *seconds*

恢复 PPP 协商的最大超时时间为默认值。

no ppp negotiation-timeout

【参数说明】

参数	描述
seconds	PPP 协商的最大超时时间(秒)，取值范围为 10-65535。

【缺省配置】 默认超时时间为 20s。

【命令模式】 接口配置模式下

【缺省级别】 14

【使用指导】 PPP 整个协商的过程中，如果协商时间太长还没有协商完，那么超时协商的超时时间则认为是协商失败。默认的最大协商的超时时间为 20s。

【配置举例】 1：配置 virtual-ppp1 口的最大协商超时时间为 200s。

```
Ruijie (config)# interface virtual-ppp 1
Ruijie(config-if-Virtual-ppp 1)# ppp negotiation-timeout 200
```

2：恢复 PPP 认证重试次数为默认值。

```
Ruijie(config-if-Virtual-ppp 1)# no ppp negotiation-timeout
```

【检验方法】 1：使用 **show running-config interface virtual-ppp** *1* 命令，查看配置是否存在。

【提示信息】 -

【常见错误】 -

【平台说明】 -

7.10 ppp pap sent-username username password password

配置 PPP PAP 认证的用户名和密码。

ppp pap sent-username *username* **password** *password*

删除配置的 PPP PAP 的用户名和密码。

no ppp pap sent-username

【参数说明】

参数	描述
username	pap 认证的用户名
password	pap 认证的密码

【命令模式】 接口配置模式下

【缺省级别】 14

【使用指导】 VPDN 和 PPPOE 拨号等都需要用到 PPP 的协商，协商的第二阶段就是用户名密码的认证，本命令主要用来配置 PAP 认证的用户名和密码。

【配置举例】 1：在 Virtual-PPP 1 口上配置 PAP 认证的用户名和密码。

```
Ruijie(config-if-Virtual-ppp 1)#ppp pap sent-username 111 password 111
Ruijie(config-if-Virtual-ppp 1)#no ppp pap sent-username
Ruijie(config-if-Virtual-ppp 1)#
```

【检验方法】 1：使用 **show running-config** 命令，查看接口下配置的 PAP 认证的用户名和密码。

【提示信息】 -

【常见错误】 -

【平台说明】 -

8 Aggregate Port

8.1 aggregateport load-balance

配置 AP 的全局流量平衡算法或者配置指定 AP 口的流量平衡算法。

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** }

将 AP 的全局流量平衡设置恢复为缺省值或者将指定 AP 口的流量平衡算法生效为全局的流量平衡算法。

no aggregateport load-balance

【参数说明】

参数	描述
dst-mac	根据输入报文的目的 MAC 地址进行流量分配。在 AP 各链路中 ,目的 MAC 地址相同的报文被送到相同的端口 ,目的 MAC 不同的报文分配到不同的端口。
src-mac	根据输入报文的源 MAC 地址进行流量分配。在 AP 各链路中，不同 MAC 地址的报文分配到不同的端口，相同的 MAC 地址的报文使用相同的端口。
src-dst-ip	根据源 IP 与目的 IP 进行流量分配。不同的源 IP+目的 IP 的流量通过不同的端口转发，同一源 IP+目的 IP 通过相同的链路转发。在三层条件下，建议采用此流量平衡的方式。
dst-ip	根据输入报文的目的 IP 地址进行流量分配。在 AP 各链路中 ,目的 IP 地址相同的报文被送到相同的端口，目的 IP 不同的报文分配到不同的端口。
src-ip	根据输入报文的源 IP 地址进行流量分配。在 AP 各链路中 ,不同 IP 地址的报文分配到不同的端口，相同的 IP 地址的报文使用相同的端口。
src-dst-mac	根据源 MAC 与目的 MAC 进行流量分配。不同的源 MAC+目的 MAC 的流量通过不同的端口转发，同一源 MAC+目的 MAC 通过相同的链路转发。
src-dst-ip-l4port	根据源 IP 与目的 IP 和源 L4 端口号与目的 L4 端口号进行流量分配。
src- l4port	根据 L4 层源端口号进行流量分配。不同的 L4 层源端口号的报文在各成员链路间平衡分配 ,具有相同的 L4 层源端口号的报文则固定分配给相同的成员链路。
dst- l4port	根据 L4 层目的端口号进行流量分配。不同的 L4 层目的端口号的报文在各成员链路间平衡分配 ,具有相同的 L4 层目的端口号的报文则固定分配给相同的成员链路。
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。不同的 L4 层源端口号+L4 层目的端口号的报文在各成员链路间平衡分配 ,具有相同的 L4 层源端口号+L4 层目的端口号的报文则固定分配给相同的成员链路。

src-ip-src-l4port	根据源 IP 与 L4 层源端口号进行流量分配。不同的源 IP+L4 层源端口号的报文在各成员链路间平衡分配，具有相同的源 IP+L4 层源端口号的报文则固定分配给相同的成员链路。
src-ip-dst-l4port	根据源 IP 与 L4 层目的端口号进行流量分配。不同的源 IP+L4 层目的端口号的报文在各成员链路间平衡分配，具有相同的源 IP+L4 层目的端口号的报文则固定分配给相同的成员链路。
dst-ip-src-l4port	根据目的 IP 与 L4 层源端口号进行流量分配。不同的目的 IP+L4 层源端口号的报文在各成员链路间平衡分配，具有相同的目的 IP+L4 层源端口号的报文则固定分配给相同的成员链路。
dst-ip-dst-l4port	根据目的 IP 与 L4 层目的端口号进行流量分配。不同的目的 IP+L4 层目的端口号的报文在各成员链路间平衡分配，具有相同的目的 IP+L4 层目的端口号的报文则固定分配给相同的成员链路。
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。不同的源 IP+L4 层源端口号+L4 层目的端口号的报文在各成员链路间平衡分配，具有相同的源 IP+L4 层源端口号+L4 层目的端口号的报文则固定分配给相同的成员链路。
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。不同的目的 IP+L4 层源端口号+L4 层目的端口号的报文在各成员链路间平衡分配，具有相同的目的 IP+L4 层源端口号+L4 层目的端口号的报文则固定分配给相同的成员链路。
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。不同的源 IP+目的 IP+L4 层源端口号的报文在各成员链路间平衡分配，具有相同的源 IP+目的 IP+L4 层源端口号的报文则固定分配给相同的成员链路。
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。不同的源 IP+目的 IP+L4 层目的端口号的报文在各成员链路间平衡分配，具有相同的源 IP+目的 IP+L4 层目的端口号的报文则固定分配给相同的成员链路。

【缺省配置】

- 对于 AP 口创建缺省为二层 AP 口的设备，根据输入报文的源 MAC 地址和目的 MAC 地址进行流量分配；对于 AP 口创建缺省为三层 AP 口的设备，根据输入报文的源 IP 地址和目的 IP 地址进行流量分配
- 对于存在 CB 类型线卡且支持增强模式的设备，AP 口根据增强模式模板设置对应的报文类型字段进行流量分配

【命令模式】 全局模式或者接口配置模式

【缺省级别】 14

【使用指导】 在某些支持基于指定 AP 口配置流量平衡的产品上，进入指定 AP 口的接口模式下进行流量平衡算法配置，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。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。

【配置举例】 1：配置基于目的 MAC 地址的 AP 全局流量平衡算法：

```
Ruijie(config)# aggregateport load-balance dst-mac
```

2：在 AP 1 口上配置基于目的 MAC 地址的流量平衡算法：

```
Ruijie(config)# interface aggregateport 1
Ruijie(config-if-AggregatePort 1)# aggregateport load-balance dst-mac
```

【检验方法】 使用 **show aggregateport load-balance** 命令查看设置的流量平衡算法。

【提示信息】 -

【常见错误】 -

【平台说明】

src-dst-ip-l4port 和 src-dst-ip-src-dst-l4port 均表示基于报文的源和目的 IP+L4 层源和目的端口号的流量均衡方式，其中，src-dst-ip-l4port 命令适用于所有支持该流量均衡模式的产品，src-dst-ip-src-dst-l4port 命令仅适用于部分产品。

8.2 aggregateport member linktrap

配置 AP 成员口发送 LinkTrap 通告功能。
aggregateport member linktrap

关闭 AP 成员口的 LinkTrap 通告功能。
no aggregateport member linktrap

【参数说明】

参数	描述
-	-

【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。

【缺省级别】 14

【使用指导】 接口模式下，不能通过[**no**] **snmp trap link-status** 命令来设置 AP 成员口是否发送 LinkTrap 通告功能，而应该在全局配置模式下，使用[**no**] **aggregateport member linktrap** 命令来设置 AP 成员口是否发送 LinkTrap 通告功能。

【配置举例】 1：下面的例子用于打开 AP 成员口的 LinkTrap 通告功能：

```
Ruijie# configure terminal
```

```
Ruijie(config)# aggregateport member linktrap
```

【检验方法】 可以通过 **show running** 命令查看配置是否存在。

【提示信息】 -

【常见错误】 -

【平台说明】 -

8.3 interface aggregateport

配置以太网 AP 口或者进入以太网 AP 口的接口配置模式。
interface aggregateport *ap-number*

删除 AP 口。
no interface aggregateport *ap-number*

【参数说明】

参数	描述
ap-number	AP 接口号。

【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。

【缺省级别】 14

【使用指导】 当 AP 口已经创建，配置 **interface aggregateport** 命令时自动进入 AP 口的接口配置模式；当 AP 口未创建，配置 **interface aggregateport** 会先创建 AP 口，如果创建成功，则进入 AP 口的接口配置模式。

【配置举例】 1：下面的例子用于创建并进入 AP 5 的接口配置模式：

```
Ruijie# configure terminal
Ruijie(config)# interfaces aggregateport 5
Ruijie(config-if-Aggregateport 5)# end
```

【检验方法】 可以通过 **show running** 命令查看配置是否存在。

【提示信息】 -

【常见错误】 -

【平台说明】 -

8.4 port-group

将一个以太网物理端口设置为静态 AP 的成员端口。
port-group *port-group-number*

删除该端口的 Aggregate Port 成员属性。
no port-group

【参数说明】

参数	描述
port-group-number	静态 AP 成员端口组的编号，即静态 AP 接口号。

【缺省配置】 以太网物理口缺省不属于任何静态 AP。

【命令模式】 接口配置模式。

【缺省级别】 14

【使用指导】 通过 **port-group** 命令将接口加入一个 AP 口时，如果该 AP 不存在，自动创建该 AP 口。物理端口和 AP 口的层次不相同时，不允许该物理端口加入到 AP 口中。

【配置举例】 1：下面的例子是将以太网接口 1/3 配置成静态 AP 3 成员：

```
Ruijie(config)# interface gigabitethernet 1/3
Ruijie(config-if-GigabitEthernet 1/3)# port-group 3
```

【检验方法】 可以通过 **show interface aggregateport** 命令查看配置是否存在及生效。

【提示信息】 -

【常见错误】 -

【平台说明】 -

8.5 show aggregateport

显示 Aggregate Port 设置信息。
show aggregateport *aggregate-port-number* [**load-balance | summary**]

【参数说明】

参数	描述
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。

【缺省配置】 -

【命令模式】 各模式均可执行。

【缺省级别】 14

【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。

【配置举例】 1：查看交换机系列和无线 AC 系列产品上 AP 1 的配置信息：

```
Ruijie# show aggregateport 1 summary
AggregatePort  MaxPorts        SwitchPort Mode    Load balance                 Ports
-------------  --------------- ---------- ------  ---------------------------
-------------------------
Ag1            8               Enabled    ACCESS  dst-mac                      Gi0/2
```

如果系统不支持基于 AP 口配置流量均衡模式，则不显示 Load balance 字段。

【检验方法】 -

【提示信息】 -

【常见错误】 -

【平台说明】 -

9 VLAN-TERMINAL

9.1 show vid-info

显示 VID 的上线数及对应 VID 的上线 IP。

show vid-info

【参数说明】

参数	描述
-	-

【缺省配置】 无。

【命令模式】 特权模式

【缺省级别】 14

【使用指导】 通过此命令可以查看当前 VID 的上线数及对应 VID 的上线 IP

【配置举例】 1：查看当前 VID 的上线数及对应 VID 的上线 IP。

```
Ruijie# show vid-info
vid            count         ip
100            1           192.168.1.2
102            2           192.168.1.10,192.168.1.12
```

【提示信息】 -

【平台说明】 -

9.2 show vlan-terminal

显示 vlan-terminal 的配置信息。

show vlan-terminal

【参数说明】

参数	描述
-	-

【缺省配置】 无。

【命令模式】 特权模式

【缺省级别】 14

【使用指导】 通过此命令可以查看当前 vlan-terminal 的配置信息

【配置举例】 1：查看当前 vlan-terminal 配置信息。

```
Ruijie# show vlan-terminal
vlan-terminal: enable
per-vlan:   20
Gi0/1:      1, 2, 60-80
Gi0/2:      4, 100-20
```

【提示信息】 -

【平台说明】 -

9.3 vlan-teminal per-vlan

配置属于同一个 vlan 的最多上线数。

vlan-terminal per-vlan *num*

【参数说明】

参数	描述
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

【缺省配置】 缺省情况下，VID 的上线数为 100 个。

【命令模式】 全局配置模式

【缺省级别】 14

【使用指导】 通过本命令配置配置属于同一个 VID 的最多上线数，范围为 1~1000。

【配置举例】 1：配置 VID 的上线数为 30。

```
Ruijie#config
Enter configuration commands, one per line.  End with CNTL/Z.
Ruijie(config)# vlan-terminal per-vlan 30
```

2：VID 的上线数恢复为默认值。

```
Ruijie#config
```

```
Enter configuration commands, one per line.  End with CNTL/Z.
Ruijie#no vlan-terminal per-vlan
```

【检验方法】 1：使用 **show run 或 show vlan-terminal** 命令，可以查看配置的最多上线数。

【提示信息】 -

【平台说明】 -

9.4 vlan-terminal enable

开启 vlan 终结功能。
vlan-terminal enable

关闭 vlan 终结功能
no vlan-terminal enable

【参数说明】

参数	描述
-	-

【缺省配置】 缺省情况下，vlan 终结功能是关闭。

【命令模式】 全局配置模式

【缺省级别】 14

【使用指导】 通过配置本命令启动 vlan 终结功能。

【配置举例】 1：开启设备的 vlan 终结功能。

```
Ruijie#config
Ruijie(config)# vlan-terminal enable
```

2：关闭设备的 vlan 终结功能。

```
Ruijie#config
Ruijie(config)#no vlan-terminal enable
```

【检验方法】 1：使用 **show run** 命令，可以 vlan 终结功能是启用还是关闭。
2：使用 **show vlan-terminal** 命令，也可以查看配置的信息

【提示信息】 -

【常见错误】 -

【平台说明】 -

9.5 vlan-terminal vlan-list

配置接口所对应的 VID。

vlan-terminal vlan-list *vlan-list*

【参数说明】

参数	描述
vlan-list	可以是单个 VID，也可以是连续的 VID，中间有逗号隔开

【缺省配置】 无。

【命令模式】 接口配置模式

【缺省级别】 14

【使用指导】 通过本命令可以配置哪些 VID 从哪个接口进出。

【配置举例】 1：配置从接口 0/1 进出的 VID 为 2，5， 40~80， 100~120。

```
Ruijie#config
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
```

2：删除配置。

```
Ruijie#config
Enter configuration commands, one per line.  End with CNTL/Z.
Ruijie(config)# interface gigabitEthernet 0/1
Ruijie(config-if-GigabitEthernet 0/1)# no vlan-terminal vlan-list
```

【检验方法】 1：使用 **show run** 或 **show vlan-terminal** 命令，可以查看配置的最多上线数。

【提示信息】 1：接口属性错误（只支持 LAN 口）。

```
%Configuration fail: no lan interface.
```

2：格式错误。

```
%Configuration fail: format error.
```

3：VID 冲突。

```
%Configuration fail： the vid is conflict.
```

【平台说明】 -

命令参考-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/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/服务

1.1 ip address

配置接口的 IP 地址。

ip address *ip-address network-mask* [**secondary**] | [**slave**]

删除指定接口的 IP 地址。

no ip address [*ip-address network-mask* [**secondary**] | [**slave**]]

【参数说明】

参数	描述
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。缺省为配置主 ip 地址。
slave	表示配置的 slave IP 地址。

【缺省配置】 接口没有配置 IP 地址

【命令模式】 接口模式

【缺省级别】 2

【使用指导】 一个设备只有配置了 IP 地址，才可以接收和发送 IP 数据报，接口配置了 IP 地址，说明该接口允许运行 IP 协议。

网络掩码也是一个 32 位比特的数值，标识着该 IP 地址的哪几个比特为网络部分。网络掩码中，值为“1”的比特对应的 IP 地址比特位就是为网络部分，值为“0”的比特对应的 IP 地址比特位就是为主机地址部分。如 A 类网络对应的网络掩码为“255.0.0.0”。你可以利用网络掩码对一个网络进行子网划分，子网划分就是将一个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。

RGOS 软件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 IP。次 IP 地址的配置理论上没有数目限制，可以随意配置，但只有配置了主 IP 地址后才能配置次 IP 地址。次 IP 地址与主 IP 以及次 IP 之间地址必须属于不同网络。在网络建设中，会经常使用到次 IP 地址，通常在以下情况下应该考虑试用次 IP 地址：

一个网络没有足够多的主机地址。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，你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。

【配置举例】

1：配置了接口主 IP 地址为 10.10.10.1，网络掩码为 255.255.255.0。

```
Ruijie(config)# interface gigabitEthernet 0/1
Ruijie(config-if-GigabitEthernet 0/1)# ip address 10.10.10.1 255.255.255.0
```

2：配置接口的主地址为 10.10.10.1/24，slave 地址为 10.10.20.1/24

```
Ruijie(config)# interface gigabitEthernet 0/1
Ruijie(config-if-GigabitEthernet 0/1)# ip address 10.10.10.1 255.255.255.0
Ruijie(config-if-GigabitEthernet 0/1)# ip address 10.10.20.1 255.255.255.0 slave
```

【检验方法】

1：**show ip interface** 可见接口下的配置情况。

2：show running-config [**interface** *interface-type interface-number*] 可见接口下的 slave ip 配置情况。

【提示信息】

1. 不允许配置 mask 为全 1 或全 0 的掩码（环回接口可以支持 32 位掩码），如果配置了，则出现以下提示：

```
Invalid IP mask.
```

2. 未配置主 ip 地址的情况下不允许配置次 ip 地址，否则会出现以下提示：

```
Cannot add IP address.
```

3. 未配置主 ip 地址的情况下不允许配置 Slave ip 地址，否则会出现以下提示：

```
Please config the primary IP address first.
```

【常见错误】

1. 未配置主 ip 地址的情况下配置次 ip 地址。
2. 未配置主 ip 地址的情况下配置 slave ip 地址。
3. 删除主地址之前没有删除所有从地址。
4. 同一个接口上不同 IP 地址的网段重叠。

【平台说明】

-

1.2 ip address negotiate

配置通过 PPP 协商获取接口的 IP 地址。

ip address negotiate

删除通过 PPP 协商获取接口的 IP 地址。

no ip address negotiate

【参数说明】

参数	描述

-	

【缺省配置】 接口没有配置通过 PPP 协商获取 IP 地址

【命令模式】 接口模式

【缺省级别】 2

【使用指导】 只有路由器的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**。

【配置举例】 1：配置通过 PPP 协商获取接口 IP 地址。

```
Ruijie(config)# interface dialer 1
Ruijie(onfig-if-dialer 1)# ip address negotiate
```

【检验方法】 1：**show ip interface** 可见接口下的配置情况。

【提示信息】 -

【常见错误】 -

【平台说明】 -

1.3 ip address-pool local

使能 IP 地址池功能。
ip address-pool local

关闭 IP 地址池功能。
no ip address-pool local

【参数说明】

参数	描述
-	

【缺省配置】 缺省使能 IP 地址池功能

【命令模式】 全局配置模式

【缺省级别】 2

【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。

【配置举例】 1：使能 IP 地址池功能。

```
Ruijie(config)# ip address-pool local
```

【检验方法】 -

【提示信息】 -

【常见错误】 -

【平台说明】 -

1.4 ip broadcast-address

配置一个接口的广播地址。

ip broadcast-address *ip-address*

取消广播地址配置。

no ip broadcast-address

【参数说明】

参数	描述
ip-address	IP 网络的广播地址。

【缺省配置】 缺省 IP 广播地址为 255.255.255.255

【命令模式】 接口模式

【缺省级别】 2

【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。

【配置举例】 1：配置接口 IP 广播报文的目标地址为 0.0.0.0。

```
Ruijie(config)# interface gigabitEthernet 0/1
Ruijie(config-if-GigabitEthernet 0/1)# ip broadcast-address    0.0.0.0
```

【检验方法】 -

【提示信息】 没有配置主 ip 地址的情况下不能配置接口下的广播配置，否则出现以下提示：

Cannot set broadcast address. No primary address exist.

【常见错误】 -

【平台说明】 -

1.5 ip directed-broadcast

启用 IP 定向广播到物理广播的转换。
ip directed-broadcast [*access-list-number*]

取消定向广播到物理广播的转换。
no ip directed-broadcast

【参数说明】

参数	描述
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。 缺省没有定义列表号，所有的子网广播报文都会发生转换。

【缺省配置】 关闭

【命令模式】 接口模式

【缺省级别】 2

【使用指导】 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。
用户可以在指定的接口上，启动定向广播到物理广播转换的功能，这样该接口就可以转发到直连网络的定向广播了。该命令只影响已到最终目标子网的定向广播报文的最后传输，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列表来控制转发哪些定向广播。当定义了访问列表，只有符合访问列表中定义的数据包才进行定向广播到物理广播的转换。
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】 1：在设备 gigabitEthernet 0/1 端口启用了定向广播的转发。

```
Ruijie(config)# interface gigabitEthernet 0/1
Ruijie(config-if-GigabitEthernet 0/1)# ip directed-broadcast
```

【检验方法】 -

【提示信息】 -

【常见错误】 -

【平台说明】 -

1.6 ip icmp error-interval

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 DF *milliseconds* [*bucket-size*]

置其它 ICMP 差错报文的发送速率。
ip icmp error-interval *milliseconds* [*bucket-size*]

把 IP 首部不可分片位触发的 ICMP 目的不可达报文的发送速率恢复成缺省值。
no ip icmp error-interval DF *milliseconds* [*bucket-size*]

把其它 ICMP 差错报文的发送速率恢复成缺省值。
no ip icmp error-interval *milliseconds* [*bucket-size*]

【参数说明】

参数	描述
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。

【缺省配置】 100 毫秒发送 10 个。

【命令模式】 全局模式

【缺省级别】 14

【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。

【配置举例】 1：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。

```
Ruijie(config)# ip icmp error-interval DF 1000 100
```

2：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 1000 10
```

【检验方法】 使用 **show running-config** 查看配置。

【提示信息】 -

【常见错误】 -

【平台说明】 -

1.7 ip local pool

创建 IP 地址池。

ip local pool *pool-name low-ip-address* [*high-ip-address*]

删除 IP 地址池。

no ip local pool *pool-name* [*low-ip-address* [*high-ip-address*]]

【参数说明】

参数	描述
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-addres	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*

【缺省配置】 缺省未配置 IP 地址池

【命令模式】 全局配置模式

【缺省级别】 2

【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。

【配置举例】 1：创建一个本地 IP 地址池，名字为 quark，IP 地址范围 172.16.23.0 到 172.16.23.255。

```
Ruijie(config)#ip local pool quark 172.16.23.0 172.16.23.255
```

【检验方法】 使用 **show ip pool** 可查看创建的地址池。

【提示信息】 不允许在没有使能地址池功能的情况下创建 ip 地址池，若创建，则提示：

```
% IP local pool is disabled!
```

1. 如果 high-ip-address 小于 low-ip-address，或者是 high-ip-address 和 low-ip-address 不在同一个网段内，则提示：

```
% Invalid address range!
```

【常见错误】 配置的 *high-ip-address* 小于 *low-ip-address*。

2. 配置的 *high-ip-address* 和 *low-ip-address* 不在同一个网段中。

【平台说明】 -

1.8 ip mask-reply

启用 ICMP 掩码应答消息。

ip mask-reply

关闭 ICMP 掩码应答消息。

no ip mask-reply

【参数说明】

参数	描述
-	-

【缺省配置】 缺省开启发送 ICMP 掩码响应报文

【命令模式】 接口模式

【缺省级别】 2

【使用指导】 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。

【配置举例】 1：设备的 gigabitEthernet 0/1 接口将会响应 ICMP 的掩码请求报文。

```
Ruijie(config)# interface gigabitEthernet 0/1
Ruijie(config-if-GigabitEthernet 0/1)# ip mask-reply
```

【检验方法】 -

【提示信息】 -

【常见错误】 -

【平台说明】 -

1.9 ip mtu

配置 IP 包最大传输单元（MTU）。
ip mtu *bytes*

恢复缺省配置。
no ip mtu

【参数说明】

参数	描述
bytes	IP 包最大传输单元，以字节为单位，范围 68~1500。

【缺省配置】 缺省与接口命令 mtu 配置的值相同。

【命令模式】 接口模式

【缺省级别】 2

【使用指导】 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。
如果用接口配置命令 mtu 对接口的最大传输单元值进行设置，IP MTU 的会自动与接口的 MTU 值保持一致。反之，如果调整了 IP MTU 的值，接口的 MTU 值不会跟着变化。

【配置举例】 1：将 gigabitEthernet 0/1 接口的 IP MTU 值设为 512 字节。

```
Ruijie(config)# interface gigabitEthernet 0/1
Ruijie(config-if-GigabitEthernet 0/1)# ip mtu 512
```

【检验方法】 1：**show ip interface gi 0/1** 可见 IP interface MTU 是：512。

【提示信息】 -

【常见错误】 -

【平台说明】 -

1.10 ip redirects

启用 ICMP 重定向消息。
ip redirects

关闭 ICMP 重定向。
no ip redirects

【参数说明】

参数	描述
-	-

【缺省配置】 缺省启用。

【命令模式】 接口模式

【缺省级别】 2

【使用指导】 当路由不是最优时，有可能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。
RGOS 软件缺省启用 ICMP 重定向。

【配置举例】 1：gigabitEthernet 0/1 接口关闭了 ICMP 重定向。

```
Ruijie(config)# interface gigabitEthernet 0/1
Ruijie(config-if-GigabitEthernet 0/1)# no ip redirects
```

【检验方法】 -

【提示信息】 -

【常见错误】 -

【平台说明】 -

1.11 ip source-route

开启 IP 源路由信息的处理功能。
ip source-route

关闭 IP 源路由信息的处理功能。

no ip source-route

【参数说明】

参数	描述
-	-

【缺省配置】 缺省启用

【命令模式】 全局模式

【缺省级别】 2

【使用指导】 RGOS 支持 IP 源路由。当设备接收到 IP 数据包时，会对 IP 报头的严格源路由、宽松源路由、记录路由等选项进行检查，这些选项在 RFC 791 中有详细描述。如果检测到该数据包启用了其中一个选项，就会执行响应的动作；如果检测到无效的选项，就会给数据源发送一个 ICMP 参数问题消息，然后丢弃该数据包。
RGOS 软件缺省情况下支持 IP 源路由特性。

【配置举例】 1：关闭了 IP 源路由信息的处理功能。

```
Ruijie(config)# no ip source-route
```

【检验方法】 -

【提示信息】 -

【常见错误】 -

【平台说明】 -

1.12 ip ttl

配置本机发送的单播报文的 TTL 值。
ip ttl *value*

取消配置本机发送的单播报文的 TTL 值。
no ip ttl

【参数说明】

参数	描述
value	TTL 值，取值范围是 0~255。

【缺省配置】 缺省值是 64

【命令模式】 全局模式

【缺省级别】 2

【使用指导】

【配置举例】 1：配置本机发送的单播报文的缺省 TTL 值为 100。

```
Ruijie(config)# ip ttl 100
```

【检验方法】 -

【提示信息】 -

【常见错误】 -

【平台说明】 -

1.13 ip unnumbered

配置接口借用 IP 地址。

ip unnumbered *interface-type interface-number*

取消该配置。

no ip unnumbered

【参数说明】

参数	描述
interface-type	关联接口类型。
interface-number	关联接口编号。

【缺省配置】 缺省情况下，没有配置无编号接口。

【命令模式】 接口模式

【缺省级别】 2

【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：

1. 以太网接口不能配置成无编号接口。
3. 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。
4. 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。

5. 不能通过无编号接口进行网络启动。

【配置举例】 1：配置接口配置为无编号接口，关联接口为 gigabitEthernet 0/1。

```
Ruijie(config)# int virtual-ppp 1
Ruijie(config-if-Virtual-ppp 1)# ip unnumbered gigabitEthernet 0/1
```

【检验方法】 -

【提示信息】 -

【常见错误】 -

【平台说明】 -

1.14 ip unreachables

启用 ICMP 协议不可达消息。

ip unreachables

关闭发送 ICMP 协议不可达消息。

no ip unreachables

【参数说明】

参数	描述
-	-

【缺省配置】 缺省启用

【命令模式】 接口模式

【缺省级别】 2

【使用指导】 如果 RGOS 软件接收到一个目标地址为自身的单播报文，又不能处理该报文的上层协议，就会发送一个 ICMP 目标不可达消息。

如果 RGOS 软件由于没有路由，而不能转发一个数据包，就会向数据源发送 ICMP 主机不可达消息。

该命令影响所有 ICMP 目标不可达消息。

【配置举例】 1：关闭 gigabitEthernet 0/1 接口发送 ICMP 目标不可达消息。

```
Ruijie(config)# interface gigabitEthernet 0/1
Ruijie(config-if-GigabitEthernet 0/1)# no ip unreachables
```

【检验方法】 -

【提示信息】 -

【常见错误】 -

【平台说明】 -

1.15 peer default ip address

为 PPP 协商分配 IP 地址给对端。
peer default ip address {*ip-address* | **pool** [*pool-name*] }

取消分配 IP 地址给对端。
no peer default ip address

【参数说明】

参数	描述
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。

【缺省配置】 缺省情况下，接口不为对端分配 IP 地址。

【命令模式】 接口模式

【缺省级别】 2

【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】 1：配置接口 dialer 为对端分配的 IP 地址为 10.0.0.1。

```
Ruijie(config)# interface dialer 1
Ruijie(config-if-dialer 1)# peer default ip address 10.0.0.1
```

【检验方法】 -

【提示信息】 -

【常见错误】 -

【平台说明】 -

1.16 show ip interface

显示接口的 IP 状态信息。

show ip interface [*interface-type interface-number* | **brief**]

【参数说明】

参数	描述
Interface-type	指定接口类型
Interface-number	指定接口编号
brief	显示三层接口的 IP 基本配置信息 (包括接口 primary ip、secondary ip 和接口状态)

【命令模式】 特权模式

【缺省级别】 1

【使用指导】 一个接口处于可用的状态，RGOS 将会在路由表中创建一条直连路由。可用的接口是指 RGOS 软件通过该接口可以收发数据包。如果接口从可用状态变为不可用状态，RGOS 软件将会从路由表中删除相应的直连路由。
如果接口处于可用状态，即允许双向通信状态，线路协议状态会显示“UP”；如果仅物理线路处于可用状态，接口状态会显示“UP”。
不同的接口类型，显示的结果可能不一样，因为有些内容是某些接口特有的选项。

【配置举例】 1：显示所有接口的 IP 状态信息。

```
Ruijie#show ip interface brief
Interface            IP-Address(Pri)  IP-Address(Sec) Status Protocol
GigabitEthernet 0/10  2.2.2.2/24      3.3.3.3/24      down     down
GigabitEthernet 0/11  no address      no address      down     down
VLAN 1                  1.1.1.1/24      no address      down     down
```

Status 描述接口的链路状态，取值有 up，down 和 administratively down (用户执行 shutdown 命令把接口强制关闭)。

Protocol 描述接口的 IPv4 协议状态。

2：显示 VLAN 1 接口的 IP 状态信息。

```
Ruijie#show ip interface vlan 1
```

```
VLAN 1
  IP interface state is: DOWN
  IP interface type is: BROADCAST
  IP interface MTU is: 1500
  IP address is:
    1.1.1.1/24 (primary)
  IP address negotiate is: OFF
  Forward direct-broadcast is: OFF
  ICMP mask reply is: ON
  Send ICMP redirect is: ON
  Send ICMP unreachabled is: ON
  Proxy ARP is: OFF
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
```

字段解释：

字段	说明
IP interface state is:	网络接口处于可用状态，其接口硬件状态和线路协议状态均为“UP”。
IP interface type is:	显示接口类型，如广播，点对点等。
IP interface MTU is:	显示接口设置的 MTU 值。
IP address is:	显示接口 IP 地址和掩码信息。
IP address negotiate is:	显示接口 IP 地址是否由协商获得。
Forward direct-boardcast is:	显示是否转发定向广播。
ICMP mask reply is:	显示是否发送 ICMP 掩码应答报文。
Send ICMP redirect is:	显示是否发送 ICMP 重定向报文。
Send ICMP unreachabled is:	显示是否发送 ICMP 不可达报文。
Proxy ARP is:	显示是否启用代理 ARP 。

ARP packet input number: 0 Request packet: 0 Reply packet: 0 Unknown packet: 0	显示接口上收到的 ARP 报文总数，包括： ARP 请求报文 ARP 应答报文 未知类型报文
TTL invalid packet number:	显示接口上收到的 TTL 无效报文个数
ICMP packet input number: 0 Echo request: 0 Echo reply: 0 Unreachable: 0 Source quench: 0 Routing redirect: 0	显示接口上收到的 ICMP 报文总数，包括如下报文： Echo 请求报文 Echo 应答报文 不可达报文 源站抑制报文 路由重定向报文

【提示信息】 -

【平台说明】 -

1.17 show ip packet queue

显示协议栈 IP 报文收发统计信息

show ip packet queue

【参数说明】

参数	描述
-	-

【命令模式】 特权模式

【缺省级别】 2

【使用指导】 -

【配置举例】

```
Ruijie#show ip packet queue
Receive 31925 packets(fragment=0):
  IP packet receive queue: length 0, max 1542, overflow 0.
  Receive 13 ICMP echo packets, 25 ICMP reply packets .
  Discards:
    Failed to alloc skb: 0.
    Receive queue overflow: 0.
    Unknow protocol drops: 0.
    ICMP rcv drops: 0. for skb check fail.
```

```
    ICMP rcv drops: 0. for skb is broadcast.
Sent packets:
  Success: 15644
  Generate 13 and send 8 ICMP reply packets, send 26 ICMP echo packets.
  It records 187 us as max time in ICMP reply process.
  Failed to alloc efbuf: 0
  Dropped by EFMP: 0
  NoRoutes: 887
  Get vrf fails: 0
  Cannot assigned address drops: 0
  Failed to encapsulate ethernet head: 0
ICMP error queue: length 0, max 1542, overflow 0.
```

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。

字段解释：

字段	说明
IP packet receive queue	协议栈 IP 接收队列参数
Discards	接收过程丢弃的报文
Sent packets	发送的 IP 报文的统计信息
ICMP error queue	ICMP 错误报文接收队列参数

【提示信息】 -

【平台说明】 -

1.18 show ip packet statistics

查看 IP 报文的统计信息。

show ip packet statistics [**total** | *interface-name*]

【参数说明】

参数	描述
total	所有接口上统计值的总和。
interface-name	接口名称

【命令模式】 特权模式

【缺省级别】 1

【使用指导】 -

【配置举例】 1：以下是该命令的信息呈现：

```
R1#show ip packet statistics
Total
  Received 113962 packets, 11948991 bytes
    Unicast:90962,Multicast:5232,Broadcast:17768
    Discards:0
      HdrErrors:0(BadChecksum:0,TTLExceeded:0,Others:0)
      NoRoutes:0
      Others:0
  Sent 34917 packets, 1863146 bytes
    Unicast:30678,Multicast:4239,Broadcast:0
GigabitEthernet 0/1
  Received 6715 packets, 416587 bytes
    Unicast:2482,Multicast:4233,Broadcast:0
    Discards:0
      HdrErrors:0(BadChecksum:0,TTLExceeded:0,Others:0)
      NoRoutes:0
      Others:0
  Sent 6720 packets, 417096 bytes
    Unicast:2481,Multicast:4239,Broadcast:0
Loopback 0
  Received 0 packets, 0 bytes
    Unicast:0,Multicast:0,Broadcast:0
    Discards:0
      HdrErrors:0(BadChecksum:0,TTLExceeded:0,Others:0)
      NoRoutes:0
      Others:0
  Sent 0 packets, 0 bytes
    Unicast:0,Multicast:0,Broadcast:0
Tunnel 1
  Received 0 packets, 0 bytes
    Unicast:0,Multicast:0,Broadcast:0
    Discards:0
      HdrErrors:0(BadChecksum:0,TTLExceeded:0,Others:0)
      NoRoutes:0
      Others:0
  Sent 21584 packets, 1122848 bytes
    Unicast:21584,Multicast:0,Broadcast:0
```

字段解释：

字段	说明

Total	表示接下来显示的是所有接口的统计值的总和
GigabitEthernet 0/1	表示接下来显示的是针对这一具体接口的统计值信息
Received	接收到的报文数目，字节数目。以及单播/组播/广播统计，包括丢包数目，以及对应的丢包原因
Sent	发送的报文数目，字节数目，单播/组播/广播数目

【提示信息】 -

【平台说明】 -

1.19 show ip pool

查看系统的 IP 地址池信息。

show ip pool [*pool-name*]

【参数说明】

参数	描述
pool-name	指定的地址池名字

【命令模式】 特权模式

【缺省级别】 2

【使用指导】 -

【配置举例】 1：查看所有创建的地址池的信息。

```
Ruijie# show ip pool
Ruijie(config)#show ip pool
Pool                Begin           End                Free    In use
default             1.1.1.1         1.1.1.1               1         0
pool1               2.2.2.2         2.2.2.254           253         0
pool2               3.1.1.1         3.2.1.1           65537         0
pool3               192.168.1.1     192.168.1.254       254         0
```

字段解释：

字段	说明
Pool	地址池的名字
Begin	地址池的起始 ip 地址
Free	当前地址池中空闲的 ip 地址。
In use	当前地址池中正在使用的 ip 地址

【提示信息】 如果没有创建任何地址池，则显示：

```
No IP local pools exist
```

【平台说明】 -

1.20 show ip raw-socket

显示所有 IPv4 原始套接字。

show ip raw-socket [*num*]

【参数说明】

参数	描述
num	协议号

【命令模式】 特权模式

【缺省级别】 2

【使用指导】 -

【配置举例】 1：查看所有 IPv4 原始套接字。

```
Ruijie# show ip raw-socket
Number Protocol Process name
1      ICMP     dhcp.elf
2      ICMP     vrrp.elf
3      IGMP     igmp.elf
4      VRRP     vrrp.elf
Total: 4
```

字段解释：

字段	说明
Number	序号
Protocol	协议号
Process name	进程名称
Total	总数

【提示信息】 -

【平台说明】 -

1.21 show ip sockets

显示所有 IPv4 套接字，可以知道哪些 UDP 端口和 TCP 端口对外提供服务。

show ip sockets

【参数说明】

参数	描述
-	-

【命令模式】 特权模式

【缺省级别】 2

【使用指导】 -

【配置举例】 1：查看所有 IPv4 套接字。

```
Ruijie# show ip sockets
Number Process name     Type     Protocol LocalIP:Port  ForeignIP:Port          State
1      dhcp.elf         RAW      ICMP     0.0.0.0:1     0.0.0.0:0               *
2      vrrp.elf         RAW      ICMP     0.0.0.0:1     0.0.0.0:0               *
3      igmp.elf         RAW      IGMP     0.0.0.0:2     0.0.0.0:0               *
4      vrrp.elf         RAW      VRRP     0.0.0.0:112   0.0.0.0:0               *
5      dhcpc.elf        DGRAM    UDP      0.0.0.0:68    0.0.0.0:0               *
6      rg-snmpd         DGRAM    UDP      0.0.0.0:161   0.0.0.0:0               *
7      wbav2            DGRAM    UDP      0.0.0.0:2000  0.0.0.0:0               *
8      vrrp_plus.elf    DGRAM    UDP      0.0.0.0:3333  0.0.0.0:0               *
9      mpls.elf         DGRAM    UDP      0.0.0.0:3503  0.0.0.0:0               *
10     rds_other_th     DGRAM    UDP      0.0.0.0:3799  0.0.0.0:0               *
11     rg-snmpd         DGRAM    UDP      0.0.0.0:14800 0.0.0.0:0               *
12     rg-sshd          STREAM   TCP      0.0.0.0:22    0.0.0.0:0               LISTEN
13     rg-telnetd       STREAM   TCP      0.0.0.0:23    0.0.0.0:0               LISTEN
14     wbard            STREAM   TCP      0.0.0.0:4389  0.0.0.0:0               LISTEN
15     wbard            STREAM   TCP      0.0.0.0:7165  0.0.0.0:0               LISTEN
Total: 15
```

字段解释：

字段	说明
Number	序号
Process name	进程名称

Protocol	协议号
LocalIP:Port	本地 IP 地址和端口
ForeignIP:Port	对端 IP 地址和端口
State	状态，只对 TCP 套接字有意义。
Total	套接字总数

【提示信息】 -

【平台说明】 -

1.22 show ip udp

显示所有 IPv4 UDP 套接字，可以知道哪些 UDP 端口对外提供服务。

show ip udp [**local-port** *num*]

显示 IPv4 UDP 套接字的统计值。

show ip udp statistics

【参数说明】

参数	描述
local-port *num*	本地端口号

【命令模式】 特权模式

【缺省级别】 2

【使用指导】 -

【配置举例】 1：查看所有 IPv4 UDP 套接字。

```
Ruijie# show ip udp
Number Local Address         Peer Address         Process name
1      0.0.0.0:68            0.0.0.0:0            dhcpc.elf
2      0.0.0.0:161           0.0.0.0:0            rg-snmpd
3      0.0.0.0:2000          0.0.0.0:0            wbav2
4      0.0.0.0:3333          0.0.0.0:0            vrrp_plus.elf
5      0.0.0.0:3503          0.0.0.0:0            mpls.elf
6      0.0.0.0:3799          0.0.0.0:0            rds_other_th
7      0.0.0.0:14800         0.0.0.0:0            rg-snmpd
```

字段解释：

字段	说明
Number	序号
Local Address	本地 IP 地址和端口
Peer Address	对端 IP 地址和端口
Process name	进程名称

【提示信息】 -

【平台说明】 -

2 ARP

2.1 arp

配置静态 ARP。

arp *ip-address mac-address type* [**description** *string*]

取消静态 ARP。

no arp *ip-address*

【参数说明】

参数	描述
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**。
string	静态 arp 描述，不超过 32 个字符长度。

【缺省配置】 ARP 缓冲表中没有任何静态映射记录。

【命令模式】 全局模式

【缺省级别】 2

【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】 1：为以太网上的主机配置 ARP 静态映射记录。

```
Ruijie(config)# arp 1.1.1.1 4e54.3800.0002 arpa
```

2：为以太网上的主机配置 ARP 静态的描述为 ABC。

```
Ruijie(config)# arp 1.1.1.1 4e54.3800.0002 arpa description ABC
```

【检验方法】 1：**show arp** 命令可见相应的表项静态表项生成。

【提示信息】 1：ARP 表项不存在或者是保留表项，导致静态 ARP 删除失败。

```
Cannot remove ARP. ARP entry does not exist or reserved.
```

2：静态 ARP 表项添加失败，一般是 ARP 缓存表满引起，也可能是对应的 IP 地址是本机地址。

Cannot add static ARP.

【常见错误】 -

【平台说明】 -

2.2 arp any-ip

开启 any IP ARP 功能。

arp any-ip

关闭 any IP ARP 功能。

no arp any-ip

【参数说明】

参数	描述
-	-

【缺省配置】 默认情况下该功能关闭。

【命令模式】 接口模式

【缺省级别】 2

【使用指导】 如下两种情况用户必须修改配置才能上网：

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。

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：

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 表项和直连路由删除，应答报文无法到达用户端。

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。

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】 1：开启 any IP ARP 功能。

```
Ruijie(config)# interface gi 0/0
Ruijie(config-if-GigabitEthernet 0/0)# arp any-ip
```

2：关闭 any IPARP 功能。

```
Ruijie(config)# interface gi 0/0
Ruijie(config-if-GigabitEthernet 0/0)# no arp any-ip
```

【检验方法】 -

【提示信息】 -

【常见错误】 -

【平台说明】 -

2.3 arp cache interface-limit

配置限制接口 ARP 学习数量。
arp cache interface-limit *limit*

恢复缺省配置。
no arp cache interface-limit

【参数说明】

参数	描述
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。

【缺省配置】 默认情况下不限制接口 ARP 学习数量。

【命令模式】 接口配置模式

【缺省级别】 2

【使用指导】 限制接口的 ARP 学习数量，可防止恶意的 ARP 攻击，让设备生成大量的 ARP 表项，占用过多的表项资源。配置的值必须不小于当前接口已经学习到的 ARP 表项数量，否则配置不生效。该限制受限于设备支持的 ARP 容量。

【配置举例】 1：配置将接口 ARP 学习数量限制为 300。

```
Ruijie(config)# interface gi 0/0
Ruijie(config-if-GigabitEthernet 0/0)# arp cache interface-limit 300
```

2：关闭限制接口 ARP 学习数量

```
Ruijie(config)# interface gi 0/0
Ruijie(config-if-GigabitEthernet 0/0)# no arp cache interface-limit
```

【检验方法】 show running-config 查看相关配置是否生效。

【提示信息】 -

【常见错误】 -

【平台说明】 -

2.4 arp gratuitous-send interval

配置定时发送免费 ARP 请求。

arp gratuitous-send interval *seconds* [*number*]

关闭定时发送免费 ARP 请求。

no arp gratuitous-send

【参数说明】

参数	描述
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>。

【缺省配置】 接口没有启用定时发送免费 ARP 请求的功能。

【命令模式】 接口模式

【缺省级别】 2

【使用指导】 当设备的网络接口做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】 1：配置向接口 VLAN 1 每秒钟发送一次免费 ARP 请求。

```
Ruijie(config)# interface vlan 1
Ruijie(config-if)# arp gratuitous-send interval 1 1
```

2：取消定时向接口 VLAN 1 发送免费 ARP 请求。

```
Ruijie(config)# interface vlan 1
Ruijie(config-if)# no arp gratuitous-send
```

【检验方法】 -

【提示信息】 -

【常见错误】 -

【平台说明】 -

2.5 arp oob

配置管理口的静态 ARP。

arp oob ip-address mac-address type

取消管理口的静态 ARP。

no arp oob ip-address

【参数说明】

参数	描述
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**。

【缺省配置】 ARP 缓冲表中没有任何管理口的静态映射记录。

【命令模式】 全局模式

【缺省级别】 2

【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 oob** 命令可以删除管理口动态学习到的 ARP 映射。

⚠ 不指定 mgmt-name 的情况默认绑定到设备的第一个管理口；如果配置指定了第一个 mgmt 口，show run 查看配置不显示 mgmt-name 参数。

【配置举例】 1：为以太网上的主机配置 ARP 静态映射记录。

```
Ruijie(config)# arp oob 1.1.1.1 4e54.3800.0002 arpa
```

【检验方法】 1：**show arp oob** 命令可见相应的静态表项生成。

【提示信息】 1：静态 ARP 表项添加失败，一般是 ARP 缓存表满引起，也可能是对应的 IP 地址是本机地址。

```
Cannot add static ARP.
```

【常见错误】 -

【平台说明】 NBR6205-E、NBR6135-E、NBR6210-E、NBR6215-E 支持 MGMT 口；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 MGMT 口。

2.6 arp retry interval

配置重传 ARP 请求的时间间隔。
arp retry interval *seconds*

恢复缺省配置。
no arp retry interval

【参数说明】

参数	描述
seconds	ARP 请求的重传时间可以设置为 1~3600 秒，默认值为 1 秒。

【缺省配置】 ARP 请求重传时间间隔为 1 秒。

【命令模式】 全局模式

【缺省级别】 2

【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。

【配置举例】 1：将 ARP 请求的重传时间设置为 30s。
Ruijie(config)# arp retry interval 30

【检验方法】 -

【提示信息】 -

【常见错误】 -

【平台说明】 -

2.7 arp retry times

配置重传 arp 请求报文的次数。
arp retry times *number*

恢复缺省配置。

no arp retry times

【参数说明】

参数	描述
number	同一个 ARP 请求的发送次数 ,范围<1-100>。当设置为 1 时 ,表示不重传 ARP 请求，只是发送 1 次 ARP 请求报文。

【缺省配置】 如果没有收到 ARP 应答报文，ARP 请求报文会发送 5 次，然后超时。

【命令模式】 全局模式。

【缺省级别】 2

【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 请求的重传次数设置小一点，一般不要将重传次数设置得太大。**

【配置举例】 1：配置本地 ARP 请求不重传。

```
Ruijie(config)# arp retry times 1
```

2：配置本地 ARP 请求重传 1 次。

```
Ruijie(config)# arp retry times 2
```

【检验方法】 -

【提示信息】 -

【常见错误】 -

【平台说明】 -

2.8 arp scan

启用 ARP 扫描功能。

arp scan [*start-ip-address end-ip-address*]

【参数说明】

参数	描述
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。

【缺省配置】 默认情况下该功能关闭。

【命令模式】 接口配置模式。

【缺省级别】 2

【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】 1：配置 ARP 扫描功能，不指定 IP 地址范围

```
Ruijie(config)# interface gi 0/0
Ruijie(config-if-GigabitEthernet 0/0)# arp scan
```

2：配置 ARP 扫描功能，指定 IP 地址范围

```
Ruijie(config)# interface gi 0/0
Ruijie(config-if-GigabitEthernet 0/0)# arp scan 1.1.1.1 1.1.1.10
```

【检验方法】 -

【提示信息】 start-ip-address 或者是 end-ip-address 不是有效主机地址，或者 start-ip-address 大于 end-ip-address，或者 start-ip-address 和 end-ip-address 和接口的 ip 地址不在同一个网段上，则提示：
%notice: Invalid ip address range.
指定范围内主机数如果大于 1024，则打印：
%notice: Failed to scan because ip address range is larger than 1024.
如果接口没有三层 up，则提示：
%notice: Failed to scan because this interface is not up.

【常见错误】 start-ip-address 大于 end-ip-address。
start-ip-address 和 end-ip-address 和接口的 ip 地址不在同一个网段上。

【平台说明】 -

2.9 arp timeout

配置 ARP 缓冲区中动态 ARP 表项的超时时间。
arp timeout *seconds*

恢复缺省配置。

no arp timeout

【参数说明】

参数	描述
seconds	超时时间，以秒为计算单位，范围 0-2147483。

【缺省配置】 缺省超时时间为 3600 秒。

【命令模式】 接口模式/全局模式

【缺省级别】 2

【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 缓冲中保存的映射表就越真实，但是 ARP 消耗网络带宽也越多，所以需要权衡利弊。除非有特别的需要，否则一般不需要配置 ARP 超时时间。

锐捷网络设备 arp 老化时间配置支持在全局和接口下共存，且接口的配置优先级大于全局配置。比如设备上全局配置 arp 老化时间为 3000s，接口 1 配置了 arp 老化时间为 1800s，则接口 1 的老化时间还是为 1800s，而其他接口（包括新建的接口）其老化时间则由全局 arp 老化时间决定，即为 3000s。

【配置举例】 1：将从 Gigabit 以太网口 gigabitEthernet 0/1 学到的动态 ARP 映射记录的超时时间设为 120 秒。

```
Ruijie(config)# interface gigabitEthernet 0/1
Ruijie(config-if-GigabitEthernet 0/1)# arp timeout 120
```

1：配置全局 arp 老化时间为 3000 秒，若接口没有配置老化时间，则所有三层接口的老化时间为 3000 秒。

```
Ruijie(config)# arp timeout 120
```

【检验方法】 1：**show arp timeout** 可见接口 1 的超时时间为 120 秒。

【提示信息】 -

【常见错误】 -

【平台说明】 -

2.10 arp trusted

配置可信任 ARP 表项的最大个数。

arp trusted *number*

恢复默认值。

no arp trusted

【参数说明】

参数	描述

number	设置可信任 ARP 表项的最大个数，取值范围最小为 10 ,最大为对应产品 arp 容量减去 1024。

【缺省配置】 缺省可信 arp 的最大表项数为 arp 总容量的一半。

【命令模式】 全局模式

【缺省级别】 2

【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】 1：配置最多可以设置 1000 个可信任 ARP。

```
Ruijie(config)# arp trusted 1000
```

【检验方法】 -

【提示信息】 -

【常见错误】 -

【平台说明】 -

2.11 arp trusted aging

配置可信任 ARP 开始老化。
arp trusted aging

恢复默认值。
no arp trusted aging

【参数说明】

参数	描述
-	-

【缺省配置】 GSN 可信任 ARP 默认不老化。

【命令模式】 全局模式

【缺省级别】 2

【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。

【配置举例】 1：配置可信任 arp 开始老化。

```
Ruijie(config)# arp trusted aging
```

【检验方法】 -

【提示信息】 -

【常见错误】 -

【平台说明】 -

2.12 arp trust-monitor enable

开启 ARP 可信检测功能。

arp trust-monitor enable

关闭 AR 可信检测功能。

no arp trust-monitor enable

【参数说明】

参数	描述
-	-

【缺省配置】 该功能关闭

【命令模式】 接口模式

【缺省级别】 2

【使用指导】 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：
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。
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。
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需要 NUD 过程。

【配置举例】 1：开启 ARP 可信检测功能。

```
Ruijie(config)# interface gi 0/0
Ruijie(config-if-GigabitEthernet 0/0)# arp trust-monitor enable
```

2：关闭 ARP 可信检测功能。

```
Ruijie(config)# interface gi 0/0
Ruijie(config-if-GigabitEthernet 0/0)# no arp trust-monitor enable
```

【检验方法】 -

【提示信息】 -

【常见错误】 -

【平台说明】 -

2.13 arp unresolve

配置 ARP 表项中未解析表项的最大个数。

arp unresolve *number*

恢复默认值。

no arp unresolve

【参数说明】

参数	描述
number	未解析 ARP 表项的最大个数，取值范围最小为 1，最大为 ARP 表项的总容量。默认值为 ARP 表项的总容量。

【缺省配置】 ARP 缓冲表中最多可以容纳的未解析表项为 ARP 表项的总容量。

【命令模式】 全局模式

【缺省级别】 2

【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。

【配置举例】 1：配置本机的未解析表项的最大个数为 500。

```
Ruijie(config)# arp unresolve 500
```

【检验方法】 -

【提示信息】 -

【常见错误】 -

【平台说明】 -

2.14 arp-learning

开启 ARP 学习功能。
arp-learning enable

关闭 ARP 学习功能。
no arp-learning enable

【参数说明】

参数	描述
-	-

【缺省配置】 默认情况下接口使能动态 ARP 学习功能。。

【命令模式】 接口配置模式

【缺省级别】 2

【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】 1：开启动态 ARP 学习功能。

```
Ruijie(config)# interface gi 0/0
Ruijie(config-if-GigabitEthernet 0/0)# arp-learning enable
```

2：关闭动态 ARP 学习功能

```
Ruijie(config)# interface gi 0/0
Ruijie(config-if-GigabitEthernet 0/0)# no arp-learning enable
```

【检验方法】 -

【提示信息】 -

【常见错误】 -

【平台说明】 -

2.15 clear arp-cache

删除 ARP 缓冲表中动态 ARP 映射记录。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 [**trusted**] [*ip* [*mask*]] | **interface** *interface-name*]

【参数说明】

参数	描述
trusted	删除可信任 ARP 的表项。缺省为删除动态 arp 表项。
ip	IP 地址参数，即清除指定 IP 地址的 ARP 表项，如果指定 **trusted** 关键字则清除可信任 ARP 表项，否则为动态 ARP 表项。缺省删除所有动态 arp 表项。
mask	mask 为子网掩码参数，即清除子网内的 ARP 表项，前面的 IP 地址必须是子网号; 如果指定 trusted 关键字则删除子网的可信任 ARP 表项。否则删除子网内的动态 ARP 表项。缺省删除前面 ip 指定的动态 arp 表项。
interface *interface-name*	清除指定接口的动态 ARP 表项。缺省删除所有接口的动态 arp 表项。

【命令模式】 特权模式

【缺省级别】 2

【使用指导】 在支持 NFPP（Network Foundation Protection Policy，基础网络保护）设备上，默认每秒每个 mac 地址(或者 IP)只收一个 ARP 报文，如果两次 **clear arp** 时间间隔在 1s 内，可能会导致第二个应答报文被过滤而短时间 ARP 解析不了的情况。

【配置举例】 1：删除所有 ARP 动态映射记录缓冲表：

```
Ruijie# clear arp-cache
```

2：删除动态 ARP 表项 1.1.1.1：

```
Ruijie# clear arp-cache 1.1.1.1
```

3：删除接口 SVI1 下的动态 ARP 表项：

```
Ruijie# clear arp-cache interface Vlan 1
```

【提示信息】 -

【常见错误】 -

【平台说明】 -

2.16 clear arp-cache oob

删除管理口上的动态 ARP 映射记录。

clear arp-cache oob [*ip* [*mask*]]

【参数说明】

参数	描述
ip	IP 地址参数，即清除指定 IP 地址的 ARP 表项。缺省删除所有动态 arp 表项。
mask	mask 为子网掩码参数，即清除子网内的 ARP 表项。缺省删除前面 ip 指定的动态 arp 表项。

【命令模式】 特权模式

【缺省级别】 2

【使用指导】 在支持 NFPP（Network Foundation Protection Policy，基础网络保护）设备上，默认每秒每个 mac 地址(或者 IP)只收一个 ARP 报文，如果两次 **clear arp oob** 时间间隔在 1s 内，可能会导致第二个应答报文被过滤而短时间 ARP 解析不了的情况。

【配置举例】 1：删除所有 ARP 动态映射记录缓冲表：

```
Ruijie# clear arp-cache oob
```

2：删除动态 ARP 表项 1.1.1.1：

```
Ruijie# clear arp-cache oob 1.1.1.1
```

3：删除指定子网内的动态 ARP 表项：

```
Ruijie# clear arp-cache oob 1.0.0.0 255.0.0.0
```

【提示信息】 -

【常见错误】 -

【平台说明】 NBR6205-E、NBR6135-E、NBR6210-E、NBR6215-E 支持 MGMT 口；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 MGMT 口。

2.17 ip proxy-arp

在接口上启用代理 ARP 功能。

ip proxy-arp

关闭代理 ARP 功能。

no ip proxy-arp

【参数说明】

参数	描述
-	-

【缺省配置】 -

【命令模式】 接口模式

【缺省级别】 2

【使用指导】 设备的代理 ARP 功能可以帮助没有路由信息的主机，获得其它网络或子网 IP 地址的 MAC 地址。比如设备接收到一个 ARP 请求，ARP 请求发送者的 IP 地址与所请求的 IP 地址不属于同一网络，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。以上过程就是代理 ARP 的功能。

【配置举例】 1：在 gigabitEthernet 0/1 启用代理 ARP 功能：

```
Ruijie(config)# interface gigabitEthernet 0/1
Ruijie(config-if-GigabitEthernet 0/1)# ip proxy-arp
```

【检验方法】 1：在打开代理的情况下，**show ip interface** 接口 1 可见 Proxy ARP 是： ON。

【提示信息】 -

【常见错误】 -

【平台说明】 -

2.18 show arp

显示地址解析协议（ARP）缓冲表。

show arp [*interface-type interface-number* | **trusted** [*ip* [*mask*]] | [*ip* [*mask*] | *mac-address* | **static** | **complete** | **incomplete**]]

【参数说明】

参数	描述
interface-type interface-number	显示指定三层端口或者二层端口的 ARP
trusted	显示可信任 ARP 表项，当前只有全局 VRF 支持可信任 ARP。

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。
static	显示所有静态 arp 表项, 以及显示静态 arp 的来源。
complete	显示所有已经解析的动态 arp 表项。
incomplete	显示所有未解析的动态 arp 表项。
mac-address	显示指定 mac 地址的 ARP 表项。

【命令模式】 特权模式

【缺省级别】 1

【使用指导】 显示 ARP 缓冲表，其中 **complete / incomplete** 关键字是用来分别显示动态 ARP 中已解析 / 未解析的表项。

【配置举例】 1：显示 **show arp** 输出结果：

```
Ruijie# show arp
Total Numbers of Arp: 7
Protocol  Address          Age(min)  Hardware        Type   Interface
Internet  192.168.195.68   0         0013.20a5.7a5f  arpa   VLAN 1
Internet  192.168.195.67   0         001a.a0b5.378d  arpa   VLAN 1
Internet  192.168.195.65   0         0018.8b7b.713e  arpa   VLAN 1
Internet  192.168.195.64   0         0018.8b7b.9106  arpa   VLAN 1
Internet  192.168.195.63   0         001a.a0b5.3990  arpa   VLAN 1
Internet  192.168.195.62   0         001a.a0b5.0b25  arpa   VLAN 1
Internet  192.168.195.5    --        00d0.f822.33b1  arpa   VLAN 1
```

2：显示 **show arp** *192.168.195.68* 的输出结果：

```
Ruijie# show arp 192.168.195.68
Protocol  Address    Age(min)  Hardware        Type   Interface
Internet  192.168.195.68   1   0013.20a5.7a5f  arpa   VLAN 1
```

3：显示 **show arp** *192.168.195.0 255.255.255.0* 的输出结果：

```
Ruijie# show arp 192.168.195.0 255.255.255.0
Protocol  Address    Age(min)  Hardware   Type   Interface
Internet  192.168.195.64   0   0018.8b7b.9106  arpa   VLAN 1
Internet  192.168.195.2    1   00d0.f8ff.f00e  arpa   VLAN 1
Internet  192.168.195.5    --   00d0.f822.33b1  arpa   VLAN 1
Internet  192.168.195.1    0   00d0.f8a6.5af7  arpa   VLAN 1
Internet  192.168.195.51   1   0018.8b82.8691  arpa   VLAN 1
```

4：显示 **show arp** *001a.a0b5.378d* 的输出结果：

```
Ruijie# show arp 001a.a0b5.378d
Protocol  Address  Age(min)  Hardware  Type   Interface
Internet  192.168.195.67   4   001a.a0b5.378d  arpa   VLAN 1
```

5：显示 **show arp static** 的输出结果：

```
Ruijie# show arp static
Protocol  Address  Age(min)  Hardware  Type   Interface         Origin
Internet  192.168.23.55    <static>  0000.0000.0010  arpa   VLAN 100   Configure
Internet  192.168.23.56    <static>  0000.0000.0020  arpa   VLAN 100   Authentication
Internet  192.168.23.57    <static>  0000.0000.0020  arpa   VLAN 100   DHCP-Snooping
2  static arp entries exist.
```

字段解释：

字段	说明
Protocol	当前只有 Internet 这个值，代表的是 IP 协议
Address	IPv4 地址
Age(min)	表项当前年龄 ,对于本机 IP, 显示’-’ ,对于静态表项 ,显示<static>, 对于动态表项，显示表项已经学习到多长时间了，单位为分钟。
Hardware	硬件地址，即 48 bit 的 MAC 地址，每 16 bit 一组，用’.’隔开。十六进制表示。
Type	当前只有 arpa 这个值
Interface	这个 ARP 表项对应的 3 层接口。对于静态 ARP 表项，有时候这个地方无信息，原因是静态 ARP 的 IP 没有在设备的任何直连网段中。
Origin	静态 ARP 表项的来源，Configure 为手工配置的，Authentication 表示通过认证生成的。

【提示信息】 -

【平台说明】 -

2.19 show arp counter

显示 ARP 缓存表中 arp 表项数量。

show arp counter

【参数说明】

参数	描述
-	-

【命令模式】 特权模式

【缺省级别】 1

【使用指导】 -

【配置举例】 1：显示 ARP 缓存表中 arp 表项数量。

```
Ruijie#sho arp counter
ARP Limit:                75000
Count of static entries:  0
Count of dynamic entries: 1 (complete: 1  incomplete: 0)
Total:                    1
```

【提示信息】 -

【平台说明】 -

2.20 show arp detail

显示 ARP 缓存表的详细信息。

show arp detail [*interface-type interface-number* | trusted [*ip* [*mask*]] |[*ip* [*mask*] | *mac-address* | **static** | **complete** | **incomplete**]

【参数说明】

参数	描述
interface-type interface-number	显示指定三层端口或者二层端口的 ARP
trusted	显示可信任 ARP 表项，当前只有全局 VRF 支持可信任 ARP。
ip	ip 地址，显示指定 ip 地址的 ARP 表项
ip mask	显示 ip mask 所包括的网段的 ARP 表项
mac-address	显示指定 mac 地址的 ARP 表项
static	显示所有静态 arp 表项
complete	显示所有已经解析的动态 arp 表项
incomplete	显示所有未解析的动态 arp 表项

【命令模式】 特权模式

【缺省级别】 1

【使用指导】 当用户想查看 ARP 的详细信息，比如 ARP 的类型（动态、静态、本地、可信任）、所在的二层端口时，可以使用此命令。

【配置举例】 1：显示 ARP 缓存表的详细信息。

```
Ruijie# show arp detail
```

```
IP Address       MAC Address      Type       Age(min)   Interface  Port     SubVlan
20.1.1.2         0020.0101.0002   Static     --         Te2/5      --       --
20.1.1.1         00d0.f822.33bb   Local      --         Te2/5      --       --
1.1.1.2          00d0.1111.1112   Dynamic    1          Vl2        Te2/1    4
1.1.1.1          00d0.f822.33bb   Local      --         Vl2        --       --
```

2：对于支持配置 description 的产品，显示包括 description 的信息。

```
Ruijie#sho arp detail
IP Address   MAC Address     Type     Age(min) Interface  Port  description
1.1.1.1      00d0.f822.33eb  Static   --       Gi0/0      --    To-lib
```

ARP 缓冲表中各字段的含义描述如下：

字段	描述
IP Address	与硬件地址对应的 IP 地址。
MAC Address	与 IP 地址对应的硬件地址。
Type	ARP 类型，包括静态、动态、可信任、本机四种类型。
Age	ARP 学习到多长时间，单位分钟。
Interface	与 IP 地址关联的三层接口。
Port	与 ARP 关联的二层端口。
SubVlan	与 ARP 关联的 subvlan。
InnerVlan	与 ARP 关联的内层 vlan，即 CE-VLAN
Location	Local：表示 ARP 表项是本端设备上生成或学习的; Remote：表示 ARP 表项是通过远端网关同步过来的
description	静态 ARP 的描述

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

【提示信息】 -

【平台说明】 -

2.21 show arp oob

显示管理口上的地址解析协议（ARP）缓冲表。

show arp oob [*ip* [*mask*] | **static** | **complete** | **incomplete** | *mac-address*]

【参数说明】

参数	描述
ip	IP 地址，显示指定 IP 地址的 ARP 表项
mask	显示 IP 子网内的 ARP 表项
static	显示所有的静态 arp 表项。
complete	显示所有已经解析的动态 arp 表项。
incomplete	显示所有未解析的动态 arp 表项。
mac-address	显示指定 mac 地址的 ARP 表项。

【命令模式】 特权模式

【缺省级别】 1

【使用指导】 显示 ARP 缓冲表，其中 **complete / incomplete** 关键字是用来分别显示动态 ARP 中已解析 / 未解析的表项。

【配置举例】 1：显示 **show arp oob** 输出结果：

```
Ruijie# show arp oob
Total Numbers of Arp: 7
Protocol  Address          Age(min)  Hardware        Type   Interface
Internet  192.168.195.68   0         0013.20a5.7a5f  arpa   mgmt 0
Internet  192.168.195.67   0         001a.a0b5.378d  arpa   mgmt 0
Internet  192.168.195.65   0         0018.8b7b.713e  arpa   mgmt 0
Internet  192.168.195.64   0         0018.8b7b.9106  arpa   mgmt 0
Internet  192.168.195.63   0         001a.a0b5.3990  arpa   mgmt 0
Internet  192.168.195.62   0         001a.a0b5.0b25  arpa   mgmt 0
Internet  192.168.195.5    --        00d0.f822.33b1  arpa   mgmt 0
```

例 2：以下是 **show arp oob** *192.168.195.68* 的输出结果

```
Ruijie# show arp oob 192.168.195.68
Protocol  Address          Age(min)  Hardware        Type   Interface
Internet  192.168.195.68   1         0013.20a5.7a5f  arpa   mgmt 0
```

例 3：以下是 **show arp oob** 192.168.195.0 255.255.255.0 的输出结果

```
Ruijie# show arp 192.168.195.0 255.255.255.0
Protocol  Address          Age(min)  Hardware        Type   Interface
Internet  192.168.195.64   0         0018.8b7b.9106  arpa   mgmt 0
Internet  192.168.195.2    1         00d0.f8ff.f00e  arpa   mgmt 0
Internet  192.168.195.5    --        00d0.f822.33b1  arpa   mgmt 0
Internet  192.168.195.1    0         00d0.f8a6.5af7  arpa   mgmt 0
```

```
Internet  192.168.195.51    1         0018.8b82.8691  arpa   mgmt 0
```

例 4：以下是 **show arp oob** *001a.a0b5.378d* 的输出结果

```
Ruijie# show arp 001a.a0b5.378d
Protocol  Address          Age(min)  Hardware        Type   Interface
Internet  192.168.195.67   4         001a.a0b5.378d  arpa   mgmt 0
```

字段解释：

字段	说明
Protocol	当前只有 Internet 这个值，代表的是 IP 协议
Address	IPv4 地址
Age(min)	表项当前年龄 ,对于本机 IP, 显示'-' ,对于静态表项 ,显示<static>, 对于动态表项，显示表项已经学习到多长时间了，单位为分钟。
Hardware	硬件地址，即 48 bit 的 MAC 地址，每 16 bit 一组，用'.'隔开。十六进制表示。
Type	当前只有 arpa 这个值
Interface	这个 ARP 表项对应的 3 层接口。对于静态 ARP 表项，有时候这个地方无信息，原因是静态 ARP 的 IP 没有在设备的任何直连网段中。

【提示信息】 -

【平台说明】 NBR6205-E、NBR6135-E、NBR6210-E、NBR6215-E 支持 MGMT 口；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 MGMT 口。

2.22 show arp packet statistics

显示 ARP 报文的统计信息。

show arp packet statistics [*interface-name*]

【参数说明】

参数	描述
interface-name	显示指定接口上的 ARP 报文统计信息

【命令模式】 特权模式

【缺省级别】 1

【使用指导】 -

【配置举例】 1：显示 ARP 统计表信息：

```
Ruijie#show arp packet statistics
Interface              Received  Received Received  Sent      Sent
Name                   R
equests  Replies  Others    Requests  Replies
--------------------   --------  -------- --------  --------  -------
GigabitEthernet 0/0    0         0        0         0         0
GigabitEthernet 0/1    143649    232      0         2         0
GigabitEthernet 0/2    0         0        0         0         0
GigabitEthernet 0/3    0         0        0         0         0
GigabitEthernet 0/4    0         0        0         0         0
GigabitEthernet 0/5    0         0        0         0         0
GigabitEthernet 0/6    0         0        0         0         0
Loopback 1             0         0        0         0         0
```

字段解释：

字段	描述
Received Requests	收到的 ARP 请求的数量。
Received Replies	收到的 ARP 应答的数量。
Received Others	收到的其它 ARP 报文的数量。
Sent Requests	发出的 ARP 请求的数量。
Sent Replies	发出的 ARP 应答的数量。

【提示信息】 -

【平台说明】 -

2.23 show arp timeout

显示动态 ARP 表项老化时间。

show arp timeout

【参数说明】

参数	描述
-	-

【命令模式】 特权模式

【缺省级别】 1

【使用指导】 -

【配置举例】 1：显示动态 ARP 表项老化时间。

```
Ruijie# show arp timeout
Interface               arp timeout(sec)
----------------------  ----------------
VLAN 1                  3600
```

【提示信息】 -

【平台说明】 -

2.24 show ip arp

显示地址解析协议（ARP）缓冲表。

show ip arp

【参数说明】

参数	描述
-	-

【命令模式】 特权模式

【缺省级别】 1

【使用指导】 -

【配置举例】 1：显示地址解析协议（ARP）缓冲表。

```
Ruijie# show ip arp
Protocol Address       Age(min)Hardware        Type
Interface
Internet 192.168.7.233  23    0007.e9d9.0488  ARPA FastEthernet 0/0
Internet 192.168.7.112  10    0050.eb08.6617  ARPA FastEthernet 0/0
Internet 192.168.7.79   12    00d0.f808.3d5c  ARPA FastEthernet 0/0
Internet 192.168.7.1    50    00d0.f84e.1c7f  ARPA FastEthernet 0/0
Internet 192.168.7.215  36    00d0.f80d.1090  ARPA FastEthernet 0/0
Internet 192.168.7.127  0     0060.97bd.ebee  ARPA FastEthernet 0/0
Internet 192.168.7.195  57    0060.97bd.ef2d  ARPA FastEthernet 0/0
Internet 192.168.7.183  --    00d0.f8fb.108b  ARPA FastEthernet 0/0
```

ARP 缓冲表中各字段的含义描述如下：

字段	说明
Protocol	网络地址的协议，该字段均为 Internet。
Address	与硬件地址对应的 IP 地址。
Age (min)	ARP 缓冲记录存在的时间，以分钟计。如果是本地的或者静态配置的，该字段值就用短线“-”表示。
Hardware	与 IP 地址对应的硬件地址。
Type	硬件地址类型，以太网地址均为 ARPA。
Interface	与 IP 地址关联的接口。

【提示信息】 -

【平台说明】 -

3 IP Event Dampening

3.1 dampening

打开接口 IP Event Dampening 功能。
dampening [*half-life-period* [*reuse-threshold suppress-threshold max-suppress* [**restart** [*restart-penalty*]]]]

关闭接口 IP Event Dampening 功能。
no dampening

恢复缺省配置（关闭该功能），与 **no dampening** 效果一样。
default dampening

【参数说明】

参数	描述
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。

【缺省配置】 关闭接口的 IP Event Dampening 功能。

【命令模式】 接口模式

【缺省级别】 2

【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。

【配置举例】 1 :对交换机接口 GigabitEthernet0/1 设置接口事件抑制功能 ,半衰期 30 秒 ,解除抑制门限 1500 ,抑制门限 10000，最长抑制时间为 100 秒。

```
Ruijie(config)#interface gigabitEthernet 0/1
Ruijie(config-if-GigabitEthernet 0/1)# no switchport
Ruijie(config-if-GigabitEthernet 0/1)# dampening 30 1500 10000 100
```

【检验方法】 1：使用 **show runuing-config** 命令，可以查看 ip event dampening 功能是启用还是关闭。
2：使用 **show interfaces dampening** 命令，可以查看 dampening 接口的详细配置信息。

【提示信息】 1 :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
```

2：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!
```

【常见错误】 1：配置的 max-suppress 太小，导致配置失败。

2：在三层交换机接口上，没有 no switchport，就直接配置 dampening 功能。

【平台说明】 -

3.2 show dampening interface

显示被惩罚的接口的统计信息。

show dampening interface

【参数说明】

参数	描述
-	-

【命令模式】 特权模式、全局模式、接口模式

【缺省级别】 2

【使用指导】 使用该命令可以查看设备上哪些接口配置了 dampening 功能，哪些接口被抑制了。

【配置举例】 1：查看被惩罚接口的统计信息。

```
Ruijie# show dampening interface
1 interfaces are configured with dampening.
No interface is being suppressed.
```

【提示信息】 -

【平台说明】 -

3.3 show interfaces dampening

显示接口 IP Event Dampening 配置情况。

show interfaces [*interface-id*] **dampening**

【参数说明】

参数	描述
interface-id	接口名称（例如 GigabitEthernet 0/1）。

【命令模式】 特权模式、全局模式、接口模式

【缺省级别】 2

【使用指导】 若指定了 interface-id，将仅显示该指定接口的 dampening 信息。

【配置举例】 1：查看接口 IP Event Dampening 配置情况。

```
Ruijie#show interfaces dampening
GigabitEthernet 0/1
  Flaps Penalty Supp    ReuseTm HalfL   ReuseV  SuppV   MaxSTm  MaxP    Restart
  0     0       FALSE   0       30      1500    10000   100     15119   0
```

字段的含义描述如下：

字段	描述
Flaps	接口翻转的次数。
Penalty	当前惩罚值的大小。
Supp	是否处于被抑制状态。
ReuseTm	离重新使用还剩多少时间（单位：秒）。
HalfL	半衰期。
ReuseV	重新使用阀值。
SuppV	抑制阀值。
MaxSTm	最大抑制时间。
MaxP	最大惩罚值。
Restart	初始惩罚值。

【提示信息】 -

【平台说明】 -

4 TCP

4.1 ip tcp adjust-mss

设置转发的 TCPv4 SYN 报文的 MSS 选项值。

ip tcp adjust-mss *max-segment-size*

恢复缺省配置。

no ip tcp adjust-mss

【参数说明】

参数	描述
max-segment-size	最大数据段大小，单位为字节，范围是 500-1460

【缺省配置】 不修改 SYN 报文的 MSS 选项值。

【命令模式】 接口模式

【缺省级别】 14

【使用指导】 MSS：TCP 报文数据载荷最大值。

TCP 的路径最大传输单元发现功能是按 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。

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。

在接口上配置本命令会使得该接口接收或发送 SYN 报文的 MSS 选项被改为接口配置的 MSS 值。如果 SYN 报文的入口和出口都配置了 MSS，那么取两个口配置的较小者。但一般建议出口和入口配置一样。本命令实际上是修改了 TCP 建立连接时交互的 SYN 报文，有些版本也会修改 SYN+ACK 报文。

这个功能的启用与关闭，对于已经建立的 TCP 连接不生效，只对后来建立的 TCP 连接生效。

【配置举例】 1：在接口 GigabitEthernet 0/0 上配置把转发的 TCPv4 SYN 报文的 MSS 选项值修改为 1000 字节。

```
Ruijie(config-if-GigabitEthernet 0/0)# ip tcp adjust-mss 1000
```

【检验方法】 -

【提示信息】 -

【常见错误】 -

【平台说明】 -

4.2 ip tcp keepalive

该命令用来开启 TCP 保活功能。

ip tcp keepalive [**interval** *num1*] [**times** *num2*] [**idle-period** *num3*]

【参数说明】

参数	描述
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。

【缺省配置】 关闭。

【命令模式】 全局模式

【缺省级别】 2

【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。

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。

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。

【配置举例】 1：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(config)# ip tcp keepalive interval 60 times 4 idle-period 180
```

【检验方法】 -

【提示信息】 -

【常见错误】 -

【平台说明】 -

4.3 ip tcp mss

设置 TCP 连接的 MSS 的最大值。

ip tcp mss *max-segment-size*

恢复缺省配置。

no ip tcp mss

【参数说明】

参数	描述
max-segment-size	MSS 的上限值。单位为字节，取值范围 68-10000。 默认使用根据 MTU 计算得到的 MSS。

【缺省配置】 -

【命令模式】 全局模式

【缺省级别】 14

【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。默认使用根据 MTU 计算得到的 MSS，如下所示：

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。

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。

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。

【配置举例】 1：设置 TCP 连接的 MSS 的上限值为 1300 字节。

```
Ruijie(config)# ip tcp mss 1300
```

【检验方法】 -

【提示信息】 -

【常见错误】 -

【平台说明】 -

4.4 ip tcp path-mtu-discovery

打开 TCP 的路径 MTU 发现功能。

ip tcp path-mtu-discovery [**age-timer** *minutes* | **age-timer infinite**]

关闭 TCP 的路径 MTU 发现功能。

no ip tcp path-mtu-discovery

【参数说明】

参数	描述

age-timer *minutes*	TCP 在发现 PMTU 后 ,重新进行探测的时间间隔。单位分钟 ,取值范围 10-30。缺省值 10。
age-timer infinite	TCP 在发现 PTMU 后，不重新探测。

【缺省配置】 关闭。

【命令模式】 全局模式

【缺省级别】 14

【使用指导】 TCP 的路径最大传输单元发现功能是按 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 PMTU 后，隔一段时间可以使用更大的 MSS 来探测新的 PMTU。这个时间间隔就是使用参数 **age-timer** 来指定。当设备发现的 PMTU 比 TCP 连接两端协商出来的 MSS 小时，设备就会按上述配置时间间隔，去尝试发现更大的 PMTU。直到 PMTU 达到 MSS 的值，或者用户停止这个定时器，这个探测过程才会停止。停止这个定时器，使用 **age-timer infinite** 参数。

【配置举例】 1：开启 PMTU 发现功能。

```
Ruijie(config)# ip tcp path-mtu-discovery
```

【检验方法】 -

【提示信息】 -

【常见错误】 -

【平台说明】 -

4.5 ip tcp send-reset

允许在收到端口不可达的 TCP 报文时发送 reset 报文。
ip tcp send-reset

禁止在收到端口不可达的 TCP 报文时发送 reset 报文。
no ip tcp send-reset

【参数说明】

参数	描述
-	-

【缺省配置】 收到端口不可达的 TCP 报文时发送 reset 报文。

【命令模式】 全局模式

【缺省级别】 14

【使用指导】 一般情况下，TCP 模块在分发 TCP 报文时，如果找不到该报文所属的 TCP 连接那么会主动回复一个 reset 报文用以终止对端的 TCP 连接。但是这也会成为攻击者的攻击目标，大量的端口不可达的 TCP 报文会对设备造成攻击，可以通过以下命令来禁止对端口不可达的报文发送 reset 报文。

【配置举例】 1：禁止在收到端口不可达的 TCP 报文时发送 reset 报文。

```
Ruijie(config)# no ip tcp send-reset
```

【检验方法】 -

【提示信息】 -

【常见错误】 -

【平台说明】 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。

4.6 ip tcp synwait-time

设置建立连接的 SYN 报文的超时时间。

ip tcp synwait-time *seconds*

恢复缺省值。

no ip tcp synwait-time

【参数说明】

参数	描述
seconds	SYN 报文超时时间。 单位为秒，取值范围 5-300，缺省值 20。

【缺省配置】 缺省超时时间为 20 秒

【命令模式】 全局模式

【缺省级别】 14

【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的增加超时时间。

【配置举例】 1：设置建立连接的 SYN 报文的超时时间为 10 秒。

```
Ruijie(config)# ip tcp synwait-time 10
```

【检验方法】 -

【提示信息】 -

【常见错误】 -

【平台说明】 11.0 版本废弃了 10.x 版本的配置命令“ip tcp syntime-out”，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。

4.7 ip tcp window-size

设置 TCP 窗口大小。

ip tcp window-size *size*

恢复缺省值。

no ip tcp window-size

【参数说明】

参数	描述
size	窗口大小。 单位是字节，取值范围 128-(65535 << 14)，缺省值是 65535。

【缺省配置】 缺省值是 65535 字节

【命令模式】 全局模式

【缺省级别】 14

【使用指导】 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。

如果窗口大于 65535 字节，自动开启窗口扩大功能。

【配置举例】 1：设置窗口大小为 16386 字节。

```
Ruijie(config)# ip tcp window-size 16386
```

【检验方法】 -

【提示信息】 -

【常见错误】 -

【平台说明】 -

4.8 service tcp-keepalives-in

开启 TCP 服务器端的保活功能。
service tcp-keepalives-in [*interval*] [**garbage**]

关闭 TCP 服务器端的保活功能
no service tcp-keepalives-in

【参数说明】

参数	描述
interval	发送保活报文的时间间隔，单位是秒，取值范围是 1 到 65535，缺省值是 60 秒
garbage	保活报文携带一个字节的无效数据，默认不携带。

【缺省配置】 关闭 TCP 服务器端的保活功能

【命令模式】 全局模式

【缺省级别】 14

【使用指导】 有时候 TCP 服务器希望知道客户端是否还在正常工作，这就需要使用 TCP 保活功能。
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，自动释放 TCP 连接。

【配置举例】 1：开启 TCP 服务器端的保活功能，发送保活报文的时间间隔是 10 秒，保活报文携带一个字节的无效数据。

```
Ruijie(config)# service tcp-keepalives-in 10 garbage
```

【检验方法】 -

【提示信息】 -

【常见错误】 -

【平台说明】 -

4.9 service tcp-keepalives-out

开启 TCP 客户端的保活功能。

service tcp-keepalives-out [*interval*] [**garbage**]

【参数说明】

参数	描述
interval	发送保活报文的时间间隔，单位是秒，取值范围是 1 到 65535，缺省值是 60 秒
garbage	保活报文携带一个字节的无效数据，默认不携带。

【缺省配置】 关闭 TCP 客户端的保活功能

【命令模式】 全局模式

【缺省级别】 14

【使用指导】 TCP 客户端可以使用保活功能探测服务器是否还在正常工作。

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，自动释放 TCP 连接。

【配置举例】 1：开启 TCP 客户端的保活功能，发送保活报文的时间间隔是 10 秒，保活报文携带一个字节的无效数据。

```
Ruijie(config)# service tcp-keepalives-out 10 garbage
```

【检验方法】 -

【提示信息】 -

【常见错误】 -

【平台说明】 -

4.10 show tcp connect

显示系统当前 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***]**

显示系统当前 IPv4 TCP 连接的统计信息。

show tcp connect statistics

【参数说明】

参数	描述
local-ip *a.b.c.d*	本地 IP 地址

local-port *num*	本地端口
peer-ip *a.b.c.d*	对端 IP 地址
peer-port *num*	对端端口
statistics	查看 IPv4 TCP 连接的统计信息

【命令模式】 特权模式

【缺省级别】 2

【使用指导】 -

【配置举例】 1：查看系统当前 IPv4 TCP 连接的基本信息。

```
Ruijie#show tcp connect
Number Local Address     Foreign Address          State       Process name
1      0.0.0.0:22        0.0.0.0:0                LISTEN      rg-sshd
2      0.0.0.0:23        0.0.0.0:0                LISTEN      rg-telnetd
3      1.1.1.1:23        1.1.1.2:64201            ESTABLISHED rg-telnetd
```

字段解释：

字段	说明
Number	序号。
Local Address	本地地址与端口号，冒号后面的数字是端口号，比如 “1.1.1.1:23”中的“23”是端口号。
Foreign Address	远端地址与端口号，冒号后面的数字是端口号，比如 “1.1.1.1:23”中的“23”是端口号。
State	TCP 连接当前的状态，有 11 种可能状态： CLOSED：连接已断开 LISTEN：监听状态 SYNSENT：SYN 报文已发出，三次握手阶段 SYNRCVD：SYN 报文已接收到，三次握手阶段 ESTABLISHED：连接已建立 FINWAIT1：本端已经发出 FIN 报文 FINWAIT2：本端发出的 FIN 报文已经被确认 CLOSEWAIT：本端收到了对端的 FIN 报文 LASTACK：本端收到了对端的 FIN 报文，然后本端发出了自己的 FIN 报文 CLOSING：本端发出 FIN 报文，在对端回应该 FIN 报文的 ACK 报文到来之前收到了对端的 FIN 报文 TIMEWAIT：本端发送的 FIN 报文被确认了，并且本端也已经确认了接收到的 FIN 报文
Process name	进程名称

2：查看系统当前 IPv4 TCP 连接的统计信息。

```
Ruijie#show tcp connect statistics
State       Count
-----       -----
ESTABLISHED 1
SYN_SENT    0
SYN_RECV    0
FIN_WAIT1   0
FIN_WAIT2   0
TIME_WAIT   0
CLOSED      0
CLOSE_WAIT  0
LAST_ACK    0
LISTEN      1
CLOSING     0
Total: 2
```

【提示信息】 -

【平台说明】 -

4.11 show tcp parameter

显示系统当前 TCP 参数信息

show tcp parameter

【参数说明】

参数	描述
-	-

【命令模式】 特权模式

【缺省级别】 2

【使用指导】 -

【配置举例】 1：查看系统当前 tcp 参数信息

```
Ruijie#show tcp parameter
Hash table information:
  Established hash bucket size: 16384
  Bind hash bucket size: 16384
Memory information:
```

```
  Global memory limit: low=92160, pressure=122880, high=184320 (unit: pages)
  Per-socket receive buffer size: min=4096, default=87380, max=3932160 (unit: bytes)
  Per-socket send buffer size: min=4096, default=16384, max=3932160 (unit: bytes)
  Current allocated memory: 0
  Current memory pressure flag: 0
SYN specific information:
  Max SYN_RECV sockets per LISTEN socket: 65535
  Max SYN retries: 5
  Max SYN ACK retries: 5
Timewait specific information:
  Max timewait sockets: 180000
  Current timewait sockets: 0
  Timewait recycle: 0
  Reuse timewait port: 0
Keepalive information:
  Keepalive on: 0
  Idle period: 900 seconds
  Interval: 75 seconds
  Max probes: 6
MTU probing:
  Enable mtu probing: 0
FIN specific information:
  FIN_WAIT_2 timeout: 60 seconds
Orphan socket information:
  Max orphans: 16384
  Max orphan retries: 0
  Current orphans: 0
```

字段解释：

字段	说明
Hash table information	TCP 连接哈希表参数信息
Memory information	TCP 连接收发缓存参数信息
SYN specific information	TCP 服务端连接侦听相关参数信息
Timewait specific information	TIMEWAIT 状态下的 TCP 连接参数信息
Keepalive information	TCP 保活时钟参数信息
MTU probing	MTU 探测相关的参数信息
FIN specific information	TCP 连接关闭的相关参数信息
Orphan socket information	未与具体应用关联的 TCP 连接的参数信息

【提示信息】 -

4.12 show tcp pmtu

显示 IPv4 TCP 连接的路径 MTU。

show tcp pmtu [local-ip *a.b.c.d***] [local-port** *num***] [peer-ip** *a.b.c.d***] [peer-port** *num***]**

【参数说明】

参数	描述
local-ip *a.b.c.d*	本地 IP 地址
local-port *num*	本地端口
peer-ip *a.b.c.d*	对端 IP 地址
peer-port *num*	对端端口

【命令模式】 特权模式

【缺省级别】 2

【使用指导】 -

【配置举例】 1：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
```

字段解释：

字段	说明
Number	序号
Local Address	本地地址与端口号，冒号后面的数字是端口号，比如“192.168.195.212.23”中的“23”是端口号。
Foreign Address	远端地址与端口号，冒号后面的数字是端口号，比如“192.168.195.212.23”中的“23”是端口号。
PMTU	路径 MTU。

【提示信息】 -

【平台说明】 -

4.13 show tcp port

显示系统当前 TCP 端口的使用情况。

show tcp port [*num***]**

【参数说明】

参数	描述
num	端口号

【命令模式】 特权模式

【缺省级别】 2

【使用指导】 -

【配置举例】 1：查看系统当前 IPv4 TCP 端口的使用情况。

```
Ruijie#show tcp port
TCP connections on port 23:
Number  Local Address Foreign Address    State
1       1.1.1.1:23    1.1.1.2:64571    ESTABLISHED
Total: 1

TCP connections on port 2650:
Number  Local Address Foreign Address    State
Total: 0
```

字段解释：

字段	说明
Number	序号
Local Address	本地地址与端口号。
Foreign Address	远端地址与端口号。

State	TCP 连接当前的状态，有 11 种可能状态： CLOSED: 连接已断开 LISTEN：监听状态 SYNSENT：SYN 报文已发出，三次握手阶段 SYNRCVD：SYN 报文已接收到，三次握手阶段 ESTABLISHED：连接已建立 FINWAIT1：本端已经发出 FIN 报文 FINWAIT2：本端发出的 FIN 报文已经被确认 CLOSEWAIT：本端收到了对端的 FIN 报文 LASTACK：本端收到了对端的 FIN 报文，然后本端发出了自己的 FIN 报文 CLOSING：本端发出 FIN 报文，在对端回应该 FIN 报文的 ACK 报文到来之前收到了对端的 FIN 报文 TIMEWAIT：本端发送的 FIN 报文被确认了，并且本端也已经确认了接收到的 FIN 报文

【提示信息】 -

【平台说明】 -

4.14 show tcp statistics

显示系统当前 TCP 统计信息，含报文接收信息，三次握手信息， time-wait 连接信息

show tcp statistics

【参数说明】

参数	描述
-	-

【命令模式】 特权模式

【缺省级别】 2

【使用指导】 -

【配置举例】 1：查看系统当前 tcp 统计信息

```
Ruijie#show tcp statistics
TCP Packets
  Received: 1103
  Errors  : 0(checksum: 0)
Three way handshake
  Request queue overflow: 0
```

```
  Accept backlog full: 0
  Web authentication limit per user: 0
  Failed to alloc memory for request sock: 0
  Failed to create open request child: 0
  SYN ACK retransmits: 0
  Timeouted requests: 0
Time-wait
  Time-wait bucket table overflow: 0
```

字段解释：

字段	说明
TCP Packets	TCP 接收到的正常报文，错误报文
Three way handshake	三次握手过程中的信息，含收到的连接请求次数，作为服务器端与客户端建立的连接次数，由于 WEB 认证限制导致三次握手失败的次数，内存不足而无法创建 TCP 套接字的次数，无法创建子连接的次数，报文的重传次数以及报文重传超时导致连接未建立的次数。
Time-wait	TIMEWAIT 状态连接信息

【提示信息】 -

5 软件 IPv4 快转

5.1 clear ip ref packet statistics

清除 IPv4 快转当前的报文统计信息。

clear ip ref packet statistics

【参数说明】

参数	描述
-	-

【命令模式】 特权模式

【缺省级别】 14

【使用指导】 -

【配置举例】 1：清除 IPv4 快转当前的报文统计信息。

```
Ruijie #clear ip ref packet statistics
```

【提示信息】 -

【平台说明】 -

5.2 ip ref load-sharing original

配置 IPv4 快转的负载均衡算法为基于目的 IP 地址和源 IP 地址负载均衡。

ip ref load-sharing original

把 IPv4 快转的负载均衡算法恢复成缺省值。

no ip ref load-sharing original

【参数说明】

参数	描述
-	-

【缺省配置】 基于目的 IP 地址负载均衡

【命令模式】 全局模式

【缺省级别】 14

【使用指导】 软件快转负责数据转发，并支持两种负载均衡算法，一种是目的 IP 负载均衡，另一种为目的 IP 和源 IP 组合的负载均衡算法。在多路径转发 IP 报文时，如当前设置为目的 IP 负载均衡，REF 将以报文的目的 IP 来匹配其中的一个条路径进行转发。缺省情况为目的 IP 负载均衡。

【配置举例】 1：配置源 IP+目的 IP 的均衡选路算法。

```
Ruijie(config)# ip ref load-sharing original
```

2：使用基于报文目的地址的均衡选路算法。

```
Ruijie(config)# no ip ref load-sharing original
```

【检验方法】 使用命令 **show run** 查看配置。

【提示信息】 -

【常见错误】 -

【平台说明】 -

5.3 show ip ref adjacency

显示特定邻接节点信息或当前所有的邻接节点信息。

s**how ip ref adjacency [glean | local |** *ip-address* | **interface** *interface_type interface_number* | **discard** | **statistics**]

【参数说明】

参数	描述
glean	集合邻接节点
local	本地邻接节点
ip-address	邻接下一跳 IP
interface_type	指定接口类型
interface_number	指定接口编号
discard	显示丢弃邻接节点
statistics	统计信息

【命令模式】 特权模式

【缺省级别】 14

【使用指导】 该命令可以显示当前 IPv4 快转的邻接表信息，可以指定显示集合邻接、本地邻接、指定 IP 对应邻接、指定接口关联邻接及所有邻接节点相关信息。

【配置举例】 1：显示所邻接表中所有邻接信息。

```
Ruijie#show ip ref adjacency
id state      type    rfct chg  ip            interface         linklayer(header data)
1  unresolved mcast   1    0   224.0.0.0
9  resolved   forward 1    0   192.168.50.78   GigabitEthernet 0/0  00 25 64 C5 9D 6A 00 D0 F8 98
76 54 08 00
7  resolved   forward 1    0   192.168.50.200  GigabitEthernet 0/0  00 04 5F 87 69 66 00 D0 F8 98
76 54 08 00
6  unresolved  glean  1    0   0.0.0.0         GigabitEthernet 0/0
4  unresolved  local  3    0   0.0.0.0         Local 1
```

显示结果各字段描述：

字段	说明
id	邻接标识
state	邻接状态 unresolve：未解析 resolved：已解析
type	邻接类型 local：本地邻接 forward：转发邻接 discard：丢弃邻接 glean：集合邻接 mcast：组播邻接
rfct	邻接被引用的计数
chg	邻接是否在变化链中
ip	邻接对应的 IP 地址
interface	出接口
linklayer	二层头

【提示信息】 -

【平台说明】 -

5.4 show ip ref exact-route

显示 IP 报文的确切转发路径。

show ip ref exact-route [**oob**] *source_ipaddress dest_ipaddress*

【参数说明】

参数	描述
oob	带外，即管理口所属的管理网络。支持管理口的设备才支持本参数。

source_ipaddress	报文的源 IP 地址
dest_ipaddress	报文的目的 IP 地址

【命令模式】 特权模式

【缺省级别】 14

【使用指导】 通过该命令，指定 IP 报文的源 IP 地址与目的 IP 地址，可以显示出特定报文的转发路径。

【配置举例】 1：查看从 192.168.217.74 到 192.168.13.1 的转发路径。

```
Ruijie# show ip ref exact-route 192.168.217.74 192.168.13.1
192.168.217.74  --> 192.168.13.1:
id state    type    rfct chg  ip            interface          linklayer(header data)
9  resolved forward 1     0   192.168.17.1  GigabitEthernet 0/0 00 25 64 C5 9D 6A 00 D0 F8 98 76 54
08 00
```

显示结果各字段描述：

字段	说明
id	邻接标识
state	邻接状态 unresolve：未解析 resolved：已解析
type	邻接类型 local：本地邻接 forward：转发邻接 discard：丢弃邻接 glean：集合邻接 mcast：组播邻接
rfct	邻接被引用的计数
chg	邻接是否在变化链中
ip	邻接对应的 IP 地址
interface	出接口
linklayer	二层头

【提示信息】 -

【平台说明】 NBR6205-E、NBR6135-E、NBR6210-E、NBR6215-E 支持 MGMT 口；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 MGMT 口。

5.5 show ip ref packet statistics

显示 IPv4 快转当前的报文统计信息。

show ip ref packet statistics

【参数说明】

参数	描述
-	-

【命令模式】 特权模式

【缺省级别】 14

【使用指导】 -

【配置举例】 1：显示 IPv4 快转当前的报文统计信息。

```
Ruijie #show ip ref packet statistic
ref packet statistic:
    bad head        : 0
    lookup fib fail : 0
    local adj       : 0
    glean adj       : 0
    forward         : 0
    redirect        : 0
    ttl expiration  : 0
    no ip routing   : 0
```

显示结果各字段描述：

字段	说明
bad head	报头错误的报文数目
lookup fib fail	快转选路失败报文数目
local adj	匹配到本地邻接的报文数目
glean adj	匹配到汇聚邻接的报文数目
forar	匹配到转发邻接的报文数目
redirect	重定向处理的报文数目
ttl expiration	报文 TTL 超时的报文数目
no ip routing	不允许转发送本地的报文数目

【提示信息】 -

【平台说明】 -

5.6 show ip ref resolve-list

显示 IPv4 快转主动解析信息。

show ip ref resolve-list

【参数说明】

参数	描述
-	-

【命令模式】 特权模式

【缺省级别】 14

【使用指导】 -

【配置举例】 1：显示 IPv4 快转主动解析信息。

```
Ruijie#show ip ref resolve-list
IP                  res_state flags interface
1.1.1.1             unres     1      GigabitEthernet 0/0
```

字段	说明
IP	IP 地址
res_state	unres：未解析，res：解析
flags	0：与邻接无关， 1：与邻接相关
interfae	接口名称

【提示信息】 -

【平台说明】 -

5.7 show ip ref route

显示当前 IPv4 快转的所有路由信息。

show ip ref route [**oob**] [**default** | *ip mask* | **statistics**]

【参数说明】

参数	描述
oob	带外，即管理口所属的管理网络。支持管理口的设备才支持本参数。
default	指定默认路由
ip	指定路由目的 IP

mask	指定路由掩码
statistics	统计信息

【命令模式】 特权模式

【缺省级别】 14

【使用指导】 可以显示当前 IPv4 快转的路由信息，可以指定显示默认路由、指定 IP/MASK 匹配的路由、所有路由信息。

【配置举例】 1：显示全局快转表中所有路由信息。

```
Ruijie#show ip ref route
Codes: * - default route
       # - zero route
 ip/mask            weight  path-id      next-hop        interface
 255.255.255.255/32 1       4            0.0.0.0         Local 1
 224.0.0.0/24       1       4            0.0.0.0         Local 1
 192.168.50.0/24    1       6            0.0.0.0         GigabitEthernet 0/0
 192.168.50.200/32  1       7            192.168.50.200  GigabitEthernet 0/0
 192.168.50.122/32  1       4            0.0.0.0         Local 1
 192.168.50.78/32   1       9            192.168.50.78   GigabitEthernet 0/0
```

显示结果各字段描述：

字段	说明
ip/mask	目的 IP 地址和掩码长度
path-id	邻接索引标识
weight	路由权重
next_hop	下一跳
interface	输出接口

【提示信息】 -

【平台说明】 NBR6205-E、NBR6135-E、NBR6210-E、NBR6215-E 支持 MGMT 口；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 MGMT 口。

6 TUNNEL

6.1 show interfaces tunnel

显示 tunnel 的配置概要。使用如下命令。

show interfaces tunnel [number]

【参数说明】

参数	描述
number	显示指定编号对应的 tunnel 的概况。不指定此参数则显示所有 tunnel 的概况。注意，如果指定了编号，则该编号对应的 tunnel 要求是已创建的。

【命令模式】 特权模式、全局模式、接口模式

【缺省级别】 2

【使用指导】 通过此命令可以查看某个 tunnel 相关的所有信息。

【配置举例】 1：查看 tunnel 1 的详细信息

```
Ruijie#show interfaces tunnel 1
```

// 这儿是接口的公共信息

```
Tunnel source 1.1.1.2, destination 1.1.1.1, routeable
  Tunnel TOS/Traffic Class not set, Tunnel TTL 254
  Tunnel config nested limit is 0, current nested number is 0
  Tunnel transport VPN is no set
```

字段解释：

字段	说明
Destination	隧道的目标地 当为 0.0.0.0 表示没有配置
Tunnel source	隧道的本端地址，是 IPv4 地址。如果配置的是 tunnel source interface,则取的是 interface 上的地址
Tunnel TTL	对应传输协议的 TTL 或者 hoplimit 字段
Tunnel TOS	对应传输协议的 TOS 或者 traffic class 字段。特例：如果为 0，且传输协议和负载协议相同，一般拷贝负载协议的相应字段到传输协议
Tunnel protocol/transport	隧道的封装模式，即 tunnel mode 所配置的模式

【提示信息】 -

【平台说明】 -

6.2 show tunnel statistics

显示 tunnel 的可配置容量和已使用个数。

show tunnel statistics

【参数说明】

参数	描述
-	无。

【命令模式】 特权模式、全局模式、接口模式

【缺省级别】 2

【使用指导】 通过此命令可以查看 tunnel 的已配置和可配置 tunnel 口的个数的信息。注意，对于交换机平台，实际转发能力还要受芯片表项个数限制，可能会出现隧道口创建成功，但实际芯片表项已满的情况。一般这种情况会有 syslog 提示。

【配置举例】 1：查看 tunnel 口的已配置个数信息。

```
Ruijie#show tunnel statistics
used: 2,  limit: 1000
```

【提示信息】 -

【平台说明】 -

6.3 tunnel destination

设置隧道接口的对端地址。

tunnel destination ip-address

删除对端地址。

no tunnel destination

【参数说明】

参数	描述
ip-address	对端的 IP 地址，是 IPv4 地址

【缺省配置】 没有配置对端地址。

【命令模式】 接口模式

【缺省级别】 2

【使用指导】 tunnel mode ipip， tunnel mode gre ip 这 2 种隧道的对端地址需要配置成 IPv4 地址。

【配置举例】 1：创建隧道接口。

```
Ruijie(config)# interface tunnel 1
```

2：设置隧道模式。

```
Ruijie(config-if)# tunnel mode gre ip
```

3：设置隧道对端地址。

```
Ruijie(config-if)# tunnel destination 1.1.1.1
```

【检验方法】 1：使用 show interface tunnel 命令，可以查看隧道配置的对端地址。

【提示信息】 1：如果在设置的对端地址同另一个隧道的对端地址相同，且 2 个隧道的源地址也相同，则提示错误。
%Maybe Tunnel XXX satisfy you

【常见错误】 1：配置的对端地址与隧道模式不匹配。
2：配置的对端地址网络不可达。

【平台说明】 -

6.4 tunnel mode

修改隧道封装模式。
tunnel mode { gre ip | ipip }

恢复隧道封装模式。
no tunnel mode

恢复缺省配置。
default tunnel mode

【参数说明】

参数	描述
gre ip	传输网络为 IPv4 网络，使用 GRE 封装。
ipip	传输网络为 IPv4 网络，不使用 GRE 封装，用户网络是 IPv4 网络。

【缺省配置】 网关、路由器为 gre ip。

【命令模式】 接口模式

【缺省级别】 2

【使用指导】 Tunnel 的封装模式就是 Tunnel 的载体协议。用户可以根据实际使用情况来设置 Tunnel 接口的封装模式。
实际的隧道模式种类与使用机型相关。

【配置举例】 1：创建隧道接口。

```
Ruijie(config)# interface tunnel 1
```

2：设置隧道模式。

```
Ruijie(config-if-Tunnel 1)# tunnel mode ip
```

【检验方法】 1：使用 show interface tunnel 命令，可以查看隧道的模式。

【提示信息】

【常见错误】 -

【平台说明】 -

6.5 tunnel source

配置 tunnel 接口的源地址。
tunnel source { ip-address | interface-type interface-number }

删除 tunnel 接口的源地址。
no tunnel source

【参数说明】

参数	描述
ip-address	用来指定 tunnel 的本端地址，是 ipv4 地址也。
interface-type	通用的接口类型，例如：异步串行接口 Async、拨号接口 Dialer、以太网接口 Ethernet、快速以太网接口 FastEthernet、Loopback 接口、Null 接口、以及其它 Tunnel 接口。
interface-number	接口编号

【缺省配置】 没有配置本端地址。

【命令模式】 接口模式

【缺省级别】 2

【使用指导】 每一种 tunnel 都需要配置本端地址。
当指明本端地址为某接口的地址时，根据 tunnel mode 选择此接口的主 IP 地址。2 个自动隧道不允许配置相同

的本端地址。

【配置举例】 1：创建隧道接口。

```
Ruijie(config)# interface tunnel 1
```

2：设置隧道模式。

```
Ruijie(config-if)# tunnel mode ip
```

3：配置隧道本端地址。

```
Ruijie(config-if)# tunnel source 1.1.1.1
```

【检验方法】 1：使用 show interface tunnel 命令，可以查看隧道配置的本端地址。

【提示信息】 -

【常见错误】 -

【平台说明】 -

6.6 tunnel tos

配置外层传送协议 IPv4 的 ToS 字节。

tunnel tos number

取消配置。

no tunnel tos

【参数说明】

参数	描述
number	外层传送协议 IPv4 的 ToS 字节的值。取值范围是 0～255。

【缺省配置】 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。

【命令模式】 接口模式

【缺省级别】 2

【使用指导】 如果希望隧道的报文优先级高一些，可以使用 tunnel tos 命令来设置。

【配置举例】 1：创建隧道接口。

```
Ruijie(config)# interface tunnel 1
```

2：设置隧道模式。

```
Ruijie(config-if)# tunnel mode ip
```

3：配置隧道 tos。

```
Ruijie(config-if)# tunnel tos 100
```

【检验方法】 1：使用 show interface tunnel 命令，可以查看 tunnel tos 的值。

【提示信息】 -

【常见错误】 -

【平台说明】 -

6.7 tunnel ttl

配置 tunnel 接口的 ttl 值。
tunnel ttl hop-count

恢复缺省配置。
no tunnel ttl

【参数说明】

参数	描述
hop-count	用来指定 tunnel 接口的 ttl 值。范围是 1~255，缺省是 254。

【缺省配置】 254。

【命令模式】 接口模式

【缺省级别】 2

【使用指导】 由于 Tunnel 是点对点的链路，所以对于负载协议来说，在路由的时候看起来只有一跳（hop），但实际上传输协议的路由花费可能不止一跳。锐捷产品允许设置 Tunnel 的 TTL，也即设置 Tunnel 所发送的封装报文中传输协议报头 TTL 值。隧道中间节点路由器会递减传输协议报头中的 TTL 值，丢弃 TTL 为 0 的报文。

【配置举例】 1：创建隧道接口。

```
Ruijie(config)# interface tunnel 1
```

2：设置隧道模式。

```
Ruijie(config-if)# tunnel mode ip
```

3：配置隧道 ttl。

```
Ruijie(config-if)# tunnel ttl 100
```

【检验方法】 1：使用 show interface tunnel 命令，可以查看 tunnel 的 ttl 值。

【提示信息】 -

【常见错误】 -

6.8 tunnel 6rd br

设置 6rd 的 br IPv4 地址，该命令的 no 形式取消设置 br 的 IPv4 地址。

tunnel 6rd br ipv4-address

no tunnel 6rd br

【参数说明】

参数	描述
ipv4-address	IPv4 地址。

【缺省配置】 -

【命令模式】 接口模式

【缺省级别】 2

【使用指导】 配置 6rd relay 路由器的 IPv4 地址。

【配置举例】 1：配置隧道 6rd 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】 1：使用 **show interface tunnel** 命令，可以查看 tunnel 6rd 的 br 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
......
```

【提示信息】 -

【常见错误】 -

【平台说明】 交换机平台不支持

6.9 tunnel 6rd ipv4

设置 6rd 域的 IPv4 通用前缀和通用后缀长度，该命令的 no 形式取消设置前缀和后缀长度。

tunnel 6rd ipv4 prefix-length prefix-length suffix-length suffix-length

no tunnel 6rd ipv4

【参数说明】

参数	描述
prefix-length	IPv4 地址。
suffix-length	IPv4 通用后缀长度。

【缺省配置】 -

【命令模式】 接口模式

【缺省级别】 2

【使用指导】 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。

【配置举例】 1：设置 tunnel 100 的 6rd 域前缀和后缀长度

```
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】 1：使用 show interface tunnel 命令，可以查看 tunnel 6rd 的 ipv4 配置。

【提示信息】 -

【常见错误】 -

【平台说明】 交换机平台不支持

6.10 tunnel 6rd prefix

设置 6rd 域的 IPv6 前缀，该命令的 no 形式删除 6rd 域的 IPv6 前缀。

tunnel 6rd prefix ipv6-prefix prefix-length

no tunnel 6rd prefix

【参数说明】

参数	描述
ipv6-prefix	6rd 前缀。
prefix-length	6rd 前缀长度。

【缺省配置】 -

【命令模式】 接口模式

【缺省级别】 2

【使用指导】 配置 6rd 的前缀。该命令为使用 6rd 的必须配置，若不配置 6rd 前缀，6rd 隧道将不能 UP，配置前缀长度为 0 等价于删除 6rd 前缀。

【配置举例】 1：设置 tunnel 100 的 6rd 前缀。

```
Ruijie# configure terminal
Ruijie(config)# interface tunnel 100
Ruijie(config-if-Tunnel 100)# tunnel 6rd prefix 2001:da8::/32
```

【检验方法】 1：使用 show interface tunnel 命令，可以查看 tunnel 6rd 的 prefix 配置。

【提示信息】 -

【常见错误】 -

【平台说明】 交换机平台不支持

7 FPM

7.1 clear ip fpm counters

清除 FPM 处理 ipv4 报文丢包计数

clear ip fpm counters

【参数说明】

参数	描述
-	-

【命令模式】 特权模式

【缺省级别】 15

【使用指导】 -

【配置举例】 **-**

【提示信息】 -

【平台说明】 -

7.2 ip session direct-trans-disable

配置不允许在满流时可以不建流直接透传报文

ip session direct-trans-disable

恢复默认设置

no ip session direct-trans-disable

【参数说明】

参数	描述

【缺省配置】 AC，AP 产品缺省在流表满时，可以执行对新连接不建流，直接透传不做加速处理的策略。其它产品无本项配置

【命令模式】 全局配置模式

【缺省级别】 15

【使用指导】 -

【配置举例】 设置设备在满流时不允许不建流直接透传报文

```
Ruijie(config)# ip session direct-trans-disable
```

【检验方法】 -

【提示信息】 -

【常见错误】

【平台说明】 -

7.3 ip session tcp-loose

配置宽松 tcp 状态变迁检查

ip session tcp-loose

恢复默认设置

no ip session tcp-loose

【参数说明】

参数	描述
-	-

【缺省配置】 FW 设备缺省不做宽松 tcp 状态检查，无线产品和 EG 一样缺省执行宽松 tcp 状态变迁检查

【命令模式】 全局配置模式

【缺省级别】 15

【使用指导】 -

【配置举例】 -

【检验方法】 -

【提示信息】 -

【常见错误】

【平台说明】 -

7.4 ip session tcp-state-inspection-disable

配置不做 tcp 的状态变迁检查

ip session tcp-state-inspection-disable

恢复默认设置

no ip session tcp-state-inspection-disable

【参数说明】

参数	描述
-	-

【缺省配置】 缺省做 tcp 的状态跟踪

【命令模式】 全局配置模式

【缺省级别】 15

【使用指导】 -

【配置举例】 设置在设备号为 1 槽号为 2 的设备上面不做 tcp 的状态变迁检查

```
Ruijie(config)# ip session 1 2 tcp-state-inspection-disable
```

【检验方法】 -

【提示信息】 -

【常见错误】

【平台说明】 -

7.5 ip session tcp-state-inspection-enable

配置打开 tcp 的状态变迁检查

ip session tcp-state-inspection- enable

恢复默认设置

no ip session tcp-state-inspection- enable

【参数说明】

参数	描述

【缺省配置】 AC、AP 产品缺省关闭 tcp 的状态变迁检查，其它产品无本项配置

【命令模式】 全局配置模式

【缺省级别】 15

【使用指导】 -

【配置举例】 设置在设备开启 tcp 的状态变迁检查

```
Ruijie(config)# ip session tcp-state-inspection-enable
```

【检验方法】 -

【提示信息】 -

【常见错误】

【平台说明】 -

7.6 ip session threshold

配置流允许接收报文数

ip session threshold {**icmp-closed** | **icmp-started** | **rawip-closed** | **tcp-syn-sent** | **tcp-syn-receive** | **tcp-closed** | **udp-closed**} { *num* }

恢复默认设置

no ip session threshold {**icmp-closed** | **icmp-started** | **rawip-closed** | **tcp-syn-sent** | **tcp-syn-receive** | **tcp-closed** | **udp-closed**}

【参数说明】

参数	描述
icmp-closed	设置协议为 ICMP 状态为关闭的流的报文通过数，默认 10（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（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（1 - 2000000000）
tcp-syn-sent	设置协议为 TCP 状态为 syn-send 的流的报文通过数，10（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（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（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（1 - 2000000000）

num	设置的报文通过数

【缺省配置】 缺省使用的是默认值

【命令模式】 全局配置模式

【缺省级别】 15

【使用指导】 要使当前配置生效，需要现在对应的设备上面配置 **ip session track-state-strictly**

【配置举例】 -

【检验方法】

【提示信息】 -

【常见错误】

【平台说明】 -

7.7 ip session timeout

配置老化时间

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* }

恢复默认时间

no 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**}

【参数说明】

参数	描述
icmp-closed	设置协议为 ICMP 状态为关闭的流的消亡时间，默认 10s（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（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（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（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（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（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（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（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（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（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（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（10 - 120）
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（5 - 30）
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（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（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（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（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（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（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（10 - 300）
num	设置的消亡时间

【缺省配置】 缺省使用的是默认值

【命令模式】 全局配置模式

【缺省级别】 15

【使用指导】 -

【配置举例】 设置设备 1 槽号为 2 的设备上面的 tcp established 状态的流消亡时间为 600s

```
Ruijie(config)# ip session 1 2 timeout tcp-established 600
```

【检验方法】

【提示信息】 -

【常见错误】

【平台说明】 -

7.8 ip session track-state-strictly

配置做流状态报文水线检查

ip session track-state-strictly

恢复默认设置

no ip session track-state-strictly

【参数说明】

参数	描述
-	-

【缺省配置】 缺省不做流状态报文水线检查

【命令模式】 全局配置模式

【缺省级别】 15

【使用指导】 -

【配置举例】 设置设备号为 1 槽号为 2 的设备上面做流状态报文水线检查

```
Ruijie(config)# ip session 1 2 track-state-strictly
```

【检验方法】

【提示信息】 -

【常见错误】

【平台说明】 -

7.9 show ip fpm counters

查看 FPM 处理 ipv4 报文丢包计数

show ip fpm counters

【参数说明】

参数	描述
-	-

【命令模式】 特权模式

【缺省级别】 15

【使用指导】 使用该命令可以查看 FPM 处理 ipv4 报文时的丢包计数信息，上半部分是针对报文的丢包信息，下半部分是针对流的信息

【配置举例】 1：查看 FPM 处理 ipv4 报文丢包计数

```
Ruijie#sh ip fpm 1 2 counters
Dropped packet counters:
Count      Reason
0          Non-IPv4 packet
0          Bad IPv4 header length
0          Bad IPv4 total length
0          Fragment pkt
0          change flow state notify FW refuse
0          Bad IPv4 checksum
0          Invalid IPv4 address
0          Invalid TCP flags
0          Invalid TCP sequence
0          Invalid ICMP message type
0          Invalid icmp initial message type
54         Invalid tcp init flags
0          Invalid tcp connection state
0          Connect over config threshold
0          Connect has been terminated
0          Invalid egress fid
0          out of vfw session limit
0          Out of capability
<end>
Rejected or terminated connection counters:
Count      Reason
0          Out of life time
1968       Flow Terminated
0          Rejected by policy
```

<end>

字段解释：

字段	说明
count	计数
Reason	丢包原因

【提示信息】 -

【平台说明】 -

7.10 show ip fpm flows

查看 ipv4 报文的流信息

show ip fpm flows

【参数说明】

参数	描述
-	-

【命令模式】 特权模式

【缺省级别】 15

【使用指导】 使用该命令可以查看 ipv4 报文的流信息

【配置举例】 1：查看 ipv4 报文的流信息

```
EG：
Ruijie#show ip fpm flows
Pr  SrcAddr                          DstAddr                          SrcPort      DstPort
Vrf          SendBytes  RecvBytes  St    srcif                    dstif
ctrl_flag
```

字段解释：

字段	说明
Pr	协议
SrcAddr	源地址
DstAddr	目的地址
SrcPort	源端口
DstPort	目的端口
Vrf	源接口所属的 vrf
SendBytes	请求方向接收的报文字节数
RecvBytes	应答方向接收的报文字节数
St	流当前状态
srcif	源接口号
dstif	目的接口号
vfw_id	虚拟防火墙 id(只有 fw 卡设备上面有此项值)
ctrl_flag	流控制字段

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。

【提示信息】 -

【平台说明】 -

7.11 show ip fpm flows filter

筛选查看 ipv4 报文的流信息

show ip fpm flows filter *protocol saddr smask daddr dmask*

【参数说明】

参数	描述
protocol	ip 协议，取值范围 0 - 255
saddr	源 ip 地址，取值范围为所有 ip 地址
smask	源 ip 地址掩码，取值范围 1 - 32
daddr	目的 ip 地址，取值范围为所有 ip 地址
dmask	目的 ip 地址掩码，取值范围 1 - 32

【命令模式】 特权模式

【缺省级别】 15

【使用指导】 使用该命令可以筛选查看 ipv4 报文的流信息

【配置举例】 1：查看 ipv4 报文的流信息

```
EG：
Ruijie#show ip fpm flows filter 1 192.168.1.1 32 192.168.2.1 30
Pr  SrcAddr                          DstAddr                          SrcPort      DstPort
Vrf          SendBytes  RecvBytes  St    srcif                    dstif
ctrl_flag
```

字段解释：

字段	说明
Pr	协议
SrcAddr	源地址
DstAddr	目的地址
SrcPort	源端口
DstPort	目的端口
Vrf	源接口所属的 vrf
SendBytes	请求方向接收的报文字节数
RecvBytes	应答方向接收的报文字节数
St	流当前状态
srcif	源接口号
dstif	目的接口号
vfw_id	虚拟防火墙 id(只有 fw 卡设备上面有此项值)
ctrl_flag	流控制字段

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。

【提示信息】 -

【平台说明】 -

7.12 show ip fpm statistics

查看 ipv4 流表统计信息

show ip fpm statistics

【参数说明】

参数	描述
-	-

【命令模式】 特权模式

【缺省级别】 15

【使用指导】 使用该命令可以查看 ipv4 流表统计信息

【配置举例】 1：在 EG 设备上面查看 ipv4 流统计信息

```
Ruijie#show ip fpm statistics
The capacity of the flow table:150016.
Active flows num:109.
event count:65,
Fpm attribute is eg.
```

字段解释：

The capacity of the flow table	总流表数
Active flows num	活跃流表数
event count:65,	当前事件计数
Fpm attribute is eg	状态跟踪表是按照网关产品的特性实现

2 在无线设备上面查看 ipv4 流统计信息

```
Ruijie#show ip fpm statistics
The capacity of the flow table:150016.
Active flows num:109.
event count:65,
Fpm state inspection disable.
```

字段解释：

The capacity of the flow table	总流表数
Active flows num	活跃流表数
event count:65,	当前事件计数
Fpm state inspection disable	在当前产品上面状态跟踪功能是关闭的

【提示信息】 -

【平台说明】 -

8 NAT

8.1 address

配置一个 NAT 空地址池的地址范围

address *start-ip end-ip* [**match interface** *interface*]

删除地址池地址范围

no address *start-ip end-ip* [**match interface** *interface*]

配置一个 NAT 空地址池的地址范围

address interface *interface* [**match interface** *interface*]

删除地址池地址范围

no address interface *interface* [**match interface** *interface*]

【参数说明】

参数	描述
start-ip	一个地址块的起始 IP 地址。
end-ip	一个地址块的结束 IP 地址。
interface *interface*	用于 NAT 有多个 outside 口的情况。Pool 里定义的地址采用接口地址，一般用于接口地址有待协商 ,刚开始未知的情况。注意要与后面的 match interface interface 合用，而且两个 interface 要一致。否则可能引起 NAT 不通。
match interface *interface*	用于 NAT 有多个 outside 口的情况。当由路由决定了报文的出口后 ,NAT 再用这个出口来选取 pool 中与之相匹配的地址。

【缺省配置】 没有定义地址范围。

【命令模式】 NAT 地址池配置模式

【缺省级别】 14

【使用指导】 如果一个地址池需要定义多个地址范围，首先需要进入 NAT 地址池配置模式，然后进行 NAT 地址范围的定义。该命令不支持使用 AP 成员口进行配置

【配置举例】 1：创建了一个 mulnets 地址池，并定义了两个地址块。

```
Ruijie(config)# ip nat pool mulnets netmask 255.255.255.0
Ruijie(config-nat)# address 172.16.10.1 172.16.10.254
```

```
Ruijie(config-nat)# address 192.168.100.1 192.168.100.50
```

【提示信息】 1：如果该命令配置的结束 IP 地址小于起始 IP 地址，配置失败，提示：

```
% End address less than start address
```

2：如果该命令配置的起始 IP 地址和结束 IP 地址不处于同个网段，配置失败，提示：

```
% Start and end addresses on different subnets
```

3：如果该命令配置的起始 IP 地址和结束 IP 地址都是 0.0.0.0，配置失败，提示：

```
% Ip address 0.0.0.0 ~ 0.0.0.0 are invalid.
```

4：如果该命令使用 AP 成员口进行配置，配置失败，提示：

```
% Not permit ap member interface.
```

5：如果一个地址池的地址范围数量超过 100，配置失败，提示：

```
% Reach max pool addr range
```

6：如果配置该命令时，内存不足，配置失败，提示：

```
% Create address range fail
```

7：如果配置的地址范围使用的是接口地址且已经存在了，配置失败，提示：

```
% already use this interface's ip address,please delete and recreate
```

8：如果配置的地址范围已经存在了，配置失败，提示：

```
% Already exist this range,please delete and recreate
```

9：如果配置的地址范围使用的是接口地址且跟已有的地址发生重叠，配置失败，提示：

```
% Use interface's ip address overlap with existing range
```

10：如果配置地址范围跟已有的地址发生冲突，配置失败，提示：

```
%Start and end addresses overlap with existing range
```

11：如果删除的是带有接口的地址范围，且不存在，配置失败，提示：

```
% address range with interface not exist
```

12：如果删除的地址范围不存在，配置失败，提示：

```
% Address range x.x.x.x-x.x.x.x not exist
```

【常见错误】 -

【平台说明】 -

8.2 ip nat

要对一个接口收发的数据流量进行 NAT 转换

ip nat { **inside** | **outside** }

使一个接口不再应用 NAT

no ip nat { **inside** | **outside** }

【参数说明】

参数	描述
inside	表示该接口连接内部网络。
outside	表示该接口连接外部网络。

【缺省配置】 接口收发数据时，没有应用 NAT。

【命令模式】 接口配置模式

【缺省级别】 14

【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。因此支持 NAT 设备必须配置至少一个 inside 接口和一个 outside 接口。

【配置举例】 1：以下配置例子，可以将 192.168.12.0/24 内部主机，动态转换到全局地址 200.168.12.0/28 网段。内部网络的其它网段主机不允许做 NAT。

```
Ruijie#configure terminal
Ruijie(config)# interface GigabitEthernet 0/0
Ruijie(config-if-GigabitEthernet 0/0)# ip address 192.168.12.6 255.255.255.0
Ruijie(config-if-GigabitEthernet 0/0)# ip nat inside
Ruijie(config-if-GigabitEthernet 0/0)# exit
Ruijie(config)# interface GigabitEthernet 0/1
Ruijie(config-if-GigabitEthernet 0/1)# ip address 200.168.12.17 255.255.255.0
Ruijie(config-if-GigabitEthernet 0/1)# ip nat outside
Ruijie(config-if-GigabitEthernet 0/1)# exit
Ruijie(config)# ip nat pool net200 200.168.12.1 200.168.12.15 netmask 255.255.255.0
Ruijie(config)# ip nat inside source list 1 pool net200
Ruijie(config)# access-list 1 permit 192.168.12.0 0.0.0.255
```

【提示信息】 1：当在 lan 口配置 ip nat outside 时，配置失败，提示：

```
can't configure this command in lan interface
```

2：当在 wan 口配置 ip nat inside 时，配置失败，提示：

```
can't configure this command in wan interface
```

3：当在配置了 ip nat inside 的接口，执行 no ip nat outside，配置失败，提示：

```
% Interface is outside enabled, try <no ip nat outside>
```

4：当在配置了 ip nat outside 的接口，执行 no ip nat inside，配置失败，提示：

```
% Interface is inside enabled, try <no ip nat inside>
```

【常见错误】 -

【平台说明】 -

8.3 ip nat application

要实现 NAT 的特殊应用

ip nat application source list *list-num* **destination** *dest-ip* { **dest-change** *ip-addr* | **src-change** *ip-addr* }

ip nat application source list *list-num* **destination** { **tcp** *dest-ip port-num* | **udp** *dest-ip port-num*} { **dest-change** *ip-addr port-num* | **src-change** *ip-addr port-num* }

取消该特殊应用

no ip nat application source list *list-num* **destination** *dest-ip* { **dest-change** *ip-addr* | **src-change** *ip-addr* }

no ip nat application source list *list-num* **destination** { **tcp** *dest-ip port-num* | **udp** *dest-ip port-num* } { **dest-change** *ip-addr port-num* | **src-change** *ip-addr port-num* }

【参数说明】

参数	描述
list-num	内部本地地址访问列表,即报文的源地址匹配条件。
dest-ip	匹配内部全局地址，即报文的目的地址匹配条件，只有目的地址匹配该地址并且源地址匹配前面定义的访问列表，才会创建 NAT 转换记录。
tcp *dest-ip port-num*	匹配内部全局地址以及目的端口，只有 tcp 报文的目的地址和目的端口匹配这里定义的条件并且源地址匹配前面定义的访问列表，才会创建 NAT 转换记录。
udp *dest-ip port-num*	匹配内部全局地址以及目的端口，只有 udp 报文的目的地址和目的端口匹配这里定义的条件并且源地址匹配前面定义的访问列表，才会创建 NAT 转换记录。
dest-change *ip-addr port-num*	修改满足条件的报文的目的地址以及目的端口。
src-change *ip-addr*	修改满足条件的报文的源地址。

【缺省配置】 没有定义该规则。

【命令模式】 全局配置模式

【缺省级别】 14

【使用指导】 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。这时就可以用到这条命令。下面的例子就是用这条命令实现域名解析中继服务(DNS relay)。

【配置举例】 1：在以下配置中将允许内网 192.168.1.0 网段的主机将 DNS 服务器指向 NAT inside 接口的 IP：192.168.1.1，由支持 NAT 设备的 NAT 功能负责将内网主机的 DNS 请求转发给真正的 DNS 服务器 202.101.98.55，并将 DNS 应答报文转发给内网主机。使用 ip nat application 命令来实现该功能 ,语义就是如果有 :源地址满足 access-list 1、目的地址是 192.168.1.1、目的端口是 53 的 UDP 报文，则修改这个 IP 报文的目的地址为 202.101.98.55、目的端口为 53。

```
Ruijie#configure terminal
Ruijie(config)# interface GigabitEthernet 0/0
Ruijie(config-if-GigabitEthernet 0/0)# ip address 192.168.1.1 255.255.255.0
Ruijie(config-if-GigabitEthernet 0/0)# ip nat inside
Ruijie(config-if-GigabitEthernet 0/0)# exit
Ruijie(config)# interface GigabitEthernet 0/1
Ruijie(config-if-GigabitEthernet 0/1)# ip address 200.168.12.1 255.255.255.0
Ruijie(config-if-GigabitEthernet 0/1)# ip nat outside
Ruijie(config-if-GigabitEthernet 0/1.)# exit
Ruijie(config)# ip nat pool net200 200.168.12.2 200.168.12.10 netmask 255.255.255.0
Ruijie(config)# ip nat inside source list 1 pool net200
Ruijie(config)# access-list 1 permit 192.168.12.0 0.0.0.255
Ruijie(config)# ip nat application source list 1 destination udp 192.168.1.1 53 dest-change
202.101.98.55 53
Ruijie(config)# access-list 1 permit 192.168.1.0 0.0.0.255
```

【提示信息】 1 如果配置的规则已经存在，则配置失败，提示：

```
% Translation already exist
```

2 如果配置该命令时，出现内存不足，配置失败，提示：

```
% create nat rule fail
```

3 如果删除未配置成功的命令，则删除失败，提示：

```
% Translation not found
```

【常见错误】 -

【平台说明】 -

8.4 ip nat inside destination

要启用 NAT 内部目标地址转换

ip nat inside destination list *access-list-number* **pool** *pool-name* [**description** *description-text*]

关闭 NAT 内部目标转换

no ip nat inside destination list *access-list-number*

【参数说明】

参数	描述
list *access-list-number*	访问列表定义的是内部全局地址，如果外部网络访问列表中的地址，内部全局地址将会转换成 pool 中定义的内部本地地址。注意这里应该使用匹配目标 IP 为虚拟 IP 的 100-199 这个范围的扩展 ACL。
pool *pool-name*	地址池中定义了内部本地地址的空间，进行目标地址转换时，将会从中分配内部本地地址。
description *description-text*	（可选）规则描述信息，缺省无描述信息，*description-text* 为 1～60 个字符的字符串。

【缺省配置】 没有启用内部源地址转换。

【命令模式】 全局配置模式

【缺省级别】 14

【使用指导】 内部目标地址的转换，可以用来实现 TCP 的流量的负载均衡。当内部网络某台主机 TCP 流量负载过重时，可能需要多台主机进行 TCP 业务的均衡负载。这时，你可以考虑用 NAT 来实现 TCP 流量的负载均衡，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。但是对于其它的 IP 流量，不做任何的改变，除非 NAT 作了其它配置。

配置 NAT 实现 TCP 负载均衡，内部网络的地址可以是合法的全局地址，也可以是私有网络地址。但是虚拟主机地址必须为合法的全局地址。

【配置举例】 1 :以下配置例子 ,内部网络对外提供了一个虚拟主机地址 10.10.10.100 ,外部网络通过该地址访问 WWW 服务，内部局域网提供服务的实际上是两台地址为 10.10.10.1、10.10.10.2 的主机。NAT 转换时，采用轮询的方式实现负载均衡。

```
Ruijie#configure terminal
Ruijie(config)# interface GigabitEthernet 0/0
Ruijie(config-if-GigabitEthernet 0/0)# ip address 10.10.10.254 255.255.255.0
Ruijie(config-if-GigabitEthernet 0/0)# ip nat inside
Ruijie(config-if-GigabitEthernet 0/0)# exit
Ruijie(config)# interface GigabitEthernet 0/1
Ruijie(config-if-GigabitEthernet 0/1)# ip address 200.168.12.17 255.255.255.0
Ruijie(config-if-GigabitEthernet 0/1)# ip nat outside
```

```
Ruijie(config-if-GigabitEthernet 0/1)# exit
Ruijie(config)# ip nat pool net10 10.10.10.1 10.10.10.2 prefix-length 24 type rotary
Ruijie(config)# ip nat inside destination list 100 pool net10
Ruijie(config)# access-list 100 permit ip any host 10.10.10.100
```

【提示信息】 1：如果配置的规则已经存在，则配置失败，提示：

```
Translation with list xxx exist,please delete and recreate
```

2：如果配置该命令时，出现内存不足，配置失败，提示：

```
% create nat rule fail
```

3：如果删除未配置成功的命令，则删除失败，提示：

```
% Translation not found
```

4：如果配置的描述符长度超过 60，提示：

```
Description is more than 60 characters
```

【常见错误】 -

【平台说明】 -

8.5 ip nat inside source

要启用内部源地址 NAT

ip nat inside source list *access-list-number* { **interface** *interface-type interface-number* | **pool** *pool-name* } [**overload**] [**description** *description-text*]

ip nat inside source static *local-ip global-ip* [**match** *interface-type interface-number* | **netmask** *mask*][**permit-inside**]
[**description** *description-text*]
ip nat inside source static *local-ip* **interface** *interface-type interface-number* [**permit-inside**] [**description** *description-text*]

ip nat inside source static { **tcp** *local-ip local-port* | **udp** *local-ip local-port* } *global-ip global-port* [**match** *interface-type interface-number* | **netmask** *mask*] [**permit-inside**] [**description** *description-text*]
ip nat inside source static { **tcp** *local-ip local-port* | **udp** *local-ip local-port* } **interface** *interface-type interface-number global-port* [**permit-inside**] [**description** *description-text*]

ip nat inside source static { **tcp** *local-ip* **port-range** *local-port1 local-port2* | **udp** *local-ip* **port-range** *local-port1 local-port2*} *global-ip* **port-range** *global-port1 global-port2* [**match** *interface-type interface-number* | **netmask** *mask*] [**permit-inside**] [**description** *description-text*]

ip nat inside source static { **tcp ip-range** *local-ip1 local-ip2 local-port* | **udp ip-range** *local-ip1 local-ip2 local-port*} **ip-range** *global-ip1 global-ip2 global-port* [**match** *interface-type interface-number* | **netmask** *mask*] [**permit-inside**] [**description** *description-text*]

ip nat inside source static { **tcp ip-range** *local-ip1 local-ip2* **port-range** *local-port1 local-port2* | **udp ip-range** *local-ip1 local-ip2* **port-range** *local-port1 local-port2*} **ip-range** *global-ip1 global-ip2* **port-range** *global-port1 global-port2* [**match** *interface-type interface-number* | **netmask** *mask*] [**permit-inside**] [**description** *description-text*]

ip nat inside source static { **tcp** *local-ip* **port-range** *local-port1 local-port2* | **udp** *local-ip* **port-range** *local-port1 local-port2*} **interface** *interface-type interface-number* **port-range** *global-port1 global-port2* [**permit-inside**] [**description** *description-text*]

关闭内部源地址 NAT

no ip nat inside source list *access-list-number*

no ip nat inside source static *local-ip global-ip*

no ip nat inside source static *local-ip* **interface** *interface-type interface-number*

no ip nat inside source static { **tcp** *local-ip local-port* | **udp** *local-ip local-port* } *global-ip global-port*

no ip nat inside source static { **tcp** *local-ip local-port* | **udp** *local-ip local-port* } **interface** *interface-type interface-number global-port*

no ip nat inside source static { **tcp** *local-ip* **port-range** *local-port1 local-port2* | **udp** *local-ip* **port-range** *local-port1 local-port2*} *global-ip* **port-range** *global-port1 global-port2* [**match** *interface-type interface-number* | **netmask** *mask*] [**permit-inside**]

no ip nat inside source static { **tcp ip-range** *local-ip1 local-ip2 local-port* | **udp ip-range** *local-ip1 local-ip2 local-port*} **ip-range** *global-ip1 global-ip2 global-port* [**match** *interface-type interface-number* | **netmask** *mask*] [**permit-inside**]

no ip nat inside source static { **tcp ip-range** *local-ip1 local-ip2* **port-range** *local-port1 local-port2* | **udp ip-range** *local-ip1 local-ip2* **port-range** *local-port1 local-port2*} **ip-range** *global-ip1 global-ip2* **port-range** *global-port1 global-port2* [**match** *interface-type interface-number* | **netmask** *mask*] [**permit-inside**]

no ip nat inside source static { **tcp** *local-ip* **port-range** *local-port1 local-port2* | **udp** *local-ip* **port-range** *local-port1 local-port2*} **interface** *interface-type interface-number* **port-range** *global-port1 global-port2* [**permit-inside**]

【参数说明】

参数	描述
list *access-list-number*	本地地址访问列表。只有源地址匹配该访问列表的流量，才会创建 NAT 转换记录。
interface *interface-type interface-number*	利用 outside 接口的全局地址做 NAPT（网络地址端口转换），也叫扩展 NAT。
pool *pool-name*	利用地址池中的全局地址做 NAT。
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。
static *local-ip global-ip*	定义简单静态 NAT。local-ip 为本地地址，global-ip 为全局地址。
static *protocol*	定义扩展静态 NAT。protocol 可以为 TCP 或 UDP。
local-port	本地地址的服务端口号。TCP 或 UDP 的端口号，每种服务都一般对应一个服务端口。
global-port	全局地址的服务端口号。外部网络通过该端口访问内部网络主机的服务。该端口号可以与 local-port 不同。
ip-range *local-ip1 local-ip2*	定义连续的 IP 映射。*local-ip1* 为内网连续起始地址， *local-ip2* 为内网连续结束地址。
ip-range *global-ip1 global-ip2*	定义连续的 IP 映射。*global-ip1* 为外网连续起始地址， *global-ip2* 为外网连续结束地址。
port-range *local-port1 local-port2*	定义连续的端口映射。*local-port1* 为内网连续起始端口， *local-port2* 为内网连续结束端口。
port-range *global-port1 global-port2*	定义连续的端口映射。*global-port1* 为外网连续起始端口， *global-port2* 为外网连续结束端口。
permit-inside	只出现在 ip nat inside source static 命令中，用于允许内网用户以 global-ip 访问 local-ip 的主机。
match *interface-type interface-number*	指定出接口（智能 DNS 中使用）。
netmask *mask*	网段到网段地址。
description *description-text*	（可选）规则描述信息，缺省无描述信息，*description-text* 为 1～60 个字符的字符串。

【缺省配置】 没有内部源地址 NAT 发生。

【命令模式】 全局配置模式

【缺省级别】 14

【使用指导】 当内部网络的 IP 地址为私有地址，又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。

对于一些网吧或企业单位，如果仅仅为了上网访问外部网络的资源，如浏览网页、收发邮件、下载文件等，而本身不对外部网络提供网络服务，可以直接利用 outside 接口的 IP 地址做全局地址，以 NAPT 方式实现地址转换。如果不作 NAT，分配私有地址的内部网络即使物理上与外部网络实现了互联，但相互之间却互通不了，因为外部网络没有私有地址的网络路由。

对于提供服务的内部主机，需要配置静态 NAT 或 NAPT。考虑到服务提供的可持续性，尽量不要利用 outside 接口的地址做静态 NAPT，因为该地址为与 ISP 互联地址，变换的可能性很大。通常情况下，内网用户访问这些内部主机提供的服务，只要用内网 IP 就可以了。但有些特殊的应用服务，要求内网用户以全局 IP 访问该服务。这时配置内部源地址静态 NAT 或内部源地址静态 NAPT 时，需要加入 permit-inside 关键字。此时最好也要在 inside 口上配上 no ip redirects，防止 inside 口发重定向的报文。

当内部有多个连续的主机或者连续的端口，需要对外网提供服务，可以配置 IP 连续或者端口连续的配置。

【配置举例】 1：以下配置例子，可以将 192.168.12.0/24 内部主机，动态转换到全局地址 200.168.12.0/28 网段。内部网络的其它网段主机不允许做 NAT。

```
Ruijie#configure terminal
Ruijie(config)# interface GigabitEthernet 0/0
Ruijie(config-if-GigabitEthernet 0/0)# ip address 192.168.12.6 255.255.255.0
Ruijie(config-if-GigabitEthernet 0/0)# ip nat inside
Ruijie(config-if-GigabitEthernet 0/0)# exit
Ruijie(config)# interface GigabitEthernet 0/1
Ruijie(config-if-GigabitEthernet 0/1)# ip address 200.168.12.17 255.255.255.0
Ruijie(config-if-GigabitEthernet 0/1)# ip nat outside
Ruijie(config-if-GigabitEthernet 0/1)# exit
Ruijie(config)# ip nat pool net200 200.168.12.1 200.168.12.15 prefix-length 28
Ruijie(config)# ip nat inside source list 1 pool net200
Ruijie(config)# access-list 1 permit 192.168.12.0 0.0.0.255
```

【提示信息】 1：当配置规则的待匹配 IP 地址已经映射过，则配置失败，提示：

```
x.x.x.x already mapped (x.x.x.x -> y.y.y.y)
```

2：当配置规则的待匹配 IP 地址映射成接口地址，且对应的接口不存在，配置失败，提示：

```
x.x.x.x already mapped
```

3：当配置规则的待转换的目标 IP 地址已经映射过，配置失败，提示：

```
x.x.x.x.x already mapped (y.y.y.y -> x.x.x.x)
```

4：当配置规则的待转换的目标接口已经映射过，配置失败，提示：

```
Interface xxx already mapped
```

5：当配置的 acl 已经映射过，则配置失败，提示：

```
Translation with list xxx exist,please delete and recreate
```

6：如果配置该命令时，出现内存不足，配置失败，提示：

```
% create nat rule fail
```

7：如果生成附属规则时，出现内存不足，配置失败，提示：

```
% create attach rule fail
```

8：如果对配置 permit-inside 命令生成的附属规则时，出现内存不足，配置失败，提示：

```
% create permit_inside attach rule fail
```

9：如果删除未配置成功的命令，则删除失败，提示：

```
% Translation not found
```

10：如果配置的描述符长度超过 60，提示：

```
Description is more than 60 characters
```

【常见错误】 -

【平台说明】 -

8.6 ip nat keepalive

要配置发送 NAT 本机地址免费 arp 报文的间隔

ip nat keepalive [*keealive_out*]

不发送 NAT 本机地址的免费 arp 报文

no ip nat keepalive

default ip nat keepalive

【参数说明】

参数	描述
keealive_out	发送 nat 本机地址免费 arp 报文的间隔

【缺省配置】 不发送 nat 本机地址的免费 arp 报文

【命令模式】 全局配置模式

【缺省级别】 14

【使用指导】 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，可以通过定期发送免费 arp 报文解决

【配置举例】 1：以下配置例子，设置发送 nat 本机地址的时间间隔为 10s

```
Ruijie#configure terminal
Ruijie(config)# ip nat keepalive 10
```

【提示信息】 -

【常见错误】 -

【平台说明】 -

8.7 ip nat outside source

要启用外部源地址 NAT

ip nat outside source list *access-list-number* **pool** *pool-name*

ip nat outside source static *global-ip local-ip*

ip nat outside source static { **tcp** *global-ip global-port* | **udp** *global-ip global-port* } *local-ip local-port*

关闭外部源地址 NAT

no ip nat outside source list *access-list-number*

no ip nat outside source static *global-ip local-ip*

no ip nat outside source static { **tcp** *global-ip global-port* | **udp** *global-ip global-port* } *local-ip local-port*

【参数说明】

参数	描述
list *access-list-number*	本地地址访问列表。只有源地址匹配该访问列表的流量，才会创建 NAT 转换记录。
pool *pool-name*	利用地址池中的全局地址做 NAT。
static *local-ip global-ip*	定义简单静态 NAT。local-ip 为本地地址，global-ip 为全局地址。
static *protocol*	定义扩展静态 NAT。protocol 可以为 TCP 或 UDP。
local-port	本地地址的服务端口号。TCP 或 UDP 的端口号，每种服务都一般对应一个服务端口。
global-port	全局地址的服务端口号。外部网络通过该端口访问内部网络主机的服务。该端口号可以与 local-port 不同。

【缺省配置】 没有外部源地址 NAT 发生。

【命令模式】 全局配置模式

【缺省级别】 14

【使用指导】 外部源地址 NAT 转换主要应用在重叠地址空间的地址转换。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，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。

重叠地址 NAT 配置，其实分为两个部分内容：1）内部源地址 NAT 配置；2）外部源地址 NAT 配置，只有与内部网络地址重叠的外部网络需要配置外部源地址转换，外部源地址转换可以采用静态 NAT 配置或动态 NAT 配置。

当内部网络建设时分配了非注册的全球 IP 地址，实现与互联网连接时，必然会发生地址重叠的情况。内部网络一般采用域名访问外部网络主机，因此支持 NAT 设备还必须支持 DNS 报文的 NAT。

【配置举例】 1：以下配置例子，内部网络 192.168.12.0/24 与外部网络的地址重叠。经过转换后，内部主机可以通过 192.168.12.0/24 网络地址访问外部网 192.168.12.0/24 网段的主机。

```
Ruijie#configure terminal
Ruijie(config)# interface GigabitEthernet 0/0
Ruijie(config-if-GigabitEthernet 0/0)# ip address 192.168.12.55 255.255.255.0
Ruijie(config-if-GigabitEthernet 0/0)# ip nat inside
Ruijie(config-if-GigabitEthernet 0/0)# exit
Ruijie(config)# interface Serial 10/1
Ruijie(config-if-GigabitEthernet 0/1)# ip address 192.168.10.1 255.255.255.0
Ruijie(config-if-GigabitEthernet 0/1)# ip nat outside
Ruijie(config-if-GigabitEthernet 0/1)# encapsulation ppp
Ruijie(config-if-GigabitEthernet 0/1)# exit
Ruijie(config)#ip nat pool net200 200.168.12.1 200.168.12.15 prefix-length 28
Ruijie(config)#ip nat pool net192 192.168.12.1 192.168.12.254 prefix-length 24
Ruijie(config)#ip nat inside source list  1 pool net200
Ruijie(config)#ip nat outside source list 1 pool net192
Ruijie(config)#access-list 1 permit 92.168.12.0 0.0.0.255
Ruijie(config)#ip route 192.168.12.0 255.255.255.0 192.168.100.2
```

【提示信息】 1：当配置规则的待匹配 IP 地址已经映射过，则配置失败，提示：

```
6.6.6.6 already mapped (6.6.6.6 -> 5.5.25.4)
```

2：当配置规则的待转换的目标 IP 地址已经映射过，配置失败，提示：

```
5.5.25.4 already mapped (6.6.6.6 -> 5.5.25.4)
```

3：当配置的 acl 已经映射过，则配置失败，提示：

```
Translation with list 1 exist,please delete and recreate
```

4：如果配置该命令时，出现内存不足，配置失败，提示：

```
% create nat rule fail
```

5：如果删除未配置成功的命令，则删除失败，提示：

```
% Translation not found
```

【常见错误】 -

【平台说明】 -

8.8 ip nat pool

要定义 NAT 的地址池

ip nat pool *pool-name start-ip end-ip* { **netmask** *netmask* | **prefix-length** *prefix-length* } [**type rotary**]

ip nat pool *pool-name* { **netmask** *netmask* | **prefix-length** *prefix-length* } [**type rotary**]

ip nat pool *pool-name* { **netmask** *netmask* | **prefix-length***prefix-length* } [**type rotary**] [**hardware**]

删除地址池

no ip nat pool *pool-name*

【参数说明】

参数	描述
pool-name	NAT 地址池名字。
start-ip	NAT 地址池的起始 IP 地址。
end-ip	NAT 地址池的结束 IP 地址。
netmask *netmask*	NAT 地址池的地址网络掩码。
type	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。
hardware	NPE80 独有，硬件类型的地址池，使用这种类型的 NAT 规则由硬件处理，可以达到较大的连接建立速率。

【缺省配置】 没有地址池被定义。

【命令模式】 全局配置模式

【缺省级别】 14

【使用指导】 如果一个地址池需要定义多个地址块，则需要先创建一个空地址池，后定义地址范围。

【配置举例】 1：以下配置例子，创建了名字为 net192 的地址池，起始地址为 192.168.12.1，结束地址为 192.168.12.254，网

络掩码长度为 24 个比特位。

```
Ruijie#configure terminal
Ruijie(config)# ip nat pool net192 192.168.12.1 192.168.12.254 prefix-length 24
```

【提示信息】 1：如果配置的地址池的掩码是 0.0.0.0，配置失败，提示

```
% netmask can not be 0
```

2：如果该命令配置的结束 IP 地址小于起始 IP 地址，配置失败，提示：

```
% End address less than start address
```

3：如果该命令配置的起始 IP 地址和结束 IP 地址不处于同个网段，配置失败，提示：

```
% Start and end addresses on different subnets
```

4：如果该命令配置的起始 IP 地址和结束 IP 地址都是 0.0.0.0，配置失败，提示：

```
% Ip address 0.0.0.0 ~ 0.0.0.0 are invalid.
```

5：如果进入相应地址池模式的 pool 类型和已配置 pool 类型不同，配置失败，提示：

```
%Cannot redefine pool type, please delete and recreate.
```

6：如果配置的地址池的数量超过 100，配置失败，提示：

```
% Exceed the max pool count
```

7：如果配置的地址池的名字超过 32，配置失败，提示

```
% Length of pool name must be no more than 32 charceters
```

8：如果配置该命令时，内存不足，配置失败，提示：

```
%create pool fail
```

9：如果配置该命令时，内存不足，配置失败，提示：

```
% create pool fail for alloc range mem
```

10：如果待删除的地址池不存在，删除失败，提示：

```
% pool xxx not exist
```

【常见错误】 -

【平台说明】 -

8.9 ip nat translation

要配置 NAT 支持的 alg

ip nat translation { **dns** [**ttl** *ttl_time*] | **ftp** [**port** *port_num*] | **tftp** | **pptp** | **h323** | **rtsp** | **sip** }

删除 NAT 支持的 alg

no ip nat translation { **dns** | **ftp** | **tftp** | **pptp** | **h323** | **rtsp** | **sip**}

【参数说明】

参数	描述
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，

【缺省配置】 打开支持 dns/ftp/tftp/pptp/h323/rtsp/sip 的 alg

【命令模式】 全局配置模式

【缺省级别】 14

【使用指导】 ALG（Application Level Gateway，应用层网关），主要完成对应用层报文的处理。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
例如，FTP 应用就由数据连接和控制连接共同完成，而且数据连接的建立动态地由控制连接中的载荷字段信息决定，这就需要应用层协议检测来完成载荷字段信息的转换，以保证后续数据连接的正确建立。

【配置举例】 1：以下配置例子，设置 dns 的缓存时间为 30s。

```
Ruijie#configure terminal
Ruijie(config)# ip nat translation dns ttl 30
```

2：以下配置例子，对 ftp 应用支持 25 端口。

```
Ruijie#configure terminal
Ruijie(config)# ip nat translation ftp port 25
```

【提示信息】 1：成功删除对应的 alg，提示：

```
unregister xxx alg success!
```

2：删除对应的 alg 失败，提示：

```
unregister xxx alg fail!
```

3：成功支持对应的 alg，提示：

```
register xxx alg success!
```

4：支持对应的 alg 失败，提示：

```
register xxx alg fail!
```

【常见错误】 -

【平台说明】 -

8.10 show ip nat translations

显示 NAT 转换记录。

show ip nat translations [*acl_num*] [**icmp** | **tcp** | **udp**] [**verbose**]

【参数说明】

参数	描述
icmp	只显示 icmp 的 nat 转换记录。
tcp	只显示 tcp 的 nat 转换记录。
udp	只显示 udp 的 nat 转换记录。
acl_num	acl 号,只支持扩展 acl，用于过滤显示内容
verbose	显示更详细的 NAT 转换记录信息。

【命令模式】 特权模式

【缺省级别】 1

【使用指导】 该命令可以显示 IP NAT 转换记录的概要情况，如协议，内部全局地址及端口号、内部本地地址及端口号、外部本地地址及端口号、外部全局地址及端口号。跟 **verbose** 参数可以显示更详细的信息 ,包括设置的各项 timeout 时间，该记录剩余时间、记录标记等。

【配置举例】 1：显示 NAT 转换记录：

```
Ruijie# show ip nat translations verbose
timeout for NAT TCP flows: 86400
timeout for NAT TCP flows after a FIN or RST: 60
timeout for NAT TCP flows after a SYN : 60
timeout for NAT UDP flows: 300
timeout for NAT DNS flows: 60
timeout for NAT ICMP flows: 60
Pro Inside global      Inside local       Outside local      Outside global timeout vrf
tcp 192.168.5.103:1987 192.168.211.21 :1987 211.67.71.7    :80    211.67.71.7:80 timeout=85139 1
udp 192.168.5.103:1041 192.168.211.183:1041 202.101.98.55  :53 202.101.98.55:53 timeout=38 1
```

字段解释：

字段	说明
Pro	协议类型。 “udp”表示该转换记录为 UDP 转换记录；

	“tcp”表示该转换记录为 TCP 转换记录。“icmp”表示该转换记录为 ICMP 转换记录。
Inside global	内部全局地址及端口号。
Inside local	内部本地地址及端口号。
Outside local	外部本地地址及端口号。
Outside global	外部全局地址及端口号。
timeout	表示该 NAT 转换记录离超时还有多长时间，单位秒。
vrf	该连接所在 vrf。

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。

【提示信息】 -

【常见错误】 -

【平台说明】 -

9 MLLB

9.1 load-monitor uplink

配置 MLLB 模块线路上行负载监控。
load-monitor uplink

恢复 MLLB 模块线路上行负载监控。
no load-monitor

恢复缺省配置。
default load-monitor

【参数说明】

参数	描述
-	-

【缺省配置】 默认负载监控线路下行方向

【命令模式】 全局模式

【缺省级别】 14

【使用指导】 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，则可能会上行流量大于下行流量，这时可以切换为用上行流量计算带宽率和阈值。

【配置举例】 1：配置 MLLB 模块负载线路上行监控功能。

```
Ruijie(config)#load-monitor uplink
```

2：取消 MLLB 模块负载线路上行监控功能。

```
Ruijie(config)#no load-monitor
```

【检验方法】 1：使用 **show mllb configure** 命令，可以查看 MLLB 模块配置信息。

【提示信息】 1：配置 MLLB 模块链路上行负载监控功能，则提示：

```
Ruijie(config)#load-monitor uplink
multi-link load balance monitor to uplink.
```

2：恢复设备 MLLB 模块负载线路下行监控功能，则提示：

```
Ruijie(config)#no load-monitor
```

```
multi-link load balance monitor to default.
```

【常见错误】 -

【平台说明】 -

9.2 mllb detect domain add

添加 mllb 需要探测的域名。
mllb detect domain add *domain-name*

删除所有 mllb 探测的域名。
no mllb detect domain add

删除指定的 mllb 探测的域名。
no mllb detect domain add *domain-name*

【参数说明】

参数	描述
domain-name	域名名称，最长支持 63 个字符

【缺省配置】 缺省没有域名配置

【命令模式】 全局模式

【缺省级别】 14

【使用指导】 如果要探测某个域名，则通过该命令进行添加。

【配置举例】 1：添加 mllb 需要探测的域名。
Ruijie(config)#mllb detect domain add www.baidu.com

2、删除 mllb 需要探测的域名。
Ruijie(config)#no mllb detect domain add www.baidu.com

【检验方法】 1：使用 **show mllb detect configure** 命令，可以查看当前已经添加的探测域名。

【提示信息】 1：如果设备添加 mllb 探测的域名，则提示：

```
Ruijie(config)#mllb detect domain add www.baidu.com
Success to add mllb detect domain name: www.baidu.com.
```

2：如果设备删除 mllb 探测的域名，则提示：

```
Ruijie(config)#no mllb detect domain add www.baidu.com
Success to delete mllb detect domain name: www.baidu.com.
```

【常见错误】 1：域名已经添加过了

Fail to add domain name:www.baidu.com, since it's exist.

2：域名长度超过 63 个字节

%The length of Domain name(111111111111111111111111111111111111111111111111111111111111111) should less than 63.

3：已经达到了添加域名的容量限制

Fail to add domain name:www.baidu.com, since overflow capacity.

【平台说明】 -

9.3 mllb detect domain dns-server

添加 mllb 需要探测的 dns 服务器以及接口。

mllb detect domain dns-server *dns-ip interface* [**source-ip** *src-ip*]

删除所有 mllb 探测的 dns 服务器与接口。

no mllb detect domain dns-server

删除指定的 mllb 探测的 dns 服务器与接口。

no mllb detect domain dns-server *dns-ip interface*

【参数说明】

参数	描述
dns-ip	dns 服务器的 ip 地址，ip 地址类型
interface	接口名称
src-ip	指定探测报文的源 ip 地址

【缺省配置】 缺省没有配置 dns 服务器与接口

【命令模式】 全局模式

【缺省级别】 14

【使用指导】 如果要探测探测某个 dns 域名服务器，则通过该命令进行添加。

【配置举例】 1：添加 mllb 需要探测的 dns 服务器以及指定接口与源 ip 地址。

Ruijie(config)#mllb detect domain dns-server 114.114.114.114 GigabitEthernet 0/4 source-ip 192.168.197.16

2、删除 mllb 需要探测的 dns 服务器以及指定接口。
Ruijie(config)#no mllb detect domain dns-server 114.114.114.114 GigabitEthernet 0/4

【检验方法】 1：使用 **show mllb detect configure** 命令，可以查看当前已经添加的探测 dns 服务器。

【提示信息】 1：如果设备添加 mllb 探测的 dns 服务器，则提示：

```
Ruijie(config)#mllb detect domain dns-server 114.114.114.114 GigabitEthernet 0/4 source-ip
192.168.197.16
Success to add.
```

2：如果设备删除 mllb 探测的域名，则提示：

```
Ruijie(config)#no mllb detect domain dns-server 114.114.114.114 GigabitEthernet 0/4
Success to delete.
```

【常见错误】 1：dns 服务器已经添加过了
Fail to add, since it's exist.

2：已经达到了添加 dns 服务器的容量限制
Fail to add, since overflow capacity.

【平台说明】 -

9.4 mllb detect domain enable

开启 mllb 探测域名功能，根据设定的时间周期轮询进行检测与探测域名的可访问性。
mllb detect domain enable

关闭 mllb 探测域名功能，不自动进行探测
no mllb detect domain enable

恢复缺省配置
default mllb detect domain enable

【参数说明】

参数	描述
-	-

【缺省配置】 关闭 mllb 探测域名功能。

【命令模式】 全局模式

【缺省级别】 14

【使用指导】 如果要使用 mllb 自动定时探测域名功能，则开启该命令。

【配置举例】 1：开启 mllb 探测域名功能。
Ruijie(config)#mllb detect domain enable

2、关闭 mllb 自动探测域名并记录数据库功能。
Ruijie(config)#no mllb detect domain enable

【检验方法】 1：使用 **show mllb detect configure** 命令，可以查看 mllb 探测域名功能是启用还是关闭。

【提示信息】 1：如果设备开启 mllb 探测域名功能，则提示：

```
Ruijie(config)#mllb detect domain enable
mllb detect domain is enabled.
```

2：如果设备关闭 mllb 探测域名功能，则提示：

```
Ruijie(config)#no mllb detect domain enable
mllb detect domain is disabled!
```

【常见错误】 -

【平台说明】 -

9.5 mllb detect domain interval

配置 mllb 探测域名功能探测周期时间。
mllb detect domain interval *interval-time*

恢复 mllb 探测域名功能探测周期时间。
no mllb detect domain interval

恢复缺省配置。
default mllb detect domain interval

【参数说明】

参数	描述
interval-time	周期范围在 1-1440（单位：分钟）

【缺省配置】 探测周期为 5 分钟

【命令模式】 全局模式

【缺省级别】 14

【使用指导】 mllb 探测域名功能默认每隔一定时间根据配置的待探测域名以及 dns 服务器、出接口，进行探测。如果用户想修改默认值，可以通过此命令调整。

λ 间隔时间受每次探测耗时影响，非绝对间隔时间，即默认 5 分钟探测间隔，本次探测发出后，一般在 5 分钟后才能进行第二次的探测，而非刚好 5 分钟进行第二次探测。

【配置举例】 1：配置 mllb 探测域名功能的探测周期为 10 分钟。

```
Ruijie(config)#mllb detect domain interval 10
```

2：恢复 mllb 探测域名功能探测周期时间。

```
Ruijie(config)#no mllb detect domain interval
```

【检验方法】 1：使用 **show mllb detect configure** 命令，可以查看 mllb 探测域名功能配置信息。

【提示信息】 1：配置 mllb 域名探测周期为 10 分钟，则提示：

```
Ruijie(config)#mllb detect domain interval 10
mllb detect domain interval set to 10 minute.
```

2：恢复 mllb 域名探测默认周期，则提示：

```
Ruijie(config)#no mllb detect domain interval
mllb detect domain interval set to default!
```

【常见错误】 -

【平台说明】 -

9.6 mllb detect network enable

开启 mllb 检测当前网络功能，根据设定的时间周期轮询进行检测，并记录数据库。
mllb detect network enable

关闭 mllb 检测当前网络功能，不记录数据库
no mllb detect network enable

恢复缺省配置
default mllb detect network enable

【参数说明】

参数	描述
-	-

【缺省配置】 关闭 mllb 检测网络记录数据库功能。

【命令模式】 全局模式

【缺省级别】 14

【使用指导】 如果要使用 mllb 自动定时检测网络并记录数据库功能，则开启该命令。

λ 功能开启后，会自动定时检测当前网络的延迟大小，包括 tcp、udp 等，同时还会统计当前网络中的半开连接数（报文发出未收到应答），以及各种选路模块作用的流量大小。

【配置举例】 1：开启 mllb 检测网络功能。

Ruijie(config)#mllb detect network enable

2、关闭 mllb 检测网络功能。

Ruijie(config)#no mllb detect network enable

【检验方法】 1：使用 **show mllb detect configure** 命令，可以查看 mllb 检测网络功能是启用还是关闭。

【提示信息】 1：如果设备开启 mllb 检测网络功能，则提示：

```
Ruijie(config)#mllb detect network enable
mllb detect network is enabled.
```

2：如果设备关闭 mllb 探测域名功能，则提示：

```
Ruijie(config)#no mllb detect network enable
mllb detect network is disabled!
```

【常见错误】 -

【平台说明】 -

9.7 mllb detect network interval

配置 mllb 检测网络功能检测周期时间。

mllb detect network interval *interval-time*

恢复 mllb 检测网络功能检测周期时间。

no mllb detect network interval

恢复缺省配置。

default mllb detect network interval

【参数说明】

参数	描述
interval-time	周期范围在 1-1440（单位：分钟）

【缺省配置】 探测周期为 5 分钟

【命令模式】 全局模式

【缺省级别】 14

【使用指导】 mllb 检测网络功能默认每隔 5 分钟自动对当前网络进行检测。如果用户想修改默认值，可以通过此命令调整。

【配置举例】 1：配置 mllb 检测网络功能的检测周期为 10 分钟。

```
Ruijie(config)#mllb detect network interval 10
```

2：恢复 mllb 检测网络功能检测周期时间。

```
Ruijie(config)#no mllb detect network interval
```

【检验方法】 1：使用 **show mllb detect configure** 命令，可以查看 mllb 检测网络功能配置信息。

【提示信息】

1：配置 mllb 网络检测周期为 10 分钟，则提示：

```
Ruijie(config)#mllb detect network interval 10
mllb detect network interval set to 10 minute.
```

2：恢复 mllb 域名探测默认周期，则提示：

```
Ruijie(config)#no mllb detect network interval
mllb detect network interval set to default!
```

【常见错误】 -

【平台说明】 -

9.8 mllb enable

开启 MLLB 模块。

mllb enable

关闭 MLLB 模块。

no mllb enable

恢复缺省配置。

default mllb enable

【参数说明】

参数	描述
-	-

【缺省配置】 关闭 MLLB 模块。

【命令模式】 全局模式

【缺省级别】 14

【使用指导】 如果要求设备支持负载均衡功能，则需要开启 MLLLB 模块。

⚠ MLLB 模块负载均衡仅适用于 ECMP 路由出口。

【配置举例】 1：启动 MLLB 模块功能。

```
Ruijie(config)# mllb enable
```

2：关闭 MLLB 模块功能。

```
Ruijie(config)#no mllb enable
```

【检验方法】 1：使用 **show mllb configure** 命令，可以查看 MLLB 模块是启用还是关闭。

【提示信息】 1：如果设备开启 MLLB 功能，则提示：

```
Ruijie(config)#mllb enable
multi-link bandwidth balance is enabled.
```

2：如果设备关闭 MLLB 模块，则提示：

```
Ruijie(config)#no mllb enable
multi-link load balance is disabled!
```

【常见错误】 -

【平台说明】 -

9.9 mllb first-choice

配置 MLLB 模块出口优先。

mllb first-choice *interface-type interface-number*

取消 MLLB 模块出口优先。
no mllb first-choice

恢复缺省配置。
default mllb first-choice

【参数说明】

参数	描述
interface-type interface-number	接口名

【缺省配置】 未配置出口优先。

【命令模式】 全局模式

【缺省级别】 14

【使用指导】 当所有出口都超过阈值时，每个出口都无法按照预定的策略选路，这时可以配置优先选择某一个出口。

first-choice 只针对默认路由 ECMP 生效，并且其出口必须是 ECMP 中的出口。

【配置举例】 1：配置 MLLB 模块出口优先走 GigabitEthernet 0/1 口。

```
Ruijie(config)# mllb first-choice GigabitEthernet 0/1
```

【检验方法】 1：使用 **show mllb configure** 命令，可以查看 MLLB 模块配置信息。

【提示信息】 1：配置 MLLB 模块出口优先功能，则提示：

```
Ruijie(config)#mllb first-choice GigabitEthernet 0/1
multi-link load balance first-choice set to GigabitEthernet 0/1
```

【常见错误】 配置 first-choice 接口不是 ECMP 中的出口。

【平台说明】 -

9.10 mllb interface

配置 mllb 接口指定均衡权重值。
mllb interface *inteface* **weight** *weight-num*

删除 mllb 接口指定均衡权重值。
no mllb interface *inteface* **weight**

恢复 mllb 默认接口均衡权重值。

default mllb interface *inteface* **weight**

【参数说明】

参数	描述
Interface	接口名称
weight-num	均衡权重值，范围在 1- 40000000（单位 kilobits）

【缺省配置】 默认均衡权重值为接口下行带宽

【命令模式】 全局模式

【缺省级别】 14

【使用指导】 mllb 默认均衡权重值为接口下行带宽，可以通过该命令人为指定均衡权重值，以实现更改指定接口的带宽利用率。如接口 GigabitEthernet 0/4 下行带宽为 100Mbits，其默认均衡权重值为 100000kilobits。需要提升其带宽利用率，可以更改权重值为 150000 kilobits；需要降低其带宽利用率，可以更改权重值为 50000 kilobits。

【配置举例】 1：配置接口均衡权重值为 100Mbits。

```
Ruijie(config)#mllb interface GigabitEthernet 0/4 weight 100000
```

2：恢复接口均衡权重值为默认接口下行带宽。

```
Ruijie(config)#no mllb interface GigabitEthernet 0/4 weight
```

【检验方法】 1：使用 **show run | include mllb** 命令，可以查看 mllb 指定接口均衡权重值信息。

【提示信息】

```
1：配置 mllb 接口权重值为 100Mbits，则提示：
Ruijie(config)# mllb interface GigabitEthernet 0/4 weight 100000
mllb interface GigabitEthernet 0/4 weight set to 100000.
```

2：恢复 mllb 接口均衡权重值，则提示：

```
Ruijie(config)#no mllb interface GigabitEthernet 0/4 weight 100000
clear mllb interface GigabitEthernet 0/4 weight!
```

【常见错误】 -

【平台说明】 -

9.11 mllb load-interval

配置 MLLB 模块负载更新周期。

mllb load-interval *refresh-time*

恢复 MLLB 模块负载更新周期。
no mllb load- interval

恢复缺省配置。
default mllb load- interval

【参数说明】

参数	描述
refresh-time	周期更新范围在 3-30（单位：秒）

【缺省配置】 负载更新周期为 5 秒

【命令模式】 全局模式

【缺省级别】 14

【使用指导】 多链路负载均衡默认每隔 5 秒计算一次接口的负载，并判断是否会超过阈值。如果用户想修改默认值，可以通过此命令调整。

【配置举例】 1：配置 MLLB 模块负载更新周期为 10 秒。

```
Ruijie(config)#mllb load-interval 10
```

2：取消 MLLB 模块负载更新功能。

```
Ruijie(config)#no mllb load-interval
```

【检验方法】 1：使用 **show mllb configure** 命令，可以查看 MLLB 模块配置信息。

【提示信息】

```
1：配置 MLLB 模块负载更新周期为 10 秒，则提示：
Ruijie(config)# mllb load-interval 10
mllb load interval set to 10 seconds.
```

2：恢复设备 MLLB 模块负载更新周期功能，则提示：

```
Ruijie(config)#no mllb load-interval
mllb load interval set to default.
```

【常见错误】 -

【平台说明】 -

9.12 mllb load-sharing original

配置 MLLB 模块基于源 IP 功能，仅针对带块策略生效，同一个源 IP 只从一个出口发送。
mllb load-sharing original

取消 MLLB 模块基于源 IP 功能。
no mllb load-sharing

恢复缺省配置。
default mllb load-sharing

【参数说明】

参数	描述
-	-

【缺省配置】 基于源 IP+目标 IP

【命令模式】 全局模式

【缺省级别】 14

【使用指导】 某些应用基于缺省源 IP+目标 IP 散列可能走多个出口，导致重连、闪断等，基于源 IP 散列能够解决该问题。

【配置举例】 1：配置 MLLB 模块基于源 IP 功能。

```
Ruijie(config)#mllb load-sharing original
```

2：取消 MLLB 模块基于源 IP 功能。

```
Ruijie(config)#no mllb load-sharing
```

【检验方法】 1：使用 **show mllb configure** 命令，可以查看 MLLB 模块配置信息。

【提示信息】 1：配置 MLLB 模块源 IP 功能，则提示：

```
Ruijie(config)#mllb load-sharing original
mllb load sharing set to original
```

2：如果取消设备 MLLB 模块基于源 IP 功能，则提示：

```
Ruijie(config)#no mllb load-sharing
mllb load sharing set to default
```

【常见错误】 -

【平台说明】 -

9.13 mllb policy

配置 MLLB 模块负载策略。

mllb policy {**bandwidth** | **load**}

恢复 MLLB 模块负载策略。

no mllb policy

恢复缺省配置。

default mllb policy

【参数说明】

参数	描述
-	-

【缺省配置】 MLLB 模块基于带宽策略。

【命令模式】 全局模式

【缺省级别】 14

【使用指导】

如果启用 MLLB 带宽策略，则必须配置出口带宽大小。

【配置举例】 1：配置 MLLB 模块带宽策略功能。

```
Ruijie(config)# mllb policy bandwidth
```

2：配置 MLLB 模块负载策略功能。

```
Ruijie(config)# mllb policy load
```

【检验方法】 1：使用 **show mllb configure** 命令，可以查看 MLLB 模块配置信息。

【提示信息】

```
1：配置 MLLB 模块基于链路带宽策略，则提示：
Ruijie(config)#mllb policy bandwidth
multi-link load balance policy set to bandwidth mode.
```

【常见错误】 1：配置带宽策略模式，但未配置出口带宽。

【平台说明】 -

9.14 mllb threshold

配置 MLLB 模块负载阈值。

mllb threshold { *percent-upper* | [**lower** *percent-lower*] }

恢复 MLLB 模块链路负载阈值。

no mllb threshold

恢复缺省配置。

default mllb threshold

【参数说明】

参数	描述
threshold *percent-upper*	上限阈值 （单位：%，范围：1-100）
lower *percent-lower*	下限阈值 （单位：%，范围：1-100）

【缺省配置】 出口阈值上限/下限分别为 100

【命令模式】 全局模式

【缺省级别】 14

【使用指导】 链路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。链路负载阈值为百分比数值，取值范围是 1-100 的整数，阈值下限小于或等于上限。

【配置举例】 1：配置 MLLB 模块负载上行阈值为 95，下行为 85。

```
Ruijie(config)#mllb threshold 95 lower 85
```

2：配置 MLLB 模块负载上行阈值为 95。

```
Ruijie(config)#mllb threshold 95
```

3：配置 MLLB 模块负载下行阈值为 85。

```
Ruijie(config)#mllb threshold lower 85
```

【检验方法】 1：使用 **show mllb configure** 命令，可以查看 MLLB 模块配置信息。

【提示信息】 1：配置 MLLB 模块负载阈值上限和下限，则提示：

```
Ruijie(config)#mllb threshold 95 lower 85
multi-link load balance threshold set 95 lower to 85.
```

2：如果设备配置负载阈值上限为 85，下限为 95，则提示：

```
Ruijie(config)#mllb threshold 85 lower 95
multi-link load balance threshold set failed.
```

【常见错误】 1：配置负载阈值上限小于下限。

【平台说明】 -

9.15 show mllb configure

查看 MLLB 配置信息。

show mllb configure

【参数说明】

参数	描述
-	-

【命令模式】 特权模式、全局模式、接口模式

【缺省级别】 14

【使用指导】 此命令用来查看设备 MLLB 模块配置信息。

【配置举例】 1：查看设备 MLLB 模块配置信息。

```
Ruijie#show mllb configure
multi-link load balance configure:
multi-link load balance state: enable
multi-link load balance policy: load
multi-link load balance load-interval: 5
multi-link load balance threshold: 90 lower: 90
multi-link load balance load-monitor: down-link
multi-link load balance first-choice set to GigabitEthernet 0/1 is up
multi-link load balance load-sharing no original
```

字段解释：

字段	说明
state	MLLB 模块状态
policy	MLLB 模块负载策略
load -interval	负载更新周期
threshold	负载阈值上限
lower	负载阈值下限
load-monitor	负载监控方向

load-sharing	负载源 IP

【提示信息】 1：如果设备上没有开启 MLLB 模块。

```
Ruijie#show mllb configure
multi-link load balance configure:
multi-link load balance state: disable
```

2：如果开启了 MLLB 模块开关，未配置出口优先。

```
Ruijie#show mllb configure
multi-link load balance configure:
multi-link load balance state: enable
multi-link load balance policy: load
multi-link load balance load-interval: 5
multi-link load balance threshold: 90 lower: 90
multi-link load balance load-monitor: down-link
multi-link load balance load-sharing no original
```

3：如果开启了 MLLB 模块开关，且配置出口优先。

```
Ruijie#show mllb configure
multi-link load balance configure:
multi-link load balance state: enable
multi-link load balance policy: load
multi-link load balance load-interval: 5
multi-link load balance threshold: 90 lower: 90
multi-link load balance load-monitor: down-link
multi-link load balance first-choice set to GigabitEthernet 0/1 is up
multi-link load balance load-sharing no original
```

【平台说明】 -

9.16 show mllb detect configure

查看 MLLB 探测功能配置信息。

show mllb detect configure

【参数说明】

参数	描述
-	-

【命令模式】 特权模式、全局模式、接口模式

【缺省级别】 14

【使用指导】 此命令用来查看设备 MLLB 探测模块配置信息。

【配置举例】 1：查看设备 MLLB 探测模块配置信息。

```
Ruijie#show mllb detect configure
mllb detect configure:
network detect state: true
network detect interval: 300 seconds
domain detect state: true
domain detect interval: 300 seconds
domain detect name:
  domain name: www.cqu.edu.cn
  domain name: www.baidu.com
  total domain number: 2
 domain detect dns server:
  dns server and interface: 114.114.114.114 GigabitEthernet 0/4 source-ip 192.168.197.16
  dns server and interface: 192.168.58.110 GigabitEthernet 0/4
  total dns server and interface number: 2
has storage: true
```

字段解释：

字段	说明
state	MLLB 自动检测网络与探测域名的开启状态
interval	MLLB 自动检测网络与探测域名的周期时间间隔
name	探测的域名
dns server	探测的 dns 域名服务器以及指定的接口
domain number	当前配置域名的个数
interface number	当前配置 dns 域名服务器与接口的个数
storage	当前设备是否存在存储设备，不存在则不会记录探测结果至数据库

【提示信息】 1：如果设备上开启了 MLLB 检测网络模块。

```
Ruijie#show mllb configure
```

其中的字段为：

```
network detect state: true
```

2：如果开启了 MLLB 探测域名模块开关。

其中的字段为：

```
domain detect state: true
```

3：如果添加了 www.baidu.com 域名进行探测。

```
Ruijie#show mllb configure
其中的字段为：
  domain name: www.baidu.com
4：如果添加了 dns 服务器 8.8.8.8 进行探测，且指定源 ip 地址为 192.168.197.16。
Ruijie#show mllb configure
其中的字段为：
  dns server and interface: 8.8.8.8 GigabitEthernet 0/4 source-ip 192.168.197.16
```

【平台说明】 -

9.17 show mllb detect domain database from

查看 MLLB 探测域名数据库信息。

show mllb detect domain database from *begin-year begin-month begin-day begin-hour* [**to** *end-year end-month end-day end-hour*]

【参数说明】

参数	描述
begin-year	时间段起始年
begin-month	时间段起始月
begin-day	时间段起始日
begin-hour	时间段起始时分秒
end-year	时间段结束年
end-month	时间段结束月
end-day	时间段结束日
end-hour	时间段结束时分秒

【命令模式】 特权模式、全局模式、接口模式

【缺省级别】 14

【使用指导】 此命令用来查看 MLLB 探测域名数据库信息。

【配置举例】 1：查看 MLLB 探测域名数据库信息。

```
Ruijie#show mllb detect domain database from 2016 1 21 0:0:0
Date & Time               Domain                          Dns-server          Ifindex
Parse-ip            Dns-time   Tcp-connect     Http_get
2016-01-21 00:00:07       www.cqu.edu.cn                  192.168.58.110      5
222.178.10.35       1          65              59/1
2016-01-21 00:00:07       www.baidu.com                   192.168.58.110      5
115.239.211.112     1          23              25/1
2016-01-21 00:00:07       www.gov.cn                      192.168.58.110      5
```

```
117.26.144.16          0          18              197/1
```

字段解释：

字段	说明
Date & Time	域名探测的时间
Domain	探测的域名
Dns-server	配置的 dns 服务器 ip 地址
Ifindex	指定的出接口索引
Parse-ip	域名解析到的 ip 地址
Dns-time	dns 域名解析消耗的时间，单位毫秒
Tcp-connect	tcp 连接消耗的时间，单位毫秒
Http_get	http get 请求消耗的时间，单位毫秒。/后面的数值，1 表示 get ok，0 表示 get 请求异常

【提示信息】 1：只指定起始时间查看 MLLB 探测域名数据库信息。

```
Ruijie#show mllb detect domain database from 2016 1 21 11:28:5
Date & Time               Domain                          Dns-server          Ifindex
Parse-ip            Dns-time    Tcp-connect     Http_get
2016-01-21 11:28:05       www.jd.com                      114.114.114.114      5
180.96.12.1          33          0               0/0
2016-01-21 11:28:05       weibo.com                       114.114.114.114      5
180.149.134.141      25          50              51/1
2016-01-21 11:28:05       www.qq.com                      114.114.114.114      5
14.17.32.211         34          21              67/1
2016-01-21 11:28:05       www.tmall.com                   114.114.114.114      5
218.67.61.254        31          17              10/1
Ruijie#
```

2：同时指定起始时间与结束时间查看 MLLB 探测域名数据库信息。

```
Ruijie#show mllb detect domain database from 2016 1 21 11:28:6 to 2016 1 21 11:28:36
Date & Time               Domain                          Dns-server          Ifindex
Parse-ip            Dns-time    Tcp-connect     Http_get
2016-01-21 11:28:36       www.cqu.edu.cn                  192.168.58.110       5
222.178.10.35        0           65              80/1
2016-01-21 11:28:36       www.baidu.com                   192.168.58.110       5
115.239.211.112      0           28              38/1
2016-01-21 11:28:36       www.gov.cn                      192.168.58.110       5
117.26.144.16        20          27              32/1
```

Ruijie#

【平台说明】 -

9.18 show mllb detect domain database select

查看 MLLB 探测域名数据库指定信息。

show mllb detect domain database select { **dns-server** *dns-ip* | **domain** domain-name | **error** | **interface** *interface* } { **error from** | **from**} *begin-year begin-month begin-day begin-hour* [**to** *end-year end-month end-day end-hour*]

【参数说明】

参数	描述
dns-ip	dns 服务器 ip 地址
domain-name	域名名称
interface	接口名称
begin-year	时间段起始年
begin-month	时间段起始月
begin-day	时间段起始日
begin-hour	时间段起始时分秒
end-year	时间段结束年
end-month	时间段结束月
end-day	时间段结束日
end-hour	时间段结束时分秒

【命令模式】 特权模式、全局模式、接口模式

【缺省级别】 14

【使用指导】 此命令用来查看 MLLB 探测域名数据库指定信息。

【配置举例】 1：查看 MLLB 探测域名数据库，探测失败的信息。

```
Ruijie#show mllb detect domain database select error from 2016 1 21 0:0:0
Date & Time               Domain                          Dns-server          Ifindex
Parse-ip            Dns-time   Tcp-connect     Http_get
2016-01-21 00:00:39       www.baidu.com                   114.114.114.114     5
115.239.210.27      33         0               0/0
2016-01-21 00:01:44       www.baidu.com                   114.114.114.114     5
115.239.210.27      22         0               0/0
2016-01-21 00:03:20       www.baidu.com                   192.168.58.110      5
115.239.210.27      0          0               0/0
```

字段解释：

字段	说明
Date & Time	域名探测的时间
Domain	探测的域名

Dns-server	配置的 dns 服务器 ip 地址
Ifindex	指定的出接口索引
Parse-ip	域名解析到的 ip 地址，为 0.0.0.0 表示解析失败
Dns-time	dns 域名解析消耗的时间，单位毫秒
Tcp-connect	tcp 连接消耗的时间，单位毫秒，为 0 表示连接失败
Http_get	http get 请求消耗的时间，单位毫秒。/后面的数值，1 表示 get ok，0 表示 get 请求异常

【提示信息】 1：查看指定起始时间的所有探测失败的信息。

```
Ruijie#show mllb detect domain database select error from 2016 1 21 12:0:0
Date & Time               Domain                          Dns-server          Ifindex
Parse-ip            Dns-time   Tcp-connect     Htp_get
2016-01-21 12:00:18       www.baidu.com                   114.114.114.114     5
115.239.210.27      34         0               0/0
2016-01-21 12:00:21       weibo.com                       114.114.114.114     5
180.149.134.141     41         0               0/0
2016-01-21 12:00:53       www.baidu.com                   192.168.58.110      5
115.239.210.27      0          0               0/0
```

2：查看指定 dns 服务器的探测信息。

```
Ruijie#show mllb detect domain database select dns-server 192.168.58.110 from 2016 1 21 12:0:0
Date & Time               Domain                          Dns-server          Ifindex
Parse-ip            Dns-time   Tcp-connect     Htp_get
2016-01-21 12:00:53       www.cqu.edu.cn                  192.168.58.110      5
222.178.10.35       1          72              82/1
2016-01-21 12:00:53       www.baidu.com                   192.168.58.110      5
115.239.210.27      0          0               0/0
2016-01-21 12:00:53       www.gov.cn                      192.168.58.110      5
122.228.84.36       1          41              49/1
```

3：查看指定域名名称的探测信息

```
Ruijie#show mllb detect domain database select domain www.qq.com from 2016 1 21 12:0:0
Date & Time               Domain                          Dns-server          Ifindex
Parse-ip            Dns-time   Tcp-connect     Htp_get
2016-01-21 12:00:21       www.qq.com                      114.114.114.114     5
59.37.96.63         43         40              38/1
2016-01-21 12:00:53       www.qq.com                      192.168.58.110      5
14.17.42.40         3          26              27/1
2016-01-21 12:01:25       www.qq.com                      114.114.114.114     5
14.17.32.211        35         27              171/1
2016-01-21 12:02:00       www.qq.com                      192.168.58.110      5
```

```
14.17.42.40          0          30              0/0
```

4：查看指定接口的探测信息

```
Ruijie#show mllb detect domain database select interface gigabitEthernet 0/4 from 2016 1 21 12:0:0
Date & Time              Domain                          Dns-server          Ifindex
Parse-ip            Dns-time   Tcp-connect     Htp_get
2016-01-21 12:00:18      www.cqu.edu.cn                  114.114.114.114     5
222.178.10.35       39         61              73/1
2016-01-21 12:00:18      www.baidu.com                   114.114.114.114     5
115.239.210.27      34         0               0/0
2016-01-21 12:00:18      www.gov.cn                      114.114.114.114     5
122.228.84.36       41         35              38/1
```

5、查看指定域名名称的探测失败信息

```
Ruijie#show mllb detect domain database select domain www.qq.com error from 2016 1 21 12:0:0
Date & Time              Domain                          Dns-server          Ifindex
Parse-ip            Dns-time   Tcp-connect     Htp_get
2016-01-21 12:02:00      www.qq.com                      192.168.58.110      5
14.17.42.40         0          30              0/0
2016-01-21 12:05:47      www.qq.com                      114.114.114.114     5
0.0.0.0             0          0               0/0
2016-01-21 12:28:39      www.qq.com                      114.114.114.114     5
14.17.42.40         38         0               0/0
```

【平台说明】 -

9.19 show mllb detect domain name

查看 MLLB 探测指定域名信息。

show mllb detect domain name *domain-name dns-ip* [*interface* [**source-ip** *src-ip*]]

【参数说明】

参数	描述
domain-name	待探测的域名
dns-ip	指定从该 dns 服务器进行域名解析
interface	指定从该接口出去进行探测
src-ip	指定探测报文的源 ip 地址

【命令模式】 特权模式、全局模式、接口模式

【缺省级别】 14

【使用指导】 此命令用来查看 MLLB 探测指定域名信息。

【配置举例】 1：查看 MLLB 探测指定域名信息。

```
Ruijie#show mllb detect domain name www.qq.com 114.114.114.114 gigabitEthernet 0/4 source-ip 192.168.197.16
Input parameter: domain www.qq.com, dns server ip 114.114.114.114, out interface GigabitEthernet 0/4.
Output:
  dns parse ok: true.
  tcp connect ok: true.
  http get ok: true.
  dns parse ip: 140.206.160.207.
  dns parse delay: 24ms, tcp connect delay: 21ms, http get delay: 21ms.
```

字段解释：

字段	说明
dns parse ok	dns 域名解析是否成功
tcp connect ok	tcp 连接是否建立成功
http get ok	http get 请求是否得到正确回应
dns parse ip	dns 域名服务器解析该域名得到的第一个 ip 地址
delay	延迟多少毫秒 ,依次为 dns 解析 ,tcp 连接 ,与 http get 请求的延迟

【提示信息】 1：如果 MLLB 探测指定的域名成功。

```
Ruijie#show mllb detect domain name www.ruijie.com.cn 114.114.114.114 gigabitEthernet 0/4
Input parameter: domain www.ruijie.com.cn, dns server ip 114.114.114.114, out interface GigabitEthernet 0/4.
Output:
  dns parse ok: true.
  tcp connect ok: true.
  http get ok: true.
  dns parse ip: 61.240.149.178.
  dns parse delay: 25ms, tcp connect delay: 30ms, http get delay: 101ms.
Ruijie#
```

2：如果 MLLB 探测指定的域名失败。

```
Ruijie#show mllb detect domain name www.ruijie.com.cn 8.8.8.8 gigabitEthernet 0/4
Input parameter: domain www.ruijie.com.cn, dns server ip 8.8.8.8, out interface GigabitEthernet 0/4.
Output:
  dns parse ok: false.
  tcp connect ok: false.
```

```
  http get ok: false.
  dns parse ip: 0.0.0.0.
  dns parse delay: 0ms, tcp connect delay: 0ms, http get delay: 0ms.
```

Ruijie#

【平台说明】 -

9.20 show mllb detect network

查看 MLLB 检测网络信息。

show mllb detect network {**interface** [*interface-name*] | *source-ip source-ip-mask destination-ip destination-ip-mask* | **database** {**select interface** *select-interface-name* **from** | **from**}} *begin-year begin-month begin-day begin-hour* [**to** *end-year end-month end-day end-hour*]

【参数说明】

参数	描述
interface-name	指定检测网络的接口名称
source-ip	指定检测网络的源 ip 地址
source-ip-mask	指定检测网络的源 ip 掩码
destination-ip	指定检测网络的目的 ip 地址
destination-ip-mask	指定检测网络的目的 ip 掩码
select-interface-name	查看检测网络数据库指定接口的信息
begin-year	时间段起始年
begin-month	时间段起始月
begin-day	时间段起始日
begin-hour	时间段起始时分秒
end-year	时间段结束年
end-month	时间段结束月
end-day	时间段结束日
end-hour	时间段结束时分秒

【命令模式】 特权模式、全局模式、接口模式

【缺省级别】 14

【使用指导】 此命令用来查看 MLLB 检测网络信息。

【配置举例】 1：查看 MLLB 检测当前网络信息。

```
Ruijie#show mllb detect network interface

The analysis of half connection:
  Interface                        Half(ALL total)    Half(TCP total)    Half(UDP total)
```

```
Half(DNS total)
  GigabitEthernet 0/4              2/11              0/7               2/4               0/0
  GigabitEthernet 0/5              0/1               0/0               0/0               0/0

The analysis of delay:
  Interface                        Total delay(Min/Aver/Max/Count)     TCP
delay(Min/Aver/Max/Count)      UDP delay(Min/Aver/Max/Count)       DNS delay(Min/Aver/Max/Count)
  GigabitEthernet 0/4              0/35/180/9                          0/15/60/7
0/105/180/2                      0/0/0/0
  GigabitEthernet 0/5              0/0/0/0                             0/0/0/0
0/0/0/0                          0/0/0/0

The analysis of route flows:
  Interface                        Route type       Total(Output/Input)Mbit
TCP(Output/Input)                UDP(Output/Input)                    DNS(Output/Input)
  GigabitEthernet 0/4              ref_ip           64/168                                64/160
0/0                              0/0
  GigabitEthernet 0/5              ref_ip           0/0                                   0/0
0/0                              0/0
Ruijie#
```

字段解释：

字段	说明
Interface	所探测的接口名称
Half(ALL total)	所有协议的半开连接数以及总连接数
Half(TCP total)	tcp 的半开连接数以及 tcp 总连接数
Half(UDP total)	udp 的半开连接数以及 udp 总连接数
Half(DNS total)	dns 应用的半开连接数以及 dns 总连接数
Total delay	所有协议的延迟大小，依次为：最小，平均，最大，计数。延迟单位为毫秒
TCP delay	tcp 的延迟大小，依次为：最小，平均，最大，计数。延迟单位为毫秒
UDP delay	udp 的延迟大小，依次为：最小，平均，最大，计数。延迟单位为毫秒
DNS delay	dns 应用的延迟大小，依次为：最小，平均，最大，计数。延迟单位为毫秒
Route type	参与选路的选路模块名称
Total(Output/Input)Mbit	所有协议的流量信息，依次为上行流量，下行流量。流量的单位为 Mbit
TCP(Output/Input)	tcp 的流量信息，依次为上行流量，下行流量。流量的单位为 Mbit

UDP(Output/Input)	udp 的流量信息，依次为上行流量，下行流量。流量的单位为 Mbit
DNS(Output/Input)	dns 应用的流量信息，依次为上行流量，下行流量。流量的单位为 Mbit

2：查看 MLLB 检测网络数据库信息

```
Ruijie#show mllb detect network database from 2016 3 10 10:0:0
Date & Time                Interface       Type                                    Total
TCP                  UDP                   DNS
2016-03-10 10:00:13        Gi0/4           half-connect-flow-count(unknow/all)     3/14
0/5                  3/9                   0/2
                                           delay(min/aver/max/count)ms             0/51/180/11
0/34/150/5           0/66/180/6            0/25/40/2
                                           ref_ip-(output/input)Mbit               64/176
64/160               0/8                   0/0
```

字段解释：

字段	说明
Date & Time	探测网络的时间
Interface	探测网络的接口
Type	数据呈现的类型，包括半开连接数、延迟信息、选路流量信息
Total	所有协议的信息
TCP	tcp 协议的信息
UDP	udp 协议的信息
DNS	dns 协议的信息

【提示信息】 1：查看指定接口的当前网络检测信息。

```
Ruijie#show mllb detect network interface gigabitEthernet 0/4

The analysis of half connection:
  Interface                       Half(ALL total)    Half(TCP total)    Half(UDP total)
Half(DNS total)
  GigabitEthernet 0/4             4/22               0/7                4/15               0/8

The analysis of delay:
  Interface                       Total delay(Min/Aver/Max/Count)    TCP
delay(Min/Aver/Max/Count)      UDP delay(Min/Aver/Max/Count)      DNS delay(Min/Aver/Max/Count)
  GigabitEthernet 0/4             0/24/180/18                        0/22/60/7
0/25/180/11                       0/1/10/8

The analysis of route flows:
```

```
  Interface                        Route type       Total(Output/Input)Mbit
TCP(Output/Input)                  UDP(Output/Input)                  DNS(Output/Input)
  GigabitEthernet 0/4              ref_ip           64/168                            64/160
0/0                                0/0
Ruijie#
```

2：查看指定源 ip 的当前网络检测信息。

```
Ruijie#show mllb detect network 192.169.255.100 255.255.255.255 0.0.0.0 0.0.0.0

The analysis of half connection:
  Interface                        Half(ALL total)    Half(TCP total)    Half(UDP total)
Half(DNS total)
  GigabitEthernet 0/4              3/17               0/7                3/10               0/4
  GigabitEthernet 0/5              0/1                0/0                0/0                0/0

The analysis of delay:
  Interface                        Total delay(Min/Aver/Max/Count)     TCP
delay(Min/Aver/Max/Count)      UDP delay(Min/Aver/Max/Count)      DNS delay(Min/Aver/Max/Count)
  GigabitEthernet 0/4              0/32/180/14                        0/22/60/7
0/42/180/7                         0/7/10/4
  GigabitEthernet 0/5              0/0/0/0                            0/0/0/0
0/0/0/0                            0/0/0/0

The analysis of route flows:
  Interface                        Route type       Total(Output/Input)Mbit
TCP(Output/Input)                  UDP(Output/Input)                  DNS(Output/Input)
  GigabitEthernet 0/4              ref_ip           64/168                            64/160
0/0                                0/0
  GigabitEthernet 0/5              ref_ip           0/0                               0/0
0/0                                0/0
Ruijie#
```

3：查看指定接口检测网络的数据库信息

```
Ruijie#show mllb detect network database select interface gigabitEthernet 0/5 from 2016 3 10 10:0:0
Date & Time               Interface       Type                                    Total
TCP                  UDP                  DNS
2016-03-10 10:50:19       Gi0/5           half-connect-flow-count(unknow/all)     0/1
0/0                  0/0                  0/0
                                          delay(min/aver/max/count)ms             0/0/0/0
0/0/0/0              0/0/0/0              0/0/0/0
                                          ref_ip-(output/input)Mbit               0/0
```

```
0/0                    0/0                    0/0
Ruijie#
```

【平台说明】 -

9.21 show mllb statistics

查看 MLLB 负载均衡出口统计信息。

show mllb statistics

【参数说明】

参数	描述
-	-

【命令模式】 特权模式、全局模式、接口模式

【缺省级别】 14

【使用指导】 此命令用来查看设备 MLLB 模块负载均衡出口统计信息。

【配置举例】 1：查看设备 MLLB 模块出口统计信息。

```
Ruijie# show mllb statistics
Interface                   Packets   Flows
--------------------------  --------  --------
GigabitEthernet 0/1         6750      879
GigabitEthernet 0/2         6580      871
```

字段解释：

字段	说明
Interface	接口名
Packets	报文数目统计
Flows	新建流信息统计

【提示信息】 1：如果设备上没有开启 MLLB 模块。

```
Ruijie#show mllb statistics
Interface                   Packets   Flows
--------------------------  --------  --------
GigabitEthernet 0/1         0         0
GigabitEthernet 0/2         0         0
```

2：如果开启了 MLLB 模块开关。

```
Ruijie# show mllb statistics
Interface                   Packets   Flows
```

```
-------------------------  --------  --------
GigabitEthernet 0/1        6750      879
GigabitEthernet 0/2        6580      871
```

【平台说明】 -

10 WAN-IP

10.1 wan-ip enable

开启多 WAN 同网段功能总开关。

wan-ip enable

关闭多 WAN 同网段功能。

no wan-ip enable

【参数说明】

参数	描述
-	-

【缺省配置】 **缺省无配置**

【命令模式】 全局模式

【缺省级别】 14

【使用指导】 此命令用于多 WAN 同网段的总开关。

【配置举例】 1：开启总开关。

```
Ruijie(config)# wan-ip enable
```

【检验方法】 使用 **show wan-ip config** 命令，可以查看本模块的配置信息。

【提示信息】 -

【常见错误】 无

【平台说明】 11.1（pj33）以及其之后的 NBR 产品

10.2 wan-ip map

配置地址转换规则。

wan-ip map *ip-address1* **nexthop** *ip-address2*

删除地址转换规则。

no wan-ip map *ip-address1* **nexthop** *ip-address2*

【参数说明】

参数	描述
ip-address1	运营商分配的 ip
ip-address2	运营商网关

【缺省配置】 无规则。

【命令模式】 接口模式

【缺省级别】 14

【使用指导】 配置地址转换规则前，必须配置 wan-ip enable 后，功能才生效。

【配置举例】 1：开启多 WAN 同网段总开关

```
Ruijie(config)# wan-ip enable
```

2：配置多 WAN 同网段规则。

```
Ruijie(config)#
Ruijie(config)# interface GigabitEthernet 0/2
Ruijie(config-if-GigabitEthernet 0/2)# wan-ip map a.b.c.3 255.255.255.0 nexthop a.b.c.1
```

【检验方法】 1：使用 **show wan-ip config** 命令，可以查看本模块的配置信息。

【提示信息】 1：如果 IP 地址输入非法，则提示：

```
Invalid IP address.
```

2：如果掩码输入非法，则提示：

```
Invalid IP mask.
```

3：如果下一跳输入非法，则提示：

```
Invalid NextHop IP address.
```

【常见错误】 1：运营商给的 IP 地址配置错误

【平台说明】 -

10.3 show wan-ip config

查看多 WAN 同网段配置信息。

show wan-ip config

【参数说明】

参数	描述
-	-

【命令模式】 特权模式、全局模式、接口模式

【缺省级别】 14

【使用指导】 查看多 WAN 同网段的配置信息。

【配置举例】 1：查看本模块的配置信息

```
Ruijie#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#
```

字段解释：

字段	说明
Enable	功能总开关是否开启
GigabitEthernet 0/7	对应接口的配置

【提示信息】 -

【平台说明】 -

命令参考-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 layer23

1.1 clear subs-mab

清除 subs 库中用于内置无感知认证绑定的 MAC 地址信息。

clear subs-mab {all | mac *mac-addr***}**

【参数说明】

参数	描述
mac-addr	web 认证成功后绑定的终端 MAC 地址

【命令模式】 特权模式

【缺省级别】 14

【使用指导】 用于清除 web 认证成功后绑定的终端 MAC 地址信息，MAC 信息清除后 subs 库内置无感知将认证失败，重新触发 web 认证流程。

【配置举例】 1：清除已绑定 MAC 所有信息。

```
Ruijie#clear subs-mal all
```

2：清除已绑定 MAC 特定信息。

```
Ruijie#clear subs-mal mac 00d0.f822.cc33
```

【提示信息】 -

【平台说明】 全系列产品

1.2 layer23 classify enable

开启二三层分类识别功能。

layer23 classify enable

关闭二三层分类识别功能。

no layer23 classify enable

【参数说明】

参数	描述
-	-

【缺省配置】 缺省情况下，二三层分类识别功能是开启的。

【命令模式】 全局模式

【缺省级别】 14

【使用指导】 启用二三层分类识别后支持基于 vid，基于源 ip 或源 mac，基于目的 ip 的对象识别。

【配置举例】 1：开启二三层分类识别。

```
Ruijie(config)# layer23 classify enable
```

2：关闭二三层广告模式。

```
Ruijie(config)# no layer23 classify enable
```

【检验方法】 1：使用 **show run | in layer23** 命令是否显示 **layer23 classify enable，**可以查看当前配置是否启用二三层分类识别功能。
2：使用 **show layer23 obj-info** 命令查看内核中是否启用二三层分类识别功能。

【提示信息】 -

【常见错误】 二三层分类识别未开启，导致基于用户的流控，审计等策略无法生效。

【平台说明】 -

1.3 layer23 deny-mode enable

开启二三层全局屏蔽模式。
layer23 deny-mode enable

关闭二三层全局屏蔽模式。
no layer23 deny-mode enable

【参数说明】

参数	描述
-	-

【缺省配置】 缺省情况下，二三层全局屏蔽模式是关闭的。

【命令模式】 全局模式

【缺省级别】 14

【使用指导】 启用二三层全局屏蔽模式后，默认丢弃所有报文，除非用户对象添加到白名单中（即排除屏蔽用户）。

【配置举例】 1：开启全局屏蔽模式。

```
Ruijie(config)# layer23 deny-mode enable
```

2：关闭全局屏蔽模式。

```
Ruijie(config)# no layer23 deny-mode enable
```

【检验方法】 1：使用 **show layer23 deny-mode** 命令，可以查看二三层屏蔽模式是启用还是关闭。
2：使用 **show run | in layer23** 命令是否显示 **layer23 deny-mode enable，**可以查看当前配置是否开启二三层全局屏蔽模式。
3：使用 **show layer23 obj-info** 命令查看内核中是否开启全局屏蔽模式。

【提示信息】 -

【常见错误】 -

【平台说明】 -

1.4 layer23 flow-detect

开启二三层流量监测功能/配置流量监测流量、时间间隔。
layer23 flow-detect { enable | flow *flowrate* **| time-interval** *time* **}**

关闭二三层流量检测下线功能。
no layer23 flow-detect { enable | flow *flowrate* **| time-interval** *time* **}**

【参数说明】

参数	描述
enable	流量检测下线开关
flow *flowrate*	配置流量
time-interval *time*	配置时间间隔

【缺省配置】 缺省情况下，二三层流量下线检测是关闭的。

【命令模式】 全局模式

【缺省级别】 14

【使用指导】 启用二三层流量检测功能后，通过设备端认证上线的 ip 和账号，当特定时间间隔内的流量达不到配置的流量参数时，设备端主动将该 ip 节点踢下线，若跟第三方有联动同时会通知第三方下线。

【配置举例】 1：开启流量检测功能，配置 30 分钟无流量下线。

```
Ruijie(config)# layer23 flow-detect enable
Ruijie(config)# layer23 flow-detect flow 0
Ruijie(config)# layer23 flow-detect time-interval 30
```

2：关闭流量检测功能。

```
Ruijie(config)# no layer23 flow-detect
```

【检验方法】 1：使用 **show layer23 flow-detect** 命令，可以查看流量检测功能是否开启及配置参数。
2：使用内置本地认证上线后，开启二三层流量检测功能，配置 15 分钟无流量检测下线后，pc 换 ip 地址，等待 15 分钟后 ip 被设备主动踢下线。

【提示信息】 -

【常见错误】 -

【平台说明】 -

1.5 layer23 sam-accip-relate enable

开启 sam 账号关联组名功能。
layer23 sam-accip-relate enable

关闭 sam 账号关联组名功能。
no layer23 sam-accip-relate enable

【参数说明】

参数	描述
-	-

【缺省配置】 缺省情况下，该功能是关闭的。

【命令模式】 全局模式

【缺省级别】 14

【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】 1：开启 sam 账号关联组名功能。

```
Ruijie(config)# layer23 sam-accip-relate enable
```

2：关闭 sam 账号关联组名功能。

```
Ruijie(config)# no layer23 sam-accip-relate enable
```

【检验方法】 1：使用 **show layer23 sam-acc** 命令，可以查看该功能是启用还是关闭。
2：使用 **show run | in layer23** 命令是否显示 **layer23 sam-acc-relate enable，**可以查看当前配置是否开启 sam 同账号分属不同组功能。
3：sam 账号同步到设备端后，**show auth-subs brief** 查看姓名中是否组合了组名称。

【提示信息】 -

【常见错误】 -

【平台说明】 -

1.6 layer23 scc-attention enable

开启实名信息设置 scc 功能。
layer23 scc-attention enable

关闭实名信息设置 scc 功能。
no layer23 scc-attention enable

【参数说明】

参数	描述
-	-

【缺省配置】 缺省情况下，该功能是开启的。

【命令模式】 全局模式

【缺省级别】 14

【使用指导】 启用该功能后，将接受到的服务器实名信息设置到 scc 表项，然后设置到 aclk 表项用于放行用户。
注意：一般情况下可以关闭该选项用于优化设备处理性能。
当存在交换机和设备端同时开启认证的场景，想要实现接入交换机上认证通过后，设备端无需认证的场景，该功能必须开启。该场景一般为部分接入交换机没有认证功能，部分有认证功能，客户希望接入交换机上认证通过的用户无需二次认证，未认为的用户在设备端实现认证。

【配置举例】 1：开启实名信息设置 scc 功能。

```
Ruijie(config)# layer23 scc-attention enable
```

2：关闭实名信息设置 scc。

```
Ruijie(config)# no layer23 scc-attention enable
```

【检验方法】 1：使用 **show layer23 state** 命令，可以查看该功能是启用还是关闭。
2：使用 **show run | in layer23** 命令是否显示 **layer23 scc-attention enable，**可以查看当前配置是否开启实名信息设置 scc 功能。

【提示信息】 -

【常见错误】 -

【平台说明】 -

1.7 layer23 strict-verification enable

开启 IP+MAC 绑定严格校验过滤模式。
layer23 strict-verification enable

关闭严格校验模式。
no layer23 strict-verification enable

【参数说明】

参数	描述
-	-

【缺省配置】 缺省情况下，该功能是关闭的。

【命令模式】 全局模式

【缺省级别】 14

【使用指导】 启用该功能后，除非静态 ARP 绑定的用户，且 IP+MAC 都正确匹配的报文才会放行，否则报文将被丢弃，请谨慎使用。

【配置举例】 1：开启 IP/MAC 绑定严格过滤模式。

```
Ruijie(config)# layer23 strict-verification enable
```

2：关闭 subs 库内置无感知认证功能。

```
Ruijie(config)# no layer23 strict-verification enable
```

【检验方法】 1：使用 **show layer23 strict-verification** 命令，可以查看该功能是启用还是关闭。
2：使用 **show run | in strict** 命令是否显示 layer23 strict-verification enable，可以查看是否开启。

【提示信息】 -

【常见错误】 -

【平台说明】 -

1.8 layer23 subs-mab enable

开启 subs 库内置无感知认证功能。
layer23 subs-mab enable

关闭 subs 库内置无感知认证功能。
no layer23 subs-mab enable

【参数说明】

参数	描述
-	-

【缺省配置】 缺省情况下，该功能是关闭的。

【命令模式】 全局模式

【缺省级别】 14

【使用指导】 启用该功能后，web 认证成功的用户会自动绑定 MAC 地址信息，下次发起内置无感知认证无需再次进行 web 认证。

【配置举例】 1：开启 subs 库内置无感知认证功能。

```
Ruijie(config)# layer23 subs-mab enable
```

2：关闭 subs 库内置无感知认证功能。

```
Ruijie(config)# no layer23 subs-mab enable
```

【检验方法】 1：使用 **show subs-mab state** 命令，可以查看该功能是启用还是关闭。
2：使用 **show run | in subs-mab** 命令是否显示 layer23 subs-mab enable，可以查看是否开启。

【提示信息】 -

【常见错误】 -

【平台说明】 全系列产品

1.9 network-group

改变网络对象的所属父对象路径。

network-group *str1* **move to parent** *str2*

【参数说明】

参数	描述
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

【缺省配置】 -

【命令模式】 特权模式

【缺省级别】 14

【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。

【配置举例】 1：将原来在根目录下的 userA 移动到 group1 下。

```
Ruijie# network-group userA move to parent group1
```

【检验方法】 使用 **show network-group brief** 命令，可以查看当前网络对象组织层次结构查询是否移动成功。

【提示信息】 1：要移动的网络对象名称不存在。

```
can not find the child-network.
```

2：移动后所属的父对象名称不存在。

```
can not find the parent-network.
```

3：不能移动到自己名称下。

```
cann't move to parent of yourself.
```

4：不能移动根对象。

```
cann't move the root.
```

5：移动到自己原本的父对象名称下，不需要。

```
the network needn't to be moved.
```

6：原本父对象不是组的对象不能移动。

```
childs of the range-network can not be moved.
```

7：移动之后的父对象只能是组对象。

```
the parent after changed should be the network group!
```

8：不能移动到自己的子节点下。

```
cann't move to the child of yourself.
```

9：移动之后组织结构深度超过最大限制。

```
the depth of the network moving is more than 5!
```

10：不能移动系统默认创建的对象。

```
can not move the system default group.
```

【常见错误】 1：移动之后的层级数超过限制，导致无法移动成功。
2：系统默认对象无法移动。

【平台说明】 -

1.10 network-group export

导出当前系统中网络对象配置到文件中。
network-group export { **txt** | **csv** } *filename*

【参数说明】

参数	描述
filename	文件名

【缺省配置】 -

【命令模式】 特权模式

【缺省级别】 14

【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。

【配置举例】 1：导出网络对象配置到文件“ip-info.txt”。

```
Ruijie# network-groupexport txt ip-info.txt
```

【检验方法】 使用 **show network-groupall 和 show network-group brief**，打开 **ip-info.txt** 查看当前配置是否已经导入到该文件中。

【提示信息】 -

【常见错误】 -

【平台说明】 -

1.11 network-group import

导入网络对象到当前配置中。

network-group import { **txt** | **csv** } *filename* [**overwrite**]

【参数说明】

参数	描述
filename	文件名
overwrite	冲突模式标志

【缺省配置】 -

【命令模式】 特权模式

【缺省级别】 14

【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。

【配置举例】 1：导入网络对象文件“ip-info.txt”。

```
Ruijie# network-groupimport txt ip-info.txt
```

【检验方法】 使用 **show network-groupall 和 show network-group brief**，查看当前配置是否含有成功导入的网络对象。

【提示信息】 -

【常见错误】 -

【平台说明】 -

1.12 network-group name

配置网络对象。

network-group name *namestr* [**parent** *parent*] [**ip-host** *ip-addr* | **ip-subnet** *subnet mask* | **ip-range** *start end*]]

删除网络对象。

no network-group name *namestr*

【参数说明】

参数	描述
namestr	网络对象名称
parent	父对象所属路径
ip-addr	单 ip 对象 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

【缺省配置】 缺省情况下，系统默认创建 Out_Server 网络对象。

【命令模式】 全局模式

【缺省级别】 14

【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。

【配置举例】 1：配置 ip 地址段网络对象“network1”，包含 192.168.196.0 网段，其父对象是“用户组 1”，“用户组 1”的父对象是“所有用户组”。

```
Ruijie(config)# network-group name network1parent  /所有用户组/用户组 1 ip-subnet 192.168.196.0 255.255.255.0
```

【检验方法】 使用 **show network-groupall**，查看网络对象所有信息。

【提示信息】 1：该网络对象不存在。

```
can not find this network!
```

2：系统默认创建对象不允许删除。

```
cannot delete the network default group.
```

3：父对象所属路径错误。

```
Parent string error.
```

4：配置的父对象错误。

```
parent subscriber error.
```

5：名称和 xxx 冲突。

```
name conflict with xxx.
```

6：网络对象组和网络对象不能交换。

```
network group and network can not exchange
```

7：和 xxx 对象 ip 配置冲突。

```
ip conflict with xxx.
```

8：ip 地址错误。

```
ip address error.
```

9：range 对象的父对象只能是用户组。

```
parent of ip range network must be network group.
```

10：ip 或者掩码错误。

```
ip or mask error
```

【常见错误】 -

【平台说明】 -

1.13 network-group rename

重命名网络对象名称。

network-group rename *oldname newname*

【参数说明】

参数	描述
oldname	原网络对象名称
newname	新网络对象名称

【缺省配置】 -

【命令模式】 特权模式

【缺省级别】 14

【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】 1：将名为 userA 的网络对象重命名为 userB。

```
Ruijie# network-grouprename userA userB
```

【检验方法】 使用 **show network-group by-name** *userB*，查看对象和重命名之前其他属性有没有变化。

【提示信息】 1：新名称已存在。

```
name is conflict with other network.
```

2：旧名称网络对象不存在。

```
can not find this network
```

3：系统默认创建对象不允许重命名。

```
can not rename the network default group.
```

【常见错误】 -

【平台说明】 -

1.14 show auth-subs

查看认证对象信息。

show auth-subs [**all** | **brief** | **parent** [*name* | **root**]]

【参数说明】

参数	描述
all	显示所有认证对象账号信息
brief	显示认证对象账号组织层次结构
parent	显示认证对象账号下子节点信息
name | **root**	认证对象账号名称或根对象

【命令模式】 特权模式、全局模式、接口模式

【缺省级别】 14

【使用指导】 用于显示认证对象的配置信息，通过指定关键字可显示不同形式的网络对象信息。

【配置举例】 1：查看所有认证对象账号的详细信息。

```
name                                    dir type index
smp_root                                1   2    2
sam_root                                1   4    3
webauth_root                            1   1    4
```

字段解释：

字段	说明
name	认证对象名称
dir	认证对象组属性
type	认证对象类型(1-auth、2-smp、3-smp+auth、4-sam)
index	认证对象索引值，惟一性

【提示信息】 -

【平台说明】 -

1.15 show network-group

查看网络对象信息。

show network-group [**all** | **brief** | **parent** [*name* | **root**]]

【参数说明】

参数	描述
all	显示所有网络对象信息
brief	显示网络对象组织层次结构
parent	显示网络对象下子节点信息
name | **root**	网络对象名称或根对象

【命令模式】 特权模式、全局模式、接口模式

【缺省级别】 14

【使用指导】 用于显示网络对象的配置信息，通过指定关键字可显示不同形式的网络对象信息。

【配置举例】 1：查看所有网络对象的详细信息。

```
name                            dir index ip
root                             1   1
Out_Server                       1   2
ii                               1   18093
jj                               1   14691
uu                               0   32105 6.6.6.3 - 6.6.6.5
uuii                             1   12652
```

字段解释：

字段	说明
name	网络对象名称
dir	网络对象组属性
index	网络对象索引值，惟一性
ip	配置网络对象 ip 地址

【提示信息】 -

【平台说明】 -

1.16 show subscriber

查看用户对象信息。

show subscriber [**all** | **brief** | **parent** [*name* | **root**] **| custom-group {all | name** *namestr* **relate-all}**]

【参数说明】

参数	描述
all	显示所有用户对象信息
brief	显示用户对象组织层次结构
parent	显示用户对象下子节点信息
name | **root**	用户对象名称或根对象
custom-group	显示所有自定义组及自定义组关联 IP 段信息
all | name	显示所有自定义组或特定自定义组关联的信息
*namestr***relate-all**	自定义组对象名称关联的所有信息

【命令模式】 特权模式、全局模式、接口模式

【缺省级别】 14

【使用指导】 用于显示用户对象的配置信息，通过指定关键字可显示不同形式的用户对象信息。

【配置举例】 1：查看所有用户对象的详细信息。

```
name                            mac               dir av-fc av-con vip rel deny pwd-e au-deny login
```

```
vpn vbr webauth ssl-deny bind h-pwd idx       ssl-radius ip
root                              0000.0000.0000   1    0     0      0   0   0    0     0
0      1   0   1   0    0    0     1          0
Default_Group                     0000.0000.0000   1    0     0      0   0   0    0     0
0      1   0   1   0    0    0     2          0
without_auth_user                 0000.0000.0000   0    0     0      0   0   0    0     0
0      0   0   1   0    0    1     4          0
xxy                               0000.0000.0000   1    0     0      0   0   0    0     0
0      1   0   1   0    0    0     549939033 0
tt                                0000.0000.0000   0    0     0      1   0   0    0     0
0      1   0   1   0    2    0     3445540573 0          3.3.3.6
Vpn_Group                         0000.0000.0000   1    0     0      0   0   0    0     0
0      1   0   1   0    0    0     3          0
五部                              0000.0000.0000   1    0     0      0   0   0    0     0
0      1   0   1   0    0    0     912778062 0
ee                                0000.0000.0000   0    0     0      0   1   0    0     0
0      1   0   1   0    2    0     680907908 0          192.168.3.81
xhl                               0000.0000.0000   0    0     0      0   0   0    0     0
0      1   0   1   0    2    0     310883589 0          172.18.3.81
eg                                0000.0000.0000   0    0     0      0   0   0    0     0
0      1   0   1   0    2    0     2753766751 0         172.18.3.100 - 172.18.3.250
uiiu                              3333.3333.3333   0    0     0      0   0   0    0     0
0      1   0   1   0    1    1     2364943795 0
ttt                               0000.0000.0000   1    0     0      0   0   0    0     0
0      1   0   1   0    0    0     1938928104 0
```

字段解释：

字段	说明
name	用户对象名称
mac	配置的 mac 地址
dir	用户对象组属性
av-fc	免流控标志
av-con	免识别、审计标志
vip	vip 标志
rel	白名单属性标志
deny	屏蔽属性标志
pwd-e	修改密码属性标志
au-deny	禁止 web 认证登陆属性标志
login	login 认证权限
vpn	vpn 认证权限
vbr	vpn 分支机构标志
webauth	web 认证权限

ssl-deny	禁止 sslvpn 认证登陆属性
bind	绑定标志：0-不绑定，1-单向绑定，2-双向绑定
h-pwd	含有密码标志
idx	对象索引值
ssl-radius	sslvpn 账号服务端校验属性
ip	配置的 ip 地址

2：查看所有自定义组的详细信息。

```
Ruijie#show subscriber custom-group all
name                                custom cnt  index
XIA                                 1      1    2973161921
yanjiuyuan                          1      2    3332760464
555                                 1      1    1040419816
556                                 1      1    754996415 ttt
```

字段解释：

字段	说明
name	用户对象名称
custom	1 表示是自定义组，0 表示非自定义组
cnt	该自定义组关联的节点数量
index	自定义组对应的索引

3：查看自定义组 yanjiuyuan 关联节点的详细信息。

```
Ruijie#show subscriber custom-group name yanjiuyuan relate-all
yanjiuyuan relate-all:
    172.18.124.10 - 172.18.124.10
    172.18.124.1 - 172.18.124.255
```

【提示信息】 -

【平台说明】 -

1.17 show subs-mab

查看 subs 库内置无感知认证开关及绑定 MAC 信息。

show subs-mab {**all | state**}

【参数说明】

参数	描述
-	-

【命令模式】 特权模式、全局模式、接口模式

【缺省级别】 14

【使用指导】 用于显示 subs 库内置无感知认证开关状态及 WEB 认证成功后绑定的 MAC 信息。

【配置举例】 1：查看 subs 库内置无感知认证开关。

```
Ruijie#show subs-mab state
layer23 subs-mab state:On.
```

2：查看 subs 库内置无感知认证已绑定 MAC 信息。

```
Ruijie#show subs-mab all
Mab current number:1
    00d0.f822.33cc
```

【提示信息】 -

【平台说明】 全系列产品

1.18 show vlan-group

查看 vlan 对象信息。

show vlan-group [*name-str*]

【参数说明】

参数	描述
name-str	显示指定 vlan 对象信息

【命令模式】 特权模式、全局模式、接口模式

【缺省级别】 14

【使用指导】 用于显示 vlan 对象信息。

【配置举例】 1：查看所有 vlan 对象的详细信息。

```
vlan-group                      index vlan_id
root                            1
tt                              36028 1,9
```

字段解释：

字段	说明
name	vlan 对象名称
index	vlan 对象索引值
vlan_id	vlan 对象所包含 vid

【提示信息】 -

【平台说明】 -

1.19 subscriber

移动用户对象到另一对象下。

subscriber *str1* **move to parent** *str2*

【参数说明】

参数	描述
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

【缺省配置】 -

【命令模式】 特权模式

【缺省级别】 14

【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。

【配置举例】 1：将原来在根目录下的 userA 移动到 group1 下。

```
Ruijie#subscriber userA move to parent group1
```

【检验方法】 使用 **showsubscriber brief** 命令，可以查看当前用户对象组织层次结构查询是否移动成功。

【提示信息】 1：要移动的用户对象名称不存在。

```
can not find the child-subs.
```

2：移动后所属的父对象名称不存在。

```
can not find the parent-subs.
```

3：不能移动到自己名称下。

```
cann't move to parent of yourself.
```

4：不能移动根对象。

```
cann't move the root.
```

5：移动到自己原本的父对象名称下，不需要。

```
the subscriber needn't to be moved.
```

6：原本父对象不是组的对象不能移动。

```
childs of the range-subscriber can not be moved.
```

7：移动之后的父对象只能是组对象。

```
the parent after changed should be the subscriber group!
```

8：不能移动到自己的子节点下。

```
cann't move to the child of yourself.
```

9：移动之后组织结构深度超过最大限制。

```
the depth of the subscriber moving is more than 5!
```

10：不能移动系统默认创建的对象。

```
can not move the system default subs.
```

【常见错误】 1：移动之后的层级数超过限制，导致无法移动成功。
2：系统默认对象无法移动。

【平台说明】 -

1.20 subscriber allow

设置用户对象账号的使用权限。
subscriber allow *string* **privilege** { **none** | { [**webauth**] [**vpn**] [**login**] } }
no 命令权限设置不生效，新配置的权限命令会覆盖原来权限配置。

【参数说明】

参数	描述
string	用户对象账号名称
none	不允许任何权限
webauth	web 认证权限
vpn	vpn 认证权限
login	login 认证权限

【缺省配置】 缺省情况下，允许用户对象账号的 vpn 认证权限和 web 认证权限。

【命令模式】 全局模式

【缺省级别】 14

【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。

login 认证目前不支持使用用户管理处的账号认证。

【配置举例】 1：设置“用户 1”vpn 权限和 login 权限。

```
Ruijie(config)#subscriber allow 用户 1 privilegevpn login
```

2：设置“用户 1”所有权限都不允许。

```
Ruijie(config)# subscriber allow 用户 1 privilegenone
```

【检验方法】 使用 **show subscriber by-name***str*，查看某用户对象下的 login，vpn 和 webauth 标志是否为 1，代表对应的该权限是否开启。

```
name                                mac              dir av-fc av-con vip rel deny pwd-e au-deny login
vpn vbr webauth bind h-pwd idx       ip
xhl                                 0000.0000.0000   0     0      0       0    0    0     0      0        0
1   0   1       2    0     310883589 172.18.3.81
```

【提示信息】 1：该用户对象不存在。

```
can not find this subscriber.
```

2：系统默认对象账号不允许设置权限。

```
can not set privi to the system default subs.
```

3：用户对象组不允许设置权限。

```
can not set privi to subscriber group.
```

【常见错误】 1：移动之后的层级数超过限制，导致无法移动成功。
2：系统默认对象无法移动。

【平台说明】 -

1.21 subscriber custom-group

设置用户对象自定义组。
subscriber custom-group *string* **relateip-range** *start end*

删除特定自定义组关联的特定 IP 段信息
no subscriber custom-group *string* **relateip-range** *start end*

删除特定自定组对象包括其下关联的所有 IP 信息
no subscriber custom-group *string*

设置自定义组属性。
subscriber custom-group *string* **attribute {deny | avoid-audit | avoid-fc | release | vip}**

删除自定义组属性

no subscriber custom-group *string* **attribute {deny | avoid-audit | avoid-fc | release | vip}**

【参数说明】

参数	描述
string	用户自定义组名称
start	IP 起始地址
end	IP 结束地址

【缺省配置】 缺省情况下，未配置自定义组。

【命令模式】 全局模式

【缺省级别】 14

【使用指导】 配置用户自定义组关联 IP 段，不检测 IP 段冲突关系，支持最大配置 100 个自定义组，每个自定义组支持关联 200 个 IP 段。

对自定义组设置属性后，可以达到对某段 IP 免流控、免内容审计和应用识别、阻断、放行的效果。

名称不能和组织树上的名称冲突。

【配置举例】 1：配置自定义组“XIA”关联 IP172.18.124.114-172.18.124.114，设置免流控属性。

```
Ruijie(config)#subscriber custom-group XIA relate ip-range 172.18.124.114 172.18.124.114
Ruijie(config)#subscriber custom-group XIA attribute avoid-fc
```

2：删除自定义组 XIA。

```
Ruijie(config)#no subscriber custom-group XIA
```

【检验方法】 使用 **show subscriber custom-group all** 查看用户自定义组是否存在。

```
Ruijie#show subscriber custom-group all
name                              custom cnt   index
XIA                               1      1     2973161921
yanjiuyuan                        1      2     3332760464
555                               1      1     1040419816
556                               1      1     754996415
```

【提示信息】 1：用户组织树种该名称已存在。

```
[SUBS-CUSTOM] xxx is exist of no-custom-group.
```

2：自定义组对象不存在无法删除。

```
[SUBS-CUSTOM]can not find the custom-group subs!
```

3：自定义组关联 IP 地址段，end 不能小于 start。

```
[SUBS-CUSTOM]ip address error.
```

4：自定义组 xxx 无法找到关联的 IP 段

[SUBS-CUSTOM]custom-group xxx cannot find the match relate.

5：无法找到该自定义组去删除关联的 IP 段。

[SUBS-CUSTOM]can not find the custom-group subs!

6：自定义组 xxx 由于容量已满导致无法创建。

[SUBS-CUSTOM] create xxx over the capacity!

7：该 IP 段已经关联该自定义组，无需再次添加。

[SUBS-CUSTOM] range-ip has been related the custom-group.

【常见错误】 自定义组名称和组织树名称冲突。

【平台说明】 -

1.22 subscriber export

导出当前系统中用户对象配置到文件中。

subscriber export { **txt** | **csv** } *filename*

【参数说明】

参数	描述
filename	文件名

【缺省配置】 -

【命令模式】 特权模式

【缺省级别】 14

【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。

【配置举例】 1：导出用户对象配置到文件“user-info.txt”。

```
Ruijie#subscriber export txt user-info.txt
```

【检验方法】 使用 **show subscriber all 和 show subscriber brief**，打开 **user-info.txt** 查看当前配置是否已经导入到该文件中。

【提示信息】 -

【常见错误】 -

【平台说明】 -

1.23 subscriber import

导入用户对象到当前配置中。

subscriber import { **txt** | **csv** } *filename* [**overwrite**]

【参数说明】

参数	描述
filename	文件名
overwrite	冲突模式标志

【缺省配置】 -

【命令模式】 特权模式

【缺省级别】 14

【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 6 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。

【配置举例】 1：导入用户对象文件“user-info.txt”。

```
Ruijie#subscriber import txt user-info.txt
```

【检验方法】 使用 **show subscriber all 和 show subscriber brief**，查看当前配置是否含有成功导入的用户对象。

【提示信息】 -

【常见错误】 -

【平台说明】 -

1.24 subscriber rename

重命名用户对象名称。

subscriber rename *oldname newname*

【参数说明】

参数	描述
oldname	原用户对象名称
newname	新用户对象名称

【缺省配置】 -

【命令模式】 特权模式

【缺省级别】 14

【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。

【配置举例】 1：将名为 userA 的用户对象重命名为 userB。

```
Ruijie#subscriber rename userA userB
```

【检验方法】 使用 **show subscriber by-name** *userB*，查看对象和重命名之前其他属性有没有变化。

【提示信息】 1：新名称已存在。

```
name is conflict with other subscriber.
```

2：旧名称用户对象不存在。

```
can not find this subscriber
```

3：系统默认创建对象不允许重命名。

```
can not rename the system default subs.
```

【常见错误】 -

【平台说明】 -

1.25 subscriber set

设置用户对象特殊属性。

subscriber set *namestr* **attribute** {**avoid-monitor**[**flow-monitor**] | **deny** | **release | vip** | **auth-deny** | **pwd-edit | ssl-auth-deny | ssl-radius-verify**}

取消用户对特殊属性。

no subscriber set *namestr* **attribute** {**avoid-monitor** | **deny** | **release | vip** | **auth-deny** |**pwd-edit | ssl-auth-deny | ssl-radius-verify** }

【参数说明】

参数	描述
namestr	用户对象名称
avoid-monitor	免监控属性包括免应用识别、内容审计和流量控制
flow-monitor	免监控同时不免除流量控制
deny	屏蔽属性
release	白名单属性。即排除屏蔽用户属性
vip	vip 属性
auth-deny	禁止登陆属性
pwd-edit	允许修改密码属性
ssl-auth-deny	禁止 sslvpn 认证属性（可基于组配置）
ssl-radius-verify	sslvpn 本地账号密码不校验属性

【缺省配置】 缺省情况下，不含任何特殊属性。

【命令模式】 全局模式

【缺省级别】 14

【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，开启上网屏蔽模式后，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）的禁止 sslvpn 认证属性。设置后，该账号或该账号组下的账号将不能 sslvpn 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】 1：对“用户 1”设置免内容审计、免应用识别，但受流量控制。

```
Ruijie(config)#subscriber set 用户 1 attribute avoid-monitor flow-monitor
```

2：去除用户对象“用户 1”的免监控属性。

```
Ruijie(config)#no subscriber set 用户 1attribute avoid-monitor
```

【检验方法】 使用 **show subscriber by-name** *userB*，查看该对象下所有信息。

【提示信息】 1：该用户对象不存在。

```
can not find this subscriber.
```

2：系统默认创建对象不允许设置特殊属性。

```
can not set attri to the system default subs.
```

3：用户对象组不支持设置特殊属性。

```
can not set attribute to subscriber group.
```

【常见错误】 -

【平台说明】 -

1.26 subscriber static

配置一个用户对象。

subscriber static name *namestr* **parent** *parstr* [[[[**ip-host** *ip-addr*] [**mac** *mac-addr*] | **ip-subnet** *subnetmask* **| 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*]

删除一个用户对象。

no subscriber static name *namestr*

【参数说明】

参数	描述

namestr	用户对象名称
parstr	所属父对象路径
ip-addr	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 password 后 0 表示明文，6 表示 md5 密文，7 表示一般密文
two-way-bind	双向绑定标志
single-way-bind	单向绑定标志
phone_number	手机号码

【缺省配置】 缺省情况下，Vpn_Group, Default_Group 和 without_auth_user 系统默认创建。

【命令模式】 全局模式

【缺省级别】 14

【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，可以使用手机号进行本地短信认证校验。

用户对象名称是惟一的，不同用户对象之间名称不能相同。

【配置举例】 1：配置“用户 1”，ip 地址是“192.168.196.156”，其父对象是“用户组 1”，“用户组 1”的父对象是“所有用户组”。

```
Ruijie(config)# subscriber static name 用户 1 parent /所有用户组/用户组 1 ip-host 192.168.196.156
```

【检验方法】 使用 **show subscriberall**，查看所有用户对象信息。

【提示信息】 1：该用户对象不存在。

```
can not find this subscriber!
```

2：系统默认创建对象不允许删除。

```
cannot delete the default group.
```

3：父对象所属路径错误。

```
Parent string error.
```

4：配置的父对象错误。

```
parent subscriber error.
```

5：含密码的对象不能作为父对象。

```
parent subscriber cannot be the have-pwd-subs.
```

6：含密码对象其父对象只能是用户组。

```
par of the have-pwd-subs must be the group.
```

7：名称和 xxx 冲突。

```
name conflict with xxx.
```

8：用户组和用户对象不能交换。

```
subscriber group and subscriber can not exchange
```

9：含有子节点的非组对象不能设置密码。

```
the no-group subs had child-subs cannot set password.
```

10：和 xxx 对象 ip 配置冲突。

```
ip conflict with xxx.
```

11：和单向绑定 ip 的 xxx 对象 ip 配置冲突。

```
ip conflict with bind-single-way xxx.
```

12：和 xxx 对象 mac 配置冲突。

```
mac conflict with xxx.
```

13：和单向绑定 mac 的 xxx 对象 mac 配置冲突。

```
mac conflict with single-bind xxx.
```

14：ip 地址错误。

```
ip address error.
```

15：range 对象的父对象只能是用户组。

```
parent of ip range subscriber must be subscriber group.
```

16：ip 或者掩码错误。

```
ip or mask error
```

17：配置的 range 对象和单向绑定 ip 的 xxx 对象 ip 配置冲突。

```
IP-RANGE: ip conflict with bind-single-way xxx.
```

18：手机号码校验错误：长度不符、字符串非法、手机号冲突不惟一。

```
the len of phone number is not 11.
the phone number is illegal.
the phone number is conflict with xxx.
```

【常见错误】 1：单双向绑定概念理解错误。
2：账号权限配置问题导致无法认证。

【平台说明】 -

1.27 vlan-group

配置 vlan 对象。
vlan-group *name* **vlan** *vid-list*

删除 vlan 对象
no vlan-group *name*

【参数说明】

参数	描述
name	vlan 对象名称
vid-list	对象 vid

【缺省配置】 -

【命令模式】 全局模式

【缺省级别】 14

【使用指导】 vlan 对象之间的 vlan id 不能冲突，多个 vlan id 之间用逗号隔开，如需配置多个连续的 vlan id 属于同一个 vlan 对象，可用“-”隔开起始 vlan id 和结束 vlan id 表示多个连续的 vlan id。

默认存在一个默认 vlan 对象“any”，开启二三层分类识别功能时，在网关模式下所有数据流默认匹配中默认对象“any”。

不同 vlan 对象之间名称不能相同，vlan 对象在网关模式下识别无效

【配置举例】 1：配置 vlan 对象“vlan-group1”包含 vlan 1、vlan 3、vlan7、vlan8、vlan9。

```
Ruijie(config)# vlan-group vlan-group1 vlan 1,3,7-9
```

【检验方法】 使用 **show vlan-groupall**，查看 vlan 对象的所有信息。

【提示信息】 -

【常见错误】 -

【平台说明】 -

2 APP-IDENTIFY

2.1 app-add

新增用户自定义应用组中的应用。
app-add *app-name*

删除用户自定义组中的应用
app-del *app-name*

【参数说明】

参数	描述
app-name	应用名称。

【缺省配置】 缺省下，新增自定义应用组无应用

【命令模式】 custom-group 配置命令模式

【缺省级别】 14

【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。

【配置举例】 1：往 MYGAME 自定义应用组中添加征途游戏。

```
Ruijie#config
Ruijie(config)#identify-application custom-group MYGAME
Ruijie(config-custom-group)#app-add 征途
```

【提示信息】 1：如果应用不存在，则提示：

```
Ruijie#config
Ruijie(config)#identify-application custom-g
Ruijie(config)#identify-application custom-group aaa
Ruijie(config-custom-group)#app-add no_exit
This application is not exist!
```

2：内存不足，则提示：

```
Ruijie#config
Ruijie(config)#identify-application custom-g
Ruijie(config)#identify-application custom-group 即时通讯软件
not enouth memory!
```

3：自定义应用组加入另一个自定义应用组，则提示：

```
Ruijie#config
Ruijie(config)#identify-application custom-group aaa
Ruijie(config-custom-group)#exit
Ruijie(config)#identify-application custom-group bbb
Ruijie(config-custom-group)#app-add aaa
One custom-group cannot join another custom-group!
```

【常见错误】 1：应用不存在
2：自定义应用组加入另一个自定义应用组

【平台说明】 -

2.2 app-del

删除用户自定义应用组中的应用。
app-del *app-name*

恢复配置。
app-add *app-name*

【参数说明】

参数	描述
app-name	应用名称。

【缺省配置】 缺省下，新增自定义应用组无应用

【命令模式】 custom-group 配置命令模式

【缺省级别】 14

【使用指导】 通过此命令可以往用户自定义应用组里面删除应用。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。

【配置举例】 1：从 MYGAME 自定义应用组中删除征途游戏。

```
Ruijie#config
Ruijie(config)#identify-application custom-group MYGAME
Ruijie(config-custom-group)#app-del 征途
```

【提示信息】 1：应用不存在，则提示：

```
Ruijie#config
Ruijie(config)#identify-application custom-group aaa
Ruijie(config-custom-group)#app-del bcd
This application doesn't exist!
```

2：应用未加入应用组，则提示：

```
Ruijie#config
Ruijie(config)#identify-application custom-group aaa
Ruijie(config-custom-group)#app-del 时通讯软件
The application doesn't join the custom-group!
```

【常见错误】 1：应用不存在
2：应用不存在于自定义应用组

【平台说明】 -

2.3 identify-application app-db enable

开启应用收集功能。
identify-application app-db enable

关闭应用收集功能。
no identify-application app-db enable

【参数说明】

参数	描述
-	-

【缺省配置】 默认开启

【命令模式】 全局配置模式

【缺省级别】 14

【使用指导】 通过此命令可以开启应用收集功能。

【配置举例】 1：开启应用收集功能。

```
Ruijie#config
Ruijie(config)#identify-application app-db enable
```

【常见错误】 -

【平台说明】 -

2.4 identify-application block

将某个应用加入阻断应用组。
identify-application block *app-name*

将某个应用移出阻断应用组。
no identify-application block *app-name*

【参数说明】

参数	描述
app-name	应用名称。

【缺省配置】 缺省不加入阻断应用组

【命令模式】 全局配置模式

【缺省级别】 14

【使用指导】 通过此命令可以将某个应用加入阻断应用组。

【配置举例】 1：将 MSN 应用加入阻断应用组。

```
Ruijie#config
Ruijie(config)#identify-application block MSN
```

【检验方法】 1：使用 **show identify-application block** 命令，可以查看阻断应用组中的所有应用。

【提示信息】 1：如果某个应用已经在其他系统应用组，则提示错误。如 MSN 已经加入抑制组的情况下，将 MSN 应用加入阻断应用组，则提示：

```
Ruijie(config)#identify-application block MSN
The application has already been joined Inhibitive_Group!
```

2：如果将未存在的应用加入阻断应用组，则提示该应用不存在。

```
Ruijie(config)#identify-application block XXX
The application does not exist!
```

【常见错误】 1：某个应用已加入其它系统应用组
2：应用不存在

【平台说明】 -

2.5 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 clear key-inhibitive-block-other group

【参数说明】

参数	描述
-	-

【缺省配置】 -

【命令模式】 全局配置模式

【缺省级别】 14

【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。

【配置举例】 1：将所有应用从关键应用组，抑制应用组和阻断应用组中删除。

```
Ruijie#config
Ruijie(config)# identify-application clear key-inhibitive-block-other group
```

【检验方法】 1：使用 **show identify-application key**、**show identify-application inhibitive**、**show identify-application-block** 和 **show identify-application other** 命令，可以查看关键、抑制、阻断和其他应用组中的所有应用。

【提示信息】 -

【常见错误】 -

【平台说明】 -

2.6 identify-application custom name

配置一条用户自定义规则。

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* **} } } }**

将某个应用移出阻断应用组。

no 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】

参数	描述
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。

【缺省配置】 缺省无用户自定义规则

【命令模式】 全局配置模式

【缺省级别】 14

【使用指导】 通过配置本命令可以添加一条用户自定义的规则。

用户自定义应用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

用户自定义应用对规则有如下限制：

1.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。

2.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

3.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

4.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

5.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。

6.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。

7.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

8.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

【配置举例】 1：配置一条用户自定义规则，应用分类为自定义游戏，应用名称为迅雷游戏，源端口范围为 1 到 10，目的端口范围为 1 到 100，协议类型为 tcp：

```
Ruijie#config
Ruijie(config)#identify-application custom name 迅雷游戏 class 自定义游戏 tcp sport 1 10 dport 1 100
```

2 :配置一条用户自定义规则 ,应用分类为 myp2p ,应用名称为 myxunlei ,源端口为任意 ,目的端口范围为 200，协议类型为 udp：

```
Ruijie#config
Ruijie(config)#identify-application custom name myxunlei class myp2p udp sport any any dport 200 200
```

3：配置一条用户自定义规则，应用分类为 myqq，应用名称为特征库中已经存在的分类 im，源端口为 111，目的端口范围为 2020，协议类型为 udp：

```
Ruijie#config
Ruijie(config)#identify-application custom name myqq class im udp sport 111 111 dport 2020 2020
```

【检验方法】 1：使用 **show identify-application custom-rule** 命令，可以显示所有自定义应用规则。

【提示信息】 1：配置规则的 ip 段超过 32 个 ip：

```
Ruijie(config)#identify-application custom name rule1 class TC_AD_KEY tcp dip 172.18.1.20 172.18.2.255 dport 2 2
High ip address must be larger than low ip address,and the range of ip address can not be larger than 32!
```

2：ip 或端口不允许配置为 any 时，提示：

```
Ruijie(config)#identify-application custom name rule1 class TC_AD_KEY tcp dip 172.18.1.20 172.18.2.255 dport any any
It's not allow for either dst ip address or dst port number are "any"!
```

3：ip 或端口冲突时，提示：

```
Ruijie(config)#identify-application custom name rule1 class TC_AD_KEY tcp dip 172.18.1.20 172.18.1.30 dport 2 2
Ruijie(config)#identify-application custom name rule1 class TC_AD_KEY tcp dip 172.18.1.25 172.18.1.35 dport 2 2
Port or ip has already used!
```

4：ip 或端口冲突时，提示：

```
Ruijie#show identify-application custom-rule
TYPE NAME                          CLASS                          SPL    SPH    DPL    DPH    SIPL
```

```
SIPH            DIPL            DIPH
---- ---------------------------- -------------------------------- ----- ----- ----- -----
--------------- --------------- --------------- ---------------
TCP  rule1                        TC_AD_KEY                        any   any   2     2     any
any             172.18.1.20     172.18.1.30
TCP  rule2                        TC_AD_KEY                        any   any   3     20    any
any             172.18.1.25     172.18.1.26
TCP  rule3                        数据库                           any   any   25    30    any
any             172.18.1.25     172.18.1.25
TCP  rule3                        数据库                           any   any   35    40    any
any             172.18.1.25     172.18.1.29
TCP  rule3                        数据库                           any   any   45    50    any
any             172.18.1.25     172.18.1.29
TCP  rule3                        数据库                           any   any   55    60    any
any             172.18.1.25     172.18.1.29
TCP  rule3                        数据库                           any   any   65    70    any
any             172.18.1.25     172.18.1.29
TCP  rule3                        数据库                           any   any   72    72    any
any             172.18.1.25     172.18.1.29
TCP  rule3                        数据库                           any   any   74    74    any
any             172.18.1.25     172.18.1.29
TCP  rule3                        数据库                           any   any   76    76    any
any             172.18.1.25     172.18.1.29
TCP  rule3                        数据库                           any   any   78    78    any
any             172.18.1.25     172.18.1.29
TCP  rule3                        数据库                           any   any   80    80    any
any             172.18.1.25     172.18.1.29
TCP  rule3                        数据库                           any   any   82    82    any
any             172.18.1.25     172.18.1.29
TCP  rule3                        数据库                           any   any   84    84    any
any             172.18.1.25     172.18.1.29
TCP  rule3                        数据库                           any   any   86    86    any
any             172.18.1.25     172.18.1.29
TCP  rule3                        数据库                           any   any   88    88    any
any             172.18.1.25     172.18.1.29
Ruijie(config)# identify-application custom name rule3 class 数据库 tcp dip 172.18.1.25 172.18.1.
29 dport 90 90
The same IP associated with different port cannot exceed 16
```

【常见错误】 1：配置规则的 ip 段超过 32 个 ip

2：ip 或端口不允许配置为 any 或者同时配置为 any

3：ip 或端口冲突

【平台说明】 -

2.7 identify-application custom-group

新增用户自定义应用组。
identify-application custom-group *group-name*

删除用户自定义应用组。
no identify-application custom-group *group-name*

【参数说明】

参数	描述
group-name	应用组名

【缺省配置】 缺省情况下无用户自定义应用组

【命令模式】 全局配置模式

【缺省级别】 14

【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 custom-group 配置命令层。

【配置举例】 1：下面命令新增用户自定义的 MYGAME 应用组：该应用组的层次和关键应用组，抑制应用组相同。

```
Ruijie#config
Ruijie(config)#identify-application custom-group MYGAME
Ruijie(config-custom-group)#
```

【提示信息】 1：删除不存在的自定义应用组，则提示：

```
Ruijie(config)#no identify-application custom-group abc
The custom-group doesn't exist!
```

2：自定义应用组名称与系统中的应用冲突，则提示：

```
Ruijie(config)#id custom-group 即时通讯软件
The application name is conflict with application in system!
```

3：应用组个数超过最大值，则提示：

```
Ruijie(config)#id custom-group group101
The number of custom-group cannot be more than 100!
```

【常见错误】 1：自定义应用组名称和系统中的应用冲突
2：自定义应用组个数超过上限

【平台说明】 -

2.8 identify-application dfi enable

开启 dfi 识别 p2p 下载流和语音流的功能。
identify-application dfi enable

使用该命令的 no 选项关闭应用识别功能。
no identify-application dfi enable

【参数说明】

参数	描述
-	-

【缺省配置】 缺省情况下关闭。也可单独开启。

【命令模式】 全局配置模式

【缺省级别】 14

【使用指导】 通过此命令可以开启 dfi 识别 p2p 下载流和语音流的功能。

【配置举例】 1：开启 dfi 识别 p2p 和语音流的功能。

```
Ruijie#config
Ruijie(config)#identify-application dfi enable
```

【检验方法】 1：使用 **show running-config** 查看功能开关。当关闭时，显示

```
identify-application dfi enable
```

【提示信息】 -

【常见错误】 -

【平台说明】 -

2.9 identify-application dpi enable

开启 DPI 识别功能。
identify-application dpi enable

关闭 DPI 识别功能。
no identify-application dpi enable

【参数说明】

参数	描述
-	-

【缺省配置】 应用识别开启情况下，缺省开启。

【命令模式】 全局配置模式

【缺省级别】 14

【使用指导】 通过此命令可以开启 DPI 识别功能。

【配置举例】 1：开启 DPI 识别。

```
Ruijie#config
Ruijie(config)#identify-application dpi enable
```

【检验方法】 1：使用 **show running-config** 查看功能开关。当关闭时，显示

```
no identify-application dpi enable
```

【提示信息】 -

【常见错误】 -

【平台说明】 -

2.10 identify-application enable

开启 应用识别全局功能。
identify-application enable

关闭 应用识别全局功能。
no identify-application enable

【参数说明】

参数	描述
-	-

【缺省配置】 缺省情况下为开启此功能。

【命令模式】 全局配置模式

【缺省级别】 14

【使用指导】 通过此命令可以开启应用识别全局功能。

【配置举例】 1：开启应用识别。

```
Ruijie#config
Ruijie(config)#identify-application enable
```

【检验方法】 1：使用 **show identify-application enable** 查看功能状态。

【提示信息】 -

【常见错误】 -

【平台说明】 -

2.11 identify-application inhibitive

将某个应用加入抑制应用组。
identify-application inhibitive *app-name*

将某个应用移出抑制应用组。
no identify-application inhibitive *app-name*

【参数说明】

参数	描述
app-name	应用名

【缺省配置】 缺省不加入抑制应用组

【命令模式】 全局配置模式

【缺省级别】 14

【使用指导】 通过此命令可以将某个应用加入抑制应用组。

【配置举例】 1：将 MSN 应用加入抑制应用组。

```
Ruijie#config
Ruijie(config)#identify-application inhibitive MSN
```

【检验方法】 1：使用 **show identify-application inhibitive** 命令，可以查看抑制应用组中的所有应用。

【提示信息】 1：如果某个应用已经在其他系统应用组，则提示错误。如 MSN 已经加入阻断应用组的情况下，将 MSN 应用加入抑制应用组，则提示：

```
Ruijie(config)#identify-application inhibitive MSN
The application has already been joined Block_Group!
```

2：如果将未存在的应用加入抑制应用组，则提示该应用不存在。

```
Ruijie(config)#identify-application inhibitive XXX
The application does not exist!
```

【常见错误】 1：应用已经在其他系统应用组
2：应用不存在

【平台说明】 -

2.12 identify-application key

将某个应用加入关键应用组。
identify-application key *app-name*

将某个应用移出关键应用组。
no identify-application key *app-name*

【参数说明】

参数	描述
app-name	应用名

【缺省配置】 缺省不加入关键应用组

【命令模式】 全局配置模式

【缺省级别】 14

【使用指导】 通过此命令可以将某个应用加入关键应用组。

【配置举例】 1：将 MSN 应用加入关键应用组。

```
Ruijie#config
Ruijie(config)#identify-application key MSN
```

【检验方法】 1：使用 **show identify-application key** 命令，可以查看关键应用组中的所有应用。

【提示信息】 1：如果某个应用已经在其他系统应用组，则提示错误。如 MSN 已经加入阻断应用组的情况下，将 MSN 应用加入关键应用组，则提示：

```
Ruijie(config)#identify-application key MSN
The application has already been joined Block_Group!
```

2：如果将未存在的应用加入关键应用组，则提示该应用不存在。

```
Ruijie(config)#identify-application key XXX
The application does not exist!
```

【常见错误】 1：应用已经在其他系统应用组
2：应用不存在

【平台说明】 -

2.13 identify-application len-seq enable

开启长度序列识别功能。
identify-application len-seq enable

关闭长度序列识别功能。
no identify-application len-seq enable

【参数说明】

参数	描述
-	-

【缺省配置】 应用识别开启情况下，缺省开启。

【命令模式】 全局配置模式

【缺省级别】 14

【使用指导】 通过此命令可以开启长度序列识别功能。

【配置举例】 1：开启长度序列识别。

```
Ruijie#config
Ruijie(config)#identify-application len-seq enable
```

【检验方法】 1：使用 **show running-config** 查看功能开关。当关闭时，显示

```
no identify-application len-seq enable
```

【提示信息】 -

【常见错误】 -

【平台说明】 -

2.14 identify-application other

将某个应用加入其它应用组。
identify-application other *app-name*

将某个应用移出其它应用组。
no identify-application other *app-name*

【参数说明】

参数	描述
app-name	应用名称。

【缺省配置】 缺省加入其它应用组

【命令模式】 全局配置模式

【缺省级别】 14

【使用指导】 通过此命令可以将某个应用加入其它应用组。

【配置举例】 1：将 MSN 应用加入其它应用组。

```
Ruijie#config
Ruijie(config)#identify-application other MSN
```

【检验方法】 1：使用 **show identify-application other** 命令，可以查看其它应用组中的所有应用。

【提示信息】 1：如果将未存在的应用加入其它应用组，则提示该应用不存在。

```
Ruijie(config)#identify-application other XXX
The application does not exist!
```

【常见错误】 1：应用不存在

【平台说明】 -

2.15 identify-application proto-detect enable

开启应用识别协议探测识别功能。
identify-application proto-detect enable

使用该命令的 no 选项关闭协议探测识别功能。
no identify-application proto-detect enable

【参数说明】

参数	描述
-	-

【缺省配置】 在开启应用识别的情况下，默认开启该功能。

【命令模式】 全局配置模式

【缺省级别】 14

【使用指导】 通过此命令可以开启协议预期识别功能。

【配置举例】 1：开启协议预期识别功能。

```
Ruijie#config
Ruijie(config)# identify-application proto-detect enable
```

【检验方法】 1：使用 **show running-config** 查看功能开关。当关闭时，显示

```
no identify-application proto-expect enable
```

【提示信息】 -

【常见错误】 -

【平台说明】 -

2.16 identify-application proto-expect enable

开启应用识别协议预期识别功能。
identify-application proto-expect enable

使用该命令的 no 选项关闭协议预期识别功能。

no identify-application proto-expect enable

【参数说明】

参数	描述
-	-

【缺省配置】 在开启应用识别的情况下，默认开启该功能。

【命令模式】 全局配置模式

【缺省级别】 14

【使用指导】 通过此命令可以开启协议预期识别功能。

【配置举例】 1：开启协议预期识别功能。

```
Ruijie#config
Ruijie(config)# identify-application proto-expect enable
```

【检验方法】 1：使用 **show running-config** 查看功能开关。当关闭时，显示

```
no identify-application proto-expect enable
```

【提示信息】 -

【常见错误】 -

【平台说明】 -

2.17 identify-application proto-expect timeout

配置协议预期节点的老化时间。
identify-application proto-expect timeout *time-seconds*

取消配置协议预期节点老化时间
no identify-application proto-expect timeout

【参数说明】

参数	描述
time-seconds	老化的秒数，参数范围 10 - 3600

【缺省配置】 缺省参数为 60 秒。

【命令模式】 全局配置模式

【缺省级别】 14

【使用指导】 通过此命令可以配置协议预期节点的老化时间。

【配置举例】 1：配置协议预期节点的老化时间为 3 分钟。

```
Ruijie#config
Ruijie(config)# identify-application proto-expect timeout 180
```

【检验方法】 1：使用 **show running-config** 查看。当有配置时，显示

```
identify-application proto-expect timeout 180
```

【提示信息】 -

【常见错误】 -

【平台说明】 -

2.18 identify-application signature update

升级特征库。

identify-application signature update

【参数说明】

参数	描述
-	-

【缺省配置】 缺省情况开机一分钟时自动升级。

【命令模式】 全局配置模式

【缺省级别】 14

【使用指导】 通过此命令可以升级更新特征库。

【配置举例】 1：从 WEB 升级界面上提供的链接下载最新特征库版本

2： 解压后，通过 tftp 方式，将特征库下载到设备上。

```
Ruijie#copy tftp://172.18.3.11/app_signature.upd flash:app_signature.upd
Accessing tftp://172.18.3.11/app_signature.upd...
!!!!!!!!!!!!!!!!
Transmission finished, file length 242952  bytes.

Download file [app_signature.upd] to file system is OK.
```

```
Ruijie#run-system-shell
~ # cp /data/app_signature.upd /sbin/signature/app_tmp/
~ # exit
Ruijie#
```

3：升级特征库。

```
Ruijie#config
Ruijie(config)# identify-application signature update
```

【检验方法】 1：使用 **show identify-application version** 查看特征库版本信息。

【提示信息】 -

【常见错误】 -

【平台说明】 -

2.19 show identify-application

显示应用规则树信息。

show identify-application

【参数说明】

参数	描述
-	-

【命令模式】 特权模式、全局模式、接口模式

【缺省级别】 -

【使用指导】 通过此命令可以打印出当前应用规则树的信息。

【配置举例】 1：显示应用规则树信息

```
Ruijie#show identify-application
any 255-4095-63-48
    即时通讯软件 1-0-0-0
        阿里旺旺 1-1-0-0
        MSN 1-6-0-0
            MSN-CHAT 1-6-1-0
            MSN-AUDIO 1-6-2-0
            MSN-FILE 1-6-3-0
            MSN-视频 1-6-4-0
            MSN-登录 1-6-5-0
```

```
        腾讯 QQ 1-7-0-0
            QQ-CHAT 1-7-1-0
            QQ-语音 1-7-2-0
            QQ-文件传输 1-7-3-0
            QQ-文件共享 1-7-4-0
            QQ-视频 1-7-5-0
            QQ-登录 1-7-14-0
        WEBIM 1-9-0-0
            MSN-WEBIM 1-9-1-0
            YAHOO-WEBIM 1-9-2-0
            AIM 1-9-3-0
        网易泡泡 1-12-0-0
        飞信 1-14-0-0
    IP 网络电话 2-0-0-0
        SKYPE 2-7-0-0
        h232 协议族 2-12-0-0
            H323-HOSTCALLSC 2-12-4-0
            CALL-SIG-TRANS 2-12-5-0
            RTCP 2-12-6-0
            RTP 2-12-7-0
           IMTC-MCS 2-12-10-0
```

【提示信息】 -

【平台说明】 -

2.20 show identify-application block

显示加入阻断应用组的应用或分类。

show identify-application block

【参数说明】

参数	描述
-	-

【命令模式】 特权模式

【缺省级别】 14

【使用指导】 通过此命令可以查看当前那些应用或分类加入了阻断应用组。

【配置举例】 1：显示阻断应用组中的应用

```
Ruijie# show identity-application block
股票软件
百度下吧
迅雷
```

【提示信息】 -

【平台说明】 -

2.21 show identify-application class

显示应用分类信息。

show identify-application class [*class-name*]

【参数说明】

参数	描述
class-name	应用分类名

【命令模式】 特权模式

【缺省级别】 14

【使用指导】 通过此命令可以查看应用分类信息，或者某个应用分类下的应用。

【配置举例】 1：查看应用分类

```
Ruijie# show identify-application class
即时通讯软件 1-0-0-0
IP 网络电话 2-0-0-0
网络游戏软件 3-0-0-0
视频流媒体软件 4-0-0-0
P2P 应用软件 5-0-0-0
股票软件 6-0-0-0
WEB 应用 7-0-0-0
HTTP 游戏 38-0-0-0
互联网文件传输 8-0-0-0
电子邮件协议 9-0-0-0
数据库 10-0-0-0
网络管理协议 11-0-0-0
路由协议 12-0-0-0
安全协议 13-0-0-0
VPN 应用 14-0-0-0
远程访问协议 15-0-0-0
```

```
软件更新 17-0-0-0
HTTP 视频 18-0-0-0
网银 19-0-0-0
网络硬盘 20-0-0-0
即时通讯_MOBILE 21-0-0-0
视频|影音_MOBILE 22-0-0-0
下载工具_MOBILE 23-0-0-0
游戏_MOBILE 24-0-0-0
```

2：查看某个应用分类下的应用

```
Ruijie# show identify-application class 互联网文件传输
FTP 8-4-0-0
HTTPS 8-7-0-0
NNTP 8-12-0-0
TFTP 8-16-0-0
IXIA 8-17-0-0
SVN 8-18-0-0
SMB 8-21-0-0
HFS 8-22-0-0
```

【提示信息】 -

【平台说明】 -

2.22 show identify-application custom-group

显示应用分组信息。

show identify-application custom-group

【参数说明】

参数	描述
-	-

【命令模式】 特权模式

【缺省级别】 14

【使用指导】 通过此命令可以所有应用分组。

【配置举例】 1：查看应用分组

```
Ruijie# show identify-application custom-group
system-group: Key_Group
```

```
system-group: Unkey_Group
system-group: Block_Group
    application: MSN (group)
system-group: Other_Group
    application: 即时通讯软件 (group)
    application: IP 网络电话 (group)
    application: 网络游戏软件 (group)
    application: 视频流媒体软件 (group)
    application: P2P 应用软件 (group)
    application: 股票软件 (group)
    application: WEB 应用 (group)
    application: HTTP 游戏 (group)
    application: 互联网文件传输 (group)
    application: 电子邮件协议 (group)
    application: 数据库 (group)
    application: 网络管理协议 (group)
    application: 路由协议 (group)
    application: 安全协议 (group)
    application: VPN 应用 (group)
    application: 远程访问协议 (group)
    application: 软件更新 (group)
    application: HTTP 视频 (group)
    application: 网银 (group)
    application: 网络硬盘 (group)
    application: 即时通讯_MOBILE (group)
    application: 视频|影音_MOBILE (group)
    application: 下载工具_MOBILE (group)
    application: 游戏_MOBILE (group)
    application: 社交_MOBILE (group)
    application: 网盘_MOBILE (group)
    application: WEB_MOBILE (group)
    application: 其他_MOBILE (group)
    application: 网购_MOBILE (group)
    application: 证券_MOBILE (group)
    application: 网上支付|网上银行_MOBILE (group)
    application: 微博 (group)
    application: 办公 OA (group)
    application: 视频会议 (group)
    application: HTTP 下载 (group)
    application: HTTP 上传 (group)
    application: RFC (group)
```

```
    application: ICMP-DETAIL (group)
    application: IP-RAW (group)
    application: IP 协议组 (group)
    application: TC_AD_KEY (group)
custom-group: TC_AD_Key
    application: WEB 应用 (group)
    application: HTTP 下载 (group)
    application: P2P-HTTP 下载
    application: 下载工具_MOBILE (group)
custom-group: route~route
    application: WEB 应用 (group)
    application: HTTP 下载 (group)
    application: HTTP 上传 (group)
custom-group: 1~route
    application: HTTP 下载 (group)
    application: HTTP 上传 (group)
```

【提示信息】 -

【平台说明】 -

2.23 show identify-application custom-rule

显示自定义应用规则。

show identify-application custom- rule

【参数说明】

参数	描述
-	-

【命令模式】 特权模式

【缺省级别】 14

【使用指导】 通过此命令可以所有自定义应用规则。

【配置举例】 1：查看应用分组

```
Ruijie# show identify-application custom- rule
TYPE NAME                        CLASS                           SPL   SPH   DPL   DPH   SIPL
SIPH            DIPL            DIPH
---- --------------------------- ------------------------------- ----- ----- ----- -----
--------------- --------------- --------------- ---------------
```

```
TCP  rule1                    TC_AD_KEY                    any   any   2     2     any
any            172.18.1.20    172.18.1.30
TCP  rule2                    TC_AD_KEY                    any   any   3     20    any
any            172.18.1.25    172.18.1.26
TCP  rule3                    数据库                       any   any   25    30    any
any            172.18.1.25    172.18.1.25
TCP  rule3                    数据库                       any   any   35    40    any
any            172.18.1.25    172.18.1.29
TCP  rule3                    数据库                       any   any   45    50    any
any            172.18.1.25    172.18.1.29
TCP  rule3                    数据库                       any   any   55    60    any
any            172.18.1.25    172.18.1.29
TCP  rule3                    数据库                       any   any   65    70    any
any            172.18.1.25    172.18.1.29
TCP  rule3                    数据库                       any   any   72    72    any
any            172.18.1.25    172.18.1.29
TCP  rule3                    数据库                       any   any   74    74    any
any            172.18.1.25    172.18.1.29
```

字段解释：

字段	说明
TYPE	协议信息。
NAME	规则名称
CLASS	规则所属应用分类
SPL	起始源端口
SPH	终止源端口
DPL	起始目的端口
DPH	终止目的端口
SIPL	起始源 IP 地址
SIPH	终止源 IP 地址
DIPL	起始目的 IP 地址
DIPH	终止目的 IP 地址

【提示信息】 -

【平台说明】 -

2.24 show identify-application dfi enable

查看应用识别 DFI 功能。

show identify-application dfi enable

【参数说明】

参数	描述
-	-

【命令模式】 特权模式

【缺省级别】 14

【使用指导】 通过此命令可以查看应用识别 DFI 功能。

【配置举例】 1：查看应用识别 DFI 功能

```
Ruijie# show identify-application dfi enable
dfi enable!
```

【提示信息】 -

【平台说明】 -

2.25 show identify-application enable

查看应用识别功能。

show identify-application enable

【参数说明】

参数	描述
-	-

【命令模式】 特权模式

【缺省级别】 14

【使用指导】 通过此命令可以查看应用识别功能。

【配置举例】 1：查看应用识别功能

```
Ruijie# show identify-application enable
on
```

【提示信息】 -

【平台说明】 -

2.26 show identify-application group-state

显示分组模式。

show identify-application group-state

【参数说明】

参数	描述
-	-

【命令模式】 特权模式

【缺省级别】 14

【使用指导】 通过此命令可以查看当前分组模式。

【配置举例】 1：显示应用分类信息：

```
Ruijie#show identity-application group-state
app group state: on
```

字段解释：

字段	说明
app group state	on 当前应用按关键应用组，抑制应用组用组，IP 协议组进行分组

【提示信息】 -

【平台说明】 -

2.27 show identify-application inhibitive

显示加入抑制应用组的应用或分类。

show identify-application inhibitive

【参数说明】

参数	描述
-	-

【命令模式】 特权模式

【缺省级别】 14

【使用指导】 通过此命令可以查看当前那些应用或分类加入了抑制应用组。

【配置举例】 1：显示抑制应用组中的应用

```
Ruijie# show identity-application inhibitive
股票软件
百度下吧
迅雷
```

【提示信息】 -

【平台说明】 -

2.28 show identify-application key

显示加入关键应用组的应用或分类。

show identify-application key

【参数说明】

参数	描述
-	-

【命令模式】 特权模式

【缺省级别】 14

【使用指导】 通过此命令可以查看当前那些应用或分类加入了关键应用组。

【配置举例】 1：显示关键应用组中的应用

```
Ruijie# show identity-application key
MSN
QQ
```

【提示信息】 -

【平台说明】 -

2.29 show identify-application other

显示其它应用组的应用或分类。

show identify-application other

【参数说明】

参数	描述
-	-

【命令模式】 特权模式

【缺省级别】 14

【使用指导】 通过此命令可以查看当前那些应用或分类加入了其它应用组。

【配置举例】 1：显示其它应用组中的应用

```
Ruijie# show identity-application other
MSN
QQ
```

【提示信息】 -

【平台说明】 -

2.30 show identify-application proto-detect enable

显示协议探测的信息。

show identify-application proto-detect enable

【参数说明】

参数	描述
-	-

【命令模式】 特权模式

【缺省级别】 14

【使用指导】 通过此命令可以查看当前的协议探测信息。

【配置举例】 1：显示协议预期基本信息

```
Ruijie#show identify-application proto-detect enable
proto-detect is on
```

【提示信息】 -

【平台说明】 -

2.31 show identify-application proto-expect enable

显示协议预期的信息。

show identify-application proto-expect enable

【参数说明】

参数	描述
-	-

【命令模式】 特权模式

【缺省级别】 14

【使用指导】 通过此命令可以查看当前的协议预期信息。

【配置举例】 1：显示协议预期基本信息

```
Ruijie#show identify-application proto-expect enable
Proto-expect is enable
Proto-expect app_db is unable
Proto-expect timeout is not set[0s]
```

【提示信息】 -

【平台说明】 -

2.32 show identify-application version

显示特征库版本号信息。

show identify-application version

【参数说明】

参数	描述
-	-

【命令模式】 特权模式

【缺省级别】 14

【使用指导】 通过此命令可以查看当前特征库版本信息。

【配置举例】 1：查看当前特征库版本信息

```
Ruijie# show identify-application version
```

```
Version:2013.06.10.13.06.10(V2.0)
```

字段解释：

字段	说明
Version	版本号。

【提示信息】 -

【平台说明】 -

3 APP-ROUTE

3.1 app route app-name

配置应用路由功能策略。

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*]

删除应用路由功能策略。

no app route priority-num *priority-num*

恢复缺省配置。

default app route priority-num *priority-num*

【参数说明】

参数	描述
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*。
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”任意。
sip-group-number	源 ip-group id，需要先进行 ip-group 的配置，指定符合该 ip-group 的源地址才进行应用路由选路。取值范围在 1-1000。
dip-group-number	目的 ip-group id，需要先进行 ip-group 的配置，指定符合该 ip-group 的目的地址才进行应用路由选路。取值范围在 1-1000。
url-group-name	url-group 名称，可以是系统自带的域名组，如“视频~sys”，也可以是用户自定义域名组，或者“any”任意。
dest-ip-address	配置 url-group 的前提下，指定该域名组域名解析需要使用的 dns 服务器地址。
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	规则关联的 track 对象的 id。
description-name	该条应用路由策略的备注，如 sys 表示快速向导自动生成的。

【缺省配置】 未配置应用路由策略。

【命令模式】 全局模式

【缺省级别】 14

【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。应用类型可以是“应用分类”，“应用软件”，“应用软件子类”或“应用分组”。应用路由仅支持可首报文识别的应用类型，随着应用识别功能能力的提高，支持应用路由的应用类型将会越来越多。具体请参考应用识别的配置文档说明。

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；应用类型存在且支持首保文识别；url-group 域名组对象存在；track 跟踪状态为生效。

【配置举例】 1：配置应用路由基于接口出口功能。

```
Ruijie(config)# app route priority-num 2 P2P 应用软件 interface GigabitEthernet 0/4 time-range any
```

2：配置应用路由基于接口组出口功能。

```
Ruijie(config)# app route priority-num 3 抑制流量~route interface-group intf_group
```

3：配置应用路由基于 time-range 功能。

```
Ruijie(config)# app route priority-num 3 抑制流量~route interface-group intf_group time-range on-work
```

4：配置应用路由基于 ip-group 功能。

1）指定源 ip-group

```
Ruijie(config)# app route priority-num 2 any sip-group 1 interface-group intf_group time-range any
```

2）指定目的 ip-group

```
Ruijie(config)# app route priority-num 2 any dip-group 2 interface-group intf_group time-range any
```

3）同时指定源与目的 ip-group

```
Ruijie(config)# app route priority-num 2 any sip-group 1 dip-group 2 interface-group intf_group time-range any
```

5：配置应用路由基于 url-group 功能。

1） 不指定域名解析使用的 dns 服务器

```
Ruijie(config)# app route priority-num 2 any url-group QQ 网吧 interface GigabitEthernet 0/3
```

```
time-range any
```

2） 指定域名解析使用的 dns 服务器

```
Ruijie(config)# app route priority-num 2 any url-group google change-dest 8.8.8.8 interface GigabitEthernet 0/3 time-range any
```

6：配置应用路由基于 track 功能。

```
Ruijie(config)# app route priority-num 2 any url-group google change-dest 8.8.8.8 interface GigabitEthernet 0/3 time-range any track 1
```

7：配置应用路由基于协议号、端口号功能。

Ruijie(config)# app route priority-num 2 any protocol tcp sport 1 1000 dport 80 interface GigabitEthernet 0/3 time-range any

【检验方法】 1：使用 **show app route** 命令，可以查看应用路由模块配置，以及是否生效信息。

2：使用 **show app route statistics** 命令可以查看应用路由模块统计信息。

3：使用 **show app route priority-num 2 session** 命令可以查看应用路由优先级 id 为 1 的会话信息。

【提示信息】 1：如果接口/接口组中成员未配置接口网关，则提示：

```
Ruijie(config)# app route priority-num 2 P2P 应用软件 interface GigabitEthernet 0/4 time-range any
%notice: App route will not work on interface GigabitEthernet 0/4 because there is not gateway on it.
```

2：如果应用路由策略接口组不存在，则提示：

```
Ruijie(config)# app route priority-num 2 P2P 应用软件 interface-group intf_group time-range any
%warning: Interface group intf_group does not exist.
```

3：如果应用路由策略接口属性为 LAN，则提示：

```
Ruijie(config)# app route priority-num 2 P2P 应用软件 interface GigabitEthernet 0/0 time-range any
%warning: Interface GigabitEthernet 0/0 is not WAN port.
```

4：如果应用路由策略条数超过 500 条，则提示：

```
Ruijie(config)# app route priority-num 2 P2P 应用软件 interface GigabitEthernet 0/4 time-range any
%warning: The num of app-route exceed limit 500, cannot add app-route.
```

5：如果应用路由策略应用对象不存在，则提示：

```
Ruijie(config)# app route priority-num 2 mytest interface GigabitEthernet 0/4 time-range any
%notice: APP route will not work because app test is not exist or not supported for app-route, please use 'show identify-application routable' to check it
```

6：如果 url-group 域名组对象不存在，则提示：

Ruijie(config)#app route priority-num 2 any url-group mytest interface gigabitEthernet 0/3 time-range any

%notice: APP route will not work because url group:"mytest" is not exist.

7：如果时间对象不存在，则提示：
Ruijie(config)#app route priority-num 2 any url-group mytest interface gigabitEthernet 0/3 time-range mytest
%notice: APP route will not work because time range:"mytest" is not exist.

8：如果针对域名组指定的域名解析 dns 服务器配置错误，则提示：
Ruijie(config)#app route priority-num 2 any url-group mytest change-dest 127.0.0.1 interface gi0/3 time-range any
%warning: Url change-dest ip address invalid.

【常见错误】 1：接口组名不存在。
2：应用路由策略接口属性为 LAN 属性。
3：应用路由策略条数超过最大 500 条。
4：应用类型不支持首保文识别。
5：时间对象不存在或者不在有效时间内。
6：域名组对象不存在。
7：端口范围结束值小于开始值。

【平台说明】 -

3.2 app route priority-num priority-number priority

配置应用路由模块优先级功能。
app route priority-num *priority-number* **priority** { **increase** | **decrease** } [*1-1999*]

【参数说明】

参数	描述
priority-num	应用路由优先级，唯一标识这条策略，取值范围在 1-10000。
[*1-1999*]	调整距离，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。

【缺省配置】 -

【命令模式】 全局模式

【缺省级别】 14

【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。配置时也可指定优先级，优先级数值越大，优先级越高。
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】 1：配置应用路由策略优先级提升 1，这里的 1 是相对的，假设当前有两条应用路由策略，其中一条优先级为

20，一条为 40，将 20 的优先级提升 1，表示其优先级变为 40，原来 40 的变为 20。

```
Ruijie(config)# app route priority-num 20 P2P 应用软件 priority increase 1
```

2、配置应用路由策略优先级降低 1，同提升，这里的 1 也是相对的。

Ruijie(config)# app route priority-num 40 P2P 应用软件 priority decrease 1

【检验方法】 1：使用 **show app route** 命令，可以查看应用路由模块配置信息。

【提示信息】

```
1：如果应用路由策略不存在，则提示：
Ruijie(config)# app route priority-num 333 priority increase 100
%warning: app route priority-num 333 is not exist.
```

【常见错误】 1：应用路由策略不存在。

【平台说明】 -

3.3 app route enable

开启应用路由模块转发使能开关。

app route enable

关闭应用路由模块转发使能。

no app route enable

恢复缺省配置。

default app route enable

【参数说明】

参数	描述
-	-

【缺省配置】 关闭应用路由转发使能功能。

【命令模式】 全局模式

【缺省级别】 14

【使用指导】 该命令用于打开应用路由转发功能。只有打开应用路由转发功能，配置的应用路由策略才能生效。

【配置举例】 1：启动应用路由模块转发使能功能。

```
Ruijie(config)# app route enable
```

2：关闭应用路由模块转发使能功能。

```
Ruijie(config)#no app route enable
```

【检验方法】 1：使用 **show app route** 命令，可以查看应用路由模块状态。

【提示信息】 -

【常见错误】 -

【平台说明】 -

3.4 app route mode new-flow

设置应用路由策略只对新建连接生效。

app route mode new-flow

设置应用路由策略对所有连接生成。

no app route mode new-flow

恢复缺省配置

default app route mode new-flow

【参数说明】

参数	描述
-	-

【缺省配置】 不同型号设备缺省值不同。

【命令模式】 全局模式

【缺省级别】 14

【使用指导】 该命令用来控制应用路由的策略是否只针对新建连接生效，开启后应用路由策略的变化将不影响已经被应用路由选路的流量，即不影响旧流的选路。关闭后，应用路由策略的变化将立即生效，即会影响所有的流量。

【配置举例】 1：开启应用路由策略只对新建连接生效。

```
Ruijie# app route mode new-flow
```

2：关闭应用路由策略只对新建连接生效。

```
Ruijie# no app route mode new-flow
```

【检验方法】 1：使用 **show run | include app route** 命令，可以查看应用路由模块状态。

【提示信息】 -

【常见错误】 -

【平台说明】 -

3.5 interface-group

配置接口组对象功能。
interface-group *interface-group-name*

删除接口组对象。
no interface-group *interface-group-name*

恢复缺省配置。
default interface-group *interface-group-name*

【参数说明】

参数	描述
interface-group-name	接口组名称

【缺省配置】 未配置接口组对象

【命令模式】 全局模式

【缺省级别】 14

【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。

【配置举例】 1：配置接口组。

```
Ruijie(config)# interface-group intf-grp
```

【检验方法】 1：使用 **show interface-group** 命令，可以查看接口组模块配置信息。

【提示信息】 1：如果接口组队形名称长度超过 31，则提示：

```
Ruijie(config)# interface-group intf-grpxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx
%warning: Interface group name can not be more than 31 characters.
```

【常见错误】 1：配置接口组对象名称长度超过 31

【平台说明】 -

3.6 interface-member

配置接口组接口成员。
interface-member *interface-name* [**weight** *weight-number*]

删除接口成员对象。
no interface-member *interface-name*

恢复缺省配置。
default interface-member *interface-name*

【参数说明】

参数	描述
interface-name	接口名。
weight-number	接口均衡权重值，取值范围在：1- 40000000，单位 kilobits。

【缺省配置】 未配置接口组接口成员。

一个接口组下最多支持 32 个接口成员，且接口成员必须是非 LAN 属性出口。

【命令模式】 接口组模式

【缺省级别】 14

【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 口默认属于非 LAN 口，可以加入接口组。
该命令支持自定义接口的均衡权重值，默认权重值为接口的下行带宽（单位 kilobits）。

【配置举例】 1：配置接口成员功能。

```
Ruijie(config-intf-group)#interface-member gi0/1
```

2：删除接口成员功能。

```
Ruijie(config-intf-group)#no interface-member gi0/1
```

3：配置接口成员均衡权重值。

```
Ruijie(config-intf-group)#interface-member gi0/1 weight 100000
```

4：删除与恢复默认接口成员均衡权重值。

```
Ruijie(config-intf-group)#interface-member gi0/1
```

【检验方法】 1：使用 **show interface-group** 命令，可以查看接口组模块配置信息。

【提示信息】 1：如果接口成员为 LAN 属性出口，则提示：

```
Ruijie(config-intf-group)#interface-member gi0/0
%warning: It's only allowed to add WAN interface to interface group.
```

2：如果接口成员数目超过 32 个，则提示：

```
Ruijie(config)# interface-member gi0/1
%warning: The num of interface in one group exceed limit 32 cannot add interface.
```

【常见错误】 1：接口成员属性 LAN。
2：接口成员数目超过 32 个。

【平台说明】 -

3.7 load-balance policy

配置接口组策略功能。
load-balance policy { **bandwidth** | **load** }

恢复接口组默认策略配置。
no load-balance policy

恢复缺省配置。
default load-balance policy

【参数说明】

参数	描述
-	-

【缺省配置】 默认基于 bandwidth 带宽方式。

【命令模式】 接口组模式

【缺省级别】 14

【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，或者自定义的接口均衡权重值，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。

【配置举例】 1：配置接口组基于带宽策略负载。

```
Ruijie(config-intf-group)#load-balance policy bandwidth
```

2：配置接口组基于负载策略负载。

```
Ruijie(config-intf-group)#load-balance policy load
```

【检验方法】 1：使用 **show interface-group** 命令，可以查看接口组配置信息。

【提示信息】 -

【常见错误】 -

【平台说明】 -

3.8 nexthop

配置接口网关功能。
nexthop *ip-address*

取消接口网关功能。
no nexthop

恢复缺省配置。
default nexthop

【参数说明】

参数	描述
ip-address	IP 地址

【缺省配置】 默认未配置网关信息

【命令模式】 接口模式

【缺省级别】 14

【使用指导】 该命令指定接口的网关，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。

【配置举例】 1：配置接口网关功能。

```
Ruijie(config-if-GigabitEthernet 0/1)#nexthop 2.2.2.2
```

2：取消接口网关功能。

```
Ruijie(config-if-GigabitEthernet 0/1)#no nexthop
```

【检验方法】 1：使用 **show run interface gigabitEthernet 0/1** 命令，可以查看接口下一跳配置信息。

【提示信息】 1：如果给 dialer 接口配置网关，则提示：

```
Ruijie(config)#interface dialer 1
Ruijie(config-if-dialer 1)#nexthop 1.1.1.1
%warning: Can't add gateway because interface dialer 1 is P2P port.
```

2：如果给配有 DHCP 地址的接口配置网关，则提示：

```
Ruijie(config-if-GigabitEthernet 0/1)#nexthop 2.2.2.2
%warning: Can't add/del gateway because interface GigabitEthernet 0/1 has dhcp address.
```

3：如果接口配置网关与接口 IP 地址相同，则提示：

```
Ruijie(config-if-GigabitEthernet 0/1)#nexthop 192.168.23.109
%warning: Invalid gateway address. (It's this router).
```

【常见错误】 1：设备在 P2P 接口配置网关。
2：DHCP 接口配置网关。
3：接口网关配置同接口 IP 地址信息。

【平台说明】 -

3.9 show app route

查看应用路由配置信息。

show app route [**statistics** | **priority-num** *priority-num* **session**]

【参数说明】

参数	描述
priority-num	应用路由优先级，唯一标识这条策略，取值范围在 1-10000。

【命令模式】 特权模式、全局模式、接口模式

【缺省级别】 14

【使用指导】 **show app route** 命令显示已配置的应用路由当前状态信息。显示排列顺序是优先级有高到低，显示在最上面的优先级最高。
show app route statics 显示应用路由总体统计信息。
show app route priority-num *priority-num* **session** 显示特定应用路由的会话信息。

【配置举例】 1：查看设备应用路由模块配置信息。

```
Ruijie(config)#show app route
CLASS                              SRC-GRP     DST-GRP(URL)
```

```
INTERFACE(GROUP)                 TIME-RANGE                 STATE
-------------------------------- ---------- ----------------------------------------------
------------------------------ ------------------------- ----------
any                                any         2(QQ 网吧;114.114.114.114)
GigabitEthernet 0/4              any                       Inactive
any                                1           any
test(group)                      any                       Inactive
```

HTTP 协议 any any

GigabitEthernet 0/3 any Active

字段解释：

字段	说明
CLASS	配置了应用路由的应用类型的名称(可以是应用软件子类名/应用软件名/应用分类名/应用分组名)。
SRC-GRP	源 ip-group 的 id 号，any 表示没有配置。
DST-GRP(URL)	目的 ip-group 的 id 号，any 表示没有配置。括号内为 url-group 的域名对象，其中 ip 地址为指定的域名解析 dns 服务器。
INTERFACE(GRPUP)	接口/接口组名。
TIME-RANGE	Time-range 对象。
STATE	路由策略当前状态。

2：查看应用路由统计信息。

```
Ruijie(config)#show app route statistics
CLASS                            SRC-GRP    DST-GRP(URL)
INTERFACE(GROUP)                 Flows
-------------------------------- ---------- ----------------------------------------------
------------------------------ ----------
any                                any         2(QQ 网吧;114.114.114.114)
GigabitEthernet 0/4              0
any                                1           any
test(group)                      0
HTTP 协议                          any         any
GigabitEthernet 0/3              0
Ruijie(config)#
```

字段解释：

字段	说明
CLASS	配置了应用路由的应用类型的名称(可以是应用软件子类名/应用软件名/应用分类名/应用分组名)。
SRC-GRP	源 ip-group 的 id 号，any 表示没有配置。
DST-GRP(URL)	目的 ip-group 的 id 号，any 表示没有配置。括号内为 url-group 的域名对象，其中 ip 地址为指定的域

	名解析 dns 服务器。
INTERFACE(GRPUP)	接口/接口组名。
Flows	该条应用路由策略所引流的连接数。

3：查看应用路由应用对象“HTTP 视频”会话信息。

```
Ruijie(config)#show app route HTTP 协议 session
SIP:PORT               DIP:PORT               PRO-NUM  INTF       SUM DATA(byte)
---------------------- ---------------------- -------- ----------
---------------------------------------
192.169.255.100:6007   14.17.41.174:80        6        Gi0/3      368/1001
192.169.255.100:6006   14.17.41.174:80        6        Gi0/3      446/6722
192.169.255.100:6006   14.17.41.174:80        6        Gi0/3      368/1452
```

字段解释：

字段	说明
SIP	源 IP
SPORT	源端口
DIP	目的 IP
DPORT	目的端口
PRO-NUM	协议号
INTF	接口名称
SUM DATA(byte)	该会话的总流量，包含上传/下载统计

【提示信息】 -

【平台说明】 -

3.10 show interface-group

查看接口组配置信息。

show interface-group

【参数说明】

参数	描述
-	-

【命令模式】 特权模式、全局模式、接口模式

【缺省级别】 14

【使用指导】 显示设备所有接口组配置信息。

【配置举例】 1：查看设备接口组模块配置信息。

```
Ruijie #show interface-group
------------------------------------------------------------
GROUP-NAME: intf_group
INTERFACE INCLUDED: di1,di2,di3
POLICY: load
STATE: UP
```

字段解释：

字段	说明
GROUP-NAME	接口组名称
INTERFACE INCLUDED	包含接口
POLICY	均衡策略
STATE	接口组状态

【提示信息】 -

【平台说明】 -

4 APP-PROXY

4.1 app-proxy enable

开启应用代理功能。
app-proxy enable

关闭应用代理功能。
no app-proxy enable

【参数说明】

参数	描述
-	-

【缺省配置】 默认开启

【命令模式】 全局配置模式

【缺省级别】 14

【使用指导】 通过此命令开启应用代理功能。

【配置举例】 1：开启应用代理功能。

```
Ruijie#config
Ruijie(config)#app-proxy enable
```

【检验方法】 1：使用 **show app-proxy enable** 命令，可以查看应用代理功能是启用还是关闭。

【提示信息】 -

【常见错误】 -

【平台说明】 -

4.2 app-proxy http enable

开启 HTTP 应用代理功能。
app-proxy http enable

关闭 HTTP 应用代理功能。

no app-proxy http enable

【参数说明】

参数	描述
-	-

【缺省配置】 默认开启

【命令模式】 全局配置模式

【缺省级别】 14

【使用指导】 通过此命令开启 HTTP 应用代理功能。

【配置举例】 1：开启 HTTP 应用代理功能。

```
Ruijie#config
Ruijie(config)#app-proxy http enable
```

【检验方法】 1：使用 **show app-proxy enable** 命令，可以查看 HTTP 应用代理功能是启用还是关闭。

【提示信息】 -

【常见错误】 -

【平台说明】 -

4.3 show app-proxy enable

查看应用代理功能开关。

show app-proxy enable

【参数说明】

参数	描述
-	-

【命令模式】 特权模式、全局模式、接口模式

【缺省级别】 14

【使用指导】 使用该命令可以查看应用代理的相关功能开关状态。

【配置举例】 1： 应用代理功能开关

```
Ruijie#show app-proxy enable
app-proxy                                :   Y
app-proxy http                           :   Y
app-proxy udp                            :   Y
app-proxy url                            :   Y
app-proxy dns                            :   Y
```

字段解释：

字段	说明
app-proxy	应用代理总开关
app-proxy http	HTTP 应用代理开关
app-proxy udp	UDP 掐流功能开关
app-proxy url	DNS 引流库使能开关
app-proxy dns	应用代理 DNS 功能开关

【提示信息】 -

【平台说明】 -

5 全局会话数限制

5.1 flow-pre-mgr { down-deny | down-permit }

对上行新建报文进行过滤

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** } } } }

删除某条过滤规则

no flow-pre-mgr { **down-deny** | **down-permit** } *id*

【参数说明】

参数	描述
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

【缺省配置】 无配置

【命令模式】 全局模式

【缺省级别】 14

【使用指导】 功能和 ip session filter 一样都是用于报文过滤，只是两者的性能上有区别，如果配置的 ACL 有大量 ACE 的话，建议使用该条命令，性能会有所提升。 该命令用于对下行兴建报文进行过滤，与之配套的还有对上行新建报文进行过滤的命令。

配置上行新建报文过滤规则时，源 IP 不能为 any。

配置下行新建报文过滤规则时，目的 IP 不嫩为 any。

Permit 和 deny 规则有各自的 ID，不会冲突。

Deny 规则的优先级大于 permit 规则。

【配置举例】 配置不允许外网访问设备除了 80 端口外的所有端口，禁止外网 IP 110.110.110.24 ping 设备。设备 IP172.18.124.118

```
Ruijie# configure terminal
Ruijie(config)# flow-pre-mgr down-deny 1 icmp src-host 110.110.110.24 dst-host 172.18.124.118
Ruijie(config)# flow-pre-mgr down-permit 1 tcp src-host any src-port any dst-host 172.18.124.118 dst-port 80
Ruijie(config)# flow-pre-mgr down-permit 2 udp src-host any src-port any dst-host 172.18.124.118 dst-port 80
```

【检验方法】 1、 使用 show flow-pre-mgr drop-count 查看丢包情况。
2、 使用 show ip session filter 查看每条规则匹配的报文数。

【提示信息】 -

【常见错误】 -

【平台说明】 -

5.2 flow-pre-mgr port-limit range { tcp | udp }

添加端口限制的端口范围
flow-pre-mgr port-limit range { **tcp** | **udp** } *port-start port-end*

删除某个端口范围
no flow-pre-mgr port-limit range { **tcp** | **udp** } *port-start port-end*

【参数说明】

参数	描述
port-start	端口范围的起始端口
port-end	端口范围的结束端口

【缺省配置】 默认设置的端口有：tcp 445

【命令模式】 全局模式

【缺省级别】 14

【使用指导】 1）默认存在 tcp 445 端口的限制。
2）配合 **flow-pre-mgr port-limit ratio** *num* 命令使用。
3）支持多个子功能的端口会话数限制：总会话数限制、新建会话数限制（真实 ip、特殊 ip 和虚拟 ip）、基于 acl 的总会话数限制、基于用户的每 ip 会话数限制。
4）所有子功能共用端口范围。

【配置举例】 配置总会话数限制 10000；配置真实 ip 新建流速率 300；配置基于用户的每 ip 会话数限制 500；配置基于 acl 的总会话数限制 5000；再配置 tcp 12200 端口为限制端口，限制百分比为百分之 10。

```
Ruijie# configure terminal
Ruijie(config)# flow-pre-mgr total-limit 10000
Ruijie(config)# flow-pre-mgr new-session-limit real-host limit 300
Ruijie(config)# flow-pre-mgr 1 access-list 1 action trust total-limit 5000
Ruijie(config)# flow-pre-mgr 2 subscriber any action trust total-limit 0 per-ip-limit 500
Ruijie(config)# flow-pre-mgr port-limit range tcp 12200 12200
Ruijie(config)# flow-pre-mgr port-limit ratio 10
```

【检验方法】
1. 使用 show flow-pre-mgr ip-info 查看每 ip 端口会话数以及限制值。
2. 使用 show flow-pre-mgr drop-count 查看丢包情况。

【提示信息】 -

【常见错误】 -

【平台说明】 EG 系列产品支持。

5.3 flow-pre-mgr port-limit ratio

配置端口限制的百分比
flow-pre-mgr port-limit ratio *num*

恢复端口限制百分比默认值
no flow-pre-mgr port-limit ratio

【参数说明】

参数	描述
num	端口限制百分比

【缺省配置】 默认百分之 5

【命令模式】 全局模式

【缺省级别】 14

【使用指导】
1）默认限制百分之 5。
2）配合 **flow-pre-mgr port-limit range** { **tcp** | **udp** } 命令使用。
3）支持多个子功能的端口会话数限制：总会话数限制、新建会话数限制（真实 ip、特殊 ip 和虚拟 ip）、基于 acl 的总会话数限制、基于用户的每 ip 会话数限制。
4）所有子功能共用端口限制百分比。

【配置举例】 配置总会话数限制 10000；配置真实 ip 新建流速率 300；配置基于用户的每 ip 会话数限制 500；配置基于 acl 的总会话数限制 5000；再配置 tcp 12200 端口为限制端口，限制百分比为百分之 10。

```
Ruijie# configure terminal
Ruijie(config)# flow-pre-mgr total-limit 10000
Ruijie(config)# flow-pre-mgr new-session-limit real-host limit 300
Ruijie(config)# flow-pre-mgr 1 access-list 1 action trust total-limit 5000
Ruijie(config)# flow-pre-mgr 2 subscriber any action trust total-limit 0 per-ip-limit 500
Ruijie(config)# flow-pre-mgr port-limit range tcp 12200 12200
Ruijie(config)# flow-pre-mgr port-limit ratio 10
```

【检验方法】
1. 使用 show flow-pre-mgr ip-info 查看没 ip 端口会话数以及限制值。
2. 使用 show flow-pre-mgr drop-count 查看丢包情况。

【提示信息】 -

【常见错误】 -

【平台说明】 EG 系列产品支持。

5.4 flow-pre-mgr { up-deny | up-permit }

对上行新建报文进行过滤

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** } } } }

删除某条过滤规则

no flow-pre-mgr { **up-deny** | **up-permit** } *id*

【参数说明】

参数	描述
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

【缺省配置】 无配置

【命令模式】 全局模式

【缺省级别】 14

【使用指导】 功能和 ip session filter 一样都是用于报文过滤，只是两者的性能上有区别，如果配置的 ACL 有大量 ACE 的话，建议使用该条命令，性能会有所提升。 该命令用于对上行兴建报文进行过滤，与之配套的还有对下行新建报文进行过滤的命令。
配置上行新建报文过滤规则时，源 IP 不能为 any。
配置下行新建报文过滤规则时，目的 IP 不嫩为 any。
Permit 和 deny 规则有各自的 ID，不会冲突。
Deny 规则的优先级大于 permit 规则。

【配置举例】 配置允许内网 192.168.1.0/24 网段和 172.18.1.0/24 网盾的 IP 上网，但是禁止其中 192.168.1.24 这个 IP 上网。

```
Ruijie# configure terminal
Ruijie(config)# flow-pre-mgr up-deny 1 ip src-host 192.168.1.24 dst-host any
Ruijie(config)# flow-pre-mgr up-permit 1 ip src-subnet 192.168.1.0 255.255.255.0 dst-host any
Ruijie(config)# flow-pre-mgr up-permit 2 ip src-subnet 172.18.1.0 255.255.255.0 dst-host any
```

【检验方法】 3、 使用 show flow-pre-mgr drop-count 查看丢包情况。
4、 使用 show ip session filter 查看每条规则匹配的报文数。

【提示信息】 -

【常见错误】 -

【平台说明】 -

5.5 flow-pre-mgr access-list

配置基于 ACL 的会话数限制值
flow-pre-mgr *rule-id* **access-list** *acl-number* **action** { **block** | **by-pass** | { **trust total-limit** *total-limit-number* } }

删除基于 ACL 的会话数限制规则
no flow-pre-mgr *rule-id*

【参数说明】

参数	描述
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 *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。

【缺省配置】 无相关配置

【命令模式】 全局模式

【缺省级别】 14

【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；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。


必须先配置 ACL。

【配置举例】 1、配置一条 ACL 用于匹配设备与外网 IP：220.200.20.20 建立的流，限制其流会话数为 30 条。

```
Ruijie# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Ruijie(config)#ip access-list extended 120
Ruijie(config-ext-nacl)#permit ip any host 220.220.20.20
Ruijie(config-ext-nacl)#deny ip any any
Ruijie(config-ext-nacl)#exit
Ruijie(config)#flow-pre-mgr 2 access-list 120 action trust total-limit 30
```

2、假设内网 IP 网段为 192.168.1.0/24，我们的需求是除了内网网段的 IP 需要创建流会话，其余的都 by-pass 处理。

```
Ruijie# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Ruijie(config)#ip access-list standard 2
Ruijie(config-std-nacl)#deny 192.168.1.0 0.0.0.255
Ruijie(config-std-nacl)#permit any
Ruijie(config-ext-nacl)#exit
Ruijie(config)# flow-pre-mgr 1 access-list 1 action by-pass
```

【检验方法】 1、使用 show flow-pre-mgr rule-info 查看配置的规则以及会话匹配情况；
2、使用 show flow-pre-mgr ip-info 查看 IP 的会话以及限制情况。

【提示信息】 1：如果规则 ID 已经被使用，则提示错误。

```
Rule id already exists, please delete it first
```

【常见错误】 未配置指定的 ACL。

【平台说明】 -

5.6 flow-pre-mgr enable

启动全局会话数限制功能
flow-pre-mgr enable

关闭全局会话数限制功能
no flow-pre-mgr enable

【参数说明】

参数	描述
-	-

【缺省配置】 开启状态

【命令模式】 全局模式

【缺省级别】 14

【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。

【配置举例】 关闭全局会话数限制功能。

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

```
Ruijie(config)# no flow-pre-mgr enable
```

【检验方法】 使用 show running-config 来查看是否存在 no flow-pre-mgr enable，不存在就是开启状态。

【提示信息】 -

【常见错误】 -

【平台说明】 -

5.7 flow-pre-mgr new-session-limit { specify | specify-range | specify-subnet }

配置真实 IP 的新建连接数限制后，可能某些特殊的 IP（如服务器）需要放宽限制值。

flow-pre-mgr new-session-limit { **specify** *ip-addr* | **specify-range** *ip-start ip-end* | **specify-subnet** *ip-subnet ip-mask* } **limit** *limit-number*

删除指定真实 IP 的新建连接限制

no flow-pre-mgr new-session-limit { **specify** *ip-addr* | **specify-range** *ip-start ip-end* | **specify-subnet** *ip-subnet ip-mask* }

【参数说明】

参数	描述
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：0-10000000

【缺省配置】 缺省配置为 0，即不限制

【命令模式】 全局模式

【缺省级别】 14

【使用指导】 配置真实 IP 的新建连接数限制后，可能某些特殊的 IP（如服务器）需要放宽限制值。

【配置举例】 配置内网真实 IP 的新建连接速度不能超过 1000，服务器网段（192.168.1.0/24）的新建连接配置成 10000。

```
Ruijie# configure terminal
Ruijie(config)# flow-pre-mgr new-session-limit real-host limit 1000
```

```
Ruijie(config)# flow-pre-mgr new-session-limit specify-subnet 192.168.1.0 255.255.255.0 limit 10000
```

【检验方法】 1、 使用 show flow-pre-mgr new-session-limit 查看配置。
2、 使用 show flow-pre-mgr drop-count 查看丢包情况。
3、 使用 show flow-pre-mgr new-session-limit attack 查看疑似攻击源。

【提示信息】 -

【常见错误】 -

【平台说明】 -

5.8 flow-pre-mgr new-session-limit { start-up | virtual-host | real-host }

设置设备启机三分内的所有虚拟 IP 的新建连接数限制，超过限制值流平台进行丢包；
设置启机三分钟后，虚拟 IP 的新建连接数限制，超过限制值流平台进行丢包；
设置真实 IP 的新建连接数限制，超过限制值流平台进行丢包。

flow-pre-mgr new-session-limit { **start-up** | **virtual-host | real-host** } **limit** *limit-number*

删除新建连接限制
no flow-pre-mgr new-session-limit { **start-up** | **virtual-host | real-host** }

【参数说明】

参数	描述
limit-number	新建连接限制值，取值范围 0-10000000

【缺省配置】 缺省配置为 0，即不限制

【命令模式】 全局模式

【缺省级别】 14

【使用指导】 为了防止内网真实 IP 因中毒等原因对设备或外网发起大量新建攻击，可以为内网 IP 配置新建连接限制。
Start-up：设备刚启机或者本内核模块重新加载的时候，所有的上线 IP 一开始都当成虚拟 IP 来处理，所有虚拟 IP 的新建连接速率是累加到一起进行计算的，即新建连接限制值是公用的，为了应对设备启机，内网用户集中上线，需要把这时候的新建连接限制放宽（经验值 20000~30000），或者不设限制值。
Virtual-host：设备启机或者本内核模块重新加载三分钟后，虚拟 IP 的新建连接速率限制值，同样也是所有虚拟 IP 的新建报文累加到一起进行新建速率计算，即新建连接限制值是所有虚拟 IP 公用的。经验值 3000 左右。
Real-host：真实 IP 的新建连接限制，每个 IP 的新建速率单独计算。

【配置举例】 配置设备启机三分钟内，虚拟 IP 的新建连接限制 20000；配置虚拟 IP 的新建连接限制 3000；配置真实 IP 的

新建连接限制 300

```
Ruijie# configure terminal
Ruijie(config)# flow-pre-mgr new-session-limit start-up limit 20000
Ruijie(config)# flow-pre-mgr new-session-limit virtual-host limit 3000
Ruijie(config)# flow-pre-mgr new-session-limit real-host limit 300
```

【检验方法】 1、 使用 show flow-pre-mgr new-session-limit 查看配置。
2、 使用 show flow-pre-mgr drop-count 查看丢包情况。
3、 使用 show flow-pre-mgr new-session-limit attack 查看疑似攻击源。

【提示信息】 -

【常见错误】 -

【平台说明】 -

5.9 flow-pre-mgr priority-swap

切换两条规则的优先级

flow-pre-mgr priority-swap *rule-id1 rule-id2*

【参数说明】

参数	描述
rule-id1	要切换优先级的规则 ID
rule-id2	要切换优先级的规则 ID

【缺省配置】 无

【命令模式】 全局模式

【缺省级别】 14

【使用指导】 使用此命令切换两条规则的优先级。

【配置举例】 切换规则 1 和规则 2 的优先级。

```
Ruijie# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Ruijie(config)# flow-pre-mgr priority-swmp 1 2
```

【检验方法】 使用 show flow-pre-mgr rule-info 查看切换后规则优先级。此命令优先级按照从高到低排列。

【提示信息】 -

【常见错误】 rule-id1 或 rule-id2 不存在，则命令不做任何处理。

【平台说明】 -

5.10 flow-pre-mgr protocol-enable

配置设备放行 OSPF、VRRP、RIP 协议
flow-pre-mgr protocol-enable

配置不放行协议
no flow-pre-mgr protocol-enable

【参数说明】

参数	描述
-	-

【缺省配置】 默认放行

【命令模式】 全局模式

【缺省级别】 14

【使用指导】 默认放行。
流预创建处理中的处理顺序是：ip session filte→协议放行→ IP 新建速率限制→buffe 保护

【配置举例】 开启协议放行。

```
Ruijie# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Ruijie(config)# flow-pre-mgr protocol-enable
```

【检验方法】 使用 show flow-pre-mgr protocol-enable 查看协议放行是否开启。

【提示信息】 -

【常见错误】 -

【平台说明】 -

5.11 flow-pre-mgr subscriber

配置基于用户/用户组的会话数限制值

flow-pre-mgr *rule-id* **subscriber** *subs_name* **action {block | by-pass | {trust total-limit** *total-limit-number* **per-ip-limit** *per-limit-number* **}}**

删除基于用户/用户组的会话数限制值

no flow-pre-mgr *rule-id*

【参数说明】

参数	描述
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。

【缺省配置】 无相关配置

【命令模式】 全局模式

【缺省级别】 14

【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；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。


必须先开启二三层用户识别以及配置对应的用户/用户组信息。

【配置举例】 配置用户组“UserGroupA”允许创建 5000 条流会话，并且“UserGroupA”下的每个 IP 允许创建的流会话数为 300，超过限制值后阻断新流的通信。

```
Ruijie# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Ruijie(config)# subscriber static name UserGroupA parent /
Ruijie(config)# subscriber static name UserA parent /UserGroupA ip-host 192.168.5.10
Ruijie(config)# subscriber static name UserB parent /UserGroupA ip-host 192.168.5.11
```

```
Ruijie(config)# flow-pre-mgr 1 subscriber UserGroupA action trust total-limit 5000 per-ip-limit 300
```

【检验方法】 1、使用 show flow-pre-mgr rule-info 查看配置的规则以及会话匹配情况；
2、使用 show flow-pre-mgr ip-info 查看 IP 的会话以及限制情况。

【提示信息】 1：如果规则 ID 已经被使用，则提示错误。

```
Rule id already exists, please delete it first
```

【常见错误】 未开启二三层用户识别或未配置用户/用户组信息。

【平台说明】 -

5.12 flow-pre-mgr per-ip-limit udp-ratio

配置基于用户/用户组的 UDP 会话数占总会话数的比例限制值
flow-pre-mgr per-ip-limit udp-ratio *ratio*

删除基于用户/用户组的 UDP 会话数占总会话数的比例限制值
no flow-pre-mgr per-ip-limit udp-ratio

【参数说明】

参数	描述
ratio	该用户/用户组下每 IP 的 UDP 流会话数占总会话数的比例限制值 ,取值范围为 0 和 30~80，其中 0 表示不限制。

【缺省配置】 0，即不限制

【命令模式】 全局模式

【缺省级别】 14

【使用指导】 1） 必须先配置基于用户/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，再配置 UDP 流会话数所占的比例值才会生效。
2） 默认配置为 0，即不限制 UDP。

> 必须先配置基于用户/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。

【配置举例】 配置所有用户允许创建的总流会话数不限制，每个 IP 允许创建的流会话数为 3000；再配置每 IP 的 UDP 流会话数占总会话数的比例为 50，超过限制值后阻断新 UDP 流的通信。

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

```
Ruijie(config)# flow-pre-mgr 1 subscriber UserGroupA action trust total-limit 0 per-ip-limit 3000
Ruijie(config)# flow-pre-mgr per-ip-limit udp-ratio 50
```

【检验方法】 1、使用 show flow-pre-mgr ip-info 查看 IP 的 UDP 会话以及限制情况。

【提示信息】 无

【常见错误】 未配置基于用户/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。

【平台说明】 NBR800G/950G/108G-P/1000G-E/1000G-C, EG680-P/2100-P/2000F 产品支持。

5.13 flow-pre-mgr total-limit

配置总的会话数限制值
flow-pre-mgr total-limit *limit-number*

删除总的会话数限制值
no flow-pre-mgr total-limit

【参数说明】

参数	描述
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。

【缺省配置】 无相关配置

【命令模式】 全局模式

【缺省级别】 14

【使用指导】 1） 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。
2） 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。

【配置举例】 配置全局的流会话数限制为 20 万，当流会话数达到 20 万时，不再允许创建流，并阻断。

```
Ruijie# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Ruijie(config)# flow-pre-mgr total-limit 200000
```

【检验方法】 1、使用 show flow-pre-mgr rule-info 查看配置的规则以及会话匹配情况；
2、使用 show flow-pre-mgr ip-info 查看 IP 的会话以及限制情况。

【提示信息】 -

【常见错误】 -

【平台说明】 -

5.14 flow-pre-mgr upload-pps-limit [virtual-host limit]

设置真实 IP/虚拟 IP 的上行包速限制。
flow-pre-mgr upload-pps-limit [virtual-host limit] *limit-number*

删除上行包速限制
no flow-pre-mgr upload-pps-limit [virtual-host]

【参数说明】

参数	描述
limit-number	上行包速限制值，取值范围 0-10000000

【缺省配置】 缺省配置为 0，即不限制

【命令模式】 全局模式

【缺省级别】 14

【使用指导】 通常在需要防上行流量攻击的情况下才开启本功能。
该命令针对识别成真实 IP/虚拟 IP 的 IP 生效，每个真实 IP/虚拟 IP 的上行报文速率单独计算。

【配置举例】 配置真实 IP 的上行包速限制为 2000。

```
Ruijie# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Ruijie(config)# flow-pre-mgr upload-pps-limit 2000
```

【检验方法】 1、 使用 show flow-pre-mgr upload-pps-limit 查看配置；
2、 使用 show flow-pre-mgr drop-count 查看上行包速限制的丢包情况。

【提示信息】 -

【常见错误】 -

【平台说明】 -

5.15 flow-pre-mgr upload-pps-limit { specify | specify-range | specify-subnet }

设置指定 IP 的上行包速限制

flow-pre-mgr upload-pps-limit { **specify** *ip-addr* | **specify-range** *ip-start ip-end* | **specify-subnet** *ip-subnet ip-mask* } **limit** *limit-number*

删除指定 IP 的上行包速限制

no flow-pre-mgr upload-pps-limit { **specify** *ip-addr* | **specify-range** *ip-start ip-end* | **specify-subnet** *ip-subnet ip-mask* }

【参数说明】

参数	描述
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：0-10000000

【缺省配置】 无相关配置

【命令模式】 全局模式

【缺省级别】 14

【使用指导】 通常在开启防上行流量攻击的情况下，要对某些特殊 IP（如内网服务器）进行个性化的设置，就可以使用该命令。

【配置举例】 配置内网用户每秒上行报文个数不能超过 3000；192.168.1.2 这个用户每秒只让他最多上行 10000 个报文。

```
Ruijie# configure terminal
Ruijie(config)# flow-pre-mgr upload-pps-limit 3000
Ruijie(config)# flow-pre-mgr upload-pps-limit specify 192.168.1.2 limit 10000
```

【检验方法】 1、 使用 show flow-pre-mgr upload-pps-limit 查看配置；
2、 使用 show flow-pre-mgr drop-count 查看上行包速限制的丢包情况。

【提示信息】 -

【常见错误】 -

【平台说明】 -

5.16 ip session filter

配置新建流过滤

Ip session filter *acl-id*

删除新建流过滤

no ip session filter

【参数说明】

参数	描述
acl-id	ACL 的 ID 号，用于新建报文过滤。

【缺省配置】 无相关配置

【命令模式】 全局模式

【缺省级别】 14

【使用指导】 设备建流前，进行 ACL 过滤，只放行合法 IP 的报文去建流，其他的都阻断。

【配置举例】 配置只允许 192.168.1.0 网段的 IP 建流，其他的都阻断。

```
Ruijie# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Ruijie(config)# ip access-list extended 190
Ruijie(config-ext-nacl)# 10 permit ip 192.168.1.0 0.0.0.255 any
Ruijie(config-ext-nacl)# exit
Ruijie(config)# ip session filter 190
```

【检验方法】 1、使用 show flow-pre-mgr drop-count 查看被 ACL 过滤掉的报文数；

【提示信息】 -

【常见错误】 -

【平台说明】 -

5.17 show flow-pre-mgr drop-count

查看 buffer 保护的日志记录

show flow-pre-mgr drop-count

【参数说明】

参数	描述
-	-

【命令模式】 特权模式、全局模式、接口模式

【缺省级别】 14

【使用指导】 使用该命令查看各个子功能的丢包数。

【配置举例】 查看丢包数

```
Ruijie#show flow-pre-mgr drop-count
DROP-TYPE           DROP-PKT
================================
Filter-pkt          42892
Session-real        0
Session-specify     0
Session-virtual     970
Session-cpu         0
PPS-real            0
PPS-specify         0
PPS-virtual         0
Session-real-port   190
Session-spec-port   0
Session-vt-port     0
Session-total-port  0
```

【提示信息】 -

【平台说明】 -

5.18 show flow-pre-mgr ip-info

查看 IP 的会话数以及限制参数

show flow-pre-mgr ip-info [*ip-address*]

【参数说明】

参数	描述
ip-address	查看指定 IP 的会话以及限制参数
default	不指定 ip-address 参数的话，则查看全部 IP。

【命令模式】 特权模式、全局模式、接口模式

【缺省级别】 14

【使用指导】 使用该命令查看 IP 的会话数以及限制参数

【配置举例】 查看 IP 的会话数以及限制参数

```
Ruijie#show flow-pre-mgr ip-info
IP-ADDRESS       flow-cnt    flow-limit    UDP-fcnt    UDP-flimit    PORT-fcnt    PORT-flimit
=============================================================================================
192.168.10.1     203         500           150         150           2            25
192.168.10.2     103         500           50          150           0            25
2001:1111::1     203         500           150         150           0            25
2001:1111::2     103         500           50          150           0            25
192.168.10.3     20          0             10          0             0            0
192.168.10.4     15          0             8           0             0            0
Ruijie#
```

字段解释：

字段	说明
IP-ADDRESS	IP 地址
flow-cnt	当前会话计数
flow-limit	会话限制值
UDP-fcnt	当前 UDP 会话计数
UDP-flimit	UDP 会话数限制值
PORT-fcnt	当前限制端口会话计数
PORT-flimit	端口会话数限制值

【提示信息】 -

【平台说明】 -

5.19 show flow-pre-mgr new-session-limit

查看配置的防新建攻击规则

show flow-pre-mgr new-session-limit

【参数说明】

参数	描述
-	-

【命令模式】 特权模式、全局模式、接口模式

【缺省级别】 14

【使用指导】 使用该命令查看当前设备的新建连接限制配置情况。

【配置举例】 查看配置

```
Ruijie# show flow-pre-mgr new-session-limit
flow-pre-mgr new-session-limit start-up limit 20000
flow-pre-mgr new-session-limit virtual-host limit 10000
flow-pre-mgr new-session-limit real-host limit 1000
flow-pre-mgr new-session-limit specify-host 192.168.1.110 limit 5000
flow-pre-mgr new-session-limit specify-host 192.168.1.112 limit 10000
```

【提示信息】 -

【平台说明】 -

5.20 show flow-pre-mgr new-session-limit attack

查看最近一次新建攻击的日志记录

show flow-pre-mgr new-session-limit attack

【参数说明】

参数	描述
-	-

【命令模式】 特权模式、全局模式、接口模式

【缺省级别】 14

【使用指导】 使用该命令查看当前设备最近一次受到新建连接攻击的记录。

【配置举例】 查看配置

```
Ruijie# show flow-pre-mgr new-session-limit attack
HOST-TYPE           HOST-IP             TIME
============================================================
real-host           172.18.8.156        2014-10-16 14:15:28
```

【提示信息】 -

【平台说明】 -

5.21 show flow-pre-mgr rule-info

查看配置的规则

show flow-pre-mgr rule-info

【参数说明】

参数	描述
-	-

【命令模式】 特权模式、全局模式、接口模式

【缺省级别】 14

【使用指导】 使用该命令查看配置的规则以及会话匹配情况。

【配置举例】 查看配置的规则以及会话匹配情况。

```
Ruijie#show flow-pre-mgr rule-info
flow-pre-mgr total-limit 200000
(active)flow-pre-mgr 1 subscriber UserGroupA action trust total-limit 5000 per-ip-limit 300 (446 flows)
(inactive)flow-pre-mgr 2 access-list 120 action block (0 flows)
```

字段解释：

字段	说明
active	规则当前是生效状态
inactive	规则当前是不生效状态
flows	当前有多少个会话匹配这个规则

【提示信息】 -

【平台说明】 -

5.22 show flow-pre-mgr upload-pps-limit

查看配置的防上行流量攻击规则

show flow-pre-mgr upload-pps-limit

【参数说明】

参数	描述

-	-

【命令模式】 特权模式、全局模式、接口模式

【缺省级别】 14

【使用指导】 使用该命令查看每 IP 上行包速限制的配置情况。

【配置举例】 查看配置

```
Ruijie# show flow-pre-mgr upload-pps-limit
flow-pre-mgr upload-pps-limit 3000
flow-pre-mgr upload-pps-limit specify 192.168.1.30 limit 5000
flow-pre-mgr upload-pps-limit specify 192.168.1.20 limit 10000
```

【提示信息】 -

【平台说明】 -

6 FLOW-CONTROL

6.1 auto-pir

使能流控通道树的 PIR 动态调整功能。

auto-pir enable [**interval** *NUM* [**root-rate** *Percentage*]] [**exclude-pass**]

关闭流控通道数的 PIR 动态调整功能。

no auto-pir enable

【参数说明】

参数	描述
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：根通道带宽利用率，处理逻辑如下： ✧ 高于阀值时触发 PIR 压制检查，按照通道优先级从低到高，如果存在通道速率超过 CIR，则压制其 PIR； ✧ 低于阀值 10 个百分点时触发 PIR 恢复，按照通道优先级从高到低进行恢复； ✧ 介于于两者之间时不做处理 不配置默认为 90，配置范围为 1～99。。以默认值 90 为例，低于 80%时触发 PIR 恢复，高于 90%时触发 PIR 压制检查，介于 80%和 90%之间时不做处理。
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。

【缺省配置】 EG 产品默认开启，NPE 产品默认关闭。

【命令模式】 **channel-tree** 配置模式。

【缺省级别】 14

【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。

【配置举例】 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** *Name* [**inbound | outbound**] **auto-pir** 可以 auto-pir 是否生效。

【提示信息】 -

【常见错误】 -

【平台说明】 -

6.2 change-priority

交换同一个流量控制组下两条策略规则的优先级：
change-priority rule1 *rule1-num* **rule2** *rule2-num* [**by-rule-number**]

【参数说明】

参数	描述
rule1-num	交换的第一条策略规则的编号，默认为优先级编号
rule2-num	交换的第二条策略规则的编号，默认为优先级编号
by-rule-number	输入表明 *rule1 -num* 和 *rule2 -num* 为规则 Number ,而不是默认的优先级编号

【缺省配置】 无

【命令模式】 流量控制组配置模式

【缺省级别】 14

【使用指导】 策略规则的优先级编号可以通过 **show flow-control-policy rule** [**group** *name*]中的 Pri_num 字段来查看。

【配置举例】 1：交换流量控制组 group1 下优先级编号 1 和 2 的两条策略规则优先级，注意 1 和 2 为优先级编号：

```
Ruijie(config)# config
Ruijie(config)# flow-control group1
Ruijie(config-flow-control)# change-priority rule1 1 rule2 2
```

【检验方法】 使用 **show flow-control-policy rule** [**group** *name*]命令，可以查看所有策略规则或者某个特定流量控制组下的策略规则的详细信息。

【提示信息】 -

【常见错误】 -

【平台说明】 -

6.3 channel-default

指定默认的流控通道。
channel-default *channel-name*

恢复缺省配置。
no channel-default

【参数说明】

参数	描述
channel-name	已经配置流控通道名字

【缺省配置】 缺省情况下，为根通道。

【命令模式】 **channel-tree** 配置模式

【缺省级别】 14

【使用指导】 通过配置本命令，所有流控策略匹配失败的流量均会入指定的默认通道

【配置举例】 指定流控组“test”的下行方向流控树上的“depart5”通道为默认通道。

```
Ruijie(config)#flow-control test
Ruijie(config-flow-control)#channel-tree inbound
Ruijie(config-channel-tree)#channel-default depart5
```

【检验方法】 使用 **show flow-control {***NAME***}**可以查看整个流控组的配置。

【提示信息】 -

【常见错误】 -

【平台说明】 -

6.4 channel-group

创建流控通道。
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**] }

配置流控通道加入共享池。

channel-group *name* **pool** *pool_name*

删除流控通道

no channel-group *name*

删除流控通道共享池

no channel-group *name* **pool** *pool_name*

【参数说明】

参数	描述
name	创建通道的名字
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，根节点不允许配置为 0。
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 PIR 不输入默认取父节点 PIR，如果不存在父节点则取 CIR 的值。
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，基于每个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
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

【缺省配置】 缺省情况下未配置流控通道

【命令模式】 **channel-tree** 配置模式

【缺省级别】 14

【使用指导】 1. 一个流控树只能存在一个根通道，根通道的 cir 和 pir 需要配置为相等的值；

2. 通道 cir 配置时，要求配置的 cir 与其所有兄弟通道 cir 之和小于等于父通道的 cir；通道的 pir 配置时，要求配置的 pir 必须小于等于父通道的 pir；

3. 高优先级的通道优先得到调度，拥塞的情况下丢包几率更低；

4. per-net 队列和 per-user 队列为公平队列，只有在拥塞情况下配置才有意义，才会体现其公平发包的特点；

5. per-net 队列 limit 之外的网段流量，将会入 per-net 队列的默认队列，该默认队列发包优先级最低，limit 之内的网段的带宽会优先保障。另外，per-pir、limit、session-limit 均不支持嵌套，如 Root 通道限制 session-limit 为 1000，Root 通道子通道限制 BT 的 session-limit 为 500，实际的含义为非 BT 流量限制 session-limit 为 1000，BT 限制 500。

6. 只支持流控树的最下面两层加入共享池，即只有叶子通道及其父通道允许加入共享池，并且共享池必须已经创建；

7. 加入 Per-IP 类型共享池，通道类型必须为 Per-IP 类型，即 Per-net 且 per-mask 为 32，并且 limit 不能大于共享池 limit 限制；

8. 共享池成员通道不能超过 8 个。

9、per-user 类型的通道不支持加入共享池。

【配置举例】 在流控组“test”的下行方向流控树上创建名为“root”的通道：

```
Ruijie(config)#flow-control test
Ruijie(config-flow-control)#channel-tree inbound
Ruijie(config-channel-tree)#channel-group root parent null cir 50000 pir 50000 pri 4 fifo
```

【检验方法】 -

【提示信息】 -

【常见错误】 -

【平台说明】 -

6.5 channel-tree

创建流控通道树。

channel-tree { **inbound** | **outbound** }

删除流控通道数。

[**no**] **channel-tree** { **inbound | outbound** }

【参数说明】

参数	描述
inbound	下行
outbound	上行

【缺省配置】 缺省没有配置流控树。

【命令模式】 Flow-control 模式

【缺省级别】 14

【使用指导】 一个流控组应该包含下行方向流控树和上行方向流控树。

【配置举例】 在流控组“test”的分别创建下行方向流控树和上行方向流控树：

```
Ruijie(config)#flow-control test
Ruijie(config-flow-control)#channel-tree inbound
Ruijie(config-channel-tree)#exit
Ruijie(config-flow-control)#channel-tree outbound
Ruijie(config-channel-tree)#exit
```

【检验方法】 使用 **show flow-control** { *NAME* }可以查看整个流控组的配置。

【提示信息】 无

【常见错误】 无

【平台说明】 -

6.6 clear flow-control

配置流量控制组的说明。

clear flow-control *name* **statistics**

【参数说明】

参数	描述
name	流控组名称，最大支持 32 个字符

【命令模式】 特权模式

【缺省级别】 14

【使用指导】 清除流控组数据统计信息值

【配置举例】 清除流控组“Gi0/1”统计信息：

```
Ruijie# clear flow-control Gi0/1 statistics
```

【提示信息】 -

【常见错误】 -

【平台说明】 -

6.7 comment

配置流量控制组的说明。
comment *Comment_String*

删除已经配置的说明字段。
[**no**] **comment** *Comment_String*

【参数说明】

参数	描述
Comment_String	说明字符串，最大支持 127 个字符，中间不能有空格

【缺省配置】 缺省情况下没有配置说明字段。

【命令模式】 **flow-control** 配置模式

【缺省级别】 14

【使用指导】 无

【配置举例】 在流控组“Gi0/1”配置说明字段：

```
Ruijie(config)#flow-control Gi0/1
Ruijie(config-flow-control)# comment Dianxin-10M
```

【检验方法】 使用 **show flow-control {***NAME***}**可以查看整个流控组的配置

【提示信息】 无

【常见错误】 无

【平台说明】 -

6.8 flow-control

配置流量控制组(简称流控组)。

flow-control { **statistics | log on |** *name* [**update bandwith** *In_bandwith Out_bandwith* [**perpir-update**]] }

删除某个特定的流控组。

no flow-control *name*

【参数说明】

参数	描述
statistics	流控转发面报文数据信息统计开关（除高性能设备，默认开启统计开关）
log	流控 Log 开关
on	Log 开关
name	流量控制组的名称
In_bandwith	期望更新的下行带宽大小，输入范围：500~ 10000000，单位：kbps
Out_bandwith	期望更新的上行带宽大小，输入范围：500~ 10000000，单位：kbps
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

.

【缺省配置】 缺省情况下，系统中只会存在流控模板配置。

【命令模式】 全局模式

【缺省级别】 14

【使用指导】

1、 通过配置本命令进入流量控制组模式，基于这个流量控制组可以进一步的配置流量控制策略规则和流量控制通道。需要注意的是，流量控制组必须应用到 WAN 口上才能使得策略规则和通道生效。

2、 通过 update 关键字用于更新已有流控组的带宽大小。其中，带宽更新影响到所有共享池和通道带宽配置，均会等比例调整。

【配置举例】

1：配置流控策略组 group1

```
Ruijie#config
Ruijie(config)#flow-control group1
```

2：配置流控策略组 group2

```
Ruijie#config
Ruijie(config)# flow-control group2
```

3：删除流控策略组 group1

```
Ruijie#config
Ruijie(config)#no flow-control group1
```

4：更新 Gi0/0 的带宽大小为 20M

```
Ruijie#config
Ruijie(config)#flow-control Gi0/0 update bandwith 20000 20000
```

【检验方法】 使用 **show flow-control {***NAME***}**可以查看整个流控组的配置

【提示信息】 无

【常见错误】 无

【平台说明】 -

6.9 flow-policy

将流量控制组应用到 wan 口上，使得在这个策略组下面配置的流控策略规则和流控策略通道可以生效：
flow-policy *name*

取消某个特定的流量控制组在接口上的应用：
no flow-policy

【参数说明】

参数	描述
name	流量控制组的名称

【缺省配置】 缺省情况下，系统中的 WAN 口上没有应用任何的流量控制组。

【命令模式】 接口配置模式

【缺省级别】 14

【使用指导】 该命令只能在 WAN 口上面配置，非 WAN 口上该命令无法使用。

【配置举例】 1：流控策略组 group1 应用到 interface gi0/1 上：

```
Ruijie#config
Ruijie(config)#interface gi0/1
Ruijie(config-if-GigabitEthernet 0/1)#flow-policy group1
```

2：interface gi0/1 接口上取消应用流控策略组 group1：

```
Ruijie#config
Ruijie(config)#interface gi0/1
Ruijie(config-if-GigabitEthernet 0/1)#no flow-policy
```

【检验方法】 使用 **show run** 命令，可以查看接口下是否配置了流控。

【提示信息】 -

【常见错误】 -

【平台说明】 -

6.10 flow-rule

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-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*]

删除一条策略。

no flow-rule *num*

禁止一条策略。

flow-rule *num* **disable**

策略解除禁止。

no flow-rule *num* **disable**

【参数说明】

参数	描述
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

【缺省配置】 缺省情况下系统中没有配置任何策略规则。

【命令模式】 流量控制组配置模式

【缺省级别】 14

【使用指导】
1. 不允许配置 num 号不同，但是关键字相同的策略规则。
2. 策略规则匹配的原则是后配置的先生效，策略规则生效的条件要求策略的两部分都配置了、关联的各个对象以及通道对象都已经配置了、同时策略规则所在的流量控制组应用到了 WAN 口上。
3. 策略配置 **Action** 为 pass 情况下，**in-channel** 或者 **out-channel** 不配置，则对应的 **in** 或者 **out** 方向不限速，双向均不配置表明双向都不做限速；
4. 策略精细化判断原则：先进行对象优先级比较，vlan 对象 > 内网 IP 对象 > 认证对象 > 外网 IP 对象 > 应用识别对象；对象优先级相同时，相同对象比较依据是子类比父类更加精细，如阿里旺旺属于即时通讯软件，其它对象均相同情况下，相比应用对象使用即时通讯软件的策略，使用阿里旺旺的策略更加精细。

【配置举例】 1：在流量控制组 group1 下，配置限制某公司行政部门的出口带宽为 3M。

```
Ruijie#config
Ruijie(config)#flow-control group1
Ruijie(config-flow-control)#flow-rule 1 vlan-group any subscriber 行政部 network-group any
app-group any time-rang any
Ruijie(config-flow-control)#flow-rule 1 action pass out-channel 行政部出口带宽 3M
```

2：在流量控制组 group2 下，配置限制某公司行政部门的张三上班时间不允许访问 sina。

```
Ruijie#config
Ruijie(config)#flow-control group1
Ruijie(config-flow-control)#flow-rule 1 vlan-group any subscriber 行政部张三 network-group sina
app-group any time-rang work
Ruijie(config-flow-control)#flow-rule 1 action drop
```

【检验方法】 -

【提示信息】 -

【常见错误】 -

【平台说明】 -

6.11 flow-template

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**]

【参数说明】

参数	描述
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

【缺省配置】 -

【命令模式】 全局模式

【缺省级别】 14

【使用指导】

1、 带宽更新影响到所有共享池和通道带宽配置，均会等比例调整。

2、 配置拷贝用于根据已有的流控组配置模板生成新的配置 ,其中的带宽更新可以认为是针对新创建的流控组，执行带宽更新；

【配置举例】 根据流控组 AAA 生成一个新的流控组 BBB，并且带宽更新为 15M

```
Ruijie#config
Ruijie(config)# flow-template copy AAA BBB bandwith 15000 15000
```

【检验方法】 -

【提示信息】 -

【常见错误】 -

【平台说明】 -

6.12 share-pool

创建共享池。

share-pool *Name* **rate** *num1* [**type** { **normal** | **per-ip** [**limit** *num2***l** }]

删除共享池。

no share-pool *Name*

【参数说明】

参数	描述
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

【缺省配置】 缺省情况下系统中没有配置任何共享池。

【命令模式】 **channel-tree** 配置模式

【缺省级别】 14

【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；

【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*：

```
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** { *NAME* }可以查看整个流控组的配置

【提示信息】 -

【常见错误】 -

【平台说明】 -

6.13 show flow control

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*]]

显示 auto-pir 的状态信息：
show flow-control *Name* [**inbound** | **outbound**] **auto-pir**

【参数说明】

参数	描述
Name	流控组的名字
inbound	下行方向流控树。
outbound	上行方向流控树。
channel-name	流控通道的配置，加上 detail 关键字用于显示 FIFO、SFQ 和 Per-net 队列运行状态信息
pool-name	共享池相关显示，不输入 Name 显示所有 Pool，输入则显示特定 Pool

【命令模式】 特权模式

【缺省级别】 14

【使用指导】 如果输入 **channel-group** *channel-name* 关键字，则只显示对应通道的配置信息，否则显示整个流控通道树上配置的所有通道配置信息。

【配置举例】 1 显示指定流控组：Gi0/6 的配置信息

```
Ruijie#sh flow-control test
flow-control test
 comment tpl-ibar
 !
 channel-tree inbound
  auto-pir enable interval 1 root-rate 90
  !
  channel-group root parent null cir 130000 pir 130000 pri 4 per-net per-mask 32 per-cir 130 per-pir
2000 limit 1000
  channel-group key parent root cir 65000 pir 91000 pri 0 per-net per-mask 32 per-cir 65 per-pir
78000 limit 1000
```

```
  channel-group normal parent root cir 52000 pir 91000 pri 4 per-net per-mask 32 per-cir 52 per-pir
78000 limit 1000
  channel-group unkey parent root cir 13000 pir 52000 pri 7 per-net per-mask 32 per-cir 13 per-pir
3003 limit 1000
  channel-default normal
 !
 channel-tree outbound
  no auto-pir enable
  !
  channel-group root parent null cir 130000 pir 130000 pri 4 per-net per-mask 32 per-cir 130 per-pir
2000 limit 1000
  channel-group key parent root cir 65000 pir 78000 pri 0 per-net per-mask 32 per-cir 65 per-pir
4998 limit 1000
  channel-group normal parent root cir 52000 pir 78000 pri 4 per-net per-mask 32 per-cir 52 per-pir
3003 limit 1000
  channel-group unkey parent root cir 13000 pir 52000 pri 7 per-net per-mask 32 per-cir 13 per-pir
3003 limit 1000
  channel-default normal
 !
 flow-rule 1000 app-group Other_Group time-range any
 flow-rule 1000 action pass in-channel normal out-channel normal default comment
Match_Normal_Group_of_NON_VPN
 flow-rule 999 app-group Key_Group time-range any
 flow-rule 999 action pass in-channel key out-channel key default comment Match_Key_Group_of_NON_VPN
 flow-rule 998 app-group Unkey_Group time-range any
 flow-rule 998 action pass in-channel unkey out-channel unkey default comment
Match_Inhib_Group_of_NON_VPN
 flow-rule 992 subscriber VIP time-range any
 flow-rule 992 action pass in-channel key out-channel key comment Match_VIP_Group_of_NON_VPN
 flow-rule 991 network-group Out_Server time-range any
 flow-rule 991 action pass in-channel key out-channel key comment Match_Out_Server_of_NON_VPN
 flow-rule 900 app-group TC_AD_Key time-range any
 flow-rule 900 action pass in-channel key out-channel key comment Match_AD_Key_of_NON_VPN
 flow-rule 900 disable
```

2 显示下行方向指定通道的配置信息:

```
Ruijie#sh flow-control test inbound channel-group root
Group-name                        CIR      PIR      Pri  Schedule
CIDR/CIR/PIR/Limit/Sess-limit/Share-pool  R
--------------------------------- -------- -------- ---- --------
----------------------------------------  -
```

```
root                              130000    130000    4     per-net   32/130/2000/1000/0
0
```

3 显示通道树下行所有通道的配置信息：

```
Ruijie#sh flow-control test inbound
Group-name                        CIR       PIR       Pri   Schedule
CIDR/CIR/PIR/Limit/Sess-limit/Share-pool  R
--------------------------------- --------- --------- ----- --------
----------------------------------------  -
root                              130000    130000    4     per-net   32/130/2000/1000/0/
0
key                               65000     91000     0     per-net   32/65/78000/1000/0/
0
normal                            52000     91000     4     per-net   32/52/78000/1000/0/
0
unkey                             13000     52000     7     per-net   32/13/3003/1000/0/
0
```

字段解释：

字段	说明
Group-name	通道名字
CIR	承诺信息速率
PIR	峰值信息速率
Pri	通道优先级
Schedule	通道队列类型
CIDR/CIR/PIR/Limit/Sess-limit/Share-pool	CIDR/CIR/PIR/Limit/Sess-limit/Share-pool

4 显示上行所有共享池的配置信息：

```
Ruijie#show flow-control test outbound share-pool
Global pool:     14            Global red obj:  0
Tree pool:       3

Share-pool      Rate        Type         Limit       Child
--------------- ----------- ---------- ---------- ----------
tcp               200         Normal      NA           1
udp               150         Normal      NA           1
p1                100         Normal      NA           2
```

字段解释：

字段	说明
Global pool	全局共享池数量
Global red obj	全局达到限制共享池对象，针对 Normal 类型共享池和 Per-IP 类型共享池的各个节点进行统计

Tree pool	对应 Channel-tree 的共享池个数
Share-pool	共享池名字
Rate	共享池限速
Type	共享池类型
Limit	Per-IP 类型共享池有效，为用户限制数
Child	成员通道数，注意只计算加入 Pool 的通道数，如有三个叶子的父通道加入共享池该统计值只加 1

5 显示上行指定共享池的信息：

```
Ruijie#show flow-control test3 outbound share-pool p1
Pool:      p1
Rate:      100         Type:      Normal     Limit:     NA
State:     Green       Child:     2          Active:    NA
Kill flow: 0

Group-name  Cir     Pir      Pri  Type       Limit     Share-pool
----------- ------ -------- ---- --------- --------- ----------
p1-tcp      150      500      4    fifo       NA          p1
p1-udp      100      500      4    fifo       NA          p1
```

字段解释：

字段	说明
Pool	共享池名字
Rate	共享池限速
Type	共享池类型
Limit	Per-IP 类型共享池有效，为用户限制数
State	Normal 类型共享池有效，Green 表明未达到限制值，Red 表明达到上限值，Per-IP 类型为 NA
Child	成员通道数，注意只计算加入 Pool 的通道数，如有三个叶子的父通道加入共享池该统计值只加 1
Limit	Per-IP 类型共享池有效，为用户限制数
Active	活动用户数，Per-IP 类型共享池有效
Kill flow	结束流次数统计，Per-IP 类型共享池有效，统计超过 Per-IP 类型共享池 Limit 限制的用户流量结束次数
Group-name	共享池成员通道名字
Cir	共享池成员通道承诺带宽
Pir	共享池成员通道峰值带宽
Type	共享池成员通道类型
Pri	共享池成员通道优先级
Limit	共享池成员通道用户数限制，Per-net 类型时有效
Share-pool	通道加入共享池名字

	注意： 如果指定显示共享池存在成员为非叶子通道，该非叶子通道的子通道也会通过该命令显示出来，其子通道有加入另外的共享池则 Share-pool 显示对应名字，否则为 NA

【提示信息】 -

【平台说明】 -

6.14 show flow-control-policy group

显示流量控制组的详细信息。

show flow-control-policy group

【参数说明】

参数	描述
-	-

【命令模式】 特权模式

【缺省级别】 14

【使用指导】 显示系统中所有流量控制组的详细信息，包括流量控制组的名称、流量控制组的编号、流量控制组应用到的接口索引值和此流控控制组下配置的策略规则总条数。

【配置举例】 显示系统中所有流量控制组的详细信息：

```
Ruijie#show flow-control-policy group
group_name                      group_id  apply_ifx     policy_entries
group1                           0           6              14
group2                           1           0              4
```

字段解释：

字段	说明
group-name	流量控制组的名称
group-id	流量控制组的编号
apply_ifx	流控控制组应用的接口索引值，为 0 表示没有应用到任何接口上
policy_entries	此流控控制组下配置的流控策略规则条数

【提示信息】 -

【平台说明】 -

6.15 show flow-control-policy rule

显示流控策略规则的详细信息。

show flow-control-policy rule [**group** *name*]

【参数说明】

参数	描述
name	流量控制组的名称。

【命令模式】 特权模式

【缺省级别】 14

【使用指导】 用例显示系统中所有策略规则或者某个流量控制组下的策略规则的详细信息，包括每条策略规则的编号、优先级编号、策略规则所属的接口索引值、各对象的 id、当前多少条流匹配到这条策略规则、这条策略规则最大会话数以及策略规则的有效性。

【配置举例】 显示系统中所有流量控制组的详细信息：

```
Ruijie#sh flow-control-policy rule

Some comment:

| prio    : priority of the rule | grp       : group the rule located | rule    : rule number in
group   |
| ifx     : interface correspond | vlan_id   : vlan identify          | subs_id : subscriber identify
|
| auth_id : auth_group identify  | net_wk_id : network identify       | app_id  : application
identify   |
| in      : in-channel identify  | out       : out-channel identify   | ses_now : session hold now
|
| ses     : config session       | stat      : disable or enable      | ef      : the effect of the
rule |

prio  grp rule  ifx  vlan_id    subs_id    auth_id    net_wk_id  app_id     in    out   ses_now
ses   stat ef
73    5   1000  0    4294967295 4294967295 4294967295 4294967295 4294967288 5     5     0       0
up   0
74    5   999   0    4294967295 4294967295 4294967295 4294967295 4294967290 1     1     0       0
up   0
```

```
75    5    998    0    4294967295 4294967295 4294967295 4294967295 4294967289 6    6    0    0
up    0
76    5    997    0    4294967295 4294967295 4294967295 4294967295 4294967295 4    4    0    0
up    0
77    5    996    0    4294967295 4294967295 4294967295 4294967295 0            3    3    0    0
up    0
78    5    995    0    4294967295 4294967295 4294967295 4294967295 0            2    2    0    0
up    0
79    5    994    0    4294967295 20069752   4294967295 4294967295 4294967295 2    2    0    0
up    0
80    5    993    0    4294967295 4294967295 4294967295 19787672   4294967295 2    2    0    0
up    0
81    5    992    0    4294967295 20069752   4294967295 4294967295 4294967295 1    1    0    0
up    0
82    5    991    0    4294967295 4294967295 4294967295 19787672   4294967295 1    1    0    0
up    0
83    5    900    0    4294967295 4294967295 4294967295 4294967295 4144963584 1    1    0    0
down  0
84    6    1000   0    4294967295 4294967295 4294967295 4294967295 4294967288 5    5    0    0
up    0
85    6    999    0    4294967295 4294967295 4294967295 4294967295 4294967290 1    1    0    0
up    0
86    6    998    0    4294967295 4294967295 4294967295 4294967295 4294967289 6    6    0    0
up    0
87    6    997    0    4294967295 4294967295 4294967295 4294967295 4294967295 4    4    0    0
up    0
88    6    996    0    4294967295 4294967295 4294967295 4294967295 0            3    3    0    0
up    0
89    6    995    0    4294967295 4294967295 4294967295 4294967295 0            2    2    0    0
up    0
90    6    994    0    4294967295 20069752   4294967295 4294967295 4294967295 2    2    0    0
up    0
91    6    993    0    4294967295 4294967295 4294967295 19787672   4294967295 2    2    0    0
up    0
92    6    992    0    4294967295 20069752   4294967295 4294967295 4294967295 1    1    0    0
up    0
93    6    991    0    4294967295 4294967295 4294967295 19787672   4294967295 1    1    0    0
up    0
```

字段解释：

字段	说明
prio	流量策略规则的优先级编号

grp	流量控制组的编号，标明本策略所属流控组
rule	流控策略编号
ifx	流控策略规则所属的接口索引值 ,为 0 表示此规则所在的流量控制组没有应用到接口
vlan_id	流控策略规则关联的 vlan-group 对象的 id，为 0 表示此 vlan-group 对象没有配置
subs_id:	流控策略规则关联的 subscriber 对象的 id ,为 0 表示此 subscriber 对象没有配置
auth_id	流控策略规则关联的 auth-group 对象的 id，为 0 表示此 auth-group 对象没有配置
net_wk_id	流控策略规则关联的 network-group 对象的 id，为 0 表示此 network-group 对象。
app_id	流控策略规则关联的 app-group 对象的 id ,为 0 表示此 app-group 对象
in	流量策略规则关联的 in-channel 通道对象的 id ,id 值为 0 表示此通道对象没有配置，NA 表示此规则没有关联 in-channel 通道对象
out	流量策略规则关联的 out-channel 通道对象的 id，id 值为 0 表示此通道对象没有配置，NA 表示此规则没有关联 out-channel 通道对象
ses_now	当前多少条流匹配到这条策略规则
ses	流控策略规则允许匹配的流最大会话数
stat	Down 标识该策略被禁用，up 未被禁用
ef	流控策略规则的有效性，为 0 表示还没有生效，为 1 表示生效了

【提示信息】 -

【平台说明】 -

6.16 small-packet

配置小报文优先走指定通道。不带 TCP 或 UDP 关键字则两种协议都支持

small-packet *name* [tcp | udp]

【参数说明】

参数	描述
name	流量通道的名称。
TCP	仅支持 TCP 小报文
UDP	仅支持 UDP 小报文

【缺省配置】 从配置模板拷贝生成配置时，对于拨号口或带宽小于等于 10M 的物理口，缺省会在上行通道开启 tcp 小报文走

关键通道

【命令模式】 channel-tree 配置模式

【缺省级别】 14

【使用指导】 对于出口带宽较小的情况下,建议在流控上行通道开启 TCP 报文的小报文优先走关键通道,这样可以提高 web 等小报文较多的应用的流量吞吐率

【配置举例】 在"test"流控策略组配置 tcp 小报文优先走关键通道

```
##进入“test”流控策略组
Ruijie(config)#flow-control test
##进入上行通道树
Ruijie(config-flow-control)#channel-tree outbound
##如果没有 key 通道先配置 key 通道
Ruijie(config-flow-control)# channel-group key parent root cir 5000 pir 10000 pri 0 per-net
##配置 tcp 小报文优先走 key 通道
Ruijie(config-flow-control)# small-packet key tcp
```

【提示信息】 -

【平台说明】 -

7 FLOW-AUDIT

7.1 flow-audit data-store

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 *num*

删除相关配置。

no flow-audit data-store

【参数说明】

参数	描述
num	单位天，取值范围 10 – 90 天

【缺省配置】 缺省情况下，默认保存 60 天。

【命令模式】 全局配置模式

【缺省级别】 14

【使用指导】 通过本命令配置可以修改除天表、周表、月表外其它信息表数据保留天数。

【配置举例】 1：设备用户上下线历史报表信息用户觉得记录保存的时间不够长，想保存时间长点，配置为 80 天。

```
Ruijie#config
Enter configuration commands, one per line.  End with CNTL/Z.
Ruijie(config)# flow-audit data-store 80
```

【检验方法】 1：使用 **show run** 命令，可以查看除天表、周表、月表外其它信息表数据保留天数。

【提示信息】 -

【常见错误】 -

【平台说明】 有内置存储的设备支持

7.2 flow-audit data-store day-report

配置流量监控审计天表历史数据保留天数

flow-audit data-store day-report *num*

删除相关配置。

no flow-audit data-store day-report

【参数说明】

参数	描述
num	单位天，取值范围 10-90 天

【缺省配置】 缺省情况下，天表历史数据保留天数为 60 天。

【命令模式】 全局配置模式

【缺省级别】 14

【使用指导】 通过本命令配置流量监控审计天表历史数据保留天数。

【配置举例】 1：硬盘使用紧张，不想保存太多的天表数据，配置为 30 天

```
Ruijie#config
Enter configuration commands, one per line.  End with CNTL/Z.
Ruijie(config)# flow-audit data-store day-report 30
```

【检验方法】 1：使用 **show run** 命令，可以查看配置流量监控审计天表历史数据保留天数。

【提示信息】 -

【常见错误】 -

【平台说明】 有内置存储的设备支持

7.3 flow-audit data-store month-report

配置流量监控审计月表历史数据保留月数

flow-audit data-store month-report *num*

删除相关配置。

no flow-audit data-store month-report

【参数说明】

参数	描述
num	单位月，取值范围 1-12 月

【缺省配置】 缺省情况下，月表历史数据保留月数为 12 个月。

【命令模式】 全局配置模式

【缺省级别】 14

【使用指导】 通过本命令配置流量监控审计月表历史数据保留月数。

【配置举例】 1：保存一年记录太多，就保存半年

```
Ruijie#config
Enter configuration commands, one per line.  End with CNTL/Z.
Ruijie(config)# flow-audit data-store month-report 6
```

【检验方法】 1：使用 **show run** 命令，可以查看配置流量监控审计月表历史数据保留月数。

【提示信息】 -

【常见错误】 -

【平台说明】 有内置存储的设备支持

7.4 flow-audit data-store week-report

配置流量监控审计周表历史数据保留周数

flow-audit data-store week-report *num*

删除相关配置。

no flow-audit data-store week-report

【参数说明】

参数	描述
num	单位周，取值范围 1-52 周

【缺省配置】 缺省情况下，周表历史数据保留周数为 8 周。

【命令模式】 全局配置模式

【缺省级别】 14

【使用指导】 通过本命令配置流量监控审计周表历史数据保留周数。

【配置举例】 1：监控设备比较长时间的流量走势，但是不想太占用硬盘，可是记录的粒度又不想太细，可以调整周表保存周期为 28 周

```
Ruijie#config
Enter configuration commands, one per line.  End with CNTL/Z.
Ruijie(config)# flow-audit data-store week-report 28
```

【检验方法】 1：使用 **show run** 命令，可以查看配置流量监控审计周表历史数据保留周数。

【提示信息】 -

【常见错误】 -

【平台说明】 有内置存储的设备支持

7.5 flow-audit enable

开启流量监控审计功能。
flow-audit enable

关闭流量监控审计功能
no flow-audit enable

【参数说明】

参数	描述
-	-

【缺省配置】 缺省情况下，流量监控审计功能打开。

【命令模式】 全局配置模式

【缺省级别】 14

【使用指导】 通过配置本命令启动流量监控审计功能。

【配置举例】 1：开启设备的流量监控审计功能。

```
Ruijie#config
Ruijie(config)# flow-audit enable
```

2：关闭设备流量监控审计功能。

```
Ruijie#config
Ruijie(config)#no flow-audit enable
```

【检验方法】 1：使用 **show run** 命令，可以流量监控审计功能是启用还是关闭。

【提示信息】 -

【常见错误】 -

【平台说明】 -

7.6 flow-audit generate-report

配置日报表/周报表/月报表预生成的时间点

flow-audit generate-report *hour*

删除相关配置。

no flow-audit generate-report

【参数说明】

参数	描述
hour	单位小时，取值范围 0-23

【缺省配置】 缺省情况下，预生成时间点为凌晨 3 点。

【命令模式】 全局配置模式

【缺省级别】 14

【使用指导】 通过本命令配置日报表/周报表/月报表预生成的时间点。

【配置举例】 1：凌晨 3 点的时候设备业务比较繁忙，凌晨 5 点的时候比较清闲，就可以配置成凌晨 5 点的时候来生成报表

```
Ruijie#config
Enter configuration commands, one per line.  End with CNTL/Z.
Ruijie(config)# flow-audit generate-report 5
```

【检验方法】 1：使用 **show run** 命令，可以查看配置日报表/周报表/月报表预生成的时间点。

【提示信息】 -

【常见错误】 -

【平台说明】 有内置存储的设备支持

7.7 flow-audit hard-disk-quota

配置流量监控的硬盘配额

flow-audit hard-disk-quota *percent*

删除相关配置。

no flow-audit generate-report

【参数说明】

参数	描述
percent	百分比，取值范围 1-100

【缺省配置】 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%。

【命令模式】 全局配置模式

【缺省级别】 14

【使用指导】 通过本命令配置流量监控的硬盘配额。

【配置举例】 1：设备硬盘使用紧张，给流量审计 50%硬盘容量太多了，想减少到 30%。

```
Ruijie#config
Enter configuration commands, one per line.  End with CNTL/Z.
Ruijie(config)# flow-audit hard-disk-quota 30
```

【检验方法】 1：使用 **show run** 命令，可以查看配置流量监控的硬盘配额。

【提示信息】 -

【常见错误】 -

【平台说明】 有内置存储的设备支持

7.8 flow-audit rt-refresh

配置流量监控实时流量刷新频率。

flow-audit rt-refresh *num*

删除相关配置。

no flow-audit rt-refresh

【参数说明】

参数	描述
num	刷新频率, 10 秒， no 命令恢复默认 30 秒

【缺省配置】 缺省情况下，默认 30 秒刷新。

【命令模式】 全局配置模式

【缺省级别】 14

【使用指导】 通过本命令配置可以修改实时流量的刷新频率。

【配置举例】 1：设备流量监控实时流量刷新频率默认 30 秒，用户觉得刷新有点慢，想看到更实时的流量信息，配置为 10 秒。

```
Ruijie#config
Enter configuration commands, one per line.  End with CNTL/Z.
Ruijie(config)# flow-audit rt-refresh 10
```

【检验方法】 1：使用 **show run** 命令，可以查看设置的流量监控实时流量刷新频率。

【提示信息】 -

【常见错误】 -

【平台说明】 -

7.9 flow-audit vpn

配置 VPN 流量监控的方式。

flow-audit vpn { **inside-ip** | **outside-ip** }

【参数说明】

参数	描述
-	-

【缺省配置】 缺省情况下，VPN 流量监控是基于外网 IP 的。

【命令模式】 全局配置模式

【缺省级别】 14

【使用指导】 通过本命令配置可以修改 VPN 流量的监控方式，用户可以根据实际需要进行配置。

【配置举例】 1：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。

```
Ruijie#config
Enter configuration commands, one per line.  End with CNTL/Z.
Ruijie(config)# flow-audit vpn outside-ip
```

2：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。

```
Ruijie#config
Enter configuration commands, one per line.  End with CNTL/Z.
Ruijie(config)# flow-audit vpn inside-ip
```

【检验方法】 1：使用 **show run** 命令，可以查看配置的 VPN 监控方式。

【提示信息】 -

【常见错误】 -

【平台说明】 -

7.10 show flowrate

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**]]

【参数说明】

参数	描述
interface-name	接口名
hour	最近小时数
begin-year	时间段起始年
begin-month	时间段起始月
begin-day	时间段起始日
begin-hour	时间段起始小时
begin-minute	时间段起始分钟
end-year	时间段结束年
end-month	时间段结束月
end-day	时间段结束日
end-hour	时间段结束小时
end-minute	时间段结束分钟
begin-hour2	时间段起始小时 2
end-hour2	时间段结束小时 2

【缺省配置】 无。

【命令模式】 特权模式

【缺省级别】 14

【使用指导】 显示整机或指定接口实时的流量信息。

- 通过指定关键字 global 来显示整机的实时流量信息；通过指定关键字 interface 显示指定接口下的实时流量信息;

eg: show flowrate global （查询整机实时流量信息）
show flowrate interface gi0/3 （查询通路名为"gi0/3"下的实时流量信息）

【配置举例】 1：显示接口 gigabitEthernet 0/1 的当前流量。

```
Ruijie# show flowrate interface gigabitEthernet 0/1
Interface: GigabitEthernet 0/1
Pass input rate: 979685 bits/sec, 114 packets/sec
Pass output rate: 107233 bits/sec, 60 packets/sec
Drop input rate: 130 bits/sec, 5 packets/sec
Drop output rate: 210 bits/sec, 4packets/sec
```

2：显示整机实时流量信息。

```
Ruijie# show flowrate global
global
Pass Input rate:          184592 bits/sec,              33 packets/sec
Pass Output rate:          30940 bits/sec,              28 packets/sec
Drop Input rate:               0 bits/sec,               0 packets/sec
Drop Output rate:              0 bits/sec,               0 packets/sec
```

【提示信息】 -

【平台说明】 时间段的过虑，仅有内置存储的设备支持

7.11 show flowrate application

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**]

【参数说明】

参数	描述
interface-name	三层接口名称，在网关模式下使用
subscriber-name	用户名
subscriber-group	用户组名
auth-group	认证对象组名

auth-name	认证对象名
Ip-address	IP 地址
application-group	应用组名
application-type	应用类型
application-name	应用名
hour	最近小时数
begin-year	时间段起始年
begin-month	时间段起始月
begin-day	时间段起始日
begin-hour	时间段起始小时
begin-minute	时间段起始分钟
end-year	时间段结束年
end-month	时间段结束月
end-day	时间段结束日
end-hour	时间段结束小时
end-minute	时间段结束分钟
begin-hour1	时间段起始小时 1
end-hour1	时间段结束小时 1
begin-hour2	时间段起始小时 2
end-hour2	时间段结束小时 2
n	前 n 条记录

【缺省配置】 无。

【命令模式】 特权模式

【缺省级别】 14

【使用指导】 显示应用相关的实时流量信息。

- 通过指定关键字 global 来显示整机应用、应用组、应用类型的实时流量信息；通过指定关键字 interface 显示指定接口下应用、应用组、应用类型的实时流量信息；通过指定关键字 vwan 显示管道加速应用、应用组、应用类型的实时流量信息；不输入任何过滤条件查询的是应用的实时流量信息；通过指定关键字 by-group 查询的是应用组的实时流量信息；通过指定关键字 by-type 查询的是应用类型的实时流量信息。
  eg: show flowrate application global （查询整机实时的应用流量信息）
  show flowrate application interface gi0/3 （查询通路名为”gi0/3”下各种应用的实时流量信息）
  show flowrate application interface gi0/3 by-group （查询通路名为”gi0/3”下所有应用组的实时流量信息）
  show flowrate application interface gi0/3 by-type （查询通路名为”gi0/3”下所有应用类型的实时流量信息）
  show flowr app vwan（查询管道加速应用的实时流量）
- 通过关键字 top 和参数 n 来显示排序结果的前 n 条记录；

eg: show flowrate application interface gi0/3 order by pass download desc top 5 （查询通路名为”gi0/3”下的实时应用流量，其结果按照下载流量降序排列，并显示前 5 条记录）

- 通过关键字 subscriber、subscriber-group、auth-subs-group、auth-subs、ip 这其中的一个或几个过滤查询实时应用流量信息；

eg: show flowrate application interface gi0/3 ip 192.168.1.5（查询通路名为”gi0/3”下的 ip 为 192.168.1.5 的实时应用流量，）

该命令支持按组统计的功能：可以用 by-group，by-type 关键字来实现按应用组和应用类型统计的功能，该命令也支持根据用户、用户组过滤实现应用用户流量信息显示；该命令也支持显示结果按照通过、丢弃的上下行流量、应用名进行升、降序；

【配置举例】 1：网关模式下，显示接口 gigabitEthernet 0/1 的当前应用流量。

```
Ruijie# show flowrate application interface gigabitEthernet 0/1
path:GigabitEthernet 0/1
count: 1
Application     Application-group   Application-type
PASS:    Upload(bps)    Download(bps)   Upload(pps)    Download(pps)
DROP:    Upload(bps)    Download(bps)   Upload(pps)    Download(pps)
App1                即时通讯软件              其它应用组
62597               65955                   15                17
0                    0                       0                 0
```

2：显示整机实时应用流量信息。

```
Ruijie# show flowr app global
global
count: 4
Application          Application-group    Application-type
PASS:    Upload(bps)    Download(bps)   Upload(pps)    Download(pps)
DROP:    Upload(bps)    Download(bps)   Upload(pps)    Download(pps)
腾讯资源              P2P 应用软件           Unkey_Group
211                 249                 0                 0
0                   0                   0                 0
QQ-登录|聊天          即时通讯软件          Key_Group
286                 373                 0                 0
0                   0                   0                 0
IP 应用               IP 协议组             Other_Group
20014               70481               12                12
0                   0                   0                 0
telnet              远程访问协议          Other_Group
64                  153                 0                 0
0                   0                   0                 0
```

3：显示管道加速实时应用流量信息。

```
Ruijie# show flowr app vwan
vwan
count: 3
Application          Application-group    Application-type
PASS:    Upload(bps)    Download(bps)   Upload(pps)    Download(pps)
DROP:    Upload(bps)    Download(bps)   Upload(pps)    Download(pps)
腾讯资源               P2P 应用软件           Unkey_Group
786                565                0                  0
0                  0                  0                  0
QQ-登录|聊天           即时通讯软件          Key_Group
211                373                0                  0
0                  0                  0                  0
IP 应用                IP 协议组             Other_Group
20014              70481              12                 12
0                  0                  0                  0
```

【提示信息】 -

【平台说明】 时间段的过虑，仅有内置存储的设备支持

7.12 show flowrate ip

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 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** }]

【参数说明】

参数	描述
interface-name	接口名，在网关模式下使用
subscriber-group	用户组名
subscriber-name	用户名

auth-group	认证对象组名
auth-name	认证对象名
Ip-address	IP 地址
application-name	应用名
application-group	应用组名
application-type	应用类型
hour	最近小时数
begin-year	时间段起始年
begin-month	时间段起始月
begin-day	时间段起始日
begin-hour	时间段起始小时
begin-minute	时间段起始分钟
end-year	时间段结束年
end-month	时间段结束月
end-day	时间段结束日
end-hour	时间段结束小时
end-minute	时间段结束分钟
begin-hour1	时间段起始小时 1
end-hour1	时间段结束小时 1
begin-hour2	时间段起始小时 2
end-hour2	时间段结束小时 2
n	前 n 条记录

【缺省配置】 无。

【命令模式】 特权模式

【缺省级别】 14

【使用指导】 显示用户相关的实时流量信息。

- 通过指定关键字 global 来显示整机用户实时的流量信息；通过指定关键字 interface 显示指定接口下用户的实时流量信息；通过指定关键字 vwan 来显示管道加速用户的实时流量信息。

  eg: show flowrate ip global （查询整机用户实时流量信息）

  show flowrate ip interface gi0/3 （查询通路名为"gi0/3"下用户实时流量信息）

  show flowrate ip vwan （查询走管道加速用户的实时流量信息）
- 通过关键字 top 和参数 n 来获取排序结果的前 n 条记录；

  eg: show flowrate ip interface gi0/3 order by pass download desc top 5 （查询通路名为" gi0/3" 下的实时用户流量，其结果按照下载流量降序排列，并显示前 5 条记录）
- 通过关键字 application、application-group、application-type 这其中的一个或几个过滤查询实时的应用流量信息。

  eg: show flowrate ip interface gi0/3 application PPTP （查询通路名为" gi0/3" 下 app 为 PPTP 的实时

用户流量）

该命令支持按组统计的功能，可以用 by-group 关键字来实现按用户组统计的功能；

【配置举例】 1：网关模式下，显示接口 gigabitEthernet 0/1 的当前用户流量。

```
Ruijie# show flowrate ip interface gigabitEthernet 0/1
Subscriber                 ip
PASS: Upload(bps)    Download(bps)   Upload(pps)    Download(pps)
DROP: Upload(bps)    Download(bps)   Upload(pps)    Download(pps)
/User_groupA/User_nameA 2.2.2.92
230                134               0                 0
0                  0                 0                 0
/User_groupB/User_nameB  172.18.3.67
259                153               0                 0
0                  0                 0                 0
```

2：显示整机的用户实时流量。

```
Ruijie# show flowr ip global
global
subscriber           ip
PASS: Upload(bps)    Download(bps)   Upload(pps)    Download(pps)
DROP: Upload(bps)    Download(bps)   Upload(pps)    Download(pps)
/172.18.3.24       172.18.3.24
896                  1008                1                  1
0                    0                   0                  0
/172.18.3.110       172.18.3.110
7526                 63712               9                  9259
0                    0                   0                  0
/192.168.183.118       192.168.183.118
18116                68729               10                 10
0                    0                   0                  0
```

【提示信息】 -

【平台说明】 时间段的过虑，仅有内置存储的设备支持

7.13 show flowrate ip-application

显示整机或指定通路下 IP、应用的实时流量信息。

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*]]

【参数说明】

参数	描述
interface-name	接口名，在网关模式下使用
subscriber-group	用户组名
subscriber-name	用户名
auth-group-name	认证对象组名
auth-name	认证对象名
ip-address	IP 地址
application-name	应用名
application-group	应用组名
application-type	应用类型
n	前 n 条记录

【缺省配置】 无。

【命令模式】 特权模式

【缺省级别】 14

【使用指导】 显示 ip、应用相关的实时流量信息。

- 通过指定关键字 global 来显示整机 IP、应用的实时流量信息；通过指定关键字 interface 显示指定接口下 IP、应用的实时流量信息；

  eg: show flowrate ip-application global ip 192.168.1.3（查询整机 IP、应用信息）

  show flowrate ip-application interface gi0/3 ip 192.168.1.3（查询通路名为"gi0/3"，ip 为 192.168.1.3 的 IP、应用的流量信息）
- 通过关键字 top 和参数 n 来显示排序结果的前 n 条记录；

  eg: show flowrate ip-application interface gi0/3 ip 192.168.1.3 order by pass download desc top 5 （查询通路名为" gi0/3" 下 ip 为 192.168.1.1 的当前应用流量，其结果按照下载流量降序排列，并显示前 5 条记录）

【配置举例】 1：网关模式下，显示接口 gigabitEthernet 0/1 的 IP 为 172.18.36.102 的应用流量。

```
Ruijie# show flowrate ip-application interface gigabitEthernet 0/1
ip 172.18.36.102
path:GigabitEthernet 0/1
Subscriber  ip   Application  Application-group  Application-type
PASS: Upload(bps)    Download(bps)   Upload(pps)    Download(pps)
DROP: Upload(bps)    Download(bps)   Upload(pps)    Download(pps)
/user_groupA/user_nameA  172.18.36.102   applicationA   application_groupA     关键应用组
```

```
46003              2093107            93                 173
0                  0                  0                  0
/user_groupA/user_nameB 172.18.36.102   applicationB  application_groupB   关键应用组
46001              2093102            193                 173
0                  0                  0                  0
/user_groupA/user_nameC172.18.36.102   applicationC application_groupC  关键应用组
4003              1093107            63                 73
0                  0                  0                  0
```

【提示信息】 -

【平台说明】 时间段的过虑，仅有内置存储的设备支持

7.14 show online ip

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**] | [**auth** *auth-name*] [**auth-group** *auth-group*]] [**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-interval** *begin-hour* **to** *end-hour* [*begin-hour2* **to** *end-hour2*]]}] [**order-by** {{**pass** | **drop**} {**upload** | **download**} | **ip** | **subscriber-group** | **subscriber** | **auth-group** | **auth** } {**desc** | **asc**}[**top** n]]

【参数说明】

参数	描述
interface-name	三层接口名称，在网关模式下使用
subscriber-name	用户名
subscriber-group	用户组名
auth-name	认证对象名
auth-group	认证对象组名
Ip-address	IP 地址
begin-minute	时间段起始分钟
end-minute	时间段结束分钟
begin-day	时间段起始日
begin-month	时间段起始月
begin-year	时间段起始年
end-day	时间段结束日
end-month	时间段结束月
end-year	时间段结束年
begin-hour	时间段起始小时

end-hour	时间段结束小时
begin-hour2	时间段起始小时 2
end-hour2	时间段结束小时 2
n	前 n 条记录

【缺省配置】 无。

【命令模式】 特权模式

【缺省级别】 14

【使用指导】 显示在线 IP 相关的上网时长、流量信息。

- 通过指定关键字 global 来显示整机实时在线 IP 流量信息；
  eg: show online ip global （查询当前整机在线 IP 流量信息）
- 通过关键字 top 和参数 n 来显示排序前 n 条记录；
  eg: show online ip global order by pass download desc top 5 （查询当前整机在线 IP 流量，其结果按照下载流量降序排列，并显示前 5 条记录）

【配置举例】 1：显示整机在线用户的时长，流量信息，并按下载流量做排序，显示前 5。

```
Ruijie# show online ip global order-by pass download desc top 5
global
Subscriber
IP                   AuthType       LoginTime            OnlineTime(min)
PASS-Upload(KB)    PASS-Download(KB)    DROP-Upload(KB)      DROP-Download(KB)
/200.200.0.6
200.200.0.6                              2013-7-3 15:38 1345
1405491              655083              0                    0
/200.200.0.7
200.200.0.7                              2013-7-3 15:38 1345
1405489              655044              0                    0
/200.200.0.8
200.200.0.8                              2013-7-3 15:38 1345
1405128              655016              0                    0
/200.200.0.2
200.200.0.2                              2013-7-3 15:38 1345
1405221              654959              0                    0
/200.200.0.9
200.200.0.9                              2013-7-3 15:38 1345
1404516              654826              0                    0
```

【提示信息】 -

【平台说明】 时间段的过虑，仅有内置存储的设备支持

7.15 show online ip-application

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**] | [**auth** *auth-name*] [**auth-group** *auth-group*]] [**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-group** | **application**} {**desc** | **asc**}] [**offset** *start –record* {**limit** record-num}]

【参数说明】

参数	描述
interface-name	三层接口名称，在网关模式下使用
subscriber-name	用户名
subscriber-group	用户组名
auth-name	认证对象名
auth-group	认证对象组名
Ip-address	IP 地址
application-name	应用名
application-group	应用组名
application-type	应用类型
start-record	偏移记录行
record-num	显示的记录行数

【缺省配置】 无。

【命令模式】 特权模式

【缺省级别】 14

【使用指导】 通过指定关键字 global 来显示整机当前在线 IP、应用的上网时长、流量信息。通过关键字 ip,subscriber,subscriber-group,application,application-group 实现条件过滤，通过关键字 order-by 来指定查询结果的排序顺序；通过 top n 来显示排名前 n 的记录

【配置举例】 1：显示整机 IP 为 172.18.181.63 的 IP 应用在线时长，流量信息。

```
Ruijie# show online ip-application global ip 200.200.0.2
global
count:2
Subscriber
```

```
IP                Application   Application-group  Application-type
LoginTime         OnlineTime(min)
PASS-Upload(KB)   PASS-Download(KB)   DROP-Upload(KB)     DROP-Download(KB)
/172.18.181.63
 172.18.181.63         BQQ  即时通讯软件  Other_Group
 2013-8-26 9:36          10456
   16703              28711              0                  0
/172.18.181.63
 172.18.181.63         MAPI  电子邮件协议  Other_Group
 2013-8-26 9:36          10456
   5107               8231               0                  0
```

【提示信息】 -

【平台说明】 时间段的过虑，仅有内置存储的设备支持

7.16 show online statistic

显示整机或指定通路下当前在线，最近 hour 小时内或指定时间段的 IP 数以及会话数；

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*]]}]

【参数说明】

参数	描述
interface-name	三层接口名称，在网关模式下使用
start-record	偏移记录行
record-num	显示的记录行数
hour	最近小时数
begin-year	时间段起始年
begin-month	时间段起始月
begin-day	时间段起始日
begin-hour	时间段起始小时
begin-minute	时间段起始分钟
end-year	时间段结束年
end-month	时间段结束月
end-day	时间段结束日
end-hour	时间段结束小时

end-minute	时间段结束分钟
begin-hour	时间段起始小时
end-hour	时间段结束小时
begin-hour2	时间段起始小时 2
end-hour2	时间段结束小时 2

【缺省配置】 无。

【命令模式】 特权模式

【缺省级别】 14

【使用指导】 显示当前在线 ip 总数
通过指定关键字 global 来显示整机当前在线 IP 总数
eg: show online statistics global （查询当前在线 IP 总数）

【配置举例】 1：显示整机的当前 IP 总数。

```
Ruijie# show online statistics global
global
online ip count: 500
```

【提示信息】 -

【平台说明】 时间段的过虑，仅有内置存储的设备支持

8 CONTENT-AUDIT

8.1 app-audit

开启应用阻断的优化审计功能，并设置间隔时间。
app-audit optimize-cache [*time*]

关闭应用阻断的优化审计功能。
no app-audit optimize-cache

开启应用控制审计对 TCP 连接的优化阻断功能，即主动发送 rst 报文断开连接。
app-audit optimize-deny

关闭应用控制审计对 TCP 连接的优化阻断功能。
no app-audit optimize-deny

【参数说明】

参数	描述
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。

【缺省配置】 缺省为开启状态。

【命令模式】 全局模式

【缺省级别】 14

【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。

【配置举例】 1：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
```

2：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。

【提示信息】 -

【常见错误】 -

【平台说明】 -

8.2 app-rule

删除策略组下所有应用控制审计规则。
app-rule delete-all

交换访问控制规则的优先级。
app-rule priority-swap *rule-id1 rule-id2*

向内容审计策略组中添加应用控制审计规则。
app-rule *rule-id* **time-range** *time-name* **app-group** *app-group-name* **action** { **permit** | **deny** } [**audit**] [**alarm**] [**vpn**] [**vip**] [**comment** *comment-string*]

删除应用控制审计规则。
no app-rule *rule-id*

【参数说明】

参数	描述
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。
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。
app-group-name	规则要控制的应用组名。
comment-string	该规则的描述。

【缺省配置】 缺省无配置。

【命令模式】 内容审计策略组配置模式

【缺省级别】 14

【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：配置为允许应用访问并审计时，为了优化审计记录会进行限制，实际上这种情况下并不进行审计。
5：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-config 中可以看到两个规则的排序发生了变化，但 show running-config 不会出现该命令。

【配置举例】 1：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
```

2：交换策略组 policyA 内应用控制审计规则 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
```

3：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
```

【检验方法】 使用 show running-config 命令可以查看配置状态。

【提示信息】 1：如果配置的 rule-id 已存在，则给出提示。

```
Ruijie(config)# app-rule 2 time-range any direction double app-group VideoAndP2PGroup action deny audit comment DenyVideoAndP2P
Rule 2 already exists, please delete it first
```

【常见错误】 -

【平台说明】 -

8.3 class

向 URL 对象中添加所包含的 URL 分类。
class *class-name*

删除 URL 对象中所包含的 URL 分类。

no class *class-name*

【参数说明】

参数	描述
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。允许最大长度为 40 字节。

【缺省配置】 缺省无配置。

【命令模式】 URL 对象配置模式

【缺省级别】 14

【使用指导】 1：URL 对象允许包含系统 URL 分类以及用户自定义的 URL 分类。

2：URL 对象允许关联不存在的 URL 分类。

【配置举例】 1：为 URL 对象 objA 添加一个名称为 classA 的 URL 分类。

```
Ruijie# configure terminal
Ruijie(config)# url-object objA
Ruijie(url-obj-config)# class classA
Ruijie(url-obj-config)# end
```

【检验方法】 使用 show running-config 命令可以查看配置状态。

【提示信息】 -

【常见错误】 -

【平台说明】 -

8.4 clear content-audit statistics

清除内容审计的实时统计信息。

clear content-audit statistics

【参数说明】

参数	描述
-	-

【命令模式】 特权模式

【缺省级别】 14

【使用指导】 使用该命令可以清除内容审计的实时统计信息。

【配置举例】 1：清除内容审计的实时统计信息。

```
Ruijie#clear content-audit statistics
```

【提示信息】 -

【平台说明】 -

8.5 comment

向 URL 分类或 URL 对象中添加描述。

comment *comment-string*

删除 URL 分类或 URL 对象中的描述。

no comment

【参数说明】

参数	描述
comment-string	URL 分类或 URL 对象的描述，最长支持 100 个字符

【缺省配置】 缺省无配置。

【命令模式】 URL 对象配置模式、URL 分类配置模式

【缺省级别】 14

【使用指导】 描述通常是用来说明 URL 分类或 URL 对象的用途。

【配置举例】 1：为 URL 对象 objA 添加描述。

```
Ruijie# configure terminal
Ruijie(config)# url-object objA
Ruijie(url-obj-config)# comment OBJA-COMMENT
Ruijie(url-obj-config)# end
```

2：为 URL 分类 classA 添加描述。

```
Ruijie# configure terminal
Ruijie(config)# url-class classA
Ruijie(url-cls-config)# comment CLASSA-COMMENT
Ruijie(url-cls-config)# end
```

【检验方法】 使用 show running-config 命令可以查看配置状态。

【提示信息】 -

【常见错误】 -

【平台说明】 -

8.6 content-audit http-port

添加一个 HTTP 端口。
content-audit http-port *port-num*

删除一个 HTTP 端口。
no content-audit http-port *port-num*

【参数说明】

参数	描述
port-num	端口号，范围：1~65535，其中 80 和 8080 为系统内定端口，不允许用户配置、删除。

【缺省配置】 无。

【命令模式】 全局模式

【缺省级别】 14

【使用指导】 应用识别未开启的情况下，当某个网站需要审计，但非 80 或 8080 端口时，可以使用该命令将此网站的端口加入到 HTTP 端口，该网站就可以审计。

【配置举例】 1：将端口 60000 添加为 HTTP 端口。

```
Ruijie# configure terminal
Ruijie(config)# content-audit http-port 60000
Ruijie(url-obj-config)# end
```

2： 将端口 60000 从 HTTP 端口中移除。

```
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 或者 show running-config 命令可以查看配置信息。

【提示信息】 -

【常见错误】 -

【平台说明】 -

8.7 content-audit https-port

添加一个 HTTPS 端口。
content-audit https-port *port-num*

删除一个 HTTPS 端口。
no content-audit https-port *port-num*

【参数说明】

参数	描述
port-num	端口号，范围：1~65535，其中 443 为系统内定端口，不允许用户配置、删除。

【缺省配置】 无。

【命令模式】 全局模式

【缺省级别】 14

【使用指导】 应用识别未开启的情况下，当某个 HTTPS 加密网站需要审计，但非 443 端口时，可以使用该命令将此网站的端口加入到 HTTPS 端口，该网站就可以审计。

【配置举例】 1：将端口 4430 添加为 HTTPS 端口。

```
Ruijie# configure terminal
Ruijie(config)# content-audit https-port 4430
Ruijie(url-obj-config)# end
```

2： 将端口 4430 从 HTTP 端口中移除。

```
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 或者 show running-config 命令可以查看配置信息。

【提示信息】 -

【常见错误】 -

【平台说明】 -

8.8 content-audit write-db

打开内容审计各业务审计信息写本地存储的开关。
content-audit write-db { url | web-search | web-bbs | web-mail | mail | im | app-control | vid }

关闭内容审计各业务审计信息写本地存储的开关。
no content-audit write-db { url | web-search | web-bbs | web-mail | mail | im | app-control | vid }

【参数说明】

参数	描述
-	-

【缺省配置】 ACE 产品：应用控制审计（app-control）缺省开启，其他业务缺省关闭；其他产品：所有业务缺省开启。

【命令模式】 全局模式

【缺省级别】 14

【使用指导】 当内容审计各业务审计信息有发送到外面 log 服务器时，可以关闭此开关，本地将不再写数据库，减轻设备负担。

【配置举例】 1：开启 url 审计信息写本地存储的开关。

```
Ruijie# configure terminal
Ruijie(config)# content-audit write-db url
Ruijie(url-obj-config)# end
```

2：关闭 url 审计信息写本地存储的开关。

```
Ruijie# configure terminal
Ruijie(config)# no content-audit write-db url
Ruijie(url-obj-config)# end
```

【检验方法】 使用 show content-audit write-db/show running-config 命令可以查看配置状态。

【提示信息】 -

【常见错误】 -

【平台说明】 有内置存储的产品支持，无内置存储的产品不支持。

8.9 content-audit alarm

开启/关闭关键字订阅功能。
[no] content-audit alarm enable

开启/关闭指定审计类型的关键字订阅功能
[no] content-audit alarm type { *audit-type* **| all }**

设置邮件发送开关
[no] content-audit alarm mail enable

设置邮件告警周期和开始时间
content-audit alarm mail cycle *n-min*
no content-audit alarm mail cycle

设置告警邮件主题
[no] content-audit alarm mail subject *text*

设置邮件告警目的地址
content-audit alarm mail to *mail-addr*
no content-audit alarm mail to { all | *mail-addr* **}**

【参数说明】

参数	描述
audit-type	审计类型 ,包括{ app_ctrl ,url ,mail ,web_mail ,im ,web_bbs ,web_search , postfile，post， ftp, telnet }
n-min	邮件发送周期，取值范围 1~1440
text	邮件发送主题，默认“内容审计告警”
mail-addr	目的邮箱地址，最大配置 6 个

【缺省配置】 无。

【命令模式】 全局模式

【缺省级别】 14

【使用指导】 使用该命令配置内容审计阻断邮件告警相关内容

【配置举例】 1：开启所有类型的邮件告警。

```
Ruijie# configure terminal
Ruijie(config)# content-audit alarm enable
Ruijie(config)# content-audit alarm type all
Ruijie(config)# content-audit alarm mail enable
Ruijie(config)# content-audit alarm mail cycle 5
Ruijie(config)# content-audit alarm mail to xxx@126.com
```

【检验方法】 使用 show content-audit alarm config 或者 show running-config 命令可以查看配置信息。

【提示信息】 -

【常见错误】 -

【平台说明】 所有网关系列产品均支持。

8.10 content-object

指定内容对象名，并进入内容对象配置模式。
content-object *object-name*

删除内容对象，及所包含的所有关键字。
no content-object *object-name*

【参数说明】

参数	描述
object-name	内容对象名称。允许最大长度为 40 字节。

【缺省配置】 缺省无配置。

【命令模式】 全局模式

【缺省级别】 14

【使用指导】 通过此命令可以配置内容对象。内容对象容量为 100。

【配置举例】 1：配置一个内容对象 objA，包含关键字 hello 和正则匹配 .ietf.org。

```
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)# end
```

【检验方法】 使用 show running-config 命令可以查看配置状态。

【提示信息】 -

【常见错误】 -

【平台说明】 -

8.11 content-policy

指定内容审计策略组名，并进入内容审计策略组配置模式。
content-policy *policy-name*

删除内容审计策略组，及所包含的所有规则。
no content-policy *policy-name*

【参数说明】

参数	描述
policy-name	内容审计策略组名称。允许最大长度为 100 字节。

【缺省配置】 缺省无配置。

【命令模式】 全局模式

【缺省级别】 14

【使用指导】 通过此命令可以配置策略组。策略组的容量为 100。

【配置举例】 1：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。

【提示信息】 -

【常见错误】 -

【平台说明】 -

8.12 content-policy-config

对自定义策略组进行全局禁用。
content-policy-config disable-all

取消自定义策略组全局禁用。
no content-policy-config disable-all

禁用某个策略组。
content-policy-config disable-policy *policy-name*

取消禁用策略组。
no content-policy-config disable-policy *policy-name*

交换两个策略组的优先级。
content-policy-config priority-swap *policy-name1 policy-name2*

【参数说明】

参数	描述
policy-name	内容审计策略组名称。
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。

【缺省配置】 缺省无配置。

【命令模式】 全局模式

【缺省级别】 14

【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：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。
3：禁用策略组不会删除策略组内容和与用户的关联。
4：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。
5：删除策略组后，禁用策略组配置也会同时被删除。
6：配置交换两个策略组的优先级后，show running-config 中可以看到两个策略组排序发生了变化，但 show running-config 不会出现该命令。

【配置举例】 1：关闭所有自定义策略组。

```
Ruijie# configure terminal
Ruijie(config)# content-policy-config disable-all
Ruijie(config)# end
```

2：禁用内容审计策略组 policyA。

```
Ruijie# configure terminal
Ruijie(config)# content-policy-config disable-policy policyA
Ruijie(config)# end
```

3：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。

【提示信息】 -

【常见错误】 -

【平台说明】 -

8.13 content-policy-relate

设置用户不继承父用户组的策略。

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。

no content-policy-relate no-inherit { **subscriber** { *subs-name1* | **any** } | **auth-subscriber** { *subs-name2* | **any** } }

将策略组关联到用户。

content-policy-relate relate { **subscriber** { *subs-name1* | **any** } | **auth-subscriber** { *subs-name2* | **any** } } **policy** *policy-name*

删除用户与策略组的关联。。

no content-policy-relate relate { **subscriber** { *subs-name1* | **any** } | **auth-subscriber** { *subs-name2* | **any** } } **policy** *policy-name*

【参数说明】

参数	描述
subs-name1	策略组关联的静态用户。网吧版 NBR 产品还可关联自定义用户组。
subs-name2	策略组关联的认证用户。
policy-name	策略组名。

【缺省配置】 缺省无配置。

【命令模式】 全局模式

【缺省级别】 14

【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：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。
3：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。
4：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。

【配置举例】 1：配置静态用户 user1 不继承其父用户组的策略。

```
Ruijie# configure terminal
Ruijie(config)# content-policy-relate no-inherit subscriber user1
Ruijie(config)# end
```

2：配置一个名为 policyA 的内容审计策略组关联到静态用户 user1、user2，另外也关联 policyA、policyB 到认证用户 auth-user3。配置一个名为 policyC 的策略组关联到自定义用户组 cstm_grp1。

```
Ruijie# configure terminal
Ruijie(config)# content-policy-relate relate subscriber usr1,user2 policy policyA
Ruijie(config)# content-policy-relate relate auth-subscriber auth-user3 policy policyA,policyB
Ruijie(config)# content-policy-relate relate subscriber cstm_grp1 policy policyC
Ruijie(config)# end
```

【检验方法】 使用 show running-config 命令可以查看配置状态。

【提示信息】 -

【常见错误】 -

【平台说明】 -

8.14 https-audit enable

启用 HTTPS 审计功能。

https-audit enable

关闭 HTTPS 审计功能。
no https-audit enable

【参数说明】

参数	描述
-	-

【缺省配置】 缺省关闭。

【命令模式】 全局模式

【缺省级别】 14

【使用指导】 须配合内容审计各子业务的规则使用。如启用 HTTPS 审计使能开关后，还需要配置 URL 规则，才能对 HTTPS 加密的网站进行域名审计和过滤。

【配置举例】 1：启用 HTTPS 审计功能。

```
Ruijie# configure terminal
Ruijie(config)# https-audit enable
Ruijie(config)# end
```

【检验方法】 使用 show running-config 命令可以查看配置状态。

【提示信息】 -

【常见错误】 -

【平台说明】 -

8.15 im-rule

启用 IM 默认审计功能。
im-rule audit-default-enable

关闭 IM 默认审计功能。
no im-rule audit-default-enable

删除策略组下所有 IM 规则。
im-rule delete-all

交换 IM 访问控制规则的优先级。

im-rule priority-swap *rule-id1 rule-id2*

向内容审计策略组中添加 IM 访问控制规则的公共部分。
im-rule *rule-id* **time-range** *time-name* **action** { **permit** | **deny** } [**audit**] [**alarm**] [**comment** *comment-string*]

向内容审计策略组中添加 IM 访问控制规则的进一步的参数描述，主要是描述规则的关键字匹配条件，该命令必须和 **im-rule** *rule-id* **time-range** 命令配合使用。
im-rule *rule-id* **im-type** *im-name* [**relation** { **and** | **or** } [**account** *content-object-name1*] [**message** *content-object-name2*]]

删除 IM 访问控制规则。
no im-rule *rule-id*

【参数说明】

参数	描述
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。
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。
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。

【缺省配置】 缺省无配置。

【命令模式】 内容审计策略组配置模式

【缺省级别】 14

【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：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）。
5：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-config 中可以看到两个规则的排序发生了变化，但 show running-config 不会出现该命令。
6：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】 1：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
```

2：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
```

3：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
```

4：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
```

【检验方法】 使用 show running-config 命令可以查看配置状态。

【提示信息】 1：如果配置的 rule-id 已存在，则给出提示。

```
Ruijie(config)# im-rule 2 time-range any action permit audit comment PermitUserAMSN
Rule 2 already exists, please delete it first
```

2：如果未配置规则的公共部分，直接配置规则的进一步说明，则给出提示。

```
Ruijie(config)# im-rule 2 im-type msn relation or account accountA message keyA
Rule 2 is not exist
```

【常见错误】 -

【平台说明】 -

8.16 keyword

向内容对象中添加关键字。
keyword *string*

删除关键字。
no keyword *string*

【参数说明】

参数	描述
string	内容对象包含的关键字。允许最大长度为 100 字节。

【缺省配置】 缺省无配置。

【命令模式】 内容对象配置模式

【缺省级别】 14

【使用指导】 通过此命令可以配置内容对象所包含的关键字。

【配置举例】 1：配置一个内容对象 objA，包含关键字 hello。

```
Ruijie# configure terminal
Ruijie(config)# content-object objA
Ruijie(content-obj-config)# keyword hello
Ruijie(content-obj-config)# end
```

【检验方法】 使用 show running-config 命令可以查看配置状态。

【提示信息】 -

【常见错误】 -

【平台说明】 -

8.17 mail-rule

启用 MAIL 默认审计功能。
mail-rule audit-default-enable

关闭 MAIL 默认审计功能。
no mail-rule audit-default-enable

删除策略组下所有 MAIL 规则。
mail-rule delete-all

交换 MAIL 访问控制规则的优先级。
mail-rule priority-swap *rule-id1 rule-id2*

向内容审计策略组中添加 MAIL 访问控制规则的公共部分。
mail-rule *rule-id* **time-range** *time-name* [**direction** { **in** | **out** | **double** }] **action** { **permit** | **deny** } [**audit**] [**alarm**] [**comment** *comment-string*]

向内容审计策略组中添加 MAIL 访问控制规则的进一步的参数描述，主要是描述规则的关键字匹配条件。该命令为可选配置，如果不配置表示对满足 **mail-rule** *rule-id* **time-range** 命令的所有 mail 信息进行审计。
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*]

删除 MAIL 访问控制规则。
no mail-rule *rule-id*

【参数说明】

参数	描述
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。
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-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。

【缺省配置】 缺省无配置。

【命令模式】 内容审计策略组配置模式

【缺省级别】 14

【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：规则配置为阻断时，relation 中实际只有 or 关系才会有效。
5：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-config 中可以看到两个规则的排序发生了变化，但 show running-config 不会出现该命令。
6：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】 1：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
```

2：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
```

3：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
```

4：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
```

【检验方法】 使用 show running-config 命令可以查看配置状态。

【提示信息】 1：如果配置的 rule-id 已存在，则给出提示。

```
Ruijie(config)# mail-rule 1 time-range any action permit audit comment mail-audit-1
Rule 1 already exists, please delete it first
```

2：如果未配置规则的公共部分，直接配置规则的进一步说明，则给出提示。

```
Ruijie(config)# mail-rule 1 relation or from OBJ-F subject OBJ-S mail-size less 20000
```

```
Rule 1 is not exist
```

【常见错误】 -

【平台说明】 -

8.18 plugin-rule

启用 QQ 聊天内容默认审计功能。
plugin-rule audit-default-enable

关闭 QQ 聊天内容默认审计功能。
no plugin-rule audit-default-enable

开启 QQ 群聊天消息审计(只针对群聊天中接收的消息，不含在群聊天中发送的消息)
plugin-grp-audit enable

关闭 QQ 群聊天消息审计(只针对群聊天中接收的消息，不含在群聊天中发送的消息)
no plugin-grp-audit enable

设置终端下载插件的协议及端口号
plugin-config set-download-protol protol *protolname* **port** *portnum*

设置终端下载插件的 URL
plugin-config set-download-url *urlstring*

删除策略组下所有 QQ 聊天内容规则，即 PLUGIN 规则。
plugin-rule delete-all

交换 PLUGIN 访问控制规则的优先级。
plugin-rule priority-swap *rule-id1 rule-id2*

向内容审计策略组中添加 PLUGIN 访问控制规则。
plugin-rule *rule-id* **time-range** *time-name* [**content** *content-object-name*] **action** { **permit** | **deny** } [**audit**] [**alarm**] [**comment** *comment-string*]

删除 PLUGIN 访问控制规则。
no plugin-rule *rule-id*

【参数说明】

参数	描述
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。
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。
protolname	从设备上下载插件使用的协议(http 或 https)
portnum	从设备上下载插件使用的协议端口
urlstring	从 URL 地址下载插件

【缺省配置】 缺省无配置。

【命令模式】 内容审计策略组配置模式

【缺省级别】 14

【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：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-config 中可以看到两个规则的排序发生了变化，但 show running-config 不会出现该命令。
5：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】 1：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
```

2：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
```

3：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
```

4;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
```

5: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
```

6:打开 QQ 接收群聊天消息的审计

```
Ruijie# configure terminal
Ruijie(config)#content-policy _AUDIT_DEFAULT
Ruijie(cont-plcy-config)#plugin-grp-audit enable
```

7:设置终端下载插件的协议及端口

```
Ruijie# configure terminal
Ruijie(config)# plugin-config set-download-protol protol https port 4430
```

8:设置终端下载插件的 URL 地址

```
Ruijie# configure terminal
Ruijie(config)#plugin-config Set-download-url http://192.168.1.111/download/
```

【检验方法】 使用 show running-config 命令可以查看配置状态。

【提示信息】 1：如果配置的 rule-id 已存在，则给出提示。

```
Ruijie(config)# plugin-rule 2 time-range any content keyword-group action deny audit comment TEST
Rule 2 already exists, please delete it first
```

【常见错误】 -

【平台说明】 ACE 系列产品不支持，其他有内置存储的网关产品支持；NBR-E 系列、EG2000F 产品支持，其他无内置存储的网关产品均不支持。

8.19 postfile-rule

启用外发文件默认审计功能。
postfile-rule audit-default-enable

关闭外发文件默认审计功能。
no postfile-rule audit-default-enable

删除策略组下所有外发文件规则， 即 POSTFILE 规则。
postfile-rule delete-all

交换 POST FILE 访问控制规则的优先级。
postfile-rule priority-swap *rule-id1 rule-id2*

向内容审计策略组中添加 POST FILE 访问控制规则。
postfile-rule *rule-id* **time-range** *time-name* [**content** *content-object-name*] **action** { **permit** | **deny** } [**audit**] [**alarm**] [**comment** *comment-string*]

删除 POST FILE 访问控制规则。
no postfile-rule *rule-id*

【参数说明】

参数	描述
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。
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。

【缺省配置】 缺省无配置。

【命令模式】 内容审计策略组配置模式

【缺省级别】 14

【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：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-config 中可以看到两个规则的排序发生了变化，但 show running-config 不会出现该命令。
5：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】 1：启用 POST FILE 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
```

2：删除策略组 policyA 中的所有 POST FILE 规则。

```
Ruijie# configure terminal
Ruijie(config)# content-policy policyA
Ruijie(cont-plcy-config)# postfile-rule delete-all
Ruijie(cont-plcy-config)# end
```

3：交换策略组 policyA 内 POST FILE 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
```

4：为内容审计策略组 policyA 添加一个 POST FILE 访问审计规则，过滤含关键字组 keyword-group 内关键字的文件上传，并且需要审计该信息。

```
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
```

【检验方法】 使用 show running-config 命令可以查看配置状态。

【提示信息】 1：如果配置的 rule-id 已存在，则给出提示。

```
Ruijie(config)# postfile-rule 2 time-range any content keyword-group action deny audit comment TEST
Rule 2 already exists, please delete it first
```

【常见错误】 -

【平台说明】 ACE 系列产品不支持，其他有内置存储的网关产品支持；NBR-E 系列、EG2000F 产品支持，其他无内置存储的网关产品均不支持。

8.20 post-rule

启用 HTTP POST 默认审计功能。
post-rule audit-default-enable

关闭 HTTP POST 默认审计功能。
no post-rule audit-default-enable

删除策略组下所有 HTTP POST 规则，即 POST 规则。
post-rule delete-all

交换 POST 访问控制规则的优先级。
post-rule priority-swap *rule-id1 rule-id2*

向内容审计策略组中添加 POST 访问控制规则。
post-rule *rule-id* **time-range** *time-name* [**content** *content-object-name*] **action** { **permit** | **deny** } [**audit**] [**alarm**] [**comment** *comment-string*]

删除 POST 访问控制规则。
no post-rule *rule-id*

【参数说明】

参数	描述
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。
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。

【缺省配置】 缺省无配置。

【命令模式】 内容审计策略组配置模式

【缺省级别】 14

【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：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-config 中可以看到两个规则的排序发生了变化，但 show running-config 不会出现该命令。
5：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】 1：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
```

2：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
```

3：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
```

4：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 HTTP POST 上传信息，并且需要审计该信息

```
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
```

【检验方法】 使用 show running-config 命令可以查看配置状态。

【提示信息】 1：如果配置的 rule-id 已存在，则给出提示。

```
Ruijie(config)# post-rule 2 time-range any content keyword-group action deny audit comment TEST
Rule 2 already exists, please delete it first
```

【常见错误】 -

【平台说明】 ACE 系列产品不支持，其他有内置存储的网关产品支持；NBR-E 系列、EG2000F 产品支持，其他无内置存储的网关产品均不支持。

8.21 ssl-audit

启用加密类审计功能。
ssl-audit enable

关闭加密类审计功能。
no ssl-audit enable

配置需要审计加密类应用的用户名
ssl-audit mode set-need-proxy
ssl-audit need-proxy subscriber *usrname*
ssl-audit need-proxy auth-subscriber *usrname*

配置不需要审计加密类应用的用户名
ssl-audit mode set-unneed-proxy
ssl-audit unneed-proxy subscriber *usrname*
ssl-audit unneed -proxy auth-subscriber *usrname*

清空名单
ssl-audit clear need-proxy
ssl-audit clear unneed -proxy

【参数说明】

参数	描述
usrname	用户名称

【缺省配置】 缺省无配置。

【命令模式】 内容审计策略组配置模式

【缺省级别】 14

【使用指导】 1 :只能在策略组名为_AUDIT_DEFAULT 的默认审计策略组内进行配置 ,在其它策略组内配置该命令则不生效。

【配置举例】 1：启用加密类审计功能。

```
Ruijie# configure terminal
Ruijie(config)# content-policy _AUDIT_DEFAULT
Ruijie(cont-plcy-config)# ssl-audit enable
Ruijie(cont-plcy-config)# end
```

2：关闭加密类审计功能。

```
Ruijie# configure terminal
Ruijie(config)# content-policy _AUDIT_DEFAULT
Ruijie(cont-plcy-config)# no ssl-audit enable
Ruijie(cont-plcy-config)# end
```

3：配置需要审计加密类应用的用户名单

```
Ruijie# configure terminal
Ruijie(config)# ssl-audit mode set-need-proxy
Ruijie(config)# ssl-audit need-proxy subscriber test_usr
Ruijie(config)# ssl-audit need-proxy auth-subscriber test_usr_auth
```

3：配置不需要审计加密类应用的用户名单

```
Ruijie# configure terminal
Ruijie(config)# ssl-audit mode set-unneed-proxy
Ruijie(config)# ssl-audit unneed-proxy subscriber test_usr
Ruijie(config)# ssl-audit unneed-proxy auth-subscriber test_usr_auth
```

【检验方法】 使用 show running-config 命令可以查看配置状态。

【提示信息】 -

【常见错误】 -

【平台说明】 ACE 系列产品不支持，其他有内置存储的网关产品支持；NBR-E 系列、EG2000F 产品支持，其他无内置存储的网关产品均不支持。

8.22 content-audit deny-stat

设定特定 IP 进行阻断信息统计功能。
content-audit deny-stat ip *A.B.C.D*

删除特定 IP 进行阻断信息统计功能(所有阻断信息都进行统计)。
no content-audit deny-stat ip *A.B.C.D*

清除内容审计的实时统计信息
clear content-audit deny-stat

【参数说明】

参数	描述
A.B.C.D	特定用户的 IP 地址

【缺省配置】 缺省无配置。

【命令模式】 全局模式

【缺省级别】 14

【使用指导】 1：设置特定 IP 后，只统计该 IP 的阻断信息
2：同一时间段只能设置一个特定 IP
3：删除特定 IP 后，所有用户的阻断信息都会进行统计

【配置举例】 1：设定特定 IP 进行阻断信息统计功能

```
Ruijie# configure terminal
Ruijie(config)# content-audit deny-stat ip 192.168.1.2
Ruijie(config)# end
```

2：删除特定 IP 进行阻断信息统计功能(所有阻断信息都进行统计)

```
Ruijie# configure terminal
Ruijie(config)#no content-audit deny-stat ip 192.168.1.2
Ruijie(config)# end
```

3：清除内容审计的阻断实时统计信息。

```
Ruijie# clear content-audit deny-stat
```

【检验方法】 使用 show running-config 命令可以查看配置状态。

【提示信息】 -

【常见错误】 -

【平台说明】

8.23 clear content-audit deny-stat

清除内容审计的阻断记录实时统计信息。

clear content-audit deny-stat

【参数说明】

参数	描述
-	-

【命令模式】 特权模式

【缺省级别】 14

【使用指导】 使用该命令可以清除内容审计的阻断记录实时统计信息。

【配置举例】 1：清除内容审计的阻断记录实时统计信息

```
Ruijie#clear content-audit deny-stat
```

【提示信息】 -

【平台说明】 所有网关系列产品均支持。

8.24 report-function

打开报表功能开关
report-function enable

关闭报表功能开关
no report-function enable

【参数说明】

参数	描述

【缺省配置】 无

【命令模式】 全局模式

【缺省级别】 14

【使用指导】 使用该命令配置报表功能是否开启

【配置举例】 1：打开报表功能开关

```
Ruijie# configure terminal
Ruijie(config)# report-function enable
```

【检验方法】 使用 show report- function 命令可以查看配置信息。

【提示信息】 -

【常见错误】 -

【平台说明】 内容审计 2.0 设备支持

8.25 report-custom-config

配置自定义报表规则

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]**

删除自定义报表规则

no report-custom-config *rule-id*

【参数说明】

参数	描述
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

【缺省配置】 无

【命令模式】 全局模式

【缺省级别】 14

【使用指导】 使用该命令配置自定义报表的统计规则

【配置举例】 1：配置统计用户 usrA 的外发文件与网页搜索情况

```
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
```

2：删除自定义报表规则

```
Ruijie# configure terminal
Ruijie(config)# no report-custom-config 1
```

【检验方法】 使用 **show report-custom-config** 命令可以查看规则配置信息。

【提示信息】 -

【常见错误】 -

【平台说明】 内容审计 2.0 并且支持硬盘的设备支持

8.26 regexp

向 URL 对象中添加 URL 正则表达式。
regexp *url-regexp*

删除 URL 正则表达式。
no regexp *url-regexp*

向内容对象中添加关键字正则表达式。
regexp *regexp*

删除关键字正则表达式。
no regexp *regexp*

【参数说明】

参数	描述
url-regexp	URL 正则表达式，支持标准的正则表示法。
regexp	关键字正则表达式，支持标准的正则表示法。

【缺省配置】 缺省无配置。

【命令模式】 URL 对象配置模式、内容对象配置模式

【缺省级别】 14

【使用指导】 通过此命令可以配置 URL 对象或内容对象所包含的正则表达式。

【配置举例】 1：为 URL 对象 url-objA 添加一个正则表达式，用于匹配 URL 中包含有 ieft 关键字的 URL。

```
Ruijie# configure terminal
Ruijie(config)# url-object url-objA
Ruijie(url-obj-config)# regexp .*ieft.*
Ruijie(url-obj-config)# end
```

2：配置一个内容对象 objA，包含关键字 hello 和正则匹配 .ietf.org。

```
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)# end
```

【检验方法】 使用 show running-config 命令可以查看配置状态。

【提示信息】 -

【常见错误】 -

【平台说明】 -

8.27 show app-audit detail

查询应用控制审计的明细信息。

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*]

【参数说明】

参数	描述
hours	近期时间段
yyyy mm dd	年月日
hh:mm:ss	小时分钟秒
hour1	时间段过滤条件：开始小时段
hour2	时间段过滤条件：结束小时段
hour3	时间段过滤条件：开始小时段
hour4	时间段过滤条件：结束小时段
intf-name	接口名称
bridge-num	桥编号
subs-name1	过滤条件：静态用户名，精确匹配
subs-name2	过滤条件：认证用户名，精确匹配
app-group-name	过滤条件：应用组名称
rule-name	过滤条件： 匹配的规则名称
addr	过滤条件：IP，精确匹配；多个 IP 用 “,” 隔开
integer1	查询结果集合中的起始位置
integer2	查询结果集合中的结束位置

【命令模式】 特权模式

【缺省级别】 14

【使用指导】 使用该命令可以查询或导出应用控制审计的明细信息。

【配置举例】 1：查询 2013-5-1 的 0 点到 2013-5-7 的 24 点，用户 userA 的应用控制审计明细信息。

```
Ruijie# show app-audit detail time-range from 2013 5 1 0:0:0 to 2013 5 7 23:59:59 subscriber userA
order-by time desc start-item 1 end-item 20
=====================================================================
Time: 2013-05-03 16:45:29
subscriber: /userA
auth-subscriber: any
Ip: 192.168.211.96
App: QQ
Rule: DenyQQ
Action: deny
......
```

【提示信息】 -

【平台说明】 有内置存储的产品支持，无内置存储的产品不支持。

8.28 show app-audit stat

查询应用控制审计的统计信息。

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**]

【参数说明】

参数	描述
hours	近期时间段
yyyy mm dd	年月日
hh:mm:ss	小时分钟秒
hour1	时间段过滤条件：开始小时段
hour2	时间段过滤条件：结束小时段
hour3	时间段过滤条件：开始小时段
hour4	时间段过滤条件：结束小时段
intf-name	接口名称

bridge-num	桥编号
subs-name1	过滤条件：静态用户名，精确匹配
subs-name2	过滤条件：认证用户名，精确匹配
addr	过滤条件：IP，精确匹配；多个 IP 用“,”隔开
app-group-name	过滤条件：应用组名称
rule-name	过滤条件： 匹配的规则名称

【命令模式】 特权模式

【缺省级别】 14

【使用指导】 使用该命令可以查询应用控制审计的统计信息。

【配置举例】 1：查询 2013-5-1 的 0 点到 2013-5-7 的 24 点，用户 userA 的应用控制审计统计信息。

```
Ruijie# show app-audit stat time-range from 2013 5 1 0:0:0 to 2013 5 7 23:59:59 subscriber userA
50
```

【提示信息】 -

【平台说明】 有内置存储的产品支持，无内置存储的产品不支持。

8.29 show content-audit http-port

显示 HTTP 端口信息。

show content-audit http-port

【参数说明】

参数	描述
-	-

【命令模式】 特权模式

【缺省级别】 14

【使用指导】 使用该命令可以查看 HTTP 端口信息。

【配置举例】 1：查看 HTTP 端口信息。

```
Ruijie#show content-audit http-port
HTTP port information in user:       80  8080 60000
HTTP port information in kernel:     80  8080 60000
```

【提示信息】 -

【平台说明】 -

8.30 show content-audit https-port

显示 HTTPS 端口信息。

show content-audit https-port

【参数说明】

参数	描述
-	-

【命令模式】 特权模式

【缺省级别】 14

【使用指导】 使用该命令可以查看 HTTPS 端口信息。

【配置举例】 1：查看 HTTPS 端口信息。

```
Ruijie#show content-audit https-port
HTTPS port information in user:     443  4430
HTTPS port information in kernel:   443  4430
```

【提示信息】 -

【平台说明】 -

8.31 show content-audit statistics

显示内容审计的实时统计信息。

show content-audit statistics { **brief** | **counts** }

【参数说明】

参数	描述
brief	显示内容审计实时统计的概要信息，只显示最近 50 条记录。
stat	显示内容审计实时统计的计数信息，包括总记录数和阻断记录数。

【命令模式】 特权模式

【缺省级别】 14

【使用指导】 使用该命令可以查看实时统计的概要信息或计数信息。

【配置举例】 1：查看实时统计的概要信息。

```
Ruijie#show content-audit statistics brief
audit-totle-number:3
    id      relate-user       audit-time           action  key-type
----------  ----------------  -------------------  ------  ----------------------------
         3  220.181.12.101    2014-02-10 00:02:50  permit  recv-mail-title: 你好
         2  113.108.16.116    2014-02-09 14:26:31  permit  recv-mail-title: 转发: hello
         1  192.168.66.111    2014-02-09 14:26:08  permit  send-mail-title: 转发: hello
```

2：查看实时统计的计数信息。

```
Ruijie#show content-audit statistics counts

start-time: 2014-02-09 14:25:22

application control information:
    totle-num: 0
    block-num: 0

url reference host:
    totle-num: 0
    block-num: 0

web-search keyword:
    totle-num: 0
    block-num: 0

web-bbs post information:
    totle-num: 0
    block-num: 0

web-mail information:
    totle-num: 0
    block-num: 0

MSN information:
    totle-num: 0
    block-num: 0

QQ information:
    totle-num: 0
```

```
    block-num: 0

POP3 mail information:
    totle-num: 2
    block-num: 0

SMTP mail information:
    totle-num: 1
    block-num: 0
```

【提示信息】 -

【平台说明】 -

8.32 show content-audit write-db

显示内容审计审计是否写本地存储的开关状态。

show content-audit write-db

【参数说明】

参数	描述
-	-

【命令模式】 特权模式

【缺省级别】 14

【使用指导】 使用该命令可以查看内容审计各业务的审计信息是否写本地存储的开关状态。

【配置举例】 1：查看内容审计各业务写本地存储的开关状态。

```
Ruijie#show content-audit write-db
url_write_db:           1
web_search_write_db:    1
web_bbs_write_db:       1
web_mail_write_db:      1
mail_write_db:          1
im_write_db:            1
app_control_write_db:   1
```

【提示信息】 -

【平台说明】 有内置存储的产品支持，无内置存储的产品不支持。

8.33 show content-audit alarm

查询内容审计关键字订阅配置信息。

show content-audit alarm

查询内容审计关键字订阅日志

show content-audit alarm log [from *yyyy mm dd hh:mm:ss* **] [to** *yyyy mm dd hh:mm:ss* **] [type** *type-name* **] [offset** *n1* **] [limit** *n2* **] [by-auth]**

【参数说明】

参数	描述
yyyy mm dd hh:mm:ss	日志开始/结束时间
type-name	告警业务类型，包括 app-ctrl ,ftp, im , mail, post, postfile, telnet, url, web-bbs, web-mail, web-search
n1	从第 n1 条开始显示
n2	显示 n2 条

【命令模式】 特权模式

【缺省级别】 14

【使用指导】

【配置举例】 1：查看内容审计阻断告警配置信息。

```
Ruijie#show content-adudit alarm config
```

2：查看内容审计阻断告警邮件发送情况

```
Ruijie#show content-adudit alarm log limit 10
```

【提示信息】 -

【平台说明】 所有网关系列产品均支持。

8.34 show content-policy

显示策略组相关信息。

show content-policy [**policy** *policy-name* | **stat** policy-*name* | **all-rule**]

【参数说明】

参数	描述
content-policy	命令到该参数直接结束，显示所有策略组及组内所有策略概况

policy	显示指定策略组及组内所有策略详情
stat	显示指定策略组的状态（策略组是否存在，id 多少）。
all-rule	按照策略组排序显示所有策略组及组内所有策略详情
policy-name	策略组名称。指定该参数表示查询名为 *policy-name* 的策略组内详细策略信息。

【命令模式】 特权模式

【缺省级别】 14

【使用指导】 使用该命令可以查询策略组相关信息。

【配置举例】 1：查看所有存在的策略组及组内所有策略概况。

```
Ruijie#show content-policy
content-policy _TOP_PRIORITY
(active)app-rule 200 time-range any app-group Block_Group action deny audit
(active)app-rule 197 time-range any app-group Block_Group action deny audit vpn

content-policy _AUDIT_DEFAULT
(active)url-rule audit-default-enable
(active)im-rule audit-default-enable
```

2：查看指定策略组及组内所有策略详情

```
Ruijie#show content-policy policy _AUDIT_DEFAULT
policy-type: url-rule

rule-id         :0
unit-id         :0
url-object      :any
rule->obj_id    :0
action          :permit
audit           :Y
time-range      :
effective       :1
comment         :default_audit

-----------------------------------------------
policy-type: im-rule

rule-id         : 0
time-range      :
```

```
rule-type       : msn,qq
keyword         :
action          : permit
audit           : Y
effective       : 1
comment         : default_audit
```

3：查看自定义策略组的状态（策略组是否存在，id 多少）。

```
Ruijie#show content-policy stat _AUDIT_DEFAULT
exist: yes
policy_id:1
```

4：所有策略组及组内所有策略详情。

```
Ruijie#show content-policy all-rule
content-policy _TOP_PRIORITY
policy-type: app-rule

rule-id         : 197
unit-id         : 2
app-name        : Block_Group
app-id          : 4294967279
action          : deny
audit           : Y
vpn             : Y
vip             : N
time-range      : any
effective       : 1
comment         :

rule-id         : 200
unit-id         : 1
app-name        : Block_Group
app-id          : 4294967279
action          : deny
audit           : Y
vpn             : N
vip             : N
time-range      : any
effective       : 1
comment         :
```

```
-----------------------------------------------


content-policy _AUDIT_DEFAULT
policy-type: url-rule

rule-id         :0
unit-id         :0
url-object      :any
rule->obj_id    :0
action          :permit
audit           :Y
time-range      :
effective       :1
comment         :default_audit

-----------------------------------------------
policy-type: im-rule

rule-id         : 0
time-range      :
rule-type       : msn,qq
keyword         :
action          : permit
audit           : Y
effective       : 1
comment         : default_audit

-----------------------------------------------
```

【提示信息】 -

【平台说明】 -

8.35 show content-policy-relate

以策略视图显示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* } }]

以用户视图显示用户和策略的关联信息。

show content-policy-relate user-view { **subscriber** { *subs-name1* | **any** } | **auth-subscriber** { *subs-name2* | **any** } | **ip** *A.B.C.D* } [**detail**]

【参数说明】

参数	描述
policy-name	策略名
subs-name1	静态用户名或自定义用户组名
subs-name2	认证用户名
A.B.C.D	IP 地址

【命令模式】 特权模式

【缺省级别】 14

【使用指导】 使用该命令可以查询策略所关联的用户信息，或查询用户所关联的策略信息。

【配置举例】 1：以策略视图查看静态用户名为 userA 的关联信息。

```
Ruijie#show content-policy-relate policy-view subscriber userA
policy-name: policyA
disable: off
pri: 1
effective: 1 (1/1/1)
subscriber: userB userA
auth-subscriber:
```

2：以用户视图查看静态用户名为 userA 的关联信息。

```
Ruijie#show content-policy-relate user-view subscriber userA
policy-name: policyA
pri: 1
disable: on
effective: 1 (1/1/1)
relation-disable: on
inherit: 0
-------------------------------------------------
policy-summary: 1/0
user-inherit: 1
```

3：以策略视图查看用户 IP 地址为 A.B.C.D 的关联信息（此 IP 加入自定义用户组 cstm_grp1）。

```
Ruijie#show content-policy-relate policy-view ip A.B.C.D
policy-name: policyC
disable: off
pri: 3
```

```
effective: 1 (1/1/1)
subscriber: cstm_grp1
auth-subscriber:
```

4：以用户视图查看用户 IP 地址为 A.B.C.D 的关联信息。

```
Ruijie#show content-policy-relate user-view ip A.B.C.D
policy-name: policyC
pri: 3
disable: on
effective: 1 (1/1/1)
relation-disable: on
inherit: 0
-------------------------------------------------
policy-summary: 1/0
user-inherit: 1
```

【提示信息】 -

【平台说明】 -

8.36 show https-audit enable

查询 HTTPS 审计使能开关状态。

show https-audit enable

【参数说明】

参数	描述
-	-

【命令模式】 特权模式

【缺省级别】 14

【使用指导】 使用该命令可以查询 HTTPS 审计使能开关状态。

【配置举例】 1：查询 HTTPS 审计使能开关状态。

```
Ruijie#show https-audit enable
{
    "code": 0,
    "msg": "",
    "data": {
        "enable": "on"
```

```
    }
}
```

【提示信息】 -

【平台说明】 EG 全系列、NBR 全系列产品支持，其他系列的网关产品不支持。

8.37 show im-audit detail

查询 IM 审计的明细信息。

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*]

【参数说明】

参数	描述
hours	近期时间段
yyyy mm dd	年月日
hh:mm:ss	小时分钟秒
hour1	时间段过滤条件：开始小时段
hour2	时间段过滤条件：结束小时段
hour3	时间段过滤条件：开始小时段
hour4	时间段过滤条件：结束小时段
intf-name	接口名称
bridge-num	桥编号
subs-name1	过滤条件：静态用户名，精确匹配
subs-name2	过滤条件：认证用户名，精确匹配
keyword	过滤条件：聊天记录
account-string	过滤条件：聊天账号
rule-name	过滤条件： 匹配的规则名称
addr	过滤条件：IP，精确匹配；多个 IP 用“,”隔开
integer1	查询结果集合中的起始位置
integer2	查询结果集合中的结束位置

【命令模式】 特权模式

【缺省级别】 14

【使用指导】 使用该命令可以查询或导出 IM 审计的明细信息。

【配置举例】 1：查询 2013-5-1 的 0 点到 2013-5-7 的 24 点，用户 userA 的 MSN 审计明细信息。

```
Ruijie# show im-audit detail time-range from 2013 5 1 0:0:0 to 2013 5 7 23:59:59 subscriber userA
type msn order-by time desc start-item 1 end-item 20
==============================================================================================
Time: 2013-05-03 15:45:59
App-type: msn
Sender: userA@hotmail.com
Receiver: userB@yahoo.com
Direction: out
Path: GigabitEthernet 0/5
Ip: 192.168.211.96
User: /userA
Auth-User:
Match-Rule: ruleA
Action: permit
Message: hello!
......
```

【提示信息】 -

【平台说明】 有内置存储的产品支持，无内置存储的产品不支持。

8.38 show im-audit stat

查询 IM 审计的统计信息。

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**]

【参数说明】

参数	描述
hours	近期时间段
yyyy mm dd	年月日
hh:mm:ss	小时分钟秒
hour1	时间段过滤条件：开始小时段
hour2	时间段过滤条件：结束小时段
hour3	时间段过滤条件：开始小时段
hour4	时间段过滤条件：结束小时段

intf-name	接口名称
bridge-num	桥编号
subs-name1	过滤条件：静态用户名，精确匹配
subs-name2	过滤条件：认证用户名，精确匹配
keyword	过滤条件：聊天记录
account-string	过滤条件：聊天账号
rule-name	过滤条件： 匹配的规则名称
addr	过滤条件：内网 ip

【命令模式】 特权模式

【缺省级别】 14

【使用指导】 使用该命令可以查询 IM 审计的统计信息。

【配置举例】 1：查询 2013-5-1 的 0 点到 2013-5-7 的 24 点，用户 userA 的 MSN 审计统计信息。

```
Ruijie# show im-audit stat time-range from 2013 5 1 0:0:0 to 2013 5 7 23:59:59 subscriber userA type msn
50
```

【提示信息】 -

【平台说明】 有内置存储的产品支持，无内置存储的产品不支持。

8.39 show mail-audit attachment-info

查询某一封邮件的附件信息。

show mail-audit attachment-info timestamp *timestamp* **rand-id** *rand-id*

【参数说明】

参数	描述
timestamp	时间戳
rand-id	随机 id

【命令模式】 特权模式

【缺省级别】 14

【使用指导】 先用命令 show mail-audit detail 查看邮件的时间戳和随机 id，再使用该命令可以查询某一封邮件的附件信息。

【配置举例】 1：查询 timestamp 为 1286849291，rand-id 为 1087821567 的邮件的附件信息。

```
Ruijie#show mail-audit attachment-info timestamp 1286849291 rand-id 1087821567
Size(Byte)   Path
============================================================
80646        mnt/sata/mail/20130503/unknown(09-01-19-44-40).gif
150528       mnt/sata/mail/20130503/test-file.doc
```

【提示信息】 -

【平台说明】 有内置存储的产品支持，所有无内置存储的设备均不支持。

8.40 show mail-audit detail

查询 MAIL 审计的明细信息。

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*]

【参数说明】

参数	描述
hours	近期时间段
yyyy mm dd	年月日
hh:mm:ss	小时分钟秒
hour1	时间段过滤条件：开始小时段
hour2	时间段过滤条件：结束小时段
hour3	时间段过滤条件：开始小时段
hour4	时间段过滤条件：结束小时段
intf-name	接口名称
bridge-num	桥编号
subs-name1	过滤条件：静态用户名，精确匹配
subs-name2	过滤条件：认证用户名，精确匹配
addr	过滤条件：IP，精确匹配；多个 IP 用“,”隔开
keyword1	过滤条件：邮件发送者关键字
keyword2	过滤条件：邮件接收者关键字
keyword3	过滤条件：邮件主题关键字
rule-name	过滤条件： 匹配的规则名称
integer1	查询结果集合中的起始位置
integer2	查询结果集合中的结束位置

【命令模式】 特权模式

【缺省级别】 14

【使用指导】 使用该命令可以查询或导出 MAIL 审计的明细信息。

【配置举例】 1：查询 2013-5-1 的 0 点到 2013-5-7 的 24 点，用户 userA 的 MAIL 审计明细信息。

```
Ruijie# show mail-audit detail time-range from 2013 5 1 0:0:0 to 2013 5 7 23:59:59 subscriber userA
order-by time desc start-item 1 end-item 20
==============================================================================================
Time: 2013-05-03 15:45:59
App-type: SMTP
Direction: out
Path: GigabitEthernet 0/5
Ip: 192.168.211.96
User: /userA
Auth-User:
Match-Rule: ruleA
Action: permit
Timestamp: 1287027112
Rand-id: 1686175891
From: userA@hotmail.com
To: userB@yahoo.com
Subject: hello
Body: hello
......
```

【提示信息】 -

【平台说明】 有内置存储的产品支持，所有无内置存储的产品均不支持。

8.41 show mail-audit stat

查询 MAIL 审计的统计信息。

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**]

【参数说明】

参数	描述

hours	近期时间段
yyyy mm dd	年月日
hh:mm:ss	小时分钟秒
hour1	时间段过滤条件：开始小时段
hour2	时间段过滤条件：结束小时段
hour3	时间段过滤条件：开始小时段
hour4	时间段过滤条件：结束小时段
intf-name	接口名称
bridge-num	桥编号
subs-name1	过滤条件：静态用户名，精确匹配
subs-name2	过滤条件：认证用户名，精确匹配
addr	过滤条件：IP，精确匹配；多个 IP 用“,”隔开
keyword1	过滤条件：邮件发送者关键字
keyword2	过滤条件：邮件接收者关键字
keyword3	过滤条件：邮件主题关键字
rule-name	过滤条件： 匹配的规则名称

【命令模式】 特权模式

【缺省级别】 14

【使用指导】 使用该命令可以查询 MAIL 审计的统计信息。

【配置举例】 1：查询 2013-5-1 的 0 点到 2013-5-7 的 24 点，用户 userA 的 MAIL 审计统计信息。

```
Ruijie# show mail-audit stat time-range from 2013 5 1 0:0:0 to 2013 5 7 23:59:59 subscriber userA
50
```

【提示信息】 -

【平台说明】 有内置存储的产品支持，所有无内置存储的产品均不支持。

8.42 show plugin-audit detail

查询 QQ 聊天内容审计的明细信息。

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*] [**message** *keyword*] [**rule-name** *rule-name*] [**permit | deny**] **order-by** { **time** | **subscriber** | **auth-subscriber | internal-ip | url** } { **asc** | **desc** } [**start-item** *integer1* **end-item** *integer2*]

【参数说明】

参数	描述
hours	近期时间段
yyyy mm dd	年月日
hh:mm:ss	小时分钟秒
hour1	时间段过滤条件：开始小时段
hour2	时间段过滤条件：结束小时段
hour3	时间段过滤条件：开始小时段
hour4	时间段过滤条件：结束小时段
intf-name	接口名称
bridge-num	桥编号
subs-name1	过滤条件：静态用户名，精确匹配
subs-name2	过滤条件：认证用户名，精确匹配
addr	过滤条件：IP，精确匹配；多个 IP 用“,”隔开
keyword	过滤条件：过滤关键字，支持多关键字过滤，不同关键字间以半角逗号隔开
rule-name	过滤条件： 匹配的规则名称，支持多规则名过滤，不同规则名间以半角逗号隔开
integer1	查询结果集合中的起始位置
integer2	查询结果集合中的结束位置

【命令模式】 特权模式

【缺省级别】 14

【使用指导】 使用该命令可以查询或导出 QQ 聊天内容审计的明细信息。

【配置举例】 1：查询 2016-11-29 的 0 点到 2016-11-29 的 24 点， QQ 聊天内容审计明细信息。

```
Ruijie#  show plugin-audit detail time-range from 2016 11 29 00:00:00 to 2016 11 29 23:59:59 order-by time desc start-item 1 end-item 20
================================================================================================
id: 157
sip: 172.21.159.221
soft: QQ
type: f
sendid: 263985410
sendname: 十六夜の月
recvid: 792941456
recvname: 丨简爱
datetime: 2016:11:29:18:00:43
flag: s
len: 5
```

```
message: hello
```

【提示信息】 -

【平台说明】 ACE 系列产品不支持，其他有内置存储的产品支持，所有无内置存储的产品均不支持。

8.43 show plugin-audit stat

查询 QQ 聊天内容审计的统计信息。

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*] [**message** *keyword*] [**rule-name** *rule-name*] [**permit** | **deny**]

【参数说明】

参数	描述
hours	近期时间段
yyyy mm dd	年月日
hh:mm:ss	小时分钟秒
hour1	时间段过滤条件：开始小时段
hour2	时间段过滤条件：结束小时段
hour3	时间段过滤条件：开始小时段
hour4	时间段过滤条件：结束小时段
intf-name	接口名称
bridge-num	桥编号
subs-name1	过滤条件：静态用户名，精确匹配
subs-name2	过滤条件：认证用户名，精确匹配
addr	过滤条件：IP，精确匹配；多个 IP 用“,”隔开
keyword	过滤条件：过滤关键字，支持多关键字过滤，不同关键字间以半角逗号隔开
rule-name	过滤条件： 匹配的规则名称，支持多规则名过滤，不同规则名间以半角逗号隔开

【命令模式】 特权模式

【缺省级别】 14

【使用指导】 使用该命令可以查询 QQ 聊天内容审计的统计信息。

【配置举例】 1：查询 2013-5-1 的 0 点到 2013-5-7 的 24 点， PLUGIN 审计统计信息。

```
Ruijie# show plugin-audit stat time-range from 2013 5 1 0:0:0 to 2013 5 7 23:59:59
50
```

【提示信息】 -

【平台说明】 ACE 系列产品不支持，其他有内置存储的产品支持，所有无内置存储的产品均不支持。

8.44 show postfile-audit detail

查询外发文件审计的明细信息。

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*] [**filename** *keyword*] [**rule-name** *rule-name*] [**permit | deny**] **order-by** { **time** | **subscriber** | **auth-subscriber | internal-ip | url** } { **asc** | **desc** } [**start-item** *integer1* **end-item** *integer2*]

【参数说明】

参数	描述
hours	近期时间段
yyyy mm dd	年月日
hh:mm:ss	小时分钟秒
hour1	时间段过滤条件：开始小时段
hour2	时间段过滤条件：结束小时段
hour3	时间段过滤条件：开始小时段
hour4	时间段过滤条件：结束小时段
intf-name	接口名称
bridge-num	桥编号
subs-name1	过滤条件：静态用户名，精确匹配
subs-name2	过滤条件：认证用户名，精确匹配
addr	过滤条件：IP，精确匹配；多个 IP 用“,”隔开
keyword	过滤条件：过滤关键字，支持多关键字过滤，不同关键字间以半角逗号隔开
rule-name	过滤条件： 匹配的规则名称，支持多规则名过滤，不同规则名间以半角逗号隔开
integer1	查询结果集合中的起始位置
integer2	查询结果集合中的结束位置

【命令模式】 特权模式

【缺省级别】 14

【使用指导】 使用该命令可以查询或导出外发文件审计的明细信息。

【配置举例】 1：查询 2016-9-4 的 0 点到 2016-11-4 的 24 点，用户 userA 的外发文件审计明细信息。

```
Ruijie# show postfile-audit detail time-range from 2016 11 4 0:0:0 to 2016 11 4 23:59:59 subscriber userA order-by time desc start-item 1 end-item 20
```

```
id: 1
time_stamp: 1480056761
day_time: 2016-11-25 14:52:41
sip: 3.3.3.54
dip: 60.28.228.9
sport: 60141
dport: 80
mac_addr: f48e.388f.f50d
usr_grp: /
usr_name: 3.3.3.54
plcy_name: _AUDIT_DEFAULT
rule_name: default_audit
obj_name:
action: permit
username: nabi2006@sina.com
nickname:
uid:
app_type: 新浪邮箱附件
filename: 叮当猫.jpg
path: /mnt/sata0/file/20161125/1480056761-000000-叮当猫.jpg
filesize: 412871
relate_id: 03030336eaed3c1ce4090050
filetype:
……
```

【提示信息】 -

【平台说明】 ACE 系列产品不支持，其他有内置存储的产品支持，所有无内置存储的产品均不支持。

8.45 show postfile-audit relate-id

查询某一封邮件或发帖的附件信息。

show postfile-audit relate-id *rand-id* **timestamp** *timestamp*

【参数说明】

参数	描述

relate-id	关联 ID。对应邮件的附件 ID
timestamp	时间戳

【命令模式】 特权模式

【缺省级别】 14

【使用指导】 先用命令 show mail-audit detail 查看邮件的时间戳和附件 id，再使用该命令可以查询某一封邮件的附件信息。

【配置举例】 1：查询 timestamp 为 1476253284，relate-id 为 03030336e7353d879e5a0050 的邮件的附件信息。

```
Ruijie#show postfile-audit relate-id 03030336e7353d879e5a0050 timestamp 1476253284
Size(Byte)   Path
=====================================================
relate_id: 03030336e7353d879e5a0050
time_stamp: 1476253284
filesize: 111
path: /mnt/sata0/file/20161013/1476339684-000000-F1.jpg
```

【提示信息】 -

【平台说明】 ACE 系列产品不支持，其他有内置存储的产品支持，所有无内置存储的设备均不支持。

8.46 show postfile-audit stat

查询外发文件审计的统计信息。

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*] [**filename** *keyword*] [**rule-name** *rule-name*] [**permit** | **deny**]

【参数说明】

参数	描述
hours	近期时间段
yyyy mm dd	年月日
hh:mm:ss	小时分钟秒
hour1	时间段过滤条件：开始小时段
hour2	时间段过滤条件：结束小时段
hour3	时间段过滤条件：开始小时段
hour4	时间段过滤条件：结束小时段
intf-name	接口名称
bridge-num	桥编号

subs-name1	过滤条件：静态用户名，精确匹配
subs-name2	过滤条件：认证用户名，精确匹配
addr	过滤条件：IP，精确匹配；多个 IP 用“,”隔开
keyword	过滤条件：过滤关键字，支持多关键字过滤，不同关键字间以半角逗号隔开
rule-name	过滤条件： 匹配的规则名称，支持多规则名过滤，不同规则名间以半角逗号隔开

【命令模式】 特权模式

【缺省级别】 14

【使用指导】 使用该命令可以查询外发文件审计的统计信息。

【配置举例】 1：查询 2013-5-1 的 0 点到 2013-5-7 的 24 点，用户 userA 的外发文件审计统计信息。

```
Ruijie# show postfile-audit stat time-range from 2013 5 1 0:0:0 to 2013 5 7 23:59:59 subscriber userA
50
```

【提示信息】 -

【平台说明】 ACE 系列产品不支持，其他有内置存储的产品支持，所有无内置存储的产品均不支持。

8.47 show post-audit detail

查询 POST 审计的明细信息。

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*]

【参数说明】

参数	描述
hours	近期时间段
yyyy mm dd	年月日
hh:mm:ss	小时分钟秒
hour1	时间段过滤条件：开始小时段
hour2	时间段过滤条件：结束小时段
hour3	时间段过滤条件：开始小时段
hour4	时间段过滤条件：结束小时段
intf-name	接口名称

bridge-num	桥编号
subs-name1	过滤条件：静态用户名，精确匹配
subs-name2	过滤条件：认证用户名，精确匹配
addr	过滤条件：IP，精确匹配；多个 IP 用“,”隔开
keyword	过滤条件：过滤关键字，支持多关键字过滤，不同关键字间以半角逗号隔开
rule-name	过滤条件： 匹配的规则名称，支持多规则名过滤，不同规则名间以半角逗号隔开
integer1	查询结果集合中的起始位置
integer2	查询结果集合中的结束位置

【命令模式】 特权模式

【缺省级别】 14

【使用指导】 使用该命令可以查询或导出 POST 审计的明细信息。

【配置举例】 1：查询 2016-11-4 的 0 点到 2016-11-4 的 24 点，用户 userA 的 POST 审计明细信息。

```
Ruijie# show post-audit detail time-range from 2016 11 4 0:0:0 to 2016 11 4 23:59:59 subscriber userA
order-by time desc start-item 1 end-item 20
================================================================================================
==================================================
id: 7
time_stamp: 1479868298
day_time: 2016-11-23 10:31:38
sip: 3.3.3.54
dip: 124.251.20.10
sport: 59199
dport: 80
mac_addr: f48e.388f.f50d
usr_grp: /
usr_name: 3.3.3.54
plcy_name: _AUDIT_DEFAULT
rule_name: default_audit
obj_name:
action: permit
app_type: 普通网页浏览
url: http://www.btime.com/
body: content[]={}
==================================================
......
```

【提示信息】 -

【平台说明】 ACE 系列产品不支持，其他有内置存储的产品支持，所有无内置存储的产品均不支持。

8.48 show post-audit stat

查询 POST 审计的统计信息。

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**]

【参数说明】

参数	描述
hours	近期时间段
yyyy mm dd	年月日
hh:mm:ss	小时分钟秒
hour1	时间段过滤条件：开始小时段
hour2	时间段过滤条件：结束小时段
hour3	时间段过滤条件：开始小时段
hour4	时间段过滤条件：结束小时段
intf-name	接口名称
bridge-num	桥编号
subs-name1	过滤条件：静态用户名，精确匹配
subs-name2	过滤条件：认证用户名，精确匹配
addr	过滤条件：IP，精确匹配；多个 IP 用“,”隔开
keyword	过滤条件：过滤关键字，支持多关键字过滤，不同关键字间以半角逗号隔开
rule-name	过滤条件： 匹配的规则名称，支持多规则名过滤，不同规则名间以半角逗号隔开

【命令模式】 特权模式

【缺省级别】 14

【使用指导】 使用该命令可以查询 POST 审计的统计信息。

【配置举例】 1：查询 2016-11-4 的 0 点到 2016-11-4 的 24 点，用户 userA 的 POST 审计统计信息。

```
Ruijie# show post-audit stat time-range from 2016 11 4 0:0:0 to 2016 11 4 23:59:59 subscriber userA
1508
```

【提示信息】 -

【平台说明】 ACE 系列产品不支持，其他有内置存储的产品支持，所有无内置存储的产品均不支持。

8.49 show content-audit deny-stat

显示内容审计的实时阻断统计信息。

show content-audit deny-stat { brief | counts |ip}

【参数说明】

参数	描述
brief	显示内容审计阻断实时统计的概要信息，只显示最近 50 条记录。
counts	显示内容审计阻断实时统计的计数信息，包括总记录数和阻断记录数。
ip	显示设定的特定 IP

【命令模式】 特权模式

【缺省级别】 14

【使用指导】 使用该命令可以查看实时统计的阻断概要信息或计数信息。

【配置举例】 1：查看实时统计的概要信息。

```
Ruijie#show content-audit deny-stat brief
audit-totle-number:1
    id       relate-user       audit-time      ca_type      app_type        plcy_name
content
---------- ---------------- ---------------- ---------- ---------------- ----------------
----------------------------
         1 10               2017-10-10 10:28:24 IM         QQ               _TOP_PRIORITY    QQ:
263985410 LOGIN
```

2：查看实时统计的计数信息。

```
Ruijie#show content-audit statistics counts
start-time: 2017-10-10 10:28:15

application control information:
    totle-num: 0
    block-num: 0

url reference host:
    totle-num: 0
```

```
    block-num: 0

web-search keyword:
    totle-num: 0
    block-num: 0

web-bbs post information:
    totle-num: 0
    block-num: 0

web-mail information:
    totle-num: 0
    block-num: 0

MSN information:
    totle-num: 0
    block-num: 0

QQ information:
    totle-num: 1
    block-num: 1

POP3 mail information:
    totle-num: 0
    block-num: 0

SMTP mail information:
    totle-num: 0
    block-num: 0

virtual id information:
    totle-num: 0
    block-num: 0

postfile information:
    totle-num: 0
    block-num: 0

post information:
    totle-num: 0
    block-num: 0
```

```
plugin information:
    totle-num: 0
    block-num: 0
```

3：查看设置的特定 IP

```
Ruijie# show content-audit deny-stat ip

content-audit deny-stat ip 192.168.1.2
```

【提示信息】 -

【平台说明】 所有网关系列产品均支持。

8.50 show url-audit detail

查询 URL 审计的明细信息。

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*]

【参数说明】

参数	描述
hours	近期时间段
yyyy mm dd	年月日
hh:mm:ss	小时分钟秒
hour1	时间段过滤条件：开始小时段
hour2	时间段过滤条件：结束小时段
hour3	时间段过滤条件：开始小时段
hour4	时间段过滤条件：结束小时段
intf-name	接口名称
bridge-num	桥编号
subs-name1	过滤条件：静态用户名，精确匹配
subs-name2	过滤条件：认证用户名，精确匹配
addr	过滤条件：IP，精确匹配；多个 IP 用 “,” 隔开
class-name	过滤条件：URL 分类名称，精确匹配
obj-name	过滤条件：URL 对象名称，精确匹配
url-string	过滤条件：URL 字符串，模糊匹配
host-string1	过滤条件：HOST 字符串，精确匹配

host-string2	过滤条件：HOST 站点，精确匹配
integer1	查询结果集合中的起始位置
integer2	查询结果集合中的结束位置

【命令模式】 特权模式

【缺省级别】 14

【使用指导】 使用该命令可以查询或导出 URL 审计的明细信息。

【配置举例】 1：查询 2013-5-1 的 0 点到 2013-5-7 的 24 点，用户 userA 的 URL 审计明细信息。

```
Ruijie# show url-audit detail time-range from 2013 5 1 0:0:0 to 2013 5 7 23:59:59 subscriber userA
order-by time desc start-item 1 end-item 20
=============================================================================================
Time: 2013-05-03 15:45:59
Ip: 192.168.211.96
Subscriber: /userA
Auth-subscriber:
Match-rule: ruleA
Action: permit
URL: http://www.ietf.org/
URL-class: 国外网站
......
```

【提示信息】 -

【平台说明】 有内置存储的网关产品支持，无内置存储的网关产品不支持。

8.51 show url-audit stat

查询 URL 审计的统计信息。

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**]

【参数说明】

参数	描述
hours	近期时间段
yyyy mm dd	年月日
hh:mm:ss	小时分钟秒
hour1	时间段过滤条件：开始小时段

hour2	时间段过滤条件：结束小时段
hour3	时间段过滤条件：开始小时段
hour4	时间段过滤条件：结束小时段
intf-name	接口名称
bridge-num	桥编号
subs-name1	过滤条件：静态用户名，精确匹配
subs-name2	过滤条件：认证用户名，精确匹配
addr	过滤条件：IP，精确匹配；多个 IP 用“,”隔开
class-name	过滤条件：URL 分类名称，精确匹配
obj-name	过滤条件：URL 对象名称，精确匹配
host-string	过滤条件：HOST 站点，精确匹配

【命令模式】 特权模式

【缺省级别】 14

【使用指导】 使用该命令可以查询 URL 审计的统计信息。

【配置举例】 1：查询 2013-5-1 的 0 点到 2013-5-7 的 24 点，用户 userA 的 URL 审计统计信息。

```
Ruijie# show url-audit stat time-range from 2013 5 1 0:0:0 to 2013 5 7 23:59:59 subscriber userA
500
```

【提示信息】 -

【平台说明】 有内置存储的网关产品支持，无内置存储的网关产品不支持。

8.52 show url-audit top

查询 URL 站点访问排名 TOPN。

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**]

【参数说明】

参数	描述
n	Top n 的个数（1~100）
hours	近期时间段
yyyy mm dd	年月日
hh:mm:ss	小时分钟秒

hour1	时间段过滤条件：开始小时段
hour2	时间段过滤条件：结束小时段
hour3	时间段过滤条件：开始小时段
hour4	时间段过滤条件：结束小时段
intf-name	接口名称
bridge-num	桥编号
subs-name1	过滤条件：静态用户名，精确匹配
subs-name2	过滤条件：认证用户名，精确匹配
addr	过滤条件：IP，精确匹配；多个 IP 用“,”隔开
class-name	过滤条件：URL 分类名称，精确匹配
obj-name	过滤条件：URL 对象名称，精确匹配
host-string	过滤条件：HOST 站点，精确匹配

【命令模式】 特权模式

【缺省级别】 14

【使用指导】 使用该命令可以查询或导出 URL 站点访问排名 TOPN。

【配置举例】 1：查询 24 小时内站点访问排名 TOP2

```
Ruijie# show url-audit top 2 recent 24
HOST                 Times          url-class          url-object
============================================================

www.ietf.org            32349             class1         obj1
www.w3c.org             30032             class2         obj2
```

【提示信息】 -

【平台说明】 有内置存储的网关产品支持，无内置存储的网关产品不支持。

8.53 show url-class system

显示系统当前的 URL 库的各分类名。

show url-class system [**class** { **id** *class-id* | **name** *class-name* }]

显示系统当前的 URL 库的描述信息。

show url-class system comment [**class** { **id** *class-id* | **name** *class-name* }]

显示系统 URL 库的当前自定义修改信息。

show url-class system custom [**class** { **id** *class-id* | **name** *class-name* }]

显示精准过滤库相关信息。

show url-class system exact

【参数说明】

参数	描述
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

【缺省级别】 14

【使用指导】 使用该命令可以查询系统 URL 库相关信息。

【配置举例】 1：查看系统当前的 URL 库的各分类名。

```
Ruijie# show url-class system
version-1.0
2010-4-22
system-url-class-number:32
大类 1
    求职招聘
    IT 类
    WEB 通信
    暴力
    病毒
大类 2
    科学
    成人
    （以下省略）
```

2：查看系统当前的 URL 库分组与分类信息。

```
Ruijie# show url-class system custom
version-1.0
2010-4-22
system-url-class-number:32
consumption-amount:2
remain-amount:998 （这几行是一些必要的统计信息）
大类 1
    url-class: 求职招聘
        comment: 求职招聘类描述
```

```
            add: add1.com
            add: add2.com
           move: move1.com
           move: move2.com
    url-class: 军事
         comment: 军事类描述
    url-class: IT 类
         comment: IT 类描述
            add: add1.com
            add: add2.com
           move: move1.com
           move: move2.com
大类 2
    url-class:
         comment:
    （以下省略）
```

3：查看系统当前的 URL 库分类与描述信息。

```
Ruijie# show url-class system comment
version-1.0
2010-4-22
System url class number:32
大类 1
    求职招聘 ： 描述信息 1
    IT 类 ： 描述信息 2
    WEB 通信 ： 描述信息 3
.....（以下略）
```

4：查看精准过滤库的相关信息

```
Ruijie# show url-class system exact
exact-filter: disable
```

【提示信息】 -

【平台说明】 -

8.54 show url-class url

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。

show url-class url *url-string*

【参数说明】

参数	描述
url-string	代表 url 的字符串

【命令模式】 特权模式

【缺省级别】 14

【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。

【配置举例】 1：显示 URL 为 ruijie.com.cn 的分类信息。

```
Ruijie# show url-class url ruijie.com.cn
url:ruijie.com.cn
default-system-class:商业
modified-system-class:
custom-class:test1
```

【提示信息】 -

【平台说明】 -

8.55 show url-class user-cfg

显示自定义 URL 分类的配置信息。

show url-class user-cfg [*class-name*]

【参数说明】

参数	描述
class-name	自定义的分类名

【命令模式】 特权模式

【缺省级别】 14

【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】 1：显示各个自定义 URL 分类配置信息。

```
Ruijie# show url-class user-cfg
url-class:CLASSA
url:ietf.org
comment:comment for CLASSA
url-class:CLASSB
url:w3c.org
```

```
comment:comment for CLASSB
```

2：显示指定 URL 分类的配置信息。

```
Ruijie# show url-class user-cfg CLASSA
url-class:CLASSA
url:ietf.org
comment:comment for CLASSA
```

【提示信息】 -

【平台说明】 -

8.56 show vid-audit detail

查询虚拟身份审计的明细信息。

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*]

【参数说明】

参数	描述
hours	近期时间段
yyyy mm dd	年月日
hh:mm:ss	小时分钟秒
hour1	时间段过滤条件：开始小时段
hour2	时间段过滤条件：结束小时段
hour3	时间段过滤条件：开始小时段
hour4	时间段过滤条件：结束小时段
subs-name1	过滤条件：静态用户名，精确匹配
subs-name2	过滤条件：认证用户名，精确匹配
uid-string	过滤条件：账号 UID
nick-string	过滤条件：账号昵称
addr1	过滤条件：IP，精确匹配；多个 IP 用“,”隔开
addr2	过滤条件：MAC 地址，精确匹配；多个地址用“,”隔开
integer1	查询结果集合中的起始位置
integer2	查询结果集合中的结束位置

【命令模式】 特权模式

【缺省级别】 14

【使用指导】 使用该命令可以查询或导出虚拟身份审计的明细信息。

【配置举例】 1：查询 2013-5-1 的 0 点到 2013-5-7 的 24 点，用户 userA 的虚拟身份审计明细信息。

```
Ruijie# show vid-audit detail time-range from 2013 5 1 0:0:0 to 2013 5 7 23:59:59 subscriber userA
type msn order-by time desc start-item 1 end-item 20
==============================================================================================
day_time: 2013-05-03 15:45:59
internal_ip: 192.168.211.96
mac_addr: 00d0.1234.abcd
usr_grp: /
usr_name: /userA
vid_type: 微信
vid_action: LOGOUT
uid: 1755006665
nick_name:
......
```

【提示信息】 -

【平台说明】 有内置存储的网关产品支持；所有无内置存储的网关产品均不支持。

8.57 show vid-audit stat

查询虚拟身份审计的统计信息。

show vid-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*]

【参数说明】

参数	描述
hours	近期时间段
yyyy mm dd	年月日
hh:mm:ss	小时分钟秒
hour1	时间段过滤条件：开始小时段
hour2	时间段过滤条件：结束小时段
hour3	时间段过滤条件：开始小时段
hour4	时间段过滤条件：结束小时段
subs-name1	过滤条件：静态用户名，精确匹配
subs-name2	过滤条件：认证用户名，精确匹配

uid-string	过滤条件：账号 UID
nick-string	过滤条件：账号昵称
addr1	过滤条件：IP，精确匹配；多个 IP 用“,”隔开
addr2	过滤条件：MAC 地址，精确匹配；多个地址用“,”隔开

【命令模式】 特权模式

【缺省级别】 14

【使用指导】 使用该命令可以查询虚拟身份审计的统计信息。

【配置举例】 1：查询 2013-5-1 的 0 点到 2013-5-7 的 24 点，用户 userA 的 MSN 审计统计信息。

```
Ruijie# show vid-audit stat time-range from 2013 5 1 0:0:0 to 2013 5 7 23:59:59 subscriber userA type msn
50
```

【提示信息】 -

【平台说明】 有内置存储的网关产品支持；所有无内置存储的网关产品均不支持。

8.58 show web-bbs-audit detail

查询 WEB-BBS 审计的明细信息。

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*]

【参数说明】

参数	描述
hours	近期时间段
yyyy mm dd	年月日
hh:mm:ss	小时分钟秒
hour1	时间段过滤条件：开始小时段
hour2	时间段过滤条件：结束小时段
hour3	时间段过滤条件：开始小时段
hour4	时间段过滤条件：结束小时段
intf-name	接口名称
bridge-num	桥编号
subs-name1	过滤条件：静态用户名，精确匹配

subs-name2	过滤条件：认证用户名，精确匹配
addr	过滤条件：IP，精确匹配；多个 IP 用“,”隔开
keyword	过滤条件：过滤关键字，支持多关键字过滤，不同关键字间以半角逗号隔开
rule-name	过滤条件： 匹配的规则名称，支持多规则名过滤，不同规则名间以半角逗号隔开
integer1	查询结果集合中的起始位置
integer2	查询结果集合中的结束位置

【命令模式】 特权模式

【缺省级别】 14

【使用指导】 使用该命令可以查询或导出 WEB-BBS 审计的明细信息。

【配置举例】 1：查询 2013-5-1 的 0 点到 2013-5-7 的 24 点，用户 userA 的 WEB-BBS 审计明细信息。

```
Ruijie# show web-bbs-audit detail time-range from 2013 5 1 0:0:0 to 2013 5 7 23:59:59 subscriber
userA order-by time desc start-item 1 end-item 20
==========================================================================
Time: 2013-05-03 16:45:29
subscriber: /userA
auth-subscriber: any
Ip: 192.168.211.96
Rule: ruleA
Action: permit
Title: hello
Body: hello
......
```

【提示信息】 -

【平台说明】 有内置存储的网关产品支持；所有无内置存储的网关产品均不支持。

8.59 show web-bbs-audit stat

查询 WEB-BBS 审计的统计信息。

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**]

【参数说明】

参数	描述
hours	近期时间段
yyyy mm dd	年月日
hh:mm:ss	小时分钟秒
hour1	时间段过滤条件：开始小时段
hour2	时间段过滤条件：结束小时段
hour3	时间段过滤条件：开始小时段
hour4	时间段过滤条件：结束小时段
intf-name	接口名称
bridge-num	桥编号
subs-name1	过滤条件：静态用户名，精确匹配
subs-name2	过滤条件：认证用户名，精确匹配
addr	过滤条件：IP，精确匹配；多个 IP 用“,”隔开
keyword	过滤条件：过滤关键字，支持多关键字过滤，不同关键字间以半角逗号隔开
rule-name	过滤条件： 匹配的规则名称，支持多规则名过滤，不同规则名间以半角逗号隔开

【命令模式】 特权模式

【缺省级别】 14

【使用指导】 使用该命令可以查询 WEB-BBS 审计的统计信息。

【配置举例】 1：查询 2013-5-1 的 0 点到 2013-5-7 的 24 点，用户 userA 的 WEB-BBS 审计统计信息。

```
Ruijie# show web-bbs-audit stat time-range from 2013 5 1 0:0:0 to 2013 5 7 23:59:59 subscriber userA 50
```

【提示信息】 -

【平台说明】 ACE 系列产品不支持，其他有内置存储的网关产品支持；所有无内置存储的网关产品均不支持。

8.60 show web-mail-audit attachment-info

查询某一封邮件的附件信息。

show web-mail-audit attachment-info timestamp *timestamp* **rand-id** *rand-id*

【参数说明】

参数	描述
timestamp	时间戳
rand-id	随机 id

【命令模式】 特权模式

【缺省级别】 14

【使用指导】 先用命令 show web-mail-audit detail 查看邮件的时间戳和随机 id，再使用该命令可以查询某一封邮件的附件信息。

【配置举例】 1：查询 timestamp 为 1286849291，rand-id 为 1087821567 的邮件的附件信息。

```
Ruijie#show web-mail-audit attachment-info timestamp 1286849291 rand-id 1087821567
Size(Byte)   Path
============================================================
80646        mnt/sata/mail/20130503/unknown(09-01-19-44-40).gif
150528       mnt/sata/mail/20130503/test-file.doc
```

【提示信息】 -

【平台说明】 有内置存储的网关产品支持；所有无内置存储的网关产品均不支持。

8.61 show web-mail-audit detail

查询 WEB-MAIL 审计的明细信息。

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*]

【参数说明】

参数	描述
hours	近期时间段
yyyy mm dd	年月日
hh:mm:ss	小时分钟秒
hour1	时间段过滤条件：开始小时段
hour2	时间段过滤条件：结束小时段
hour3	时间段过滤条件：开始小时段
hour4	时间段过滤条件：结束小时段
intf-name	接口名称
bridge-num	桥编号
subs-name1	过滤条件：静态用户名，精确匹配

subs-name2	过滤条件：认证用户名，精确匹配
addr	过滤条件：IP，精确匹配；多个 IP 用“,”隔开
keyword1	过滤条件：邮件发送者关键字
keyword2	过滤条件：邮件接收者关键字
keyword3	过滤条件：邮件主题关键字
rule-name	过滤条件： 匹配的规则名称
integer1	查询结果集合中的起始位置
integer2	查询结果集合中的结束位置

【命令模式】 特权模式

【缺省级别】 14

【使用指导】 使用该命令可以查询或导出 WEB-MAIL 审计的明细信息。

【配置举例】 1：查询 2013-5-1 的 0 点到 2013-5-7 的 24 点，用户 userA 的 WEB-MAIL 审计明细信息。

```
Ruijie# show web-mail-audit detail time-range from 2013 5 1 0:0:0 to 2013 5 7 23:59:59 subscriber
userA order-by time desc start-item 1 end-item 20
=============================================================================================
Time: 2013-05-03 15:45:59
Direction: out
Path: GigabitEthernet 0/5
Ip: 192.168.211.96
User: /userA
Auth-User:
Match-Rule: ruleA
Action: permit
Timestamp: 1287027112
Rand-id: 1686175891
From: userA@hotmail.com
To: userB@yahoo.com
Subject: hello
Body: hello
......
```

【提示信息】 -

【平台说明】 有内置存储的网关产品支持；所有无内置存储的网关产品均不支持。

8.62 show web-mail-audit stat

查询 WEB-MAIL 审计的统计信息。

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**]

【参数说明】

参数	描述
hours	近期时间段
yyyy mm dd	年月日
hh:mm:ss	小时分钟秒
hour1	时间段过滤条件：开始小时段
hour2	时间段过滤条件：结束小时段
hour3	时间段过滤条件：开始小时段
hour4	时间段过滤条件：结束小时段
intf-name	接口名称
bridge-num	桥编号
subs-name1	过滤条件：静态用户名，精确匹配
subs-name2	过滤条件：认证用户名，精确匹配
addr	过滤条件：IP，精确匹配；多个 IP 用 “,” 隔开
keyword1	过滤条件：邮件发送者关键字
keyword2	过滤条件：邮件接收者关键字
keyword3	过滤条件：邮件主题关键字
rule-name	过滤条件： 匹配的规则名称

【命令模式】 特权模式

【缺省级别】 14

【使用指导】 使用该命令可以查询 WEB-MAIL 审计的统计信息。

【配置举例】 1：查询 2013-5-1 的 0 点到 2013-5-7 的 24 点，用户 userA 的 WEB-MAIL 审计统计信息。

```
Ruijie# show web-mail-audit stat time-range from 2013 5 1 0:0:0 to 2013 5 7 23:59:59 subscriber userA
50
```

【提示信息】 -

【平台说明】 有内置存储的网关产品支持；所有无内置存储的网关产品均不支持。

8.63 show web-search-audit detail

查询 WEB-SEARCH 审计的明细信息。

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*]

【参数说明】

参数	描述
hours	近期时间段
yyyy mm dd	年月日
hh:mm:ss	小时分钟秒
hour1	时间段过滤条件：开始小时段
hour2	时间段过滤条件：结束小时段
hour3	时间段过滤条件：开始小时段
hour4	时间段过滤条件：结束小时段
intf-name	接口名称
bridge-num	桥编号
subs-name1	过滤条件：静态用户名，精确匹配
subs-name2	过滤条件：认证用户名，精确匹配
addr	过滤条件：IP，精确匹配；多个 IP 用 “,” 隔开
keyword	过滤条件：过滤关键字，支持多关键字过滤，不同关键字间以半角逗号隔开
rule-name	过滤条件： 匹配的规则名称，支持多规则名过滤，不同规则名间以半角逗号隔开
integer1	查询结果集合中的起始位置
integer2	查询结果集合中的结束位置

【命令模式】 特权模式

【缺省级别】 14

【使用指导】 使用该命令可以查询或导出 WEB-SEARCH 审计的明细信息。

【配置举例】 1：查询 2013-5-1 的 0 点到 2013-5-7 的 24 点，用户 userA 的 WEB-SEARCH 审计明细信息。

```
Ruijie# show web-search-audit detail time-range from 2013 5 1 0:0:0 to 2013 5 7 23:59:59 subscriber
userA order-by time desc start-item 1 end-item 20
==================================================================
Time: 2013-05-03 16:45:29
```

```
subscriber: /userA
auth-subscriber: any
Ip: 192.168.211.96
Rule: ruleA
Action: permit
URL: http://www.baidu.com/s?ie=utf-8&bs=hello&rsv_bp=1&rsv_spt=3&wd=hello
search-word: hello
……
```

【提示信息】 -

【平台说明】 有内置存储的网关产品支持；所有无内置存储的网关产品均不支持。

8.64 show web-search-audit stat

查询 WEB-SEARCH 审计的统计信息。

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**]

【参数说明】

参数	描述
hours	近期时间段
yyyy mm dd	年月日
hh:mm:ss	小时分钟秒
hour1	时间段过滤条件：开始小时段
hour2	时间段过滤条件：结束小时段
hour3	时间段过滤条件：开始小时段
hour4	时间段过滤条件：结束小时段
intf-name	接口名称
bridge-num	桥编号
subs-name1	过滤条件：静态用户名，精确匹配
subs-name2	过滤条件：认证用户名，精确匹配
addr	过滤条件：IP，精确匹配；多个 IP 用“,”隔开
keyword	过滤条件：过滤关键字，支持多关键字过滤，不同关键字间以半角逗号隔开
rule-name	过滤条件： 匹配的规则名称，支持多规则名过滤，不同规则名间以半角逗号隔开

【命令模式】 特权模式

【缺省级别】 14

【使用指导】 使用该命令可以查询 WEB-SEARCH 审计的统计信息。

【配置举例】 1：查询 2013-5-1 的 0 点到 2013-5-7 的 24 点，用户 userA 的 WEB-SEARCH 审计统计信息。

```
Ruijie# show web-search-audit stat time-range from 2013 5 1 0:0:0 to 2013 5 7 23:59:59 subscriber userA
50
```

【提示信息】 -

【平台说明】 有内置存储的网关产品支持；所有无内置存储的网关产品均不支持。

8.65 url

向 URL 分类中添加 URL 条目。
url *url-string*

删除 URL 条目。
no url *url-string*

【参数说明】

参数	描述
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。

【缺省配置】 缺省无配置。

【命令模式】 URL 分类配置模式

【缺省级别】 14

【使用指导】 1：URL 模式匹配目前仅支持 2 级目录，不允许用户配置“ietf.org/2006/12/1”；
2：URL 子域名模式匹配目前仅支持 4 级子域名，若用户配置为“test.rfc.download.ietf.org”，则仅能匹配精确域名。

【配置举例】 1：为 URL 分类 classA 添加一个条目：ietf.org。

```
Ruijie# configure terminal
Ruijie(config)# url-class classA
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。

【提示信息】 1：如果配置的 URL 格式不正确，则给出提示。

```
Ruijie(config)# url ietf.org/2006/12/1
Format error
```

【常见错误】 -

【平台说明】 -

8.66 url-audit

开启相应的 URL 优化审计功能。

url-audit { **exact-filter** | **except-postfix** | **except-regexp** [*regexp*] | **only-get** | **optimize-cache** [*time*] }

关闭相应的 URL 优化审计功能。

no url-audit { **exact-filter** | **except-postfix** | **except-regexp** [*regexp*] | **only-get** | **optimize-cache** [*time*] }

【参数说明】

参数	描述
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。

【缺省配置】 默认开启，并且命令不显示出来。只有在执行了 no 命令后，命令才显示出来。

【命令模式】 全局模式

【缺省级别】 14

【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。

【配置举例】 1：开启只审计 HTTP 的 GET。

```
Ruijie# configure terminal
Ruijie(config)# url-audit only-get
Ruijie(config)#end
```

2：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
```

3：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
```

4：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
```

【检验方法】 使用 show running-config 命令可以查看配置状态。

【提示信息】 -

【常见错误】 -

【平台说明】 -

8.67 url-class

指定 URL 分类名，并进入 URL 分类配置模式。
url-class *class-name*

删除 URL 分类。
no url-class *class-name*

【参数说明】

参数	描述
class-name	URL 分类名称

【缺省配置】 缺省无配置。

【命令模式】 全局模式

【缺省级别】 14

【使用指导】 通过此命令可以配置 URL 分类。

【配置举例】 1：新增一个 URL 分类 classA。

```
Ruijie# configure terminal
Ruijie(config)# url-class classA
Ruijie(url-obj-config)#end
```

【检验方法】 使用 show running-config 命令可以查看配置状态。

【提示信息】 -

【常见错误】 -

【平台说明】 -

8.68 url-filter-notice

配置 URL 过滤提示页面显示的内容。
url-filter-notice display [*text*]

关闭 URL 过滤提示页面显示功能。
no url-filter-notice

【参数说明】

参数	描述
text	URL 过滤提示页面上显示的信息。不输入显示默认信息。

【缺省配置】 默认开启。默认显示内容为：
"You are forbidden to visit the website, please contact webmaster!"

【命令模式】 全局模式

【缺省级别】 14

【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。

【配置举例】 1：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。

【提示信息】 -

【常见错误】 -

【平台说明】 -

8.69 url-object

指定 URL 对象名，并进入 URL 对象配置模式。
url-object *object-name*

删除 URL 对象。
no url-object *object -name*

【参数说明】

参数	描述
object-name	URL 对象名称。允许最大长度为 40 字节。

【缺省配置】 缺省无配置。

【命令模式】 全局模式

【缺省级别】 14

【使用指导】 通过此命令可以配置 URL 对象。URL 对象容量为 100。

【配置举例】 1：新增一个 URL 对象 objA。

```
Ruijie# configure terminal
Ruijie(config)# url-object objA
Ruijie(url-obj-config)# end
```

【检验方法】 使用 show running-config 命令可以查看配置状态。

【提示信息】 -

【常见错误】 -

【平台说明】 -

8.70 url-redirect-rule

删除策略组下所有 URL 重定向规则。
url-redirect-rule delete-all

交换 URL 重定向访问控制规则的优先级。
url-redirect-rule priority-swap *rule-id1 rule-id2*

向内容审计策略组中添加 URL 重定向访问控制规则。
url-redirect-rule *rule-id* **time-range** *time-name* **from** *url-1* **to** *url-2* [**comment** *comment-string*]

删除 URL 重定向访问控制规则。
no url-redirect-rule *rule-id*

【参数说明】

参数	描述
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。
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。

【缺省配置】 缺省无配置。

【命令模式】 内容审计策略组配置模式

【缺省级别】 14

【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：交换优先级命令是用于对调两条 URL 重定向规则的优先级，运行该命令后，show running-config 中可以看到两个规则的排序发生了变化，但 show running-config 不会出现该命令。

【配置举例】 1：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
```

3：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
```

4：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
```

【检验方法】 使用 show running-config 命令可以查看配置状态。

【提示信息】 1：如果配置的 rule-id 已存在，则给出提示。

```
Ruijie(config)# url-redirect-rule 2 time-range any from www.sina.com.cn to www.ruijie.com.cn comment
sina-redirect
Rule 2 already exists, please delete it first
```

【常见错误】 -

【平台说明】 -

8.71 telent-rule

启用 TELNET 默认审计功能。
telnet-rule audit-default-enable

关闭 TELNET 默认审计功能。
no telnet-rule audit-default-enable

删除策略组下所有 TELNET 规则。
telnet-rule delete-all

交换 TELNET 访问控制规则的优先级。
telnet-rule priority-swap *rule-id1 rule-id2*

向内容审计策略组中添加 TELNET 访问控制规则。

telnet-rule *rule-id* **time-range** *time-name* **action** { **permit** | **deny** } [**audit**] [**alarm**] [**comment** *comment-string*]

删除 TELNET 访问控制规则。

no telnet-rule *rule-id*

【参数说明】

参数	描述
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。
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。

【缺省配置】 缺省无配置。

【命令模式】 内容审计策略组配置模式

【缺省级别】 14

【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：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-config 中可以看到两个规则的排序发生了变化，但 show running-config 不会出现该命令。

5：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】 1：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
```

2：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
```

3：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
```

4：为内容审计策略组 policyA 添加一个 TELNET 访问审计规则，过滤 TELNET 行为，并且需要审计该信息。

```
Ruijie# configure terminal
Ruijie(config)# content-policy policyA
Ruijie(cont-plcy-config)# telnet-rule 2 time-range any action deny audit comment TEST
Ruijie(cont-plcy-config)# end
```

【检验方法】 使用 show running-config 命令可以查看配置状态。

【提示信息】 1：如果配置的 rule-id 已存在，则给出提示。

```
Ruijie(config)# telnet-rule 2 time-range any action deny audit comment TEST
Rule 2 already exists, please delete it first
```

【常见错误】 -

【平台说明】 ACE 系列产品不支持，其他有内置存储的网关产品支持；NBR-E 系列、EG2000F 产品支持，其他无内置存储的网关产品均不支持。

8.72 ftp-rule

启用 FTP 默认审计功能。
ftp-rule audit-default-enable

关闭 FTP 默认审计功能。
no ftp-rule audit-default-enable

删除策略组下所有 FTP 规则。
ftp-rule delete-all

交换 FTP 访问控制规则的优先级。
ftp-rule priority-swap *rule-id1 rule-id2*

向内容审计策略组中添加 FTP 访问控制规则。
ftp-rule *rule-id* **time-range** *time-name* [**filename** *content-object-name*] **action** { **permit** | **deny** } [**audit**] [**alarm**] [**comment** *comment-string*]

删除 FTP 访问控制规则。
no ftp-rule *rule-id*

开关 FTP 上传文件内容审计。

[no] ftp-upload-file-audit enable

【参数说明】

参数	描述
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。
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	FTP 文件名匹配对象
comment-string	该规则的描述。

【缺省配置】 缺省无配置。

【命令模式】 内容审计策略组配置模式

【缺省级别】 14

【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：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-config 中可以看到两个规则的排序发生了变化，但 show running-config 不会出现该命令。

5：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】 1：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
```

2：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
```

3：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
```

4：为内容审计策略组 policyA 添加一个 FTP 审计规则，过滤含关键字组 keyword-group 内关键字的文件名上传，并且需要审计该信息。

```
Ruijie# configure terminal
Ruijie(config)# content-policy policyA
Ruijie(cont-plcy-config)# ftp-rule 2 time-range any filename keyword-group action deny audit comment TEST
Ruijie(cont-plcy-config)# end
```

5：开关 FTP 上传文件内容审计。

```
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。

【提示信息】 1：如果配置的 rule-id 已存在，则给出提示。

```
Ruijie(config)# ftp-rule 2 time-range any action deny audit comment TEST
Rule 2 already exists, please delete it first
```

【常见错误】 -

【平台说明】 ACE 系列产品不支持，其他有内置存储的网关产品支持；NBR-E 系列、EG2000F 产品支持，其他无内置存储的网关产品均不支持。

8.73 show telnet-audit detail

查询 TELNET 审计的明细信息。

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*] [**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*]

【参数说明】

参数	描述
hours	近期时间段
yyyy mm dd	年月日
hh:mm:ss	小时分钟秒
subs-name1	过滤条件：静态用户名，精确匹配

subs-name2	过滤条件：认证用户名，精确匹配
hour1	时间段过滤条件：开始小时段
hour2	时间段过滤条件：结束小时段
hour3	时间段过滤条件：开始小时段
hour4	时间段过滤条件：结束小时段
addr1	过滤条件：内网 IP，精确匹配；多个 IP 用“,”隔开
addr2	过滤条件：服务器 IP，精确匹配；多个 IP 用“,”隔开
rule-name	过滤条件： 匹配的规则名称，支持多规则名过滤，不同规则名间以半角逗号隔开
integer1	查询结果集合中的起始位置
integer2	查询结果集合中的结束位置

【命令模式】 特权模式

【缺省级别】 14

【使用指导】 使用该命令可以查询或导出 TELNET 的明细信息。

【配置举例】 1：查询 2016-9-4 的 0 点到 2016-11-4 的 24 点，用户 userA 的 TELNET 审计明细信息。

```
Ruijie# show telnet-audit detail time-range from 2016 11 4 0:0:0 to 2016 11 4 23:59:59 subscriber userA order-by time desc start-item 1 end-item 20
```

```
id: 1
time_stamp: 1480056761
day_time: 2016-11-25 14:52:41
sip: 3.3.3.54
dip: 60.28.228.9
sport: 60141
dport: 23
mac_addr: f48e.388f.f50d
usr_grp: /
usr_name: 3.3.3.54
plcy_name: _AUDIT_DEFAULT
rule_name: default_audit
app_type: telnet
state:connect
……
```

【提示信息】 -

【平台说明】 ACE 系列产品不支持，其他有内置存储的产品支持，所有无内置存储的产品均不支持。

8.74 show telnet-audit stat

查询 TELNET 审计的统计信息。

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*] [**ip** *addr1*] [**service-ip** *addr2*] [**conn** | **disconn**] [**rule-name** *rule-name*] [**permit** | **deny**]

【参数说明】

参数	描述
hours	近期时间段
yyyy mm dd	年月日
hh:mm:ss	小时分钟秒
hour1	时间段过滤条件：开始小时段
hour2	时间段过滤条件：结束小时段
hour3	时间段过滤条件：开始小时段
hour4	时间段过滤条件：结束小时段
subs-name1	过滤条件：静态用户名，精确匹配
subs-name2	过滤条件：认证用户名，精确匹配
addr1	过滤条件：IP，精确匹配；多个 IP 用 “,” 隔开
addr2	过滤条件：服务器 IP，精确匹配；多个 IP 用 “,” 隔开
rule-name	过滤条件： 匹配的规则名称，支持多规则名过滤，不同规则名间以半角逗号隔开

【命令模式】 特权模式

【缺省级别】 14

【使用指导】 使用该命令可以查询 TELNET 审计的统计信息。

【配置举例】 1：查询 2013-5-1 的 0 点到 2013-5-7 的 24 点，用户 userA 的 TELNET 审计统计信息。

```
Ruijie# show telnet-audit stat time-range from 2013 5 1 0:0:0 to 2013 5 7 23:59:59 subscriber userA
50
```

【提示信息】 -

【平台说明】 ACE 系列产品不支持，其他有内置存储的产品支持，所有无内置存储的产品均不支持。

8.75 show ftp-audit detail

查询 ftp 审计的明细信息。

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*] [**ip** *addr1*] [**file-name** *keyword*] [**rule-name** *rule-name*] [**permit | deny**] **order-by** { **time** | **subscriber** | **auth-subscriber | internal-ip** } { **asc** | **desc** } [**start-item** *integer1* **end-item** *integer2*]

【参数说明】

参数	描述
hours	近期时间段
yyyy mm dd	年月日
hh:mm:ss	小时分钟秒
subs-name1	过滤条件：静态用户名，精确匹配
subs-name2	过滤条件：认证用户名，精确匹配
hour1	时间段过滤条件：开始小时段
hour2	时间段过滤条件：结束小时段
hour3	时间段过滤条件：开始小时段
hour4	时间段过滤条件：结束小时段
keyword	过滤条件：匹配文件名关键字，支持多关键字过滤，不同关键字间以半角逗号隔开
rule-name	过滤条件： 匹配的规则名称，支持多规则名过滤，不同规则名间以半角逗号隔开
addr1	过滤条件：内网 IP，精确匹配；多个 IP 用 “,” 隔开
integer1	查询结果集合中的起始位置
integer2	查询结果集合中的结束位置

【命令模式】 特权模式

【缺省级别】 14

【使用指导】 使用该命令可以查询或导出 FTP 审计的明细信息。

【配置举例】 1：查询 2016-9-4 的 0 点到 2016-11-4 的 24 点，用户 userA 的 FTP 审计明细信息。

```
Ruijie# show ftp-audit detail time-range from 2016 11 4 0:0:0 to 2016 11 4 23:59:59 subscriber userA order-by time desc start-item 1 end-item 20
```

```
id: 1
time_stamp: 1480056761
day_time: 2016-11-25 14:52:41
sip: 3.3.3.54
dip: 60.28.228.9
sport: 60141
dport: 21
mac_addr: f48e.388f.f50d
```

```
file name:aaa.txt
usr_grp: /
usr_name: 3.3.3.54
plcy_name: _AUDIT_DEFAULT
rule_name: default_audit
state:upload
action:permit
```

【提示信息】 -

【平台说明】 ACE 系列产品不支持，其他有内置存储的产品支持，所有无内置存储的产品均不支持。

8.76 show ftp-audit stat

查询 ftp 审计的统计信息。

show ftp-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*] [**ip** *addr1*] [**file-name** *keyword*] [**rule-name** *rule-name*] [**permit** | **deny**]

【参数说明】

参数	描述
hours	近期时间段
yyyy mm dd	年月日
hh:mm:ss	小时分钟秒
hour1	时间段过滤条件：开始小时段
hour2	时间段过滤条件：结束小时段
hour3	时间段过滤条件：开始小时段
hour4	时间段过滤条件：结束小时段
subs-name1	过滤条件：静态用户名，精确匹配
subs-name2	过滤条件：认证用户名，精确匹配
addr1	过滤条件：内网 IP，精确匹配；多个 IP 用“,”隔开
keyword	过滤条件：匹配文件名关键字，支持多关键字过滤，不同关键字间以半角逗号隔开
rule-name	过滤条件： 匹配的规则名称，支持多规则名过滤，不同规则名间以半角逗号隔开

【命令模式】 特权模式

【缺省级别】 14

【使用指导】 使用该命令可以查询 FTP 审计的统计信息。

【配置举例】 1：查询 2013-5-1 的 0 点到 2013-5-7 的 24 点，用户 userA 的 FTP 审计统计信息。

```
Ruijie# show ftp-audit stat time-range from 2013 5 1 0:0:0 to 2013 5 7 23:59:59 subscriber userA
50
```

【提示信息】 -

【平台说明】 ACE 系列产品不支持，其他有内置存储的产品支持，所有无内置存储的产品均不支持。

8.77 file-rule

删除策略组下所有 FILE 规则。
file-rule delete-all

交换 FILE 访问控制规则的优先级。
file-rule priority-swap *rule-id1 rule-id2*

向内容审计策略组中添加 FILE 访问控制规则。
file-rule *rule-id* **time-range** *time-name* **action** { **permit** | **deny** } [**audit**] [**alarm**] [**comment** *comment-string*]
file-rule *rule-id* **relation** { **and** | **or** } [**file-name** *content-obj-string1*] [**file-type** *content-obj-string2*]

删除 FILE 访问控制规则。
no file-rule *rule-id*

【参数说明】

参数	描述
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。
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

【缺省配置】 缺省无配置。

【命令模式】 内容审计策略组配置模式

【缺省级别】 14

【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：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-config 中可以看到两个规则的排序发生了变化，但 show running-config 不会出现该命令。

【配置举例】

1：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
```

3：交换策略组 policyA 内 FILE 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)# file-rule priority-swap 10 20
Ruijie(cont-plcy-config)# end
```

4：为内容审计策略组 policyA 添加一个 FILE 访问审计规则，过滤文件名行为，并且需要审计该信息。

```
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
```

【检验方法】 使用 show running-config 命令可以查看配置状态。

【提示信息】 1：如果配置的 rule-id 已存在，则给出提示。

```
Ruijie(config)# file-rule 2 time-range any action deny audit comment TEST
Rule 2 already exists, please delete it first
```

【常见错误】 -

【平台说明】 ACE 系列产品不支持，其他有内置存储的网关产品支持；其他无内置存储的网关产品均不支持。

8.78 content-attach-to-elog enable

启用附件上传 elog 的功能。
content-attach-to-elog enable

关闭附件上传 elog 功能。
no content-attach-to-elog enable

【参数说明】

参数	描述
-	-

【缺省配置】 缺省关闭。

【命令模式】 全局模式

【缺省级别】 14

【使用指导】 NPE 模式且有硬盘的情况下有效。

【配置举例】 1：NPE 模式且有硬盘的情况下，启用附件上传 elog 的功能。

```
Ruijie# configure terminal
Ruijie(config)# content-attach-to-elog enable
Ruijie(config)# end
```

【检验方法】 使用 show running-config 命令可以查看配置状态。

【提示信息】 -

【常见错误】 -

【平台说明】 EG2000XE/UE、EG3000XE/UE 支持，其他网关产品不支持。

8.79 show report-function

查询报表功能是否打开
show report-function

【参数说明】

参数	描述

【缺省配置】 无

【命令模式】 特权模式

【缺省级别】 14

【使用指导】 使用该命令查看报表功能是否打开

【配置举例】 1：查询报表功能是否开启

```
Ruijie#show report-function
```

【检验方法】 查看输出数据是否正确

【提示信息】 -

【常见错误】 -

【平台说明】 内容审计 2.0 设备支持

8.80 show report-custom-config

查询自定义报表规则配置情况

show report-custom-config { *rule-id* **}**

【参数说明】

参数	描述
rule-id	自定义报表规则号

【缺省配置】 无

【命令模式】 特权模式

【缺省级别】 14

【使用指导】 使用该命令查看自定义报表规则配置情况

【配置举例】 1：查询所有自定义报表规则信息

```
Ruijie#show report-custom-config
```

【检验方法】 查看输出数据是否正确

【提示信息】 -

【常见错误】 -

【平台说明】 内容审计 2.0 并且支持硬盘的设备支持

8.81 show report-custom-data

查询自定义报表规则生成的自定义报表数据

show report-custom-data *rule-id*

【参数说明】

参数	描述
rule-id	自定义报表规则号

【缺省配置】 无

【命令模式】 特权模式

【缺省级别】 14

【使用指导】 使用该命令查看自定义报表规则生成的自定义报表数据

【配置举例】 1：查询自定义报表规则 1 的报表统计记录

```
Ruijie#show report-custom-data 1
```

【检验方法】 查看输出数据是否正确

【提示信息】 -

【常见错误】 -

【平台说明】 内容审计 2.0 并且支持硬盘的设备支持

8.82 url-rule

启用 URL 默认审计功能。
url-rule audit-default-enable

关闭 URL 默认审计功能。
no url-rule audit-default-enable

删除策略组下所有 URL 规则。
url-rule delete-all

交换 URL 访问控制规则的优先级。
url-rule priority-swap *rule-id1 rule-id2*

向内容审计策略组中添加 URL 访问控制规则。
url-rule *rule-id* **url-object** *url-obj-name* **time-range** *time-name* **action** { **permit** | **deny** } [**audit**] [**alarm**] [**comment** *comment-string*]

删除 URL 访问控制规则。
no url-rule *rule-id*

开启 URL 宽松白名单功能。
url-rule apply-referer

关闭 URL 宽松白名单功能。
no url-rule apply-referer

【参数说明】

参数	描述
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。
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。

【缺省配置】 缺省无配置。

【命令模式】 内容审计策略组配置模式

【缺省级别】 14

【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：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-config 中可以看到两个规则的排序发生了变化，但 show running-config 不会出现该命令。

5：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。

6：url-rule 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。主要应用于 URL 白名单策略，可以对白名单列表中的网站及其子网站都放行。

【配置举例】 1：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
```

2：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
```

3：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
```

4：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
```

5：开启 URL 宽松白名单功能。

```
Ruijie# configure terminal
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。

【提示信息】 1：如果配置的 rule-id 已存在，则给出提示。

```
Ruijie(config)# url-rule 2 url-object url-objA time-range any action deny audit
Rule 2 already exists, please delete it first
```

【常见错误】 -

【平台说明】 -

8.83 vid-rule

启用虚拟身份默认审计功能。
vid-rule audit-default-enable

关闭虚拟身份默认审计功能。
no vid-rule audit-default-enable

【参数说明】

参数	描述
-	-

【缺省配置】 缺省无配置。

【命令模式】 内容审计策略组配置模式

【缺省级别】 14

【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。

【配置举例】 1：启用虚拟身份默认审计。

```
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。

【提示信息】 -

【常见错误】 -

【平台说明】 -

8.84 web-bbs-rule

启用 WEB-BBS 默认审计功能。
web-bbs-rule audit-default-enable

关闭 WEB-BBS 默认审计功能。
no web-bbs-rule audit-default-enable

删除策略组下所有 WEB-BBS 规则。
web-bbs-rule delete-all

交换 WEB-BBS 访问控制规则的优先级。
web-bbs-rule priority-swap *rule-id1 rule-id2*

向内容审计策略组中添加 WEB-BBS 访问控制规则。
web-bbs-rule *rule-id* **time-range** *time-name* [**content** *content-object-name*] **action** { **permit** | **deny** } [**audit**] [**alarm**] [**comment** *comment-string*]

删除 WEB-BBS 访问控制规则。
no web-bbs-rule *rule-id*

【参数说明】

参数	描述
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。
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。

【缺省配置】 缺省无配置。

【命令模式】 内容审计策略组配置模式

【缺省级别】 14

【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：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-config 中可以看到两个规则的排序发生了变化，但 show running-config 不会出现该命令。
5：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】 1：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
```

2：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
```

3：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
```

4：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
```

【检验方法】 使用 show running-config 命令可以查看配置状态。

【提示信息】 1：如果配置的 rule-id 已存在，则给出提示。

```
Ruijie(config)# web-bbs-rule 2 time-range any content keyword-group action deny audit comment DenyInvalidBBS
Rule 2 already exists, please delete it first
```

【常见错误】 -

【平台说明】 -

8.85 web-mail-rule

启用 WEB-MAIL 默认审计功能。
web-mail-rule audit-default-enable

关闭 WEB-MAIL 默认审计功能。
no web-mail-rule audit-default-enable

删除策略组下所有 WEB-MAIL 规则。
web-mail-rule delete-all

交换 WEB-MAIL 访问控制规则的优先级。
web-mail-rule priority-swap *rule-id1 rule-id2*

向内容审计策略组中添加 WEB-MAIL 访问控制规则的公共部分。
web-mail-rule *rule-id* **time-range** *time-name* [**direction** { **in** | **out** | **double** }] **action** { **permit** | **deny** } **audit** [**alarm**] [**comment** *comment-string*]

向内容审计策略组中添加 WEB-MAIL 访问控制规则的进一步的参数描述，主要是描述规则的关键字匹配条件。该命令为可选配置，如果不配置表示对满足 **web-mail-rule** *rule-id* **time-range** 命令的所有 mail 信息进行审计。
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*]

删除 WEB-MAIL 访问控制规则。
no web-mail-rule *rule-id*

【参数说明】

参数	描述
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。
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-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。

【缺省配置】 缺省无配置。

【命令模式】 内容审计策略组配置模式

【缺省级别】 14

【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：规则配置为阻断时，relation 中实际只有 or 关系才会有效。
5：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-config 中可以看到两个规则的排序发生了变化，但 show running-config 不会出现该命令。
6：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】 1：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
```

2：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
```

3：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
```

4：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
```

【检验方法】 使用 show running-config 命令可以查看配置状态。

【提示信息】 1：如果配置的 rule-id 已存在，则给出提示。

```
Ruijie(config)# web-mail-rule 1 time-range any action permit audit comment mail-audit-1
Rule 1 already exists, please delete it first
```

2：如果未配置规则的公共部分，直接配置规则的进一步说明，则给出提示。

```
Ruijie(config)# web-mail-rule 1 relation or from OBJ-F subject OBJ-S
Rule 1 is not exist
```

【常见错误】 -

【平台说明】 -

8.86 web-search-rule

启用 WEB-SEARCH 默认审计功能。
web-search-rule audit-default-enable

关闭 WEB-SEARCH 默认审计功能。
no web-search-rule audit-default-enable

删除策略组下所有 WEB-SEARCH 规则。
web-search-rule delete-all

交换 WEB-SEARCH 访问控制规则的优先级。
web-search-rule priority-swap *rule-id1 rule-id2*

向内容审计策略组中添加 WEB-SEARCH 访问控制规则。
web-search-rule *rule-id* **time-range** *time-name* [**content** *content-object-name*] **action** { **permit** | **deny** } [**audit**] [**alarm**] [**comment** *comment-string*]

删除 WEB-SEARCH 访问控制规则。
no web-search-rule *rule-id*

【参数说明】

参数	描述
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。
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。

【缺省配置】 缺省无配置。

【命令模式】 内容审计策略组配置模式

【缺省级别】 14

【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：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-config 中可以看到两个规则的排序发生了变化，但 show running-config 不会出现该命令。
5：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】 1：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
```

2：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
```

3：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
```

4：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
```

【检验方法】 使用 show running-config 命令可以查看配置状态。

【提示信息】 1：如果配置的 rule-id 已存在，则给出提示。

```
Ruijie(config)# web-search-rule 2 time-range any content keyword-group action deny audit comment
DenyInvalidSearch
Rule 2 already exists, please delete it first
```

【常见错误】 -

【平台说明】 -

9 LINE-QUALITY

9.1 debug line-quality { detect | route | track }

打开线路质量监控的调试开关。
debug line-quality detect
打开流量逃生的调试开关
debug line-quality route
打开线路检测的调试开关
debug line-quality track

关闭线路质量监控的调试开关。
no debug line-quality detect
关闭流量逃生的调试开关
no debug line-quality route
关闭线路检测的调试开关
no debug line-quality track

恢复缺省配置。
default debug line-quality detect
default debug line-quality ping
default debug line-quality track

【参数说明】

参数	描述
-	-

【缺省配置】 关闭调试开关。

【命令模式】 特权模式

【缺省级别】 14

【使用指导】 调试信息包括模块运行过程中各种事件的调试信息：

- TRACK 消息处理事件
- CLI 执行事件
- 流量逃生处理事件
- 其它运行异常的事件

查看处理失败时的调试信息，有助于故障诊断和定位。

【配置举例】 1：打开线路质量监控的调试开关。

```
Ruijie# debug line-quality track
```

2：关闭线路质量监控的调试开关。

```
Ruijie# no debug line-quality track
```

【调试信息】 1：TRACK 消息处理事件

调试信息	*Nov 1 17:43:36: %LQ-7-DEBUG: [lq_track_msg_proc:1079]recv track 300, state up.
信息解释	track 300 为 id 300 的 track 对象，state 是收到的信息状态，包括 up，down，undefined，obj_undef Track 的添加、删除、事件触发都会发送消息。
产生原因	TRACK 添加、删除、事件触发。
处理建议	-

2：CLI 执行事件

调试信息	*Nov 1 17:43:34: %LQ-7-DEBUG: [line_quality_exec:41]CLI:enable *Nov 1 17:43:34: %LQ-7-DEBUG: [line_quality_exec:41]CLI:config *Nov 1 17:43:34: %LQ-7-DEBUG: [lq_cil_exec_result:26]CLI-R:Enter configuration commands, one per line. End with CNTL/Z. *Nov 1 17:43:34: %LQ-7-DEBUG: [line_quality_exec:41]CLI:no track 300 *Nov 1 17:43:34: %LQ-7-DEBUG: [line_quality_exec:41]CLI:no ip rns 300 *Nov 1 17:43:34: %LQ-7-DEBUG: [line_quality_exec:41]CLI:ip rns 300 *Nov 1 17:43:35: %LQ-7-DEBUG: [line_quality_exec:41]CLI:icmp-echo www.baidu.com out-interface GigabitEthernet 0/5 next-hop 172.21.3.1 *Nov 1 17:43:35: %LQ-7-DEBUG: [line_quality_exec:41]CLI:deep *Nov 1 17:43:35: %LQ-7-DEBUG: [line_quality_exec:41]CLI:threshold 2000 *Nov 1 17:43:35: %LQ-7-DEBUG: [line_quality_exec:41]CLI:timeout 2000 *Nov 1 17:43:35: %LQ-7-DEBUG: [line_quality_exec:41]CLI:frequency 10000 *Nov 1 17:43:35: %LQ-7-DEBUG: [line_quality_exec:41]CLI:exit *Nov 1 17:43:35: %LQ-7-DEBUG: [line_quality_exec:41]CLI:track 300 rns 300 *Nov 1 17:43:35: %LQ-7-DEBUG: [line_quality_exec:41]CLI:delay up 60 *Nov 1 17:43:35: %LQ-7-DEBUG: [line_quality_exec:41]CLI:delay down 60 *Nov 1 17:43:35: %LQ-7-DEBUG: [line_quality_exec:41]CLI:exit
信息解释	CLI 执行，添加 TRACK 和 RNS 配置
产生原因	用户配置了线路检测，或者线路状态有新的变化。
处理建议	-

3：流量逃生处理事件

调试信息	*Nov 2 09:40:06: %LQ-7-DEBUG: [lq_route_state_notice:206]interface 5 route state notice : 1 1 1 1 2 1

信息解释	线路质量信息通告，后面一串数字表示各个告警项明细，1 表示无告警，2 表示有告警 该告警定时触发。
产生原因	线路质量定期检测。
处理建议	-

【提示信息】 无

【平台说明】 -

9.2 line-quality enable

启动线路质量监控。
line-quanlity enable

关闭线路质量监控。
no line-quanlity enable

恢复缺省配置。
default line-quanlity enable

【参数说明】

参数	描述
-	-

【缺省配置】 开启线路质量监控。

【命令模式】 全局配置模式

【缺省级别】 14

【使用指导】 默认开启，为线路质量监控和流量逃生提供数据。

如果关闭将使得线路质量监控没有数据，以及流量逃生不能工作。

【配置举例】 1：启动线路质量监控。

```
Ruijie(config)# line-quanlity enable
```

【检验方法】 -

【提示信息】 -

【常见错误】 -

【平台说明】 -

9.3 line-quality senior-detect on

启动线路质量监控高级查询开关。
line-quanlity senior-detect on

关闭线路质量探测。
no line-quanlity senior-detect on

【参数说明】

参数	描述
-	-

【缺省配置】 关闭线路质量监控高级查询开关。

【命令模式】 全局配置模式

【缺省级别】 14

【使用指导】 默认关闭，开启后通过 **show line-quality detect** 查询出的数据更详细。

【配置举例】 1：启动线路质量监控高级查询。

```
Ruijie(config)# line-quanlity senior-detect on
```

【检验方法】 show line-quality detect interface g 0/6 recent 1 命令显示的 json 格式中，more_info 取值为 on

【提示信息】 -

【常见错误】 -

【平台说明】 -

9.4 line-quality refresh

配置线路质量监控数据采集频率。
line-quanlity refresh *secs*

恢复线路质量监控数据采集默认频率。

no line-quanlity refresh

【参数说明】

参数	描述
secs	采集频率，单位秒，取值范围 30~600

【缺省配置】 300 秒

【命令模式】 全局配置模式

【缺省级别】 14

【使用指导】 一般采用默认配置即可，当需要更高精度的监控数据，可以适当调大频率。



调大频率，意味着需要消耗更多的资源去采集监控信息，以及更大的存储容量去存储数据。

【配置举例】 1：配置监控数据采集频率为 60 秒。

```
Ruijie(config)# line-quanlity refresh 60
```

【检验方法】 -

【提示信息】 -

【常见错误】 -

【平台说明】 -

9.5 line-quality data-store

配置线路质量监控数据保存时限。

line-quanlity data-store *hours*

关闭线路质量探测。

no line-quanlity data-store

【参数说明】

参数	描述
hours	保存时间长度，取值范围 1~168，单位：小时

【缺省配置】 72 小时。

【命令模式】 全局配置模式

【缺省级别】 14

【使用指导】 一般采用默认值即可。

调大存储时限，需要更大的存储空间，需要进行预先评估。

【配置举例】 1：设置线路质量监控数据保存时间。

```
Ruijie(config)# line-quanlity data-store 24
```

【检验方法】 -

【提示信息】 -

【常见错误】 -

【平台说明】 -

9.6 line-quality effect

启动线路质量监控告警阀值。

line-quanlity effect { ping-range | half-connect | delay-time | rnfp_drop | flow_gate } *min-val max-val*

取消线路质量监控告警阀值。

no line-quanlity effect { ping-range | half-connect | delay-time | rnfp_drop | flow_gate }

【参数说明】

参数	描述
min-val	普通告警参数，ping-range、half_connect 、flow_gate、rnfp_drop 的单位为百分比，delay_time 单位为毫秒。
max-val	红色告警参数，单位同上

【缺省配置】 min_val：ping 成功率为 50%，half_connect（半连接数）为 30%，rnfpd 丢包数暂无，flow_gate 低流量告警为 1%。

max_val：ping 成功率为 20%，half_connect（半连接数）为 50%，rnfpd 丢包数暂无，flow_gate 高流量告警为 50%。

【命令模式】 全局配置模式

【缺省级别】 14

【使用指导】 可以直接使用默认值。

流量阀值的修订，会影响到流量逃生的判断。

【配置举例】 1：配置 ping 成功率红色告警为 30%，普通告警为 60%。

```
Ruijie(config)# line-quanlity effect 60 30
```

【检验方法】 通过 show line-quality config 查看其配置

【提示信息】 -

【常见错误】 -

【平台说明】 -

9.7 line-quality track enable

启动线路检测开关。
line-quanlity track enable

关闭线路质量探测。
no line-quanlity track enable

【参数说明】

参数	描述
-	-

【缺省配置】 关闭线路检测。

【命令模式】 全局配置模式

【缺省级别】 14

【使用指导】 开启、关闭仅停止线路检测的运行，不会删除配置，配置依然有效。

开启过程中关闭，如果某个线路被线路检测关闭过，则在关闭线路检测功能时，会将该线路重新打开。

【配置举例】 1：启动线路检测。

```
Ruijie(config)# line-quanlity track enable
```

【检验方法】 -

【提示信息】 -

【常见错误】 -

【平台说明】 -

9.8 line-quality 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 log-only

关闭线路质量检测仅记录检测结果。
no line-quanlity track set log-only

【参数说明】

参数	描述
-	-

【缺省配置】 关闭线路检测仅记录日志。

【命令模式】 全局配置模式

【缺省级别】 14

【使用指导】 默认关闭。有时仅为了观察线路检测效果而不实际 DOWN 接口才打开，不建议长时间打开。

⚠ 接口没有 up/down，下发的 track 和 rns 配置还是按原逻辑来的。

【配置举例】 1：启动线路检测仅记录日志。

```
Ruijie(config)# line-quanlity set log-only
```

【检验方法】 -

【提示信息】 -

【常见错误】 -

【平台说明】 -

9.9 line-quality track set flow-gate

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 flow-gate *percent*

取消线路质量检测仅记录检测结果。

no line-quanlity track set flow-gate

【参数说明】

参数	描述
percent	接口带宽的百分比

【缺省配置】 50%。

【命令模式】 全局配置模式

【缺省级别】 14

【使用指导】 该命令配置接口流量达到阀值时，不去 DOWN 接口，避免因为接口流量过大导致丢包，引起误判。

【配置举例】 1：设置线路检测接口流量阀值为 60%。

```
Ruijie(config)# line-quanlity track set flow-gate 60
```

【检验方法】 -

【提示信息】 -

【常见错误】 -

【平台说明】 -

9.10 line-quality track set interface

设置监控线路探测的源地址。

line-quanlity track set interface *interface-name* **source** *ipaddr*

取消设置监控线路探测的源地址。

no line-quanlity track set interface *interface-name* **source**

【参数说明】

参数	描述
interface-name	接口名称
ipaddr	源地址

【缺省配置】 -

【命令模式】 全局配置模式

【缺省级别】 14

【使用指导】 在一些特殊场景，比如公网模式、多 WAN 口同网段模式等，需要配置该命令，以使得检测能够正常进行。

如果在特殊场景未配置该命令，将使得检测误判。

【配置举例】 1：设置线路质量监控接口的源 IP。

```
Ruijie(config)# line-quanlity track set interface g 0/5 source 172.21.3.55
```

【检验方法】 show line-quality track interface g 0/6 中显示配置的源 IP

【提示信息】 -

【常见错误】 -

【平台说明】 -

9.11 line-quality track set timeout

设置线路检测探测超时时间。

line-quanlity track set timeout *msecs*

取消设置线路检测探测超时时间。

no line-quanlity track set timeout

【参数说明】

参数	描述
msecs	探测超时事件，单位毫秒

【缺省配置】 2000 毫秒。

【命令模式】 全局配置模式

【缺省级别】 14

【使用指导】 一般采用默认值即可。在探测精度要求较高时，可将该参数调小。

【配置举例】 1：启动线路质量监控。

```
Ruijie(config)# line-quanlity track set timeout 1000
```

【检验方法】 show line-quality track 中可以看到 line quality track timeout 选项的取值

【提示信息】 -

【常见错误】 -

【平台说明】 -

9.12 line-quality track set { up | down }

设置线路检测频率和确认时间

line-quanlity track set { up | down } frequency *f-secs* **delay** *d-secs*

取消设置线路检测频率和确认时间

no line-quanlity track set { up | down }

【参数说明】

参数	描述
f-secs	线路探测频率，单位秒
d-secs	线路探测确认事件，单位秒

【缺省配置】 接口 UP 时，探测频率 10s，确认时间 12s
接口 DOWN 时，探测频率 3s，确认时间 60s

【命令模式】 全局配置模式

【缺省级别】 14

【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+2s+12s=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。

> 一般确认时间要大于等于探测频率+超时时间，否则将使得探测状态和策略频繁变化，可能影响网络稳定性。同时，接口 DOWN 状态要 UP 起来的确认时间应该比较长（默认 60s），否则，在网络不稳定的时候，可能误判网络状况良好，从而出现接口频繁的 UP/DOWN。

【配置举例】 1：设置线路质量 DOWN 时的时延为 300s。

```
Ruijie(config)# line-quanlity set down frequency 3 delay 300
```

【检验方法】 show line-quality track 显示结果中，以下两行为实际内容：
line quality track up :[freq:10 ; delay:12]
line quality track down :[freq:3 ; delay:60]

【提示信息】 -

【常见错误】 -

【平台说明】 -

9.13 line-quality track permit-interface

配置可以探测的接口。
line-quanlity track permit-interface *interface-name*

关闭线路质量探测。
no line-quanlity track permit-interface *interface-name*

【参数说明】

参数	描述
interface-name	接口名称

【缺省配置】 关闭

【命令模式】 全局配置模式

【缺省级别】 14

【使用指导】 一般将主线路设置为可配置的线路。该配置不是强制性的，仅作为 web 选择接口的依据。

如果未配置该命令，web 在配置时无法选择该接口。

【配置举例】 1：设置 g 0/5 口可检测。

```
Ruijie(config)# line-quanlity track permit-interface g 0/5
```

【检验方法】 show line-quality track 以下字段显示：
line quality permit interface:
[5] GigabitEthernet 0/6

【提示信息】 -

【常见错误】 提示配置的可探测接口超过最大限制值：
Max permit interface number is 15.

【平台说明】 -

9.14 line-quality track interface interface-name enable

开启某条线路的探测功能
line-quanlity track interface *interface-name* **enable**

关闭某条线路的探测功能。
no line-quanlity track interface *interface-name* **enable**

【参数说明】

参数	描述
interface-name	接口名称

【缺省配置】 关闭。

【命令模式】 全局配置模式

【缺省级别】 14

【使用指导】 配置接口探测信息时，要先开启该接口的探测功能。关闭该接口的探测功能时，则该接口下的配置都会清空。

如果该接口曾经在关闭功能前，协议状态是被程序 DOWN 的状态，则会先主动 UP 起来。

【配置举例】 1：启动线路质量监控。

```
Ruijie(config)# line-quanlity track interface g 0/5 enable
```

【检验方法】 show line-quality track interface g 0/5 中，
GigabitEthernet 0/5, index:4, stat:USED, ctrl:UP, source 0.0.0.0
stat 状态为 USED 或 STOP，则表示功能开启，如果功能关闭，则是没有显示内容或者 stat 为 DEL

【提示信息】 -

【常见错误】 -

【平台说明】 -

9.15 line-quality track interface interface-name { icmp | dns | tcp }

配置线路检测 ICMP 方式。
line-quanlity track interface *interface-name* **icmp { enable |** *ip* **|** *url* **}**
配置线路检测 DNS 方式。
line-quanlity track interface *interface-name* **dns { enable |** *ip* **}**
配置线路检测 TCP 方式。
line-quanlity track interface *interface-name* **tcp { enable |** *ip* **|** *url* **}**

取消配置线路检测 ICMP 方式。
no line-quanlity track interface *interface-name* **icmp [enable]**
取消配置线路检测 DNS 方式。
no line-quanlity track interface *interface-name* **dns [enable]**
取消配置线路检测 TCP 方式。
no line-quanlity track interface *interface-name* **tcp [enable]**

【参数说明】

参数	描述
interface-name	接口名称
enable	开启对应协议的功能，关闭时不清空协议配置
ip	协议对应的探测目标 IP
url	协议对应的探测目标 URL

【缺省配置】 关闭

【命令模式】 全局配置模式

【缺省级别】 14

【使用指导】 开启接口的探测功能，要分 2 步，分别是配置探测目标和开启协议的功能。（一般是先配置探测目标，再开启协议功能）
探测目标可以是 IP 或者 URL，两者都配的话，优先选择 IP 作为探测目标。
如果开启的多个探测协议，则遵循以下规则：
1） 如果开启 ICMP 探测，探测成功则不再进行 DNS 和 TCP 探测
2） 如果 ICMP 未开启或者探测失败，则再进行 DNS 和 TCP 探测
3） ICMP、DNS、TCP 任何一个协议探测成功，则认为接口正常
4） 所有配置的协议都探测失败，则认为接口异常。
5） ICMP 探测如果不配置探测目标，则默认探测下一跳，其他协议不配置探测目标，则不探测。


配置多个协议可以增加探测准确度，但同时也使得判断事件更长，消耗资源更多些。

【配置举例】 1：配置在 g 0/5 口使用 ICMP 探测百度是否可达

```
Ruijie(config)# line-quanlity track interface g 0/5 icmp www.baidu.com
Ruijie(config)# line-quality track interface g 0/5 icmp enable
```

【检验方法】 show line-quality track interface g 0/5 显示如下，红色部分为配置的内容：

GigabitEthernet 0/5, index:4, stat:USED, ctrl:UP, source 0.0.0.0
  ICMP: enable
    url: www.baidu.com
    ip : 0.0.0.0
    track_id : 300; rns_id: 300
    track_msg: UP; track_stat: UP
    last time: 2016-11-02 12:03:28
  DNS: disable
    ip : 0.0.0.0
    track_id : 0; rns_id: 0
    track_msg: NONE; track_stat: NONE
    last time:
  TCP: disable
    url:
    ip : 0.0.0.0
    track_id : 0; rns_id: 0
    track_msg: NONE; track_stat: NONE
    last time:

【提示信息】 -

【常见错误】 -

【平台说明】 -

9.16 line-quality track interface interface-name up

强制 UP 接口的协议状态。

line-quality track interface *interface-name* **up**

强制 DOWN 接口的协议状态。

no line-quality track interface *interface-name* **up**

【参数说明】

参数	描述
interface-name	接口名称

【缺省配置】 -

【命令模式】 全局配置模式

【缺省级别】 14

【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

> 该接口只是在协议层面对接口进行 UP/DOWN。

【配置举例】 1：设置 g 0/5 口协议层 UP。

```
Ruijie(config)# line-quanlity track interface g 0/5 up
```

【检验方法】 Ruijie#show line-quality track interface line

Interface	Status	Protocol	Last-ctrl
GigabitEthernet 0/5	UP	UP	--
GigabitEthernet 0/6	UP	UP	--

【提示信息】 -

【常见错误】 -

【平台说明】 -

9.17 line-quality route

配置一个新的流量逃生策略，并进入策略配置模式

line-quanlity route *id*

取消线路逃生策略

no line-quanlity route *id*

【参数说明】

参数	描述
id	线路逃生策略 ID

【缺省配置】 -

【命令模式】 全局配置模式

【缺省级别】 14

【使用指导】 执行后，进入策略配置模式。

【配置举例】 1：配置一个新的流量逃生策略，并进入配置模式。

```
Ruijie(config)# line-quanlity route 1
Ruijie(line-quality-route)#
```

【检验方法】 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

【提示信息】 -

【常见错误】 1）删除的策略 ID 不存在
line-quality route %d is not exist. !
2）配置的策略格式达到上限（5 个）。
line-quality route caption is full. !

【平台说明】 -

9.18 condition

配置流量逃生策略的条件。
condition interface *interface-name* **[ping] [dns] [half-connect] [delay] [{flow-low | flow-high}]**

取消流量逃生策略条件
no condition interface *interface-name*

【参数说明】

参数	描述
interface-name	接口名称
ping	线路监控 ping 告警
dns	线路监控 dns 告警
half-connect	线路监控半连接告警
delay	线路监控新建连接延迟告警
flow-low	线路流量过低告警
flow-high	线路流量过高告警

【缺省配置】 -

【命令模式】 流量逃生策略配置模式（line-quality-route）

【缺省级别】 14

【使用指导】 流量逃生，就是根据线路监控的告警信息来使能应用路由策略，根据需要配置。

【配置举例】 1：配置当接口流量过高时，生效应用路由 1。

```
Ruijie(config)# line-quanlity route 1
Ruijie(line-quality-route)#condition interface g 0/5 flow-high
Ruijie(line-quality-route)#route id 1 enable
Ruijie(line-quality-route)#active
Ruijie(line-quality-route)#exit
Ruijie(config)#
```

【检验方法】

```
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 38
```

【提示信息】 -

【常见错误】 -

【平台说明】 -

9.19 route id

配置要作用的应用路由策略 ID。

route id *id-val* **{ enable | disable }**

关闭线路质量探测。

no route id *id-val*

【参数说明】

参数	描述
id-val	应用路由策略 ID
enable	条件触发后，生效这条应用路由策略
disable	条件触发后，失效这条应用路由策略

【缺省配置】 -

【命令模式】 流量逃生策略配置模式（line-quality-route）

【缺省级别】 14

【使用指导】 应用路由策略可以配置多条，最多 5 条。

选择的策略应该和应用路由策略一起考虑，避免因为流量逃生引入其他问题

【配置举例】

```
Ruijie(config)# line-quanlity route 1
Ruijie(line-quality-route)#condition interface g 0/5 flow-high
Ruijie(line-quality-route)#route id 1 enable
Ruijie(line-quality-route)#active
Ruijie(line-quality-route)#exit
Ruijie(config)#
```

【检验方法】 -

【提示信息】 -

【常见错误】 选择的路由策略超过 5 条
add line-quality route %d fail.!

【平台说明】 -

9.20 active

激活流量逃生策略。
active

暂停流量逃生策略。
no active

【参数说明】

参数	描述

-	-

【缺省配置】 不开启

【命令模式】 流量逃生策略配置模式（line-quality-route）

【缺省级别】 14

【使用指导】 -

【配置举例】
```
Ruijie(config)# line-quanlity route 1
Ruijie(line-quality-route)#condition interface g 0/5 flow-high
Ruijie(line-quality-route)#route id 1 enable
Ruijie(line-quality-route)#active
Ruijie(line-quality-route)#exit
Ruijie(config)#
```

【检验方法】 -

【提示信息】 -

【常见错误】 -

【平台说明】 -

9.21 show line-quality config

查看线路质量监控告警阀值

show line-quality config

【参数说明】

参数	描述
-	-

【命令模式】 特权模式、全局模式、接口模式

【缺省级别】 14

【使用指导】 -

【配置举例】 1：查看线路质量监控告警阀值
```
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   %
```

【提示信息】 -

【平台说明】 -

9.22 show line-quality {detect | detail-detect}

显示线路质量监控明细。

show line-quality { detect | detail-detect } interface *interface-name* **{{ recent** *hour* **} | { time-interval** *yyyy mm dd hh*:*mm* **to** *yyyy mm dd hh:mm* **}}**

【参数说明】

参数	描述
detect	显示 json 格式
detail-detect	显示详细的数据库字段信息
interface-name	接口名称
hour	最近 N 小时，N 取值 1~168
time-interval *yyyy mm dd hh:mm* **to** *yyyy mm dd hh:mm*	具体时间段，yyyy mm dd hh:mm 表示年月日时分

【命令模式】 特权模式、全局模式、接口模式

【缺省级别】 14

【使用指导】 -

【配置举例】 1：查看接口告警信息

```
Ruijie#show line-quality detect interface gigabitEthernet 0/6 recent 1
{ "code": 0, "msg": "", "data": { "more_info": "on", "quality_data": [ { "time": "2016-11-02 15:10:00","level": 1, "event": "新建会话平均延迟 598ms" }, { "time": "2016-11-02 15:15:00", "level": 1, "event": "新建会话平均延迟 598ms" }, { "time": "2016-11-02 15:20:00", "level": 1, "event": "新建会话平均延迟 598ms" }, { "time": "2016-11-02 15:25:00", "level": 1, "event": "新建会话平均延迟 598ms" }, { "time": "2016-11-02 15:30:00", "level": 1, "event": "新建会话平均延迟 598ms" },
```

{ "time": "2016-11-02 15:35:00", "level": 1, "event": "新建会话平均延迟 598ms" }, { "time": "2016-11-02 15:40:00", "level": 1, "event": "新建会话平均延迟 598ms" }, { "time": "2016-11-02 15:45:00", "level": 1, "event": "新建会话平均延迟 598ms" }, { "time": "2016-11-02 15:50:00", "level": 1, "event": "新建会话平均延迟 598ms" }, { "time": "2016-11-02 15:55:00", "level": 1, "event": "新建会话平均延迟 598ms" }, { "time": "2016-11-02 16:00:00", "level": 1, "event": "新建会话平均延迟 598ms" }, { "time": "2016-11-02 16:05:00", "level": 1, "event": "新建会话平均延迟 598ms" }] } }

字段解释：

字段	说明
code	返回值，固定为 0
msg	错误消息，为空
data	告警数据列表
time	告警时间
level	告警级别，1 为普通，2 为严重
event	告警事件列表

2：查看接口告警信息（数据库数据）

```
Ruijie#show line-quality detail-detect interface gigabitEthernet 0/6 recent 1
time                stat msg  ping       conn       half       delay      rnfp       dns1
parse_ip1       dns2            parse_ip2
2016-11-02 15:35:00 1    128  100        5          0          598        0
192.168.58.110  119.75.217.109  114.114.114.114 14.215.177.37
2016-11-02 15:40:00 1    128  100        5          0          598        0
192.168.58.110  119.75.218.70   114.114.114.114 14.215.177.37
2016-11-02 15:45:00 1    128  100        5          0          598        0
192.168.58.110  119.75.218.70   114.114.114.114 14.215.177.37
2016-11-02 15:50:00 1    128  100        5          0          598        0
192.168.58.110  119.75.218.70   114.114.114.114 14.215.177.38
2016-11-02 15:55:00 1    128  100        5          0          598        0
192.168.58.110  119.75.217.109  114.114.114.114 14.215.177.37
2016-11-02 16:00:00 1    128  100        5          0          598        0
192.168.58.110  119.75.218.70   114.114.114.114 14.215.177.38
```

【提示信息】 -

【平台说明】 -

9.23 show line-quality track

查看线路检测配置信息

show line-quality track

【参数说明】

参数	描述
-	-

【命令模式】 特权模式、全局模式、接口模式

【缺省级别】 14

【使用指导】 使用该命令可以查看设备的接口检测配置参数。

【配置举例】 1：查看所线路质量监控接口检测信息

```
Ruijie#show line-quality track
line quality track           :enable
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:3  ; delay:60 ]
line quality permit interface:
  [5] GigabitEthernet 0/6
```

字段解释：

字段	说明
line quality track	接口检查开关
line quality track log-only	是否只记录日志
line quality track flow-gate	流量阀值，接口流量达到带宽的该百分比，不对接口做 down 操作
line quality track timeout	接口探测的超时时间
line quality track intf count	已配置的接口数
line quality track up/down	接口 UP/DOWN 状态下的探测频率和确认时间
line quality permit interface	允许探测的接口列表

【提示信息】 -

【平台说明】 -

9.24 show line-quality track interface

查看接口配置的检测信息和状态。

show line-quality track interface [*interface-name*]

【参数说明】

参数	描述
interface-name	指定查看的接口，未指定则查询所有接口

【命令模式】 特权模式、全局模式、接口模式

【缺省级别】 14

【使用指导】 使用该命令可以查看接口上配置的线路检测配置和状态

【配置举例】 1：查看接口上配置的线路检测配置和状态

```
Ruijie#show line-quality track interface g 0/5
GigabitEthernet 0/5, index:4, stat:USED, ctrl:UP, source 0.0.0.0
  ICMP: enable
    url: www.baidu.com
    ip : 0.0.0.0
    track_id : 300; rns_id: 300
    track_msg: UP; track_stat: UP
    last time: 2016-11-02 16:34:19
  DNS: disable
    ip : 0.0.0.0
    track_id : 0; rns_id: 0
    track_msg: NONE; track_stat: NONE
    last time:
  TCP: disable
    url:
    ip : 0.0.0.0
    track_id : 0; rns_id: 0
    track_msg: NONE; track_stat: NONE
    last time:
```

字段解释：

字段	说明
index	接口索引
stat	接口配置状态，USED 在用，STOP 暂停，DEL 删除中
ctrl	接口控制状态，UP 打开，DOWN 关闭，NONE 未控制
source	接口源 IP
ICMP/DNS/TCP	具体的探测协议开关，enable 为打开，disable 为关闭
url/ip	探测的目标地址
track_id,rns_id	探测对应 track 和 rns 配置 ID

track_msg	探测的最后消息类型
track_stat	当前探测的状态
last time	最后探测消息达到时间

【提示信息】 -

【平台说明】 -

9.25 show line-quality track interface line

查看线路状态

show line-quality track interface line

【参数说明】

参数	描述
-	-

【命令模式】 特权模式、全局模式、接口模式

【缺省级别】 14

【使用指导】 使用该命令可以查看所有允许配置探测的接口的物理状态、协议状态以及程序最后的控制状态

【配置举例】 1：查看接口的状态信息，包括物理状态和链路层协议状态

```
Ruijie#show line-quality track interface l
Interface                      Status Protocol Last-ctrl
GigabitEthernet 0/5            UP     UP       UP
GigabitEthernet 0/6            UP     UP       --
```

字段解释：

字段	说明
Interface	接口名称
Status	接口物理状态
Protocol	接口协议状态
Last-ctrl	进程最后的控制状态

【提示信息】 -

【平台说明】 -

9.26 show line-quality route

查看流量逃生策略信息。

show line-quality route [*id*]

【参数说明】

参数	描述
id	流量逃生策略 ID，未指定表示查看所有策略

【命令模式】 特权模式、全局模式、接口模式

【缺省级别】 14

【使用指导】 使用该命令可以查看接口上的流量逃生策略信息。

【配置举例】 1：查看流量逃生策略信息

```
Ruijie#show line-quality route
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 4
```

字段解释：

字段	说明
line-quality route 1	流量逃生策略 ID
active: yes	策略激活
condition	策略条件，包括接口和详细条件：ping,dns,half,delay,flow-l,flow-h，分别表示 ping 告警，dns 告警，半连接数告警，新建流延迟告警，流量低告警，流量高告警
route list	控制的应用路由策略列表
state: down	当前策略状态是否触发，下面显示每个条件的连续触发次数

【提示信息】 -

【平台说明】 -

9.27 show line-quality log

查看模块日志

show line-quality log [**type** *type-num*] [**limit** *count*]

【参数说明】

参数	描述
type *type-num*	日志类型
limit *count*	限制条数

【命令模式】 特权模式、全局模式、接口模式

【缺省级别】 14

【使用指导】 使用该命令可以查看本模块的日志信息。

【配置举例】 1：查看本模块日志信息

```
Ruijie#show line-quality log limit 5
time                type log
------------------------------
2016-11-02 16:34:42 2    interface 4 track modify.
2016-11-02 16:34:42 22   interface 4 delay up, prot=ICMP.
2016-11-02 16:34:19 2    interface 4 track modify.
2016-11-02 16:34:19 22   recv track 300 event, state=up.
2016-11-02 16:34:16 4    interface 4 add track 300, prot=ICMP, state=UP.
```

字段解释：

字段	说明
time	日志时间
type	日志类型
log	日志消息

【提示信息】 -

【平台说明】 -

命令参考-应用协议

本分册介绍应用协议相关内容，包括以下章节：

1. DHCP
2. DNS
3. DDNS
4. NTP
5. SNTP
6. DNS Proxy
7. DNS-CACHE
8. FTP-Server
9. FTP Client
10. TIME RANGE
11. 网络连通性测试工具

1 DHCP

1.1 address range

要在 DHCP 地址池关联的 CLASS 下指定 CLASS 所能分配的地址网段范围 ,用地址池 class 配置模式下的 **address range** 命令

address range *low-ip-address high-ip-address*

该命令的 **no** 形式可以删除该网段范围。

no address range

【参数说明】

参数	描述
low-ip-address	网段范围中的起始地址。
high-ip-address	网段范围中的终止地址。

【缺省配置】 缺省关联的 CLASS 未配置网段范围，默认为地址池的网段范围。

【命令模式】 地址池 CLASS 配置模式

【使用指导】 该命令属于 Server 配置；每个 CLASS 对应一个网段范围，网段范围必须从低地址到高地址，可以允许多个 CLASS 之间的网段范围重复。如果指明了地址池关联的 CLASS，但对应的网段范围没有配置，则该 CLASS 默认的网段范围和 CLASS 所处的地址池的网段范围相同。

【配置举例】 1：配置地址池 mypool0 关联 class1 的网段范围 172.16.1.1—172.16.1.8。

```
Ruijie(config)# ip dhcp pool mypool0
Ruijie(dhcp-config)# class class1
Ruijie(config-dhcp-pool-class)# address range 172.16.1.1  172.16.1.8
```

【检验方法】 通过 **show run** 可见配置成功

【提示信息】 -

【常见错误】 -

【平台说明】 -

1.2 bootfile

要定义 DHCP 客户端缺省启动映像文件名，用 DHCP 地址池配置命令 **bootfile**
bootfile *file-name*

no 形式可以取消定义
no bootfile

恢复默认值
default bootfile

【参数说明】

参数	描述
file-name	定义用于启动的文件名

【缺省配置】 缺省没有定义启动文件名

【命令模式】 DHCP 地址池配置模式

【缺省级别】 14

【使用指导】 该命令属于 Server 配置；有些 DHCP 客户端在启动过程中需要下载操作系统、配置文件等，DHCP 服务器必须提供启动时需要的映像文件名，DHCP 客户端才可以通过相应的服务器（如 TFTP）下载文件。其它服务器通过 **next-server** 命令进行定义

【配置举例】 1：设备启用了 DHCP 服务器和中继特性。

```
Ruijie(dhcp-config)# bootfile router.conf
```

【检验方法】 通过 **show run** 可见配置成功

【提示信息】 -

【常见错误】 -

【平台说明】 -

1.3 class

要在 DHCP 地址池中配置关联的 CLASS，用 DHCP 地址池配置模式下的 class 命令
class *class-name*

no 形式可以取消定义
no class *class-name*

【参数说明】

参数	描述
class-name	输入 CLASS 的名称，可以是字符串或数字，如 myclass 或者 1。

【缺省配置】 缺省地址池未关联任何 CLASS。

【命令模式】 DHCP 地址池配置模式。

【缺省级别】 14

【使用指导】 该命令属于 Server 配置；每个 DHCP 地址池可以根据 Option82 匹配信息进行地址分配，我们把 Option82 信息进行匹配归类，在 DHCP 地址池中为这些归类分别指定可以分配的网段范围。这个归类称为 CLASS，一个 DHCP 地址池可以关联多个 CLASS，每个 CLASS 可以指定不同的网段范围。

在地址分配过程中先根据客户端所处的网段确定可以分配的地址池，再根据其 Option82 信息进一步确定其所属的 CLASS，从 CLASS 对应的网段范围中分配 IP 地址。当一个请求报文匹配地址池中的多个 CLASS 时，按照 CLASS 在地址池中配置的先后顺序从对应的 CLASS 网段范围中分配地址 ,如果该 CLASS 分配地址已达到上限，则继续从下一个匹配的 CLASS 进行分配，依此类推。每个 CLASS 对应一个网段范围，网段范围必须从低地址到高地址，可以允许多个 CLASS 之间的网段范围重复。如果指明了地址池关联的 CLASS，并且未配置 CLASS 网段，则该 CLASS 默认的网段范围和 CLASS 所处的地址池的网段范围相同。

【配置举例】 1：配置地址池 mypool0 关联 class1。

```
Ruijie(config)# ip dhcp pool mypool0
Ruijie(dhcp-config)# class class1
```

【检验方法】 通过 **show run** 可见配置成功

【提示信息】 -

【常见错误】 -

【平台说明】 -

1.4 clear ip dhcp auth-agent

要清除 DHCP 待授权表项，在特权用户模式用 **clear ip dhcp auth-agent** 命令
clear ip dhcp auth-agent { * | *mac-addr* }

【参数说明】

参数	描述

*	删除所有的 DCHP 待授权表项
mac-addr	删除指定 mac 地址待授权记录

【命令模式】 特权用户模式

【缺省级别】 14

【使用指导】 该命令属于 Server 配置；该命令只能清除由于地址池开启的固态属性，终端接入但由于未固态绑定授权而产生的待授权表项

【配置举例】 1：清除了 mac 地址为 00d0.5564.8899 的 DHCP 待授权表项

```
Ruijie# clear ip dhcp auth-agent 00d0.5564.8899
```

【提示信息】 -

【平台说明】 -

1.5 clear ip dhcp binding

要清除 DHCP 绑定表，在特权用户模式用 **clear ip dhcp binding** 命令

clear ip dhcp binding { * | *ip-address* }

【参数说明】

参数	描述
*	删除所有的 DCHP 绑定
ip-address	删除指定 IP 地址记录

【命令模式】 特权用户模式

【缺省级别】 14

【使用指导】 该命令属于 Server 配置；该命令只能清除 DHCP 自动绑定，DHCP 手工绑定的删除可以通过 **no ip dhcp pool** 命令

【配置举例】 1：清除了 IP 地址为 192.168.12.100 的 DHCP 绑定

```
Ruijie# clear ip dhcp binding 192.168.12.100
```

【提示信息】 -

【平台说明】 -

1.6 clear ip dhcp conflict

要清除 DHCP 冲突记录，在特权用户模式用 **clear ip dhcp conflict** 命令

clear ip dhcp conflict { * | *ip-address* }

【参数说明】

参数	描述
*	删除所有的 DCHP 地址冲突记录
ip-address	删除指定 IP 地址冲突记录

【命令模式】 特权用户模式

【缺省级别】 14

【使用指导】 该命令属于 Server 配置；DHCP 服务器检测地址冲突用 ping 会话，DHCP 客户端检测地址冲突用地址解析协议（ARP）。**clear ip dhcp conflict** 可以删除历史冲突记录

【配置举例】 1：清除了所有地址冲突记录

```
Ruijie# clear ip dhcp conflict *
```

【提示信息】 -

【平台说明】 -

1.7 clear ip dhcp dynamic-binding

清除 DHCP 动态在线的表项，在特权用户模式用 **clear ip dhcp dynamic-binding** 命令

clear ip dhcp dynamic-binding { * | *mac-addr* }

【参数说明】

参数	描述
*	删除所有的 DCHP 动态在线表项
mac-addr	删除指定 mac 地址终端的动态在线表项

【命令模式】 特权用户模式

【缺省级别】 14

【使用指导】 该命令属于 Server 配置；该命令只能清除动态分配在线的终端表项，固态在线的表项无法清除。

【配置举例】 1：清除了 mac 地址为 00d0.5564.8899 的终端动态在线表项

```
Ruijie# clear ip dhcp dynamic-binding 00d0.5564.8899
```

【提示信息】 -

【平台说明】 -

1.8 clear ip dhcp history

要清除 DHCP 历史记录，在特权用户模式用 **clear ip dhcp history** 命令

clear ip dhcp history{ * | *mac-address* }

【参数说明】

参数	描述
*	删除所有的 DCHP 地址历史记录
mac-address	删除指定 mac 地址历史记录

【命令模式】 特权用户模式

【缺省级别】 14

【使用指导】 该命令属于 Server 清除；Server 保留了所有曾经分配过的地址信息，**clear ip dhcp history** 可以删除历史记录

【配置举例】 1：清除了所有地址历史记录

```
Ruijie# clear ip dhcp history *
```

【提示信息】 -

【平台说明】 -

1.9 clear ip dhcp record-history

清除 DHCP 历史在线数量统计信息，在特权用户模式用 **clear ip dhcp record-history** 命令

clear ip dhcp record-history

【参数说明】

参数	描述
-	-

【命令模式】 特权用户模式

【缺省级别】 14

【使用指导】 该命令属于 Server 配置；该命令用于清楚在线 IP 地址数量的历史统计信息。

【配置举例】 1：清除 DHCP 在线历史信息

```
Ruijie# clear ip dhcp record-history
```

【提示信息】 -

【平台说明】 -

1.10 clear ip dhcp relay statistics

复位 DHCP 中继的计数器。

clear ip dhcp relay statistics

【参数说明】

参数	描述
-	-

【命令模式】 特权用户模式

【缺省级别】 14

【使用指导】 该命令属于 Relay 配置 ;DHCP 中继报文统计 ,对 DHCP 中继接收和发送的各类报文进行了统计。**clear ip dhcp relay statistics** 命令可以删除历史计数记录，从新开始统计。

【配置举例】 1：清除 DHCP 中继的统计记录

```
Ruijie# clear ip dhcp relay statistics
```

【提示信息】 -

【平台说明】 -

1.11 clear ip dhcp server detect

要清除 DHCP 伪服务器记录

clear ip dhcp server detect { * | *ip-address* }

【参数说明】

参数	描述
*	删除所有的 DHCP 伪服务器记录
ip-address	删除指定的 DHCP 伪服务器记录

【命令模式】 特权用户模式

【缺省级别】 14

【使用指导】 该命令属于 Server 配置；Server 会保留探测的到伪服务器地址，clear ip dhcp server detect 可以清除伪服务器记录

【配置举例】 1：清除所有的 DHCP 伪服务器记录

```
Ruijie# clear ip dhcp server detect *
```

【提示信息】 -

【平台说明】 -

1.12 clear ip dhcp server rate

要复位 DHCP 服务器的报文在各相关模块处理数率统计

clear ip dhcp server rate

【参数说明】

参数	描述
-	-

【命令模式】 特权用户模式

【缺省级别】 14

【使用指导】 该命令属于 Server 配置 ;用于清除 dhcp 服务器统计每条报文在不同模块的处理数率 ,如 arp、热备、lsm、socket 等

【配置举例】 1：要复位 DHCP 服务器的报文在各相关模块处理数率统计

```
Ruijie# clear ip dhcp server rate
```

【提示信息】 -

【平台说明】 -

1.13 clear ip dhcp server statistics

要复位 DHCP 服务器的计数器

clear ip dhcp server statistics

【参数说明】

参数	描述
-	-

【命令模式】 特权用户模式

【缺省级别】 14

【使用指导】 该命令属于 Server 配置；DHCP 服务器报文统计，记录 DHCP 地址池、自动绑定、手工绑定和过期绑定的数目，并对 DHCP 服务器接收和发送的各类报文进行了统计。**clear ip dhcp server statistics** 命令可以删除历史计数记录，从新开始统计。

【配置举例】 1：清除 DHCP 服务器的统计记录

```
Ruijie# clear ip dhcp server statistics
```

【提示信息】 -

【平台说明】 -

1.14 clear ip dhcp solid-binding

清除 DHCP 固态绑定态在线的表项，在特权用户模式用 **clear ip dhcp solid-binding** 命令
clear ip dhcp solid-binding all

【参数说明】

参数	描述
-	-

【命令模式】 特权用户模式

【缺省级别】 14

【使用指导】 该命令属于 Server 配置；该命令只能清除固态绑定后分配在线的终端表项且删除固态绑定信息，未固态绑定分配在线的表项无法清除。

【配置举例】 1：清除所有固态绑定信息

```
Ruijie# clear ip dhcp solid-binding all
```

【提示信息】 -

【平台说明】 -

1.15 clear ip dhcp warn-log

清除 DHCP 业务告警信息，在特权用户模式用 **clear ip dhcp warn-log** 命令

clear ip dhcp warn-log { history | current }

【参数说明】

参数	描述
history	历史告警信息
Current	当前告警信息

【命令模式】 特权用户模式

【缺省级别】 14

【使用指导】 该命令属于 Server 配置；该命令用于清除终端迁移、地址耗尽、待授权终端、地址冲突的告警信息。

【配置举例】 1：清除历史告警信息

```
Ruijie# clear ip dhcp warn-log history
```

【提示信息】 -

【平台说明】 -

1.16 client-identifier

要定义 DHCP 客户端的唯一标识（以点隔开的十六进制数表示），用 DHCP 地址池配置命令 **client-identifier**

client-identifier *unique-identifier*

no 形式可以删除客户端标识

no client-identifier

恢复默认值

default client-identifier

【参数说明】

参数	描述
unique-identifier	DHCP 客户端的标识，以点隔开的十六进制表示。如：0100.d0f8.2233.b467.6967.6162.6974.4574.6865.726e.6574.302f.31

【缺省配置】 没有缺省值

【命令模式】 DHCP 地址池配置模式

【缺省级别】 14

【使用指导】 该命令属于 Server 配置；有些 DHCP 客户端请求 DHCP 服务器分配 IP 地址时，用客户端标识而非硬件地址用来代表客户端。客户端标识由媒介类型、MAC 地址和接口名称组成，如 MAC 地址为 00d0.f822.33b4、接口名称为 GigabitEthernet 0/1 对应的客户端标识为 0100.d0f8.2233.b467.6967.6162.6974.4574.6865.726e.6574.302f.31，其中 01 代表以太网媒介类型，67.6967.6162.6974.4574.6865.726e.6574.302f.31 为 GigabitEthernet0/1 的十六进制码。关于媒介代码的定义，可以参见 RFC1700 文档的“Address Resolution Protocol Parameters”章节。
只有在进行 DHCP 手工绑定定义时，才可以使用该命令。

【配置举例】 1：定义了 MAC 地址为 00d0.f822.33b4 的以太网 DHCP 客户端的客户端标识。

```
Ruijie(dhcp-config)# client-identifier
0100.d0f8.2233.b467.6967.6162.6974.4574.6865.726e.6574.302f.31
```

【检验方法】 通过 **show run** 可见配置成功

【提示信息】 -

【常见错误】 -

【平台说明】 -

1.17 client-name

要定义 DHCP 客户端的名字，用 DHCP 地址池配置命令 **client-name**
client-name *client-name*

no 形式删除 DHCP 客户端的名字
no client-name

恢复默认值
default client-name

【参数说明】

参数	描述
client-name	定义 DHCP 客户端的名字。可以用任何标准的 ASCII 字符集。名字不应包括后缀域名，比如定义 river 为 DHCP 客户端名字，不能定义为 river.i-net.com.cn

【缺省配置】 缺省没有定义客户端名字

【命令模式】 DHCP 地址池配置模式

【缺省级别】 14

【使用指导】 该命令属于 Server 配置；只有在进行 DHCP 手工绑定定义时，才可以利用该命令定义 DHCP 客户端的名字。该名字不应该包括后缀域名

【配置举例】 1：定义了一个字符串 river 作为客户端的名字。

```
Ruijie(dhcp-config)# lease 0 1
```

2：将 DHCP 租期设为 1 分钟。

```
Ruijie(dhcp-config)# lease 0 0 1
```

【检验方法】 通过 **show run** 可见配置成功

【提示信息】 -

【常见错误】 -

【平台说明】 -

1.18 default-router

定义 DHCP 客户端的缺省网关，用 DHCP 地址池配置命令 **default-router**
default-router *ip-address* [*ip-address2…ip-address8*]

no 形式可以删除缺省网关的定义
no default-router

恢复默认值
defaut default-router

【参数说明】

参数	描述
ip-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 个网关。缺省情况只有一个 IP 地址

【缺省配置】 缺省没有定义缺省网关

【命令模式】 DHCP 地址池配置模式

【缺省级别】 14

【使用指导】 该命令属于 Server 配置；一般情况下，DHCP 客户端需要从 DHCP 服务器获得缺省网关信息。DHCP 服务器

至少需要为客户端指定一个网关 IP 地址，该地址必须与分配给客户的地址在同一个网段。

【配置举例】 1：定义了 192.168.12.1 作为缺省网关

```
Ruijie(dhcp-config)# default-router 192.168.12.1
```

【检验方法】 通过 **show run** 可见配置成功

【提示信息】 1：配置非法地址

```
Ruijie(dhcp-config)# default-router 225.2.2.2
% Error: ip address (225.2.2.2) is not valid!
```

【常见错误】 1.配置非单播地址
2.配置超过 8 个有效地址

【平台说明】 -

1.19 dns-server

要定义 DHCP 客户端的 DNS 服务器，用 DHCP 地址池配置命令 **dns-server**
dns-server { *ip-address* [*ip-address2…ip-address8*] | **use-dhcp-client** *interface-type interface-number* }

no 形式可以删除 DNS 服务器的定义
no dns-server

恢复默认值
defaut dns-server

【参数说明】

参数	描述
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

【缺省配置】 缺省没有定义 DNS 服务器

【命令模式】 DHCP 地址池配置模式

【缺省级别】 14

【使用指导】 该命令属于 Server 配置；定义多个 DNS 服务器时，写在前面的优先权高，DHCP 客户端只有与排在前头的 DNS 服务器通讯失败，才会选择下一个 DNS 服务器。

RGOS 软件同时也做 DHCP 客户端时，可以将通过客户端获得的 DNS 服务器信息，传送给 DHCP 客户端。

【配置举例】 1：DHCP 客户端指定了 DNS 服务器 192.168.12.3

```
Ruijie(dhcp-config)# dns-server 192.168.12.3
```

【检验方法】 通过 **show run** 可见配置成功

【提示信息】 1：配置非法地址

```
Ruijie(dhcp-config)# dns-server 225.2.2.2
% Error: ip address (225.2.2.2) is not valid!
```

【常见错误】 1.配置非单播地址
2.配置超过 8 个有效地址

1.20 domain-name

要定义 DHCP 客户端的后缀域名，用 DHCP 地址池命令 **domain-name**
domain-name *domain-name*

no 形式可以删除后缀域名
no domain-name

恢复默认值
defaut domain-name

【参数说明】

参数	描述
domain-name	定义 DHCP 客户端的后缀域名字符串

【缺省配置】 缺省没有后缀域名

【命令模式】 DHCP 地址池配置模式

【缺省级别】 14

【使用指导】 该命令属于 Server 配置；DHCP 客户端获得了指定后缀域名后，当访问具有同样后缀域名的主机时，直接通过主机名就可以了

【配置举例】 1：给 DHCP 客户端定义了后缀域名 i-net.com.cn

```
Ruijie(dhcp-config)# domain-name i-net.com.cn
```

【检验方法】 通过 **show run** 可见配置成功

【提示信息】 1：配置客户端后缀域名

```
Ruijie(dhcp-config)#domain-name ruijie.com.cn
```

【常见错误】 -

1.21 hardware-address

要定义 DHCP 客户端的硬件地址，用 DHCP 地址池配置命令 **hardware-address**
hardware-address *hardware-address* [*type*]

no 形式可以删除硬件地址的定义
no hardware-address

恢复默认值
defaut hardware-address

【参数说明】

参数	描述
hardware-address	定义 DHCP 客户端的 MAC 地址
type	标识 DHCP 客户端的硬件平台协议 ,可以用字符串或数字定义。字符串选项： ■ ethernet ■ ieee802 数字选项： ■ 1（10M ethernet） ■ 6（IEEE 802）

【缺省配置】 缺省没有硬件地址
如果定义硬件地址时没跟选项，缺省为 ethernet

【命令模式】 DHCP 地址池配置模式

【缺省级别】 14

【使用指导】 该命令属于 Server 配置；只有在进行 DHCP 手工绑定定义时，才可以使用该命令

【配置举例】 1：定义了类型为 ethernet 的 MAC 地址 00d0.f838.bf3d

```
Ruijie(dhcp-config)# hardware-address 00d0.f838.bf3d
```

【检验方法】 通过 **show run** 可见配置成功

【提示信息】 -

【常见错误】 -

1.22 host

要定义 DHCP 客户端主机的 IP 地址和网络掩码，用 DHCP 地址池配置命令 **host**
host *ip-address* [*netmask*]

no 形式可以删除 DHCP 客户端 IP 地址和网络掩码的定义
no host

恢复默认值
defaut host

【参数说明】

参数	描述
host *ip-address* [*netmask*]	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

【缺省配置】 没有定义主机的 IP 地址和网络掩码

【命令模式】 DHCP 地址池配置模式

【缺省级别】 14

【使用指导】 该命令属于 Server 配置；如果网络掩码没有明确定义，DHCP 服务器将利用该 IP 地址的自然网络掩码。A 类地址网络掩码为 255.0.0.0；B 类地址网络掩码为 255.255.0；C 类地址网络掩码为 255.255.255.0。
只有在进行 DHCP 手工绑定定义时，才可以使用该命令。

【配置举例】 1：将客户端 IP 地址设为 192.168.12.91，掩码为避免 255.255.255.240

```
Ruijie(dhcp-config)# host 192.168.12.91 255.255.255.240
```

【检验方法】 通过 **show run** 可见配置成功

【提示信息】 1：配置非法地址

```
Ruijie(dhcp-config)# host 225.2.2.2 255.0.0.0
% Error: ip address 225.2.2.2 is not valid!
```

【常见错误】 1.配置非法地址

1.23 ip address dhcp

要使得以太网或者 PPP、HDLC、FR 封装的接口能够通过 DHCP 获得 IP 地址信息，用接口配置命令 **ip address dhcp**

ip address dhcp

no 形式可以取消该配置

no ip address dhcp

恢复默认值

defaut ip address dhcp

【参数说明】

参数	描述
-	-

【缺省配置】 缺省接口不能通过 DHCP 获得 IP 地址

【命令模式】 接口配置模式

【缺省级别】 14

【使用指导】 该命令属于 Client 配置；RGOS 软件的 DHCP 客户端，在请求 IP 地址时，还要求 DHCP 服务器提供五个配置参数信息：1）DHCP 选项 1，客户端子网掩码；2）DHCP 选项 3，同一子网上的网关信息；3）DHCP 选项 6，DNS 服务器信息；4）DHCP 选项 15，主机后缀域名；DHCP 选项 44，WINS 服务器信息（可选配置）。
RGOS 软件的客户端允许在 PPP、FR、HDLC 连路上通过 dhcp 获得地址，这个需要服务器的支持，目前我们的服务器支持该功能

【配置举例】 1：使得 FastEthernet 0 端口自动获得 IP 地址

```
Ruijie(config)# interface GigabitEthernet 0/1
Ruijie(config-if-GigabitEthernet 0/1) ip address dhcp
```

【检验方法】 通过 **show run** 可见配置成功

【提示信息】 -

【常见错误】 1.在二层口上开户客启端功能

1.24 ip dhcp add-client

针对指定接入位置、指定用户主机名称、指定终端 MAC 地址分配固定 IP 地址，添加固态绑定的配置命令为

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* **}**

该命令的 no 形式可以取消这种定义
no ip dhcp add-client { solidify-ip ip *ip-addr* **| solidify-location ip** *ip-addr* **| solidify-mac mac** *mac-addr* **}**

恢复缺省配置
default ip dhcp add-client { solidify-ip ip *ip-addr* **| solidify-location ip** *ip-addr* **| solidify-mac mac** *mac-addr* **}**

【参数说明】

参数	描述
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

【缺省配置】 默认不配置固态绑定用户

【命令模式】 全局配置模式

【缺省级别】 14

【使用指导】 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】 1：在全局配置模式下配置根据终端 MAC 地址信息分配固定 IP 地址

```
Ruijie(config)# ip dhcp add-client solidify-ip ip 192.168.100.100 mac 00d0.cce2.eefa binding-type ip-mac
```

【检验方法】 通过 **show run** 可以观察配置成功

【提示信息】 Failed to set solidify agent(x.x.x.x. type = XX), because of wrong parameter(ip = 0.0.0.0).
固态绑定配置失败，绑定 IP 未配置

Failed to set solidify agent(H.H.H type = XX),because of wrong parameter(mac = 0000.0000.0000).
固态绑定配置失败，绑定终端 MAC 信息未配置

Solidify agent(%s type = %s) ip has been set by other solidify.
终端重复固态绑定

Failed to set solidify agent(%s type = %s), because of wrong parameter (hostname is NULL).
固态绑定配置失败，绑定主机名信息未配置

Failed to set solidify agent(%s type = %s), because of wrong parameter (acc-dev ip = 0.0.0.0).
Failed to set solidify agent(%s type = %s), because of wrong parameter (acc-dev mac = 0000.0000.0000).
固态绑定配置失败，绑定接入位置信息未配置

Solidify agent(%s type = %s) has been set by static(ret = %d).
固态绑定配置失败，与静态绑定配置冲突

Solidify agent(%s type = %s) has been set by dynamic.
固态绑定配置失败，与在线的动态用户终端信息冲突

【常见错误】 -

【平台说明】 支持外置存储和 PG 数据库的平台

1.25 ip dhcp class

要定义一个 CLASS 并进入全局 CLASS 配置模式，用全局配置模式下的 **ip dhcp class** 命令
ip dhcp class *class-name*

no 形式可以删除全局的 CLASS
no ip dhcp class *class-name*

【参数说明】

参数	描述
class-name	输入 CLASS 的名称，可以是字符串或数字，如 myclass 或者 1。

【缺省配置】 缺省未配置 class。

【命令模式】 全局配置模式

【缺省级别】 14

【使用指导】 该命令属于 Server 配置；执行该命令，就会进入全局 CLASS 配置模式，在这个配置模式中，可以配置 CLASS 匹配的 Option82 信息、CLASS 的标识信息

【配置举例】 1： 配置一个全局的 CLASS

```
Ruijie(config)# ip dhcp class myclass
```

【检验方法】 通过 **show run** 可见配置成功

【提示信息】 -

【常见错误】 -

【平台说明】 -

1.26 ip dhcp excluded-address

要定义某些 IP 地址，使得 DHCP 服务器不会将其分配给 DHCP 客户端，用全局配置命令
ip dhcp excluded-address *low-ip-address* [*high-ip-address*]

该命令的 no 形式可以取消这种定义
no ip dhcp excluded-address *low-ip-address* [*high-ip-address*]

恢复缺省配置
default ip dhcp excluded-address *low-ip-address* [*high-ip-address*]

【参数说明】

参数	描述
low-ip-address	排斥 IP 地址，或者排斥 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。缺省情况其值为 low-ip-address

【缺省配置】 缺省 DHCP 服务器分配整个地址池的 IP 地址

【命令模式】 全局配置模式

【缺省级别】 14

【使用指导】 该命令属于 Server 配置；如果没有配置排斥 IP 地址，DHCP 服务器会试图分配 DHCP 地址池中的所有 IP 地址。该命令可以为特定主机保留一些 IP 地址，避免这些地址被分配给 DHCP 客户端。精确地定义排斥 IP 地址，也可以减少 DHCP 服务器分配地址时的冲突检测时间

【配置举例】 1：DHCP 服务器将不会试图分配 192.168.12.100~150 范围内的 IP 地址

```
Ruijie(config)#ip dhcp excluded-address 192.168.12.100 192.168.12.150
```

2：删除例 1 中排除地址范围

```
Ruijie(config)#no ip dhcp excluded-address 192.168.12.100 192.168.12.150
```

【检验方法】 通过 **show run** 可以观察配置成功

【提示信息】 1：配置非法排除地址

```
Ruijie(config)#ip dh excluded-address 225.1.1.1
% Error:  Ip address 225.1.1.1 or 225.1.1.1 is not valid!
```

2：删除不存在的排除地址

```
Ruijie(config)#no ip dhcp excluded-address 20.1.1.1
% Range [20.1.1.1, 20.1.1.1] is not in the database.
```

【常见错误】 1.配置非法排除地址
2.删除不存在的排除地址

【平台说明】 -

1.27 ip dhcp force-send-nak

要配置强制发送 NAK 报文功能
ip dhcp force-send-nak

取消强制发送 NAK 报文功能
no ip dhcp force-send-nak

恢复缺省配置
default ip dhcp force-send-nak

【参数说明】

参数	描述
-	-

【缺省配置】 缺省配置下开启强制发送 NAK 报文功能

【命令模式】 全局配置模式

【缺省级别】 14

【使用指导】 该命令属于 Server 配置；DHCP 客户端在每次设备启动的时候都会检查之前使用过的 IP 地址，发送 DHCPREQUEST 请求报文进行续约，希望能够再次使用该 IP 地址。如果该地址不可用时，DHCP 服务器发

送 NAK 报文，使客户端重新发起 DHCPDISCOVER 申请新的地址。如果当前服务器不存在对应的租约记录，客户端将会持续发送 DHCPREQUEST 续租请求，在无线应用中为了加快用户重新发起 DHCPDISCOVER 请求，增加强制发送 NAK 报文功能

【配置举例】 1：全局配置模式下打开强制发送 NAK 功能

```
Ruijie(config)# ip dhcp force-send-nak
```

【检验方法】 通过 **show run** 可看到配置成功

【常见错误】 -

【平台说明】 -

1.28 ip dhcp monitor-vrrp-state

要监控 VRRP 的状态，使 DHCP Server 仅处理当前设备处于 Master 状态的 vrrp 接口上来的请求报文
ip dhcp monitor-vrrp-state

取消对 vrrp 状态的监控，此时无论 Master 或者 Backup 状态的 VRRP 接口上来的请求报文都将被处理
no ip dhcp monitor-vrrp-state

恢复缺省配置
default ip dhcp monitor-vrrp-state

【参数说明】

参数	描述
-	-

【命令模式】 三层接口配置模式

【缺省级别】 14

【缺省配置】 缺省配置下不对接口 VRRP 状态进行监控

【使用指导】 该命令属于 Server 配置；如果接口下配置了 VRRP 地址，DHCP 服务器仅处理处于主设备（Master）状态的接口请求报文，丢弃处于非（Master）状态的接口请求报文。对于未配置 VRRP 地址的接口，DHCP 服务器不再监控 VRRP 状态，所有 DHCP 请求报文都将被处理

【配置举例】 1：DHCP 服务器对当前三层接口的 VRRP 状态进行监控

```
Ruijie(config-if)# ip dhcp monitor-vrrp-state
```

【检验方法】 -

【提示信息】 1：在二层接口配置 VRRP 状态监控

```
Ruijie(config-if-GigabitEthernet 0/2)#ip dhcp monitor-vrrp-state
% Invalid input detected at '^' marker.
```

【常见错误】 1：在二层接口配置 VRRP 状态监控

【平台说明】 -

1.29 ip dhcp ping packets

要配置 DHCP 服务器检测地址冲突时，ping 该地址的次数
ip dhcp ping packets [*number*]

no 形式恢复缺省配置
no ip dhcp ping packets

恢复缺省配置
default ip dhcp ping packets

【参数说明】

参数	描述
number	（可选）范围从 0 到 10，0 表示关闭 ping 操作。缺省 ping 两个包

【缺省配置】 缺省 ping 包各数为 2

【命令模式】 全局配置模式

【缺省级别】 14

【使用指导】 该命令属于 Server 配置；DHCP 服务器从 DHCP 地址池中试图分配 IP 地址时，会用 ping 操作来检测该地址是否已被其它主机占用，如果占用就记录下来，如果没占用就分配给 DHCP 客户端。Ping 操作缺省为发送两个数据包，最多可以发送 10 个包

【配置举例】 1：将 ping 操作发送数据包数设为 3 个

```
Ruijie(config)# ip dhcp ping packets 3
```

【检验方法】 通过 **show run** 可看到配置成功

【提示信息】 -

【常见错误】 -

【平台说明】 -

1.30 ip dhcp ping timeout

要配置 DHCP 服务器用 ping 操作检测地址冲突时，等待应答的超时时间
ip dhcp ping timeout *milli-seconds*

no 形式可以恢复缺省配置
no ip dhcp ping timeout

恢复缺省配置
default ip dhcp ping timeout

【参数说明】

参数	描述
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

【缺省配置】 缺省超时时间为 500 毫秒

【命令模式】 全局配置模式

【缺省级别】 14

【使用指导】 该命令属于 Server 配置；定义等待一个 ping 应答包的时间

【配置举例】 1： ping 应答包等待时间设为 600ms

```
Ruijie(config)# ip dhcp ping timeout 600
```

【检验方法】 通过 **show run** 可看到配置成功

【提示信息】 -

【常见错误】 -

【平台说明】 -

1.31 ip dhcp pool

要定义一个 DHCP 地址池名并进入 DHCP 地址池的配置模式
ip dhcp pool *pool-name* **[set-real-pool** *rpool-name* **| unset-real-pool]**

no 形式可以删除 DHCP 地址池
no ip dhcp pool *pool-name*

恢复默认值删除地址池
default ip dhcp pool *pool-name*

【参数说明】

参数	描述
pool-name	地址池名称
rpool-name	实体机地址池名称

【缺省配置】 缺省没有定义 DHCP 地址池

【命令模式】 全局配置模式

【缺省级别】 14

【使用指导】 该命令属于 Server 配置；
1：执行该命令，就会进入 DHCP 地址池配置模式，显示为

```
Ruijie(dhcp-config)#
```

在这个配置模式中，可以配置 IP 地址范围、DNS 服务器、缺省网关等参数
2: **set-real-pool 用于设置虚拟地址池和实地址池的关联，关联后实地址池用于为实体机分配地址，虚地址池用于为虚拟机分配地址。**

【配置举例】 1：定义了一个名为 mypool0 的 DHCP 地址池。

```
Ruijie(config)#ip dhcp pool mypool0
Ruijie(dhcp-config)#
```

2：定义地址池 test 为地址池 real 的虚拟地址池。

```
Ruijie(config)#ip dhcp pool test set-real-pool real
```

【检验方法】 通过 **show ip dhcp pool** *mypool0* 可观察配置成功
通过 show run 配置可以观察虚实地址池是否关联

【提示信息】 -

【常见错误】 1. 虚拟地址池或实地址池不存在。

【平台说明】 -

1.32 ip dhcp refresh arp

重新下发可信 ARP

ip dhcp refresh arp

【参数说明】

参数	描述
-	-

【缺省配置】 -

【命令模式】 全局配置模式

【缺省级别】 14

【使用指导】 该命令属于 Server 配置；
执行该命令，就会根据从配置 **update arp** 的地址池中分配的租约重新下发可信 ARP

【配置举例】 1：重新下发可信 ARP。

```
Ruijie(config)#ip dhcp refresh arp
```

【检验方法】 通过 **show arp trusted** 可以看到重新下发的可信 ARP

【提示信息】 -

【常见错误】 -

【平台说明】 -

1.33 ip dhcp relay check server-id

启用 DHCP relay check server-di 功能。
ip dhcp relay check server-id

关闭 DHCP relay check server-id 功能。
no ip dhcp relay check server-id

【参数说明】

参数	描述
-	-

【缺省配置】 关闭 DHCP relay check server-id 功能。

【命令模式】 全局模式

【缺省级别】 14

【使用指导】 该命令属于 Server 配置；当配置命令 **ip dhcp relay check server-id** 后，DHCP Relay 仅将 DHCP 请求报文转发到 option server-id 中指定的服务器。如果没有配置该命令，则向所有配置的 DHCP 服务器转发 DHCP 请求报文。

【配置举例】 1：启用 DHCP relay check server-di 功能。

```
Ruijie(config)# ip dhcp relay check server-id
```

2：关闭 DHCP relay check server-id 功能。

```
Ruijie(config)# no ip dhcp relay check server-id
```

【检验方法】 1：使用 **show running-config** 命令，可以查看是否配置成功。

【提示信息】 -

【常见错误】 -

【平台说明】 -

1.34 ip dhcp relay information option82

启用 DHCP option82 功能。
ip dhcp relay information option82 [standard-format | verbose-format]

关闭 DHCP option82 功能。
no ip dhcp relay information option82 [standard-format | verbose-format]

【参数说明】

参数	描述
-	-

【缺省配置】 关闭 DHCP option82 功能。

【命令模式】 全局模式

【缺省级别】 14

【使用指导】 该命令属于 Relay 配置；
当配置 **ip dhcp relay information option82** 命令时，设备做为 DHCP 中继，在转发 DHCP 请求报文过程中，在 DHCP 请求报文中添加 option82 信息 ,其中 circuit-id 封装格式是 :slot(1):port(1):dev_name(<=64) ,remote-id 封装格式是 user_mac(6):iftype(4):port_name(<=64):vid(2)；
当配置 **ip dhcp relay information option82 standard-format** 命令时 ,DHCP 请求报文中添加 option82 信息，其中 circuit-id 封装格式是：vid(2):slot(1):port(1)，remote-id 封装格式是 sys_mac(6)；

当配置 **ip dhcp relay information option82 verbose-format** 命令时，DHCP 请求报文中添加 option82 信息，其中 circuit-id 封装格式是：mac port_name vid（每个字段以空格分隔），remote-id 封装格式是 hostname。上面 3 条添加 option82 命令互斥，仅有一种模式生效。当删除某种封装模式命令时，会关闭 DHCP option82 功能。。

【配置举例】 1：启用 DHCP option82 功能。

```
Ruijie(config)# ip dhcp relay information option82
```

2：关闭 DHCP option82 功能。

```
Ruijie(config)# no ip dhcp relay information option82
```

【检验方法】 1：使用 **show running-config** 命令，可以查看是否配置成功。

【提示信息】 -

【常见错误】 -

【平台说明】 -

1.35 ip dhcp server detect

启用 DHCP 伪服务器检测功能。
ip dhcp server detect

关闭 DHCP 伪服务器检测功能。
no ip dhcp server detect

恢复默认关闭 DHCP 伪服务器检测功能。
default ip dhcp server detect

【参数说明】

参数	描述
-	-

【缺省配置】 关闭 DHCP 伪服务器功能。

【命令模式】 全局模式

【缺省级别】 14

【使用指导】 该命令属于 Server 配置；配置 DHCP 伪服务器检测功能后，如果网络中存在伪服务器，会记录在日志中。

【配置举例】 1：启用 DHCP 伪服务器功能。

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

【检验方法】 1：使用 **show running-config** 命令，可以查看是否配置成功。

【提示信息】 -

【常见错误】

【平台说明】 -

1.36 ip dhcp use class

要配置启用 CLASS 进行地址分配，用全局配置模式下的 **ip dhcp use class** 命令，该命令的 no 形式可以关闭使用 CLASS 进行地址分配。

ip dhcp use class

no ip dhcp use class

【参数说明】

参数	描述
-	-

【缺省配置】 缺省启用 CLASS 进行地址分配。

【命令模式】 全局配置模式。

【使用指导】 该命令属于 Server 配置；

【配置举例】 1：配置启用 CLASS 进行地址分配。

```
Ruijie(config)# ip dhcp use class
```

【检验方法】 通过 **show run** 可看到配置成功

【提示信息】 -

【常见错误】 -

【平台说明】 -

1.37 ip helper-address

添加一个全局或对应接口下的 DHCP 服务器地址。

ip helper-address { cycle-mode *A.B.C.D* **}**

删除一个全局或对应接口下的 DHCP 服务器地址。

no ip helper-address { cycle-mode *A.B.C.D* **}**

【参数说明】

参数	描述
cycle-mode	开启 dhcp 请求报文转发所有 dhcp 服务器
A.B.C.D	DHCP 服务器地址

【缺省配置】 DHCP 服务器列表为空。

【命令模式】 全局模式、接口模式

【缺省级别】 14

【使用指导】 该命令属于 Relay 配置；在配置 DHCP 服务器的 IP 地址后，设备将收到的 DHCP 请求报文将转发给它；同时，将收到的 DHCP 服务器响应报文转发给 DHCP 客户端。

DHCP 服务器地址可以全局配置，也可以在三层接口上配置。全局或者每个三层接口上最多可以配置 20 个 DHCP 服务器地址。在接口上收到 DHCP 请求报文时，首先使用接口上的 DHCP 服务器列表；如果接口上面没有配置 DHCP 服务器列表，则使用全局配置的 DHCP 服务器列表。

全局配置模式下可对 dhcp relay 的 cycle-mode 参数进行配置，当启用 cycle-mode 的时候表示 dhcp relay 允许把接收到的 dhcp client 请求报文转发到以上规则的所有 dhcp server 上 当不启用 cycle-mode 的时候表示 dhcp relay 只把接收到的 dhcp client 请求报文转发到以上规则的第一个 dhcp server 上。cycle-mode 只在全局配置模式下配置，作用于全局和接口，默认为启用。

【配置举例】 1：在 intterface vlan 1 上配置一个 DHCP 服务器的 IP 地址 192.168.11.1

```
Ruijie# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Ruijie(config)# interface vlan 1
Ruijie(config-if)# ip helper-address 192.168.11.1
```

2：删除 intterface vlan 1 上已经配置 DHCP 服务器的 IP 地址 192.168.11.1

```
Ruijie(config-if)# no ip helper-address 192.168.11.1
```

3：配置一个全局的 DHCP 服务器的 IP 地址 192.168.100.1。

```
Ruijie# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Ruijie(config)# ip helper-address 192.168.100.1
```

4：删除之前配置的全局的 DHCP 服务器的 IP 地址 192.168.100.1。

```
Ruijie(config)# no ip helper-address 192.168.100.1
```

5：开启 dhcp 请求报文转发所有 dhcp 服务器。

```
Ruijie(config)# ip helper-address cycle-mode
```

6：关闭 dhcp 请求报文转发所有 dhcp 服务器。

```
Ruijie(config)# no ip helper-address cycle-mode
```

【检验方法】 1：使用 **show running-config** 命令，可以查看是否配置成功。

【提示信息】 -

【常见错误】 1：**ip helper-address** 配置命令只能全局配置或在三层接口上配置，不能在二层接口上配置
2：开启 **ip helper-address** 功能之前需要确保 DHCP Relay 功能已经开启
3：将客户端部署为既可以通过 DHCP Relay 获取地址，又可以通过 DHCP Server 直接获取地址，会导致客户端可能无法获取正确地址

【平台说明】 -

1.38 lease

要定义 DHCP 服务器分配给客户端地址的租期时间，用 DHCP 地址池配置命令 **lease。**该命令的 **no** 形式恢复缺省配置。有限租期范围从 1 分钟到 365 天 23 小时 59 分钟
lease {*days* [*hours*] [*minutes*] | **infinite**}

no 形式恢复缺省配置
no lease

恢复默认值
defaut lease

【参数说明】

参数	描述
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。缺省为 0
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 ,缺省为 0
infinite	定义没有限制的租期

【缺省配置】 静态地址池的缺省租期为 infinite。其它地址池的缺省租期为一天

【命令模式】 DHCP 地址池配置模式

【缺省级别】 14

【使用指导】 该命令属于 Server 配置；当租期快到时，DHCP 客户端会发送续租请求。DHCP 服务器一般会允许续租，续租的地址保持不变

【配置举例】 1：将 DHCP 租期设为 1 小时

```
Ruijie(dhcp-config)# lease 0 1
```

2：将 DHCP 租期设为 1 分钟

```
Ruijie(dhcp-config)# lease 0 0 1
```

【检验方法】 通过 **show run** 可见配置成功

【提示信息】 -

【常见错误】 -

1.39 lease-threshold

要定义 DHCP 地址池的告警百分比，用 DHCP 地址池配置命令 **lease-threshold**
lease-threshold *percentage*

no 形式关闭告警功能
no lease-threshold

恢复默认值
defaut lease-threshold

【参数说明】

参数	描述
percentage	定义地址池告警的百分比，取值范围为 60 到 100

【缺省配置】 缺省为 90%

【命令模式】 DHCP 地址池配置模式

【缺省级别】 14

【使用指导】 该命令属于 Server 配置；如果地址池的最大 IP 利用率到达门限值，DHCP 服务器将产生 SYSLOG 告警信息。IP 利用率表示当前已分配的地址数与当前地址池可分配地址总数的比值。如果分配的地址数目一直处于告警阈值以上，那么每 5 分钟将产生一次告警信息

【配置举例】 1：将地址池告警阈值设为 80%：

```
Ruijie(dhcp-config)# lease-threshold 80
```

2：关闭地址池告警功能

```
Ruijie(dhcp-config)# no lease-threshold
```

【检验方法】 通过 **show run** 可见配置成功

【提示信息】 -

【常见错误】 -

1.40 netbios-name-server

要配置微软 DHCP 客户端 NETBIOS 的 WINS 名字服务器
netbios-name-server *ip-address* [*ip-address2…ip-address8*]

删除 WINS 服务器
no netbios-name-server

恢复默认值
defaut netbios-name-server

【参数说明】

参数	描述
ip-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

【缺省配置】 缺省没有定义 WINS 服务器

【命令模式】 DHCP 地址池配置模式

【缺省级别】 14

【使用指导】 该命令属于 Server 配置；定义多个 WINS 服务器时，写在前面的优先权高，DHCP 客户端只有与排在前头的 WINS 服务器通讯失败，才会选择下一个 WINS 服务器

【配置举例】 1：为 DHCP 客户端指定了 WINS 服务器 192.168.12.3

```
Ruijie(dhcp-config)# netbios-name-server 192.168.12.3
```

【检验方法】 通过 **show run** 可见配置成功

【提示信息】 1：配置非法地址

```
Ruijie(dhcp-config)#netbios-name-server 225.2.2.2
%Error: ip address (225.2.2.2) is not valid!
```

【常见错误】 1.配置非单播地址
2.配置超过 8 个有效地址

1.41 netbios-node-type

要定义微软 DHCP 客户端主 NetBIOS 的节点类型，用 DHCP 地址池配置命令 **netbios-node-type**
netbios-node-type *type*

删除 NetBIOS 节点类型配置
no netbios-node-type

恢复默认值
defaut netbios-node-type

【参数说明】

参数	描述
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： ■ 代表 b-node ■ 代表 p-node ■ 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

【缺省配置】 缺省没有定义 NetBIOS 节点类型

【命令模式】 DHCP 地址池配置模式

【缺省级别】 14

【使用指导】 该命令属于 Server 配置；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。建议将 NetBIOS 的节点类型设为 Hybrid

【配置举例】 1：将微软 DHCP 客户端的 NetBIOS 节点设为复合型节点：

```
Ruijie(dhcp-config)# netbios-node-type h-node
```

【检验方法】 通过 **show run** 可见配置成功

【提示信息】 -

【常见错误】 -

1.42 network

要定义 DHCP 地址池的网络号和网络掩码，用 DHCP 地址池配置命令 **network;**
要通告瘦 AP 上配置 DHCP 地址池的网络号和网络掩码，可在 AC 的 ap-config/或者 ap-group 模式下配置 **network** 命令。
network *network-number net-mask* [*low-ip-address high-ip-address*]

no 形式可以删除定义；
在 AC 的 ap-config 或者 ap-group 模式下删除定义；
no network

恢复默认值，AC 的 ap-config 或者 ap-group 不支持。
defaut network

【参数说明】

参数	描述
network-number	DHCP 地址池的 IP 地址网络号
net-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
low-ip-address	可用起始 IP 地址（AC 的 ap-config 或者 ap-group 模式不支持）
high-ip-address	可用结束 IP 地址（AC 的 ap-config 或者 ap-group 模式不支持）

【缺省配置】 缺省没有定义网络号和网络掩码

【命令模式】 DHCP 地址池配置模式

【缺省级别】 14

【使用指导】 该命令属于 Server 配置；定义新建地址池的子网及其掩码，为 DHCP 服务器提供了一个可分配给客户端的地址空间。除非有地址排斥配置，否则所有地址池中的地址都有可能分配给客户端。DHCP 在分配地址池中的地址，是按顺序进行的，如果该地址已经在 DHCP 绑定表中或者检测到该地址已经在该网段中存在，就检查下一个地址，直到分配一个有效的地址。
地址的分配情况可用 **show ip dhcp binding** 命令查看 ,地址检测冲突情况可用 **show ip dhcp conflict** 命令查看。

【配置举例】 1：定义了 DHCP 地址池的网络号为 192.168.12.0，掩码为 255.255.255.240

```
Ruijie(dhcp-config)# network 192.168.12.0 255.255.255.240
```

2：AC 通告 AP 定义了 DHCP 地址池的网络号为 192.168.12.0，掩码为 255.255.255.240

```
Ruijie(config)# ap-group default
Ruijie(config-group) # network 192.168.12.0 255.255.255.240
```

【检验方法】 通过 **show run** 可见配置成功

【提示信息】 1：配置非法地址

```
Ruijie(dhcp-config)#network 238.5.5.5 255.0.0.0
238.5.5.5 / 255.0.0.0 is an invalid network
```

【常见错误】 1.配置非单播地址

1.43 next-server

要定义 DHCP 客户端启动过程中需要访问的启动服务器列表，用 DHCP 地址池配置命令 **next-server**
next-server *ip-address* [*ip-address2…ip-address8*]

no 形式可以删除启动服务器列表的定义
no next-server

恢复默认值
defaut next-server

【参数说明】

参数	描述
ip-address	定义启动服务器的 IP 地址，通常为 TFTP 服务器。要求至少配置一个
ip-address2…ip-address8	（可选）最多可以配置 8 启动服务器

【缺省配置】 无缺省配置

【命令模式】 DHCP 地址池配置模式

【缺省级别】 14

【使用指导】 该命令属于 Server 配置；定义多个启动服务器时，写在前面的优先权高，DHCP 客户端只有与排在前头的启动服务器通讯失败，才会选择下一个启动服务器。

【配置举例】 1：为 DHCP 客户端指定了启动服务器 192.168.12.4

```
Ruijie(dhcp-config)# next-server 192.168.12.4
```

【检验方法】 通过 **show run** 可见配置成功

【提示信息】 1：配置非法地址

```
Ruijie(dhcp-config)# next-server 238.5.5.5
% Error: ip address(238.5.5.5) is invalid!
```

【常见错误】 1.配置非单播地址
2.配置超过 8 个服务器地址列表

1.44 option

要配置 DHCP 服务器的选项，用 DHCP 地址池配置命令 **option**
option *code* { **ascii** *string* | **hex** *string* | **ip** *ip-address* }

no 形式可以删除 option 的定义
no option

恢复默认值
defaut option

【参数说明】

参数	描述
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

【缺省配置】 无缺省配置

【命令模式】 DHCP 地址池配置模式

【缺省级别】 14

【使用指导】 该命令属于 Server 配置；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。关于当前 DHCP option 的定义，请参见 RFC 2132 文档。

【配置举例】 1：对选项代码 19 进行了定义，该选项决定了 DHCP 客户端是否启用 IP 包转发。0 表示关闭 IP 包转发；1 表示启用 IP 包转发。以下配置，使得 DHCP 客户端启用 IP 包转发

```
Ruijie(dhcp-config)# option 19 hex 1
```

2：对选项代码 33 进行了定义，该选项给 DHCP 客户端提供了静态路由信息，DHCP 客户端将安装两条静态路由：

```
Ruijie(dhcp-config)# option 33 ip 172.16.12.0 192.168.12.12 172.16.16.0 192.168.12.16
```

【检验方法】 通过 **show run** 可见配置成功

【提示信息】 1：配置非法静态路由地址

```
Ruijie(dhcp-config)#option 56 ip 2.2.2.2 225.5.5.5
% Error: ip address 225.5.5.5 is not valid!
```

2：配置非法十六进制字符串

```
Ruijie(dhcp-config)#option 253 hex abcdef_
% DHCP could not parse the hexadecimal string. Check character 6 (_).
```

【常见错误】
1. 配置非单播地址
2. 配置超过 8 个静态路由地址
3. 配置非法的 16 进制字符串

1.45 pool-status

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。该命令不提供 **no** 形式

pool-status {**enable | disable**}

【参数说明】

参数	描述
enable	启用地址池
disable	关闭地址池

【缺省配置】 配置了地址池后该地址池自动启用

【命令模式】 DHCP 地址池配置模式

【缺省级别】 14

【使用指导】 该命令属于 Server 配置；在使用 DHCP 服务器中可以通过该命令来临时关闭或者启用对应的地址池

【配置举例】 1：将地址池关闭

```
Ruijie(dhcp-config)# pool-status disable
```

【检验方法】 通过 **show run** 可见配置成功

【提示信息】 -

【常见错误】 -

1.46 relay agent information

要在全局的 CLASS 中进入 Option82 匹配信息配置模式，用全局 CLASS 配置模式下的 **relay agent information** 命令，该命令的 no 形式可以删除该 CLASS 的所有 Option82 匹配信息

relay agent information

no relay agent information

【参数说明】

参数	描述
-	-

【缺省配置】 -

【命令模式】 全局 CLASS 配置模式。

【使用指导】 该命令属于 Server 配置；

执行该命令，就会进入 Option82 匹配信息配置模式，显示为：

```
Ruijie (config-dhcp-class-relayinfo)#
```

在这个配置模式中，可以配置 class 匹配多个 Option82 信息。

【配置举例】 1：配置一个全局的 CLASS 并进入 Option82 匹配信息配置模式。

```
Ruijie(config)# ip dhcp class myclass
Ruijie(config-dhcp-class)# relay agent information
Ruijie(config-dhcp-class-relayinfo)#
```

【检验方法】 通过 **show run** 可见配置成功

【提示信息】 -

【常见错误】 -

1.47 relay-information hex

在全局 CLASS 下的 Option82 信息配置模式下 ,配置 option82 的匹配信息 ,调用 **relay-information hex** 命令，该命令的 **no** 形式可以删除一条匹配信息

relay-information hex *aabb.ccdd.eeff…* [*]

no relay-information hex *aabb.ccdd.eeff…* [*]

【参数说明】

参数	描述
aabb.ccdd.eeff… [*]	16 进制的 Option82 匹配信息，*代表不完全匹配，只需要匹配前面部

	分即可表示通过匹配，不带*代表需要完全匹配。

【缺省配置】 -

【命令模式】 全局 CLASS 配置模式。

【使用指导】 该命令属于 Server 配置；

【配置举例】 1：配置一个全局的 CLASS 可以匹配多个 option82 信息。

```
Ruijie(config)# ip dhcp class myclass
Ruijie(config-dhcp-class)# relay agent information
Ruijie(config-dhcp-class-relayinfo)# relay-information hex 0102256535
Ruijie(config-dhcp-class-relayinfo)# relay-information hex 010225654565
Ruijie(config-dhcp-class-relayinfo)# relay-information hex 060225654565
Ruijie(config-dhcp-class-relayinfo)# relay-information hex 060223*
```

【检验方法】 通过 **show run** 可见配置成功

【提示信息】 -

【常见错误】 -

1.48 remark

要在全局的 CLASS 中配置描述该 CLASS 的标识信息
remark *class-remark*

no 形式可以删除该标识信息
no remark

【参数说明】

参数	描述
class-remark	标识该 CLASS 的信息，可以是字符串，中间可以带空格

【缺省配置】 -

【命令模式】 全局 CLASS 配置模式。

【缺省级别】 14

【使用指导】 该命令属于 Server 配置；

【配置举例】 1： 配置一个全局的 CLASS 的标识信息。

```
Ruijie(config)# ip dhcp class myclass
Ruijie(config-dhcp-class)# remark used in #1 build
```

【检验方法】 通过 **show run** 可见配置成功

【提示信息】 -

【常见错误】 -

1.49 service dhcp

要在设备上启用 DHCP 服务器和中继代理特性，用全局配置命令 **service dhcp**
要通告瘦 AP 上启用 DHCP 服务器和中继代理特性，可在 AC 的 ap-config/或者 ap-group 模式下配置 **service dhcp** 命令
service dhcp

no 形式可以关闭 DHCP 服务器和中继代理特性
或者在 AC 的 ap-config/或者 ap-group 模式下关闭 AP 的 DHCP 服务和中继代理特性
no service dhcp

恢复默认值，AC 的 ap-config 或者 ap-group 不支持
defaut service dhcp

【参数说明】

参数	描述
-	-

【缺省配置】 该命令属于 Server 配置；缺省关闭 DHCP 服务器和中继代理特性

【命令模式】 全局配置模式、ap-config/ap-group 模式

【缺省级别】 14

【使用指导】 DHCP 服务器可以自动给客户端分配 IP 地址，并提供 DNS 服务器地址、缺省网关地址等网络配置信息。DHCP 中继特性可以将 DHCP 请求转发给其它服务器，并将返回的 DHCP 应答包在转发给 DHCP 客户端，起着 DHCP 报文中转作用。
在某些产品上可能出现 DHCP 功能和其他功能冲突的现象，具体的问题请查看相关产品的细节说明，以及配置失败的提示信息

【配置举例】 1：设备启用了 DHCP 服务器和中继特性

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

2：AC 通告 AP 启用了 DHCP 服务器和中继特性

```
Ruijie(config)# ap-group default
Ruijie(config-group) # service dhcp
```

【检验方法】 通过 **show run** 可见配置成功

【提示信息】 -

【常见错误】 -

1.50 show dhcp lease

显示 DHCP 客户获得的租约信息

show dhcp lease

【参数说明】

参数	描述
-	-

【缺省配置】 无缺省行为

【命令模式】 特权用户模式

【缺省级别】 14

【使用指导】 该命令属于 Client 配置；显示作为客户端申请到的 ip 地址的相关信息

【配置举例】 1：显示 DHCP 客户获得的租约信息

```
Ruijie# show dhcp lease
Temp IP addr: 192.168.5.71  for peer on Interface: FastEthernet0/0
Temp  sub net mask: 255.255.255.0
DHCP Lease server: 192.168.5.70, state: 7 Bound
DHCP transaction id: 337beed
Lease: 600 secs,  Renewal: 300 secs,  Rebind: 525 secs
Temp default-gateway addr: 192.168.5.1
Next timer fires after: 00:04:29
Retry count: 0   Client-ID: 0100d0f82233e3476967616269744574686572 6E6574302F31
```

【检验方法】 -

【提示信息】 -

【常见错误】 -

1.51 show ip dhcp binding

显示 DHCP 地址绑定情况

show ip dhcp binding [*ip-address*]

【参数说明】

参数	描述
ip-address	（可选）只显示指定 IP 地址的绑定情况。缺省情况显示所有绑定信息

【缺省配置】 无缺省行为

【命令模式】 特权用户模式

【缺省级别】 14

【使用指导】 该命令属于 Server 配置；如果没有定义 IP 地址，将显示所有地址的绑定情况。如果定义了 IP 地址，将只显示该 IP 地址的绑定情况

【配置举例】 1：显示 DHCP 地址绑定情况

```
Ruijie# show ip dhcp binding
Total number of clients   : 4
Expired clients           : 3
Running clients           : 1

IP address        Hardware address       Lease expiration            Type
20.1.1.1          2000.0000.2011         000 days 23 hours 59 mins   Automatic
```

显示结果的各字段含义阐述如下：

IP address	分配给 DHCP 客户端的 IP 地址。
Hardware address	DHCP 客户端的硬件地址
Lease expiration	离租期到期时间。Infinite 表示没有时间限制；IDLE 表示当前空闲的地址 ,空前原因可能是过期没续祖或者 DHCP 客户端主动释放。
Type	地址绑定类型。Automatic 表示自动分配 ;Manual 表示手工分配。

【检验方法】 -

【提示信息】 -

【常见错误】 -

1.52 show ip dhcp conflict

显示 DHCP 服务器的冲突记录

show ip dhcp conflict

【参数说明】

参数	描述
-	-

【缺省配置】 无缺省行为

【命令模式】 特权用户模式

【缺省级别】 14

【使用指导】 该命令属于 Server 配置；该命令可以显示 DHCP 服务器检测到的冲突地址列表

【配置举例】 1：显示 DHCP 服务器的冲突记录

```
Ruijie# show ip dhcp conflict
IP address     Detection Method
192.168.12.1              Ping
```

显示结果的各字段含义阐述如下：

IP address	不可分配给 DHCP 客户端的 IP 地址。
Detection Method	冲突检测方法。

【检验方法】 -

【提示信息】 -

【常见错误】 -

1.53 show ip dhcp history

显示 DHCP 历史租约记录

show ip dhcp history

【参数说明】

参数	描述
-	-

【缺省配置】 无缺省行为

【命令模式】 特权用户模式

【缺省级别】 14

【使用指导】 该命令属于 Server 配置；该命令可以显示 DHCP 已分配过的租约信息

【配置举例】 1：显示 DHCP 已分配过的租约信息

```
Ruijie#show ip dhcp history
Expired clients           : 3
IP address        Hardware address       Lease expiration          Vlan/Relay
10.1.1.5          2222.abcd.47ac         IDLE                      4097
10.1.1.4          2222.abcd.47ae         IDLE                      4097
10.1.1.3          2222.abcd.47ad         IDLE                      4097
Running clients           : 0
```

显示结果的各字段含义阐述如下：

IP address	已分配给 DHCP 客户端的 IP 地址。
Hardware address	DHCP 客户端的 mac 地址
Lease expiration	离租期到期时间。Infinite 表示没有时间限制；IDLE 表示当前空闲的地址 ,空前原因可能是过期没续祖或者 DHCP 客户端主动释放。
Vlan/Relay	DHCP 客户端经过 DHCP Relay 到 DHCP Server 申请地址则显示 DHCP Relay 的地址 ;否则显示收到 DHCP 报文的端口 ifindex

【检验方法】 -

【提示信息】 -

【常见错误】 -

1.54 show ip dhcp pool

显示 DHCP 服务器的地址池使用情况及其利用率等信息

show ip dhcp pool [*poolname*]

【参数说明】

参数	描述
poolname	（可选）只查看指定名称的地址池信息。缺省情况显示所有地址池配置

【缺省配置】 无缺省行为

【命令模式】 特权用户模式

【缺省级别】 14

【使用指导】 该命令属于 Server 配置；该命令可以显示 DHCP 服务器地址池使用情况以及地址利用率等信息

【配置举例】 1：显示 DHCP 服务器的地址池使用情况及其利用率等信息

```
Ruijie# show ip dhcp pool
Ruijie#sh ip dh pool
Pool  name       Total     Distributed  Remained   Percentage
------------  -----------  -----------  --------   -----------
net20          253          11           242        4.34782
test           0            0            0          0.00000
```

显示结果的各字段含义阐述如下

Pool address	地址池名字。
Total	地址池可供分配的地址池总数。
Distributed	已分配的地址数目。
Remained	包括未分配和可复用的剩余地址数目。
Percentage	当前地址池的地址利用率

【检验方法】 -

【提示信息】 -

【常见错误】 -

1.55 show ip dhcp relay-statistics

显示 DHCP 服务器的各种统计数据

show ip dhcp relay-statistics

【参数说明】

参数	描述
-	-

【缺省配置】 无缺省行为

【命令模式】 特权用户模式

【缺省级别】 14

【使用指导】 该命令属于 Relay 配置

【配置举例】 1. 显示 DHCP -Relay 的各种统计数据

```
Ruijie#show ip dhcp relay-statistics
Cycle mode                0

Message                   Count
Discover                  0
Offer                     0
Request                   0
Ack                       0
Nak                       0
Decline                   0
Release                   0
Info                      0
Bad                       0

Direction                 Count
Rx client                 0
Rx client uni             0
Rx client bro             0
Tx client                 0
Tx client uni             0
Tx client bro             0
Rx server                 0
```

【检验方法】 -

【提示信息】 -

【常见错误】 -

1.56 show ip dhcp server detect

显示 DHCP 检测到伪服务器列表

show ip dhcp server detect

【参数说明】

参数	描述
-	-

【缺省配置】 无缺省行为

【命令模式】 特权用户模式

【缺省级别】 14

【使用指导】 该命令属于 Server 配置

【配置举例】 1. 显示 DHCP Server 检测到的伪服务器列表

```
Ruijie#show ip dhcp server detect
The DHCP Server information:
Server IP = 10.1.10.40, DHCP server interface = GigabitEthernet 0/1
```

【检验方法】 -

【提示信息】 -

【常见错误】 -

1.57 show ip dhcp server statistics

显示 DHCP 服务器的各种统计数据

show ip dhcp server statistics

【参数说明】

参数	描述
-	-

【缺省配置】 无缺省行为

【命令模式】 特权用户模式

【缺省级别】 14

【使用指导】 该命令属于 Server 配置；该命令可以显示 DHCP 服务器当前的各项统计数据

【配置举例】 1. 显示 DHCP 服务器的各种统计数据

```
Ruijie# show ip dhcp server statistics
Address pools            2
Lease counter            4
Active  Lease Counter    0
Expired Lease Counter    4
Malformed messages       0
```

```
Dropped messages          0

Message                   Received
BOOTREQUEST             216
DHCPDISCOVER            33
DHCPREQUEST             25
DHCPDECLINE              0
DHCPRELEASE              1
DHCPINFORM              150

Message                    Sent
BOOTREPLY                 16
DHCPOFFER                 9
DHCPACK                    7
DHCPNAK                    0
DHCPREQTIMES              0
DHCPREQSUCTIMES          0
DISCOVER-PROCESS-ERROR 0
LEASE-IN-PINGSTATE         0
NO-LEASE-RESOURCE        0
SERVERID-NO-MATCH         0
-----------------------------------------
recv                          0
send                         0
```

显示结果的各字段含义阐述如下

Address pools	地址池个数
Automatic bindings	自动地址绑定的数目。
Manual bindings	手工地址绑定的数目。
Expired bindings	过期地址绑定的数目。
Malformed messages	DHCP 接受到不正常报文的数目。
Message Received or Sent	DHCP 服务器接收和发送每种报文的数目。
DHCPREQTIMES	DHCP 收到的请求报文总的数目
DHCPREQSUCTIMES	DHCP 收到的请求被成功处理的报文数目
DISCOVER-PROCESS-ERROR	DHCP 收到的 DISCOVER 报文处理出错的数目
LEASE-IN-PINGSTATE	当前处在 PING 检测状态的租约数目

recv	收到的 DISCOVER，REQUEST，INFORM 报文汇总数目
send	本应发送的响应报文数目统计

【检验方法】 -

【提示信息】 -

【常见错误】 -

1.58 show ip dhcp socket

显示 DHCP 服务器用到的接字索引

show ip dhcp socket

【参数说明】

参数	描述
-	-

【命令模式】 特权用户模式

【缺省级别】 14

【使用指导】 -

【配置举例】 1：显示 DHCP 服务器的用的套接字索引

```
ruijie#show ip dhcp socket
dhcp socket = 47.
```

【提示信息】 -

【平台说明】 -

1.59 update arp

要让 DHCP 分配地址时添加可信 ARP，用 DHCP 地址池配置命令 update arp

update arp

no 形式表示 DHCP 分配地址时不添加可信 ARP

no update arp

恢复默认值

defaut update arp

【参数说明】

参数	描述
-	-

【缺省配置】 缺省情况下 DHCP 分配地址时不添加可信 ARP

【命令模式】 DHCP 地址池配置模式

【缺省级别】 14

【使用指导】 该命令属于 Server 配置。地址池配置 **update arp** 后，DHCP 从地址池分配地址时会添加可信 ARP，可信 ARP 的优先级比动态 ARP 的优先级高，不会被动态 ARP 覆盖。

【配置举例】 1：让 DHCP 分配地址时添加可信 ARP

```
Ruijie(dhcp-config)# update arp
```

【检验方法】 通过 **show run** 可见配置成功

【提示信息】 -

【常见错误】 -

2 DNS

2.1 clear host

清除动态主机名缓冲表。

clear host [* | *host-name*]

【参数说明】

参数	描述
host-name	可以删除某个指定的动态域名缓冲。
*	表示删除所有的动态域名缓冲

【命令模式】 特权用户模式

【缺省级别】 14

【使用指导】 主机名缓冲表中的映射记录，有两个来源：

- 通过 **ip host** 静态配置；
- 通过 DNS 动态学习。执行该命令，会删除当前通过 DNS 动态学习到的主机名记录。

【配置举例】 1：以下配置中，会删除主机名-IP 地址缓冲表中所有动态学习到的映射记录。

```
Ruijie(config)#clear host *
```

【提示信息】 -

【平台说明】 -

2.2 ip domain-lookup

启动 DNS 进行域名解析。

ip domain-lookup

关闭 DNS 域名解析功能。

no ip domain-lookup

【参数说明】

参数	描述
-	-

【缺省配置】 缺省情况为打开 DNS 域名解析功能

【命令模式】 全局配置模式

【缺省级别】 14

【使用指导】 该命令为打开 DNS 域名解析功能的开关，执行该命令，则启动 DNS 进行域名解析。

【配置举例】 1：关闭 DNS 域名解析功能。

```
Ruijie(config)# no ip domain-lookup
```

【检验方法】 通过 **show run** 查看配置，不存在 **ip domain-lookup** 配置。

【提示信息】 -

【常见错误】 -

【平台说明】 -

2.3 ip host

手工配置主机名和 IP 地址的映射。
ip host *host-name ip-address*

删除主机列表。
no ip host *host-name ip-address*

【参数说明】

参数	描述
host-name	设备的主机名
ip-address	设备的 IP 地址

【缺省配置】 -

【命令模式】 全局配置模式

【缺省级别】 14

【使用指导】

【配置举例】 1：静态配置 www .test.com 域名为 192.168.5.243

```
Ruijie(config)# ip host www.test.com 192.168.5.243
```

【检验方法】 **show run** 查看配置，存在所配置的命令
show hosts 查看当前域名和 IP 对应关系，存在所配置的域名和 IP 对应表项

【提示信息】 -

【常见错误】 -

【平台说明】 -

2.4 ip name-server

配置域名服务器的 IP 地址。
ip name-server [**oob**] { *ip-address* | *ipv6-address* }

删除配置的域名服务器。
no ip name-server [**oob**] { *ip-address* | *ipv6-address* }

【参数说明】

参数	描述
oob	mgmt 口
ip-address	域名服务器的 IP 地址
ipv6-address	域名服务器的 IPv6 地址

【缺省配置】 缺省没有配置域名服务器

【命令模式】 全局配置模式

【缺省级别】 14

【使用指导】 只有配置了域名服务器才能进行动态域名解析。
添加 DNS Server 的 IP 地址。每次执行这条命令，设备都会添加一个 DNS Server。当无法从第一个 Server 获取到域名时，设备会尝试向后续几个 Server 发送 DNS 请求，直到正确收到回应为止。
系统最多支持 6 个服务器。删除 DNS Server 时，如果您指定了 *ip-address* 参数，则只删除指定的服务器，否则删除所有的 DNS 服务器地址。

【配置举例】 -

【检验方法】 **show run** 查看配置，存在所配置的命令

【提示信息】 -

【常见错误】 -

【平台说明】 NBR6205-E、NBR6135-E、NBR6210-E、NBR6215-E 支持 MGMT 口；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 MGMT 口。

2.5 show hosts

显示 DNS 的配置信息。

show hosts [*hostname*]

【参数说明】

参数	描述
hostname	查看指定域名。缺省情况查看所有的域名信息

【命令模式】 全局模式

【缺省级别】 14

【使用指导】 显示 DNS 的相关配置信息

【配置举例】 1：查看所有域名信息

```
Ruijie# show hosts
Name servers are:
192.168.5.134 static

Host                type          Address               TTL(sec)
switch              static        192.168.5.243          ---
www.ruijie.com    dynamic       192.168.5.123          126
```

字段解释：

字段	说明
Name servers	域名服务器
Host	域名
type	解析类型：静态解析或者动态解析
Address	域名对应的 IP
TTL	域名/IP 对应表项存活时间

【提示信息】 -

【平台说明】 -

3 DDNS

命令	作用
ddns service [domain] username password [interface]	设置动态域名账号密码并绑定接口。
show ddns	查看动态域名账号状态。

3.1 ddns service [domain] username password [interface]

设置动态域名账号密码并绑定接口。

ddns service *service* [**domain** *domain*] **username** *username* **password** *password* **service** *service* [**interface** *interface-name*]

删除花生壳动态域名

no ddns service *oray* **username** *username*

删除 3322 动态域名

no ddns service *3322* **domain** *domain*

【参数说明】

参数	描述
service *service*	动态域名平台： 3322: 3322 动态域名 oray: 花生壳动态域名
domain *domain*	3322 域名（仅在 service 选择 3322 时需要输入）
username *username*	动态域名账号
password *password*	密码
interface *interface-name*	设备外网接口(支持物理口和拨号口)

【缺省配置】 无配置动态域名账号密码。

【命令模式】 全局模式

【缺省级别】 14

【使用指导】 配置动态域名账号密码后，设备会自动同动态域名服务器进行连接。如果有设置绑定设备接口，会将接口 IP 和账号的域名绑定。

【配置举例】 1：配置花生壳动态域名账号。

```
Ruijie#configure terminal
```

```
Ruijie (config)# ddns service oray username ruijie password ruijie interface GigabitEthernet 0/7
```

2：配置 3322 动态域名账号。

```
Ruijie#configure terminal
Ruijie (config)# ddns service 3322 domain ruijie.f3322.net username ruijie password ruijie interface GigabitEthernet 0/7
```

【检验方法】 1：使用 **show ddns** 命令，可以查看动态域名账号密码及连接设备的接口和状态。

【提示信息】 -

【常见错误】 1：动态账号密码错误。
2：设备未正确配置 DNS，无法正确解析出动态域名服务器 IP。
3：动态域名服务器不可达。

【平台说明】 -

3.2 show ddns

查看动态域名账号状态。

show ddns

【参数说明】

参数	描述
-	-

【命令模式】 特权模式、全局模式

【缺省级别】 14

【使用指导】 使用该命令可以查看设备上的动态账号状态。

【配置举例】 1：查看设备上的动态域名账号状态

```
Ruijie#show ddns
------------------[0]-------------------
status: Success
code: none
service: oray
username: hy84119
```

```
password: hy123456

domain: 21p7o78186.imwork.net

interface: Gi0/7

------------------[1]------------------

status: Success

code: good

service: 3322

username: hy84111

password: hy123456

domain: hy84111.f3322.net

interface:
```

字段解释：

字段	说明
state	连接状态
code	状态码： none 无 good 域名 IP 更新成功 nochg 域名 IP 无变化 badauth 认证失败 badsys 域名错误(不是动态域名) badagent 客户端被拒绝 notfqdn 域名错误(没有域名参数) nohost 域名错误(域名不存在) !donator 无法离线 !yours 域名错误(不是该用户所有) !active 域名被关闭 abuse 域名被禁止 dnserr DNS 服务器错误 interror 服务器内部错误 connerr 连接错误
service	动态域名服务平台
username	账号
password	密码
domain	账号当前使用的域名
interface	绑定的设备接口

【提示信息】 -

【平台说明】 -

4 NTP

4.1 no ntp

关闭 NTP 同步服务，停止与时间服务器的同步，清除 ntp 的所有配置信息。

no ntp

【参数说明】

参数	描述
-	-

【缺省配置】 缺省情况下 NTP 服务是关闭的。

【命令模式】 全局配置模式

【缺省级别】 14

【使用指导】 在缺省情况下，NTP 功能是关闭的，但只要配置了 NTP 服务器或 NTP 安全识别机制，NTP 功能就会被打开。

【配置举例】 1：关闭 NTP 服务。

```
Ruijie(config)# no ntp
```

【检验方法】 **show run** 查看是否还存在 NTP 配置

【提示信息】 -

【常见错误】 -

【平台说明】 -

4.2 ntp access-group

配置 NTP 服务的访问控制权限。

ntp access-group { **peer** | **serve** | **serve-only** | **query-only** } *access-list-number* | *access-list-name*

取消设置的访问控制权限。

no ntp access-group {**peer** | **serve** | **serve-only** | **query-only**} *access-list-number* | *access-list-name*

【参数说明】

参数	描述
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。
access-list-name	IP 访问控制列表名。

【缺省配置】 缺省情况下未配置任何 NTP 访问控制规则。

【命令模式】 全局配置模式

【缺省级别】 14

【使用指导】 设置对本地设备 NTP 服务的访问控制权限。这里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。

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**。

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。

⚠ 目前系统暂未支持控制查询功能。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。

【配置举例】 1：配置只允许 192.168.1.1 的设备对本地设备进行时间请求

```
Ruijie(config)# access-list 1 permit 192.168.1.1
Ruijie(config)# ntp access-group serve-only 1
```

【检验方法】 -

【提示信息】 -

【常见错误】 -

【平台说明】 -

4.3 ntp authenticate

配置 NTP 服务使用 NTP 全局认证机制。

ntp authenticate

关闭全局安全识别机制。

no ntp authenticate

【参数说明】

参数	描述
-	-

【缺省配置】 缺省情况下 NTP 全局认证机制是关闭的。

【命令模式】 全局配置模式

【缺省级别】 14

【使用指导】 如果未使用全局安全识别机制，则不对同步通信进行加密处理。打开全局安全识别机制，同时完成其他的全局密钥配置，才可能发起与服务器的加密通信。

验证的标准是通过 **ntp authentication-key**、**ntp trusted-key** 指定的信任密钥。

【配置举例】 1：在配置了相应的全局认证密钥并将其指定为全局信任密钥后，打开认证机制。

```
Ruijie(config)# ntp authentication-key 6 md5 wooooop
Ruijie(config)# ntp trusted-key 6
Ruijie(config)# ntp authenticate
```

【检验方法】 -

【提示信息】 -

【常见错误】 -

【平台说明】 -

4.4 ntp authentication-key

为 NTP 服务配置一个全局 NTP 认证密钥。

ntp authentication-key *key-id* **md5** *key-string* [*enc-type*]

取消全局 NTP 认证密钥。

no ntp authentication-key *key-id*

【参数说明】

参数	描述
key-id	密钥 ID；取值范围 1～4294967295。
key-string	密钥字符串。
enc-type	（可选）该密钥是否是加密的，0 表示无加密，7 表示简单加密。默认是无

	加密。

【缺省配置】 缺省没有配置认证密钥。

【命令模式】 全局配置模式

【缺省级别】 14

【使用指导】 配置全局认证密钥，并采用 md5 进行加密，每个密钥有一个唯一的 key-id 标识，客户可以用 **ntp trusted-key** 将该 key-id 对应的密钥设置为全局信任密钥。
密钥上限为 1024 个，但是每个服务器仅仅支持一个密钥。

【配置举例】 1：配置一个 ID 为 6 的认证密钥：

```
Ruijie(config)# ntp authentication-key 6 md5 wooooop
```

【检验方法】 -

【提示信息】 -

【常见错误】 -

【平台说明】 -

4.5 ntp disable

关闭对应接口接收 NTP 报文的功能。
ntp disable

【参数说明】

参数	描述
-	-

【缺省配置】 缺省情况下接口都可以接受 NTP 报文。

【命令模式】 接口配置模式

【缺省级别】 14

【使用指导】 在缺省情况下，任意接口上接受的 NTP 报文都可以提供给客户端进行时钟调整，通过设置这个功能，可以屏蔽对应接口上收到的 NTP 报文。

⚠ 能够进行该项配置的接口肯定是能够配置 IP 收发报文的接口，在其他接口上没有该命令。

【配置举例】 1：关闭接口接收 NTP 报文：

```
Ruijie(config-if)# no ntp disable
```

【检验方法】 -

【提示信息】 -

【常见错误】 -

【平台说明】 -

4.6 ntp master

设置本地时钟作为 NTP 主时钟（本地时钟参考源可靠），为其它设备提供同步时间。

ntp master [*stratum*]

取消 NTP 主时钟设置。

no ntp master

【参数说明】

参数	描述
stratum	（可选）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。

【缺省配置】 缺省没有配置 NTP 主时钟功能。

【命令模式】 全局配置模式

【缺省级别】 14

【使用指导】 在通常情况下，本地系统都会直接或间接地与外部的时钟源进行同步。但若由于网络连接故障等原因而导致本地系统无法与外部时钟源同步时，可以通过该命令设置本地时钟参考源可靠，为其他设备提供同步时间。一旦进行了此设置，系统便不会与比其时钟层数数值更高的时钟源进行同步。

⚠ 使用此命令时必须特别小心。将本地时钟设置为主时钟（尤其是指定了较低的时钟层数值时）很有可能将真正的有效时钟源覆盖。如果对同一网络中的多个设备都使用了该命令，则可能由于设备之间的时钟差异导致网络的时钟同步不稳定。

⚠ 使用该命令前若系统从未与外部时钟源同步过，则有可能需要手动校准系统时钟以保证其不会有过大的偏差。

【配置举例】 1：设置本地时钟参考源可靠，并设置其时钟层数为 12。

```
Ruijie(config)# ntp master 12
```

【检验方法】 1：使用 **show ntp status** 命令查看 NTP 相关配置。

【提示信息】 -

【常见错误】 -

【平台说明】 -

4.7 ntp server

为 NTP 客户端指定一个 NTP 服务器。

ntp server [oob] { *ip-addr* | *domain* | **ip** *domain* | **ipv6** *domain* } [**version** *version*] [**source** *if-name*] [**key** *keyid*] [**prefer**]

删除指定的 NTP 服务器。

no ntp server *ip-addr*

【参数说明】

参数	描述
oob	（可选）指定从 MGMT 接入 NTP 服务器，默认情况不走 MGMT。
ip-addr	设置 NTP 服务器的 IP 地址；
domain	设置 NTP 服务器的域名；
version	（可选）指定 NTP 的版本（1-3），默认采用 NTPv3 版本；
if-name	（可选）指定发送 NTP 报文的源接口（三层接口），默认情况按设备路由；
keyid	（可选）指定与对应服务器通信采用的加密密钥，默认情况不加密。取值范围 1～4294967295。
prefer	（可选）指定对应的服务器为系统 Prefer 服务器，默认情况不是 prefer 服务器

【缺省配置】 缺省没有配置 NTP 服务器。

【命令模式】 全局配置模式。

【缺省级别】 14

【使用指导】 目前锐捷 RGOS 系统仅支持客户端没有服务器端，支持的同步服务器上限为 20 个。

要进行与服务器的加密通信，首先需要设置全局加密密钥以及全局信任密钥，然后指定对应的密钥为服务器信任密钥，才可以发起与服务器的加密通信，要完成与服务器的加密通信要求服务器有相同的全局加密密钥与全局信任密钥

在相同情况（精确度）下，优先选择 prefer 时钟进行同步

配置 NTP 发送报文的源接口的时候应该注意一下 ,配置的接口必须为配置了 IP 的并可以和对应 NTP 服务器通

信的接口。

【配置举例】 1：配置网络上的设备为 NTP server。

```
Ruijie(config)# ntp server 192.168.210.222  //IPv4 配置
```

【检验方法】 -

【提示信息】 -

【常见错误】 -

【平台说明】 NBR6205-E、NBR6135-E、NBR6210-E、NBR6215-E 支持 MGMT 口；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 MGMT 口。

4.8 ntp trusted-key

将一个 ID 对应的密钥配置为全局信任密钥。
ntp trusted-key *key-id*

删除 ID 对应的全局信任密钥。
no ntp trusted-key *key-id*

【参数说明】

参数	描述
key-id	全局信任密钥 ID。取值范围 1～4294967295。

【缺省配置】 默认情况下没有信任密钥。

【命令模式】 全局配置模式

【缺省级别】 14

【使用指导】 在 NTP 通讯双方必须采用相同的信任密钥，通过 ID 来查找密钥，而密钥本身是不传输的，以提高安全性。

【配置举例】 1：配置一个认证密钥，并把此密钥设置为对应服务器信任密钥。

```
Ruijie(config)# ntp authentication-key 6 md5 wooooop
Ruijie(config)# ntp trusted-key 6
Ruijie(config)# ntp server 192.168.210.222 key 6
```

【检验方法】 -

【提示信息】 -

【常见错误】 -

【平台说明】 -

4.9 ntp update-calendar

设置 NTP 客户端定期使用从外部时钟源同步得来的时钟值更新设备的硬件时钟。
ntp update-calendar

取消定期更新硬件时钟功能。
no ntp update-calendar

【参数说明】

参数	描述
-	-

【缺省配置】 默认未配置定期更新硬件时钟功能。

【命令模式】 全局配置模式

【缺省级别】 14

【使用指导】 使用此功能可以让 NTP 客户端定期使用从外部时钟源同步得来的时钟值更新设备的硬件时钟。设备的硬件时钟即使在设备关机或在设备复位的情况下仍然能够继续走动。
在缺省情况下没有配置 NTP 更新硬件时钟。配置之后，NTP 客户端会在每次与外部时钟源同步成功时也同时更新设备的硬件时钟。

【配置举例】 1：配置 NTP 定期更新硬件时钟

```
Ruijie(config)# ntp update-calendar
```

【检验方法】 -

【提示信息】 -

【常见错误】 -

【平台说明】 -

4.10 show ntp server

显示 NTP 服务器信息。

show ntp server

【参数说明】

参数	描述
-	-

【命令模式】 特权用户模式、全局配置模式、接口配置模式、VLAN 配置模式。

【缺省级别】 14

【使用指导】 如果有配置 NTP 服务，则显示当前的 NTP 服务器信息，否则该命令不会打印任何信息。

【配置举例】 1：显示当前系统的 NTP 服务器信息

```
Ruijie# show ntp server
ntp-server                              source    keyid       prefer  version
--------------------------------------  --------  ----------  ------  -------
10::2                                   None      None        FALSE   3
192.168.210.222                         None      None        FALSE   3
```

字段解释：

字段	说明
ntp-server	表示 NTP 服务器的 IP 地址或域名
source	表示 NTP 服务器的源端口
keyid	表示与对应服务器通信是否采用的加密密钥
prefer	表示对应的服务器是否为系统 prefer 服务器
version	表示 NTP 的版本（1-3）

【提示信息】 -

【平台说明】 -

4.11 show ntp status

显示 NTP 信息。

show ntp status

【参数说明】

参数	描述
-	-

【命令模式】 特权用户模式、全局配置模式、接口配置模式、VLAN 配置模式。

【缺省级别】 14

【使用指导】 如果系统的 NTP 服务打开，则显示当前的 NTP 信息，在第一次添加同步服务器之前该命令不会打印任何信息。

【配置举例】 1：显示当前系统的 NTP 信息

```
Ruijie# show ntp status
Clock is synchronized, stratum 8, reference is 127.127.1.1
nominal freq is 250.0000 Hz, actual freq is 250.0000 Hz, precision is 2**24
reference time is D4BD819B.433892EE (01:27:55.000 UTC )
clock offset is 0.00000 sec, root delay is 0.00000 sec
root dispersion is 0.00002 msec, peer dispersion is 0.00002 msec
```

字段解释：

字段	说明
stratum	表示当前时钟等级；
reference	表示同步服务器的地址；
freq	表示当前系统时钟频率；
precision	表示当前系统时钟精度；
reference time	表示同步服务器参考时钟的 UTC 时间值；
clock offset	表示当前时钟偏移；
root delay	表示当前时钟延迟；
root dispersion	表示顶级服务器时间精度；
peer dispersion	表示同步服务器时间精度。

【提示信息】 -

【平台说明】 -

5 SNTP

5.1 show sntp

显示 SNTP 的相关参数。

show sntp

【参数说明】

参数	描述
-	-

【命令模式】 特权用户模式、全局配置模式、接口配置模式

【缺省级别】 14

【使用指导】 -

【配置举例】 1：查看 SNTP 的相关参数。

```
Ruijie# show  sntp
SNTP state             : Enable
SNTP server            : 192.168.4.12
SNTP sync interval   : 60
Time zone               : +8
```

字段解释：

字段	说明
state	表示 sntp 开启状态
server	表示时间同步服务器
sync interval	表示时间同步间隔
Time zone	当前时区
SNTP server source	表示时间同步报文的填充的源 IP 地址

【提示信息】 -

【平台说明】 -

1.60 sntp enable

设置打开 SNTP 功能。

sntp enable

将该设置恢复为缺省值—Disable。

no sntp enable

【参数说明】

参数	描述
-	-

【缺省配置】 缺省 SNTP 状态是 Disable

【命令模式】 全局配置模式

【缺省级别】 14

【使用指导】 -

【配置举例】 1：开启 SNTP 功能

```
Ruijie(config)# sntp enable
```

【检验方法】 1：使用 **show sntp** 命令查看 SNTP 相关参数。

【提示信息】 -

【常见错误】 -

【平台说明】 -

5.2 sntp interval

设置 SNTP Client 需要定时和 NTP/SNTP Server 同步时钟的时间间隔。

sntp interval *seconds*

取消 SNTP 同步间隔设置，恢复到缺省的同步时间间隔。

no sntp interval

【参数说明】

参数	描述
seconds	定时同步的间隔，单位为秒。取值范围 60～65535。

【缺省配置】 1800s

【命令模式】 全局配置模式

【缺省级别】 14

【使用指导】 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】 1：配置 SNTP 每小时同步一次时间

```
Ruijie(config)# sntp interval 3600
```

【检验方法】 1：使用 **show sntp** 命令查看 SNTP 相关参数。

【提示信息】 -

【常见错误】 -

【平台说明】 -

5.3 sntp server

设置 SNTP Server。

sntp server [**oob**] { *ip- address* | *domain* } [**source** *source-ip-address*]

删除指定的 SNTP Server

no sntp server

【参数说明】

参数	描述
oob	（可选）指定从 MGMT 接入 SNTP 服务器，默认情况不走 MGMT
ip-address	SNTP 服务器的 IP 地址
domain	SNTP 服务器的域名
source-ip-address	（可选）SNTP 指定源 IP 地址

【缺省配置】 缺省没有设置任何 SNTP 服务器

【命令模式】 全局配置模式

【缺省级别】 14

【使用指导】 由于 SNTP 协议和 NTP 完全兼容，所以设置的 SNTP Server 完全可以配置成 internet 上公用的 NTP Server。

【配置举例】 1：配置网络上的 SNTP 服务器

```
Ruijie(config)# sntp server 192.168.4.12
```

【检验方法】 1：使用 **show sntp** 命令查看 SNTP 相关参数。

【提示信息】 -

【常见错误】 -

【平台说明】 NBR6205-E、NBR6135-E、NBR6210-E、NBR6215-E 支持 MGMT 口；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 MGMT 口。

6 DNS Proxy

6.1 blacklist domain-ip

增加 dns 防攻击黑名单
blacklist domain-ip *start-ip [end-ip]*

删除 dns 防攻击黑名单
no blacklist domain-ip *start-ip [end-ip]*

【参数说明】

参数	描述
start-ip	黑名单的起始 IP
end-ip	黑名单的结束 IP

【缺省配置】 缺省配置防劫持黑名单为空。

【命令模式】 dns-proxy 模式

【缺省级别】 14

【使用指导】 dns 黑名单会屏幕符合规则的 IP 或域名，该命令可以检查 DNS 应答报文里的域名 IP 是否合法，用于防止互联网上一些黑客冒充 dns 应答而把用户引导到一些非法 IP。最大可配置容量 10 条。

【配置举例】 1：dns-proxy 模式下配置把域名 IP 网段 1.1.1.1-1.1.1.100 加入防劫持黑名单。

```
Ruijie(config-dns-proxy)# blacklist domain-ip 1.1.1.1 1.1.1.100
```

【检验方法】 1：使用 **show running-config** 命令，可以查看是否配置成功。

【提示信息】 -

【常见错误】 -

【平台说明】 -

6.2 clear dns-proxy statistics

特权模式下重置 dns-proxy 的统计信息。
clear dns-proxy statistics

【参数说明】

参数	描述
-	-

【命令模式】 特权模式

【缺省级别】 14

【使用指导】 重置 dns-proxy 的统计信息。

【配置举例】 1：在特权模式下重置 dns-proxy 的统计信息。

```
Ruijie# clear dns-proxy statistics
```

【提示信息】 1：重置 dns-proxy 的统计信息。

```
Ruijie# clear dns-proxy statistics
```

【平台说明】 -

6.3 debug dns-proxy

打开 DNS proxy 事件的调试开关。

debug dns-proxy

关闭 DNS proxy 事件的调试开关。

no debug dns-proxy

【参数说明】

参数	描述
-	-

【缺省配置】 关闭调试开关。

【命令模式】 特权模式

【缺省级别】 14

【使用指导】 调试信息包括 DNS proxy 运行过程中各种事件的调试信息：

- DNS proxy 变化事件
- 协议状态机变化时发生的各种处理事件
- 收到各种协议报文时的处理
- 接口相关的事件处理

打开此调试开关，几乎可以显示 DNS proxy 所有事件和处理，常用于跟踪 DNS proxy 工作过程。

查看处理失败时的调试信息，有助于故障诊断和定位。

【配置举例】 1：打开 DNS proxy 事件的调试开关。

```
Ruijie# debug dns-proxy
```

2：关闭 DNS proxy 事件的调试开关。

```
Ruijie# no debug dns-proxy
```

【调试信息】 1：出口带宽变动

调试信息	dns-proxy recv bw change: ifindex = 3, bw = 50
信息解释	出口带宽变动。
产生原因	出口带宽变动。
处理建议	-

2：配置 blacklist domain-ip end 地址比 start 地址小

调试信息	%warning: The end_ip must greater than the start_ip, set failed
信息解释	配置 blacklist domain-ip end 地址要大于 start 地址
产生原因	配置 blacklist domain-ip end 地址比 start 地址小
处理建议	-

【提示信息】 -

【平台说明】 -

6.4 dns-proxy

全局模式下进入 dns-proxy 配置模式

dns-proxy

【参数说明】

参数	描述
-	-

【缺省配置】 无

【命令模式】 全局模式

【缺省级别】 14

【使用指导】 要配置 dns-proxy 的功能，需先进入 dns-proxy 配置模式。

【配置举例】 1：全局模式下进入 dns-proxy。

```
Ruijie(config)#dns-proxy
Ruijie(config-dns-proxy)#exit
Ruijie(config)#
```

【检验方法】 1：查看是否能够进入 dns-proxy 配置模式。

【提示信息】 -

【常见错误】 -

【平台说明】 -

6.5 dns-proxy enable

配置开启 dns-proxy 功能
dns-proxy enable

配置关闭 dns-proxy 功能
no dns-proxy enable

【参数说明】

参数	描述
-	-

【缺省配置】 缺省是关闭的。

【命令模式】 接口模式

【缺省级别】 14

【使用指导】 某三层口要开启 dns-proxy 功能，要在接口上开启 dns-proxy enable。dns-proxy 对该三层口是 WAN 还是 LAN 口并无限制，但一般情况下 dns-proxy 提供内网对外网的服务，用户在 LAN 口上配置 **dns-proxy enable**，在 WAN 口配置 **ip name-server**。

【配置举例】 1：配置在 gi0/1 开启 dns-proxy 功能。

```
Ruijie(config)#int gi0/1
Ruijie(config-if-GigabitEthernet 0/1)#dns-proxy enable
```

【检验方法】 1：使用 **show running-config** 命令，可以查看是否配置成功。

【提示信息】 -

【常见错误】 1：**dns-proxy enable** 要配置在三层接口模式下。

【平台说明】 -

6.6 ip name-server

配置域名服务器的 IP 地址
ip name-server *ip-address* [**track** *id*]

删除域名服务器的 IP 地址
no ip name-server *ip-address* [**track** *id*]

【参数说明】

参数	描述
ip-address	指定的 IP 地址
id	关联的 track ID

【缺省配置】 缺省配置为空

【命令模式】 接口模式

【缺省级别】 14

【使用指导】 WAN 口需要配置 DNS 服务器才能使用 dns-proxy 功能，一般情况下运营商会给出一个主和一个备用 DNS 服务器，可以把这两个 DNS 服务器都配置在接口上，dns-proxy 自动在一个失效时启用另一个，一个接口能最多能配置 4 个域名服务器。
可以配置与 track 联动，通过 track 来跟踪到该 dns server 的链路是否可达，如果没有配置 track 联动，默认认为在接口 up 的情况下，链路是可达的。

【配置举例】 1：gi0/1 是电信出口，在 gi0/1 口上配置两个电信的 dns 服务器。

```
Ruijie(config)#int gi0/1
Ruijie(config-if-GigabitEthernet 0/1)#ip name-server 218.85.157.99
Ruijie(config-if-GigabitEthernet 0/1)#ip name-server 218.85.152.99 track 1
```

【检验方法】 1：使用 **show running-config** 命令，可以查看是否配置成功。

【提示信息】 -

【常见错误】 -

【平台说明】 -

6.7 load-balance

配置负载均衡策略
load-balance {**load | bandwidth**}

还原负载均衡策略
no load-balance

【参数说明】

参数	描述
load	带宽利用率策略
bandwidth	带宽策略

【缺省配置】 缺省配置为 **bandwidth** 策略。

【命令模式】 dns-proxy 模式

【缺省级别】 14

【使用指导】 该用于切换 dns-proxy 的负载均稀策略，默认情况下负载均衡策略为带宽策略，用户可以手动切换为带宽利用率策略。

【配置举例】 1：dns-proxy 模式下配置 dns-proxy 的负载均衡策略为带宽利用率策略。

```
Ruijie(config-dns-proxy)#load-balance load
```

2：dns-proxy 模式下配置 dns-proxy 的负载均衡策略为带宽策略。

```
Ruijie(config-dns-proxy)#load-balance bandwidth
```

【检验方法】 1：使用 **show running-config** 命令，可以查看是否配置成功。

【提示信息】 -

【常见错误】 1：**load-balance** 要在 dns-proxy 模式下配置。

【平台说明】 -

6.8 show dns-proxy configure

特权模式下查看 dns-proxy 的全部配置信息。

show dns-proxy configure

【参数说明】

参数	描述
-	-

【命令模式】 特权模式、全局模式、接口模式

【缺省级别】 14

【使用指导】 显示 dns-proxy 的全部配置信息。

【配置举例】 1：在特权模式下查看 dns-proxy 的全部配置信息。

```
Ruijie(config)# show dns-proxy configure
>dns-proxy load balance:bandwidth
------------------------------------------------------------------------------
>dns-proxy whitelist
------------------------------------------------------------------------------
Type:source-ip
Source-ip:192.168.1.1 192.168.1.10

Type:name-server
Nameserver:8.8.8.8

>Dns-proxy blacklist
--------------------------------------------------------------
Start-ip         End-ip
---------------  ---------------
1.1.1.1          1.1.1.10
```

字段解释：

字段	说明
bandwidth	带宽策略
whitelist	白名单
source-ip	源 IP 地址
name-server	DNS 服务器
blacklist	防劫持

【提示信息】 1：查看 dns-proxy 的负载均衡模式。

```
Ruijie(config)# show dns-proxy configure
>dns-proxy load balance:bandwidth
```

【平台说明】 -

6.9 show dns-proxy configure blacklist

特权模式下查看 dns-proxy 的防劫持配置信息。

show dns-proxy configure blacklist

【参数说明】

参数	描述
-	-

【命令模式】 特权模式、全局模式、接口模式

【缺省级别】 14

【使用指导】 显示 dns-proxy 的防劫持配置信息。

【配置举例】 1：在特权模式下查看 dns-proxy 的防劫持配置信息。

```
Ruijie(config)#show dns-proxy configure blacklist
>Dns-proxy blacklist
------------------------------------------------------------
Start-ip         End-ip
---------------  ---------------
1.1.1.1          1.1.1.10
```

字段解释：

字段	说明
blacklist	防劫持
Start-ip	启始地址
End-ip	结束地址

【提示信息】 1：显示 dns-proxy 的防劫持配置信息。

```
Ruijie(config)#show dns-proxy configure blacklist
>Dns-proxy blacklist
------------------------------------------------------------
Start-ip         End-ip
---------------  ---------------
1.1.1.1          1.1.1.10
```

【平台说明】 -

6.10 show dns-proxy configure whitelist

特权模式下查看 dns-proxy 的白名单配置信息。

show dns-proxy configure whitelist

【参数说明】

参数	描述
-	-

【命令模式】 特权模式、全局模式、接口模式

【缺省级别】 14

【使用指导】 显示 dns-proxy 的白名单配置信息。

【配置举例】 1：在特权模式下查看 dns-proxy 的白名单配置信息。

```
Ruijie(config)#show dns-proxy configure whitelist
>dns-proxy whitelist
------------------------------------------------------------------


Type:source-ip
Source-ip:192.168.1.1  192.168.1.10

Type:name-server
Nameserver:8.8.8.8
```

字段解释：

字段	说明
whitelist	白名单
source-ip	源 IP 地址
name-server	DNS 服务器

【提示信息】 1：显示 dns-proxy 的白名单配置信息。

```
Ruijie(config)#show dns-proxy configure whitelist
>dns-proxy whitelist
------------------------------------------------------------------
Type: source-ip
Host-name: 192.168.1.1  192.168.1.10
```

【平台说明】 -

6.11 show dns-proxy name-server

特权模式下查看 dns-proxy 的域名服务器配置信息。

show dns-proxy name-server

【参数说明】

参数	描述
-	-

【命令模式】 特权模式、全局模式、接口模式

【缺省级别】 14

【使用指导】 显示 dns-proxy 的域名服务器配置信息。

【配置举例】 1：在特权模式下查看 dns-proxy 的域名服务器配置信息。

```
Ruijie(config)#show dns-proxy name-server
>Dns-proxy name-server
------------------------------------------------------------------------
Interface                 Dns-server       TrackId  State  Description
--------------------------  ---------------  -------  -----  -----------
GigabitEthernet 0/0         192.168.58.110   1        down   static
```

字段解释：

字段	说明
Interface	接口信息
dns-server	域名服务器
trackid	track 线路
state	状态

【提示信息】 1：显示 dns-proxy 的域名服务器配置信息。

```
Ruijie(config)#show dns-proxy name-server
>Dns-proxy name-server
------------------------------------------------------------------------
Interface                 Dns-server       TrackId  State  Description
--------------------------  ---------------  -------  -----  -----------
GigabitEthernet 0/0         192.168.58.110   1        down   static
```

【平台说明】 -

6.12 show dns-proxy statistics

特权模式下查看 dns-proxy 的统计信息。

show dns-proxy statistics

【参数说明】

参数	描述
-	-

【命令模式】 特权模式、全局模式、接口模式

【缺省级别】 14

【使用指导】 显示 dns-proxy 的统计信息。

【配置举例】 1：在特权模式下查看 dns-proxy 的统计信息。

```
Ruijie# show dns-proxy statistics
>recv dns request counts:494
>send dns request counts:463
>recv dns reply counts:493
>send dns reply counts:473
>hit the whitelist counts:11
>hit the anti-hijacklist counts:30

>dns proxy load-balance:
interface               dns server        Send Requests
----------------------  ----------------  --------------
GigabitEthernet 0/0     202.101.98.54     110
                        202.101.98.52     50
GigabitEthernet 0/1     202.101.98.54     110
                        202.101.98.52     50
```

字段解释：

字段	说明
recv dns request counts	接收到的 DNS 请求报文统计
send dns request counts	发送出去的 DNS 请求报文统计
recv dns reply counts	接收到的 DNS 应答报文统计
send dns reply counts	发送出去的 DNS 应答报文统计
hit the whitelist counts	命中白名单统计
hit the anti-hijacklist counts	命中防劫持统计

【提示信息】 1：显示 dns-proxy 的统计信息。

```
Ruijie# show dns-proxy statistics
>recv dns request counts:494
>send dns request counts:463
>recv dns reply counts:493
>send dns reply counts:473
>hit the whitelist counts:11
>hit the anti-hijacklist counts:30
```

【平台说明】 -

6.13 whitelist

配置白名单
whitelist {source-ip *start-ip[end-ip]* **| name-server** *ip* **[increase | decrease** *num***]}**

删除白名单
no whitelist {source-ip *start-ip [end-ip]* **| name-server** *ip* **}**

【参数说明】

参数	描述
start-ip	白名单的源 IP 起始 IP
end-ip	白名单的源 IP 结束 IP
ip	dns 服务器
num	配置项上移或下移的行数

【缺省配置】 缺省配置白名单为空。

【命令模式】 dns-proxy 模式

【缺省级别】 14

【使用指导】 该命令可以用于允许符合白名单规则的 dns 报文不受 dns-proxy 拦截，这些规则有：网段，域名，目的 dns 服务品，域名支持最长后缀匹配方式和精确匹配两种方式。
配置项容量最大 10 条，配置项优先级以位于前面的配置优先匹配，可通过 increase 上移或 decrease 下移位置改变优先级。

【配置举例】 例 1：dns-proxy 模式下配置 dns-proxy 把域名服务器 8.8.8.8 加入白名单。

```
Ruijie(config-dns-proxy)#whitelist name-server 8.8.8.8
```

【检验方法】 1：使用 **show running-config** 命令，可以查看是否配置成功。

【提示信息】 -

【常见错误】 -

【平台说明】 -

7 DNS-CACHE

7.1 dns-cache enable

开启 DNS 缓存功能。
dns-cache enable

关闭 DNS 缓存功能
no dns-cache enable

【参数说明】

参数	描述
-	-

【缺省配置】 缺省情况下，DNS 缓存功能打开。

【命令模式】 全局配置模式

【缺省级别】 14

【使用指导】 通过配置本命令启动 DNS 缓存功能。

【配置举例】 1：开启设备的 DNS 缓存功能。

```
Ruijie#config
Ruijie(config)# dns-cache enable
```

2：关闭设备 DNS 缓存功能。

```
Ruijie#config
Ruijie(config)#no dns-cache enable
```

【检验方法】 1：使用 **show run** 命令，可以查看 DNS 缓存功能是启用还是关闭。开启的时候 **show run** 默认不显示

【提示信息】 -

【常见错误】 -

【平台说明】 -

7.2 dns-cache old-time

配置结点缓存时间。
dns-cache old-time *time*

删除结点缓存时间相关配置。
no dns-cache old-time

【参数说明】

参数	描述
time	老化时间，可配置范围 1-600 秒， no 命令恢复默认 300 秒

【缺省配置】 缺省情况下，默认缓存 300 秒。

【命令模式】 全局配置模式

【缺省级别】 14

【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】 1：设备结点缓存时间设置为 500 秒。

```
Ruijie#config
Enter configuration commands, one per line.  End with CNTL/Z.
Ruijie(config)# dns-cache old-time 500
```

【检验方法】 1：使用 **show run** 命令，可以查看结点缓存时间，默认时间不显示。

【提示信息】 -

【常见错误】 -

【平台说明】 -

7.3 dns-cache static domain

配置用户自定义静态缓存
dns-cache static domain *domain* **ip** *"ip1 ip2 …"*

删除相关配置。
no dns-cache static domain *domain*

【参数说明】

参数	描述

domain	域名，最长长度不超过 64 字节
ip	ip，最多可以配置 8 个 ip，ip 之间以空格隔开

【缺省配置】 -

【命令模式】 全局配置模式

【缺省级别】 14

【使用指导】 通过本命令配置用户自定义静态缓存。

【配置举例】 1：用户想让**错误！超链接引用无效。** 。

```
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】 1：使用 **show run** 命令，可以查看静态缓存。

【提示信息】 -

【常见错误】 -

【平台说明】 -

7.4 show dns-cache enable

显示 DNS 缓存功能是否开启。

show dns-cache enable

【参数说明】

参数	描述
-	-

【缺省配置】 无。

【命令模式】 特权模式

【缺省级别】 14

【使用指导】 显示 DNS 缓存功能是否开启。

【配置举例】 显示 DNS 缓存功能是否开启。。

```
Ruijie#show dns-cache enable
```

```
dns-cache is on
```

【提示信息】 -

【平台说明】 -

7.5 show dns-cache state

显示 DNS 缓存功能运行状态。

show dns-cache state

【参数说明】

参数	描述
-	-

【缺省配置】 无。

【命令模式】 特权模式

【缺省级别】 14

【使用指导】 显示 DNS 缓存功能运行状态。

各参数含义说明：

dns-cache-enable： DNS 缓存功能是否开启，on 开启，off 关闭

old-time：节点老化时间，单位为秒

capacity：节点容量

free_node：当前空闲节点容量

dns-question：dns 请求次数

hit-cache：dns 请求命中缓存次数

【配置举例】 显示 DNS 缓存功能是否开启。。

```
Ruijie#show dns state
dns-cache-enable:on
old-time:300
capacity:10000
free_node:10000
dns-question:0
hit-cache:0
Ruijie#
```

【提示信息】 -

【平台说明】 -

8 FTP-Server

8.1 ftp-server enable

启动 FTP 服务器

ftp-server enable

恢复缺省配置

default ftp-server enable

【参数说明】

参数	描述
-	-

【缺省配置】 关闭状态

【命令模式】 全局配置模式

【缺省级别】 14

【使用指导】 当 FTP 服务器启用时，通过 FTP 客户端可以与之连接，并进行文件上传或下载等操作，必须同时配置此命令和 ftp-server topdir 命令才能使 FTP 客户端访问 FTP 服务器上的文件

【配置举例】 1：启动 FTP 服务器并限制客户端仅能访问 syslog 子目录：

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

2：关闭 FTP 服务器：

```
Ruijie(config)# no ftp-server enable
```

【检验方法】 1:**show ftp-server** 可看到配置成功。

【常见错误】 -

【平台说明】 -

8.2 ftp-server login timeout

配置 FTP 会话登陆的有效时长

ftp-server login timeout *time*

使用该命令的 no 形式恢复空闲时限为默认值（2 分钟）
no ftp-server login timeout

恢复缺省配置
default ftp-server login timeout

【参数说明】

参数	描述
time	空闲时限（单位：分钟；范围：1-30）

【缺省配置】 默认时限为 2 分钟

【命令模式】 全局配置模式

【缺省级别】 14

【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。

【配置举例】 1：以下示范如何配置空闲时限为 5 分钟：

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

2：以下示范如何恢复空闲时限为默认值（10 分钟）：

```
Ruijie(config)# no ftp-server login timeout
```

【检验方法】

【提示信息】 -

【常见错误】 -

【平台说明】 -

8.3 ftp-server login times

配置 FTP 会话的登陆有效次数
ftp-server login times *time*

使用该命令的 no 形式恢复为默认值（3 次）
no ftp-server login times

恢复缺省配置

default ftp-server timeout

【参数说明】

参数	描述
time	空闲时限（范围：1-10）

【缺省配置】 默认次数为 3 次

【命令模式】 全局配置模式

【缺省级别】 14

【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。

【配置举例】 1：以下示范如何配置空闲时限为 5 分钟：

```
Ruijie(config)# ftp-server login times 5
```

2：以下示范如何恢复空闲时限为默认值（3 次）：

```
Ruijie(config)# no ftp-server login times
```

【检验方法】

【提示信息】 -

【常见错误】 -

【平台说明】 -

8.4 ftp-server timeout

配置 FTP 会话的空闲时限（Session idle timeout）
ftp-server timeout *time*

使用该命令的 no 形式恢复空闲时限为默认值（10 分钟）
no ftp-server timeout

恢复缺省配置
default ftp-server timeout

【参数说明】

参数	描述
time	空闲时限（单位：分钟；范围：1-3600）

【缺省配置】 默认时限为 10 分钟

【命令模式】 全局配置模式

【缺省级别】 14

【使用指导】 配置 FTP 会话的空闲时限。如果当前会话在指定的时限中没有进行任何操作（会话空闲），FTP 服务器即可认为连接已经失效，而断开与该用户的连接
会话的空闲时间是指在一个 FTP 会话中从上次 FTP 操作完成后到下次 FTP 操作开始之间的时间。服务器在一个 FTP 命令服务完成后（如一个文件全部传输完毕后）从 0 开始计算会话空闲时间；在下个命令到来的时候停止计算会话空闲时间。因此会话空闲时限的配置并不会对某些耗时的文件传输操作带来任何影响

【配置举例】 1：以下示范如何配置空闲时限为 5 分钟：

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

2：以下示范如何恢复空闲时限为默认值（10 分钟）：

```
Ruijie(config)# no ftp-server timeout
```

【检验方法】 1.**show ftp-server** 可看到配置成功

【提示信息】 -

【常见错误】 -

【平台说明】 -

8.5 ftp-server topdir

限制 FTP 客户端能够进行文件读写操作的目录范围
ftp-server topdir *directory*

使用该命令的 no 形式彻底禁止客户端访问 FTP 服务器上任何文件
no ftp-server topdir

恢复缺省配置
default ftp-server topdir

【参数说明】

参数	描述
directory	FTP 客户端能够进行操作的顶层目录

【缺省配置】 默认无顶层目录设置（不允许读写任何目录）

【命令模式】 全局配置模式

【缺省级别】 14

【使用指导】 FTP 服务器顶层目录限定了客户端登录后可以访问的文件目录范围。必须正确指定顶层目录才能让 FTP 客户端访问 FTP 服务器上的文件
若没有配置该命令，FTP 客户端将无法访问服务器上任何文件或目录

【配置举例】 1：以下示范如何启动 FTP 服务器并限制客户端仅能访问 syslog 子目录。

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

2：以下示范如何取消根目录的配置。

```
Ruijie(config)# no ftp-server topdir
```

【检验方法】 1：**show ftp-server** 可看到配置成功

【提示信息】 1：未配置访问目录

```
%FTPSRV-4-USER: Haven't config topdir!
```

2：配置不存在的目录

```
Ruijie(config)#ftp-server topdir ab
folder /ab don't exist!
```

【常见错误】 1.配置非法目录
2.未配置目录

【平台说明】 -

8.6 ftp-server username password

配置 FTP 服务器的登录用户名和密码
ftp-server username *username* **password** [*type*] *password*

使用该命令的 no 形式取消用户名配置
no ftp-server username *username*

恢复缺省配置
default ftp-server username *username*

【参数说明】

参数	描述
username	登录用户名
password	登录密码

【缺省配置】 默认无用户名，无密码

【命令模式】 全局配置模式

【缺省级别】 14

【使用指导】 配置客户端登陆 FTP 服务器时需要提供的用户名。客户端登录时需要同时提供正确的用户名和密码才能登录。
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。FTP 服务器最多只能配置一个用户名
密码必须包含字母或数字，密码前后可以有空格，但将被忽略；密码中间的空格作为密码的一部分。
明文密码的最小长度为 1 个字符、最大长度为 25 个字符；密文密码的最小长度为 4 个字符、最大长度为 52 个字符
FTP 服务器必须配置登录用户名和登录密码以便对客户端连接进行身份验证，密码和用户一一配对。FTP 服务器不支持匿名用户登录，如果清除了用户名配置客户端将无法通过服务器的身份验证

【配置举例】 例 1：以下示范如何配置用户名为 user：

```
Ruijie(config)# ftp-server username user password pass
```

例 2：以下示范如何取消用户名配置：

```
Ruijie(config)# no ftp-server username user
```

【检验方法】 1:**show ftp-server** 可见配置成功

【提示信息】 1:未配置用户名，用户尝试连接

```
%FTPSRV-4-USER: Haven't config username!
```

2.配置用户名过长

```
Ruijie(config)#$sssssssssssssssssssssssssssssssssssssddddddddddddddd
Username abcdefghjijklnn,sssssssssssssssssssssssssssssssssssssddddddddddddddd
is NULL or too long, max length is 64.
```

3：Server 端未配置密码，用户尝试连接

```
%FTPSRV-4-PASS: Haven't config password!
```

4：配置密文密码长度太短

```
Ruijie(config)#ftp-server username user password 7 2
Invalid encrypted password, min length is 4, max length is 52.
```

5：配置明文密码太长

```
Ruijie(config)#ftp-server username user password abcdefghijklmnopqrstuvwxyz
% Password is too long, max length is 25
```

【常见错误】 1.配置用户名包含非法字符或过长
2.未配置用户名就尝试连接
3.用户未配置密码

4.配置密码长度太短或者太长

5.输入非法密码

【平台说明】 -

8.7 show ftp-server

显示 FTP 服务器的相关状态信息

show ftp-server

【参数说明】

参数	描述
-	-

【缺省配置】 -

【命令模式】 特权用户模式

【缺省级别】 14

【使用指导】 显示 FTP 服务器的相关状态信息，包括：

- 服务器是否启动
- 服务器顶层目录
- 服务器用户信息：用户名、密码、连接个数。若有连接则显示连接相关 IP,Port，传输类型，主动模式或被动模式等信息。

【配置举例】 1:以下示范如何查看 FTP 服务器的相关状态信息：

```
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]
```

【检验方法】 -

【提示信息】 -

【常见错误】 -

【平台说明】 -

9 FTP Client

9.1 ftp-client ascii

使用文本（ASCII）方式进行 FTP 传输。
ftp-client [**vrf** *vrf-name*] **ascii**

取消文本传输方式，使用二进制传输方式。
no ftp-client [**vrf** *vrf-name*] **ascii**

恢复缺省配置.。
default ftp-client [**vrf** *vrf-name*]

【参数说明】

参数	描述
vrf *vrf-name*	指定 VRF。缺省为公网实例。

【缺省配置】 默认情况下 FTP 传输模式为二进制（BINARY）方式

【命令模式】 全局配置模式

【缺省级别】 14

【使用指导】

注意使用 default 命令时，将 FTP Client 恢复为缺省配置，即数据连接为被动（PASV）方式，文件传输为二进制（BINARY）模式，客户端源 IP 地址不进行绑定。

【配置举例】 1：配置使用文本（ASCII）方式进行 FTP 传输。

```
Ruijie(config)# ftp-client ascii
```

2：配置 *vrf-name* 使用文本（ASCII）方式进行 FTP 传输。

```
Ruijie(config)# ftp-client vrf vrf-name ascii
```

3：配置使用文本（BINARY）方式进行 FTP 传输。

```
Ruijie(config)# no ftp-client ascii
```

4：配置 *vrf-name* 使用文本（BINARY）方式进行 FTP 传输。

```
Ruijie(config)# no ftp-client vrf vrf-name ascii
```

5：FTP Client 恢复为缺省配置。

```
Ruijie(config)# default ftp-client
```

6：FTP Client vrf-name 上恢复为缺省配置。

```
Ruijie(config)# default ftp-client vrf vrf-name
```

【检验方法】 1：使用 **show run** 命令，可以查看 **ftp-client ascii** 配置。
2：使用 **show run** 命令，可以查看 **ftp-client vrf** *vrf-name* **ascii** 配置。

【提示信息】 1：一定配置成功，不会出现任何提示。
2：如果 vrf-name 在本地设备上不存在，则会提示错误：% VPN Routing/Forwarding instance name error；否则配置成功，不会出现任何提示。
3：一定配置成功，不会出现任何提示。
4：如果 vrf-name 在本地设备上不存在，则会提示错误：% VPN Routing/Forwarding instance name error；否则配置成功，不会出现任何提示。

【常见错误】 -

【平台说明】 -

9.2 ftp-client port

配置 FTP 使用主动（PORT）方式进行数据连接。
ftp-client [**vrf** *vrf-name*] **port**

恢复为被动方式。
no ftp-client [**vrf** *vrf-name*] **port**

恢复缺省配置.。
default ftp-client [**vrf** *vrf-name*]

【参数说明】

参数	描述
vrf *vrf-name*	指定 VRF。缺省为公网实例。

【缺省配置】 默认情况下 FTP 连接为被动（PASV）方式

【命令模式】 全局配置模式

【缺省级别】 14

【使用指导】 使用该命令可以将连接模式设置为主动方式，即服务器主动去连接客户端。

注意使用 default 命令时，将 FTP Client 恢复为缺省配置，即数据连接为被动（PASV）方式，文件传输为二进制（BINARY）模式，客户端源 IP 地址不进行绑定。

【配置举例】 1：配置 FTP 使用主动（PORT）方式进行数据连接。

```
Ruijie(config)# ftp-client port
```

2：配置 FTP*vrf-name* 使用主动（PORT）方式进行数据连接。

```
Ruijie(config)# ftp-client vrf vrf-name port
```

3：配置 FTP 连接为被动（PASV）方式。

```
Ruijie(config)# no ftp-client port
```

4：配置 FTP *vrf-name* 连接为被动（PASV）方式。

```
Ruijie(config)# no ftp-client vrf vrf-name port
```

5：FTP Client 恢复为缺省配置。

```
Ruijie(config)# default ftp-client
```

6：FTP Client vrf-name 上恢复为缺省配置。

```
Ruijie(config)# default ftp-client vrf vrf-name
```

【检验方法】 1：使用 **show run** 命令，可以查看 **ftp-client port** 配置。
2：使用 **show run** 命令，可以查看 **ftp-client vrf** *vrf-name* port 配置。

【提示信息】 1：一定配置成功，不会出现任何提示。
2：如果 vrf-name 在本地设备上不存在，则会提示错误：% VPN Routing/Forwarding instance name error；否则配置成功，不会出现任何提示。
3：一定配置成功，不会出现任何提示。
4：如果 vrf-name 在本地设备上不存在，则会提示错误：% VPN Routing/Forwarding instance name error；否则配置成功，不会出现任何提示。

【常见错误】 -

【平台说明】 -

9.3 ftp-client source

FTP Client 可以绑定客户端源 IP 地址，使用该 IP 地址与服务器端 IP 地址进行通信。

ftp-client [**vrf** *vrf-name*] **source** {*ip-address* **|** *ipv6-address* | *interface*}

取消对客户端源 IP 地址绑定。

no ftp-client [**vrf** *vrf-name*] **source**

恢复缺省配置.。

default ftp-client [**vrf** *vrf-name*]

【参数说明】

参数	描述
vrf *vrf-name*	指定 VRF。缺省为公网实例。

【缺省配置】 缺省情况下，客户端不进行本地 IP 绑定，由路由进行选择。

【命令模式】 全局配置模式

【缺省级别】 14

【使用指导】

注意使用 default 命令时，将 FTP Client 恢复为缺省配置，即数据连接为被动（PASV）方式，文件传输为二进制（BINARY）模式，客户端源 IP 地址不进行绑定。

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。

【配置举例】 1：配置 FTP Client 绑定客户端源 IP 为 192.168.23.236 地址。

```
Ruijie(config)# ftp-client source 192.168.23.236
```

2：配置 FTP Client 绑定客户端源 IP 为 2003:0:0:0::2 地址。

```
Ruijie(config)# ftp-client source 2003:0:0:0::2
```

3：配置 FTP Client *vrf-name* 绑定客户端源 IP 为 192.168.23.236 地址。

```
Ruijie(config)# ftp-client vrf vrf-name source 192.168.23.236
```

4：配置 FTP Client *vrf-name* 绑定客户端源接口为 tenGigabitEthernet 1/0/1 接口地址。

```
Ruijie(config)# ftp-client source tenGigabitEthernet 1/0/1
```

4：配置 FTP Client *vrf-name* 绑定客户端源 IP 为 2003:0:0:0::2 地址。

```
Ruijie(config)# ftp-client vrf vrf-name source 2003:0:0:0::2
```

5：no 命令取消对客户端源 IP 地址绑定。

```
Ruijie(config)# no ftp-client source
```

6：no 命令取消对客户端源 IP 地址绑定。

```
Ruijie(config)# no ftp-client vrf vrf-name source
```

7：FTP Client 恢复为缺省配置。

```
Ruijie(config)# default ftp-client
```

8：FTP Client vrf-name 上恢复为缺省配置。

```
Ruijie(config)# default ftp-client vrf vrf-name
```

【检验方法】 1：使用 **show run** 命令，可以查看 ftp-client source192.168.23.236 配置。
2：使用 **show run** 命令，可以查看 ftp-client source 2003:0:0:0::2 配置。
3：使用 **show run** 命令，可以查看 ftp-client vrf vft-name source192.168.23.236 配置。
4：使用 **show run** 命令，可以查看 ftp-client vrf vft-name source 2003:0:0:0::2 配置。

【提示信息】 1：如果 192.168.23.236 不是本地地址，则会提示错误；如果是，则配置成功，不会出现任何提示。
2：如果 2003:0:0:0::2 不是本地地址，则会提示错误：Bind failed: the specified source address is non-local ip；如果是，则配置成功，不会出现任何提示。
3：如果 vrf-name 在本地设备上不存在提示： 192.168.23.236 不是本地地址，则会提示错误：Bind failed: the specified source address is non-local ip；如果存在且是，则配置成功，不会出现任何提示。
4：如果 vrf-name 在本地设备上不存在提示：% VPN Routing/Forwarding instance name error，2003:0:0:0::2 不是本地地址，则会提示错误：Bind failed: the specified source address is non-local ip；如果存在且是，则配置成功，不会出现任何提示。
5：一定配置成功，不会出现任何提示。
6：如果 vrf-name 在本地设备上不存在，则会提示错误；如果是，则配置成功，不会出现任何提示。

【常见错误】 -

【平台说明】 -

9.4 ftp-client source-address

FTP Client 可以绑定客户端源 IP 地址，使用该 IP 地址与服务器端 IP 地址进行通信。
ftp-client [**vrf** *vrf-name*] **source-address** {*ip-address* **|** *ipv6-address*}

取消对客户端源 IP 地址绑定。

no ftp-client [**vrf** *vrf-name*] **source-address**

恢复缺省配置.。
default ftp-client [**vrf** *vrf-name*]

【参数说明】

参数	描述
vrf *vrf-name*	指定 VRF。缺省为公网实例。

【缺省配置】 缺省情况下，客户端不进行本地 IP 绑定，由路由进行选择。

【命令模式】 全局配置模式

【缺省级别】 14

【使用指导】

注意使用 default 命令时，将 FTP Client 恢复为缺省配置，即数据连接为被动（PASV）方式，文件传输为二进制（BINARY）模式，客户端源 IP 地址不进行绑定。

【配置举例】 1：配置 FTP Client 绑定客户端源 IP 为了 192.168.23.236 地址。

```
Ruijie(config)# ftp-client source-address 192.168.23.236
```

2：配置 FTP Client 绑定客户端源 IP 为了 2003:0:0:0::2 地址。

```
Ruijie(config)# ftp-client source-address 2003:0:0:0::2
```

3：配置 FTP Client *vrf-name* 绑定客户端源 IP 为了 192.168.23.236 地址。

```
Ruijie(config)# ftp-client vrf vrf-name source-address 192.168.23.236
```

4：配置 FTP Client *vrf-name* 绑定客户端源 IP 为了 2003:0:0:0::2 地址。

```
Ruijie(config)# ftp-client vrf vrf-name source-address 2003:0:0:0::2
```

5：no 命令取消对客户端源 IP 地址绑定。

```
Ruijie(config)# no ftp-client source-address
```

6：no 命令取消对客户端源 IP 地址绑定。

```
Ruijie(config)# no ftp-client vrf vrf-name source-address
```

7：FTP Client 恢复为缺省配置。

```
Ruijie(config)# default ftp-client
```

8：FTP Client vrf-name 上恢复为缺省配置。

```
Ruijie(config)# default ftp-client vrf vrf-name
```

【检验方法】 1：使用 **show run** 命令，可以查看 **ftp-client source-address**192.168.23.236 配置。
2：使用 **show run** 命令，可以查看 **ftp-client source-address** 2003:0:0:0::2 配置。
3：使用 **show run** 命令，可以查看 **ftp-client vrf** *vft-name* **source-address**192.168.23.236 配置。
4：使用 **show run** 命令，可以查看 **ftp-client vrf vft-name source-address 2003:0:0:0::2** 配置。

【提示信息】 1：如果 192.168.23.236 不是本地地址，则会提示错误；如果是，则配置成功，不会出现任何提示。
2：如果 2003:0:0:0::2 不是本地地址，则会提示错误：Bind failed: the specified source address is non-local ip；如果是，则配置成功，不会出现任何提示。
3：如果 vrf-name 在本地设备上不存在提示： 192.168.23.236 不是本地地址，则会提示错误：Bind failed: the specified source address is non-local ip；如果存在且是，则配置成功，不会出现任何提示。
4：如果 vrf-name 在本地设备上不存在提示：% VPN Routing/Forwarding instance name error，2003:0:0:0::2 不是本地地址，则会提示错误：Bind failed: the specified source address is non-local ip；如果存在且是，则配置成功，不会出现任何提示。
5：一定配置成功，不会出现任何提示。
6：如果 vrf-name 在本地设备上不存在，则会提示错误；如果是，则配置成功，不会出现任何提示。

【常见错误】 -

【平台说明】 -

9.5 copy ftp

使用 FTP Client 从服务器把文件下载到设备。
copy ftp://*username:password@dest-address* [/*remote-directory*] / *remote-file* **flash:**[*local-directory*/] *local-file*

【参数说明】

参数	描述
username	登录 FTP Server 的账号名，长度限制 32 字节，不可包含“:”、“/”和空格等字符，不可省略
password	登录 FTP Server 的账户密码，长度限制 32 字节，不可包含“:”、“/”和空格等字符，不可省略
dest-address	访问的 FTP Server 的 IP 地址
remote-directory	可选的 FTP Server 上的文件路径名，长度限制 255 字节，不支持空格和中文字符，如果为空，表示 FTP 服务器当前工作路径

remote-file	远程服务器上的文件名，长度限制 255 字节，不支持空格和中文字符
local-directory	可选的本地设备文件夹路径，如果指定了该文件路径，则必须保证该文件夹路径已经事先创建，此命令不支持文件夹自动创建；如果为空则表示在设备当前目录，长度限制 255 字节，不支持空格和中文字符
local-file	本地设备上的文件名，长度限制 255 字节，不支持空格和中文字符

【缺省配置】 无

【命令模式】 特权模式

【缺省级别】 14

【使用指导】 -

【配置举例】 1 :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
```

2：把设备 home 目录中的 local-file 文件上传到 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】 使用 **dir** 在本地地设备上查看 local-file 文件是否存在，存在下载成功，不存在下载失败。

【提示信息】 下载不成功，打开 **debug ftp-client** 会提示相应的错误，成功会提示 success。

【常见错误】 -

【平台说明】 -

9.6 copy flash

使用 FTP Client 把本地设备的文件上传到服务器。

copy flash:[*local-directory/*] *local-file* **ftp:**//*username:password@dest-address* [*/remote-directory*] */remote-file*

【参数说明】

参数	描述
username	登录 FTP Server 的账号名，长度限制 32 字节，不可包含“:”、“/”和空格等字符，不可省略
password	登录 FTP Server 的账户密码，长度限制 32 字节，不可包含“:”、“/”和空格等字符，不可省略

dest-address	访问的 FTP Server 的 IP 地址
remote-directory	可选的 FTP Server 上的文件路径名，长度限制 255 字节，不支持空格和中文字符，如果为空，表示 FTP 服务器当前工作路径
remote-file	远程服务器上的文件名，长度限制 255 字节，不支持空格和中文字符
local-directory	可选的本地设备文件夹路径，如果指定了该文件路径，则必须保证该文件夹路径已经事先创建，此命令不支持文件夹自动创建；如果为空则表示在设备当前目录，长度限制 255 字节，不支持空格和中文字符
local-file	本地设备上的文件名，长度限制 255 字节，不支持空格和中文字符

【缺省配置】 无

【命令模式】 特权模式

【缺省级别】 14

【使用指导】 -

【配置举例】 1：从用户名为 user，密码为 pass，IP 地址为 192.168.23.69 的 FTP Server，把设备 home 目录中的 local-file 文件上传到 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 Server 的 root 目录下查看 local-file 文件是否存在，存在下载成功，不存在下载失败。

【提示信息】 上传不成功，打开 **debug ftp-client** 会提示相应的错误， 成功会提示 success。

【常见错误】 -

【平台说明】 -

10 TIME RANGE

10.1 absolute

设置绝对时间区间。

absolute { [**star**t *time date*] [**end** *time date*] }

删除已存在的绝对时间区间。

no absolute

【参数说明】

参数	描述
start *time date*	区间的开始时间
end *time date*	区间的结束时间

【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

【缺省级别】 14

【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。最大时间区间为 0 年 1 月 1 日 00：00，9999 年 12 月 31 日 23：59。

【配置举例】 1：创建一个 time range 并进入 time range 模式

```
Ruijie(config)# time-range no-http
Ruijie(config-time-range)#
```

2：配置绝对时间区间

```
Ruijie(config-time-range)# absolute start 1:1 1 JAN 2013 end 1:1 1 JAN 2014
```

【检验方法】 1：使用 **show time-range** [*time-range-name*]命令，可以查看 time range 的配置情况。

【提示信息】 -

【常见错误】 -

【平台说明】 -

10.2 periodic

设置周期时间。

periodic *day-of-the-week time* **to** [*day-of-the-week*] *time*

删除已存在的周期时间。

no periodic *day-of-the-week time* **to** [*day-of-the-week*] *time*

【参数说明】

参数	描述
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

【缺省级别】 14

【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。

【配置举例】 1：创建一个 time range 并进入 time range 模式

```
Ruijie(config)# time-range no-http
Ruijie(config-time-range)#
```

2：配置绝对时间区间

```
Ruijie(config-time-range)# periodic Monday 1:1 to Tuesday 2:2
```

【检验方法】 1：使用 **show time-range** [*time-range-name*]命令，可以查看 time range 的配置情况。

【提示信息】 -

【常见错误】 -

【平台说明】 -

10.3 show time-range

显示 time range 信息。

show time-range [*time-range-name*]

【参数说明】

参数	描述
time-range-name	可以指定显示某个 time range 的信息

【命令模式】 特权模式

【缺省级别】 14

【使用指导】 可以通过该命令验证配置的 time range 是否正确。

【配置举例】 1：显示 time range 信息

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

【提示信息】 -

【平台说明】 -

10.4 time-range

创建 time range，并进入 time range 配置模式。
time-range *time-range-name*

删除已存在的 time range。
no time-range *time-range-name*

【参数说明】

参数	描述
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

【缺省级别】 2

【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。

【配置举例】 1：创建一个 time range

```
Ruijie(config)# time-range no-http
```

```
Ruijie(config-time-range)#
```

【检验方法】 1：使用 **show time-range** [*time-range-name*]命令，可以查看 time range 是否存在。

【提示信息】 -

【常见错误】 -

【平台说明】 -

11 网络连通性测试工具

11.1 clear rping table all

清除 Rping 所有表项。

clear rping table [**all |** [**ping-object** *owner test-name*] | [**trace-object** *owner test-name*]]

【参数说明】

参数	描述
owner	用户索引
test-name	测试索引

【命令模式】 特权模式

【缺省级别】 14

【使用指导】 此命令用来删除设备上 Rping 管理的用户的所有探测相关表项。

【配置举例】 1：清除 Rping 所有表项信息。

```
Ruijie# clear rping table all
```

2: 清除用户为 user，探测名 ruijie 的概念行。

```
Ruijie# clear rping table user ruijie
```

【提示信息】 1：如果设备上没有指定概念行，则提示相应信息。

【平台说明】 -

11.2 ping

检测指定 IPv4 地址是否可达，并输出相关信息。

ping [oob | **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】

参数	描述
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。 仅在支持 MGMT 的设备上支持。
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

【缺省配置】 缺省在指定的时间（缺省为 2 秒）内，送 5 个长度为 100Byte 的数据包到指定的 IP 地址。

【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。

【缺省级别】 0

【使用指导】 运行 **ping** 功能，如果有应答，则显示出应答的相关信息，最后输出一个统计信息。在扩展 **ping** 中，可以指定发送数据包的个数、长度、超时的时间等等，和基本的 **ping** 功能一样，最后也输出一个统计信息。
要使用域名功能，则要先配置域名服务器，具体配置请参考 DNS 配置部分。

【配置举例】 1：普通 **ping** 的实例。指定目的 IP 地址为 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
*Apr 16 09:16:08: %PING-7-DEBUG: Ping vrf index -1.
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.2：扩展 **ping** 的实例。指定目的 IP 地址为 192.168.21.26，发送数据包长度为 1500，发送数据包个数为 20，超时的时间为 3 秒，报文填充数据为 ffff，并设置源 IP 地址为 192.168.21.99。

常规 ping

```
Ruijie# ping 192.168.21.26 length 1500 ntimes 100 data ffff source 192.168.21.99 timeout 3
Sending 100, 1500-byte ICMP Echoes to 192.168.21.26, timeout is 3 seconds:
  < press Ctrl+C to break >
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!
Success rate is 100 percent (100/100), round-trip min/avg/max = 2/2/3 ms
```

显示 detail 的 ping

```
ping 192.168.21.26 length 1500 ntimes 20 data ffff source 192.168.21.99 timeout 3 detail
Sending 20, 1500-byte ICMP Echoes to 192.168.21.26, timeout is 3 seconds:
  < press Ctrl+C to break >
Reply from 192.168.21.26: bytes=1500 time=1ms TTL=64
Reply from 192.168.21.26: bytes=1500 time=1ms TTL=64
Reply from 192.168.21.26: bytes=1500 time=1ms TTL=64
Reply from 192.168.21.26: bytes=1500 time=1ms TTL=64
Reply from 192.168.21.26: bytes=1500 time=1ms TTL=64
Reply from 192.168.21.26: bytes=1500 time=1ms TTL=64
Reply from 192.168.21.26: bytes=1500 time=1ms TTL=64
Reply from 192.168.21.26: bytes=1500 time=2ms TTL=64
Reply from 192.168.21.26: bytes=1500 time=1ms TTL=64
Reply from 192.168.21.26: bytes=1500 time=1ms TTL=64
Reply from 192.168.21.26: bytes=1500 time=1ms TTL=64
Reply from 192.168.21.26: bytes=1500 time=1ms TTL=64
Reply from 192.168.21.26: bytes=1500 time=1ms TTL=64
Reply from 192.168.21.26: bytes=1500 time=1ms TTL=64
Reply from 192.168.21.26: bytes=1500 time=1ms TTL=64
Reply from 192.168.21.26: bytes=1500 time=1ms TTL=64
Reply from 192.168.21.26: bytes=1500 time=1ms TTL=64
Reply from 192.168.21.26: bytes=1500 time=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.
```

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。

【检验方法】 -

【提示信息】 -

【常见错误】 -

【平台说明】 NBR6205-E、NBR6135-E、NBR6210-E、NBR6215-E 支持 MGMT 口；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 MGMT 口。

11.3 ping ipv6

检测指定 IPv6 地址是否可达，并输出相关信息。

ping [[**oob**] **ipv6**] [*ip-address* [**via** *mgmt-name*] [**length** *length*] [**ntimes** *times*] [**timeout** *seconds*] [**data** *data*] [**source** *source*] [**detail**] [**interval** millisecond] [**out-interface** interface [**next-hop** *next-hop*]]]

【参数说明】

参数	描述
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。 仅在支持 MGMT 的设备上支持。
ip-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。
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

【缺省配置】 缺省在指定的时间（缺省为 2 秒）内，送 5 个长度为 100Byte 的数据包到指定的 IP 地址。

【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。

【缺省级别】 0

【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，如果应答的数据内容与请求的数据内容不匹配，则显示 一个‘Request receive error.’，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】 1：普通 **ping ipv6** 的实例。指定目的 IP 地址为 2001::5。

常规 ping

```
Ruijie# ping ipv6 2001::5
Sending 5, 100-byte ICMP Echoes to 2001::5, 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.
```

2：扩展 **ping ipv6** 的实例。指定目的 IP 地址为 2001::5，发送数据包长度为 1500，发送数据包个数为 20，超时的时间为 3 秒，报文填充数据为 ffff，并设置源 IP 地址为 2001::9。

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 >
!!!!!
```

```
Reply from 2001::5: bytes=1500 time=1ms
Reply from 2001::5: bytes=1500 time=1ms
Reply from 2001::5: bytes=1500 time=1ms
Reply from 2001::5: bytes=1500 time=1ms
Reply from 2001::5: bytes=1500 time=1ms
Reply from 2001::5: bytes=1500 time=1ms
Reply from 2001::5: bytes=1500 time=1ms

Success rate is 100 percent (10/10), round-trip min/avg/max = 1/1/1 ms.
```

【检验方法】 -

【提示信息】 -

【常见错误】 -

【平台说明】 NBR6205-E、NBR6135-E、NBR6210-E、NBR6215-E 支持 MGMT 口；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 MGMT 口。

11.4 show rping detail

查看 Rping 信息。

show rping detail

【参数说明】

参数	描述
-	-

【命令模式】 特权模式、全局模式、接口模式

【缺省级别】 14

【使用指导】 使用该命令可以查看设备上的 Rping 中管理的对象的总数，用户数等信息。

【配置举例】 1：查看 Rping 的详细信息

```
Ruijie#show rping detail
Total owner number: 2
Total test number: 4
owner: user1
   test name: taget_1         storage type: volatile
   test name: taget_2         storage type: nonVolatile
owner: user2
   test name: taget_1         storage type: permanent
   test name: taget_2         storage type: readOnly
```

字段解释：

字段	说明
Total owner number	用户总数
Total test number	测试总数
owner	用户名
test name	测试名
storage type	概念行存储类型

【提示信息】

【平台说明】 -

11.5 traceroute

显示 IPv4 数据包从源地址到目的地址所经过的网关。

traceroute [oob | **ip**] [*adress* [**probe** *number*] [**source** *source*] [**timeout** *seconds*] [**ttl** *minimum maximum*] [**out-interface** interface **[next-hop next-hop]]]**

【参数说明】

参数	描述
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。 仅在支持 MGMT 的设备上支持。
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

【缺省配置】 缺省超时时间为 3 秒，发送探测的数量为 3，最小和最大 TTL 分别为 1 和 255。

【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。

【缺省级别】 0

【使用指导】 **Traceroute** 命令主要用于检查网络的连通性，并在网络故障发生时，准确的定位故障发生的位置。要使用域名功能，则要先配置域名服务器，具体配置请参考 DNS 配置部分。

【配置举例】 1：列举网络畅通的 traceroute 例子。

```
Ruijie# traceroute 61.154.22.36
< press Ctrl+C to break >
Tracing the route to 61.154.22.36
1       192.168.12.1      0 msec  0 msec  0 msec
2       192.168.9.2       4 msec  4 msec 4 msec
3       192.168.9.1       8 msec  8 msec  4 msec
4       192.168.0.10      4 msec  28 msec  12 msec
5       202.101.143.130     4 msec  16 msec  8 msec
6       202.101.143.154    12 msec  8 msec  24 msec
7       61.154.22.36      12 msec  8 msec  22 msec
```

从上面的结果可以看到，从源地址要访问 IP 地址为 61.154.22.36 的主机，网络数据包都经过了哪些网关（1－6），同时给出了到达该网关所花费的时间。

2：列举网络中某些网关不通的 traceroute 例子。

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

```
15      202.106.192.226    88 msec  52 msec  52 msec
16      202.106.192.174    52 msec  52 msec  88 msec
17      210.74.176.158    100 msec  52 msec  84 msec
18      202.108.37.42      48 msec  48 msec  52 msec
```

从上面的结果可以看到，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。

3：列举使用域名功能的例子。

```
Ruijie# traceroute www.ietf.org
Translating " www.ietf.org "...[OK]
< press Ctrl+C to break >
Tracing the route to 64.170.98.32
1       192.168.217.1    0 msec  0 msec  0 msec
2       10.10.25.1         0 msec  0 msec  0 msec
3       10.10.24.1         0 msec  0 msec  0 msec
4       10.10.30.1         10 msec 0 msec  0 msec
5       218.5.3.254        0 msec  0 msec  0 msec
6       61.154.8.49        10 msec 0 msec  0 msec
7       202.109.204.210    0 msec  0 msec  0 msec
8       202.97.41.69       20 msec 10 msec 20 msec
9       202.97.34.65       40 msec 40 msec 50 msec
10      202.97.57.222      50 msec 40 msec 40 msec
11      219.141.130.122    40 msec 50 msec 40 msec
12      219.142.11.10      40 msec 50 msec 30 msec
13      211.157.37.14      50 msec 40 msec 50 msec
14      222.35.65.1        40 msec 50 msec 40 msec
15      222.35.65.18       40 msec 40 msec 40 msec
16      222.35.15.109      50 msec 50 msec 50 msec
17      *       *       *
18     64.170.98.32      40 msec 40 msec 40 msec
```

【检验方法】 -

【提示信息】 -

【常见错误】 -

【平台说明】 NBR6205-E、NBR6135-E、NBR6210-E、NBR6215-E 支持 MGMT 口；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 MGMT 口。

11.6 traceroute ipv6

显示 IPv6 数据包从源地址到目的地址所经过的网关。

traceroute [[**oob**] **ipv6**] [*address* [**via** *mgmt-name*] [**probe** *number*] [**timeout** *seconds*] [**ttl** *minimum maximum*] [**out-interface** interface [**next-hop** *next-hop*]]]

【参数说明】

参数	描述
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。 仅在支持 MGMT 的设备上支持。
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

【缺省配置】 缺省超时时间为 3 秒，发送探测的数量为 3，最小和最大 TTL 分别为 1 和 255。

【命令模式】 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。

【缺省级别】 0

【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】 1：列举网络畅通的 **traceroute ipv6** 例子。

```
Ruijie# traceroute ipv6 3004::1
  < press Ctrl+C to break >
Tracing the route to 3004::1
1       3000::1          0 msec  0 msec  0 msec
2       3001::1          4 msec  4 msec 4 msec
3       3002::1          8 msec  8 msec  4 msec
4       3004::1          4 msec  28 msec  12 msec
```

从上面的结果可以看到，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。

2：列举网络中某些网关不通的 **traceroute ipv6** 例子。

```
Ruijie# traceroute ipv6 3004::1
  < press Ctrl+C to break >
```

```
Tracing the route to 3004::1
1       3000::1          0 msec  0 msec  0 msec
2       3001::1          4 msec  4 msec 4 msec
3       3002::1          8 msec  8 msec  4 msec
4       * * *
5       3004::1          4 msec  28 msec  12 msec
```

从上面的结果可以看到，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。

【检验方法】 -

【提示信息】 -

【常见错误】 -

【平台说明】 NBR6205-E、NBR6135-E、NBR6210-E、NBR6215-E 支持 MGMT 口；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 MGMT 口。

命令参考-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. 协议无关
8. NSM

1 策略路由

1.1 clear ip pbr statistics

清除 IPv4 PBR 转发的报文个数统计值

clear ip pbr statistics [**interface** *if-name* **| local**]

【参数说明】

参数	描述
interface *if-name*	指定 if-name，则清除指定接口上 IPv4 策略路由转发的报文个数 不带可选参数，清除所有应用 IPv4 策略路由的接口转发的报文个数
local	清除 local 口上 IPv4 策略路由转发的报文个数

【命令模式】 特权模式。

【缺省级别】 14

【使用指导】 为了清除 IPv4 策略路由转发的报文个数，可以使用该命令进行。

【配置举例】 1：清除 IPv4 策略路由转发的报文个数

```
Ruijie#clear ip pbr statistics
```

【提示信息】 -

【平台说明】 -

1.2 clear ipv6 pbr statistics

清除 IPv6 PBR 转发的报文个数统计值

clear ipv6 pbr statistics [**interface** *if-name* **| local**]

【参数说明】

参数	描述
interface *if-name*	指定 if-name，则清除指定接口上 IPv6 策略路由转发的报文个数 不带可选参数，清除所有应用 IPv6 策略路由的接口转发的报文个数
local	清除 local 口上 IPv6 策略路由转发的报文个数

【命令模式】 特权模式。

【缺省级别】 14

【使用指导】 为了清除 IPv6 策略路由转发的报文个数，可以使用该命令进行。

【配置举例】 1：清除 IPv6 策略路由转发的报文个数

```
Ruijie#clear ipv6 pbr statistics
```

【提示信息】 -

【平台说明】 -

1.3 ip local policy route-map

对本地发送的报文应用策略路由

ip local policy route-map *route-map-name*

关闭策略路由的应用。

no ip local policy route-map

【参数说明】

参数	描述
route-map-name	路由图名称。

【缺省配置】 缺省未应用策略路由。

【命令模式】 全局配置模式。

【缺省级别】 14

【使用指导】 该命令只对本地发送出去的符合策略的 IP 报文进行策略路由，发送给本地的 IP 报文不受该命令控制。

应用策略路由，必须要指定策略路由使用的路由图，并且要创建路由图。一个路由图由很多条策略组成，每个策略都定义了 1 个或多个的匹配规则和对应操作。一个接口应用策略路由后，将对该接口接收到的所有包进行检查，不符合路由图任何策略的数据包将按照通常的路由转发进行处理，符合路由图中某个策略的数据包就按照该策略中定义的操作进行处理。

策略路由配置 **set interface** 不支持负载均衡。如果 **set interface** 多个接口，则冗余备份。

【配置举例】 1：使本机所有以 192.168.217.10 为源地址发送的报文从 serial2/0 口出去。

步骤一：定义匹配 IP 报文的 ACL

```
Ruijie(config)#access-list 1 permit host 192.168.217.10
```

步骤二：定义路由图

```
Ruijie(config)#route-map lab1 permit 10
Ruijie(config-route-map)#match ip address 1
Ruijie(config-route-map)#set interface serial 2/0
```

```
Ruijie(config-route-map)#exit
```

步骤三：在设备上应用策略路由

```
Ruijie(config)#ip local policy route-map lab1
```

【检验方法】 1：使用 **show running-config** 命令查看配置。

【提示信息】 -

【常见错误】 -

【平台说明】 -

1.4 ip policy

设置策略路由的 **set ip** [**default**] **nexthop** 的多个下一跳间采用冗余备份或负载均衡方式。

ip policy { **load-balance** | **redundance** }

恢复策略路由的转发模式。

no ip policy

【参数说明】

参数	描述
load-balance	负载均衡
Redundance	冗余备份

【缺省配置】 缺省采用冗余备份。

【命令模式】 全局配置模式。

【缺省级别】 14

【使用指导】 在配置 **set ip next-hop** 时，可以配置多个下一跳，但是设置了冗余备份时，策略路由只有第一个可以解析的下一跳起作用；设置了负载均衡时，策略路由有多个解析的下一跳起作用，WCMP 最多可以设置 8 个下一跳，ECMP 最多可以设置 32 个下一跳。

解析的下一跳是指已经学习到对应的 MAC 的下一跳。

【配置举例】 1：路由图中设置了多个 nexthop,在全局配置模式下设置了冗余备份后，则应用在 GigabitEthernet 0/0 上的策略路由只有第一个 nexthop 起作用。

步骤一：配置匹配 IP 报文的 ACL

```
Ruijie(config)#access-list 1 permit host 10.0.0.1
Ruijie(config)#access-list 2 permit host 20.0.0.1
```

步骤二：定义路由图

```
Ruijie(config)#route-map lab1 permit 10
Ruijie(config-route-map)#match ip address 1
Ruijie(config-route-map)#set ip next-hop 196.168.4.6
Ruijie(config-route-map)#set ip next-hop 196.168.4.7
Ruijie(config-route-map)#set ip next-hop 196.168.4.8
Ruijie(config-route-map)#exit
Ruijie(config)#route-map lab1 permit 20
Ruijie(config-route-map)#match ip address 2
Ruijie(config-route-map)#set ip next-hop 196.168.5.6
Ruijie(config-route-map)#set ip next-hop 196.168.5.7
Ruijie(config-route-map)#set ip next-hop 196.168.5.8
Ruijie(config-route-map)#exit
```

步骤三：在接口上应用策略路由

```
Ruijie(config)#interface GigabitEthernet 0/0
Ruijie(config-if)#ip policy route-map lab1
Ruijie(config-if)#exit
Ruijie(config)#ip policy redundance
```

【检验方法】 1：使用 **show running-config** 命令查看配置。

【提示信息】 -

【常见错误】 -

【平台说明】 -

1.5 ip policy route-map

在一个接口应用策略路由。

ip policy route-map *route-map*

关闭接口上应用的策略路由。

no ip policy route-map

【参数说明】

参数	描述
route-map	路由图名称。

【缺省配置】 缺省关闭策略路由。

【命令模式】 接口配置模式。

【缺省级别】 14

【使用指导】 策略路由必须在指定的接口上应用，只对该接口接收到的数据包进行策略路由，对于该接口发送出去的数据包不会进行策略路由。

应用策略路由，必须要指定策略路由使用的路由图，并且要创建路由图。一个路由图由很多条策略组成，每个策略都定义了 1 个或多个的匹配规则和对应操作。一个接口应用策略路由后，将对该接口接收到的所有包进行检查，不符合路由图任何策略的数据包将按照通常的路由转发进行处理，符合路由图中某个策略的数据包就按照该策略中定义的操作进行处理。

设备上一个接口最多只能配置一个路由图，在同一个接口上多次配置路由图，后配置的路由图将覆盖先前配置的路由图。

【配置举例】 1：当快速以太网接口 GigabitEthernet 0/0 接收到数据报，如果数据报源地址为 10.0.0.1，则设置下一跳为 196.168.4.6，如果源地址为 20.0.0.1 则设置下一跳为 196.168.5.6，否则进行普通转发。

步骤一：配置匹配 IP 报文的 ACL

```
Ruijie(config)#access-list 1 permit host 10.0.0.1
Ruijie(config)#access-list 2 permit host 20.0.0.1
```

步骤二：定义路由图

```
Ruijie(config)#route-map lab1 permit 10
Ruijie (config-route-map)#match ip address 1
Ruijie(config-route-map)#set ip next-hop 196.168.4.6
Ruijie(config-route-map)#exit
Ruijie(config)#route-map lab1 permit 20
Ruijie(config-route-map)#match ip address 2
Ruijie(config-route-map)#set ip next-hop 196.168.5.6
Ruijie(config-route-map)#exit
```

步骤三：在接口上应用策略路由

```
Ruijie(config)#interface GigabitEthernet 0/0
Ruijie(config-if)#ip policy route-map lab1
Ruijie(config-if)#exit
```

【检验方法】 1：使用 **show running-config** 命令查看配置。

【提示信息】 -

【常见错误】 -

【平台说明】 -

1.6 ipv6 local policy route-map

对设备自己发送的 IPv6 报文应用策略路由。
ipv6 local policy route-map *route-map-name*

关闭设备本地发送报文的策略路由控制功能。
no ipv6 local policy route-map

【参数说明】

参数	描述
route-map-name	应用于本地策略路由路由图的名称，是通过 **route-map** 命令配置的。

【缺省配置】 缺省未应用策略路由功能。

【命令模式】 全局配置模式。

【缺省级别】 14

【使用指导】 该命令只对本地发送出去的符合策略的 IPv6 报文(如用于管理的 ping 报文)进行策略路由 ,发送给本地的 IPv6 报文不受该命令控制。
应用策略路由，必须要指定策略路由使用的路由图，并且要创建路由图。一个路由图由很多条策略组成，每个策略都定义了 1 个或多个的匹配规则和对应操作。一个接口应用策略路由后，将对该接口接收到的所有包进行检查，不符合路由图任何策略的数据包将按照通常的路由转发进行处理，符合路由图中某个策略的数据包就按照该策略中定义的操作进行处理。

【配置举例】 1：设备应用期望策略路由过程。从源 2003:1000::10/80 去往 2001:100::/64 的数据报文，会匹配 aaa 的 ACL6 被发给设备 2003:1001::2。
步骤一：配置关联的 ACL6

```
Ruijie(config)#ipv6 access-list aaa
Ruijie(config-ipv6-acl)#permit ipv6 2003:1000::10/80 2001:100::/64
```

步骤二：配置 route-map

```
Ruijie(config)#route-map pbr-aaa permit 10
Ruijie(config-route-map)#match ipv6 address aaa
Ruijie(config-route-map)#set ipv6 next-hop 2003:1001::2
```

步骤三：在设备上应用策略路由

```
Ruijie(config)#ipv6 local policy route-map pbr-aaa
```

【检验方法】 1：使用 **show running-config** 命令查看配置。

【提示信息】 -

【常见错误】 -

【平台说明】 -

1.7 ipv6 policy

设置策略路由的 **set ipv6** [**default**] **nexthop** 的多个下一跳间采用冗余备份或负载均衡方式。
ipv6 policy { **load-balance** | **redundance** }

恢复缺省模式。
no ipv6 policy

【参数说明】

参数	描述
load-balance	负载均衡
redundance	冗余备份

【缺省配置】 冗余备份模式。

【命令模式】 全局配置模式。

【缺省级别】 14

【使用指导】 该功能对 set 中多个下一跳行为生效。
在配置策略中 **set ipv6 next-hop** 时，可以配置多个下一跳，但是设置了冗余备份时，策略路由只有第一个可以解析的下一跳起作用。只有当第一个下一跳失效时，设置的第二个下一跳才生效；若第一个下一跳恢复，重新生效，则第一个下一跳会恢复起作用。
设置了负载均衡时，策略路由有多个解析的下一跳起作用。
WCMP 最多可以设置 8 个下一跳，ECMP 最多可以设置 32 个下一跳。

⚠ 解析的下一跳是指已经学习到对应的 MAC 的下一跳。

【配置举例】 1：多个 nexthop 之间为负载均衡模式。
步骤一：配置匹配 IP 报文的 ACL

```
Ruijie(config)# ipv6 access-list 1
Ruijie(config-ipv6-acl )# permit ipv6 1000::1 any
Ruijie(config)# ipv6 access-list 2
Ruijie(config-ipv6-acl )# permit ipv6 2000::1 any
```

步骤二：定义路由图

```
Ruijie(config)# route-map lab1 permit 10
Ruijie(config-route-map)# match ipv6 address 1
Ruijie(config-route-map)# set ipv6 next-hop 2002::1
Ruijie(config-route-map)# set ipv6 next-hop 2002::2
```

```
Ruijie(config-route-map)# set ipv6 next-hop 2002::3
Ruijie(config-route-map)# exit
Ruijie(config)# route-map lab1 permit 20
Ruijie(config-route-map)# match ipv6 address 2
Ruijie(config-route-map)# set ipv6 next-hop 2002::5
Ruijie(config-route-map)# set ipv6 next-hop 2002::6
Ruijie(config-route-map)# set ipv6 next-hop 2002::7
Ruijie(config-route-map)# exit
```

步骤三：在接口上应用策略路由

```
Ruijie(config)# interface GigabitEthernet 0/0
Ruijie(config-if)# ipv6 policy route-map lab1
Ruijie(config-if)# exit
Ruijie(config)# ipv6 policy load-balance
```

【检验方法】 1：使用 **show running-config** 命令查看配置。

【提示信息】 -

【常见错误】 -

【平台说明】 -

1.8 ipv6 policy route-map

在接口上应用 IPv6 策略路由。
ipv6 policy route-map *route-map-name*

取消接口上应用的 IPv6 策略路由。
no ipv6 policy route-map

【参数说明】

参数	描述
route-map-name	路由图的名称，是通过 **route-map** 命令配置的。

【缺省配置】 接口下未应用任何策略路由功能。

【命令模式】 接口配置模式。

【缺省级别】 14

【使用指导】 在接口上应用 IPv6 策略路由，只对该接口接收到的 IPv6 报文进行策略路由，对于该接口发送出去的 IPv6 报文不会进行策略路由。

应用策略路由，必须要指定策略路由使用的路由图，并且要创建路由图。一个路由图由很多条策略组成，每个策略都定义了 1 个或多个的匹配规则和对应操作。一个接口应用策略路由后，将对该接口接收到的所有包进行检查，不符合路由图任何策略的数据包将按照通常的路由转发进行处理，符合路由图中某个策略的数据包就按照该策略中定义的操作进行处理

设备上一个接口最多只能配置一个 IPv6 的路由图，在同一个接口上多次配置路由图，后配置的路由图将覆盖先前配置的路由图。

被 IPv6 策略路由引用的路由图的规则必须是 IPv6 支持的规则，否则该策略路由不会生效。

【配置举例】 1：当快速以太网接口 GigabitEthernet 0/0 接收到 IPv6 的数据报文时，如果数据报源地址为 10::/64 网段的数据报文，则转发到下一跳为 2000：1；如果源地址为 20：：/64 网段的数据报文，则设转发到下一跳为 2000::2，否则进行普通转发。

步骤一：配置匹配 IP 报文的 ACL

```
Ruijie(config)# ipv6 access-list acl_for_pbr1
Ruijie (config-ipv6-acl)# permit ipv6 10::/64  any
Ruijie(config)# ipv6 access-list acl_for_pbr2
Ruijie (config-ipv6-acl)# permit ipv6 20::/64  any
```

步骤二：定义路由图

```
Ruijie(config)# route-map rm_pbr  permit 10
Ruijie (config-route-map)# match ipv6 address acl_for_pbr1
Ruijie(config-route-map)# set ipv6 next-hop 2000::1
Ruijie(config-route-map)# exit
Ruijie(config)# route-map rm_pbr  permit 20
Ruijie(config-route-map)# match ipv6 address acl_for_pbr2
Ruijie(config-route-map)# set ipv6 next-hop 2000::2
Ruijie(config-route-map)# exit
```

步骤三：在接口上应用路由图

```
Ruijie(config)# interface GigabitEthernet 0/0
Ruijie(config-if)# no switchport
Ruijie(config-if)# ipv6 policy route-map rm_pbr
Ruijie(config-if)# exit
```

【检验方法】 1：使用 **show running-config** 命令查看配置。

【提示信息】 -

【常见错误】 -

【平台说明】 -

1.9 show ip pbr route

显示接口上应用的 IPv4 策略路由

show ip pbr route [**interface** *if-name* **| local**]

【参数说明】

参数	描述
interface *if-name*	指定 if-name，则显示指定接口上应用 IPv4 策略路由。 不带可选参数，显示所有应用 IPv4 策略路由的接口。
Local	显示 local 口上应用的 IPv4 策略路由。

【命令模式】 特权模式。

【缺省级别】 14

【使用指导】 为了验证接口配置的策略路由，可以使用该命令进行查看。

【配置举例】 1：显示接口配置的策略路由的情况。

```
Ruijie#show ip pbr route
PBR IPv4 Route Summay : 1
Interface        : GigabitEthernet 0/1
  Sequence       : 10
  ACL[0]         : 2900
  ACL_CLS[0]     : 0
  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
```

字段解释：

字段	说明

PBR IPv4 Route Summay	IPv4 策略路由条目数
Interface	应用策略路由的接口
Sequence	策略路由对应的序例号
ACL	Match 规则中引用的 ACL ID
ACL_CLS	Match 规则中引用的 ACL 类型，比如 IP 标准 ACL。
Min Length	Match length 中设置的匹配报文最小长度
Max Length	Match length 中设置的匹配报文最大长度
VRF ID	接口关联的 VRF ID
Route Flags	策略路由的标志位： Route Type ：策略路由类型，值为 PBR 表示 PBR 路由，值为 Normal 表示普通路由 Direct :策略路由的匹配模式，permit 或 deny Priority ：策略路由的优先级，High 或 Low Tos_Dscp ：是否设置 tos 或 dscp 规则 Precedence ：是否设置 set ip precedence 规则
Mode	设置下一跳为冗余备份或负载均衡模式
Nexthop Count	设置下一跳的个数，ECMP 最多支持 32 个下一跳
Nexthop	设置下一跳 IPv4 地址
Weight	设置下一跳权重值
Ifindex	设置下一跳对应的出接口索引

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。

【提示信息】 -

【平台说明】 -

1.10 show ip pbr route-map

显示 IPv4 PBR 应用的路由图信息

show ip pbr route-map *route-map-name*

【参数说明】

参数	描述
route-map-name	路由图的名称，是通过 **route-map** 命令配置的。

【命令模式】 特权模式。

【缺省级别】 14

【使用指导】 为了验证 IPv4 PBR 路由图信息，可以使用该命令进行查看。

【配置举例】 1：显示 IPv4 路由图信息

```
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 :      0, ACL CLS: 0, Name: acl1
    Set rule:
      IPv4 Nexthop: 192.168.8.100, (VRF Name: , ID: 0), Weight: 0
      PBR state info ifx: GigabitEthernet 0/1, Connected: True, Track State: Up
```

字段解释：

字段	说明
Pbr VRF	VRF 名称和 VRF ID
Forward Mode	设置下一跳为负载均衡或冗余备份模式
Forwarding	是否开启 IP 路由转发
Route-map index	路由子图序列号和类型
Match rule	Match 规则
Set rule	Set 规则
PBR state info	PBR 私有数据信息，比如下一跳的出接口及连接状态等

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。

【提示信息】 -

【平台说明】 -

1.11 show ip pbr statistics

显示 IPv4 PBR 转发的报文个数

show ip pbr statistics [**interface** *if-name* **| local**]

【参数说明】

参数	描述
interface *if-name*	指定 if-name，则显示指定接口上 IPv4 策略路由转发的报文个数 不带可选参数，显示所有应用 IPv4 策略路由的接口转发的报文个数
local	显示 local 口上 IPv4 策略路由转发的报文个数

【命令模式】 特权模式。

【缺省级别】 14

【使用指导】 为了验证 IPv4 策略路由转发的报文个数，可以使用该命令进行查看。

【配置举例】 1：显示 IPv4 策略路由转发的报文个数

```
Ruijie#show ip pbr statistics
IPv4 Policy-based route statistic
 gigabitEthernet 0/1
   statistics : 10
```

【提示信息】 -

【平台说明】 -

1.12 show ip policy

显示当前所有配置了策略路由的接口及该接口上应用的路由图的名称。

show ip policy [*route-map-name*]

【参数说明】

参数	描述
route-map-name	指定显示名称为 *route-map-name* 的路由图应用在哪几个接口上。 不带可选参数，显示所有配置了策略路由的接口。

【命令模式】 特权模式。

【缺省级别】 14

【使用指导】 为了验证当前系统配置的策略路由，可以使用该命令进行查看。

【配置举例】 1：显示当前系统配置的策略路由的情况。

```
Ruijie# show ip policy
Banlance Mode: redundance
Interface               Route map
local                   test
GigabitEthernet 0/0     test
```

字段解释：

字段	说明
Banlance Mode:	多个下一跳之间的运行模式。
Interface	接口名称。
Route map	路由图名称。

【提示信息】 -

【平台说明】 -

1.13 show ipv6 pbr route

显示接口上应用的 IPv6 策略路由

show ipv6 pbr route [**interface** *if-name* **| local**]

【参数说明】

参数	描述
interface *if-name*	指定 *if-name*，则显示指定接口上应用 IPv6 策略路由。 不带可选参数，显示所有应用 IPv6 策略路由的接口。
local	显示 local 口上应用的 IPv6 策略路由。

【命令模式】 特权模式。

【缺省级别】 14

【使用指导】 为了验证接口配置的策略路由，可以使用该命令进行查看。

【配置举例】 1：显示接口配置的策略路由的情况。

```
Ruijie#show ipv6 pbr route
PBR IPv6 Route Summary : 1
Interface        : GigabitEthernet 0/2
  Sequence       : 10
  ACL[0]         : 2901
  ACL_CLS[0]     : 0
  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::1
```

```
  Weight[0]     : 1
  Ifindex[0]    : 3
```

字段解释：同 **show ip pbr route** 命令。

【提示信息】 -

【平台说明】 -

1.14 show ipv6 pbr route-map

显示 IPv6 PBR 应用的路由图信息

show ipv6 pbr route-map *route-map-name*

【参数说明】

参数	描述
route-map-name	路由图的名称，是通过 **route-map** 命令配置的。

【命令模式】 特权模式。

【缺省级别】 14

【使用指导】 为了验证 IPv6 PBR 路由图信息，可以使用该命令进行查看。

【配置举例】 1：显示 IPv6 路由图信息

```
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 :      0, ACL CLS: 0, Name: acl6
    Set rule:
      IPv6 Nexthop: 10::1, (VRF Name: , ID: 0), Weight: 0
      PBR state info ifx: GigabitEthernet 0/0, Connected: True, Track State: Up
```

字段解释：

字段	说明
Pbr VRF	VRF 名称和 VRF ID
Forward Mode	设置下一跳为负载均衡或冗余备份模式
Forwarding	是否开启 IP 路由转发
Route-map index	路由子图序列号和类型

Match rule	Match 规则
Set rule	Set 规则
PBR state info	PBR 私有数据信息，比如下一跳的出接口及连接状态等

【提示信息】 -

【平台说明】 -

1.15 show ipv6 pbr statistics

显示 IPv6 PBR 转发的报文个数

show ipv6 pbr statistics [**interface** *if-name* **| local**]

【参数说明】

参数	描述
interface *if-name*	指定 if-name，则显示指定接口上 IPv6 策略路由转发的报文个数 不带可选参数，显示所有应用 IPv6 策略路由的接口转发的报文个数
local	显示 local 口上 IPv6 策略路由转发的报文个数

【命令模式】 特权模式。

【缺省级别】 14

【使用指导】 为了验证 IPv6 策略路由转发的报文个数，可以使用该命令进行查看。

【配置举例】 1：显示 IPv6 策略路由转发的报文个数

```
Ruijie#show ipv6 pbr statistics
IPv6 Policy-based route statistic
 gigabitEthernet 0/1
   statistics : 20
```

【提示信息】 -

【平台说明】 -

1.16 show ipv6 policy

显示当前所有配置了 IPv6 策略路由的接口及该接口上应用的路由图的名称。

show ipv6 policy [*route-map-name*]

【参数说明】

参数	描述

route-map-name	策略路由路由图名称

【命令模式】 特权模式。

【缺省级别】 14

【使用指导】 为了查看当前系统哪些三层接口应用了 IPv6 相关的策略路由，可以使用该命令

【配置举例】 1：显示了当前系统上应用的策略路由。

```
Ruijie#show ipv6 policy
Banlance Mode: redundance
Interface               Route map
VLAN 1                  RM_for_Vlan_1
VLAN 2                  RM_for_Vlan_2
```

字段解释：

字段	说明
Banlance Mode	当前设备策略路由运行模式
Interface	应用了策略路由的接口名称
Route map	被应用到接口上的路由图名称

【提示信息】 -

【平台说明】 -

2 ROUTE-DB

2.1 route-auto-choose

配置一条地址库命令。
route-auto-choose { **cnc** | **cnii** | **cernet** | **cmcc** | *word* } *interface next-hop* [**tag** *num*] [*distance*]

删除一条地址库配置。
no route-auto-choose { **cnc** | **cnii** | **cernet** | **cmcc** | *word* } *interface next-hop* [**tag** *num*] [*distance*]

恢复缺省配置。
default route-auto-choose { **cnc** | **cnii** | **cernet** | **cmcc** | *word* } *interface next-hop* [**tag** *num*] [*distance*]

【参数说明】

参数	描述
cnc	配置联通地址库。
cnii	配置电信地址库
cernet	配置教育网地址库。
cmcc	配置移动地址库。
word	配置其他类型的地址库
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。

【缺省配置】 缺省情况下为关闭此功能。

【命令模式】 全局配置模式

【缺省级别】 14

【使用指导】 通过配置本命令可以指定特定接口关联地址库。

【配置举例】 1：配置一条地址库命令，启用电信地址库，接口为 gigabitEthernet 0/1，下一跳地址为 202.100.12.5。

```
Ruijie# config
Ruijie(config)# route-auto-choose cnii gigabitEthernet 0/1 202.100.12.5
```

【检验方法】 使用 **show route-db-info cnii** 命令，可以查看对应的电信地址库信息。

【提示信息】 1：如果配置地址库的下一跳为本设备 ip，提示相应信息。

```
Ruijie(config)#route-auto-choose cmcc gi 0/5 192.168.55.111
%Invalid next hop address (it's this router)
```

【常见错误】 -

【平台说明】 -

2.2 route-auto-choose update

更新地址库文件，执行命令后根据当前的地址库文件更新正在执行的地址库，使文件更新后即配即用。
route-auto-choose update

【参数说明】

参数	描述
-	-

【命令模式】 全局配置模式

【缺省级别】 14

【使用指导】 通过此命令可以更新地址库。

【配置举例】 1：更新地址库文件

```
Ruijie# config
Ruijie(config)# route-auto-choose update
```

【提示信息】 -

【平台说明】 -

2.3 route-auto-choose user-defined

添加自定义地址库命令：
route-auto-choose user-defined name *string* [*ip_address ip_mask*]
删除自定义地址库的命令
no route-auto-choose user-defined name *string* [*ip_address ip_mask*]
通过设备上指定格式的自定义库文件，升级自定义库信息。
route-auto-choose user-defined update *file_path*

【参数说明】

参数	描述
string	自定义地址库的名称

ip_address	自定义地址库的 IP
ip_mask	自定义地址库的掩码
file_path	自定义地址库升级文件在 shell 目录下的绝对路径

【命令模式】 全局配置模式

【缺省级别】 14

【使用指导】 通过此命令可以添加自定义地址库，或对自定义地址库进行升级。

【配置举例】 1：创建并添加一条名为 test1 的自定义地址库，ip 为 1.2.3.0，掩码为 255.255.255.0

```
Ruijie# config
Ruijie(config)# route-auto-choose user-defined name test1 1.2.3.0 255.255.255.0
```

【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。

【提示信息】 1：如果重复配置某个自定义地址库信息时，提示如下信息

```
Ruijie(config)#route-auto-choose user-defined name test1
No need to create "test1": already exists
Ruijie(config)#route-auto-choose user-defined name test1 1.2.3.0 255.255.255.0
1.2.3.0 255.255.255.0 already exists in "test1"
```

2：自定义地址库不能添加私网和其它一些特殊网段的 ip，若添加则提示如下信息

```
Ruijie(config)#route-auto-choose user-defined name test1 10.2.3.0 255.255.255.0
Invalid ip or mask detected! Please check again.
```

【平台说明】 -

2.4 show route-db-info

查看地址库信息命令。

show route-db-info { **cnc** | **cnii** | **cernet** | **cmcc** | *word* | **db-type** | *ip_address* | **user-defined** }

【参数说明】

参数	描述
cnc	查询联通地址库信息
cnii	查询电信地址库信息
cernet	查询教育网地址库信息
cmcc	查询移动地址库信息
word	查询其他类型地址库信息
db-type	查询当前地址库文件中有多少运营商类型
ip_address	查询某个 ip 所属的运营商类型

user-defined	查询用户自定义地址库信息

【命令模式】 所有模式

【缺省级别】 14

【使用指导】 可以查询地址库信息。

【配置举例】 查询地址库中所有运营商类型

```
Ruijie# show route-db-info db-type
```

【检验方法】 显示出当前地址库文件中有多少运营商类型，一共三列，第一列为字母缩写，第二列为中文缩写，第三列为每个运营商的地址库版本。

【提示信息】 -

【常见错误】 -

【平台说明】 -

3 RIP

3.1 auto-summary

启用 RIP 路由自动汇总功能。
auto-summary

关闭路由自动汇总功能。
no auto-summary

【参数说明】

参数	描述
-	-

【缺省配置】 缺省启用自动汇总功能。

【命令模式】 路由进程配置模式。

【缺省级别】 14

【使用指导】 RIP 路由自动汇总，就是当子网路由穿越有类网络边界时，将自动汇总成有类网络路由。RIPv1 和 RIPv2 缺省情况下将进行路由自动汇总。
RIP 的路由自动汇总功能，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：

- 当查找 RIP 数据库时，汇总路由会得到优先处理；
- 当查找 RIP 数据库时，任何子路由将被忽略，减少了处理时间；
- 有时可能希望学到具体的子网路由 ,而不愿意只看到汇总后的网络路由 ,这时需要关闭路由自动汇总功能。但只有配置 RIPv2 时，才可以关闭路由自动汇总功能，RIPv1 总是应用路由自动汇总。

超网路由范围比有类网络更大，所以该命令对超网路由无效。

【配置举例】 1：关闭 RIPv2 的路由自动汇总。

```
Ruijie(config)# router rip
Ruijie(config-router)# version 2
Ruijie(config-router)# no auto-summary
```

【检验方法】 使用 show ip rip database 可以查看所配置的聚合路由

【提示信息】 -

【常见错误】 -

【平台说明】 -

3.2 default-information originate

在 RIP 进程里产生一条缺省路由

default-information originate [**always**] [**metric** *metric-value*] [**route-map** *map-name*]

取消生成缺省路由。

no default-information originate [**always**] [**metric**] [**route-map** *map-name*]

【参数说明】

参数	描述
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

【缺省配置】 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。

【命令模式】 路由进程配置模式

【缺省级别】 14

【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。

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。

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。

【配置举例】 1：产生一条缺省路由到 RIP 路由表。

```
Ruijie(config-router)# default-information originate always
```

【检验方法】 show ip rip database 查看是否有默认路由生成

【提示信息】 -

【常见错误】 -

【平台说明】 -

3.3 default-metric

定义 RIP 缺省的量度值。
default-metric *metric-value*

恢复缺省配置。
no default-metric

【参数说明】

参数	描述
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。

【缺省配置】 重分发路由缺省度量为 1。

【命令模式】 路由进程配置模式。

【缺省级别】 14

【使用指导】 该命令需要与路由协议配置命令 **redistribute** 配合使用。当路由从另外一个路由协议进程，重新分布到 RIP 路由进程时，由于不同路由协议的量度计算机制的不兼容性，路由量度值无法转换。因此在转换时，需要定义重分布路由在 RIP 路由域中的量度值。如果重分布一个路由协议进程时，没有明确定义量度值，RIP 将使用 default-metric 定义的量度值；如果有明确定义量度值，该值将覆盖 default-metric 定义的量度值。不配置该命令则 default-metric 值缺省为 1。

【配置举例】 1：RIP 路由协议对 OSPF 路由协议学到的路由进行重新分布，初始 RIP 量度值设置为 3。

```
Ruijie(config)# router rip
Ruijie(config-router)# default-metric 3
Ruijie(config-router)# redistribute ospf 100
```

【检验方法】 show ip rip database 查看重分发进 rip 的路由的度量是否有相应的变化

【提示信息】 -

【常见错误】 -

【平台说明】 -

3.4 distance

设置 RIP 路由的管理距离。
distance *distance* [*ip-address wildcard*]

恢复缺省设置。
no distance [*distance ip-address wildcard*]

【参数说明】

参数	描述
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。

【缺省配置】 管理距离缺省为 120。

【命令模式】 路由进程配置模式。

【缺省级别】 14

【使用指导】 使用该命令设置 RIP 路由的管理距离。
可以使用此命令创建多条带源地址前缀的管理距离，当 RIP 路由源地址在这些前缀范围内，则应用相应的管理距离，否则该路由应用 RIP 设置的管理距离。

【配置举例】 1：配置 RIP 路由管理距离为 160，指定从 192.168.12.1 学习到的路由的管理距离为 123。

```
Ruijie(config)# router rip
Ruijie(config-router)# distance 160
Ruijie(config-router)# distance 123 192.168.12.1 0.0.0.0
```

【检验方法】 使用 show ip rip 可以查看当前配置的管理距离

【提示信息】 1：配置的掩码错误。

```
% Invalid mask value
```

【常见错误】 1：该命令配置了错误的掩码

【平台说明】 -

3.5 distribute-list in

控制路由更新处理，以实现路由过滤。

distribute-list { [*access-list-number* | *name*] | **prefix** *prefix-list-name* [**gateway** *prefix-list-name*] | [**gateway** *prefix-list-name*] } **in** [*interface-type interface-number*]

删除控制路由更新处理，以实现路由过滤。

no distribute-list { [*access-list-number* | *name*] | **prefix** *prefix-list-name* [**gateway** *prefix-list-name*] | [**gateway** *prefix-list-name*] } **in** [*interface-type interface-number*]

【参数说明】

参数	描述
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。

【缺省配置】 缺省没有定义分布列表。

【命令模式】 路由进程配置模式。

【缺省级别】 14

【使用指导】 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。

【配置举例】 1：RIP 对从 Fastethernet 0/0 端口接收的路由进行控制处理，只允许接收 172.16 开头的路由。

```
Ruijie(config)# router rip
Ruijie(config-router)# network 200.168.23.0
Ruijie(config-router)# distribute-list 10 in fastethernet 0/0
Ruijie(config-router)# no auto-summary
Ruijie(config)# access-list 10 permit 172.16.0.0 0.0.255.255
```

【检验方法】 使用 show ip route rip 看过滤是否有生效

【提示信息】

【常见错误】 -

【平台说明】 -

3.6 distribute-list out

控制路由更新通告，以实现路由过滤。

distribute-list { [*access-list-number* | *name*] | **prefix** *prefix-list-name* } **out** [*interface* **|** [**connected | ospf** *process-id* **| rip | static**]]

删除控制路由更新通告，以实现路由过滤。

no distribute-list { [*access-list-number* | *name*] | **prefix** *prefix-list-name* } **out** [*interface* **|** [**connected | ospf** *process-id* **| rip | static**]]

【参数说明】

参数	描述
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。

【缺省配置】 缺省没有控制路由更新通告。

【命令模式】 路由进程配置模式。

【缺省级别】 14

【使用指导】 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。

【配置举例】 1：RIP 路由进程只对外通告 192.168.12.0/24 路由。

```
Ruijie(config)# router rip
Ruijie(config-router)# network 200.4.4.0
Ruijie(config-router)# network 192.168.12.0
Ruijie(config-router)# distribute-list 10 out
Ruijie(config-router)# version 2
Ruijie(config)# access-list 10 permit 192.168.12.0 0.0.0.255
```

【检验方法】 对端设备使用 show ip route rip 看过滤是否有生效。

【提示信息】 1：gateway 过滤默认不能用于 out 配置。

```
% Gateway not allowed with OUT in distribute-list cmd
```

【常见错误】 -

【平台说明】 -

3.7 graceful-restart

配置设备的 RIP 优雅重启(Graceful Restart，GR)功能。
graceful-restart [**grace-period** *grace-period*]

恢复为默认配置。
no graceful-restart [**grace-period**]

【参数说明】

参数	描述
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。

【缺省配置】 缺省使能 GR Restart 能力。

【命令模式】 路由进程配置模式。

【缺省级别】 14

【使用指导】 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。
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。
在 RIP 优雅重启运行过程中，请保持网络环境的稳定。

【配置举例】 1：使能 RIP 的 GR 功能以及配置 GR 功能的重启周期参数：

```
Ruijie(config)# router rip
Ruijie(config-router)# graceful-restart grace-period 90
```

【检验方法】 使用 show ip rip 查看当前 gr 是否已经开启和相应配置的 grace-period

【提示信息】 -

【常见错误】 -

【平台说明】 -

3.8 ip rip authentication key-chain

启用 RIP 认证，并指定 RIP 认证所使用的密钥串。
ip rip authentication key-chain *name-of-keychain*

删除指定的密钥串。
no ip rip authentication key-chain

【参数说明】

参数	描述
name-of-keychain	密钥串名字，指定 RIP 认证所使用的密钥串。

【缺省配置】 缺省未关联密钥串。

【命令模式】 接口配置模式。

【缺省级别】 14

【使用指导】 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。
RIPv1 不支持 RIP 数据包认证，只有 RIPv2 支持。

【配置举例】 1：fastEthernet 0/1 接口启用 RIP 认证，关联的密钥串为 ripchain：

```
Ruijie(config)# interface fastEthernet 0/1
Ruijie(config-if-FastEthernet 0/1)# ip rip authentication key-chain ripchain
```

2：使用 **key chain** 定义该密钥串：

```
Ruijie(config)# key chain ripchain
Ruijie(config-keychain)# key 1
Ruijie(config-keychain-key)# key-string Hello
```

【检验方法】 show ip rip interface 查看相关配置。

【提示信息】 -

【常见错误】 1：配置 md5 认证的时候，没有优先配置 key-chain。

【平台说明】 -

3.9 ip rip authentication mode

定义 RIP 认证的模式。
ip rip authentication mode { **text** | **md5** }

恢复缺省 RIP 认证模式。
no ip rip authentication mode

【参数说明】

参数	描述
text	RIP 认证模式为明文认证。
md5	RIP 认证模式为 MD5 认证。

【缺省配置】 缺省为明文认证模式。

【命令模式】 接口配置模式。

【缺省级别】 14

【使用指导】 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。
RIPv1 不支持 RIP 数据包认证，只有 RIPv2 支持。

【配置举例】 1：fastEthernet 0/1 接口的 RIP 认证模式设为 MD5。

```
Ruijie(config)# interface fastEthernet 0/1
Ruijie(config-if-FastEthernet 0/1)# ip rip authentication mode md5
```

【检验方法】 show ip rip interface 查看相关配置

【提示信息】 -

【常见错误】 -

【平台说明】 -

3.10 ip rip authentication text-password

启用 RIP 认证，并设置 RIP 明文认证字符串。

ip rip authentication text-password [**0** | **7**] *password-string*

删除明文认证的字符串。

no ip rip authentication text-password

【参数说明】

参数	描述
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。

【缺省配置】 缺省未设置明文认证字符串。

【命令模式】 接口配置模式。

【缺省级别】 14

【使用指导】 该命令仅在明文认证模式下生效。

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。

RIPv1 不支持 RIP 数据包认证，只有 RIPv2 支持。

【配置举例】 1：fastEthernet 0/1 接口的启用 RIP 明文认证，设置明文认证字符串为 hello。

```
Ruijie(config)# interface fastEthernet 0/1
Ruijie(config-if-FastEthernet 0/1)# ip rip authentication text-password hello
```

【检验方法】 show ip rip interface 查看相关配置

【提示信息】 -

【常见错误】 -

【平台说明】 -

3.11 ip rip default-information

在某 RIP 接口进行缺省路由通告。

ip rip default-information { **only** | **originate** } [**metric** *metric-value*]

取消在该接口通告缺省路由。
no ip rip default-information

【参数说明】

参数	描述
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

【缺省配置】 默认没有缺省路由配置。*metric* 默认为 1。

【命令模式】 接口配置模式。

【缺省级别】 14

【使用指导】 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。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。

【配置举例】 1：在接口 ethernet0/1 上创建一条缺省路由，该接口只通告该缺省路由。

```
Ruijie(config)# interface ethernet 0/1
Ruijie(config-if-Ethernet 0/1)# ip rip default-information only
```

【检验方法】 使用 show ip rip interface 来查看该接口 default-information 配置状态

【提示信息】

【常见错误】 -

【平台说明】 -

3.12 ip rip receive enable

允许 RIP 在一个指定接口上接收 RIP 数据包.
ip rip receive enable

禁止 RIP 在一个指定接口上接收 RIP 数据包。
no ip rip receive enable

【参数说明】

参数	描述
-	-

【缺省配置】 缺省允许接口接收 RIP 数据包

【命令模式】 接口配置模式。

【缺省级别】 14

【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。

【配置举例】 1：fastEthernet 0/1 接口禁止接收 RIP 的数据包。

```
Ruijie(config)# interface fastEthernet 0/1
Ruijie(config-if-FastEthernet 0/1)# no ip rip receive enable
```

【检验方法】 使用 show ip rip interface 来查看该接口的收包配置状态

【提示信息】 -

【常见错误】 -

【平台说明】 -

3.13 ip rip receive version

定义 RIP 在一个接口上将接收哪个版本的 RIP 数据包.
ip rip receive version [**1**] [**2**]

恢复缺省配置。
no ip rip receive version

【参数说明】

参数	描述
1	只接收 RIPv1 的数据包。
2	只接收 RIPv2 的数据包。

【缺省配置】 缺省行为取决于 **version** 命令的配置。

【命令模式】 接口配置模式。

【缺省级别】 14

【使用指导】 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】 1：使 fastEthernet 0/1 接口可以接收 RIPv1 和 RIPv2 的数据包。

```
Ruijie(config)# interface fastEthernet 0/1
Ruijie(config-if-FastEthernet 0/1)# ip rip receive version 1 2
```

【检验方法】 使用 show ip rip interface 或 show ip rip 来查看接口接收 RIP 报文版本号的状态

【提示信息】 -

【常见错误】 -

【平台说明】 -

3.14 ip rip send enable

允许 RIP 在一个指定接口上发送 RIP 数据包.
ip rip send enable

禁止 RIP 在一个指定接口上发送 RIP 数据包。
no ip rip send enable

【参数说明】

参数	描述
-	-

【缺省配置】 缺省允许接口发送 RIP 数据包

【命令模式】 接口配置模式

【缺省级别】 14

【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。

【配置举例】 1：使 fastEthernet 0/0 接口禁止发送 RIP 的数据包。

```
Ruijie(config)# interface fastEthernet 0/1
Ruijie(config-if-FastEthernet 0/1)# no ip rip send enable
```

【检验方法】 使用 show ip rip interface 来查看该接口的发包配置状态

【提示信息】 -

【常见错误】 -

【平台说明】 -

3.15 ip rip send supernet-routes

允许 RIP 在一个指定接口上发送 RIP 超网路由。
ip rip send supernet-routes

禁止 RIP 在一个指定接口上发送 RIP 超网路由。
no ip rip send supernet-routes

【参数说明】

参数	描述
-	-

【缺省配置】 缺省允许接口发送 RIP 超网路由

【命令模式】 接口配置模式

【缺省级别】 14

【使用指导】 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。

【配置举例】 1：使 fastEthernet 0/1 接口禁止发送 RIP 的超网路由。

```
Ruijie(config)# interface fastEthernet 0/1
Ruijie(config-if-FastEthernet 0/1)# no ip rip send supernet-routes
```

【检验方法】 show running-config 查看是否配置成功

【提示信息】 -

【常见错误】 -

【平台说明】 -

3.16 ip rip send version

定义 RIP 在一个接口上将发送哪个版本的 RIP 数据包。
ip rip send version [**1**] [**2**]

恢复缺省配置。
no ip rip send version

【参数说明】

参数	描述
1	只发送 RIPv1 的数据包。
2	只发送 RIPv2 的数据包。

【缺省配置】 缺省行为取决于 **version** 命令的配置。

【命令模式】 接口配置模式。

【缺省级别】 14

【使用指导】 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。

【配置举例】 1：使 fastEthernet 0/1 接口可以发送 RIPv1 和 RIPv2 的数据包。

```
Ruijie(config)# interface fastEthernet 0/1
Ruijie(config-if-FastEthernet 0/1)# ip rip send version 1 2
```

【检验方法】 使用 show ip rip interface 或 show ip rip 来查看接口发送 RIP 报文版本号的状态

【提示信息】 -

【常见错误】 -

【平台说明】 -

3.17 ip rip split-horizon

启用 RIP 水平分割功能。
ip rip split-horizon [**poisoned-reverse**]

关闭 RIP 水平分割功能。
no ip rip split-horizon [**poisoned-reverse**]

【参数说明】

参数	描述
poisoned-reverse	启用带毒性逆转的水平分割

【缺省配置】 启用不带毒性逆转的水平分割

【命令模式】 接口配置模式。

【缺省级别】 14

【使用指导】 多台设备连接在 IP 广播类型网络上，又运行距离向量路由协议时，就有必要采用水平分割的机制以避免路由环路的形成。水平分割可以防止设备将某些路由信息从学习到这些路由信息的接口通告出去，这种行为优化了多个设备之间的路由信息交换。
然而对于非广播多路访问网络（如帧中继、X.25 网络），水平分割可能造成部分设备学习不到全部的路由信息。在这种情况下，可能需要关闭水平分割。如果一个接口配置了次 IP 地址，也需要注意水平分割的问题。
如果配置了 **poisoned-reverse** 参数，将启用带毒性逆转的水平分割，设备仍然会将路由信息从学习到这些路由信息的接口通告出去，但是将路由信息的度量值设置为不可达。
RIP 路由协议属于距离向量路由协议，在实际应用中要注意水平分割问题。如果不能确定一个接口是否启用了水平分割，可以用 show ip rip 命令进行判断。另外通过 **neighbor** 命令定义的邻居，将不会受到 RIP 水平分割的影响。

【配置举例】 1：fastEthernet 0/1 接口关闭 RIP 水平分割功能。

```
Ruijie(config)# interface fastEthernet 0/1
Ruijie(config-if-FastEthernet 0/1)# no ip rip split-horizon
```

【检验方法】 使用 show ip rip interface 看水平分割是否配置成功

【提示信息】 -

【常见错误】 -

【平台说明】 -

3.18 ip rip summary-address

在某个接口下配置 RIP 的接口级汇聚。
ip rip summary-address *ip-address ip-network-mask*

关闭指定地址或子网的汇聚。
no ip rip summary-address *ip-address ip-network-mask*

【参数说明】

参数	描述
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

【缺省配置】 RIP 自动汇聚到有类网络边界

【命令模式】 接口配置模式。

【缺省级别】 14

【使用指导】 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。

【配置举例】 1：关闭 RIPv2 的路由自动汇总。配置接口汇聚，fastEthernet 0/1 将通告汇聚后的路由 172.16.0.0/16。

```
Ruijie(config)# interface fastEthernet 0/1
Ruijie(config-if-FastEthernet 0/1)# ip rip summary-address 172.16.0.0 255.255.0.0
Ruijie(config-if-FastEthernet 0/1)# ip address 172.16.1.1 255.255.255.0
Ruijie(config)# router rip
Ruijie(config-router)# network 172.16.0.0
Ruijie(config-router)# version 2
Ruijie(config-router)# no auto-summary
```

【检验方法】

【提示信息】 1：输入的掩码错误，请使用正确的掩码

```
RIP: Invalid mask input
```

2：汇聚的地址错误，如 0 地址等

```
% Invalid summary-address value.
```

3：汇聚的掩码应该比主网的掩码来长度来的大

```
% Summary mask must be greater or equal to major net.
```

【常见错误】 -

【平台说明】 -

3.19 ip rip triggered

启用按需链路的 RIP 触发扩展功能。

ip rip triggered

关闭 RIP 触发扩展功能。
no ip rip triggered

配置按需链路的 RIP 触发扩展的重传时间
ip rip triggered retransmit-timer *timer*

恢复按需链路的 RIP 触发扩展的重传时间
no ip rip triggered retransmit-timer

配置按需链路的 RIP 触发扩展的重传次数
ip rip triggered retransmit-count *count*

恢复按需链路的 RIP 触发扩展的重传次数
no ip rip triggered retransmit-count

【参数说明】

参数	描述
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

【缺省配置】 缺省未启用 RIP 触发扩展功能

【命令模式】 接口配置模式。

【缺省级别】 14

【使用指导】 RIP 触发扩展功能（TRIP，Triggered RIP）是 RIP 协议在广域网（WAN，Wide Area Network）上的扩展，主要应用于按需链路。
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。

由于取消了 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。
在以下两种情况下允许启用该功能：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 PPP、帧中继、X.25 等链路层协议上启用该功能；

建议在配置该功能的接口上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；
必须要保证同一链路的所有路由设备都启用了该功能，否则将导致该功能失效，无法正确交互路由信息；
不支持该功能与 BFD 联动 RIP 功能同时启用；
启用该功能时，请保证链路两端的 RIP 配置一致，如：RIP 认证，接口支持的 RIP 协议版本等；
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**），对该接口的报文都进行源地址校验。

【配置举例】 1：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。

```
Ruijie(config)# interface fastEthernet 0/1
Ruijie(config-if-FastEthernet 0/1)# ip rip triggered
Ruijie(config-if-FastEthernet 0/1)# ip rip triggered retransmit-timer 10
Ruijie(config-if-FastEthernet 0/1)# ip rip triggered retransmit-count 18
```

【检验方法】 Show running-config 查看是否配置成功

【提示信息】 1：提示开启 triggered 有可能会影响路由学习

```
% Warning: The configurations for Triggered RIP peer shall be same, or it would affect the route learning.
```

【常见错误】 -

【平台说明】 -

3.20 ip rip v2-broadcast

允许 RIP version 2 报文以广播而非多播的方式在接口上发送报文。
ip rip v2-broadcast

恢复缺省配置。
no ip rip v2-broadcast

【参数说明】

参数	描述
-	-

【缺省配置】 缺省行为取决于 **version** 命令的配置。

【命令模式】 接口配置模式。

【缺省级别】 14

【使用指导】 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。

【配置举例】 1：使 fastEthernet 0/1 接口以广播发送 RIPv2 报文。

```
Ruijie(config)# interface fastEthernet 0/1
Ruijie(config-if-FastEthernet 0/1)# ip rip v2-broadcast
```

【检验方法】 使用 show ip rip interface 来查看配置是否成功

【提示信息】 -

【常见错误】 -

【平台说明】 -

3.21 neighbor

定义 RIP 邻居的 IP 地址。
neighbor *ip-address*

删除邻居定义。
no neighbor *ip-address*

【参数说明】

参数	描述
ip-address	邻居的 IP 地址。应该是本地设备直连网络地址。

【缺省配置】 缺省没有定义邻居。

【命令模式】 路由进程配置模式

【缺省级别】 14

【使用指导】 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。

【配置举例】 1：定义 RIP 只向邻居 192.168.1.2 通告路由信息。

```
Ruijie(config)# router rip
Ruijie(config-router)# passive-interface default
Ruijie(config-router)# neighbor 192.168.1.2
```

【检验方法】 Show running-config 查看是否配置成功

【提示信息】 1：相同配置已经存在。

```
% Static neighbor configuration exists
```

【常见错误】 -

【平台说明】 -

3.22 network

定义 RIP 路由进程要通告的网络列表。

network *network-number* [*wildcard*]

删除已定义的网络。

no network *network-number* [*wildcard*]

【参数说明】

参数	描述
network-number	直连网络的网络号。该网络号为自然类网络号，IP 地址属于该自然网络的所有接口都可发送和接收 RIP 数据包。
wildcard	定义 IP 地址比较比特位，0 表示精确匹配，1 表不做比较。

【缺省配置】 -

【命令模式】 路由进程配置模式。

【缺省级别】 14

【使用指导】 用户可以同时配置 *network-number* 和 *wildcard* 参数，使落在该地址范围内的接口地址参与 RIP 运行。

如果未配置 *wildcard* 参数，RGOS 将默认按照有类地址范围来处理，使落在该有类地址范围内的接口地址参与 RIP 运行。

只有接口地址落在 RIP 定义的网络列表中，该接口才可以对外发送 RIP 路由更新报文，并接收 RIP 路由更新报文。

【配置举例】 1：允许落在 192.168.12.0/24 和 172.16.0.0/24 范围内的接口地址参与 RIP 运行：

```
Ruijie(config)# router rip
Ruijie(config-router)# network 192.168.12.0
Ruijie(config-router)# network 172.16.0.0 0.0.0.255
```

【检验方法】 Show running-config 查看是否配置成功，也可以使用 show ip rip interface 查看接口是否已经加入到 RIP 进程

中。

【提示信息】

【常见错误】 -

【平台说明】 -

3.23 offset-list

增加接收或发送的 RIP 路由的 metric 值。

offset-list { *access-list-number* | *name* } { **in** | **out** } *offset* [*interface-type interface-number*]

删除指定的 offset 列表。

no offset-list { *access-list-number* | *name* } { **in** | **out** } *offset* [*interface-type interface-number*]

【参数说明】

参数	描述
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

【缺省配置】 缺省没有指定 offset。

【命令模式】 路由进程配置模式。

【缺省级别】 14

【使用指导】 若某条 RIP 路由同时满足指定接口的 offset-list 以及未指定接口的全局 offset-list，则该 RIP 路由将会增加指定接口的 offset-list 的 metric 值。

【配置举例】 1：在 acl 7 指定的范围内的 RIP 路由才会对 metric 增加 7。

```
Ruijie(config-router)# offset-list 7 out 7
```

2：通过 fastethernet0/1 学习的在 acl 8 指定的范围内的 RIP 路由才会对 metric 增加 7。

```
Ruijie(config-router)# offset-list 8 in 7 fastethernet 0/1
```

【检验方法】 使用 show ip rip database 来查看接口进来的路由是否有增加该命令对应设置的值

【提示信息】 1：接口不存在或着接口非法。

```
% Interface is invalid.
```

【常见错误】 -

【平台说明】 -

3.24 output-delay

改变 RIP 更新报文的发送延时。
output-delay *delay*

取消对更新报文的发送延时设置。
no output-delay

【参数说明】

参数	描述
Delay	设置报文间发送延时，单位为毫秒，范围是<8-50>

【缺省配置】 缺省设置为无发送延时。

【命令模式】 路由进程配置模式。

【缺省级别】 14

【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】 1：将 RIP 的更新报文发送延时设置为 30 毫秒

```
Ruijie(config)# router rip
Ruijie(config-router)# output-delay 30
```

【检验方法】 -

【提示信息】 -

【常见错误】 -

【平台说明】 -

3.25 passive-interface

取消在一个接口上发送更新报文的功能。
passive-interface { **default** | *interface-type interface-num* }

重新启用发送更新报文的功能。
no passive-interface { **default** | *interface-type interface-num* }

【参数说明】

参数	描述
default	该参数设置所有接口为 passive 模式
interface-type interface-num	接口类型与序号

【缺省配置】 缺省情况下，接口为非 passive 模式。

【命令模式】 路由进程配置模式。

【缺省级别】 14

【使用指导】 **passive-interface default** 命令将所有接口设置为 passive 模式，这时可以使用 **no passive-interface** *interface-type interface-num* 命令设置某些接口为非 passive 模式。
将接口设置为 passive 模式后，接口将不再发送 RIP 路由更新，但仍然能够接收 RIP 路由更新报文。此时在这些接口上可以通过 neighbor 命令向指定的邻居发送路由更新。
如果要完全控制接口是否发送和接收路由更新报文，请使用命令 ip rip send enable 和 ip rip receive enable 来控制。

【配置举例】 1：设置所有接口为 passive 模式，然后设置 ethernet0/1 为非 passive 模式

```
Ruijie(config-router)# passive-interface default
Ruijie(config-router)# no passive-interface ethernet 0/1
```

【检验方法】 使用 show ip rip 或者 show ip rip interface 来查看实例和接口的被动口配置

【提示信息】 1：接口不存在或着接口非法。

```
% Interface is invalid.
```

【常见错误】 -

【平台说明】 -

3.26 redistribute

配置重分布外部路由信息。

redistribute { **connected** | **ospf** *process-id* | **static** } [**match** { **internal | external** [**1 | 2**] **| nssa-external** [**1 | 2**] }] [**metric** *metric-value*] [**route-map** *route-map-name*]

取消重分布外部路由。

no 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】

参数	描述
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

【缺省配置】 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。

【命令模式】 路由进程配置模式。

【缺省级别】 14

【使用指导】 使用该命令将外部路由信息重分布到 RIP 中。

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。

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。

⚠ 重分布命令不能将其他协议的缺省路由引入到 RIP 中，如果要引入缺省路由到 RIP，请使用 **default-information originate** 命令。

【配置举例】 1：重分布静态路由到 RIP

```
Ruijie(config-router)# redistribute static
```

【检验方法】 使用 show ip rip database 查看重分发所配置的路由协议中的路由是否有进入到 rip 的数据库当中。

【提示信息】 -

【常见错误】 -

【平台说明】 -

3.27 router rip

创建 RIP 路由进程并进入路由进程配置模式。
router rip

删除 RIP 路由进程。
no router rip

【参数说明】

参数	描述
-	-

【缺省配置】 没有 RIP 路由进程在运行。

【命令模式】 全局配置模式。

【缺省级别】 14

【使用指导】 一个 RIP 路由进程，至少要定义一个网络号。如果异步线路上运行动态路由协议，需要在异步接口配置 **async default routing**。

【配置举例】 1：创建 RIP 路由进程，进入路由进程配置模式。

```
Ruijie(config)# router rip
Ruijie(config-router)#
```

【检验方法】 使用 show ip rip 查看实例是否创建成功，成功则会有对应的信息输出

【提示信息】 -

【常见错误】 -

【平台说明】 -

3.28 show ip rip

显示 RIP 路由协议进程的基本信息。

show ip rip

【参数说明】

参数	描述
-	-

【命令模式】 特权模式、全局配置模式、路由进程配置模式。

【缺省级别】 14

【使用指导】 可用于快速显示 RIP 路由协议进程的三个计时器、路由分发、路由重分布状态、接口 rip 版本、rip 接口与网络范围、metric 与 distance 等。

【配置举例】 1：显示 RIP 路由协议进程的基本信息，如更新时间、管理距离等。

```
Ruijie# show ip rip
Routing Protocol is "rip"
Sending updates every 10 seconds
Invalid after 20 seconds, flushed after 10 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 2
Redistributing: connected
Default version control: send version 2, receive version 2
Interface              Send  Recv
FastEthernet 0/1       2     2
FastEthernet 0/2       2     2
Routing for Networks:
192.168.26.0 255.255.255.0
192.168.64.0 255.255.255.0
Distance: (default is 50)
Graceful-restart enabled
  Restart grace period 60 secs
  Current Restart remaining time 16 secs
```

字段解释：

字段	说明
Sending updates	报文更新时间

Invalid	失效时间
flushed	刷新时间
Outgoing update filter list for all interface	对所有输出的路由进行过滤
Incoming update filter list for all interface	对接收的所有路由进行过滤
Default redistribution metric	默认配置的重分发度量
Redistributing	重分发的协议
Default version control	实例默认运行的 RIP 协议版本
Routing for Networks:	RIP 向外通告的路由网段
Distance	实例的管理距离
Graceful-restart	GR 功能是否开启
Restart grace period	GR 时间
Current Restart remaining time	剩余的 GR 时间

【提示信息】 -

【平台说明】 -

3.29 show ip rip database

显示 RIP 路由数据库中路由汇总信息。

show ip rip database [*network-number network-mask*] [**count**]

【参数说明】

参数	描述
network-number	路由信息的子网号。
network-mask	子网掩码。如果网络号设定，子网掩码必须指定
count	显示 RIP 数据库中的路由统计信息摘要

【命令模式】 特权模式、全局配置模式、路由进程配置模式。

【缺省级别】 14

【使用指导】 当相关的子路由被汇总时，汇总地址项目信息才会显示在 RIP 路由数据库中。当汇总地址项目信息的最后一个子路由信息变为无效时，汇总地址信息也将从数据库中删除。

【配置举例】 1：显示 RIP 路由数据库中所有汇总地址项目信息

```
Ruijie# show ip rip database
192.168.1.0/24      auto-summary
192.168.1.0/30      directly connected, Loopback 3
```

```
192.168.1.8/30      directly connected, FastEthernet 0/1
192.168.121.0/24    auto-summary
192.168.121.0/24    redistributed
 [1] via 192.168.2.22, FastEthernet 0/2
192.168.122.0/24    auto-summary
192.168.122.0/24
 [1] via 192.168.4.22, Serial 0/1  00:28    permanent
```

2：显示 RIP 路由数据库中关于 192.168.121.0/24 的汇总地址项目信息

```
Ruijie# show ip rip database 192.168.121.0 255.255.255.0
192.168.121.0/24    redistributed
 [1] via 192.168.2.22, FastEthernet 0/1
```

3：显示 RIP 路由数据库中各种类型路由的统计信息摘要

```
Ruijie# show ip rip database count
                All     Valid   Invalid
database        5       5       0
auto-summary    5       5       0

connected       1       1       0
rip             4       4       0
```

字段解释：

字段	说明
auto-summary	汇总后的路由
directly connected	直连的路由
redistributed	重分发进来的路由
database	Rip 自己的路由数据库
All	所有路由计数
Valid	有效路由计数
Invalid	无效路由计数

【提示信息】

【平台说明】 -

3.30 show ip rip external

显示 RIP 重分布的外部路由信息。

show ip rip external [**connected** | **ospf** *process-id* | **static**]

【参数说明】

参数	描述
connected	显示重分布的直连路由。
ospf *process-id*	显示重分布的 OSPF 路由。*process-id* 为 OSPF 进程号，取值范围 1-65535
static	显示重分布的静态路由。

【命令模式】 特权模式、全局配置模式、路由进程配置模式。

【缺省级别】 14

【使用指导】

【配置举例】 1：显示 RIP 重分布的直连路由信息。

```
Ruijie# show ip rip external
Protocol connected route:
[connected] 192.100.3.0/24 metric=0
     nhop=0.0.0.0, if=2
 [connected] 192.101.1.0/24 metric=0
     nhop=0.0.0.0, if=3
Protocol static route:
 [static] 10.1.1.1/32 metric=0
     nhop=0.0.0.0, if=4096
 [static] 10.1.2.1/32 metric=0
     nhop=0.0.0.0, if=4096
Protocol ospf 1 route:
 [ospf] 1.1.1.1/32 metric=2
     nhop=192.100.3.2, if=2
 [ospf] 90.1.1.1/32 metric=2
     nhop=192.100.3.2, if=2
```

字段解释：

字段	说明
Protocol connected route	重分发的路由类型
connected	重分发的路由
metric	重分发路由度量
nhop	重分发路由下一跳
if	重分发路由的出接口

【提示信息】 14

【平台说明】 -

3.31 show ip rip interface

显示 RIP 接口信息。

show ip rip interface [*interface-type interface-number*]

【参数说明】

参数	描述
-	-
interface-type interface-number	指定的接口类型和编号

【命令模式】 特权模式、全局配置模式、路由进程配置模式。

【缺省级别】 14

【使用指导】 该命令用于显示 RIP 接口信息，若不存在 RIP 接口，则不显示任何信息。

【配置举例】 1：显示 RIP 的接口信息。

```
Ruijie# show ip rip interface
FastEthernet 0/1 is up, line protocol is up
Routing Protocol: RIP
Receive RIPv2 packets only
Send RIPv2 packets only
Recv RIP packet total: 0
Send RIP packet total: 3
Passive interface: Disabled
Split Horizon with Poisoned Reverse: Enabled
Triggered RIP Enabled:
Retransmit-timer: 5, Retransmit-count: 36
V2 Broadcast: Disabled
Multicast registe: Registed
Interface Summary Rip:
Not Configured
Authentication mode: Text
Authentication key-chain: ripk1
Authentication text-password: ruijie
Default-information: only, metric 5
IP interface address:
192.168.64.100/24, next update due in 14 seconds
```

```
2.2.1.1/24, next update due in 24 seconds
    neighbor 2.2.1.6, next update due in 3 seconds
    neighbor 2.2.1.77, next update due in 13 seconds
2.2.2.57/24, next update due in 16 seconds
```

如果启用 RIP 与 BFD 联动，会增加显示 BFD 信息:

```
Ruijie#show ip rip interface
Serial 0/1 is up, line protocol is up
  Routing Protocol: RIP
    Receive RIPv1 and RIPv2 packets
    Send RIPv1 packets only
    Receive RIP packet: Enabled
    Send RIP packet: Enabled
    Send RIP supernet routes: Enabled
    Recv RIP packet total: 0
    Send RIP packet total: 3
    Passive interface: Disabled
Split Horizon: Enabled
Triggered RIP Disabled
    BFD: Enabled
    V2 Broadcast: Disabled
    Multicast registe: Registed
    Interface Summary Rip:
      Not Configured
    IP interface address:
      2.2.2.111/24, next update due in 14 seconds
```

字段解释：

字段	说明
Receive RIPv1 and RIPv2 packets	接口可以接收什么类型的报文
Send RIPv1 packets only	接口可以发送什么类型的报文
Receive RIP packet	接口是否允许接收报文
Send RIP packet	接口是否允许发送报文
Passive interface	被动口是否开启
Send RIP supernet routes	接口是否允许发送超网路由
Recv RIP packet total	接口接收报文总数
Send RIP packet total	接口发送报文总数
Split Horizon with Poisoned Reverse	水平分割毒性反正是否开启
Triggered RIP	Triggered 功能是否开启
Retransmit-timer	重发时间
Retransmit-count	重发次数
V2 Broadcast	V2 广播报文
Multicast register	组播是否注册

Interface Summary Rip	接口是否开启汇总
Authentication mode	认证模式
Authentication key-chain	认证使用的 key-chain
Authentication text-password	认证字符串
Default-information	默认度量，默认路由等信息
IP interface address	接口的 ip 地址
BFD	是否开启 bfd 功能

【提示信息】 -

【平台说明】 -

3.32 show ip rip peer

显示 RIP 邻居信息。

show ip rip peer [*ip-address*]

【参数说明】

参数	描述
ip-address	指定的 RIP 邻居地址

【命令模式】 特权模式、全局配置模式、路由进程配置模式。

【缺省级别】 14

【使用指导】 RIP 为学习到的 RIP 的路由信息源(RIP 路由更新报文的源地址)记录了摘要信息，以方便用户监控，这些路由信息源被称为 RIP 邻居信息。

该命令用于显示 RIP 邻居信息，若不存在 RIP 邻居，则不显示任何信息。

【配置举例】 1：显示 RIP 的邻居信息。

```
Ruijie# show ip rip peer
Peer 192.168.3.2:
  Local address: 192.168.3.1
  Input interface: GigabitEthernet 0/2
  Peer version: RIPv1
  Received bad packets: 3
  Received bad routes: 0
  BFD session state up
```

字段解释：

字段	说明
Peer	邻居 ip 地址
Local address	本地地址
Input interface	相连的接口
Peer version	邻居的 RIP 版本号
Received bad packets	从邻居收到的错误的报文
Received bad routes	收到错误路由
BFD session state	BFD 会话状态

【提示信息】 -

【平台说明】 -

3.33 timers basic

调整 RIP 的时钟。

timers basic *update invalid flush*

恢复缺省配置。

no timers basic

【参数说明】

参数	描述
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。

【缺省配置】 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。

【命令模式】 路由进程配置模式。

【缺省级别】 14

【使用指导】 通过调整以上时钟，可能会加快路由协议的收敛时间以及故障恢复时间。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。
当前的 RIP 时钟参数设置，可以用 **show ip rip** 命令进行查看。

⚠ 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。

【配置举例】 1：配置 RIP 更新报文每隔 10 秒种发送一次。如果 30 秒内没有收到更新报文，相应的路由将变为无效路由，并进入 invalid 状态；该路由进入 invalid 状态后，超过 90 秒，将被清除。

```
Ruijie(config)# router rip
Ruijie(config-router)# timers basic 10 30 90
```

【检验方法】 使用 show ip rip 查看各个时间配置的值

【提示信息】 -

【常见错误】 不同设备的 RIP 进程更新时间等设置的不一致

【平台说明】 -

3.34 validate-update-source

对接收到的 RIP 路由更新报文的源地址，进行有效性验证。
validate-update-source

关闭更新报文源地址验证。
no validate-update-source

【参数说明】

参数	描述
-	-

【缺省配置】 缺省启用更新报文源地址验证。

【命令模式】 路由进程配置模式。

【缺省级别】 14

【使用指导】 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。
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。
另外对于 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**。

【配置举例】 1：关闭更新报文源地址验证。

```
Ruijie(config)# router rip
Ruijie(config-router)# no validate-update-source
```

【检验方法】 使用 show running-config 查看配置是否成功

【提示信息】 -

【常见错误】 -

【平台说明】 -

3.35 version

定义整个设备的 RIP 版本号。
version { **1** | **2** }

恢复缺省配置。
no version

【参数说明】

参数	描述
1	定义 RIP 版本号为 1。
2	定义 RIP 版本号为 2。

【缺省配置】 缺省可以接收 RIPv1 和 RIPv2 的路由更新报文，但只发送 RIPv1 的路由更新报文。

【命令模式】 路由进程配置模式。

【缺省级别】 14

【使用指导】 用于定义整个设备 RIP 运行的版本号。可以用 **ip rip receive version**、**ip rip send version** 命令，对每个接口处理哪个版本的 RIP 报文进行重新定义。

【配置举例】 1：将 RIP 的版本号设置为 2。

```
Ruijie(config)# router rip
Ruijie(config-router)# version 2
```

【检验方法】 使用 show ip rip 查看当前配置的版本

【提示信息】 -

【常见错误】 1：将本端 RIP 实例设置成 version 1，而对端发送过来的是 version 2 的报文，造成解析失败

【平台说明】 -

4 RIPNG

4.1 clear ipv6 rip

清除 RIPng 路由。
clear ipv6 rip

【参数说明】

参数	描述
-	-

【命令模式】 特权模式。

【缺省级别】 14

【使用指导】 执行该命令会删除所有 RIPng 下发的路由，对整个协议影响较大。
执行此命令要慎重。

【配置举例】 1：清除 RIPng 路由

```
Ruijie# clear ipv6 rip
```

【提示信息】 -

【平台说明】 -

4.2 default-metric

定义重分布其它路由协议时 RIPng 缺省的度量值。
default-metric *metric*

恢复缺省配置。
no default-metric

【参数说明】

参数	描述
metric	缺省的度量值，有效值为 1 到 16。如果 metric 值大于等于 16，设备将认为该路由不可达。

【缺省配置】 重分发路由度量缺省为 1

【命令模式】 路由进程配置模式

【缺省级别】 14

【使用指导】 该命令需要与路由协议配置命令 **redistribute** 配合使用。当路由从另外一个路由协议进程，重新分布到 RIP 路由进程时，由于不同路由协议的度量计算机制的不兼容性，路由度量值无法转换。因此在转换时，需要定义重分布路由在 RIP 路由域中的度量值。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】 1：重分布 OSPF 100 进程的路由到 RIP 路由进程时，度量值设置为 3。

```
Ruijie(config-router)# default-metric 3
Ruijie(config-router)# redistribute ospf 100
```

【检验方法】 show ipv6 rip database 查看重分发进 rip 的路由的度量是否有相应的变化

【提示信息】 -

【常见错误】 -

【平台说明】 -

4.3 distance

设置 RIPng 路由的管理距离。
distance *distance*

恢复缺省设置。
no distance

【参数说明】

参数	描述
distance	设置 RIPng 路由管理距离，允许设置<1-254>之间的整数。

【缺省配置】 管理距离缺省为 120

【命令模式】 路由进程配置模式

【缺省级别】 14

【使用指导】 为 RIPng 路由设置管理距离，用此命令。

【配置举例】 1：配置 RIPng 路由管理距离为 160

```
Ruijie(config)# ipv6 router rip
Ruijie(config-router)# distance 160
```

【检验方法】 使用 show ipv6 rip 可以查看当前配置的管理距离

【提示信息】 -

【常见错误】 -

【平台说明】 -

4.4 distribute-list

使用 prefix-list 表对进/出更新路由进行过滤。

distribute-list prefix-list *prefix-list-name* { **in** | **out** } [*interface-type interface-name*]

取消相应的过滤。

no distribute-list prefix-list *prefix-list-name* { **in** | **out** } [*interface-type interface-name*]

【参数说明】

参数	描述
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

【缺省配置】 默认没有定义分布列表。

【命令模式】 路由进程配置模式。

【缺省级别】 14

【使用指导】 为了拒绝接收或者发送某些指定路由，可以通过配置路由分布控制列表，对所有的路由更新报文进行过滤。如果没指定接口，就对所有的接口的路由更新报文进行过滤。

【配置举例】 1：在接口 eth0 上对收到的更新路由进行过滤，只接收 **prefix-list** *allowpre* 前缀表范围内的更新路由。

```
Ruijie(config)# ipv6 router rip
Ruijie(config-router)# distribute-list prefix-list allowpre in eth0
```

【检验方法】 使用 debug ipv6 rip interface 看过滤是否有生效

【提示信息】 -

【常见错误】 -

【平台说明】 -

4.5 graceful-restart

配置设备的 RIPng 优雅重启(Graceful Restart，GR)功能。
graceful-restart [**grace-period** *grace-period*]

恢复为默认配置。
no graceful-restart [**grace-period**]

【参数说明】

参数	描述
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。

【缺省配置】 缺省使能 GR Restart 能力。

【命令模式】 路由进程配置模式。

【缺省级别】 14

【使用指导】 优雅重启功能基于 RIPng 实例配置，不同的 RIPng 实例可以根据情况配置不同的参数。
优雅重启周期为执行 RIPng 重启到 RIPng 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 RIPng 路由恢复工作，使 RIPng 恢复到协议重启前的状态。当重启周期到期后，RIPng 将退出 GR 状态，执行普通的 RIPng 操作。
graceful-restart grace-period 允许用户显式修改重启周期。注意，要能够保证在 RIPng 路由无效时间之内完成 GR 重启，并经过一次 RIPng 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** 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。
在 RIPng 优雅重启运行过程中，请保持网络环境的稳定。

【配置举例】 1：使能 RIPng 的 GR 功能以及配置 GR 功能的重启周期参数：

```
Ruijie(config)# ipv6 router rip
Ruijie(config-router)# graceful-restart grace-period 90
```

【检验方法】 使用 show ipv6 rip 查看当前 gr 是否已经开启和相应配置的 grace-period

【提示信息】 -

【常见错误】 -

【平台说明】 -

4.6 ipv6 rip default-information

产生一条默认 IPv6 的路径到 RIPng。
ipv6 rip default-information { **only** | **originate** } [**metric** *metric-value*]

删除默认路径。
no ipv6 rip default-information

【参数说明】

参数	描述
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。

【缺省配置】 默认没有默认路由配置

【命令模式】 接口配置模式

【缺省级别】 14

【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。

【配置举例】 1：在接口 ethernet0/0 上创建一条默认路由到 RIPng 路由进程，该接口只通告该默认路由。

```
Ruijie(config)# interface ethernet 0/0
Ruijie(config-if)# ipv6 rip default-information only
```

【检验方法】 使用 show ipv6 rip interface 来查看该接口 default-information 配置状态

【提示信息】 -

【常见错误】 -

【平台说明】 -

4.7 ipv6 rip enable

使接口加入 RIPng 运行。
ipv6 rip enable

取消在特定接口上运行 RIPng。
no ipv6 rip enable

【参数说明】

参数	描述
-	-

【缺省配置】 默认接口不运行 RIPng

【命令模式】 接口配置模式。

【缺省级别】 14

【使用指导】 该命令用于设置参与 RIPng 协议运行的接口。在配置该命令之前，如果没有运行 RIPng 协议，则配置该命令会自动运行 RIPng 路由协议。

【配置举例】 1：将接口 ethenet 0/0 加入 RIPng 运行。

```
Ruijie(config)# interface ethernet 0/0
Ruijie(config-if)# ipv6 rip enable
```

【检验方法】 执行 show ipv6 rip interface 可以看到加入 RIPng 中的接口

【提示信息】 -

【常见错误】 -

【平台说明】 -

4.8 ipv6 rip metric-offset

设置接口上的度量值。
ipv6 rip metric-offset *value*

取消相应的设置。

no ipv6 rip metric-offset

【参数说明】

参数	描述
value	接口度量值，取值范围：1-16。

【缺省配置】 接口度量默认值为 1

【命令模式】 接口配置模式

【缺省级别】 14

【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。

【配置举例】 1：将接口 ethernet 0/1 上的接口度量值设置为 5。

```
Ruijie(config)# interface ethernet 0/1
Ruijie(config-if)# ipv6 rip metric-offset 5
```

【检验方法】 使用 show ipv6 rip database 可以查看接口进来的路由是否有增加该命令对应设置的值

【提示信息】 -

【常见错误】 -

【平台说明】 -

4.9 ipv6 router rip

创建 RIPng 路由进程并进入路由进程配置模式。

ipv6 router rip

删除 RIPng 路由进程。

no ipv6 router rip

【参数说明】

参数	描述
-	-

【缺省配置】 没有 RIPng 路由进程在运行

【命令模式】 全局配置模式

【缺省级别】 14

【使用指导】 该命令用于创建 RIPng 路由进程并进入路由进程配置模式。

【配置举例】 1：创建 RIPng 路由进程，进入路由进程配置模式。

```
Ruijie(config)# ipv6 router rip
```

【检验方法】 使用 show ipv6 rip 看实例是否建立

【提示信息】 1：当 ipv6 单播功能未开启时不能进行配置

```
IPv6 unicast-routing not enabled, RIPng process can't configure
```

【常见错误】 -

【平台说明】 -

4.10 passive-interface

取消在一个接口上发送更新报文的功能。
passive-interface { **default** | *interface-type interface-num* }

重新启用发送更新报文的功能。
no passive-interface { **default** | *interface-type interface-num* }

【参数说明】

参数	描述
default	该参数设置所有接口为 passive 模式
interface-type interface-num	接口类型与序号

【缺省配置】 没有接口设置为 passive 模式。

【命令模式】 路由进程配置模式。

【缺省级别】 14

【使用指导】 **passive-interface default** 命令将所有接口设置为 passive 模式，这时可以使用 **no passive-interface** *intface-type interface-num* 命令设置某些接口为非 passive 模式。

【配置举例】 1：设置除 ethernet0/0 以外的所有接口为 passive 模式。

```
Ruijie(config-router)# passive-interface default
Ruijie(config-router)# no passive-interface ethernet 0/0
```

【检验方法】 使用 show running-config 查看是否配置

【提示信息】 1：配置的接口非法或着不存在

```
% Interface is invalid.
```

【常见错误】 -

【平台说明】 -

4.11 redistribute

将其它路由域的路径重分布到 RIPng 内

redistribute { **bgp | connected | isis** [*area-tag*] **| ospf** *process-id* **| static** } [**metric** *metric-value* | **route-map** *route-map-name*]

取消相应的重分布配置。

no redistribute { **bgp | connected | isis** [*area-tag*] **| ospf** *process-id* **| static** } [**metric** *metric-value* | **route-map** *route-map-name*]

【参数说明】

参数	描述
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

【缺省配置】 默认不重分布其它路由协议的路径。

如果没有设置 **default-metric，metric** 默认为 1。

默认不设置 **route-map**。

默认重分布指定路由进程的所有子类型路由。

【命令模式】 路由进程配置模式

【缺省级别】 14

【使用指导】 使用该命令将外部路由信息重分布到 RIPng 中。

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。

配置重分布多实例协议时，需要指定具体从哪个实例重分布路由信息到 RIPng。

【配置举例】 1：从静态路由重分布，使用路由图 *mymap* 进行过滤，度量值设置为 8。

```
Ruijie(config)# ipv6 router rip
Ruijie(config-router)# redistribute static route-map mymap metric 8
```

【检验方法】 使用 show ipv6 rip database 查看重分发所配置的路由协议中的路由是否有进入到 rip 的数据库当中。

【提示信息】 -

【常见错误】

【平台说明】 -

4.12 show ipv6 rip

显示 RIPng 路由协议协进程的参数和各个统计数据。

show ipv6 rip

【参数说明】

参数	描述
-	-

【命令模式】 用户模式、特权模式

【缺省级别】 14

【使用指导】 可用于快速显示 RIPng 路由协议进程的三个计时器、路由分发、路由重分布状态、接口 ripng 版本、ripng 接口与网络范围、metric 与 distance 等。

【配置举例】 1：显示 RIPNG 信息概要

```
Ruijie# show ipv6 rip
Routing Protocol is "RIPng"
  Sending updates every 10 seconds with +/-50%, next due in 8 seconds
  Timeout after 30 seconds, garbage collect after 60 seconds
  Outgoing update filter list for all interface is:
    distribute-list prefix aa out
  Incoming update filter list for all interface is: not set
  Default redistribution metric is 1
  Distance: 120 (default is 120)  Redistribution:
      Redistributing protocol connected route-map rm
      Redistributing protocol static
```

```
    Redistributing protocol ospf 1
Default version control:  send version 1, receive version 1
Interface                 Send   Recv
    VLAN 1                1      1
    Loopback 1            1      1
Routing Information Sources:
    None
```

字段解释：

字段	说明
Sending update	发送更新的时间间隔
Sending update	失效时间
garbage	回收时间
Outgoing update filter list	所配置的发送过滤表
Incoming update filter	所配置的接收过滤表
Default redistribution metric	默认的重分发度量
distance	管理距离
Redistribution	重分发的路由协议
Default version control	默认收发版本
Interface	所加入 RIPng 的接口
Routing Information Sources:	路由信息

【提示信息】 -

【平台说明】 -

4.13 show ipv6 rip database

显示 RIPng 路由表的各项目信息。

show ipv6 rip database

【参数说明】

参数	描述
-	-

【命令模式】 用户模式、特权模式

【缺省级别】 14

【使用指导】 使用该命令显示 RIPng 路由表的各项信息。

【配置举例】 1：显示 RIPNG 数据库信息

```
Ruijie# show ipv6 rip database
Codes: R - RIPng,C - Connected,S - Static,O - OSPF,B - BGP
sub-codes:n - normal,s - static,d - default,r - redistribute,
          i - interface, a/s - aggregated/suppressed
S(r)   2001:db8:1::/64, metric 1, tag 0
          Loopback 0/::
S(r)   2001:db8:2::/64, metric 1, tag 0
          Loopback 0/::
C(r)   2001:db8:3::/64, metric 1, tag 0
          VLAN 1/::
S(r)   2001:db8:4::/64, metric 1, tag 0
          Null 0/::
C(i)   2001:db8:5::/64, metric 1, tag 0
          Loopback 1/::
S(r)   2001:db8:6::/64, metric 1, tag 0
          Null 0/::
```

字段解释：

字段	说明
codes	路由类型以及对应的缩写描述
2001:db8:1::	路由对应的前缀。
metric 1	路由对应的 metric
VLAN 1/::	路由接口

【提示信息】 -

【平台说明】 -

4.14 split-horizon

启用 RIPng 水平分割功能。

split-horizon

启用带毒性逆转的水平分割。

split-horizon poisoned-reverse

取消带毒性逆转的水平分割。

no split-horizon poisoned-reverse

【参数说明】

参数	描述
poisoned-reverse	启用带毒性逆转的水平分割

【缺省配置】 缺省为接口启用不带毒性逆转的水平分割。

【命令模式】 路由进程配置模式

【缺省级别】 14

【使用指导】 在更新报文中，水平分割可以防止设备将某些路由信息从学习到这些路由信息的接口通告出去；带毒性逆转的水平分割将某些路由信息从学习到这些路由信息的接口通告出去，但是将相应的 *metric* 设置为 16。
RIPng 路由协议属于距离向量路由协议，在实际应用中要注意水平分割问题。如果不能确定 RIPng 是否启用了水平分割，可以用 **show ipv6 rip** 命令进行判断。

【配置举例】 1：关闭 RIPng 水平分割功能。

```
Ruijie(config)# ipv6 router rip
Ruijie(config-router)# no split-horizon
```

【检验方法】 使用 show ipv6 rip 来查看水平分割的状态

【提示信息】 -

【常见错误】 -

【平台说明】 -

4.15 timers

调整 RIPng 的时钟。
timers *update invalid flush*

恢复缺省配置。
no timers

【参数说明】

参数	描述
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。

【缺省配置】 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。

【命令模式】 路由进程配置模式

【缺省级别】 14

【使用指导】 通过调整以上时钟，可能会加快路由协议的收敛时间以及故障恢复时间。连接在同一网络上的设备，RIPng 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。
当前的 RIPng 时钟参数设置，可以用 **show ipv6 rip** 令进行查看。

⚠ 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。

【配置举例】 1：RIP 更新报文每隔 10 秒种发送一次。如果 30 秒内没有收到更新报文，相应的路由将变为无效路由，并进入 invalid 状态；该路由进入 invalid 状态后，超过 90 秒，将被清除。

```
Ruijie(config)# ipv6 router rip
Ruijie(config-router)# timers 10 30 90
```

【检验方法】 使用 show ipv6 rip 来查看当前配置的时间状态

【提示信息】 -

【常见错误】 1：不同设备间配置的 timer 不一样，导致路由学习异常。

【平台说明】 -

5 OSPFv2

5.1 area

配置指定的区域。
area *area-id*

删除指定的 OSPF 区域。
no area *area-id*

【参数说明】

参数	描述
area-id	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。

【缺省配置】 没有配置 OSPF 区域。

【命令模式】 路由进程配置模式。

【缺省级别】 14

【使用指导】 用户可以使用本命令的 no 形式，清除指定 OSPF 区域的配置并删除该区域，包括清除 **area authentication**、**area default-cost**、**area filter-list**、**area nssa** 等基于区域的配置命令。
在如下情况下，用户无法清除 OSPF 区域的配置：
要清除主干区域的所有配置，但存在虚链路的配置。此时必须先清除虚链路配置，才能删除主干区域。
任何一个区域，存在对应的 **network area** 命令。此时必须先清除所有加入该区域的网段命令，才能删除该区域。

【配置举例】 1：删除 OSPF 区域 2 的相关配置：

```
Ruijie(config)# router ospf 2
Ruijie(config-router)# no area 2
```

【检验方法】 1：使用 show ip ospf 命令可以查看所配置的区域。

【提示信息】 1：若未删除 network 而删除 area 配置则提示错误。

```
% Error: Area 1 cannot be deleted before its network command is removed
```

【常见错误】 1：未删除 network 而删除 area 配置。

【平台说明】 -

5.2 area authentication

启用 OSPF 区域认证。

area *area-id* **authentication** [**message-digest**]

关闭 OSPF 区域认证。

no area *area-id* **authentication**

【参数说明】

参数	描述
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。

【缺省配置】 没有采用 OSPF 区域认证。

【命令模式】 路由进程配置模式。

【缺省级别】 14

【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。

【配置举例】 1：OSPF 路由进程的区域 0（骨干区域）采用 MD5 认证，认证口令为 backbone。

```
Ruijie(config)# interface fastEthernet 0/1
Ruijie(config-if-FastEthernet 0/1)# ip address 192.168.12.1 255.255.255.0
Ruijie(config-if-FastEthernet 0/1)# ip ospf message-digest-key 1 md5 backbone
Ruijie(config)# router ospf 1
Ruijie(config-router)# network 192.168.12.0 0.0.0.255 area 0
Ruijie(config-router)# area 0 authentication message-digest
```

【检验方法】 1：使用 show ip ospf 命令可以查看所配置的认证方式。

【提示信息】 -

【常见错误】 -

【平台说明】 -

5.3 area default-cost

定义通告给 Stub 区域或者 NSSA 缺省路由的花费值（OSPF 的量度值）。
area *area-id* **default-cost** *cost*

恢复缺省配置。
no area *area-id* **default-cost**

【参数说明】

参数	描述
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。

【缺省配置】 缺省为 1。

【命令模式】 路由进程配置模式。

【缺省级别】 14

【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。

【配置举例】 1：将缺省汇聚路由的花费值设置为 50。

```
Ruijie(config)# router ospf 1
Ruijie(config-router)# network 172.16.0.0 0.0.255.255 area 0
Ruijie(config-router)# network 192.168.12.0 0.0.0.255 area 1
Ruijie(config-router)# area 1 stub
Ruijie(config-router)# area 1 default-cost 50
```

【检验方法】 -

【提示信息】 1：在非 Stub 或者 NSSA 域意外的区域中配置该命令，提示错误。

```
% The area is neither stub, nor NSSA
```

2：向骨干区域中配置该命令，提示错误。

```
% You can't configure default-cost to backbone
```

【常见错误】 1：在非 Stub 或者 NSSA 域意外的区域中配置该命令。
2：在骨干区域中配置该命令。

【平台说明】 -

5.4 area filter-list

ABR 上设置，过滤不同区域之间的区内路由的相互学习。

area *area-id* **filter-list** { **access** *acl-name*| **prefix** *prefix-name*} { **in** | **out** }

取下区域过滤配置

no area *area-id* **filter-list** { **access** *acl-name* | **prefix** *prefix-name*} { **in** | **out** }

【参数说明】

参数	描述
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

【缺省配置】 未启用 ABR 上过滤

【命令模式】 路由进程配置模式。

【缺省级别】 14

【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。

【配置举例】 1：将配置 area 1 只学习到属于 172.22.0.0/8 范围内的区间路由。

```
Ruijie# configure terminal
Ruijie(config)# access-list 1 permit 172.22.0.0 0.255.255.255
Ruijie(config)# router ospf 100
Ruijie(config-router)# area 1 filter-list access 1 in
```

【检验方法】 -

【提示信息】 -

【常见错误】 -

【平台说明】 -

5.5 area nssa

将一个 OSPF 区域设置为 NSSA。

area *area-id* **nssa** [**no-redistribution**] [**default-information-originate** [**metric** *value*] [**metric-type** *type*]] [**no-summary**] [**translator** [**stability-interval** *seconds* | **always**]]

删除 NSSA 区域或 NSSA 区域的配置。

no area *area-id* **nssa** [**no-redistribution**] [**default-information-originate** [**metric** *value*] [**metric-type** *type*]] [**no-summary**] [**translator** [**stability-interval** | **always**]]

【参数说明】

参数	描述
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。

【缺省配置】 没有定义 NSSA 区域。

【命令模式】 路由进程配置模式。

【缺省级别】 14

【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。

在 Type-7 转 Type-5 的时候，新生成的 Type-5 LSA 默认继承 Type-7 LSA 的转发地址(FA)

【配置举例】 1：将区域 1 设置为 NSSA 区域，所有属于该区域的路由设备都必须配置。

```
Ruijie(config)# router ospf 1
Ruijie(config-router)# network 172.16.0.0 0.0.255.255 area 0
Ruijie(config-router)# network 192.168.12.0 0.0.0.255 area 1
Ruijie(config-router)# area 1 nssa
```

【检验方法】 使用 show ip ospf 命令可以看到所配置的区域拥有 NSSA 属性

【提示信息】 1：将骨干区配置为 NSSA 区域时提示错误。

```
% You can't configure NSSA to backbone
```

【常见错误】 1：将骨干区配置为 NSSA 区域时提示错误

【平台说明】 -

5.6 area range

配置 OSPF 区域之间的路由汇聚。

area *area-id* **range** *ip-address net-mask* [**advertise** | **not-advertise**] [**cost** *cost*]

删除已配置的路由汇聚，**no** 前缀与 **cost** 参数组合可以恢复汇聚路由默认的度量值，但不会删除路由汇聚。

no area *area-id* **range** *ip-address net-mask* [**cost**]

【参数说明】

参数	描述
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。

【缺省配置】 缺省没有配置区域间汇聚路由。
缺省公布配置的汇聚范围。
汇聚路由的默认度量值与是否兼容 RFC1583 有关，如果配置了兼容 RFC1583 模式，默认度量值是被汇聚的路由 cost 的最小值，否则默认度量值是被汇聚的路由 cost 的最大值。

【命令模式】 路由进程配置模式。

【缺省级别】 14

【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。

【配置举例】 1：将区域 1 的路由汇聚成一条路由 172.16.16.0/20。

```
Ruijie(config)# router ospf 1
Ruijie(config-router)# network 172.16.0.0 0.0.15.255 area 0
Ruijie(config-router)# network 172.16.17.0 0.0.15.255 area 1
Ruijie(config-router)# area 1 range 172.16.16.0 255.255.240.0
```

【检验方法】 -

【提示信息】 1：已有不同的区域配置了该 area range。

```
% OSPF: This range in different area 1
```

【常见错误】 1：已有不同的区域配置了该 area range

【平台说明】 -

5.7 area stub

将一个 OSPF 区域设置为残域或全残域。
area *area-id* **stub** [**no-summary**]

删除残域或全残域的配置。
no area *area-id* **stub** [**no-summary**]

【参数说明】

参数	描述
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。

【缺省配置】 缺省没有定义残域。

【命令模式】 路由进程配置模式。

【缺省级别】 14

【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）。

【配置举例】 1：将区域 1 设置为残域，所有属于该区域的路由设备都必须配置。

```
Ruijie(config)# router ospf 1
Ruijie(config-router)# network 172.16.0.0 0.0.255.255 area 0
Ruijie(config-router)# network 192.168.12.0 0.0.0.255 area 1
Ruijie(config-router)# area 1 stub
```

【检验方法】 使用 show ip ospf 命令可以看到所配置的区域拥有 Stub 属性

【提示信息】 1：骨干区不能设置为 Stub 区域。

```
% You can't configure stub to backbone
```

2：将 NSSA 区域配置为 Stub 区域时提示错误。

```
% The area is configured as NSSA area already
```

【常见错误】 1：骨干区不能设置为 Stub 区域。

2：将 NSSA 区域配置为 Stub 区域时提示错误。

【平台说明】 -

5.8 area virtual-link

定义 OSPF 虚拟链路。

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*]]

删除虚拟链路的定义。

no area *area-id* **virtual-link** *router-id* [**authentication**] [**dead-interval**] [**hello-interval**] [**retransmit-interval**] [**transmit-delay**] [[**authentication-key**] | [**message-digest-key** *key-id*]]

【参数说明】

参数	描述
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。路由设备表示可以通过 show ip ospf 命令查看。
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。该时间的设置应该考虑到数据包在该链路上的往返时间。
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。该值增加 LSA 的存活时间，当 LSA 的存活时间达到一定时间时，该 LSA 将被刷新。
authentication-key [**0** | **7**] *key*	定义 OSPF 明文认证的密钥。邻居之间的明文认证的密钥必须一致。service password-encryption 命令可以使该密钥以加密的方式显示。 **0** 指定密钥以明文显示 **7** 指定密钥以密文显示
message-digest-key *key-id* **md5** [**0** | **7**] key	定义 OSPF MD5 认证的密钥标识符和密钥。邻居之间的 MD5 认证的密钥标识符和密钥必须一致。service password-encryption 命令可以使该密钥以加密的方式显示。 **0** 指定密钥以明文显示 **7** 指定密钥以密文显示
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。

【缺省配置】 **dead-interval** ：40 秒；
hello-interval ：10 秒；
retransmit-interval ：5 秒；
transmit-delay ：1 秒；
缺省不认证；
缺省不启用 Fast Hello 功能；
其余参数没有缺省值。

【命令模式】 路由进程配置模式。

【缺省级别】 14

【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 Hello 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 Hello 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】 1：以区域 1 作为过渡区域，与邻居 2.2.2.2 建立虚拟链路。

```
Ruijie(config)# router ospf 1
Ruijie(config-router)# network 172.16.0.0 0.0.15.255 area 0
Ruijie(config-router)# network 172.16.17.0 0.0.15.255 area 1
Ruijie(config-router)# area 1 virtual-link 2.2.2.2
```

2：以区域 1 作为过渡区域，与邻居 1.1.1.1 建立虚拟链路。该虚拟链路连接了区域 10 和骨干区域，虚拟链路

采用 OSPF 报文认证，认证方式为 MD5。

```
Ruijie(config)# router ospf 1
Ruijie(config-router)# network 172.16.17.0 0.0.15.255 area 1
Ruijie(config-router)# network 172.16.252.0 0.0.0.255 area 10
Ruijie(config-router)# area 0 authentication message-digest
Ruijie(config-router)# area 1 virtual-link 1.1.1.1 message-digest-key 1 md5 hello
```

3：以区域 1 作为过渡区域，与邻居 1.1.1.1 建立虚拟链路，并在虚链路启用 Fast Hello 功能，设置乘数为 3。

```
Ruijie(config)# router ospf 1
Ruijie(config-router)# network 172.16.17.0 0.0.15.255 area 1
Ruijie(config-router)# network 172.16.252.0 0.0.0.255 area 10
Ruijie(config-router)# area 1 virtual-link 1.1.1.1 dead-interval minimal hello-multiplier 3
```

【检验方法】 1：使用 **show ip ospf virtual-links** 命令可以查看所配置的虚链路信息。

【提示信息】 1：在骨干区配置虚链路时，提示错误。

```
% You can't configure virtual-link transit to backbone
```

2：往 Stub 或 NSSA 区域中配置虚链路时，提示错误。

```
% Area is a stub or nssa so virtual links are not allowed
```

【常见错误】 1：在骨干区配置虚链路时，提示错误。

2：往 Stub 或 NSSA 区域中配置虚链路时，提示错误。

【平台说明】 -

5.9 auto-cost

设置自动生成接口代价的参考值，用于计算接口 cost 值。

auto-cost reference-bandwidth *ref-bw*

恢复缺省值。

no auto-cost reference-bandwidth

【参数说明】

参数	描述
ref-bw	参考带宽值。以 Mbps 为单位， 范围: 1-4294967

【缺省配置】 缺省为 100Mbps。

【命令模式】 路由进程配置模式。

【缺省级别】 14

【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。

【配置举例】 1：将参考带宽设置为 10M。

```
Ruijie(config)# router ospf 1

Ruijie(config-router)# network 172.16.10.0 0.0.0.255 area 0

Ruijie(config-router)# auto-cost reference-bandwidth 10
```

【检验方法】 1：使用 show ip ospf interface 命令可以查看所配置的参考代码是否生效。

【提示信息】 1：改变接口代价时提示。

```
% OSPF: Reference bandwidth is changed.
        Please ensure reference bandwidth is consistent across all routers
```

【常见错误】 -

【平台说明】 -

5.10 capability opaque

启动 Opaque LSA 处理能力。
capability opaque

禁用 Opaque LSA 处理能力。
no capability opaque

【参数说明】

参数	描述
-	-

【缺省配置】 缺省支持 Opaque LSA 处理。

【命令模式】 路由进程配置模式。

【缺省级别】 14

【使用指导】 -

【配置举例】 1：禁用 Opaque LSA 处理能力。

```
Ruijie(config)# router ospf 1
Ruijie(config-router)# no capability opaque
```

【检验方法】 1：使用 show ip ospf 命令可以查看所配置的 Opaque LSA 处理能力。

【提示信息】 -

【常见错误】 -

【平台说明】 -

5.11 clear ip ospf process

清除并重启 OSPF 实例。

clear ip ospf [*process-id*] **process**

【参数说明】

参数	描述
process-id	OSPF 进程号 指定该选项时，清除并重启指定 OSPF 实例。 未指定该选项时，清除并重启所有正在运行的 OSPF 实例。

【命令模式】 特权模式。

【缺省级别】 14

【使用指导】 复位整个 OSPF 进程，所有邻居重新建立，对整个协议影响较大。
执行此命令时，会要求用户确认。

【配置举例】 1：清除并重启 OSPF 实例 1

```
Ruijie# clear ip ospf 1 process
```

【提示信息】 1：重启不存在的实例时。

```
%OSPF: No router process 1
```

【平台说明】 -

5.12 compatible rfc1583

当存在多条路径到达同一个 AS 外部目的地时，必须确定最优路径，该命令是确定采用 RFC1583 中使用的优先规则。

compatible rfc1583

取消采用 RFC1583 规则

no compatible rfc1583

【参数说明】

参数	描述
-	-

【缺省配置】 缺省是采用 RFC1583 规则。

【命令模式】 路由进程配置模式。

【缺省级别】 14

【使用指导】 -

【配置举例】 1：使用 rfc 2328 的规则来确定最佳路由。

```
Ruijie(config)# router ospf 1
Ruijie(config-router)# no compatible rfc1583
```

【检验方法】 1：使用 show ip ospf 命令可以查看是否采用 RFC1583 规则。

【提示信息】 -

【常见错误】 -

【平台说明】 -

5.13 default-information originate

产生一条缺省的路由注入 OSPF 路由域。

default-information originate [**always**] [**metric** *metric*] [**metric-type** *type*] [**route-map** *map-name*]

关闭缺省路由。

no default-information originate [**always**] [**metric**] [**metric-type**] [**route-map** *map-name*]

【参数说明】

参数	描述
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

【缺省配置】 缺省不产生缺省路由。

metric 缺省为 1。

metric-type 缺省为类型 2。

【命令模式】 路由进程配置模式。

【缺省级别】 14

【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。

该命令产生的是 5 类 LSA 的缺省路由，不会洪泛到 NSSA 区域。若希望在 NSSA 区域产生一条缺省路由，请使用 **area nssa default-information-originate** 命令。

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】 1：OSPF 产生一条外部缺省路由，注入到 OSPF 路由域中，类型设置为 1，量度值设置为 50。

```
Ruijie(config)# router ospf 1

Ruijie(config-router)# network 172.16.24.0 0.0.0.255 area 0
```

```
Ruijie(config-router)# default-information originate always metric 50 metric-type 1
```

【检验方法】 1：使用 show ip ospf database 命令可以查看是否引入缺省路由。

【提示信息】 -

【常见错误】 -

【平台说明】 -

5.14 default-metric

设置 OSPF 重分布路由的缺省量度值。
default-metric *metric*

恢复缺省配置。
no default-metric

【参数说明】

参数	描述
metric	定义 OSPF 重分布路由的缺省量度值，取值范围：1-16777214。

【缺省配置】 缺省未配置。

【命令模式】 路由进程配置模式

【缺省级别】 14

【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。

【配置举例】 1：将 OSPF 重分布路由的初始化度量值设为 50。

```
Ruijie(config)# router rip
Ruijie(config-router)# network 192.168.12.0
Ruijie(config-router)# version 2
Ruijie(config-router)# exit
Ruijie(config)# router  ospf 1
Ruijie(config-router)# network 172.16.10.0 0.0.0.255 area 0
Ruijie(config-router)# default-metric 50
Ruijie(config-router)# redistribute rip subnets
```

【检验方法】 1：使用 show ip ospf database 命令可以查看重分布路由的度量值。

【提示信息】 -

【常见错误】 -

【平台说明】 -

5.15 discard-route

允许 discard 路由添加到核心路由表。
discard-route { **internal** | **external** }

禁止 discard 路由添加到核心路由表。
no discard-route { **internal** | **external** }

【参数说明】

参数	描述
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。

【缺省配置】 缺省情况允许添加 discard 路由。

【命令模式】 路由进程配置模式。

【缺省级别】 14

【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】 1：禁止添加 area range 生成的 discard 路由。

```
Ruijie(config)# router ospf 1
Ruijie(config-router)# no discard-route internal
```

【检验方法】 1：使用 show ip route 命令可以查看是否添加 discard 路由。

【提示信息】 -

【常见错误】 -

【平台说明】 -

5.16 distance ospf

设置不同类型 OSPF 路由对应的管理距离。

distance { *distance* | **ospf** { [**intra-area** *distance*] [**inter-area** *distance*] [**external** *distance*] } }

恢复缺省配置。

no distance [**ospf**]

【参数说明】

参数	描述
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。

【缺省配置】 缺省为 110；
区内路由管理距离：缺省为 110；
区间路由管理距离：缺省为 110；
外部路由管理距离：缺省为 110。

【命令模式】 OSPF 路由进程配置模式。

【缺省级别】 14

【使用指导】

【配置举例】 1：配置 OSPF 外部路由管理距离为 160

```
Ruijie(config)# router ospf 1

Ruijie(config-router)# distance ospf external 160
```

【检验方法】 1：使用 show ip route 命令可以查看 ospf 路由的管理距离。

【提示信息】 -

【常见错误】 -

【平台说明】 -

5.17 distribute-list in

配置对收到的 LSA 计算出的路由进行过滤。

distribute-list { [*access-list-number* | *name*] | **prefix** *prefix-list-name* [**gateway** *prefix-list-name*] | **route-map** *route-map-name* | [**gateway** *prefix-list-name*] } **in** [*interface-type interface-number*]

取消对收到的 LSA 计算出的路由过滤。

no distribute-list { [*access-list-number* | *name*] | **prefix** *prefix-list-name* [**gateway** *prefix-list-name*] | **route-map** *route-map-name* | [**gateway** *prefix-list-name*]} **in** [*interface-type interface-number*]

【参数说明】

参数	描述
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。

【缺省配置】 缺省为无配置，即全通过。

【命令模式】 路由进程配置模式。

【缺省级别】 14

【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。此命令中引用的 route-map 支持以下 match 命令：

match interface
match ip address
match ip address prefix-list
match ip next-hop
match ip next-hop prefix-list
match metric
match route-type
match tag

⚠ 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 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。

【配置举例】 1：对收到 LSA 计算出的路由进行过滤。

```
Ruijie(config)# access-list 3 permit 172.16.0.0 0.0.127.255

Ruijie(config)# router ospf 25
Ruijie(config-router)# distribute-list 3 in ethernet 0/1
```

【检验方法】 1：使用 show ip route 命令可以查看路由是否被正确过滤。

【提示信息】 1：配置了无效的接口。

```
% Interface is invalid.
```

2：配置了无效的 ACL 名字。

```
% ACL name abc-acl is invalid
```

3：不允许过滤由本实例导入的路由。

```
% Distribute-list of "ospf 1" via "ospf 1" not allowed
```

【常见错误】 -

【平台说明】 -

5.18 distribute-list out

配置过滤重分布路由，功能类似 **redistribute** 命令。

distribute-list { [*access-list-number* | *name*] | **prefix** *prefix-list-name* } **out** [**connected | ospf** *process-id* **| rip | static**]

取消过滤重分布路由。

no distribute-list { [*access-list-number* | *name*] | **prefix** *prefix-list-name* } **out** [**connected** | **ospf** *process-id* | **rip | static**]

【参数说明】

参数	描述
access-list-number | *name*	使用 acl 过滤规则
prefix *prefix-list-name*	使用 prefix-list 过滤规则
connected	过滤直连路由
ospf *process-id*	过滤 OSPF 路由
rip	过滤 RIP 路由
static	过滤静态路由

【缺省配置】 缺省为无配置，即全通过。

【命令模式】 路由进程配置模式。

【缺省级别】 14

【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。

【配置举例】 1：对重分布的静态路由进行过滤

```
Ruijie(config)# router ospf 1
Ruijie(config-router)# redistribute static subnets
Ruijie(config-router)# distribute-list 22 out static
Ruijie(config-router)# distribute-list prefix jjj out static
% Access-list filter exists , please de-config first
```

【检验方法】 1：使用 show ip ospf database 命令可以查看重分布路由是否被正确过滤。

【提示信息】 1：重分布过滤不允许 **gateway** 参数。

```
% Gateway not allowed with OUT in distribute-list cmd
```

【常见错误】 -

【平台说明】 -

5.19 enable mib-binding

将 MIB 绑定到指定的 OSPFv2 进程上。
enable mib-binding

恢复缺省绑定。
no enable mib-binding

【参数说明】

参数	描述
-	-

【缺省配置】 MIB 绑定在进程号最小的 OSPFv2 进程上。

【命令模式】 路由进程配置模式

【缺省级别】 14

【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。

【配置举例】 1：通过 SNMP 操作进程号为 100 的 OSPFv2 进程：

```
Ruijie(config)# router ospf 100
Ruijie(config-router)# enable mib-binding
```

【检验方法】 -

【提示信息】 -

【常见错误】 -

【平台说明】 -

5.20 enable traps

配置启动指定 TRAP 信息的发送。
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**]]

关闭指定 TRAP 信息的发送。
no 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】

参数	描述
error	配置所有与 error 有关的 traps 开关，该参数还可以配置如下特定的 error traps 开关： **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
	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
lsa	配置所有与 lsa 有关的 traps 开关，该参数还可以配置如下特定的 lsa traps 开关：	
	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
retransmit	配置所有与 retransmit 有关的 traps 开关，该参数还可以配置如下特定的 retransmit traps 开关：	
	IfTxRetransmit	接口上发生报文重传
	VirtIfTxRetransmit	虚接口上发生报文重传
state-change	配置所有与 state-change 有关的 traps 开关，该参数还可以配置如下特定的 state-change traps 开关：	
	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

【缺省配置】 缺省是关闭全部 traps 开关。

【命令模式】 路由进程配置模式。

【缺省级别】 14

【使用指导】 OSPFv2 进程目前支持发送 16 种 TRAP 信息，分为 4 种类型。
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。

【配置举例】 1：打开 OSPFv2 进程 100 的全部 TRAP 开关：

```
Ruijie(config)# router ospf 100
Ruijie(config-router)# enable traps
```

【检验方法】 -

【提示信息】 -

【常见错误】 -

【平台说明】 -

5.21 graceful-restart

启动 OSPF Restarter 能力，设置重启周期。
graceful-restart [**grace-period** *grace-period* | **inconsistent-lsa-checking**]

关闭 OSPF GR 功能或恢复重启周期的缺省值。
no graceful-restart [*grace-period*]

【参数说明】

参数	描述
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，缺省开启检测。

【缺省配置】 开启 GR Restarter 能力。

【命令模式】 路由进程配置模式

【缺省级别】 14

【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。
在 Fast Hello 功能下，不支持启用优雅重启功能。
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。

【配置举例】 1：使能 OSPF 实例 1 的 GR 功能以及配置 GR 功能的重启周期参数：

```
Ruijie(config)# router ospf 1
Ruijie(config-router)# graceful-restart
Ruijie(config-router)# graceful-restart grace-period 60
```

【检验方法】 1：使用 show ip ospf 命令可以查看所配置的 GR 功能和运行状态。

【提示信息】 -

【常见错误】 -

【平台说明】 -

5.22 graceful-restart helper

启动 OSPF GR helper 功能，设置相关机制。
graceful-restart helper disable

禁用 OSPF GR helper 功能。
no graceful-restart helper disable

配置 OSPF GR helper 的拓扑变化检测方式。
graceful-restart helper { **strict-lsa-checking | internal-lsa-checking** }

取消配置 OSPF GR helper 的拓扑变化检测方式。
no graceful-restart helper { **strict-lsa-checking | internal-lsa-checking** }

【参数说明】

参数	描述
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。

【缺省配置】 启动 GR Help 能力。

设备进入 GR Helper 后，缺省不检查 LSA 变化。

【命令模式】 路由进程配置模式

【缺省级别】 14

【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】 1：禁止 OSPF 实例 1 的 GR 辅助功能以及如何修改检测网络变化的策略：

```
Ruijie(config)# router ospf 1
Ruijie(config-router)# graceful-restart helper disable
Ruijie(config-router)# no graceful-restart helper disable
Ruijie(config-router)# graceful-restart helper strict-lsa-checking
```

【检验方法】 1：使用 show ip ospf 命令可以查看所配置的 GR Helper 功能和运行状态。

【提示信息】 -

【常见错误】 -

【平台说明】 -

5.23 ip ospf authentication

配置接口的认证方式。
ip ospf authentication [**message-digest** | **null**]

将认证方式恢复为缺省。
no ip ospf authentication
`

【参数说明】

参数	描述
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。

【缺省配置】 缺省接口上没有设置认证方式，此时接口上采用的是所在的区域的认证类型。

【命令模式】 接口配置模式。

【缺省级别】 14

【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。

【配置举例】 1：设置 fastEthernet 0/1 端口的 OSPF 认证类型为 MD5 认证。

```
Ruijie(config)# interface fastEthernet 0/1
Ruijie(config-if-FastEthernet 0/1)# ip address 172.16.1.1 255.255.255.0
Ruijie(config-if-FastEthernet 0/1)# ip ospf authentication message-digest
```

【检验方法】 -

【提示信息】 -

【常见错误】 -

【平台说明】 -

5.24 ip ospf authentication-key

配置 OSPF 的明文认证密钥。
ip ospf authentication-key [**0** | **7**] *key*

删除明文认证密钥。
no ip ospf authentication-key

【参数说明】

参数	描述
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。

【缺省配置】 缺省没有配置认证密钥。

【命令模式】 接口配置模式。

【缺省级别】 14

【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。

【配置举例】 1：设置 fastEthernet 0/1 端口的 OSPF 认证密钥为 ospfauth。

```
Ruijie(config)# interface fastethernet 0/1
Ruijie(config-if-FastEthernet 0/1)# ip address 172.16.1.1 255.255.255.0
Ruijie(config-if-FastEthernet 0/1)# ip ospf authentication-key ospfauth
```

【检验方法】 -

【提示信息】 -

【常见错误】 -

【平台说明】 -

5.25 ip ospf cost

设置 OSPF 接口发送一个数据包的花费（OSPF 接口 cost）。
ip ospf cost *cost*

恢复缺省值。
no ip ospf cost

【参数说明】

参数	描述
cost	OSPF 接口的花费值，取值范围：0-65535。

【缺省配置】 OSPF 接口 cost 等于自动代价参考值/接口带宽。

【命令模式】 接口配置模式。

【缺省级别】 14

【使用指导】 缺省情况下，OSPF 接口 cost 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。
通过 **ip ospf cost** 命令配置 OSPF 接口 cost，会覆盖缺省配置。

【配置举例】 1：设置 fastEthernet *0*/1 接口 cost 为 100。

```
Ruijie(config)# interface fastEthernet 0/1

Ruijie(config-if-FastEthernet 0/1)# ip ospf cost 100
```

【检验方法】 使用 show ip ospf interface 命令可以查看相应接口的 cost 配置

【提示信息】 -

【常见错误】 -

【平台说明】 -

5.26 ip ospf database-filter all out

设置接口不向外扩散 LSA 报文，即不在该接口上发送 LSA 的更新报文.
ip ospf database-filter all out

恢复默认值.
no ip ospf database-filter

【参数说明】

参数	描述
-	-

【缺省配置】 缺省该功能被关闭， 可以在该接口上发送任何 LSA 更新报文。

【命令模式】 接口配置模式。

【缺省级别】 14

【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。

【配置举例】 1: 阻止 LSA 更新报 1 文在 fastEthernet 0/1 接口上发送。

```
Ruijie(config)# interface fastEthernet 0/1
Ruijie(config-if-FastEthernet 0/1)# ip address 172.16.10.1 255.255.255.0
Ruijie(config-if-FastEthernet 0/1)# ip ospf database-filter all out
```

【检验方法】 配置完后使用 show ip ospf interface 命令可以查看相应接口拥有 Database-filter all out 的属性

【提示信息】 -

【常见错误】 -

【平台说明】 -

5.27 ip ospf dead-interval

设置 OSPF 判断指定接口邻居死亡的时间.
ip ospf dead-interval { *seconds* **| minimal hello-multiplier** *multiplier* }

恢复缺省配置。
no ip ospf dead-interval

【参数说明】

参数	描述
seconds	定义判断邻居死亡的时间，以秒为单位，取值范围：0-2147483647。
minimal	启用 Fast Hello 功能，将死亡时间设置为 1s。
hello-multiplier *multiplier*	Fast Hello 功能中，每秒钟发送的 Hello 报文的次数。取值范围：3-20。

【缺省配置】 dead-interval 缺省为 hello-interval 的 4 倍。
缺省未启用 Fast Hello 功能。

【命令模式】 接口配置模式。

【缺省级别】 14

【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。

OSPF 支持 Fast Hello 功能：

启用 OSPF Fast Hello 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 Hello 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。

当某个接口配置了 Fast Hello 功能，从该接口通告的 Hello 报文的 Hello 间隔字段设置为 0，从该接口接收的 Hello 报文的 Hello 间隔字段被忽略。

无论是否启用 Fast Hello 功能，在同一个网段中，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 interface** 命令监控接口配置的死亡间隔和 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】 1：将 fastEthernet *0*/1 接口的 OSPF 判断邻居死亡时间间隔设为 30。

```
Ruijie(config)# interface fastEthernet 0/1
Ruijie(config-if-FastEthernet 0/1)# ip address 172.16.10.1 255.255.255.0
Ruijie(config-if-FastEthernet 0/1)# ip ospf dead-interval 30
```

2：启用 fastEthernet 0/1 接口的 Fast Hello 功能，配置 hello-multiplier 为 3。

```
Ruijie(config)# interface fastEthernet 0/1
Ruijie(config-if-FastEthernet 0/1)# ip address 172.16.10.1 255.255.255.0
Ruijie(config-if-FastEthernet 0/1)# ip ospf dead-interval minimal hello-multiplier 3
```

【检验方法】 1：执行 show ip ospf interface 命令可以查看相应端口下配置的邻居死亡时间间隔

【提示信息】 -

【常见错误】 1：同一区域中不同端口间所配置的邻居死亡时间间隔不同

【平台说明】 -

5.28 ip ospf disable all

指定接口不再产生 ospf 报文。

ip ospf disable all

恢复为默认状态。

no ip ospf disable all

【参数说明】

参数	描述
-	-

【缺省配置】 接口允许产生 ospf 报文

【命令模式】 接口配置模式。

【缺省级别】 14

【使用指导】 配置该命令的接口将忽略了 network area 是否匹配，配置完该命令后，即使接口属于该 network，也将不再产生 ospf 数据报。因此它不会接收和发送任何 OSPF 报文，也不参与 OSPF 的计算。

【配置举例】 1:设置接口 FastEthernet 0/1 不在产生 OSPF 报文

```
Ruijie(config)# interface fastEthernet 0/1
Ruijie(config-if-FastEthernet 0/1)# ip address 172.16.10.1 255.255.255.0
Ruijie(config-if-FastEthernet 0/1)# ip ospf disable all
```

【检验方法】 -

【提示信息】 1：使用 show ip ospf interface 命令可以查看接口是否加入 ospf 运行。

【常见错误】 -

【平台说明】 -

5.29 ip ospf hello-interval

设置 OSPF 发送 Hello 报文的时间间隔.
ip ospf hello-interval *seconds*

恢复缺省配置。
no ip ospf hello-interval

【参数说明】

参数	描述
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。

【缺省配置】 以太网 10 秒；
PPP、HDLC 封装的接口 10 秒；
帧中继点到点子
接口 10 秒；
非帧中继点到点子接口、X.25 接口 30 秒。

【命令模式】 接口配置模式。

【缺省级别】 14

【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。

【配置举例】 1：将 fastEthernet 0/1 接口的 OSPF 发送 Hello 报文时间间隔设为 15 秒。

```
Ruijie(config)# interface fastEthernet 0/1
Ruijie(config-if-FastEthernet 0/1)# ip address 172.16.10.1 255.255.255.0
Ruijie(config-if-FastEthernet 0/1)# ip ospf hello-interval 15
```

【检验方法】 1：执行 show ip ospf interface 可以查看对应接口的 Hello 报文时间间隔。

【提示信息】 -

【常见错误】 1：同一区域的不同端口配置的 Hello 报文时间间隔不同。

【平台说明】 -

5.30 ip ospf message-digest-key

配置 OSPF 报文 MD5 认证密钥.
ip ospf message-digest-key *key-id* **md5** [**0** | **7**] *key*

删除已配置的 OSPF 报文 MD5 认证密钥。
no ip ospf message-digest-key *key-id*

【参数说明】

参数	描述
key	密钥，最多可以由 16 个字符组成。
0	指定密钥以明文显示
7	指定密钥以密文显示
key-id	密钥标识符，从 1 到 255。

【缺省配置】 缺省没有配置 MD5 密钥。

【命令模式】 接口配置模式。

【缺省级别】 14

【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】 1：fastEthernet 0/1 端口增加了一个新的 OSPF 认证密钥，密钥号为 5，密钥为 hello5。

```
Ruijie(config)# interface fastEthernet 0/1
Ruijie(config-if-FastEthernet 0/1)# ip address 172.16.24.2 255.255.255.0
Ruijie(config-if-FastEthernet 0/1)# ip ospf authentication message-digest
Ruijie(config-if-FastEthernet 0/1)# ip ospf message-digest-key 10 md5 hello10
Ruijie(config-if-FastEthernet 0/1)# ip ospf message-digest-key 5 md5 hello5
```

2:等所有的邻居都增加了新的密钥后，全部路由设备都需要删除旧的密钥。

```
Ruijie(config)# interface fastEthernet 0/1
Ruijie(config-if-FastEthernet 0/1)# no ip ospf message-digest-key 10 md5 hello10
```

【检验方法】 -

【提示信息】 1：删除未配置的密钥。

```
OSPF: Key 1 does not exist
```

2：重复配置已配置的密钥。

```
OSPF: Key 1 already exists
```

3：密文过长，将被截断为 16 个字符。

```
%OSPF: Warning: The password/key will be truncated to 16 characters
```

【常见错误】 -

【平台说明】 -

5.31 ip ospf mtu-ignore

忽略该接口在收到数据库描述报文后对 mtu 的校验.
ip ospf mtu-ignore

恢复缺省配置。
no ip ospf mtu-ignore

【参数说明】

参数	描述
-	-

【缺省配置】 缺省不对 mtu 进行校验。

【命令模式】 接口配置模式。

【缺省级别】 14

【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】 1：将 fastEthernet 0/1 的 MTU 校验功能关闭。

```
Ruijie(config)# interface fastEthernet 0/1
Ruijie(config-if-FastEthernet 0/1)# ip ospf mtu-ignore
```

【检验方法】 -

【提示信息】 -

【常见错误】 -

【平台说明】 -

5.32 ip ospf network

设定接口的 OSPF 网络类型。

ip ospf network { **broadcast** | **non-broadcast** | **point-to-multipoint** [**non-broadcast**] | **point-to-point** }

恢复缺省配置。

no ip ospf network

【参数说明】

参数	描述
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。

【缺省配置】 广播类型：以太网封装；

P2P 类型：PPP、SLIP、帧中继点到点子接口、X.25 点到点子接口封装；
NBMA 类型：帧中继（点到点子接口除外）、X.25 封装（点到点子接口除外）；
缺省没有接口为 P2MP 类型。

【命令模式】 接口配置模式。

【缺省级别】 14

【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。

【配置举例】 1：将帧中继接口设定为 P2P 类型，适合 1 对 1 互联的。

```
Ruijie(config)# interface Serial 1/0
Ruijie(config-Serial 1/0)#ip address 172.16.24.4 255.255.255.0
Ruijie(config-Serial 1/0)# encapsulation frame-relay
Ruijie(config-Serial 1/0)# ip ospf network point-to-point
```

2：将帧中继接口设定为 NBMA 类型，适合全网状连接。

```
Ruijie(config)# interface Serial 1/0
Ruijie(config-Serial 1/0)# ip address 172.16.24.4 255.255.255.0
Ruijie(config-Serial 1/0)# encapsulation frame-relay
Ruijie(config-Serial 1/0)# ip ospf network non-broadcast
Ruijie(config-Serial 1/0)#exit
Ruijie(config)# router ospf 20
Ruijie(config-router)# neighbor 172.16.24.2 priority 1 poll-interval 150
```

【检验方法】 1：使用 show ip ospf interface 命令可以查看所配置的网络类型。

【提示信息】 -

【常见错误】 -

【平台说明】 -

5.33 ip ospf priority

配置接口的 OSPF 优先权值
ip ospf priority *priority*

恢复缺省配置。
no ip ospf priority

【参数说明】

参数	描述
priority	设置接口的 OSPF 优先权值，取值范围：0-255。

【缺省配置】 优先权值缺省为 1。

【命令模式】 接口配置模式。

【缺省级别】 14

【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】 1:将 fastethernet 0/1 接口的优先权值设为 0。

```
Ruijie(config)# interface fastethernet 0/1
Ruijie(config-if-FastEthernet 0/1)# ip ospf priority 0
```

【检验方法】 1：使用 show ip ospf interface 命令可以查看所配置的接口优先级。

【提示信息】 -

【常见错误】 -

【平台说明】 -

5.34 ip ospf retransmit-interval

定义接口 LSU（链路状态更新）报文重传时间间隔.
ip ospf retransmit-interval *seconds*

恢复缺省配置。
no ip ospf retransmit-interval

【参数说明】

参数	描述
seconds	LSU 重传时间间隔，以秒为单位，取值范围：0-65535。该时间必须大于两个邻居之间的数据包往返传输延时。

【缺省配置】 缺省为 5 秒。

【命令模式】 接口配置模式。

【缺省级别】 14

【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。

【配置举例】 1：将 fastEthernet 0/1 接口的 LSU 报文重传时间设为 10 秒。

```
Ruijie(config)# interface fastEthernet 0/1
Ruijie(config-if-FastEthernet 0/1)# ip ospf retransmit-interval 10
```

【检验方法】 1：使用 show ip ospf interface 命令可以查看所配置的重传时间间隔。

【提示信息】 -

【常见错误】 -

【平台说明】 -

5.35 ip ospf source-check-ignore

配置在点对点链路上对收到的报文不进行源地址校验。
ip ospf source-check-ignore

形式恢复缺省配置。
no ip ospf source-check-ignore

【参数说明】

参数	描述
-	-

【缺省配置】 缺省点对点链路进行源地址校验。

【命令模式】 接口配置模式。

【缺省级别】 14

【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】 1：以下的配置例子，将关闭对点对点链路的源地址校验。

```
Ruijie(config)# interface serial 1/0
Ruijie(config-if-FastEthernet 0/1)# ip ospf source-check-ignore
```

【检验方法】 -

【提示信息】 -

【常见错误】 -

【平台说明】 -

5.36 ip ospf transmit-delay

定义 OSPF 接口传输 LSU 报文的延时.
ip ospf transmit-delay *seconds*

恢复缺省配置。
no ip ospf transmit-delay

【参数说明】

参数	描述
seconds	定义 OSPF 接口传输 LSU 报文的延时，以秒为单位，取值范围：0-65535。

【缺省配置】 缺省为 1 秒。

【命令模式】 接口配置模式。

【缺省级别】 14

【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。
RGOS 软件对 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。

【配置举例】 1：将 fastEthernet 0/1 的传输延时设为 10。

```
Ruijie(config)# interface fastEthernet 0/1
Ruijie(config-if-FastEthernet 0/1)# ip ospf transmit-delay 10
```

【检验方法】 1：使用 show ip ospf interface 命令可以查看所配置的报文发送延迟时间。

【提示信息】 -

【常见错误】 -

【平台说明】 -

5.37 log-adj-changes

设置是否记录邻接状态变化的日志.
log-adj-changes [**detail**]

关闭记录邻接状态变化的日志..
no log-adj-changes [**detail**]

【参数说明】

参数	描述
detail	记录全部状态变化信息

【缺省配置】 缺省该功能打开，不带 detail 参数，只记录以下 4 类事件的日志信息：
邻接状态达到 Full 状态；
邻接状态离开 Full 状态；
邻接状态达到 Down 状态；
邻接状态离开 Down 状态。

【命令模式】 路由进程配置模式。

【缺省级别】 14

【使用指导】 -

【配置举例】 1：打开邻居状态变化的日志记录。

```
Ruijie(config)# router ospf 1
Ruijie(config-router)# log-adj-changes detail
```

【检验方法】 1：使用 show ip ospf 命令可以查看所配置的日志记录开关状态。

【提示信息】 -

【常见错误】 -

【平台说明】 -

5.38 max-concurrent-dd

配置用于设置当前 OSPF 实例同时并发交互（发起或接受）的邻居最大数目。
max-concurrent-dd *number*

恢复为默认配置。
no max-concurrent-dd

【参数说明】

参数	描述
number	指定并发交互的邻居最大数目 范围 1-65535

【缺省配置】 缺省为 5。

【命令模式】 路由进程配置模式。

【缺省级别】 14

【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。

【配置举例】 1：将并发交互（发起或接受）的邻居最大数目设置为 4，该配置的效果是大量邻居交互的过程中，本设备最大允许同时发起与 4 个邻居交互，并最大允许同时接受 4 个邻居发起的交互，即本设备最多可以同时与 8 个邻居进行交互。

```
Ruijie(config)# router ospf 10
Ruijie(config-router)# max-concurrent-dd 4
```

【检验方法】 1：执行 show ip ospf 命令可以看到对应最大允许交互个数。

【提示信息】 -

【常见错误】 -

【平台说明】 -

5.39 max-metric

配置运行 OSPF 协议的路由设备通告最大度量，以使其它路由设备在 SPF 计算中不优先将该设备作为传输节点.

max-metric router-lsa [**external-lsa** [*max-metric-value*]] [**include-stub**] [**on-startup** [*seconds*]] [**summary-lsa** [*max-metric-value*]]

取消通告最大度量。

no max-metric router-lsa [**external-lsa** [*max-metric-value*]] [**include-stub**] [**on-startup** [*seconds*]] [**summary-lsa** [*max-metric-value*]]

【参数说明】

参数	描述
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。

【缺省配置】 缺省通告正常度量的 LSAs。

【命令模式】 路由进程配置模式。

【缺省级别】 14

【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。

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。

【配置举例】 1：配置开机后通告最大度量 100 秒：

```
Ruijie(config)# router ospf 20
Ruijie(config-router)# max-metric router-lsa on-startup 100
```

【检验方法】 1：使用 show ip ospf 命令可以查看所配置的 max-metric 功能。

【提示信息】 -

【常见错误】 -

【平台说明】 -

5.40 neighbor

定义 OSPF 邻居.
neighbor *ip-address* [**poll-interval** *seconds*] [**priority** *priority*] [**cost** *cost*]

删除指定的邻居。
no neighbor *ip-address* [**poll-interval**] [**priority**] | [**cost**]

【参数说明】

参数	描述
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。

【缺省配置】 缺省没有定义邻居；
邻居轮询时间间隔：缺省 120 秒；
非广播网络邻居的优先权值：缺省为 0。

【命令模式】 路由进程配置模式。

【缺省级别】 14

【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。

【配置举例】 1：在 NBMA 网络上指定一个邻居，IP 地址为 172.16.24.2，优先权值为 1，轮询间隔为 150 秒。

```
Ruijie(config)# router ospf 20
Ruijie(config-router)# network 172.16.24.0 0.0.0.255 area 0
Ruijie(config-router)# neighbor 172.16.24.2 priority 1 poll-interval 150
```

【检验方法】 1：若邻居配置正确则可以正常建立邻居，使用 show ip ospf neighbor 可以看到对应的邻居。

【提示信息】 1：配置的邻居地址为本机地址，提示错误。

```
%OSPF: Warning: OSPF neighbor address 192.168.1.1 is our address
```

【常见错误】

【平台说明】 -

5.41 network area

定义哪些接口将运行 OSPF，以及所属 OSPF 区域.
network *ip-address wildcard* **area** *area-id*

删除接口的 OSPF 区域定义。
no network *ip-address wildcard* **area** *area-id*

【参数说明】

参数	描述
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。

【缺省配置】 缺省没有配置 OSPF 区域。

【命令模式】 路由进程配置模式。

【缺省级别】 14

【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。

【配置举例】 1：定义 3 个区域：0，1，172.16.16.0。将 IP 地址落在 192.168.12.0/24 范围内的接口定义到区域 1，将 IP 地址落在 172.16.16.0/20 范围内的接口定义到区域 172.16.16.0，将其余接口定义到区域 0。

```
Ruijie(config)# router ospf 20
Ruijie(config-router)# network 172.16.16.0 0.0.15.255 area 172.16.16.0
Ruijie(config-router)# network 192.168.12.0 0.0.0.255 area 1
Ruijie(config-router)# network 0.0.0.0 255.255.255.255 area 0
```

【检验方法】 1：使用 show ip ospf interface 命令可以查看所配置的 network 网段所包含的接口加入 ospf 协议运行；
2：使用 show ip ospf database 命令可以查看 LSA 信息中生成接口对应的信息。

【提示信息】 1：无效的 IP 地址/掩码组合。

```
OSPF: Invalid address/mask combination
```

【常见错误】

【平台说明】 -

5.42 overflow database

配置当前 OSPF 实例所支持的 LSA 的最大数目。
overflow database *number* [**hard | soft**]

恢复为缺省配置。
no overflow database

【参数说明】

参数	描述
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

【缺省配置】 缺省不限制当前 OSPF 实例所支持的 LSA 的最大数目。

【命令模式】 路由进程配置模式。

【缺省级别】 14

【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

【配置举例】 1：配置当 LSA 超过 10 条时，关闭 OSPF 10 实例。

```
Ruijie(config)# router ospf 10
Ruijie(config-router)# overflow database 10 hard
```

【检验方法】 -

【提示信息】 -

【常见错误】 -

【平台说明】 -

5.43 overflow database external

配置 external LSA 的最大数目与从溢出状态恢复正常状态所需等待的时间。
overflow database external *max-dbsize wait-time*

恢复为缺省配置。
no overflow database external

【参数说明】

参数	描述
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。

【缺省配置】 缺省不限制 external-LSA 的最大数目。
如果限制了 external-LSA 最大数，当 external-LSA 的数目超过配置的最大值后，不再恢复正常状态。

【命令模式】 路由进程配置模式。

【缺省级别】 14

【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】 1：配置 external lsa 最大数目为 10，超过则变为 overflow 状态，尝试从 overflow 状态恢复到的时间间隔为 3 秒。

```
Ruijie(config)# router ospf 10
Ruijie(config-router)# overflow database external 10 3
```

【检验方法】 -

【提示信息】 -

【常见错误】 -

【平台说明】 -

5.44 overflow memory-lack

允许在内存不足时 OSPF 进入 OVERFLOW 状态。
overflow memory-lack

关闭内存不足时 OSPF 进入 OVERFLOW 状态。
no overflow memory-lack

【参数说明】

参数	描述
-	-

【缺省配置】 内存不足情况下 OSPF 允许进入 OVERFLOW 状态。

【命令模式】 路由进程配置模式

【缺省级别】 14

【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。

【配置举例】 1：在内存不足情况下，不进入 OVERFLOW 状态

```
Ruijie(config)# router ospf 1
```

```
Ruijie(config-router)# no overflow memory-lack
```

【检验方法】 -

【提示信息】 -

【常见错误】 -

【平台说明】 -

5.45 passive-interface

配置本路由设备的指定的网络接口为被动接口。
passive-interface { **default** | *interface-type interface-number* | *interface-type interface-number ip-address* }

恢复缺省配置。
no passive-interface { **default** | *interface-type interface-number* | *interface-type interface-number ip-address* }

【参数说明】

参数	描述
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-number ip-address	指定接口下的地址为被动地址。

【缺省配置】 缺省情况下，没有接口被设置为被动接口，允许所有接口收发 OSPF 报文。

【命令模式】 路由进程配置模式。

【缺省级别】 14

【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。

【配置举例】 1：将接口 fastEthernet 0/1 设置为被动接口，指定该接口下的 IP 1.1.1.1 为被动 IP 地址。

```
Ruijie(config)# router ospf 30
Ruijie(config-router)# passive-interface fastEthernet 0/1
Ruijie(config-router)# passive-interface fastEthernet 0/1 1.1.1.1
```

【检验方法】 1：show ip ospf interface 查看对应的状态。

【提示信息】 1：指定了无效的接口。

```
% Interface is invalid.
```

【常见错误】

【平台说明】 -

5.46 redistribute

重分布外部路由信息。

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*]

no 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】

参数	描述
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

【缺省配置】 缺省情况下不支持重分布配置。

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 BGP 路由缺省 metric 为 1，其余类型路由生成的 LSA 缺省的 metric 为 20；

metric-type 缺省为 E-2；

缺省不关联 route-map。

【命令模式】 路由配置模式

【缺省级别】 14

【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 路由，只有重分布的路由满足配置的 match 或 level 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。

【配置举例】

1：**show run** 显示结果如下：

```
router ospf 1
redistribute ospf 2 match external 1 internal subnets
```

【检验方法】 1：使用 show ip ospf database 命令可以查看引入了所配置的路由信息。

【提示信息】 1：不允许重分布本实例的路由。

```
% Redistribution of "ospf 1" via "ospf 1" not allowed
```

2：仅重分布有类网段。

```
% Only classful networks will be redistributed
```

【常见错误】 同一个 ospf 实例进行重分发

【平台说明】 -

5.47 router ospf

创建 OSPF 路由进程并进入 OSPF 路由配置模式。

router ospf

删除已定义的 OSPF 路由进程。
no router ospf *process-id*

【参数说明】

参数	描述
process-id	OSPF 进程号。未配置进程号时，表示配置进程 1。

【缺省配置】 缺省不存在 OSPF 路由进程。

【命令模式】 全局配置模式。

【缺省级别】 14

【使用指导】 RGOS10.1 在原实现基础上增加了进程号参数，扩展为多实例 OSPF。不同 OSPF 实例间相互独立，可以近似认为是两个独立运行的路由协议。

【配置举例】 -

【检验方法】 执行 show ip ospf 可以看到对应进程号的 ospf 实例是否创建成功。

【提示信息】 1：无法分配到 router-id 则相应 ospf 进程无法启动

```
%OSPF-4-NORTRID: OSPF process 1 failed to allocate unique router-id and cannot start.
```

【常见错误】 -

【平台说明】 -

5.48 router ospf max-concurrent-dd

配置用于设置所有 OSPF 路由进程同时并发交互（发起或接受）的邻居最大数目。
router ospf max-concurrent-dd *number*

恢复缺省配置。
no router ospf max-concurrent-dd

【参数说明】

参数	描述
number	并发交互的邻居最大数目 范围 1-65535

【缺省配置】 缺省为 10。

【命令模式】 全局配置模式。

【缺省级别】 14

【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】 1：将所有 OSPF 实例并发交互（发起或接受）的邻居最大数目设置为 4，该配置的效果是大量邻居交互的过程中，本设备最大允许同时发起与 4 个邻居交互，并最大允许同时接受 4 个邻居发起的交互，即本设备最多可以同时与 8 个邻居进行交互。

```
Ruijie(config)# router ospf max-concurrent-dd 4
```

【检验方法】 -

【提示信息】 -

【常见错误】 -

【平台说明】 -

5.49 router-id

置该路由设备的 ID。
router-id *router-id*

删除所设置的 Router ID，恢复使用缺省的 Router ID。
no router-id

【参数说明】

参数	描述
router-id	要设置的路由设备的 ID，以 IP 地址形式表示

【缺省配置】 OSPF 路由进程选举所有回环（loopback）接口 IP 地址最大的作为路由设备标识；
如果没有配置 IP 地址的回环（loopback）接口，那么 OSPF 将选取它所有的物理接口 IP 地址最大的作为路由设备标识。

【命令模式】 路由进程配置模式。

【缺省级别】 14

【使用指导】 可以配置任何一个 IP 地址作为该路由设备的路由设备标识，但是每台路由设备的路由设备标识必须唯一。注意由于改变后，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。建议在生成 LSA 之前先设置好指定的 router-id。

【配置举例】 1：修改路由设备的 router-id 为 0.0.0.36。

```
Ruijie(config)# router ospf 20
Ruijie(config-router)# router-id 0.0.0.36
```

【检验方法】 执行 show ip ospf 命令可以看到对应 ospf 实例的 Router-ID。

【提示信息】 1：配置 Router-ID 为 0.0.0.0 提示该操作会导致 OSPF 进程停止运行。

```
% OSPF: router-id set to 0.0.0.0, process will not run.
```

2：配置的 router-id 和其它实例的 router-id 重复。

```
% OSPF: router-id 192.168.1.1 is in use by process 1
```

【常见错误】 -

【平台说明】 -

5.50 show ip ospf

显示 OSPF 信息概要

show ip ospf [*process-id*]

【参数说明】

参数	描述
process-id	OSPF 进程号

【命令模式】 特权模式

【缺省级别】 14

【使用指导】 应用该命令可以显示 OSPF 路由进程的运行信息概要。

【配置举例】 1：显示 OSPF 信息概要

```
Ruijie# show ip ospf
Routing Process "ospf 1" with ID 1.1.1.1
  Domain ID type 0x0105, value 0x010101010101
Process uptime is 4 minutes
Process bound to VRF default
Memory Overflow is enabled.
Router is not in overflow state now.
Conforms to RFC2328, and RFC1583Compatibility flag isenabled
Supports only single TOS(TOS0) routes
Enable two-way-maintain
```

```
Enable ispf
Supports opaque LSA
Supports Graceful Restart
This router is an ASBR (injecting external routing information)
Originating router-LSAs with maximum metric
    Condition: on startup for 100 seconds, State: inactive
    Advertise stub links with maximum metric in router-LSAs
    Advertise summary-LSAs with metric 16711680
    Advertise external-LSAs with metric 16711680
    Unset reason: timer expired, Originated for 100 seconds
    Unset time: 00:02:02.080, Time elapsed: 00:23:54.656
SPF schedule delay 5 secs, Hold time between two SPFs 10 secs
Initial LSA throttle delay 0 msecs
Minimum hold time for LSA throttle 5000 msecs
Maximum wait time for LSA throttle 5000 msecs
Lsa Transmit Pacing timer 40 msecs, 1 LS-Upd
Minimum LSA arrival 1000 msecs
Pacing lsa-group: 30 secs
Number of incomming current DD exchange neighbors 0/5
Number of outgoing current DD exchange neighbors 0/5
Number of external LSA 4. Checksum 0x0278E0
Number of opaque AS LSA 0. Checksum 0x000000
Number of non-default external LSA 4
External LSA database is unlimited.
Number of LSA originated 6
Number of LSA received 2
Log Neighbor Adjency Changes : Enabled
Graceful-restart disabled
Graceful-restart helper support enabled
Number of areas attached to this router: 1
BFD enabled
Area 0 (BACKBONE)
Number of interfaces in this area is 1(1)
Number of fully adjacent neighbors in this area is 1
Area has no authentication
SPF algorithm last executed 00:01:26.640 ago
SPF algorithm executed 4 times
iSPF algorithm executed 0 timesNumber of LSA 3. Checksum 0x0204bf
Area 1 (NSSA)
Number of interfaces in this area is 1(1)
Number of fully adjacent neighbors in this area is 0
```

```
Number of fully adjacent virtual neighbors through this area is 0
Area has no authentication
SPF algorithm last executed 02:09:23.040 ago
SPF algorithm executed 4 times
iSPF algorithm executed 0 times
Number of LSA 6. Checksum 0x028638
NSSA Translator State is disabled,Stability Interval expired in 00:00:03
```

字段解释：

字段	说明
Router ID	路由设备标识符。
Process uptime	本 OSPF 进程生效的时间（router-id 为 0.0.0.0 时进程是不生效的）。
Bound to VRF	本 OSPF 进程所属的 VRF。
Conforms to RFC2328	与 RFC2328 一致。
RFC1583Compatibility flag	在计算外部路由时采用的是 RFC1583 规则还是 RFC2328 的规则；在选择最佳的 ASBR 和路由比较时该规则将被用到。
Support Tos	只支持 TOS0。
Supports opaque LSA	支持 opaque-LSA。
Graceful-restart	RFC3623 Graceful Restart 描述的 GR Restart 能力。
Graceful-restart helper	RFC3623 Graceful Restart 描述的 GR Help 能力。
Router Type	OSPF 路由设备类型有 normal 、ABR 、ASBR。
SPF Delay	收到拓扑变化调用 SPF 运算所要延迟的时间。
SPF-holdtime	两次 SPF 计算之间至少要维持的时间。
LsaGroupPacing	LSA 的更新，校验和计算，老化等的时间间隔。
Incomming current DD exchange neighbors	正在交互的邻居数量 ,incomming 指首次进入 exstart 状态的邻居。
Outgoing current DD exchange neighbors	正在交互的邻居数量，outgoing 指从更高状态退回 exstart 重新交互的邻居。
Number of external LSA	数据库中存储的外部 LSA 的数量。
External LSA Checksum Sum	数据库中存储的外部 LSA 的检验和的总和。
Number of opaque LSA	数据库中存储的 opaque-LSA 的数量。
Opaque LSA Checksum Sum	数据库中存储的 opaque-LSA 的检验和的总和。
Number of non-default external LSA	非缺省路由的 external-LSA 的数量。
External LSA database limit	external-LSA 数量限制。
Exit database overflow state interval	判断离开 overflow 状态的时间。
Database overflow state	当前 OSPF 进程是否处于 overflow 状态。
Number of LSA originated	生成的 LSA 数量。
Number of LSA received	接收到的 LSA 数量。
Log Neighbor Adjency Changes	邻居状态变化记录开关是否打开。

Number of areas attached to this router	该路由设备上的区域总数。
Area type	区域类型，值有 Default， Stub，NSSA。
Number of interfaces in this area	属于该区域的接口数目。
Number of fully adjacent neighbors in this area	属于该区域的 Full 的邻居数量。
Number of fully adjacent virtual neighbors through this area	属于该区域的 Full 的虚链接的邻居数量 ;只有在非骨干的默认类型的区域有效。
Area authentication	区域的认证方式。
SPF algorithm last executed	上次 SPF 计算到目前所经过的时间。
SPF algorithm executed times	SPF 计算的次数。
Number of LSA	属于该区域的 LSA 的总的数量。
Checksum Sum	该区域的 LSA 的校验和的总和。
NSSA Translator State	是否将 NSSA LSA 转换为 External LSA ;仅对 NSSA 区，并且是 ABR 的 OSPF 进程有效。
BFD enabled	表示启用 OSPF 与 BFD 联动

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

【提示信息】 -

【平台说明】 -

5.51 show ip ospf border-routers

显示到 ABR/ASBR 的 OSPF 内部路由表。

show ip ospf [*process-id*] **border-routers**

【参数说明】

参数	描述
process-id	ospf 进程号

【命令模式】 特权模式

【缺省级别】 14

【使用指导】 应用该命令，可以显示本地路由设备到 ABR 或 ASBR 路由设备的 OSPF 内部路由。OSPF 内部路由表不同于 **show ip route** 显示的路由表，OSPF 内部路由表的目标地址为 OSPF 路由设备标识，而不是目标网络。

【配置举例】 1：显示到 ABR/ASBR 的 OSPF 内部路由表。

```
Ruijie# show ip ospf border-routers
OSPF internal Routing Table
Codes: i - Intra-area route, I - Inter-area route
i 1.1.1.1 [2] via 10.0.0.1, FastEthernet 0/1, ABR, ASBR, Area 0.0.0.1 select
```

字段解释：

字段	说明
Codes	路由类型代码定义。i 表示区域内部路由，I 表示区域之间路由。
I	表示该路由为区域内部路由。
1.1.1.1	显示边界路由设备的 OSPF 标识符。
[2]	显示到达该边界路由设备的花费（cost）。
via 10.0.0.1	显示到达边界路由设备的下一跳网关。
FastEthernet 0/1	显示到达边界路由设备的接口。
ABR, ASBR	显示边界路由设备的类型，有 ABR 和 ASBR 两种，可以同时是 ABR 和 ASBR。
Area 0.0.0.1	显示学习到该路由的区域。
select	当有多条路径到达 ASBR 时 ,select 表示当前选择的最优路径。

【提示信息】 -

【平台说明】 -

5.52 show ip ospf database

显示 OSPF 链路状态数据库信息，该命令的不同格式显示不同链路状态描述（LSAs）信息。

show ip ospf [*process-id* [*area-id* | *ip-address*]] **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**]

【参数说明】

参数	描述
process-id	OSPF 进程号
area-id	OSPF 区域号，数字形式，如 1
ip-address	OSPF 区域号，IP 地址形式，如 0.0.0.1
adv-router	显示由指定公告路由设备生成的链路状态描述信息。
link-state-id	只显示指定 OSPF 链路状态标识的链路状态描述信息。
self-originate	显示由本路由设备自己生成的链路状态描述信息。
max-age	显示已到老化时间的 LSA
router	显示 OSPF 路由设备链路状态描述信息。
network	显示 OSPF 网络链路状态描述信息。
summary	显示 OSPF 摘要链路状态描述信息。
asbr-summary	显示关于 ASBR 的摘要链路状态描述信息。
external	显示 OSPF 外部链路状态描述信息。
nssa-external	显示 OSPF 第七类外部链路状态描述信息。

opaque-area	显示第十类 LSA
opaque-as	显示第十一类 LSA
opaque-link	显示第九类 LSA
database-summary	显示 OSPF 链路状态数据库各种 LSA 统计信息。
detail	显示 OSPF 所有 LSA 的详细信息。
brief	显示指定类型的 LSA 摘要信息。

【命令模式】 特权模式

【缺省级别】 14

【使用指导】 当 OSPF 链路状态数据库很大时，分项显示是十分必要的。正确地使用这些命令，有助于 OSPF 故障的排除。

【配置举例】 1：**show ip ospf database** 命令的显示结果

```
Ruijie# show ip ospf database
OSPF Router with ID (1.1.1.1) (Process ID 1)
Router Link States (Area 0.0.0.0)
Link ID         ADV Router      Age  Seq#       CkSum  Link count
1.1.1.1         1.1.1.1         2    0x80000011 0x6f39 2
3.3.3.3         3.3.3.3         120  0x80000002 0x26ac 1
Network Link States (Area 0.0.0.0)
Link ID         ADV Router      Age  Seq#       CkSum
192.88.88.27    1.1.1.1         120  0x80000001 0x5366
Summary Link States (Area 0.0.0.0)
Link ID         ADV Router      Age  Seq#       CkSum  Route
10.0.0.0        1.1.1.1         2    0x80000003 0x350d 10.0.0.0/24
100.0.0.0       1.1.1.1         2    0x8000000c 0x1ecb 100.0.0.0/16
Router Link States (Area 0.0.0.1 [NSSA])
Link ID         ADV Router      Age  Seq#       CkSum  Link count
1.1.1.1         1.1.1.1         2    0x80000001 0x91a2 1
Summary Link States (Area 0.0.0.1 [NSSA])
Link ID         ADV Router      Age  Seq#       CkSum  Route
100.0.0.0       1.1.1.1         2    0x80000001 0x52a4 100.0.0.0/16
192.88.88.0     1.1.1.1         2    0x80000001 0xbb2d 192.88.88.0/24
NSSA-external Link States (Area 0.0.0.1 [NSSA])
Link ID    ADV Router    Age  Seq#       CkSum  Route           Tag
20.0.0.0     1.1.1.1     1    0x80000001 0x033c E2 20.0.0.0/24  0
100.0.0.0   1.1.1.1      1    0x80000001 0x9469 E2 100.0.0.0/28 0
AS External Link States
Link ID   ADV Router     Age  Seq#       CkSum  Route           Tag
20.0.0.0   1.1.1.1       380  0x8000000a 0x7627 E2 20.0.0.0/24  0
```

```
100.0.0.0      1.1.1.1       620   0x8000000a 0x0854 E2 100.0.0.0/28 0
```

字段解释：

字段	说明
OSPF Router with ID	显示 OSPF 链路状态数据库的路由设备标识符与本 OSPF 对应的进程号
Router Link States	表示以下内容为路由设备链路状态描述信息。
Net Link States	表示以下内容为网络链路状态描述信息。
Summary Net Link States	表示以下内容为摘要网络链路状态描述信息。
NSSA-external Link States	表示以下内容为第七类的自治域外部链路状态描述信息
AS External Link States	表示以下内容为第五类的自治域外部链路状态描述信息。
Link ID	链路标识。
ADV Router	通告该链路状态描述的路由设备标识。
Age	显示该链路状态描述的存在时间。
Seq#	显示该链路状态描述的序号，用于检测老的或重复的 LSA。
Cksum	显示该链路状态描述的校验和。
Link-Count	显示路由设备链路状态描述信息中的链路的数量
Route	显示此 LSA 包含的路由信息
Tag	显示该链路状态描述的标记。

2：**show ip ospf database asbr-summary** 命令的显示结果

```
Ruijie# show ip ospf database asbr-summary
OSPF Router with ID (1.1.1.35) (Process ID 1)
ASBR-Summary Link States (Area 0.0.0.1)
LS age: 47
Options: 0x2 (*|-|-|-|-|-|E|-)
LS Type: ASBR-summary-LSA
Link State ID: 3.3.3.3 (AS Boundary Router address)
Advertising Router: 1.1.1.1
LS Seq Number: 80000001
Checksum: 0xbe8c
Length: 28
Network Mask: /0
TOS: 0  Metric: 1
```

字段解释：

字段	说明
OSPF Router with ID	显示以下信息对应的路由设备标识符与本 OSPF 对应的进程号

AS Summary Link States	表示以下显示的是 AS 摘要链路描述信息。
LS age	显示该链路状态描述的存在时间。
Options	选项。
LS Type	显示该链路状态描述的类型。
Link State ID	显示该链路状态描述的链路标识。
Advertising Router	显示该链路状态描述的通告路由设备。
LS Seq Number	显示该链路状态描述的序号。
Checksum	显示该链路状态描述的校验和。
Length	显示该链路状态描述的长度，以字节为单位。
Network Mask	显示该链路状态描述对应路由的网络掩码。
TOS	TOS 值，目前只能为 0。
Metric	显示该链路状态描述对应路由的量度值。

3： **show ip ospf database external** 命令的显示结果

```
Ruijie# show ip ospf database external
OSPF Router with ID (1.1.1.35) (Process ID 1)
AS External Link States
LS age: 752
Options: 0x2 (*|-|-|-|-|-|E|-)
LS Type: AS-external-LSA
Link State ID: 20.0.0.0 (External Network Number)
Advertising Router: 1.1.1.1
LS Seq Number: 8000000a
Checksum: 0x7627
Length: 36
Network Mask: /24
Metric Type: 2 (Larger than any link state path)
TOS: 0
Metric: 20
Forward Address: 0.0.0.0
External Route Tag: 0
```

字段解释：

字段	说明
OSPF Router with ID	显示以下信息对应的路由设备标识符与本 OSPF 对应的进程号。。
Type-5 AS External Link States	表示以下信息为自治域外部链路状态描述信息。
LS age	显示该链路状态描述的存在时间。
Options	选项。
LS Type	显示该链路状态描述的类型。
Link State ID	显示该链路状态描述的链路标识。

Advertising Router	显示该链路状态描述的通告路由设备。
LS Seq Number	显示该链路状态描述的序号。
Checksum	显示该链路状态描述的校验和。
Length	显示该链路状态描述的长度，以字节为单位。
Network Mask	显示该链路状态描述对应路由的网络掩码。
Metric Type	表示外部链路类型。
TOS	TOS 值，目前只能为 0。
Metric	显示该链路状态描述对应路由的量度值。
Forward Address	到该目标网络的数据流量，将被转发到该 IP 地址。如果该地址为 0.0.0.0，则数据流量会被转发到产生该链路状态的路由设备。
External Route Tag	外部路由标记，每个外部路由都有 32 个比特路由标记。OSPF 本身不使用该路由标记，在其它路由进程路由重分布 OSPF 路由时会应用到。

4：**show ip ospf database network** 命令的显示结果

```
Ruijie# show ip ospf database network
OSPF Router with ID (1.1.1.1) (Process ID 1)
Network Link States (Area 0.0.0.0)
LS age: 572
Options: 0x2 (*|-|-|-|-|-|E|-)
LS Type: network-LSA
Link State ID: 192.88.88.27 (address of Designated Router)
Advertising Router: 1.1.1.1
LS Seq Number: 80000001
Checksum: 0x5366
Length: 32
Network Mask: /24
Attached Router: 1.1.1.1
Attached Router: 3.3.3.3
```

字段解释：

字段	说明
OSPF Router with ID	显示以下信息对应的路由设备标识符与本 OSPF 对应的进程号。
Network Link States	表示以下为网络链路状态描述信息。
LS age	显示该链路状态描述的存在时间。
Options	选项。
LS Type	显示该链路状态描述的类型。
Link State ID	显示该链路状态描述的链路标识。
Advertising Router	显示该链路状态描述的通告路由设备。

LS Seq Number	显示该链路状态描述的序号。
Checksum	显示该链路状态描述的校验和。
Length	显示该链路状态描述的长度，以字节为单位。
Network Mask	显示该链路状态描述对应网络的网络掩码。
Attached Router	显示该网络上所连接的路由设备。

5：**show ip ospf database router** 命令的显示结果

```
Ruijie# show ip ospf database router
OSPF Router with ID (1.1.1.1) (Process ID 1)
Router Link States (Area 0.0.0.0)
LS age: 322
Options: 0x2 (*|-|-|-|-|-|E|-)
Flags: 0x3 : ABR ASBR
LS Type: router-LSA
Link State ID: 1.1.1.1
Advertising Router: 1.1.1.1
LS Seq Number: 80000012
Checksum: 0x6d3a
Length: 48
Number of Links: 2
Link connected to: Stub Network
(Link ID) Network/subnet number: 100.0.1.1
(Link Data) Network Mask: 255.255.255.255
Number of TOS metrics: 0
TOS 0 Metric: 0
```

字段解释：

字段	说明
OSPF Router with ID	显示以下信息对应的路由设备标识符与本 OSPF 对应的进程号。
Router Link States	表示以下为路由设备链路状态描述信息。
LS age	显示该链路状态描述的存在时间。
Options	选项
Flag	router 的标志
LS Type	显示该链路状态描述的类型。
Link State ID	显示该链路状态描述的链路标识。
Advertising Router	显示该链路状态描述的通告路由设备。
LS Seq Number	显示该链路状态描述的序号。
Checksum	显示该链路状态描述的校验和。
Length	显示该链路状态描述的长度，以字节为单位。
Number of Links	显示该路由设备关联的链路数。

Link connected to	显示链路跟谁连接，以及网络类型。
(Link ID)	链路标识。
(Link Data)	链路数据。
Number of TOS metrics	TOS 值，只支持 TOS0。
TOS 0 Metrics	TOS 0 量度值。

6：**show ip ospf database summary** 命令的显示结果

```
Ruijie# show ip ospf database summary
OSPF Router with ID (1.1.1.1) (Process ID 1)
Summary Link States (Area 0.0.0.0)
LS age: 499
Options: 0x2 (*|-|-|-|-|-|E|-)
LS Type: summary-LSA
Link State ID: 10.0.0.0 (summary Network Number)
Advertising Router: 1.1.1.1
LS Seq Number: 80000004
Checksum: 0x330e
Length: 28
Network Mask: /24
TOS: 0  Metric: 11
```

字段解释：

字段	说明
OSPF Router with ID	显示以下信息对应的路由设备标识符与本 OSPF 对应的进程号。
Summary Net Link States	表示以下为摘要网络链路状态描述信息。
LS age	显示该链路状态描述的存在时间。
Options	选项。
LS Type	显示该链路状态描述的类型。
Link State ID	显示该链路状态描述的链路标识。
Advertising Router	显示该链路状态描述的通告路由设备。
LS Seq Number	显示该链路状态描述的序号。
Checksum	显示该链路状态描述的校验和。
Length	显示该链路状态描述的长度，以字节为单位。
Network Mask	显示该链路状态描述对应路由的网络掩码。
TOS	TOS 值，目前只能为 0。
Metric	显示该链路状态描述对应路由的量度值。

7：**show ip ospf database nssa-external** 命令的显示结果

```
Ruijie# show ip ospf database nssa-external
OSPF Router with ID (1.1.1.1) (Process ID 1)
```

```
NSSA-external Link States (Area 0.0.0.1 [NSSA])
LS age: 1
Options: 0x0 (*|-|-|-|-|-|-|-)
LS Type: AS-NSSA-LSA
Link State ID: 20.0.0.0 (External Network Number For NSSA)
Advertising Router: 1.1.1.1
LS Seq Number: 80000001
Checksum: 0x033c
Length: 36
Network Mask: /24
Metric Type: 2 (Larger than any link state path)
TOS: 0
Metric: 20
NSSA: Forward Address: 100.0.2.1
External Route Tag: 0
```

字段解释：

字段	说明
OSPF Router with ID	显示以下信息对应的路由设备标识符与本 OSPF 对应的进程号。
NSSA-external Link States	表示以下信息为第七类自治域外部链路状态描述信息。
LS age	显示该链路状态描述的存在时间。
Options	选项。
LS Type	显示该链路状态描述的类型。
Link State ID	显示该链路状态描述的链路标识。
Advertising Router	显示该链路状态描述的通告路由设备。
LS Seq Number	显示该链路状态描述的序号。
Checksum	显示该链路状态描述的校验和。
Length	显示该链路状态描述的长度，以字节为单位。
Network Mask	显示该链路状态描述对应路由的网络掩码。
Metric Type	表示外部链路类型。
TOS	TOS 值，目前只能为 0。
Metric	显示该链路状态描述对应路由的量度值。
NSSA:Forward Address	到该目标网络的数据流量，将被转发到该 IP 地址。如果该地址为 0.0.0.0，则数据流量会被转发到产生该链路状态的路由设备。
External Route Tag	外部路由标记，每个外部路由都有 32 个比特路由标记。OSPF 本身不使用该路由标记，在其它路由进程路由重分布 OSPF 路由时会应用到。

8：**show ip ospf database external** 命令的显示结果

```
Ruijie# show ip ospf database external
OSPF Router with ID (1.1.1.1) (Process ID 1)
AS External Link States
LS age: 1290
Options: 0x2 (*|-|-|-|-|-|E|-)
LS Type: AS-external-LSA
Link State ID: 20.0.0.0 (External Network Number)
Advertising Router: 1.1.1.1
LS Seq Number: 8000000a
Checksum: 0x7627
Length: 36
Network Mask: /24
Metric Type: 2 (Larger than any link state path)
TOS: 0
Metric: 20
Forward Address: 0.0.0.0
External Route Tag: 0
```

字段解释：

字段	说明
OSPF Router with ID	显示以下信息对应的路由设备标识符与本 OSPF 对应的进程号。
Type-7 AS External Link States	表示以下信息为第七类自治域外部链路状态描述信息。
LS age	显示该链路状态描述的存在时间。
Options	选项。
LS Type	显示该链路状态描述的类型。
Link State ID	显示该链路状态描述的链路标识。
Advertising Router	显示该链路状态描述的通告路由设备。
LS Seq Number	显示该链路状态描述的序号。
Checksum	显示该链路状态描述的校验和。
Length	显示该链路状态描述的长度，以字节为单位。
Network Mask	显示该链路状态描述对应路由的网络掩码。
Metric Type	表示外部链路类型。
TOS	TOS 值，目前只能为 0。
Metric	显示该链路状态描述对应路由的量度值。
Forward Address	到该目标网络的数据流量，将被转发到该 IP 地址。如果该地址为 0.0.0.0，则数据流量会被转发到产生该链路状态的路由设备。
External Route Tag	外部路由标记，每个外部路由都有 32 个比特路由标

	记。OSPF 本身不使用该路由标记，在其它路由进程路由重分布 OSPF 路由时会应用到。

9：**show ip ospf database database-summary** 命令的显示结果

```
Ruijie# show ip ospf database database-summary
OSPF process 1:
Router Link States       : 4
Network Link States      : 2
Summary Link States      : 4
ASBR-Summary Link States : 0
AS External Link States  : 4
NSSA-external Link States: 2
```

字段解释：

字段	说明
OSPF Process	显示以下信息对应的路由进程号
Router Link	在该区域中，OSPF 路由设备 LSA 的数目。
Network Link	在该区域中，OSPF 网络 LSA 的数目。
Summary Link	在该区域中，OSPF 网络摘要 LSA 的数目。
ASBR-Summary Link	在该区域中，OSPFASBR 摘要 LSA 的数目。
AS External Link	在该区域中，OSPF 外部 LSA 的数目
NSSA-external Link	该路由设备中，OSPF NSSA LSA 的数目

【提示信息】 -

【平台说明】 -

5.53 show ip ospf interface

显示与 OSPF 关联的接口信息。

show ip ospf [*process-id*] **interface** [*interface-type interface-number* **| brief**]

【参数说明】

参数	描述
process-id	OSPF 进程号
interface-type	指定接口的接口类型。
interface-number	指定接口的接口编号。
brief	显示接口的摘要。

【命令模式】 特权模式

【缺省级别】 14

【使用指导】 此命令可以显示哪些接口运行 OSPF，以及这些接口跟 OSPF 相关的设置信息。

【配置举例】 1：显示与 OSPF 关联的接口信息。

```
Ruijie# show ip ospf interface fastEthernet 0/1
FastEthernet 0/1 is up, line protocol is up
Internet Address 192.88.88.27/24, Ifindex 4, Area 0.0.0.0, MTU 1500
Matching network config: 192.88.88.0/24
Process ID 1, Router ID 1.1.1.1, Network Type BROADCAST, Cost: 1
Transmit Delay is 1 sec, State DR, Priority 1, BFD enabled
Designated Router (ID) 1.1.1.1, Interface Address 192.88.88.27
Backup Designated Router (ID) 3.3.3.3, Interface Address 192.88.88.72
Timer intervals configured,Hello 10,Dead 40,Wait 40,Retransmit 5
Hello due in 00:00:03
Neighbor Count is 1, Adjacent neighbor count is 1
Crypt Sequence Number is 70784
Hello received 1786 sent 1787, DD received 13 sent 8
LS-Req received 2 sent 2, LS-Upd received 29 sent 53
LS-Ack received 46 sent 23, Discarded 1
```

字段解释：

字段	说明
FastEthernet 0/1 State	该网络接口的状态，UP 说明正常工作，Down 说明有故障。
Internet Address	接口 IP 地址。
Area	接口所属 OSPF 区域。
MTU	对应的 MTU
Matching network config	对应 OSPF 进程的 network area 配置
Process ID	对应的进程号
Router ID	OSPF 路由设备标识。
Network Type	OSPF 网络类型。
Cost	OSPF 接口花费。
Transmit Delay is	OSPF 接口传输延时。
State	DR/BDR 状态标识。
Priority	该接口的优先级
Designated Router(ID)	该接口的 DR 的路由设备标识
DR's Interface address	该接口的 DR 的接口地址
Backup designated router(ID)	该接口的 BDR 的路由设备标识
BDR's Interface address	该接口的 BDR 的接口地址

Time intervals configured	接口对应的 Hello，Dead，Wait，Retransmit 时间
Hello due in	上次 HELLO 发送的时间
Neighbor count	邻居总数
Adjacent neighbor count	Full 的邻居数量
Crypt Sequence Number	本接口对应的 md5 认证的序号
Hello received send	收到与发出的 HELLO 报文统计。
DD received send	收到与发出的 DD 报文统计。
LS-Req received send	收到与发出的 LS 请求报文统计。
LS-Upd received send	收到与发出的 LS 更新报文统计。
LS-Ack received send	收到与发出的 LS 响应报文统计。
Discard	被丢弃的 OSPF 报文统计。
BFD enabled	表示启用 OSPF 与 BFD 联动

【提示信息】 -

【平台说明】 -

5.54 show ip ospf neighbor

显示 OSPF 的邻居表

show ip ospf [*process-id*] **neighbor** [**statistics** | { [*interface-type interface-number*] | [*neighbor-id*] | [**detail**] }]

【参数说明】

参数	描述
process-id	OSPF 进程号
detail	显示邻居详细的信息。
interface-type interface-number	显示指定接口的邻居信息。
neighbor-id	显示指定邻居信息。
statistics	显示邻居的统计信息。

【命令模式】 特权模式

【缺省级别】 14

【使用指导】 该命令可以显示邻居的信息，经常用该命令来确认 OSPF 是否已经正常运行。

【配置举例】 1：显示 OSPF 的邻居表。

```
Ruijie# show ip ospf neighbor
OSPF process 1, 1 Neighbors, 1 is Full:
Neighbor ID   Pri   State     BFD State   Dead Time   Address        Interface
```

```
3.3.3.3         1       Full/BDR  Up          00:00:32    192.88.88.72    FastEthernet 0/1
```

```
Ruijie# show ip ospf neighbor detail
Neighbor 3.3.3.3, interface address 192.88.88.72
In the area 0.0.0.0 via interface FastEthernet 0/1
Neighbor priority is 1, State is Full, 11 state changes
DR is 192.88.88.27, BDR is 192.88.88.72
Options is 0x52 (*|O|-|EA|-|-|E|-)
Dead timer due in 00:00:32
Neighbor is up for 05:11:27
Database Summary List 0
Link State Request List 0
Link State Retransmission List 0
Crypt Sequence Number is 0
Thread Inactivity Timer on
Thread Database Description Retransmission off
Thread Link State Request Retransmission off
Thread Link State Update Retransmission off
Thread Poll Timer on
Graceful-restart helper disabled
BFD session state up
```

字段解释：

字段	说明
Neighbor ID	邻居路由设备标识。
Pri	邻居优先级（选举 DR 用）
State	邻居状态
Dead Time	邻居到 Dead 状态还剩余时间
Address	该邻居对应接口地址
Interface	该邻居对应接口
interface address	邻居路由设备的接口地址
In the area	显示学习到该邻居的区域
via interface	显示学到该邻居的接口。
Neighbor priority	邻居 OSPF 优先权值。
State	OSPF 邻居连接状态。FULL 说明处于稳定状态；DR 说明该邻居为指定路由设备；BDR 说明该邻居为备份指定路由设备；DROTHER 说明该邻居不是 DR/BDR。点到点网络类型没有 DR 或 BDR。
State changes times	邻居状态变化的次数
Dead Time	显示宣布该邻居无效时间：
DR	邻居路由设备选举的 DR 的接口地址(即 Hello 报文的

	DR 字段)
BDR	邻居路由设备选举的 BDR 的接口地址(即 Hello 报文的 BDR 字段)
Options	Hello 报文 E 比特选项内容，0 说明该区域为 Stub；2 说明该区域不是 Stub 区域。
Dead timer due in	邻居路由设备离死亡的时间。
Neighbor up time	发现邻居路由设备到现在所经过的时间
Database Summary List	邻居 DD 报文统计
Link State Request List	邻居 LS 请求报文统计
Link State Retransmission List	邻居重传报文统计
Crypt Sequence Number	区域 MD5 认证码
Thread Inactivity Timer	邻居无效定时器状态
Thread Database Description Retransmission	此接口 DD 报文定时器状态
Thread Link State Request Retransmission	此接口 LS 请求报文定时器状态
Thread Link State Update Retransmission	此接口 LS 更新报文定时器状态
Thread Poll Timer	静态配置的邻居，Poll Timer 启动状态
Graceful-restart helper	是否能够成为指定邻居的 GR Helper

【提示信息】 -

【平台说明】 -

5.55 show ip ospf route

显示 OSPF 路由。

show ip ospf [*process-id*] **route** [**count |** *ip-address mask*]

【参数说明】

参数	描述
process-id	OSPF 进程号
count	显示各种 OSPF 路由的统计信息
ip-address mask	显示指定前缀和掩码的路由信息

【命令模式】 特权模式

【缺省级别】 14

【使用指导】 该命令用于显示 OSPF 路由信息，count 选项用于显示 OSPF 路由的统计信息。

【配置举例】 1：显示 OSPF 路由。

```
Ruijie# show ip ospf route
```

```
OSPF process 1:
Codes: C - connected, D - Discard, B – Backup, 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
E2 100.0.0.0/24 [1/20] via 192.88.88.126, FastEthernet 0/1
B                      via 192.88.89.126, FastEthernet 0/2
C  192.88.88.0/24 [1] is directly connected,FastEthernet 0/1,Area 0.0.0.1
```

字段解释：

字段	说明
codes	路由类型以及对应的缩写描述
100.0.0.0/24	路由对应的前缀。
[1]	路由对应的 cost
via	路由下一跳与接口

【提示信息】 -

【平台说明】 -

5.56 show ip ospf spf

显示 OSPF 区域的路由计算次数

show ip ospf [*process-id*] **spf**

【参数说明】

参数	描述
process-id	OSPF 进程号

【命令模式】 特权模式

【缺省级别】 14

【使用指导】 该命令用来查看 OSFP 区域近 30 分钟内路由计算的次数以及至当前时间路由计算的总次数。

【配置举例】 1：显示 OSPF 区域的路由计算次数。

```
Ruijie# show ip ospf 1 spf

OSPF process 1:
Area_id      30min_counts   Total_counts
0            32             1235
1            6              356
```

字段解释：

字段	说明
Area_id	OSPF 区域 ID
30min_counts	最近 30 分钟时间内，OSPF 路由计算的次数
Total_counts	至当前时间，OSPF 路由计算的总次数

【提示信息】 -

【平台说明】 -

5.57 show ip ospf summary-address

显示 OSPF 所有重分布路由的汇聚路由

show ip ospf [*process-id*] **summary-address**

【参数说明】

参数	描述
process-id	OSPF 进程号

【命令模式】 特权模式

【缺省级别】 14

【使用指导】 目前该命令只能在 NSSA 的 ABR 上执行才有效，而且只显示在本地做汇聚操作的路由。

【配置举例】 1：显示 OSPF 所有重分布路由的汇聚路由。

```
Ruijie# show ip ospf summary-address
OSPF Process 1, Summary-address:
172.16.0.0/16, Metric 20, Type 2, Tag 0, Match count 3, advertise
```

字段解释：

字段	说明
Summary Address	汇聚的地址
Summary Mask	汇聚的范围。
Advertise	是否公告该汇聚的路由
Status	该汇聚范围是否生效
Aggregated subnets	有多少外部路由被汇聚在该范围里面

【提示信息】 -

【平台说明】 -

5.58 show ip ospf virtual-links

显示 OSPF 虚拟链路的信息

show ip ospf [*process-id*] **virtual-links** [*ip-address*]

【参数说明】

参数	描述
process-id	OSPF 进程号
ip-address	虚拟链路邻居关联 ID

【命令模式】 特权模式

【缺省级别】 14

【使用指导】 如果有配置虚拟链路，只能通过该命令显示邻居的状态，以及其它相关信息。**show ip ospf neighbor** 命令不会显示虚拟链路的邻居。

【配置举例】 1：显示 OSPF 虚拟链路的信息。

```
Ruijie# show ip ospf virtual-links
Virtual Link VLINK0 to router 1.1.1.1 is up
Transit area 0.0.0.1 via interface FastEthernet 0/1
Local address 10.0.0.37/32
Remote address 10.0.0.27/32
Transmit Delay is 1 sec, State Point-To-Point,
Timer intervals configured,Hello 10,Dead 40,Wait 40,Retransmit 5
Hello due in 00:00:05
Adjacency state Full
```

字段解释：

字段	说明
Virtual Link VLINK0 to router	显示虚拟链路的邻居以及状态
Virtual Link state	该虚拟链路的状态.
Transit area	显示虚拟链路的传输区域。
via interface	显示虚拟链路的关联接口。
Local address	本端接口地址
Remote Address	对端接口地址
Transmit Delay	显示虚拟链路的传输延时。
State	接口状态
Time intervals configured	接口对应的 Hello，Dead，Wait，Retransmit 时间
Adjacency State	毗邻状态。FULL 为稳定状态。

【提示信息】 -

【平台说明】 -

5.59 summary-address

配置 OSPF 路由域外部路由的汇聚路由。
summary-address *ip-address net-mask* [**not-advertise** | **tag** *value* | **cost** *cost*]

删除聚合路由的定义。
no summary-address *ip-address net-mask* [**not-advertise** | **tag** | **cost**]

【参数说明】

参数	描述
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
cost *cost*	设置汇聚路由的 cost 值，取值范围：0-16777214

【缺省配置】 缺省没有配置汇聚路由。

【命令模式】 路由进程配置模式。

【缺省级别】 14

【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。

【配置举例】 1：产生一条外部汇聚路由 100.100.0.0/16。

```
Ruijie(config)# router ospf 20
Ruijie(config-router)# summary-address 100.100.0.0 255.255.0.0
Ruijie(config-router)# redistribute static subnets
Ruijie(config-router)# network 200.2.2.0 0.0.0.255 area 1
Ruijie(config-router)# network 172.16.24.0 0.0.0.255 area 0
Ruijie(config-router)# area 1 nssa
```

【检验方法】 1：使用 show ip ospf summary-address 命令可以查看所配置的聚合路由。

【提示信息】 1：配置了错误的掩码。

```
OSPF: Invalid mask input
```

【常见错误】 -

【平台说明】 -

5.60 timers lsa arrival

配置 LSA 重复接收延时。

timers lsa arrival *arrival-time*

恢复缺省配置。

no timers lsa arrival

【参数说明】

参数	描述
arrival-time	配置接收相同 LSA 时延时。取值范围：0-600000，单位：毫秒

【缺省配置】 缺省为 1000 毫秒

【命令模式】 路由进程配置模式

【缺省级别】 14

【使用指导】 配置指定时间之内接收到相同 LSA 时，不做处理。

【配置举例】 1：以下的配置例子，配置相同 LSA 延时时间最少为 2s

```
Ruijie(config)# router ospf 1
Ruijie(config-router)# timers lsa arrival 2000
```

【检验方法】 1：使用 show ip ospf 命令可以查看所配置的 LSA 重复接收延时。

【提示信息】 -

【常见错误】 -

【平台说明】 -

5.61 timers pacing lsa-group

设置 LSA 被分组然后对整组进行刷新以及老化的的时间链路状态更新时间。
timers pacing lsa-group *seconds*

恢复缺省配置。
no timers pacing lsa-group

【参数说明】

参数	描述
seconds	LSA 组步调更新的步调时间，取值范围: 10-1800，单位：秒。

【缺省配置】 30 秒

【命令模式】 路由进程配置模式

【缺省级别】 14

【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

【配置举例】 1：将步调时间设置为 120 秒。

```
Ruijie(config)#router ospf 20
Ruijie(config-router)#timers pacing lsa-group 120
```

【检验方法】 1：使用 show ip ospf 命令可以查看所配置的 LSA 组步调更新的步调时间。

【提示信息】 -

【常见错误】 -

【平台说明】 -

5.62 timers pacing lsa-transmit

配置 LSA 发送分组更新。

timers pacing lsa-transmit *transmit-time transmit-count*

恢复缺省配置。
no timers pacing lsa-transmit

【参数说明】

参数	描述
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

【缺省配置】 **transimit-time** ：40 毫秒；
transimit-count ：1 个。

【命令模式】 路由进程配置模式。

【缺省级别】 14

【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。

【配置举例】 1：配置接口下每 50ms 发送一次 LS-UPD 报文，每次允许发送 20 个报文。

```
Ruijie(config)# router ospf 1
Ruijie(config-router)# timers pacing lsa-transmit 50 20
```

【检验方法】 1：使用 show ip ospf 命令可以查看所配置的发送分组更新间隔。

【提示信息】 -

【常见错误】 -

【平台说明】 -

5.63 timers spf

配置 OSPF 在接收到拓扑的变化信息，进行 SPF 计算的延时时间，以及两次 SPF 计算的时间间隔。
timers spf *spf-delay spf-holdtime*

恢复缺省配置。
no timers spf

【参数说明】

参数	描述

spf-delay	定义 SPF 计算的等待时间，以秒为单位，范围 0-2147483647(秒)。OSPF 路由进程接收到拓扑变化，必须等指定的时间后，才进行 SPF 运算。
spf-holdtime	定义两次 SPF 运算之间的时间间隔，以秒为单位，范围 0-2147483647(秒)。等待时间到了，两次运算间隔时间没到，还是不能进行 SPF 运算。

【缺省配置】 在 RGOS 10.4 版本之前，不支持 **timers throttle spf** 命令。系统缺省值为 **timers spf** 5 10。
RGOS 10.4 版本开始，支持 **timers throttle spf** 命令。此时缺省情况下 **timers spf** 命令不生效，SPF 计算延时是以 **timers throttle spf** 命令的缺省配置为准，参见 **timers throttle spf** 命令说明。

【命令模式】 路由进程配置模式。

【缺省级别】 14

【使用指导】 *spf-delay* 和 *spf-holdtime* 时间设置得越小，OSPF 适应拓扑变化的时间也越短，也就是说网络收敛时间越短，但是会占用路由设备更多的 CPU 时间。
timers spf 配置与 **timers throttle spf** 配置会互相覆盖。

【配置举例】 1：将 OSPF 的延时和保持时间分别设为 3 和 9 秒。

```
Ruijie(config)# router ospf 20
Ruijie(config-router)# timers spf 3 9
```

【检验方法】 1：使用 show ip ospf 命令可以查看所配置的 SPF 计算延迟。

【提示信息】 -

【常见错误】 -

【平台说明】 -

5.64 timers throttle lsa all

配置 LSA 生成指数退避算法。
timers throttle lsa all *delay-time hold-time max-wait-time*

恢复默认配置。
no timers throttle lsa all

【参数说明】

参数	描述
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

【缺省配置】 缺省情况下：
delay-time ：0 毫秒；
hold-time ：5000 毫秒；
max-wait-time ：5000 毫秒。

【命令模式】 路由进程配置模式。

【缺省级别】 14

【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。

【配置举例】 1：配置首次延迟时间为 10ms，hold-time 为 1s，最长延迟时间为 5s。

```
Ruijie(config)# router ospf 1
Ruijie(config-router)# timers throttle lsa all 10 1000 5000
```

【检验方法】 1：使用 show ip ospf 命令可以查看所配置的 LSA 生成延迟。

【提示信息】 1：当配置 max-wait-time 比 hold-time 小的时候。

```
% Warning: max-wait-time should be no less than hold-time, set to (5).
```

2：当配置 hold-time 比 delay-time 小的时候。

```
% Warning: hold-time should be no less than delay-time, set to (5).
```

【常见错误】 1：配置的 hold-time 比 delay-time 小或着 max-wait-time 比 hold-time 小。

【平台说明】 -

5.65 timers throttle route

配置 OSPF 在接收到变化的区间、外部 LSA 时，进行路由计算的延时时间。
timers throttle route { **inter-area** *ia-delay* | **ase** *ase-delay* }

恢复默认配置。
no timers throttle route { **inter-area** | **ase** }

【参数说明】

参数	描述

inter-area	区间路由计算。
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。OSPF 接收到区间 LSA 变化，触发的路由计算至少要在 ia-delay 时间间隔后执行。
ase	外部路由计算。
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。OSPF 接收到外部 LSA 变化，触发的路由计算至少要在 ase-delay 时间间隔后执行。

【缺省配置】 缺省情况下：
ia-delay：0 毫秒；
ase-delay：0 毫秒。

【命令模式】 路由进程配置模式。

【缺省级别】 14

【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】 1：将 OSPF 的区间路由计算延迟 1 秒，配置如下。

```
Ruijie(config)# router ospf 1
Ruijie(config-router)# timers throttle route inter-area 1000
```

【检验方法】 1：使用 show running-config 查看配置。

【提示信息】 -

【常见错误】 -

【平台说明】 -

5.66 timers throttle spf

配置 OSPF 在接收到拓扑的变化信息，进行 SPF 计算的延时时间、两次 SPF 计算的最小时间间隔、最大时间间隔。
timers throttle spf *spf-delay spf-holdtime spf-max-waittime*

恢复缺省配置。
no timers throttle spf

【参数说明】

参数	描述

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。

【缺省配置】 *spf-delay*：1000 毫秒；
spf-holdtime：5000 毫秒；
spf-max-waittime：10000 毫秒。

【命令模式】 路由进程配置模式。

【缺省级别】 14

【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】 1：将 OSPF 的 SPF 计算时延、最小时间间隔、最大时间间隔分别设为 5 毫秒、1000 毫秒、90000 毫秒。若拓扑连续变化，则 SPF 计算时间分别为：
5ms，1s，3s，7s，15s，31s，63s，89s，179s，179+90 .....

```
Ruijie(config)# router ospf 20
Ruijie(config-router)# timers spf 5 1000 90000
```

【检验方法】 1：使用 show ip ospf 命令可以查看所配置的 SPF 计算延迟。

【提示信息】 1：当配置 max-wait-time 比 hold-time 小的时候。

```
% Warning: max-wait-time should be no less than hold-time, set to (5).
```

2：当配置 hold-time 比 delay-time 小的时候。

```
% Warning: hold-time should be no less than delay-time, set to (5).
```

【常见错误】 1：配置的 hold-time 比 delay-time 小或着 max-wait-time 比 hold-time 小。

【平台说明】 -

5.67 two-way-maintain

启用 OSPF 双向维持功能
two-way-maintain

禁用 OSPF 双向维持功能。
no two-way-maintain

【参数说明】

参数	描述
-	-

【缺省配置】 缺省启用 OSPF 双向维持功能。

【命令模式】 路由进程配置模式。

【缺省级别】 14

【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】 1：禁用 OSPF 双向维持功能。

```
Ruijie(config)# router ospf 1
Ruijie(config-router)# no two-way-maintain
```

【检验方法】 1：使用 show ip ospf 命令可以查看所配置的双向维持是否启用。

【提示信息】 -

【常见错误】 -

【平台说明】 -

6 OSPFv3

6.1 area authentication

启用 OSPFv3 区域认证.

area *area-id* **authentication ipsec spi** *spi* [**md5 | sha1**] [**0 | 7**] *key*

关闭 OSPFv3 区域认证。

no area *area-id* **authentication**

【参数说明】

参数	描述
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

【缺省配置】 缺省没有采用认证。

【命令模式】 路由进程配置模式

【缺省级别】 14

【使用指导】 RGOS 软件可以支持三种认证类型：

- 不要求认证，没有配置的时候；
- 为 MD5 认证模式；
- 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。

【配置举例】 1：OSPFv3 路由进程的区域 1 采用 MD5 认证，认证口令为 aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa。

```
Ruijie(config-router)# area 1 authentication ipsec spi 300 md5 aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
```

【检验方法】 -

【提示信息】 1：本模块其它地方已经使用了该 spi。

```
% OSPFv3: SPI is already in use.
```

2：其它模块已经使用了该 spi。

```
% OSPFv3: SPI is already in use by others.
```

3：当前区域已经配置了该 spi。

```
% OSPFv3: Area is already configured with the same SPI.
```

4：区域已经配置了加密不能在配置认证。

```
% OSPFv3: Area is already configured with encryption so cannot configure authentication.
```

【常见错误】 -

【平台说明】 -

6.2 area default-cost

在 Stub 或者 NSSA 区域的 ABR 上设置该命令，用来定义 Stub 或者 NSSA 区域内缺省路由的代价。

area *area-id* **default-cost** *cost*

恢复缺省值。

no area *area-id* **default-cost**

【参数说明】

参数	描述
area-id	Stub 或者 NSSA 区域的区域号。 其可以指定为一个整数或者一个 IPv4 前缀。
cost	Stub 或者 NSSA 区域内缺省路由的代价。 范围 0-16777215。

【缺省配置】 缺省 **default-cost** 的值为 1。

【命令模式】 路由进程配置模式

【缺省级别】 14

【使用指导】

【配置举例】 1：将 stub 区域 50 缺省路由的代价设置为 100：

```
Ruijie(config)# ipv6 router ospf 1
Ruijie(config-router)# area 50 stub
Ruijie(config-router)# area 50 default-cost 100
```

【检验方法】 -

【提示信息】 1：在骨干区域中配置该命令，提示错误。

```
% You can't configure default-cost to backbone
```

2：在非 Stub 或者 NSSA 区域中配置该命令，提示错误。

```
% The area is neither stub, nor NSSA
```

【常见错误】 1：在骨干区域中配置该命令，提示错误。

2：在非 Stub 或者 NSSA 区域中配置该命令，提示错误。

【平台说明】 -

6.3 area encryption

启用 OSPFv3 区域加密认证。

area *area-id* **encryption ipsec spi** *spi* **esp [null | [des** | **3des | aes-cbc [128 | 192 | 256]**] [**0 | 7**] *des-key* **]** [**md5 | sha1**] [**0 | 7**] *key*

关闭 OSPFv3 区域加密认证。

no area *area-id* **encryption**

【参数说明】

参数	描述
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	采用 null 加密模式。
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。
aes-cbc[128 | 192 | 256]	采用 AES-CBC(Advanced Encryption Standard-Cipher Block Chaining，高级加密标准-密码块链接)加密模式，指定加密密钥长度为 128,192,256 比特。
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

【缺省配置】 缺省没有采用加密认证。

【命令模式】 路由进程配置模式

【缺省级别】 14

【使用指导】 RGOS 软件可以支持：

- 三种加密类型：DES 加密模式；3DES 加密模式；AES-CBC 加密模式。
- 二种认证类型：MD5 认证模式；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。

【配置举例】 1：OSPFv3 路由进程的区域 1 采用 null 加密和 MD5 认证，认证口令为 aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa。

```
Ruijie(config-router)# area 1 encryption ipsec spi 300 esp null md5 aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
```

【检验方法】 -

【提示信息】 1：本模块其它地方已经使用了该 spi。

```
% OSPFv3: SPI is already in use.
```

2：其它模块已经使用了该 spi 。

```
% OSPFv3: SPI is already in use by others.
```

3：当前区域已经配置了该 spi。

```
% OSPFv3: Area is already configured with the same SPI.
```

4：区域已经配置了认证不能在配置加密。

```
% OSPFv3: Area is already configured with authentication so cannot configure encryption.
```

【常见错误】 -

【平台说明】 -

6.4 area range

设置区间汇聚地址范围。

area *area-id* **range** *ipv6-prefix*/*prefix-length* [**advertise | not-advertise**]

删除已配置的汇聚范围或者恢复汇聚范围的缺省参数。

no area *area-id* **range** *ipv6-prefix*/*prefix-length*

【参数说明】

参数	描述
area-id	将要进行路由汇聚的区域号。 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	公告该汇聚范围。
not-advertise	不公告该汇聚范围。 缺省为公告。

【缺省配置】 未定义区间汇聚地址范围

【命令模式】 路由进程配置模式

【缺省级别】 14

【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。

【配置举例】 1：对区域 1 的路由进行汇聚：

```
Ruijie(config)# ipv6 router ospf 1
Ruijie(config-router)# area 1 range 2001:DB8:1:2::/64
```

【检验方法】 -

【提示信息】 1：删除的汇聚条目不存在。

```
% Can't find specified area range.
```

【常见错误】 -

【平台说明】 -

6.5 area stub

创建一个 stub 区域或者设置 stub 区域的属性。
area *area-id* **stub** [**no-summary**]

恢复为普通区域或者删除 stub 区域的配置。
no area *area-id* **stub** [**no-summary**]

【参数说明】

参数	描述
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。

【缺省配置】 未定义 stub 区域

【命令模式】 路由进程配置模式

【缺省级别】 14

【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。

【配置举例】 1：stub 区域 10 的 ABR 上只将缺省路由公告到 stub 区域中：

```
Ruijie(config)# ipv6 router ospf 1
Ruijie(config-router)# area 10 stub
Ruijie(config-router)# area 10 stub no-summary
```

【检验方法】 使用 show ipv6 ospf 命令可以看到所配置的区域拥有 stub 属性

【提示信息】 1：在骨干区配置该命令时提示错误。

```
% You can't configure stub to backbone
```

2：Stub 区域配置虚链路则提示先要删除虚链路改配置才能生效。

```
% First deconfigure all virtual link through this area
```

【常见错误】 1：在骨干区配置该命令时提示错误。
2：Stub 区域配置虚链路则提示先要删除虚链路改配置才能生效。

【平台说明】 -

6.6 area virtual-link

创建一个虚拟连接或者设置虚拟连接的参数。
area *area-id* **virtual-link** *router-id* [**hello-interval** *seconds*] [**dead-interval** *seconds*] [**retransmit-interval** *seconds*] [**transmit-delay** *seconds*] [**instance** *instance-id*] [**authentication ipsec spi** *spi* [**md5 | sha1**] [**0 | 7**] *key*] [**encryption ipsec spi** *spi* **esp null** [**md5 | sha1**] [**0 | 7**] *key*]

删除一个虚拟连接或者恢复虚拟连接的缺省参数。
no area *area-id* **virtual-link** *router-id* [**hello-interval**] [**dead-interval**] [**retransmit-interval**] [**transmit-delay**] [**instance**] [**authentication**] [**encryption**]

【参数说明】

参数	描述
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)。
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。
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。
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。 范围 1-65535 秒。
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
authentication ipsec spi *spi* [**md5 | sha1**] [**0 | 7**] *key*	定义 OSPFv3 认证。 邻居之间的认证必须一致。**service password-encryption** 命令可以使配置的密钥以加密的方式显示。 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
encryption ipsec spi *spi* **esp [null |** [**des** | **3des | aes-cbc [128 | 192 | 256]**] [**0 | 7**] *des-key* **]** [**md5 | sha1**] [**0 | 7**] *key*	定义 OSPFv3 加密认证。 邻居之间的加密认证必须一致。service password-encryption 命令可以使配置的密钥以加密的方式显示。 **spi** 安全参数索引， 范围是 256-4294967295 null 不采用加密 des 指定 des 加密模式 3des 指定 3des 加密模式 aes-cbc 128 指定 128 比特长度的 aes-cbc 加密模式 aes-cbc 192 指定 192 比特长度的 aes-cbc 加密模式 aes-cbc 256 指定 256 比特长度的 aes-cbc 加密模式 des-key 加密密钥 **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

【缺省配置】 未定义虚拟连接。
hello-interval 缺省为 10 秒。
dead-interval 缺省为 hello-interval 的四倍。
retransmit-interval 缺省为 5 秒。
transmit-delay 缺省为 1 秒。
authentication 缺省不认证。
encryption 缺省不加密。

【命令模式】 路由进程配置模式。

【缺省级别】 14

【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】 1：配置一个虚拟连接：

```
Ruijie(config)# ipv6 router ospf 1
Ruijie(config-router)# area 1 virtual-link 192.1.1.1
```

【检验方法】 1：使用 show ipv6 ospf virtual-links 命令可以查看所配置的虚链路信息。

【提示信息】 1：在骨干区域配置虚链路时，提示错误。

```
% You can't configure virtual-link transit to backbone
```

2：在 Stub 或 NSSA 区域中配置虚链路时，提示错误。

```
% Area is a stub or NSSA so virtual links are not allowed
```

【常见错误】 1：在骨干区域配置虚链路时，提示错误。
2：在 Stub 或 NSSA 区域中配置虚链路时，提示错误。

【平台说明】 -

6.7 auto-cost

启动根据带宽进行接口的度量计算或者修改带宽参考值。
auto-cost reference-bandwidth *ref-bw*

关闭根据带宽进行接口的度量计算或者恢复缺省带宽参考值。

no auto-cost reference-bandwidth

【参数说明】

参数	描述
reference-bandwidth *ref-bw*	带宽的参考值，以 Mbps 为单位。范围 1-4294967。

【缺省配置】 根据带宽参考值进行接口的度量计算，带宽参考值为 100Mbps

【命令模式】 路由进程配置模式

【缺省级别】 14

【使用指导】 使用 **no auto-cost reference-bandwidth** 将恢复缺省的带宽参考值。

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。

【配置举例】 1：修改带宽参考值为 10M：

```
Ruijie(config)# ipv6 router ospf 1
Ruijie(config-router)# auto-cost reference-bandwidth 10
```

【检验方法】 1：使用 show ipv6 ospf interface 命令可以查看所配置的参考代码是否生效。

【提示信息】 1：改变接口代价时提示。

```
% OSPFv3: Reference bandwidth is changed.
Please ensure reference bandwidth  is consistent across all routers
```

【常见错误】 -

【平台说明】 -

6.8 clear ipv6 ospf process

使用该命令清除并重启 OSPFv3 实例。

clear ipv6 ospf [*process-id*] **process**

【参数说明】

参数	描述
process-id	指定 OSPFv3 进程号，范围 1-65535

【命令模式】 特权模式

【缺省级别】 14

【使用指导】 正常情况下，无需使用本命令。
使用 *process-id* 参数指定只清除某个 OSPFv3 实例。如果没有指定 *process-id* 参数，则清除所有 OSPFv3 实例。

【配置举例】 1：重新启动所有 OSPFv3 实例

```
Ruijie# clear ipv6 ospf process
```

【提示信息】 1：指定错误的进程号。

```
% OSPFv3: No router process 1.
```

【平台说明】 -

6.9 default-information originate

产生一条缺省的路由注入 OSPFv3 路由域。
default-information originate [**always**] [**metric** *metric*] [**metric-type** *type*] [**route-map** *map*]

取消产生一条缺省的路由或者恢复产生缺省路由的默认参数。
no default-information originate [**always**] [**metric**] [**metric-type**] [**route-map** *map*]

【参数说明】

参数	描述
always	该关键字使得 OSPFv3 无条件产生缺省路由，不管本地是否存在缺省路由。
metric *metric*	缺省路由初始的度量值，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。OSPFv3 外部路由有两种类型：类型 1，不同路由设备上看到的度量值不一样；类型 2，所有路由设备看到的度量值都一样。类型 1 的外部路由比类型 2 可信。
route-map *map*	关联的 route-map 的名字，缺省没有关联 route-map。

【缺省配置】 缺省不产生缺省路由；
初始度量值缺省为 1；
路由类型缺省为类型 2。

【命令模式】 路由进程配置模式。

【缺省级别】 14

【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** 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** 只显示类型 1 那条路由。
该命令产生的是 5 类 LSA 的缺省路由，不会洪泛到 NSSA 区域。若希望在 NSSA 区域产生一条缺省路由，请使用 **area nssa default-information-originate** 命令。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】 1：配置重分产生缺省路由：

```
Ruijie(config)# ipv6 router ospf 1
Ruijie(config-router)# default-information originate always
```

【检验方法】 1：执行 **show ipv6 ospf database** 命令可以查看生成默认路由对应的数据库。

【提示信息】 -

【常见错误】 -

【平台说明】 -

6.10 default-metric

设置重分发路由的缺省度量值。
default-metric *metric-value*

恢复缺省值。
no default-metric

【参数说明】

参数	描述
metric-value	重分发路由的缺省度量值。 范围 1-16777214，缺省值 20

【缺省配置】 参数缺省值为 20

【命令模式】 路由进程配置模式

【缺省级别】 14

【使用指导】 该命令同 **redistribute** 命令一起使用，用来设置重分发路由的缺省度量值。但该命令对两类路由无效：
default-information originate 命令生成的缺省路由；
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。

【配置举例】 1：配置重分发路由的缺省 metric 为 10：

```
Ruijie(config)# ipv6 router ospf 1
Ruijie(config-router)# default-metric 10
```

【检验方法】 -

【提示信息】 -

【常见错误】 -

【平台说明】 -

6.11 distance

设置不同类型 OSPFv3 路由对应的管理距离。
distance { *distance* | **ospf** { [**intra-area** *distance*] [**inter-area** *distance*] [**external** *distance*] } }

恢复缺省值。
no distance [**ospf**]

【参数说明】

参数	描述
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。

【缺省配置】 缺省为 110；
区内路由管理距离：缺省为 110。
区间路由管理距离：缺省为 110。
外部路由管理距离：缺省为 110。

【命令模式】 路由进程配置模式

【缺省级别】 14

【使用指导】 若要指定 OSPFv3 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】 1：配置 OSPFv3 外部路由管理距离为 160

```
Ruijie(config)# ipv6 router ospf 1
Ruijie(config-router)# distance ospf external 160
```

【检验方法】 -

【提示信息】 -

【常见错误】 -

【平台说明】 -

6.12 distribute-list in

配置对收到的 LSA 计算出的路由进行过滤。
distribute-list { *name* | **prefix-list** *prefix-list-name* } **in** [*interface-type interface-number*]

取消过滤。
no distribute-list { *name* | **prefix-list** *prefix-list-name* } **in** [*interface-type interface-number*]

【参数说明】

参数	描述
name	使用 ACL 过滤规则
prefix-list *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

【缺省配置】 未配置对学习的路由过滤

【命令模式】 路由进程配置模式

【缺省级别】 14

【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】 1：配置只将 2001::/64 加入核心路由表中。

```
Ruijie(config)# ipv6 prefix-list aaa seq 10 permit 2001::/64
Ruijie(config)# ipv6 router ospf 25
Ruijie(config-router)# redistribute rip metric 100
Ruijie(config-router)# distribute-list prefix-list aaa in ethernet 0/1
```

【检验方法】

【提示信息】 1：配置了无效的接口。

```
% Interface is invalid.
```

2：配置了无效的 ACL 名字。

```
% ACL name abc-acl is invalid
```

3：不允许过滤由本实例导入的路由。

```
% Distribute-list of "ospf 1" via "ospf 1" not allowed
```

【常见错误】 -

【平台说明】 -

6.13 distribute-list out

配置过滤重分布路由，功能类似 **redistribute** 命令。

distribute-list { *name* | **prefix-list** *prefix-list-name* } **out** [**bgp** | **connected** | **isis** [*area-tag*] | **ospf** *process-id* | **rip** | **static**]

取消过滤。

no distribute-list { *name* | **prefix-list** *prefix-list-name* } **out** [**bgp** | **connected** | **isis** [*area-tag*] | **ospf** *process-id* | **rip** | **static**]

【参数说明】

参数	描述
name	使用 ACL 过滤规则
prefix-list *prefix-list-name*	使用 prefix-list 过滤规则
bgp	过滤 BGP 路由
connected	过滤直连路由
isis [*area-tag*]	过滤 ISIS 路由
ospf *process-id*	过滤 OSPF 路由
rip	过滤 RIP 路由

static	过滤静态路由

【缺省配置】 未配置 ospf 外部路由过滤。

【命令模式】 路由进程配置模式

【缺省级别】 14

【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。

【配置举例】 1：对重分布的静态路由进行过滤

```
Ruijie(config)# ipv6 router ospf 1
Ruijie(config-router)# redistribute static
Ruijie(config-router)# distribute-list prefix-list jjj out static
```

【检验方法】 -

【提示信息】 -

【常见错误】 -

【平台说明】 -

6.14 enable mib-binding

将 MIB 绑定到指定的 OSPFv3 进程上。

enable mib-binding

恢复缺省绑定。

no enable mib-binding

【参数说明】

参数	描述
-	-

【缺省配置】 MIB 绑定在进程号最小的 OSPFv3 进程上。

【命令模式】 路由进程配置模式。

【缺省级别】 14

【使用指导】 由于 OSPFv3 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。

【配置举例】 1：通过 SNMP 操作进程号为 100 的 OSPFv3 进程：

```
Ruijie(config)# ipv6 router ospf 100
Ruijie(config-router)# enable mib-binding
```

【检验方法】 -

【提示信息】 -

【常见错误】 -

【平台说明】 -

6.15 enable traps

配置启动指定 TRAP 信息的发送。

enable traps [**error** [**IfConfigError | IfRxBadPacket | VirtIfConfigError | VirtIfRxBadPacket**] | **state-change** [**IfStateChange | NbrStateChange | NssaTranslatorStatusChange | VirtIfStateChange | VirtNbrStateChange | RestartStatusChange | NbrRestartHelperStatusChange | VirtNbrRestartHelperStatusChange**]]

关闭指定 TRAP 信息的发送。

no enable traps [**error** [**IfConfigError | IfRxBadPacket | VirtIfConfigError | VirtIfRxBadPacket**] | **state-change** [**IfStateChange | NbrStateChange | NssaTranslatorStatusChange | VirtIfStateChange | VirtNbrStateChange | RestartStatusChange | NbrRestartHelperStatusChange | VirtNbrRestartHelperStatusChange**]]

【参数说明】

参数	描述
error	配置所有与 error 有关的 traps 开关，该参数还可以配置如下特定的 error traps 开关： **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
state-change	配置所有与 state-change 有关的 traps 开关，该参数还可以配置如下特定的 state-change traps 开关： **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

【缺省配置】 缺省是关闭全部 traps 开关。

【命令模式】 路由进程配置模式。

【缺省级别】 14

【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 ospfv3 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。

【配置举例】 1：打开 OSPFv3 进程 100 的全部 TRAP 开关：

```
Ruijie(config)#ipv6 router ospf 100
Ruijie(config-router)# enable traps
```

【检验方法】 -

【提示信息】 -

【常见错误】 -

【平台说明】 -

6.16 graceful-restart

启动 OSPFv3 Restarter 能力，设置重启周期。
graceful-restart [**grace-period** *grace-period* | **inconsistent-lsa-checking**]

关闭 OSPFv3 GR 功能或恢复重启周期的缺省值。
no graceful-restart [*grace-period*]

【参数说明】

参数	描述
grace-period *grace-period*	配置 GR 重启周期，重启周期为从 OSPFv3 失效到 OSPFv3 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，缺省开启检测。

【缺省配置】 缺省开启 GR 功能。

【命令模式】 路由进程配置模式

【缺省级别】 14

【使用指导】 优雅重启功能基于 OSPFv3 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 OSPFv3 恢复到原有状态。当重启周期到期后，OSPFv3 将退出 GR 状态，执行普通的 OSPFv3 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，OSPFv3 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。

３）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;

４）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。

【配置举例】 1：使能 OSPFv3 实例 1 的 GR 功能以及配置 GR 功能的重启周期参数：

```
Ruijie(config)# ipv6 router ospf 1

Ruijie(config-router)# graceful-restart

Ruijie(config-router)# graceful-restart grace-period 60
```

【检验方法】 1：使用 show ipv6 ospf 命令可以查看所配置的 GR 功能和运行状态。

【提示信息】 -

【常见错误】 -

【平台说明】 -

6.17 graceful-restart helper

启动 OSPFv3 GR helper 功能，设置相关机制。
graceful-restart helper disable

禁用 OSPFv3 GR helper 功能。
no graceful-restart helper disable

配置 OSPFv3 GR helper 的拓扑变化检测方式。
graceful-restart helper { **strict-lsa-checking | internal-lsa-checking** }

取消配置 OSPFv3 GR helper 的拓扑变化检测方式。
no graceful-restart helper { **strict-lsa-checking | internal-lsa-checking** }

【参数说明】

参数	描述
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。

【缺省配置】 启动 GR Help 能力。
设备进入 GR Helper 后，缺省不检查 LSA 变化。

【命令模式】 路由进程配置模式

【缺省级别】 14

【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】 1：禁止 OSPFv3 实例 1 的 GR 辅助功能以及如何修改检测网络变化的策略：

```
Ruijie(config)# ipv6 router ospf 1
Ruijie(config-router)# graceful-restart helper disable
```

```
Ruijie(config-router)# no graceful-restart helper disable
Ruijie(config-router)# graceful-restart helper strict-lsa-checking
```

【检验方法】 1：使用 show ipv6 ospf 命令可以查看所配置的 GR Helper 功能和运行状态。

【提示信息】 -

【常见错误】 -

【平台说明】 -

6.18 ipv6 ospf area

设置接口参与 OSPFv3 路由进程。
ipv6 ospf *process-id* **area** *area-id* [**instance** *instance-id*]

取消配置。
no ipv6 ospf *process-id* **area** [**instance** *instance-id*]

【参数说明】

参数	描述
process-id	ospf 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。

【缺省配置】 接口未启动 OSPFv3 路由进程

【命令模式】 接口配置模式

【缺省级别】 14

【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 ospf area** 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。

【配置举例】 1：在接口 fastethernet 0/0 上启动 OSPFv3 进程，参与指定的实例的指定区域运行：

```
Ruijie(config)# int fastethernet 0/0
Ruijie(config-if)# ipv6 ospf 1 area 2 instance 2
```

【检验方法】 执行 show ipv6 ospf interface 可以查看相应接口所配置的 OSPFv3 进程

【提示信息】 -

【常见错误】 -

【平台说明】 -

6.19 ipv6 ospf authentication

配置 OSPFv3 接口认证。

ipv6 ospf authentication [**null | ipsec spi** *spi* [**md5 | sha1**] [**0 | 7**] *key*] [**instance** *instance-id*]

关闭 OSPFv3 接口认证。

no ipv6 ospf authentication [**instance** *instance-id*]

【参数说明】

参数	描述
null	不进行认证。
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。

【缺省配置】 缺省没有采用认证。

【命令模式】 接口配置模式

【缺省级别】 14

【使用指导】 RGOS 软件可以支持三种认证类型：

- 不要求认证，没有配置的时候；
- 为 MD5 认证模式；

- 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。

【配置举例】 1：OSPFv3 接口模式下采用 MD5 认证，认证口令为 aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa。

```
Ruijie(config-if)# ipv6 ospf authentication ipsec spi 300 md5 aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
```

【检验方法】 -

【提示信息】 1：本模块其它地方已经使用了该 spi 。

```
% OSPFv3: SPI is already in use.
```

2：其它模块已经使用了该 spi 。

```
% OSPFv3: SPI is already in use by others.
```

3：当前接口已经配置了该 spi。

```
% OSPFv3: Interface is already configured with the same SPI.
```

4：接口已经配置了加密不能在配置认证。

```
% OSPFv3: Interface is already configured with encryption so cannot configure authentication.
```

【常见错误】 -

【平台说明】 -

6.20 ipv6 ospf cost

设置接口的代价。

ipv6 ospf cost *cost* [**instance** *instance-id*]

恢复缺省值。

no ipv6 ospf cost [**instance** *instance-id*]

【参数说明】

参数	描述
cost	接口的代价。 范围 1-65535。
instance *instance-id*	对接口特定 OSPFv3 实体进行配置，范围 0-255。

【缺省配置】 缺省的接口花费为参考带宽/Bandwidth（参考带宽默认为 100Mbps）。

【命令模式】 接口配置模式。

【缺省级别】 14

【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 OSPFv3 缺省接口花费为：

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。

通过 **ipv6 ospf cost** 命令配置的 OSPFv3 花费，会覆盖缺省配置。

【配置举例】 1：配置接口的代价为 1：

```
Ruijie(config)# int fastethernet 0/0
Ruijie(config-if)# ipv6 ospf cost 1
```

【检验方法】 执行 show ipv6 ospf interface 可以查看相应接口所配置的 cost 值

【提示信息】 -

【常见错误】 -

【平台说明】 -

6.21 ipv6 ospf dead-interval

设置接口上的邻居死亡时间。

ipv6 ospf dead-interval { *seconds* | **minimal hello-multiplier** *multiplier* } [**instance** *instance-id*]

恢复缺省值。

no ipv6 ospf dead-interval [**instance** *instance-id*]

【参数说明】

参数	描述
seconds	邻居死亡时间。单位为秒，取值范围 1-65535。
minimal hello-multiplier *multiplier*	启用 Fast Hello 功能，邻居死亡时间为 1s。 *multiplier* 为每秒钟发送的 Hello 报文的次数。取值范围 3-20。
instance *instance-id*	对接口特定 OSPFv3 实体进行配置，范围 0-255。

【缺省配置】 未启用 Fast Hello 功能，邻居死亡时间为 hello 报文发送间隔的 4 倍。

如果修改了 hello 报文的发送间隔，将自动修改邻居死亡时间。

【命令模式】 接口配置模式

【缺省级别】 14

【使用指导】 邻居死亡时间必须大于邻居发送 hello 报文的时间间隔。

启用 OSPFv3 Fast Hello 功能将加速 OSPFv3 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 OSPFv3 Fast Hello 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。

当接口启动 Fast Hello 功能时，从该接口通告的 Hello 报文的 hello-interval 字段会被设置为 0，从该接口接收的 Hello 报文的 hello-interval 字段会被忽略。

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。

无论是否启用 Fast Hello 功能，邻居接口之间，邻居死亡时间必须保持一致。**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 ipv6 ospf interface** 命令监控接口配置的死亡间隔和 Fast Hello 间隔。

【配置举例】 1：设置接口上的邻居死亡时间为 60s：

```
Ruijie(config)# int fastethernet 0/0
Ruijie(config-if)# ipv6 ospf dead-interval 60
```

【检验方法】 1：执行 show ip ospf interface 命令可以查看相应端口下配置的邻居死亡时间间隔

【提示信息】 1：配置 dead 时间小于 hello 时间的时候提示。

```
% Warning: OSPFv3 dead interval should be higher than hello interval
```

1：如果已经配置了 hello 时间再配置 fasthello。

```
% OSPFv3: Hello interval configured with hello-interval.
```

【常见错误】 1：同一区域中不同端口间所配置的邻居死亡时间间隔不同

【平台说明】 -

6.22 ipv6 ospf encryption

启用 OSPFv3 接口加密认证。

ipv6 ospf encryption [**null | ipsec spi** *spi* **esp [null |** [**des** | **3des | aes-cbc [128 | 192 | 256]**] [**0 | 7**] *des-key* **]** [**md5 | sha1**] [**0 | 7**] *key*] [**instance** *instance-id*]

关闭 OSPFv3 接口加密认证。

no ipv6 ospf encryption [**instance** *instance-id*]

【参数说明】

参数	描述
null	不进行认证加密
spi	安全参数索引，范围 256-4294967295。

null	不加密。
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。
aes-cbc[128 | 192 | 256]	采用 AES-CBC(Advanced Encryption Standard-Cipher Block Chaining，高级加密标准-密码块链接)加密模式，指定加密密钥长度为 128,192,256 比特。
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

【缺省配置】 缺省没有采用加密认证。

【命令模式】 接口配置模式

【缺省级别】 14

【使用指导】

RGOS 软件可以支持：

- 三种加密类型：DES 加密模式；3DES 加密模式；AES-CBC 加密模式。
- 二种认证类型：MD5 认证模式；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】 1：OSPFv3 接口模式下采用 null 加密和 MD5 认证，认证口令为 aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa。

```
Ruijie(config-if)# ipv6 ospf encryption ipsec spi 300 esp null md5 aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
```

【检验方法】 1：执行 show ip ospf interface 命令可以查看相应端口下的配置。

【提示信息】 1：本模块其它地方已经使用了该 spi 。

```
% OSPFv3: SPI is already in use.
```

2：其它模块已经使用了该 spi 。

```
% OSPFv3: SPI is already in use by others.
```

3：当前接口已经配置了该 spi 。

```
% OSPFv3: Interface is already configured with the same SPI.
```

4：接口已经配置了认证不能在配置加密。

```
% OSPFv3: Interface is already configured with authentication so cannot configure encryption.
```

【常见错误】 -

【平台说明】 -

6.23 ipv6 ospf hello-interval

设置接口上发送 Hello 报文的时间间隔。

ipv6 ospf hello-interval *seconds* [**instance** *instance-id*]

恢复缺省值。

no ipv6 ospf hello-interval [**instance** *instance-id*]

【参数说明】

参数	描述
seconds	发送 Hello 报文时间间隔。 范围 1-65535(秒)。
instance *instance-id*	对接口特定 OSPFv3 实体进行配置 范围 0-255。

【缺省配置】 广播网络与点对点网络为 10 秒；点对多点网络与 NBMA 网络缺省为 30 秒。

【命令模式】 接口配置模式。

【缺省级别】 14

【使用指导】 邻居之间发送 Hello 报文的时间间隔值必须相同，否则将无法建立正常的邻接关系。

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】 1：设置本接口发送 hello 报文的时间间隔为 20s：

```
Ruijie(config)# int fastethernet 0/0
Ruijie(config-if)# ipv6 ospf hello-interval 20
```

【检验方法】 1：执行 show ipv6 ospf interface 命令可以查看相应端口下的配置。

【提示信息】 1：如果已经配置时候提示

```
% OSPFv3: Hello interval configured with hello-multiplier.
```

【常见错误】 -

【平台说明】 -

6.24 ipv6 ospf mtu-ignore

在接口收到数据库描述报文时可以忽略对 MTU 的校验。
ipv6 ospf mtu-ignore [**instance** *instance-id*]

恢复缺省配置。
no ipv6 ospf mtu-ignore [**instance** *instance-id*]

【参数说明】

参数	描述
instance *instance-id*	对接口特定 OSPFv3 实体进行配置 范围 0-255。

【缺省配置】 缺省对 MTU 进行校验。

【命令模式】 接口配置模式。

【缺省级别】 14

【使用指导】 OSPFv3 在收到数据库描述报文时会校验邻居接口的 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邻居接口的 MTU 大于自己接收接口的 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】 1：以下的配置例子，将 ethernet 1/0 的 MTU 校验功能关闭。

```
Ruijie(config)# interface ethernet 1/0
Ruijie(config-if)# ipv6 ospf mtu-ignore
```

【检验方法】 -

【提示信息】 -

【常见错误】 -

【平台说明】 -

6.25 ipv6 ospf neighbor

手工配置 OSPFv3 的邻居。
ipv6 ospf neighbor *ipv6-address* [**cost** *cost* | [**poll-interval** *seconds*] [**priority** *value*]] [**instance** *instance-id*]

恢复缺省值。

no ipv6 ospf neighbor *ipv6-address* [**cost** *cost* | [**poll-interval** *seconds*] [**priority** *value*]] [**instance** *instance-id*]

【参数说明】

参数	描述
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。

【缺省配置】 缺省没有定义邻居；
邻居轮询时间间隔：缺省 120 秒；
非广播网络邻居的优先权值：缺省为 0。

【命令模式】 接口配置模式。

【缺省级别】 14

【使用指导】 -

【配置举例】 1：以下的配置例子，设置 OSPFv3 的邻居，IPv6 地址为 2001:DB8:4::1，优先权值为 1，轮询间隔为 150 秒。

```
Ruijie(config)# interface fastEthernet 0/1
Ruijie(config-if)# ipv6 ospf neighbor 2001:DB8:4::1 priority 1 poll-interval 150
```

【检验方法】 -

【提示信息】 1：非 NBMA and point-to-multipoint 网络下配置邻居。

```
% Neighbor command is allowed only on NBMA and point-to-multipoint networks.
```

2：指定的邻居不是 ipv6 链路地址。

```
% OSPFv3: Neighbor address needs to be a link-local address.
```

【常见错误】 配置的接口地址非对应接口的 IPV6 链路地址。

【平台说明】 -

6.26 ipv6 ospf network

设置接口的网络类型。

ipv6 ospf network { **broadcast | non-broadcast** | **point-to-point | point-to-multipoint** [**non-broadcast**] } [**instance** *instance-id*]

恢复缺省值。

no ipv6 ospf network [**broadcast | non-broadcast** | **point-to-point | point-to-multipoint** [**non-broadcast**]] [**instance** *instance-id*]

【参数说明】

参数	描述
broadcast	设置广播网络类型。
non-broadcast	设置非广播网络类型
point-to-point	设置点对点网络类型。
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
instance *instance-id*	对接口特定 OSPFv3 实体进行配置 范围 0-255。

【缺省配置】 点到点网络类型：PPP、SLIP、帧中继点到点子接口、X.25 点到点子接口封装；
NBMA 网络类型：帧中继（点到点子接口除外）、X.25 封装（点到点子接口除外）；
广播网络类型：以太网封装；
缺省网络类型没有为点到多点网络类型。

【命令模式】 接口配置模式

【缺省级别】 14

【使用指导】 -

【配置举例】 1：下面例子，用于设置参与 OSPFv3 运行的接口的网络类型为点对点接口：

```
Ruijie(config)# interface ethernet 1/0
Ruijie(config-if)# ipv6 ospf network point-to-point
```

【检验方法】 1：使用 show ipv6 ospf interface 命令可以查看所配置的网络类型。

【提示信息】 -

【常见错误】 -

【平台说明】 -

6.27 ipv6 ospf priority

设置接口的优先级。
ipv6 ospf priority *number-value* [**instance** *instance-id*]

恢复缺省值。
no ipv6 ospf priority [**instance** *instance-id*]

【参数说明】

参数	描述
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。

【缺省配置】 优先权值缺省为 1。

【命令模式】 接口配置模式

【缺省级别】 14

【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】 1：下面例子，使得接口在 DR/BDR 选举时，不再成为 DR 或 BDR：

```
Ruijie(config)# interface ethernet 1/0
Ruijie(config-if)# ipv6 ospf priority 0
```

【检验方法】 1：使用 show ipv6 ospf interface 命令可以查看所配置的接口优先级。

【提示信息】 -

【常见错误】 -

【平台说明】 -

6.28 ipv6 ospf retransmit-interval

设置接口上发送 LSA 的重传间隔。
ipv6 ospf retransmit-interval *seconds* [**instance** *instance-id*]

恢复缺省值。

no ipv6 ospf retransmit-interval [**instance** *instance-id*]

【参数说明】

参数	描述
seconds	发送 LSA 的重传间隔。 范围 1-65535(秒)。
instance *instance-id*	对接口特定 OSPFv3 实体进行配置 范围 0-255。

【缺省配置】 5 秒

【命令模式】 接口配置模式

【缺省级别】 14

【使用指导】 为了保证路由信息传送的可靠性，朝邻居发送 LSA 时，都需要得到邻居确认。用户可以根据实际运行环境，通过本命令设置允许等待邻居确认的时间间隔，如果在指定的时间内无法得到确认，将重传 LSA 信息。

【配置举例】 1：下面例子，用于设置重传 LSA 的时间间隔为 10s：

```
Ruijie(config)# interface ethernet 1/0
Ruijie(config-if)# ipv6 ospf retransmit-interval 10
```

【检验方法】 1：使用 show ipv6 ospf interface 命令可以查看所配置的重传时间间隔

【提示信息】 -

【常见错误】 -

【平台说明】 -

6.29 ipv6 ospf transmit-delay

设置在接口上传送 LSA 时的延迟时间。

ipv6 ospf transmit-delay *seconds* [**instance** *instance-id*]

恢复缺省值。

no ipv6 ospf transmit-delay [**instance** *instance-id*]

【参数说明】

参数	描述
seconds	发送 LSA 的延迟时间。

	范围 1-65535(秒)。
instance *instance-id*	对接口特定 OSPFv3 实体进行配置 范围 0-255。

【缺省配置】 1 秒

【命令模式】 接口配置模式

【缺省级别】 14

【使用指导】 -

【配置举例】 1：下面例子，用于设置在接口上传输 LSA 的延迟时间：

```
Ruijie(config)# interface ethernet 1/0
Ruijie(config-if)# ipv6 ospf transmit-delay 2
```

【检验方法】 1：使用 show ipv6 ospf interface 命令可以查看所配置的报文发送延迟时间。

【提示信息】 -

【常见错误】 -

【平台说明】 -

6.30 ipv6 router ospf

打开 OSPFv3 路由进程。
ipv6 router ospf [*process-id* [**vrf** *vrf-name*]]

关闭 OSPFv3 路由进程。
no ipv6 router ospf *process-id*

【参数说明】

参数	描述
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

【缺省配置】 没有打开 OSPFv3 路由进程。

【命令模式】 全局配置模式。

【缺省级别】 14

【使用指导】 打开 OSPFv3 进程后，将进入路由进程配置模式。
目前，最多支持配置 32 个 OSPFv3 进程。

【配置举例】 1：下面例子，用于在指定 vrf: vpn_1 内启动 OSPFv3 进程：

```
Ruijie(config)# ipv6 router ospf 1 vrf vpn_1
```

【检验方法】 执行 show ipv6 ospf 可以看到已经配置 ospfv3 进程。

【提示信息】 1：IPv6 unicast-routing 未开启则无法配置 OSPFv3 进程。

```
IPv6 unicast-routing not enabled, OSPFv3 process can't configure
```

2： 无法分配到 router-id 则相应 ospfv3 进程无法启动。

```
%OSPFV3-4-NORTRID: OSPFv3 process 1 failed to allocate unique router-id and cannot start.
```

【常见错误】 -

【平台说明】 -

6.31 ipv6 router ospf max-concurrent-dd

设置所有 OSPFv3 路由进程允许同时并发交互（发起或接受）的邻居最大数目。
ipv6 router ospf max-concurrent-dd *number*

恢复缺省值。

no ipv6 router ospf max-concurrent-dd

【参数说明】

参数	描述
number	并发交互的邻居最大数目 范围 1-65535

【缺省配置】 缺省为 10 个。

【命令模式】 全局配置模式。

【缺省级别】 14

【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 OSPFv3 路由进程允许同时并发交互（发起或接受）的邻居最大数目。

【配置举例】 1：如下例子将所有 OSPFv3 路由进程允许同时并发交互（发起或接受）的邻居最大数目设置为 4，该配置的

效果是大量邻居交互的过程中，本设备最大允许同时发起与 4 个邻居交互，并最大允许同时接受 4 个邻居发起的交互，即本设备最多可以同时与 8 个邻居进行交互：

```
Ruijie(config)#ipv6 router ospf max-concurrent-dd 4
```

【检验方法】 -

【提示信息】 -

【常见错误】 -

【平台说明】 -

6.32 log-adj-changes

设置是否记录邻接状态变化的日志。

log-adj-changes [**detail**]

关闭设置是否记录邻接状态变化的日志功能。

no log-adj-changes [**detail**]

【参数说明】

参数	描述
detail	显示详细的邻居状态变迁信息

【缺省配置】 缺省该功能打开，不带 detail 参数，只记录以下 4 类事件的日志信息：
邻接状态达到 Full 状态；
邻接状态离开 Full 状态；
邻接状态达到 Down 状态；
邻接状态离开 Down 状态。

【命令模式】 路由进程配置模式。

【缺省级别】 14

【使用指导】 -

【配置举例】 1：以下的配置例子，将打开详细的邻居状态变化的日志记录。

```
Ruijie(config)# ipv6 router ospf 1
Ruijie(config-router)# log-adj-changes detail
```

【检验方法】 1：使用 show ipv6 ospf 命令可以查看所配置的日志记录开关状态。

【提示信息】 -

【常见错误】 -

【平台说明】 -

6.33 max-concurrent-dd

设置当前 OSPFv3 路由进程允许同时并发交互（发起或接受）的邻居最大数目。
max-concurrent-dd *number*

恢复缺省配置
no max-concurrent-dd

【参数说明】

参数	描述
number	并发交互的邻居最大数目。范围 1-65535

【缺省配置】 缺省为 5。

【命令模式】 路由进程配置模式。

【缺省级别】 14

【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 OSPFv3 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】 1：如下例子将当前 OSPFv3 路由进程允许同时并发交（发起或接受）互的邻居最大数目设置为 4，该配置的效果是大量邻居交互的过程中，本设备最大允许同时发起与 4 个邻居交互，并最大允许同时接受 4 个邻居发起的交互，即本设备最多可以同时与 8 个邻居进行交互：

```
Ruijie(config)# ipv6 router ospf 1
Ruijie(config-router)# max-concurrent-dd 4
```

【检验方法】 1：执行 show ipv6 ospf 命令可以看到对应最大允许交互个数

【提示信息】 -

【常见错误】 -

【平台说明】 -

6.34 passive-interface

设置消极接口。

passive-interface { **default** | *interface-type interface-number* }

取消设置的消极接口。

no passive-interface { **default** | *interface-type interface-number* }

【参数说明】

参数	描述
default	将所有接口设置为消极接口。
interface-type *interface-number*	将指定接口设置为消极接口。

【缺省配置】 未设置消极接口。

【命令模式】 路由进程配置模式。

【缺省级别】 14

【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。

【配置举例】 1：只允许 VLAN1 接口参与 OSPFv3 运行：

```
Ruijie(config)# ipv6 router ospf 1
Ruijie(config-router)# passive-interface default
Ruijie(config-router)# no passive-interface vlan 1
```

【检验方法】 1：show ipv6 ospf interface 查看对应的状态。

【提示信息】 1：指定了无效的接口

```
% Interface is invalid.
```

【常见错误】 -

【平台说明】 -

6.35 redistribute

启动路由重分发，将其他路由协议的路由信息注入到 OSPFv3 路由进程中。

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*]

取消该功能或者修改重分发的参数。

no 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-type** } | **route-map** *route-map-name* | **tag** *tag-value*]

【参数说明】

参数	描述
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**	只针对配置重分发 IS-IS 路由时使用 ,用于指定特定 level 的路由进行重分发。
match	只针对配置重分发 OSPFv3 路由时使用，用于过滤特定路由进行重分发： internal：区内路由与区间路由； external [1|2]：E1、E2 或所有的外部路由 **nssa-external** [**1 | 2**]：N1、N2 或者所有 NSSA 区域外部路由
metric *metric-value*	设置 OSPFv3 external 2 LSA 的 metric ,通过 metric-value 指定 metric 大小，取值范围：0-16777214
metric-type {*1* | *2* }	设置外部路由的度量类型为 E-1 或 E-2
route-map *route-map-name*	重分发路由关联的路由策略。 map-tag 的名字不超过 32 字符。
tag *tag-value*	设置重分布到 OSPFv3 内路由的 tag 值，取值范围：0-4294967295

【缺省配置】 没有打开该功能；
metric-type 缺省为 2；
重分发 ISIS 时，缺省重分发 level-2 路由；
重分发 OSPFv3 时，缺省重分发所有子类型的 OSPFv3 路由；
缺省未关联 route-map。

【命令模式】 路由进程配置模式。

【缺省级别】 14

【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；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：

4. 如果 no 命令指定某些参数，则将这些参数恢复缺省配置；
5. 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**，使用命令 **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**。

【配置举例】 1：重分发直连路由，并关联 route-map test：

```
Ruijie(config)# ipv6 router ospf 1
Ruijie(config-router)# redistribute connect metric 10 route-map test
```

2：关联的路由图配置为：

```
Ruijie(config)# route-map test permit 10
Ruijie(config-route-map)#match metric 20
Ruijie(config-route-map)#set metric 30
```

此时以上配置的功能，是将重分发的路由中 metric 值为 20 的，将其 metric 设置为 30；重分发的其它路由的 metric 设置为 10。

【检验方法】 1：使用 show ipv6 ospf database 命令可以查看引入了所配置的路由信息。

【提示信息】 1：不允许重分布本实例的路由。

```
% Redistribution of ″ospf 1″ via ″ospf 1″ not allowed
```

【常见错误】 -

【平台说明】 -

6.36 router-id

设置设备的标识(Router ID)。

router-id *router-id*

删除设置的 Router ID，恢复缺省的 Router ID。

no router-id

【参数说明】

参数	描述
router-id	设备的标识。 使用 IPv4 地址格式表示。

【缺省配置】 OSPFv3 路由进程选举所有回环（loopback）接口 IPv4 地址最大的作为路由设备标识；
如果没有配置 IPv4 地址的回环（loopback）接口，那么 OSPFv3 进程将选取其他所有接口 IPv4 地址最大的作为路由设备标识。

【命令模式】 路由进程配置模式。

【缺省级别】 14

【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。

【配置举例】 1：下面例子，用于设置本设备参与 OSPFv3 运行的标识为 1.1.1.1：

```
Ruijie(config)# ipv6 router ospf 1
Ruijie(config-router)# router-id 1.1.1.1
```

【检验方法】 执行 show ipv6 ospf 命令可以看到对应 ospf 进程的 Router-ID。

【提示信息】 1：配置 Router-ID 为 0.0.0.0 提示该操作会导致 ospfv3 进程停止运行。

```
% OSPFv3: router-id set to 0.0.0.0, process will not run.
```

2：配置的 router-id 和其它实例的 router-id 重复。

```
% OSPFv3: router-id %r is in use by process %s
```

【常见错误】 -

【平台说明】 -

6.37 summary-prefix

配置 OSPFv3 路由域外部路由的汇聚路由。
summary-prefix *ipv6-prefix*/*prefix-length* [**not-advertise** | [**tag** *number*] [**cost** *cost*]]

恢复缺省配置。
no summary-prefix *ipv6-prefix*/*prefix-length* [**not-advertise |** [**tag**] [**cost**]]

【参数说明】

参数	描述
ipv6-prefix/*prefix-length*	汇聚的地址范围。
not-advertise	不向邻居通告此汇聚路由 无此参数表示通告
tag *number*	设置重分布到 OSPFv3 内路由的 tag 值 范围 0-4294967295
cost *cost*	设置汇聚路由的 cost 值，取值范围：0-16777214

【缺省配置】 缺省没有配置汇聚路由。

【命令模式】 路由进程配置模式。

【缺省级别】 14

【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 ,area range 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】 1：下面例子，用于配置将 2001:DB8::/64 范围内的外部路由的汇聚为 2001:DB8::/64 路由进行通告：

```
Ruijie(config)# ipv6 router ospf 1
Ruijie(config-router)# summary-prefix 2001:DB8::/64
```

【检验方法】 1：使用 show ipv6 ospf summary-address 命令可以查看所配置的聚合路由。

【提示信息】 -

【常见错误】 -

【平台说明】 -

6.38 show ipv6 ospf

显示 OSPFv3 进程信息。

show ipv6 ospf [*process-id*]

【参数说明】

参数	描述
process- id	ospf 进程号

【命令模式】 路由配置模式

【缺省级别】 14

【使用指导】 -

【配置举例】 1：显示 OSPFv3 进程信息

```
Ruijie# show ipv6 ospf
Routing Process "OSPFv3 (1)" with ID 1.1.1.1
Process uptime is 24 minutes
Enable two-way-maintain
SPF schedule delay 5 secs, Hold time between SPFs 10 secs
Initial LSA throttle delay 0 msecs
Minimum hold time for LSA throttle 5000 msecs
Maximum wait time for LSA throttle 5000 msecs
Lsa Transmit Pacing timer 40 msecs, 1 LS-Upd
Minimum LSA arrival 1000 msecs
Pacing lsa-group: 30 secs
Number of incomming current DD exchange neighbors 0/5
Number of outgoing current DD exchange neighbors 0/5
Number of external LSA 0. Checksum Sum 0x0000
Number of AS-Scoped Unknown LSA 0
Number of LSA originated 11
Number of LSA received 4
Log Neighbor Adjency Changes : Enabled
BFD enabled
Number of areas in this router is 2
   Area BACKBONE(0)
        Number of interfaces in this area is 1(1)
        SPF algorithm executed 4 times
        Number of LSA 3.  Checksum Sum 0x1DDF1
        Number of Unknown LSA 0
  Area 0.0.0.1 (NSSA)
        Number of interfaces in this area is 1(1)
        SPF algorithm executed 5 times
        Number of LSA 7.  Checksum Sum 0x445FE
        Number of Unknown LSA 0
```

NSSA Translator State is elected 字段解释：

字段	说明
Routing Process "OSPFv3 (x)" with ID A.B.C.D	OSPF 进程号和 OSPF 的 Router ID

Process uptime	本 OSPF 进程生效的时间（router-id 为 0.0.0.0 时进程是不生效的）。
Enable two-way-maintain	启用 OSPFv3 双向维持功能
SPF schedule delay	收到拓扑变化调用 SPF 运算所要延迟的时间
SPF Hold time	两次 SPF 计算之间至少要维持的时间
Initial LSA throttle delay	生成 LSA 的最小延迟时间
Minimum hold time for LSA throttle	两次 SPF 运算之间的最小时间间隔
Maximum wait time for LSA throttle	两次 SPF 运算之间的最大时间间隔
Lsa Transmit Pacing timer	Lsa 分组更新频率
Minimum LSA arrival	Lsa 最小接收延迟时间
Pacing lsa-group	组步调时间间隔
Incomming current DD exchange neighbors	正在交互的邻居数量 ,incomming 指首次进入 exstart 状态的邻居
Outgoing current DD exchange neighbors	正在交互的邻居数量，outgoing 指从更高状态退回 exstart 重新交互的邻居
Number of external LSA	数据库中存储的外部 LSA 的数量
External LSA Checksum Sum	数据库中存储的外部 LSA 的检验和的总和
Number of AS-Scoped Unknown LSA	收到 as 泛洪范围的未知 lsa 个数
Number of LSA originated	生成的 LSA 数量
Number of LSA received	接收到的 LSA 数量
Log Neighbor Adjency Changes	邻居状态变化记录开关是否打开
BFD enabled	表示启用 OSPF 与 BFD 联动
Number of areas in this router	该路由设备上的区域总数
Number of interfaces in this area	属于该区域的接口数目
SPF algorithm executed	SPF 计算的次数
Number of LSA	属于该区域的 LSA 的总的数量
Checksum Sum	该区域的 LSA 的校验和的总和
Number of Unknown LSA	该区域收到未知类型 lsa 的个数
NSSA Translator State	是否将 NSSA LSA 转换为 External LSA ,仅对 NSSA 区，并且是 ABR 的 OSPF 进程有效。

【提示信息】 -

【平台说明】 -

6.39 show ipv6 ospf database

显示 OSPFv3 进程数据库信息。

show ipv6 ospf [*process- id*] **database** [**database-summary** | *lsa-type* [**adv-router** *router-id*]]

【参数说明】

参数	描述
process- id	OSPFv3 进程号
lsa-type	LSA 类型，有以下几类： NSSA-external-LSA 、 AS-external-LSAs 、 Link-LSAs 、 Inter-Area-Prefix-LSAs、Inter-Area-Router-LSAs、 Intra-Area-Prefix-LSAs、Network-LSAs、Router-LSAs 没配此参数时，显示所有 LSA 信息
adv-route*r router-id*	显示指定 router 产生的 LSA 信息。
database-summary	显示 OSPFv3 链路状态数据库各种 LSA 统计信息。

【命令模式】 特权模式

【缺省级别】 14

【使用指导】

【配置举例】 1：显示 OSPFv3 进程数据库信息

```
Ruijie# show ipv6 ospf database
OSPFv3 Router with ID (1.1.1.1) (Process 1)
Link-LSA (Interface FastEthernet 1/0)
Link State ID   ADV Router    Age   Seq#        CkSum    Prefix
0.0.0.2         1.1.1.1       197   0x80000001  0x7cd8   0
0.0.0.5         2.2.2.2       206   0x80000001  0x8c86   0
Link-LSA (Interface Loopback 1)
Link State ID   ADV Router    Age   Seq#        CkSum    Prefix
0.0.64.1        1.1.1.1       82    0x80000001  0xb760   0
Router-LSA (Area 0.0.0.0)
Link State ID   ADV Router    Age   Seq#        CkSum    Link
0.0.0.0         1.1.1.1       17    0x80000006  0x62a1   1
0.0.0.0         2.2.2.2       156   0x80000003  0x8653   1
Network-LSA (Area 0.0.0.0)
Link State ID   ADV Router    Age   Seq#        CkSum
0.0.0.5         2.2.2.2       157   0x80000001  0xf8f6
Router-LSA (Area 0.0.0.1)
Link State ID   ADV Router    Age   Seq#        CkSum    Link
0.0.0.0         1.1.1.1       17    0x80000002  0x0529   0
Inter-Area-Prefix-LSA (Area 0.0.0.1)
Link State ID   ADV Router    Age   Seq#        CkSum
0.0.0.1         1.1.1.1       77    0x80000002  0x83b4
AS-external-LSA
Link State ID   ADV Router    Age   Seq#        CkSum
```

```
0.0.0.1          1.1.1.1          1       0x80000001   0x6035 E2
```

字段解释：

字段	说明
Link-LSA (Interface FastEthernet 1/0)	OSPFv3 Link-LSA，OSPFv3 中 LSA 主要有： Type-1 LSA—Router-LSA Type-2 LSA—Network-LSA Type-3 LSA—Inter-Area-Prefix-LSA Type-4 LSA—Inter-Area-Router-LSA Type-5 LSA—AS-External-LSA Type-7 LSA—NSSA-external-LSA Type-8 LSA—Link-LSA Type-9 LSA—Intra-Area-Prefix-LSA
Link State ID	LSA 的链路状态 ID
ADV Router	LSA 的通告路由器
Age	LSA 的老化时间
Seq#	LSA 的序列号
CkSum	LSA 的校验和
Prefix	Type-8 LSA 中携带的 ipv6 地址前缀数
Link	Type-1 LSA 中携带的链路信息数

【提示信息】

【平台说明】 -

6.40 show ipv6 ospf interface

显示 OSPFv3 接口信息。

show ipv6 ospf [*process- id*] **interface** [*interface-type interface-number* | **brief**]

【参数说明】

参数	描述
process- id	OSPFv3 进程号
interface-type interface-number	指定接口类型和编号。
brief	显示接口的摘要。

【命令模式】 特权模式

【缺省级别】 14

【使用指导】 -

【配置举例】 1：显示 OSPFv3 接口信息

```
Ruijie# show ipv6 ospf interface
FastEthernet 1/0 is up, line protocol is up
Interface ID 2
IPv6 Prefixes
fe80::2d0:22ff:fe22:2223/64 (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 BDR, Priority 1, BFD enabled
Designated Router (ID) 2.2.2.2
Interface Address fe80::c800:eff:fe84:1c
Backup Designated Router (ID) 1.1.1.1
Interface Address fe80::2d0:22ff:fe22:2223
Timer interval configured,Hello 10,Dead 40,Wait 40,Retransmit 5
Hello due in 00:00:02
Neighbor Count is 1, Adjacent neighbor count is 1
Hello received 26 sent 26, DD received 5 sent 4
LS-Req received 1 sent 1, LS-Upd received 3 sent 6
LS-Ack received 6 sent 2, Discarded 0
```

字段解释：

字段	说明
FastEthernet 1/0 is up, line protocol is up	链路和协议状态
Interface ID	接口索引
IPv6 Prefixes	接口的 ipv6 前缀信息
OSPFv3 Process (1)	接口所在的 ospfv3 的进程
Area	接口所在的区域
Instance ID	接口所在的实例
Router ID	OSPF 路由设备标识
Network Type	OSPF 网络类型
Cost	OSPF 接口花费
Transmit Delay	OSPF 接口传输延时
State	DR/BDR 状态标识
Priority	OSPF 接口优先级
BFD enabled	表示启用 OSPF 与 BFD 联动
Designated Router (ID)	该接口的 DR 的路由设备标识
DR's Interface address	该接口的 DR 的接口地址
Backup Designated Router (ID)	该接口的 BDR 的路由设备标识
BDR's Interface address	该接口的 BDR 的接口地址
Time intervals configured	接口对应的 Hello，Dead，Wait，Retransmit 时间

Hello due in	上次 HELLO 发送的时间
Neighbor Count	邻居总数
Adjacent neighbor count	Full 的邻居数量
Hello received sent	收到与发出的 HELLO 报文统计
DD received send	收到与发出的 DD 报文统计
LS-Req received send	收到与发出的 LS 请求报文统计
LS-Upd received send	收到与发出的 LS 更新报文统计
LS-Ack received send	收到与发出的 LS 响应报文统计
Discard	被丢弃的 OSPF 报文统计

【提示信息】

【平台说明】 -

6.41 show ipv6 ospf neighbor

显示 OSPFv3 进程邻居信息。

show ipv6 ospf [*process- id*] **neighbor** [*interface-type interface-number* [**detail**] | *neighbor-id* | **detail** | **statistics**]

【参数说明】

参数	描述
process-id	OSPFv3 进程号
detail	显示邻居详细信息。
interface-type interface-number	指定接口类型。
neighbor-id	指定邻居 Router ID。
statistics	显示邻居的统计信息。

【命令模式】 特权模式

【缺省级别】 14

【使用指导】

【配置举例】 1：查看 OSPFv3 邻居摘要信息

```
Ruijie# show ipv6 ospf neighbor
OSPFv3 Process (1) , 1 Neighbors, 1 is Full:
Neighbor ID  Pri  State     Dead Time   Interface         Instance ID
2.2.2.2      1    Full/DR   00:00:33    FastEthernet 1/0  0
Ruijie# show ipv6 ospf neighbor detail
```

```
Neighbor 2.2.2.2, interface address fe80::c800:eff:fe84:1c
In the area 0.0.0.0 via interface FastEthernet 1/0
Neighbor priority is 1, State is Full, 6 state changes
DR is 2.2.2.2 BDR is 1.1.1.1
Options is 0x000013 (-|R|-|-|E|V6)
Dead timer due in 00:00:36
Database Summary List 0
Link State Request List 0
Link State Retransmission List 0
BFD session state up
```

字段解释：

字段	说明
OSPFv3 Process (1) , 1 Neighbors, 1 is Full:	进程号，邻居个数，full 的邻居个数
Neighbor ID	邻居设备的 Router ID
Pri	邻居设备的优先级
State	邻居的状态，包括： Down—邻居会话的初始状态 Attempt—当 NBMA 网络中上具有 DR 选举资格的设备与其邻居相连的接口变为有效时，将会把邻居的状态置为 Attempt，该状态仅对 NBMA 网络上的邻居有效 Init—收到邻居的 Hello 报文，但是 Hello 报文中没有包含自己的邻居 ID 2-Way—从邻居收到的 Hello 报文中看到了自己的 RouterID，表明双向通信已经建立 Exstart—设备和邻居建立主/从关系，确定 DD 报文的序列号，为交换 DD 报文做好准备 Exchange—设备向其邻居发送描述自己整个链路状态数据库信息的 DD 报文 Loading—设备向邻居发送链路状态请求报文，用来请求最新的 LSA Full—设备与邻居之间建立起完全邻接关系 OSPF 在广播、NBMA 网络中设备的角色，包括： DR—指定路由器（Designate Router），仅在广播、NBMA 网络中存在 BDR—备份指定路由器（Buckup Designate Router），仅在广播、NBMA 网络中存在 DRother—广播、NBMA 网络中除 DR、BDR 外的所有设备 在 P2P、P2MP 网络中，不存在上述角色，show 信息中该字段用“-”标识

Dead Time	邻居到 Dead 状态还剩余时间
Instance ID	邻居实例 id
Interface	与邻居设备所在网络相连的接口
Interface address	邻居路由设备的接口地址
In the area	显示学习到该邻居的区域
via interface	显示学到该邻居的接口
Neighbor priority	邻居 OSPF 优先权值
State changes times	邻居状态变化的次数
DR	邻居路由设备选举的 DR 的接口地址(即 Hello 报文的 DR 字段)
BDR	邻居路由设备选举的 BDR 的接口地址(即 Hello 报文的 BDR 字段)
Options	Hello 报文可选项内容
Dead Time due in	显示宣布该邻居无效时间
Database Summary List	邻居 DD 报文统计
Link State Request List	邻居 LS 请求报文统计
Link State Retransmission List	邻居重传报文统计
BFD session state up	bfd 联动的状态

【提示信息】 -

【平台说明】 -

6.42 show ipv6 ospf restart

显示 OSPFv3 GR 相关信息。

show ipv6 ospf [*process- id*] **restart**

【参数说明】

参数	描述
process- id	OSPFv3 进程号

【命令模式】 特权模式

【缺省级别】 14

【使用指导】

【配置举例】 1：查看 Restarter 当前状态

```
Ruijie# show ipv6 ospf restart
```

```
Routing Process is ospf 1
 Graceful-restart enabled
   Restart grace period 120 secs
   Current Restart status is plannedRestart
   Current Restart remaining time 50 secs
Graceful-restart helper support enabled
```

字段解释：

字段	说明
Routing Process is ospf	启用 restart 的进程号
Graceful-restart enabled	是否启用 restart 功能
Restart grace period	Restart 周期
Current Restart status	当前 restart 状态
Current Restart remaining time	当前剩余 restart 时间
Graceful-restart helper support enabled	是否支持 restart helper

2：查看 Helper 当前状态

```
Ruijie# show ipv6 ospf restart
Routing Process is ospf 1
 Neighbor 10.1.1.2, interface addr 10.1.1.2
   In the area 0.0.0.0 via interface GigabitEthernet 6/0/0
   Graceful-restart helper enabled
     Current helper status is helping
     Current helper remaining time 50 secs
```

字段解释：

字段	说明
Neighbor	Helper 的邻居的设备标识
interface addr	helper 对应的接口地址
In the area	作为 helper 的区域
interface GigabitEthernet	Helper 对应的接口
Graceful-restart helper enabled	是否启用 helper 功能
Current helper status	当前 helper 状态
Current helper remaining time	作为 helper 状态剩余时间

【提示信息】 -

【平台说明】 -

6.43 show ipv6 ospf route

显示 OSPFv3 路由。

show ipv6 ospf [*process- id*] **route** [**count**]

【参数说明】

参数	描述
process- id	OSPFv3 进程号
count	显示 OSPFv3 路由数量汇总

【命令模式】 特权模式

【缺省级别】 14

【使用指导】

【配置举例】 1：查看 OSPFv3 路由信息

```
Ruijie# show ipv6 ospf route
OSPFv3 Process (1)
Codes: C - connected, D - Discard, 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 2Destination          Metric   Next-hop
E2 2001:DB8:1::/64   1/20     via fe80::c800:eff:fe84:1c, FastEthernet 1/0
O  2001:DB8:2::/64   11       via fe80::c800:eff:fe84:1c, FastEthernet 1/0, Area 0.0.0.0
```

字段解释：

字段	说明
OSPFv3 Process (1)	OSPFv3 进程号
Destination	OSPF 路由类型和目的网络。OSPF 中路由类型包括以下几种： C：直连路由 D：黑洞路由 O：OSPF 区域内路由 IA：OSPF 区域间路由 N1：OSPF NSSA 外部类型 1 路由 N2：OSPF NSSA 外部类型 2 路由 E1：OSPF 外部类型 1 路由 E2：OSPF 外部类型 2 路由
Metric	路由成本值
Next-hop	路由下一跳

【提示信息】 -

【平台说明】 -

6.44 show ipv6 ospf summary-prefix

显示 OSPFv3 外部路由汇聚信息。

show ipv6 ospf [*process-id*] **summary-prefix**

【参数说明】

参数	描述
process- id	OSPFv3 进程号

【命令模式】 特权模式

【缺省级别】 14

【使用指导】

【配置举例】 1：查看 OSPFv3 外部路由汇聚信息

```
Ruijie# show ipv6 ospf summary-prefix
OSPFv3 Process 1, Summary-prefix:
2001:1::/64, Metric 20, Type 2, Tag 0, Match count 5, advertise
```

字段解释：

字段	说明
Summary-prefix	汇聚路由前缀
Metric	汇聚后路由度量
Type	汇聚后路由类型
Match count	汇聚成员个数
Advertise	汇聚后是否向外发布
Tag	汇聚后路由标记

【提示信息】 -

【平台说明】 -

6.45 show ipv6 ospf topology

显示 OSPFv3 每个区的拓扑信息。

show ipv6 ospf [*process- id*] **topology** [**area** *area-id*]

【参数说明】

参数	描述
process- id	OSPFv3 进程号
area-id	指定的区

【命令模式】 特权模式

【缺省级别】 14

【使用指导】 -

【配置举例】 1：显示 OSPFv3 每个区拓扑信息

```
Ruijie# show ipv6 ospf topology
OSPFv3 Process (1)
OSPFv3 paths to Area (0.0.0.0) routers
Router ID        Bits  Metric     Interface             Next-Hop(router/address)
1.1.1.1             B  --
2.2.2.2            EB  1          GigabitEthernet 0/6   2.2.2.2/fe80::21a:a9ff:fe41:5b06

OSPFv3 paths to Area (0.0.0.1) routers
Router ID        Bits  Metric     Interface             Next-Hop(router/address)
1.1.1.1           V B  --
2.2.2.2           VEB  1          GigabitEthernet 0/6   2.2.2.2/fe80::21a:a9ff:fe41:5b06
```

字段解释：

字段	说明
OSPFv3 paths to Area	对应区域的拓扑信息
Router ID	节点的设备标识
Bits	节点中的可选项内容
Metric	该节点到根节点的度量
Interface	到该节点的出接口
Next-Hop(router/address)	到该节点的下一跳

【提示信息】 -

【平台说明】 -

6.46 show ipv6 ospf virtual-links

显示 OSPFv3 进程虚链路信息。

show ipv6 ospf [*process- id*] **virtual-links**

【参数说明】

参数	描述
process- id	OSPFv3 进程号

【命令模式】 特权模式

【缺省级别】 14

【使用指导】

【配置举例】 1：显示 OSPFv3 虚拟链路的信息

```
Ruijie# show ipv6 ospf virtual-links
Virtual Link VLINK1 to router 1.1.1.1 is up
  Transit area 0.0.0.1 via interface FastEthernet 0/1, instance ID 0
  Local address 2001::2/128
  Remote address 2001::1/128
  Transmit Delay is 1 sec, State Point-To-Point,
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
        Hello due in 00:00:08
        Adajcency state Full
```

字段解释：

字段	说明
Virtual Link VLINK1 to router	显示虚拟链路的邻居以及状态
Transit area	显示虚拟链路的传输区域
via interface	显示虚拟链路的关联接口
Local address	虚链路本端接口地址
Remote address	虚链路对端接口地址
Transmit Delay	显示虚拟链路的传输延时
State	虚链接网络类型
Timer intervals configured	虚链接定时器，包括 Hello、Dead、Retransmit
Hello due in	距离下一次发送 Hello 报文的时间
Adjacency state	虚链接邻居状态

【提示信息】 -

【平台说明】 -

6.47 timers lsa arrival

配置 LSA 重复接收延时。
timers lsa arrival *arrival-time*

恢复默认配置。
no timers lsa arrival

【参数说明】

参数	描述
arrival-time	接收相同 LSA 的延时。单位毫秒，取值范围 0-600000，缺省值 1000。

【缺省配置】 参数缺省值

【命令模式】 路由进程配置模式

【缺省级别】 14

【使用指导】 配置指定时间之内接收到相同 LSA 时，不做处理。

【配置举例】 1：配置相同 LSA 延时时间最少为 2s

```
Ruijie(config)# ipv6 router ospf 1
Ruijie(config-router)# timers lsa arrival 2000
```

【检验方法】 1：使用 show ipv6 ospf 命令可以查看所配置的 LSA 重复接收延时。

【提示信息】 -

【常见错误】 -

【平台说明】 -

6.48 timers pacing lsa-group

调整 LSA 分组刷新时间。
timers pacing lsa-group *seconds*

恢复缺省配置。

no timers pacing lsa-group

【参数说明】

参数	描述
seconds	组步调间隔。单位秒，取值范围 10-1800，缺省值 30。

【缺省配置】 参数缺省值

【命令模式】 路由进程配置模式

【缺省级别】 14

【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，我们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，我们建议用户降低步调间隔。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。

【配置举例】 1：以下的配置例子，将步调时间设置为 120 秒。

```
Ruijie(config)# ipv6 router ospf 1
Ruijie(config-router)#timers pacing lsa-group 120
```

【检验方法】 1：使用 show ipv6 ospf 命令可以查看所配置的 LSA 组步调更新的步调时间。

【提示信息】 -

【常见错误】 -

【平台说明】 -

6.49 timers pacing lsa-transmit

配置 LSA 发送分组更新。

timers pacing lsa-transmit *transmit-time transmit-count*

恢复默认配置。

no timers pacing lsa-transmit

【参数说明】

参数	描述

transmit-time	LSA 分组发送间隔。单位毫秒，取值范围 10-1000，缺省值 40。
transmit-count	每组 LS-UPD 报文的个数。取值范围 1-200，缺省值 1。

【缺省配置】 参数缺省值

【命令模式】 路由进程配置模式

【缺省级别】 14

【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。

【配置举例】 1：配置接口下每 50ms 发送一次 LS-UPD 报文，每次允许发送 20 个报文。

```
Ruijie(config)# ipv6 router ospf 1
Ruijie(config-router)# timers pacing lsa-transmit 50 20
```

【检验方法】 1：使用 show ipv6 ospf 命令可以查看所配置的发送分组更新间隔。

【提示信息】 -

【常见错误】 -

【平台说明】 -

6.50 timers spf

配置 OSPFv3 在接收到拓扑的变化信息，进行 SPF 计算的延时时间，以及两次 SPF 计算的时间间隔。
timers spf *spf-delay spf-holdtime*

恢复缺省配置。
no timers spf

【参数说明】

参数	描述
spf-delay	定义 SPF 计算的等待时间，以秒为单位，范围 0-2147483647 (秒)。OSPF 路由进程接收到拓扑变化，必须等指定的时间后，才进行 SPF 运算。
spf-holdtime	定义两次 SPF 运算之间的时间间隔 ,以秒为单位 ,范围 0-2147483647 (秒)。等待时间到了，两次运算间隔时间没到，还是不能进行 SPF 运算。

【缺省配置】

- RGOS 10.4 版本之前，不支持 **timers throttle spf** 命令。系统缺省值为 **timers spf** 5 10。

- RGOS 10.4 版本开始，支持 **timers throttle spf** 命令。此时缺省情况下 **timers spf** 命令不生效，SPF 计算延时是以 **timers throttle spf** 命令的缺省配置为准，参见 **timers throttle spf** 命令说明。

【命令模式】 路由进程配置模式。

【缺省级别】 14

【使用指导】 spf-delay 和 spf-holdtime 时间设置得越小，OSPF 适应拓扑变化的时间也越短，也就是说网络收敛时间越短，但是会占用路由设备更多的 CPU 时间。
timers spf 配置与 timers throttle spf 配置会互相覆盖。

【配置举例】 1：将 OSPFv3 的延时和保持时间分别设为 3 和 9 秒。

```
Ruijie(config)# ipv6 router ospf 20
Ruijie(config-router)# timers spf 3 9
```

【检验方法】 1：使用 show ipv6 ospf 命令可以查看所配置的 SPF 计算延迟。

【提示信息】 -

【常见错误】 -

【平台说明】 -

6.51 timers throttle lsa all

配置 LSA 生成指数退避算法。
timers throttle lsa all *delay-time hold-time max-wait-time*

恢复默认配置。
no timers throttle lsa all

【参数说明】

参数	描述
delay-time	生成 LSA 的最小延迟时间（数据库中的第一份 LSA 总是立即生成的）。 单位毫秒。取值范围 0-600000，缺省值 0。
hold-time	首次与第 2 次刷新 LSA 时的最短时间间隔。 单位毫秒，取值范围 1-600000，缺省值 5000。
max-wait-time	连续刷新 LSA 时，两次刷新 LSA 的最大时间间隔（这个时间间隔也是判断 LSA 是否连续刷新的值）。 单位毫秒，取值范围 1-600000，缺省值 5000。

【缺省配置】 参数缺省值

【命令模式】 路由进程配置模式

【缺省级别】 14

【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。

hold-time 不允许小于 delay-time，max-wait-time 也不允许小于 hold-time。

【配置举例】 1：配置首次延迟时间为 10ms，hold-time 为 1s，最长延迟时间为 5s。

```
Ruijie(config)# ipv6 router ospf 1
Ruijie(config-router)# timers throttle lsa all 10 1000 5000
```

【检验方法】 1：使用 show ipv6 ospf 命令可以查看所配置的 LSA 生成延迟。

【提示信息】 1：当配置 max-wait-time 比 hold-time 小的时候。

```
% Warning: max-wait-time should be no less than hold-time, set to (5)
```

2：当配置 hold-time 比 delay-time 小的时候。

```
% Warning: hold-time should be no less than delay-time, set to (5).
```

【常见错误】 1：配置的 hold-time 比 delay-time 小或者 max-wait-time 比 hold-time 小。

【平台说明】 -

6.52 timers throttle route

配置 OSPFv3 在接收到变化的区间、外部 LSA 时，进行路由计算的延时时间。
timers throttle route { **inter-area** *ia-delay* | **ase** *ase-delay* }

恢复默认配置。
no timers throttle route { **inter-area** | **ase** }

【参数说明】

参数	描述
inter-area	区间路由计算。
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。OSPF 接收到区间 LSA 变化，触发的路由计算至少要在 ia-delay 时间间隔后执行。
ase	外部路由计算。
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。OSPF 接收到外部 LSA 变化 触发的路由计算至少要在 ase-delay 时间间隔后执行。

【缺省配置】 缺省情况下：
ia-delay：0 毫秒；
ase-delay：0 毫秒。

【命令模式】 路由进程配置模式。

【缺省级别】 14

【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】 1：将 OSPFv3 的区间路由计算延迟 1 秒，配置如下。

```
Ruijie(config)# ipv6 router ospf 1
Ruijie(config-router)# timers throttle route inter-area 1000
```

【检验方法】 1：使用 show running-config 查看配置。

【提示信息】 -

【常见错误】 -

【平台说明】 -

6.53 timers throttle spf

配置 OSPFv3 在接收到拓扑的变化信息，进行 SPF 计算的延时时间、两次 SPF 计算的最小时间间隔、最大时间间隔。
timers throttle spf *spf-delay spf-holdtime spf-max-waittime*

恢复缺省配置。
no timers throttle spf

【参数说明】

参数	描述
spf-delay	接收到拓扑变化后，触发 SPF 计算的延迟时间。 单位毫秒，取值范围 1-600000，缺省值 1000。
spf-holdtime	两次 SPF 运算之间的最小时间间隔。 单位毫秒，取值范围 1-600000，缺省值 5000。
spf-max-waittime	两次 SPF 运算之间的最大时间间隔。 单位毫秒，取值范围 1-600000，缺省值 10000。

【缺省配置】 参数缺省值

【命令模式】 路由进程配置模式

【缺省级别】 14

【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，所以更加推荐使用 **timers throttle spf** 命令进行配置。

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；

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。

timers throttle spf 配置与 **timers spf** 配置会互相覆盖。

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】 1：将 OSPFv3 的 SPF 计算延时、保持时间、最大等待时间分别设为 5 毫秒、1000 毫秒、90000 毫秒。若拓扑连续变化，则 SPF 计算时间分别为：

5ms，1s，3s，7s，15s，31s，63s，89s，179s，179+90 .....

```
Ruijie(config)# ipv6 router ospf 20
Ruijie(config-router)# timers spf 5 1000 90000
```

【检验方法】 1：使用 show ipv6 ospf 命令可以查看所配置的 SPF 计算延迟。

【提示信息】 1：当配置 max-wait-time 比 hold-time 小的时候。

```
% Warning: max-wait-time should be no less than hold-time, set to (5).
```

2：当配置 hold-time 比 delay-time 小的时候。

```
% Warning: hold-time should be no less than delay-time, set to (5).
```

【常见错误】 1：配置的 hold-time 比 delay-time 小或者 max-wait-time 比 hold-time 小。

【平台说明】 -

6.54 two-way-maintain

启用 OSPFv3 双向维持功能。

two-way-maintain

禁用 OSPF 双向维持功能。
no two-way-maintain

【参数说明】

参数	描述
-	-

【缺省配置】 启用 OSPF 双向维持功能

【命令模式】 路由进程配置模式

【缺省级别】 14

【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】 1：禁用 OSPF 双向维持功能。

```
Ruijie(config)# ipv6 router ospf 1
Ruijie(config-router)# no two-way-maintain
```

【检验方法】 1：使用 show ipv6 ospf 命令可以查看所配置的双向维持是否启用。

【提示信息】 -

【常见错误】 -

【平台说明】 -

7 协议无关

7.1 accept-lifetime

配置密钥链接收方向的生存期。

accept-lifetime *start-time* { **infinite |** *end-time* **| duration** *seconds* }

删除密钥链接收方向的生存期。

no accept-lifetime

【参数说明】

参数	描述
start-time	指定生存期的开始时间
infinite	该参数表示该密钥从开始时间一直有效
end-time	密钥有效期结束时间，必须晚于 start-time
duration *seconds*	指定有效期从 start-time 开始的持续时间，取值范围：1-2147483646

【缺省配置】 没有定义密钥链接收生存期

【命令模式】 密钥链密钥配置模式

【缺省级别】 14

【使用指导】 -

【配置举例】 1： 配置密钥链 kc，进入密钥链配置模式，配置密钥 1，进入密钥 1 配置模式，并定义密钥链接收生存期

```
Ruijie(config)#key chain kc
Ruijie(config-keychain)#key 1
Ruijie(config-keychain-key)#key-string Hello
Ruijie(config-keychain-key)#accept-lifetime 16:30:00 Oct 1 2010 duration 43200
```

【检验方法】 1：使用 **show running-config** 命令查看配置。

【常见错误】 -

【平台说明】 -

7.2 ip as-path access-list

定义基于正则表达式的 AS 路径过滤规则。

ip as-path access-list *path-list-num* { **permit** | **deny** } *regular-expression*

删除基于正则表达式的 AS 路径过滤规则。

no ip as-path access-list *path-list-num* [{ **permit** | **deny** } *regular-expression*]

【参数说明】

参数	描述
path-list-num	基于正则表达式的 AS 路径控制列表名 ,AS 路径列表标识符 ,范围 :1---500。
permit	允许访问
deny	拒绝访问
regular-expression	正则表达式。范围：1..255 字符。

【缺省配置】 没有定义列表

【命令模式】 全局配置模式

【缺省级别】 14

【使用指导】 关于正则表达式的介绍请参见配置指南。

【配置举例】 1： 创建 AS 路径过滤规则，匹配只包含 AS 号 123 的路径信息。

```
Ruijie(config)# ip as-path access-list 105 deny ^123$
```

【检验方法】 1：使用 **show running-config** 命令查看配置。

【提示信息】 1：删除 AS 路径过滤规则时，输入的规则名称或过滤规则不存在，则提示错误信息。

```
% This object doesn't exist
```

2：如果输入无效的过滤规则，则提示错误信息。

```
% Can't compile regexp
```

3：如果配置规则重复的 AS 路径过滤规则，则提示错误信息。

```
% Insertion failed with duplicate policy
```

【常见错误】 -

【平台说明】 -

7.3 ip community-list

定义团体属性列表
定义标准类型的团体属性列表，并控制对它的访问。
ip community-list { *community-list-number* **| standard** *community-list-name* } { **permit | deny** } [{ *community-list-number* | **internet** | **local-AS** }]
定义扩展类型的团体属性列表，并控制对它的访问。
ip community-list { *community-list-number* | **expanded** *community-list-name* } { **permit | deny** } [*regular-expression*]

删除团体属性列表。
no ip community-list { { **standard** | **expanded** } *community-list-name* | *community-list-number* }

【参数说明】

参数	描述
standard	标准团体列表
expanded	扩展团体列表
community-list-name	团体列表名字 团体列表名不超过 80 字符
community-list-number	团体列表号 标准团体列表：编号范围为 1-99 扩展团体列表：编号范围为 100-199
permit	允许访问
deny	拒绝访问
community-number	团体属性值。 格式为 AA:NN(自治系统号：2 字节数字)，或者是一个数值，范围 0-4294967295。
internet	表示 Internet 团体，所有的路径都属于该团体。
local-AS	表示本路径不发布到本 AS 外部，当配置联盟时，本路径不发布给其它的自治系统或子自治系统。

【缺省配置】 没有定义团体列表

【命令模式】 全局配置模式

【缺省级别】 14

【使用指导】 使用该命令来定义用于 BGP 的团体列表。
目前每个团体列表最多能够支持设置 32 个团体值，包含 internet、local-AS、no-advertise 和 no-export。

【配置举例】 1：定义标准团体属性列表，拒绝团体属性 100：20 和 200：20。

```
Ruijie(config)# ip community-list standard test deny 100:20 200:20
```

2：定义标准团体属性列表，允许团体属性 internet。

```
Ruijie(config)# ip community-list standard test2 permit internet
```

【检验方法】 1：使用 **show running-config** 命令查看配置。

【提示信息】 1：如果指定的团体属性列表名字全是数字，则提示错误信息。

```
% Community-list name cannot have all digits
```

2：如果指定的团体属性列表名字长度超过 80 字符，则提示错误信息。

```
% Community-list name lengths should be less than 80 chars
```

3：删除时如果输入的列表或过滤规则不存在，则提示错误信息。

```
% This object doesn't exist
```

4：如果配置规则重复的团体属性过滤规则，则提示错误信息。

```
% Insertion failed with duplicate policy
```

5：如果配置序列号重复的团体属性过滤规则，则提示错误信息。

```
% Community-list entry with this sequence already exist
```

6：如果同时定义包含相同名字的标准和扩展团体属性列表，则提示错误信息。

```
% Community-list name conflict with previous defined
```

【常见错误】 -

【平台说明】 -

7.4 ip extcommunity-list

定义 Route Map 中引用的扩展团体属性列表，关联该列表的 Route Map 将在 BGP/MPLS VPN 应用中用来控制 VPN 路由的过滤。

ip extcommunity-list {*expanded-list* | **expanded** *list-name* } { **permit | deny** } [*regular-expression*]

定义标准类型的扩展团体属性列表。

ip extcommunity-list {*standard-list* **| standard** *list-name* } { **permit | deny** } [**rt** *value*] [**soo** *value*]

删除扩展团体属性列表。

no ip extcommunity-list {*expanded-list* **| expanded** *list-name* **|** *standard-list* **| standard** *list-name* }

创建的扩展团体属性列表，可以进入 **ip extcommunity-list** 的配置模式

ip extcommunity-list {*expanded-list* | **expanded** *list-name*| *standard-list* | **standard** *list-name* }

删除扩展属性列表。

no ip extcommunity-list {*expanded-list* | **expanded** *list-name* | *standard-list* | **standard** *list-name*}

【参数说明】

参数	描述
expand-list	取值范围[100~199]，用来标识扩展的 extcommunity 列表，一个 extcommunity 列表可包含多个规则。
standard-list	取值范围[1~99]，用来标识标准的 extcommunity 列表，一个 extcommunity 表可以包含多个规则。
expanded *list-name*	扩展 extcommunity 的名称，使用该参数将进入扩展团体属性列表的配置模式。名字长度不超过 32 个字符。
standard *list-name*	标准 extcommunity 的名称，用来标识标准的 extcommunity 表的名称，使用该参数将进入扩展团体属性列表的配置模式。名字长度不超过 32 个字符。
permit	定义一个允许的 extcommunity 规则。
deny	定义一个拒绝的 extcommunity 规则。
regular-expression	（可选）定义匹配的模板，用来匹配 extcommunity。
sequence-number	（可选）定义该规则的顺序序列号，范围从 1 到 2147483647。如果不指定，缺省情况下每增加一个规则其序列号自动以 10 递增，起始从 10 开始编号。
rt	（可选）设置 RT 属性值，该命令只能用在标准 extcommunity 配置，不能用于扩展 extcommunity 配置
soo	（可选）设置 SOO 属性值，该命令只能用在标准 extcommunity 配置，不能用于扩展 extcommunity 配置
value	扩展团体的值（extend_community_value） extend_community_value 可以有三种不同的参数： ● extend_community _value = as_num：nn。 an_num 是公共的自治域系统号（2 字节 AS），nn 用户自己定义，范围为 0..4294967295。 ● extend_community_value = ip_addr：nn。 ip_addr 地址必须是全局的 IP 地址，nn 用户自己定义，范围为 0..65535。 ● extend_community_value = as4_num：nn。 an4_num 是公共的自治域系统号（4 字节 AS），nn 用户自己定义，范围为 1..65535 在 10.4(3)或以后的版本中，增加支持 4 字节 AS 号，即新的 AS 号范围为 1..4294967295，用圆点模式表示为 1..65535.65535。

【缺省配置】 缺省未定义扩展团体属性列表规则。

【命令模式】 全局配置模式、ip extcommunity-list 配置模式

【缺省级别】 14

【使用指导】 **ip extcommunity-list** 命令用来创建一个含有多个 extcommunity 值的 extcommunity 规则列表，它主要应用于 RouteMap 的 **match extcommunity** 规则，用它来匹配 BGP 路由的扩展团体属性从而达到路由过滤的目的。对于扩展的 extcommunity 规则的定义，其 *regular-expression* 的规则如下：

字符	符号	特殊意义
句号	.	匹配任意单字符
星号	*	匹配字符串中的零个或者任意序列
加号	+	匹配字符串中的一个或者任意序列
问号	?	匹配字符串中的零个或者一个符号
加字号	^	匹配字符串的开始
美元号	$	匹配字符串的结束
下划线	_	匹配逗号、括号、字符串的开始和结束、空格
方括号	[]	匹配一定范围中的单个字符

- expanded ip extcommunity-list 配置模式下的命令有：
  [sequence-number**]deny** regular-expression 定义一个拒绝的 extcommunity 规则。
  [sequence-number**] permit** regular-expression 定义一个允许的 extcommunity 规则。
  exit 退出当前退出模式。
  no [sequence-number**]deny** regular-expression 删除一个拒绝的 extcommunity 规则。
  no [sequence-number**] permit** regular-expression 删除一个允许的 extcommunity 规则。

- standard ip extcommunity-list 配置模式下的命令有：
  [sequence-number**] deny {[rt** value] [**soo** value]**}** 定义一个拒绝的 extcommunity 规则。
  [sequence-number**] permit {[rt** value] [**soo** value]**}** 定义一个允许的 extcommunity 规则。
  exit 退出当前退出模式。
  no [sequence-number**] deny {[rt** value] [**soo** value]**}** 删除一个拒绝的 extcommunity 规则。
  no [sequence-number**] permit {[rt** value] [**soo** value]**}** 删除一个允许的 extcommunity 规则。

【配置举例】 1：定义 ip extcommunity-list：

```
Ruijie(config)# ip extcommunity-list 1 permit rt 100：1
Ruijie(config)# ip extcommunity-list standard aaa permit rt
100：2
Ruijie(config)# ip extcommunity-list expanded ext1 permit 200：[0~9][0~9]
```

2：ip extcommunity 的使用方法：

```
Ruijie(config)# route-map rt_in_filter
Ruijie(config-route-map)# match extcommunity 1
Ruijie(config-route-map)# match extcommunity ext1
Ruijie(config)# router bgp 100
Ruijie(config-router)# address-family vpn
Ruijie(config-router-af)#neighbor 3.3.3.3 send-community extended
Ruijie(config-router-af)#neighbor 3.3.3.3 route-map rt_in_filter in
```

【检验方法】 1：使用 **show running-config** 命令查看配置。

【提示信息】 1：删除时如果输入的列表或过滤规则不存在，则提示错误信息。

```
% This object doesn't exist
```

2：如果配置规则重复的扩展团体属性过滤规则，则提示错误信息。

```
% Insertion failed with duplicate policy
```

3：如果配置序列号重复的扩展团体属性过滤规则，则提示错误信息。

```
% Extcommunity-list entry with this sequence already exist
```

4：如果同时定义包含相同名字的标准和扩展的扩展团体属性列表，则提示错误信息。

```
% Extcommunity-list name conflict with previous defined
```

【常见错误】 -

【平台说明】 -

7.5 ip prefix-list

创建一个前缀列表或者增加一条前缀列表表项。

ip prefix-list *prefix-list-name* [**seq** *seq-number*] { **deny** | **permit** } *ip-prefix* [**ge** *minimum-prefix-length*] [**le** *maximum-prefix-length*]

删除一个前缀列表或前缀列表表项。

no ip prefix-list *prefix-list-name* [**seq** *seq-number*] { **deny** | **permit** } *ip-prefix* [**ge** *minimum-prefix-length*] [**le** *maximum-prefix-length*]

【参数说明】

参数	描述
prefix-list-name	前缀列表名字
seq-number	给一条前缀列表表项赋以序列号。其范围是 1 到 2147483647。如果命令中没有包含这个序列号 ,则系统会为这条前缀列表表项分配一个默认的序列号。

	第一个表项的默认序列号是 5，后续每一个未赋值的表项的默认序列号数值是比前一个序列号大的第一个 5 的倍数的数值。
deny	对于匹配情况拒绝访问
permit	对于匹配情况允许访问
ip-prefix	配置网络地址以及掩码。掩码长度从 0 到 32。
minimum-prefix-length	指定的最小范围值(即范围的起始长度) **ge** 关键字代表的是大于等于运算。 当 **ge**、**le** 都未设置时，掩码长度必须完全相同规则才会匹配。
maximum-prefix-length	指定的最大范围值(即范围的终止长度) **le** 关键字代表的是小于等于运算。 当 **ge**、**le** 都未设置时，掩码长度必须完全相同规则才会匹配。

【缺省配置】 没有创建任何前缀列表

【命令模式】 全局配置模式

【缺省级别】 14

【使用指导】 **ip prefix-list** 命令用于配置 IP 前缀过滤。 前缀列表用 permit 或者 deny 关键字来决定在匹配的情况下的拒绝和接受的动作。

前缀列表被用来定义对于一个前缀的精确匹配或者范围匹配。ge 或者 le 关键字用来定义一个用于匹配的前缀的范围，提供了比单纯输入 ip-prefix 更加灵活的匹配配置。如果命令中没有 ge 或者 le 关键字，则 ip-prefix 提供了精确的前缀范围匹配。如果仅输入 ge，则匹配范围是 minimum-prefix-length 到 32。如果仅输入 le，则匹配范围是 ip-prefix 的掩码长度到 maximum-prefix-length。如果二者都有输入，则匹配范围就是从 minimum-prefix-length 到 maximum-prefix-length。即 ip-prefix 掩码、minimum-prefix-length 和 maximum-prefix-length 的关系是：ip-prefix 掩码长度 < minimum-prefix-length < maximum-prefix-length <= 32。

【配置举例】 1：对 OSPF 协议中重分发 RIP 时输出的路由分发信息按照目的 IP 进行过滤，过滤规则在关联的 IP 前缀列表中定义(只允许目的 IP 在 201.1.1.0/24 范围内的路由信息被分发出去)。

```
Ruijie# configure terminal
Ruijie(config)# ip prefix-list pre1 permit 201.1.1.0/24
Ruijie(config)# router ospf
Ruijie(config-router)# distribute-list prefix pre1 out rip
Ruijie(config-router)# end
```

【检验方法】 1：使用 **show running-config** 命令查看配置。

【提示信息】 -1：如果配置规则重复的前缀列表表项，则提示错误信息。

```
% Insertion failed with duplicate policy
```

【常见错误】 -

【平台说明】 -

7.6 ip prefix-list description

为一个前缀列表添加文字描述。
ip prefix-list *prefix-list-name* **description** *descripton-text*

删除一个前缀列表的描述。
no ip prefix-list *prefix-list-name* **description**

【参数说明】

参数	描述
prefix-list-name	前缀列表名字
descripton-text	前缀列表文字描述

【缺省配置】 没有添加前缀列表文字描述

【命令模式】 全局配置模式

【缺省级别】 14

【使用指导】 -

【配置举例】 1：为 IP 前缀列表添加文字描述 Deny routes from Net-A。

```
Ruijie# configure terminal
Ruijie(config)# ip prefix-list pre description Deny routes from Net-A
```

【检验方法】 1：使用 **show running-config** 命令查看配置。

【提示信息】 -

【常见错误】 -

【平台说明】 -

7.7 ip prefix-list sequence-number

为前缀列表启用排序功能。
ip prefix-list sequence-number

取消前缀列表的排序功能。
no ip prefix-list sequence-number

【参数说明】

参数	描述
-	-

【缺省配置】 没有启用前缀列表排序功能

【命令模式】 全局配置模式

【缺省级别】 14

【使用指导】 -

【配置举例】 1：为前缀列表启用排序功能。

```
Ruijie# configure terminal
Ruijie(config)# ip prefix-list sequence-number
```

【检验方法】 1：使用 **show running-config** 命令查看配置。

【提示信息】 -

【常见错误】 -

【平台说明】 -

7.8 key

在密钥链中定义一个密钥。
key *key-id*

删除密钥链中的密钥。
no key *key-id*

【参数说明】

参数	描述

key-id	密钥链中认证密钥的 ID，取值范围：0-2147483647

【缺省配置】 -

【命令模式】 密钥链配置模式

【缺省级别】 14

【使用指导】 **-**

【配置举例】 1：配置密钥链 ripkeys，并进入密钥链配置模式，配置密钥 1

```
Ruijie(config)# key chain ripkeys
Ruijie(config-keychain)# key 1
```

【检验方法】 1：使用 **show running-config** 命令查看配置。

【提示信息】 -

【常见错误】 -

【平台说明】 -

7.9 key chain

定义密钥链，并进入密钥链配置模式。
key chain *key-chain-name*

删除密钥链。
no key chain *key-chain-name*

【参数说明】

参数	描述
key-chain-name	密钥链名。

【缺省配置】 -

【命令模式】 全局配置模式

【缺省级别】 14

【使用指导】 要使密钥链生效，必须配置至少一个密钥。

【配置举例】 1：配置密钥链 ripkeys，并进入密钥链配置模式。

```
Ruijie(config)# key chain ripkeys
```

【检验方法】 1：使用 **show running-config** 命令查看配置。

【提示信息】 -

【常见错误】 -

【平台说明】 -

7.10 key-string

在密钥链密钥模式中指定认证串。

key-string [**0**|**7**] *text*

删除密钥认证串

no key-string

【参数说明】

参数	描述
0	指定密钥以明文显示
7	指定密钥以密文显示
text	指定的认证串字符

【缺省配置】 -

【命令模式】 密钥链密钥配置模式

【缺省级别】 14

【使用指导】 **-**

【配置举例】 1：配置密钥链 ripkeys，进入密钥链配置模式，配置密钥 1，进入密钥 1 配置模式，并定义密钥串为 abc。

```
Ruijie(config)# key chain ripkeys
Ruijie(config-keychain)# key 1
Ruijie(config-keychain-key)# key-string abc
```

【检验方法】 1：使用 **show running-config** 命令查看配置。

【提示信息】 1：如果配置明文密码长度大于 80 或密文密码长度大于 162，则提示错误信息。

```
%Error: key string too long
```

2：如果配置的密文密码不符合加密规则，如 key-string 7 123 则提示错误信息。

```
% Invalid encrypted password: 123
```

【常见错误】 -

【平台说明】 -

7.11 match community

重分布访问列表中允许的 COMMUNITY 属性路由。

match community { *community-list-number* | *community-list-name* } [**exact-match**] [{ *community-list-number* | *community-list-name* } [**exact-match**] …]

删除已有配置。

no match community { *community-list-number* | *community-list-name* } [**exact-match**] [{ *community-list-number* | *community-list-name* } [**exact-match**] …]

【参数说明】

参数	描述
community-list-number	团体列表号 标准团体列表：编号范围为 1-99 扩展团体列表：编号范围为 100-199
communitys-list-name	团体列表名字 团体列表名不超过 80 字符
exact-match	完全匹配列表

【缺省配置】 -

【命令模式】 路由图配置模式

【缺省级别】 14

【使用指导】 **match community** 命令后面可以跟多个团体列表号或者团体列表名字，但两者数目总和不大于 6。

每个 **exact-match** 关键字仅修饰前一个列表，而不是修饰所有的匹配列表。

一个路由图规则配置中，可以执行 1 个或多个的 **match** 命令和 1 个或多个的 **set** 命令。如果没有 **match** 命令，则匹配所有；如果没有 **set** 命令，则不做任何操作。

【配置举例】 1：配置路由图，针对团体属性列表 1 完全匹配的路由，设置本地优先属性为 20。

```
Ruijie(config)# ip community-list 1 permit 100:2 100:30
Ruijie(config)# route-map set_lopref
```

```
Ruijie(config-route-map)# match community 1 exact-match
Ruijie(config-route-map)# set local-preference 20
```

【检验方法】 1：使用 **show running-config** 命令查看配置。

【提示信息】 -1：如果指定的 name 型 Community-list 名字全是数字，则提示错误信息。

```
% Community-list name cannot have all digits
```

2：如果指定的 Community-list 列表名字长度超过或等于 80 字符，则提示错误信息。

```
% Community-list name lengths should be less than 80 chars
```

3：如果单条命令配置的 Community-list 列表个数超过 6 个，则提示错误信息。

```
% Match community command only support six community-list
```

4：如果配置的 Community-list 列表总个数超过 6 个，则提示错误信息。

```
% Match community can't exceed 6!
```

【常见错误】 -

【平台说明】 -

7.12 match interface

匹配下一跳出口为指定接口。

match interface *interface-type interface-number* [*…interface-type interface-number*]

删除匹配下一跳出口为指定接口的配置。

no match interface [*interface-type interface-number* [*…interface-type interface-number*]]

【参数说明】

参数	描述
interface-type	接口类型
interface-number	接口编号

【缺省配置】 -

【命令模式】 路由图配置模式

【缺省级别】 14

【使用指导】 **match interface** 命令后面可以跟多个接口。

路由信息可以从一个路由进程重分布到另外一个路由进程的功能。比如可以将 OSPF 路由域的路由重新分布后

通告到 RIP 路由域中，也可以将 RIP 路由域的路由重新分布后通告到 OSPF 路由域中。
在路由重分布中，经常通过路由图（route maps）的应用，对两个路由域之间的路由相互分布进行有条件的控制。一个路由图规则配置中，可以执行 1 个或多个的 **match** 命令和 1 个或多个的 **set** 命令。如果没有 **match** 命令，则匹配所有；如果没有 **set** 命令，则不做任何操作。
路由图的配置十分灵活，可以应用在路由重分布和策略路由的配置上。不管如何应用路由图，其配置原理是一样的，只是适用的命令集不同而已。即使同样应用在路由重分布上，不同的路由协议应用路由图，其能够使用的命令也不尽相同。

缺省情况下，删除配置时不输入接口类型、接口编号将删除所有匹配接口的配置。

【配置举例】 1：配置 OSPF 路由协议重分布 RIP 路由，要求只重分布下一跳为 GigabitEthernet 0/0 的 RIP 路由。

```
Ruijie(config)# router ospf
Ruijie(config-router)# redistribute rip subnets route-map redrip
Ruijie(config-router)# network 192.168.12.0 0.0.0.255 area 0
Ruijie(config-router)# exit
Ruijie(config)# route-map redrip permit 10
Ruijie(config-route-map)# match interface GigabitEthernet 0/0
```

【检验方法】 1：使用 **show running-config** 命令查看配置。

【提示信息】 -1：如果指定的 interface 个数超过 4 个，则提示错误信息。

```
% Match interface can't exceed 4!
```

2：如果指定的 interface 为二层口（例如二层口 GigabitEthernet 0/0），则提示错误信息。

```
% Invalid parameter: GigabitEthernet 0/0, only support layer 3 interface.
```

【常见错误】 -

【平台说明】 -

7.13 match ip address

重分布访问列表或前缀列表中允许的目标网络路由。
match ip address { *access-list-number* [*access-list-number...* | *access-list-name...*] | *access-list-name* [*access-list-number...*| *access-list-name*] | **prefix-list** *prefix-list-name* [*prefix-list-name...*] }

删除已有配置。
no match ip address [*access-list-number* [*access-list-number...* | *access-list-name...*] | *access-list-name* [*access-list-number...* | *access-list-name*] | **prefix-list** *prefix-list-name* [*prefix-list-name...*]]

【参数说明】

参数	描述
access-list-number	访问列表号。 标准访问列表号范围：1-99，1300-1999。 扩展访问列表号范围：100-199，2000-2699。
access-list-name	访问列表名字
prefix-list *prefix-list-name*	要匹配的前缀列表名字

【缺省配置】 -

【命令模式】 路由图配置模式

【缺省级别】 14

【使用指导】 **match ip address** 命令后面可以跟多个访问列表号或者访问列表名字。

路由信息可以从一个路由进程重分布到另外一个路由进程的功能。比如可以将 OSPF 路由域的路由重新分布后通告到 RIP 路由域中，也可以将 RIP 路由域的路由重新分布后通告到 OSPF 路由域中。路由的相互重分布可以在所有的 IP 路由协议之间进行。

在路由重分布中，经常通过路由图（route maps）的应用，对两个路由域之间的路由相互分布进行有条件的控制。一个路由图规则配置中，可以执行 1 个或多个的 **match** 命令和 1 个或多个的 **set** 命令。如果没有 **match** 命令，则匹配所有；如果没有 **set** 命令，则不做任何操作。

路由图的配置十分灵活，可以应用在路由重分布和策略路由的配置上。不管如何应用路由图，其配置原理是一样的，只是适用的命令集不同而已。即使同样应用在路由重分布上，不同的路由协议应用路由图，其能够使用的命令也不尽相同。

缺省情况下，删除配置时不输入列表号将删除所有列表。

【配置举例】 1：配置 OSPF 路由协议重分布 RIP 路由，要求只重分布符合访问列表 10 的 RIP 路由，在 OSPF 路由域中，该路由的类型为外部路由 type-1，初始量度值为 40。

```
Ruijie(config)# router ospf
Ruijie(config-router)# redistribute rip subnets route-map redrip
Ruijie(config-router)# network 192.168.12.0 0.0.0.255 area 0
Ruijie(config-router)# exit
Ruijie(config)# access-list 10 permit 200.168.23.0 0.0.0.255
Ruijie(config)# route-map redrip permit 10
Ruijie(config-route-map)# match ip address 10
Ruijie(config-route-map)# set metric 40
Ruijie(config-route-map)# set metric-type type-1
```

【检验方法】 1：使用 **show running-config** 命令查看配置。

【提示信息】 -1：如果指定的 ACL 名字不合法（例如 match ip address 12345），则提示错误信息。

```
% ACL name 12345 is invalid
```

2：如果之前已经配置了匹配 prefix-list，再配置匹配 ACL 则提示错误信息。

```
% Can't set access-list match with prefix-list exits!
```

3：如果之前已经配置了匹配 ACL，再配置匹配 prefix-list 则提示错误信息。

```
% Can't set prefix-list match with access-list exists!
```

4：如果单条命令指定的 ACL 个数超过 6 个，则提示错误信息。

```
% Match ip address command only support six IP access-list
```

5：如果总共配置的 ACL 个数超过 6 个，则提示错误信息。

```
% ACL can't exceed 6!
```

6：如果单条命令指定的 prefix-list 个数超过 6 个，则提示错误信息。

```
% Match ip address command only support six IP prefix-list
```

7：如果总共配置的 prefix-list 个数超过 6 个，则提示错误信息。

```
% Prefix-list can't exceed 6!
```

【常见错误】 -

【平台说明】 -

7.14 match ip next-hop

重分布下一跳 IP 地址符合访问列表或前缀列表规则的目标网络路由。

match ip next-hop { *access-list-number* [*access-list-number...* | *access-list-name...*] | *access-list-name* [*access-list-number...* | *access-list-name*] | **prefix-list** *prefix-list-name* [*prefix-list-name...*] }

删除已有配置。

no match ip next-hop [*access-list-number* [*access-list-number...* | *access-list-name...*] | *access-list-name* [*access-list-number...* | *access-list-name*] | **prefix-list** *prefix-list-name* [*prefix-list-name...*]]

【参数说明】

参数	描述
access-list-number	访问列表号 标准访问列表号范围：1-99，1300-1999。 扩展访问列表号范围：100-199，2000-2699。
access-list-name	访问列表名字
prefix-list *prefix-list-name*	要匹配的前缀列表名字

【缺省配置】 -

【命令模式】 路由图配置模式。

【缺省级别】 14

【使用指导】 **match ip next-hop** 命令后面可以跟多个访问列表号或者访问列表名字。
路由信息可以从一个路由进程重分布到另外一个路由进程的功能。 比如可以将 OSPF 路由域进程重分布到另外一个路由进程的功能。比如可以将 OSPF 路由域的路由重新分布后通告到 RIP 路由域中，也可以将 RIP 路由域的路由重新分布后通告到 OSPF 路由域中。路由的相互重分布可以在所有的 IP 路由协议之间进行。
在路由重分布中，经常通过路由图（route maps）的应用，对两个路由域之间的路由相互分布进行有条件的控制。一个路由图规则配置中，可以执行 1 个或多个的 **match** 命令和 1 个或多个的 **set** 命令。如果没有 **match** 命令，则匹配所有；如果没有 **set** 命令，则不做任何操作。

缺省情况下，删除配置时不输入列表号将删除所有列表。

【配置举例】 1：配置 OSPF 路由协议重分布 RIP 路由。只要 RIP 路由的下一跳地址符合访问列表 10 或 20，OSPF 就允许其重分布。

```
Ruijie(config)# router ospf
Ruijie(config-router)# redistribute rip subnets route-map redrip
Ruijie(config-router)# network 192.168.12.0 0.0.0.255 area 0
Ruijie(config-router)# exit
Ruijie(config)# access-list 10 permit host 192.168.10.1
Ruijie(config)# access-list 20 permit host 172.16.20.1
Ruijie(config)# route-map redrip permit 10
Ruijie(config-route-map)# match ip next-hop 10 20
```

【检验方法】 1：使用 **show running-config** 命令查看配置。

【提示信息】 -1：如果指定的 ACL 名字不合法（例如 match ip next-hop 12345），则提示错误信息。

```
% ACL name 12345 is invalid
```

2：如果之前已经配置了匹配 prefix-list，再配置匹配 ACL 则提示错误信息。

```
% Can't set access-list match with prefix-list exits!
```

3：如果之前已经配置了匹配 ACL，再配置匹配 prefix-list 则提示错误信息。

```
% Can't set prefix-list match with access-list exists!
```

4：如果单条命令指定的 ACL 个数超过 6 个，则提示错误信息。

```
% Match ip next-hop command only support six IP access-list
```

5：如果总共配置的 ACL 个数超过 6 个，则提示错误信息。

```
% ACL can't exceed 6!
```

6：如果单条命令指定的 prefix-list 个数超过 6 个，则提示错误信息。

```
% Match ip next-hop command only support six IP prefix-list
```

7：如果总共配置的 prefix-list 个数超过 6 个，则提示错误信息。

```
% Prefix-list can't exceed 6!
```

【常见错误】 -

【平台说明】 -

7.15 match ip route-source

重分布路由源 IP 地址符合访问列表或前缀列表规则的目标网络路由。

match ip route-source { *access-list-number* [*access-list-number...* | *access-list-name...*] | *access-list-name* [*access-list-number...* | *access-list-name*] | **prefix-list** *prefix-list-name* [*prefix-list-name...*] }

删除已有配置。

no match ip route-source [*access-list-number* [*access-list-number...* | *access-list-name...*] | *access-list-name* [*access-list-number...* | *access-list-name*] | **prefix-list** *prefix-list-name* [*prefix-list-name...*]]

【参数说明】

参数	描述
access-list-number	访问列表号
access-list-name	访问列表名字
prefix-list *prefix-list-name*	要匹配的前缀列表名字

【缺省配置】 -

【命令模式】 路由图配置模式

【缺省级别】 14

【使用指导】 **match ip route-source** 命令后面可以跟多个访问列表号。

路由信息可以从一个路由进程重分布到另外一个路由进程的功能。比如可以将 OSPF 路由域的路由重新分布后通告到 RIP 路由域中，也可以将 RIP 路由域的路由重新分布后通告到 OSPF 路由域中。路由的相互重分布可以在所有的 IP 路由协议之间进行。

在路由重分布中，经常通过路由图（route maps）的应用，对两个路由域之间的路由相互分布进行有条件的控制。一个路由图规则配置中，可以执行 1 个或多个的 **match** 命令和 1 个或多个的 **set** 命令。如果没有 **match** 命令，则匹配所有；如果没有 **set** 命令，则不做任何操作。

缺省情况下，删除配置时不输入列表号将删除所有列表。

【配置举例】 1：配置 OSPF 路由协议重分布 RIP 路由。只要 RIP 路由的路由源 IP 地址符合访问列表 5，OSPF 就允许其重分布。

```
Ruijie(config)# router ospf
Ruijie(config-router)# redistribute rip subnets Ruijie(config-router)# route-map redrip
Ruijie(config-router)# network 192.168.12.0 0.0.0.255 area 0
Ruijie(config-router)# exit
Ruijie(config)# access-list 5 permit host 192.168.100.1
Ruijie(config)# route-map redrip permit 10
Ruijie(config-route-map)# match ip route-source 5
```

【检验方法】 1：使用 **show running-config** 命令查看配置。

【提示信息】 -1：如果指定的 ACL 名字不合法（例如 match ip route-source 12345），则提示错误信息。

```
% ACL name 12345 is invalid
```

2：如果之前已经配置了匹配 prefix-list，再配置匹配 ACL 则提示错误信息。

```
% Can't set access-list match with prefix-list exits!
```

3：如果之前已经配置了匹配 ACL，再配置匹配 prefix-list 则提示错误信息。

```
% Can't set prefix-list match with access-list exists!
```

4：如果单条命令指定的 ACL 个数超过 6 个，则提示错误信息。

```
% Match ip route-source command only support six IP access-list
```

5：如果总共配置的 ACL 个数超过 6 个，则提示错误信息。

```
% ACL can't exceed 6!
```

6：如果单条命令指定的 prefix-list 个数超过 6 个，则提示错误信息。

```
% Match ip route-source command only support six IP prefix-list
```

7：如果总共配置的 prefix-list 个数超过 6 个，则提示错误信息。

```
% Prefix-list can't exceed 6!
```

【常见错误】 -

【平台说明】 -

7.16 match length

配置基于 IP 数据包长度进行策略路由。
match length *min-length max-length*

删除已有配置
no match length *min-length max-length*

【参数说明】

参数	描述
min-length	IP 数据包最小长度，取值范围：0~65535
max-length	IP 数据包最大长度，取值范围：0~65535

【缺省配置】 -

【命令模式】 路由图配置模式

【缺省级别】 14

【使用指导】 策略路由是一种比基于目标网络进行路由更加灵活的数据包路由转发机制。应用了策略路由，本设备将通过路由图决定如何对需要路由的数据包进行处理，路由图决定了一个数据包的下一跳转发设备。
应用策略路由，必须要指定策略路由使用的路由图，并且要创建路由图。一个路由图由很多条策略组成，每个策略都定义了 1 个或多个的匹配规则和对应操作。一个接口应用策略路由后，将对该接口接收到的所有包进行检查，不符合路由图任何策略的数据包将按照通常的路由转发进行处理，符合路由图中某个策略的数据包就按照该策略中定义的操作进行处理。
如果需要将交互式流量和大批量流量，分别走不同的路径，就可以使用基于数据包大小的策略路由。

【配置举例】 1：在 GigabitEthernet 1/0 启用策略路由，将数据包小于 500 字节的流量，从 GigabitEthernet 1/2 接口发送出去。

```
Ruijie(config)# interface GigabitEthernet 1/0
Ruijie(config-if)# ip policy route-map smallpak
Ruijie(config-if)# exit
Ruijie(config)# route-map smallpak permit 10
Ruijie(config-route-map)# match length 0 500
Ruijie(config-route-map)# set interface GigabitEthernet 1/2
```

【检验方法】 1：使用 **show running-config** 命令查看配置。

【提示信息】 -

【常见错误】 -

【平台说明】

7.17 match metric

匹配路由的度量值。
match metric *metric*

删除匹配路由度量值。
no match metric

【参数说明】

参数	描述
metric	路由量度值，取值范围：0-4294967295。

【缺省配置】 -

【命令模式】 路由图配置模式

【缺省级别】 14

【使用指导】 路由信息可以从一个路由进程重分布到另外一个路由进程的功能。比如可以将 OSPF 路由域的路由重新分布后通告到 RIP 路由域中，也可以将 RIP 路由域的路由重新分布后通告到 OSPF 路由域中。路由的相互重分布可以在所有的 IP 路由协议之间进行。
在路由重分布中，经常通过路由图（route maps）的应用，对两个路由域之间的路由相互分布进行有条件的控制。一个路由图规则配置中，可以执行 1 个或多个的 **match** 命令和 1 个或多个的 **set** 命令。如果没有 **match** 命令，则匹配所有；如果没有 **set** 命令，则不做任何操作。

【配置举例】 1：OSPF 路由协议重分布 RIP 路由。只有量度值为 10 的 RIP 路由，OSPF 才会重分布。

```
Ruijie(config)# router ospf
Ruijie(config-router)# redistribute rip subnets route-map redist-rip
Ruijie(config-router)# network 192.168.12.0 0.0.0.255 area 0
Ruijie(config-router)# exit
Ruijie(config)# route-map redist-rip permit 10
Ruijie(config-route-map)# match metric 10
```

【检验方法】 1：使用 **show running-config** 命令查看配置。

【提示信息】 -

【常见错误】 -

【平台说明】 -

7.18 match route-type

匹配路由的路由类型。
match route-type { **static | connect | rip | local | internal | external** [**type-1 | type-2**] }

删除路由类型的匹配。
no match route-type [**static | connect | rip | local | internal | external** [**type-1 | type-2**]]

【参数说明】

参数	描述
static	静态路由
connect	直连路由
rip	RIP 路由
local	本地生成的路由
Internal	OSPF 的内部路由
external	外部路由(OSPF 的外部路由)
type-1 | **type-2**	OSPF 的类型 1 或类型 2 外部路由

【缺省配置】 -

【命令模式】 路由图配置模式

【缺省级别】 14

【使用指导】 路由信息可以从一个路由进程重分布到另外一个路由进程的功能。比如可以将 OSPF 路由域的路由重新分布后通告到 RIP 路由域中，也可以将 RIP 路由域的路由重新分布后通告到 OSPF 路由域中。路由的相互重分布可以在所有的 IP 路由协议之间进行。
在路由重分布中，经常通过路由图（route maps）的应用，对两个路由域之间的路由相互分布进行有条件的控制。一个路由图规则配置中，可以执行 1 个或多个的 **match** 命令和 1 个或多个的 **set** 命令。如果没有 **match** 命令，则匹配所有；如果没有 **set** 命令，则不做任何操作。

【配置举例】 1：配置 RIP 路由协议重分布 OSPF 路由。RIP 只重分布 OSPF 路由域的内部路由。

```
Ruijie(config)# router rip
Ruijie(config-router)# redistribute ospf route-map redrip
Ruijie(config-router)# network 192.168.12.0
Ruijie(config-router)# exit
Ruijie(config)# route-map redrip permit 10
Ruijie(config-route-map)# match route-type internal
```

【检验方法】 1：使用 **show running-config** 命令查看配置。

【提示信息】 -

【常见错误】 -

【平台说明】 -

7.19 match tag

匹配路由的标记。
match tag *tag* [*…tag*]

删除匹配路由的标记。
no match tag [*tag* [*…tag*]]

【参数说明】

参数	描述
tag	路由的标记值。 缺省请况下，删除配置时不输入可选参数，将删除所有匹配的路由的标记。

【缺省配置】 -

【命令模式】 路由图配置模式

【缺省级别】 14

【使用指导】 **match tag** 命令后面可以跟多个 tag。
路由信息可以从一个路由进程重分布到另外一个路由进程。比如可以将 OSPF 路由域的路由重新分布后通告到 RIP 路由域中，也可以将 RIP 路由域的路由重新分布后通告到 OSPF 路由域中。路由的相互重分布可以在所有的 IP 路由协议之间进行。
在路由重分布中，经常通过路由图（route maps）的应用，对两个路由域之间的路由相互分布进行有条件的控制。一个路由图规则配置中，可以执行 1 个或多个的 **match** 命令和 1 个或多个的 **set** 命令。如果没有 **match** 命令，则匹配所有；如果没有 **set** 命令，则不做任何操作。

【配置举例】 1：配置 RIP 路由协议重分布 OSPF 路由。RIP 只重分布 OSPF 路由域中标记为 50 和 80 的路由。

```
Ruijie(config)# router rip
Ruijie(config-router)# redistribute ospf 100 route-map redrip
Ruijie(config-router)# network 192.168.12.0
Ruijie(config-router)# exit
Ruijie(config)# route-map redrip permit 10
```

```
Ruijie(config-route-map)# match tag 50 80
```

【检验方法】 1：使用 **show running-config** 命令查看配置。

【提示信息】 -1：如果总共配置的 tag 个数超过 4 个，则提示错误信息。

```
% Match tag can't exceed 4!
```

【常见错误】 -

【平台说明】 -

7.20 memory-lack exit-policy

内存到达 lower 线后，指定上层路由协议的退出策略。
memory-lack exit-policy { **ospf** | **Rip** }

恢复默认退出策略。
no memory-lack exit-policy

【参数说明】

参数	描述
ospf	指定内存不足时 OSPF 协议优先退出
rip	指定内存不足时 RIP 协议优先退出

【缺省配置】 缺省退出策略：退出内存占用最大的路由协议

【命令模式】 全局配置模式

【缺省级别】 14

【使用指导】 内存达到 lower 线时，为保护系统的其它协议运行，将关闭一个路由协议，释放出内存资源。

用户应当知道哪些路由协议支撑了其网络的主要业务，在内存不足的情况下，关闭一个最不重要的协议，以便在这种极端情况下保护主要业务的运行。

对于未开启的路由协议，指定为优先退出的路由协议，并不能帮助系统获得足够的内存资源。

指定了该策略仅仅是一定程度上保护系统内存不足时的重要网络业务，若内存进一步消耗，所有路由协议都将退出并停止运行。

【配置举例】 -

【检验方法】 1：使用 **show running-config** 命令查看配置。

【提示信息】 -

【常见错误】 -

【平台说明】 -

7.21 route-map

定义路由图，并进入路由图配置模式。
route-map *route-map-name* [**permit** | **deny**] [*sequence-number*]

删除指定路由图的定义。
no route-map *route-map-name* [{ **permit** | **deny** } *sequence-number*]

【参数说明】

参数	描述
route-map-name	给路由图定义一个便于记忆的名字。路由进程重分布配置命令是通过该名字引用路由图的。一个路由图可以定义多个路由图策略，一个路由图策略对应一个序号
permit	如果定义了 permit 关键字，又符合 match 定义的匹配规则。则 set 命令对重分布路由进行控制；对于策略路由，set 命令将对数据包转发进行控制。并退出路由图的操作。 如果定义了 permit 关键字，而不符合 match 定义的匹配规则。则将进入第二个路由图策略进行操作。直到最终执行了 set 命令
deny	如果定义了 deny 关键字，又符合 match 定义的匹配规则。则不会执行任何操作，该路由图策略不允许进行路由重分布或策略路由，而且退出路由图操作。 如果定义了 deny 关键字，而不符合 match 定义的匹配规则。则将进入下一个路由图策略进行操作。直到最终执行了 set 命令。
sequence-number	路由图策略对应的序号。低序号的策略优先得到使用，因此需要注意序号的设置。

【缺省配置】 缺省没有配置路由图

【命令模式】 全局配置模式

【缺省级别】 14

【使用指导】 目前 RGOS 软件的路由图主要用在两个地方：路由重分布控制、策略路由。
路由重分布控制路由信息可以从一个路由进程重分布到另外一个路由进程的功能。比如可以将 OSPF 路由域的

路由重新分布后通告到 RIP 路由域中，也可以将 RIP 路由域的路由重新分布后通告到 OSPF 路由域中。路由的相互重分布可以在所有的 IP 路由协议之间进行。

在路由重分布中，经常通过路由图（route maps）的应用，对两个路由域之间的路由相互分布进行有条件的控制。一个路由图规则配置中，可以执行 1 个或多个的 **match** 命令和 1 个或多个的 **set** 命令。如果没有 **match** 命令，则匹配所有；如果没有 **set** 命令，则不做任何操作。

当配置路由图时，路由图序号的使用需要注意以下几点：

- 如果是创建第一个路由图策略，没有指定 *sequence-number*，缺省为 10；
- 如果只存在一个路由图策略，没有指定 *sequence-number*，不会创建新的路由图策略，直接进入已有的路由图策略进行配置；
- 如果存在多个路由图策略，操作必须要指定序号，否则将出现错误提示。

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

```
Ruijie(config)# router ospf
Ruijie(config-router)# redistribute rip subnets route-map redrip
Ruijie(config-router)# network 192.168.12.0 0.0.0.255 area 0
Ruijie(config-router)# exit
Ruijie(config)# route-map redrip permit 10
Ruijie(config-route-map)# match metric 4
Ruijie(config-route-map)# set metric 40
Ruijie(config-route-map)# set metric-type type-1
Ruijie(config-route-map)# set tag 40
```

【检验方法】 1：使用 **show running-config** 命令查看配置。

【提示信息】 -1：如果指定的 route-map 名字长度超过 32 个，则提示错误信息。

```
% Route-map name string length can not exceed 32.
```

【常见错误】 -

【平台说明】 -

7.22 send-lifetime

配置密钥链发送方向的生存期。

send-lifetime *start-time* { **infinite |** *end-time* **| duration** *seconds* }

删除密钥链接收方向的生存期。

no send-lifetime

【参数说明】

参数	描述
start-time	指定生存期的开始时间
infinite	该参数表示该密钥从开始时间一直有效
end-time	密钥有效期结束时间，必须晚于 start-time
duration *seconds*	指定有效期从 start-time 开始的持续时间，取值范围：1-2147483646

【缺省配置】 没有定义密钥链发送生存期

【命令模式】 密钥链密钥配置模式

【缺省级别】 14

【使用指导】 -

【配置举例】 1： 配置密钥链 kc，进入密钥链配置模式，配置密钥 1，进入密钥 1 配置模式，并定义密钥链接收生存期

```
Ruijie(config)#key chain kc
Ruijie(config-keychain)#key 1
Ruijie(config-keychain-key)#key-string World
Ruijie(config-keychain-key)#send-lifetime 16:30:00 Oct 1 2010 duration 43200
```

【检验方法】 1：使用 **show running-config** 命令查看配置。

【常见错误】 -

【平台说明】 -

7.23 set default interface

对匹配 match 规则并且没有明确路由出口的数据包指定缺省转发接口。

set default interface *interface-type interface-number* [*…interface-type interface-number*]

删除设置的缺省转发接口。

no set default interface *interface-type interface-number* [*…interface-type interface-number*]

【参数说明】

参数	描述
interface-type	接口类型
interface-number	接口编码

【缺省配置】 -

【命令模式】 路由图配置模式

【缺省级别】 14

【使用指导】 **set default interface** 命令后面可以跟多个接口。
策略路由是一种比基于目标网络进行路由更加灵活的数据包路由转发机制。应用了策略路由，设备将通过路由图决定如何对需要路由的数据包进行处理，路由图决定了一个数据包的下一跳转发设备。
应用策略路由，必须要指定策略路由使用的路由图，并且要创建路由图。一个路由图由很多条策略组成，每个策略都定义了 1 个或多个的匹配规则和对应操作。一个接口应用策略路由后，将对该接口接收到的所有包进行检查，不符合路由图任何策略的数据包将按照通常的路由转发进行处理，符合路由图中某个策略的数据包就按照该策略中定义的操作进行处理。
如果第一个定义的接口状态变为 down，将尝试第二个 **set** 命令设置的接口。一个路由图策略中可以有多个 **set** 操作。

【配置举例】 1：在 serial 1/0 启用策略路由，当该接口接收到数据包小于 500 字节的流量，而且路由表中没有明确的路由，将从 GigabitEthernet 1/0 接口发送数据包。

```
Ruijie(config)# interface serial 1/0
Ruijie(config-if)# ip policy route-map smallpak
Ruijie(config-if)# exit
Ruijie(config)# route-map smallpak permit 10
Ruijie(config-route-map)# match length 0 500
Ruijie(config-route-map)# set default interface GigabitEthernet 1/0
```

【检验方法】 1：使用 **show running-config** 命令查看配置。

【提示信息】

1：如果指定的 interface 个数超过 4 个，则提示错误信息。

```
% Set default interface can't exceed 4!
```

2：如果指定的 interface 为二层口（例如二层口 GigabitEthernet 0/0），则提示错误信息。

```
% Invalid parameter: GigabitEthernet 0/0, only support layer 3 interface.
```

【常见错误】 -

【平台说明】 -

7.24 set interface

对匹配 match 规则的报文指定转发接口。
set interface *interface-type interface-number* [*…interface-type interface-number*]

删除设置转发接口的配置。

no set interface *interface-type interface-number* [*…interface-type interface-number*]

【参数说明】

参数	描述
interface-type	接口类型
interface-number	接口编号

【缺省配置】 -

【命令模式】 路由图配置模式

【缺省级别】 14

【使用指导】 **set interface** 命令后面可以配置多个接口。

策略路由是一种比基于目标网络进行路由更加灵活的数据包路由转发机制。应用了策略路由，设备将通过路由图决定如何对需要路由的数据包进行处理，路由图决定了一个数据包的下一跳转发设备。

应用策略路由，必须要指定策略路由使用的路由图，并且要创建路由图。一个路由图由很多条策略组成，每个策略都定义了 1 个或多个的匹配规则和对应操作。一个接口应用策略路由后，将对该接口接收到的所有包进行检查，不符合路由图任何策略的数据包将按照通常的路由转发进行处理，符合路由图中某个策略的数据包就按照该策略中定义的操作进行处理。

如果第一个定义的接口状态变为 down，将尝试第二个 **set** 命令设置的接口。一个路由图策略中可以有多个 **set** 操作。

如果将接口设置为 null 0，数据包将被丢弃。

【配置举例】 1：在 serial 1/0 启用策略路由，将接口收到的小于 500 字节的数据包，从 GigabitEthernet 0/0 接口发送出去。

```
Ruijie(config)#interface serial 1/0
Ruijie(config-if)#ip policy route-map smallpak
Ruijie(config)#route-map smallpak permit 10
Ruijie(config-route-map)#match length 0 500
Ruijie(config-route-map)#set interface GigabitEthernet 0/0
```

【检验方法】 1：使用 **show running-config** 命令查看配置。

【提示信息】

1：如果指定的 interface 个数超过 4 个，则提示错误信息。

```
% Set interface can't exceed 4!
```

2：如果指定的 interface 为二层口（例如二层口 GigabitEthernet 0/0），则提示错误信息。

```
% Invalid parameter: GigabitEthernet 0/0, only support layer 3 interface.
```

【常见错误】 -

【平台说明】 -

7.25 set ip default next-hop

对匹配 match 规则的数据包指定默认下一跳 IP 地址。
set ip default next-hop *ip-address* [*weight*] [*…ip-address* [*weight*]]

删除设置默认下一跳的配置。
no set ip default next-hop [*ip-address* [*weight*] [*…ip-address* [*weight*]]]

【参数说明】

参数	描述
ip-address	下一跳 IP 地址
weight	本下一跳的权重

【缺省配置】 -

【命令模式】 路由图配置模式

【缺省级别】 14

【使用指导】 本条 set 命令有两种运行模式：WCMP 负载均衡运行模式，非 WCMP 负载均衡运行模式。在前一种运行模式下，系统将根据用户输入的 weight 数值对流量进行 WCMP 负载均衡。
set ip default next-hop 命令后面可以跟多个 IP 地址，最多不超过 32 个。
如果在 ip address 后增加 weight 数值，则最多可以配置不超过 4 个的 nexthop 地址。

⚠ 在任何一个 next-hop 后跟随 weight 数值，将使得本 set 命令的运行模式自动切换为 WCMP 负载均衡运行模式。在 WCMP 负载均衡运行模式下，对于那些没有配置对应 weight 的 nexthop 地址，其 weight 缺省为 1。

set ip next-hop 和 **set ip default next-hop** 命令的区别在于： 配置了 **set ip next-hop** 命令的系统在转发报文优先使用策略路由；配置了 **set ip default next-hop** 的系统会在转发报文时优先使用路由转发表。
使用本条命令为特定用户提供设置一条定制默认路由的功能。如果软件上无法为待转发的报文找到转发路由，则将该报文转发到本命令配置的下一跳(nexthop)上。
应用策略路由，必须要指定策略路由使用的路由图，并且要创建路由图。一个路由图由很多条策略组成，每个策略都定义了 1 个或多个的匹配规则和对应操作。一个接口应用策略路由后，将对该接口接收到的所有包进行检查，不符合路由图任何策略的数据包将按照通常的路由转发进行处理，符合路由图中某个策略的数据包就按照该策略中定义的操作进行处理。
一个路由图策略中可以有多个 set 操作。

【配置举例】 1：在同步接口 1 上接收的从 1.1.1.1 发出的报文，如果软件找不到转发路由时，就被转发到设备 6.6.6.6 去；而接收到的从 2.2.2.2 发出的报文，如果软件找不到转发路由时，就被转发到设备 7.7.7.7 去。其他的报文如果软件找不到转发路由时就丢弃处理。

```
Ruijie(config)#access-list 1 permit 1.1.1.1 0.0.0.0
Ruijie(config)#access-list 2 permit 2.2.2.2 0.0.0.0
Ruijie(config)#interface async 1
Ruijie(config-if)#ip policy route-map equal-access
Ruijie(config)#route-map equal-access permit 10
Ruijie(config- route-map)#match ip address 1
Ruijie(config-route-map)#set ip default next-hop 6.6.6.6
Ruijie(config)#route-map equal-access permit 20
Ruijie(config-route-map)#match ip address 2
Ruijie(config-route-map)#set ip default next-hop 7.7.7.7
Ruijie(config)#route-map equal-access permit 30
Ruijie(config- route-map)#set default interface null 0
```

【检验方法】 1：使用 **show running-config** 命令查看配置。

【提示信息】 -

【常见错误】 -

【平台说明】 -

7.26 set ip dscp

对匹配 match 规则的报文设置 DSCP 值。
set ip dscp *dscp_value*

删除设置 DSCP 值。
no set ip dscp

【参数说明】

参数	描述
dscp_value	设置 IP 报文中 IP 头 DSCP 值

【缺省配置】 -

【命令模式】 路由图配置模式

【缺省级别】 14

【使用指导】 -

【配置举例】 -

【检验方法】 1：使用 **show running-config** 命令查看配置。

【提示信息】 -1：如果之前已经配置了 set ip tos/precedence，则提示错误信息。

```
% Route-map: can not set ip dscp.
% Remove set ip tos/precedence clause before set ip dscp.
```

【常见错误】 -

【平台说明】 -

7.27 set ip next-hop

对匹配 match 规则的数据包指定下一跳 IP 地址。

set ip next-hop *ip-address* [*weight*] [*…ip-address* [*weight*]]

删除设置下一跳 IP。

no set ip next-hop [*ip-address* [*weight*] [*…ip-address* [*weight*]]]

【参数说明】

参数	描述
ip-address	下一跳 IP 地址
weight	本下一跳的权重

【缺省配置】 -

【命令模式】 路由图配置模式

【缺省级别】 14

【使用指导】 本命令仅用于策略路由配置。

本条 **set** 命令有两种运行模式：WCMP 负载均衡运行模式，非 WCMP 负载均衡运行模式。在前一种运行模式下，系统将根据用户输入的 weight 数值对流量进行 WCMP 负载均衡。

set ip next-hop 命令后面可以跟多个 IP 地址，最多不超过 32 个。

如果在 ip address 后增加 weight 数值，则最多可以配置不超过 4 个的 nexthop 地址。

在任何一个 next-hop 后跟随 weight 数值，将使得本 **set** 命令的运行模式自动切换为 WCMP 负载均衡运行模式。在 WCMP 负载均衡运行模式下，对于哪些没有配置对应 weight 的 nexthop 地址，其 weight 缺

省为 1。

策略路由是一种比基于目标网络进行路由更加灵活的数据包路由转发机制。应用了策略路由，本设备将通过路由图决定如何对需要路由的数据包进行处理，路由图决定了一个数据包的下一跳转发设备。
应用策略路由，必须要指定策略路由使用的路由图，并且要创建路由图。一个路由图由很多条策略组成，每个策略都定义了 1 个或多个的匹配规则和对应操作。一个接口应用策略路由后，将对该接口接收到的所有包进行检查，不符合路由图任何策略的数据包将按照通常的路由转发进行处理，符合路由图中某个策略的数据包就按照该策略中定义的操作进行处理。
一个路由图策略中可以有多个 **set** 操作。

【配置举例】 1：在 serial 1/0 上启用策略路由。如果接口接收到源地址在 10.0.0.0/8 范围内的数据包，将发送到 192.168.100.1；源网络为 172.16.0.0/16 范围内的数据包的流量，将发送到 172.16.100.1；其余的数据流量将全部丢弃。

```
Ruijie(config)#interface serial 1/0
Ruijie(config-if)#ip policy route-map load-balance
Ruijie(config)#access-list 10 permit 10.0.0.0 0.255.255.255
Ruijie(config)#access-list 20 permit 172.16.0.0 0.0.255.255
Ruijie(config)#route-map load-balance permit 10
Ruijie(config-route-map)#match ip address 10
Ruijie(config-route-map)#set ip next-hop 192.168.100.1
Ruijie(config)#route-map load-balance permit 20
Ruijie(config-route-map)#match ip address 20
Ruijie(config-route-map)#set ip next-hop 172.16.100.1
Ruijie(config)#route-map load-balance permit 30
Ruijie(config-route-map)#set interface Null 0
```

【检验方法】 1：使用 **show running-config** 命令查看配置。

【提示信息】 -

【常见错误】 -

【平台说明】 -

7.28 set ip next-hop verify-availability

指定确认下一跳 IP 地址的可达性。
set ip next-hop verify-availability *ip-address* [**track** *track-obj-number*]

删除已有配置。
no set ip next-hop verify-availability *ip-address* [**track** *track-obj-number*]

【参数说明】

参数	描述
ip-address	下一跳 IP 地址
track	通过 Track 方式检测以判断下一跳是否生效
track-obj-number	跟踪对象编号

【缺省配置】 -

【命令模式】 路由图配置模式

【缺省级别】 14

【使用指导】 本命令仅用于策略路由配置。

【配置举例】 1：指定确认下一跳 192.168.1.2 的可达性，跟踪对象编号为 1。

```
Ruijie(config)# route-map rmap permit 10
Ruijie(config-route-map)# set ip  next-hop verify-availability 192.168.1.2 track 1
```

【检验方法】 1：使用 **show running-config** 命令查看配置。

【提示信息】 -

【常见错误】 -

【平台说明】 -

7.29 set ip precedence

对匹配 match 规则的报文设置 IP 头的优先级。

set ip precedence { *number* | **critical** | **flash** | **flash-override** | **immediate** | **internet** | **network** | **priority** | **routine** }

删除设置 IP 头的优先级的配置。

no set ip precedence

【参数说明】

参数	描述
number	用数字表示 IP 头的优先级。取值范围 0-7。 7：critical 6：flash 5：flash-override 4：immediate

	3：internet 2：network 1：priority 0：routine
critical | **flash** | **flash-override** | **immediate** | **internet** | **network** | **priority** | **routine**	IP 头的优先级。

【缺省配置】 -

【命令模式】 路由图配置模式

【缺省级别】 14

【使用指导】 经常设置 IP 报文头中的优先级值来使策略路由选路的 IP 报文进行不同优先级的传送。
在路由图配置规则中，可以配置多个 **set ip precedence** 命令，但是只有最后一个设置有效，并且只要是策略路由匹配的报文 IP 报头都会设置指定的优先级。

【配置举例】 1：对从接口 GigabitEthernet 0/0 进来的源地址为 192.168.217.68 的报文设置 precedence 为 4。

```
Ruijie(config)#access-list 1 permit 192.168.217.68 0.0.0.0
Ruijie(config)#route-map name
Ruijie(config-route-map)#match ip address 1
Ruijie(config-route-map)#set ip precedence 4
Ruijie(config)#interface GigabitEthernet 0/0
Ruijie(config-if)#ip policy route-map name
```

【检验方法】 1：使用 **show running-config** 命令查看配置。

【提示信息】 -1：如果之前已经配置了 set ip dscp，则提示错误信息。

```
% Route-map: can not set ip precedence.
% Remove set ip dscp clause before set ip precedence.
```

【常见错误】 -

【平台说明】 -

7.30 set ip tos

对匹配 match 规则的报文设置报文 IP 头的 TOS。
set ip tos { *number* | **max-reliability | max-throughput | min-delay | min-monetary-cost | normal** }

删除已有配置。

no set ip tos

【参数说明】

参数	描述
number	用数字表示 IP 头的 TOS。取值范围 0-15。
max-reliability | max-throughput | min-delay | min-monetary-cost | normal	IP 头的优先级。与数字的对应关系： **max-reliability**：2 **max-throughput**：4 **min-delay**：8 **min-monetary-cost**：1 **normal**：0

【缺省配置】 -

【命令模式】 路由图配置模式

【缺省级别】 14

【使用指导】 经常通过设置 IP 报文头中的 TOS 值对使用策略路由选路的 IP 报文进行不同服务质量的传送。
只要是策略路由匹配的报文 IP 报头都会被设置上指定的 TOS 值。

【配置举例】 1：对从接口 GigabitEthernet 0/0 进来的源地址为 192.168.217.68 的报文设置 tos 为 4。

```
Ruijie(config)#access-list 1 permit 192.168.217.68 0.0.0.0
Ruijie(config)#route-map name
Ruijie(config-route-map)#match ip address 1
Ruijie(config-route-map)#set ip tos 4
Ruijie(config)#interface GigabitEthernet 0/0
Ruijie(config-if)#ip policy route-map name
```

【检验方法】 1：使用 **show running-config** 命令查看配置。

【提示信息】 -1：如果之前已经配置了 set ip dscp，则提示错误信息。

```
% Route-map: can not set ip tos.
% Remove set ip dscp clause before set ip tos.
```

【常见错误】 -

【平台说明】 -

7.31 set level

对匹配 match 规则的路由指明要导入的目标区域类型。

set level { **stub-area** | **backbone** }

删除已有配置。

no set level

【参数说明】

参数	描述
stub-area	指定重分发路由通告到 OSPF Stub Area
backbone	指定重分发路由通告到 OSPF 骨干区

【缺省配置】 -

【命令模式】 路由图配置模式

【缺省级别】 14

【使用指导】 -

【配置举例】 1：OSPF 路由协议重分布 RIP 路由到 backbone 区域。

```
Ruijie(config)# router ospf
Ruijie(config-router)# redistribute rip subnets route-map redrip
Ruijie(config-router)# network 192.168.12.0 0.0.0.255 area 0
Ruijie(config-router)# exit
Ruijie(config)# route-map redrip permit 10
Ruijie(config-route-map)# set level backbone
```

【检验方法】 1：使用 **show running-config** 命令查看配置。

【提示信息】 -

【常见错误】 -

【平台说明】 -

7.32 set metric

对匹配 match 规则的路由设置度量值。

set metric [+ *metric-value* | **-** *metric-value* | *metric-value*]

删除已有配置。

no set metric

【参数说明】

参数	描述
+	增加（在原路由的 metric 上增加）
-	减少（在原路由的 metric 上减少）
metric-value	设置重分布路由的量度，取值范围：0-4294967295

【缺省配置】 -

【命令模式】 路由图配置模式

【缺省级别】 14

【使用指导】 路由量度值会影响路由的选择，因此需要根据实际的网络拓扑，谨慎地进行设置。其中进行 set metric、以及‘+’或‘-’metric 的操作应注意各个路由协议的上下限值。如对于 RIP 协议重分布其它协议路由时，metric 增减后的结果范围为 1-16。

路由信息可以从一个路由进程重分布到另外一个路由进程的功能。比如可以将 OSPF 路由域的路由重新分布后通告到 RIP 路由域中，也可以将 RIP 路由域的路由重新分布后通告到 OSPF 路由域中。路由的相互重分布可以在所有的 IP 路由协议之间进行。

在路由重分布中，经常通过路由图（route maps）的应用，对两个路由域之间的路由相互分布进行有条件的控制。一个路由图规则配置中，可以执行 1 个或多个的 **match** 命令和 1 个或多个的 **set** 命令。如果没有 **match** 命令，则匹配所有；如果没有 **set** 命令，则不做任何操作。

【配置举例】 1：配置 OSPF 路由协议重分布 RIP 路由，并将重分布路由的初始量度值设置为 40。

```
Ruijie(config)# router ospf
Ruijie(config-router)# redistribute rip subnets route-map redrip
Ruijie(config-router)# network 192.168.12.0 0.0.0.255 area 0
Ruijie(config-router)# exit
Ruijie(config)# route-map redrip permit 10
Ruijie(config-route-map)# set metric 40
```

【检验方法】 1：使用 **show running-config** 命令查看配置。

【提示信息】 -

【常见错误】 -

【平台说明】 -

7.33 set metric-type

对匹配 match 规则的路由设置度量值类型。
set metric-type *type*

删除设置路由度量值类型。
no set metric-type

【参数说明】

参数	描述
type	设置重分布路由的类型。 OSPF 重分布路由的类型缺省为 type-2。

【缺省配置】 -

【命令模式】 路由图配置模式

【缺省级别】 14

【使用指导】 路由信息可以从一个路由进程重分布到另外一个路由进程的功能。比如可以将 OSPF 路由域的路由重新分布后通告到 RIP 路由域中，也可以将 RIP 路由域的路由重新分布后通告到 OSPF 路由域中。路由的相互重分布可以在所有的 IP 路由协议之间进行。
在路由重分布中，经常通过路由图（route maps）的应用，对两个路由域之间的路由相互分布进行有条件的控制。一个路由图规则配置中，可以执行 1 个或多个的 **match** 命令和 1 个或多个的 **set** 命令。如果没有 **match** 命令，则匹配所有；如果没有 **set** 命令，则不做任何操作。

【配置举例】 1：配置 OSPF 路由协议重分布 RIP 路由，并将重分布路由的类型设置为 type-1。

```
Ruijie(config)# router ospf
Ruijie(config-router)# redistribute rip subnets route-map redrip
Ruijie(config-router)# network 192.168.12.0 0.0.0.255 area 0
Ruijie(config-router)# exit
Ruijie(config)# route-map redrip permit 10
Ruijie(config-route-map)# set metric-type type-1
```

【检验方法】 1：使用 **show running-config** 命令查看配置。

【提示信息】 -

【常见错误】 -

【平台说明】 -

7.34 set next-hop

对匹配 match 规则的路由信息指定下一跳 IP 地址。
set next-hop *ip-address*

删除设置路由下一跳。
no set next-hop

【参数说明】

参数	描述
ip-address	下一跳 IP 地址

【缺省配置】 -

【命令模式】 路由图配置模式

【缺省级别】 14

【使用指导】 本命令仅用于路由策略配置。
路由信息可以从一个路由进程重分布到另外一个路由进程的功能。比如可以将 OSPF 路由域的路由重新分布后通告到 RIP 路由域中，也可以将 RIP 路由域的路由重新分布后通告到 OSPF 路由域中。路由的相互重分布可以在所有的 IP 路由协议之间进行。
在路由重分布中，经常通过路由图（route maps）的应用，对两个路由域之间的路由相互分布进行有条件的控制。一个路由图规则配置中，可以执行 1 个或多个的 **match** 命令和 1 个或多个的 **set** 命令。如果没有 **match** 命令，则匹配所有；如果没有 **set** 命令，则不做任何操作。

【配置举例】 1：将匹配访问控制表 1 的路由的下一跳设置为 192.168.1.2。

```
Ruijie(config)# route-map redrip permit 10
Ruijie(config-route-map)# match ip address 1
Ruijie(config-route-map)# set next-hop 192.168.1.2
```

【检验方法】 1：使用 **show running-config** 命令查看配置。

【提示信息】 **-**

2：如果配置的 IP 地址不是有效的主机地址（有效包括 A 类除以 0 和 127 开头、B 类和 C 类），则提示错误信息。

```
% Can't set invalid nexthop address!
```

【常见错误】 -

【平台说明】 -

7.35 set tag

对匹配 match 规则的路由设置标记。

set tag *tag*

删除设置路由标记。

no set tag

【参数说明】

参数	描述
tag	设置重分布路由的标记，取值范围：0-4294967295

【缺省配置】 -

【命令模式】 路由图配置模式

【缺省级别】 14

【使用指导】 该命令只适用于路由重分布时才有效。如果没有配置该命令，将继承原来的路由标记。

【配置举例】 1：配置 OSPF 路由协议重分布 RIP 路由，并将重分布路由的标记设置为 100。

```
Ruijie(config)# router ospf
Ruijie(config-router)# redistribute rip subnets route-map redrip
Ruijie(config-router)# network 192.168.12.0 0.0.0.255 area 0
Ruijie(config-router)# exit
Ruijie(config)# route-map redrip permit 10
Ruijie(config-route-map)# set tag 100
```

【检验方法】 1：使用 **show running-config** 命令查看配置。

【提示信息】 -

【常见错误】 -

【平台说明】 -

7.36 show ip as-path-access-list

显示团体列表的信息。

show ip as-path-access-list [*num*]

【参数说明】

参数	描述
num	as-path-access-list 号。

【命令模式】 特权模式、全局配置模式、接口配置模式、路由协议配置模式、路由图配置模式等。

【缺省级别】 14

【使用指导】 使用该命令来查看 as-path-access-list 的信息。

【配置举例】 1：显示 AS 路径列表。

```
Ruijie# show ip as-path-access-list
AS path access list 30
permit ^30$
```

字段解释：

字段	说明
AS path access list	AS 路径列表的名字。
permit	过滤规则的模式。
^30$	具体的正则表达式规则。

【提示信息】 -

【平台说明】 -

7.37 show ip community-list

显示团体列表的信息。

show ip community-list [*community-list-number* | *community-list-name*]

【参数说明】

参数	描述
community-list-number	要显示信息的团体列表号。 标准团体列表：编号范围为 1-99 扩展团体列表：编号范围为 100-199
community-list-name	要显示信息的团体列表名字。 团体列表名不超过 80 字符。

【命令模式】 特权模式、全局配置模式、接口配置模式、路由协议配置模式、路由图配置模式等。

【缺省级别】 14

【使用指导】 使用该命令来查看团体列表的信息。

【配置举例】 1： 显示团体属性列表。

```
Ruijie# show ip community-list
Community-list standard local
permit local-AS
Community-list standard Red-Giant
permit 0:10
deny 0:20
```

字段解释：

字段	说明
Community-list standard local	团体属性列表的类型和名字。
permit	过滤规则的模式。
local-AS	团体属性值。
0:10	团体属性值。

【提示信息】 -

【平台说明】 -

7.38 show ip extcommunity-list

显示扩展团体属性列表的配置信息。

show ip extcommunity-list [*extcommunity-list-num* | *extcommunity-list-name*]

【参数说明】

参数	描述
extcommunity-list-num	取值范围[1~199]，数值 id，用来标识标准（或扩展）的 extcommunity 列表。
extcommunity-list-name	标准（或扩展）extcommunity 列表的名称

【命令模式】 特权模式、全局配置模式、接口配置模式、路由协议配置模式、路由图配置模式等。

【缺省级别】 14

【使用指导】 -

【配置举例】 1： 显示扩展团体属性列表。

```
Ruijie # show ip extcommunity-list
Standard extended community-list 1
     10 permit RT:1:200
```

```
     20 permit RT:1:100
Standard extended community-list 2
     10 permit RT:1:200
Expanded extended community-list rt_filter
     13 permit 1:100
```

字段解释：

字段	说明
Standard extended community-list 1	扩展团体属性列表的类型和名字。
10	过滤规则的序列号。
permit	过滤规则的模式。
RT:1:200	扩展团体属性值。

【提示信息】 -

【平台说明】 -

7.39 show ip prefix-list

查看前缀列表信息或者前缀列表表项信息。

show ip prefix-list [*prefix-name*]

【参数说明】

参数	描述
prefix-name	前缀列表名字

【命令模式】 特权用户模式、全局配置模式、接口配置模式、路由协议配置模式、路由图配置模式等。

【缺省级别】 14

【使用指导】 如果没有指定前缀列表名字，就会显示所有前缀列表的配置信息，否则只显示指定前缀列表的配置信息。

【配置举例】 1：显示 IPv4 前缀列表。

```
Ruijie# show ip prefix-list
ip prefix-list pre: 2 entries
seq 5 permit 192.168.64.0/24
seq 10 permit 192.2.2.0/24
```

字段解释：

字段	说明
ip prefix-list pre	IPv4 前缀列表名字。
2 entries	前缀列表包含的规则数目。
seq 5	过滤规则的序列号。

permit	过滤规则的模式。
192.168.64.0/24	IPv4 路由前缀。

【提示信息】 -

【平台说明】 -

7.40 show ip protocols

查看当前运行的 IPv4 路由协议状态信息。

show ip protocols { **Ospf | Rip** }

【参数说明】

参数	描述
ospf	显示 OSPF 协议状态信息。
rip	显示 RIP 协议状态信息。
-	显示所有运行的路由协议状态信息。

【命令模式】 特权用户模式、全局配置模式、接口配置模式、路由协议配置模式、路由图配置模式等。

【缺省级别】 14

【使用指导】 仅显示当前运行的路由协议的状态信息，未开启的路由协议不会显示。

【配置举例】 -

【提示信息】 -

【平台说明】 -

7.41 show key chain

显示密钥链的配置信息。

show key chain [*keychain name*]

【参数说明】

参数	描述
keychain name	只显示指定密钥链的配置信息

【命令模式】 特权用户模式、全局配置模式、接口配置模式、路由协议配置模式、路由图配置模式等。

【缺省级别】 14

【使用指导】 如果没有指定密钥链名字，就会显示所有密钥链的配置信息，否则只显示指定密钥链的配置信息。

【配置举例】 1：显示密钥链。

```
Ruijie# show key chain
route-map AAA, permit, sequence 10
Match clauses:
ip address 2
Set clauses:
metric 10
Ruijie(config)#show key chain
key chain kc
    key 1 -- text "ruijie"
        accept-lifetime (12:11:00 May  2 2001) - (infinite)
        send-lifetime (always valid) - (always valid) [valid now]
```

字段解释：

字段	说明
key chain	密钥链名字
key	密钥 id 以及密钥字符串
accept-lifetime	密钥链接收方向的生存期
send-lifetime	密钥链发送方向的生存期

【提示信息】 -

【平台说明】 -

7.42 show route-map

显示路由图的配置信息。

show route-map [*route-map-name*]

【参数说明】

参数	描述
route-map-name	只显示指定路由图的配置信息

【命令模式】 特权用户模式、全局配置模式、接口配置模式、路由协议配置模式、路由图配置模式等。

【缺省级别】 14

【使用指导】 如果没有指定路由图名字，就会显示所有路由图的配置信息，否则只显示指定路由图的配置信息。

【配置举例】 1：显示路由图。

```
Ruijie# show route-map
route-map AAA, permit, sequence 10
Match clauses:
ip address 2
Set clauses:
metric 10
```

字段解释：

字段	说明
route-map	路由图名字
Permit	路由图策略包含 permit 关键字
sequence 10	路由图策略对应的序号
Match clauses	定义匹配规则。根据路由图策略是 permit 还是 deny 关键字决定是否执行 set 操作
Set clauses	定义符合 match 匹配规则后的操作

【提示信息】 -

【平台说明】 -

8 NSM

8.1 clear ip route

要清空路由表缓存，可以在特权用户模式执行 **clear ip route** 命令。

clear ip route { ***** **|** *network* [*netmask*] | }

【参数说明】

参数	描述
*	清空全部路由缓存
network	要清空缓存的网络或子网地址
netmask	（可选）网络掩码，不指定掩码时，表示使用 network 最长匹配路由表中的路由，清空缓存

【命令模式】 特权用户模式

【缺省级别】 14

【使用指导】 清空路由缓存会删除对应的路由，然后触发路由协议重新学习。必须注意如果清空整个路由表的缓存，将造成整个网络的短暂通信中断。

【配置举例】 清空 192.168.12.0 最长匹配到的路由表项的缓存。

```
clear ip route 192.168.12.0
```

【提示信息】 -

【平台说明】 -

8.2 ip default-gateway

在二层设备上配置默认网关。

ip default-gateway *ip-address*

删除默认网关。

no ip default-gateway

恢复缺省配置

default ip default-gateway

【参数说明】

参数	描述
ip-address	默认网关 ipv4 地址

【缺省配置】 未配置默认网关

【命令模式】 全局配置模式

【缺省级别】 14

【使用指导】 如果在设备中不知道将数据包发送到哪一个目标地址时，将该数据包发送到默认网关。

该命令在二层设备上支持。或者在三层设备执行了 no ip routing 命令后支持。

【配置举例】 设置默认网关为 192.168.1.1。

```
ip default-gateway 192.168.1.1
```

【检验方法】 可使用 **show ip redirects** 命令查看默认网关设置。

【提示信息】 -

【常见错误】 -

【平台说明】 -

8.3 ip default-network

配置缺省网络。
ip default-network *network*

删除缺省网络。
no ip default-network *network*

恢复缺省配置
default ip default-network *network*

【参数说明】

参数	描述
network	缺省网络的网络号。

【缺省配置】 缺省为 0.0.0.0/0。

【命令模式】 全局配置模式。

【缺省级别】 14

【使用指导】 配置缺省网络的目的是为了产生缺省路由，通过 **default-network** 产生缺省路由需要满足以下条件：该缺省网络不是直连接口网络，但在路由表中可到达。
缺省网络总是以“*”号开头，表示它是缺省路由的候选者。如果缺省网络中有 connected 路由和没有下一跳的路由，则缺省路由要求是静态路由。

【配置举例】 1 :将 192.168.100.0 网络设为缺省网络 ,由于配置了到该网络的静态路由 ,所以设备将自动产生一条缺省路由。

```
Ruijie(config)# ip route 192.168.100.0 255.255.255.0 serial  0/1
Ruijie(config)# ip default-network 192.168.100.0
```

2：将 200.200.200.0 网络设为缺省网络，只要当 200.200.200.0 出现在路由表中，该路由成为缺省路由。

```
Ruijie(config)# ip default-network 200.200.200.0
```

【检验方法】 可使用 show ip route 查看缺省路由。

【提示信息】 -

【常见错误】 -

【平台说明】 -

8.4 ip route

配置静态路由。
ip route *network net-mask* { *ip-address* | *interface* [*ip-address*] } [*distance*] [**tag** *tag*] [**permanent | track** *object-number*] [**weight** *number*] [**description** *description-text*] [**disabled** | **enabled**]

删除已配置的静态路由。
no ip route *network net-mask* { *ip-address* | *interface* [*ip-address*] } [*distance*]

恢复缺省配置
default ip route *network net-mask* { *ip-address* | *interface* [*ip-address*] } [*distance*]

【参数说明】

参数	描述
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 *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】 无静态路由。

【命令模式】 全局配置模式。

【缺省级别】 14

【使用指导】 静态路由的缺省管理距离为 1，通过设置管理距离，可以允许动态路由学到的路由覆盖静态路由，只有当动态路由学不到时，才使用静态路由。通过设置静态路由的管理距离可以实现线路的备份，此时的静态路由，一般又称为浮动路由。比如 OSPF 路由协议的管理距离为 110，可以将静态路由的管理距离设置为 125，这样当跑 OSPF 的线路故障时，数据流量自然就可以切换到静态路由的线路上。

静态路由的默认权重为 1，可以使用 **show ip route weight** 命令查看非默认权重的静态路由。权重参数 weight 用于实现 WCMP 功能，当存在负载均衡路由可到达某地址时，网络设备会根据各条路由的权重值分配数据流量，weight 较大的路由会分担较多的数据报文，较小者会分担较少的数据报文。路由器的 WCMP 限制一般为 32，而交换机则由于各款芯片所能支持的权重不同，所以其 WCMP 限制数量与型号有关；当负载均衡路由的权重之和大于该限制时，超出限制的路由不会生效。

静态路由的使能标志控制静态路由是否有效，如果无效则不会用于转发。永久路由配置进转发表，除非通过网管来删除掉，否则将一直存在。

要通过以太网接口配置静态路由时，尽量避免下一跳直接为接口（如 ip route 0.0.0.0 0.0.0.0 GigabitEthernet 0/0）。这样会让设备觉得所有未知目标网络，都是直连在 GigabitEthernet 0/0 接口，因此对每个目标主机都发送一个 ARP 请求，会占用许多 CPU 和内存资源。所以一般不建议将静态路由直接指向以太网接口。

可以指定静态路由与 track 联动。如果配置静态路由与指定 track 对象联动，当该 track 对象通告的状态为不活动时，该静态路由不生效；当该 track 对象通告的状态为活动时，还需要根据其它状态来决定路由是否生效。与 track 联动主要用于利用 track 对象所关注的第三方状态来决定路由是否生效的场合。Track 联动与 permanent 互斥。

【配置举例】 1：增加了一条到 172.16.100.0/24 目标网络的静态路由，下一跳为 192.168.12.1，管理距离为 115。

```
ip route 172.16.100.0 255.255.255.0 192.168.12.1 115
```

2：如果静态路由没有指定接口，当正常发送接口故障时，可能会使得数据流量从其它接口发送。要避免该情况发生 就需要指定接口。以下的配置例子 到目标网络 172.16.100.0/24 的数据流量只能从 GigabitEthernet 0/0 接口转发。

```
Ruijie(config)# ip route 172.16.100.0 255.255.255.0 GigabitEthernet 0/0 192.168.12.1
```

【检验方法】 可使用 show ip route 查看路由表。

【提示信息】 -

【常见错误】 -

【平台说明】 -

8.5 ip routing

启用 RGOS 软件的 IP 路由功能。
ip routing

关闭 IP 路由功能。
no ip routing

恢复缺省配置
default ip routing

【参数说明】

参数	描述
-	-

【缺省配置】 启用 IP 路由。

【命令模式】 全局配置模式。

【缺省级别】 14

【使用指导】 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 IP 路由转发功能。这时可以关闭 RGOS 的 IP 路由功能。
关闭 IP 路由功能后，设备与普通主机表现一样，可以本机收发包，但不能做转发。所有路由相关的配置都被删除。静态路由配置是个例外，由于静态路由可能配置的较多，若用户无意间配置了 no ip routing 可能导致大量的静态路由配置丢失。为避免这种情况，当执行 no ip routing 时，静态路由配置将会暂时隐藏，若用户重新执行 ip routing，静态路由配置可以恢复。
注意，若在 no ip routing 情况下，进程重启或者整机系统重启，静态路由配置将不会保留。

【配置举例】 关闭了 RGOS 软件的 IP 路由功能。

```
Ruijie(config)# no ip routing
```

【检验方法】 -

【提示信息】 -

【常见错误】 -

【平台说明】 -

8.6 ip static route-limit

配置静态路由的条数上限。
ip static route-limit *number*

配置默认路由条数。
no ip static route-limit

恢复缺省配置
default ip static route-limit

【参数说明】

参数	描述
number	路由上限，范围 1-10000

【缺省配置】 缺省为 1024。

【命令模式】 全局配置模式。

【缺省级别】 14

【使用指导】 配置静态路由数上限的目的是为了控制静态路由的条数，通过 **ip static route-limit** 配置静态路由数上限后会产生如下效果，配置的静态路由数不会超过设置的上限。通过 **show running-config** 可以查看目前配置的非默认静态路由数上限。

【配置举例】 设置静态路由数上限为 900 条，然后恢复默认值。

```
Ruijie(config)#ip static route-limit ?
  <1-10000>  Value(default value: 1024)
Ruijie(config)# ip static route-limit 900
Ruijie(config)# no ip static route-limit
```

【检验方法】 -

【提示信息】 -

【常见错误】 -

【平台说明】 -

8.7 ipv6 default-gateway

在二层设备上配置默认网关。
ipv6 default-gateway *ipv6-address*

删除默认网关。
no ipv6 default-gateway

恢复缺省配置
default ipv6 default-gateway

【参数说明】

参数	描述
ipv6-address	默认网关 ipv6 地址

【缺省配置】 未配置默认网关。

【命令模式】 全局配置模式

【缺省级别】 14

【使用指导】 如果在设备中不知道将数据包发送到哪一个目标地址时，将该数据包发送到默认网关。可使用 **show ipv6 redirects** 命令查看默认网关设置。

【配置举例】 设置默认网关为 10::1。

```
Ruijie(config)# ipv6 default-gateway 10::1
```

【检验方法】 可使用 show ipv6 redirects 查看 ipv6 网关配置。

【提示信息】 -

【常见错误】 -

【平台说明】 该命令在二层设备上支持。或者在三层设备执行了 no ip routing 命令后支持。

8.8 ipv6 route

配置 ipv6 静态路由.

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*] [**tag** *tag*] [**weight** *number*] [**description** *description-text*]

删除已配置的静态路由。

no 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*]

删除所有已配置的静态路由

no ipv6 route [**vrf** *vrf_name*] **all**

恢复缺省配置

default 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*]

default ipv6 route [**vrf** *vrf_name*] **all**

【参数说明】

参数	描述
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。
tag	（可选）静态路由的 Tag 值，缺省为 0。
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。
all	（可选）删除指定 VRF 下的所有静态 IPv6 路由。

【缺省配置】 无 ipv6 静态路由。

【命令模式】 全局配置模式

【缺省级别】 14

【使用指导】 多协议 VRF 删除 IPv6 地址族时，将删除路由 VRF 或者下一跳 VRF 是该 VRF 的 IPv6 静态路由。
如果 IPv6 静态路由的接口所属 VRF 和配置的下一跳 VRF 不一致，那么这条 IPv6 静态路由不生效。
静态路由的缺省管理距离为 1，通过设置管理距离，可以允许动态路由学到的路由覆盖静态路由，只有当动态路由学不到时，才使用静态路由。通过设置静态路由的管理距离可以实现线路的备份，此时的静态路由，一般又称为浮动路由。比如 OSPF 路由协议的管理距离为 110，可以将静态路由的管理距离设置为 125，这样当跑 OSPF 的线路故障时，数据流量自然就可以切换到静态路由的线路上。

【配置举例】 1：增加了一条到 2001::/64 目标网络的静态路由，下一跳为 2002::2，管理距离为 115。

```
Ruijie(config)# ipv6 route 2001::/64 2002::2 115
```

2：如果静态路由没有指定接口，当正常发送接口故障时，可能会使得数据流量从其它接口发送。要避免该情况发生，就需要指定接口。以下的配置例子，到目标网络 2001::/64 的数据流量只能从 GigabitEthernet 0/0 接口转发。

```
Ruijie(config)# ipv6 route 2001::/64 GigabitEthernet 0/0 2002::2
```

【检验方法】 可使用 show ipv6 route 查看 ipv6 路由表。

【提示信息】 -

【常见错误】 -

【平台说明】 本命令在二层设备上不支持。

8.9 ipv6 static route-limit

配置静态路由的条数上限。
ipv6 static route-limit { number | **default-vrf** *number* | **vrf** *vrf-name number* }

配置默认路由条数。
no ipv6 static route-limit [**default-vrf**] | [**vrf** *vrf-name*]

恢复缺省配置

default ipv6 static route-limit [**default-vrf**] | [**vrf** *vrf-name*]

【参数说明】

参数	描述
number	设备所有静态路由上限，范围 1-1000000
default-vrf *number*	默认 vrf 下静态路由上限，范围 1-10000。
vrf *vrf-name number*	vrf 下静态路由上限，范围 1-10000。

【缺省配置】 缺省为 1000

【命令模式】 全局配置模式

【缺省级别】 14

【使用指导】 配置静态路由数上限的目的是为了控制静态路由的条数，通过 **ipv6 static route-limit** 配置静态路由数上限后会产生如下效果，配置的静态路由数不会超过设置的上限。通过 **show running config** 可以查看目前配置的非默认静态路由数上限。

【配置举例】 设置全局 ipv6 静态路由数上限为 900 条，默认 vrf 静态路由上限为 200 条，vrf test 静态路由上限为 100 条，然后全部恢复默认值。

```
Ruijie(config)#ipv6 static route-limit ?
  <1-1000000>  Global limit value(default value: 1024)
  default-vrf  Default Routing/Forwarding instance
  vrf          VPN Routing/Forwarding instance
Ruijie(config)# ipv6 static route-limit 900
Ruijie(config)# ipv6 static route-limit default-vrf  200
Ruijie(config)# ipv6 static route-limit vrf test 100
Ruijie(config)# no ipv6 static route-limit
Ruijie(config)# no ipv6 static route-limit default-vrf
Ruijie(config)# no ipv6 static route-limit vrf test
```

【检验方法】 -

【提示信息】 -

【常见错误】 -

【平台说明】 该命令在二层设备上不支持。

8.10 ipv6 unicast-routing

启用 RGOS 软件的 IPv6 路由功能。

ipv6 unicast-routing

关闭 IPv6 路由功能。
no ipv6 unicast-routing

恢复缺省配置
default ipv6 unicast-routing

【参数说明】

参数	描述
-	-

【缺省配置】 启用 IPv6 路由

【命令模式】 全局配置模式

【缺省级别】 14

【使用指导】 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。

【配置举例】 关闭了 RGOS 软件的 IPv6 路由功能。

```
Ruijie(config)# no ipv6 unicast-routing
```

【检验方法】 -

【提示信息】 -

【常见错误】 -

【平台说明】 该命令在二层设备上不支持。

8.11 maximum-paths

配置等价路由的条数。
maximum-paths *number*

配置默认等价路由条数。
no maximum-paths

恢复缺省配置
default maximum-paths

【参数说明】

参数	描述
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】 全局配置模式

【缺省级别】 14

【使用指导】

配置等价路由条数的目的是为了控制等价路由的条数，通过 **maximum-paths** 配置等价路由条数后会产生如下效果，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。通过 **show running config** 可以查看目前配置的等价路由数。S8600/S5750/S7600 支持 64 组等价路径，每组等价路径最大支持 32 条等价路径条目数。S3760/S5760 的最大等价路径条目数为 8 条，没有等价路径组的限制，也就是说，每一条路由都支持等价路径。等价路径组是指一个前缀的多个等价的下一跳。在 S8600/ S5750/S7600 上，如果整机已配置了 64 组等价路径，现在需要为某一个前缀配置等价路径，如果该等价路径在已存在的 64 组中，则可以成功配置，否则就会失败。

【配置举例】 设置等价路由最多为 10 条，然后恢复默认值。

```
Ruijie(config)# maximum-paths 10
Ruijie(config)# no maximum-paths
```

【检验方法】 通过 show ip route 查看具体 ecmp 路由的情况。

【提示信息】 -

【常见错误】 -

【平台说明】 -

8.12 show ip redirects

显示默认网关。

show ip redirects

【参数说明】

参数	描述
-	-

【命令模式】 特权用户模式

【缺省级别】 14

【使用指导】 该命令用于显示设备的网关配置。可以在二层设备上使用，或者在三层设备执行了 no ip routing 命令后使用。

【配置举例】 下面为 show ip redirects 的输出结果。

```
Ruijie# show ip redirects
Default Gateway: 192.168.195.1
```

字段解释：

字段	说明
Default Gateway	默认网关的 ip 地址

【提示信息】 -

【平台说明】 -

8.13 show ip route

查看 IP 路由表信息。

show ip route [[*network* [*mask* [**longer-prefix**]] | **count** | *protocol* [*process-id*] | **weight**]]

根据路由 ecmp 属性等查看 IP 路由表信息。

show ip route [[**normal** | **ecmp**] [*network* [*mask*]]]

【参数说明】

参数	描述
network	（可选）只显示到该目标网络的路由信息，缺省显示所有路由
mask	（可选）只显示该掩码的目标网络的路由，缺省显示最长匹配前缀的路由。
longer-prefix	(可选) 显示匹配指定前缀范围内所有明细路由
count	（可选）显示当前路由条数（对于 ECMP/WCMP 路由，按一条路由计算），缺省不显示路由条数统计信息。
protocol	（可选）路由协议或者关键词：**connected**, **static**；当显示特定协议路由时，使用下述关键词： **ospf**, **rip**。缺省显示所有协议。
process-id	（可选）路由协议进程号，缺省显示所有进程。
weight	（可选）只显示非默认权重的路由，缺省显示所有权重的路由。
normal	（可选）显示普通路由，不显示等价路由和快速重路由，缺省显示所有类型的路由。
ecmp	（可选）只显示等价路由，缺省显示所有类型的路由。

【命令模式】 特权用户模式、全局配置模式、接口配置模式、路由协议配置模式、路由图配置模式等。

【缺省级别】 14

【使用指导】 该命令可以按照选项，灵活地显示指定路由信息。

show ip route 用于显示实际可以用于转发的表项，如果要看各类属性的表项，请指定 **normal** | **ecmp** 参数。

【配置举例】 1：以下为 **show ip route** 命令的显示结果：

```
Ruijie# show ip route

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, * - candidate default
Gateway of last resort is no set
S    20.0.0.0/8 is directly connected, VLAN 1
S    22.0.0.0/8 [1/0] via 20.0.0.1
O E2 30.0.0.0/8 [110/20] via 192.1.1.1, 00:00:06, VLAN 1
R    40.0.0.0/8 [120/20] via 192.1.1.2, 00:00:23, VLAN 1
B    50.0.0.0/8 [120/0] via 192.1.1.3, 00:00:41
C    192.1.1.0/24 is directly connected, VLAN 1
C    192.1.1.254/32 is local host.
```

2：以下为 **show ip route** *network* 命令的显示结果：

```
Ruijie# show ip route 30.0.0.0
Routing entry for 30.0.0.0/8
Distance 110, metric 20
Routing Descriptor Blocks:
192.1.1.1, 00:01:11 ago, via VLAN 1, generated by OSPF, extern 2
```

3：以下为 **show ip route count** 命令的显示结果：

```
Ruijie# show ip route count
--------- route info ----------
the num of active route: 5
```

4：以下为 **show ip route weight** 命令的显示结果：

```
Ruijie# show ip route weight
------------[distance/metric/weight]-----------
S    23.0.0.0/8 [1/0/2] via 192.1.1.20
S    172.0.0.0/16 [1/0/4] via 192.0.0.1
```

5：**show ip route normal** 命令的显示结果：

```
Ruijie#show ip route normal

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, * - candidate default
Gateway of last resort is no set
S    20.0.0.0/8 is directly connected, VLAN 1
S    22.0.0.0/8 [1/0] via 20.0.0.1
O E2 30.0.0.0/8 [110/20] via 192.1.1.1, 00:00:06, VLAN 1
R    40.0.0.0/8 [120/20] via 192.1.1.2, 00:00:23, VLAN 1
B    50.0.0.0/8 [120/0] via 192.1.1.3, 00:00:41
C    192.1.1.0/24 is directly connected, VLAN 1
C    192.1.1.254/32 is local host
```

6：**show ip route ecmp** 命令的显示结果：

```
Ruijie#show ip route ecmp

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, * - candidate default
Gateway of last resort is 192.168.1.2 to network 0.0.0.0
S*   0.0.0.0/0 [1/0] via 192.168.1.2
               [1/0] via 192.168.2.2
O IA 192.168.10.0/24 [110/1] via 35.1.10.2, 00:38:26, VLAN 1
                             [110/1] via 35.1.30.2, 00:38:26, VLAN 3
```

字段解释：

字段	说明
O	说明该路由的源路由协议。该字段可能取值为： C：直连路由； L：本地路由；S：静态路由； R：RIP 路由； B：BGP 路由； O：OSPF 路由；

	I ：IS-IS 路由。
E2	路由类型。该字段可能取值为： E1：OSPF 外部路由类型 1 ； E2：OSPF 外部路由类型 2 ； N1：OSPF NSSA 外部路由类型 1； N2：OSPF NSSA 外部路由类型 2； SU：IS-IS 汇总路由； L1：IS-IS 1 级路由； L2：IS-IS 2 级路由； IA：路由域内部路由。
20.0.0.0/8	目标网络的网络地址和掩码长度
[1/0]	管理距离 / 度量值
Via 20.0.0.1	下一跳 IP 地址
00:00:06	协议路由存活时间
VLAN 1	下一跳转发接口
Routing Descriptor Blocks	显示路由信息的下一跳 IP 地址、路由来源、更新时间、经由哪个接口、源路由协议、类型、BGP 团体属性值等。

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。

【提示信息】 -

【平台说明】 -

8.14 show ip route summary

查看单张路由表的统计信息。
show ip route summary

查看所有路由表的统计信息。
show ip route summary all

【参数说明】

参数	描述
-	-

【命令模式】 特权用户模式

【缺省级别】 14

【使用指导】 通过该命令可以查看路由表的统计信息。

【配置举例】 1：查看全局路由表的统计信息。

```
Ruijie# show ip route summary
Codes:  NORMAL – Normal route  ECMP – ECMP route  FRR – Fast-Reroute route

    Memory: 2000 bytes
Entries: 22 , based on route prefixes
                    NORMAL  ECMP    FRR     TOTAL
         Connected   3       0       0       3
         Static      2       1       1       4
         RIP         1       2       1       4
         OSPF        2       1       1       4
         ISIS        1       2       0       3
         BGP         2       1       1       4
         TOTAL       11      7       4       22
```

2：查看所有路由表的统计信息。

```
 Ruijie# show ip route summary all
Codes:  NORMAL – Normal route  ECMP – ECMP route  FRR – Fast-Reroute route

IP routing table count:2
Total
     Memory: 4000 bytes
     Entries: 44 , based on route prefixes
                    NORMAL  ECMP    FRR     TOTAL
         Connected   6       0       0       6
         Static      4       2       2       8
         RIP         2       4       2       8
         OSPF        4       2       2       8
         ISIS        2       4       0       6
         BGP         4       2       2       8
         TOTAL       22      14      8       44

Global
     Memory: 2000 bytes
     Entries: 22 , based on route prefixes
                    NORMAL  ECMP    FRR     TOTAL
         Connected   3       0       0       3
         Static      2       1       1       4
         RIP         1       2       1       4
         OSPF        2       1       1       4
```

```
        ISIS        1       2       0       3
        BGP         2       1       1       4
        TOTAL       11      7       4       22

VRF1
    Memory: 2000 bytes
     Entries: 22 , based on route prefixes
                    NORMAL  ECMP    FRR     TOTAL
        Connected   3       0       0       3
        Static      2       1       1       4
        RIP         1       2       1       4
        OSPF        2       1       1       4
        ISIS        1       2       0       3
        BGP         2       1       1       4
        TOTAL       11      7       4       22
```

字段解释：

字段	说明
NORMAL	说明分类的表项类型。该字段可能取值为： NORMAL :普通路由表项(非 ECMP 或 FRR 路由)； ECMP：等价多路径路由表项； FRR：快速重路由表项； TOTAL：所有类型表项条目合计。
Memory	当前路由表占用内存大小。
Entries	当前路由表包含表项条目 (基于表项前缀条目，而非下一跳条目) 。
Connected	说明该行表项协议类型。该字段可能取值为： Connected：直连路由表项 Static：静态路由表项 RIP：RIP 路由表项 OSPF：OSPF 路由表项 ISIS：ISIS 路由表项 BGP：BGP 路由表项 TOTAL：所有协议表项条目合计
IP routing table count	路由表个数
Global	说明当前路由表名称。该字段可能取值为： Global：全局 (即缺省 VRF) VRF1：VRF 名称 TOTAL：所有 VRF 路由表合计信息

为准。

【提示信息】 -

【平台说明】 -

8.15 show ip route track-table

查看 IP 路由联动 Track 信息。

show ip route track-table

【参数说明】

参数	描述
-	-

【命令模式】 特权用户模式。

【缺省级别】 14

【使用指导】 用户查看 IP 路由联动 Track 信息

【配置举例】 以下为 **show ip route track-table** 命令的显示结果：

```
Ruijie(config)#show ip route track-table
ip route 10.0.0.0 255.0.0.0 GigabitEthernet 0/0 track 2 state is [up]
ip route 20.0.0.0 255.0.0.0 GigabitEthernet 0/0  2 track 3 state is [down]
```

字段解释：

字段	说明
track	track 对象索引
state	track 对象状态

【提示信息】 -

【平台说明】 -

8.16 show ipv6 redirects

显示 ipv6 默认网关。

show ipv6 redirects

【参数说明】

参数	描述
-	-

【命令模式】 特权用户模式

【缺省级别】 14

【使用指导】 该命令用于显示设备的网关配置。可以在二层设备上使用 ,或者在三层设备执行了 no ipv6 routing 命令后使用。

【配置举例】 下面为 **show ipv6 redirects** 的输出结果。

```
Ruijie# show ipv6 redirects
Default Gateway: 10::1
```

字段解释：

字段	说明
Default Gatewa	默认网关的 IPv6 地址

【提示信息】 -

【平台说明】 该命令在二层设备上支持。。或者在三层设备执行了 no ipv6 routing 命令后支持。

8.17 show ipv6 route

显示 IPv6 的路由信息。

show ipv6 route [[**vrf** *vrf_name*] [*ipv6-prefix* / *prefix-length* [**longer-prefixes**] | *protocol* [*process-id*] | **weight**]]

【参数说明】

参数	描述
vrf *vrf-name*	（可选）VRF 名称，不指定 VRF 时，表示在全局 VRF 中执行
ipv6-prefix/*prefix-length*	（可选）显示完全匹配指定前缀的 v6 路由，缺省显示所有路由
longer-prefixes	（可选）显示最长匹配指定前缀的 v6 路由，缺省显示所有路由
protocol	（可选）路由协议或者关键词：**connected**, **local, static**；当显示特定协议路由时，使用下述关键词：**bgp**, **isis**, **ospf**, **rip**，缺省显示所有协议的路由
process-id	（可选）路由协议进程号，缺省显示所有进程号的路由
weight	（可选）只显示非默认权重的路由，缺省显示所有权重的路由

【命令模式】 特权用户模式

【缺省级别】 14

【使用指导】 通过该命令可以查看 IPv6 路由表的信息。

【配置举例】 显示全局 VRF 的 ipv6 路由表

```
Ruijie(config)# show ipv6 route

IPv6 routing table -  Default - 7 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       10::/64  via Loopback 1, directly connected
L       10::1/128  via Loopback 1, local host
S       20::/64  [20/0] via 10::4, Loopback 1C
C       FE80::/10 via Null 0, directly connected
C       FE80::/64  via Loopback 1, directly connected
L       FE80::2D0:F8FF:FE22:33AB/128  via Loopback 1, local host
```

字段解释：

字段	说明
S	说明该路由的源路由协议。该字段可能取值为： C：直连路由； L：本地路由 S：静态路由； R：RIP 路由； B：BGP 路由； O：OSPF 路由； I ：ISIS 路由
E2	路由类型。该字段可能取值为： E1：OSPF 外部路由类型 1 ； E2：OSPF 外部路由类型 2 ； N1：OSPF NSSA 外部路由类型 1； N2：OSPF NSSA 外部路由类型 2； SU：IS-IS 汇总路由； L1：IS-IS 1 级路由； L2：IS-IS 2 级路由； IA：路由域内部路由。

20::/64	目标网络的网络地址和掩码长度
[20/0]	管理距离 / 度量值
via 10::4	下一跳 IPv6 地址
Loopback 1	下一跳转发接口

【提示信息】 -

【平台说明】 本命令在二层设备上不支持。

8.18 show ipv6 route summary

查看单张 IPv6 路由表的统计信息。
show ipv6 route [**vrf** *vrf-name*] **summary**

查看所有 IPv6 路由表的统计信息。
show ipv6 route summary all

【参数说明】

参数	描述
vrf-name	（可选）VRF 名称，不指定 VRF 时，表示在全局 VRF 中执行

【命令模式】 特权用户模式

【缺省级别】 14

【使用指导】 通过该命令可以查看 IPv6 路由表的统计信息。

【配置举例】 1：查看全局路由表的统计信息。

```
Ruijie#show ipv6 route summary
IPv6 routing table name is -  Default(0) global scope - 5 entries
IPv6 routing table default maximum-paths is 32
Local           2
Connected       3
Static          0
PIP             0
OSPF            0
BGP             0
------------------------
Total           5
```

2：查看所有 IPv6 路由表的统计信息。

```
Ruijie#show ipv6 route summary all

IPv6 routing table count: 2
Total
  Memory: 2000 bytes
  Entries: 20
    Local:2,Connected:2,Static:8,RIP:2,OSPF:2,ISIS:2,BGP:2

Global
  Memory: 1000 bytes
  Entries: 10
    Local:1,Connected:1,Static:4,RIP:1,OSPF:1,ISIS:1,BGP:1

VRF1
  Memory: 1000 bytes
  Entries: 10
    Local:1,Connected:1,Static:4,RIP:1,OSPF:1,ISIS:1,BGP:1
```

字段解释：

字段	说明
Memory	当前路由表占用内存大小。
Entries	当前路由表包含表项条目（基于表项前缀条目，而非下一跳条目）。
Connected	说明该行表项协议类型。该字段可能取值为： Connected：直连路由表项 Static：静态路由表项 RIP：RIP 路由表项 OSPF：OSPF 路由表项 ISIS：ISIS 路由表项 BGP：BGP 路由表项 TOTAL：所有协议表项条目合计
IPv6 routing table count	路由表个数
Global	说明当前路由表名称。该字段可能取值为： Global：全局（即缺省 VRF） VRF1：VRF 名称 TOTAL：所有 VRF 路由表合计信息

【提示信息】 -

【平台说明】 本命令在二层设备上不支持。

命令参考-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. VPDN
9. IPSEC-IKE
10. AAA
11. RADIUS
12. TACACS+
13. Web 认证配置命令
14. 全局 IP+MAC 绑定
15. IPoE
16. IP-GROUP
17. app-auth
18. webservice
19. ANTI-PAP
20. 广告配置命令
21. Local-Account
22. 防火墙

1 ACL

1.1 命令标识符表

标识符	含义
Id	ACL 数值标号。可配范围 IP 标准 ACL：1-99，1300-1999 IP 扩展 ACL：100-199，2000-2699 MAC 扩展 ACL：700–799 专家扩展 ACL：2700–2899
Name	ACL 名字
Sn	ACL 表项序号(支持按优先级设置产品)
start-sn	序号起始值
inc-sn	序号增量
Deny	如果匹配，则拒绝访问
Permit	如果匹配，则允许访问
Port	协议编号，对于 IPv6 的该字段可为 ipv6 ,icmp ,tcp ,udp 及数值 0-255 ,对于 IPv4，可以是eigrp，gre，ipinip，igmp，nos，ospf，icmp，udp，tcp，ip 中的一个，也可以是代表 IP 协议的 0-255 编号，一些重要协议如 icmp/tcp/udp 等单独列出进行说明
interface idx	输入匹配的接口
src	报文源地址（主机地址或网络地址）
src-wildcard	源地址通配符。可以使不连续的，如 0.255.0.32
src-ipv6-pfix	源 IPv6 网络地址或网络类型
dst-ipv6-pfix	目的 IPv6 网络地址或网络类型
pfix-len	高位起掩码位数
src-ipv6-addr	源 IPv6 地址
dst-ipv6-addr	目的 IPv6 地址
dscp	有差服务码点，码点值， 范围 0-63
flow-label	流标签，流标签值范围 0-1048575
dst	报文目标地址（主机地址或网络地址）
dst-wildcard	目标地址通配符。可以不连续，如 0.255.0.32
fragment	报文分片的过滤

precedence	报文的优先级别（按从高到低为 0-7）
range	报文的四层端口号范围
time-range tm-rng-name	报文过滤的时间区，名称为 tm-rng-name
tos	报文的服务类型（0-15）
cos	报文 cos 值(0-7)
cos inner cos	报文内部 tag 中的 cos
icmp-type	ICMP 报文的消息类型（0-255）
icmp-code	ICMP 报文的消息类型代码（0-255）
icmp-message	ICMP 报文的消息类型名称
operator port[port]	Operator 为操作符（lt-小于，eq-等于，gt-大于，neq-不等于，range-范围） port 端口号，二目操作需要两个端口号码，其他的操作符只要一个端口号
src-mac-addr	源主机的物理地址
dst-mac-addr	目的主机的物理地址
VID vid	指定的 vlan id
VID inner vid	指定定内部 tag 中的 vid
ethernet-type	以太网协议类型，可以输入 0x 数值
match-all tcpf	匹配 tcp flag 的所有位
established	匹配 tcp flag 标志中的 rst 或 ack 位，其他位不匹配
text	注释信息
in	对进入该接口的报文进行过滤
out	对从该接口输出的报文进行过滤
{rule mask offset}+	rule 十六进制的值域，mask 十六进制的掩码域 offset 为偏移量，可参考偏移量表 “+”号表示至少一组
log	报文匹配 ACL 规则时，输出匹配日志信息

1.2 access-list

该命令创建一条 ACL 并往该 ACL 中添加一条 ACL 规则，用于过滤数据报文。不同类型 ACL 的创建命令如下：

1. 创建一条 IP 标准 ACL，并往该 ACL 中添加一条 ACL 规则

access-list *id* { **deny** | **permit** } { *source source-wildcard* | **host** *source* | **any** } [**time-range** *tm-range-name*] [**log**]

2. 创建一条 IP 扩展 ACL，并往该 ACL 中添加一条 ACL 规则

access-list *id* { **deny** | **permit** } *protocol* { *source source-wildcard* | **host** *source* | **any** } { *destination destination-wildcard* | **host** *destination* | **any** } [**precedence** *precedence*] [**range** *lower upper*] [**time-range** *time-range-name*] [**log**]

3. 创建一条 MAC 扩展 ACL，并往该 ACL 中添加一条 ACL 规则

access-list *id* { **deny** | **permit** } { **any** | *src-mac-addr* mask } { **any** | *dst-mac-addr* mask } [**cos** [*out*] [**inner** *in*]]

4. 创建一条专家级扩展 ACL，并往该 ACL 中添加一条 ACL 规则

access-list *id* { **deny** | **permit** } [*protocol* | [**cos** [*out*] [**inner** *in*]]] [**VID** [*out*] [**inner** *in*]] { *source source-wildcard* | **host** *source* | **any** } { **any** } { *destination destination-wildcard* | **host** *destination* | **any** } { **any** }] [**precedence** *precedence*] [**range** *lower upper*] [**time-range** *time-range-name*]

选择字段包含以太网类型或 cos 字段时：

access-list *id* { **deny** | **permit** } { **cos** [*out*] [**inner** *in*] } [**VID** [*out*] [**inner** *in*]] { **s***ource source-wildcard* | **host** *source* | **any** } { **any** } { *destination destination-wildcard* | **host** *destination* | **any** } { **any** } [**time-range** *time-range-name*]

选择协议 Protocol 字段时：

access-list *id* { **deny** | **permit** } *protocol* [**VID** [*out*] [**inner** *in*]] { *source source-wildcard* | **host** *source* | **any** } { **any** } { *destination destination-wildcard* | **host** *destination* | **any** } { **any** } [**precedence** *precedence*] [**range** *lower upper*] [**time-range** *time-range-name*]

一些重要协议的专家级扩展 ACL：

Internet Control Message Protocol (ICMP)：

access-list *id* { **deny** | **permit** } **icmp** [**VID** [*out*] [**inner** *in*]] { *source source-wildcard* | **host** *source* | **any** } { **any** } { *destination destination-wildcard* | **host** *destination* | **any** } { **any** } [*icmp-type*] [[*icmp-type* [*icmp-code*]] | [*icmp-message*]] [**precedence** *precedence*] [**time-range** *time-range-name*]

Transmission Control Protocol (TCP)：

access-list *id* { **deny** | **permit** } **tcp** [**VID** [*out*] [**inner** *in*]] { *source source-wildcard* | **host** *Source* | **any** } { **any** } [**operator** port [*port*]] { *destination destination-wildcard* | **host** *destination* | **any** } { **any** } [**operator port** [*port*]] [**precedence** *precedence*] [**range** *lower upper*] [**time-range** *time-range-name*]

User Datagram Protocol (UDP)：

access-list *id* { **deny** | **permit** } **udp**[**VID** [*out*] [**inner** *in*]] { *source source –wildcard* | **host** *source* | **any** } { **any** } [**operator port** [*port*]] { *destination destination-wildcard* | **host** *destination* | **any** } { **any** } [**operator port** [*port*]] [**precedence** *precedence*] [**range** *lower upper*] [**time-range** *time-range-name*]

删除指定的 ACL。

no access-list *id*

【参数说明】

参数	描述
id	ACL 编号，可配范围： □ IP 标准 ACL（1-99，1300-1999） □ IP 扩展 ACL（ 100-199，2700 – 2899） □ MAC 扩展 ACL（700 – 799） □ 专家级扩展 ACL（2000-2699）
deny	如果匹配，则拒绝访问。
permit	如果匹配，则允许访问。
source	报文源地址（主机地址或网络地址）
source-wildcard	源地址通配符。可以是不连续的，如 0.255.0.32
protocol	IP 协议编号，可以是 EIGRP、GRE、IPINIP、IGMP、NOS、OSPF、ICMP、UDP、TCP、IP 中的一个，也可以是代表 IP 协议的 0-255 编号。一些重要协议如 ICMP/TCP/UDP 等单独列出进行说明。
destination	报文目标地址（主机地址或网络地址）
destination-wildcard	目标地址通配符。可以是不连续的，如 0.255.0.32
precedence	报文的优先级别
precedence	报文的优先级别值（0-7）
range	报文的四层端口号范围
lower	四层端口号范围的下限
upper	四层端口号范围的上限
time-range	报文过滤的时间区
time-range-name	报文过滤的时间区名称
icmp-type	ICMP 报文的消息类型（0-255）
icmp-code	ICMP 报文的消息类型代码（0-255）
icmp-message	ICMP 报文的消息类型名称
operator	操作符（lt-小于，eq-等于，gt-大于，neq-不等于，range-范围）
port [*port*]	端口号，*range* 需要两个端口号码，其他的操作符只要一个端口号。
text	注释信息

【缺省配置】 没有 ACL 配置，也没有 ACL 规则配置

【命令模式】 全局模式

【缺省级别】 14

【使用指导】 为了使用访问列表对数据进行过滤，首先必须通过命令 **access-list** 定义一系列访问列表规则语句。您可以根据具体实际需要使用不同种类的访问列表：

- IP 标准 ACL （1-99，1300-1999）只对源地址进行控制。
- IP 扩展 ACL（100-199，2000-2699），可以根据源目的地址进行复杂的控制。
- MAC 扩展 ACL（700-799），可以根据源和目的 MAC 地址以及以太网类型进行匹配
- 专家级扩展访问列表（2700-2899），IP 标准 ACL、IP 扩展 ACL 以及 MAC 扩展 ACL 的综合。允许在专家级扩展 ACL 中同时配置上述三种 ACL 规则，另外，专家级扩展 ACL 还可以对 VLAN ID 进行匹配过滤。

对于三层路由协议（包括单播路由协议、多播路由协议）而言，访问列表规则中以下参数不支持：**precedence** *precedence* /**range** *lower upper*/ **time-range** *time-range-name*。

TCP Flag 包含以下部分或全部：

- urg
- ack
- psh
- rst
- syn
- fin

报文优先级别名称如下：

- critical
- flash
- flash-override
- immediate
- internet
- network
- priority
- routine

服务类型名称如下：

- max-reliability
- max-throughput
- min-delay
- min-monetary-cost
- normal

ICMP 报文消息类型名称如下：

- administratively-prohibited
- dod-host-prohibited
- dod-net-prohibited
- echo
- echo-reply
- fragment-time-exceeded
- general-parameter-problem
- host-isolated
- host-precedence-unreachable

- host-redirect
- host-tos-redirect
- host-tos-unreachable
- host-unknown
- host-unreachable
- information-reply
- information-request
- mask-reply
- mask-request
- mobile-redirect
- net-redirect
- net-tos-redirect
- net-tos-unreachable
- net-unreachable
- network-unknown
- no-room-for-option
- option-missing
- packet-too-big
- parameter-problem
- port-unreachable
- precedence-unreachable
- protocol-unreachable
- redirect
- router-advertisement
- router-solicitation
- source-quench
- source-route-failed
- time-exceeded
- timestamp-reply
- timestamp-request
- ttl-exceeded
- unreachable

下面是 TCP 端口名称，TCP 可以使用端口名称或端口号来指定具体的端口：

- bgp
- chargen
- cmd
- daytime
- discard
- domain
- echo
- exec

- finger
- ftp
- ftp-data
- gopher
- hostname
- ident
- irc
- klogin
- kshell
- login
- nntp
- pim-auto-rp
- pop2
- pop3
- smtp
- sunrpc
- syslog
- tacacs
- talk
- telnet
- time
- uucp
- whois
- www

下面是 UDP 端口名称，UDP 可以使用端口名称或端口号来指定具体的端口：

- biff
- bootpc
- bootps
- discard
- dnsix
- domain
- echo
- isakmp
- mobile-ip
- nameserver
- netbios-dgm
- netbios-ns
- netbios-ss
- ntp
- pim-auto-rp
- rip

- snmp
- snmptrap
- sunrpc
- syslog
- tacacs
- talk
- tftp
- time
- who
- xdmcp

如果要删除 ACL 规则，需要进入 ACL 模式通过 **no {sn | permit | deny}**命令删除。

【配置举例】 1：IP 标准访问列表示例

下面的 IP 基本访问列表允许源地址为 192.168.1.64 - 192.168.1.127 的报文通过，其他的所有报文拒绝：

```
Ruijie(config)# access-list 1 permit 192.168.1.64 0.0.0.63
```

2：IP 扩展访问列表示例

下面的 IP 扩展访问列表允许 DNS 报文和 ICMP 报文通过：

```
Ruijie(config)# access-list 102 permit tcp any any eq domain log
Ruijie(config)# access-list 102 permit udp any any eq domain log
Ruijie(config)# access-list 102 permit icmp any any echo log
Ruijie(config)# access-list 102 permit icmp any any echo-reply
```

3：MAC 扩展访问列表示例

拒绝 MAC 为 00d0f8000c0c 的源主机发送类型为 100 的以太网帧，并应用到接口 gigabitethernet 1/1。

```
Ruijie(config)# access-list 702 deny host 00d0f8000c0c any aarp
Ruijie(config)# interface gigabitethernet 1/1
Ruijie(config-if-GigabitEthernet 1/1)# mac access-group 702 in
```

4：Expert 扩展访问列表示例

创建及显示一条 Expert Extended ACL，该专家 ACL 拒绝源 IP 地址为 192.168.12.3 并且源 MAC 地址为 00d0.f800.0044 的所有 TCP 报文。

```
Ruijie(config)# access-list 2702 deny tcp host
192.168.12.3 mac 00d0.f800.0044 any any
Ruijie(config)# access-list 2702 permit any any any any
Ruijie(config)# show access-lists
expert access-list extended 2702
10 deny tcp  host  192.168.12.3 mac 00d0.f800.0044 any any
20 permit any any any any
```

【检验方法】 1：使用 **show access-lists** 命令可以查看到所有 ACL 的配置信息，包括 ACL 规则信息。
2：使用 **show access-lists** *id* 命令可以查看到指定 ACL 的配置信息，包括 ACL 规则信息。
3：使用 **show access-lists** *name* 令可以查看到指定 ACL 的配置信息，包括 ACL 规则信息。

【提示信息】 如果往同一条 ACL 里重复添加相同的 ACL 规则时，则提示错误信息：

```
failed, for the entry is existed or the sequence number has been allocated!
```

【常见错误】 -

【平台说明】 -

1.3 access-list list-remark

为指定的 ACL 添加注释信息。
access-list *id* **list-remark** *text*

删除 ACL 注释信息
no access-list *id* **list-remark**

【参数说明】

参数	描述
id	ACL 编号。可配范围：IP 标准 ACL（1-99，1300-1999）、IP 扩展 ACL（100-199，2000-2699）、MAC 扩展 ACL（700–799）、专家扩展 ACL（2700–2899）
text	注释信息

【缺省配置】 没有 ACL 注释信息

【命令模式】 全局模式

【缺省级别】 14

【使用指导】 为了便于查看某条 ACL 的作用，可以使用本命令为指定的 ACL 添加注释信息。如果指定的 ACL 不存在，本命令会先创建该 ACL，然后再添加注释信息。

【配置举例】 1：创建编号为 1 的 ACL 并为该 ACL 添加“this acl is to filter the host 192.168.4.12”的注释信息：

```
Ruijie(config)# ip access-list extended 100
Ruijie(config)# access-list 100 list-remark this acl is to filter the host 192.168.4.12
```

【检验方法】 1：使用 **show access-lists** 命令可以查看到所有 ACL 的配置信息，包括 ACL 的注释信息。
2：使用 **show access-list** *sid* 命令可以查看到指定 ACL 的配置信息，包括该 ACL 的注释信息。
3：使用 **show access-lists** *name* 令可以查看到指定 ACL 的配置信息，包括该 ACL 的注释信息。

【提示信息】 -

【常见错误】 -

【平台说明】 -

1.4 access-list remark

为接下来要配置的 ACL 规则添加注释信息。
access-list *id* **remark** *text*

删除 ACL 规则注释信息
no access-list *id* **remark** *text*

【参数说明】

参数	描述
id	ACL 编号。可配范围：IP 标准 ACL（1-99，1300-1999）、IP 扩展 ACL（100-199，2000-2699）、MAC 扩展 ACL（700–799）、专家扩展 ACL（2700–2899）
text	注释信息

【缺省配置】 没有 ACL 规则注释信息

【命令模式】 全局模式

【缺省级别】 14

【使用指导】 为了便于查看某条 ACL 规则的作用，可以使用本命令为指定的 ACL 规则添加注释信息。如果指定的 ACL 不存在，本命令会先创建该 ACL，然后再添加 ACL 规则注释信息

【配置举例】 1：在编号为 102 的 ACL 中添加一条 ACL 规则注释信息：

```
Ruijie(config)# access-list 102 remark deny-host-10.1.1.1
```

【检验方法】 1：使用 **show access-lists** 命令可以查看到所有 ACL 的配置信息，包括 ACL 规则的注释信息。
2：使用 **show access-lists** *id* 命令可以查看到指定 ACL 的配置信息，包括该 ACL 规则的注释信息。
3：使用 **show access-lists** *name* 令可以查看到指定 ACL 的配置信息，包括该 ACL 规则的注释信息。

【提示信息】 如果在同一条 ACL 下重复添加相同的 ACL 规则注释信息，则提示错误信息：

```
Remark is duplicate
```

【常见错误】 -

【平台说明】 -

1.5 clear access-list counters

清除 ACL deny 的报文统计数。

clear access-list counters [*id* | *name*]

【参数说明】

参数	描述
id	ACL 的编号。可配范围：IP 标准 ACL（1-99，1300-1999）、IP 扩展 ACL（100-199，2000-2699）、MAC 扩展 ACL（700–799）、专家扩展 ACL（2700–2899）
name	ACL 的名字

【命令模式】 特权模式

【缺省级别】 14

【使用指导】 如果想重新开始统计指定 ACL 被 deny 的报文匹配信息，可以执行该命令先将该 ACL 的 deny 报文匹配统计计数值清零。

【配置举例】 1：将编号为 1 的 ACL 的报文匹配统计的计数值清零。

使用此命令前：

```
Ruijie #show access-lists
ip access-list standard 1
    10 deny host 50.1.1.2 (10 matches)
    20 permit host 60.1.1.2 (15 matches)
    (10 packets filtered)
```

使用此命令后：

```
Ruijie# end
Ruijie# clear access-list counters
Ruijie# show access-lists
ip access-list standard 1
    10 deny host 50.1.1.2 (10 matches)
    20 permit host 60.1.1.2 (15 matches)
```

【提示信息】 -

【平台说明】 -

1.6 clear counters access-list

清除 ACL 的报文匹配统计计数。

clear counters access-list [*id* | *name*]

【参数说明】

参数	描述
id	ACL 的编号。可配范围：IP 标准 ACL（1-99，1300-1999）、IP 扩展 ACL（100-199，2000-2699）、MAC 扩展 ACL（700–799）、专家扩展 ACL（2700–2899）
name	ACL 的名字

【命令模式】 特权模式

【缺省级别】 14

【使用指导】 如果想重新开始统计指定 ACL 的报文匹配信息，可以执行该命令先将该 ACL 的报文匹配统计计数值清零。

【配置举例】 1：将编号为 2700 的 ACL 的报文匹配统计的计数值清零。

使用此命令前：

```
Ruijie #show access-lists 2700
expert access-list extended 2700
    10 permit ip VID 4 host 192.168.3.55 any host 192.168.99.6 any  (88 matches)
    20 deny tcp any any eq login any any (33455 matches)
    30 permit tcp any any host 192.168.6.9 any (10 matches)
```

使用此命令后：

```
Ruijie# clear counters access-list 2700
Ruijie #show access-lists 2700
expert access-list extended 2700
    10 permit ip VID 4 host 192.168.3.55 any host 192.168.99.6 any
    20 deny tcp any any eq login any any
    30 permit tcp any any host 192.168.6.9 any
```

【提示信息】 -

【平台说明】 -

1.7 deny

往一条 ACL 中添加/删除一个拒绝类型的 ACL 规则。

1. IP 标准 ACL

- 往 IP 标准 ACL 中添加一条拒绝类型的 ACL 规则

[*sn*] **deny** { *source source-wildcard* | **host** *source* | **any** } [**time-range** *tm-range-name*] [**log**]

- 从 IP 标准 ACL 中删除一条拒绝类型的 ACL 规则

no { *sn* | { **deny** { *source source-wildcard* | **host** *source* | **any** } [**time-range** *tm-range-name*] [**log**] } }

2. IP 扩展 ACL

- 往 IP 扩展 ACL 中添加一条拒绝类型的 ACL 规则

[*sn*] **deny** *protocol source source-wildcard destination destination-wildcard* [**precedence** *precedence*] [**range** *lower upper*] [**time-range** *time-range-name*] [**log**]

- 从 IP 扩展 ACL 中删除一条拒绝类型的 ACL 规则

no { *sn* | { **deny** *protocol source source-wildcard destination destination-wildcard* [**precedence** *precedence*] [**range** *lower upper*] [**time-range** *time-range-name*] [**log**] } }

一些重要协议的 IP 扩展访问控制列表：

Internet Control Message Protocol (ICMP)

[*sn*] **deny icmp** { *source source-wildcard* | **host** *source* | **any** } { *destination destination-wildcard* | **host** *destination* | **any** } [*icmp-type*] [[*icmp-type* [*icmp-code*]] | [*icmp-message*]] [**precedence** *precedence*] [**time-range** *time-range-name*]

Transmission Control Protocol (TCP)

[*sn*] **deny tcp** { *source source-wildcard* | **host** *Source* | **any** } [*operator* **port** [*port*]] { *destination destination-wildcard* | **host** *destination* | **any** } [*operator* **port** [*port*]] [**precedence** *precedence*] [**range** *lower upper*] [**time-range** *time-range-name*]

User Datagram Protocol (UDP)

[*sn*] **deny udp** { *source source –wildcard* | **host** *source* | **any** } [*operator* **port** [*port*]] { *destination destination-wildcard* | **host** *destination* | **any** } [*operator* **port** [*port*]] [**precedence** *precedence*] [**range** *lower upper*] [**time-range** *time-range-name*]

3. MAC 扩展 ACL

- 往 MAC 扩展 ACL 中添加一条拒绝类型的 ACL 规则

[*sn*] **deny** { **any** } { **any** } [**cos** [*out*] [**inner** *in*]]

- 从 MAC 扩展 ACL 中删除一条拒绝类型的 ACL 规则

no { *sn* | {**deny** { **any** } { **any** | **host** *destination-mac-address*} [**cos** [*out*] [**inner** *in*]] } }

4. 专家级扩展 ACL

- 往专家级扩展 ACL 中添加一条拒绝类型的 ACL 规则

[*sn*] **deny**[*protocol* | [**cos** [*out*] [**inner** *in*]]] [[**VID** [*out*] [**inner** *in*]]] { *source source-wildcard* | **host** *source* | **any**}{ **any** } { *destination destination-wildcard* | **host** *destination* | **any** } { **any** } [**precedence** *precedence*] [**range** *lower upper*] [**time-range** *time-range-name*]

- 从专家级扩展 ACL 中删除一条拒绝类型的 ACL 规则

no { *sn* | { **deny** [*protocol* | [**cos** [*out*] [**inner** *in*]]] [[**VID** [*out*] [**inner** *in*]]] { *source source-wildcard* | **host** *source* | **any** } { **any** } { *destination destination-wildcard* | **host** *destination* | **any** } { **any** } [**precedence** *precedence*] [**range** *lower upper*] [**time-range** *time-range-name*] } }

选择字段包含以太网类型 cos 字段时

[*sn*] **deny** { [**cos** [*out*] [**inner** *in*]] } [[**VID** [*out*] [**inner** *in*]]] { *source source-wildcard* | **host** *source* | **any** } { **any** } { *destination destination-wildcard* | **host** *destination* | **any** } { **any** } [**time-range** *time-range-name*]

选择协议 protocol 字段时

[*sn*] **deny protocol** [[**VID** [*out*] [**inner** *in*]]] { *source source-wildcard* | **host** *source* | **any** } { **any** } { *destinationdestination-wildcard* | **host** *destination* | **any** } { **any** } [**precedence** *precedence*] [**range** *lower upper*] [**time-range** *time-range-name*]

一些重要协议的 expert 扩展访问列表：

Internet Control Message Protocol (ICMP)

[*sn*] **deny icmp** [[**VID** [*out*] [**inner** *in*]]] { *source source-wildcard* | **host** *source* | **any** } { **any** } { *destination destination-wildcard* | **host** *destination* | **any** } { **any** } [*icmp-type*] [[*icmp-type* [*icmp-code*]] | [*icmp-message*]] [**precedence** *precedence*] [**time-range** *time-range-name*]

Transmission Control Protocol (TCP)

[*sn*] **deny tcp** [[**VID** [*out*] [**inner** *in*]]] { *source source-wildcard* | **host** *Source* | **any** } { **any** } [*operator* **port** [*port*]] { *destination destination-wildcard* | **host** *destination* | **any** } { **any** } [*operator* **port** [*port*]] [**precedence** *precedence*] [**range** *lower upper*] [**time-range** *time-range-name*]

User Datagram Protocol (UDP)

[*sn*] **deny udp** [[**VID** [*out*] [**inner** *in*]]] { *source source –wildcard* | **host** *source* | **any** } { **any** } [*operator* **port** [*port*]] { *destination destination-wildcard* | **host** *destination* | **any** } { **any** } [*operator* **port** [*port*]] [**precedence** *precedence*] [**range** *lower upper*] [**time-range** *time-range-name*]

Address Resolution Protocol (ARP)

[*sn*] **deny arp** { **vid** *vlan-id* } [*source-mac-address source-wildcard* | **any**] [**host** *destination –mac-address* | **any**] { *sender-ip sender-ip–wildcard* | **host** *sender-ip* | **any** } { *sender-mac sender-mac-wildcard* | **host** *sender-mac* | **any** } { *target-ip target-ip–wildcard* | **host** *target-ip* | **any** }

【参数说明】

参数	描述
sn	ACL 规则序号
time-range	报文过滤的时间区
time-range-name	报文过滤的时间区名称

【缺省配置】 没有 ACL 规则。

【命令模式】 ACL 模式

【缺省级别】 14

【使用指导】 当想拒绝某些报文进入网络时，可以使用该命令往指定的 ACL 里添加一些拒绝类型的 ACL 规则。

【配置举例】 1：下例显示如何创建及显示一条 Expert Extended ACL，该专家 ACL 拒绝源 IP 地址为 192.168.4.12 并且源 MAC 地址为 001300498272 的所有 TCP 报文。

```
Ruijie(config)# expert access-list extended 2702
Ruijie(config-exp-nacl)# deny tcp  host
192.168.4.12 host 0013.0049.8272 any any
Ruijie(config-exp-nacl)# permit any any any any
Ruijie(config-exp-nacl)# show access-lists
expert access-list extended 2702
10 deny tcp  host  192.168.4.12 host 0013.0049.8272 any any
20 permit any any any any
Ruijie(config-exp-nacl)#
```

2：下面是 IP 扩展 ACL 使用范例，目的是拒绝 IP 为 192.168.4.12 的源主机提供 TCP 端口为 100 的服务，并应用到接口γιγαβιτετηερνετ 1/1。配置方法：

```
Ruijie(config)# ip access-list extended ip-ext-acl
Ruijie(config-ext-nacl)# deny tcp host 192.168.4.12 eq 100 any
Ruijie(config-ext-nacl)# show access-lists
ip access-list extended ip-ext-acl
10 deny tcp host 192.168.4.12 eq 100 any
Ruijie(config-ext-nacl)# exit
Ruijie(config)# interface gigabitethernet 1/1
Ruijie(config-if-GigabitEthernet 0/1)# ip access-group ip-ext-acl in
```

3：下面是 MAC 扩展 ACL 使用范例，目的是拒绝 MAC 为 0013.0049.8272 的源主机发送类型为 100 的以太网

帧，并应用到接口γιγαβιτετηερνετ 1/1。配置方法

```
Ruijie(config)# mac access-list extended mac1
Ruijie(config-mac-nacl)# deny host 0013.0049.8272 any aarp
Ruijie(config-mac-nacl)# show access-lists
mac access-list extended mac1
10 deny host 0013.0049.8272 any aarp
Ruijie(config-mac-nacl)# exit
Ruijie(config)# interface gigabitethernet 1/1
Ruijie(config-if-GigabitEthernet 1/1)# mac access-group mac1 in
```

4：下面是 IP 标准 ACL 使用范例，目的是拒绝 IP 为 192.168.4.12 的源主机，并应用到接口 gigabitethernet 1/1。配置方法：

```
Ruijie(config)# ip access-list standard 34
Ruijie(config-ext-nacl)# deny host 192.168.4.12
Ruijie(config-ext-nacl)# show access-lists
ip access-list standard 34
10 deny host 192.168.4.12
Ruijie(config-ext-nacl)# exit
Ruijie(config)# interface gigabitethernet 1/1
Ruijie(config-if-GigabitEthernet 1/1)# ip access-group 34 in
```

【检验方法】 1：使用 **show access-lists** 命令可以查看到所有 ACL 的配置信息，包括 ACL 下配置的所有规则。
2：使用 **show access-lists** *id* 命令可以查看到指定 ACL 的配置信息，包括该 ACL 下配置的所有规则。
3：使用 **show access-lists** *name* 令可以查看到指定 ACL 的配置信息，包括该 ACL 下配置的所有规则。

【提示信息】 -

【常见错误】 -

【平台说明】 -

1.8 ip access-group

将指定的 ACL 应用于全局模式或接口
ip access-group { *id* | *name* } { **in** | **out** }

取消 ACL 和全局模式或接口的关联
no ip access-group { *id* | *name* } { **in** | **out** }

【参数说明】

参数	描述

id	IP 标准 ACL 或 IP 扩展 ACL 的编号（1-199，1300-2699）
name	IP 标准 ACL 或 IP 扩展 ACL 的名字
in	对进入该接口的报文进行过滤
out	对从该接口输出的报文进行过滤

【缺省配置】 全局、接口模式上没有应用 ACL。

【命令模式】 全局、接口模式

【缺省级别】 14

【使用指导】 要使得 IP 标准 ACL 或 IP 扩展 ACL 生效，可以使用本命令将 ACL 应用到全局、某个接口上，这样就可以对所有接口、指定的接口上的进出的报文进行控制。

【配置举例】 1：在 fastEthernet0/0 上应用编号为 120 的 ACL 对进入的报文进行过滤：

```
Ruijie(config)# interface fastEthernet 0/0
Ruijie(config-if-GigabitEthernet 0/0)#ip access-group 120 in
```

【检验方法】 1：使用 **show ip access-group** 命令可以查看到所有 IP 标准和 IP 扩展 ACL 的应用信息

2：使用 **show ip access-group {interface } {***interface-name* | *vni***}**命令可以查看到指定接口模式上的 IP 标准和 IP 扩展 ACL 的应用信息。

【提示信息】

```
1：在接口上应用 ACL 时，如果已经有一条以下类型的 ACL 应用在该接口的同一方向上，则提示错误信息：
IP 标准 ACL、IP 扩展 ACL、MAC 扩展 ACL、专家级 ACL。
Another acl has attached at GigabitEthernet 0/2, Operation fail.
```

2：取消接口上的 ACL 应用时，如果指定的 ACL 没有应用在该接口的指定方向上，则提示错误信息：

```
The acl has not attached at %s, Operation fail
```

【常见错误】 -

【平台说明】 -

1.9 ip access-list

创建 IP 标准 ACL 或 IP 扩展 ACL，并进入 ACL 模式

ip access-list { **extended** | **standard** } { *id* | *name* }

删除该 ACL

no ip access-list { **extended** | **standard** } { *id* | *name* }

【参数说明】

参数	描述
id	IP 访问列表的编号，标准（1-99，1300-1999），扩展（100-199，2000-2699）
name	IP 访问列表的名字

【缺省配置】 没有任何 ACL

【命令模式】 全局模式

【缺省级别】 14

【使用指导】 如果只想基于源 IP 对 IP 报文进行匹配过滤，可以创建 IP 标准 ACL；如果想更想精细地控制 IP 报文，比如还想基于目的 IP 或者甚至基于四层信息来对报文进行匹配过滤，就需要创建 IP 扩展 ACL。两种 IP ACL 可匹配的字段请参考 **deny** 和 **permit** 命令的标准和扩展形式。使用 **show access-lists** 命令查看 ACL 设置。

【配置举例】 1：创建名为“std-acl”的标准 IP ACL：

```
Ruijie(config)# ip access-list standard std-acl
Ruijie(config-std-nacl)# show access-lists
ip access-list standard std-acl
Ruijie(config-std-nacl)#
```

2 ：创建编号为“123“的扩展 ACL：

```
Ruijie(config)# ip access-list extended 123
Ruijie(config-ext-nacl)# show access-lists
ip access-list extended 123
```

【检验方法】 使用 **show access-lists** 命令可以查看 ACL 配置。

【提示信息】 1：创建命名的 IP 标准或 IP 扩展 ACL 时，如果指定的名字已经被其他类型的 ACL 使用了，则提示错误信息：

```
ACL type error, current ACL has been set to type %s.
```

（其中%s 为 ip standard、ip extended、mac extended、expert extended、expert advanced 以及 ipv6 的其中之一）。

2：当创建命名的 IP 标准或 IP 扩展 ACL 时，如果设备中已创建的命名 ACL（所有类型的命名 ACL）数量已经达到 500 条，则提示错误信息：

```
Failed to create user-defined acl for the max-limit has been reached
```

3：当创建命名的 IP 标准或 IP 扩展 ACL 时，如果输入的名字长度超过 99 个字符，则提示错误信息：

```
Name is too long
```

4：当创建命名的 IP 标准或 IP 扩展 ACL 时，如果输入的名字以数字开头，或名字为“in”或“out”，则提示错误信息：

```
Invalid name
```

【常见错误】 -

【平台说明】 -

1.10 ip access-list counter

开启 IP 标准 ACL 或 IP 扩展 ACL 的报文匹配统计功能。

ip access-list counter { *id* | *name* }

关闭 IP 标准 ACL 或 IP 扩展 ACL 的报文匹配统计功能

no ip access-list counter { *id* | *name* }

【参数说明】

参数	描述
id	IP 标识 ACL 或 IP 扩展 ACL 的编号，标准（1-99，1300-1999），扩展（100-199，2000-2699）
name	IP 标准 ACL 或 IP 扩展 ACL 名字

【缺省配置】 关闭 IP 标准 ACL 或 IP 扩展 ACL 的报文匹配统计功能

【命令模式】 全局模式

【缺省级别】 14

【使用指导】 如果想监控某条 IP 标准 ACL 或 IP 扩展 ACL 的报文匹配情况，可以使用本命令开启。

【配置举例】 1：开启 IP 标准 ACL 的报文统计功能：

```
Ruijie(config)# ip access-list counter std-acl
Ruijie(config-std-nacl)# show access-lists
ip access-list standard std-acl
 10 permit 195.168.6.0 0.0.0.255 (999 matches)
 20 deny host 5.5.5.5 time-range tm (2000 matches)
```

2 ：关闭 IP 标准 ACL 的报文统计功能：

```
Ruijie(config)#no ip access-list counter std-acl
Ruijie(config-std-nacl)# show access-lists
ip access-list standard std-acl
 10 permit 195.168.6.0 0.0.0.255
```

```
20 deny host 5.5.5.5 time-range tm
```

【检验方法】 使用 **show running** 命令可以查看到哪些 ACL 上开启了报文匹配统计功能

【提示信息】 -

【常见错误】 -

【平台说明】 -

1.11 ip access-list log-update interval

配置 IPv4 ACL 报文匹配日志更新间隔
ip access-list log-update interval *time*

恢复默认值
no ip access-list log-update interval

【参数说明】

参数	描述
time	对于带日志输出选项的 ACL 规则，达到 ACL logging 输出间隔时间就输出报文命中的情况。取值范围为 [0, 1440]，默认值为 5，表示按照每隔 5 分钟输出一次某条流的 ACL 匹配日志，配置为 0 表示不输出 ACL logging。

【缺省配置】 5 分钟

【命令模式】 全局模式

【缺省级别】 14

【使用指导】 对于开启了 logging 功能的 IP 标准或 IP 扩展 ACL 的规则，只要在指定的一段时间内（默认 5 分钟）有匹配到报文，在这段时间超时时会输出一条报文匹配计数的日志信息。如果想改变这个日志输出时间间隔，可以使用本命令进行设置。

【配置举例】 1：将 IPv4 ACL 的报文匹配日志的更新门限值配置为 10 分钟：

```
Ruijie# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Ruijie(config)# ip access-list log-update interval 10
```

【检验方法】 使用 **show running** 命令可以查看到设置的 IPv4 ACL 报文匹配日志更新间隔信息。

【提示信息】 -

【常见错误】 -

【平台说明】 -

1.12 ip access-list resequence

对 IP 标准 ACL 或 IP 扩展 ACL 的规则表项的序号进行重排

ip access-list resequence { *id* | *name* } *start-sn inc-sn*

恢复默认值

no ip access-list resequence { *id* | *name* }

【参数说明】

参数	描述
id	IP 标准 ACL 或 IP 扩展 ACL 的编号，标准（1-99，1300-1999），扩展（100-199，2000-2699）
name	IP 标准 ACL 或 IP 扩展 ACL 的 ACL 名字
start-sn	序号起始值（1-2147483647）
inc-sn	序号增量（1-2147483647）

【缺省配置】 start-sn：10

inc-sn：10

【命令模式】 全局模式

【缺省级别】 14

【使用指导】 在实际使用中，有可能会在 IP 标准 ACL 或 IP 扩展 ACL 中执行多次的添加和删除规则的操作，一段时间后，序号会变得比较凌乱，此时，可以使用本命令对 ACL 规则表项的序号进行重排，使序号变规整。

【配置举例】 1：对编号为 1 的 ACL 规则表项按照起始序号为 21、增量为 43 进序号重排。

配置此命令前：

```
Ruijie# show access-lists
ip access-list standard 1
10 permit host 192.168.4.12
20 deny any any
```

配置此命令之后：

```
Ruijie# config
Ruijie(config)# ip access-list resequence 1 21 43
Ruijie(config)# exit
Ruijie# show access-lists
```

```
ip access-list standard 1
21 permit host 192.168.4.12
64 deny any any
```

【检验方法】 1：使用 **show access-lists** 命令可以查看到所有 ACL 下的规则表项最新序号。
2：使用 **show access-lists** *id* 命令可以查看到指定 ACL 下的规则表项最新序号。
3：使用 **show access-lists** *name* 令可以查看到指定 ACL 下的规则表项最新序号。

【提示信息】 -

【常见错误】 -

【平台说明】 -

1.13 ipv6 access-list

创建 IPv6 ACL，并进入该配置模式
ipv6 access-list *name*

删除该 ACL
no ipv6 access-list *name*

【参数说明】

参数	描述
name	IPv6 ACL 名字

【缺省配置】 没有 IPv6 ACL

【命令模式】 全局模式

【缺省级别】 14

【使用指导】 如果要对网络中的 IPv6 报文进行安全过滤，需要使用 IPv6 ACL，首先要使用本命令创建 IPv6 ACL。

【配置举例】 1：创建名为“v6-acl ”的 IPv6 ACL：

```
Ruijie(config)# ipv6 access-list v6-acl
Ruijie(config-ipv6-nacl)# show access-lists
ipv6 access-list v6-acl
Ruijie(config-ipv6-nacl)#
```

【检验方法】 1：使用 **show access-lists** 命令可以看到所有 ACL（包括 IPv6 ACL）的配置信息。
2：使用 **show access-lists** *name* 命令可以看到指定 ACL（包括 IPv6 ACL）的配置信息

【提示信息】 -

【常见错误】 -

【平台说明】 -

1.14 ipv6 access-list counter

开启 IPv6 ACL 的报文匹配统计功能
ipv6 access-list counter *name*

关闭该 ACL 的报文匹配统计功能
no ipv6 access-list counter*name*

【参数说明】

参数	描述
name	IPv6 ACL 的名字

【缺省配置】 关闭 IPv6 ACL 的报文匹配统计功能

【命令模式】 全局模式

【缺省级别】 14

【使用指导】 要了解 IPv6 ACL 的运行情况，可以通过本命令开启 IPv6 ACL 的报文匹配统计功能，达到监控 IPv6 报文的匹配过滤情况。

【配置举例】 1：开启 IPv6 ACL 的报文匹配统计功能：

```
Ruijie(config)# ipv6 access-list v6-acl
Ruijie(config-ipv6-nacl)# show access-lists
ipv6 access-list v6-acl
 10 permit icmp any any (7 matches)
 20 deny tcp any any (7 matches)
```

2：关闭 IPv6 ACL 的报文匹配统计功能：

```
Ruijie(config)#no ipv6 access-list v6-acl counter
Ruijie(config-ipv6-nacl)# show access-lists
ipv6 access-list v6-acl
 10 permit icmp any any
```

```
20 deny tcp any any
```

【检验方法】 使用 **show running** 命令可以查看到到哪些 ACL 上开启了报文匹配统计功能

【提示信息】 -

【常见错误】 -

【平台说明】 -

1.15 ipv6 access-list log-update interval

配置 IPv6 ACL 报文匹配日志更新间隔
ipv6 access-list log-update interval *time*

恢复默认值
no ipv6 access-list log-update interval

【参数说明】

参数	描述
time	对于带日志输出选项的 ACL 规则 ,达到 ACL logging 输出间隔时间就输出报文命中的情况。取值范围为 [0, 1440] , 默认值为 5 , 表示按照每隔 5 分钟输出一次某条流的 ACL 匹配日志，配置为 0 表示不输出 ACL logging。

【缺省配置】 5 分钟

【命令模式】 全局模式

【缺省级别】 14

【使用指导】 对于开启了 logging 功能的 IPv6 ACL，只要在指定的一段时间内（默认 5 分钟）有匹配到报文，在这段时间超时时会输出一条报文匹配计数的日志信息。如果想改变这个日志输出时间间隔，比如想每隔 10 分钟输出这 10 分钟内的 IPv6 ACL 规则匹配到的 IPv6 报文匹配统计日志，可以使用本命令进行设置。

【配置举例】 1：将 IPv6 ACL 的报文匹配日志的更新间隔配置为 10 分钟。

```
Ruijie# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Ruijie(config)# ipv6 access-list log-update interval 9
```

【检验方法】 使用 **show running** 命令可以查看到哪些 ACL 上设置了报文匹配日志更新间隔。

【提示信息】 -

【常见错误】 -

【平台说明】 -

1.16 ipv6 access-list resequence

对 IPV6 ACL 的规则表项的序号进行重排

ipv6 access-list resequence *name start-sn inc-sn*

恢复默认值

no ipv6 access-list resequence *name*

【参数说明】

参数	描述
name	IPv6 ACL 名字
start-sn	序号起始值（1-2147483647）
inc-sn	序号增量（1-2147483647）

【缺省配置】 start-sn：10

inc-sn：10

【命令模式】 全局模式

【缺省级别】 14

【使用指导】 在实际使用中，有可能会在 IPV6 ACL 中执行多次的添加和删除规则的操作，一段时间后，序号会变得比较凌乱，此时，可以使用本命令对 ACL 规则表项的序号进行重排，使序号变规整。

【配置举例】 1：对名为“v6-acl ”的 IPv6 ACL 规则表项按照起始序号为 21、增量为 43 进序号重排。

配置此命令前：

```
Ruijie# show access-lists
ipv6 access-list v6-acl
 10 permit ipv6 any any
 20 deny ipv6 any any
```

配置此命令之后：

```
Ruijie# config
Ruijie(config)# ipv6 access-list resequence v6-acl 21 43
Ruijie(config)# exit
Ruijie# show access-lists
```

```
ipv6 access-list v6-acl
 21 permit ipv6 any any
 64 deny ipv6 any any
```

【检验方法】 1：使用 **show access-lists** 命令可以查看到所有 ACL 下的规则表项最新序号。
2：使用 **show access-lists** *name* 令可以查看到指定 ACL 下的规则表项最新序号。

【提示信息】 -

【常见错误】 -

【平台说明】 -

1.17 ipv6 traffic-filter

将一条 IPv6 ACL 应用到指定 vxlan 模式或者接口上
ipv6 traffic-filter *name* { **in** | **out** }

取消 IPv6 ACL 应用
no ipv6 traffic-filter *name* { **in** | **out** }

【参数说明】

参数	描述
name	IPv6 ACL 的名字
in	对进入该接口的报文进行过滤
out	对从该接口输出的报文进行过滤

【缺省配置】 接口、vxlan 模式上没有应用 IPv6 ACL。

【命令模式】 接口、vxlan 模式

【缺省级别】 14

【使用指导】 要使得 IPv6 ACL 生效，可以使用本命令将 ACL 应用到某个 vxlan 模式或者接口上，这样就可以实现对该 vxlan 模式或者接口上的进出的 IPv6 报文进行控制。

【配置举例】 1：将 access-list v6-acl 应用于 Gigabit 接口 0/1 上：

```
Ruijie(config)# interface GigaEthernet 0/1
Ruijie(config-if-GigabitEthernet 0/1)# ipv6 traffic-filter v6-acl in
```

2：将 access-list v6-acl 应用于 vxlan 1 上：

```
Ruijie(config)#vxlan 1
Ruijie(config-vxlan)#ipv6 traffic-filter v6-acl in
```

【检验方法】 1：使用 **show ipv6 traffic-filter** 命令可以查看到所有 IPv6 ACL 的应用配置。
2：使用 **show ipv6 traffic-filter {interface | vxlan} {***interface-name* | *vni}* 命令可以查看到指定接口或 vxlan 模式上的 IPv6 ACL 应用配置。

【提示信息】 -

【常见错误】 -

【平台说明】 -

1.18 list-remark

为指定的 ACL 添加注释信息
list-remark *text*

删除 ACL 注释信息
no list-remark

【参数说明】

参数	描述
text	注释信息

【缺省配置】 没有 ACL 注释信息

【命令模式】 ACL 模式

【缺省级别】 14

【使用指导】 为了便于查看某条 ACL 的作用，可以使用本命令为指定的 ACL 添加注释信息。也可以在全局配置模式下直接使用 **access-list list-remark** 命令为 ACL 添加注释信息。

【配置举例】 1：为编号为 102 的 IP 扩展 ACL 添加“this acl is to filter the host 192.168.4.12”的注释信息：

```
Ruijie(config)# ip access-list extended 102
Ruijie(config-ext-nacl)# list-remark this acl is to filter the host 192.168.4.12
Ruijie(config-ext-nacl)# show access-lists
ip access-list extended 102
deny ip host 192.168.4.12 any
1000 hits
this acl is to filter the host 192.168.4.12
Ruijie(config-ext-nacl)#
```

【检验方法】 1：使用 **show access-lists** 命令可以查看到所有 ACL 的配置信息，包括 ACL 的注释信息。
2：使用 **show access-lists** *id* 命令可以查看到指定 ACL 的配置信息，包括该 ACL 的注释信息。
3：使用 **show access-lists** *name* 令可以查看到指定 ACL 的配置信息，包括该 ACL 的注释信息。

【提示信息】 -

【常见错误】 -

【平台说明】 -

1.19 permit

往一条 ACL 中添加/删除一个允许类型的 ACL 规则。

5. IP 标准 ACL

- 往 IP 标准 ACL 中添加一条允许类型的 ACL 规则

[*sn*] **permit** { *source source-wildcard* | **host** *source* | **any** } [**time-range** *tm-range-name*] [**log**]

- 从 IP 标准 ACL 中删除一条允许类型的 ACL 规则

no { *sn* | { **permit** { *source source-wildcard* | **host** *source* | **any** } [**time-range** *tm-range-name*] [**log**] } }

6. IP 扩展 ACL

- 往 IP 扩展 ACL 中添加一条允许类型的 ACL 规则

[*sn*] **permit protocol** *source source-wildcard destination destination-wildcard* [**precedence** *precedence*] [**range** *lower upper*] [**time-range** *time-range-name*] [**log**]

- 从 IP 扩展 ACL 中删除一条允许类型的 ACL 规则

no { *sn* | { **permit protocol** *source source-wildcard destination destination-wildcard* [**precedence** *precedence*] [**range** *lower upper*] [**time-range** *time-range-name*] [**log**] } }

一些重要协议的 IP 扩展访问控制列表：

Internet Control Message Protocol (ICMP)：
[*sn*] **permit icmp** { *source source-wildcard* | **host** *source* | **any** } { *destination destination-wildcard* | **host** *destination* | **any** } [*icmp-type*] [[*icmp-type* [*icmp-code*]] | [*icmp-message*]] [**precedence** *precedence*] [**time-range** *time-range-name*]

Transmission Control Protocol (TCP)：

[*sn*] **permit tcp** { *source source-wildcard* | **host** *Source* | **any** } [*operator* **port** [*port*]] { *destination destination-wildcard* | **host** *destination* | **any** } [*operator* **port** [*port*]] [**precedence** *precedence*] [**range** *lower upper*] [**time-range** *time-range-name*]

User Datagram Protocol (UDP)：
[*sn*] **permit udp** { *source source –wildcard* | **host** *source* | **any** } [*operator* **port** [*port*]] { *destination destination-wildcard* | **host** *destination* | **any** } [**operator port** [*port*]] [**precedence** *precedence*] [**range** *lower upper*] [**time-range** *time-range-name*]

7. MAC 扩展 ACL

- 往 MAC 扩展 ACL 中添加一条允许类型的 ACL 规则

[*sn*] **permit** { **any** | *source-mac-address mask*} { **any** | *destination -mac-address mask* } [**cos** [*out*] [**inner** *in*]]

- 从 MAC 扩展 ACL 中删除一条允许类型的 ACL 规则

no { *sn* | { **permit** { **any** | *source-mac-address mask*} { **any** | *destination -mac-address mask* } [**cos** [*out*] [**inner** *in*]] } }

8. 专家级扩展 ACL

- 往专家级扩展 ACL 中添加一条允许类型的 ACL 规则

[*sn*] **permit** [**protocol** | [**cos** [*out*] [**inner** *in*]]] [**VID** [*out*] [**inner** *in*]] { *source source-wildcard* | **host** *source* | **any** } { **any** } { *destination destination-wildcard* | **host** *destination* | **any** } { **any** } [**precedence** *precedence*] [**range** *lower upper*] [**time-range** *time-range-name*]

- 从专家级扩展 ACL 中删除一条允许类型的 ACL 规则

no { *sn* | { **permit** [**protocol** | [**cos** [*out*] [**inner** *in*]]] [**VID** [*out*] [**inner** *in*]] { *source source-wildcard* | **host** *source* | **any** } { **any** } { *destination destination-wildcard* | **host** *destination* | **any** } { **any** } [**precedence** *precedence*] [**range** *lower upper*] [**time-range** *time-range-name*] } }

选择字段包含以太网类型或 cos 字段时：
[*sn*] **permit** { **cos** [*out*] [**inner** *in*] } [**VID** [*out*] [**inner** *in*]] { *source source-wildcard* | **host** *source* | **any** } { **any** } { *destination destination-wildcard* | **host** *destination* | **any** } { **any** } [**time-range** *time-range-name*]

选择协议 Protocol 字段时：
[*sn*] **permit protocol** [**VID** [*out*] [**inner** *in*] { *source source-wildcard* | **host** *Source* | **any** } { **any** } { *destination destination-wildcard* | **host** *destination* | **any** } { **any** } [**precedence** *precedence*] [**range** *lower upper*] [**time-range** *time-range-name*]

一些重要协议的 Expert 扩展访问列表：

Internet Control Message Protocol (ICMP)：

[*sn*] **permit icmp** [**VID** [*out*] [**inner** *in*]] { *source source-wildcard* | **host** *source* | **any** } { **any** } { *destination destination-wildcard* | **host** *destination* | **any** } { **any** } [*icmp-type*] [[*icmp-type* [*icmp-code*]] | [*icmp-message*]] [**precedence** *precedence*] [**time-range** *time-range-name*]

Transmission Control Protocol (TCP)：

[*sn*] **permit tcp** [**VID** [*out*] [**inner** *in*]] { *source source-wildcard* | **host** *Source* | **any** } { **any** } [*operator* **port** [*port*]] { *destination destination-wildcard* | **host** *destination* | **any** } { **any** } [*operator* **port** [*port*]] [**precedence** *precedence*] [**range** *lower upper*] [**time-range** *time-range-name*]

User Datagram Protocol (UDP)

[*sn*] **permit udp** [**VID** [*out*] [**inner** *in*]] { *source source –wildcard* | **host** *source* | **any** } { **any** } [*operator* **port** [*port*]] { *destination destination-wildcard* | **host** *destination* | **any** } { **any** } [*operator* **port** [*port*]] [**precedence** *precedence*] [**range** *lower upper*] [**time-range** *time-range-name*]

Address Resolution Protocol (ARP)

[*sn*] **permit arp** { **vid** *vlan-id* } [**any**] [**host** *destination –mac-address* | **any**] { *sender-ip sender-ip–wildcard* | **host** *sender-ip* | **any** } { *sender-mac sender-mac-wildcard* | **host** *sender-mac* | **any** } { *target-ip target-ip–wildcard* | **host** *target-ip* | **any** }

9. 专家级高级 ACL

- 往专家级高级 ACL 中添加一条允许类型的 ACL 规则

[*sn*] **permit** *hex hex-mask offset*

- 从专家级高级 ACL 中删除一条允许类型的 ACL 规则

no { *sn* | **permit** *hex hex-mask offset* }

【参数说明】

参数	描述
sn	ACL 规则序号
time-range	报文过滤的时间区
time-range-name	报文过滤的时间区名称

【缺省配置】 没有 ACL 规则配置

【命令模式】 ACL 模式

【缺省级别】 14

【使用指导】 当想允许某些报文进入网络时，可以使用该命令往指定的 ACL 里添加一些允许类型的 ACL 规则。

【配置举例】 1：下例显示如何创建及显示一条 Expert Extended ACL，该专家 ACL 允许源 IP 地址为 192.168.4.12 并且源 MAC 地址为 001300498272 的所有 TCP 报文。

```
Ruijie(config)# expert access-list extended exp-acl
Ruijie(config-exp-nacl)# permit tcp  host  192.168.4.12 host 0013.0049.8272 any any
Ruijie(config-exp-nacl)# deny any any any any
Ruijie(config-exp-nacl)# show access-lists
expert access-list extended exp-acl
10 permit tcp  host  192.168.4.12 host 0013.0049.8272 any any
20 deny any any any any
Ruijie(config-exp-nacl)#
```

2：下面是 IP 扩展 ACL 使用范例，目的是准许 IP 为 192.168.4.12 的源主机提供 TCP 端口为 100 的服务，并应用到接口 gigabitethernet 1/1。配置方法：

```
Ruijie(config)# ip access-list extended 102
Ruijie(config-ext-nacl)# permit tcp host 192.168.4.12 eq 100 any
Ruijie(config-ext-nacl)# show access-lists
ip access-list extended 102
10 permit tcp host 192.168.4.12 eq 100 any
Ruijie(config-ext-nacl)# exit
Ruijie(config)# interface gigabitethernet 1/1
Ruijie(config-if-GigabitEthernet 1/1)# ip access-group 102 in
```

3：下面是 MAC 扩展 ACL 使用范例，目的是准许 MAC 为 0013.0049.8272 的源主机发送类型为 100 的以太网帧，并应用到接口 gigabitethernet 1/1。配置方法：

```
Ruijie(config)# mac access-list extended 702
Ruijie(config-mac-nacl)# permit host 0013.0049.8272 any aarp
Ruijie(config-mac-nacl)# show access-lists
mac access-list extended
10 permit host 0013.0049.8272 any aarp702
Ruijie(config-mac-nacl)# exit
Ruijie(config)# interface gigabitethernet 1/1
Ruijie(config-if-GigabitEthernet 1/1)# mac access-group 702 in
```

4：下面是 ip 标准 ACL 使用范例，目的是允许 IP 为 192.168.4.12 的源主机，并应用到接口 1。配置方法：

```
Ruijie(config)# ip access-list standard std-acl
Ruijie(config-std-nacl)# permit host 192.168.4.12
Ruijie(config-std-nacl)# show access-lists
ip access-list standard std-acl
10 permit host 192.168.4.12
Ruijie(config-std-nacl)# exit
```

```
Ruijie(config)# interface gigabitethernet 1/1
Ruijie(config-if-GigabitEthernet 1/1)# ip access-group std-acl in
```

5：下面是专家级高级 ACL 使用范例，目的是允许 IP 为 192.168.4.12 的源主机，并应用到接口 gigabitethernet 1/1。配置方法：

```
Ruijie(config)# expert access-list advanced adv-acl
Ruijie(config-exp-dacl)# permit a0c8040c ffffffff 38
Ruijie(config-exp-dacl)# show access-lists
expert access-list advanced adv-acl
 10 permit a0c8040c ffffffff 38
Ruijie(config-exp-dacl)# exit
Ruijie(config)# interface gigabitethernet 1/1
Ruijie(config-if)# expert access-group adv-acl in
```

【检验方法】 1：使用 **show access-lists** 命令可以查看到所有 ACL 的配置信息，包括 ACL 下配置的所有规则。
2：使用 **show access-lists** *id* 命令可以查看到指定 ACL 的配置信息，包括该 ACL 下配置的所有规则。
3：使用 **show access-lists** *name* 令可以查看到指定 ACL 的配置信息，包括该 ACL 下配置的所有规则。

【提示信息】 -

【常见错误】 -

【平台说明】 -

1.20 remark

在 ACL 中给 ACE 添加注释信息
remark *text*

删除 ACE 注释信息
no remark *text*

【参数说明】

参数	描述
text	注释信息

【缺省配置】 ACE 没有注释信息

【命令模式】 ACL 模式

【缺省级别】 14

【使用指导】 为指定的 ACE 添加注释信息。

只允许至多 100 个字符，不允许一个 ACL 内出现 2 条相同内容注释。

删除 ace 时候会将该条 ace 与对应的注释信息也一起删除。

【配置举例】 1：在编号为 102 的 IP 扩展 ACL 中为 ACE 添加注释信息：

```
Ruijie(config)# ip access-list extended 102
Ruijie(config-ext-nacl)# remark first_remark
Ruijie(config-ext-nacl)# permit tcp 1.1.1.1 0.0.0.0 2.2.2.2 0.0.0.0
Ruijie(config-ext-nacl)# remark second_remark
Ruijie(config-ext-nacl)# permit tcp 3.3.3.3 0.0.0.0 4.4.4.4 0.0.0.0
Ruijie(config-ext-nacl)# end
Ruijie#
```

【检验方法】 1：使用 **show access-lists** 命令可以查看到所有 ACL 的配置信息。包括 ACL 规则表项的注释信息。
2：使用 **show access-lists** *id* 命令可以查看到指定 ACL 的配置信息。包括 ACL 规则表项的注释信息。
3：使用 **show access-lists** *name* 令可以查看到指定 ACL 的配置信息。包括 ACL 规则表项的注释信息。

【提示信息】 -

【常见错误】 -

【平台说明】 -

1.21 show access-group

显示接口上应用的 ACL 配置

show access-group [**interface** *interface-name*] | [**wlan** wlan-id]

【参数说明】

参数	描述
interface *Interface-name*	指定的接口名字
wlan *wlan-id*	指定的 wlan-id

【命令模式】 特权模式

【缺省级别】 14

【使用指导】 如果想查看指定接口上是否有应用 ACL，或者想查看哪些接口上有应用了 ACL，可以使用本命令。

【配置举例】 1：查看设备中有哪些接口上应用了 ACL，以及应用的方向：

```
Ruijie# show access-group
```

```
ip access-list standard ipstd3 in
Applied On interface GigabitEthernet 0/1.
ip access-list standard ipstd4 out
Applied On interface GigabitEthernet 0/2.
ip access-list extended 101 in
Applied On interface GigabitEthernet 0/3.
ip access-list extended 102 in
Applied On interface GigabitEthernet 0/8.
```

2：查看接口 GigabitEthernet 0/3 上是否应用了 ACL，以及应用的方向：

```
Ruijie# show access-group interface GigabitEthernet 0/3
ip access-list extended 101
Applied On interface GigabitEthernet 0/3 in.
```

【提示信息】 -

【平台说明】 -

1.22 show access-lists

显示所有 ACL 配置或指定的 ACL 的配置

show access-lists [*id* | *name*] [**summary**]

【参数说明】

参数	描述
id	ACL 的编号
name	ACL 的名字
summary	ACL 的汇总信息

【命令模式】 全局模式

【缺省级别】 14

【使用指导】 显示指定的 ACL 配置信息，若没有指定 ACL 编号或名字，则显示所有的 ACL 配置信息。

【配置举例】 1：查看名字为“n_acl”的 ACL 配置信息：

```
Ruijie# show access-lists n_acl
ip access-list standard n_acl
Ruijie# show access-lists 102
ip access-list extended 102
```

2：查看所有 ACL 配置信息：

```
Ruijie# show access-lists
```

```
ip access-list standard n_acl
ip access-list extended 101
  permit icmp host 192.168.1.1 any log (1080 matches)
  permit tcp host 1.1.1.1 any established
  deny ip any any (80021 matches)
mac access-list extended mac-acl
expert access-list extended exp-acl
ipv6 access-list extended v6-acl
  petmit ipv6 ::192.168.4.12 any (100 matches)
  deny any any (9 matches)
```

【提示信息】 -

【平台说明】 -

1.23 show ip access-group

显示接口上应用的 IP 标准和 IP 扩展 ACL 配置

show ip access-group [**interface** *interface-name*] | [**wlan** wlan-id]

【参数说明】

参数	描述
interface *Interface-name*	指定的接口名字
wlan *wlan-id*	指定的 wlan-id

【命令模式】 特权模式

【缺省级别】 14

【使用指导】 显示接口上应用的 IP 标准和 IP 扩展 ACL，若没有指定接口，则显示所有接口上应用的 IP 标准 和 IP 扩展 ACL。

【配置举例】 1：查看接口 GigabitEthernet 0/1 上是否应用了 IP 标准和 IP 扩展 ACL，以及应用的方向：

```
Ruijie# show ip access-group interface gigabitethernet 0/1
ip access-group aaa in
Applied On interface GigabitEthernet 0/1.
```

【提示信息】 -

【平台说明】 -

1.24 show ipv6 traffic-filter

显示接口上应用的 IPv6 ACL 配置

show ipv6 traffic-filter [**interface** *interface-name*]

【参数说明】

参数	描述
interface *Interface-name*	指定的接口名字

【命令模式】 特权模式

【缺省级别】 14

【使用指导】 显示接口上应用的 IPv6 ACL，若没有指定接口，则显示所有接口上应用的 IPv6 ACL。

【配置举例】 1：查看接口 GigabitEthernet 0/1 上是否应用了 IPv6 ACL，以及应用的方向：

```
Ruijie# show ipv6 traffic-filter interface gigabitethernet 0/4
ipv6 traffic-filter v6 in
Applied On interface GigabitEthernet 0/4.
```

【提示信息】 -

【平台说明】 -

2 RPL

2.1 reverse-path

开启 RPL 模块。
reverse-path

关闭 RPL 模块。
no reverse-path

恢复缺省配置。
default reverse-path

【参数说明】

参数	描述
-	-

【缺省配置】 关闭 RPL 模块。

【命令模式】 接口模式

【缺省级别】 14

【使用指导】 保证通过该接口的新的数据流，其反向流能够经过该接口原路返回，使用本命令的 no 形式取消此项设置，该命令只适用于新建流。

【配置举例】 1：启动 RPL 模块功能。

```
Ruijie(config-if-GigabitEthernet 0/1)# reverse-path
```

2：关闭 RPL 模块功能。

```
Ruijie(config-if-GigabitEthernet 0/1)#no reverse-path
```

【检验方法】 show running-config 可以看到相关配置

【提示信息】 -

【常见错误】 -

【平台说明】 -

3 REF-RNFP

3.1 acpp

配置 acpp。
acpp bw-rate *rate* **bw-burst-rate** *burst-rate* [**log**]

关闭 acpp。
no acpp

恢复缺省配置。
default acpp

【参数说明】

参数	描述
rate	速率限制（单位为 pps）。可配置范围为 1-600。
burst-rate	突发速率限制（单位为 pps）。可配置范围为 1-600。
log	控制台打印 log。

【缺省配置】 缺省情况下，ACPP 是关闭的。

【命令模式】 control-plane 配置模式，可以配置在三个子接口

【缺省级别】 14

【使用指导】 要配置集中控制平面保护（ACPP），请在 control-plane 配置模式下使用命令 acpp。

【配置举例】 1：以下的配置例子，配置业务类的流量速率为 200pps，允许的突发值为 300pps。

```
Ruijie(config)# control-plane data
Ruijie(config-cp)# acpp bw-rate 200 bw-burst-rate 300
```

【检验方法】 1：使用 **show ef-rnfp acpp** { **data** | **manage** | **protocol** }命令，可以查看 acpp 是启用还是关闭，以及其丢包状态。

【提示信息】 1：如果在子接口上没有配置对应的 acpp 策略，在进行 no 或者 default 操作的时候会提示删除策略失败。

```
Ruijie(config)# control-plane manage
Ruijie(config-cp)# no acpp
EF-RNFP: delete acpp rule failed
Ruijie(config-cp)# default acpp
EF-RNFP: delete acpp rule failed
```

【常见错误】 -

【平台说明】 -

3.2 anti-arp-spoof

配置 arp 攻击探测。
anti-arp-spoof [**scan** *arp-num*]

关闭 arp 攻击探测。
no anti-arp-spoof [**scan** *arp-num*]

恢复缺省配置。
default anti-arp-spoof [**scan** *arp-num*]

【参数说明】

参数	描述
anti-arp-spoof	开启 arp 攻击检测功能。
arp-num	配置 arp 扫描值。

【缺省配置】 缺省情况下，功能是关闭的。

【命令模式】 Control-plane 配置模式

【缺省级别】 14

【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】 1：开启 arp 攻击检测，并设置 arp 扫描阀值为 30。

```
Ruijie(config)# control-plane
Ruijie(config-cp)# anti-arp-spoof
Ruijie(config-cp)# anti-arp-spoof 30
```

【检验方法】 1：使用 **show ef-rnfp anti-arp-spoof** 命令，可以查看本功能是启用还是关闭。
2：使用 **show arp-suspect** 命令，可以查看当前 arp 嫌疑列表。

【提示信息】 -

【常见错误】 -

【平台说明】 -

3.3 arp-car

配置 arp-car 限速。
arp-car *packet_rate_per_group* [**log**]

关闭 arp-car。
no arp-car

恢复缺省配置。
default arp-car

【参数说明】

参数	描述
packet_rate_per_group	arp-car 限速值（单位为 pps）。可配置范围为 1-20
log	控制台打印 log

【缺省配置】 缺省情况下，arp-car 是关闭的。

【命令模式】 control-plane 配置模式，只能配置在管理类子接口。

【缺省级别】 14

【使用指导】 要对接收到的 ARP 报文进行限速，配置 Glean-CAR 限速，请在 control-plane 配置模式下使用命令 arp-car。

【配置举例】 1：以下的配置例子，在管理类子接口上，对哈希到同一个组的用户（源）发起的 ARP 的流限速为 10pps。

```
Ruijie(config)# control-plane manage
Ruijie(config-cp)# arp-car 10
```

【检验方法】 1：使用 **show ef-rnfp arp-car** 命令，可以查看 arp-car 是启用还是关闭，以及其丢包状态。

【提示信息】 1：如果在业务类子接口上没有配置对应的 glean-car 策略，在进行 no 或者 default 操作的时候会提示删除策略失败。

```
Ruijie(config)# control-plane data
Ruijie(config-cp)# no glean-car
EF-RNFP: delete glean-car rule failed
Ruijie(config-cp)# default glean-car
EF-RNFP: delete glean-car rule failed
```

【常见错误】 -

【平台说明】 -

3.4 attack threshold

配置攻击确认阀值。
attack threshold *drop-num*

删除攻击确认阀值。
no attack threshold

恢复缺省配置。
default attack threshold

【参数说明】

参数	描述
drop-num	丢包速率超过该值就判断为被攻击。可配置范围为 100~100000pps。

【缺省配置】 attack threshold 500

【命令模式】 Control-plane 配置模式

【缺省级别】 14

【使用指导】 当每秒丢包达到该值时设备认为网络中存在攻击，当本身网络环境就比较脏的情况，建议将该值配置的大一些。

【配置举例】 1：配置攻击判断阀值为 1000。

```
Ruijie(config)# control-plane
Ruijie(config-cp)# attack threshold 1000
```

【检验方法】 1：使用 **show run** 命令，可以查看攻击阀值的具体值大小。

【提示信息】 -

【常见错误】 -

【平台说明】 -

3.5 clear attack-info history

清空攻击历史记录。

clear attack-info history

【参数说明】

参数	描述
history	攻击历史记录。

【缺省配置】 -

【命令模式】 特权模式

【缺省级别】 14

【使用指导】 -

【配置举例】 1：清空历史记录。

```
Ruijie# clear attack-info history
```

【检验方法】 1：使用 **show attack-info history** 命令，可以查看攻击历史信息。

【提示信息】 清空成功提示如下。

```
Ruijie# clear attack-info history
The history attack record has been cleared!
```

3.6 control-plane

进入 control-plane 配置模式。

control-plane [**protocol** | **manage** | **data**]

【参数说明】

参数	描述
protocol	进入协议子接口。
manage	进入管理子接口。
data	进入数据子接口。
-	配置本地防攻击全局参数。

【缺省配置】 -

【命令模式】 全局模式

【缺省级别】 14

【使用指导】 由于不同的规则在不同的子接口下面，所以需要进入各个不同的子接口，才能配置不同的限速规则。

【配置举例】 1：进入协议子接口。

```
Ruijie(config)# control-plane protocol
Ruijie(config-cp)#
```

【检验方法】 -

【提示信息】 -

【常见错误】 -

【平台说明】 -

3.7 ef-rnfp enable

开启本地防攻击功能开关。
ef-rnfp enable

关闭本地防攻击。
no ef-rnfp enable

恢复缺省配置。
default ef-rnfp enable

【参数说明】

参数	描述
enable	功能开关。

【缺省配置】 缺省情况下，开关是关闭的。

【命令模式】 control-plane 配置模式

【缺省级别】 14

【使用指导】 启用设备防攻击可以使用命令 ef-rnfp enable，只有配置了这条命令设备防攻击才会开启。
如果在开启时各个子接口上没有配置任何的策略的话，那么就自动生成默认的限速策略。

【配置举例】 1：以下的配置例子，开启设备防攻击。

```
Ruijie(config)# control-plane
Ruijie(config-cp)# ef-rnfp enable
```

【检验方法】 1：使用 **show run** 命令，可以查看本地防攻击是启用还是关闭。

【提示信息】 -

【常见错误】 -

【平台说明】 -

3.8 glean-car

配置 glean-car 限速。
glean-car *packet_rate_per_group* [**log**]

关闭 glean-car。
no glean-car

恢复缺省配置。
default glean-car

【参数说明】

参数	描述
packet_rate_per_group	glean-car 限速值（单位为 pps）。
log	控制台打印 log

【缺省配置】 缺省情况下，Glean-CAR 是关闭的。

【命令模式】 control-plane 配置模式，只能配置在业务类子接口

【缺省级别】 14

【使用指导】 要对路由后匹配到直连路由但目的 IP 还没有解析的流量，配置 Glean-CAR 限速，请在 control-plane 配置模式下使用命令 glean-car。

【配置举例】 1：以下的配置例子，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为 10pps。

```
Ruijie(config)# control-plane data
Ruijie(config-cp)# glean-car 10
```

【检验方法】 使用 **show ef-rnfp glean-car** 命令，可以查看 glean-car 是启用还是关闭，以及其丢包状态。

【提示信息】 如果在业务类子接口上没有配置对应的 glean-car 策略，在进行 no 或者 default 操作的时候会提示删除策略失败。

```
Ruijie(config)# control-plane data
Ruijie(config-cp)# no glean-car
EF-RNFP: delete glean-car rule failed
Ruijie(config-cp)# default glean-car
EF-RNFP: delete glean-car rule failed
```

【常见错误】 -

【平台说明】 -

3.9 management-interface

配置管理平面保护。
management-interface *interface* **allow** { **ftp** | **http** | **ssh** | **snmp** | **telnet** | **tftp** } [**log**]

关闭某个接口的管理平面保护。
no management-interface *interface*

恢复缺省配置。
default management-interface

【参数说明】

参数	描述
interface	指定的管理接口。
ftp	配置只有指定的管理接口能接受 ftp 协议
http	配置只有指定的管理接口能接受 http 协议
ssh	配置只有指定的管理接口能接受 ssh 协议
snmp	配置只有指定的管理接口能接受 snmp 协议
telnet	配置只有指定的管理接口能接受 telnet 协议
tftp	配置只有指定的管理接口能接受 tftp 协议
log	控制台打印 log

【缺省配置】 缺省情况下，MPP 功能是关闭的。

【命令模式】 control-plane 配置模式，只能配置在管理类子接口。

【缺省级别】 14

【使用指导】 管理平面保护（MPP）功能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。要配

置 MPP，请在 control-plane 配置模式下使用命令 management-interface。

【配置举例】 1：以下的配置例子，指定 gi0/0 口为带内管理接口，并只允许 gi0/0 口接收 telnet，snmp 管理协议报文：

```
Ruijie(config)# control-plane manage
Ruijie(config-cp)# management-interface gi 0/0 allow snmp telnet
```

【检验方法】 1：使用 **show ef-rnfp mpp** 命令，可以查看 mpp 是启用还是关闭，以及其丢包状态。

【提示信息】 1：如果在管理类子接口上没有配置对应的 mpp 策略，在进行 no 操作的时候会提示删除策略失败。

```
Ruijie(config)# control-plane manage
Ruijie(config-cp)# no management-interface gi 0/1
EF-RNFP: delete mpp rule failed
```

【常见错误】 -

【平台说明】 -

3.10 port-filter

配置 port-filter。
port-filter [**log**]

关闭 port-filter。
no port-filter

恢复缺省配置。
default port-filter

【参数说明】

参数	描述
port-filter	开启功能。
log	控制台打印 log

【缺省配置】 缺省情况下，port-filter 是关闭的。

【命令模式】 control-plane 配置模式，只能配置在管理类子接口

【缺省级别】 14

【使用指导】 port-Filter 功能可以过滤掉到达的本地的非法传输层报文，这些报文的目的端口在本地并没有被打开。需要配置 port-Filter 功能请在 control-plane 配置模式下使用命令 port-filter。

【配置举例】 1：以下的配置例子，在管理类子接口上，启用 Port-Filter 功能：

```
Ruijie(config)# control-plane manage
Ruijie(config-cp)# port-filter
```

【检验方法】 1：使用 **show ef-rnfp port-filter** 命令，可以查看 port-filter 是启用还是关闭，以及其丢包状态。

【提示信息】 1：如果在业务类子接口上没有配置对应的 port-filter 策略，在进行 no 或者 default 操作的时候会提示删除策略失败。

```
Ruijie(config)# control-plane manage
Ruijie(config-cp)# no port-filter
EF-RNFP: delete port-filter rule failed
Ruijie(config-cp)# default port-filter
EF-RNFP: delete port-filter rule failed
```

【常见错误】 -

【平台说明】 -

3.11 scpp

配置分类控制平面保护（SCPP），在每类流量内根据策略来进一步进行流量区分和限速：连接限制，半连接控制，流量带宽限制。

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**]

关闭 SCPP。

no scpp list *acl_no*

恢复缺省配置。

default scpp

【参数说明】

参数	描述
acl_no	匹配策略，对匹配的流进行区分和限速。
bw-rate *rate* **bw-burst-rate** *burst-rate*	配置速率限制和突发速率限制，单位 pps。
conn-create-rate *create-rate* **conn-create-burst-rate** *create-burst-rate*	配置新建连接速率和突发新建连接速率。
conn-total *num*	配置允许的总连接数。
log	是否记录 log 信息。

【缺省配置】 缺省情况下，SCPP 功能是关闭的。

【命令模式】 control-plane 配置模式，可以配置在三个子接口。

【缺省级别】 14

【使用指导】 -

【配置举例】 在管理类子接口上，对 192.168.52.0 网段发起的到本地管理类子接口上的 TCP 协议报文流量，限速为 100pps，允许的突发值为 150pps；允许得连接总数为 30 个，新建连接速率为 5 个每秒，突发新建连接速率为 7 个每秒。

```
Ruijie(config)# access-list 100 permit tcp 192.168.52.0 0.0.0.255 any
Ruijie(config)# control-plane manage
Ruijie(config-cp)# scpp list 100 bw-rate 100 bw-burst-rate 150 conn-create-rate 5
conn-create-burst-rate 7 conn-total 30
```

【检验方法】 1：使用 **show ef-rnfp scpp manage** 命令，可以查看管理类子接口上 scpp 是启用还是关闭，以及其丢包状态。

【提示信息】 1：如果子接口上没有配置对应 acl 的 scpp 策略，删除时则提示错误信息。

```
Ruijie(config-cp)#no scpp lis 200
EF-RNFP: delete scpp rule failed
```

【常见错误】 1：scpp 引用了 acl 但是却没有配置该 acl。

【平台说明】 -

3.12 security deny

配置用户禁止 telent 设备，禁止 web 登录设备。

security deny { **lan-ping** | **lan-web** | **wan-ping** | **wan-web** | **lan-telnet-ssh** | **lan-snmp** | **wan-telnet-ssh** | **wan-snmp** }

关闭功能。

no security deny { **lan-ping** | **lan-web** | **wan-ping** | **wan-web** | **lan-telnet-ssh** | **lan-snmp** | **wan-telnet-ssh** | **wan-snmp** }

恢复缺省配置。

default security deny { **lan-ping** | **lan-web** | **wan-ping** | **wan-web** | **lan-telnet-ssh** | **lan-snmp** | **wan-telnet-ssh** | **wan-snmp** }

【参数说明】

参数	描述
lan-ping	禁止内网 ping 设备。
lan-web	禁止内网访问设备 web 界面
wan-ping	禁止外网 ping 设备
wan-web	禁止外网访问设备 web 界面
lan-telnet-ssh	禁止内网用户使用 telnet，ssh 访问设备
lan-snmp	禁止内网服务器使用 snmp 协议管理设备。
wan-telnet-ssh	禁止外网用户使用 telnet，ssh 访问设备
wan-snmp	禁止外网服务器使用 snmp 协议管理设备。

【缺省配置】 缺省情况下，功能是关闭的。

【命令模式】 Control-plane 配置模式

【缺省级别】 14

【使用指导】 针对目前网络上经常采用 ping 和 web 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。使用该命令的 no 选项删除相应配置。

【配置举例】 1：以下的配置例子，禁止内网 pc ping 设备。

```
Ruijie(config)# control-plane
Ruijie(config-cp)# security deny lan-ping
```

2：以下的配置例子，禁止内网 pc 登录设备的 web 界面。

```
Ruijie(config)# control-plane
Ruijie(config-cp)# security deny lan-web
```

3：以下的配置例子，禁止内网服务器使用 snmp 协议管理设备。

```
Ruijie(config)# control-plane
Ruijie(config-cp)# security deny lan-snmp
```

4：以下的配置例子，禁止内网 pc 登录设备的 web 界面。

```
Ruijie(config)# control-plane
Ruijie(config-cp)# security deny lan-telnet-ssh
```

【检验方法】 1：使用 **show run** 命令，可以查看对应配置。

【提示信息】 -

【常见错误】 -

【平台说明】 -

3.13 security web permit

配置白名单用户。
security web permit *low-ip-address* [*high-ip-address*]

删除白名单用户。
no security web permit *low-ip-address* [*high-ip-address*]

恢复缺省配置。
default security web permit *low-ip-address* [*high-ip-address*]

【参数说明】

参数	描述
low-ip-address	允许的 ip 地址或者允许的 ip 地址范围起始地址。
high-ip-address	允许地址范围的结束 ip 地址。

【缺省配置】 缺省情况下，功能是关闭的。

【命令模式】 Control-plane 配置模式

【缺省级别】 14

【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】 1：配置 192.168.1.2-192.168.1.100 为白名单用户。

```
Ruijie(config)# control-plane
Ruijie(config-cp)# security web permit 192.168.1.2 192.168.1.100
```

【检验方法】 1：使用 **show ef-rnfp web-permit-ip** 命令，可以查看所配置的白名单用户。

【提示信息】 -

【常见错误】 -

【平台说明】 -

3.14 show arp-suspect

查看 arp 攻击嫌疑列表。

show arp-suspect

【参数说明】

参数	描述
arp-suspect	查看哪些主机被加入 arp 欺骗嫌疑列表。

【命令模式】 特权模式、全局模式、接口模式

【缺省级别】 14

【使用指导】 使用该命令可以查看设备上检测到的 arp 攻击嫌疑列表。

【配置举例】 1：查看设备上检测到的 arp 攻击嫌疑列表

```
Ruijie#Ruijie#show arp-suspect
IP address      MAC address
1.1.1.1         00d0.1234.5678
```

字段解释：

字段	说明
IP address	Arp 攻击嫌疑的 ip 地址
MAC address	Arp 攻击嫌疑的 mac 地址

【提示信息】 -

【平台说明】 -

3.15 show attack-info

查看设备被攻击信息

show attack-info { **current** | **history** }

【参数说明】

参数	描述
current	查看系统目前的攻击信息。
history	查看系统历史的攻击信息

【命令模式】 特权模式、全局模式、接口模式

【缺省级别】 14

【使用指导】 使用该命令可以查看设备上是否正在被攻击，以及过去被攻击的历史情况。

【配置举例】 1：查看所有 PIM 接口的详细信息

```
Ruijie# show attack-info history
System attack record at 1970-1-5 15:37:4, System in attack 8s
ALL: 1514 packets, 141600 bytes
PROTOCOL          packets         bytes
ARP               2               120
UDP               1512            141480
TOP4 IP attack:
IP                packets         bytes             interface
172.18.3.58       1500            138000            Gi0/1
100.100.100.73    10              2982              Gi0/1
10.10.3.1         2               120               Gi0/1
172.18.3.81       2               498               Gi0/1

System attack record at 1970-1-5 15:30:10, System in attack 6s
ALL: 259 packets, 25015 bytes
PROTOCOL          packets         bytes
ARP               3               180
UDP               256             24835
TOP4 IP attack:
IP                packets         bytes             interface
172.18.3.69       250             23000             Gi0/1
100.100.100.73    4               1291              Gi0/1
172.18.3.110      3               180               Gi0/1
172.18.3.22       2               544               Gi0/1
```

【提示信息】 -

【平台说明】 -

3.16 show ef-rnfp

查看本地防攻击的信息

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** }

【参数说明】

参数	描述
acpp	查看 acpp 配置以及丢包情况。
data	Data 子接口下的丢包情况

manage	Manage 子接口下的丢包情况
protocol	Protocol 子接口下的丢包情况
scpp	查看 scpp 配置以及丢包情况。
glean-car	查看 glean-car 配置以及丢包情况。
port-filter	查看 port-filter 配置以及丢包情况。
mpp	查看 mpp 配置以及丢包情况。
all	查看三个子接口下 acpp，scpp，glean-car，port-filter，mpp 的配置和丢包情况。
web-permit-ip	查看本地防攻击白名单。
anti-arp-spoof	查看 arp 欺骗嫌疑检测配置。

【命令模式】 特权模式、全局模式、接口模式

【缺省级别】 14

【使用指导】 使用该命令可以查看本地防攻击丢包以及配置信息。

【配置举例】 1：查看 arp-car 的丢包信息

```
Ruijie# show ef-rnfp arp-car
ARP CAR information:
  Manage subinterface: enable
    RULE:
      allow packet rate per source: 10(pps)
      log: off
    STATISTIC:
      dropped 17000657 packets
```

字段解释：

字段	说明
enable	功能开启
allow packet rate per source: x(pps)	每个源 ip 允许的 arp 速率为 x
log	是否记录 log 信息
dropped xxx packets	报文丢了 xx 个

【提示信息】 -

【平台说明】 -

4 SSH

4.1 crypto key generate

生成服务器端的公共密钥

crypto key generate { **rsa | dsa** }

【参数说明】

参数	描述
rsa	生成 RSA 密钥
dsa	生成 DSA 密钥

【缺省配置】 默认情况下 SSH Server 没有生成公共密钥。

【命令模式】 全局配置模式

【缺省级别】 14

【使用指导】 当需要打开 SSH Server 服务时，通过此命令生成 SSH 服务器端的公共密钥。同时执行 **enable service ssh-server** 命令，打开 SSH Server 功能。SSH 1 使用 RSA 密钥；SSH 2 使用 RSA 或者 DSA 密钥。因此，如果当前已生成 RSA 密钥，则 SSH1 与 SSH2 都可以使用；如果仅生成 DSA 密钥，则仅有 SSH2 可以使用。

虽然一个客户端在一次连接过程中，只会采用 DSA 和 RSA 公钥算法中的一种来认证服务器，但是由于不同客户端支持的公钥算法不同，为了确保客户端能够成功登录服务器，建议在服务器上生成 DSA 和 RSA 两种密钥对。

RSA 主机密钥的模数最小长度为 512 位，DSA 主机密钥的模数最小长度为 360 位，二者的模数最大长度均为 2048 位。在 SSH2 中，有些客户端（比如 SCP 文件传输客户端）会要求服务器端生成的密钥长度必须大于或等于 768 位。建议用户在配置 RSA 和 DSA 主机密钥的时候，将主机密钥模数指定为 768 位或大于 768 位。

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。

【配置举例】 1：生成服务端的 rsa 密钥。

```
Ruijie# configure terminal
Ruijie(config)# crypto key generate rsa
```

【检验方法】 1：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。

【提示信息】 1：如果第一次生成服务端的 rsa 密钥，则提示选择密钥位数以及生成成功或失败的信息。

```
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]
```

2：如果 rsa 密钥已存在服务端，则提示是否进行替换的信息。如果是，则提示重新选择密钥位数以及生成成功或失败的信息，否则，直接退出。

```
Ruijie(config)#crypto key generate rsa
% You already have RSA keys.
% Do you really want to replace them? [yes/no]:yes
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]:
```

3：如果输入的 rsa 密钥位数不在 512~2048 范围之内，则提示输入位数出错，并提示重新输入。

```
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]:360
sshd: rsa key in the range of 512 to 2048
How many bits in the modulus [512]:2590
sshd: bad data bits
How many bits in the modulus [512]:
```

【常见错误】 -

【平台说明】 -

4.2 crypto key zeroize

删除 SSH 服务器端的公共密钥。

crypto key zeroize { **rsa** | **dsa** }

【参数说明】

参数	描述
rsa	删除 RSA 密钥
dsa	删除 DSA 密钥

【缺省配置】 -

【命令模式】 全局配置模式

【缺省级别】 14

【使用指导】 通过此命令来删除服务器的公共密钥。密钥被删除后，SSH Server 的状态成为 DISABLE。如果需要关闭 SSH Server，需要执行 **no enable service ssh-server** 命令。

【配置举例】 1：删除服务端的 rsa 密钥。

```
Ruijie# configure terminal
Ruijie(config)# crypto key zeroize rsa
```

【检验方法】 1：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 是否已经删除。

【提示信息】 1：如果 rsa 密钥已存在服务端，则提示是否删除 rsa 密钥。

```
Ruijie(config)#crypto key zeroize rsa
% Keys to be removed
% All router certs issued using these keys will also be removed.
Do you really want to remove these keys? [yes/no]:yes
*Jan 16 06:52:57: %P17050-7-DEBUG: sshd: delete key file /rsa_private.bin
*Jan 16 06:52:57: %P17050-7-DEBUG: sshd: delete key file /rsa1_private.bin
```

2：如果 rsa 密钥没有生成，则提示 rsa 密钥不存在。

```
Ruijie(config)#crypto key zeroize rsa
% The specified RSA keypair does not exist.
```

【常见错误】 1：使用 no 和 default 命令前缀来删除密钥，则密钥将无法被删除。

【平台说明】 -

4.3 disconnect ssh

断开已经建立的 SSH 连接会话。

disconnect ssh [**vty**] *session-id*

【参数说明】

参数	描述
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

【缺省配置】 -

【命令模式】 特权用户模式

【缺省级别】 14

【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。

【配置举例】 1：输入指定的 SSH 连接会话号，断开已经建立的 SSH 连接。

```
Ruijie# disconnect ssh 1
```

2：输入指定的 VTY 连接会话号，断开指定的 SSH 连接。

```
Ruijie# disconnect ssh vty 1
```

【检验方法】 1：使用 **show ssh** 命令，可以查看指定的 SSH 连接是否已经被断开。

【提示信息】 -

【常见错误】 -

【平台说明】 -

4.4 disconnect ssh-session

断开挂起的 SSH Client 连接。

disconnect ssh-session *session-id*

【参数说明】

参数	描述
session-id	挂起的 SSH Client 连接会话号

【缺省配置】 -

【命令模式】 普通用户模式

【缺省级别】 1

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

【配置举例】 1：输入指定的 SSH Client 连接会话号，断开指定的 SSH Client 连接。

```
Ruijie# disconnect ssh-session 1
```

【检验方法】 1：使用 **show ssh-session** 命令，可以查看指定的 SSH Client 连接是否已经被断开。

【提示信息】 -

【常见错误】 -

【平台说明】 -

4.5 ip scp server enable

在网络设备上打开 SCP 服务器功能。
ip scp server enable

关闭 SCP 服务器功能。
no ip scp server enable

【参数说明】

参数	描述
-	-

【缺省配置】 缺省设置不开启 SCP 服务器功能。

【命令模式】 全局配置模式

【缺省级别】 14

【使用指导】 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。

【配置举例】 1：开启 scp 功能。

```
Ruijie# configure terminal
Ruijie(config)# ip scp server enable
```

【检验方法】 1：使用 **show ip ssh** 命令，可以查看 SCP 服务器功能是否打开。

【提示信息】 -

【常见错误】 -

【平台说明】 -

4.6 ip scp server topdir

设置 SCP 服务器文件上传和下载路径。

ip scp server topdir {flash:/*path* **| flash2:/***path* **| usb0:/***path* **| usb1:/***path* **| sd0:/***path* **| sata0:/***path* **| tmp:/***path* **}**

恢复 SCP 服务器文件传输路径为缺省值。

no ip scp server topdir

【参数说明】

参数	描述
flash	传输文件路径选择在扩展 FLASH 当中，默认情况下文件传输路径为 **flash:/**
flash2	传输文件路径选择在扩展 FLASH2 当中，此选项需要设备具有 data2 分区时才支持
usb0	传输文件路径选择在 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	传输文件路径选择在 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
sd0	传输文件路径选择在 SD 卡当中，此选项需要设备具有 SD 卡接口时才支持，并插入扩展的 SD 卡设备
sata0	传输文件路径选择在硬盘当中，此选项需要设备具有 SATA 分区时才支持
tmp	传输文件路径选择在临时的 tmp/vsd/目录中

【缺省配置】 缺省设置文件传输路径为 **flash:/**。

【命令模式】 全局配置模式

【缺省级别】 14

【使用指导】 用户可以使用此命令对修改文件传输路径，包括文件上传和文件下载。

【配置举例】 1：修改文件传输路径为 tmp/vsd 目录下。

```
Ruijie# configure terminal
Ruijie(config)# ip scp server topdir tmp:/
```

【检验方法】 -

【提示信息】 -

【常见错误】 -

【平台说明】 -

4.7 ip ssh access-class

设置 SSH Server 的 ACL 过滤规则。
ip ssh access-class { *access-list-number* | *access-list-name* }

删除 SSH Server 的 ACL 过滤规则。
no ip ssh access-class

【参数说明】

参数	描述
access-list-number	ACL 编号，可配范围：IP 标准 ACL(1-99，1300-1999)；IP 扩展 ACL(100-199，2000-2699)。
access-list-name	ACL 名称。

【缺省配置】 -

【命令模式】 全局配置模式

【缺省级别】 14

【使用指导】 用户可以使用此命令对 SSH 的所有连接进行 ACL 过滤。line 下的 ACL 过滤只是对特定的线路进行 ACL 过滤，而 SSH 的 ACL 过滤规则可以对所有的 SSH 连接进行 ACL 过滤。

【配置举例】 1：配置 SSH 的所有连接进行名字为 testv4 的 ACL 过滤。

```
Ruijie# configure terminal
Ruijie(config)# ip ssh access-class testv4
```

【检验方法】 -

【提示信息】 -

【常见错误】 -

【平台说明】 -

4.8 ip ssh authentication-retries

设置 SSH Server 用户认证的重认证次数。
ip ssh authentication-retries *retry times*

恢复为缺省设置。、
no ip ssh authentication-retries

【参数说明】

参数	描述
retry times	配置用户认证的重认证次数，取值范围为 0~5

【缺省配置】 重认证次数为 3 次。

【命令模式】 全局配置模式

【缺省级别】 14

【使用指导】 该命令配置 SSH Server 进行用户认证的重认证次数。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。

【配置举例】 1：设置用户认证的重认证次数为 2。

```
Ruijie# configure terminal
Ruijie(config)# ip ssh authentication-retries 2
```

【检验方法】 1：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。

【提示信息】 -

【常见错误】 -

【平台说明】 -

4.9 ip ssh cipher-mode

设置 SSH Server 支持的加密模式。
ip ssh cipher-mode { **cbc** | **ctr** | **others** }

使用该命令的 no 选项将 SSH Server 支持的加密模式为缺省设置。
no ip ssh cipher-mode

【参数说明】

参数	描述
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

【缺省配置】 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）。

【命令模式】 全局配置模式

【缺省级别】 14

【使用指导】 该命令配置 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。

【配置举例】 1：设置 SSH Server 支持加密模式为 ctr 模式。

```
Ruijie# configure terminal
Ruijie(config)# ip ssh cipher-mode ctr
```

【检验方法】 -

【提示信息】 -

【常见错误】 -

【平台说明】 -

4.10 ip ssh hmac-algorithm

设置 SSH Server 支持的消息认证算法。
ip ssh hmac-algorithm { **md5** | **md5-96** | **sha1** | **sha1-96** }

使用该命令的 no 选项将 SSH Server 支持的消息认证算法恢复为缺省设置。
no ip ssh hmac-algorith

【参数说明】

参数	描述
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

【缺省配置】 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）。

【命令模式】 全局配置模式

【缺省级别】 14

【使用指导】 该命令配置 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。

【配置举例】 1：设置 SSH Server 支持的消息认证算法为 sha1。

```
Ruijie# configure terminal
Ruijie(config)# ip ssh hmac-algorithm sha1
```

【检验方法】 -

【提示信息】 -

【常见错误】 -

【平台说明】 -

4.11 ip ssh key-exchange

设置 SSH Server 支持的 DH 密钥交换算法。
ip ssh key-exchange { dh_group_exchange_sha1 | dh_group14_sha1 | dh_group1_sha1 }

使用该命令的 no 选项将 SSH Server 支持的 DH 密钥交换算法恢复为缺省设置。
no ip ssh key-exchange

【参数说明】

参数	描述
dh_group_exchange_sha1	配置 DH 密钥交换算法为 diffie-hellman-group-exchange-sha1。密钥长度默认为 2048 字节，不支持可配置。
dh_group14_sha1	配置 DH 密钥交换算法为 diffie-hellman-group14-sha1。密钥长度为 2048 字节。
dh_group1_sha1	配置 DH 密钥交换算法为 diffie-hellman-group1-sha1。密钥长度为 1024 字节。

【缺省配置】 缺省情况下 SSH Server 支持的 DH 密钥交换算法为：SSHv1 不支持，SSHv2 支持 3 种（diffie-hellman-group-exchange-sha1、diffie-hellman-group14-sha1、diffie-hellman-group1-sha1）。

【命令模式】 全局配置模式

【缺省级别】 14

【使用指导】 该命令配置 SSH Server 支持的 DH 密钥交换算法。
在锐捷设备当中，SSHv1 Server 不支持 DH 密钥交换算法；SSHv2 Server 支持的 DH 密钥交换算法为：diffie-hellman-group-exchange-sha1、diffie-hellman-group14-sha1、diffie-hellman-group1-sha1。用户可以依据实际需要选择 SSH Server 支持的 DH 密钥交换算法。

【配置举例】 1：设置 SSH Server 支持的 DH 密钥交换算法为 diffie-hellman-group14-sha1。

```
Ruijie# configure terminal
Ruijie(config)# ip ssh key-exchange dh_group14_sha1
```

【检验方法】 -

【提示信息】 -

【常见错误】 -

【平台说明】 -

4.12 ip ssh peer

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。
ip ssh peer *username* **public-key** { **rsa** | **dsa** } *filename*

取消客户端的公钥文件与用户名关联。
no ip ssh peer *username* **public-key** { **rsa** | **dsa** } *filename*

【参数说明】

参数	描述
username	用户名
filename	公钥文件名
rsa	public-key 类型为 rsa
dsa	public-key 类型为 dsa

【缺省配置】 -

【命令模式】 全局配置模式

【缺省级别】 14

【使用指导】 -

【配置举例】 1：设置用户 *test* 关联的 RSA 和 DSA 公钥文件。

```
Ruijie# configure terminal
Ruijie(config)# ip ssh peer test public-key rsa flash:rsa.pub
Ruijie(config)# ip ssh peer test public-key dsa flash:dsa.pub
```

【检验方法】 -

【提示信息】 1：如果关联的公钥文件超出 SSH Public Key 支持的最大个数 1024 个，则提示超出范围。

```
Ruijie(config)# ip ssh peer test public-key rsa flash:rsa.pub
%% Too many public-keys, system support max public key 1024
```

2：如果为输入关联的公钥文件名，则提示公钥文件名无效。

```
Ruijie(config)#ip ssh peer test public-key rsa flash:
% Invalid file name
```

【常见错误】 -

【平台说明】 -

4.13 ip ssh port

设置 SSH Server 的监听端口号。

ip ssh port *port*

将 SSH Server 的监听端口号设置恢复为缺省设置。

no ip ssh port

ip ssh port 22

【参数说明】

参数	描述
port	配置 SSH Server 的监听端口号，取值范围为 1025~65535

【缺省配置】 -

【命令模式】 全局配置模式

【缺省级别】 14

【使用指导】 -

【配置举例】 1：修改 SSH Server 的监听端口号为 10000。

```
Ruijie# configure terminal
Ruijie(config)# ip ssh port 10000
```

【检验方法】 1：使用 **show ip ssh** 命令，可以查看 SSH Server 的监听端口号配置信息。

【提示信息】 1：如果配置的端口号与当前值一样，则提示端口号已经是需要配置的值。

```
Ruijie(config)# ip ssh port 22
% SSH tcp-port has been 22
```

2：如果配置的端口号已经处于监听状态，则提示端口号已处于监听状态，请使用另外一个端口号，当前设备还是使用旧的端口号。

```
Ruijie(config)# ip ssh port 10000
% SSH open tcp-port(10000) failed, please use another tcp-port,otherwise the system will use the old tcp-port(22)!
```

3：如果配置的端口号启动监听出现错误，则提示配置端口号失败。

```
Ruijie(config)# ip ssh port 10000
% SSH change to tcp-port(10000) fail!
```

2：如果配置的端口号成功，则提示配置端口号成功。

```
Ruijie(config)# ip ssh port 10000
% SSH change to tcp-port(10000) success!
```

【常见错误】 -

【平台说明】 -

4.14 ip ssh source-interface

指定 SSH Client 的源接口。

ip ssh source-interface *interface-name*

清除 SSH Client 的源接口配置。

no ip ssh source-interface

【参数说明】

参数	描述
interface-name	指定该接口上面的 IP 地址将作为 SSH Client 的源地址。

【缺省配置】 缺省情况下，SSH 协议报文将使用目的地址的发包源地址，作为报文的源地址。

【命令模式】 全局配置模式

【缺省级别】 14

【使用指导】 该命令用于指定接口上的 IP 地址作为 SSH Client 连接的全局源地址。在使用 ssh 命令登录连接一台 SSH 服务器的时候，如果没有为该 SSH 连接单独指定源接口或源地址，可以通过本命令实现此配置。使用 **no ip ssh source-interface** 命令将设置恢复为默认值。

【配置举例】 1：下面的示例命令，指定 Loopback 1 接口上的 IP 地址作为全局 SSH 连接的源地址：

```
Ruijie(config)# ip ssh source-interface Loopback 1
```

【检验方法】 -

【提示信息】 -

【常见错误】 -

【平台说明】 -

4.15 ip ssh time-out

设置 SSH Server 的用户认证超时时间。
ip ssh time-out *time*

将用户认证超时时间设置恢复为缺省设置。
no ip ssh time-out

【参数说明】

参数	描述
time	配置用户认证的超时时间，取值范围为 1~120s，单位为秒

【缺省配置】 超时时间为 120s。

【命令模式】 全局配置模式

【缺省级别】 14

【使用指导】 该命令配置SSH Server进行用户认证的超时时间。从接受用户连接请求开始计时，当超过120s没有认证成功时，则认为认证超时失败。

【配置举例】 1：配置超时时间为 100s：

```
Ruijie# configure terminal
Ruijie(config)# ip ssh time-out 100
```

【检验方法】 1：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。

【提示信息】 -

【常见错误】 -

【平台说明】 -

4.16 ip ssh version

设置 SSH Server 的版本。
ip ssh version { **1** | **2** }

将版本设置恢复为缺省设置。

no ip ssh version

【参数说明】

参数	描述
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

【缺省配置】 兼容 SSH 版本 1 和 2。

【命令模式】 全局配置模式

【缺省级别】 14

【使用指导】 该命令用来配置 SSH Server 所支持的 SSH 连接的协议版本。默认情况下，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。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。

【配置举例】 1：设置只使用版本 2：

```
Ruijie# configure terminal
Ruijie(config)# ip ssh version 2
```

【检验方法】 1：使用 **show ip ssh** 命令，可以查看 SSH Server 当前支持的 SSH 协议版本。

【提示信息】 -

【常见错误】 -

【平台说明】 -

4.17 ipv6 ssh access-class

设置 SSH Server 的 IPv6 ACL 过滤规则。

ipv6 ssh access-class *accessv6-list-name*

删除 SSH Server 的 IPv6 ACL 过滤规则。

no ipv6 ssh access-class

【参数说明】

参数	描述
accessv6-list-name	IPv6 ACL 名称。

【缺省配置】 -

【命令模式】 全局配置模式

【缺省级别】 14

【使用指导】 用户可以使用此命令对 SSH 的所有连接进行 IPv6 ACL 过滤。line 下的 IPv6 ACL 过滤只是对特定的线路进行 IPv6 ACL 过滤，而 SSH 的 IPv6 ACL 过滤规则可以对所有的 SSH 连接进行 IPv6 ACL 过滤。

【配置举例】 1：配置 SSH 的所有连接进行名字为 testv6 的 IPv6 ACL 过滤。

```
Ruijie# configure terminal
Ruijie(config)# ipv6 ssh access-class testv6
```

【检验方法】 -

【提示信息】 -

【常见错误】 -

【平台说明】 -

4.18 show crypto key mypubkey

显示 SSH Server 公共密钥的公开密钥部分的信息。

show crypto key mypubkey { **rsa | dsa** }

【参数说明】

参数	描述
rsa	显示 RSA 密钥
dsa	显示 DSA 密钥

【命令模式】 特权用户模式、全局配置模式

【缺省级别】 14

【使用指导】 显示已经生成的 SSH Server 公共密钥的公开密钥部分的信息。包括：密钥生成时间、密钥名字、公开密钥部分内容等信息。

【配置举例】 1：显示已经生成的 SSH Server 公共密钥 RSA 的公开密钥部分的信息。

```
Ruijie(config)#show crypto key mypubkey rsa
% Key pair was generated at: 7:1:25 UTC Jan 16 2013
```

```
Key name: RSA1 private
Usage: SSH Purpose Key
Key is not exportable.
Key Data:
        AAAAAwEA AQAAAEEA 2m6H/J+2 xOMLW5MR 8tOmpW1I XU1QItVN mLdR+G7O Q1Okz+4/
        /IgYROge 1sZNg32u dFEifZ6D zfLySPqC MTWLfw==

% Key pair was generated at: 7:1:25 UTC Jan 16 2013
Key name: RSA private
Usage: SSH Purpose Key
Key is not exportable.
Key Data:
        AAAAAwEA AQAAAEEA OE5w2HOk v744uTIR yZBd/7AM 8pLItnW3 XH3LhEEi BbZGZvn3
        LEYYfQ9s pgYLOZQf SOs/GYOX gJOMsc6z i8OAkQ==
```

字段解释：

字段	说明
Key pair was generated at	密钥生成时间
Key name	密钥名字
Usage	密钥使用说明
Key Data	公开密钥部分内容

【提示信息】 -

【平台说明】 -

4.19 show ip ssh

显示 SSH Server 的当前生效的配置信息。

show ip ssh

【参数说明】

参数	描述
-	-

【命令模式】 特权用户模式、全局配置模式

【缺省级别】 14

【使用指导】 显示 SSH Server 当前生效的配置信息。包括：版本、是否打开 SSH Server、超时时间、重认证次数。

即使配置了对应的 SSH 版本，如果没有生成对应的服务器端密钥，仍然显示该 SSH 版本为不可用。

【配置举例】 1：显示 SSH Server 当前生效的配置信息。

```
// 显示 SSH Server 功能和 SCP 功能均未打开的配置信息
Ruijie(config)#show ip ssh
SSH Disable - version 1.99
please generate rsa and dsa key to enable SSH
Authentication timeout: 120 secs
Authentication retries: 3
SSH SCP Server: disabled

// 显示 SSH Server 功能和 SCP 功能均已打开的配置信息
Ruijie(config)#show ip ssh
SSH Enable - version 1.99
Authentication timeout: 120 secs
Authentication retries: 3
SSH SCP Server: enabled
```

字段解释：

字段	说明
SSH Enable/Disable	SSH Server 服务功能打开/关闭
version 1|2	SSH Server 支持的 SSH 协议版本
please generate rsa and dsa key to enable SSH	生成 rsa/dsa 公共密钥来打开 SSH Server 服务功能
Authentication timeout	用户认证的超时时间
Authentication retries	用户认证的重认证次数
SSH SCP Server enaled/disabled	SSH SCP 服务功能打开/关闭

【提示信息】 -

【平台说明】 -

4.20 show ssh

显示已经建立的 SSH 连接的每个连接信息。

show ssh

【参数说明】

参数	描述
-	-

【命令模式】 特权用户模式、全局配置模式

【缺省级别】 14

【使用指导】 显示已经建立的 SSH 连接的连接信息。包括：连接所占用的 VTY 号、SSH 版本、加密算法、消息认证算法、连接状态、用户名。

【配置举例】 1：显示已经建立的 SSH 连接的连接信息。

```
Ruijie#show ssh
Connection Version Encryption       Hmac         Compress   State           Username
         0     1.5 blowfish                      zlib       Session started test
         1     2.0 aes256-cbc       hmac-sha1    zlib       Session started test
```

字段解释：

字段	说明
Connection	连接所占用的 VTY 号
Version	SSH 客户端支持的 SSH 协议版本
Encryption	加密算法
Hmac	消息认证算法
Compress	压缩算法
State	连接状态
Username	用户名

【提示信息】 -

【平台说明】 -

4.21 show ssh-session

显示已经建立的 SSH Client 实例的每个实例信息。

show ssh-session

【参数说明】

参数	描述
-	-

【命令模式】 普通用户模式

【缺省级别】 1

【使用指导】 显示已经建立的 SSH Client 实例的每个实例信息，包括：连接所占用的 VTY 号、SSH 版本号、服务器地址。

【配置举例】 1：显示已建立的 SSH Client 会话连接信息。

```
Ruijie#show ssh-session
Connect No.  SSH Version  Server Address
-----------  -----------  ---------------
0            2.0          192.168.23.122
1            1.5          192.168.23.122
```

【提示信息】 -

【平台说明】 -

4.22 ssh

在普通用户模式下，使用 **ssh** 命令，建立一个到远程网络设备的加密会话。

ssh [**oob**] [**-v** { **1** | **2** }] [**-c** { **3des** | **aes128-cbc** | **aes192-cbc** | **aes256-cbc | aes128-ctr | aes192-ctr | aes256-ctr** }] [**-l** *username*] [**-m** { **hmac-md5-96** | **hmac-md5-128** | **hmac-sha1-96** | **hmac-sha1-160** }] [**-p** *port-num*] { *ip-addr* | *hostname* } [**via** *mgmt-name*] [**/source** { **ip** *A.B.C.D* **| ipv6** *X:X:X:X::X* **| interface** *interface-name* }] [**/vrf** *vrf-name*]

【参数说明】

参数	描述
oob	通过带外通信（一般指通过 MGMT 接口）远程连接到 SSH 服务器，只有在设备具备 MGMT 管理口的时候才会有该选项
-v	（可选）指定用于连接到服务器的 SSH 版本号。如果没有指定，默认使用 SSHv2。 ● **1** – 使用 SSHv1 进行连接。

	● **2** – 使用 SSHv2 进行连接。
-c { **3des** | **aes128-cbc** | **aes192-cbc** | **aes256-cbc** | **aes128-ctr** | **aes192-ctr** | **aes256-ctr** }	（可选）指定数据加密算法，其可选类型有：数据加密标准（DES）、三重数据加密标准（3DES），或高级加密标准（AES）。高级加密标准（AES）算法依据密钥长度和模式不同，可以支持六种类型：aes128-cbc（128 位密钥），aes192-cbc（192 位密钥）、aes256-cbc（256 位密钥）、aes128-ctr（128 位密钥），aes192-ctr（192 位密钥）、aes256-ctr（256 位密钥）。 ● 如果用户没有指定**-c** 选项，在算法协商时，将把 SSH 客户端支持的所有算法列表，发往服务器。 ● 如果用户指定**-c** 选项，在算法协商时，SSH 客户端只会将用户指定的加密算法发往服务器，此时，若服务器不支持用户指定的加密算法，则会关闭连接。
-l *username*	（必选）指定登录的用户名
-m { **hmac-md5-96** | **hmac-md5-128** | **hmac-sha1-96** | **hmac-sha1-160** }	（可选）指定一种哈希消息认证码（HMAC）算法。 ● SSHv1 不支持 HMACs，如果用户同时指定了 SSHv1 和 HMACs，则直接忽略掉 HMACs。 ● 如果用户没有指定**-m**选项，在算法协商时，将把SSH客户端支持的所有算法列表，发往服务器。 ● 如果用户指定了**-m** 选项，在算法协商时，SSH 客户端只会将用户指定的 HMAC 算法发往服务器，此时，若服务器不支持用户指定的 HMAC 算法，则会关闭连接。
-p *port-num*	（可选)指定连接远程服务器时期望的端口号。默认情况下，端口号为 22。
ip-addr | *hostname*	（必选）指定远程服务器的 IPv4/IPv6 地址或主机名。
via *mgmt-name*	指定 oob 选项时使用的 MGMT 口
/source	指定 SSH Client 使用的源 IP 或者源接口
ip A.B.C.D	指定 SSH Client 使用的源 IPV4 地址
ipv6 X:X:X:X::X	指定 SSH Client 使用的源 IPV6 地址
interface *interface-name*	指定 SSH Client 使用的源接口
/vrf *vrf-name*	指定查询的 VRF 路由表

【缺省配置】 -

【命令模式】 普通用户模式

【缺省级别】 1

【使用指导】 **ssh** 命令用来从当前设备（作为 SSH 客户端）建立一个安全、加密的连接到另外一个设备（作为 SSH 服务器）或其它支持 SSHv1 或 SSHv2 的服务器。该连接提供了一种类似于 Telnet 连接的机制，与 Telnet 不同的是基于该连接所有的传输都是加密的。基于认证和加密，SSH Client 将在不安全的网络上面建立一个安全的连接。

⚠ SSHv1 只支持 DES（56 位密钥）和 3DES（168 位密钥）加密算法。

⚠ SSHv2 可以支持以下 AES 高级加密算法：ase128-cbc、aes192-cbc、aes256-cbc、ase128-ctr、

aes192-ctr 和 aes256-ctr。

⚠ SSHv1 不支持 HMAC 认证码算法。

⚠ 若用户在选择 SSH 版本号的同时，指定了不匹配的加密算法或认证算法，在建立连接时，将会忽略掉不匹配的算法。

【配置举例】 1：从当前设备，通过 SSH 以用户名 admin 登录到远程支持 SSH 服务器的设备 192.168.23.122：

```
Ruijie#ssh -l admin 192.168.23.122
```

2：从当前设备，通过 SSHv2，首选 aes128-cbc 为加密算法、hmac-md5-128 为认证算法，以用户名 admin 登录到远程支持 SSH 服务器的设备 192.168.23.122：

```
Ruijie#ssh -v 2 -c aes128-cbc  -m hmac-md5-128 -l admin 192.168.23.122
```

【检验方法】 -

【提示信息】 -

【常见错误】 -

【平台说明】 -

4.23 ssh-session

恢复已经建立的 SSH Client 会话连接。

ssh-session *session-id*

【参数说明】

参数	描述
session-id	已经建立的 SSH Client 会话连接索引。

【缺省配置】 -

【命令模式】 普通用户模式

【缺省级别】 1

【使用指导】 该命令用于恢复使用已经建立的 SSH Client 会话连接。当使用 **ssh** 命令发起 SSH 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 **ssh-session** 命令进行恢复。同时，如果连接已建立，可以使用 **show ssh-session** 命令查看已建立的连接信息。

【配置举例】 1：恢复已经建立的 SSH Client 会话连接。

```
Ruijie# ssh-session 1
```

【检验方法】 -

【提示信息】 -

【常见错误】 -

【平台说明】 -

5 DHCP Snooping

5.1 clear ip dhcp snooping binding

要删除 DHCP Snooping 数据库中的所有动态用户，需要在特权模式下执行此命令。

clear ip dhcp snooping binding [*ip*] [*mac*] [**vlan** *vlan-id*] [**interface** *interface-id* | **wlan** *wlan-id*]

【参数说明】

参数	描述
mac	指定删除的用户的 MAC 地址。
vlan-id	指定删除的用户的 vlan id。
ip	指定删除的用户的 IP 地址。
interface-id	指定删除的用户所属的接口。
wlan-id	指定删除的用户所属的 WLAN

【命令模式】 特权模式

【缺省级别】 14

【使用指导】 执行该命令，可以删除 DHCP snooping 数据库中的所有动态用户。

执行该命令后，所有连接到开启 IP Source Guard 功能接口的 DHCP 用户需要重新申请地址，否则无法访问网络。

【配置举例】 1：下面删除 DHCP snooping 数据库中所有动态用户的例子：

```
Ruijie# clear ip dhcp snooping binding
Ruijie# show ip dhcp snooping binding
Total number of bindings: 0
NO.    MACADDRESS          IPADDRESS       LEASE(SEC)    TYPE          VLAN   INTERFACE
-----  ------------------  --------------  ------------  ------------  -----  --------------------
```

【提示信息】 -

【平台说明】 -

5.2 ip dhcp snooping

启动全局 DHCP Snooping 功能。

ip dhcp snooping

关闭全局 DHCP Snooping 功能。

no ip dhcp snooping

【参数说明】

参数	描述
-	-

【缺省配置】 该功能缺省关闭。

【命令模式】 全局配置模式

【缺省级别】 14

【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。

【配置举例】 1：下面是打开 DHCP snooping 全局功能开关的例子：

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

【检验方法】 1：使用 **show ip dhcp snooping** 命令，可以查看 DHCP Snooping 是启用还是关闭。

【提示信息】 1：如果全局下开启了 DHCP Snooping 监控功能，无法再配置 DHCP Snooping 功能。

```
% Failed to execute command, because of "Conflict with DHCP snooping monitor".
```

【常见错误】 -

【平台说明】 -

5.3 ip dhcp snooping bootp-bind

启动 DHCP Snooping 支持 Bootp 绑定功能。

ip dhcp snooping bootp-bind

关闭 DHCP snooping 支持 Bootp 绑定功能。

no ip dhcp snooping bootp-bind

【参数说明】

参数	描述
-	-

【缺省配置】 该功能缺省关闭。

【命令模式】 全局配置模式

【缺省级别】 14

【使用指导】 缺省情况下，DHCP Snooping 功能仅对 Bootp 报文进行转发。打开该功能后，DHCP Snooping 功能对 Bootp 协议报文进行窥探。当 Bootp 客户端成功申请地址后，DHCP Snooping 将 Bootp 用户添加到静态绑定数据库中。

【配置举例】 1：下面是打开 DHCP Snooping 支持 Bootp 绑定的例子：

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

【检验方法】 1：使用 **show ip dhcp snooping** 命令，可以查看 DHCP Snooping 是否支持 Bootp 绑定。

【提示信息】 -

【常见错误】 -

【平台说明】 -

5.4 ip dhcp snooping check-giaddr

启动 DHCP Snooping 支持处理 Relay 请求报文功能。
ip dhcp snooping check-giaddr

关闭 DHCP snooping 支持处理 Relay 请求报文功能。
no ip dhcp snooping check-giaddr

【参数说明】

参数	描述
-	-

【缺省配置】 该功能缺省关闭。

【命令模式】 全局配置模式

【缺省级别】 14

【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/dot1x

认证等，否则可能导致用户无法上网。
开启此功能后，不能配置 ip dhcp snooping verify mac-address，否则 Relay 的 DHCP 请求报文会被丢弃，导致用户无法获取地址。

【配置举例】 1：下面是打开 DHCP Snooping 支持处理 Relay 请求报文功能的例子：

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

【检验方法】 1：使用 **show run** 命令，可以查看 DHCP Snooping 是否支持处理 Relay 请求报文功能。

【提示信息】 -

【常见错误】 -

【平台说明】 -

5.5 ip dhcp snooping database

定时将 DHCP Snooping 数据库中所有动态用户信息写入指定备份类型文件。
ip dhcp snooping database sata0 [interval *time*]

关闭定时写入备份文件功能。
no ip dhcp snooping database sata0

【参数说明】

参数	描述
time	保存数据库记录的周期，单位为秒，取值范围为 10~86400 不带参数配置时使用默认周期，默认周期为 300 秒

【缺省配置】 该功能缺省关闭。

【命令模式】 全局配置模式

【缺省级别】 14

【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。

【配置举例】 1：下面是配置默认时间间隔定时写 SATA0 硬盘文件的例子：

```
Ruijie# configure terminal
```

```
Ruijie(config)# ip dhcp snooping database sata0
Ruijie(config)# end
```

【检验方法】 1：使用 **show ip dhcp snooping** 命令，可以查看当前的保存记录时间间隔。
2：使用 **show run** 命令查看当前备份方式。

【提示信息】 -

【常见错误】 1：设置的周期值不在限定的范围内。

【平台说明】 NBR2500D-E、NBR3000D-E、NBR3000D-UE 出厂带 SATA 硬盘。NBR108G-P 、NBR800G、NBR950G、NBR1500G、NBR2000G、NBR1000G-C、NBR2000G-C、NBR3000G-S、NBR1000G-E、NBR6120-E、NBR1300G-E、NBR1700G-E、NBR2100G-E、NBR6205-E、NBR6135-E、NBR6210-E、NBR6215-E 出厂无 SATA 硬盘。其中 NBR6205-E、NBR6135-E、NBR6210-E、NBR6215-E 可自行购买 SATA 硬盘使用。

5.6 ip dhcp snooping database write-delay

定时将 DHCP Snooping 数据库中所有动态用户信息写入 FLASH。
ip dhcp snooping database write-delay *time*

关闭定时写入 FLASH 功能。
no ip dhcp snooping database write-delay

【参数说明】

参数	描述
time	保存数据库记录的周期，单位为秒，取值范围为 600~86400

【缺省配置】 该功能缺省关闭。

【命令模式】 全局配置模式

【缺省级别】 14

【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。

⚠ 保存频率过快会降低 flash 的使用寿命。

【配置举例】 1：下面是配置交换机定时写 flash 时间间隔为 3600 的例子：

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

【检验方法】 1：使用 **show ip dhcp snooping** 命令，可以查看当前的保存记录时间间隔。

【提示信息】 -

【常见错误】 1：设置的周期值不在限定的范围内。

【平台说明】 -

5.7 ip dhcp snooping database write-to-flash

配置设备实时将 DHCP Snooping 数据库的动态用户信息写入 FLASH 文件。
ip dhcp snooping database write-to-flash

【参数说明】

参数	描述
-	-

【缺省配置】 -

【命令模式】 全局配置模式

【缺省级别】 14

【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。

【配置举例】 1：下面是将 DHCP 绑定数据库的动态用户信息实时写入 flash 的例子：

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

【检验方法】 -

【提示信息】 -

【常见错误】 -

【平台说明】 -

5.8 ip dhcp snooping information option

设置在 DHCP 请求报文中加入 option82 选项。

ip dhcp snooping information option [**standard-format**]

取消在 DHCP 请求报文中加入 option82 选项。

no ip dhcp snooping information option [**standard-format | dot1x-format**]

【参数说明】

参数	描述
standard-format	Option82 选项使用标准格式。

【缺省配置】 该功能缺省关闭。

【命令模式】 全局配置模式

【缺省级别】 14

【使用指导】 1：通过配置该命令，将在 DHCP 请求报文中添加 option82 信息，DHCP 服务器根据 option82 选项信息进行更加合理的地址分配。

2：启用 option82 选项功能时，该功能默认处于扩展模式。

3：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。

⚠ DHCP Snooping option82 功能与 DHCP Relay option82 功能不能共用。

【配置举例】 1：下面是配置在 DHCP 请求报文中加入 option82 选项功能的例子：

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

【检验方法】 1：使用 **show ip dhcp snooping** 命令，可以查看 Option82 功能是启用还是关闭。

【提示信息】 -

【常见错误】 1：与 DHCP Relay 的 option82 功能同时开启。会导致最终 DHCP 报文中的 option82 字段值出错。

【平台说明】 -

5.9 ip dhcp snooping information option format remote-id

设置 option82 选项处于扩展模式时，子选项 remote-id 为自定义字符串或是主机名。
ip dhcp snooping information option format remote-id { **string** *ascii-string* **| hostname** }

取消设置 option82 选项的子选项 remote-id 为自定义字符串或是主机名。
no ip dhcp snooping information option format remote-id { **string** *ascii-string* **| hostname** }

【参数说明】

参数	描述
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。

【缺省配置】 该功能缺省关闭。

【命令模式】 全局配置模式

【缺省级别】 14

【使用指导】 通过配置该命令，当 DHCP 报文 option82 选项功能开启，且处于扩展模式时，将 option82 选项中的子选项 remote-id 设置为自定义内容。

【配置举例】 1：下面配置是在 DHCP 请求报文中加入 option82 选项 remote-id，内容为主机名的例子：

```
Ruijie# configure terminal
Ruijie(config)# ip dhcp snooping information option format remote-id hostname
```

【检验方法】 1：使用 **show ip dhcp snooping** 命令，可以查看 Option82 选项格式。

【提示信息】 1：当命令参数 *ascii-string* 超过 63 个字符的限制时，则提示错误。

```
% Failed to execute command, because of "Remote-ID string cannot exceed 63 characters".
```

【常见错误】 -

【平台说明】 -

5.10 ip dhcp snooping monitor

启动全局 DHCP Snooping 监控功能。
ip dhcp snooping monitor

关闭全局 DHCP Snooping 监控功能。

no ip dhcp snooping monitor

【参数说明】

参数	描述
-	-

【缺省配置】 该功能缺省关闭。

【命令模式】 全局配置模式

【缺省级别】 14

【使用指导】 打开 DHCP Snooping 监控功能后，仅拷贝 DHCP 报文根据交互情况生成绑定表项，但不检查报文合法性。
DHCP Snooping 监控功能和 DHCP Snooping 功能互斥，只能配置其中一个。
开启 DHCP Snooping 监控功能时，针对路由口生成的绑定表项，show ip dhcp snooping binding 时 VLAN 字段显示为 0，表示不带有 VLAN 信息。

【配置举例】 1：下面是打开 DHCP snooping 监控功能开关的例子：

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

【检验方法】 1：使用 **show run** 命令，可以查看 DHCP Snooping 监控是启用还是关闭。

【提示信息】 1：如果全局下开启了 DHCP Snooping 功能，无法再配置 DHCP Snooping 监控功能。

```
% Failed to execute command, because of "Conflict with DHCP snooping".
```

【常见错误】 -

【平台说明】 -

5.11 ip dhcp snooping suppression

配置接口为 suppression 状态，丢弃发往该接口的所有 DHCP 报文。
ip dhcp snooping suppression

取消接口 suppression 状态。
no ip dhcp snooping suppression

【参数说明】

参数	描述
-	-

【缺省配置】 该功能缺省关闭。

【命令模式】 接口配置模式或者无线安全配置模式

【缺省级别】 14

【使用指导】 1：通过配置该命令，可拒绝 UNTRUST 接口下所有 DHCP 报文，即禁止该接口下的所有用户通过 DHCP 方式申请地址。
2：该命令配置在二层交换口、AP 口、无线安全配置模式上会立刻生效。其他接口上将配置失败。

【配置举例】 1：下面是配置 GigabitEthernet 0/2 与 WLAN 1 下为 suppression 状态的例子：

```
Ruijie# configure terminal
Ruijie(config)# interface GigabitEthernet 0/2
Ruijie(config-if-GigabitEthernet 0/2)# ip dhcp snooping suppression
Ruijie(config-if-GigabitEthernet 0/2)# end
Ruijie# configure terminal
Ruijie(config)# wlansec 1
Ruijie(config-wlansec)# ip dhcp snooping suppression
Ruijie(config-if-wlansec)# end
```

【检验方法】 1：使用 **show run** 命令，来查看对应接口上配置的报文抑制状态。

【提示信息】 1：当在 DHCP TRUST 口上配置时，则提示错误。

```
% Failed to execute command, because of "Security config conflict".
```

2：当有线接入不是在 2 层交换口、AP 口或者 2 层封装子接口上上执行该命令时，则提示错误。

```
% Failed to execute command, because of "Configure is not supported on current interface".
```

【常见错误】 -

【平台说明】 -

5.12 ip dhcp snooping verify mac-address

打开源 MAC 地址校验功能。
ip dhcp snooping verify mac-address

关闭源 MAC 地址检验功能。
no ip dhcp snooping verify mac-address

【参数说明】

参数	描述

-	-

【缺省配置】 该功能缺省关闭。

【命令模式】 全局配置模式

【缺省级别】 14

【使用指导】 源 MAC 地址检验功能，是对来自 UNTRUST 接口上的 DHCP 请求报文进行检查，检查链路层头部源 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。

【配置举例】 1：下面是打开 DHCP 报文源 MAC 检查的例子：

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

【检验方法】 1：使用 **show ip dhcp snooping** 命令，可以查看功能是否开启。

【提示信息】 -

【常见错误】 -

【平台说明】 -

5.13 ip dhcp snooping vlan

打开指定 VLAN 上的 DHCP Snooping 功能。
ip dhcp snooping vlan { *vlan-rng* **|** { *vlan-min* [*vlan-max*] } }

关闭对应 VLAN 上的 DHCP Snooping 功能。
no ip dhcp snooping vlan { *vlan-rng* **|** { *vlan-min* [*vlan-max*] } }

【参数说明】

参数	描述
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。

【缺省配置】 缺省情况下，开启全局 DHCP Snooping 功能后，所有 VLAN 上都将启用 DHCP Snooping 功能。

【命令模式】 全局配置模式

【缺省级别】 14

【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。

【配置举例】 1：下面是在 VLAN1000 上打开 DHCP Snooping 功能的例子：

```
Ruijie# configure terminal
Ruijie(config)# ip dhcp snooping vlan 1000
Ruijie(config)# end
```

2：下面是在 VLAN1 至 VLAN10 上打开 DHCP Snooping 功能的例子：

```
Ruijie# configure terminal
Ruijie(config)# ip dhcp snooping vlan 1-10
Ruijie(config)# end
```

【检验方法】 1：使用 **show run** 命令，可以查看哪些 VLAN 处于关闭模式。

【提示信息】 1：若设置的 VLAN 值不在 1~4094 范围内，则提示错误。

```
% Failed to execute command, because of "Not supported vlan range".
```

2：若指定的 VLAN 不存在，则提示错误。

```
% Failed to execute command, because of "VLAN not exist".
```

【常见错误】 -

【平台说明】 -

5.14 renew ip dhcp snooping database

手动地把当前备份文件中的信息导入 DHCP Snooping 绑定数据库。

renew ip dhcp snooping database

【参数说明】

参数	描述
-	-

【缺省配置】 -

【命令模式】 特权模式

【缺省级别】 14

【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。

文件中租约过期的记录会被忽略。

仅添加当前数据库中不存在的记录。

【配置举例】 1：下面是将备份文件信息导入 DHCP Snooping 数据库中的例子：

```
Ruijie# renew ip dhcp snooping database
```

【检验方法】 1：使用命令 **show ip dhcp snooping binding**，可以查看记录是否导入。

【提示信息】 -

【常见错误】 -

【平台说明】 -

5.15 show ip dhcp snooping

要查看 DHCP Snooping 当前的配置情况，需要在特权模式下执行此命令。

show ip dhcp snooping

【参数说明】

参数	描述
-	-

【命令模式】 特权模式

【缺省级别】 14

【使用指导】 执行此命令，可以查看当前 DHCP Snooping 的配置情况。

【配置举例】 1：下面是查看当前 DHCP Snooping 配置情况的例子：

```
Ruijie# show ip dhcp snooping
Switch DHCP snooping  status                    :   ENABLE
DHCP snooping  Verification of hwaddr status    :   DISABLE
DHCP snooping database write-delay time         :   0 seconds
DHCP snooping option 82 status                  :   DISABLE
DHCP snooping Support bootp bind status         :   DISABLE

Interface                                       Trusted            Rate limit(pps)
------------------------                        ----------------   ----------------
GigabitEthernet 0/4                             YES                unlimited
```

```
Default                                  No
```

字段解释：

字段	说明
Switch DHCP snooping status	设备的全局 DHCP Snooping 功能是否开启。
Verification of hwaddr field status	DHCP snooping 报文源 mac 检查开关状态。
DHCP snooping database write-delay time	定时写备份文件的时间间隔。
DHCP snooping option 82 status	是否在 DHCP 请求报文中加入 option82 选项。
DHCP snooping Support Bootp bind status	是否打开 DHCP Snooping 支持 Bootp 绑定功能。
Interface	接口名称。
Trusted	该接口是否是 TRUST 口。
Rate limit	该接口的 DHCP 报文限速值

【提示信息】 -

【平台说明】 -

5.16 show ip dhcp snooping binding

查看 DHCP Snooping 数据库中的用户信息。

show ip dhcp snooping binding

【参数说明】

参数	描述
-	-

【命令模式】 特权模式

【缺省级别】 14

【使用指导】 执行此命令，可以查看当前 DHCP Snooping 数据库中所有的用户信息。

【配置举例】 1：下面是显示例子：

```
Ruijie# show ip dhcp snooping binding
Total number of bindings: 1
NO.    MACADDRESS          IPADDRESS       LEASE(SEC)    TYPE           VLAN  INTERFACE
-----  ------------------  --------------  ------------  -------------  ----  --------------------
1      0000.0000.0001      1.1.1.1         78128         DHCP-Snooping  1     GigabitEthernet 0/1
2      0000.0000.0002      2.2.2.2         78111         DHCP-Snooping  1     WLAN 1
```

2：对于支持 QINQ 终结的产品，显示包括 inner-vlan 的信息。

```
Ruijie# show ip dhcp snooping binding
Total number of bindings: 1
```

```
NO.    MACADDRESS          IPADDRESS       LEASE(SEC)    TYPE           VLAN   INNER-VLAN INTERFACE
-----  ------------------  --------------- ------------  -------------  -----  ----------
--------------------
1      0000.0000.0001      1.1.1.1         78128         DHCP-Snooping 1      10
GigabitEthernet 0/1
```

字段解释：

字段	说明
Total number of bindings	当前 DHCP Snooping Binding 数据库中绑定的个数。
NO.	记录序号
MacAddress	用户 MAC 地址。
IpAddress	用户 IP 地址。
Lease(sec)	记录租约时间。
Type	记录类型。
VLAN	用户所属 VLAN。
INNER-VLAN	用户的内层 vlan id，适用于 QINQ 终结的产品
Interface	用户连接端口，有线接入接口或者无线接入 WLAN

【提示信息】 -

【平台说明】 -

6 ARP Check

6.1 arp-check

开启 ARP 报文检查。
arp-check

关闭 ARP 报文检查。
no arp-check

【参数说明】

参数	描述
-	-

【缺省配置】 关闭 ARP Check 功能

【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

【缺省级别】 14

【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】 下面是在端口 GigabitEthernet 0/1 上开启 ARP Check 的例子：

```
Ruijie# configure terminal
Ruijie(config)# interface GigabitEthernet 0/1
Ruijie(config-if-GigabitEthernet 0/1)# arp-check
Ruijie(config-if-GigabitEthernet 0/1)# end
Ruijie# configure terminal
Ruijie(config)# wlansec 1
Ruijie(config-wlansec)# arp-check
Ruijie(config-wlansec)# end
```

【检验方法】 1：使用 **show interface arp-check list** 命令，可以查看接口下实际生效的 ARP Check 表项。

【提示信息】 -

【常见错误】 -

【平台说明】 -

6.2 show interfaces arp-check list

查看接口下实际生效的 ARP Check 表项。

show { **interfaces** [*interface-type interface-number*] | **wlan** [*wlan-id*] } **arp-check list**

【参数说明】

参数	描述
interface-type	有线接口类型；
interface-number	有线接口编号；
wlan-id	无线 WLAN ID

【命令模式】 特权模式

【缺省级别】 14

【使用指导】 执行此命令，可以查看当前 IP 源地址绑定数据库的配置情况。

【配置举例】 下面是显示例子：

```
Ruijie(config)#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 0/4                     192.168.1.3      port-security
GigabitEthernet 0/5      00D0.F800.0003 192.168.1.3      address-bind
GigabitEthernet 0/7      00D0.F800.0006 192.168.1.6      AAA ip-auth-mode
GigabitEthernet 0/8      00D0.F800.0007 192.168.1.7      GSN
Ruijie(config)#show wlan arp-check list
INTERFACE                SENDER MAC     SENDER IP        POLICY SOURCE
-----------------------  -------------- ---------------- --------------------
WLAN 1                   00D0.F800.0008 192.168.1.8      GSN
```

字段解释：

字段	说明
INTERFACE	接口名称
SENDER MAC	源 MAC 地址
SENDER IP	源 IP 地址
POLICY SOURCE	记录来源

【提示信息】 -

【平台说明】 -

7 IP Source Guard

7.1 ip source binding

在 IP 源地址绑定数据库中添加静态用户信息。

ip source binding *mac-address* **{ vlan** *vlan-id* **}** *ip-address* { **interface** *interface-id* **| wlan** *wlan-id* **| ip-mac | ip-only** }

删除对应的静态用户。

no ip source binding *mac-address* **{ vlan** *vlan-id* **}** *ip-address* { **interface** *interface-id* **| wlan** *wlan-id* **| ip-mac | ip-only** }

【参数说明】

参数	描述
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 终结的产品，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入口。
wlan *wlan-id*	静态添加的用户所属的无线接入 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。

【缺省配置】 没有添加任何静态用户的地址。

【命令模式】 全局配置模式

【缺省级别】 14

【使用指导】 1：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。

2：只支持在有线接入 2 层交换口、AP 口、封装子接口或者无线接入 WLAN 上使用该命令进行配置。其他类型的端口将配置失败。

3：可以通过配置全局绑定用户记录，使得部分用户可以在所有端口口上通过 IP Source Guard 的检测。

4：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。

一条配置的绑定记录要么在有线接入接口上生效，要么在无线接入 WLAN 上生效，要么在全局范围内生效。

相同的用户记录，新记录将覆盖旧记录的属性。

【配置举例】 1：下面是设置配置一个静态用户到有线交换口或者无线 WLAN 的例子：

```
Ruijie# configure terminal
Ruijie(config)# ip source binding 0000.0000.0001 vlan 1 1.1.1.1 interface GigabitEthernet 0/1
Ruijie(config)# ip source binding 0000.0000.0002 vlan 1 1.1.1.2 wlan 1
Ruijie(config)# end
```

2：下面是设置一个静态用户在全局范围内生效，并且过滤类型是 IP+MAC 绑定的例子：

```
Ruijie# configure terminal
Ruijie(config)# ip source binding 0000.0000.0001 vlan 1 1.1.1.1 ip-mac
Ruijie(config)# end
```

3：下面是设置一个静态用户在全局范围内生效，并且过滤类型是仅 IP 绑定的例子：

```
Ruijie# configure terminal
Ruijie(config)# ip source binding 0000.0000.0001 vlan 1 1.1.1.1 ip-only
Ruijie(config)# end
```

4：下面是设置一个 QINQ 场景下的静态用户在全局范围内生效，并且过滤类型是仅 IP 绑定的例子：

```
Ruijie# configure terminal
Ruijie(config)# ip source binding 0000.0000.0001 vlan 1 inner-vlan 10 1.1.1.1 ip-only
Ruijie(config)# end
```

【检验方法】 1：使用 **show ip source binding** 命令，可以查看 IP 源地址绑定数据库。

【提示信息】 1：使用 no 命令删除静态配置时，输入的参数与之前配置时的参数不一致，则提示错误。

```
% Failed to execute command, because of "No such binding entry
[mac 0000.0000.0001 ip 1.1.1.1 vlan 2  GLOBAL]".
```

2：配置用户记录时，若输入的 VLAN 并不存在，则提示错误。

```
% Failed to execute command, because of "VLAN 4094 not exist".
```

3：配置用户记录时，若输入的有线接口不是二层交换口、AP 口或者封装子接口，则提示错误。

```
% Failed to execute command, because of "Configure is not supported on current interface".
```

【常见错误】 -

【平台说明】 -

7.2 ip verify source

打开端口上的 IP Source Guard 功能。

ip verify source [**port-security**]

关闭端口上的 IP Source Guard 功能。

no ip verify source

【参数说明】

参数	描述
port-security	配置 IP Source Guard 功能进行基于 IP+MAC 检测。

【缺省配置】 该功能缺省关闭。

【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

【缺省级别】 14

【使用指导】 1：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。

2：仅支持在有线接入的 2 层交换口、AP 口、封装子接口以及无线接入 WLAN 上配置该命令。其他类型的接口上将配置失败。

3：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。

⚠ 目前锐捷设备 IP Source Gourd 功能依赖的合法用户数量来源于 DHCP Snooping 与用户静态配置。若端口上仅仅开启了 IP Source Gourd 功能，但是没有配置合法数据来源，会导致连接到该端口的用户无法正常使用网络。

【配置举例】 1：下面是配置有线交换口和无线 WLAN 上的 IP Source Guard 功能，仅对用户进行基于 IP 的检测：

```
Ruijie# configure terminal
Ruijie(config)# interface GigabitEthernet 0/1
Ruijie(config-if-GigabitEthernet 0/1)# ip verify source
Ruijie(config-if)# end
Ruijie(config)# wlansec 1
Ruijie(config-wlansec)# ip verify source
Ruijie(config-wlansec)# end
```

2：下面是配置接口 2 上的 IP Source Guard 功能，对用户进行基于 IP+MAC 的检测：

```
Ruijie# configure terminal
Ruijie(config)# interface GigabitEthernet 0/2
Ruijie(config-if-GigabitEthernet 0/2)# ip verify source port-security
Ruijie(config-if)# end
Ruijie(config)# wlansec 2
Ruijie(config-wlansec)# ip verify source port-security
Ruijie(config-wlansec)# end
```

【检验方法】 1：使用 **show ip source binding** 命令，可以查看 IP Source Guard 用户过滤表项。
2：使用 **show run** 命令，可以查看命令是否配置成功。

【提示信息】 1：如果在 DHCP 信任口上操作，则提示错误。

```
% Failed to execute command, because of “Security configuration conflict in interface name”.
```

【常见错误】 1：开启 IP Source Gourd，而不配置合法用户记录的来源。

【平台说明】 -

7.3 Ip verify source exclude-vlan

端口上指定 IP Source Guard 的例外 VLAN 功能。
ip verify source exclude-vlan *vlan-id*

删除端口上 IP Source Guard 的例外 VLAN 功能。
no ip verify source exclude-vlan *vlan-id*

【参数说明】

参数	描述
vlan-id	不受端口上 IP Source Guard 控制的 vlan id

【缺省配置】 该功能缺省关闭。

【命令模式】 接口配置模式或者无线安全配置模式

【缺省级别】 14

【使用指导】 1：启动 IP Source Guard 的端口上，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。
2：端口上关闭 IP Source Guard 后，指定的例外 VLAN 也会被自动清除。
3：支持在有线接入的 2 层交换口、AP 口、封装子接口或者无线接入的 WLAN 下配置。

⚠ 接口下必须先启动 IP Source Guard 才可以指定例外 VLAN。

【配置举例】 1：下面是配置端口上的 IP Source Guard 功能并指定例外 VLAN：

```
Ruijie# configure terminal
Ruijie(config)# interface GigabitEthernet 0/1
Ruijie(config-if-GigabitEthernet 0/1)# ip verify source
Ruijie(config-if-GigabitEthernet 0/1)# ip verify exclude-vlan 1
Ruijie(config-if)# end
Ruijie(config)# wlansec 1
```

```
Ruijie(config-wlansec)# ip verify source
Ruijie(config-wlansec)# ip verify exclude-vlan 1
Ruijie(config-wlansec)# end
```

【检验方法】 1：使用 **show run** 命令，可以查看命令是否配置成功。

【提示信息】 -

【常见错误】 -

【平台说明】 -

7.4 show ip source binding

查看 IP 源地址绑定数据库的信息。

show ip source binding [*ip-address*] [*mac-address*] [**dhcp-snooping**] [**static**] [**vlan** *vlan-id*] [**interface** *interface-id*] [**wlan** *wlan-id*]

【参数说明】

参数	描述
ip-address	显示对应 ip 的用户绑定信息；
mac-address	显示对应 mac 的用户绑定信息；
dhcp-snooping	显示动态用户的绑定信息；
static	显示静态用户的绑定信息；
vlan-id	显示对应 vlan 的用户绑定信息；
interface-id	显示对应有线接入接口的用户绑定信息；
wlan-id	显示对应无线接入 WLAN 的用户绑定信息；

【命令模式】 特权模式

【缺省级别】 14

【使用指导】 执行此命令，可以查看当前 IP 源地址绑定数据库的配置情况。

【配置举例】 1：下面是显示例子：

```
Ruijie# show ip source binding static
Ruijie#show ip source binding static
Total number of bindings: 5
NO.    MACADDRESS         IPADDRESS       LEASE(SEC)    TYPE          VLAN  INTERFACE
-----  -----------------  --------------  ------------  ------------  ----  --------------------
1      0001.0002.0001     1.2.3.2         Infinite      Static        1     Global
2      0001.0002.0002     1.2.3.3         Infinite      Static        1     GigabitEthernet 0/5
```

```
3      0001.0002.0003      1.2.3.4          Infinite      Static         1      Global
4      0001.0002.0004      1.2.3.5          Infinite      Static         1      Global
5      0001.0002.0005      1.2.3.6          Infinite      Static         1      WLAN 1
```

2：对于支持 QINQ 终结的产品，显示包括 inner-vlan 的信息。

```
Ruijie# show ip source binding inner-vlan 10
Total number of bindings: 1
NO.    MACADDRESS          IPADDRESS       LEASE(SEC)    TYPE           VLAN   INNER-VLAN INTERFACE
----- ------------------ --------------- ------------ ------------- ----- ----------
--------------------
1      0001.0002.0001      1.2.3.2          Infinite      Static         1      10         Global
```

字段解释：

字段	说明
Total number of bindings	当前 Binding 数据库中绑定的个数
NO.	记录序号
MACADDRESS	用户 MAC 地址
IPADDRESS	用户 IP 地址
LEASE(SEC)	记录租约时间
TYPE	记录类型
VLAN	用户所属 VLAN
INTERFACE	有线接口名称或者无线 WLAN ID
INNER-VLAN	用户的内层 vlan id，适用于 QINQ 终结的产品

【提示信息】 -

【平台说明】 -

7.5 show ip verify source

查看 IP Source Guard 用户过滤表项。

show ip verify source [**interface** *interface-id*] [**wlan** *wlan-id*]

【参数说明】

参数	描述
interface-id	显示对应有线接口的用户过滤表项
wlan-id	显示对应无线 WLAN 的用户过滤表项

【命令模式】 特权模式

【缺省级别】 14

【使用指导】 执行此命令，可以查看当前IP源地址绑定用户记录的生效情况。目前IP Source Guard支持的记录状态包括如下：

- Inactive-restrict-off，绑定记录所属的接口没有开启 IP Source Guard 功能。
- Inactive-not-apply，由于系统错误，无法将绑定的用户记录转换成过滤表项。
- Active，绑定的用户记录表项对应的过滤表项已经生效。

【配置举例】 1：下面是显示例子：

```
Ruijie # show ip verify source
Total number of bindings: 7
NO.    INTERFACE            FILTERTYPE  FILTERSTATUS           IPADDRESS       MACADDRESS
VLAN TYPE
-----  -------------------- ----------- ---------------------  --------------- ---------------
-------- -------------
1      Global               IP+MAC      Inactive-not-apply     192.168.0.127   0001.0002.0003  1
Static
2      GigabitEthernet 0/5  IP-ONLY     Active                 1.2.3.4         0001.0002.0004  1
DHCP-Snooping
3      Global               IP-ONLY     Active                 1.2.3.7         0001.0002.0007  1
Static
4      Global               IP+MAC      Active                 1.2.3.6         0001.0002.0006  1
Static
5      GigabitEthernet 0/1  UNSET       Inactive-restrict-off  1.2.3.9         0001.0002.0009  1
DHCP-Snooping
6      GigabitEthernet 0/5  IP-ONLY     Active                 Deny-All
7      WLAN 1               IP-ONLY     Active                 Deny-ALL
```

2：对于支持 QINQ 终结的产品，显示包括 inner-vlan 的信息。

```
Ruijie # show ip verify source
Total number of bindings: 2
NO.    INTERFACE            FILTERTYPE  FILTERSTATUS           IPADDRESS       MACADDRESS
VLAN   INNER-VLAN   TYPE
-----  -------------------- ----------- ---------------------  --------------- ---------------
-------- -------- -------------
1      Global               IP+MAC      Inactive-not-apply     192.168.0.127   0001.0002.0003  1
15     Static
2      Global               IP-ONLY     Active                 1.2.3.7         0001.0002.0007  1
10     Static
```

字段解释：

字段	说明
NO.	记录序号
INTERFACE	有线接入接口或者无线接入 WLAN
FILTERTYPE	过滤策略
FILTERSTATUS	状态
IPADDRESS	用户 IP 地址
MACADDRESS	用户 MAC 地址
VLAN	用户所属 VLAN
TYPE	用户类型，包括 DHCP Snooping 动态生成或者静态配置生成
INNER-VLAN	用户的内层 vlan id，适用于 QINQ 终结的产品

【提示信息】 -

【平台说明】 -

8 VPDN

8.1 accept dialin

设置隧道工作模式为接受拨入。
accept-dialin

恢复系统缺省设置
no accept-dialin

【参数说明】

参数	描述
-	-

【缺省配置】 缺省情况下，系统没有设置隧道工作模式。

【命令模式】 VPDN-Group 接口配置模式

【缺省级别】 14

【使用指导】 缺省情况下，系统没有为 VPDN-Group 指定任何隧道工作模式。用户必须首先设置隧道工作模式才能进一步设置隧道工作协议与绑定的虚模板接口。本命令的有效设置或者改变会立即导致已经存在地相关隧道被主动强制拆除。

【配置举例】 1：设置隧道工作模式为接受拨入。

```
Ruijie(config)#vpdn-group 1
Ruijie(config-vpdn)#accept-dialin
Ruijie(config-vpdn-acc-in)#
```

【检验方法】 使用 **show running-config** 命令，可以查看隧道工作模式是否为接受拨入。

【提示信息】 -

【常见错误】 本命令的有效设置或者改变会立即导致已经存在地相关隧道被主动强制拆除。

【平台说明】 -

8.2 authentication (L2TP)

启用通道验证功能。
authentication

恢复系统缺省设置
no authentication

【参数说明】

参数	描述
-	-

【缺省配置】 缺省情况下，系统禁用通道验证功能。

【命令模式】 L2TP-Class 接口配置模式

【缺省级别】 14

【使用指导】 用户可以根据需要启用或者禁用通道验证功能。

【配置举例】 1：启用通道验证功能。

```
Ruijie(config)#l2tp-class 1
Ruijie(config-l2tp-class)#authentication
Ruijie(config-l2tp-class)#
```

【检验方法】 使用 **show running-config** 命令，可以查看是否通道验证功能。

【提示信息】 -

【常见错误】 对通道验证功能设置的有效改变都会导致引用该 L2TP-Class 的相关隧道被主动强制拆除。

【平台说明】 -

8.3 clear vpdn log

清除日志文件中保存的用户上下线信息
clear vpdn log

【参数说明】

参数	描述
-	-

【命令模式】 特权用户模式

【缺省级别】 14

【使用指导】 本命令将清除日志文件中保存的用户上下线信息

【配置举例】 1：清除日志文件中保存的用户上下线信息

```
Ruijie# show vpdn log
Username                        IP          State  Online time         Offline time
user-1                          100.1.1.2   out    2014-11-16-14:09:04  2014-11-16-14:29:26
user-2                          100.1.2.2   out    2014-11-16-15:09:05  2014-11-16-16:09:27
Ruijie# clear vpdn log
Ruijie#
Ruijie# show vpdn log
%No vpdn logs.
Ruijie#
```

【提示信息】 -

【平台说明】 -

8.4 clear vpdn tunnel

强制清除指定的隧道。

clear vpdn tunnel [{ **l2tp** | **pptp** } [**id** *locid*] | [*remote-host-name*] **]**

【参数说明】

参数	描述
l2tp	L2TP 隧道
pptp	PPTP 隧道
remote-host-name	隧道对端主机名称
locid	指定隧道 ID 删除对应隧道

【命令模式】 特权用户模式

【缺省级别】 14

【使用指导】 本命令将强制清除指定的隧道。如果不使用参数，那么将强制清除所有已经存在的隧道(包括 PPTP 与 L2TP 隧道)；如果仅仅指定隧道协议，那么将强制清除对应隧道协议的所有隧道；如果还指定了隧道对端主机名称，那么将强制清除对应隧道协议相关隧道中隧道对端主机名称匹配指定名称的隧道。

指定隧道 ID 删除隧道中使用的 ID 是 show vpdn 中 tunID 信息

【配置举例】 1：清除所有存在的 L2TP 隧道。

```
Ruijie# show vpdn
L2TP Tunnel and Session Information Total tunnels 1 sessions 1
LocID RemID Remote Name   State  Remote Address  Port  Sessions L2TP Class/
VPDN Group
1     1     BLIZZARD   est    192.168.12.213  1701  1  1
LocID      RemID      TunID      Username, Intf/
State  Last Chg                        Vcid, Circuit
1          1          1          ms,Vi1               est
00:46:30
%No active PPTP tunnels
Ruijie# clear vpdn tunnel l2tp
Ruijie#
%UPDOWN: Line protocol on Interface Virtual-Access1, changed state to down
%CHANGED: Interface Virtual-Access1, changed state to administratively down
Ruijie# show vpdn
%No active L2TP tunnels
%No active PPTP tunnels
Ruijie#
```

【提示信息】 -

【平台说明】 -

8.5 encapsulation (L2TP)

设置隧道的数据封装模式。

encapsulation l2tpv2

【参数说明】

参数	描述
l2tpv2	使用 RFC 2661 规范设定的 L2TP 来传输隧道数据

【缺省配置】 缺省情况下，系统没有设置隧道的数据封装模式。

【命令模式】 Pseudowire-Class 接口配置模式

【缺省级别】 14

【使用指导】 在 pseudowire-class 接口上，必须首先设定隧道数据封装模式才能进一步设置隧道数据传输参数

【配置举例】 1：设置隧道数据封装模式为 l2tpv2。

```
Ruijie(config)#
Ruijie(config)#pseudowire-class 1
Ruijie(config-pw-class)#encapsulation l2tpv2
Ruijie(config-pw-class)#
```

【检验方法】 使用 **show running-config** 命令，可以查看隧道的数据封装模式。

【提示信息】 -

【常见错误】 -

【平台说明】 -

8.6 force-local-chap

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。

force-local-chap

恢复系统缺省设置

no force-local-chap

【参数说明】

参数	描述
-	-

【缺省配置】 缺省情况下，LNS 不需要再对 Clinet 进行认证。

【命令模式】 VPDN-Group 接口配置模式

【缺省级别】 14

【使用指导】 只有当 vpdn enable 配置以后该命令可以配置

【配置举例】 1：设置隧道重新认证 PPP LCP。

```
Ruijie(config-vpdn)# force-local-chap
Ruijie(config-vpdn)#
```

【检验方法】 使用 **show running-config** 命令，可查看是否对 Clinet 进行认证。

【提示信息】 -

【常见错误】 -

【平台说明】 -

8.7 force-local-lcp

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 进行协商。该命令只在 LNS 上有效。

force-local-lcp

恢复系统缺省设置

no force-local-lcp

【参数说明】

参数	描述
-	-

【缺省配置】 缺省情况下，LNS 不需要再对 Clinet 进行 lcp 协商。

【命令模式】 VPDN-Group 接口配置模式

【缺省级别】 14

【使用指导】 只有当 vpdn enable 配置以后该命令可以配置

【配置举例】 1：设置隧道重新认证 PPP LCP。

```
Ruijie(config-vpdn)# force-local-lcp
Ruijie(config-vpdn)#
```

【检验方法】 使用 **show running-config** 命令，可查看是否对 Clinet 进行协商。

【提示信息】 -

【常见错误】 -

【平台说明】 -

8.8 hello

本命令设置为实现 L2TP 通道 Keepalive 而发送的 Hello 消息的发送间隔。
hello *interval*

恢复系统缺省设置
no hello

【参数说明】

参数	描述
interval	Hello 消息发送间隔，单位是秒，取值范围是 1-1000

【缺省配置】 缺省情况下，Hello 消息发送间隔为 60 秒。

【命令模式】 L2TP-Class 接口配置模式

【缺省级别】 14

【使用指导】 用户可以根据网络环境来设置 Hello 消息发送间隔以检测 L2TP 通道是否依然可用。如果网络稳定可靠，就可以将 Hello 消息发送间隔设为一个较大值。

【配置举例】 1：设置 Hello 消息发送间隔为 120 秒。

```
Ruijie(config-l2tp-class)# hello 120
Ruijie(config-l2tp-class)#
```

【检验方法】 使用 **show running-config** 命令，可以查看发送的 Hello 消息的发送间隔

【提示信息】

【常见错误】 任何对 Hello 发送间隔设置的有效改变都会导致对应的已经存在的 L2TP 隧道被主动强制拆除

【平台说明】 -

8.9 hostname (L2TP)

设置 L2TP 隧道本地端主机名称。
hostname *local-hostname-string*

恢复系统缺省设置
no hostname

【参数说明】

参数	描述
local-hostname-string	隧道本地端主机名称

【缺省配置】 缺省情况下，系统使用路由器的名称作为隧道本地端主机名称。

【命令模式】 L2TP-Class 接口配置模式

【缺省级别】 14

【使用指导】 用户可以按照需要设置隧道本地端主机名称用以进行隧道标识。任何对隧道本地端主机名称的有效改变都会导致已经存在的对应 L2TP 隧道被强制主动拆除

【配置举例】 1：将设置隧道本地端主机名称为”LAC”。

```
Ruijie(config-l2tp-class)# hostname LAC
Ruijie(config-l2tp-class)#
```

【检验方法】 使用 **show running-config** 命令，可以查看隧道本地端主机名称

【提示信息】

【常见错误】 -

【平台说明】 -

8.10 ip dfbit set

禁止隧道数据被分片发送。
ip dfbit set

恢复系统默认值
no ip dfbit set

【参数说明】

参数	描述
-	-

【缺省配置】 缺省情况下，系统允许隧道数据被分片发送。

【命令模式】 Pseudowire-Class 接口配置模式

【缺省级别】 14

【使用指导】 用户可以根据需要设置是否允许隧道数据被分片发送。任何对隧道数据分片发送功能的设置的有效改动都会立即反映到隧道数据传输上，但是不会导致对应的 L2TP 隧道被强制拆除

【配置举例】 1：禁止隧道数据被分片发送。

```
Ruijie(config-pw-class)# ip dfbit set
Ruijie(config-pw-class)#
```

【检验方法】 使用 **show running-config** 命令，可以查看是否禁止隧道数据被分片发送

【提示信息】

【常见错误】

【平台说明】 -

8.11 ip local interface

设置隧道使用的本地(源)接口。
ip local interface *interface-name*

恢复系统缺省设置
no ip local interface *interface-name*

【参数说明】

参数	描述
interface-name	本地接口名称

【缺省配置】 缺省情况下，统没有指定隧道使用的本地(源)接口。

【命令模式】 Pseudowire-Class 接口配置模式

【缺省级别】 14

【使用指导】 用户可以指定路由器上的网络接口作为隧道的本地(源)接口。任何对隧道本地(源)接口设置的有效改变都会导致对应的 L2TP 隧道被主动强制拆除

【配置举例】 1：设置隧道的本地(源)接口为 Serial 0。

```
Ruijie(config-pw-class)# ip local interface serial 0
Ruijie(config-pw-class)#
```

【检验方法】 使用 **show running-config** 命令，可以查看隧道使用的本地(源)接口

【提示信息】

【常见错误】

【平台说明】 -

8.12 ip precedence

设置负载隧道的 IP 头优先级域。

ip precedence { *precedence-value* **| critical | flash | flash-override | immediate | internet | network | priority | routine }**

恢复系统缺省设置

no ip precedence

【参数说明】

参数	描述
precedence-value	优先级域的值，取值范围为 0~7
critical	优先级域的值为 5
flash	优先级域的值为 3
flash-override	优先级域的值为 4
immediate	优先级域的值为 2
internet	优先级域的值为 6
network	优先级域的值为 7
priority	优先级域的值为 1
routine	优先级域的值为 0

【缺省配置】 缺省情况下，系统设置负载隧道的 IP 头优先级域值为零即 **routine**。

【命令模式】 VPDN-Group 接口配置模式

【缺省级别】 14

【使用指导】 如果用户需要设置隧道数据的优先级可以使用本命令实现。本命令的有效设置会立即影响隧道数据传输，但不会导致相关的隧道被主动强制拆毁。

【配置举例】 1：设置隧道数据的优先级为 7。

```
Ruijie(config-vpdn)# ip precedence 7
Ruijie(config-vpdn)#
```

【检验方法】 使用 **show running-config** 命令，可以查看负载隧道的 IP 头优先级域

【提示信息】

【常见错误】 该命令只对 L2TP 生效，对 PPTP 不生效

【平台说明】 -

8.13 ip tos

设置负载隧道的 IP 头 TOS(Type of Service)域。

ip tos { *tos-value* | **max-reliability** | **max-throughput** | **min-delay** | **min- monetary-cost** | **normal** | **reflect** }

恢复系统缺省设置

no ip tos

【参数说明】

参数	描述
tos-value	TOS 域的值，取值范围为 0~15
max-reliability	TOS 域的值为 2
max-throughput	TOS 域的值为 4
min-delay	TOS 域的值为 8
min-monetary-cost	TOS 域的值为 1
normal	TOS 域的值为 0
reflect	使用隧道负载的 IP 数据包的 TOS 作为负载隧道的 IP 头的 TOS 域

【缺省配置】 缺省情况下，负载隧道的 IP 头的 TOS 域为零。

【命令模式】 VPDN-Group 接口配置模式

【缺省级别】 14

【使用指导】 如果用户需要设置隧道数据的 TOS 可以使用本命令实现。本命令的有效设置会立即影响隧道数据传输，但不会导致相关的隧道被主动强制拆毁。

【配置举例】 1：设置隧道数据的 TOS 为 **min-delay**。

```
Ruijie(config-vpdn)# ip tos min-delay
Ruijie(config-vpdn)#
```

【检验方法】 使用 **show running-config** 命令，可以查看负载隧道的 IP 头 TOS(Type of Service)域

【提示信息】

【常见错误】

【平台说明】 -

8.14 ip ttl

设置负载隧道数据的 IP 头的 TTL 域。
ip ttl *ttl-value*

恢复系统缺省设置
no ip ttl

【参数说明】

参数	描述
ttl-value	TTL 域的值，取值范围为 1~255

【缺省配置】 缺省情况下，系统设置负载隧道数据的 IP 头的 TTL 域为 255

【命令模式】 Pseudowire-Class 接口配置模式

【缺省级别】 14

【使用指导】 用户可以按照需要设置负载隧道数据的 IP 头的 TTL 域。任何对负载隧道数据的 IP 头的 TTL 域的设置的有效改动都会立即反映到隧道数据传输上，但是不会导致对应的 L2TP 隧道被强制拆除

【配置举例】 1：设置负载隧道数据的 IP 头的 TTL 域为 253。

```
Ruijie(config-pw-class)# ip ttl 253
Ruijie(config-pw-class)#
```

【检验方法】 使用 **show running-config** 命令，可以查看是否有设置负载隧道数据的 IP 头的 TTL 域

【提示信息】

【常见错误】

【平台说明】 -

8.15 l2tp ip udp checksum

本命令要求负载隧道数据的 UDP 报文计算并填充 Checksum 域。
l2tp ip udp checksum

恢复系统缺省设置
no l2tp ip udp checksum

【参数说明】

参数	描述
-	-

【缺省配置】 缺省情况下，系统要求负载隧道数据的 UDP 报文的 Checksum 域为空(即为零)。

【命令模式】 VPDN-Group 接口配置模式

【缺省级别】 14

【使用指导】 用户可以依据需要设置是否要求负载隧道数据的UDP报文计算并填充Checksum域。必须先配置protocol l2tp 或者 protocol any 该命令才会显示出来。

【配置举例】 1：要求负载隧道数据的 UDP 报文提供 Checksum。

```
Ruijie(config)#
Ruijie(config)#vpdn-group 1
Ruijie(config-vpdn)#accept-dialin
Ruijie(config-vpdn-acc-in)#protocol any
Ruijie(config-vpdn-acc-in)#exit
Ruijie(config-vpdn)#l2tp ip udp checksum
Ruijie(config-vpdn)#
```

【检验方法】 使用 **show running-config** 命令，可以查看是否按负载隧道数据的 UDP 报文计算

【提示信息】

【常见错误】 任何对负载隧道数据的 UDP 报文的 Checksum 域的设置的有效改动都会立即反映到隧道数据传输上，但是不会导致对应的 L2TP 隧道被强制拆除

【平台说明】 -

8.16 l2tp tunnel authentication

启用通道验证功能。
l2tp tunnel authentication

恢复系统缺省设置
no l2tp tunnel authentication

【参数说明】

参数	描述
-	-

【缺省配置】 缺省情况下，系统禁用通道验证功能。

【命令模式】 VPDN-Group 接口配置模式

【缺省级别】 14

【使用指导】 用户可以根据需要启用或者禁用通道验证功能。任何对通道验证功能设置的有效改动都会导致相关的 L2TP 隧道被强制主动拆除，必须先配置 protocol l2tp 或者 protocol any 该命令才会显示出来。

【配置举例】 1：启用通道验证功能。

```
Ruijie(config)#
Ruijie(config)#vpdn-group 1
Ruijie(config-vpdn)#accept-dialin
Ruijie(config-vpdn-acc-in)#protocol any
Ruijie(config-vpdn-acc-in)#exit
Ruijie(config-vpdn)#l2tp tunnel authentication
Ruijie(config-vpdn)#
```

【检验方法】 使用 **show running-config** 命令，可以查看是否启用通道验证功能

【提示信息】

【常见错误】

【平台说明】 -

8.17 l2tp tunnel avp-hidden-compatible

配置本命令表示兼容支持 RFC2661 标准 AVP Hidden 解析算法，默认情况下支持 Cisco 标准 AVP Hidden 解析算法。
l2tp tunnel avp-hidden-compatible

恢复系统缺省设置
no l2tp tunnel avp-hidden-compatible

【参数说明】

参数	描述
-	-

【缺省配置】 缺省情况下，系统采用 Cisco 标准 AVP Hidden 解析算法。

【命令模式】 VPDN-Group 接口配置模式

【缺省级别】 14

【使用指导】 用户可以根据需要启用或者禁用兼容 RFC2661 AVP Hidden 解析算法。如果需要支持两种 AVP Hidden 解析算法，可以通过配置多个 VPDN-Group 来达到目的。配置该命令不会影响当前 L2TP 隧道

【配置举例】 1：配置兼容 RFC2661 标准 AVP Hidden 解析功能。

```
Ruijie(config-vpdn)# l2tp tunnel avp-hidden-compatible
Ruijie(config-vpdn)#
```

【检验方法】 使用 **show running-config** 命令，可以查看是否兼容支持 RFC2661 标准 AVP Hidden 解析算法

【提示信息】

【常见错误】

【平台说明】 -

8.18 l2tp tunnel force_ipsec

配置本命令表示和 IPSEC 一起使用，在外加密情况下使用，表示报文必须加密才能通过 VPDN 隧道。
l2tp tunnel force_ipsec

恢复系统缺省设置
no l2tp tunnel force_ipsec

【参数说明】

参数	描述
-	-

【缺省配置】 缺省情况下，系统不启用强制报文加密。

【命令模式】 VPDN-Group 接口配置模式

【缺省级别】 14

【使用指导】 用户可以根据需要启用或者禁用强制加密功能。任何对通道验证功能设置的有效改动都会导致相关的 L2TP 隧道被强制主动拆除

【配置举例】 1：系统启动强制加密功能。

```
Ruijie(config-vpdn)# l2tp tunnel force_ipsec
Ruijie(config-vpdn)#
```

【检验方法】 使用 **show running-config** 命令，可以查看是否报文必须加密才能通过 VPDN 隧道

【提示信息】

【常见错误】

【平台说明】 -

8.19 l2tp tunnel hello

实现通道 Keepalive 的 Hello 消息发送间隔。
l2tp tunnel hello *interval*

恢复系统缺省设置
no l2tp tunnel hello

【参数说明】

参数	描述
interval	Hello 消息发送间隔，以秒为单位

【缺省配置】 缺省情况下，系统设定 Hello 消息发送间隔为 60 秒。

【命令模式】 VPDN-Group 接口配置模式

【缺省级别】 14

【使用指导】 用户可以按照需要以及网络环境来设置 Hello 消息发送间隔。任何对通道 Hello 消息发送间隔设置的有效改变都会导致对应的 L2TP 隧道被强制主动清除

【配置举例】 1：设置 Hello 消息的发送间隔为 30 秒。

```
Ruijie(config-vpdn)# l2tp tunnel hello 30
Ruijie(config-vpdn)#
```

【检验方法】 使用 **show running-config** 命令，可以查看通道 Keepalive 的 Hello 消息发送间隔

【提示信息】

【常见错误】

【平台说明】 -

8.20 l2tp tunnel password

用于通道验证的口令。
l2tp tunnel password *password-string*

清除通道验证口令的设置
no l2tp tunnel password

【参数说明】

参数	描述
password-string	通道验证口令

【缺省配置】 缺省情况下，系统没有设置通道验证口令。

【命令模式】 VPDN-Group 接口配置模式

【缺省级别】 14

【使用指导】 如果用户要进行通道验证，那么隧道两端都必须启用通道验证功能并使用相同的验证口令。任何对通道验证口令的设置的有效改变都会导致对应的 L2TP 隧道被强制主动拆除

【配置举例】 1：设置通道验证口令为”share”。

```
Ruijie(config-vpdn)# l2tp tunnel password share
Ruijie(config-vpdn)#
```

【检验方法】 使用 **show running-config** 命令，可以查看通道验证的口令

【提示信息】

【常见错误】

【平台说明】 -

8.21 l2tp tunnel receive-window

设置通道控制消息接受窗口尺寸。
l2tp tunnel receive-window *size*

恢复系统缺省设置
no l2tp tunnel receive-window

【参数说明】

参数	描述
size	通道控制消息接受窗口尺寸

【缺省配置】 缺省情况下，通道控制消息接受窗口尺寸为 4。

【命令模式】 VPDN-Group 接口配置模式

【缺省级别】 14

【使用指导】 任何对通道控制消息接受窗口尺寸大小设置的有效改变都会导致对应的 L2TP 隧道被强制拆除

【配置举例】 1：设置控制消息接受窗口尺寸大小为 12。

```
Ruijie(config-vpdn)# l2tp tunnel receive-window 12
Ruijie(config-vpdn)#
```

【检验方法】 使用 **show running-config** 命令，可以查看通道控制消息接受窗口尺寸

【提示信息】

【常见错误】

【平台说明】 -

8.22 l2tp tunnel retransmit

设置 L2TP 通道控制消息重传参数。

l2tp tunnel retransmit { retries *number* **| timeout { min | max }** *seconds* **}**

恢复系统缺省设置

no l2tp tunnel retransmit { **retries** | **timeout** { **min** | **max** } }

【参数说明】

参数	描述
number	控制消息重传次数
seconds	控制消息重传间隔

【缺省配置】 缺省情况下，控制消息最大重传次数为 5，控制消息重传最小间隔为 1 秒，最大间隔为 8 秒。

【命令模式】 VPDN-Group 接口配置模式

【缺省级别】 14

【使用指导】 任何对通道控制消息重传参数设定的有效修改都会导致对应的 L2TP 隧道被强制主动拆除

【配置举例】 1：设置控制消息最大重传次数为 10。

```
Ruijie(config-vpdn)# l2tp tunnel retransmit retries 10
Ruijie(config-vpdn)#
```

【检验方法】 使用 **show running-config** 命令，可以查看 L2TP 通道控制消息重传参数

【提示信息】

【常见错误】

【平台说明】 -

8.23 l2tp tunnel timeout

设置 L2TP 允许的最大的无会话/控制连接时间间隔。

l2tp tunnel timeout { no-session | setup } *seconds*

恢复系统缺省设置

no l2tp tunnel timeout { **no-session** | **setup** }

【参数说明】

参数	描述
no-session	通道已经建立但是会话未建立的状态
setup	控制连接(通道)未建立的状态
seconds	时间间隔，单位为秒

【缺省配置】 缺省情况下，系统允许的最大无会话的时间间隔为 600 秒，系统允许的最大的控制连接(通道)建立的时间花费为 300 秒。

【命令模式】 VPDN-Group 接口配置模式

【缺省级别】 14

【使用指导】 任何对已有的通道允许的无会话/控制连接建立最大时间间隔的设定的有效改变都会导致相关的 L2TP 隧道被强制主动拆除

【配置举例】 1：设置通道允许的无会话时间间隔为 1200 秒。

```
Ruijie(config-vpdn)# l2tp tunnel timeout no-session 1200
Ruijie(config-vpdn)#
```

【检验方法】 使用 **show running-config** 命令，可以查看 L2TP 允许的最大的无会话/控制连接时间间隔

【提示信息】

【常见错误】

【平台说明】 -

8.24 l2tp-class

设置指定名称的 l2tp-class 接口，如果不存在对应名称的接口就创建以指定名称为名称的 l2tp-class 接口。
l2tp-class *l2tp-class-name*

删除指定名称的 l2tp-class 接口
no l2tp-class *l2tp-class-name*

【参数说明】

参数	描述
l2tp-class-name	L2TP-Class 接口的名称

【缺省配置】 缺省情况下，系统没有设置任何 L2TP-Class 接口。

【命令模式】 全局配置模式

【缺省级别】 14

【使用指导】 用户可以通过配置并引用 L2TP-Class 来实现对 L2TP 控制连接工作参数的设定

【配置举例】 1：系统创建名称为"l2x"的 L2TP-Class 接口。

```
Ruijie(config)# l2tp-class l2x
Ruijie(config-l2tp-class)#
```

【检验方法】 使用 **show running-config** 命令，可以查看指定名称的 l2tp-class 接口

【提示信息】

【常见错误】

【平台说明】 -

8.25 lcp renegotiation always

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。
lcp renegotiation always

恢复系统缺省设置
no lcp renegotiation always

【参数说明】

参数	描述
-	-

【缺省配置】 缺省情况下，接收 L2TP 控制报文必须严格符合规范。

【命令模式】 VPDN-Group 接口配置模式

【缺省级别】 14

【使用指导】 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

【配置举例】 1：设置隧道重新认证 PPP LCP。

```
Ruijie(config-vpdn)# lcp renegotiation always
Ruijie(config-vpdn)#
```

【检验方法】 使用 **show running-config** 命令，可以查看是否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

【提示信息】 -

【常见错误】 -

【平台说明】 -

8.26 local name

设置隧道本地端的主机名称。
local name *local-hostname-string*

恢复系统缺省设置
no local name

【参数说明】

参数	描述
local-hostname-*string*	隧道本地端主机名称

【缺省配置】 缺省情况下，系统使用路由器的名称作为隧道本地端主机名称的字符串。

【命令模式】 VPDN-Group 接口配置模式

【缺省级别】 14

【使用指导】 用户可以在路由器上设置隧道本地端主机名称以便标识隧道。本命令的有效设置或者改变会立即导致已经存在地相关隧道被主动强制拆除

【配置举例】 1：设置隧道本地端主机名称为"LNS"。

```
Ruijie(config-vpdn)# local name LNS
Ruijie(config-vpdn)#
```

【检验方法】 使用 **show running-config** 命令，可以查看隧道本地端的主机名称

【提示信息】

【常见错误】

【平台说明】 -

8.27 password (L2TP)

设置用于通道验证的口令。
password *password-string*

恢复系统缺省设置
no password

【参数说明】

参数	描述
password-string	用于通道验证的口令

【缺省配置】 缺省情况下，系统禁用通道验证功能自然也没有设置用于通道验证的口令。

【命令模式】 L2TP-Class 接口配置模式

【缺省级别】 14

【使用指导】 如果用户要进行通道验证，那么隧道两端都必须启用通道验证功能并使用相同的验证口令。任何对通道验证口令的设置的有效改变都会导致对应的 L2TP 隧道被强制主动拆除

【配置举例】 1：设置通道验证口令为”share”。

```
Ruijie(config-l2tp-class)# password share
Ruijie(config-l2tp-class)#
```

【检验方法】 使用 **show running-config** 命令，可以查看通道验证的口令

【提示信息】

【常见错误】

【平台说明】 -

8.28 pptp flow-control receive-window

定义 pptp 会话的对端在收到本端的报文 ack 之前允许发送的最大报文数。
pptp flow-control receive-window *packets*

恢复系统缺省设置
no pptp flow-control receive-window

【参数说明】

参数	描述
packets	pptp 会话的对端在收到本端的报文 ack 之前允许发送的最大报文数。取值范围是 1---64

【缺省配置】 PNS 的缺省值为 64，PAC 的缺省值为 16。

【命令模式】 vpdn-group 配置模式

【缺省级别】 14

【使用指导】 这是 PPTP 协议专用的配置命令，所以用户必须先配置 **protocol pptp** 或者 **protocol any** 命令后，系统才允许显示和配置这条命令。

根据 PPTP 协议 RFC2637 的建议，会话双方将协商过程中收到的对方的最大接收窗口的一半作为本端的初始发送窗口。当发送窗口满时，系统将停止该会话向对端发送报文并将发送窗口减半直到为 1，并在收到对端对已发送报文的 ACK 后恢复报文发送。当连续向对方发送当前窗口大小个数个报文都没有出现 ACK 超时的情况时，则将本端的发送窗口大小加 1，直到等于对端的最大接收窗口值。等待 ACK 超时的时间间隔，根据 RFC2637 的建议，使用专门的算法进行计算。必须先配置 protocol pptp 或者 protocol any 该命令才会显示出来。

【配置举例】 1：配置本端 pptp 会话的最大接收窗口值为 32。

```
Ruijie(config-vpdn)# accept-dialin
Ruijie(config-vpdn-acc-in)# protocol pptp
Ruijie(config-vpdn-acc-in)# exit
Ruijie(config-vpdn)# pptp flow-control receive-window 32
Ruijie(config-vpdn)#
```

【检验方法】 使用 **show running-config** 命令，可以查看允许发送的最大报文数

【提示信息】

【常见错误】

【平台说明】 -

8.29 pptp flow-control static-rtt

定义 pptp 会话在发送单个数据报文后等待该报文 ACK 应答的静态参考超时时间。

pptp flow-control static-rtt *timeout-interval*

恢复系统缺省设置

no pptp flow-control static-rtt

【参数说明】

参数	描述
timeout-interval	pptp 会话在发送单个数据报文后等待该报文 ACK 应答的静态参考超时时间，以毫秒为单位。取值范围是 100---5000

【缺省配置】 缺省值为 1500 毫秒。

【命令模式】 vpdn-group 配置模式

【缺省级别】 14

【使用指导】 这是 PPTP 协议专用的配置命令，所以用户必须先配置 **protocol pptp** 或者 **protocol any** 命令后，系统才允许显示和配置这条命令。

根据 PPTP 协议 RFC2637 的建议，PPTP 发送数据报文后等待 ACK 超时的时间间隔(ATO，Acknowledgment Time-Outs)，使用专门的算法进行计算，其中使用了动态计算的 RTT (Round-Trip Time) 时间。本命令配置的 static-rtt 时间作为 RTT 计算的参考初值

【配置举例】 1：配置本端 pptp 会话的最大接收窗口值为 32。

```
Ruijie(config-vpdn)# accept-dialin
Ruijie(config-vpdn-acc-in)# protocol pptp
Ruijie(config-vpdn-acc-in)# exit
Ruijie(config-vpdn)# pptp flow-control static-rtt 32
Ruijie(config-vpdn)#
```

【检验方法】 使用 **show running-config** 命令，可以查看 pptp 会话在发送单个数据报文后等待该报文 ACK 应答的静态参考超时时间

【提示信息】

【常见错误】

【平台说明】 -

8.30 pptp tunnel echo

配置 pptp 隧道主动发送 echo request 的间隔时间。

pptp tunnel echo *echo-packet-interval*

恢复系统缺省设置

no pptp tunnel echo

【参数说明】

参数	描述
echo-packet-interval	pptp 隧道 echo request 报文发送间隔时间，以秒为单位。取值范围是 0---1000

【缺省配置】 缺省间隔时间为 60 秒。

【命令模式】 vpdn-group 配置模式

【缺省级别】 14

【使用指导】 这是 PPTP 协议专用的配置命令，所以用户必须先配置 **protocol pptp** 或者 **protocol any** 命令后，系统才允许显示和配置这条命令。当配置 *echo-packet-interval* 为 0 时，将不主动发送 echo 报文。

当 *echo-packet-interval* 不为 0 时，PPTP 隧道在连续 *echo-packet-interval* 秒的时间里没有收到对端的任何合法协议或者数据报文，则主动发送一个 echo request 以探测隧道的状态，并开始计时等待对端的 **echo reply** 应答。等待应答的时间初始为 1 秒，若第一次应答超时，则立即发送第二个 **echo request**，并将等待应答的时间在前一次的基础上延长一倍，如此类推。若连续 5 次不能收到对端的 **echo reply** 则认为隧道通讯异常，此隧道及其包含的会话将被关闭。必须先配置 protocol pptp 或者 protocol any 该命令才会显示出来。

【配置举例】 1：配置 pptp echo request 为 30 秒。

```
Ruijie(config-vpdn)# accept-dialin
Ruijie(config-vpdn-acc-in)# protocol pptp
Ruijie(config-vpdn-acc-in)# exit
Ruijie(config-vpdn)# pptp tunnel echo 30
Ruijie(config-vpdn)#
```

【检验方法】 使用 **show running-config** 命令，可以查看 pptp 隧道主动发送 echo request 的间隔时间

【提示信息】

【常见错误】

【平台说明】 -

8.31 protocol

设置隧道使用隧道协议。

protocol { **any** | **l2tp** | **pptp** }

恢复系统缺省设置

no protocol

【参数说明】

参数	描述
any	匹配可用的所有隧道协议
l2tp	匹配隧道协议 L2TP
pptp	匹配隧道协议 PPTP

【缺省配置】 缺省情况下，系统没有为隧道指定配置的隧道协议。

【命令模式】 VPDN-Group 隧道工作模式接口配置模式

【缺省级别】 14

【使用指导】 用户必须指定隧道所使用的隧道协议，任何对隧道协议的有效设置或者更改都会导致所有已经存在的相关隧道被主动拆除，必须先配置 accept-dialin 命令，该命令才会显示出来。

【配置举例】 1：设置隧道协议为 L2TP。

```
Ruijie(config-vpdn)# accept-dialin
Ruijie(config-vpdn-acc-in)# protocol l2tp
Ruijie(config-vpdn-acc-in)#
```

【检验方法】 使用 **show running-config** 命令，可以查看隧道使用隧道协议

【提示信息】

【常见错误】

【平台说明】 -

8.32 protocol (L2TP)

设置 L2TP 控制连接参数。

protocol *l2tpv2* [*l2tp-class-name*]

恢复系统缺省设置

no protocol

【参数说明】

参数	描述
l2tpv2	使用 L2TP 作为隧道协议
l2tp-class-name	引用的 L2TP-Class 接口名称

【缺省配置】 缺省情况下，系统默认使用 L2TPv2 作为 L2TP 隧道协议。

【命令模式】 Pseudowire-Class 接口配置模式

【缺省级别】 14

【使用指导】 任何对控制连接参数设定的有效改变都会导致对应的 L2TP 隧道被强制主动拆除

【配置举例】 1：设置隧道协议为 l2tpv2 并应用 L2TP-Class l2x 来设定控制连接参数。

```
Ruijie(config-pw-class)# protocol l2tpv2 l2x
Ruijie(config-pw-class)#
```

【检验方法】 使用 **show running-config** 命令，可以查看 L2TP 控制连接参数

【提示信息】

【常见错误】

【平台说明】 -

8.33 pseudowire

设置 pseudowire 规则。
Pseudowire *peer-ip-address vcid* { **encapsulation l2tpv2** [**pw-class** *pw-class-name*] | **pw-class** *pw-class-name* }

恢复系统缺省设置
no pseudowire

用 hostname 参数配置 pseudowire
pseudowire hostname *peer-hostname vcid* { **encapsulation** *l2tpv2* [**pw-class** *pw-class-name*] | **pw-class** *pw-class-name* }

恢复系统缺省设置
no pseudowire

【参数说明】

参数	描述

peer-ip-address	远程 L2TP Server(LNS)地址
peer-hostname	远程 L2TP Server(LNS)在 DNS 上注册的和其地址相对应的 hostname
vcid	pseudowire 全局标记量
l2tpv2	使用 l2tpv2(RFC 2661)作为隧道协议
pw-class-name	引用的 pseudowire-class 单元的名称

【缺省配置】 缺省情况下，系统没有设置任何 pseudowire 规则。

【命令模式】 接口配置模式

【缺省级别】 14

【使用指导】 pseudowire 规则只能在 virtual-ppp 接口上配置。任何对 virtual-ppp 接口上的 pseudowire 规则的有效改变都会导致对应的 L2TP 会话被强制主动拆除

【配置举例】 1：在 virtual-ppp 接口上设置 pseudowire 规则，其中设置 LNS 地址为 192.168.12.213 并引用 pseudowire-class 接口"pw"

```
Ruijie(config)# interface virtual-ppp 1
Ruijie(config-if)# pseudowire 192.168.12.213 33 pw-class pw
Ruijie(config-if)#
```

2：hostname 配置示例

打开 DNS 服务，配置 DNS 服务器地址，配置到服务器的路由

```
ip domain-lookup
l2tp-class 1
pseudowire-class 1
 encapsulation l2tpv2
ip name-server 192.168.5.119
ip name-server 61.154.22.41
interface FastEthernet 0/0
 ip ref
 ip address 192.168.52.90 255.255.255.0
 duplex auto
 speed auto
interface Virtual-ppp 1
 pseudowire hostname mm.hxs.meibu.com 1 encapsulation l2tpv2
 ppp pap sent-username user1 password  11
 ip address negotiate
ip route 0.0.0.0 0.0.0.0 192.168.52.1
```

【检验方法】 使用 **show running-config** 命令，可以查看 pseudowire 规则

【提示信息】

【常见错误】

【平台说明】 -

8.34 pseudowire-class

设置指定名称的 pseudowire-class 接口，如果不存在指定名称的 pseudowire- class 接口就创建以指定名称为名称的 pseudowire-class 接口。
pseudowire-class *pseudowire-class-name*

删除指定名称的 pseudowire-class 接口
no pseudowire-class *pseudowire-class-name*

【参数说明】

参数	描述
pseudowire-class-name	pseudowire-class 接口名称

【缺省配置】 缺省情况下，系统上没有设置任何 pseudowire-class 接口。

【命令模式】 全局配置模式

【缺省级别】 14

【使用指导】 用户可以通过配置并引用 pseudowire-class 接口来设置 L2TP 隧道工作参数

【配置举例】 1：创建名称为”pw”的 pseudowire-class 接口。

```
Ruijie(config)# pseudowire-class pw
Ruijie(config-pw-class)#
```

【检验方法】 使用 **show running-config** 命令，可以查看指定名称的 pseudowire-class 接口

【提示信息】

【常见错误】

【平台说明】 -

8.35 receive-window

设置隧道控制消息接受窗口尺寸。
receive-window *size*

恢复系统缺省设置
no receive-window

【参数说明】

参数	描述
size	控制消息接受窗口尺寸

【缺省配置】 缺省情况下，控制消息接受窗口尺寸为 8。

【命令模式】 L2TP-Class 接口配置模式

【缺省级别】 14

【使用指导】 任何对隧道控制消息接受窗口尺寸的有效改变都会导致对应的 L2TP 隧道被强制主动拆除

【配置举例】 1：设置控制消息接受窗口尺寸为 12。

```
Ruijie(config-l2tp-class)# receive-window 12
Ruijie(config-l2tp-class)#
```

【检验方法】 使用 **show running-config** 命令，可以查看隧道控制消息接受窗口尺寸

【提示信息】

【常见错误】

【平台说明】 -

8.36 retransmit

设置控制消息重传参数。
retransmit {**initial** {**retries** *initial-retries* | **timeout** {**max** | **min**} *initial-timeout*} | **retries** *retries* | **timeout** {**max** | **min**} *timeout*}

恢复系统缺省设置
no retransmit { **initial** {**retries** | **timeout** {**max** | **min**} }| **retries** | **timeout** {**max** | **min**} }

【参数说明】

参数	描述
initial-retries	SCCRQ 重传次数，取值范围是 1-1000
initial-timeout	SCCRQ 重传时间间隔，取值范围是 1-8
retries	其他控制消息重传次数，取值范围是 5-1000
timeout	其他控制消息重传时间间隔，取值范围是 1-8

【缺省配置】 缺省情况下，SCCRQ 重传次数为 2，其他控制消息重传次数为 5，控制消息重传的最小时间间隔为 1 秒，控制消息重传的最大时间间隔为 8 秒。

【命令模式】 L2TP-Class 接口配置模式

【缺省级别】 14

【使用指导】 任何对控制消息重传参数设定的有效改变都会导致对应的 L2TP 隧道被强制主动拆除

【配置举例】 1：设置 SCCRQ 重传次数为 3。

```
Ruijie(config-l2tp-class)# retransmit initial retries 3
Ruijie(config-l2tp-class)#
```

【检验方法】 使用 **show running-config** 命令，可以查看控制消息重传参数

【提示信息】

【常见错误】

【平台说明】 -

8.37 show l2tp-class

显示当前系统上指定的 l2tp-class 接口的配置信息

show l2tp-class [*l2tp-class-name*]

【参数说明】

参数	描述
l2tp-class-name	指定 l2tp-class 的名称

【缺省配置】 -

【命令模式】 普通用户模式、特权用户模式

【缺省级别】 14

【使用指导】 用户可以使本命令来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。

【配置举例】 1：显示当前系统上所有的 l2tp-class 接口的详细配置信息。

```
Ruijie# show l2tp-class
L2TP Class class-default:
  hidden disable, authentication disable
  hello interval 60 second(s)
  hostname Router, password Router
  timeout setup 120 seconds
  receive-window 8, no cookie space
  retransmit retries 5, retransmit initial retries 2
  retransmit timeout max 8 second(s), retransmit timeout min 1 second(s)
  retransmit initial timeout max 8 second(s)
  retransmit initial timeout min 1 second(s)

L2TP Class l2x:
  hidden disable, authentication disable
  hello interval 60 second(s)
  hostname Router, password Router
  timeout setup 120 seconds
  receive-window 8, no cookie space
  retransmit retries 5, retransmit initial retries 2
  retransmit timeout max 8 second(s), retransmit timeout min 1 second(s)
  retransmit initial timeout max 8 second(s)
  retransmit initial timeout min 1 second(s)
Ruijie#
```

2：显示指定的名称的 l2tp-class 接口的详细配置信息

```
Ruijie# show l2tp-class l2x
L2TP Class l2x:
  hidden disable, authentication disable
  hello interval 60 second(s)
  hostname Router, password Router
  timeout setup 120 seconds
  receive-window 8, no cookie space
  retransmit retries 5, retransmit initial retries 2
  retransmit timeout max 8 second(s), retransmit timeout min 1 second(s)
  retransmit initial timeout max 8 second(s)
  retransmit initial timeout min 1 second(s)
  reference count: 1
```

字段解释：

字段	说明
hidden	avp 是否隐藏，disable 不隐藏
authentication	是否支持隧道认证，disable 不支持隧道认证
hello interval	发送 hello 报文的间隔时间
timeout setup	设置系统允许的建立控制连接最大时间
receive-window	隧道控制消息接受窗口尺寸
retransmit retries	其他控制消息(除 SCCRQ)重传次数
retransmit initial retries	SCCRQ 报文重传次数
retransmit timeout max	其他控制消息(除 SCCRQ)重传时间间隔的最大值
retransmit timeout min	其他控制消息(除 SCCRQ)重传时间间隔的最小值
retransmit initial timeout max	SCCRQ 报文重传时间间隔的最大值
retransmit initial timeout min	SCCRQ 报文重传时间间隔的最小值
reference count	关联该 l2tp-class 接口的 pseudowire-class 接口个数

【提示信息】 -

【平台说明】 -

8.38 show pseudowire-class

显示当前系统上指定的 pseudowire-class 接口的配置信息

show pseudowire-class [*pseudowire-class-name*]

【参数说明】

参数	描述
l2tp-class-name	指定 pseudowire-class 接口名称

【缺省配置】 -

【命令模式】 普通用户模式、特权用户模式

【缺省级别】 14

【使用指导】 用户可以使本命令来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。

【配置举例】 1：显示当前系统上所有的 pseudowire-class 接口详细配置信息。

```
Ruijie# show pseudowire-class
```

```
Pseudowire Class pw:
  encapsulation l2tpv2, protocol l2tpv2 on l2tp-class l2x
  ip dfbit set disable, ip pmtu disable, ip ttl 255
  ip tos reflect disable, ip tos value 0
  reference count: 1000

Pseudowire Class pw1:
  encapsulation l2tpv2
  ip dfbit set disable, ip pmtu disable, ip ttl 255
  ip tos reflect disable, ip tos value 0
  reference count: 0

Pseudowire Class pw2:
  encapsulation l2tpv2, protocol l2tpv2 on l2tp-class l2x
  ip dfbit set disable, ip pmtu disable, ip ttl 255
  ip tos reflect disable, ip tos value 0
  reference count: 0
Ruijie#
```

2：显示指定的名称的 pseudowire-class 接口的详细配置信息

```
Ruijie# show pseudowire-class pw

Pseudowire Class pw:
  encapsulation l2tpv2, protocol l2tpv2 on l2tp-class l2x
  ip dfbit set disable, ip pmtu disable, ip ttl 255
  ip tos reflect disable, ip tos value 0
  reference count: 1000
Ruijie#
```

字段解释：

字段	说明
encapsulation	封装的协议
protocol	使用的协议
l2tp-class	关联的 l2tp-class 接口
ip dfbit	隧道数据是否允许分片
ip ttl	负载隧道数据的 IP 头的 TTL 域
ip tos	负载隧道的 IP 头 TOS(Type of Service)域
reference count	关联该 pseudowire-class 接口的 virtual-ppp 接口个数

【提示信息】 -

【平台说明】 -

8.39 show vpdn

显示当前系统上指定的 VPDN 隧道信息。

show vpdn [**session | tunnel** [{ **l2tp** | **pptp** } *locid*]]

【参数说明】

参数	描述
session	显示所有会话。
tunnel	显示所有通道
l2tp *locid*	显示指定 id 的 L2TP 隧道的明细信息。取值范围是 1-65535
pptp *locid*	显示指定 id 的 PPTP 隧道的明细信息。取值范围是 0-65535

【缺省配置】 -

【命令模式】 普通用户模式、特权用户模式

【缺省级别】 14

【使用指导】 用户可以使本命令来实时考察当前系统上的 VPDN 隧道信息。如果不指定参数将显示当前系统上所有的 VPDN 通道与会话。

注意：由于用户名的长度是任意的，为了格式对齐，因此 show 的时候规定，仅显示前 12 字节的用户名长度，超过此长度的是不会显示完整的。

如果要显示用户名全名，可以使用 show vpdn tunnel l2tp locid 、show vpdn tunnel pptp locid 来查看

【配置举例】 1：考察当前系统上所有的 VPDN 隧道信息。

```
Ruijie# show vpdn
L2TP Tunnel and Session Information Total tunnels 1 sessions 1
LocID RemID Remote Name   State  Remote Address  Port  Sessions L2TP Class/
VPDN Group
4     77    BLIZZARD      est    192.168.12.213  1701  1        1
LocID      RemID      TunID      Username, Intf/      State  Last Chg
                                 Vcid, Circuit
1          1          4          ms,Vi1               est    00:33:58
%No active PPTP tunnels
Ruijie#
```

显示当前系统上所有 VPDN 通道的信息

```
Ruijie# show vpdn tunnel
L2TP Tunnel Information Total tunnels 1
LocID RemID Remote Name   State  Remote Address  Port  Sessions L2TP Class/
VPDN Group
```

```
4     77    BLIZZARD      est    192.168.12.213  1701  1        1
%No active PPTP tunnels
Ruijie#
```

显示当前系统上所有 VPDN 会话的信息

```
Ruijie# show vpdn session
L2TP Session Information Total sessions 1
LocID      RemID      TunID      Username, Intf/      State  Last Chg
                                 Vcid, Circuit
1          1          4          ms,Vi1               est    00:37:03
%No active PPTP tunnels
Ruijie#
```

2：显示指定的 PPTP 或 L2TP 隧道明细信息

显示指定隧道 id 为指定值的 L2TP 隧道明细信息：

```
Ruijie# show vpdn tunnel l2tp 4
L2TP tunnel locid 4 is up,remote id is 77, 1 active sessions
  Tunnel state is est
  Tunnel transport is UDP
  Remote tunnel name is BLIZZARD
    Internet Address 192.168.12.213, port 1701
  Local tunnel name is LNStest
    Internet Address 192.168.12.212, port 1701
  VPDN group for tunnel is 1
  Tunnel domain unknown
  ip mtu adjust disabled
  Control Ns 2, Nr 4
```

显示指定隧道 id 为指定值的 PPTP 隧道明细信息：

```
Ruijie#show vpdn tunnel
%No active L2TP tunnels
PPTP Tunnel Information Total tunnels 1
LocID Remote Name     State       Remote Address  Port  Sessions
2                    estbed       192.168.45.160  3077  1
Ruijie#
Ruijie#show vpdn tunnel pptp 2
PPTP tunnel id 2 is up, remote id is 0, 1 active session
  Tunnel state is estbed
  Remote tunnel name is
    Internet Address 192.168.45.160, port 3077
  Local tunnel name is
    Internet Address 192.168.45.161
```

字段解释：

字段	说明

L2TP Tunnel	L2TP 通道
Session Information	会话信息
LocID	本地 ID
RemID	远端 ID
TunID	通道 ID
Username, Intf:	用户名和接口
State	状态
Last Chg	最后改变时间
Remote Address	对端地址
Port	端口

【提示信息】 -

【平台说明】 -

8.40 show vpdn log

显示当前日志文件中保存的用户上下线信息

show vpdn log [user *username***]**

【参数说明】

参数	描述
username	指定的用户名

【缺省配置】 -

【命令模式】 普通用户模式、特权用户模式

【缺省级别】 14

【使用指导】 用户可以使本命令来查看当前日志文件中所有的或指定用户的上下线信息

【配置举例】 1：显示当前日志文件中所有的用户上下线信息

```
Ruijie# show vpdn log
Username                        IP          State  Online time          Offline time
user-1                          100.1.1.2   out    2014-11-16-14:09:04  2014-11-16-14:29:26
user-2                          100.1.2.2   out    2014-11-16-15:09:05  2014-11-16-16:09:27
user-3                          100.1.3.2   out    2014-11-16-17:09:04  2014-11-16-18:09:26
user-4                          100.1.4.2   in     2014-11-16-18:09:05
Ruijie#
```

2：显示当前日志文件中指定用户的上下线信息

```
Ruijie# show vpdn log user user-1
Username                        IP          State  Online time         Offline time
user-1                          100.1.1.2   out    2014-11-16-14:09:04  2014-11-16-14:29:26
Ruijie#
Ruijie#show vpdn log user ruijie
%No vpdn logs for username: ruijie.
Ruijie#
```

字段解释：

字段	说明
Username	用户名
IP	对端 IP
State	当前状态
Online time	上线时间
Offline time	下线时间

【提示信息】 -

【平台说明】 -

8.41 source-ip

设置当前 VPDN-Group 对应隧道使用本地(源)地址。

source-ip *A.B.C.D*

恢复系统缺省设置

no source-ip

【参数说明】

参数	描述
A.B.C.D	当前 VPDN-Group 对应隧道使用的本地(源)地址

【缺省配置】 缺省情况下，系统没有限制 VPDN-Group 建立隧道时使用的本地(源)地址。

【命令模式】 VPDN-Group 接口配置模式

【缺省级别】 14

【使用指导】 如果已经设置了全局的 VPDN 功能使用的本地(源)地址，那么 VPDN-Group 建立隧道时使用的本地(源)地址必须与之一致。本命令的有效设置或者改变会立即导致已经存在的相关隧道被主动强制拆除

【配置举例】 1：设置当前 VPDN-Group 使用的源地址为 202.101.92.73。

```
Ruijie(config-vpdn)# source-ip 202.101.92.73
```

```
Ruijie(config-vpdn)#
```

【检验方法】 使用 **show running-config** 命令，可以查看当前 VPDN-Group 对应隧道使用本地(源)地址

【提示信息】

【常见错误】

【平台说明】 -

8.42 terminate-from

指定隧道对端的主机名称。
terminate-from hostname *remote-hostname-string*

恢复系统默认设置
no terminate-from

【参数说明】

参数	描述
remote-hostname-string	隧道对端主机名称

【缺省配置】 缺省情况下，系统没有设置隧道对端主机名称。

【命令模式】 VPDN-Group 接口配置模式

【缺省级别】 14

【使用指导】 用户可以使用本命令来限制远程接入的用户主机名称，如果没有设置隧道对端主机名称，那么该 VPDN-Group 将不限制远程接入的用户主机名称。任何对隧道远程主机名称的有效更改都会导致所在 VPDN-Group 对应的已经存在的所有隧道被强制主动拆除

【配置举例】 1：设置隧道对端主机名称为"LAC"。

```
Ruijie(config-vpdn)# terminate-from hostname LAC
Ruijie(config-vpdn)#
```

【检验方法】 使用 **show running-config** 命令，可以查看隧道对端的主机名称

【提示信息】

【常见错误】

【平台说明】 -

8.43 timeout setup

设置系统允许的建立控制连接最大时间花费。
timeout setup *seconds*

恢复系统缺省设置
no timeout setup

【参数说明】

参数	描述
seconds	系统允许的建立控制连接的最大时间花费，单位为秒。取值范围是 60-6000

【缺省配置】 缺省情况下，系统允许的建立控制连接的最大时间花费为 120 秒。

【命令模式】 L2TP-Class 接口配置模式

【缺省级别】 14

【使用指导】 任何对系统允许的建立控制连接的最大时间花费设定的有效修改都会导致相关的 L2TP 隧道被强制主动清除

【配置举例】 1：设置系统允许的建立控制连接的最大时间花费为 240 秒。

```
Ruijie(config-l2tp-class)# timeout setup 240
Ruijie(config-l2tp-class)#
```

【检验方法】 使用 **show running-config** 命令，可以查看系统允许的建立控制连接最大时间花费

【提示信息】

【常见错误】

【平台说明】 -

8.44 virtual-template

设置当前 VPDN-Group 绑定的虚模板接口。
virtual-template *number*

恢复系统缺省设置

no virtual-template

【参数说明】

参数	描述
number	虚模板接口序号，取值范围是 1-1200

【缺省配置】 缺省情况下，系统没有绑定任何虚模板接口到 VPDN-Group 上。

【命令模式】 VPDN-Group 隧道工作模式接口配置模式

【缺省级别】 14

【使用指导】 用户可以使用本命令来绑定 VPDN-Group 使用的虚模板接口从而决定负载会话的网络接口参数。如果希望 VPDN-Group 提供就必须绑定虚模板接口。任何对 VPDN- Group 绑定的虚模板接口的有效更改都将导致该 VPDN-Group 对应的已经存在的隧道被强制拆除。

只有配置 protocol 配置后才能配置，否则命令不可见

【配置举例】 1：绑定虚模板接口 1 到所在 VPDN-Group 上。

```
Ruijie(config)#
Ruijie(config)#vpdn-group 1
Ruijie(config-vpdn)#accept-dialin
Ruijie(config-vpdn-acc-in)#protocol any
Ruijie(config-vpdn-acc-in)#virtual-template 1
Ruijie(config-vpdn-acc-in)#
```

【检验方法】 使用 **show running-config** 命令，可以查看当前 VPDN-Group 绑定的虚模板接口

【提示信息】

【常见错误】

【平台说明】

8.45 vpdn congestion_avoidanc

启用 VPDN 拥塞控制。

vpdn congestion_avoidanc

禁用 VPDNVPDN 拥塞控制。

no vpdn congestion_avoidanc

【参数说明】

参数	描述
-	-

【缺省配置】 缺省情况下，系统禁用 VPDN 拥塞控制功能。

【命令模式】 全局配置模式

【缺省级别】 14

【使用指导】 用户可以根据当前网络环境来决定是否开启拥塞控制。

【配置举例】 1：系统启用 VPDN 拥塞控制功能。

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

【检验方法】 使用 **show running-config** 命令，可以查看是否启用 VPDN 功能

【提示信息】 -

【提示信息】 -

【平台说明】 -

8.46 vpdn enable

启用 VPDN 功能。
vpdn enable

禁用 VPDN 功能
no vpdn enable

【参数说明】

参数	描述
-	-

【缺省配置】 缺省情况下，系统禁用 VPDN 功能。

【命令模式】 全局配置模式

【缺省级别】 14

【使用指导】 除了客户端发起(Client-Initiated Tunnel)的 L2TP 隧道不要求系统启用 VPDN 功能外，RGOS 无论是提供 LAC 还是 LNS 功能，无论是使用 PPTP 还是使用 L2TP 协议均要求系统启用 VPDN 功能。本命令的有效设置或者改变会立即导致已经存在的相关隧道被主动强制拆除。

【配置举例】 1：系统启用 VPDN 功能。

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

【检验方法】 使用 **show running-config** 命令，可以查看是否启用 VPDN 功能

【提示信息】

【常见错误】

【平台说明】 -

8.47 vpdn ignore_source

启用 VPDN 源地忽略功能，开启该命令后对方发送过来的数据报文将不检查源地址匹配情况。
vpdn ignore_source

严格的检查对端报文的源地址
no vpdn ignore_source

【参数说明】

参数	描述
-	-

【缺省配置】 缺省情况下，系统检查隧道报文的源地址匹配情况。

【命令模式】 全局配置模式

【缺省级别】 14

【使用指导】 本命令启用 VPDN 源地忽略功能，开启该命令后对方发送过来的数据报文将不检查源地址匹配情况。仅针对快转数据有用

【配置举例】 1：系统启用 VPDN 源地址忽略功能。

```
Ruijie(config)# vpdn ignore_source
Ruijie(config)#
```

【检验方法】 使用 **show running-config** 命令，可以查看是否启用 VPDN 源地忽略功能

【提示信息】

【常见错误】

【平台说明】

8.48 vpdn limit_rate

设置当前系统提供 VPDN 每秒允许建立的隧道个数，限制 VPDN 的建立速度。
vpdn limit_rate *rate_num*

关闭 VPDN 的连接速率的限制
no vpdn limit_rate

【参数说明】

参数	描述
rate_num	5-100，系统每秒允许建立的 VPDN 隧道个数最小 5 最大 100

【缺省配置】 10.x 缺省情况下不会对 VPDN 隧道建立过程进行限速，11.x 的修订为默认对 VPDN 隧道建立过程进行限速，默认取值为每秒 15 路。

【命令模式】 全局配置模式

【缺省级别】 14

【使用指导】 当同时有太多 VPDN 拨入影响到系统整体性能时，可使用此命令对拨入数进行限制。

【配置举例】 1：设定当前接受的每秒协商隧道条数为 50。

```
Ruijie(config)# vpdn limit_rate 50
Ruijie(config)#
```

【检验方法】 使用 **show running-config** 命令，可以查看 VPDN 每秒允许建立的隧道个数

【提示信息】

【常见错误】

【平台说明】

8.49 vpdn session-limit

设置当前系统提供 VPDN 功能时所允许的最大会话数。

vpdn session-limit *sessions*

恢复系统缺省设置

no vpdn session-limit

【参数说明】

参数	描述
sessions	系统提供 VPDN 功能时允许的最大会话数，取值范围是 1-300

【缺省配置】 缺省情况下，该值被设定为本系统所能够提供的最大会话数，其中 36 系列为 300。

【命令模式】 全局配置模式

【缺省级别】 14

【使用指导】 当同时有太多 VPDN 拨入影响到系统整体性能时，可使用此命令对拨入数进行限制。必须先使能 vpdn enable 命令。

【配置举例】 1：设定当前接受的最大会话数为 100。

```
Ruijie(config)# vpdn session-limit 100
Ruijie(config)#
```

【检验方法】 使用 **show running-config** 命令，可以查看当前系统提供 VPDN 功能时所允许的最大会话数

【提示信息】

【常见错误】

【平台说明】

8.50 vpdn source-ip

设置当前系统提供 VPDN 功能时使用的本地(源)地址。

vpdn source-ip *A.B.C.D*

恢复系统缺省设置

no vpdn source-ip *A.B.C.D*

【参数说明】

参数	描述
A.B.C.D	系统提供 VPDN 功能时使用的本地地址

【缺省配置】 缺省情况下，系统没有为提供 VPDN 功能设定使用的本地(源)地址。

【命令模式】 全局配置模式

【缺省级别】 14

【使用指导】 如果系统提供 LNS(L2TP)或者 HGW(PPTP)功能，就可以使用本命令来限定当前所有接受的隧道连接请求的目的地址为设定的地址。本命令的有效设置或者改变会立即导致已经存在的相关隧道被主动强制拆除。必须先使能 vpdn enable 命令。

【配置举例】 1：设定当前接受的所有隧道连接请求的目的地址必须为 192.168.12.223。

```
Ruijie(config)# vpdn source-ip 192.168.12.223
Ruijie(config)#
```

【检验方法】 使用 **show running-config** 命令，可以查看当前系统提供 VPDN 功能时使用的本地(源)地址

【提示信息】

【常见错误】

【平台说明】

8.51 vpdn-group

设置指定名称 VPDN-Group 接口，如果不存在对应的 VPDN-Group 接口就创建一个以指定名称为名称的 VPDN-Group 接口。

vpdn-group *vpdn-group-name*

删除指定名称的 VPDN-Group 接口

no vpdn-group *vpdn-group-name*

【参数说明】

参数	描述
vpdn-group-name	vpdn-group 接口的名称

【缺省配置】 缺省情况下，系统没有设置任何 *vpdn-group* 接口。

【命令模式】 全局配置模式

【缺省级别】 14

【使用指导】 用户如果想路由器充当 LNS 或者 HGW，就必须创建并设置 VPDN-Group 接口。用户可以使用本命令管理 VPDN-Group 接口。VPDN-Group 接口的删除将直接导致对应的已经存在的隧道被主动强制拆除。必须先使能 vpdn enable 命令。

【配置举例】 1：创建名称为"1"的 vpdn-group 接口。

```
Ruijie(config)#
Ruijie(config)#vpdn enable
Ruijie(config)#vpdn-group 1
Ruijie(config-vpdn)#
```

【检验方法】 使用 **show running-config** 命令，可以查看指定名称 VPDN-Group 接口

【提示信息】

【常见错误】

【平台说明】

9 IPSEC-IKE

9.1 authentication (IKE policy)

指定 IKE 策略的认证方法。

authentication { **pre-share** }

恢复缺省配置。

no authentication

【参数说明】

参数	描述
pre-share	预共享密钥验证。

【缺省配置】 缺省是预共享密钥验证.。

【命令模式】 IKE 策略配置模式。

【缺省级别】 14

【使用指导】

目前 IKE 协商策略中验证方式默认采用预共享密钥验证.。

【配置举例】 1：配置一个优先级为 10 的 IKE 策略，采用预共享秘钥验证。

```
Ruijie(config)# crypto isakmp policy 10
Ruijie(isakmp-policy)#authentication pre-share
```

【检验方法】 -

【提示信息】 -

【平台说明】 -

9.2 clear crypto isakmp

清除正在运行的 IKE 安全联盟。

clear crypto isakmp [*connection-id*]

【参数说明】

参数	描述

connection-id	IKE 安全联盟的 ID 号。缺省为清除所有存在的 IKE 安全联盟。取值范围<0-65535>。

【命令模式】 特权模式。

【缺省级别】 14

【使用指导】 一般情况下，只清除某个具体的 IKE 安全联盟，您可以先使用 **show crypto isakmp sa** 命令查看您要清除安全联盟的 ID 号，然后再使用 **clear crypto isakmp** 带 ID 清除某个具体的 IKE 安全联盟。。

【配置举例】 1：清除所有 IKE 安全联盟。

```
Ruijie# clear crypto isakmp
```

【提示信息】 -

【平台说明】 -

9.3 clear crypto log

清除 IPSec VPN 的登录注销日志。

clear crypto log

【参数说明】

参数	描述
-	-

【命令模式】 特权模式

【缺省级别】 14

【使用指导】 -

【配置举例】 清除 IPSec VPN 的登录注销日志。

```
Ruijie # clear crypto log
```

【提示信息】 -

【常见错误】

```
Ruijie # clear crypto log
ipsec is writing or reading log now, can not delete file
```

这表示 ipsec 进程正在写入或读取 log 文件，此时无法删除 log 文件

【平台说明】 -

9.4 clear crypto sa

清除 IPSec 安全联盟。
clear crypto sa

根据 IP 或主机名清除对应远端对等体的 IPSec 安全联盟。
clear crypto sa peer { *ip-address* | *peer-name* }

根据加密映射名称清除对应远端对等体的 IPSec 安全联盟。
clear crypto sa map *map-name*

根据 IP 地址和安全参数索引清除对应远端对等体的 IPSec 安全联盟。
clear crypto sa spi *destination-address* { **ah** | **esp** } *spi*

【参数说明】

参数	描述
ip-address	远端对等体的 IP 地址。
peer-name	远端对等体的主机名。
map-name	加密映射名称
destination-address	本地或远程对等体的 IP 地址
spi	指定一个安全参数索引，取值范围<0-4294967295>

【命令模式】 特权模式

【缺省级别】 14

【使用指导】 1、上述命令用于清除 IPSec 安全联盟，如果没有使用 peer、map、spi 等关键字，则默认所有的 IPSec 安全联盟都将被删除。
2、如果安全联盟是通过 IKE 建立的，那么它们将被清除，当接口检测到有激活 IPSec 的报文，IPSec 重新协商新的安全联盟。如果安全联盟是通过手工建立的，那么安全联盟将被清除并且立即重新建立。
3、配置了新参数，只对随后协商的安全联盟起作用，不会影响现有安全联盟。为了新参数作用于现有安全联盟，可通过该命令清除现有安全联盟，进行重新协商。
4、安全联盟被清除，将导致通信中断，为了不使其他的IPSec联盟通信中断，应该使用peer、map、spi明确指定特定的安全联盟。
5、当然，如果只有一个安全联盟，或者其他安全联盟没有什么数据在通信，可以清除所有安全联盟进行重新协商。

【配置举例】 1：清除所有安全联盟。

```
Ruijie# clear crypto sa
```

【提示信息】 -

【平台说明】 -

9.5 crypto dynamic-map

创建动态加密映射条目并进入加密映射配置模式。

crypto dynamic-map *dynamic-map-name dynamic-seq-num*

删除加密映射集或条目。

no crypto dynamic-map *dynamic-map-name* [*dynamic-seq-num*]

【参数说明】

参数	描述
dynamic-map-name	指定加密映射集的名称。
dynamic-seq-num	指定加密映射的条目号。范围 1 到 65535

【缺省配置】 没有动态加密映射存在。

【命令模式】 全局模式

【缺省级别】 14

【使用指导】

【配置举例】

【检验方法】 -

【提示信息】 -

【常见错误】 -

【平台说明】 -

9.6 crypto IPSec df-bit

对全部接口设置封装头的 DF 值。

crypto IPSec df-bit { **clear** | **set** | **copy** }

【参数说明】

参数	描述
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。

【缺省配置】 命令缺省禁用。

【命令模式】 全局模式

【缺省级别】 14

【使用指导】 在隧道模式 IPSEC 下用 **clear** 设置，你能发送比 MTU 值大的包，或者你不知道 MTU 到底是多大。

如果这个命令没有用明确的设定值启用，设备将用 **copy** 作为缺省值。

【配置举例】 1：在所有接口把 DF Bit 清除。

```
Ruijie(config)# crypto IPSec df-bit clear
```

【检验方法】 -

【提示信息】 -

【常见错误】 -

【平台说明】 -

9.7 crypto IPSec multicast disable

关闭对多播、广播报文的 IPSec 处理。

crypto IPSec multicast disable

打开对多播、广播报文的 IPSec 处理。

no crypto IPSec multicast disable

【参数说明】

参数	描述
-	-

【缺省配置】 没有配置的情况下，且 ACL 包含了多播、广播报文，将对其进行 IPSec 处理。

【命令模式】 全局模式

【缺省级别】 14

【使用指导】 如果不需要对多播、组播报文进行 IPSec 处理，配置此命令可以跳过 IPSec 处理。

【配置举例】 1：完成关闭多播、广播报文 IPSec 处理的配置。

```
Ruijie(config)# crypto IPSec multicast disable
```

【检验方法】 -

【提示信息】 -

【常见错误】 -

【平台说明】 -

9.8 crypto IPSec optional

关闭 IPSec 安全检查。

crypto IPSec optional

打开 IPSec 安全检查。

no crypto IPSec optional

【参数说明】

参数	描述
-	-

【缺省配置】 缺省情况该命令关闭。

【命令模式】 全局模式

【缺省级别】 14

【使用指导】 安全检查本身对资源开销比较大，关闭该功能可以节约 cpu 资源。l2tp over IPSec 的模型中，l2tp 可以指定强制 IPSec 功能，也可以实现报文必须经过 IPSec 加密的报文才能通过。可以根据实际需要组合使用。

【配置举例】 1：取消安全检查。

```
Ruijie(config)# crypto IPSec optional
```

【检验方法】 -

【提示信息】 -

【常见错误】 -

【平台说明】 -

9.9 crypto IPSec profile (global IPSec-profile)

创建或修改一个 Profile 的加密映射。
crypto IPSec profile *profile-name*

取消一个 Profile 的加密映射或条目。
no crypto IPSec profile *profile-name*

【参数说明】

参数	描述
profile-name	Profile 加密映射集合的名称

【缺省配置】 不存在加密映射。

【命令模式】 全局模式，使用该命令将进入 Profile 加密映射配置模式。

【缺省级别】 14

【使用指导】 在 Tunnel 接口上对数据进行加密保护时，首先需要定义 Profile 的加密映射，然后应用到该 Tunnel 接口。在该 Profile 加密映射表中需要定义加密通信参数，主要包括以下参数：
1、对这些通信应该应用哪些 IPSec 安全策略：从一个或多个变换集组成的列表中选择。
2、安全联盟的生命期。
3、安全联盟是被手工建立还是通过 IKE 建立。
将 Tunnel 的加密映射集合应用到 Tunnel 接口上，这样所有通过这个接口的 IP 通信都将被应用在接口上的加密映射集合进行加密。在配置完成后，自动发起 IKE 协商，或者在收到该接口的报文，来触发 IKE 协商。在加密映射条目中描述的策略将在安全联盟的协商过程中被使用，为了使两个 IPSec 对等体之间的 IPSec 能够顺利进行，两个对等体的 Tunnel 加密映射条目必须包含互相兼容的配置语句。当两个对等体试图建立安全联盟时，双方都必须至少有一条加密映射条目和对方对等体的一条加密映射条目相兼容至少满足以下条件：
1、加密映射条目必须包含兼容的加密访问列表（如镜像映像访问列表）。
2、双方的加密映射条目都必须确定对方对等体地址（除非对等体正在使用动态加密映射）。
3、加密映射条目必须至少有一个相同的变换。
4、对于单个接口只应用一个加密映射集合。加密映射集合中包含了 IPSec/IKE.
如果存在下面几种情况中的一种，就必须为一个接口创建多个加密映射条目：
1、如果此接口上不同的数据流将由不同的 IPSec 对等体进行处理。
2、如果想要对不同类型的通信（发往相同或不同的对等体）应用不同的 IPSec 安全性；例如，想让一组子网间的通信被认证，而另一组子网间的通信既被认证又被加密。在这种情况下，不同类型的通信应该在两个不同的访问列表中被定义，并且必须为每个加密访问列表创建一个单独的加密映射条目。

【配置举例】 1：Profile 加密映射集合的最小配置，profile 名为 testprofile，变换集合名为 mytest。

```
Ruijie(config)# crypto IPSec profile testprofile
Ruijie(config-crypto-map)# set transform-set myset
```

【检验方法】 -

【提示信息】 -

【常见错误】 -

【平台说明】 -

9.10 crypto IPSec security-association lifetime

修改 IPSec 安全联盟协商时所使用的全局生命周期值。
crypto IPSec security-association lifetime { **seconds** *seconds* | **kilobytes** *kilobytes* }

将生命周期恢复成缺省值。
no crypto IPSec security-association lifetime { **seconds** | **kilobytes** }

【参数说明】

参数	描述
seconds *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。范围 0，或者 120 秒到 86400 秒
kilobytes *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。范围 0，或 2560KB 到 536870912KB

【缺省配置】 3600 秒（1 小时）和 4,608,000KB（以每秒 10MB 的速率通信 1 个小时）。

【命令模式】 全局模式

【缺省级别】 14

【使用指导】 1、Sec 安全联盟加密通信是建立在使用共享密钥的基础上。为了确保安全，安全联盟将在经过一定时间或通信量之后超时，重新协商，并使用新的共享密钥。当设备在进行安全联盟协商时，使用对等体提议的和本地设备配置的生命周期值中较小者作为新安全联盟的生命周期。
2、周期有两种：时间生命周期、通信量生命周期。这两个生命周期中无论哪个先到期，安全联盟都将超时。如果改变了全局生命周期，此改变只作用于随后协商的新的安全联盟，不会影响现存安全联盟。如果想让新的设置尽快生效，可以使用 clear crypto sa 命令清除部分或全部安全联盟数据库的内容。
3、改全局的时间生命周期，请使用命令 crypto IPSec security-association lifetime seconds。时间生命周期指定了安全联盟在经过了一定的秒数后超时。要修改全局的通信量生命周期，请使用命令的 crypto IPSec security-association lifetime kilobytes。通信量生命周期指定了安全联盟使用安全联盟密钥加密的通信量（以 KB 计）达到了一定数量以后超时。

4、周期值越短，则破解密钥的攻击越难成功，因为攻击者用来进行分析的同一密钥加密的数据越少。但是，生命周期越短，用于建立新安全联盟的 CPU 处理时间就越多。在手工建立的安全联盟是没有生命周期。

5、周期的工作原理：经过了一定的时间（由 seconds 关键字指定）或已通信了一定字节的数据通信量（由 kilobytes 关键字指定），这两件事情无论哪件先发生，安全联盟（以及相应的密钥）都将超时。新的安全联盟在原有安全联盟的生命周期极限值到达以前就开始进行协商，以确保当原有安全联盟超时的时候，已经有一个新的安全联盟可以使用了。新安全联盟在 seconds 生命周期超时前 30 秒，或经由这条隧道的数据通信量距 kilobytes 生命周期还有 256KB 时开始进行协商（根据哪个先发生）。如果在一个安全联盟的整个生命周期中都没有通信经过这条隧道，那么当此安全联盟超时的时候不会进行新安全联盟的协商。相应地，新的安全联盟只有当 IPSec 看见应该受到保护的分组时才开始进行协商。

6、 时间生命周期和通信量生命周期不能同时为零，否则不能成功协商。本地配置不检查，需要用户自己保证。

【配置举例】 1：将 IPSec 安全联盟的时间周期设为 2500 秒，通信量生命周期设为 2304000KB(以 10MB 速率通信半个小时)。

```
Ruijie(config)# crypto IPSec security-association lifetime seconds 2500
Ruijie(config)# crypto IPSec security-association lifetime kilobytes 2304000
```

【检验方法】 -

【提示信息】 -

【常见错误】 -

【平台说明】 -

9.11 crypto IPSec security-association lifetime not_based_on initiator

修改 IPsec 第二阶段生命周期的协商匹配规则，即第二阶段生命周期最终协商结果为：分支和总部生命周期两者之间的较小者。

crypto IPSec security-association lifetime not_based_on initiator

恢复第二阶段生命周期的默认匹配方式：最终的协商结果以分支为准。

no crypto IPSec security-association lifetime { **seconds** | **kilobytes** }

【参数说明】

参数	描述
-	-

【缺省配置】 第二阶段生命周期，默认使用分支的生命周期为最终的协商结果。

【命令模式】 全局模式

【缺省级别】 14

【使用指导】 在默认情况下，第二阶段生命周期的协商结果以分支为准，即总部和分支均采用分支所配置的值作为第二阶段生命周期。可以通过该指令修改第二阶段生命周期的匹配规则，即修改为：使用分支和总部所配置值的较小者作为最终的协商结果。

【配置举例】 1：修改第二阶段生命周期的匹配规则。

```
Ruijie(config)# crypto IPSec security-association lifetime not_based_on initiator
```

【检验方法】 -

【提示信息】 -

【常见错误】 -

【平台说明】 -

9.12 crypto IPSec security-association replay disable

抗重播开关命令，设为不检查重传报文模式。
crypto IPSec security-association replay disable

设为检查重传报文模式。
no crypto IPSec security-association replay disable

【参数说明】

参数	描述
-	-

【缺省配置】 缺省重播检查默认打开，缺省情况不显示。

【命令模式】 全局模式

【缺省级别】 14

【使用指导】 命令打开后不检查报文重传，可以提高报文处理效率，同时，被 dos 攻击的可能性增加。

【配置举例】 1：关闭重传报文检查。

```
Ruijie(config)# crypto IPSec security-association replay disable
```

【检验方法】 -

【提示信息】 -

【常见错误】 -

【平台说明】 -

9.13 crypto IPSec transform-set

定义供安全联盟使用的变换集合。
crypto IPSec transform-set *transform-set-name transform1 [transform2 [transform3]]*

删除一个变换集合。
no crypto IPSec transform-set *transform-set-name*

【参数说明】

参数	描述
transform-set-name	变换集的名称
transform1 、 *transform2* 、 *transform3*	安全联盟使用的安全协议和算法，具体的请参考安全配置指导。

【缺省配置】 无变换集合。

【命令模式】 全局模式

【缺省级别】 14

【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。

【配置举例】 1：定义变换集合，保护方式为 ESP-DES-MD5（提供加密和验证服务）。

```
Ruijie(config)# crypto IPSec transform-set myset esp-des esp-md5-hmac
```

【检验方法】 -

【提示信息】 -

【常见错误】 -

【平台说明】 -

9.14 crypto isakmp enable

要使用 IKE 进行 IPSec 安全联盟协商，必须先使能 IKE。
crypto isakmp enable

禁止 IKE。
no crypto isakmp enable

【参数说明】

参数	描述
-	-

【缺省配置】 IKE 缺省情况下是打开的。

【命令模式】 全局模式

【缺省级别】 14

【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。

【配置举例】 1：使能 IKE。

```
Ruijie(config)# crypto isakmp enable
```

【检验方法】 -

【提示信息】 -

【常见错误】 -

【平台说明】 -

9.15 crypto isakmp keepalive

发送对等体检测消息给远程对等体。
crypto isakmp keepalive *secs* [**on-demand | periodic**]
crypto isakmp keepalive *secs retries* [**on-demand | periodic**]

关闭对等体检测消息功能。

no crypto isakmp keepalive

【参数说明】

参数	描述
secs	隧道存活时间，范围是 5 秒到 3600 秒。
retries	重发报文的时间间隔，范围 2 秒到 60 秒。
on-demand	按转发报文空闲时间发送消息。
periodic	按配置间隔时间发送消息。

【缺省配置】 不发送对等体检测消息。

【命令模式】 全局模式

【缺省级别】 14

【使用指导】 使用 **crypto isakmp keepalive** 使设备定时发送死对等体检测消息给远程对等体，来发现是否远程对等体还存在。

【配置举例】 1：配置隧道闲置时间为 60 秒，重发时间间隔为 5 秒，**on-demand** 方式。

```
Ruijie(config)# crypto isakmp  keepalive  60 5 on-demand
```

【检验方法】 -

【提示信息】 -

【常见错误】 -

【平台说明】 -

9.16 crypto isakmp key

指定 IKE 协商使用的预共享密钥。

crypto isakmp key { **0 | 7** } *keystring* { **hostname** *peer-hostname* | **address** *peer-address* [*mask*] }

删除指定的预共享密钥。

no crypto isakmp key { **0 | 7**} *keystring* { **hostname** *peer-hostname* | **address** *peer-address* [*mask*] }

【参数说明】

参数	描述
0 | 7	0 为密钥显示明文 7 为密钥显示密文。
keystring	预共享密钥字符串，最长可以使用 128 个字符。
peer-hostname	远程对等体的主机名。

peer-address	远程对等体的 IP 地址。
mask	指定的 IP 地址为一个网段的地址时的地址掩码。

【缺省配置】 没有指定任何预共享密码。

【命令模式】 全局模式

【缺省级别】 14

【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。

【配置举例】 1：指定与对等体 172.16.1.1 进行 IKE 协商的预共享密钥为 mysecret。

```
Ruijie(config)# crypto isakmp key 0  mysecret address 172.16.1.1
```

【检验方法】 -

【提示信息】 -

【常见错误】 -

【平台说明】 -

9.17 crypto isakmp limit disable

关闭 IKE 的协商限速功能。
crypto isakmp limit disable

打开 IKE 协商限速功能。
no crypto isakmp limit disable

【参数说明】

参数	描述
-	-

【缺省配置】 默认情况下，IKE 的协商限速功能处在打开状态，协商速率为 1000。

【命令模式】 全局模式

【缺省级别】 14

【使用指导】 关闭 IKE 的协商限速功能。

【配置举例】 1：关闭 IKE 的协商限速功能。

```
Ruijie(config)# crypto isakmp limit disable
```

【检验方法】 -

【提示信息】 -

【常见错误】 -

【平台说明】 -

9.18 crypto isakmp limit rate

限制 IKE 的协商速率，即设置最多同时能有多少路隧道协商正在进行。
crypto isakmp limit rate *numbers*

取消所设置的限速速率，恢复默认值。
no crypto isakmp limit rate

【参数说明】

参数	描述
numbers	所设定限速速率

【缺省配置】 缺省情况下限速速率为 1000，即同时支持 1000 路 ipsec 隧道发起协商。

【命令模式】 全局模式

【缺省级别】 14

【使用指导】 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。

【配置举例】 1：配置 IKE 的协商速率。

```
Ruijie(config)# crypto isakmp limit rate 500
```

【检验方法】 -

【提示信息】 -

【常见错误】 -

【平台说明】 -

9.19 crypto isakmp mode-detect

本地安全网关用主模式无法完成对端发起的 IKE 协商时，自动采用积极模式进行协商。
crypto isakmp mode-detect

关闭自动积极模式。
no crypto isakmp mode-detect

【参数说明】

参数	描述
-	-

【缺省配置】 没有配置的情况下，只采用主模式进行协商。

【命令模式】 全局模式

【缺省级别】 14

【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。

【配置举例】 1：对采用积极模式发起的协商进行自动识别。

```
Ruijie(config)# crypto isakmp mode-detect
```

【检验方法】 -

【提示信息】 -

【常见错误】 -

【平台说明】 -

9.20 crypto isakmp nat keepalive

配置 nat keepalive 发送间隔。
crypto isakmp nat keepalive *secs*

取消配置的 nat keepalive 发送间隔，恢复默认发送间隔。

no crypto isakmp nat keepalive

【参数说明】

参数	描述
secs	隧道存活时间，范围是 5 秒到 3600 秒

【缺省配置】 5 分钟。

【命令模式】 全局模式

【缺省级别】 14

【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】 1：配置隧道 keepalive 发送报文间隔 1 分钟。

```
Ruijie(config)# crypto isakmp  nat keepalive  60
```

【检验方法】 -

【提示信息】 -

【常见错误】 -

【平台说明】 -

9.21 crypto isakmp nat-traversal disable

关闭 nat-traversal 功能。

crypto isakmp nat-traversal disable

开启 nat- traversal 功能。

no crypto isakmp nat-traversal disable

【参数说明】

参数	描述
-	-

【缺省配置】 默认情况开启 nat-traversal。

【命令模式】 全局模式

【缺省级别】 14

【使用指导】 某些厂商实现协议，nat-traversal 功能支持存在兼容问题，特殊情况下可以关闭 nat-traversal 功能，实现互通。

【配置举例】 1：关闭 nat-traversal 功能。

```
Ruijie(config)# crypto isakmp nat-traversal disable
```

【检验方法】 -

【提示信息】 -

【常见错误】 -

【平台说明】 -

9.22 crypto isakmp next-payload disable

禁用 next-payload 检查选项。
crypto isakmp next-payload disable

开启 next-payload 检查选项。
no crypto isakmp next-payload disable

【参数说明】

参数	描述
-	-

【缺省配置】 默认情况下，出现无法识别的 doi 信息会认为协商无法继续，返回失败。

【命令模式】 全局模式

【缺省级别】 14

【使用指导】 关闭 next-payload 检查后，忽略无法识别的 doi 字段，协商继续处理。但是出现保留字段不为 0，或者字段长度不匹配的情况，仍然会返回失败。

【配置举例】 1：关闭 next-payload 检查。

```
Ruijie(config)# crypto isakmp next-payload disable
```

【检验方法】 -

【提示信息】 -

【常见错误】 -

【平台说明】 -

9.23 crypto isakmp peer

多 peer 的情况下，指定首个发起协商的 peer。
crypto isakmp peer { bind | random }

取消指定的首个发起协商的 peer 优先级。
no crypto isakmp peer

【参数说明】

参数	描述
bind	仅 3G 环境生效，3G 卡配置多 peer 拨号，和 IPSec 拨号对端地址绑定，按照配置顺序，第一组拨号配置对应第一个 peer 配置。
random	随机选择首次尝试协商的 peer。

【缺省配置】 缺省情况下，按照配置顺序，从第一个 peer 开始尝试。

【命令模式】 全局模式

【缺省级别】 14

【使用指导】 和 3G 链路一起使用的时候，3G 拨号配置多组拨号地址，和 IPSec map 中 peer 配置一一对应，可以打开 peer 绑定功能，加快拨号速度。否则需要重试多次才能找到当前对应的 peer，第一次建立隧道的时间会比较长。

【配置举例】 1：开启随机选择隧道连接地址。

```
Ruijie(config)# crypto isakmp peer random
```

【检验方法】 -

【提示信息】 -

【常见错误】 -

【平台说明】 -

9.24 crypto isakmp policy

定义 IKE 某个优先级的策略，并进入 IKE 策略配置模式。
crypto isakmp policy *priority*

删除某个优先级的策略。
no crypto isakmp policy *priority*

【参数说明】

参数	描述
priority	IKE 策略的优先级。使用 1 到 10000 的整数，1 是最高优先级而 10000 是最低优先级。

【缺省配置】 没有缺省优先级。

【命令模式】 全局模式

【缺省级别】 14

【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。

【配置举例】 1：配置一个优先级为 100 的 IKE 策略。

```
Ruijie(config)# crypto isakmp policy 100
Ruijie(isakmp-policy)# authentication pre-share
Ruijie(isakmp-policy)# encryption des
Ruijie(isakmp-policy)# group  2
Ruijie(isakmp-policy)# hash  sha
```

【检验方法】 -

【提示信息】 -

【常见错误】 -

【平台说明】 -

9.25 crypto isakmp vendorid disable

关闭 IKE 协商过程中的锐捷厂商信息。
crypto isakmp vendorid disable

打开 IKE 协商过程中的锐捷厂商信息。
crypto isakmp vendorid disable

【参数说明】

参数	描述
-	-

【缺省配置】 默认情况下，IKE 协商过程中带有锐捷厂商信息。

【命令模式】 全局模式

【缺省级别】 14

【使用指导】 在 IKE 协商过程中，某些厂商出现不能识别私有 VID，造成协商不通过，可以使用此命令关闭锐捷厂商 VID 信息的发送。

【配置举例】 1：关闭协商过程中的 vendorid。

```
Ruijie(config)# crypto isakmp vendorid disable
```

【检验方法】 -

【提示信息】 -

【常见错误】 -

【平台说明】 -

9.26 crypto map (global IPSec)

创建或修改一个加密映射。
crypto map *map-name seq-num* { **ipsec-manual** | **ipsec-isakmp** [**dynamic** *dynamic-map-name*] }

取消一个加密映射或条目。
no crypto map *map-name* [*seq-num*]

【参数说明】

参数	描述
map-name	加密映射集合的名称。
seq-num	加密映射条目的序列号。取值范围 1 到 65535
IPSec-manual	指定映射条目用于建立手工 IPSec 安全联盟。
IPSec-isakmp	指定映射条目用于建立 IKE 协商的 IPSec 安全联盟。
dynamic-map-name	指定作为策略模板的动态加密映射集的名称。

【缺省配置】 不存在加密映射。

【命令模式】 全局模式，使用该命令将进入加密映射配置模式。

【缺省级别】 14

【使用指导】 要使用 IPSec 对数据进行加密保护，首先必须定义一个加密映射，然后将加密映射应用于具体的接口。在加密映射中定义加密通信的参数，主要包括以下参数：

1、通信应该受到 IPSec 保护：关联已配置好的加密访问列表。

2、受 IPSec 保护的通信将被发送到哪里去：谁是远端 IPSec 对等体。

3、用于 IPSec 通信的本地地址：将加密映射集合应用到接口上，IPSec 使用通信接口的地址作为本地对等体的地址。

4、对这些通信应该应用哪些 IPSec 安全策略：从一个或多个变换集组成的列表中选择。

5、安全联盟的生命期。

6、安全联盟是被手工建立还是通过 IKE 建立。

具有相同加密映射名（但映射序列号不同）的加密映射条目组成一个加密映射集合。将加密映射集合应用到接口上，这样所有通过这个接口的 IP 通信都将被应用在接口上的加密映射集合进行判断。如果一个加密映射条目发现了应该受到保护的出站 IP 通信，并且加密映射指定了使用 IKE，将根据该加密映射条目中所包含的参数与远端对等体进行安全联盟协商；如果加密映射条目指定了使用手工建立的安全联盟，那么一个安全联盟在进行配置时就必须已经被建立好了。无论手工建立还是 IKE 协商，只要安全联盟成功建立，数据将被加密传输，如果安全联盟协商失败，数据将被丢弃。

在加密映射条目中描述的策略将在安全联盟的协商过程中被使用，为了使两个 IPSec 对等体之间的 IPSec 能够顺利进行，两个对等体的加密映射条目必须包含互相兼容的配置语句。当两个对等体试图建立安全联盟时，双方都必须至少有一条加密映射条目和对方对等体的一条加密映射条目相兼容至少满足以下条件：

1、加密映射条目必须包含兼容的加密访问列表（如镜像映像访问列表）。

2、双方的加密映射条目都必须确定对方对等体地址（除非对等体正在使用动态加密映射）。

3、加密映射条目必须至少有一个相同的变换。

4、对于单个接口只应用一个加密映射集合。加密映射集合中包含了 IPSec/IKE，或 IPSec/手工条目的组合。

如果为给定的接口创建多个加密映射条目，那么就要使用映射条目的 seq- num 参数将这些映射条目排序；seq-num 值越小，优先级越高。

如果存在下面几种情况中的一种，就必须为一个接口创建多个加密映射条目：

1、如果此接口上不同的数据流将由不同的 IPSec 对等体进行处理。

2、如果想要对不同类型的通信（发往相同或不同的对等体）应用不同的 IPSec 安全性；例如，想让一组子网

间的通信被认证，而另一组子网间的通信既被认证又被加密。在这种情况下，不同类型的通信应该在两个不同的访问列表中被定义，并且必须为每个加密访问列表创建一个单独的加密映射条目。
动态加密映射使用参看 crypto dynamic-map 的使用指南。

【配置举例】 1：手工 IPSec 安全联盟最小配置。

```
Ruijie(config)# crypto map mymap 3 IPSec-manual
Ruijie(config-crypto-map)# set peer 2.2.2.2
Ruijie(config-crypto-map)# set session-key inbound esp 301 cipher abcdef1234567890
Ruijie(config-crypto-map)# set sesession-key outbound esp 300 cipher abcdef1234567890
Ruijie(config-crypto-map)# set transform-set myset
Ruijie(config-crypto-map)# match address 101
```

2：IKE 协商的 IPSec 安全联盟的最小配置。

```
Ruijie(config)# crypto map mymap 4 IPSec-isakmp
Ruijie(config-crypto-map)# set peer 2.2.2.2
Ruijie(config-crypto-map)# set transform-set myset
Ruijie(config-crypto-map)# match address 101
```

【检验方法】 -

【提示信息】 -

【常见错误】 -

【平台说明】 -

9.27 crypto map (interface IPSec)

将预先定义好的加密映射集合运用到接口上。
crypto map *map-name*

从一个接口上取消加密映射集合关联。
no crypto map [*map-name*]

【参数说明】

参数	描述
map-name	加密映射名称

【缺省配置】 没有任何加密映射应用到接口上。

【命令模式】 接口配置模式

【缺省级别】 14

【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。
一个加密映射集只能配置在一个接口上。

【配置举例】 1：将名称为 mymap 的加密映射应用于接口 s0 上。

```
Ruijie(config)# interface  serial  0
Ruijie(config-if)# crypto map mymap
```

【检验方法】 -

【提示信息】 -

【常见错误】 -

【平台说明】 -

9.28 crypto map local-address

指定 IPSec 的固定本地地址。
crypto map *map-name* **local-address** *interface-type interface-number*

取消对 IPSec 本地地址的指定。
no crypto map *map-name* **local-address**

【参数说明】

参数	描述
map-name	IPSec 加密映射名称。
interface-type	作为 IPSec 本地地址的接口类型。
interface-number	作为 IPSec 本地地址的接口编号。

【缺省配置】 IPSec 数据从哪个接口出去，就以当前接口的地址为 IPSec 本地地址。

【命令模式】 全局模式

【缺省级别】 14

【使用指导】 如果一个加密映射应用于多个接口且没有用这个命令，对相同的远程对等体且相同的流量 RGOS 将在每个接口创建各自的 IPSec 安全联盟，默认情况下用加密流量进出口的 IP 作为本地地址。使用该命令指定本地地址

以后，同一个加密映射应用于几个接口，将只创建一个 IPSec 安全联盟，统一使用一个安全联盟进行通讯。
如果一台设备有多个接口允许进行 IPSec 通信，为了方便进行管理，可以使用该命令指定 IPSec 本地地址，这样 RGOS 将使用固定的单一地址与外部路由进行通信。
一般情况下，我们建议使用 loopback 地址作为 IPSec 本地地址。

【配置举例】 1：指定 Loopback0 地址作为 IPSec 的本地地址。

```
Ruijie(config)# crypto map mymap local - address loopback 0
```

【检验方法】 -

【提示信息】 -

【常见错误】 -

【平台说明】 -

9.29 debug crypto engine

打开加密卡工作状态调试开关。
debug crypto engine

关闭加密卡工作状态调试开关。
no debug crypto engine

【参数说明】

参数	描述
-	-

【缺省配置】 关闭调试开关。

【命令模式】 特权模式

【缺省级别】 14

【使用指导】 -

【配置举例】 1：打开加密卡工作状态的调试开关。

```
Ruijie# debug crypto engine
```

2：关闭加密卡工作状态的调试开关。

```
Ruijie# no debug crypto engine
```

【调试信息】

【提示信息】 -

【平台说明】 -

9.30 debug crypto IPSec

打开 IPSEC 报文转发调试开关。
debug crypto IPSec

关闭 IPSEC 报文转发调试开关。
no debug crypto IPSec

【参数说明】

参数	描述
-	-

【缺省配置】 关闭调试开关。

【命令模式】 特权模式

【缺省级别】 14

【使用指导】 -

【配置举例】 1：打开 IPSEC 报文转发调试开关。

```
Ruijie# debug crypto IPSec
```

2：关闭 IPSEC 报文转发调试开关。

```
Ruijie# no debug crypto IPSec
```

【调试信息】 1：报文加解密事件

调试信息	can not find sa 727130249, vrf 0
信息解释	在 vrf 0 中没有找到 SPI 为 727130249 的安全联盟。
产生原因	当收到报文需要解密时，IPSEC 会根据报文中的 SPI 等信息查找安全联盟即 SA 进行解密，如果没有找到会提示以上信息。这种情况多会出现在 3G 链路下，由于链路不稳定，容易出现 IPSEC

	两端致，即一端存在而另一端不存在。
处理建议	如果这种情况出现的比较频繁，需要配置 IPSEC 的保活机制 DPD。

调试信息	packet need encrypto but not!
信息解释	IPSEC 收到了应该加密却没有加密的报文。
产生原因	多是因为一端配置有 IPSEC 而另一端没有配造成的，当配置有 IPSEC 的一端收到报文时，发现报文没有加密就会丢弃。
处理建议	检查两端的配置。

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。

【提示信息】 -

【平台说明】 -

9.31 debug crypto isakmp

打开 IKE 调试开关。

debug crypto isakmp

关闭 IKE 调试开关。

no debug crypto isakmp

【参数说明】

参数	描述
-	-

【缺省配置】 关闭调试开关。

【命令模式】 特权模式

【缺省级别】 14

【使用指导】 -

【配置举例】 1：打开 IKE 调试开关。

```
Ruijie# debug crypto isakmp
```

2：关闭 IKE 调试开关。

```
Ruijie# no debug crypto isakmp
```

【调试信息】 1：协议报文事件

调试信息	received packet from 9.9.9.1, (R) MM_SR1_WI2, MM_KEY_EXCH

信息解释	收到 9.9.9.1 发来的 IKE 协商报文，协商模式为主模式，收到报文时本方已经发出了第一个报文 SR1，正在等待发起方的第 2 个报文 WI2。
产生原因	IKE 协商过程中处理接收报文的每一个函数都有类似的打印。
处理建议	-

2：一阶段策略匹配事件

调试信息	(main mode)process in I1:no fit sa attribute was accepted!
信息解释	接收方处理发起方的第一个协商消息 I1 时，没有找到合适的一阶段策略配置。
产生原因	接收方和发起方配置的一阶段策略不一致。
处理建议	检查两端设备的 IKE 策略配置是否一致。

3：协商认证事件

调试信息	Check main mode hash payload fail!
信息解释	主模式 IKE 协商认证失败。
产生原因	IKE 协商的最后阶段需要认证对方的身份，在预共享认证方式下，协商双方都需要用配置的预共享密钥来认证对方。
处理建议	确认协商双方的预共享密钥配置是否一致。

【提示信息】 -

【平台说明】 -

9.32 encryption (IKE policy)

指定 IKE 策略的加密算法。

encryption { **des** | **3des | aes-128 | aes-192 | aes-256** }

恢复缺省加密算法。

no encryption

【参数说明】

参数	描述
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。

【缺省配置】 56 比特的 DES-CBC 加密算法。

【命令模式】 IKE 策略配置模式

【缺省级别】 14

【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。

【配置举例】 1：指定 IKE 策略的加密算法为 DES。

```
Ruijie(config)# crypto  isakmp policy 10
Ruijie(isakmp-policy)# encryption des
```

【检验方法】 -

【提示信息】 -

【常见错误】 -

【平台说明】 -

9.33 group (IKE policy)

指定 IKE 策略中的 Diffie-Hellman 组标识。
group { **1 | 2 | 5** }

恢复 Diffie-Hellman 组标识为缺省值。
no group

【参数说明】

参数	描述
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

【缺省配置】 768 比特 Diffie-Hellman 组（group 1）。

【命令模式】 IKE 策略配置模式

【缺省级别】 14

【使用指导】 使用该命令指定 IKE 策略中使用的 Diffie-Hellman 组。

【配置举例】 1：指定 IKE 策略的 Diffie-Hellman 组为 1024 比特。

```
Ruijie(config)# crypto  isakmp policy 10
Ruijie(isakmp-policy)# group 2
```

【检验方法】 -

【提示信息】 -

【常见错误】 -

【平台说明】 -

9.34 hash (IKE policy)

指定 IKE 策略中的 HASH 算法。
hash { **sha | md5** }

恢复 hash 算法为缺省值。
no hash

【参数说明】

参数	描述
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。

【缺省配置】 缺省 HASH 算法为 sha。

【命令模式】 IKE 策略配置模式

【缺省级别】 14

【使用指导】 使用该命令指定 IKE 策略中使用的 HASH 算法。

【配置举例】 1：指定 HASH 算法为 md5。

```
Ruijie(config)# crypto  isakmp policy 10
Ruijie(isakmp-policy)# hash md5
```

【检验方法】 -

【提示信息】 -

【常见错误】 -

【平台说明】 -

9.35 lifetime (IKE policy)

指定 IKE 安全联盟的生命周期。
lifetime *seconds*

恢复生命周期为缺省值。
no lifetime

【参数说明】

参数	描述
seconds	IKE 生命周期值（秒）。使用 60 到 86400 秒之间的整数。

【缺省配置】 86400 秒（1 天）。

【命令模式】 IKE 策略配置模式

【缺省级别】 14

【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）。

【配置举例】 1：设置 IKE 安全联盟的生命周期为 1000 秒。

```
Ruijie(config)# crypto  isakmp policy 10
Ruijie(isakmp-policy)# lifetime 1000
```

【检验方法】 -

【提示信息】 -

【常见错误】 -

【平台说明】 -

9.36 match address (IPSec)

指定加密映射条目的访问列表。

match address *access-list-number*

删除加密映射条目中的访问列表。
no match address

【参数说明】

参数	描述
access-list-number	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。

【缺省配置】 加密映射条目没有指定的访问列表。

【命令模式】 加密映射配置模式

【缺省级别】 14

【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。

【配置举例】 1：在名称为 mymap 的加密映射上关联访问列表 101。

```
Ruijie(config)# crypto map mymap 4 IPSec-isakmp
Ruijie(config-crypto-map)# match address 101
```

【检验方法】 -

【提示信息】 -

【常见错误】 -

【平台说明】 -

9.37 match any

指定感兴趣流为本端 ip 地址/掩码(0.0.0.0/0.0.0.0)、对端 ip 地址/掩码(0.0.0.0/0.0.0.0)。
match any

取消指定感兴趣流为本端 ip 地址/掩码(0.0.0.0/0.0.0.0)、对端 ip 地址/掩码(0.0.0.0/0.0.0.0)。
no match any

【参数说明】

参数	描述

-	-

【缺省配置】 感兴趣流默认不为本端 ip 地址/掩码(0.0.0.0/0.0.0.0)、对端 ip 地址/掩码(0.0.0.0/0.0.0.0)。

【命令模式】 加密映射配置模式

【缺省级别】 14

【使用指导】 该命令用于指定 profile 加密映射集的感兴趣流为本端 ip 地址/掩码(0.0.0.0/0.0.0.0)、对端 ip 地址/掩码(0.0.0.0/0.0.0.0)。该 profile 主要用于 ipsec over gre 和 l2tp over ipsec。
如果 ipsec over gre 的 profile 配置了 match any，ipsec 第二阶段协商的感兴趣流为：本端 ip 地址/掩码(0.0.0.0/0.0.0.0)、对端 ip 地址/掩码(0.0.0.0/0.0.0.0)

【配置举例】 1：在名称为 test 的 profile 加密映射上。

```
Ruijie(config)#crypto ipsec profile test
Ruijie(config-crypto-profile)#match any
```

【检验方法】 -

【提示信息】 -

【常见错误】 -

【平台说明】 -

9.38 mode (IPSec)

改变加密变换集合的模式。
mode { **tunnel** | **transport** }

恢复默认模式。
no mode

【参数说明】

参数	描述
tunnel	指定变换集合的模式：通道模式
transport	指定变换集合的模式：传输模式

【缺省配置】 通道模式。

【命令模式】 加密变换配置模式

【缺省级别】 14

【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。

【配置举例】 1：指定变换集合的模式为通道模式。

```
Ruijie(config)#
Ruijie(config)#crypto ipsec transform-set myset
Ruijie(cfg-crypto-trans)#mode tunnel
Ruijie(cfg-crypto-trans)#mode transport
Ruijie(cfg-crypto-trans)#
```

【检验方法】 -

【提示信息】 -

【常见错误】 -

【平台说明】 -

9.39 reverse-route

反向路由注入功能，配置后隧道协商完成后 IPSec 模块自动添加一条静态路由，指向隧道对端，或者指定 ip。
启用方向路由注入功能。
reverse-route [**remote-peer** *ip-address*] [*distance*]

删除反向路由注入功能。
no reverse-route [**remote-peer** *ip-address*] [*distance*]

【参数说明】

参数	描述
ip-address	指定下一跳地址，可选。
distance	下一跳距离。取值范围：1 到 255

【缺省配置】 缺省不启用。

【命令模式】 加密映射配置模式

【缺省级别】 14

【使用指导】 添加的路由可以使用 show ip route 看到。
通过 debug crypto IPSec 命令可以看到添加删除过程。

【配置举例】 -1：指定变换集合的模式为通道模式。

```
Ruijie(config)# crypto  map mymap 5 ipsec-isakmp
Ruijie(config-crypto-map)# reverse-route
```

【检验方法】 -

【提示信息】 -

【常见错误】 -

【平台说明】

9.40 self-identity

指定本地身份采用的形式。
self-identity { **address** | **fqdn** *fqdn* | **user-fqdn** *user-fqdn* }

恢复默认的本体身份形式。
no self-identity

【参数说明】

参数	描述
address	本地 IP 地址。
fqdn	本地设置的域名。
user-fqdn	本地设置的用户和域名。

【缺省配置】 本地 IP 地址。

【命令模式】 全局配置模式

【缺省级别】 14

【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。

【配置举例】 1：以下示例完成身份设定：

```
Ruijie(config)# self-identity fqdn www.vpdn.com
Ruijie(config)# self-identity address
```

【检验方法】 -

【提示信息】 -

【常见错误】 -

【平台说明】 -

9.41 set autoup

设置隧道自动连接。

set autoup

恢复默认。

no set autoup

【参数说明】

参数	描述
access-list-number	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。

【缺省配置】 不启用。

【命令模式】 加密映射配置模式

【缺省级别】 14

【使用指导】 可以避免因为协商隧道造成的丢包。对数据传输敏感，需要隧道随时 up 的场景下使用。

【配置举例】 1：完成工作模式的设置(积极模式)。

```
Ruijie(config)# crypto map mymap 10  IPSec-isakmp
Ruijie(config-crypto-map)# set autoup
```

【检验方法】 -

【提示信息】 -

【常见错误】 -

【平台说明】 -

9.42 set exchange-mode

设置对等体间 IKE 协商中第一阶段采用的工作模式。
set exchange-mode { **main** | **aggressive** }

恢复默认工作模式。
no set exchange-mode

【参数说明】

参数	描述
main	主模式。
aggressive	积极模式

【缺省配置】 主模式。

【命令模式】 加密映射配置模式

【缺省级别】 14

【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。

【配置举例】 1：工作模式的设置(积极模式)。

```
Ruijie(config)# crypto map mymap 10 IPSec-isakmp
Ruijie(config-crypto-map)# set exchange-mode aggressive
```

【检验方法】 -

【提示信息】 -

【常见错误】 -

【平台说明】 -

9.43 set isakmp-policy

指定对应 map 的协商 policy。
set isakmp-policy *number*

不指定 policy 协商
no set isakmp-policy

【参数说明】

参数	描述
number	所指定的协商 policy 序列号

【缺省配置】 不指定 policy 进行协商

【命令模式】 加密映射配置模式

【缺省级别】 14

【使用指导】 在积极模式下，分支默认只发送优先级最高的 policy 至总部进行协商，因此如果同一个分支跟多个总部以积极模式进行协商，则需要所有总部优先级最高的 policy 跟分支均一致，这种要求降低了设备兼容性。使用该命令，则可以指定对应 map 使用所配置 policy 进行协商，继而不需要总部优先级最高的 policy 均一致。该命令只在静态 map 下生效，动态 map 无法配置。

【配置举例】 1：指定静态 map ruijie 使用序列号为 2 的 policy 进行协商。

```
11.x_site1(config)#crypto map ruijie 100 ipsec-isakmp
11.x_site1(config-crypto-map)#set isakmp-policy 2
```

【检验方法】 -

【提示信息】 -

【常见错误】 -

【平台说明】 -

9.44 set local (IPSec)

指定加密映射条目中本地 ip。
set local *ip-address*

删除加密映射条目中的远程对等体。

no set local *ip-address*

【参数说明】

参数	描述
ip-address	本段使用的 IP 地址。

【缺省配置】 不指定任何远程对等体。

【命令模式】 加密映射配置模式

【缺省级别】 14

【使用指导】 用于设置本段协商使用的 ip 地址，没有配置的情况下使用接口主地址协商。配置后使用指定地址。

【配置举例】 1：加密映射 mymap 指定一个远程对等体（2.2.2.2）。

```
Ruijie(config)# crypto  map mymap 5 IPSec-isakmp
Ruijie(config-crypto-map)# set local 2.2.2.2
```

【检验方法】 -

【提示信息】 -

【常见错误】 -

【平台说明】 -

9.45 set mtu

设置 IPSec 预分片模式（隧道模式有效）。

set mtu *length*

不使用预分片模式。

no set mtu

【参数说明】

参数	描述
length	封装前数据包分片大小，范围为 512-1500。

【缺省配置】 不使用预分片模式。

【命令模式】 加密映射配置模式

【缺省级别】 14

【使用指导】 指定 IPSec 隧道封装使用预分片模式。

【配置举例】 1：加密映射 mymap 指定预分片模式。

```
Ruijie(config)# crypto  map mymap 5 IPSec-isakmp
Ruijie(config-crypto-map)# set mtu 1000
```

【检验方法】 -

【提示信息】 -

【常见错误】 -

【平台说明】 -

9.46 set peer (IPSec)

指定加密映射条目中远程对等体。
set peer { *hostname* | *ip-address* }

删除加密映射条目中的远程对等体。
no set peer { *hostname* | *ip-address* }

【参数说明】

参数	描述
ip-address	远程对等体的 IP 地址。
hostname	远程对等体的主机名。

【缺省配置】 不指定任何远程对等体。

【命令模式】 加密映射配置模式

【缺省级别】 14

【使用指导】 对使用的加密映射都必须指定一个远程对等体。
当本地存在多个证书链的情况，根据每个 peer 指定证书链，在没有指定本地证书链的情况下使用对端证书链 ca 证书验证。在没有指定对端证书链的情况使用默认证书链 ca 证书验证。。

【配置举例】 1：加密映射 mymap 指定一个远程对等体（2.2.2.2）。

```
Ruijie(config)# crypto  map mymap 5 IPSec-isakmp
Ruijie(config-crypto-map)# set peer 2.2.2.2
```

【检验方法】 -

【提示信息】 -

【常见错误】 -

【平台说明】 -

9.47 set peer-identical

指定多个 ace 第二阶段协商时使用相同的远程对等体。
set peer-identical

删除指定多个 ace 第二阶段协商时使用相同的远程对等体。
no set peer-identical

【参数说明】

参数	描述
-	-

【缺省配置】 不指定多个 ace 第二阶段协商时使用相同的远程对等体。

【命令模式】 加密映射配置模式

【缺省级别】 14

【使用指导】 当一个 acl 下配置了多个 ace 时，同时配置了多个远程对等体，为了保证所有的 ace 协商都和相同的对等体进行协商时必须配置此命令。

【配置举例】 1：加密映射 mymap 指定 ace 使用相同的远程对等体。

```
Ruijie(config)# crypto  map mymap 5 IPSec-isakmp
Ruijie(config-crypto-map)# set peer-identical
```

【检验方法】 -

【提示信息】 -

【常见错误】 -

【平台说明】 -

9.48 set peer-preempt

指定高优先级的远程对等体发起抢占。
set peer-preempt

删除指定高优先级的远程对等体发起抢占。
no set peer-preempt

【参数说明】

参数	描述
-	-

【缺省配置】 不指定指定高优先级的远程对等体发起抢占。

【命令模式】 加密映射配置模式

【缺省级别】 14

【使用指导】 用于配置了多个远程对等体时，使用高优先级的对等体进行协商。
一个加密映射 map 可以配置多个远程对等体，先配置的优先级比较高，首先使用高优先级的对等体进行协商，当隧道断开之后，切换到一个对等体进行协商，这时候如果高优先级的对等体可以发起协商，使用高优先级的进行协商和转发，同时断开低优先级的隧道协商时，必须配置此命令

【配置举例】 1：加密映射 mymap 指定优先级的远程对等体发起抢占。

```
Ruijie(config)# crypto  map mymap 5 IPSec-isakmp
Ruijie(config-crypto-map)# set peer-preempt
```

【检验方法】 -

【提示信息】 -

【常见错误】 -

【平台说明】 -

9.49 set peer-identical

指定多个 ace 第二阶段协商时使用相同的远程对等体。
set peer-identical

删除指定多个 ace 第二阶段协商时使用相同的远程对等体。

no set peer-identical

【参数说明】

参数	描述
-	-

【缺省配置】 不指定多个 ace 第二阶段协商时使用相同的远程对等体。

【命令模式】 加密映射配置模式

【缺省级别】 14

【使用指导】 当一个 acl 下配置了多个 ace 时，同时配置了多个远程对等体，为了保证所有的 ace 协商都和相同的对等体进行协商时必须配置此命令。

【配置举例】 1：加密映射 mymap 指定 ace 使用相同的远程对等体。

```
Ruijie(config)# crypto  map mymap 5 IPSec-isakmp
Ruijie(config-crypto-map)# set peer-identical
```

【检验方法】 -

【提示信息】 -

【常见错误】 -

【平台说明】 -

9.50 set peer-preempt

指定高优先级的远程对等体发起抢占。
set peer-preempt

删除指定高优先级的远程对等体发起抢占。
no set peer-preempt

【参数说明】

参数	描述
-	-

【缺省配置】 不指定指定高优先级的远程对等体发起抢占。

【命令模式】 加密映射配置模式

【缺省级别】 14

【使用指导】 用于配置了多个远程对等体时，使用高优先级的对等体进行协商。
一个加密映射 map 可以配置多个远程对等体，先配置的优先级比较高，首先使用高优先级的对等体进行协商，当隧道断开之后，切换到一个对等体进行协商，这时候如果高优先级的对等体可以发起协商，使用高优先级的进行协商和转发，同时断开低优先级的隧道协商时，必须配置此命令

【配置举例】 1：加密映射 mymap 指定优先级的远程对等体发起抢占。

```
Ruijie(config)# crypto  map mymap 5 IPSec-isakmp
Ruijie(config-crypto-map)# set peer-preempt
```

【检验方法】 -

【提示信息】 -

【常见错误】 -

【平台说明】 -

9.51 set pfs (IPSec)

指定 IPSec 隧道封装使用 Diffie-Hellman 组标识。
set pfs { **group1 | group2** }

隧道封装不使用 Diffie-Hellman 组标识。
no set pfs

【参数说明】

参数	描述
group1	768 位。
group2	1024 位。

【缺省配置】 不使用 Diffie-Hellman 组。

【命令模式】 加密映射配置模式

【缺省级别】 14

【使用指导】 指定 IPSec 隧道封装使用 Diffie-Hellman 组标识。

【配置举例】 1：加密映射 mymap 指定 1024 位 Diffie-Hellman。

```
Ruijie(config)# crypto  map mymap 5 IPSec-isakmp
```

```
Ruijie(config-crypto-map)# set pfs group2
```

【检验方法】 -

【提示信息】 -

【常见错误】 -

【平台说明】 -

9.52 set security-association lifetime

替换某个加密映射进行 IPSec 安全联盟协商的全局生命周期。
set security-association lifetime { **seconds** *seconds* | **kilobytes** *kilobytes*] }

恢复加密映射进行 IPSec 安全联盟协商的全局生命周期的默认值。
no set security-association lifetime { **seconds** | **kilobytes** }

【参数说明】

参数	描述
seconds *seconds*	安全联盟超时时间（秒）。范围 120 秒到 86400 秒
kilobytes *kilobytes*	安全联盟的超时通信量（以千字节计）。范围 2560KB 到 536870912KB

【缺省配置】 加密映射的安全联盟根据全局生命周期值进行协商。

【命令模式】 加密映射配置模式

【缺省级别】 14

【使用指导】 该命令只对使用 IKE 建立 IPSec 安全联盟的加密映射有用。手工建立的安全联盟的加密映射没有该命令。
在缺省情况下，所有 IPSec 安全联盟都是采用全局生命周期值进行协商，如果需要针对某个目标地址采用不同于全局生命周期值的生命周期进行协商，可以在与该目标地址进行协商的加密映射条目中使用该命令修改生命周期值。

> 该命令修改生命周期值只改变某个具体映射进行 IPSec 安全联盟协商的生命周期值，不影响全局生命周期值。

【配置举例】 1：改加密映射 mymap 条目 5 的生命周期为 2500 秒。

```
Ruijie(config)# crypto  map mymap 5 IPSec-isakmp
Ruijie(config-crypto-map)# set security-association lifetime  seconds 2500
```

【检验方法】 -

【提示信息】 -

【常见错误】 -

【平台说明】 -

9.53 set session-key

为出站和入站的受保护通信设置相关算法的安全参数索引（SPIs）和密码。

set session-key { **inbound | outbound** } **ah** *spi hex-key-data*

set session-key { **inbound | outbound** } **esp** *spi* { **cipher** *hex-key-data* **| authenticator** *hex-key-data* }

删除相关算法的安全参数索引（SPIs）和密码。

no set session-key { **inbound** | **outbound** } **ah**

no set session-key { **inbound | outbound** } **esp**

【参数说明】

参数	描述
spi	安全参数索引。
hex-key-data	是一个 16 进制密码。

【缺省配置】 不指定任何相关算法的安全参数索引和密码。

【命令模式】 加密映射配置模式

【缺省级别】 14

【使用指导】 用于手工创建安全联盟，只在 IPSec-manual 中使用。

【配置举例】 1：加密映射 mymap 指定 esp 封装，解封装密码 abcdef1234567890。

```
Ruijie(config)# crypto  map mymap 5 ipsec-manual
Ruijie(config-crypto-map)# set session-key inbound esp 301 cipher abcdef1234567890
Ruijie(config-crypto-map)# set session-key outbound esp 300 cipher abcdef1234567890
```

【检验方法】 -

【提示信息】 -

【常见错误】 -

【平台说明】 -

9.54 set transform-set

为某个加密映射条目指定使用哪些变换集合。

Set transform-set *transform-set-name1* [*transform-set-name2*] [*transform-set-name3*] [*transform-set-name4*] [*transform-set-name5*] [*transform-set-name6*]

加密映射条目不使用变换集合。

no set pfs

【参数说明】

参数	描述
transform-set-name1 , [*transform-set-name2*] , [*transform-set-name3*] , [*transform-set-name4*] , [*transform-set-name5*] , [*transform-set-name6*]	变换集合名称，最多可以为加密映射条目指定六个变换集合。

【缺省配置】 没有指定任何变换集合。

【命令模式】 加密映射配置模式

【缺省级别】 14

【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。

【配置举例】 1：指定加密映射条目的变换集合为 myset。

```
Ruijie(config)# crypto IPSec transform-set myset  esp-des esp-sha-hmac
Ruijie(config)# crypto  map mymap 5 IPSec-isakmp
Ruijie(config-crypto-map)# set transform-set myset
```

【检验方法】 -

【提示信息】 -

【常见错误】 -

【平台说明】 -

9.55 show crypto dynamic-map (IPSec)

查看动态加密映射的信息。

show crypto dynamic-map [*map-name*]

【参数说明】

参数	描述
map-name	加密映射的名称。

【命令模式】 特权模式

【缺省级别】 14

【使用指导】 使用该命令可以查看设备上的 PIM 接口、接口上的 PIM 邻居、Hello 消息发送间隔、DR 地址等信息。

【配置举例】 1：查看所有动态加密映射的信息

```
Ruijie# show crypto dynamic-map
        Crypto Map Template "mydmap" 1
No matching address list set.
Security association lifetime: 4608000 kilobytes/3600 seconds(id=34)
PFS (Y/N): N
Transform sets = {  }
```

【提示信息】 -

【平台说明】 -

9.56 show crypto IPSec sa

查看当前活动 IPSec 安全联盟的具体信息。

show crypto IPSec sa

【参数说明】

参数	描述
-	-

【命令模式】 特权模式

【缺省级别】 14

【使用指导】 -

【配置举例】 1：查看当前活动 IPSec 安全联盟的具体信息。

```
Interface: GigabitEthernet 1/0/0
        Crypto map tag:mymap, local addr 2.2.2.3
        media mtu 1500
        sub_map type:static, seqno:7, id=0
        local  ident (addr/mask/prot/port): (2.2.2.3/0.0.0.0/0/0))
        remote  ident (addr/mask/prot/port): (2.2.2.2/0.0.0.0/0/0))
        PERMIT
        #pkts encaps: 0, #pkts encrypt: 0, #pkts digest 0
        #pkts decaps: 0, #pkts decrypt: 0, #pkts verify 0
        #send errors 0, #recv errors 0
        Inbound esp sas:
             spi:0x79b8e4bb (2042160315)
              transform: esp-3des
              in use settings={Tunnel,}
              crypto map mymap 7
              sa timing: remaining key lifetime (k/sec): (4607000/3505)
              IV size: 8 bytes
              max reply windows size: 0
              Replay detection support:Y


        Outbound esp sas:
             spi:0x293b8b55 (691768149)
              transform: esp-3des
              in use settings={Tunnel,}
              crypto map mymap 7
              sa timing: remaining key lifetime (k/sec): (4607000/3505)
              IV size: 8 bytes
              max reply windows size: 0
              Replay detection support:Y
```

【提示信息】 -

【平台说明】 -

9.57 show crypto IPSec transform-set

查看设备配置的变换集的信息。

show crypto IPSec transform-set

【参数说明】

参数	描述
-	-

【命令模式】 特权模式

【缺省级别】 14

【使用指导】 -

【配置举例】 1：查看设备配置的变换集的信息。

```
Ruijie# show crypto IPSec transform-set
transform set myset3: { esp-des,}
        will negotiate = {Tunnel,}
```

【提示信息】 -

【平台说明】 -

9.58 show crypto isakmp policy

查看设备配置的 IKE 策略信息。

show crypto isakmp policy

【参数说明】

参数	描述
-	-

【命令模式】 特权模式

【缺省级别】 14

【使用指导】 -

【配置举例】 1：查看设备配置的 IKE 策略信息。

```
Ruijie# show crypto isakmp policy
Protection suite of priority 9
encryption algorithm:   3DES - Data Encryption Standard (56 bit keys).
hash algorithm:         Message Digest 5
authentication method:  Pre-Shared Key
Diffie-Hellman group:   #2 (1024 bit)
lifetime:               1000 seconds
Protection suite of priority 10
```

```
encryption algorithm:   DES - Data Encryption Standard (56 bit keys).
hash algorithm:         Message Digest 5
authentication method:  Pre-Shared Key
Diffie-Hellman group:   #2 (1024 bit)
lifetime:               1000 seconds
Default protection suite
encryption algorithm:   DES - Data Encryption Standard (56 bit keys).
hash algorithm:         Secure Hash Standard
authentication method:  Pre-Shared Key
Diffie-Hellman group:   #1 (768 bit)
lifetime:               86400seconds
```

【提示信息】 -

【平台说明】 -

9.59 show crypto isakmp sa

查看设备上当前活动的 IKE 安全联盟。

show crypto isakmp sa

【参数说明】

参数	描述
-	-

【命令模式】 特权模式

【缺省级别】 14

【使用指导】 -

【配置举例】 1：查看设备上当前活动的 IKE 安全联盟。

```
Ruijie# show crypto isakmp sa
destination   source    state     conn-id   lifetime(second)
 1.1.1.1      1.1.1.2   IKE_IDLE  59         32254
```

【提示信息】 -

【平台说明】 -

9.60 show crypto log

查看 IPSec VPN 的登录注销日志。

show crypto log

【参数说明】

参数	描述
-	-

【命令模式】 特权模式

【缺省级别】 14

【使用指导】 -

【配置举例】 查看 IPSec VPN 的登录注销日志。

```
Ruijie # sh cr log
Time                    RemoteName
PeerIP/Port                                    Action          Reason          Interface
Proto:(Local)ip/mask/port <--> (Peer)ip/mask/port

--------------------   ------------------------------------------------------------
--------------------------------------------  --------------- ---------------
----------------------
-------------------------------------------------------------------------------------------
------------
2014-11-15-01:07:06    3.3.3.3
3.3.3.3/500                                    logout          DEL_IPS_PKT     Gi0/1
17:3.3.3.3/32/1701<-->3.3.3.3/32/1701
2014-11-15-01:07:06    3.3.3.3
3.3.3.3/500                                    logout          DEL_ISA_PKT     Gi0/1
NULL
```

【提示信息】 -

【平台说明】 -

9.61 show crypto log remotename

指定对端名称(IP 等)筛选查看 IPSec VPN 的登录注销日志。

show crypto log remotename *name*

【参数说明】

参数	描述
name	指定显示 log 的对端名称

【命令模式】 特权模式

【缺省级别】 14

【使用指导】 -

【配置举例】 指定对端名称(IP 等)筛选查看 IPSec VPN 的登录注销日志。

```
11.x_site1#show crypto log remotename 61.100.1.20

total log numbers: 184



Time                   RemoteName
PeerIP/Port                                    Action          Reason          Interface
Proto:(Local)ip/mask/port <--> (Peer)ip/mask/pot

--------------------   ------------------------------------------------------------
--------------------------------------------  --------------- ---------------
----------------------  ------------------------------------------------
2015-10-16-03:50:14    61.100.1.20
61.100.1.20/500                                login           NA              Gi0/2
NULL
2015-10-16-03:50:14    61.100.1.20
61.100.1.20/500                                login           NA              Gi0/2
0:1.1.1.0/24/0<-->2.2.2.0/24/0
2015-10-16-03:55:50    61.100.1.20
61.100.1.20/500                                logout          CLR_ISA_SA      Gi0/2
0:1.1.1.0/24/0<-->2.2.2.0/24/0
2015-10-16-03:56:51    61.100.1.20
61.100.1.20/500                                logout          IDLE_TIMER      Gi0/2
NULL
Filter log numbers: 4
11.x_site1#
```

【提示信息】 -

【平台说明】 -

9.62 show crypto log remotename name start start_lines end end_lines

指定对端名称(IP 等)筛选查看 IPSec VPN 的登录注销日志，并在筛选结果中指定行数显示。

show crypto log remotename *name* **start** *start_lines* **end** *end_lines*

【参数说明】

参数	描述
name	指定显示 log 的对端名称
start_lines	指定显示 log 的起始行
end_lines	指定显示 log 的终止行

【命令模式】 特权模式

【缺省级别】 14

【使用指导】 -

【配置举例】 指定对端名称(IP 等)筛选查看 IPSec VPN 的登录注销日志，并在筛选结果中指定行数显示。

```
11.x_site1#show crypto log remotename 61.100.1.20 start 1 end 2

total log numbers: 188



Time                    RemoteName
PeerIP/Port                                     Action          Reason          Interface
Proto:(Local)ip/mask/port <--> (Peer)ip/mask/pot

--------------------    ------------------------------------------------------------
-------------------------------------------  ---------------- ----------------
----------------------  ---------------------------------------------
2015-10-16-03:50:14     61.100.1.20
61.100.1.20/500                                 login           NA              Gi0/2
NULL
2015-10-16-03:50:14     61.100.1.20
61.100.1.20/500                                 login           NA              Gi0/2
0:1.1.1.0/24/0<-->2.2.2.0/24/0
Filter log numbers: 4
```

【提示信息】 -

【平台说明】 -

9.63 show crypto log start start_lines end end_lines

指定行数查看 IPSec VPN 的登录注销日志。

show crypto log start *start_lines* **end** *end_lines*

【参数说明】

参数	描述
start_lines	指定显示 log 的起始行
end_lines	指定显示 log 的终止行

【命令模式】 特权模式

【缺省级别】 14

【使用指导】 -

【配置举例】 指定行数查看 IPSec VPN 的登录注销日志。

```
11.x_site1#show crypto log start 1 end 2

total log numbers: 184



Time                    RemoteName
PeerIP/Port                                     Action          Reason          Interface
Proto:(Local)ip/mask/port <--> (Peer)ip/mask/pot

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

2015-10-16-03:23:55     NO_NAME                                                         (null)/0
restart          IPSEC_RESTART                              NULL
2015-10-16-03:42:57     NO_NAME                                                         (null)/0
restart          IPSEC_RESTART                              NULL
11.x_site1#
```

【提示信息】 -

【平台说明】 -

9.64 show crypto map (IPSec)

查看加密映射的信息。

show crypto map [*map-name*]

【参数说明】

参数	描述
map-name	加密映射的名称。

【命令模式】 特权模式

【缺省级别】 14

【使用指导】 -

【配置举例】 1：查看所有加密映射的信息。

```
Ruijie# show crypto map

Crypto Map:"mymap1" 1 IPSec-isakmp, (Complete)
        Extended IP access list 100
        Security association lifetime: 0 kilobytes/120 seconds(id=2)
        PFS (Y/N): N
        Transform sets = { myset3,  }

        Interfaces using crypto map mymap1:
                GigabitEthernet 1/1/0
```

【提示信息】 -

【平台说明】 -

9.65 tunnel protection IPSec profile

将预先定义好的 Profile 加密映射集合运用到 Tunnel 接口上。

tunnel protection IPSec profile [*profile-name*]

从一个接口上取消加密映射集合关联。

no tunnel protection IPSec profile [*profile-name*]

【参数说明】

参数	描述
profile-name	Profile 加密映射名称。

【缺省配置】 没有任何加密映射应用到 Tunnel 接口上。

【命令模式】 接口配置模式

【缺省级别】 14

【使用指导】 使用此命令将加密映射集合应用于接口。要对 Tunnel 口上的所有报文进行 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。

Profile map 只能支持 GRE、IPIP 的 Tunnel 隧道上的应用，如果配置在了不支持的 Tunnel 隧道上，会配置失败，或者修改 Tunnel 隧道模式为 Profile 不支持的模式，Tunnel 接口上 map 会被删除。

【配置举例】 1：将名称为 profile-name 的加密映射应用于接口 Tunnel 1 上。

```
Ruijie(config)# interface tunnel 1
Ruijie(config-if-Tunnel 1) # tunnel protection IPSec profile profile-name
```

2：将名称为 test 的加密映射应用于接口 virtual-ppp 1 上：

```
Ruijie(config)#crypto ipsec profile test
Ruijie(config-crypto-profile)#exit
Ruijie(config)#
Ruijie(config)#int virtual-ppp 1
Ruijie(config-if-Virtual-ppp 1)#tunnel protection ipsec profile test
Ruijie(config-if-Virtual-ppp 1)#exit
Ruijie(config)#
```

【检验方法】 -

【提示信息】 -

【常见错误】 -

【平台说明】 -

10 AAA

10.1 aaa accounting commands

对登录到 NAS 上的用户所执行的命令活动进行记账，管理用户活动。
aaa accounting commands *level* { **default** | *list-name* } **start-stop** *method1* [*method2*...]

取消命令记账功能。
no aaa accounting commands *level* { **default** | *list-name* }

【参数说明】

参数	描述
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命令记账的默认方法。
list-name	定义一个命令记账的方法列表，可以是任何字符串。
method	必须“**none、group**”所列关键字之一，一个方法列表最多有 4 个方法：
none	不进行记账
group	使用服务器组进行记账，目前支持 TACACS+服务器组

【缺省配置】 记账功能关闭

【命令模式】 全局模式。

【缺省级别】 14

【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。

【配置举例】 1：下面的示例使用 TACACS+对用户执行的命令请求进行记账，要求记账的命令级别为 15 级：

```
Ruijie(config)# aaa accounting commands 15 default start-stop group tacacs+
```

【检验方法】 使用 **show aaa method-list** 命令可以查看已配置的命令记账方法列表信息。

【提示信息】 1：如果设备上没有定义指定的 group，则提示错误。

```
%Group XXX is not existed
```

2：如果 group 类型不支持此记账类型，则提示错误。

```
The accounting does not support this type of group
```

3：如果重复配置此命令，则新配置覆盖原有配置。

【常见错误】 -

【平台说明】 -

10.2 aaa accounting exec

对用户登录 NAS 的访问活动进行记账，管理用户活动。
aaa accounting exec { **default** | *list-name* } **start-stop** *method1* [*method2*...]

取消 Exec 记账功能。
no aaa accounting exec { **default** | *list-name* }

【参数说明】

参数	描述
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“**none、group**”所列关键字之一，一个方法列表最多有 4 个方法
none	不进行记账
group	使用服务器组进行记账，目前支持 RADIUS 和 TACACS+服务器组

【缺省配置】 关闭记账功能

【命令模式】 全局模式。

【缺省级别】 14

【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。

【配置举例】 1：下面的示例使用 RADIUS 对用户登录 NAS 的活动进行记账，并在开始和结束时发送记账报文：

```
Ruijie(config)# aaa accounting exec default start-stop group radius
```

【检验方法】 使用 **show aaa method-list** 命令可以查看已配置的 Exec 记账方法列表信息。

【提示信息】 1：如果设备上没有定义指定的 group，则提示错误。

```
%Group XXX is not existed
```

2：如果 group 类型不支持此记账类型，则提示错误。

```
The accounting does not support this type of group
```

3：如果重复配置此命令，则新配置覆盖原有配置。

【常见错误】 -

【平台说明】 -

10.3 aaa accounting network

出于网络费用的统计或管理用户活动，需要对用户的访问活动进行记账。

aaa accounting network { **default** | *list-name* } **start-stop** *method1* [*method2*...]

取消网络记账功能。

no aaa accounting network { **default** | *list-name* }

【参数说明】

参数	描述
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	记账方法列表名。
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	必须下表所列关键字之一，一个方法列表最多有 4 个方法
none	不进行记账
group	使用服务器组进行记账，目前支持 RADIUS 和 TACACS+服务器组

【缺省配置】 关闭记账功能

【命令模式】 全局模式。

【缺省级别】 14

【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。

【配置举例】 1：下面的示例使用 RADIUS 对用户的网络服务请求进行记账，并在开始和结束时发送记账报文：

```
Ruijie(config)# aaa accounting network default start-stop group radius
```

【检验方法】 使用 **show aaa method-list** 命令可以查看已配置的网络记账方法列表信息。

【提示信息】 1：如果设备上没有定义指定的 group，则提示错误。

```
%Group XXX is not existed
```

2：如果 group 类型不支持此记账类型，则提示错误。

```
The accounting does not support this type of group
```

3：如果重复配置此命令，则新配置覆盖原有配置。

【常见错误】 -

【平台说明】 -

10.4 aaa accounting update

启用记账更新功能，用于使能全局记账更新。

aaa accounting update

关闭记账更新功能。

no aaa accounting update

【参数说明】

参数	描述
-	-

【缺省配置】 记账更新功能缺省关闭。

【命令模式】 全局模式。

【缺省级别】 14

【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。

【配置举例】 1：下面的示例演示设置记账更新使能。

```
Ruijie(config)# aaa new-model
Ruijie(config)# aaa accounting update
```

【检验方法】 使用 **show aaa accounting update** 命令可以查看记账更新功能是否开启。

【提示信息】 -

【常见错误】 -

【平台说明】 -

10.5 aaa accounting update periodic

设置已经启用记账更新功能的记账更新间隔。
aaa accounting update periodic *interval*

配置默认的记账更新间隔。
no aaa accounting update periodic

【参数说明】

参数	描述
interval	记账更新间隔，以分钟为单位，最小为 1 分钟。

【缺省配置】 5 分钟。

【命令模式】 全局模式。

【缺省级别】 14

【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】 1：下面的示例演示设置每隔 1 分钟记账更新。

```
Ruijie(config)# aaa new-model
Ruijie(config)# aaa accounting update
Ruijie(config)# aaa accounting update periodic 1
```

【检验方法】 使用 **show aaa accounting update** 命令可以查看记账更新间隔的配置信息。

【提示信息】 1：如果重复配置此命令，则新配置覆盖原有配置。

【常见错误】 -

【平台说明】 -

10.6 aaa authentication enable

要使用 AAA 进行 Enable 认证，请执行全局配置命令 **aaa authentication enable** 配置 Enable 认证的方法列

表。

aaa authentication enable default *method1* [*method2*...]

删除认证的方法列表。

no aaa authentication enable default

【参数说明】

参数	描述
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。Enable 认证是基于全局的认证，目前只支持设置默认的认证方法列表。
method	必须是“local、none、group、enable”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认证
none	不进行认证
group	使用服务器组进行认证，目前支持 RADIUS 和 TACACS+服务器组
enable	使用 enable 方法进行认证

【缺省配置】 -

【命令模式】 全局模式。

【缺省级别】 14

【使用指导】 如果设备启用 AAA Enable 认证服务，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。

Enable 认证方法列表配置以后，Enable 认证功能自动生效。

【配置举例】 :1：下面的示例定义 AAA Enable 身份认证方法列表。该认证方法列表先使用 RADIUS 安全服务器进行身份认证，如果在一定时限内没有收到 RADIUS 安全服务器的应答，则使用本地用户数据库进行身份认证。

```
Ruijie(config)# aaa authentication enable default group radius local
```

【检验方法】 使用 **show aaa method-list** 命令可以查看已配置的 Enable 认证方法列表信息。

【提示信息】 1：如果设备上没有定义指定的 group，则提示错误。

```
%Group XXX is not existed
```

2：如果 group 类型不支持此认证类型，则提示错误。

```
The authentication does not support this type of group
```

3：如果重复配置此命令，则新配置覆盖原有配置。

【常见错误】 -

【平台说明】 -

10.7 aaa authentication iportal

要使用 AAA 进行设备内置 Portal Web 用户认证，请执行全局配置命令 **aaa authentication iportal** 配置设备内置 Portal Web 用户认证的方法列表。

aaa authentication iportal { **default** | *list-name* } *method1* [*method2*...]

删除认证的方法列表。

no aaa authentication iportal { **default** | *list-name* }

【参数说明】

参数	描述
Default	使用该参数，则后面定义的方法列表作为设备内置 Portal Web 用户认证的默认方法。
list-name	定义一个设备内置 Portal Web 用户认证的方法列表，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认证
none	不进行身份认证
group	使用服务器组进行认证，目前支持 RADIUS 服务器组
subs	使用 subs 数据库进行认证。

【缺省配置】 -

【命令模式】 全局模式。

【缺省级别】 14

【使用指导】 如果设备启用 AAA 设备内置 Portal Web 安全服务，用户就必须使用 AAA 进行设备内置 Portal Web 用户认证协商。您必须使用 **aaa authentication iportal** 命令配置默认的或可选的方法列表用于设备内置 Portal Web 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。

【配置举例】 1：下面的示例定义一个名为 rds_web 的 AAA 设备内置 Portal Web 认证方法列表。该认证方法列表先使用 RADIUS 安全服务器进行认证，如果在一定时限内没有收到 RADIUS 安全服务器的应答，则使用本地用户数据库进行认证。

```
Ruijie(config)# aaa authentication iportal rds_web group radius local
```

【检验方法】 使用 **show aaa method-list** 命令可以查看已配置的 iportal 认证方法列表信息。

【提示信息】 1：如果设备上没有定义指定的 group，则提示错误。

```
%Group XXX is not existed
```

2：如果 group 类型不支持此认证类型，则提示错误。

```
The authentication does not support this type of group
```

3：如果重复配置此命令，则新配置覆盖原有配置。

【常见错误】 -

【平台说明】 -

10.8 aaa authentication login

要使用 AAA 进行 Login（登录）认证，请执行全局配置命令 **aaa authentication login** 配置 Login 认证的方法列表。

aaa authentication login { **default** | *list-name* } *method1* [*method2*...]

删除认证的方法列表。

no aaa authentication login { **default** | *list-name* }

【参数说明】

参数	描述
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 数据库进行认证。

【缺省配置】 -

【命令模式】 全局模式。

【缺省级别】 14

【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。

【配置举例】 1：下面的示例定义一个名为 list-1 的 AAA Login 认证方法列表。该认证方法列表先使用 RADIUS 安全服务器进行认证，如果在一定时限内没有收到 RADIUS 安全服务器的应答，则使用本地用户数据库进行认证。

```
Ruijie(config)# aaa authentication login list-1 group radius local
```

【检验方法】 使用 **show aaa method-list** 命令可以查看已配置的 Login 认证方法列表信息。

【提示信息】 1：如果设备上没有定义指定的 group，则提示错误。

```
%Group XXX is not existed
```

2：如果 group 类型不支持此认证类型，则提示错误。

```
The authentication does not support this type of group
```

3：如果重复配置此命令，则新配置覆盖原有配置。

【常见错误】 -

【平台说明】 -

10.9 aaa authentication ppp

要使用 AAA 进行 PPP 用户认证，请执行全局配置命令 **aaa authentication ppp** 配置 PPP 用户认证的方法列表。

aaa authentication ppp { **default** | *list-name* } *method1* [*method2*...]

删除认证的方法列表。

no aaa authentication ppp { **default** | *list-name* }

【参数说明】

参数	描述
default	使用该参数，则后面定义的方法列表作为 PPP 用户认证的默认方法。
list-name	定义一个 PPP 用户认证的方法列表，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认证
none	不进行身份认证
group	使用服务器组进行认证，目前支持 RADIUS 服务器组
subs	使用 subs 数据库进行认证。

【缺省配置】 -

【命令模式】 全局模式。

【缺省级别】 14

【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。

【配置举例】 :1：下面的示例定义一个名为 rds_ppp 的 AAA PPP 认证方法列表。该认证方法列表先使用 RADIUS 安全服务器进行认证，如果在一定时限内没有收到 RADIUS 安全服务器的应答，则使用本地用户数据库进行认证。

```
Ruijie(config)# aaa authentication ppp rds_ppp group radius local
```

【检验方法】 使用 **show aaa method-list** 命令可以查看已配置的 PPP 认证方法列表信息。

【提示信息】 1：如果设备上没有定义指定的 group，则提示错误。

```
%Group XXX is not existed
```

2：如果 group 类型不支持此认证类型，则提示错误。

```
The authentication does not support this type of group
```

3：如果重复配置此命令，则新配置覆盖原有配置。

【常见错误】 -

【平台说明】 -

10.10 aaa authentication sslvpn

要使用 AAA 进行 sslvpn 用户认证，请执行全局配置命令 **aaa authentication sslvpn** 配置 sslvpn 用户认证的方法列表。
aaa authentication sslvpn { **default** | *list-name* } *method1* [*method2*...]

删除 sslvpn 用户认证的方法列表。
no aaa authentication sslvpn { **default** | *list-name* }

【参数说明】

参数	描述
default	使用该参数，则后面定义的方法列表作为 sslvpn 用户认证的默认方法。
list-name	定义一个 sslvpn 用户认证的方法列表，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认证

none	不进行认证
group	使用服务器组进行认证，目前支持 RADIUS 服务器组
subs	使用 subs 数据库进行认证。

【缺省配置】 -

【命令模式】 全局模式。

【缺省级别】 14

【使用指导】 如果设备启用 sslvpn 服务，用户就必须使用 AAA 进行 sslvpn 用户认证协商。您必须使用 **aaa authentication sslvpn** 命令配置默认的或可选的方法列表用于 sslvpn 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。

【配置举例】 1：下面的示例定义一个名为 rds_sslvpn 的 AAA sslvpn 用户认证方法列表。该认证方法列表先使用 RADIUS 安全服务器进行认证，如果在一定时限内没有收到 RADIUS 安全服务器的应答，则使用本地用户数据库进行认证。

```
Ruijie(config)# aaa authentication sslvpn rds_sslvpn group radius local
```

【检验方法】 使用 **show aaa method-list** 命令可以查看已配置的 sslvpn 认证方法列表信息。

【提示信息】 1：如果设备上没有定义指定的 group，则提示错误。

```
%Group XXX is not existed
```

2：如果 group 类型不支持此认证类型，则提示错误。

```
The authentication does not support this type of group
```

3：如果重复配置此命令，则新配置覆盖原有配置。

【常见错误】 -

【平台说明】 -

10.11 aaa authorization commands

对于已登录到 NAS 的 CLI 界面上的用户，要使用 AAA 命令授权功能对用户执行的命令进行授权，允许或禁止某个用户执行具体的命令。请执行全局配置命令 **aaa authorization commands**。
aaa authorization commands *level* { **default** | *list-name* } *method1* [*method2*...]

关闭 AAA 命令授权功能。
no aaa authorization commands *level* { **default** | *list-name* }

【参数说明】

参数	描述
level	要进行授权的命令级别，范围 0~15，决定哪个级别的命令需要授权通过后才能执行。
default	使用该参数，则后面定义的方法列表作为命令授权的默认方法
list-name	定义一个命令授权的方法列表，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	不进行授权
group	使用服务器组进行授权，目前支持 TACACS+服务器组

【缺省配置】 关闭 AAA 命令授权功能。

【命令模式】 全局模式。

【缺省级别】 14

【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。

【配置举例】 1：下面的示例使用 TACACS+服务器对 15 级命令进行授权：

```
Ruijie(config)# aaa authorization commands 15 default group tacacs+
```

【检验方法】 使用 **show aaa method-list** 命令可以查看已配置的命令授权方法列表信息。

【提示信息】 1：如果设备上没有定义指定的 group，则提示错误。

```
%Group XXX is not existed
```

2：如果 group 类型不支持此授权类型，则提示错误。

```
The authorization does not support this type of group
```

3：如果重复配置此命令，则新配置覆盖原有配置。

【常见错误】 -

【平台说明】 -

10.12 aaa authorization config-commands

要使用 AAA 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，执行全局配置命令 **aaa authorization config-commands**。

aaa authorization config-commands

关闭 AAA 对配置模式下的命令进行授权的功能。

no aaa authorization config-commands

【参数说明】

参数	描述
-	-

【缺省配置】 关闭 AAA 对配置模式下的命令进行授权的功能。

【命令模式】 全局模式。

【缺省级别】 14

【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。

【配置举例】 1：下面的示例打开对配置模式下命令的授权功能：

```
Ruijie(config)# aaa authorization config-commands
```

【检验方法】 -

【提示信息】 -

【常见错误】 -

【平台说明】 -

10.13 aaa authorization console

要使用 AAA 对通过控制台登录的用户，所执行的命令进行授权，执行全局配置命令 **aaa authorization console**。

aaa authorization console

关闭 AAA 对通过控制台登录的用户所执行命令的授权功能。

no aaa authorization console

【参数说明】

参数	描述
-	

【缺省配置】 关闭 AAA 对通过控制台登录的用户所执行命令的授权功能。

【命令模式】 全局模式。

【缺省级别】 14

【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】 1：下面的示例配置控制台登录用户的命令授权功能：

```
Ruijie(config)# aaa authorization console
```

【检验方法】 -

【提示信息】 -

【常见错误】 -

【平台说明】 -

10.14 aaa authorization exec

要使用 AAA 对登录到 NAS 的 CLI 界面的用户进行 Exec 授权，赋予其权限级别，执行全局配置命令 **aaa authorization exec**。

aaa authorization exec { **default** | *list-name* } *method1* [*method2*...]

关闭 AAA Exec 的授权功能。

no aaa authorization exec { **default** | *list-name* }

【参数说明】

参数	描述
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授权
none	不进行授权
group	使用服务器组进行授权，目前支持 RADIUS 和 TACACS+服务器组

【缺省配置】 关闭 AAA Exec 授权功能。

【命令模式】 全局模式。

【缺省级别】 14

【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。

【配置举例】 1：下面的示例使用 RADIUS 服务器进行 Exec 授权：

```
Ruijie(config)# aaa authorization exec default group radius
```

【检验方法】 使用 **show aaa method-list** 命令可以查看已配置的 Exec 授权方法列表信息。

【提示信息】 1：如果设备上没有定义指定的 group，则提示错误。

```
%Group XXX is not existed
```

2：如果 group 类型不支持此授权类型，则提示错误。

```
The authorization does not support this type of group
```

3：如果重复配置此命令，则新配置覆盖原有配置。

【常见错误】 -

【平台说明】 -

10.15 aaa authorization network

要使用 AAA 对访问网络用户的服务请求（包括 PPP、SLIP 等协议）进行授权，执行全局配置命令 **aaa authorization network**。

aaa authorization network { **default** | *list-name* } *method1* [*method2*...]

关闭 AAA 的授权功能。

no aaa authorization network { **default** | *list-name* }

【参数说明】

参数	描述
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。
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	不进行网络授权

group	使用服务器组进行授权，目前支持 RADIUS 和 TACACS+服务器组

【缺省配置】 关闭 AAA Network 授权功能。

【命令模式】 全局模式。

【缺省级别】 14

【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。

【配置举例】 1：下面的示例使用 RADIUS 服务器对网络服务进行授权：

```
Ruijie(config)# aaa authorization network default group radius
```

【检验方法】 使用 **show aaa method-list** 命令可以查看已配置的 Network 授权方法列表信息。

【提示信息】 1：如果设备上没有定义指定的 group，则提示错误。

```
%Group XXX is not existed
```

2：如果 group 类型不支持此授权类型，则提示错误。

```
The authorization does not support this type of group
```

3：如果重复配置此命令，则新配置覆盖原有配置。

【常见错误】 -

【平台说明】 -

10.16 aaa domain

进入域配置模式，配置域的属性。
aaa domain { **default** | *domain-name* }

取消该命令。
no aaa domain { **default** | *domain-name* }

【参数说明】

参数	描述

default	使用该参数，进行缺省域的配置
domain-name	指定域的名称

【缺省配置】 没有配置任何域。

【命令模式】 全局模式。

【缺省级别】 14

【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。

【配置举例】 1：下面的示例演示设置域名配置：

```
Ruijie(config)# aaa domain ruijie.com
Ruijie(config-aaa-domain)#
```

【检验方法】 使用 **show aaa domain** 命令查看域配置信息。

【提示信息】 -

【常见错误】 -

【平台说明】 -

10.17 aaa domain enable

基于域名的 AAA 服务总开关，默认情况下为关闭状态。当打开该开关的时候，所有 AAA 服务优先使用基于域名的 AAA 服务配置。

aaa domain enable

关闭该开关。

no aaa domain enable

【参数说明】

参数	描述
-	-

【缺省配置】 基于域名的 AAA 服务开关关闭。

【命令模式】 全局模式。

【缺省级别】 14

【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。

【配置举例】 1：打开基于域名的 AAA 服务开关：

```
Ruijie(config)# aaa domain enable
```

【检验方法】 使用 **show aaa domain** 命令查看域配置信息。

【提示信息】 -

【常见错误】 -

【平台说明】 -

10.18 aaa local authentication attempts

配置 login 登录用户尝试登录失败次数。

aaa local authentication attempts *max-attempts*

【参数说明】

参数	描述
max-attempts：	最大尝试失败次数，取值范围 1~2147483647。

【缺省配置】 缺省值为 3 次。

【命令模式】 全局模式。

【缺省级别】 14

【使用指导】 该命令配置 Login 登录用户尝试登录失败次数。

【配置举例】 1：配置 Login 登录用户尝试登录失败次数为 6 次

```
Ruijie# configure terminal
Ruijie(config)# aaa local authentication attempts 6
```

【检验方法】 使用 **show aaa lockout** 命令查看锁定配置信息。

【提示信息】 -

【常见错误】 -

【平台说明】 -

10.19 aaa local authentication lockout-time

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。

aaa local authentication lockout-time *lockout-time*

【参数说明】

参数	描述
lockout-time	锁定时间（单位：分钟），取值范围 1~2147483647

【缺省配置】 缺省值为 15 分钟。

【命令模式】 全局模式。

【缺省级别】 14

【使用指导】 配置 Login 登录用户尝试超过配置登录失败次数后被锁定的时间长度。

【配置举例】 1：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为 5 分钟

```
Ruijie# configure terminal
Ruijie(config)# aaa local authentication lockout-time 5
```

【检验方法】 使用 **show aaa lockout** 命令查看锁定配置信息。

【提示信息】 -

【常见错误】 -

【平台说明】 -

10.20 aaa local user allow public account

配置 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。

aaa local user allow public account

【参数说明】

参数	描述
-	-

【缺省配置】 关闭，即不允许一个本地账户被多个终端共享。

【命令模式】 全局模式。

【缺省级别】 14

【使用指导】 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。

【配置举例】 1：配置 Login 登录用户尝试登录失败次数为 6 次

```
Ruijie#configure terminal
Ruijie(config)#aaa local user allow public account
```

【检验方法】 使用 **show run** 命令查看配置信息。

【提示信息】 -

【常见错误】 -

【平台说明】 -

10.21 aaa log enable

要打印 AAA 用户认证通过的 syslog，请执行 aaa log enable 命令打开开关。
aaa log enable

不打印 AAA 用户认证通过的 syslog。
no aaa log enable

【参数说明】

参数	描述
-	-

【缺省配置】 打印 AAA 用户认证通过的 syslog。

【命令模式】 全局模式。

【缺省级别】 14

【使用指导】 大量用户上线时打印 AAA 用户认证通过的 syslog，可能会造成刷屏或设备性能下降，因此可以通过配置本命令来关闭打印功能。

【配置举例】 1：下面的示例关闭打印 aaa 用户认证通过的 syslog。

```
Ruijie(config)# no aaa log enable
```

【检验方法】 使用 **show running-config** 命令查看打印 aaa 用户认证通过 syslog 功能是否使能。

【提示信息】 -

【常见错误】 -

【平台说明】 -

10.22 aaa log rate-limit

要调整 AAA 用户认证通过的 syslog 的打印速率，请执行 aaa log rate-limit 命令进行配置。
aaa log rate-limit *num*

恢复 AAA 用户认证通过的 syslog 的默认打印速率。
no aaa log rate-limit

【参数说明】

参数	描述
num	每秒钟打印 syslog 的条数，范围为 0 - 65535： 0：表示不限制打印速率 1 - 65535：可配置的打印速率范围，默认值为 5。

【缺省配置】 5，即每秒打印 5 条 AAA 用户认证通过的 syslog。

【命令模式】 全局模式。

【缺省级别】 14

【使用指导】 大量用户上线时打印 AAA 用户认证通过的 syslog，可能会造成刷屏或设备性能下降。因此可以通过配置此命令来调整用户认证通过的 syslog 的打印速率。

【配置举例】 1：下面的示例调整 AAA 用户认证通过的 syslog 的打印速率为每秒 10 条

```
Ruijie(config)# aaa log rate-limit 10
```

【检验方法】 使用 **show running-config** 命令查看 AAA 用户认证通过的 syslog 的打印速率。

【提示信息】 -

【常见错误】 -

【平台说明】 -

10.23 aaa new-model

要使用 RGOS 的 AAA 安全服务功能，请执行全局配置命令 **aaa new-model** 使能 AAA。
aaa new-model

关闭 AAA 安全服务。
no aaa new-model

【参数说明】

参数	描述
-	-

【缺省配置】 关闭 AAA 安全服务。

【命令模式】 全局模式。

【缺省级别】 14

【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。

【配置举例】 1：下面的示例使能 AAA 安全服务。

```
Ruijie(config)# aaa new-model
```

【检验方法】 使用 **show running-config** 命令查看 AAA 安全服务是否使能。

【提示信息】 -

【常见错误】 -

【平台说明】 -

10.24 access-limit

设置域的用户数量限制，只对 IEEE802.1x 用户有效。
access-limit *num*

取消对域用户数量的限制。
no access-limit

【参数说明】

参数	描述

num	域用户的数量限制，只限制 IEEE802.1x 用户

【缺省配置】 缺省情况下不限制用户数量。

【命令模式】 域配置模式。

【缺省级别】 14

【使用指导】 使用该命令对域的用户数量进行限制。

【配置举例】 1：下面的示例演示设置域名为 ruijie.com 的域的用户数量为 20。

```
Ruijie(config)# aaa domain ruijie.com
Ruijie(config-aaa-domain)# access-limit 20
```

【检验方法】 使用 **show aaa domain** 命令可以查看域的用户数量限制配置信息。

【提示信息】 -

【常见错误】 -

【平台说明】 -

10.25 accounting network

在域配置模式下配置 Network 记账列表。
accounting network { **default |** *list-name* }

取消命令。
no accounting network

【参数说明】

参数	描述
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

【缺省配置】 在没有指定方法列表时，如果有用户发起请求，网络设备会尝试给该用户指定 default 方法列表。

【命令模式】 域配置模式。

【缺省级别】 14

【使用指导】 为域指定使用的 Network 记账方法列表。

【配置举例】 1：下面的示例演示设置域指定 Network 记账方法列表：

```
Ruijie(config)# aaa domain ruijie.com
Ruijie(config-aaa-domain)# accounting network default
```

【检验方法】 使用 **show aaa domain** 命令可以查看域指定的 Network 记账方法列表配置信息。

【提示信息】 1：如果指定的方法列表名超过长度限制，则提示错误。

```
Method list name is too long
```

2：如果指定的方法列表尚未配置，则提示错误。

```
%WARNING: method list named XXX for this type is not existed
```

3：如果重复配置此命令，则新配置覆盖原有配置。

【常见错误】 -

【平台说明】 -

10.26 authentication dot1x

在域配置模式下配置 IEEE802.1x 认证列表。
authentication dot1x { **default** | *list-name* }

取消命令。
no authentication dot1x

【参数说明】

参数	描述
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

【缺省配置】 在没有指定方法列表时，如果有用户发起请求，网络设备会尝试给该用户指定 default 方法列表。

【命令模式】 域配置模式。

【缺省级别】 14

【使用指导】 为域指定一个 802.1x 认证方法列表。

【配置举例】 1：下面的示例演示设置域指定 802.1x 认证方法列表：

```
Ruijie(config)# aaa domain ruijie.com
```

```
Ruijie(config-aaa-domain)# authentication dot1x default
```

【检验方法】 使用 **show aaa domain** 命令可以查看域指定的 802.1x 认证方法列表配置信息。

【提示信息】 1：如果指定的方法列表名超过长度限制，则提示错误。

```
Method list name is too long
```

2：如果指定的方法列表尚未配置，则提示错误。

```
%WARNING: method list named XXX for this type is not existed
```

3：如果重复配置此命令，则新配置覆盖原有配置。

【常见错误】 -

【平台说明】 -

10.27 authorization network

在域配置模式下配置 Network 授权列表。

authorization network { **default** | *list-name* }

取消命令。

no authorization network

【参数说明】

参数	描述
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

【缺省配置】 在没有指定方法列表时，如果有用户发起请求，网络设备会尝试给该用户指定 default 方法列表。

【命令模式】 域配置模式。

【缺省级别】 14

【使用指导】 -

【配置举例】 1：下面的示例演示设置域指定 Network 授权方法列表：

```
Ruijie(config)# aaa domain ruijie.com
Ruijie(config-aaa-domain)# authorization network default
```

【检验方法】 使用 **show aaa domain** 命令可以查看域指定的 Network 授权方法列表配置信息。

【提示信息】 1：如果指定的方法列表名超过长度限制，则提示错误。

```
Method list name is too long
```

2：如果指定的方法列表尚未配置，则提示错误。

```
%WARNING: method list named XXX for this type is not existed
```

3：如果重复配置此命令，则新配置覆盖原有配置。

【常见错误】 -

【平台说明】 -

10.28 clear aaa local user lockout

清除被锁定的用户列表。

clear aaa local user lockout { **all** | **user-name** *word* }

【参数说明】

参数	描述
all	表示所有被锁定的用户
user-name *word*	指定被锁定用户 ID

【命令模式】 特权模式。

【缺省级别】 14

【使用指导】 清除被锁定的用户列表，可以全部清除也可以指定用户清除。

【配置举例】 1：清除所有被锁定的用户。

```
Ruijie# clear aaa local user lockout all
```

【提示信息】 1：如果清除指定某一个用户时并且该用户存在，则提示信息。

```
User XXX unlocked
```

【平台说明】 -

10.29 show aaa accounting update

显示记账更新相关的信息。

show aaa accounting update

【参数说明】

参数	描述
-	-

【命令模式】 特权模式、全局模式、接口模式

【缺省级别】 14

【使用指导】 显示记账更新相关的信息，包括记账更新开关是否打开以及记账更新间隔信息。

【配置举例】 1：显示记账更新相关信息

```
Ruijie# show aaa accounting update
```

【提示信息】 -

【平台说明】 -

10.30 show aaa domain

显示当前所有配置域信息。

show aaa domain [**default** | *domain-name*]

【参数说明】

参数	描述
default	使用该参数，指定显示默认的域信息
domain-name	显示指定域名的域信息

【命令模式】 特权模式、全局模式、接口模式。

【缺省级别】 14

【使用指导】 如果不指定域名，则显示所有的域信息。

【配置举例】 1：下面的示例显示指定域名为 domain.com 的域信息。

```
Ruijie# show aaa domain domain.com

============Domain domain.com=============
State: Active
Username format: Without-domain
Access limit: No limit
802.1X Access statistic: 0
```

```
Selected method list:
 authentication dot1x default
```

【提示信息】 -

【平台说明】 -

10.31 show aaa group

显示 AAA 配置的所有服务器组。

show aaa group

【参数说明】

参数	描述
-	-

【命令模式】 特权模式、全局模式、接口模式。

【缺省级别】 14

【使用指导】 该命令显示 AAA 所有已配置的服务器组。

【配置举例】 1：显示 AAA 所有已配置的服务器组

```
Ruijie# show aaa group
Type        Reference  Name
----------- ---------- ----------
radius      1          radius
tacacs+     1          tacacs+
radius      1          dot1x_group
radius      1          login_group
radius      1          enable_group
```

【提示信息】 -

【平台说明】 -

10.32 show aaa lockout

显示当前 login 的锁定配置参数。

show aaa lockout

【参数说明】

参数	描述
-	-

【命令模式】 特权模式、全局模式、接口模式。

【缺省级别】 14

【使用指导】 该命令显示当前 login 的锁定配置参数。

【配置举例】 1：显示当前 login 的锁定配置

```
Ruijie# show aaa lockout
Lock tries:    3
Lock timeout:  15 minutes
```

【提示信息】 -

【平台说明】 -

10.33 show aaa method-list

显示 AAA 所有的方法列表。

show aaa method-list

【参数说明】

参数	描述
-	-

【命令模式】 特权模式、全局模式、接口模式。

【缺省级别】 14

【使用指导】 该命令显示 AAA 所有的方法列表。

【配置举例】 1：下面的示例显示 AAA 方法列表。

```
Ruijie# show aaa method-list
Authentication method-list
aaa authentication login default group radius
aaa authentication ppp default group radius
aaa authentication dot1x default group radius
aaa authentication dot1x san-f local  group angel group rain none
aaa authentication enable default group radius
Accounting method-list
```

```
aaa accounting network default start-stop group radius
Authorization method-list
aaa authorizating network default group radius
```

【提示信息】 -

【平台说明】 -

10.34 show aaa user

显示 aaa 用户相关信息。

show aaa user { **all | lockout | by-id** *session-id* **| by-name** *user-name* }

【参数说明】

参数	描述
all	查看所有 AAA 用户信息
lockout	查看当前被锁定的 AAA 用户列表信息
by-id *session-id*	查看指定 session id 的 AAA 用户信息
by-name *user-name*	查看指定用户名的 AAA 用户信息

【命令模式】 特权模式、全局模式、接口模式。

【缺省级别】 14

【使用指导】 显示 AAA 用户相关信息。

【配置举例】 1：下面的示例显示 AAA 用户相关信息

```
Ruijie#show aaa user all
------------------------------
        Id ----- Name
 2345687901      wwxy
------------------------------
Ruijie# show aaa user by-id 2345687901
------------------------------
        Id ----- Name
 2345687901      wwxy
```

```
Ruijie# show aaa user by-name wwxy
------------------------------
        Id ----- Name
 2345687901      wwxy
------------------------------
```

```
Ruijie# show aaa user lockout

Name                            Tries      Lock       Timeout(min)
------------------------------- ---------- ---------- ------------
Ruijie#
```

【提示信息】 -

【平台说明】 -

10.35 state

设置域是否有效。
state { **block** | **active** }

恢复成默认配置。
no state

【参数说明】

参数	描述
block	配置的域有效
active	配置的域无效

【缺省配置】 缺省情况下为域有效。

【命令模式】 域配置模式。

【缺省级别】 14

【使用指导】 指定配置的域是否有效。

【配置举例】 1：下面的示例演示设置域无效。

```
Ruijie(config)# aaa domain ruijie.com
Ruijie(config-aaa-domain)# state block
```

【检验方法】 使用 **show aaa domain** 命令可以查看域是否有效。

【提示信息】 -

【常见错误】 -

【平台说明】 -

10.36 username-format

在域配置模式下配置 NAS 与服务器交互时用户名中是否携带域信息。
username-format { **without-domain** | **with-domain** }

恢复成默认配置。
no username-format

【参数说明】

参数	描述
without-domain	剥离域信息
with-domain	不剥离域信息

【缺省配置】 缺省情况下不剥离域信息。

【命令模式】 域配置模式。

【缺省级别】 14

【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。

【配置举例】 1：下面的示例演示设置剥离域信息：

```
Ruijie(config)# aaa domain ruijie.com
Ruijie(config-aaa-domain)# username-domain without-domain
```

【检验方法】 使用 **show aaa domain** 命令可以查看域的是否携带域名的信息。

【提示信息】 -

【常见错误】 -

【平台说明】 -

11 RADIUS

11.1 aaa group server radius

进入 AAA 服务器组配置模式。
aaa group server radius *name*

删除服务器组。
no aaa group server radius *name*

【参数说明】

参数	描述
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。

【缺省配置】 -

【命令模式】 全局配置模式。

【缺省级别】 14

【使用指导】 该命令配置 RADIUS 类型的 AAA 服务器组。

【配置举例】 1：下面示例配置了一个 RADIUS 类型的 AAA 服务器组，组名为 ss。

```
Ruijie(config)# aaa group server radius ss
Ruijie(config-gs-radius)# end
Ruijie# show aaa group
Type       Reference  Name
---------- ---------- ----------
radius     1          radius
tacacs+    1          tacacs+
radius     1          ss
```

【检验方法】 使用命令 **show running-config** 可以查看 radius 报文的源地址接口配置信息

【提示信息】 -

【常见错误】 -

【平台说明】 -

11.2 ip oob

为 AAA 服务器组选择 mgmt 口。
ip oob

删除 AAA 服务器组选择 mgmt 口。
no ip oob

【参数说明】

参数	描述
-	-

【缺省配置】 -

【命令模式】 服务器组配置模式。

【缺省级别】 14

【使用指导】 配置此命令前，必须通过命令 aaa group server radius 进入 radius 组配置模式。
为指定服务器组选择 mgmt 口。
没指定哪个 mgmt 口时，默认为 mgmt0 口

【配置举例】 -

【检验方法】 使用 **show radius group** 命令查看 RADIUS 类型服务器组的 oob 配置信息。

【提示信息】 -

【常见错误】 -

【平台说明】 NBR6205-E、NBR6135-E、NBR6210-E、NBR6215-E 支持 MGMT 口；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 MGMT 口。

11.3 ip radius source-interface

指定 RADIUS 报文的源地址。
ip radius source-interface *interface-name*

删除指定的 RADIUS 报文源地址。

no radius source-interface *interface-name*

【参数说明】

参数	描述
interface-name	radius 报文的源地址接口

【缺省配置】 缺省 radius 报文的源地址由网络层设置

【命令模式】 全局模式

【缺省级别】 14

【使用指导】 为了减少在 radius 服务器上维护大量的 nas 信息的工作量，可以通过该命令来设置 radius 报文的源地址。该命令将把指定接口的第一个 ip 地址作为 radius 报文的源地址，该命令在三层设备使用。

【配置举例】 1：指定 radius 报文从 FastEthernet 0/0 接口获取 ip 地址来作为 radius 报文的源地址:。

```
Ruijie(config)# ip radius source-interface fastEthernet 0/0
```

【检验方法】 使用命令 **show running-config** 可以查看 radius 报文的源地址接口配置信息

【提示信息】 -

【常见错误】 -

【平台说明】 -

11.4 radius set qos cos

设置 radius 下发的 qos 值为接口 cos 值

radius set qos cos

恢复默认 radius 下发的 qos 值

no radius set qos cos

【参数说明】

参数	描述
-	-

【缺省配置】 缺省 qos 配置为 dscp 值

【命令模式】 全局模式

【缺省级别】 14

【使用指导】 -

【配置举例】 1： 设置 radius 下发的 qos 值为接口 cos 值。

```
Ruijie(config)# radius set qos cos
```

【检验方法】 使用 **show running-config** 查看 qos 值的配置信息

【提示信息】 -

【常见错误】 -

【平台说明】 -

11.5 radius support cui

设置 radius 支持 cui 属性
radius support cui

关闭 radius 支持 cui 属性的功能
no radius support cui

【参数说明】

参数	描述
-	-

【缺省配置】 缺省不支持 cui 属性

【命令模式】 全局模式

【缺省级别】 14

【使用指导】 使用该命令可以根据需要配置 radius 是否支持 cui 属性

【配置举例】 1： 配置 radius 支持 cui 属性。

```
Ruijie(config)# radius support cui
```

【检验方法】 使用 **show running-config** 查看 radius 支持 cui 属性的支持情况

【提示信息】 -

【常见错误】 -

【平台说明】 -

11.6 radius vendor-specific attribute support

配置 radius 支持解析报文中思科、华为、微软的私有属性
radius vendor-specific attribute support { cisco | huawei | ms}

配置 radius 不支持解析报文中思科、华为、微软的私有属性
no radius vendor-specific attribute support { cisco | huawei | ms}

【参数说明】

参数	描述
cisco	思科私有属性
huawei	华为私有属性
ms	微软私有属性

【缺省配置】 支持解析报文中思科、华为、微软的私有属性

【命令模式】 全局模式

【缺省级别】 14

【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】 1：配置 radius 支持解析报文中的华为私有属性。

```
Ruijie(config)# radius vendor-specific attribute support huawei
```

2：配置 radius 不支持解析报文中的华为私有属性。

```
Ruijie(config)# no radius vendor-specific attribute support huawei
```

【检验方法】 使用 **show running-config** 查看该命令配置是否生效。支持解析是缺省配置不进行展现，**show running-config** 可查看对哪些厂商的不支持解析进行了配置。

【提示信息】 -

【常见错误】 -

【平台说明】 -

11.7 radius vendor-specific extend

设置 radius 解析报文不区分私有厂商 id
radius vendor-specific extend

恢复为只识别我司私有厂商 id
no radius vendor-specific extend

【参数说明】

参数	描述
-	-

【缺省配置】 只识别我司私有厂商 id

【命令模式】 全局模式

【缺省级别】 14

【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。

【配置举例】 1：配置 radius 解析私有属性不区分私有厂商 id。

```
Ruijie(config)# radius vendor-specific extend
```

【检验方法】 使用 **show running-config** 查看该命令配置是否生效。

【提示信息】 -

【常见错误】 -

【平台说明】 -

11.8 radius-server account attribute

配置在 RADIUS 记帐请求报文中携带指定属性
radius-server account attribute *type* **package**

配置在 RADIUS 记帐请求报文中不携带指定属性
radius-server account attribute *type* **unpackage**
恢复在记帐请求报文中指定属性是否携带的默认配置
no radius-server account attribute *type* **package**

default radius-server account attribute *type* **package**
no radius-server account attribute *type* **unpackage**
default radius-server account attribute *type* **unpackage**

【参数说明】

参数	描述
type	Radius 属性类型。可设置范围为 1-255

【缺省配置】 RFC 强制规定记帐请求必须携带的属性默认为携带，规定不需携带的属性默认为不携带
其它属性默认为未设置状态，即可携带也可不携带状态

【命令模式】 全局模式

【缺省级别】 14

【使用指导】 使用该命令配置 RADIUS 记帐请求报文是否发送相应的属性
RFC 强制规定记帐请求必须携带的属性不能修改为不携带，不需携带的属性不能修改为携带。
no 与 default 命令将属性的配置恢复为缺省状态。

【配置举例】 1：下面的示例在 radius 记帐请求报文中不发送 NAS-PORT-ID 属性。
Ruijie(config)# radius-server account attribute 87 unpackage

【检验方法】 在 radius 服务器抓包，查看 radius 记帐请求报文中应不携带 87 相关属性

11.9 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。
radius-server account update retransmit

恢复默认记账更新报文进行重传的配置。
no radius-server account update retransmit

【参数说明】

参数	描述
-	-

【缺省配置】 缺省配置不重传记账更新报文。

【命令模式】 全局模式

【缺省级别】 14

【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】 1：配置认证用户的记账更新报文进行重传的功能。

```
Ruijie(config)#radius-server account update retransmit
```

【检验方法】 使用命令 **show running-config** 查看配置。

【提示信息】 -

【常见错误】 -

【平台说明】 -

11.10 radius-server account vendor

配置 RADIUS 记帐请求报文中携带相关产商的私有属性
radius-server account vendor [cmcc | microsoft | cisco] package

恢复默认配置，在记帐请求报文中不携带相关产商的私有属性
no radius-server account vendor *vendor_name* **package**
default radius-server account vendor *vendor_name* **package**

【参数说明】

参数	描述
cmcc | microsoft | cisco	产商类型，cmcc 中移动，microsoft 微软，cisco 思科

【缺省配置】 记帐请求报文中不携带其它产商的私有属性

【命令模式】 全局模式

【缺省级别】 14

【使用指导】 使用该命令配置 RADIUS 记帐请求报文是否携带指定产商的私有属性

【配置举例】 1：下面的示例在 radius 记帐请求报文中携带 cmcc 的私有属性。

```
Ruijie(config)# radius-server account vendor cmcc package
```

【检验方法】 在 radius 服务器抓包，可以查看 radius 记帐请求报文中应不携带 cmcc 要求的记帐属性

11.11 radius-server attribute class

配置 RADIUS 的 Class 属性的解析方式：
radius-server attribute class user-flow-control { **format-16bytes** | **format-32bytes** }

关闭对 RADIUS 的 Class 属性的解析：
no radius-server attribute class user-flow-control

【参数说明】

参数	描述
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

【缺省配置】 缺省情况下不从 class 属性中解析限速。

【命令模式】 全局模式

【缺省级别】 14

【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。

【配置举例】 1：启用从 Class 属性中解析限速配置的功能，解析的格式为 32 字节。

```
Ruijie(config)#radius-server attribute class user-flow-control format-32bytes
```

【检验方法】 使用 **show running-config** 查看 radius 的配置。

【提示信息】 -

【常见错误】 -

【平台说明】 -

11.12 radius-server attribute 31

指定 RADIUS Calling-Station-ID 属性（基于 MAC）的格式。
radius-server attribute 31 mac format { **ietf | normal | unformatted** }

恢复默认 RADIUS Calling-Station-ID 属性（基于 MAC）的格式
no radius-server attribute 31 mac format

【参数说明】

参数	描述
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。

【缺省配置】 使用 unformatted 格式

【命令模式】 全局模式

【缺省级别】 14

【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。

【配置举例】 1：下面的示例定义 RADIUS Calling-Station-ID 属性为 IETF 格式。

```
Ruijie(config)# radius-server attribute 31 mac format ietf
```

【检验方法】 使用 **show running-config** 查看 radius 组装 mac 的格式设置信息。

【提示信息】 -

【常见错误】 -

【平台说明】 -

11.13 radius-server authentication attribute

配置在 RADIUS 认证请求报文中携带指定属性
radius-server authentication attribute *type* **package**

配置在 radius 认证请求报文中不携带指定属性
radius-server authentication attribute *type* **unpackage**

恢复在认证请求报文中指定的属性是否携带的默认配置
no radius-server authentication attribute *type* **package**
default radius-server authentication attribute *type* **package**
no radius-server authentication attribute *type* **unpackage**

default radius-server authentication attribute *type* **unpackage**

【参数说明】

参数	描述
type	Radius 属性类型。可设置范围为 1-255

【缺省配置】 RFC 强制规定认证请求必须携带的属性默认为携带，规定不需携带的属性默认为不携带
其它属性默认为未设置状态，即可携带也可不携带状态

【命令模式】 全局模式

【缺省级别】 14

【使用指导】 使用该命令配置 RADIUS 认证请求报文是否发送相应的属性。
RFC 强制规定认证请求必须携带的属性不能修改为不携带，不需携带的属性不能修改为携带。
no 与 default 命令将属性的配置恢复为缺省状态。

【配置举例】 1：下面的示例在 radius 认证请求报文中不发送 NAS-PORT-ID 属性。

```
Ruijie(config)# radius-server authentication attribute 87 unpackage
```

【检验方法】 在 radius 服务器抓包，查看 radius 请求报文中应不携带 87 属性

11.14 radius-server authentication vendor

配置 RADIUS 认证请求报文中携带相关产商的私有属性
radius-server authentication vendor [cmcc | microsoft | cisco] package

恢复默认配置，在认证请求报文中不携带相关产商的私有属性
no radius-server authentication vendor *vendor_name* **package**
default radius-server authentication vendor *vendor_name* **package**

【参数说明】

参数	描述
cmcc | microsoft | cisco	产商类型，cmcc 中移动，microsoft 微软，cisco 思科

【缺省配置】 认证请求报文中不携带其它产商的私有属性

【命令模式】 全局模式

【缺省级别】 14

【使用指导】 使用该命令配置 RADIUS 认证请求报文是否携带指定产商的私有属性

【配置举例】 1：下面的示例在 radius 认证请求报文中携带 cmcc 的私有属性。

```
Ruijie(config)# radius-server authentication vendor cmcc package
```

【检验方法】 在 radius 服务器抓包，可以查看 radius 认证请求报文中应不携带 cmcc 要求的私有属性

11.15 radius-server dead-criteria

配置设备判定 RADIUS 安全服务器不可达的标准。

radius-server dead-criteria { **time** *seconds* [**tries** *number*] | **tries** *number* }

恢复设备判断 RADIUS 安全服务器不可达的标准为默认值

no radius-server dead-criteria { **time** *seconds* [**tries** *number*] | **tries** *number* }

【参数说明】

参数	描述
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。

【缺省配置】 **time** *seconds* 的默认值为 60 秒。

tries *number* 的默认值为 10 次。

【命令模式】 全局模式

【缺省级别】 14

【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。

【配置举例】 1：下面的示例指定时长为 120 秒，连续超时次数为 20 次。

```
Ruijie(config)# radius-server dead-criteria time 120 tries 20
```

【检验方法】 使用 **show radius parameter** 可以查看设备判定 RADIUS 安全服务器不可达的标准的配置信息。

【提示信息】 -

【常见错误】 -

【平台说明】 -

11.16 radius-server deadtime

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报文的时间长度。
radius-server deadtime *minutes*

恢复设备停止向处于不可达状态的 RADIUS 安全服务器发送请求报文的时间长度为默认值。
no radius-server deadtime

【参数说明】

参数	描述
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）。

【缺省配置】 *minutes* 的默认值为 0 分钟（即使 RADIUS 安全服务器不可达，设备仍然往该 RADIUS 服务器发送请求）

【命令模式】 全局模式

【缺省级别】 14

【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】 1：下面的示例指定停止发送时长为 1 分钟。

```
Ruijie(config)# radius-server deadtime 1
```

【检验方法】 使用 **show radius parameter** 可以查看设备停止向处于不可达状态的 RADIUS 安全服务器发送请求报文的时间长度的配置信息。

【提示信息】 -

【常见错误】 -

【平台说明】 -

11.17 radius-server host

指定 RADIUS 安全服务器主机。
radius-server host [**oob**] { *ipv4-address* | *ipv6-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*]

删除指定的 RADIUS 安全服务器主机。

no radius-server host { *ipv4-address* | *ipv6-address* }

【参数说明】

参数	描述
oob	oob 认证，即向此服务器发送报文时源接口为 mgmt 口。 配置 oob，默认为 mgmt0 口。
ipv4-address	RADIUS 安全服务器主机的 IPv4 地址。
ipv6-address	RADIUS 安全服务器主机的 IPv6 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。

【缺省配置】 没有指定的 RADIUS 主机

【命令模式】 全局模式

【缺省级别】 14

【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，则设备向应用服务器发送 radius 报文时使用全局路由表。

【配置举例】 1：下面的示例定义一个 IPv4 环境下的 RADIUS 安全服务器主机。

```
Ruijie(config)# radius-server host 192.168.12.1
```

2：下面的示例定义一个 IPv4 环境下的 RADIUS 安全服务器主机，开启主动探测功能，检测间隔周期为 60 分钟，关闭对记账 UDP 口的检测。

```
Ruijie(config)# radius-server host 192.168.100.1 test username test idle-time 60 ignore-acct-port
```

3：下面的示例定义一个 IPv6 环境下的 RADIUS 安全服务器主机。

```
Ruijie(config)# radius-server host 3000::100
```

【检验方法】 使用 **show radius server** 可以查看 RADIUS 安全服务器的配置信息。

【提示信息】 -

【常见错误】 -

【平台说明】 NBR6205-E、NBR6135-E、NBR6210-E、NBR6215-E 支持 MGMT 口；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 MGMT 口。

11.18 radius-server key

定义网络访问服务器（路由设备）与 RADIUS 安全服务器进行通信的共享口令。

radius-server key [**0** | **7**] *text-string*

取消指定的共享口令。

no radius-server key

【参数说明】

参数	描述
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】 没有指定共享口令。

【命令模式】 全局模式

【缺省级别】 14

【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】 1：下面的示例定义 RADIUS 安全服务器的共享口令为 aaa。

```
Ruijie(config)# radius-server key aaa
```

【检验方法】 使用 **show radius server** 可以查看 RADIUS 安全服务器的共享口令的配置信息。

【提示信息】 -

【常见错误】 -

【平台说明】 -

11.19 radius-server retransmit

配置设备在认为 RADIUS 安全服务器没有反应以前重发报文的次数。
radius-server retransmit *retries*

恢复默认重发次数。
no radius-server retransmit

【参数说明】

参数	描述
retries	RADIUS 尝试重发次数，取值范围是 1-100。

【缺省配置】 默认重发次数为 3。

【命令模式】 全局模式

【缺省级别】 14

【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。

【配置举例】 1：下面的示例指定重发次数为 4。

```
Ruijie(config)# radius-server retransmit 4
```

【检验方法】 使用命令 **show radius parameter** 可以查看 radius 的重传次数配置信息。

【提示信息】 -

【常见错误】 -

【平台说明】 -

11.20 radius-server source-port

配置设备发送 RADIUS 报文的源端口。
radius-server source-port *port*

恢复默认值。

no radius-server source-port

【参数说明】

参数	描述
port	要设置的端口。可设置的值范围为 1-65535。

【缺省配置】 随机端口

【命令模式】 全局模式

【缺省级别】 14

【使用指导】 设备发送 RADIUS 报文的源端口默认情况下是随机的。如果需要指定源端口，使用该命令配置。

【配置举例】 1：下面的示例将发送 radius 报文的源端口定义为 10000。

```
Ruijie(config)# radius-server source-port 10000
```

【检验方法】 使用 **show running-config** 可以查看设备 radius 报文的源端口配置信息。

【提示信息】 -

【常见错误】 -

【平台说明】 -

11.21 radius-server timeout

配置设备重发 RADIUS 报文等待安全服务器应答的时间。

radius-server timeout *seconds*

恢复默认值。

no radius-server timeout

【参数说明】

参数	描述
seconds	超时时间（单位为秒）。可设置的值范围为 1-1000 秒。

【缺省配置】 默认为 5 秒

【命令模式】 全局模式

【缺省级别】 14

【使用指导】 使用该命令配置设备重发 RADIUS 报文等待安全服务器应答的时间。

【配置举例】 1：下面的示例将超时时间定义为 10 秒。

```
Ruijie(config)# radius-server timeout  10
```

【检验方法】 使用 **show radius parameter** 可以查看设备重发 RADIUS 报文等待安全服务器应答的时间的配置信息。

【提示信息】 -

【常见错误】 -

【平台说明】 -

11.22 server auth-port acct-port

添加 AAA 服务器组的服务器，**no** 形式删除。

server { *ipv4-addr* } [**auth-port** *port1*] [**acct-port** *port2*]

no server { *ipv4-addr* } [**auth-port** *port1*] [**acct-port** *port2*]

【参数说明】

参数	描述
ip-addr	服务器 ip 地址
port1	服务器认证端口
port2	服务器记账端口

【缺省配置】 无服务器配置

【命令模式】 服务器组配置模式。

【缺省级别】 14

【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】 1：下面示例为服务器组 ss 添加服务器 192.168.4.12 并制定其记账端口为 5 和认证端口为 6。

```
Ruijie(config)# aaa group server radius ss
Ruijie(config-gs-radius)# server 192.168.4.12 acct-port 5 auth-port 6
Ruijie(config-gs-radius)# end
Ruijie# show aaa group
Type       Reference  Name
---------- ---------- ----------
```

```
radius      1          radius
tacacs+     1          tacacs+
radius      1          ss
```

【检验方法】 使用 **show radius group** 命令查看 RADIUS 类型服务器组的服务器信息。

【提示信息】 -

【相关命令】

命令	描述
aaa group server	配置 aaa 服务器组
show aaa group	显示 aaa 服务器组

【常见错误】 -

【平台说明】 -

11.23 show radius acct statistics

显示 RADIUS 计费相关统计信息。

show radius radius acct statistics

【参数说明】

参数	描述
-	-

【命令模式】 全局模式、特权模式、接口模式

【缺省级别】 14

【使用指导】 -

【配置举例】 1：显示 RADIUS 计费相关统计信息。

```
Ruijie#show radius acct statistics
Accounting Servers:

Server Index..................................... 1
Server Address................................... 192.168.1.1
Server Port...................................... 1813
Msg Round Trip Time.............................. 0 (msec)
First Requests................................... 1
Retry Requests................................... 1
Accounting Responses............................. 0
```

```
Malformed Msgs..................................... 0
Bad Authenticator Msgs............................. 0
Pending Requests................................... 1
```

【提示信息】 -

【平台说明】 -

11.24 show radius attribute

显示 RADIUS 属性。

show radius attribute

【参数说明】

参数	描述
-	-

【命令模式】 全局模式、特权模式、接口模式

【缺省级别】 14

【使用指导】 -

【配置举例】 1：显示 RADIUS 属性。

```
Ruijie#sh radius attribute
type          implicate
----          ---------
   1.........User-Name
   2.........User-Password
   3.........Chap-Password
   4.........NAS-Ip-Addr
   5.........Nas-Ip-Port
   6.........Service-Type
   7.........Framed-Protocol
   8.........Frame-Ip-Address
   9.........Framed-Ip-Mask
  10.........Framed-Routing
  11.........Filter-Id
  12.........Framed-Mtu
  13.........Framed-Compress
  14.........Login-Ip-Host
```

```
15.........Login-Service
16.........Login-Tcp-Port
18.........Reply-Message
19.........Callback-Num
20.........Callback-Id
22.........Framed-Route
23.........Framed-IPX-Network
24.........State
25.........Class
26.........Vendor-Specific
27.........Session-Timeout
28.........Idle-Timeout
29.........Termination-Action
30.........Called-Station-Id
31.........Calling-Station-Id
32.........Nas-Id
33.........Proxy-State
34.........Login-LAT-Service
35.........Login-LAT-Node
36.........Login-LAT-Group
37.........Framed-AppleTalk-Link
38.........Framed-AppleTalk-Net
39.........Framed-AppleTalk-Zone
40.........Acct-Status-Type
41.........Acct-Delay-Time
42.........Acct-Input-Octets
43.........Acct-Output-Octets
44.........Acct-Session-Id
45.........Acct-Authentic
46.........Acct-Session-Time
47.........Acct-Input-Packet
48.........Acct-Output-Packet
49.........Acct-Terminate-Cause
50.........Acct-Multi-Session-ID
51.........Acct-Link-Count
52.........Acct-Input-Gigawords
53.........Acct-Output-Gigawords
60.........Chap-Challenge
61.........Nas-Port-Type
62.........Port-Limit
63.........Login-Lat-Port
```

```
64.........Tunnel-Type
65.........Tunnel-Medium-Type
66.........Tunnel-Client-EndPoint
67.........Tunnel-Service-EndPoint
79.........eap msg
80.........Message-Authenticator
81.........group id
85.........Acct-Interim-Interval
87.........Nas-Port-Id
89.........cui
96.........Framed-Interface-Id
```

【提示信息】 -

【平台说明】 -

11.25 show radius auth statistics

显示 RADIUS 认证相关统计信息。

show radius auth statistics

【参数说明】

参数	描述
-	-

【命令模式】 全局模式、特权模式、接口模式

【缺省级别】 14

【使用指导】 -

【配置举例】 1：显示 RADIUS 认证相关统计信息。

```
Ruijie#show radius auth statistics
Authentication Servers:

Server Index..................................... 1
Server Address................................... 192.168.1.1
Server Port...................................... 1812
Msg Round Trip Time.............................. 0 (msec)
First Requests................................... 0
Retry Requests................................... 0
Accept Responses................................. 0
```

```
Reject Responses.............................. 0
Challenge Responses........................... 0
Malformed Msgs................................ 0
Bad Authenticator Msgs........................ 0
Pending Requests.............................. 0
Timeout Requests.............................. 0
Unknowntype Msgs.............................. 0
Other Drops................................... 0
```

【提示信息】 -

【平台说明】 -

11.26 show radius group

显示 RADIUS 服务器组的配置。

show radius group

【参数说明】

参数	描述
-	-

【命令模式】 全局模式、特权模式、接口模式

【缺省级别】 14

【使用指导】 -

【配置举例】 1：显示 RADIUS 服务器组的配置。

```
Ruijie#show radius group
==========Radius group radius==========
Vrf:not-set
Server:192.168.1.1
  Server key:ruijie
  Authentication port:1812
  Accounting port:1813
  State:Active
```

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。

【提示信息】 -

【平台说明】 -

11.27 show radius parameter

显示 RADIUS 服务器全局参数。

show radius parameter

【参数说明】

参数	描述
-	-

【命令模式】 全局模式、特权模式、接口模式

【缺省级别】 14

【使用指导】 -

【配置举例】 1：显示 RADIUS 服务器全局参数。

```
Ruijie# show radius parameter
Server Timout:   5 Seconds
Server Deadtime: 0 Minutes
Server Retries:  3
Server Dead Critera:
Time:         10 Seconds
Tries:        10
```

【提示信息】 -

【平台说明】 -

11.28 show radius server

显示 RADIUS 服务器配置情况。

show radius server

【参数说明】

参数	描述
-	-

【命令模式】 全局模式、特权模式、接口模式

【缺省级别】 14

【使用指导】 -

【配置举例】 1：显示 RADIUS 服务器配置情况。

```
Ruijie# show radius server
Server IP:    192.168.4.12
Accounting  Port:  23
Authen  Port:     77
Test Username:    test
Test Idle Time:   10 Minutes
Test Ports:        Authen
Server State:     Active
    Current duration 765s, previous duration 0s
Dead: total time 0s, count 0
Statistics:
Authen: request 15, timeouts 1
Author: request 0, timeouts 0
Account: request 0, timeouts 0

Server IP:    192.168.4.13
Accounting Port:  45
Authen  Port:     74
Test Username:    <Not Configured>
Test Idle Time:   60 Minutes
Test Ports:        Authen and Accounting
Server State:     Active
Current duration 765s, previous duration 0s
Dead: total time 0s, count 0
Statistics:
Authen: request 0, timeouts 0
Author: request 0, timeouts 0
Account: request 20, timeouts 0
```

【提示信息】 -

【平台说明】 -

11.29 show radius vendor-specific

显示 RADIUS 私有属性类型配置。

show radius vendor-specific

【参数说明】

参数	描述
-	-

【命令模式】 全局模式、特权模式、接口模式

【缺省级别】 14

【使用指导】 -

【配置举例】 1：显示 RADIUS 私有属性类型配置。

```
Ruijie#show radius vendor-specific
id    vendor-specific      type-value
----- -------------------- ----------
1     max-down-rate        1
2     port-priority        2
3     user-ip              3
4     vlan-id              4
5     last-supplicant-vers 5
      ion
6     net-ip               6
7     user-name            7
8     password             8
9     file-directory       9
10    file-count           10
11    file-name-0          11
12    file-name-1          12
13    file-name-2          13
14    file-name-3          14
15    file-name-4          15
16    max-up-rate          16
17    current-supplicant-v 17
      ersion
18    flux-max-high32      18
19    flux-max-low32       19
20    proxy-avoid          20
21    dialup-avoid         21
22    ip-privilege         22
23    login-privilege      42
27    ipv4-multicast-addre 87
```

```
ss
```

【提示信息】 -

【平台说明】 -

12 TACACS+

12.1 aaa group server tacacs+

此命令配置 TACACS+服务器组，将不同的 TACACS+服务器划分到不同的组。
aaa group server tacacs+ *group-name*

删除服务器组。
no aaa group server tacacs+ *group-name*

【参数说明】

参数	描述
group-name	TACACS+服务器组名，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。

【缺省级别】 14

【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。

【配置举例】 1：下面的示例配置一个名字为 tac1 的 TACACS+服务器组，并且在该组中配置一个 1.1.1.1 的 TACACS+服务器地址：

```
Ruijie(config)# aaa group server tacacs+ tac1
Ruijie(config-gs-tacacs+)#server 1.1.1.1
```

【检验方法】 使用 **show running-config** 命令可以查看已配置的 TACACS+服务器组信息。

【提示信息】 -

【常见错误】 -

【平台说明】 -

12.2 ip tacacs source-interface

指定 TACACS+报文的源地址。

ip tacacs source-interface *interface-name*

删除指定的 TACACS+报文源地址。
no tacacs source-interface *interface-name*

【参数说明】

参数	描述
interface-name	tacacs+报文的源地址接口

【缺省配置】 缺省 tacacs+报文的源地址由网络层设置

【命令模式】 全局模式

【缺省级别】 14

【使用指导】 为了减少在 tacacs+服务器上维护大量的 nas 信息的工作量，可以通过该命令来设置 tacacs+报文的源地址。该命令将把指定接口的第一个 ip 地址作为 tacacs+报文的源地址，该命令在三层设备使用。

【配置举例】 1：指定 tacacs+报文从 gigabitEthernet 0/0 接口获取 ip 地址来作为源地址。

```
Ruijie(config)# ip tacacs source-interface gigabitEthernet 0/0
```

【检验方法】 使用命令 **show running-config** 可以查看 tacacs+报文的源地址接口配置信息。

【提示信息】 -

【常见错误】 -

【平台说明】 -

12.3 server

添加 TACACS+服务器组的服务器。
server {*ipv4-address* }

删除添加的服务器。
no server {*ipv4-address* }

【参数说明】

参数	描述
ipv4-address	服务器 IPv4 地址

【缺省配置】 无服务器配置。

【命令模式】 TACACS+服务器组配置模式。

【缺省级别】 14

【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。

【配置举例】 1：下面的示例配置一个名字为 tac1 的 TACACS+服务器组，并且在该组中配置一个 1.1.1.1 的 TACACS+服务器地址。

```
Ruijie(config)# aaa group server tacacs+ tac1
Ruijie(config-gs-tacacs+)# server 1.1.1.1
```

【检验方法】 使用命令 **show running-config** 可以查看服务器组的 server 配置信息。

【提示信息】 1：如果指定的 server 尚未配置，则提示错误。

```
Warning: Server 1.1.1.1 is not defined.
```

【常见错误】 -

【平台说明】 -

12.4 show tacacs

显示和各 TACACS+服务器的交互运行情况。
show tacacs

【参数说明】

参数	描述
-	-

【命令模式】 特权模式、全局模式、接口模式。

【缺省级别】 14

【使用指导】 使用该命令显示和各 TACACS+服务器的交互运行情况。

【配置举例】 1：下面的示例显示已经配置的 TACACS+服务器的相关信息。

```
Ruijie# show tacacs
Tacacs+ Server : 172.19.192.80/49
```

```
Socket Opens: 0
Socket Closes: 0
Total Packets Sent: 0
Total Packets Recv: 0
Reference Count: 0
```

【提示信息】 -

【平台说明】 -

12.5 tacacs-server host

此命令配置 TACACS+服务器的相关信息。
tacacs-server host [**oob**] { *ipv4-address* | *ipv6-address* } [**port** *integer*] [**timeout** *integer*] [**key** [**0** | **7**] *text-string*]

删除 TACACS+服务器。
no tacacs-server host {*ipv4-address* }

【参数说明】

参数	描述
ipv4-address	TACACS+服务器的 IPv4 地址。
Ipv6-address	TACACS+服务器的 Ipv6 地址。
oob	TACACS+通信使用的源接口为 mgmt 口，默认为使用非 mgmt 口进行通信。
port *integer*	TACACS+通信使用的 TCP 端口，默认为 TCP 端口 49，可配置范围为 1 ~ 65535。
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。可配置范围为 1 ~ 1000。
key *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】 没有指定的 TACACS+主机

【命令模式】 全局模式

【缺省级别】 14

【使用指导】 为了使用 TACACS+实现 AAA 安全服务，必须定义 TACACS+服务器。您可以使用 **tacacs-server host** 命令定义一个或多个 TACACS+服务器。

【配置举例】 1：下面的示例定义一个 IPv4 环境下的 TACACS+服务器。

```
Ruijie(config)# tacacs-server host 192.168.12.1
```

【检验方法】 使用 **show radius server** 可以查看 TACACS+服务器的配置信息。

【提示信息】 -

【常见错误】 -

【平台说明】 NBR6205-E、NBR6135-E、NBR6210-E、NBR6215-E 支持 MGMT 口；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 MGMT 口。

12.6 tacacs-server key

定义网络访问服务器（路由设备）与 TACACS+服务器进行通信的共享密钥。
tacacs-server key [**0 | 7**] *text-string*

取消指定的共享密钥。
no tacacs-server key

【参数说明】

参数	描述
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】 没有指定共享密钥。

【命令模式】 全局模式

【缺省级别】 14

【使用指导】 该命令配置全局使用的共享密钥。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。

【配置举例】 1：下面的示例定义 TACACS+服务器的共享口令为 aaa。

```
Ruijie(config)# tacacs-server key aaa
```

【检验方法】 使用 **show running-config** 可以查看 TACACS+服务器的共享口令的配置信息。

【提示信息】 -

【常见错误】 -

【平台说明】 -

12.7 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。
tacacs-server timeout *seconds*

恢复默认值。
no tacacs-server timeout

【参数说明】

参数	描述
seconds	超时时间（单位为秒）。可设置的值范围为 1-1000 秒。

【缺省配置】 默认为 5 秒

【命令模式】 全局模式

【缺省级别】 14

【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。

【配置举例】 1：下面的示例将超时时间定义为 10 秒。

```
Ruijie(config)# tacacs-server timeout 10
```

【检验方法】 使用 **show running-config** 可以查看 TACACS+报文超时时间的配置信息。

【提示信息】 -

【常见错误】 -

【平台说明】 -

13 Web 认证配置命令

13.1 accounting

设置模板的记账方法。
accounting { *method-list* }

重置为默认的记账方法。
no accounting

【参数说明】

参数	描述
method-list	方法列表名。

【缺省配置】 缺省使用 default 方法。

【命令模式】 模板配置模式。

【缺省级别】 14

【使用指导】

本命令中的方法列表名需要和 AAA 中配置的网络记账方法列表名称保持一致。

【配置举例】 -

【检验方法】 使用 **show web-auth template** 来查看当前配置的模板参数

【提示信息】 -

【常见错误】 -

【平台说明】 -

13.2 authentication

设置模板的认证方法。
authentication { *method-list* }

重置为默认的认证方法。

no authentication

【参数说明】

参数	描述
method-list	方法列表名。

【缺省配置】 缺省使用 default 方法。

【命令模式】 模板配置模式。

【缺省级别】 14

【使用指导】

- 本命令中的方法列表名需要和 AAA 中配置的 web 认证方法列表名称保持一致。
- 一代认证不支持方法列表配置

【配置举例】 -

【检验方法】 使用 **show web-auth template** 来查看当前配置的模板参数

【提示信息】 -

【常见错误】 -

【平台说明】 -

13.3 bindmode

设置模板绑定模式。

bindmode

重置模板绑定模式。

no bindmode

【参数说明】

参数	描述
-	-

【缺省配置】 -

【命令模式】 模板配置模式。

【缺省级别】 14

【使用指导】 -

【配置举例】 -

【检验方法】 使用 **show web-auth template** 来查看当前配置的模板参数

【提示信息】 -

【常见错误】 -

【平台说明】 -

13.4 clear web-auth direct-arp

在设备上删除所有的 arp 资源

clear web-auth direct-arp

【参数说明】

参数	描述

【命令模式】 特权模式。

【缺省级别】 14

【使用指导】 -

【配置举例】 1：将所有直通 arp 的资源删除

```
Ruijie# clear web-auth direct-arp
```

【提示信息】 -

【平台说明】 -

13.5 clear web-auth direct-host

在设备上删除所有免认证用户

clear web-auth direct-host [range]

【参数说明】

参数	描述

【命令模式】 特权模式。

【缺省级别】 14

【使用指导】 -

【配置举例】 1：将所有免认证用户删除

```
Ruijie# clear web-auth direct-host
```

2：将所有连续的免认证用户删除

Ruijie# clear web-auth direct-host range

【提示信息】 -

【平台说明】 -

13.6 clear web-auth direct-site

在设备上删除所有免认证网络资源

clear web-auth direct-site [range]

【参数说明】

参数	描述

【命令模式】 特权模式。

【缺省级别】 14

【使用指导】 -

【配置举例】 1：将所有免认证网络资源删除

```
Ruijie# clear web-auth direct-site
```

1：将所有连续的免认证网络资源删除

Ruijie# clear web-auth direct-site range

【提示信息】 -

【平台说明】 -

13.7 clear web-auth group

在设备上删除所有分组信息

clear web-auth group

【参数说明】

参数	描述

【命令模式】 特权模式。

【缺省级别】 14

【使用指导】 -

【配置举例】 1：将所有的组信息删除

```
Ruijie# clear web-auth group
```

【提示信息】 -

【平台说明】 -

13.8 clear web-auth user

在设备上强制用户下线。

clear web-auth user { **all** | **ip {** *ip-address }* | **mac** *mac-address* **| name** *name-string* | **session-id** *num* }

【参数说明】

参数	描述
ip-address	指定用户的 IPv4 地址。
mac-address	指定用户的 MAC 地址
name-string	指定用户名
num	指定用户的 AAA 会话 ID

【命令模式】 特权模式。

【缺省级别】 14

【使用指导】 -

【配置举例】 1：将所有用户强制下线。

```
Ruijie# clear web-auth user all
```

【提示信息】 -

【平台说明】 -

13.9 fmt

1 代模板配置模式下，设置重定向报文 url 格式。

fmt { ace | ruijie | custom }

定制化 URL 格式，1 代模板下设置 URL 格式。

fmt custom [encry { md5 | des | des_ecb | des_ecb3 | none }] [user-ip *userip-str* **] [user-mac** *usermac-str* **mac-format [dot | line | none]] [user-vid** *uservid-str* **]** [**user-id** *userid-str*] **[nas-ip** *nasip-str* **] [nas-id** *nasid-str* **] [nas-id2** *nasid2-str* **] [ac-name** *acname-str* **] [ac-name** acname-str **] [ap-mac** *apmac-str* **mac-format [dot | line | none]] [url** *url-str* **] [ssid** *ssid-str* **] [port** *port-str* **] [ac-serialno** *ac-sno-str* **] [ap-serialno** *ap-sno-str* **]**

删除配置。

no fmt custom [user-ip] [user-mac] [user-vid] [**user-id**] **[nas-ip] [nas-id] [nas-id2] [ac-name] [ap-mac] [url] [ssid] [port] [ac-serialno] [ap-serialno]**

【参数说明】

参数	描述
cmcc-ext1	中移动扩展 url 格式。
cmcc-ext2	辽宁移动 url 格式。
cmcc-ext2	宁波/嘉兴移动 AC 厂商 URL 格式。
cmcc-mtx	中移动 AC 厂商 url 格式。
cmcc-normal	中移动标准 url 格式。
ace	支持 ACE 联动。
ruijie	锐捷 url 格式。
custom	定制化格式。
userip-str	用户 ip 对应的参数名称
usermac-str	用户 mac 对应的参数名称
uservid-str	用户 vid 对应的参数名称
userid-str	用户 id 对应的参数名称
nasip-str	设备 ip 对应的参数名称
nasid-str	NAS 设备 ID 对应的参数名称
nasid2-str	NAS 设备 ID 对应的参数名称(支持定制两个 nasid 参数)
ac-name	设备名称对应的参数名称
apmac-str	关联 AP 的 MAC 地址对应的参数名称
url-str	用户原始访问 url 对应的参数名称
ssid-str	SSID 对应的参数名称
port-str	用户认证端口对应的参数名称
ac-sno-str	ac 设备序列号对应的参数名称
ap-sno-str	ap 设备序列号对应的参数名称
md5	所配置参数采用 md5 加密
des	所配置参数采用 des 加密
des_ecb	所配置参数采用 des_ecb 加密

des_ecb3	所配置参数采用 des_ecb3 加密
none	所配置参数不加密，明文传输

【缺省配置】 默认为 ruijie 格式。

【命令模式】 模板配置模式。

【缺省级别】 14

【使用指导】 根据 portal 服务器的对接规范，设置不同的 url 类型。

10.x 运营商版本是使用全局的命令 http redirect url-fmt {cmcc-normal | cmcc-ext1 | cmcc-ext2} 来设置 url 类型。11.x 废弃该命令，做成隐藏。如果用户执行该命令，将转为模板下的 fmt 配置命令保存。

【配置举例】 -

【检验方法】 使用 **show web-auth template** 查看配置的模板

【提示信息】

【常见错误】 -

【平台说明】 -

13.10 http redirect direct-arp

设置直通 ARP 地址范围。

http redirect direct-arp { *ip-address* [*ip-mask*] }

删除配置。

No http redirect direct- arp { *ip-address* [*ip-mask*] }

【参数说明】

参数	描述
ip-address	Ipv4 地址。
Ip-mask	（可选）Ipv4 地址掩码。

【缺省配置】 缺省没有设置直通 ARP 资源。

【命令模式】 全局配置模式。

【缺省级别】 14

【使用指导】 开启 ARP CHECK 功能时，ARP 学习功能受控，用户无法学习到网关等设备的 ARP，此时需要使用本命令来放行指定地址/网段的 ARP 学习。

【配置举例】 1：设置 IP 地址为 172.16.0.1 的网站为直通 ARP 资源。

```
Ruijie(config)# http redirect direct-arp 172.16.0.1
```

【检验方法】 使用 **show web-auth direct-arp** 查看配置的直通 ARP 地址范围

【提示信息】 1：非法 IP/掩码格式。

```
%Error: Invalid IP address.
```

【常见错误】 -

【平台说明】 -

13.11 http redirect direct-site

设置免认证的网络资源范围。

http redirect direct-site { *ipv4-address* [*ip-mask*] [**arp**]| *mac-address* | range *starip-address endip-address*} [description *description-str*] [group *group-name*]

删除免认证的网络资源范围。

No http redirect direct-site { *ipv4-address* [*ip-mask*] | *mac-address* | range *startip-address endip-address* }

【参数说明】

参数	描述
Ipv4-address	免认证网络资源的 Ipv4 地址。
Ip-mask	（可选）免认证网络资源的 Ipv4 地址掩码。
Arp	（可选）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进行 ARP 绑定，需要配置 **arp** 关键字。仅在设置 IPv4 网络资源时需要。
Mac-address	免认证的网络 MAC
Startip-address	连续免认证站点的起始 ip
Endip-address	连续免认证站点的结束 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

【缺省配置】 缺省没有设置免认证的网络资源。

【命令模式】 全局配置模式。

【缺省级别】 14

【使用指导】 启动 Web 认证后，所有用户需先通过 Web 认证，才能访问网络资源。若要开放某些网络资源，未认证用户也可以访问这些开放的网络资源，使用此命令。当某个网站属于免认证的网络资源，那么所有用户都可以访问这个网站。
最多允许配置 50 个免认证的网络资源范围

【配置举例】 1：设置 IP 地址为 172.16.0.1 的网站为免认证访问的网络资源。

```
Ruijie(config)# http redirect direct-site 172.16.0.1
```

2：设置 MAC 地址为 0000:5e00:0101 的目的网站为免认证访问的网络资源。

```
Ruijie(config)# http redirect direct-site 0000:5e00:0101
```

3. 设置连续的免认证网络资源范围为 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】 使用 **show web-auth direct-site [range]**查看配置的免认证网络资源范围

【提示信息】 1：非法 IP/掩码格式。

```
%Error: Invalid IP address.
```

【常见错误】 -

【平台说明】 -

13.12 http redirect port

设置对用户发出的特定目的端口号的 HTTP 的 WEB 请求进行重定向。
http redirect port *port-num*

删除对特定的目的端口号的 HTTP 的 WEB 请求进行重定向。
no http redirect port *port-num*

【参数说明】

参数	描述
port-num	HTTP 的 WEB 请求的目的端口号。

【缺省配置】 缺省拦截用户发出的端口 80 的 HTTP 报文。

【命令模式】 全局配置模式。

【缺省级别】 14

【使用指导】 1、当用户访问网络资源时，此时用户会发出 HTTP 报文，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。
2、缺省情况下，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。
3、要更改设备拦截用户发出的特定端口号的 HTTP 报文，使用此命令。
4、最大允许配置 10 个不同的目的端口号，端口号 80 也含在该总数量范围内。

【配置举例】 1：对用户发出的端口号为 8080 的 HTTP 的 WEB 请求进行重定向。

```
Ruijie(config)# http redirect port 8080
```

2：不对用户发出的端口号为 80 的 HTTP 的 WEB 请求进行重定向。

```
Ruijie(config)# no http redirect port 80
```

【检验方法】 使用 **show web-auth rdpor**t 查看当前端口侦听情况

【提示信息】 1：不允许拦截知名协议端口，比如 23。

```
%Error: Can't set local reserved port(23) as redirection port.
```

【常见错误】 -

【平台说明】 -

13.13 http redirect session-limit

设置全局同一未认证用户的最大 HTTP 会话数，或每个端口下的未认证用户的 HTTP 会话总数。
http redirect session-limit *session-num* [**port** *port-session-num*]

恢复未认证用户的最大 HTTP 会话数。
no http redirect session-limit

【参数说明】

参数	描述
session-num	全局同一未认证用户的最大 HTTP 会话数，取值范围 1-255。
port-session-num	（可选）每个端口下的未认证用户的 HTTP 会话总数，取值范围 1-65535。

【缺省配置】 缺省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。

【命令模式】 全局配置模式。

【缺省级别】 14

【使用指导】 为了防止未认证用户发起 HTTP 攻击，而导致设备的 TCP 连接耗尽，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。

【配置举例】 1：设置未认证用户的最大 HTTP 会话数为 4。

```
Ruijie(config)# http redirect session-limit 4
```

【检验方法】 使用 **show web-auth parameter** 命令查看配置参数

【提示信息】 -

【常见错误】 -

【平台说明】 -

13.14 http redirect timeout

设置维持重定向连接的超时时间。
http redirect timeout *seconds*

恢复维持重定向连接的超时时间为 3 秒。
no http redirect timeout

【参数说明】

参数	描述
seconds	设置维持重定向连接的超时时间；*seconds*，取值范围 1-10。

【缺省配置】 缺省维持重定向连接的超时时间为 3 秒。

【命令模式】 全局配置模式

【缺省级别】 14

【使用指导】 设置维持重定向连接的超时时间。因为三次握手成功后，需要等待用户发出的 HTTP 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。

【配置举例】 1：设置维持重定向连接的超时时间为 4。

```
Ruijie(config)# http redirect timeout 4
```

【检验方法】 使用 **show web-auth parameter** 命令查看配置参数

【提示信息】 -

【常见错误】 -

【平台说明】 -

13.15 ip

要配置 portal 服务器的 IP 地址功能，请执行模板配置模式下的命令 **ip**。
ip { *ip-address* }

清除 HTTP 重定向的 IP 地址。
no ip

【参数说明】

参数	描述
ip-address	portal 服务器的 IPv4 地址。

【缺省配置】 缺省没有设置 portal 服务器的 IP 地址。

【命令模式】 模板配置模式

【缺省级别】 14

【使用指导】

本命令替换原有的 **http redirect** [*ip-address*]命令；原有命令被隐藏实现为兼容命令

【配置举例】 1：指定 eportalv1 模板的 IP 地址为 172.16.0.1。

```
Ruijie(config.tmplt.eportalv1)#ip 172.16.0.1
Ruijie(config.tmplt.eportalv1)#
```

【检验方法】 使用 **show web-auth template** 来查看当前配置的模板参数

【提示信息】 1：不允许直接修改服务器 IP 地址。

```
%Error: Modify portal ip is unsupportted.
```

2：不允许设置非法 IP。

```
%Error: Invalid portal ip address.
```

【常见错误】 -

【平台说明】 -

13.16 ip portal source-interface

指定 portal 通信端口。

ip portal source-interface *interface-type interface-num*

恢复默认配置。

no ip portal source-interface

【参数说明】

参数	描述
interface-type	接口类型
interface-num	接口索引

【缺省配置】 无配置。

【命令模式】 全局配置模式。

【缺省级别】 14

【使用指导】 -

【配置举例】 1：使用聚合口当作 portal 通信端口。

```
Ruijie (config)# ip portal source-interface Aggregateport 1
```

【检验方法】 使用 **show running-config** 来查看当前配置

【提示信息】 -

【常见错误】 -

【平台说明】 -

13.17 iportal nat enable

配置内置 web 认证支持 NAT 功能。

iportal nat enable

恢复默认配置。

no iportal nat enable

【参数说明】

参数	描述

【缺省配置】 无配置。

【命令模式】 全局配置模式。

【缺省级别】 14

【使用指导】 -

【配置举例】 1：开启内置 web 认证支持 NAT 功能。

```
Ruijie (config)# iportal nat enable
```

【检验方法】 使用 **show running-config** 来查看当前配置

【提示信息】 -

【常见错误】 -

【平台说明】 -

13.18 iportal retransmit

配置内置 web 认证 http 连接重传次数。

iportal retransmit *times*

恢复默认配置。

no iportal retransmit

【参数说明】

参数	描述
times	重传次数

【缺省配置】 默认 3 次。

【命令模式】 全局配置模式。

【缺省级别】 14

【使用指导】 -

【配置举例】 1：配置 http 连接重传次数为 5 次。

```
Ruijie (config)# iportal retransmit 5
```

【检验方法】 使用 **show running-config** 来查看当前配置

【提示信息】 -

【常见错误】 -

【平台说明】 -

13.19 iportal service

配置内置 web 认证使用的服务模板。

iportal service [internet *internet-name***] [local** *local-name* **]**

恢复默认配置。

no iportal service [internet *internet-name***] [local** *local-name* **]**

【参数说明】

参数	描述
internet-name	外部服务名称
local-name	本地服务名称

【缺省配置】 无配置。

【命令模式】 全局配置模式。

【缺省级别】 14

【使用指导】 -

【配置举例】 1：配置内置 web 认证本地服务名称。

```
Ruijie (config)# iportal service local local-srv
```

【检验方法】 使用 **show running-config** 来查看当前配置

【提示信息】 -

【常见错误】 -

【平台说明】 -

13.20 iportal user-agent

配置用户 UA 字段对应的终端名称。
iportal user-agent *ua-name* **type mobile** *ua-string*

删除配置。
no iportal user-agent *ua-name* **type mobile** *ua-string*

【参数说明】

参数	描述
ua-name	UA 字段名称
ua-string	UA 字段对应字符串

【缺省配置】 无配置。

【命令模式】 全局配置模式。

【缺省级别】 14

【使用指导】 命令已经无效，采用终端识别功能来实现。

【配置举例】

【检验方法】 -

【提示信息】 -

【常见错误】 -

【平台说明】 -

13.21 login-popup

设置认证前广告地址。
login-popup *url-string*

删除认证前广告地址。
no login-popup

【参数说明】

参数	描述
url-string	广告地址链接。

【缺省配置】 缺省无配置。

【命令模式】 模板配置模式。

【缺省级别】 14

【使用指导】

以 http://或 https://开头。

【配置举例】 1：配置认证前广告页面

```
Ruijie(config.tmplt.iportal)#login-popup http://www.ruijie.com.cn
```

【检验方法】 使用 **show web-auth template** 来查看当前配置的模板参数

【提示信息】 -

【常见错误】 -

【平台说明】 -

13.22 online-popup

设置用户上线弹广告地址。
online-popup *url-string*

删除用户上线弹广告地址。
no online-popup

【参数说明】

参数	描述
url-string	广告地址链接。

【缺省配置】 缺省无配置。

【命令模式】 模板配置模式。

【缺省级别】 14

【使用指导】

以 http://或 https://开头。

【配置举例】 1：配置认证后广告页面

```
Ruijie(config.tmplt.iportal)#online-popup http://www.ruijie.com.cn
```

【检验方法】 使用 **show web-auth template** 来查看当前配置的模板参数

【提示信息】 -

【常见错误】 -

【平台说明】 -

13.23 page-suite

设置内置认证页面包。

page-suite *filename*

删除指定的页面包。

no page-suite

【参数说明】

参数	描述
Filename	页面包的文件名。

【缺省配置】 缺省使用设备自带的页面包。

【命令模式】 模板配置模式。

【缺省级别】 14

【使用指导】

页面包需要提前下载到 FLASH 的 portal/zip 目录。

【配置举例】 1：指定内置页面包

```
Ruijie(config.tmplt.iportal)#page-suite ruijiepage
```

【检验方法】 使用 **show web-auth template** 来查看当前配置的模板参数

【提示信息】 -

【常见错误】 -

【平台说明】 -

13.24 port

设置 portal 服务器的交互端口。
port { *port-num* }

重置服务器端口为默认端口号。
no port

【参数说明】

参数	描述
port	portal 服务器通信端口号，如果是内置认证，该端口是本机监听的 http 端口。

【缺省配置】 缺省端口号为 50100，基于 UDP 协议。

【命令模式】 模板配置模式。

【缺省级别】 14

【使用指导】 -

【配置举例】 -

【检验方法】 使用 **show web-auth template** 来查看当前配置的模板参数

【提示信息】 -

【常见错误】 -

【平台说明】 -

13.25 redirect

设置重定向报文格式。
redirect { ***http*** **|** ***js*** }

恢复默认重定向方式。

no redirect

【参数说明】

参数	描述
http	采用 HTTP 302 协议做 url 跳转。
js	采用 HTTP 200 报文，附带 js 脚本做 url 跳转。

【缺省配置】 缺省锐捷格式采用 js，cmcc 相关格式采用 http。

【命令模式】 模板配置模式。

【缺省级别】 14

【使用指导】 -

【配置举例】 -

【检验方法】 使用 **show web-auth template** 来查看当前配置的模板参数

【提示信息】 -

【常见错误】 -

【平台说明】 -

13.26 show web-auth cgi

显示 CGI 配置。

show web-auth cgi

【参数说明】

参数	描述
-	-

【命令模式】 特权模式

【缺省级别】 14

【使用指导】 用于查看 web 认证的 CGI 配置情况。

【配置举例】 1：显示 CGI 配置。

```
Ruijie# show web-auth cgi
Total 0 cgi items:
```

```
id-string           url-string
---------------     ---------------------------------
```

字段	说明
id-string	CGI 命令对应 ID。
url-string	CGI 命令字符串。

【提示信息】 -

【平台说明】 -

13.27 show web-auth control

显示认证受控配置。

show web-auth control

【参数说明】

参数	描述
-	-

【命令模式】 特权模式

【缺省级别】 14

【使用指导】 -

【配置举例】 1：显示接口上的认证配置和统计信息。

```
Ruijie(config)#show web-auth control
 Port                     Control  Server Name           Online User Count Vlan Control List
 ------------------------ -------- --------------------- ----------------- -----------------
 GigabitEthernet 0/1      On       <not configured>      0                 2-17,19
Ruijie(config)#
```

字段	说明
Port	受控口名称。
Cont□ol	该端口是否打开 Web 认证。
Server Name	端口上自定义的服务器名，<not configured>表示未配置
Online User Count	接口上的在线用户数

【提示信息】 -

【平台说明】 -

13.28 show web-auth direct-arp

显示直通 ARP 范围。

show web-auth direct-arp

【参数说明】

参数	描述
-	-

【命令模式】 特权模式

【缺省级别】 14

【使用指导】 -

【配置举例】 1：显示直通网站配置。

```
Ruijie(config)#show web-auth direct-arp
Direct arps:
  Address         Mask
  --------------- ---------------
  1.1.1.1         255.255.255.255
  2.2.2.2         255.255.255.255
Ruijie(config)#
```

字段	说明
Address	IP 地址。
M□sk	IP 地址掩码。

【提示信息】 -

【平台说明】 -

13.29 show web-auth direct-host

显示免 web 认证的用户范围。

show web-auth direct-host [range]

【参数说明】

参数	描述
-	-

【命令模式】 特权模式

【缺省级别】 14

【使用指导】 使用本命令查看免认证用户配置信息

【配置举例】 1：显示无需认证的用户。

```
Ruijie# show web-auth direct-host
Direct hosts:
  Address          Mask             Port       ARP Binding  Group      Description
  ---------------- ---------------- ---------- ------------ ---------- -------------
  192.168.0.1      255.255.255.255  Gi0/2      On           N/A        N/A
  192.168.4.11     255.255.255.255  Gi0/10     On           N/A        N/A
  192.168.5.0      255.255.255.0    Gi0/16     Off          N/A        N/A
```

字段	说明
Address	无□认证用户的 IP 地址。
Mask	无需认证用户的 IP 地址掩码。
Port	与用户 IP 绑定□设备的端口。
ARP Bin□ing	是否进行 ARP 绑定。
Group	所属的分组
Description	描述信息

2. 显示连续的免认证用户

```
Ruijie# show web-auth direct-host range
Direct host Ranges: 1
  Start Address    End Address      Port       Group        Description
  ---------------- ---------------- ---------- ------------ -----------
  192.168.0.1      192.168.100.1    Gi0/2      N/A          N/A
```

字段	说明
Start Address	连续免认证用户的起始 ip

End Address	连续免认证用户的结束 ip
Port	与用户 IP 绑定□设备的端口。
Group	所属的分组
Description	描述信息

【提示信息】 -

【平台说明】 -

13.30 show web-auth direct-site

显示直通网站范围。

show web-auth direct-site [range]

【参数说明】

参数	描述
-	-

【命令模式】 特权模式

【缺省级别】 14

【使用指导】 -

【配置举例】 1：显示直通网站配置。

```
Ruijie(config)#show web-auth direct-site
Direct sites:
  Address         Mask            ARP Binding Group      Description
  --------------- --------------- ----------- ---------- -------------
  1.1.1.1         255.255.255.255 Off         N/A        N/A
  2.2.2.2         255.255.255.255 On          N/A        N/A
Ruijie(config)#
```

字段	说明
Addres	IP 地址。
Mask	IP 地址掩码。
ARP Binding	是否进行 ARP 绑定。
Group	所属的分组

Description	描述信息

2. 显示直通网站的连续网络配置

```
Ruijie(config)#show web-auth direct-site range
Direct site Ranges: 1
  Start Address   End Address     Group          Description
  --------------- --------------- -------------- -------------
  1.1.1.1         5.5.5.5         N/A            N/A
Ruijie(config)#
```

字段	说明
Start Addres	起始 IP 地址。
End Address	终止 ip 地址
Group	所属的分组
Description	描述信息

【提示信息】 -

【平台说明】 -

13.31 show web-auth global

显示全局 WEB 认证配置信息。

show web-auth global

【参数说明】

参数	描述
-	-

【命令模式】 特权模式

【缺省级别】 14

【使用指导】 用于查看全局 web 认证的基本参数配置情况。

【配置举例】 1：显示全局 WEB 认证配置信息。

```
Ruijie# show web-auth parameter
Webauth.....................................enable
Webauth-type................................external
Customized-pages............................(Not Configured)
```

```
Server-port.....................................8081
Public account..................................disable
Authentication..................................(Not Configured)
Current global template:
    name:.......................................eportalv1
    type:.......................................v1
    Ip:.........................................192.168.197.79
    URL:........................................http://192.168.197.79:8080/eportal/index.jsp
```

字段	说明
Webauth-type	Web 认证类型。
Customized-pages	内置 WEB 认证定制页面信息。
Server-port	内置 WEB 认证服务器监听端口。
Public acc□unt	共享帐号开□状态。
Authenti□ation	认证方法。
Current gl□bal t□mplate	当前全局模板信□。

【提示信息】 -

【平台说明】 -

13.32 show web-auth global authentication

显示全局 WEB 认证方法。

show web-auth global authentication

【参数说明】

参数	描述
-	-

【命令模式】 特权模式

【缺省级别】 14

【使用指导】 用于查看 web 认证的基本参数配置情况。

【配置举例】 1：显示全局 WEB 认证方法。

```
Ruijie# show web-auth global authentication
Webauth.....................................enable
```

```
Authentication.................................(Not Configured)
```

字段	说明
Webauth	WEB 认证开启状态。
Authentication	认证方法。

【提示信息】 -

【平台说明】 -

13.33 show web-auth global customized-pages

显示 WEB 认证定制页面信息。

show web-auth global customized-pages

【参数说明】

参数	描述
-	-

【命令模式】 特权模式

【缺省级别】 14

【使用指导】 用于查看 WEB 认证定制页面信息。

【配置举例】 1：显示 WEB 认证定制页面信息。

```
Ruijie# show web-auth global customized-pages
Webauth.....................................enable
Customized-pages.............................(Not Configured)
```

字段	说明
Webauth	WEB 认证开启状态。
Customized-pages	定制页面信息。

【提示信息】 -

【平台说明】 -

13.34 show web-auth global local-portal

显示内置认证服务器信息。

show web-auth global local-portal

【参数说明】

参数	描述
-	-

【命令模式】 特权模式

【缺省级别】 14

【使用指导】 用于查看内置认证服务器信息。

【配置举例】 1：显示内置认证服务器信息。

```
Ruijie# show web-auth global local-portal
Webauth.....................................enable
Server-port.................................8081
Public account..............................disable
```

字段	说明
Webauth	WEB 认证开启状态。
Server-port	服务器监听端口。
Public account	共享帐号开启状态。

【提示信息】 -

【平台说明】 -

13.35 show web-auth global template

显示全局 web 认证模板信息。

show web-auth global template

【参数说明】

参数	描述
-	-

【命令模式】 特权模式

【缺省级别】 14

【使用指导】 用于查看全局 web 认证模板信息。

【配置举例】 1：显示全局 web 认证模板信息。

```
Ruijie# show web-auth global template
Webauth.....................................enable
Current global template:
    name:...................................eportalv1
    type:...................................v1
    Ip:.....................................192.168.197.79
    URL:....................................http://192.168.197.79:8080/eportal/index.jsp
```

字段	说明
Webauth	WEB 认证开启状态。
Current global template	当前全局模板信息。

【提示信息】 -

【平台说明】 -

13.36 show web-auth global webauth-type

显示全局 web 认证类型。

show web-auth global webauth-type

【参数说明】

参数	描述
-	-

【命令模式】 特权模式

【缺省级别】 14

【使用指导】 用于查看全局 web 认证类型。

【配置举例】 1：显示全局 web 认证类型。

```
Ruijie# show web-auth global webauth-type
Webauth.....................................enable
Webauth-type................................external
```

字段	说明
Webauth	WEB 认证开启状态。
Webauth-type	WEB 认证类型。

【提示信息】 -

【平台说明】 -

13.37 show web-auth info

查看 WEB 认证配置信息。

show web-auth info

【参数说明】

参数	描述
-	-

【命令模式】 特权模式

【缺省级别】 14

【使用指导】 用于查看 WEB 认证配置信息。

【配置举例】 1：显示 WEB 认证配置信息。

```
Ruijie# show web-auth cgi
web-auth info:
    Update interval: 180
    User mode: ip
    Portal key: ruijie
```

字段	说明
Update interval	用户信息更新周期。
User mode	绑定用户模式。
Portal key	Portal 通信密钥。

【提示信息】 -

【平台说明】 -

13.38 show web-auth ip-mapping

显示配置的服务器和用户的映射关系

show web-auth ip-mapping

【参数说明】

参数	描述

【缺省配置】 无配置。

【命令模式】 特权模式

【缺省级别】 14

【使用指导】

【配置举例】 1：配置映射关系

```
Ruijie(config)#show web-auth ip-mapping
------------------------------------------------------------
  Name:       iportal
  Ip:         0.0.0.0
  Url:
  Ip-Mapping:
------------------------------------------------------------
  Name:       eportalv1
  Ip:         172.18.105.9
  Url:        http://172.18.105.9:8080/eportal/index.jsp
  Ip-Mapping:
              1.1.1.0-255.255.255.0           GlobalRuijie(config)#
```

【检验方法】

【提示信息】 -

【常见错误】 -

【平台说明】 -

13.39 show web-auth local-portal

内置 web 认证信息。

show web-auth local-portal

【参数说明】

参数	描述
-	-

【命令模式】 特权模式

【缺省级别】 14

【使用指导】 用于查看内置 web 认证信息。

【配置举例】 1：显示内置 web 认证信息。

```
Ruijie# show web-auth local-portal
Local web-auth info:
    Server-port:                8081
    AAA method-list:            (Not Configured)
    Public account:             disable
```

字段	说明
Server-port	内置 WEB 认证监听服务器端口信息。
AAA method-list	AAA 方法列表。
Public account	共享帐号功能状态。

【提示信息】 -

【平台说明】 -

13.40 show web-auth parameter

显示 HTTP 重定向的配置。

show web-auth parameter

【参数说明】

参数	描述
-	-

【命令模式】 特权模式

【缺省级别】 14

【使用指导】 用于查看 web 认证的基本参数配置情况。

【配置举例】 1：显示 HTTP 重定向的配置。

```
Ruijie# show web-auth parameter
  session-limit: 10
  timeout:         5
```

字段	说明
session-limit	同一未认证用户的最大 HTTP 会话数。
timeout	维持重定向连接的超时时间。

【提示信息】 -

【平台说明】 -

13.41 show web-auth portal-check

显示配置的 portal-check 参数信息

show web-auth portal-check

【参数说明】

参数	描述

【缺省配置】 无配置。

【命令模式】 特权模式

【缺省级别】 14

【使用指导】

【配置举例】 1：配置 portal-check 功能:

```
Ruijie#sh web portal-check
Check:         Enable
  Interval:    3s
  Timeout:     5s
  Retransmit:  3
```

```
Escape:        Enable
Nokick:        Disable
```

【检验方法】

【提示信息】 -

【常见错误】 -

【平台说明】 -

13.42 show web-auth rdport

显示 TCP 拦截端口。

show web-auth rdport

【参数说明】

参数	描述
-	-

【命令模式】 特权模式

【缺省级别】 14

【使用指导】 -

【配置举例】 1：显示 TCP 拦截端口配置。

```
Ruijie#show web-auth  rdport
Rd-Port:
80 443
Ruijie#
```

【提示信息】 -

【平台说明】 -

13.43 show web-auth syslog ip

查询用户的上下记录

show web-auth syslog ip *ip-address*

【参数说明】

参数	描述
Ip-address	根据用户的 ip 查询

【命令模式】 特权模式

【缺省级别】 14

【使用指导】 使用本命令查询用户上下线记录，限制说明：该命令不支持热备后原有数据的保存。

【配置举例】 1：显示用户上下线记录。

```
Ruijie#show web-auth syslog ip 192.168.197.35
Address: 192.168.197.35  Core-index 0 Current index 2
Index:            0
 Time:             2015-10-16 20:37:34
 Behavior:         ONLINE
 Mac:              00d0.f822.33e7
 Vid:              101
 Port:             Gi3/1
 Timeused:         0d 00:00:00
 Flow_up:          0
 Flow_down:        0

 Index:            1
 Time:             2015-10-16 20:42:08
 Behavior:         OFFLINE
 Mac:              00d0.f822.33e7
 Vid:              101
 Port:             Gi3/1
 Timeused:         0d 00:04:27
 Flow_up:          2107872
 Flow_down:        2108224
```

字段	说明
Index	记录编号
Time	记录发生的时间
Behavior	动作，代表上线或者下线
MAC	用户 mac
Vid	用户 vid

Port	用户端口
Timeused	上线时间
Flow UP	用户上行流量
Flow down	用户下行流量

【提示信息】 -

【平台说明】 -

13.44 show web-auth template

显示 portal 服务器配置。

show web-auth template

【参数说明】

参数	描述
-	-

【命令模式】 特权模式

【缺省级别】 14

【使用指导】 使用本命令查看服务器配置信息

【配置举例】 1：显示无需认证的用户。

```
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
```

字段	说明
Name	模板名称
Url	服务器主页地址
Ip	服务器 IP 地址
Type	服务器类型。一代 portal 服务器为 v1，二代为 v2，内置为 intra

Port	服务器协议报文通信端口，仅二代 portal 服务器存在
Acctmlist	记账方法列表名，仅二代和内置认证存在
Authmlist	认证方法列表名，仅二代和内置认证存在

【提示信息】 -

【平台说明】 -

13.45 show web-auth user

显示所有用户或是指定用户的在线信息，包括用户 IP 地址、接口、在线时间等信息。

show web-auth user { **all** | **ip** *ip-address* | **mac** *mac-address* | **name** *name-string* | **session-id** *num* | **escape**}

【参数说明】

参数	描述
ip-address	指定用户的 IPv4 地址。
mac-address	指定用户的 MAC 地址
name-string	指定用户名
num	指定用户的 AAA 会话 ID

【命令模式】 特权模式。

【缺省级别】 14

【使用指导】

escape 只在微信连 wifi 的使用场景支持，用于显示逃生用户表项

【配置举例】 1：显示 web 认证全局配置和统计信息。

```
Ruijie# show web-auth user all
Current user num :  4, online 2

Address           Online   Time Limit     Time Used    Status  Name
--------------- -------  ------------ -------------- -------- ---------
192.168.0.11    On       0d 01:00:00   0d 00:15:10    Active
192.168.0.13    On       0d 01:00:00   0d 00:00:59    Active   111
192.168.0.25    Off      0d 01:00:00   0d 00:00:59    Create
192.168.0.46    Off      0d 01:00:00   0d 01:00:00    Destroy  222

Ruijie# show web-auth user ip 192.168.0.11
Address       :   192.168.0.11
```

```
Mac             :   00d0.f800.2233
Port            :   Gi0/2
Online          :   On
Time Limit      :   0d 01:00:00
Time Used       :   0d 00:15:10
Time Start      :   2009-02-22 20:05:10
Status          :   Active
```

字段	说明
Address	用户的 IP 地址。
Mac	用户的 MAC 地址。
Port	用户连接的设备的端口。
Online	用户是否在线。
Time Limit	用户的可用时长限制，0 表示无限制。
Time Used	用户已经在线时间。
Time Start	用户认证通过、开始上线的时间。
Status	用户状态，Active 表示用户正常在线，Create 表示用户刚被创建、还未完成设置，Destroy 表示用户刚被删除、暂未完成清除设置。
Name	用户名，一代认证用户设备无法显示用户名，该列为空

【提示信息】 -

【平台说明】 -

13.46 time-interval

设置内置认证广告弹出时间间隔。
time-interval *{ hour }*

恢复默认时间间隔。
no time-interval

【参数说明】

参数	描述
hour	广告弹出时间间隔，默认 1 小时，取值范围为 0-24。

【缺省配置】 缺省 1 小时。

【命令模式】 模板配置模式。

【缺省级别】 14

【使用指导】

配置成 0，表示关闭时间周期检测。

【配置举例】 1：配置广告弹出时间间隔为 2 小时

```
Ruijie(config.tmplt.iportal)#time-interval 2
```

【检验方法】 使用 **show web-auth template** 来查看当前配置的模板参数

【提示信息】 -

【常见错误】 -

【平台说明】 -

13.47 url

设置 portal 服务器的页面地址。
url *url-string*

删除认证页面的主页地址。
no url

【参数说明】

参数	描述
url-string	页面地址，应以“http://”或“https://”开头，否则提示配置不成功，最大长度为 255 个字符。

【缺省配置】 一代，二代，内置认证缺省没有设置 portal 服务器的页面地址。
微信连 wifi 模板下缺省配置为与 mcp/wmc 服务器使用微信与短信认证共存时的跳转地址

【命令模式】 模板配置模式。

【缺省级别】 14

【使用指导】

本命令替换原有的 **http redirect homepage** [*url-string*]命令；原有命令被隐藏实现为兼容命令。

url 不配置的话会采用默认格式：http://[ip-address]，[ip-address]为通过 IP 命令配置的服务器 IP 地址。

【配置举例】 1：指定 eportalv1 模板的页面地址为 “http://www.web-auth.net/login”。

```
Ruijie(config.tmplt.eportalv1)#url http://www.web-auth.net/login
```

【检验方法】 使用 **show web-auth template** 来查看当前配置的模板参数

【提示信息】 1、非法 URL 格式。

```
%Error: Invalid homepage URL.
```

【常见错误】 -

【平台说明】 -

13.48 web-auth accout-share ip-limit

对内置使用 local 认证，开启账号共享功能，此时可以限制账号登陆的用户个数。

web-auth account-share ip-limit {limit-num}

删除配置。

no web-auth account-share

【参数说明】

参数	描述
Limit-num	限制同名账号的上线个数

【缺省配置】 无配置。

【命令模式】 Config 配置模式

【缺省级别】 14

【使用指导】

【配置举例】 1：配置 limit 参数。

```
Ruijie (config)# web-auth account-share ip-limit {limit-num}
```

【检验方法】 使用 **show running-config** 来查看当前配置

【提示信息】 -

【常见错误】 -

【平台说明】 -

13.49 web-auth acl

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。

web-auth acl { **black-ip** *ip*|**black-port** *port* | **black-url** *name* | **white-url** *name* }

删除配置。

no web-auth acl { **black-ip** *ip* | **black-port** *port* **| black-url** *name* **| white-url** *name* }

【参数说明】

参数	描述
ip	黑名单 ip 地址。
port	黑名单端口，取值范围 1-65535
name	黑名单/白名单的 URL。

【缺省配置】 无。

【命令模式】 全局配置模式。无线上还支持 wlansec 模式。

【缺省级别】 14

【使用指导】

【配置举例】 1：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】 使用 **show running-config** 来查看当前配置

【提示信息】 -

【常见错误】 -

【平台说明】 -

13.50 web-auth customized-logo enable

配置开启内置 portal 的 logo 替换功能

web-auth customized-logo enable

删除配置。

no web-auth customized-logo

【参数说明】

参数	描述
-	-

【缺省配置】 -

【命令模式】 全局配置模式。

【缺省级别】 14

【使用指导】 -

【配置举例】 1：配置开启内置 portal 的 logo 替换功能

```
Ruijie (config)# web customized-logo enable
```

【检验方法】 使用 **show running-config** 来查看当前配置

【提示信息】 -

【常见错误】 -

13.51 web-auth direct-host

设置无需认证用户 IP/MAC 范围。

web-auth direct-host { *ipv4-address* [i*p-mask*] [**arp**] | *mac-address* | range *starip-address endip-address* } [**port** *interface-name*] [description *description-str*] [group *group-name*]

取消无需认证用户。

no web-auth direct-host { *ipv4-address* [i*p-mask*] | *mac-address* | range *starip-address endip-address* }

【参数说明】

参数	描述
Ipv4-address	无需认证用户的 IPv4 地址。
ip-mask	（可选）无需认证用户的 IPv4 地址掩码。
port *interface-name*	（可选）将用户 IP 与设备的端口进行绑定。
arp	（可选）如果设备启用了 ARP CHECK 功能，那么需要对免认证的用户 IP 范围进行 ARP 绑定，需要配置 **arp** 关键字。仅在设置 IPv4 地址时需要。
mac-address	无需认证用户的 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	免认证用户所属的组
Description-str	免认证用户的描述信息

【缺省配置】 缺省没有设置无需认证用户，所有用户都必须先通过 Web 认证，才能访问受限的网络资源。

【命令模式】 全局配置模式。

【缺省级别】 14

【使用指导】 设置用户为无需认证的用户，那么该用户不需要进行 Web 认证，也可以访问所有可达的网络资源。
最大允许 50 个无需认证用户网络范围。

【配置举例】 1：设置 IP 地址为 172.16.0.1 的用户为无需认证用户。

```
Ruijie(config)# web-auth direct-host 172.16.0.1
```

2：设置 IP 地址为 FF02::/64 的用户为无需认证用户。

```
Ruijie(config)# web-auth direct-host FF02::/64
```

3：设置 MAC 地址为 0000:5e00:0101 的用户为无需认证用户。

```
Ruijie(config)# web-auth direct-host 0000:5e00:0101
```

4. 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】 使用 **show web-auth direct-host [range]**命令查看配置参数

【提示信息】 1：非法 IP/掩码格式

```
%Error: Invalid IP address.
```

【常见错误】 -

【平台说明】 -

13.52 web-auth enable

在端口上启动 Web 认证。兼容原 **web-auth port-control** 命令
web-auth enable

在端口上关闭 Web 认证。
no web-auth enable

【参数说明】

参数	描述
-	-

【缺省配置】 缺省在端口上关闭 Web 认证。

缺省使用 **eportalv1** 模板

【命令模式】 接口配置模式。

【缺省级别】 14

【使用指导】 要成功应用 Web 认证功能，必须配置认证页面的主页地址。
由于将模板的应用集成到受控开关，原有未开启认证的接口上的模板/服务器应用配置将被自动清除。
兼容实现原全局应用模板/服务器功能。

【配置举例】 1：在端口 gigabitEthernet 0/14 上启动 Web 认证。

```
Ruijie(config)# interface GigabitEthernet 0/14
Ruijie(config-if-GigabitEthernet 0/14)# web-auth enable
```

【检验方法】 通过 **show web-auth control** 查看受控口配置信息

【提示信息】 -

【常见错误】 -

【平台说明】 -

13.53 web-auth group

配置组信息
web-auth group *group-name* [description *description-str*]

删除配置。
no web-auth group *group-name*

【参数说明】

参数	描述
Group-name	创建的组名
Description-str	组的描述信息

【缺省配置】 -

【命令模式】 Config 配置模式

【缺省级别】 14

【使用指导】

【配置举例】 1：创建组信息

```
Ruijie (config)# web-auth group group-1 [description DESC]
```

【检验方法】 使用 **show running-config** 来查看当前配置

【提示信息】 -

【常见错误】 -

【平台说明】 -

13.54 web-auth logging enable

启用 Web 认证 SYSLOG 功能。

web-auth logging enable { *num* }

关闭该功能。

no web-auth logging enable

【参数说明】

参数	描述
num	SYSLOG 打印速率，每秒钟打印的 SYSLOG 条数。范围[0, 65535]，0 为不限制

【缺省配置】 缺省为关闭 web 认证 SYSLOG 功能。

【命令模式】 全局配置模式。

【缺省级别】 14

【使用指导】 该命令仅限制模块正常情况下打印的 SYSLOG，异常或严重的 SYSLOG 不受限制。

【配置举例】 1：配置模块 SYSLOG 打印不限速。

```
Ruijie(config)# web-auth logging enable 0
```

【检验方法】 通过 **show running-config** 查看配置信息

【提示信息】 -

【常见错误】 -

【平台说明】 -

13.55 web-auth portal

指定认证使用的 Portal 服务器（交换/EG 平台支持配置不同网段用户使用不同的 Portal 服务器）。

web-auth portal { eportalv1 | iportal | *name* **}[ip-mapping** *ipv4 mask***]**

删除配置。

no web-auth portal { eportalv1 | iportal | *name* **}[ip-mapping** *ipv4 mask***]**

【参数说明】

参数	描述
name	指定的模板名称
ipv4	映射用户的 ip 网段
mask	映射用户的 ip 掩码

【缺省配置】 默认无配置。

【命令模式】 全局配置模式。

【缺省级别】 14

【使用指导】 -

【配置举例】 1：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】 使用 **show running-config** 来查看当前配置

【提示信息】 -

【常见错误】 -

【平台说明】 -

13.56 web-auth portal key

设置设备与认证服务器之间进行通信的密钥。

web-auth portal key *key-string*

清除用户的 HTTP 的 WEB 请求被重定向后的新的 WEB 请求与认证服务器进行通信的密钥。
no web-auth portal key

【参数说明】

参数	描述
key-string	设备与认证服务器之间进行通信的密钥，最大长度为 255 个字符。

【缺省配置】 缺省没有设置密钥。

【命令模式】 全局配置模式。

【缺省级别】 14

【使用指导】 要成功应用 Web 认证功能，必须设置设备与认证服务器之间进行通信的密钥。
当前服务器密钥仅支持全局配置，不支持为每个独立服务器指定密钥。

【配置举例】 1：设置设备与认证服务器之间进行通信的密钥为 *web-auth*。

```
Ruijie(config)# web-auth portal key web-auth
```

【检验方法】 通过 **show running-config** 查看服务器密钥配置

【提示信息】 -

【常见错误】 -

【平台说明】 -

13.57 web-auth portal-check

检测 portal 服务器是否可用。
web-auth portal-check [**interval** *intsec*] [**timeout** *tosec*] [**retransmit** *retires*]

恢复默认配置。
no web-auth porta-check

【参数说明】

参数	描述
intsec	检测周期，默认 10 秒，取值范围 1-1000。
tosec	报文超时时间，默认 5 秒，取值范围 1-1000。
retries	超时重传次数，默认 3 次，取值范围 1-100。

【缺省配置】 关闭 portal 检测。

【命令模式】 全局配置模式。

【缺省级别】 14

【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】 1：配置 portal 检测。

```
Ruijie (config)# web-auth portal-check interval 20 timeout 2 retransmit 2
```

【检验方法】 使用 **show running-config** 来查看当前配置

【提示信息】 -

【常见错误】 -

【平台说明】 -

13.58 web-auth portal-escape

配置 portal 逃生，当配置的 portal 服务器都不可用时，新接入网络的用户免认证。
web-auth portal-escape

恢复默认配置。
no web-auth portal-escape

【参数说明】

参数	描述

【缺省配置】 关闭。

【命令模式】 全局配置模式。

【缺省级别】 14

【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】 1：配置 portal 逃生

```
Ruijie (config)# web-auth portal-escape
```

【检验方法】 使用 **show running-config** 来查看当前配置

【提示信息】 -

【常见错误】 -

【平台说明】 -

13.59 web-auth template

创建并进入默认一代认证模板配置模式。
web-auth template eportalv1

创建并进入自定义一代认证模板配置模式。
web-auth template { template-name } **v1**

创建并进入默认二代认证模板配置模式。
web-auth template eportalv2

创建并进入自定义二代认证模板配置模式。
web-auth template { *template-name* } **v2**

【参数说明】

参数	描述
eportalv1	默认的一代认证模板
eportalv2	默认的二代认证模板
iportal	默认的内置认证模板
template-name	自定义的认证模板名称

【缺省配置】 无服务器配置

【命令模式】 全局配置模式。

【缺省级别】 14

【使用指导】

通过进入 eportalv1 模板模式进行 ip 和 url 的配置，来替换原有的 **http redirect** 和 **http redirect homepage** 命令，同时设备需要兼容原有 **http redirect** 和 **http redirect homepage** 命令配置方式，内部自动转换为本命令格式。

兼容原有的 **portal-server** 命令配置方式，自动转为新的命令。

要成功应用 Web 认证功能，必须配置一个可用的 portal 服务器，并应用该 portal 服务器；默认 eportalv1 模板会被系统默认应用；eportalv1 模板通常包含 IP 地址和 url 和通讯密钥需要进行设置，url 不配置的话会采用默认格式：http://*[ip-address]*。portal 服务器的 IP 地址也是一个免认证的网络资源，未认证用户也可以访问，但为了防止被攻击，设备对用户访问该 IP 的上行流量进行了限制，具体的限制值上限与设备的物理端口数成正比。

【配置举例】 1：配置 eportalv1 模板。

```
Ruijie(config)# web-auth template eportalv1
Ruijie(config.tmplt.eportalv1)#
```

【检验方法】 使用 **show web-auth template** 来查看当前配置成功的模板

【提示信息】 1、不允许变更模板类型

```
%Notice: Template has been created, it is a v2 template.
```

【常见错误】 -

【平台说明】 -

13.60 web-auth update-interval

配置在线用户更新时间间隔。
web-auth update-interval {seconds}

恢复默认配置。
no web-auth update-interval

【参数说明】

参数	描述
seconds	信息更新时间间隔，单位为秒。取值范围 30-3600。默认为 180 秒。

【缺省配置】 180 秒。

【命令模式】 全局配置模式。

【缺省级别】 14

【使用指导】 -

【配置举例】 1：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】 使用 **show running-config** 来查看当前配置

【提示信息】 -

【常见错误】 -

【平台说明】 -

14 全局 IP+MAC 绑定

14.1 address-bind

设置全局 IP+MAC 地址绑定。

address-bind { *ip-address* | *ipv6-address* } *mac-address*

删掉全局 IP+MAC 地址绑定。

no address-bind { *ip-address* | *ipv6-address* } *mac-address*

【参数说明】

参数	描述
ip-address	绑定的 IPv4 地址
ipv6-address	绑定的 IPv6 地址
mac-address	绑定的 MAC 地址

【缺省配置】 无

【命令模式】 全局配置模式

【缺省级别】 14

【使用指导】 -

【配置举例】 1：下面的例子是全局配置 IPv4+MAC 地址绑定：

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

【检验方法】 1：使用 **show run** 或者 **show address-bind** 命令查看

【提示信息】 -

【常见错误】 -

【平台说明】 -

14.2 address-bind binding-filter logging

配置打开绑定过滤日志。
address-bind binding-filter logging [**rate-limit** *rate*]

配置关闭绑定过滤日志。
no address-bind binding-filter logging

【参数说明】

参数	描述
rate-limit *rate*	全局 IPv4+MAC 绑定过滤日志打印速率，默认每分钟 10 条日志，可配置范围为每分钟 1-120 条

【缺省配置】 关闭绑定过滤日志

【命令模式】 全局配置模式

【缺省级别】 14

【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】 配置打开绑定过滤日志：

```
Ruijie# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Ruijie(config)# address-bind binding-filter logging
Ruijie(config)# end
```

【检验方法】 1：使用 **show run** 命令查看。

【提示信息】 -

【常见错误】 -

【平台说明】 -

14.3 address-bind install

全局地址绑定功能开启
address-bind install

关闭地址绑定功能

no address-bind install

【参数说明】

参数	描述
-	-

【缺省配置】 不开启地址绑定功能。

【命令模式】 全局配置模式

【缺省级别】 14

【使用指导】 开启后全局 IPv4+MAC 地址绑定生效，开始控制 IPv4 或者 IPv6 报文的转发。

【配置举例】 1：下面是设置端口 gigabitethernet 1/1 所有安全地址的老化时间为 8 分钟：

```
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】 1：使用 **show run** 命令查看。

【提示信息】 -

【常见错误】 -

【平台说明】 -

14.4 address-bind ipv6-mode

改变 IPv6 地址绑定模式

address-bind ipv6-mode { **compatible** | **loose** | **strict** }

恢复默认模式

no address-bind ipv6-mode

【参数说明】

参数	描述
compatible	兼容模式
loose	宽松模式
strict	严格模式

【缺省配置】 严格模式

【命令模式】 全局配置模式

【缺省级别】 14

【使用指导】 -

【配置举例】 1：改变 IPv6 地址绑定模式：

```
Ruijie# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Ruijie(config)# address-bind ipv6-mode compatible
```

【检验方法】 使用 **show run** 命令可以查看。

【提示信息】 -

【常见错误】 -

【平台说明】 -

14.5 address-bind uplink

配置地址绑定例外端口
address-bind uplink *interface-id*

恢复默认模式
no address-bind uplink *interface-id*

【参数说明】

参数	描述
interface-id	交换口或者 L2AP 口

【缺省配置】 所有端口均为非例外口

【命令模式】 全局配置模式

【缺省级别】 14

【使用指导】 -

【配置举例】 1：改变 IPv6 地址绑定模式：

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

【检验方法】 使用 **show run** 或者 **show address-bind uplink** 命令可以查看。

【提示信息】 -

【常见错误】 -

【平台说明】 -

14.6 show address-bind

显示配置的全局 IPv4+MAC 地址绑定。

show address-bind

【参数说明】

参数	描述
-	-

【命令模式】 特权模式

【缺省级别】 14

【使用指导】 -

【配置举例】 1：下面的例子显示的是全局 IPv4+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
```

字段解释：

字段	说明
Total Bind Addresses in System	当前设备上配置的全局 IPv4+MAC 地址绑定个数
IP Address	绑定的 IP 地址
Binding MAC Addr	绑定的 MAC 地址

【提示信息】 -

【平台说明】 -

14.7 show address-bind uplink

显示配置的地址绑定例外端口。

show address-bind uplink

【参数说明】

参数	描述
-	-

【命令模式】 特权模式

【缺省级别】 14

【使用指导】 -

【配置举例】 1：下面的例子显示的是地址绑定例外端口

```
Ruijie#show address-bind uplink
Port       State
---------- ---------
Gi0/1      Enabled
Default    Disabled
```

字段解释：

字段	说明
Port	例外端口简称，默认所有端口为非例外端口
State	是否为例外端口，Enabled 表示例外端口，Disabled 表示非例外端口

【提示信息】 -

【平台说明】 -

15 IPoE

15.1 clear ipoe-auth user

清除 IPv4 IPoE 认证用户，强制用户下线

clear ipoe-auth user { **all** | **ip** *ip-address* | **mac** *mac-address* }

【参数说明】

参数	描述
ip-address	指定 IP 地址
mac-address	指定源 MAC 地址

【缺省配置】 无缺省行为

【命令模式】 特权用户模式

【缺省级别】 14

【使用指导】 清除 IPv4 IPoE 认证用户，强制用户下线。

【配置举例】 1：清除所有 IPv4 IPoE 认证用户。

```
Ruijie# clear ipoe-auth user all
```

【检验方法】 1：执行 **show ipoe-auth summary** 命令，看不到任何用户表项。

【提示信息】 -

【常见错误】 -

【平台说明】 -

15.2 ipoe-auth enable

使能 IPv4 IPoE 功能

ipoe-auth enable

恢复缺省情况

no ipoe-auth enable

【参数说明】

参数	描述

-	-

【缺省配置】 IPv4 IPoE 功能处于关闭状态。

【命令模式】 全局模式

【缺省级别】 14

【使用指导】 只有使能了 IPv4 IPoE 功能后，其它的 IPv4 IPoE 相关配置才能生效。

【配置举例】 1：使能 IPv4 IPoE 功能。

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

【检验方法】 1：使用 **show running-config** 命令，可以查看是否配置成功。

【提示信息】 -

【常见错误】 -

【平台说明】 -

15.3 ipoe-auth quiet-period

配置 IPv4 IPoE 认证用户的静默时间
ipoe-auth quiet-period *time*

恢复缺省情况
no ipoe-auth quiet-period

【参数说明】

参数	描述
time	静默时间，输入范围 0～65535，单位：秒，不输入默认为 10

【缺省配置】 IPv4 IPoE 认证用户的静默时间默认为 10 秒。

【命令模式】 全局模式

【缺省级别】 14

【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。静默期后，如果设备再次收到该用户的报文，则依然可以对其进行认证处理。

【配置举例】 1：在全局上配置 IPv4 IPoE 认证用户的静默时间为 100 秒。

```
Ruijie#configure
Enter configuration commands, one per line.  End with CNTL/Z.
Ruijie(config)# ipoe-auth quiet-period 100
```

【检验方法】 1：使用 **show running-config** 命令，可以查看是否配置成功。

【提示信息】 -

【常见错误】 -

【平台说明】 -

15.4 ipoe-auth server-timeout

配置 IPv4 IPoE 认证超时时间
ipoe-auth server-timeout *time*

恢复缺省情况
no ipoe-auth server-timeout

【参数说明】

参数	描述
time	认证超时时间，输入范围 1～65535，单位：秒，不输入默认为 30

【缺省配置】 IPv4 IPoE 认证超时时间默认为 30 秒。

【命令模式】 全局模式

【缺省级别】 14

【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】 1：在全局上配置 IPv4 IPoE 认证超时时间为 30 秒。

```
Ruijie#configure
Enter configuration commands, one per line.  End with CNTL/Z.
Ruijie(config)# ipoe-auth server-timeout 100
```

【检验方法】 1：使用 **show running-config** 命令，可以查看是否配置成功。

【提示信息】 -

【常见错误】 -

【平台说明】 -

15.5 ipoe-auth user-limit

配置允许的 IPv4 IPoE 认证用户的最大数
ipoe-auth user-limit *number*

恢复缺省情况
no ipoe-auth user-limit

【参数说明】

参数	描述
number	IPoE 认证最大用户数，输入范围 1～1000000，不输入默认为 0，表示不做限制

【缺省配置】 未限制 IPv4 IPoE 认证用户数目。

【命令模式】 全局模式

【缺省级别】 14

【使用指导】 创建的 IPv4 IPoE 认证用户数目达到最大值后，后续用户上线将不能进行 IPoE 认证用户。

【配置举例】 1：配置允许创建的 IPv4 IPoE 认证用户最大数为 100。

```
Ruijie#configure
Enter configuration commands, one per line.  End with CNTL/Z.
Ruijie(config)# ipoe-auth user-limit 100
```

【检验方法】 1：使用 **show running-config** 命令，可以查看是否配置成功。

【提示信息】 -

【常见错误】 -

【平台说明】 -

15.6 show ipoe-auth summary

查看 IPv4 IPoE 认证用户的相关信息。

show ipoe-auth summary

【参数说明】

参数	描述
-	-

【命令模式】 特权模式、全局模式、接口模式

【缺省级别】 14

【使用指导】 显示 IPv4 IPoE 认证用户的统计信息。

【配置举例】 1：在特权模式下查看 IPv4 IPoE 认证用户的统计信息。

```
Ruijie#show ipoe-authe summary

ID       User       MAC             Interface VLAN INNER-VLAN Auth-State      Backend-State
Port-Status User-Type Time

-------- ---------- --------------  --------- ---- ---------- ---------------- -------------
---------- --------- ------------------
```

字段解释：

字段	说明
ID	从 AAA 获取的 ID，可使用 show aaa user all 命令对照查看
User	用户名
MAC	认证终端的 mac 地址
Interface	认证终端所在端口
VLAN	认证终端所在 vlan id
INNER-VLAN	认证终端所在的内层 vlan id，支持认证用户双层 tag 的设备上支持该字段
Auth-State	认证状态机状态
Backend-State	认证状态机状态
Port-State	端口认证状态
User-Type	认证类型
Time	在线时间

【提示信息】 -

【平台说明】 -

15.7 show ipoe-auth user

查看动态触发的 IPv4 IPoE 认证用户信息。

show ipoe-auth user [**mac** *mac-address*] [**username** *name*]

【参数说明】

参数	描述
mac-address	源 MAC 地址
name	用户名

【命令模式】 特权模式、全局模式、接口模式

【缺省级别】 14

【使用指导】 显示动态触发的 IPv4 IPoE 认证用户信息。

【配置举例】 1：在特权模式下查看动态触发的 IPv4 IPoE 认证用户信息。

```
Ruijie# show ipoe-auth user mac 0000.0000.0001
User name: 000000000001
User id: 150994945
Type: static
Mac address is 0000.0000.0001
Vlan id is 10
Access from port Gi4/8
Time online: 0days 0h 0m20s
User ip address is 192.168.197.159
Max user number on this port is 10
Authorization session time is 20736000 seconds
Start accounting
```

字段解释：

字段	说明
User name	用户名称
Type	用户类型
Mac address	用户的 mac 地址
Vlan id	用户的 vlan id
Access from port	用户所在的端口
Time online	用户在线时间

User ip address	用户的 IP 地址
Max user number on this port	该端口的最大用户数
Authorization session time	该用户的授权时间

【提示信息】 -

【平台说明】 -

16 IP-GROUP

16.1 description

配置 ip-group 组的说明。
description [*name*]

删除 ip-group 组的说明
no description

【参数说明】

参数	描述
name	说明字符串，最大支持 32 个字符，中间不能有空格

【缺省配置】 缺省情况下没有配置说明字段

【命令模式】 ip-group 配置模式

【缺省级别】 14

【使用指导】 无。

【配置举例】 1：配置 ip-group 组的说明字段。

```
Ruijie(config-ip-group)#description test
```

2：清除 ip-group 组的说明。

```
Ruijie(config-ip-group)#no description
```

【校验方法】 使用 **show ip-group** [*id*]命令，可以查看整个 ip-group 组的配置。

【提示信息】 -

【平台说明】 -

16.2 ip-group

配置 ip-group 组。
ip-group *id*

删除 ip-group 组。
no ip-group *id*

【参数说明】

参数	描述
id	ip-group 组的索引，范围是 1-1000

【缺省配置】 未配置 ip-group 组

【命令模式】 全局模式

【缺省级别】 14

【使用指导】 无

【配置举例】 1：配置 ip-group 组。

```
Ruijie(config)#ip-group 1
```

2：删除 ip-group 组。

```
Ruijie(config)# no ip-group 1
```

【检验方法】 使用 **show ip-group** [*id*]命令，可以查看整个 ip-group 组的配置。

【提示信息】 -

【常见错误】 -

【平台说明】 -

16.3 ip-range

配置 ip 地址范围。
ip-range *start* [*end*]

删除 ip 地址范围。
no ip-range *start* [*end*]

【参数说明】

参数	描述
start	ip range 起始地址
end	ip range 结束地址，没有配置 end 该值默认为 start

【缺省配置】 缺省情况下没有配置 ip-range 范围

【命令模式】 ip-group 配置模式

【缺省级别】 14

【使用指导】 无

【配置举例】 1：配置 ip-range 的地址范围是 1.1.1.1 到 1.1.1.10。

```
Ruijie(config-ip-group)#p-range 1.1.1.2 1.1.1.10
```

2：删除 ip-range 的地址范围配置。

```
Ruijie(config-ip-group)#no ip-range 1.1.1.2 1.1.1.10
```

【检验方法】 使用 **show ip-group** [*id*]命令，可以查看整个 ip-group 组的配置。

【提示信息】 -

【常见错误】 -

【平台说明】 -

16.4 ip-subnet

配置 ip 地址网段。

ip-subnet *subnet {mask | mask_len }*

删除 ip 地址网段。

no ip-subnet *subnet mask_len*

【参数说明】

参数	描述
subnet	ip 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 ip 地址网段

【命令模式】 ip-group 配置模式

【缺省级别】 14

【使用指导】 无

【配置举例】 1：配置 ip 地址网段。

```
Ruijie(config-ip-group)#ip-subnet 10.10.10.0 24
```

2：删除 ip 地址网段。

```
Ruijie(config-ip-group)#no ip-subnet 10.10.10.0 24
```

【检验方法】 使用 **show ip-group** [*id*]命令，可以查看整个 ip-group 组的配置。

【提示信息】 -

【常见错误】 -

【平台说明】 -

16.5 route-db

配置路由地址库。
route-db *name*

删除路由地址库。
no route-db *name*

【参数说明】

参数	描述
name	路由地址库名称

【缺省配置】 缺省情况下没有路由地址库信息

【命令模式】 ip-group 配置模式

【缺省级别】 14

【使用指导】 无

【配置举例】 1：配置 ip 地址网段。

```
Ruijie(config-ip-group)#route-db cmc
```

2：删除 ip 地址网段。

```
Ruijie(config-ip-group)#no route-db cmc
```

【检验方法】 使用 **show ip-group** [*id*]命令，可以查看整个 ip-group 组的配置。

【提示信息】 -

【常见错误】 -

【平台说明】 -

16.6 show ip-group

查看 ip-group 组的配置。

show ip-group [*id*]

【参数说明】

参数	描述
id	ip-group 组的 id

【命令模式】 特权模式、全局模式、接口模式

【缺省级别】 14

【缺省级别】 如果输入 id，只显示对应 ip-group 的配置，否则显示所有 ip-group 组的配置信息。

【配置举例】 1：查看 ip-group 组的配置信息。

```
Ruijie#show ip-group 1
ip-group 1
 description test
 ip-range 1.1.1.2 1.1.1.10
 ip-subnet 10.10.10.0 24
 ip-range 10.10.10.10 10.10.10.15
 ip-subnet 10.10.11.0 30
 ip-range 20.10.10.10 20.10.20.200
!
```

【提示信息】 -

【常见错误】 -

【平台说明】 -

16.7 show ip-group statistics

查看 ip-group 的统计信息。

show ip-group statistics

【参数说明】

参数	描述
-	-

【命令模式】 特权模式、全局模式、接口模式

【缺省级别】 14

【使用指导】 如果输入 id，只显示对应 ip-group 的路由信息，否则显示所有 ip-group 组的路由信息。

【配置举例】 查看 ip-group 的统计信息。

```
Ruijie#show ip-group statistics
ip-group server: 1.1.1.1
ip-group state: down
ip-group cnt: 0.
ip-group add event: 0.
ip-group del event: 0.
ip-group syn event: 0.
ip-group error event: 0.
ip-group enq err event: 0.
ip-group add table failed: 0
ip-group del table failed: 0
ip-group add entry failed: 0
ip-group del entry failed: 0
ip-group db-acct cnt: 0
```

字段解释：

字段	说明
ip-group server	数据库连接的服务端 ip 地址
ip-group state	和数据库连接状态
ip-group add event	添加 ip 信息的统计
ip-group del event	删除 ip 信息的统计
ip-group syn event	同步 ip 信息的统计
ip-group error event	收到错误 ip 信息的统计
ip-group enq err event	Ip 信息入队出错的统计
Ip-group add table failed	添加路由表失败次数
Ip-group del table failed	删除路由表失败次数

Ip-group add entry failed	添加表项失败次数
Ip-group del entry failed	删除表项失败次数
ip-group db-acct cnt	acct 表同步操作次数

【提示信息】 -

【常见错误】 -

【平台说明】 -

17 app-auth

17.1 app-auth ad-url

设置 app 认证下推送的重定向 url 地址。

app-auth ad-url *string*

删除重定向地址

no app-auth ad-url

【参数说明】

参数	描述
string	重定向 url 地址

【缺省配置】 默认不开启

【命令模式】 全局配置模式

【缺省级别】 14

【使用指导】 1、 在内置认证情况下，重定向地址通常用于推送广告

2、 在与服务器联动认证时，该地址通常配置成外置 portal 地址

【配置举例】 1：配置重定向地址为锐捷官网。

```
Ruijie(config)# app-auth ad-url http://www.ruijie.com.cn
```

【检验方法】 1：使用 **show app-auth statistics** 命令显示重定向 url 地址。

```
Ruijie#show app-auth statistics
------------------------------start---------------------------------
app_auth_enable: on
cwmp_enable: on
cwmp_bak: on
non_http_pass: off
device_serialno: 1234942570024
basename: 401034053077
portal_key: ruijie
g_wan_ip: 172.18.124.109
priv_info:
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:http://www.ruijie.com.cn
avoid app_name:
        directApp(247-250-0-0)
auth app_name:
        authModeApp(247-251-0-0)
auth_url:

distri msg. up: 0, down: 0, inq: 0, attent:0
rcv_msg_num: 8878, rcv_query_msg_num: 0
----------------------------------end--------------------------------
```

【提示信息】 -

【常见错误】 设备 dns 未配置，导致重定向 url 地址未解析放行。

【平台说明】 -

17.2 app-auth auth-rule ip

设置进行 app 认证的网段
app-auth auth-rule ip *start-ip* [*end-ip*]

删除认证网段
no app-auth auth-rule ip *start-ip* [*end-ip*]

【参数说明】

参数	描述
start-ip	起始 ip
end-ip	结束 ip

【缺省配置】 默认不配置，app 认证功能开启后所有用户都需要进行处理

【命令模式】 全局配置模式

【缺省级别】 14

【使用指导】 1、 为配置情况下，所有用户都会进入 app 认证处理。配置后只有该网段的用户才会进入 app 认证处理

【配置举例】 1：配置对网段 192.168.1.0/24 的用户进行 app 认证

```
Ruijie(config)# app-auth auth-rule ip 192.168.1.1 192.168.1.255
```

【检验方法】 1：使用 **show app-auth auth-rule ip** 命令显示重定向 url 地址。

```
Ruijie#show app-auth auth-rule
auth rule ip:
        192.168.1.1 - 192.168.1.255
```

【提示信息】 -

【常见错误】

【平台说明】 -

17.3 app-auth cfg-opt

应用认证选项配置

app-auth cfg-opt [**id-ip | id-mac | rdt--for-wx | rdt-for-wx2 | rdt-fo-wifidog | rdt-default | tup** num **| local-relay [enable | port** port-num | **exclude-online | syn-proxy {count** syn-num**}]**

【参数说明】

参数	描述
id-ip	网络拓扑为三层网络，使用 ip 标示用户
id-mac	网络拓扑为二层网络，使用 mac 标示用户
rdt-for-wx	微信连 wifi 1.X 重定向格式
rdt-for-wx2	微信连 wifi 3.X 重定向格式
rdt-for-wifidog	wifidog 重定向格式
rdt-default	tr069 重定向方式
tup	临时放行 IOS 的时间，用户控制 IOS 弹窗.
num	临时放行 IOS 的时间，单位秒
local-relay	配置重定向本地中转
enable	重定向中转功能开启
port	本地中转重定向端口，需要与进程 webservice 服务一致
port-num	进程 webservice 的监听端口
exclude-online	不对在线用户进行流量监测
syn-proxy	是否启用 syn 监测代理
syn-num	监测到 syn 重发几次后进行代理

【缺省配置】 1、 默认二层网络，使用 MAC 唯一标示用户。
2、 默认开启应用识别依赖。
3、 默认使用 tr069 重定向方式。

4、 默认严格放行 IOS 时间为 120 秒。
5、 默认开启本地重定向中转功能。
6、 默认本地重定向中转端口为 2060.
7、 默认对在线用户进行流量监测
8、 默认开启对 syn 报文进行监测代理，监测次数默认为 3

【命令模式】 全局配置模式

【缺省级别】 14

【使用指导】 1、 IP 地址可以用于三层网络中唯一标示一个用户，MAC 用于在二层网络中唯一标识用户。
2、 在配置认证应用和免认证应用时需要开启应用识别依赖
3、 使用外置 WEB 认证方式时，会按照外置 WEB 认证的地址格式在 ad-url 后添加参数
4、 临时放行期间重定向认证 url 适用于 IOS 需要自动弹出广告，又需要实现对认证 url 重定向的场景

【配置举例】 1：使用 ip 地址唯一表示一个用户

```
Ruijie(config)#app-auth cfg-opt id-ip
```

2：使用 wifidog 重定向格式

```
Ruijie(config)#app-auth cfg-opt rdt-for-wifidog
```

【检验方法】 1：使用 **show app-auth cfg-opt** 命令显示开启哪些认证选项。

```
Ruijie#show app-auth cfg-opt
pp_auth_cfg_id: 1
app_auth_cfg_rdt_style: 8
app_auth_rdt_style_str: app-auth
app_auth_cfg_rdt_mode_url: 0
app_auth_cfg_strict_tup: 1
app_auth_cfg_dep_idy: 1
app_auth_cfg_aply_ref: 0
app_auth_cfg_proxy:1
app_auth_cfg_relay_enable: 1
app_auth_cfg_relay_port: 2060
app_auth_cfg_relay_enhance: 1
app_auth_enable_mac_inq: 1
app_auth_cfg_strict_tup: 1
app_auth_cfg_no_detect_online: 0
app_auth_cfg_rdt_style_302: 1
app_auth_cfg_id 为 1 表示二层网络，使用 mac 标示用户，为 2 表示三层网络，使用 ip 标示用户
```

【提示信息】 -

【常见错误】 -

【平台说明】 -

17.4 app-auth clear

批量清除所有禁止的 mac 配置
app-auth clear deny-mac
批量清除所有允许的 mac 配置
app-auth clear direct-mac
批量清除外网直通 url 地址
app-auth clear direct-url

【参数说明】

参数	描述
-	-

【缺省配置】

【命令模式】 特权模式

【缺省级别】 14

【使用指导】 外置服务器下发命令时可以先是使用批量命令进行清除，防止先前的配置造成影响

【配置举例】 -

【检验方法】

【提示信息】 -

【常见错误】 -

【平台说明】 -

17.5 app-auth cwmp enable

开启外置认证功能
app-auth cwmp enable

关闭外置认证功能

no app-auth cwmp enable

【参数说明】

参数	描述
-	-

【缺省配置】 默认不开启外置认证。

【命令模式】 全局配置模式

【缺省级别】 14

【使用指导】 开启外置认证，由外置服务器控制用户的上线行为 。设备在匹配认证 APP 或者认证 URL 时会向服务器发送 Attention 消息，由服务器根据设置来选择用户是否认证通过。

【配置举例】 1：开启外置认证功能

```
Ruijie(config)# app-auth cwmp enable
```

【检验方法】 1：使用 **show app-auth statistics** 命令显示是否开启外置认证开关。

```
Ruijie#show app-auth statistics
------------------------------start---------------------------------
app_auth_enable: off
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:
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:
auth app_name:
auth_url:
```

```
distri msg. up: 0, down: 0, inq: 0, attent:0
rcv_msg_num: 0, rcv_query_msg_num: 0
----------------------------------end---------------------------------
```

cwmp_enable 字段为 “off” 表示关闭，为”on”表示开启。

【提示信息】 -

【常见错误】 -

【平台说明】 -

17.6 app-auth deny-mac

设置禁止的内网 mac 地址。

app-auth deny-mac *mac_addr* [**aging-time** *time*] [**comment** *string*]

删除免认证直通外网 ip

no app-auth deny-mac *mac_addr*

【参数说明】

参数	描述
mac_addr	内网 MAC 地址
time	本配置的老化时间，单位分钟
String	本配置的描述

【缺省配置】

【命令模式】 全局配置模式

【缺省级别】 14

【使用指导】 禁止内网指定 MAC 上网时配置。在二层网络中使用

【配置举例】 1：设置 MAC 00d0.11ff.2233 禁止上网

```
Ruijie(config)# app-auth deny-mac 00d0.11ff.2233
```

【检验方法】 使用 show app-auth deny-mac 命令查看

```
app-auth deny-mac num: 1
        mac: 00d0.11ff.2233, flag: 1
```

【提示信息】 -

【常见错误】 -

【平台说明】 -

17.7 app-auth direct-app

设置免认证 app 名称。
app-auth direct-app *app-name*

删除免认证 app 名称
no app-auth direct-app *app-name*

【参数说明】

参数	描述
app-name	app 名称

【缺省配置】 -

【命令模式】 全局配置模式

【缺省级别】 14

【使用指导】 当应用识别出来是某应用时，配置直通后，直接放行该应用。

【配置举例】 1：配置微博应用放行。

```
Ruijie(config)# app-auth direct-app 新浪微博
```

【检验方法】 1：使用 **show app-auth statistics** 命令查看应用是否配置成免认证。

```
Ruijie(config)#show app-auth statistics
------------------------------start---------------------------------
app_auth_enable: off
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:
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:

distri msg. up: 0, down: 0, inq: 0, attent:0
rcv_msg_num: 0, rcv_query_msg_num: 0
----------------------------------end--------------------------------
avoid app_name 字段对应免认证应用
```

2：使用该应用产生流量，查看是否直接放行。

【提示信息】 -

【常见错误】 -通过 show identify-application 确认该应用名在应用识别库中是否存在

【平台说明】 -

17.8 app-auth direct-dstip

设置直通的外网 ip 地址, ip_end 不配置时默认配置单个 ip 地址。

app-auth direct-dstip *ip_start* [*ip_end*] [**aging-time** *time*] [**comment** *string*]

删除免认证直通外网 ip

no app-auth direct-dstip *ip_start* [*ip_end*]

【参数说明】

参数	描述
ip_start	起始 ip 地址
ip_end	结束 ip 地址
time	本配置的老化时间，单位分钟
String	本配置的描述

【缺省配置】 -

【命令模式】 全局配置模式

【缺省级别】 14

【使用指导】 当 app 认证未通过之前，想要直接访问外部服务器的话就可以直接将服务器 ip 地址加入免认证外网 ip 中。

【配置举例】 1：设置 3.3.3.3 该服务器为直通外网地址。

```
Ruijie(config)# app-auth direct-dstip 3.3.3.3
```

【检验方法】 1、 使用 **show app-auth direct-dstip** 命令查看是否配置直通外网 ip 地址；

```
Ruijie(config)#show app-auth direct-dstip
direct dst-ip:
        3.3.3.3
```

2、 开启 app 认证后，未认证通过前直接访问外网地址，查看是否可以访问。

【提示信息】 -

【常见错误】 -

【平台说明】 -

17.9 app-auth direct-mac

设置免认证内网 mac 地址。

app-auth direct-mac *mac_addr* [**aging-time** *time*] [**comment** *string*]

删除免认证直通外网 ip

no app-auth direct-mac *mac_addr*

【参数说明】

参数	描述
mac_addr	内网 MAC 地址
time	本配置的老化时间，单位分钟
String	本配置的描述

【缺省配置】 -

【命令模式】 全局配置模式

【缺省级别】 14

【使用指导】 指定 MAC 免认证时配置。在二层网络中使用

【配置举例】 1：设置 MAC 00d0.11ff.2233 为免认证

```
Ruijie(config)# app-auth direct-mac 00d0.11ff.2233
```

【检验方法】 使用 **show app-auth direct-mac** 命令查看

```
app-auth direct-mac num: 1
        mac: 0010.1144.3344, flag: 0
```

【提示信息】 -

【常见错误】 -

【平台说明】 -

17.10 app-auth direct-srcip

配置免认证内网 ip 地址，设置直通的内网 ip 地址，ip_end 不配置时默认配置单个 ip 地址。
app-auth direct-srcip *ip_start* [*ip_end*] [**aging-time** *time*] [**comment** *string*]

删除免认证直通内网 ip
no app-auth direct-srcip *ip_start* [*ip_end*]

【参数说明】

参数	描述
ip_start	起始 ip 地址
ip_end	结束 ip 地址
time	本配置的老化时间，单位分钟
String	本配置的描述

【缺省配置】 -

【命令模式】 全局配置模式

【缺省级别】 14

【使用指导】 当 app 认证未通过之前，内网某 IP 地址不需要通过认证就能直接外网，可以将该 pc 的 ip 地址加入免认证内网 ip 地址。

【配置举例】 1：配置内网 192.168.1.100-192.168.1.120 不需要经过 app 认证。

```
Ruijie(config)# app-auth direct-srcip 192.168.1.100 192.168.1.120
```

【检验方法】 1、 使用 **show app-auth direct-srcip** 命令查看是否配置直通内网网 ip 地址；

```
Ruijie(config)#show app-auth direct-srcip
direct src-ip:
        192.168.1.100 - 192.168.1.120
```

2、 开启 app 认证后，未认证通过前该内网网段的 PC 直接访问外网，查看是否可以访问。

【提示信息】 -

【常见错误】 -

【平台说明】 -

17.11 app-auth direct-url

设置外网直通的 url 地址。

app-auth direct-url *string*

删除免认证域名地址

no app-auth direct-domain *string*

【参数说明】

参数	描述
string	url 地址

【缺省配置】 -

【命令模式】 全局配置模式

【缺省级别】 14

【使用指导】 app 认证未通过前，若想要直接能够访问某个网址，可以将其加入免认证域名地址中。

该命令支持配置 https://, http://, ftp://格式的配置，设备将不保存前缀部分。当该地址是 https 或者 ftp 方式时，需要依赖终端进行 dns 请求后设备才会放行该地址。

非加密且是 http 访问情况下，可直接放行。否则需要依赖终端进行 dns 学习

【配置举例】 1：设置锐捷官网为直通域名地址。

```
Ruijie(config)# app-auth direct-url http://www.ruijie.com.cn
```

【检验方法】 1、 使用 **show app-authd direct-url** 命令查看是否配置直通 url 地址；

```
Ruijie(config)#show app-auth direct-url
direct url:
        www.ruijie.com.cn
       ccbc.com.cn
```

配置的 http://前缀会自动删除，其他前缀如 https://或者 ftp://会进行保留。

2、 开启 app 认证后，未认证通过前 PC 直接访问该 url 地址，查看是否可以访问。

【提示信息】 -

【常见错误】 配置后可能无法立即放行。需要终端清空缓存后重新进行 dns 学习

【平台说明】 -

17.12 app-auth enable

开启 app 认证。

app-auth enable

关闭 app 认证。

no app-auth enable

【参数说明】

参数	描述
-	-

【缺省配置】 默认不开启 app 认证。

【命令模式】 全局配置模式

【缺省级别】 14

【使用指导】 开启后，用户无法上网

【配置举例】 1：功能开启

```
Ruijie(config)# app-auth enable
```

【检验方法】 1：使用 **show app-auth statistics** 命令显示是否开启外置认证开关。

```
Ruijie#show app-auth statistics
------------------------------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:
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:

distri msg. up: 0, down: 0, inq: 0, attent:0
rcv_msg_num: 0, rcv_query_msg_num: 0
---------------------------------end--------------------------------
```

【提示信息】 -

【常见错误】 -

【平台说明】 -

17.13 app-auth kick

根据 ip 地址强制剔除当前 app 认证在线的节点。

app-auth kick ip *ip-addr*

剔除所有在线节点。

app-auth kick all

【参数说明】

参数	描述
ip-addr	ip 地址

【缺省配置】 -

【命令模式】 特权模式

【缺省级别】 14

【使用指导】 根据 ip 地址查找当前的在线节点信息，将其踢下线，需要重新 app 认证。
当关闭 app 认证后，要剔除所有当前在线的节点。

【配置举例】 1：将在线 2.2.2.2 剔除下线。

```
Ruijie# app-auth kick-ip 2.2.2.2
```

【检验方法】 未踢下线前，**show app-auth online** 查看当前在线节点信息；
踢下线后，**show app-auth online** 查看该 ip 地址是否在线。

【提示信息】 -

【常见错误】 -

【平台说明】 -

17.14 app-auth local-auth authorize

设置二维码授权功能
app-auth local-auth authorize { **check** | **restrict-times** *times* }
设置默认次数
no app-auth local-auth authorize restrict-times *times*
关闭功能
no app-auth local-auth authorize check

【参数说明】

参数	描述
times	授权次数

【缺省配置】 关闭。

【命令模式】 全局配置模式

【缺省级别】 14

【使用指导】 -

【配置举例】 1：在网关上配置开启二维码授权认证，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
```

【检验方法】 1. 使用 show app-auth local-auth config

```
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    state:  Not exist
  pc:
    global: false
    name:
    state:  Idle
```

【提示信息】 -

【常见错误】 -

【平台说明】 网关系列产品

17.15 app-auth local-auth authorize-time

用户授权后可以上网的时长

app-auth local-auth authorize authorize-time *minute*

恢复默认上网时长

no app-auth local-auth authorize-time

【参数说明】

参数	描述
minute	授权认证后的可用时长

【缺省配置】 关闭。

【命令模式】 全局配置模式

【缺省级别】 14

【使用指导】 -

【配置举例】 1：在网关上配置开启二维码授权认证，认证后可以使用的时长为 60 分钟

```
Ruijie# configure terminal
Ruijie(config)# app-auth local-auth authorize-time 60
```

【检验方法】 1. 使用 show app-auth local-auth config

```
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    state:  Not exist
pc:
  global: false
  name:
  state:  Idle
```

【提示信息】 -

【常见错误】 -

【平台说明】 网关系列产品

17.16 app-auth local-auth data-store

设置本地认证用户数据库自动老化时间

app-auth local-auth data-store { **enable | age day** *day* }

设置默认时间

no app-auth local-auth data-store age

关闭功能

no app-auth local-auth data-store enable

【参数说明】

参数	描述
day	老化周期
enable	功能开启

【缺省配置】 关闭。

【命令模式】 全局配置模式

【缺省级别】 14

【使用指导】 -

【配置举例】 1：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】 1. 使用 show app-auth local-auth config 中的 data-store-age-day 项

```
Ruijie# show app-auth local-auth config
enable: True
data-store-enable: True
data-store-age-day: 5
user-mac-limit: 5
online-time: 1
authorize-time: 33
restrict-range information:
  mobile:
    global: true
    name:   day
    state:  Not exist
  pc:
    global: false
    name:
    state:  Idle
```

【提示信息】 -

【常见错误】 -

【平台说明】 网关系列产品

17.17 app-auth local-auth enable

开启本地认证

app-auth local-auth enable

关闭本地认证。

no app-auth local-auth enable

【参数说明】

参数	描述
enable	开启本地认证

【缺省配置】 不开启本地认证。

【命令模式】 全局配置模式

【缺省级别】 14

【使用指导】 -

【配置举例】 1：开启本地认证。

```
Ruijie(config)# app-auth local-auth enable
```

【检验方法】 1：使用 show app-auth local-auth config 命令显示是否开启本地认证。

```
Ruijie#show app-auth local-auth config
app-auth local-auth enable
```

【提示信息】 -

【常见错误】 -

【平台说明】 网关系列产品

17.18 app-auth local-auth online-time

本地用户认证成功后的用户可用时长

app-auth local-auth online-time *time*

恢复默认时长。

no app-auth local-auth online-time

【参数说明】

参数	描述
time	时长，单位分钟

【缺省配置】 不限制时长。

【命令模式】 全局配置模式

【缺省级别】 14

【使用指导】 不对授权类型的认证用户生效

【配置举例】 1：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(config)# app-auth local-auth online-time 10
```

【检验方法】 1：使用 show app-auth local-auth config 命令查看。

```
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
```

【提示信息】 -

【常见错误】 -

【平台说明】 网关系列产品

17.19 app-auth local-auth restrict

配置限制终端类型上网

app-auth local-auth restrict { **pc** | **mobile** } [**exclude time-range** *time*]

恢复默认时长。

no app-auth local-auth restrict { **pc** | **mobile** }

【参数说明】

参数	描述
pc	限制 pc 上网
mobile	限制手机上网
time	不限制上网的起始时间

【缺省配置】 不限制时长。

【命令模式】 全局配置模式

【缺省级别】 14

【使用指导】 用于限制用户的上网行为

【配置举例】 1：限制移动用户不能上网，其中在“day”这个时间段内不生效。

```
Ruijie(config)# app-auth local-auth restrict mobile exclude time-range day
```

【检验方法】 1：使用 show app-auth local-auth config 命令查看。

```
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
```

【提示信息】 -

【常见错误】 -

【平台说明】 网关系列产品

17.20 app-auth local-auth subscriber mac-limit

配置本地认证每用户可导入的终端上限

app-auth local-auth subscirber mac-limit *limit-num*

恢复默认配置

no app-auth local-auth ubscirber mac-limit

【参数说明】

参数	描述
limit-num	限制个数

【缺省配置】 无

【命令模式】 全局配置模式

【缺省级别】 14

【使用指导】 -

【配置举例】 1：配置用户组。

```
Ruijie# configure terminal
Ruijie(config)# app-auth local-auth subscirber mac-limit 5
```

【检验方法】 1. 使用 show app-auth local-auth config 中的 user-mac-limit 项

```
Ruijie# show app-auth local-auth config
enable: True
data-store-enable: True
data-store-age-day: 36
user-mac-limit: 5
online-time: 1
authorize-time: 33
restrict-range information:
  mobile:
    global: true
    name:   day
    state:  Not exist
  pc:
    global: false
```

```
    name:

    state:  Idle
```

【提示信息】 -

【常见错误】 -

【平台说明】 网关系列产品

17.21 app-auth local-auth subs-name

配置本地认证的用户信息

app-auth local-auth subs-name *name* **type local**

删除本地认证的用户信息

no app-auth local-auth subs-name *name* **type local**

【参数说明】

参数	描述
name	用户名称
type	用户类型
local	本地用户

【缺省配置】 **无**

【命令模式】 全局配置模式

【缺省级别】 14

【使用指导】 -

【配置举例】 1：配置用户。

```
Ruijie# configure terminal
Ruijie(config)# app-auth local-auth subs-name abc type ad
```

【检验方法】 1：使用 show app-auth local-auth subs all 命令查看配置。

```
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
```

【提示信息】 -

【常见错误】 -

【平台说明】 网关系列产品

17.22 app-auth local-auth vip-group

设置本地认证用户为特权用户。

app-auth local-auth vip-group *user-name* **local**

删除特权用户

no app-auth local-auth vip-group *user-name* **local**

【参数说明】

参数	描述
vip-group	特权组
user-name	需要加入特权组的用户
local	本地用户

【缺省配置】 **无**

【命令模式】 全局配置模式

【缺省级别】 14

【使用指导】 -

【配置举例】 1：配置用户 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】 1：使用 `show app-auth local-auth vip-group all` 查看 vip 用户。

```
Ruijie# Ruijie# show app-auth local-auth vip-group all

cnt: 1/100. ad_any_vip: 0
```

```
Group-name                                                          type       idx
------------------------------------------------------------------------------
aaa                                                                 local      0
```

【提示信息】 -

【常见错误】 -

【平台说明】 网关系列产品

17.23 app-auth offline-detect

设置流量检测下线。
app-auth offline-detect [**time-interval** *time* **flowrate** *flow*]

关闭流量检测下线功能。
no app-auth offline-detect

【参数说明】

参数	描述
time	时间间隔，单位 min。配置范围 1~65535，不配置默认为 15
flow	流量，单位 bps。配置范围 0~1000000bps,不配置为 0

【缺省配置】 不开启流量下线检测。

【命令模式】 全局配置模式

【缺省级别】 14

【使用指导】 -

【配置举例】 1：配置 app 认证通过后，15 分钟内流量小于 10Kbps 下线。

```
Ruijie(config)# app-auth offline-detect time-interval 15 flowrate 10000
```

【检验方法】 配置流量检测下线后，使用 app 认证通过后，手机关机等时间间隔超过后，**show app-auth online** 查看当前该 ip 地址已经不在线。

【提示信息】 -

【常见错误】 -

【平台说明】 -

17.24 app-auth portal-key

设置数据加密秘钥

app-auth portal-key *password*

【参数说明】

参数	描述
password	与服务器通信时，使用该秘钥加密数据

【缺省配置】 缺省无配置

【命令模式】 全局配置模式

【缺省级别】 14

【使用指导】 -

【配置举例】 1：配置加密秘钥为”ruijie”

```
Ruijie(config)# app-auth portal-key ruijie
```

【检验方法】 show app-auth statistics 可以查看该配置

【提示信息】 -

【常见错误】 -

【平台说明】 -

17.25 app-auth priv-info

设置重定向时私有的信息

app-auth priv-info *info*

【参数说明】

参数	描述
info	重定向时配置的私有信息

【缺省配置】 缺省无配置

【命令模式】 全局配置模式

【缺省级别】 14

【使用指导】 配置该参数后，在重定向中可以携带该私有信息。

【配置举例】 1：配置重定向的私有信息为 siteid =ruijie

```
Ruijie(config)#app-auth priv-info siteid=ruijie
```

【检验方法】 show app-auth statistics 可以查看该配置

```
Ruijie#show app-auth statistics
------------------------------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:
        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: 0, rcv_query_msg_num: 0
---------------------------------end---------------------------------
```

【提示信息】 -

【常见错误】 -默认不配置该私有信息。需要依据具体项目与客户约定私有信息内容。

【平台说明】 -

17.26 app-auth proxy-url

设置代理 url

app-auth proxy-url *url* {**rdt-type** *num*}

删除代理 url

no app-auth proxy-url

【参数说明】

参数	描述
url	需要进行代理的 url。实际需要配置为 ip 地址形式。如 http://10.1.0.6/redirect
rdt-type	配置重定向方式
num	特殊重定向方式编号

【缺省配置】 缺省无配置

【命令模式】 全局配置模式

【缺省级别】 14

【使用指导】 该命令用于定制认证方案情况下，对代理 url 使用特殊的重定向方法。未配置特殊重定向方式编号时，则只进行代理，重定向方式使用默认的。

配置成代理 url 的地址不能分配给内网的实际主机。

该命令用于微信连 wifi 认证中及客户定制 APP 认证方式中。

【配置举例】 1：配置 10.1.0.6 为代理 url

```
Ruijie(config)#app-auth proxy-url http://10.1.0.6
```

【检验方法】 show app-auth statistics 可以查看该配置

```
Ruijie#show app-auth statistics
------------------------------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:
        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: 0, rcv_query_msg_num: 0
---------------------------------end--------------------------------
```

【提示信息】 -

【常见错误】 默认不配置该私有信息。需要依据具体项目与客户约定私有信息内容。

【平台说明】 -

17.27 app-auth policy

新增一个认证策略

app-auth policy *name*

删除一个认证策略

no app-auth policy *name*

【参数说明】

参数	描述
name	策略名

【缺省配置】 缺省无配置

【命令模式】 全局配置模式

【缺省级别】 14

【使用指导】 新增一个认证策略

【配置举例】 1：配置认证策略 aaa

```
Ruijie(config)# app-auth policy aaa
```

【检验方法】 show app-auth policy 可以查看该配置

```
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
```

【提示信息】 -

【常见错误】 无。

【平台说明】 网关系列产品

17.28 app-auth policy-swap

交换两个策略的优先级

app-auth policy-swap *rule-name1 rule-name2*

【参数说明】

参数	描述
rule-name1	需要交换的策略名
rule-name2	需要交换的策略名

【缺省配置】 缺省无配置

【命令模式】 全局配置模式

【缺省级别】 14

【使用指导】 用于交换两条策略的优先级。

【配置举例】 1：交换 rule1 和 rule2 的优先级

```
Ruijie(config)#app-auth policy-swap rule1 rule2
```

【检验方法】

```
show app-auth policy 可以查看该配置
Ruijie# show app-auth policy
app-auth policy rule2 type sms
app-auth policy rule1 type weixin
```

【提示信息】 -

【常见错误】 无。

【平台说明】 网关系列产品

17.29 app-auth set-hz

设置场所编号、场所名

app-auth set-hz siteid *id-num* **sitename** *name* {**ip-range** *ip-start ip-end* }

【参数说明】

参数	描述
id-num	场所编号
name	场所名
ip-start	起始网段
ip-end	终止网段

【缺省配置】 缺省无配置

【命令模式】 全局配置模式

【缺省级别】 14

【使用指导】 id-num、name 作为重定向的参数进行传输。未配置网段下，id-num、name 为全局生效，配置网段后，只有该网段才匹配该 id-num、name。

【配置举例】 1：配置全局场所编号为 111，场所名称为 ruijie

```
Ruijie(config)# app-auth set-hz siteid 111 sitename ruijie
```

【检验方法】 **show app-auth hz-info** 可以查看该配置

```
Ruijie# show app-auth hz-info
{"root":{"siteid":"111", "sitename":"ruijie"}, "branch": [] }
```

【提示信息】 -

【常见错误】 -

【平台说明】 -

17.30 app-auth server

配置认证服务器

app-auth server *name* **type** { **qrcode-alone** | **qrcode-authorize** | **sms** | **weixin** }

恢复默认配置

no app-auth server *name*

【参数说明】

参数	描述
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

【缺省配置】 无

【命令模式】 全局配置模式

【缺省级别】 14

【使用指导】 -

【配置举例】 1：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】 1. 使用 show app-auth server all

```
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
```

【提示信息】 -

【常见错误】 -

【平台说明】 网关系列产品

17.31 app-auth set-ssid

设置 ssid

app-auth set-ssid *ssid* {***ip-range*** *ip-start ip-end*}

【参数说明】

参数	描述
ssid	ssid 名称
ip-range	配置 ip 范围
ip-start	起始网段
ip-end	终止网段

【缺省配置】 缺省无配置

【命令模式】 全局配置模式

【缺省级别】 14

【使用指导】 ssid 作为重定向的参数进行传输。未配置网段下，ssid 为全局生效，配置网段后，只有该网段才匹配该 ssid。

【配置举例】 1：配置全局 ssid 为"@@test"

```
Ruijie(config)# app-auth set-ssid @@test
```

【检验方法】 **show app-auth ssid-cfg** 可以查看该配置

```
Ruijie#show app-auth ssid-cfg
global: @@test
```

【提示信息】 -

【常见错误】 -

【平台说明】 -

17.32 app-auth snp enable

开启联动 dhcp snooping 功能

app-auth snp enable

【参数说明】

参数	描述
-	-

【缺省配置】 缺省无配置

【命令模式】 全局配置模式

【缺省级别】 14

【使用指导】 在三层网络环境下，可以通过 dhcp snooping 获取到终端的 mac 信息。 dhcp 组件需要开启 dhcp snooping 功能。在微信认证等需要获取终端 mac 时使用

【配置举例】 1：开启联动 dhcp snooping 功能

```
Ruijie(config)#app-auth snp enable
```

【检验方法】 **show app-auth snp-cfg** 可以查看该配置

```
Ruijie#show app-auth snp-cfg
snp: 1
```

【提示信息】 -

【常见错误】 dhcp 组件没有启用 snooping 功能

【平台说明】 -

17.33 app-auth tcp-socket

设置 tcp 长连接

app-auth tcp-socket [***enable*** **|** ***server*** *server-url* **|** ***keepalive*** *time_1* **|** ***user-inform*** *time_2*]

【参数说明】

参数	描述
enable	开启 tcp 长连接功能
server	配置服务器
server-url	服务器地址
keepalive	tcp 保活周期
time_1	tcp 保活周期，配置范围 30~3600，单位秒。默认 30 秒
user-inform	定时同步用户信息
time_2	定时同步用户周期，配置范围 30~3600， 单位秒。默认 300 秒

【缺省配置】 缺省无配置

【命令模式】 全局配置模式

【缺省级别】 14

【使用指导】 开启 tcp 长连接后，设备和服务器可定时同步用户信息，可适用于认证计费等对用户同步要求高的场景中。如功能开启，但未配置服务器地址，则使用广告重定向地址作为默认的长连接服务器。

【配置举例】 1：配置 tcp 长连接地址为 172.18.124.56

```
Ruijie(config)# app-auth tcp-socket server http://172.18.124.56
Ruijie(config)# app-auth tcp-socket enable
```

【检验方法】 **show app-auth tcp** 可以查看该配置

```
Ruijie#show app-auth tcp-info
tcp_server_url: http://172.18.124.56
tcp_enable: 1
tcp_keepalive_period: 300
user_inform_period: 300
tcp_sock: -1
tcp_state: 1
server_ip: 0.0.0.0, port: 0
server_change: 1
```

```
rcv_pkt_num: 0
rcv_error_pkt_num: 0
keepalive_last_send_time: 0
keepalive_last_rcv_time: 0
user_inform_last_send_time: 0
user_inform_last_rcv_time: 0
```

【提示信息】 -

【常见错误】 -

【平台说明】 -

17.34 app-auth tup-app

设置临时放行的 app 名称。
app-auth tup-app *app-name*

删除免认证 app 名称
no app-auth tup-app *app-name*

【参数说明】

参数	描述
app-name	app 名称

【缺省配置】 -

【命令模式】 全局配置模式

【缺省级别】 14

【使用指导】 该命令用于在微信连 wifi 协议中，由 portal 触发后临时放行微信等。因此对 portal 存在依赖关系

【配置举例】 1：配置微信临时放行。

```
Ruijie(config)# app-auth tup-app 微信
```

【检验方法】 1：使用 **show app-auth statistics** 命令查看应用是否配置成临时放行应用。

```
Ruijie(config)#show app-auth statistics
------------------------------start---------------------------------
app_auth_enable: off
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:
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)
tup app_name:
        微信 ( 7-10-0-0 )
auth app_name:
auth_url:

distri msg. up: 0, down: 0, inq: 0, attent:0
rcv_msg_num: 0, rcv_query_msg_num: 0
---------------------------------end--------------------------------
```

tup app_name 字段对应临时放行应用

【提示信息】 -

【常见错误】 -通过 show identify-application 确认该应用名在应用识别库中是否存在

【平台说明】 -

17.35 app-auth proxy-option

开启 https 重定向

app-auth proxy-option [**https | session total** *total_limit* **per-ip** *per_ip_limit*]

【参数说明】

参数	描述
https	开启 https 重定向
session total *total_limit*	总会话数限制

per-ip *per_ip_limit*	每 ip 会话数限制

【缺省配置】 缺省无配置

【命令模式】 全局配置模式

【缺省级别】 14

【使用指导】 开启该功能后， https 流量都会被设备重定向到指定 portal 页。

【配置举例】 1：开启 https 重定向

```
Ruijie(config)# app-auth proxy-option https
```

2：配置会话数限制

```
Ruijie(config)# app-auth proxy-option session total 10000 per-ip 200
```

【检验方法】 **通过 show app-auth proxy-option config** 可以查看该配置

```
Ruijie#show app-auth proxy-option config
---------- App-Auth Option Config Info ----------
Redirect for https  : Enable
Session total limit : 20001
Session per-ip limit: 201
----------------------- End ---------------------
Ruijie#
```

【提示信息】 -

【常见错误】 -

【平台说明】 -

17.36 local-auth qrcode

设置二维码认证。

local-auth qrcode { **ip** *ip-address* | **key** *key-str* | **comment** *comment-str* }

删除二维码认证

no local-auth qrcode { **ip** | **key** | **comment** }

【参数说明】

参数	描述
ip-address	可以使用该 ip 访问二维码
key-str	二维码的动态码

comment-str	提示信息字符串

【缺省配置】 无

【命令模式】 认证服务器模式

【缺省级别】 14

【使用指导】 -

【配置举例】 1：配置二维码认证

```
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
Ruijie(config-app-auth-server)# local-auth qrcode key test
Ruijie(config-app-auth-server)# local-auth qrcode comment zizhu
```

【检验方法】 1：使用 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
```

【提示信息】 -

【常见错误】 -

【平台说明】 网关系列产品

17.37 local-auth sms

设置短信认证。

local-auth sms { **mode prior** | **server** { **aliyun-v1** | **aliyun-v2** } | **keyid** *id* **keysecret** *string* **sign** *string* **templet** string }

删除短信认证

no local-auth sms { **mode prior** | **server** | **keyid** }

【参数说明】

参数	描述
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
server	短信服务器类型
aliyun-v1	阿里云短信 v1
aliyun-v2	阿里云短信 v2
mode	短信模式
prior	预先录入模式

【缺省配置】 无

【命令模式】 认证服务器模式

【缺省级别】 14

【使用指导】 -

【配置举例】 1：配置短信认证

```
Ruijie# configure terminal
Ruijie(config)# app-auth server sms-auth type sms
Ruijie(app-auth-policy)# local-auth sms keyid aaabbb keysecret cccddd sign eeefff templet ggghhh
Ruijie(app-auth-policy)# local-auth sms server aliyun-v1
Ruijie(app-auth-policy)# local-auth sms mode prior
```

【检验方法】 1：使用 show app-auth server all 查看服务器

```
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
```

【提示信息】 -

【常见错误】 -

【平台说明】 网关系列产品

17.38 local-auth weixin

设置微信认证。

local-auth weixin { **shopid** *shopid-str* **appid** *appid-str* **secretkey** *secretkey-str* | **ssid** *ssid-str* }

删除微信认证

no local-auth weixin { **shopid** | **ssid** }

【参数说明】

参数	描述
shopid-str	门店 id
appid-str	appid
secretkey-str	密钥
ssid-str	网络的 ssid

【缺省配置】 无

【命令模式】 认证服务器模式

【缺省级别】 14

【使用指导】 -

【配置举例】 1：配置微信认证

```
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
Ruijie(config-app-auth-server)# local-auth weixin ssid ssid_test
```

【检验方法】 1：使用 show app-auth server all 查看服务器

```
Ruijie# show app-auth server all
```

```
server name: wechat
type: weixin
    decrypt-flag: 0
    shopid: 111
    appid: bbb
    secretkey: ccc
    ssid: ssid_test
```

【提示信息】 -

【常见错误】 -

【平台说明】 网关系列产品

17.39 mac

配置本地认证用户的终端信息。

mac *mac-address* { **auto** | **manual** } **type** { **pc** | **mobile** }

删除本地认证用户的终端信息

no mac *mac-address*

【参数说明】

参数	描述
mac-address	mac 地址
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

【缺省配置】 无

【命令模式】 app-auth 的用户配置模式

【缺省级别】 14

【使用指导】 -

【配置举例】 1：配置本地认证用户，以及其终端信息

```
Ruijie# configure terminal
```

```
Ruijie(config)# app-auth local-auth subs-name abc type ad
Ruijie(config-app-auth-subs)# mac 0011.2233.4455 manual type pc
```

【检验方法】 1：使用 show app-auth local-auth subs all 查看终端信息

```
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
```

【提示信息】 -

【常见错误】 -

【平台说明】 网关系列产品

17.40 relate server

设置认证策略关联的认证服务器

relate server *server-name*

设置策略失效

no relate server *server-name*

【参数说明】

参数	描述
server-name	认证服务器名

【缺省配置】 无

【命令模式】 app-auth 的策略配置模式

【缺省级别】 14

【使用指导】 配置后该规则才生效

【配置举例】 1：配置规则使能

```
Ruijie(config)# app-auth policy aaa
Ruijie(app-auth-policy)# relate server wechat
```

【检验方法】 1：使用 show app-auth policy all 查看策略

```
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
```

【提示信息】 -

【常见错误】 -

【平台说明】 网关系列产品

17.41 rule enable

设置策略使能。

rule enable

设置策略失效

no rule enable

【参数说明】

参数	描述
enable	设置策略使能

【缺省配置】 无

【命令模式】 app-auth 的策略配置模式

【缺省级别】 14

【使用指导】 配置后该规则才生效

【配置举例】 1：配置规则使能

```
Ruijie(config)# app-auth policy aaa
Ruijie(app-auth-policy)# rule enable
```

【检验方法】 1：使用 show app-auth policy 查看策略

```
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
```

【提示信息】 -

【常见错误】 -

【平台说明】 网关系列产品

17.42 rule ip-range

配置策略生效的网段。

rule ip-range { [*ip1* { *ip2* }] | **all** }

删除网段

no rule ip-range

【参数说明】

参数	描述
ip1	生效的起始 ip
ip2	生效的终止 ip
all	对所有 ip 生效

【缺省配置】 无

【命令模式】 app-auth 的策略配置模式

【缺省级别】 14

【使用指导】 配置后需要匹配该网段的 ip 才会命中此策略

【配置举例】 1：配置规则对所有 ip 生效

```
Ruijie(config)# app-auth policy aaa
Ruijie(app-auth-policy)# rule ip-range all
```

【检验方法】 1：使用 show app-auth policy 查看策略

```
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
```

【提示信息】 -

【常见错误】 -

【平台说明】 网关系列产品

17.43 rule ssid

设置认证策略的 ssid

rule ssid *ssid*

删除认证策略的 ssid

no rule ssid

【参数说明】

参数	描述

ssid	该策略需要标识的 ssid

【缺省配置】 无

【命令模式】 app-auth 的策略配置模式

【缺省级别】 14

【使用指导】 -

【配置举例】 1：网关上配置认证策略 abc，且其的 ssid 为 test

```
Ruijie# configure terminal
Ruijie(config)# app-auth policy abc type qrcode
Ruijie(app-auth-policy)# rule ssid test
```

【检验方法】 1：使用 **show app-auth policy all** 查看策略

```
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
```

【提示信息】 -

【常见错误】 -

【平台说明】 网关系列产品

17.44 rule type pwd

配置帐号密码认证。
rule type pwd
删除帐号密码认证
no rule type pwd

【参数说明】

参数	描述
pwd	帐号密码认证

【缺省配置】 无

【命令模式】 app-auth 的策略配置模式

【缺省级别】 14

【使用指导】 只能在 app-auth 的策略组模式下使用

【配置举例】 1：配置认证策略 aaa，并使其有帐号密码认证类型

```
Ruijie(config)# app-auth policy aaa
Ruijie(app-auth-policy)# rule type pwd
```

【检验方法】 1：使用 show app-auth policy all 查看策略

```
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
```

【提示信息】 -

【常见错误】 -

【平台说明】 网关系列产品

17.45 show app-auth auth-rule

显示认证网段 ip

show app-auth auth-rule

【参数说明】

参数	描述
-	-

【命令模式】 全局模式、特权模式

【缺省级别】 14

【使用指导】 显示所有认证网段

【配置举例】 1：显示所有认证网段

```
Ruijie#show app-auth auth-rule
auth rule ip:
```

```
        192.168.1.1 - 192.168.1.255
```

【提示信息】 -

【平台说明】 -

17.46 show app-auth deny-mac

显示禁止的 Mac 地址

show app-auth deny-mac

【参数说明】

参数	描述
-	-

【命令模式】 全局模式、特权模式

【缺省级别】 14

【使用指导】 显示所有禁止的内网 mac

【配置举例】 1：显示禁止的内网 mac 地址

```
Ruijie#show app-auth deny-mac
app-auth deny-mac num: 1
        mac: 0010.1144.3344, flag: 1
```

【提示信息】 -

【平台说明】 -

17.47 show app-auth direct-dstip

显示直通的外网 IP 地址

show app-auth direct-dstip

【参数说明】

参数	描述
-	-

【命令模式】 全局模式、特权模式

【缺省级别】 14

【使用指导】 显示直通的外网 IP 地址

【配置举例】 1：显示直通的外网 IP 地址

```
Ruijie(config)#show app-auth direct-dstip
direct dst-ip:
        192.168.5.120
        1.1.1.1
```

【提示信息】 -

【平台说明】 -

17.48 show app-auth direct-mac

显示免认证的 Mac 地址

show app-auth direct-mac

【参数说明】

参数	描述
-	-

【命令模式】 全局模式、特权模式

【缺省级别】 14

【使用指导】 显示所有免认证的的内网 mac

【配置举例】 1：显示免认证的内网 mac 地址

```
Ruijie#show app-auth direct-mac
app-auth deny-mac num: 0
        mac: 0010.1144.3344, flag: 0
```

【提示信息】 -

【平台说明】 -

17.49 show app-auth direct-srcip

显示直通的外网 IP 地址

show app-auth direct-srcip

【参数说明】

参数	描述
-	-

【命令模式】 全局模式、特权模式

【缺省级别】 14

【使用指导】 显示内网免认证 IP 地址

【配置举例】 1：显示直通的外网 IP 地址

```
Ruijie(config)#show app-auth direct-srcip
direct src-ip:
        192.168.5.120
        1.1.1.1
```

【提示信息】 -

【平台说明】 -

17.50 show app-auth direct-url

显示直通的外网 url 地址

show app-auth direct-url

【参数说明】

参数	描述
-	-

【命令模式】 全局模式、特权模式

【缺省级别】 14

【使用指导】 显示内网免认证 IP 地址

【配置举例】 1：显示直通的外网 url 地址

```
Ruijie#show app-auth direct-url
direct url:
        www.baidu.com
```

【提示信息】 -

【平台说明】 -

17.51 show app-auth local-auth config

查看本地认证的配置参数。

show app-auth local-auth config

【参数说明】

参数	描述
-	-

【命令模式】 特权模式、全局模式

【缺省级别】 14

【使用指导】 使用该命令可以查看设备上的本地认证相关的配置参数。

【配置举例】 1：查看本地认证配置信息

```
Ruijie# show app-auth local-auth config
enable: False
data-store-enable: True
data-store-age-day: 36
user-mac-limit: 0
online-time: 1
authorize-time: 33
restrict-range information:
  mobile:
    global: false
    name:
    state:  Idle
  pc:
    global: false
    name:
    state:  Idle
```

字段解释：

字段	说明
enable	功能是否开启

data-store-enable	用户数据写入存储开关
data-store-age-day	用户数据老化时间
user-mac-limit	每个用户允许多少个 mac
online-time	用户认证成功后允许的上网时长
authorize-time	被授权用户认证成功后允许的上网时长
restrict-range information	终端上网限制策略信息
mobile	移动终端用户
pc	电脑终端用户
global	全局状态是否使能
name	时间对象名
state	本策略是否生效

【提示信息】 -

【平台说明】 网关系列产品

17.52 show app-auth local-auth subs

查看本地认证的用户信息。

show app-auth local-auth subs { **all** | **by-mac** *mac-address* | **by-name** *name-string* }

【参数说明】

参数	描述
all	所有用户
by-mac	通过 mac 显示用户
mac-address	用户 mac
by-name	通过用户名显示用户。
name-string	用户名

【命令模式】 特权模式、全局模式

【缺省级别】 14

【使用指导】 使用该命令可以查看设备上的本地认证用户信息。

【配置举例】 1：查看本地认证 bbb 用户的信息

```
Ruijie# show app-auth local-auth subs by-name bbb
--------------------------------------------------------------------------------
Name                                          Mac_num Type     source  Mode
```

```
       Mac             Auto/Manual terminal   time

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

bbb                                              1       local    pwd     manual

 |---- aabb.1111.2222  manual      mobile     2018-5-6 17:21:39
```

字段解释：

字段	说明
Name	用户名
Mac num	Mac 个数
Type	用户类型
Source	用户认证源
Mode	用户生成方式
Mac	终端 mac
Auto/manual	终端生成方式
Terminal	终端类型
Time	该 mac 最后一次使用时间

【提示信息】 -

【平台说明】 网关系列产品

17.53 show app-auth local-auth vip-group

查看本地认证的特权用户信息

show app-auth local-auth vip-group { **all** | **by-name** *name-string* }

【参数说明】

参数	描述
all	所有用户。
by-name	通过用户名显示用户。
name-string	用户名

【命令模式】 特权模式、全局模式

【缺省级别】 14

【使用指导】 使用该命令可以查看设备上的本地认证特权用户信息。

【配置举例】 1：查看所有特权用户信息

```
Ruijie#show app-auth local-auth vip-group all
```

```
cnt: 1/100. ad_any_vip: 0

Group-name                                                      type       idx

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

aaa                                                             local      0
```

字段解释：

字段	说明
Cnt	当前用户组个数
Group-name	用户组名
Type	用户组类型
Idx	用户组索引

【提示信息】 -

【平台说明】 网关系列产品

17.54 show app-auth local-online

查看本地认证的在线用户。

show app-auth local-auth { [**all** | **by-name** *name-str*] **from** *num1* **to** *num2* | **by-ip** *ip-address* }

【参数说明】

参数	描述
all	显示所有用户。
by-name	通过用户名显示用户。
name-str	用户名
from	从第几条记录开始。
num1	起始记录偏移
to	到第几条记录
num2	终止用户偏移
by-ip	通过 ip 显示用户

【命令模式】 特权模式、全局模式

【缺省级别】 14

【使用指导】 使用该命令可以查看设备上的本地认证用户信息。

【配置举例】 1：查看本地认证用户在线信息

```
Ruijie# show app-auth local-online all from  1 to 1

{"code": 0, "msg": "OK", "data": {"total": 1, "online": [{"name": "haha", "ip": "192.168.234.228",
```

```
"mac": "001a.a91f.e7a0", "type": "pwd", "time": "3118-9-28 16:29:46" } ] } }
```

字段解释：

字段	说明
Code	状态码
Msg	提示信息
Data	数据
Total	总用户数
Online	在线用户数
name	用户名
Ip	用户 Ip
Mac	用户 mac
Type	认证类型
Time	认证时间

【提示信息】 -

【平台说明】 网关系列产品

17.55 show app-auth policy

查看认证策略。

show app-auth policy [**all** | **by-name** *name-string*]

【参数说明】

参数	描述
all	所有策略信息。
by-name	通过名称查看。
name-string	策略名。

【命令模式】 特权模式、全局模式

【缺省级别】 14

【使用指导】 使用该命令可以查看设备上的认证策略信息。

【配置举例】 1：查看所有认证策略的详细信息

```
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 认证策略 1
  enable: True
  pid: 1
  mode: pwd
  state: 0
  ip-range number: 1
  cfile-path: plcy1.php
  pwd: 0
  sms: 1
  qrcode-alone: 1
  qrcode-authorize: 1
  act-directory: 1
  weixin: 1
ip-range info:
    1. ALL
  server number 5:
    1. name:微信服务器    type: weixin
    2. name:二维码扫码服务器    type: qrcode-authorize
    3. name:自主扫码服务器    type: qrcode-alone
    4. name:短信服务器    type: sms
```

字段解释：

字段	说明
Global information	策略信息
policy_cnt	策略个数
Global Ip-range	策略生效的网段信息
Detail	策略具体信息
Policy	策略名
enable	策略是否开启
pid	策略 id
mode	策略模式
state	策略状态

ip-range number	策略生效的 ip 段个数
cfile-path	策略参数文件
pwd	关联的本地帐号密码验证服务器个数
sms	关联的短信认证服务器个数
qrcode-alone	关联的自助扫码服务器个数
weixin	关联的 weixin 服务器个数
ip-range info	生效的网段的具体信息
server number	服务器信息

【提示信息】 -

【平台说明】 网关系列产品

17.56 show app-auth hz-info

显示场所 id、场所名配置信息

show app-auth hz-info

【参数说明】

参数	描述
-	-

【命令模式】 全局模式、特权模式、接口模式

【缺省级别】 14

【使用指导】 显示场所 id、场所名配置信息，在服务器需要获取场所 id、场所名时使用

【配置举例】 -

【提示信息】 -

【平台说明】 -

17.57 show app-auth proxy-url

显示代理 url 配置信息

show app-auth proxy-url

【参数说明】

参数	描述

【命令模式】 全局模式、特权模式、接口模式

【缺省级别】 14

【使用指导】 显示代理 url 配置信息

【配置举例】 -

【提示信息】 -

【平台说明】 -

17.58 show app-auth ssid-cfg

显示网段/ssid 配置信息

show app-auth ssid-cfg

【参数说明】

参数	描述
-	-

【命令模式】 全局模式、特权模式、接口模式

【缺省级别】 14

【使用指导】 显示网段/ssid 配置信息，在服务器需要获取 ssid 信息时使用

【配置举例】

【提示信息】 -

【平台说明】 -

17.59 show app-auth statistics

显示所有 app 认证相关的配置参数。

show app-auth statistics

【参数说明】

参数	描述
-	-

【命令模式】 全局模式、特权模式、接口模式

【缺省级别】 14

【使用指导】 显示所有 app 认证相关的配置参数，该命令提供给 web 调用。

【配置举例】 1：显示 app 认证相关的配置参数。

```
Ruijie# show app-auth statistics
```

【提示信息】 -

【平台说明】 -

17.60 show app-auth tcp-info

显示 tcp 长连接相关配置

show app-auth tcp-info

【参数说明】

参数	描述
-	-

【命令模式】 全局模式、特权模式、接口模式

【缺省级别】 14

【使用指导】 显示 tcp 长连接相关配置

【配置举例】 1：显示 tcp 长连接相关配置

```
Ruijie#show app-auth tcp-info
tcp_server_url:
tcp_enable: 1
tcp_keepalive_period: 300
user_inform_period: 300
tcp_sock: -1
tcp_state: 1
server_ip: 0.0.0.0, port: 0
server_change: 1
rcv_pkt_num: 0
rcv_error_pkt_num: 0
keepalive_last_send_time: 0
keepalive_last_rcv_time: 0
```

```
user_inform_last_send_time: 0
user_inform_last_rcv_time: 0
```

【提示信息】 -

【平台说明】 -

17.61 show app-auth user

显示 app 认证通过的所有在线节点信息。

show app-auth user {all | online | by-ip *ip-addr* **| by-name** *name* **}**

【参数说明】

参数	描述
all	显示所有用户信息
online	显示在线用户信息
by-ip	通过 IP 指定查询
ip-addr	IP 地址
by-name	通过用户名查询
name	用户名

【命令模式】 全局模式、特权模式、接口模式

【缺省级别】 14

【使用指导】 显示 app 认证通过的所有在线节点信息。

【配置举例】 1：显示当前在线 ip 节点信息。

```
Ruijie# show app-auth online
ip          mac           status
```

ip：ip 地址

mac：mac 地址

status：该节点是否处于在线状态，effective、ineffective

app-id：通过哪种应用索引认证上线

【提示信息】 -

【平台说明】 -

17.62 show app-auth proxy-option config

查看 https 重定向信息。

show app-auth proxy-option config

【参数说明】

参数	描述
-	-

【命令模式】 全局模式、特权模式、接口模式

【缺省级别】 14

【使用指导】 显示 https 重定向信息。

【配置举例】

```
Ruijie#show app-auth proxy-option config
---------- App-Auth Option Config Info ----------
Redirect for https  : Enable
Session total limit : 20001
Session per-ip limit: 201
---------------------- End ---------------------
Ruijie#
```

Redirect for https：是否开启了 https 重定向

Session total limit：默认 https 连接限制总数

Session per-ip limit：当前每 ip https 连接限制数

【提示信息】 -

【平台说明】 -

18 webservice

18.1 webservice monitor-addr

设置监控地址

webservice monitor-addr *url* { **ip-range** *ip-start ip-end* }

删除监控地址

no webservice monitor-addr *url* { **ip-range** *ip-start ip-end* }

【参数说明】

参数	描述
url	配置监控服务器 url
ip-start	起始 ip
ip-end	终止 ip

【缺省配置】 默认不开启

【命令模式】 全局配置模式

【缺省级别】 14

【使用指导】 配置监控服务器地址。用于与 hz portal 联动场景，当用户上线成功后，会将用户信息推送给监控服务器。

【配置举例】 -

【检验方法】 1：使用 **show webservice hz-info** 命令查看。

```
Ruijie#show webservice hz-info
{"root":{"monitor-addr":"http://202.80.193.155:8090/"}, "branch": [] }
```

【提示信息】 -

【常见错误】

【平台说明】 -

18.2 webservice portal-check

设置 portal 检测

webservice portal-check [**enable | interval** *time_1* **| retransmit** *num*]

删除 portal 检测相关配置

no webservice portal-check [enable | interval | restransmit]

【参数说明】

参数	描述
enable	功能开启
interval	检测周期，默认 30 秒
time_1	检测周期，单位秒。默认 30 秒
retransmit	检测重试次数。即失败情况下，连续重试几次
num	检测重试次数，默认为 3

【缺省配置】 默认不开启

【命令模式】 全局配置模式

【缺省级别】 14

【使用指导】 1、 用于检测服务器是否存在。如检测到异常，则会关闭 app-auth 认证功能。服务器恢复后自动开启 app-auth。

2、 确认服务器支持该功能下才开启

【配置举例】 -

【检验方法】 1：使用 **show webservcie config** 命令查看。

```
Ruijie#show webservice config
service-url:
sec-service-url:
webs-online: 0
webs-tmponline: 1
redirect_302: 1
portal-check: on
portal-check retransmit: 3
portal-check interval: 30

portal-ping: on
portal-ping retransmit: 1
portal-ping interval: 300

client-sync: off
client-sync intveral: 30
```

```
get_wanip_enable: on
get_wanip_interval: 120
webs_sin_ip: 0.0.0.0
wx_auth_enable: 0
wx_auth intveral: 72000
```

【提示信息】 -

【常见错误】 服务器不支持情况下开启该功能导致用户无需认证

【平台说明】 -

18.3 webservice sec-service-url

设置服务器第二个地址
webservice sec-service-url *url*

删除服务器 url
no webservice sec-service-url

【参数说明】

参数	描述
url	配置服务器 url

【缺省配置】 默认不开启

【命令模式】 全局配置模式

【缺省级别】 14

【使用指导】 1、 配置服务器地址。用于与 wmc/mcp 联动场景，且配置微信连 wifi 和短信共存时， webserver-url 配置微信连 wifi 通讯地址， webservice sec-service-url 配置为 wifidog 通讯地址

【配置举例】 -

【检验方法】 1：使用 **show webservcie config** 命令查看。

【提示信息】 -

【常见错误】

【平台说明】 -

18.4 webservice service-url

设置服务器 url
webservice service-url *url*

删除服务器 url
no webservice service-url

【参数说明】

参数	描述
url	配置服务器 url

【缺省配置】 默认不开启

【命令模式】 全局配置模式

【缺省级别】 14

【使用指导】 1、 配置服务器地址。用于与 wmc/mcp 联动场景，且设备选择 wifido 或者微信连 wifi 协议时。

【配置举例】 -

【检验方法】 1：使用 **show webservcie config** 命令查看。

【提示信息】 -

【常见错误】

【平台说明】 -

18.5 webservice monitor fmt

设置监控服务器数据类型为”新网程”
webservice monitor fmt *xwc*

删除监控服务器格式

no webservice monitor fmt

【参数说明】

参数	描述
xwc	数据格式类型为”新网程”

【缺省配置】 默认不开启

【命令模式】 全局配置模式

【缺省级别】 14

【使用指导】 配置监控服务器地址。用于与新网程联动场景，当用户上线成功后，会将用户信息推送给监控服务器。

【配置举例】 -

【检验方法】 1：使用 **show run | i monitor fmt** 命令查看。

```
Ruijie# show run | i monitor fmt

webservice monitor fmt xwc
```

【提示信息】 -

【常见错误】

【平台说明】 网关系列产品

19 ANTI-PAP

19.1 anti-pap avoid-block

添加免阻断服务器资源。
anti-pap avoid-block ip-gourp *id*

删除免阻断服务器资源。
no anti-pap avoid-block ip-gourp *id*

恢复缺省配置。
default anti-pap avoid-block

【参数说明】

参数	描述
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

【缺省级别】 14

【使用指导】 当内网用户访问认证服务器等特殊资源的报文会经过设备时，需要配置该命令防止被阻断。

【配置举例】 1：添加免阻断服务器。

```
Ruijie(config)# anti-pap avoid-block ip-group 1
```

【检验方法】 1：执行 **show anti-pap config** 命令，可看到所配信息。

【提示信息】 -

【常见错误】 -

【平台说明】 -

19.2 anti-pap control

惩罚指定用户一段时间。

anti-pap control *addr* [*time*] { **block** | **limit down** *rate1* **up** *rate2*] } **base** { **user** | **ip** }

【参数说明】

参数	描述
addr	指定用户的 IP 地址。
time	阻断时间，取值范围 1～1440，单位：分。缺省为 10 分钟。
user	基于用户名阻断用户。
ip	基于 IP 阻断用户。

【命令模式】 特权模式

【缺省级别】 14

【使用指导】 -

【配置举例】 1：基于用户名阻断用户 20 分钟。

```
Ruijie# anti-pap control 192.168.1.2 20 block base user
```

【提示信息】 -

【常见错误】 -

【平台说明】 -

19.3 anti-pap monitor

对指定用户进行检测，同时指定/更新期望的终端类型，以及是否阻断。

anti-pap monitor { **subscriber** { *subs-name1* | **any** } | **auth-subscriber** { *subs-name2* | **any** } } [**expected-terminal pc**] [{ **block** [*time*] | **limit** [*time*] **down** *rate1* **up** *rate2* } **base** { **user** | **ip** }]

取消对指定用户进行检测。

no anti-pap monitor [**subscriber** { *subs-name1* | **any** } | **auth-subscriber** { *subs-name2* | **any** }]

恢复缺省配置。

default anti-pap monitor

【参数说明】

参数	描述
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	指定期望的终端类型为 PC。缺省为任意终端类型。
block	阻断用户网络。缺省不阻断。
time	控制(阻断、限速)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。
rate1	下行带宽，取值范围 1～1000。单位 Kbps。
rate2	上行带宽，取值范围 1～1000。单位 Kbps。
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

【缺省级别】 14

【使用指导】 用户名通常是配用户组名。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。

【配置举例】 1：对所有的期望终端类型为 PC 的认证用户进行检测，发现用户私接 AP 后阻断用户上网。

```
Ruijie(config)# anti-pap monitor auth-subscriber any expected-terminal pc block
```

【检验方法】 1：执行 **show anti-pap config** 命令，可看到所配信息。

【提示信息】 -

【常见错误】 -

【平台说明】 -

19.4 clear anti-pap control

取消对指定用户的惩罚。

clear anti-pap control *addr*

【参数说明】

参数	描述
addr	配置用户的 IP 地址

【命令模式】 特权模式

【缺省级别】 14

【使用指导】 -

【配置举例】 1：取消对用户的阻断。

```
Ruijie# clear anti-pap control 192.168.1.4
```

【提示信息】 -

【平台说明】 -

19.5 show anti-pap config

显示免阻断服务器和待检测用户对象的配置信息。

show anti-pap config

【参数说明】

参数	描述
-	-

【命令模式】 全局模式、特权模式

【缺省级别】 14

【使用指导】 -

【配置举例】 1：显示配置信息

```
Ruijie# show anti-pap config
{
    "code": 0,
    "msg": "",
    "data": {
        "avoid-block": [
            1
        ],
        "monitor": [
            {
                "User": "any",
                "Auth": "no",
                "Invalid": false,
                "Exp-Term": "any",
                "Ctrl": "block",
                "Time": 10,
                "ByUser": false
```

```
            }
        ]
    }
}
```

字段解释：

字段	说明
avoid-block	免阻断服务器资源。
User	用户名。
Auth	是否是认证用户。可能的值为 no 或 yes。
Invalid	是否是无效的
Exp-Term	期望的终端类型。可能的值如下： any - 不指定终端类型 pc - PC 终端
Ctrl	惩罚方式。可能的值如下： 空字符 – 不惩罚 block – 阻断 limit – 限速
Time	惩罚时长
ByUser	是否基于用户惩罚。否表示基于 IP 地址惩罚。

【提示信息】 -

【平台说明】 -

19.6 show anti-pap log

显示日志。

show anti-pap log detail 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*]

显示日志数量。

show anti-pap log stat from *y1 m1 d1* [*H1:M1:S1*] **to** *y2 m2 d2* [*H2:M2:S2*] [**subscriber** *subs-name1* | **auth-subscriber** *subs-name2*] [**ip** *addr*]

【参数说明】

参数	描述
y1 m1 d1	设置查询的起始年月日。
H1:M1:S1	设置查询的起始时分秒。缺省为 00:00:00。
y2 m2 d2	设置查询的终止年月日。
H2:M2:S2	设置查询的终止时分秒。缺省为 23:59:59。
subscriber *subs-name1* |	设置查询的本地用户名或认证用户名。缺省不限定用户。

auth-subscriber *subs-name2*	
ip *addr*	设置查询的 IP 地址，多个 IP 用 “,” 隔开。缺省不限定 IP。
time	设置查询结果按时间排序。
subscriber	设置查询结果按本地用户名排序。
auth-subscriber	设置查询结果按认证用户名排序。
ip	设置查询结果按 IP 地址排序。
asc	设置查询结果升序排列。
desc	设置查询结果降序排列。
start-item *num1* **end-item** *num2*	设置查询结果集合中的起始和结束位置。缺省查询所有记录。

【命令模式】 全局模式、特权模式

【缺省级别】 14

【使用指导】 -

【配置举例】 1：显示日志

```
Ruijie# show anti-pap log from 2016-10-11 0:0:0 to 2016-10-11 23:59:59 order-by time desc start-item
1 end-item 20
{
    "code": 0,
    "msg": "",
    "data": [
        {
            "IP": "192.168.203.8",
            "User": "pc4",
            "Auth": false,
            "Manual": false,
            "Time": "2017-02-16 11:38:39",
            "Reason": [
                "PC",
                "Mobile"
            ],
            "Ctrl": "block"
        }
    ]
}
```

字段解释：

字段	说明
IP	用户 IP 地址。
User	用户名（完整路径）。

Auth	是否是认证用户。可能的值为 no 或 yes。
Manual	是否是手动惩罚。
Time	日志产生时间，即用户被惩罚的时间。
Ctrl	惩罚方式。可能的值如下： 空字符 – 不惩罚 block – 阻断 limit – 限速
Reason	惩罚原因，及发现的终端信息，各类信息以分号分隔。可能的信息如下： PC - 检测到一台 PC 终端 PC* - 检测到多台 PC 终端 Mobile - 检测到一台移动终端 Mobile* - 检测到多台移动终端 VID - 检测到用户同时登录的虚拟身份账号数量超过了限制

【提示信息】 -

【平台说明】 -

19.7 show anti-pap user

显示用户检测信息。

show anti-pap user [**normal** | **controlled** | **subscriber** *subs-name1* | **auth-subscriber** *subs-name2* | **ip** *addr*]

【参数说明】

参数	描述
normal	设置查找的用户为正常用户。
controlled	设置查找的用户为私接用户。
subscriber *subs-name1* | **auth-subscriber** *subs-name2*	设置查找的本地用户名或认证用户名。
ip *addr*	设置查找的用户 IP 地址。

【命令模式】 全局模式、特权模式

【缺省级别】 14

【使用指导】 -

【配置举例】 1：显示用户的检测信息

```
Ruijie# show anti-pap user
```

```
{
    "code": 0,
    "msg": "",
    "data": [
        {
            "IP": "192.168.203.6",
            "User": "pc4",
            "Auth": false,
            "Controlled": false,
            "Ctrl": "block"
        },
        {
            "IP": "192.168.203.5",
            "User": "pc4",
            "Auth": false,
            "Controlled": true,
            "Manual": false,
            "Time": "2017-02-16 11:36:33",
            "Reason": [
                "PC",
                "Mobile"
            ],
            "Ctrl": ""
        }
    ]
}
```


字段解释：

字段	说明
IP	用户 IP 地址。
User	用户名。
Auth	是否是认证用户。
Controlled	是否被惩罚，即是否有私接行为。
Manual	是否是手动惩罚
Ctrl	惩罚方式。可能的值如下： 空字符串 – 不惩罚 block –阻断 limit – 限速
Time	Reason 字段最近更新的时间。
Reason	最近检测到的终端信息，可能的值与 **show anti-pap log** 命令输出的同名字段一样。

【提示信息】 -

【平台说明】 -

20 广告配置命令

20.1 advertising enable

在全局上启动广告服务。兼容原 **advertising webauth-free-user** 命令
advertising enable

在全局关闭动广告服务。
no advertising enable

【参数说明】

参数	描述
-	

【缺省配置】 缺省没有设置。

【命令模式】 全局配置模式。

【缺省级别】 14

【使用指导】 要成功应用广告服务，必须配置广告推送的网段范围和广告弹出框的页面地址。

【配置举例】 1：开启广告。

```
Ruijie(config)# advertising enable
```

【检验方法】 使用 **show advertising** 查看配置

【提示信息】 -

【常见错误】 -

【平台说明】 -

20.2 advertising free-user

设置广告推送的网段范围。兼容原 **webauth-free-user address <** *ip-address* **> mask <** *ip-mask***>**命令
advertising free-user ip < *ip-address* > **mask** < *ip-mask* >

删除某个网段范围。

no advertising free-user ip < *ip-address* > **mask** < *ip-mask* >

【参数说明】

参数	描述
ip-address	ip 地址，点分十进制格式。
ip-mask	子网掩码，点分十进制格式。

【缺省配置】 缺省未配置。

【命令模式】 全局配置模式。

【缺省级别】 14

【使用指导】 最大只支持 50 个网段的配置。

【配置举例】 1：设置某个网段。

```
Ruijie(config)# advertising free-user ip 192.168.198.1 mask 255.255.255.0
```

2：配置全网段。兼容原 **advertising all-user without-webauth** 命令

```
Ruijie(config)# advertising free-user ip 0.0.0.0 mask 255.255.255.255
```

【检验方法】

【提示信息】 1：配置第 51 条网段。

```
%Error: Has reached the 50 rules limit.
```

【常见错误】 -

【平台说明】 -

20.3 advertising min-interval

设置周期性拦截的时间间隔。

advertising min-interval *interval-value*

删除周期性拦截的时间间隔。

no advertising min-interval

【参数说明】

参数	描述
interval-value	间隔值<30-1440>，单位为分，默认 30 分钟。

【缺省配置】 开启周期性拦截后，缺省拦截周期间隔为 30 分钟。

【命令模式】 全局配置模式。

【缺省级别】 14

【使用指导】
10. 未开启周期性拦截，缺省为 0。
11. 开启周期性拦截，缺省为 30。
12. 开启周期性拦截后，删除该配置会出错。

【配置举例】 1：设置周期性拦截的时间间隔。

```
Ruijie(config)# advertising min-interval 30
```

【检验方法】 使用 **show advertising** 查看配置

【提示信息】 1：开启周期性拦截后，不允许删除时间间隔配置。

```
%Warning: Should set min-interval to default value: 30mins, due to advertising suppress.
```

【常见错误】 -

【平台说明】 -

20.4 advertising popup-page

开启确保广告弹出框不被浏览器拦截功能。兼容原 **web-auth advert popup-page** 命令
advertising popup-page

关闭确保广告弹出框不被浏览器拦截功能。
no advertising popup-page

【参数说明】

参数	描述
-	

【缺省配置】 缺省未配置。

【命令模式】 全局配置模式

【缺省级别】 14

【使用指导】 命令设为隐藏模式，所以，不支持简写模式。

【配置举例】 1：开启确保广告弹出框不被浏览器拦截功能。

```
Ruijie(config)# advertising popup-page
```

【检验方法】 使用 **show advertising** 查看配置

【提示信息】 -

【常见错误】 -

【平台说明】 -

20.5 advertising suppress

开启周期性拦截。
advertising suppress

关闭周期性拦截。
no advertising suppress

【参数说明】

参数	描述
-	

【缺省配置】 缺省没有开启。

【命令模式】 全局配置模式。

【缺省级别】 14

【使用指导】 开启周期性拦截后，默认周期间隔为 30 分钟。

【配置举例】 1：开启周期性拦截。

```
Ruijie(config)# advertising suppress
```

【检验方法】 使用 **show advertising** 查看配置

【提示信息】 -

【常见错误】 -

【平台说明】 -

20.6 advertising url

设置广告弹出框的页面地址。
advertising url *url-string*

删除广告弹出框的页面地址。
no advertising url

【参数说明】

参数	描述
url-string	页面地址，应以“http://”或“https://”开头，否则提示配置不成功，最大长度为255 个字符。

【缺省配置】 缺省没有设置。

【命令模式】 全局配置模式。

【缺省级别】 14

【使用指导】 -

【配置举例】 1：配置 url。

```
Ruijie(config)# advertising url http://www.baidu.com/
```

【检验方法】 使用 **show advertising** 查看配置

【提示信息】 1：非法 url 格式。

```
%Warning: Illegal URL, ignored. URL can not point to a file, URL must point to a HTML page.
```

【常见错误】 -

【平台说明】 -

20.7 show advertising

显示广告的基本配置。
show advertising

【参数说明】

参数	描述
-	-

【命令模式】 特权模式

【缺省级别】 14

【使用指导】 用于查看广告的基本参数配置情况。

【配置举例】 1：显示广告的基本配置。

```
Ruijie#show advertising
advertising enable:       On
advertising url:          http://www.baidu.com/
advertising suppress:     On
advertising popup-page:   On
advertising min-interval: 30
advertising free-user:
  192.168.198.0    255.255.255.0
  1.1.1.1          255.255.0.0
```

字段	说明
advertising popup-page	只在开启时显示。
advertising free-user	只在有网段配置时显示。

【提示信息】 -

【平台说明】 -

20.8 show advertising free-user

显示广告用户所属的网段范围。兼容原 **show webauth-free-user** 命令

show advertising free-user

【参数说明】

参数	描述
-	-

【命令模式】 特权模式

【缺省级别】 14

【使用指导】 用于查看广告用户所属的网段范围。

【配置举例】 1：显示广告用户所属的网段范围。

```
Ruijie#show advertising free-user
free-user configuration:
  Address         Mask
  --------------- ---------------
  192.168.198.0   255.255.255.0
  1.1.1.1         255.255.0.0
  2.2.2.2         255.0.0.0
```

字段	说明
Address	IP 地址。
Mask	IP 地址掩码。

【提示信息】 -

【平台说明】 -

20.9 show advertising user

显示广告用户超时(推送间隔)链表。兼容原 **show advertising tmo** 命令
show advertising user

【参数说明】

参数	描述
-	-

【命令模式】 特权模式

【缺省级别】 14

【使用指导】 用来查看广告用户超时(推送间隔)链表

【配置举例】 1：显示广告用户超时(推送间隔)链表。

```
Ruijie(config)#show adv user
Current online advertising user num: 1
Address         Online  Time Limit     Time used      Name
--------------- ------- -------------- -------------- ---------
192.168.198.34  On      0d 00:30:00    0d 00:08:50    AD_USER
```

字段	说明

Address	IP 地址。
Online	在线状态。
Time Limit	推送间隔
Time used	已在线时间
Name	默认用户名：AD_USER

【提示信息】 -

【平台说明】 -

21 Local-Account

21.1 debug local-account

打开 debug 开关。

debug local-account { client *num* **| http_proxy | server }**

关闭 debug 开关。

no debug local-account { client *num* **| http_proxy | server }**

【参数说明】

参数	描述
client	客户端 debug 开关
num	客户端编号
http_proxy	http 代理 debug 开关
server	服务器 debug 开关

【命令模式】 特权模式

【缺省级别】 14

【使用指导】 此命令用来查看本模块的调试信息

【配置举例】 1：开启客户端的 debug。

```
Ruijie# debug local-account server
```

【提示信息】 1：开启成功。

```
Ruijie#show debug
debug:
  local account debug debugging is on

Ruijie#
```

【平台说明】 -

21.2 description

配置用户的描述信息。

description *string*

【参数说明】

参数	描述
description *string*	用户的描述信息

【缺省配置】 无。

【命令模式】 local-account-user 模式

【缺省级别】 14

【使用指导】 无。

【配置举例】 1：为用户绑定 ip192.168.1.2

```
Ruijie# configure terminal
Ruijie(config)# local-account user test
Ruijie(local-account-user)# description test
Ruijie(local-account-user)# exit
Ruijie(config)# end
```

【检验方法】 1: 使用命令 show local-account users 可以查看用户描述信息情况。

```
Ruijie#show local-account users

(O) Online  (S) State: 0=Invalid 1=Normal 3=Overdue
-------------------------------------------------------------------------------
Name          O  S  Policy      Ip addr           Mac addr           Note
-------------------------------------------------------------------------------
test          0  3  2018/01/21  192.168.1.2       11:11:22:22:33:33  test

total:1    upper limit:150
Ruijie
```

【提示信息】 无。

【常见错误】 无

【平台说明】 -

21.3 ip

对用户进行 ip 绑定。

ip *a.b.c.d*

【参数说明】

参数	描述
ip *a.b.c.d*	用户绑定的 ip 地址

【缺省配置】 无。

【命令模式】 local-account-user 模式

【缺省级别】 14

【使用指导】 无。

【配置举例】 1：为用户绑定 ip192.168.1.2

```
Ruijie# configure terminal
Ruijie(config)# local-account user test
Ruijie(local-account-user)# ip 192.168.1.2
Ruijie(local-account-user)# exit
Ruijie(config)# end
```

【检验方法】 1: 使用命令 show local-account users 可以查看用户 ip 绑定情况。当 Ip addr 一列有 ip 的时候，表示这个用户有 ip 绑定。

```
Ruijie#show local-account users

(O) Online  (S) State: 0=Invalid 1=Normal 3=Overdue
-------------------------------------------------------------------------------------------
Name          O  S  Policy      Ip addr           Mac addr            Note
-------------------------------------------------------------------------------------------
test          0  3  2018/01/21  192.168.1.2       11:11:22:22:33:33   test

total:1    upper limit:150
Ruijie
```

【提示信息】 无。

【常见错误】 无

【平台说明】 -

21.4 local-account user

添加一个用户。

local-account user *username*

【参数说明】

参数	描述
user *username*	配置用户的用户名

【缺省配置】 无。

【命令模式】 全局模式

【缺省级别】 14

【使用指导】 无。

【配置举例】 1：添加用户 test

```
Ruijie# configure terminal
Ruijie(config)# local-account user test
Ruijie(local-account-user)# exit
Ruijie(config)# end
```

【检验方法】 1: 使用命令 show local-account users 可以查看用户状态。

```
Ruijie#show local-account users

(O) Online  (S) State: 0=Invalid 1=Normal 3=Overdue
-------------------------------------------------------------------------------------------
Name          O  S  Policy      Ip addr          Mac addr           Note
-------------------------------------------------------------------------------------------
test          0  3  2018/01/21  192.168.1.2      11:11:22:22:33:33  test

total:1    upper limit:150
```

```
Ruijie
```

【提示信息】 无。

【常见错误】 无

【平台说明】 -

21.5 local-account period

配置外部模块通告相关功能。

local-account period *time*

【参数说明】

参数	描述
period *time*	外部模块通告的时间间隔

【缺省配置】 无。

【命令模式】 全局模式

【缺省级别】 14

【使用指导】 无。

【配置举例】 1：配置通告时间间隔为 60s

```
Ruijie# configure terminal
Ruijie(config)# local-account period 60
Ruijie(config)# end
```

【检验方法】 1: 使用命令 show local-account config 可以查看用户状态。

```
Ruijie#show local-account config
users-limit: 150
acct-period: 60s
notice: on
notice-time: 5h
notice-interval: 10m
Ruijie
```

【提示信息】 无。

【常见错误】 无

【平台说明】 -

21.6 local-account notice

配置用户通告系统。

local-account notice { enable | date-rule *hour interval-min* **}**

【参数说明】

参数	描述
notice	用户通告系统
enable	开启用户通告
date-rule	按照日期规则进行通告
hour	距离到期多久前开始通告
interval-min	每次通告的时间间隔

【缺省配置】 无。

【命令模式】 全局模式

【缺省级别】 14

【使用指导】 无。

【配置举例】 1：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

```
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】 1: 使用命令 show local-account config 可以查看用户状态。

```
Ruijie#show local-account config
users-limit: 150
acct-period: 20s
notice: on
```

```
notice-time: 5h

notice-interval: 10m

Ruijie
```

【提示信息】 无。

【常见错误】 无

【平台说明】 -

21.7 mac

对用户进行 mac 绑定。

mac { *mac-address* | **auto** }

【参数说明】

参数	描述
mac	对 mac 进行绑定
mac-address	Mac 手动绑定
auto	Mac 自动绑定

【缺省配置】 无。

【命令模式】 local-account-user 模式

【缺省级别】 14

【使用指导】 无。

【配置举例】 1：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

```
Ruijie# configure terminal

Ruijie(config)# local-account user test

Ruijie(local-account-user)# mac 1111.2222.3333

Ruijie(local-account-user)# exit

Ruijie(config)# end
```

【检验方法】 1: 使用命令 show local-account config 可以查看用户状态。

```
Ruijie#show local-account users
```

```
(O) Online  (S) State: 0=Invalid 1=Normal 3=Overdue
-------------------------------------------------------------------------------------------
Name          O  S  Policy      Ip addr           Mac addr           Note
-------------------------------------------------------------------------------------------
test          0  3  2018/01/21  192.168.1.2       11:11:22:22:33:33  test

total:1    upper limit:150
Ruijie
```

【提示信息】 无。

【常见错误】 无

【平台说明】 -

21.8 policy

配置用户的计费策略。

policy date *yyyy mm dd*

【参数说明】

参数	描述
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

【缺省配置】 无。

【命令模式】 local-account-user 模式

【缺省级别】 14

【使用指导】 无。

【配置举例】 1：配置计费策略，用户可以使用到 2020 年 12 月 12 日

```
Ruijie# configure terminal
```

```
Ruijie(config)# local-account user test
Ruijie(local-account-user)# policy date 2020 12 12
Ruijie(local-account-user)# exit
Ruijie(config)# end
```

【检验方法】 1: 使用命令 show local-account users 可以查看用户状态。

```
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  2020/12/12  192.168.1.2       11:11:22:22:33:33   test

total:1    upper limit:150
Ruijie
```

【提示信息】 无。

【常见错误】 无

【平台说明】 -

21.9 show local-account config

查看本模块的配置信息。

show local-account config

【参数说明】

参数	描述
config	查看本模块的配置、参数信息

【缺省配置】 无。

【命令模式】 特权模式

【缺省级别】 14

【使用指导】 无。

【配置举例】 无。

【检验方法】 1: 使用命令 show local-account config 可以查看本模块的配置信息。

```
Ruijie# show local-account config

users-limit: 150

acct-period: 20s

notice: on

notice-time: 48h

notice-interval: 60m

Ruijie#
```

字段解释：

字段	说明
lacc	本地计费功能是否开启
users-limit	可使用的用户总数
acct-period	外部模块通告的时间间隔(s)
notice	到期用户通告系统是否开启
notice-time	距离到期多久前开始通告
notice-interval	每次通告的时间间隔

【提示信息】 无。

【常见错误】 无

【平台说明】 -

21.10 show local-account online

查看在线用户信息。

show local-account online [**by-name** *name*]

【参数说明】

参数	描述
online	查看在线用户
by-name	通过用户名过滤搜索
name	用户名

【缺省配置】 无。

【命令模式】 特权模式

【缺省级别】 14

【使用指导】 无。

【配置举例】 无。

【检验方法】 1: 使用命令 show local-account online by-name test1 可以查看该用户是否有在线信息。

```
Ruijie#show local-account online by-name test1


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

Name          Ip addr           Mac addr            Start                Online

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

test1         192.168.0.13      00:23:24:03:03:03   2018/01/22 14:06:43  0days 00:02:55


Total:1

Ruijie#
```

字段解释：

字段	说明
Name	用户名
Ip addr	用户 ip

Mac addr	用户 mac
Start	上线时间
Online	在线时长
Total	该帐号下一共有多少个用户

【提示信息】 无。

【常见错误】 无

【平台说明】 -

21.11 show local-account users

查看用户信息。

show local-account users [**by-name** *name*]

【参数说明】

参数	描述
users	查看用户
by-name	通过用户名过滤搜索
name	用户名

【缺省配置】 无。

【命令模式】 特权模式

【缺省级别】 14

【使用指导】 无。

【配置举例】 无。

【检验方法】 1: 使用命令 show local-account users 可以查看用户信息。

```
Ruijie# show local-account users


(O) Online  (S) State: 0=Invalid 1=Normal 3=Overdue
```

```
-------------------------------------------------------------------------------------------------
Name          O  S  Policy      Ip addr          Mac addr           Note
-------------------------------------------------------------------------------------------------
test1         0  1  N/A         N/A              N/A                testtest

Total:1    Upper limit:150
Ruijie#
```

字段解释：

字段	说明
Name	用户名
O	Online，表示是否在线
S	State，表示该用户处于的状态
Policy	该用户的计费策略
Ip addr	该用户 ip 绑定的属性
Mac addr	该用户 mac 绑定的属性
Note	该用户的备注信息
Total	当前用户总数
Upper limit	系统总的支持用户数

【提示信息】 无。

【常见错误】 无

【平台说明】 -

22 防火墙

22.1 网络防攻击

22.1.1 bypass

设置进入网络防攻击域的直通流量
bypass *src-ip-address* [**mask** *src-ip-mask*] [**proto** { **tcp** [**dest-port** *dest-port-num*] | **udp** [**dest-port** *dest-port-num*] | **icmp** | *protocol-num* }]

删除指定进入网络防攻击域的直通流量
no bypass *src-ip-address* [**mask** *src-ip-mask*] [**proto** { **tcp** [**dest-port** *dest-port-num*] | **udp** [**dest-port** *dest-port-num*] | **icmp** | *protocol-num* }]

恢复缺省配置。
default bypass *src-ip-address* [**mask** *src-ip-mask*] [**proto** { **tcp** [**dest-port** *dest-port-num*] | **udp** [**dest-port** *dest-port-num*] | **icmp** | *protocol-num* }]

【参数说明】

参数	描述
src-ip-address	源 IP 地址
src-ip-mask	源 IP 子网掩码
tcp	TCP 协议
udp	UDP 协议
icmp	ICMP 协议
protocol-num	协议编号
dest-port-num	目的端口号

【缺省配置】 无缺省配置

【命令模式】 config-defend-zone 配置模式

【缺省级别】 14

【使用指导】 命中一条则将此流量作为直通流量。

【配置举例】 例: 在出口网关/无线 AC 配置允许从主机 192.168.9.2 发出的 TCP 报文（目的端口为 80）直接穿过网络防攻击域 web

```
Ruijie(config)# defend-zone web
```

```
Ruijie(config-defend-zone)# bypass 192.168.9.2 proto tcp dest-port 80
Ruijie(config-defend-zone)# exit
```

【检验方法】 使用 **show running** 命令，可以查看协议类防攻击是否配置成功。

【提示信息】 -

【常见错误】 -

【平台说明】 -

22.1.2 blacklist

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

blacklist *ip-address*

删除指定黑名单

no blacklist [*ip-address*]

恢复缺省配置。

default blacklist [*ip-address*]

【参数说明】

参数	描述
ip-address	列入黑名单的主机 IP 地址

【缺省配置】 无缺省配置

【命令模式】 config-defend-zone 配置模式

【缺省级别】 14

【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

【配置举例】 例: 禁止主机 192.168.9.2 的报文穿过网络防攻击域 web

```
Ruijie(config-defend-zone)# blacklist 192.168.9.2
Ruijie(config-defend-zone)# exit
```

【检验方法】 使用 **show running** 命令，可以查看协议类防攻击是否配置成功。

【提示信息】 -

【常见错误】 -

【平台说明】 -

22.1.3 clear defend

清空防攻击的丢包统计信息。

clear defend drop

【参数说明】

参数	描述
-	-

【命令模式】 特权模式

【缺省级别】 14

【使用指导】 该命令将清空防攻击的丢包统计信息

【配置举例】 例: 清空防攻击的丢包计数统计

```
Ruijie# clear defend drop
```

【提示信息】 -

【平台说明】 -

22.1.4 clear defend-zone

清空网络防攻击域统计信息。

clear defend-zone *net-defend-zone-name* **counters**

清空全局防护统计信息。

clear defend-zone global counters

【参数说明】

参数	描述
net-defend-zone-name	网络防攻击对象名称
global	网络防攻击的全局防护

【命令模式】 特权模式

【缺省级别】 14

【使用指导】 该命令将清空数据收发统计信息和流量监视中的 topn 列表

【配置举例】 例: 清空网络防攻击域 web 的计数统计

```
Ruijie# clear defend-zone web counters
```

【提示信息】 -

【平台说明】 -

22.1.5 defend

启动指定的协议类攻击防御。

defend { **winnuke | source-route | route-record | icmp-unreachable | fraggle | land | large-icmp** [*icmp-length*] }

关闭指定的协议类攻击防御。

no defend { **winnuke | source-route | route-record | icmp-unreachable | fraggle | land | large-icmp** }

恢复缺省配置。

default defend { **winnuke | source-route | route-record | icmp-unreachable | fraggle | land | large-icmp** }

【参数说明】

参数	描述
winnuke	配置防火墙的防 winnuke 攻击，winnuke 攻击包被丢弃。
source-route	配置防火墙的防源路由攻击，发现该选项的 IP 包被丢弃。
route-record	配置防火墙的防 route-record 攻击，发现该选项的 IP 包被丢弃。
icmp-unreachable	配置防火墙的防 icmp 不可达攻击，收到 icmp 不可达报文被丢弃。
fraggle	配置防火墙的防 fraggle 攻击功能.
land	用于配置防火墙的防 Land 攻击，收到源 IP 等于目的 IP 报文被丢弃
large-icmp	配置防火墙的防超长 icmp 攻击
icmp-length	允许的 icmp 报文长度（单位字节），超过该长度 icmp 包被丢弃，缺省值是 4000 字节。取值范围：28~ 65499。

【缺省配置】 防 Land 攻击缺省启用

【命令模式】 全局配置模式

【缺省级别】 14

【使用指导】 启动各类协议类攻击防御。

⚠ 有时一些特殊的合法应用（如 BFD）可能出现源 IP 地址等于目的 IP 地址的情况，这时防火墙需要关

闭防止 Land 攻击的功能

【配置举例】 例: 启用 winnuke 防攻击

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

【检验方法】 1：使用 **show running** 命令，可以查看协议类防攻击是否配置成功。
2：使用 **show defend drop** 命令，可以查看协议类防攻击丢包情况。

【提示信息】 -

【常见错误】 无

【平台说明】 -

22.1.6 defend-zone

配置网络防攻击域。
defend-zone *net-defend-zone-name*

删除网络防攻击域
no defend-zone *net-defend-zone-name*

恢复缺省配置。
default defend-zone *net-defend-zone-name*

【参数说明】

参数	描述
net-defend-zone-name	网络防攻击域名称。

【缺省配置】 无

【命令模式】 全局配置模式

【缺省级别】 14

【使用指导】 设备通过配置网络防攻击域来针对不同保护对象实施独立的防护措施和防护管理。每个网络防攻击域至少包含了攻击防护主机集合的定义（关联 ACL）和防护策略两个部分。
路由模式下，如果保护的接口直连网段较大，例如掩码为 16 位左右，则需要在路由模式防攻击域中配置防扫描策略，避免扫描攻击导致交换机异常

【配置举例】

【检验方法】 1：使用 **show running** 命令，可以查看协议类防攻击是否配置成功。
2： 使用 **show defend-zone** *net-defend-zone-name* 可见网络防攻击域状态。

【提示信息】 -

【常见错误】

【平台说明】 -

22.1.7 defend-zone global

配置全局防攻击
defend-zone global

关闭全局防攻击。
no defend-zone global

恢复缺省配置。
default defend-zone global

【参数说明】

参数	描述
-	-

【缺省配置】 全局防攻击缺省启用

【命令模式】 全局配置模式

【缺省级别】 14

【使用指导】 全局防攻击可以直接对当前设备下的所有流量进行分类限制。这种全局防护可以有效的防御 TCP flooding，并且通过对 UDP、ICMP、Other-protocol 的报文进行新建速率限制的方式，限制这些攻击。实施这些防御和限制可以有效地增强防火墙自身免受攻击，同时也能减少各类 Flooding 流量对网络资源的占用。
全局防护缺省启用。测试防火墙性能与容量的时候需要关闭全局防护。

【配置举例】 例: 进入全局防攻击配置

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

【检验方法】 1：使用 **show running** 命令，可以查看全局防护是否配置成功。

2：使用 **show defend drop** 命令，可以查看全局防攻击丢包情况。

【提示信息】 -

【常见错误】 -

【平台说明】 -

22.1.8 description

配置网络防攻击域的描述信息。
description *description-string*

关闭。
no description

恢复缺省配置。
default description

【参数说明】

参数	描述
description-string	网络防攻击域的描述信息，不超过 100 个字符

【缺省配置】 无描述信息

【命令模式】 config-defend-zone

【缺省级别】 14

【使用指导】 过此命令可以配置网络防攻击域的描述信息

【配置举例】 例: 为网络防攻击域 web 设置描述信息

```
Ruijie(config)#  defend-zone web
Ruijie(config-defend-zone)# description “Defend policy for zone abc”
```

【检验方法】 使用 **show defend-zone** *net-defend-zone-name* 可见网络防攻击域的描述信息。

【提示信息】 -

【常见错误】 无

【平台说明】 -

22.1.9 detect

配置扫描的检测敏感度、周期和持续次数.

detect { **low | medium | high** } { **period** *time-interval* | **times** *last-times* }

删除扫描的检测敏感度、周期和持续次数的配置。

no detect { **low | medium | high** } { **period** | **times** }

恢复缺省配置。

default detect { **low | medium | high** } { **period** | **times** }

【参数说明】

参数	描述
low	低敏感度检测
medium	中等敏感度检测
high	高敏感度检测
time-interval	扫描检测周期。取值范围 1~2000，单位秒
last-times	扫描行为的持续周期数。即扫描行为连续次数达到此数值才被认定为扫描。取值范围 1~10，缺省为 1

【缺省配置】 各参数的缺省配置下，通过执行“**show scan parameter**”可以得到。具体参数值在 **show scan parameter** 中说明。

【命令模式】 config-scan-policy 配置模式

【缺省级别】 14

【使用指导】 设置每个级别的扫描敏感度。

【配置举例】 例: 设置低敏感度检测周期为 100 秒

```
Ruijie(config)# scan policy
Ruijie(config-scan-policy)# detect low period 100
```

【检验方法】 使用 **show scan parameter** 命令，可以查看参数调整结果。

【提示信息】 -

【常见错误】 -

【平台说明】 -

22.1.10 icmp auth-src-in

针对来自真实源主机的 ICMP 流量的策略。

icmp auth-src-in src-ip threshold *threshold-num* [**timeout** *seconds*] **action** { **limit | blocking | notify** }

删除针对来自真实源主机的 ICMP 流量的策略。

no icmp auth-src-in src-ip

恢复缺省配置。

default icmp auth-src-in src-ip

【参数说明】

参数	描述
auth-src-in	进入网络防攻击域的来自真实性源主机的报文。
src-ip	该策略针对每个源主机进行识别
threshold *threshold-num*	pps, 取值 1~100,000,000
timeout *seconds*	策略的最小执行时间，单位秒，缺省值为 60。可配置范围 10～86400 秒。
limit	限制对应的流量在 *threshold-num* 以下
blocking	阻塞该主机进出防攻击域的双向流量
notify	仅记录此次攻击

【缺省配置】 无策略

【命令模式】 config-defend-zone 配置模式

【缺省级别】 14

【使用指导】 当任何真实源主机发出的进入网络防攻击域的 ICMP 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)或者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 ）。策略执行时间不少于 *seconds.*

【配置举例】 例: 为网络防攻击域 web 创建防御来自真实源主机的 ICMP flood 的策略。当每个源主机（通过源验证）向网络防攻击域 web 发送的 ICMP 报文超过每秒 100 个时，阻塞这个主机的所有流量（至少 60 秒）

```
Ruijie(config)# defend-zone web
Ruijie(config-defend-zone)# icmp auth-src-in src-ip threshold 100 action blocking
Ruijie(config-defend-zone)# exit
```

【检验方法】 -

【提示信息】 -

【常见错误】 -

【平台说明】 -

22.1.11 icmp pkt-in

限制进入网络防攻击域的 ICMP 流量。
icmp pkt-in { **dst-ip | global** } **threshold** *threshold-num* [**timeout** *seconds*] **action** { **limit | notify** }

删除限制进入网络防攻击域的 ICMP 流量策略
no icmp pkt-in { **dst-ip |global** }

恢复缺省配置。
default icmp pkt-in { **dst-ip |global** }

【参数说明】

参数	描述
pkt-in	进入网络防攻击域的所有类型的报文。
threshold *threshold-num*	pps, 取值 1~100,000,000
timeout *seconds*	策略的最小执行时间，单位秒，缺省值为 60。可配置范围 10～86400 秒
dst-ip	针对每个目的主机进行识别
global	针对整个域进行识别
limit	限制对应的流量在 *threshold-num* 以下
notify	仅记录此次攻击

【缺省配置】

【命令模式】 config-defend-zone 配置模式

【缺省级别】 14

【使用指导】 当进入网络防攻击域的 ICMP 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。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 ICMP 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。

【配置举例】 例: 为网络防攻击域 web 创建防御 ICMP flood 策略。当针对网络防攻击域 web 中每一台目的主机的 ICMP 报文速率超过每秒 100 个时，对此该主机的 ICMP 流量进行限制（不超过每秒 100 个）。

```
Ruijie(config)# defend-zone web
Ruijie(config-defend-zone)# icmp pkt-in dst-ip threshold 100 action limit
Ruijie(config-defend-zone)# exit
```

【检验方法】 -

【提示信息】 -

【常见错误】 -

【平台说明】 -

22.1.12 icmp unauth-src-in

启用针对未通过真实源验证的 ICMP 流量的策略。
icmp unauth-src-in { **dst-ip** | **global** } **threshold** *threshold-num* [**timeout** *seconds*] **action** { **limit** | **drop** | **notify** }

删除针对未通过真实源验证的 ICMP 流量的策略
no icmp unauth-src-in { **dst-ip** | **global** }

恢复缺省配置
default icmp unauth-src-in { **dst-ip** | **global** }

【参数说明】

参数	描述
unauth-src-in	进入网络防攻击域的未通过真实源验证的报文。
threshold *threshold-num*	pps，取值 1~100,000,000
timeout *seconds*	策略的最小执行时间，单位秒，缺省值为 60。可配置范围 10～86400 秒
dst-ip	针对每个目的主机进行识别
global	针对整个域进行识别
limit	限制对应的流量在 *threshold-num* 以下
drop	丢弃对应的流量
notify	仅记录此次攻击

【缺省配置】 -

【命令模式】 config-defend-zone 配置模式

【缺省级别】 14

【使用指导】 当进入网络防攻击域的未通过真实源验证的 ICMP 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）或者全部丢弃此类报文。
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 ICMP 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

【配置举例】 例: 为网络防攻击域 web 创建防御伪造源的 ICMP flood 策略。当针对网络防攻击域 web 中每一台目的主机的疑似伪造源 ICMP 报文的速率超过每秒 100 个时，对该主机的疑似伪造源 ICMP 流量进行限制（不超过每秒

100 个），当攻击停止后，此限制策略将保持 1 小时。

```
Ruijie(config)# defend-zone web
Ruijie(config-defend-zone)# icmp unauth-src-in global threshold 100 timeout 3600 action rate-limit
```

【检验方法】 -

【提示信息】 -

【常见错误】 -

【平台说明】 -

22.1.13 ignore

设置扫描检测忽略对应的扫描类别

ignore protocol { **tcp** | **udp** | **icmp** | **other-protocol** }

取消扫描检测忽略对应的扫描类别

no ignore protocol { **tcp** | **udp** | **icmp** | **other-protocol** }

恢复缺省配置

default ignore protocol { **tcp** | **udp** | **icmp** | **other-protocol** }

【参数说明】

参数	描述
icmp	ICMP 协议
other-protocol	除了 TCP，UDP，ICMP 以外的协议
tcp	TCP 协议
udp	UDP 协议

【缺省配置】 针对所有类别实施扫描检测

【命令模式】 config-scan-policy 配置模式

【缺省级别】 14

【使用指导】 忽略对应的扫描类别，用户可以选择忽略某一种协议的扫描行为。该命令可以配置多条。

【配置举例】 例: 防扫描检测忽略 TCP 类型的扫描

```
Ruijie(config)# scan policy
Ruijie(config-scan-policy)# ignore protocol tcp
```

【检验方法】 -

【提示信息】 -

【常见错误】 -

【平台说明】 -

22.1.14 ip access-group

配置网络防攻击域关联的 ACL

ip access-group *access-list*

取消网络防攻击域的 ACL 关联

no ip access-group

恢复缺省配置

default ip access-group

【参数说明】

参数	描述
access-list	关联的 ip 标准 acl 名称

【缺省配置】 无关联

【命令模式】 config-defend-zone 配置模式

【缺省级别】 14

【使用指导】 通过配置网络防攻击域关联的 ACL 来划定网络防攻击域的防护区域。

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。

【配置举例】 例: 设置网络防攻击域 web 防护的主机为 192.168.3.X 网段的所有主机（定义在 ACL server 中）。

```
Ruijie(config)# ip access-list standard server
```

```
Ruijie(config-std-nal)#10 permit 192.168.3.0 0.0.0.255
Ruijie(config-std-nal)#exit
Ruijie(config)# defend-zone web
Ruijie(config-defend-zone)# ip access-group server
Ruijie(config-defend-zone)# exit
```

【检验方法】 使用 **show defend-zone** 命令查看当前关联的 ACL 以及 ACL 是否正确关联上。

【提示信息】 -

【常见错误】 -

【平台说明】 -

22.1.15 log

开启对应类型攻击的日志

log { **tcp-auth | tcp-unauth | icmp | udp | other-protocol | scan | all** } [**syslog** | **save**]

关闭对应攻击类型的日志记录

no log { **tcp-auth | tcp-unauth | icmp | udp | other-protocol | scan | all** } [**syslog** | **save**]

恢复缺省配置。

default log { **tcp-auth | tcp-unauth | icmp | udp | other-protocol | scan | all** } [**syslog** | **save**]

【参数说明】

参数	描述
tcp-auth	对于所有由真实源产生的 TCP 攻击记录日志。
tcp-unauth	对于所有的未通过真实源验证的 TCP 攻击记录日志。
Icmp	对于所有的 ICMP 攻击记录日志。
udp	对于所有的 UDP 攻击记录日志。
other-protocol	对于所有的其他协议类型（除了 TCP，UDP，ICMP）攻击记录日志。
scan	对于扫描攻击记录日志
all	对于所有类型攻击记录日志
syslog	将攻击日志以 SYSLOG 的形式打印出来。
save	将攻击信息保存到数据库中。

【缺省配置】 无缺省配置

【命令模式】 config-defend-zone 配置模式

【缺省级别】 14

【使用指导】 开启对应类型攻击的日志。all 关键字表示开启所有类型的攻击日志。当不带有 syslog 或者 save 参数时表示将攻击信息同时记录到数据库以及通过 syslog 打印出来。

【配置举例】 例: 将所有 ICMP 攻击日志存档

```
Ruijie(config)# defend-zone web

Ruijie(config-defend-zone)# log icmp save

Ruijie(config-defend-zone)# exit
```

【检验方法】 发生攻击后，通过 **show defend-zone** *net-defend-zone-name* **report** 命令来查看攻击结果。

【提示信息】 -

【常见错误】 -

【平台说明】 -

22.1.16 net-defend enable

启动网络防攻击功能
net-defend enable

关闭网络防攻击功能
no net-defend enable

恢复缺省配置
default net-defend enable

【参数说明】

参数	描述
-	-

【缺省配置】 未启动

【命令模式】 全局配置模式

【缺省级别】 14

【使用指导】 需要使用网络防攻击的时候开启，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。

【配置举例】 例: 启动网络防攻击功能

```
Ruijie(config)# net-defend enable
```

【检验方法】 -

【提示信息】 -

【常见错误】 -

【平台说明】 出口网关支持该命令，防火墙缺省开启网络反攻击功能，不支持此命令

22.1.17 net-defend learning

启动针对网络防攻击域的防御策略自学习功能
net-defend learning *net-defend-zone-name* [**days** *days*]

启动全局防护的防御策略自学习功能
net-defend learning global [**days** *days*]

【参数说明】

参数	描述
net-defend-zone-name	网络防攻击对象名称
global	网络防攻击的全局防护
days	策略学习的天数

【命令模式】 特权模式

【缺省级别】 14

【使用指导】 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。在策略的学习期间，系统会为启动策略学习的网络防攻击域默认启用基于会话的 TCP SYN flooding 攻击防御策略，防止网络防攻击域在策略学习期间遭受此类攻击。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。

【配置举例】 例：启动针对网络防攻击域 web 的策略学习，学习时间为 7 天

```
Ruijie(config)# defend-zone web
Ruijie(config-defend-zone)#  ip access-group server
Ruijie(config-defend-zone)# exit
Ruijie# net-defend learning web
Net defend policies learning for defend-zone ‘web’ begin. (Period:  7 days)
```

【提示信息】 1. 正常配置成功

```
Ruijie# net-defend learning web
Net defend policies learning for defend-zone ‘web’ begin. (Period:  7 days)
```

2. 已经有防御策略时，无法启动策略学习

```
Ruijie#net-defend learning web
Learning policy for ’web’ fail: policies have been configured.
```

【平台说明】 -

22.1.18 net-defend mode

设置网络反攻击的模式

net-defend mode { **nat** | **no-nat** }

取消网络反攻击的模式设置

no net-defend mode { **nat** | **no-nat** }

恢复缺省配置

default i net-defend mode { **nat** | **no-nat** }

【参数说明】

参数	描述
nat	NAT 模式
no-nat	非 NAT 模式

【缺省配置】 网关模式缺省为 NAT 模式；网桥模式缺省为非 NAT 模式。

【命令模式】 全局配置模式

【缺省级别】 14

【使用指导】 环境中部署了 NAT 则需要设置网络反攻击的模式为 NAT 模式。网桥模式不支持 NAT，不可配置 NAT 模式。

【配置举例】 例: 设置网络反攻击为 nat 模式

```
Ruijie(config)# net-defend mode nat
```

【检验方法】 -

【提示信息】 -

【常见错误】 -

【平台说明】 出口网关支持该命令，防火墙不支持 nat，不支持此命令

22.1.19 ratelimit

设置出入网络防攻击域的流量带宽限制
ratelimit { **in | out** } [**src-ip | dst-ip**] **bandwidth** *bps-num*

取消出入网络防攻击域的流量带宽限制
no ratelimit { **in | out** } [**src-ip | dst-ip**]

恢复缺省配置。
default ratelimit { **in | out** } [**src-ip | dst-ip**]

【参数说明】

参数	描述
in	针对进入网络防攻击域的流量实施限制
out	针对外出网络防攻击域的流量实施限制
src-ip	针对每个源 IP 实施限制
dst-ip	针对每个目的 IP 实施限制
bps-number	限制的带宽，单位 bps，取值范围 1~1,000,000,000 bps

【缺省配置】 无缺省配置

【命令模式】 config-defend-zone 配置模式

【缺省级别】 14

【使用指导】 **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

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。

【配置举例】 例: 限制进入网络防攻击域 web 的总体带宽不超过 100,000,000bps

```
Ruijie(config)# defend-zone web
Ruijie(config-defend-zone)# ratelimit in bandwidth 100000000
```

```
Ruijie(config-defend-zone)# exit
```

【检验方法】 -

【提示信息】 -

【常见错误】 -

【平台说明】 -

22.1.20 session-limit

全局防护

设置会话的建立速度限制

session-limit { **unauth-src-new-session | tcp | udp | icmp | other-protocol** } *new-session-per-second*

取消会话的建立速度限制

no session-limit { **unauth-src-new-session | tcp | udp | icmp | other-protocol** }

恢复缺省配置

default session-limit { **unauth-src-new-session | tcp | udp | icmp | other-protocol** }

防攻击域

设置出入网络防攻击域的会话建立速度限制

session-limit { in | out } [src-ip | dst-ip] session-rate *new-session-per-second*

取消会话的建立速度限制

no session-limit { in | out } [src-ip | dst-ip]

恢复缺省配置

default session-limit { in | out } [src-ip | dst-ip]

【参数说明】

参数	描述
new-session-per-second	每秒新建会话数量,取值范围 1~1,000,000
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
in	针对进入网络防攻击域的会话建立速度实施限制
out	针对外出网络防攻击域的会话建立速度实施限制
src-ip	针对每个源 IP 实施限制

dst-ip	针对每个目的 IP 实施限制

【缺省配置】 全局防护的 session-limit 命令缺省值如下：

unauth-src-new-session: 300000
tcp: 300000
udp: 300000
icmp: 100000
other-protocol: 100000

防攻击域内的 session-limit 命令缺省不启用。

【命令模式】 config-defend-zone 配置模式

【缺省级别】 14

【使用指导】 限制各类会话建立速率。
全局防护缺省启用。测试防火墙性能与容量的时候需要关闭全局防护。

【配置举例】 例: 限制经过设备的所有未通过源验证的会话的每秒新建速率低于 1 万

```
Ruijie(config)# defend-zone global
Ruijie(config-defend-zone)# session-limit unauth-src-new-session  10000
```

【检验方法】 -

【提示信息】 -

【常见错误】 -

【平台说明】 -

22.1.21 scan

设置防扫描策略
scan { **in | out** } **src-ip threshold** { **low** | **medium** | **high** } [**timeout** *seconds*] **action** { **blocking** | **notify** }

取消防扫描策略
no scan { **in | out** } **src-ip**

恢复缺省配置
default scan { **in | out** } **src-ip**

【参数说明】

参数	描述

in	针对进入网络防攻击域方向的流量进行检测
out	针对外出网络防攻击域方向的流量进行检测
low	使用低敏感度进行检测
medium	使用中等敏感度进行检测
high	使用高敏感度进行检测
timeout *seconds*	策略的最小执行时间，单位秒，缺省值为 60。可配置范围 10～86400 秒
notify	仅记录攻击
blocking	发现攻击后阻塞该攻击的所有流量

【缺省配置】 无

【命令模式】 config-defend-zone 配置模式

【缺省级别】 14

【使用指导】 防御网络防攻击域内外的扫描行为。
路由模式下，如果保护的接口直连网段较大，例如掩码为 16 位左右，则需要在路由模式防攻击域中配置防扫描策略，避免扫描攻击导致交换机异常

【配置举例】 例: 检测外部对网络防攻击域 web 内的扫描行为，采用低敏感度进行检测。当发现扫描行为后，阻塞该主机进出网络防攻击域 web 的所有流量，阻塞的时间为 1800 秒

```
Ruijie(config)# defend-zone web
Ruijie(config-defend-zone)# scan in src-ip threshold low timeout 1800 action blocking
Ruijie(config-defend-zone)# exit
```

【检验方法】 -

【提示信息】 -

【常见错误】 -

【平台说明】 -

22.1.22 scan policy

重新定义缺省的防扫描参数
scan policy

删除定义缺省的防扫描参数
no scan policy

恢复缺省配置。

default scan policy

【参数说明】

参数	描述
-	-

【缺省配置】 各参数的缺省配置下，通过执行“**show scan parameter**”可以得到。具体参数值在 **show scan parameter** 中说明。

【命令模式】 全局配置模式

【缺省级别】 14

【使用指导】 用户进入防扫描参数定制界面。该命令将在防扫描策略可以重新定义缺省的防扫描参数。

【配置举例】 例: 进入防扫描配置

```
Ruijie(config)# scan policy
Ruijie(config-scan-policy)# exit
```

【检验方法】 使用 **show scan parameter** 命令，可以查看参数调整结果。

【提示信息】 -

【常见错误】 -

【平台说明】 -

22.1.23 show defend

查看网络防攻击功能的整体丢弃统计

show defend drop

【参数说明】

参数	描述
-	-

【命令模式】 特权模式

【缺省级别】 14

【使用指导】 查看防攻击全局丢包统计

【配置举例】 例：查看防攻击所有的丢弃信息：

```
Ruijie# show defend drop
```

```
    Drops packet:          1,192
         Winnuke:          20
         Land:             80
         Global protect:   102
         Zone 'web':       890
         Zone 'ftp':       100
    Drops flow:            120
         Global protect:   50
     Zone 'web':       270
```

字段解释：

字段	说明
Drops packet	丢弃的报文
Drops flow	丢弃的流数
Winnuke	防御 Winnuke 攻击
Land	防御 land 攻击
Global protect	全局防攻击
Zone	网络防攻击域

【提示信息】 如果对应的攻击没有丢弃任何报文，则不显示此项内容。

【平台说明】 -

22.1.24 show defend module

显示当前防攻击业务模块的整体工作状态

show defend module

【参数说明】

参数	描述

【命令模式】 特权模式

【缺省级别】 14

【使用指导】 查看当前防攻击业务模块的接入情况。

【配置举例】 查看当前防攻击业务模块的接入情况：

```
Ruijie# show defend module
    Defend services module: 2
     Group     Slot     CPU      State
----------------------------------------
      0        3         0       Connect
```

```
    0        5        1        Online
```

字段解释：

字段	说明
Defend services module	当前接入的防攻击业务模块数量
Group	防攻击业务组
Slot	业务模块所在的插槽
CPU	业务模块所在的 CPU 编号
State	业务模块当前的状态
Connect	已经完成连接，尚未完成业务配置
Online	完成连接并且已经完成业务配置

【提示信息】 -

【平台说明】 -

22.1.25 show defend-zone

查看网络防攻击域的各种状态、统计参数

show defend-zone *net-defend-zone-name* [**counters | host**]

查看全局防护的统计参数

show defend-zone global counters

【参数说明】

参数	描述
net-defend-zone-name	网络防攻击域名称
global	网络防攻击的全局防护
counters	各类统计计数
host	查看主机耗费计数

【命令模式】 特权模式

【缺省级别】 14

【使用指导】 查看网络防攻击域的各种状态、统计参数、攻击信息等

【配置举例】 1：查看网络防攻击域的状态

```
Ruijie# show defend-zone web
    Description : web-servers-protect-zone
    Zone state: Running
    ACL associated: server-zone
    Traffic monitor: tcp, http, udp, icmp, ip
```

字段解释：

字段	说明
Description	该域的描述信息
Zone state	该域的状态。有运行：Running；停止：Stopped 和学习 Learning 三种状态
ACL associated	关联的 ACL 名称
Traffic monitor	开启的流量监视

2：查看网络防攻击域的统计计数

```
Ruijie# show defend-zone web counters
    Counters :
        Received:            8234
        Forwarded:           7981
        Dropped(packets):    20
        Dropped(flows):      10
        Replied:             105
    Dropped:
        Black-list:          0
        rate-limit:          5
        policy-drop(packets):15
        policy-drop(flows): 5
```

字段解释：

字段	说明
Received	该域总接收处理的报文数
Forwarded	转发的报文数
Dropped(packets)	丢弃的报文数
Dropped(flows)	丢弃的流数
Replied	应答的报文数。应答报文的目的是用于 TCP SYN cookie
Dropped	丢弃列表
Black-list	黑名单丢报文数
rate-limit	限速策略丢失报文数
policy-drop(packets)	其他策略丢弃的报文数
policy-drop(flowss)	其他策略丢弃的流数

3. 查看域相关的主机对象统计信息

```
Ruijie# show defend-zone web host
    Host protected (inside defend object): 178
    Host monitored (outside defend object): 5732
    Free host objects: 8372783 (Total)
```

字段解释：

字段	说明
Host protected (inside defend object)	网络防攻击域内建立的监视主机数量
Host monitored (outside defend object)	网络防攻击域外建立的监视主机数量
Free host objects	整机空闲的主机对象数量

【提示信息】 -

【平台说明】 -

22.1.26 show defend-zone traffic-snapshot

查看网络防攻击域的当前的流量快照

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**] }

【参数说明】

参数	描述
net-defend-zone-name	网络防攻击域名称
tcp	针对 TCP 数据流的统计
http	针对 HTTP 数据流的统计
ip	针对 IP 数据流的统计
udp	针对 UDP 数据流的统计
icmp	针对 ICMP 数据流的统计
syns-in	进入网络防攻击域的 TCP SYN 报文的速率
conn-in	进入网络防攻击域的并发连接数
half-conn-in	进入网络防攻击域的半连接数
bandwidth	进入网络防攻击域的带宽
topn	列出前 10 名的主机
pkts	每秒报文数

【命令模式】 特权模式

【缺省级别】 14

【使用指导】 查看网络防攻击域的当前流量快照。可以通过输入参数来只显示特定类型的流量快照。

【配置举例】 1. 查看当前所有流量的快转

```
Ruijie# show defend-zone web traffic-snapshot
                    Total Pkts    current bps
  Received          1234567891    12567893
  Dropped           1934823       289302
```

```
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
```

字段解释：

字段	说明
Total Pkts	报文数量
current bps	当前波特率
Received	接收统计
Dropped	丢弃统计
Replied	应答统计
Syns in	进入网络防攻击域的 SYN 报文的速率
Connections(in)	进入网络防攻击域的并发连接数
Half-connections (in)	进入网络防攻击域的半连接数
Bandwidth (in)	进入网络防攻击域的带宽

Bandwidth (out)	外出网络防攻击域的带宽
Pkts (in)	进入网络防攻击域的报文数
Pkts (out)	外出网络防攻击域的报文数

2. 查看当前 tcp 新建连接速率快照并且给出当前 tcp 新建连接速率数最多的主机

```
Ruijie #show defend-zone web traffic-snapshot tcp syns-in topN
    TCP FLOW
    Syns-in : 1200 pps
    Top 10 Sources:
          10.23.45.21          450
          121.2.65.90          350
          121.2.65.94          300
          121.2.62.97          120
          121.2.66.121         60
          121.2.61.9           35
          121.2.60.81          35
          121.2.60.82          23
          121.2.60.84          10
          121.2.60.86          8
```

字段解释：

字段	说明
Top 10 Sources	当前数量最多的 10 台主机

【提示信息】 -

【平台说明】 -

22.1.27 show defend-zone running-protect

查看网络防攻击域的当前正在发生的攻击和防护

show defend-zone *net-defend-zone-name* **running-protect** [**tcp-auth | tcp-unauth | icmp | udp | other-protocol | scan |** *protect-id* | **attack** { **tcp-syn-flood | tcp-conn-flood | udp-spoof-flood | icmp-spoof-flood | other-spoof-flood | udp-flood | icmp-flood | other-flood | scan** }]

【参数说明】

参数	描述
net-defend-zone-name	网络防攻击域名称
tcp-auth	由“**tcp-auth**”类型策略触发的攻击
tcp-unauth	由“**tcp-unauth**”类型策略触发的攻击
icmp	由“**icmp**”类型策略触发的攻击
udp	由“**udp**”类型策略触发的攻击

other-protocol	由“**other-protocol**”类型策略触发的攻击
protect-id	防护 ID。系统将为每个攻击开启一个防护，这个 ID 号可以唯一标识一个防护。
tcp-syn-flood	TCP syn flood 攻击类型
tcp-conn-flood	TCP connection flood 攻击类型
udp-spoof-flood	UDP flood 攻击类型
icmp-spoof-flood	ICMP flood 攻击类型
other-spoof-flood	其他 flood 攻击类型
udp-flood	UDP flood 攻击类型
icmp-flood	ICMP flood 攻击类型
other-flood	其他 flood 攻击类型
scan	扫描类型攻击

【命令模式】 特权模式

【缺省级别】 14

【使用指导】 查看网络防攻击域的当前正在发生的攻击和防护。可以通过触发攻击防护的策略分类查看，也可以通过攻击类型进行分类查看。

【配置举例】 1. 显示网络防攻击域正在实施的防护

```
Ruijie # show defend-zone web running-protect
     Defend zone: ‘web’, Total report: 1
     Attack type: ‘TCP SYN Flood’
 id: 823
        Begin:2012-5-9 12:03:04 ,timeout 60s
        Flow: * → 172.15.0.12, Action: Anti-spoofing(syn cookie)
        Policy: tcp-unauth:half-conn:dst_ip
        Threshold:100 , current: 80
        Received:2300 , Replied: 1300, Dropped:103, Auth host: 108
```

字段解释：

字段	说明
Attack type	攻击类型
id	Id 攻击编号，每个攻击实例都会产生一个唯一的编号
Begin	攻击发生的时间
timeout	攻击行为停止后，防护持续的时间
Flow	表示攻击数据流。 ‘*’ 表示不是固定 IP
Action	针对此攻击的防护行为
Policy	该攻击由哪个策略识别出来的
Threshold	水线

Received	该防护处理的报文数量
Replied	该防护应答的报文数量
Dropped	该防护丢弃的报文数量
Auth host	验证主机的数量

【提示信息】 -

【平台说明】 -

22.1.28 show defend-zone report

查看网络防攻击域的已经结束的各类攻击

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** }]

【参数说明】

参数	描述
net-defend-zone-name	网络防攻击域名称
begin-date	格式 YYYY-MM-DD，起始日期
begin-hour	起始小时，取值 0~23
end-date	格式 YYYY-MM-DD，结束日期
end-hour	结束小时，取值 0~23
tcp-auth	由“**tcp-auth**”类型策略触发的攻击
tcp-unauth	由“**tcp-unauth**”类型策略触发的攻击
icmp	由“**icmp**”类型策略触发的攻击
udp	由“**udp**”类型策略触发的攻击
other-protocol	由“**other-protocol**”类型策略触发的攻击
tcp-syn-flood	TCP syn flood 攻击类型
tcp-conn-flood	TCP connection flood 攻击类型
udp-spoof-flood	UDP flood 攻击类型
icmp-spoof-flood	ICMP flood 攻击类型
other-spoof-flood	其他 flood 攻击类型
udp-flood	UDP flood 攻击类型
icmp-flood	ICMP flood 攻击类型
other-flood	其他 flood 攻击类型
scan	扫描类型攻击

【命令模式】 特权模式

【缺省级别】 14

【使用指导】 查看网络防攻击域中已经结束的攻击。可以通过触发攻击防护的策略分类查看，也可以通过攻击类型进行分类查看。用户可以指定查看的日期范围。

网络防攻击记录 7 日内的攻击报告

【配置举例】 1. 显示 2012-5-9 日归档的攻击防护报告

```
Ruijie # show defend-zone web report 2012-5-9
    Defend zone: web, Total report: 1
   Attack type:  'TCP SYN Flood'
        2012-5-9 12:03:04 ~ 2012-5-9 15:06:04
        Flow: * -> 172.15.0.12 ,  Action: Anti-spoofing(syn cookie)
        Policy: tcp-unauth:half-conn:dst_ip
        Threshold: 100, Action:  Anti-spoofing(syn cookie)
        Received: 10928, Replied: 8790, Dropped: 405
```

字段解释：

字段	说明
2012-5-9 12:03:04 ~ 2012-5-9 15:06:04	攻击开始和结束时间
Attack type	攻击类型
Flow	表示攻击数据流。 '*' 表示不是固定 IP
Action	针对此攻击的防护行为
Policy	该攻击由哪个策略识别出来的
Threshold	水线
Received	该防护处理的报文数量
Replied	该防护应答的报文数量
Dropped	该防护丢弃的报文数量

【提示信息】 -

【平台说明】 -

22.1.29 show net-defend learning

查看对应网络防攻击域策略学习的结果

show net-defend learning *net-defend-zone-name*

查看全局防护策略学习的结果

show net-defend learningglobal

【参数说明】

参数	描述
net-defend-zone-name	网络防攻击域名称
global	网络防攻击的全局防护

【命令模式】 特权模式

【缺省级别】 14

【使用指导】 通过执行此命令可以查看策略学习结果。用户对于学习到的策略需要检查和阈值调整后方可配置到设备中。在策略学习尚未结束时，用户也可以查看策略学习结果，此时查看的仅仅是针对当前学习时间内的流量导出策略。

【配置举例】 查看当前防攻击业务模块的接入情况：

```
Ruijie# show net-defend learning web
Learning status：Finished (End time: 2012-3-12 15:00:30)
<TCP flow statistic (in)>
     Every dst-ip:
         Max half connection: 200
         Max syns (pps): 100
     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 dst-ip:
         Max UDP flow rate(pps): 3024
    Every auth-src-ip:
         Max UDP flow rate(pps): 1000
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 dst-ip threshold  200 action anti-spoofing
tcp-unauth half-conn-in global threshold  293829 action anti-spoofing
tcp-unauth syns-in dst-ip threshold  100 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
udp pkt-in dst-ip threshold 3024 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
```

字段解释：

字段	说明
Learning status	策略学习状态
End time	结束时间
Every dst-ip	每一台目的主机
Every auth-src-ip	每一台通过源验证（真实非伪造）的主机
Global	整个域
Max half connection	最大并发半连接数
Max syns (pps)	TCP SYN 报文最大速率（pps）
Max connection	最大并发连接数
Unauth-src UDP flow rate(pps)	未通过源验证（可能是伪造源）UDP 流速率
Unauth-src ICMP flow rate(pps)	未通过源验证（可能是伪造源）ICMP 流速率
Unauth-src Other-protocol flow rate(pps)	未通过源验证（可能是伪造源）其他类型流速率
Max UDP flow rate(pps)	最大的 UDP 报文速率
Max ICMP flow rate(pps)	最大的 ICMP 报文速率
Max Other-protocol flow rate(pps)	最大的其他类型报文速率

【提示信息】 -

【平台说明】 -

22.1.30 show scan parameter

查看防扫描参数设置情况

show scan parameter

【参数说明】

参数	描述
-	-

【命令模式】 特权模式

【缺省级别】 14

【使用指导】 查看防扫描参数设置情况，对于修订过的参数，将在数字后面的括号中显示原本的缺省值.
参数缺省值使用 scan policy 中的命令进行调整

【配置举例】 例: 查看当前的防扫描参数

```
Ruijie# show scan parameter
          Period        Times     New conns     Rejected conns     IP count      port count
-------------------------------------------------------------------------------------------
TCP(L)          100(60)        3(1)       NA              50              30              30
TCP(M)          90             1          50              25              25              25
TCP(H)          300            1          50              20              20              20
UDP(L)          100(60)        3(1)       NA              50              30              30
UDP(M)          90             1          50              20              25              25
UDP(L)          300            1          50              17              20              20
ICMP(L)         100(60)        3(1)       NA              50              35              NA
ICMP(M)         90             1          40              25              25              NA
ICMP(H)         300            1          30              20              20              NA
Other-
protocol(L)     100(60)        3(1)       NA              50              30              30
Other-
protocol(M)     90             1          40              30              25              25
Other-
protocol(H)     300            1          40              20              20              20
```

字段解释：

字段	说明
Period	扫描行为探测功能计数器恢复周期，即在该周期内如果检测到达所设的防扫描阈值则判断为扫描行为
Times	扫描行为检测周期数，即被连续检测多少个周期有扫描行为时，才判断为发生了扫描行为
New conns	新建非正常连接数，即检测周期内没有形成 establish 状态的新建连接数
Rejected cons	被拒绝连接数，在检测周期内被拒绝的连接数，例如：对端回复 rst，

	unreachable 等报文
IP count	检测周期内新建连接的目的 ip 变化数
Port count	检测周期内新建连接的目的端口变化数

【提示信息】 -

【平台说明】 -

22.1.31 stop net-defend learning

停止网络防攻击域的策略学习

stop net-defend learning *net-defend-zone-name*

停止全局防护的策略学习

stop net-defend learning global

【参数说明】

参数	描述
net-defend-zone-name	网络防攻击域名称
global	网络防攻击的全局防护

【命令模式】 特权模式

【缺省级别】 14

【使用指导】 用户通过这条命令停止对应的策略学习

【配置举例】 1：停止策略学习

```
Ruijie# stop net-defend learning web
```

【提示信息】 -

【平台说明】 -

22.1.32 sync defend config

将当前防攻击配置手工同步到内核模块上

sync defend config [*net-defend-zone-name*] [**force**]

【参数说明】

参数	描述
net-defend-zone-name	网络防攻击域名称
force	强制清空防火墙业务模块上的防攻击配置后，再进行配置同步

【命令模式】 特权模式

【缺省级别】 14

【使用指导】 当工作在防火墙业务模块上的防攻击业务模块出现故障时（例如资源不足等），用户可以通过重新同步配置的方式恢复防火墙业务模块上的防攻击业务模块的状态。以下命令将同步当前防攻击配置。
当指定网络防攻击域名时，同步该网络防攻击域的配置到对应的防火墙内核业务模块上，如果不指定，则同步当前所有网络防攻的配置到防火墙内核业务模块上。
当使用 force 关键字时，则将先清空该防火墙业务模块上对应的配置，然后再启动同步。

【配置举例】 例: 强制同步的所有网络防攻击配置到防火墙内核业务模块上。

```
Ruijie# sync defend config force
```

【提示信息】

```
-
```

【平台说明】 -

22.1.33 tcp

设置全局防攻击中针对所有防火墙流量实施防御 TCP SYN Flood 攻击。
tcp { **syns-in** | **half-conn-in** } **global** **threshold** *threshold-num* **action anti-spoofing**

取消全局防攻击中针对所有防火墙流量实施防御 TCP SYN Flood 攻击。
no tcp { **syns-in** | **half-conn-in** } **global**

恢复缺省配置。
default tcp { **syns-in** | **half-conn-in** } **global**

【参数说明】

参数	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。
threshold *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。
anti-spoofing	对超过阈值部分的流量实施 TCP SYN cookie 防伪

【缺省配置】 **syn-in** 策略的缺省阈值为 300000，**half-conn-in** 策略的缺省阈值为 4000000

【命令模式】 config-defend-zone 配置模式

【缺省级别】 14

【使用指导】 针对所有防火墙流量实施防御 TCP SYN Flood 攻击。
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。
全局防护缺省启用。测试防火墙性能与容量的时候需要关闭全局防护。

全局防护不产生日志记录。

【配置举例】 例:当前设备 TCP 半连接数超过 10 万个时，对超过部分实施 TCP syn cookie 防伪

```
Ruijie(config)# defend-zone global
Ruijie(config-defend-global)# tcp half-conn-in global  threshold 100000 action anti-spoofing
```

【检验方法】 -

【提示信息】 -

【常见错误】 -

【平台说明】 -

22.1.34 tcp-auth

启用针对来自真实源的 TCP 流量的防御策略
tcp-auth { **conn-in | half-conn-in | syns-in** } **src-ip threshold** *threshold-num* [**timeout** *seconds*] **action** { **limit | blocking | notify** }

取消针对来自真实源的 TCP 流量的防御策略
no tcp-auth { **conn-in | half-conn-in | syns-in** } **src-ip**

恢复缺省配置。
default tcp-auth { **conn-in | half-conn-in | syns-in** } **src-ip**

【参数说明】

参数	描述
conn-in	向网络防攻击域发起的 TCP 连接数量。
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。
threshold *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
timeout *seconds*	策略的最小执行时间，单位秒，缺省值为 60。可配置范围 10～86400 秒
src-ip	该策略针对每个源主机进行识别
limit	限制对应的流量在 *threshold-num* 以下
blocking	阻塞该主机进出防攻击域的双向流量
notify	仅记录此次攻击

【缺省配置】 无缺省配置

【命令模式】 config-defend-zone 配置模式

【缺省级别】 14

【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)或者是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）。策略执行时间不少于 *seconds.*

【配置举例】 例: 当某个源主机（真实源）对网络防攻击域 web 发起的 TCP 半连接数超过 200 个时，阻塞这台主机进出该域的所有流量，阻塞时间为 60 秒。

```
Ruijie(config)# defend-zone web
Ruijie(config-defend-zone)# tcp-auth half-conn-in src-ip threshold 200 timeout 3600 action blocking
Ruijie(config-defend-zone)# exit
```

【检验方法】 -

【提示信息】 -

【常见错误】 -

【平台说明】 -

22.1.35 tcp-unauth

启用 TCP SYN Flood 防御策略。

tcp-unauth { **syns-in | half-conn-in** } { **dst-ip | global** } **threshold** *threshold-num* [**timeout** *seconds*] **action** { **anti-spoofing | notify** }

取消启用 TCP SYN Flood 防御策略。

no tcp-unauth {**syns-in | half-conn-in** } {**dst-ip | global** }

恢复缺省配置。

default tcp-unauth {**syns-in | half-conn-in** } {**dst-ip | global** }

【参数说明】

参数	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。
threshold *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。
timeout *seconds*	策略的最小执行时间，单位秒，缺省值为 60。可配置范围 10～86400 秒
dst-ip	针对每个目的主机进行识别
global	针对整个域进行识别
anti-spoofing	对 TCPsyn 报文实施 TCP SYN cookie 防伪
notify	仅记录此次攻击

【缺省配置】 无缺省配置

【命令模式】 config-defend-zone 配置模式

【缺省级别】 14

【使用指导】 当进入网络防攻击域的 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)，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 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(anti-spoofing)，执行时间不少于 seconds。

【配置举例】 例: 当针对网络防攻击域的任何一台目睹主机的 TCP 半连接数超过 1000 时，针对该目的主机的所有 TCP 启动防伪。

```
Ruijie(config)# defend-zone web
Ruijie(config-defend-zone)# tcp-unauth half-conn-in dst-ip threshold 1000 action anti-spoofing
Ruijie(config-defend-zone)# exit
```

【检验方法】 -

【提示信息】 -

【常见错误】 -

【平台说明】 -

22.1.36 threshold

配置扫描检测的各敏感度的阈值。
threshold { **low | medium | high } [protocol { tcp | udp | icmp | other-protocol }] { ip-count | port-count | new-conn | reject-conn }** *threshold-num*

删除扫描检测的各敏感度的阈值配置。
no threshold { **low | medium | high } [protocol { tcp | udp | icmp | other-protocol }] { ip-count |**

port-count | new-conn | reject-conn }

恢复缺省配置。

default threshold { **low | medium | high } [protocol { tcp | udp | icmp | other-protocol }] { ip-count | port-count | new-conn | reject-conn }**

【参数说明】

参数	描述
low	低敏感度检测
medium	中等敏感度检测
high	高敏感度检测
icmp	ICMP 协议
other-protocol	除了 TCP，UDP，ICMP 以外的协议
tcp	TCP 协议
udp	UDP 协议
ip-count	扫描行为的 IP 变化的阈值
port-count	扫描行为的端口变化的阈值
new-conn	扫描行为的新建连接数的阈值
reject-conn	扫描行为的被拒绝连接数的阈值
threshold-num	扫描检测参数的阈值，参数为 **ip-count、port-count、reject-conn** 时，取值 1~2000；参数为 **new-conn** 时，取值 10~2000

【缺省配置】 各参数的缺省配置下，通过执行“**show scan parameter**”可以得到。具体参数值在 **show scan parameter** 中说明。

【命令模式】 config-scan-policy 配置模式

【缺省级别】 14

【使用指导】 设置每个级别的扫描敏感度。

【配置举例】 例: 设置低敏感度检测，tcp 协议端口变化阈值为 100

```
Ruijie(config)# scan policy
Ruijie(config-scan-policy)# threshold low protocol tcp port-count 100
```

【检验方法】 使用 **show scan parameter** 命令，可以查看参数调整结果。

【提示信息】 -

【常见错误】 -

【平台说明】 -

22.1.37 traffic-monitor

启用各类流量监控。
traffic-monitor { **tcp** | **http** | **udp** | **icmp | ip | all** }

取消各类流量监控。
no traffic-monitor { **tcp** | **http** | **udp** | **icmp | ip | all** }

恢复缺省配置。
default traffic-monitor { **tcp** | **http** | **udp** | **icmp | ip | all** }

【参数说明】

参数	描述
tcp	监视进入网络防攻击域的 tcp 流量
http	监视进入网络防攻击域的 http 流量
udp	监视进入网络防攻击域的 udp 流量
icmp	监视进入网络防攻击域的 icmp 流量
ip	监视进入网络防攻击域的 ip 流量
all	监视以上所有流量

【缺省配置】 无缺省配置

【命令模式】 config-defend-zone 配置模式

【缺省级别】 14

【使用指导】 开启各类监控: TCP、HTTP、UDP、ICMP、IP 流量数据。如果使用 all 关键字则开启所有监控开关

【配置举例】 例: 启动针对网络防攻击域 web 的 TCP 流量监视

```
Ruijie(config)#defend-zone web
Ruijie(config-defend-zone)# traffic-monitor tcp
```

【检验方法】 使用 **show defend-zone** *net-defend-zone-name* **traffic-snapshot** 命令查看分类流量信息。

【提示信息】 -

【常见错误】 -

【平台说明】 -

22.1.38 udp auth-src-in

设置针对来自真实源主机的 UDP 流量的策略

udp auth-src-in src-ip threshold *threshold-num* [**timeout** *seconds*] **action** { **limit | blocking | notify** }

取消针对来自真实源主机的 UDP 流量的策略

No udp auth-src-in src-ip

恢复缺省配置。

default udp auth-src-in src-ip

【参数说明】

参数	描述
auth-src-in	进入网络防攻击域的来自真实性源主机的报文。
src-ip	该策略针对每个源主机进行识别
threshold *threshold-num*	pps，取值 1~100,000,000
timeout *seconds*	策略的最小执行时间，单位秒，缺省值为 60。可配置范围 10～86400 秒
limit	限制对应的流量在 *threshold-num* 以下
blocking	阻塞该主机进出防攻击域的双向流量
notify	仅记录此次攻击

【缺省配置】 无缺省配置

【命令模式】 config-defend-zone 配置模式

【缺省级别】 14

【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 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）或者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）。策略执行时间不少于 *seconds.*

【配置举例】 例: 当任何真实源主机发往网络防攻击域 web 的 UDP 报文超过每秒 100 个时，阻塞这个源 IP 向该域发送任何报文，时间为 60 秒

```
Ruijie(config)# defend-zone web
Ruijie(config-defend-zone)# udp auth-src-in src-ip threshold 100 action blocking
Ruijie(config-defend-zone)# exit
```

【检验方法】 -

【提示信息】 -

【常见错误】 -

【平台说明】 -

22.1.39 udp pkt-in

设置进入网络防攻击域的 UDP 流量限制。
udp pkt-in { **dst-ip | global** } **threshold** *threshold-num* [**timeout** *seconds*] **action** { **limit | notify** }

取消进入网络防攻击域的 UDP 流量限制。
no udp pkt-in { **dst-ip | global** }

恢复缺省配置。
default udp pkt-in { **dst-ip | global** }

【参数说明】

参数	描述
pkt-in	进入网络防攻击域的所有类型的报文。
threshold *threshold-num*	pps, 取值 1~100,000,000
timeout *seconds*	策略的最小执行时间，单位秒，缺省值为 60。可配置范围 10～86400 秒
dst-ip	针对每个目的主机进行识别
global	针对整个域进行识别
limit	限制对应的流量在 *threshold-num* 以下
notify	仅记录此次攻击

【缺省配置】 无缺省配置

【命令模式】 config-defend-zone 配置模式

【缺省级别】 14

【使用指导】 当进入网络防攻击域的 UDP 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。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 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*

【配置举例】 例: 当网络防攻击域 web 中的任何一台主机收到的 UDP 报文速率超过每秒 100 个时，限制发往该主机的 UDP 报文的速率（控制在阈值以下）。

```
Ruijie(config)# defend-zone web
Ruijie(config-defend-zone)# udp pkt-in dst-ip threshold 100 action limit
Ruijie(config-defend-zone)# exit
```

【检验方法】 -

【提示信息】 -

【常见错误】 -

【平台说明】 -

22.1.40 udp unauth-src-in

启用针对未通过真实源验证的 UDP 流量的策略。
udp unauth-src-in { **dst-ip** | **global** } **threshold** *threshold-num* [**timeout** *seconds*] **action** { **limit** | **drop** | **notify** }

取消针对未通过真实源验证的 UDP 流量的策略
no udp unauth-src-in { **dst-ip** | **global** }

恢复缺省配置。
default udp unauth-src-in { **dst-ip** | **global** }

【参数说明】

参数	描述
unauth-src-in	进入网络防攻击域的未通过真实源验证的报文。
threshold *threshold-num*	pps，取值 1~100,000,000
timeout *seconds*	策略的最小执行时间，单位秒，缺省值为 60。可配置范围 10～86400 秒
dst-ip	针对每个目的主机进行识别
global	针对整个域进行识别
limit	限制对应的流量在 *threshold-num* 以下
drop	丢弃对应的流量
notify	仅记录此次攻击

【缺省配置】 无缺省配置

【命令模式】 config-defend-zone 配置模式

【缺省级别】 14

【使用指导】 当进入网络防攻击域的未通过真实源验证的 UDP 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）或者全部丢弃此类报文。
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 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。

【配置举例】 例: 当进入网络防攻击域 web 的所有疑似伪造源的 UDP 报文超过每秒 100 个时，限制此类报文进入网络防攻击域的速度不超过阈值，当攻击停止后，继续该防护 1 小时。

```
Ruijie(config)# defend-zone web
Ruijie(config-defend-zone)# udp unauth-src-in global threshold 100 timeout 3600 action limit
```

```
Ruijie(config-defend-zone)# exit
```

【检验方法】 -

【提示信息】

```
-
```

【常见错误】 -

【平台说明】 -

22.1.41 other-protocol auth-src-in

启用针对来自真实源主机的其他协议(除 TCP,UDP,ICMP 之外)流量的策略。
other-protocol auth-src-in src-ip threshold *threshold-num* [**timeout** *seconds*] **action** { **limit | blocking | notify** }

取消启用针对来自真实源主机的其他协议(除 TCP,UDP,ICMP 之外)流量的策略。
no other-protocol auth-src-in src-ip

恢复缺省配置。
default other-protocol auth-src-in src-ip

【参数说明】

参数	描述
auth-src-in	进入网络防攻击域的来自真实性源主机的报文。
src-ip	该策略针对每个源主机进行识别
threshold *threshold-num*	pps, 取值 1~100,000,000
timeout *seconds*	策略的最小执行时间，单位秒，缺省值为 60。可配置范围 10～86400 秒
limit	限制对应的流量在 *threshold-num* 以下
blocking	阻塞该主机进出防攻击域的双向流量
notify	仅记录此次攻击

【缺省配置】 无缺省配置

【命令模式】 config-defend-zone 配置模式

【缺省级别】 14

【使用指导】 当任何真实源主机发出的进入网络防攻击域的其他协议(除 TCP,UDP,ICMP 之外)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)或者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）。策略执行时间不少于 *seconds.*

【配置举例】 例: 当任何真实源主机发往网络防攻击域的其他协议流量超过每秒 100 个时，将阻塞这个源主机向该域收发任何报文。

```
Ruijie(config)#defend-zone web
Ruijie(config-defend-zone)# other-protocol auth-src-in src-ip threshold 100 action blocking
Ruijie(config-defend-zone)# exit
```

【检验方法】 -

【提示信息】 -

【常见错误】 -

【平台说明】 -

22.1.42 other-protocol pkt-in

限制进入网络防攻击域的其他协议(除 TCP,UDP,ICMP 外)流量。

other-protocol pkt-in { **dst-ip | global** } **threshold** *threshold-num* [**timeout** *seconds*] **action limit**

取消进入网络防攻击域的其他协议(除 TCP,UDP,ICMP 外)流量限制。

no other-protocol pkt-in { **dst-ip | global** }

恢复缺省配置。

default other-protocol pkt-in { **dst-ip | global** }

【参数说明】

参数	描述
pkt-in	进入网络防攻击域的所有类型的报文。
threshold *threshold-num*	pps，取值 1~100,000,000
timeout *seconds*	策略的最小执行时间，单位秒，缺省值为 60。可配置范围 10～86400 秒
dst-ip	针对每个目的主机进行识别
global	针对整个域进行识别
limit	限制对应的流量在 *threshold-num* 以下
notify	仅记录此次攻击

【缺省配置】 无缺省配置

【命令模式】 config-defend-zone 配置模式

【缺省级别】 14

【使用指导】 当进入网络防攻击域的其他协议（除了 TCP，UDP 和 ICMP 以外）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。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其他协议（除了 TCP，UDP 和 ICMP 以外）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*。

【配置举例】 例: 当网络防攻击域 web 中的任何一台主机收到的其他类型协议报文速率超过每秒 100 个时，限制发往该主机的该类报文的速率（控制在阈值以下）。

```
Ruijie(config)# defend-zone web
Ruijie(config-defend-zone)# other-protocol pkt-in dst-ip threshold 100 action limit
Ruijie(config-defend-zone)# exit
```

【检验方法】 -

【提示信息】 -

【常见错误】 -

【平台说明】 -

22.1.43 other-protocol unauth-src-in

启用针对未通过真实源验证的其他协议（除了 TCP，UDP 和 ICMP 以外）流量的策略。
other-protocol unauth-src-in { **dst-ip** | **global** } **threshold** *threshold-num* [**timeout** *seconds*] **action** { **limit** | **drop | notify** }

取消进入网络防攻击域的其他协议(除 TCP,UDP,ICMP 外)流量限制。
no other-protocol unauth-src-in { **dst-ip** | **global** }

恢复缺省配置。
default other-protocol unauth-src-in { **dst-ip** | **global** }

【参数说明】

参数	描述
unauth-src-in	进入网络防攻击域的未通过真实源验证的报文。
threshold *threshold-num*	pps，取值 1~100,000,000
timeout *seconds*	策略的最小执行时间，单位秒，缺省值为 60。可配置范围 10～86400 秒
dst-ip	针对每个目的主机进行识别
global	针对整个域进行识别
limit	限制对应的流量在 *threshold-num* 以下
drop	丢弃对应的流量
notify	仅记录此次攻击

【缺省配置】 无缺省配置

【命令模式】 config-defend-zone 配置模式

【缺省级别】 14

【使用指导】 当进入网络防攻击域的未通过真实源验证的其他协议（除了 TCP，UDP 和 ICMP 以外）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）或者全部丢弃此类报文。
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其他协议（除了 TCP，UDP 和 ICMP 以外）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。

【配置举例】 例: 当进入网络防攻击域 web 的所有疑似伪造源的其他类型协议报文超过每秒 100 个时，限制此类报文进入网络防攻击域的速度不超过阈值，当攻击停止后，继续该防护 1 小时。

```
Ruijie(config)# defend-zone web
Ruijie(config-defend-zone)# other-protocol unauth-src-in global threshold 100 timeout 3600 action limit
Ruijie(config-defend-zone)# exit
```

【检验方法】 -

【提示信息】 -

【常见错误】 -

【平台说明】 -

22.2 安全域

22.2.1 description

设置安全域描述字符串。
description *string*

删除安全域描述字符串。
no description

恢复缺省配置。
default description

【参数说明】

参数	描述
string	安全域的描述字符串，长度为 1~40 字符。

【缺省配置】 没有描述字符串。

【命令模式】 安全域模式

【缺省级别】 14

【使用指导】 -

【配置举例】 1：安全域描述字符串设置为 trust。

```
Ruijie(config-vfw)#security-zone hello
Ruijie(config-vfw-security-zone)#description trust
```

【检验方法】 1：使用 **show security-zone** 命令，可以查看安全域的描述字符串。

【提示信息】 -

【常见错误】 -

【平台说明】 -

22.2.2 inner-zone-access

设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。
inner-zone-access

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。
no inner-zone-access

恢复缺省配置。
default inner-zone-access

【参数说明】

参数	描述
-	-

【缺省配置】 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。

【命令模式】 安全域模式

【缺省级别】 14

【使用指导】 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。

【配置举例】 1：配置虚拟防火墙 vfw1 的安全域 abc 内访问策略无法匹配时允许该安全域内的 IP 互相访问。

```
Ruijie(config)#firewall-config vfw1
Ruijie(config-vfw)#security-zone abc
Ruijie(config-vfw-security-zone)#inner-zone-access
Ruijie(config-vfw-security-zone)#description trust
```

【检验方法】 1：使用 **show security-zone** 命令，可以查看安全域域内访问策略无法匹配时是否允许安全域内的 IP 互相访问。

【提示信息】 -

【常见错误】 -

【平台说明】 -

22.2.3 interface

接口加入安全域。
interface *interface-name*

接口离开安全域。
no interface *interface-name*

恢复缺省配置。
default interface *interface-name*

【参数说明】

参数	描述
interface-name	接口的名称

【缺省配置】 加入虚拟防火墙的接口当未加入安全域时属于 default 安全域。

【命令模式】 安全域模式

【缺省级别】 14

【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。
- 非路由虚拟防火墙，只有 vlan 接口才可以加入安全域。
- 路由虚拟防火墙【route-mode-vfw】，三层物理口、三层 AP 口、SVI 接口才可以加入安全域

【配置举例】 1：接口 vlan2 加入安全域 hello。

```
Ruijie(config-vfw)#security-zone hello
Ruijie(config-vfw-security-zone)#interface vlan 2
```

【检验方法】 1：使用 **show security-zone** 命令，可以查看安全域关联的接口。

【提示信息】 -

【常见错误】 -

【平台说明】 -

22.2.4 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-inner-zone-access

全局配置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。
no loose-inner-zone-access

恢复缺省配置。
default loose-inner-zone-access

【参数说明】

参数	描述
-	-

【缺省配置】 安全域内访问策略无法匹配时互相不能访问。

【命令模式】 虚拟防火墙配置模式

【缺省级别】 14

【使用指导】 该命令优先级低于安全域模式下的 **inner-zone-access** 命令。

【配置举例】 1：配置虚拟防火墙 vfw1 的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。

```
Ruijie(config)#firewall-config vfw1
Ruijie(config-vfw)#loose-inner-zone-access
```

【检验方法】 1：使用 **show security-access-global** 命令，可以查看安全域全局访问策略。

【提示信息】 -

【常见错误】 -

【平台说明】 -

22.2.5 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。
loose-inter-zone-access

全局配置安全域间访问策略无法匹配时不允许安全域优先级相同的安全域间互相访问。
no loose-inter-zone-access

恢复缺省配置。
default loose-inter-zone-access

【参数说明】

参数	描述
-	-

【缺省配置】 安全域间访问策略无法匹配时安全域优先级相同的安全域间互相不允许访问。

【命令模式】 虚拟防火墙配置模式

【缺省级别】 14

【使用指导】 -

【配置举例】 1：配置虚拟防火墙 vfw1 的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。

```
Ruijie(config)#firewall-config vfw1
Ruijie(config-vfw)#loose-inter-zone-access
```

【检验方法】 1：使用 **show security-access-global** 命令，可以查看安全域的全局访问策略。

【提示信息】 -

【常见错误】 -

【平台说明】 -

22.2.6 security-access

当报文匹配安全域访问策略使用 ACL 进行匹配时，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，单向有效。

security-access [**sequence** *sequence-number*] **from** *zone-name* **to** *zone-nameaccess-list* [**inactive**] [**description** *string*]

删除从一个安全域访问另外一个安全域的基于 ACL 的 IPV4 报文访问策略。

no security-access { **sequence** *sequence-number* | **from** *zone-name* **to** *zone-name access-list* }

删除从一个安全域访问另外一个安全域的基于 ACL 的 IPV4 报文访问策略。

default security-access { **sequence** *sequence-number* | **from** *zone-name* **to** *zone-name access-list* }

当报文匹配安全域访问策略使用对象进行匹配时，配置从一个安全域访问另外一个安全域的 IPV4 访问策略，单向有效。

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*]

删除从一个安全域访问另外一个安全域的基于对象的 IPV4 报文访问策略。

no 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*] }

删除从一个安全域访问另外一个安全域的基于对象的 IPV4 报文访问策略。

default 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*] }

设置安全域 IPV4 访问策略激活。

security-access sequence *sequence-number* **active**

删除安全域 IPV4 访问策略或设置为未激活。

no security-access sequence *sequence-number* [**active**]

【参数说明】

参数	描述
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
active	规则激活

【缺省配置】 未配置 IPV4 报文的安全域访问策略

【命令模式】 虚拟防火墙配置模式

【缺省级别】 14

【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。
使用ACL进行匹配和使用对象进行匹配不会同时存在，受 **security-access-match-object** 命令的控制。使用对象进行匹配的访问策略只在基于网络接口划分的安全域才生效。

【配置举例】 1：配置虚拟防火墙 vfw1 从安全域 aaa 到安全域 bbb 的 IPV4 报文单向访问策略，引用 ACL hello。

```
Ruijie(config)#firewall-config vfw1
Ruijie(config-vfw)#security-access from aaa to bbb hello
```

2：配置虚拟防火墙 vfw1 从安全域 aaa 到安全域 bbb 的 IPV4 报文单向访问策略，引用地址对象和服务对象。

```
Ruijie(config)#firewall-config vfw1
Ruijie(config-vfw)#security-access sequence 10 from aaa to bbb permit src-address-object TERM
dest-address-object Server service myweb
```

【检验方法】 1：使用 **show security-access-rule** 命令，可以查看安全域 IPV4 报文访问策略。

【提示信息】 -

【常见错误】 -

【平台说明】 -

22.2.7 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-match-object

恢复报文匹配安全域访问策略时使用 ACL 进行匹配。

no security-access-match-object

恢复报文匹配安全域访问策略时使用 ACL 进行匹配。
default security-access-match-object

【参数说明】

参数	描述
-	-

【缺省配置】 报文匹配安全域访问策略时使用 ACL 进行匹配。

【命令模式】 虚拟防火墙配置模式

【缺省级别】 14

【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 **security-access** *access-list* 将被删除，命令被隐藏屏蔽。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 **security-access** [**sequence** *sequence-number*]将被删除，命令被隐藏屏蔽。

该命令只在基于网络接口划分的安全域才生效。

【配置举例】 1：配置虚拟防火墙 vfw1 报文匹配安全域策略时使用对象进行匹配。

```
Ruijie(config)#firewall-config vfw1
Ruijie(config-vfw)#security-access-match-object
```

【检验方法】 -

【提示信息】 -

【常见错误】 -

【平台说明】 -

22.2.8 security-access-step

配置安全域访问策略默认增加的序号值。
security-access-step *step-number*

恢复安全域访问策略默认增加的序号缺省值 10。
no security-access-step

恢复安全域访问策略默认增加的序号缺省值 10。
default security-access-step

【参数说明】

参数	描述
step-number	security-access 和 security-access-ipv6 命令默认递增的序号值，取值范围是 1 到 2147483647。

【缺省配置】 缺省是 10。

【命令模式】 虚拟防火墙配置模式

【缺省级别】 14

【使用指导】 -

【配置举例】 1：虚拟防火墙 vfw1 的安全域访问策略默认增加的序号值是 20。

```
Ruijie(config)#firewall-config vfw1
Ruijie(config-vfw)#security-access-step 20
```

【检验方法】 1：使用 **show security-access-global** 命令，可以查看安全域访问策略默认增加的序号值。

【提示信息】 -

【常见错误】 -

【平台说明】 -

22.2.9 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（SYSLOG）。
security-deny-access-log

配置违反安全域访问策略而丢弃报文时不产生日志（SYSLOG）。
no security-deny-access-log

恢复缺省配置。
default security-deny-access-log

【参数说明】

参数	描述
-	-

【缺省配置】 缺省违反安全域访问策略而丢弃报文时不产生日志。

【命令模式】 虚拟防火墙配置模式

【缺省级别】 14

【使用指导】 该命令一般仅用于故障诊断，启用后转发性能有所下降。

> 报文因违反安全域策略而被丢弃时，如果需要产生日志，则会立刻产生。当前的版本只支持将日志发送到日志服务器，无法将日志输出到控制台、缓冲区等。

【配置举例】 1：配置虚拟防火墙 vfw1 违反安全域访问策略而丢弃报文时需要产生日志。

```
Ruijie(config)#firewall-config vfw1
Ruijie(config-vfw)#security-deny-access-log
```

【检验方法】 1：使用 **show security-access-global** 命令，可以查看违反安全域访问策略而丢弃报文时是否产生日志。

【提示信息】 -

【常见错误】 -

【平台说明】 -

22.2.10 security-level

配置安全域优先级。
security-level *level-num*

删除安全域优先级。
no security-level

恢复缺省配置。
default security-level

【参数说明】

参数	描述
level-num	安全域优先级，取值范围 1~100。数值越大优先级别越高。

【缺省配置】 缺省情况下安全域没有优先级。

【命令模式】 安全域模式

【缺省级别】 14

【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。

【配置举例】 1：配置某安全域的优先级为最高。

```
Ruijie(config-vfw)# security-zone hello
Ruijie(config-vfw-security-zone)#security-level 100
```

【检验方法】 1：使用 **show security-zone** 命令，可以查看安全域的优先级。

【提示信息】 -

【常见错误】 -

【平台说明】 -

22.2.11 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（SYSLOG）。
security-permit-access-log

配置报文流匹配安全域策略在连接撤销时不产生日志（SYSLOG）。
no security-permit-access-log

恢复缺省配置。
default security-permit-access-log

【参数说明】

参数	描述
-	-

【缺省配置】 匹配安全域策略时不产生日志。

【命令模式】 虚拟防火墙配置模式

【缺省级别】 14

【使用指导】 该命令一般仅用于故障诊断，启用后转发性能有所下降。

报文满足安全域策略时，如果需要产生日志，则要等到连接撤销时才会产生。当前的版本只支持将日志发送到日志服务器，无法将日志输出到控制台、缓冲区等。

【配置举例】 1：配置虚拟防火墙 vfw1 报文流匹配安全域策略时在连接建立和撤销时产生日志。

```
Ruijie(config)#firewall-config vfw1
Ruijie(config-vfw)#security-permit-access-log
```

【检验方法】 1：使用 **show security-access-global** 命令，可以查看匹配安全域访问策略是否产生日志

【提示信息】 -

【常见错误】 -

【平台说明】 -

22.2.12 security-zone

创建一个安全域或进入已经存在的安全域。
security-zone *zone-name*

删除一个安全域。
no security-zone *zone-name*

恢复缺省配置。
default security-zone *zone-name*

【参数说明】

参数	描述
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。

【缺省配置】 未创建一个安全域，只有一个 default 安全域存在。

【命令模式】 虚拟防火墙配置模式

【缺省级别】 14

【使用指导】 每个虚拟防火墙默认存在一个 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。

【配置举例】 1：虚拟防火墙 vfw1 创建名为 hello 的安全域。

```
Ruijie(config-vfw)#security-zone hello
Ruijie(config-vfw-security-zone)#
```

【检验方法】 1：使用 **show security-zone** 命令，可以查看安全域信息。

【提示信息】 -

【常见错误】 -

【平台说明】 -

22.2.13 security-zone-base interface

设置以网络接口划分安全域。
security-zone-base interface

设置以 IP 地址集合划分安全域。
no security-zone-base interface

恢复缺省配置。
default security-zone-base interface

【参数说明】

参数	描述
-	-

【缺省配置】 以网络接口划分安全域。

【命令模式】 虚拟防火墙配置模式

【缺省级别】 14

【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策略以及全局安全域访问策略。

⚠ 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。

【配置举例】 1：虚拟防火墙 vfw1 以 IP 地址集合划分安全域。

```
Ruijie(config-vfw)#no security-zone-base interface
```

2：虚拟防火墙 vfw1 以网络接口划分安全域。

```
Ruijie(config-vfw)#security-zone-base interface
```

【检验方法】 1：使用 **show security-access-global** 命令，可以查看安全域的划分方式。

【提示信息】 -

【常见错误】 -

【平台说明】 -

22.2.14 show security-access-global

查看虚拟防火墙全局安全域访问策略。
show security-access-global *firewall-name*

【参数说明】

参数	描述
firewall-name	虚拟防火墙名称。

【命令模式】 特权模式、全局模式、接口模式

【缺省级别】 14

【使用指导】 全局的访问策略优先级低于具体某两个安全域间（如果两个安全域名称相同表示是安全域内）的访问策略，只有在未匹配具体的安全域间访问策略时全局访问策略才生效。使用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、安全域访问策略是基于 ACL 还是对象、匹配安全域策略在连接建立和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、安全域间策略匹配统计开关、安全域访问策略命令递增的序号。

【配置举例】 1：查看虚拟防火墙 vfw1 全局的访问策略。

```
Ruijie#show security-access-global vfw1
security zone is base interface
security rule is base ACL
inner-zone access:on
inter-zone access between same level:on
permit access log:off
deny access log:off
access statistics:off
web-auth enable:off
access rule step:10
```

字段解释：

字段	说明
security zone is base	安全域划分方式
security rule is base	安全域访问策略是基于 ACL 还是对象
inner-zone access	安全域内访问策略无法匹配时是否允许安全域内的 IP 互相访问
inter-zone access between same level	安全域间访问策略无法匹配时允许安全域间 security-level 相同的 IP 互相访问
permit access log	匹配安全域策略在连接建立/撤销时是否产生日志
deny access log	违反安全域访问策略而丢弃报文时是否产生日志
access statistics	安全域间的策略匹配统计是否使能
web-auth enable	web 认证功能是否使能
access rules step	security-access 和 security-access-ipv6 命令递增的序号

【提示信息】 -

【平台说明】 -

22.2.15 show security-access-rules

查看安全域 IPV4 报文访问策略。

show security-access-rules { [**from** *zone-name1*] *firewall-name* **|** [**to** *zone-name2*] *firewall-name* | *firewall-name* }

【参数说明】

参数	描述
zone-name1	安全域 1 的名称。
zone-name2	安全域 2 的名称。
firewall-name	虚拟防火墙名称

【命令模式】 特权模式、全局模式、接口模式

【缺省级别】 14

【使用指导】

【配置举例】 1：查看虚拟防火墙 vfw1 所有 IPV4 访问策略

```
Ruijie#show security-access-rules vfw1
security-access 100 from trust to untrust 10
security-access 101 from dmz to trust 20
security-aceess 102 from dmz to default 30
```

2：查看虚拟防火墙 vfw1 源安全域是 trust 的所有 IPV4 访问策略

```
Ruijie#show security-access-rules trust vfw1
security-access 100 from trust to untrust 10
security-access 101 from trust  to dmz 20
```

3：查看虚拟防火墙 vfw1 目的安全域是 trustB 的所有 IPV4 访问策略

```
Ruijie#show security-access-rules to trustB vfw1
security-access 100 from trustA  to trustB 10
security-access 101 from dmz  to trustB 20
```

字段解释：

字段	说明
100	IPV4 ACL
101	IPV4 ACL
102	IPV4 ACL
trust	安全域名称

untrust	安全域名称
dmz	安全域名称
default	安全域名称
trustA	安全域名称
trustB	安全域名称
10	序号
20	序号
30	序号

【提示信息】 -

【平台说明】 -

22.2.16 show security-zone

查看全部或单个安全域的配置。

show security-zone [*zone-name*] *firewall-name*

【参数说明】

参数	描述
zone-name	安全域名称。缺省是所有的安全域。
firewall-name	虚拟防火墙名称

【命令模式】 特权模式、全局模式、接口模式

【缺省级别】 14

【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】 1：查看虚拟防火墙 vfw1 的安全域 TERM 配置信息。

```
Ruijie#show security-zone TERM vfw1
security-zone:TERM
description:terminal_client_zone
level: 80
inner-zone access:on
ip access-group:10
```

2：查看虚拟防火墙 vfw1 的全部安全域配置信息。

```
Ruijie#show security-zone vfw1
security-zone:TERM
description:terminal_client_zone
```

```
level: 80
inner-zone access:on
ip access-group:10

security-zone:default
description:terminal_client_zone
level: 90
inner-zone access:on
```

字段解释：

字段	说明
security- zone	安全域名称
description	安全域描述字符串
level	安全域优先级
inner-zone access	安全域内访问策略无法匹配时是否允许安全域内的 IP 互相访问
ip access-group	安全域关联的 ACL

【提示信息】 -

【平台说明】 -

22.2.17 show security-zone-match

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 firewall-name*

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*

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*

【参数说明】

参数	描述
ip-protocol	IP 协议
1	ICMP 协议
6	TCP 报文
17	UDP 报文
tcp	TCP 报文
udp	UDP 报文

source-ip	源 IP
dst-ip	目的 IP
src-port	源端口。缺省时等于 0。
dst-port	目的端口。缺省时等于 0。
type	ICMP type。缺省时等 8。
code	ICMP code。缺省时等 0。
src-interface	源接口名称
dst-interface	目的接口名称
firewall-name	虚拟防火墙名称

【命令模式】 特权模式、全局模式、接口模式

【缺省级别】 14

【使用指导】 该命令一般用来诊断配置的问题。

【配置举例】 1：给定 IPV4 报文特征，显示安全域策略匹配的结果。

```
Ruijie#show security-zone-match udp 192.168.1.1 192.168.2.1 3456 80 from vlan 2 to vlan 3 vfw1
Allowed for permitted by inner zone accessing control
```

字段解释：

字段	说明
Denied for a unpredictable error occurs	因防火墙内部错误被拒绝
Denied for inner-zone access is forbidden	因域内不允许访问而被拒绝
Denied for inter-zone access with same level is forbidden	因源安全域优先级等于目的安全域优先级而被拒绝
Denied for the level of src_zone is less than dst_zone's	因源安全域优先级低于目的安全域优先级而被拒绝
Denied for hitting a security zone rule (deny)	因命中 deny 的安全域访问策略而被拒绝
Denied for not match the security policy	因找不到对应的安全域策略被拒绝
Allowed for the desitination ip is a broadcast ip or multicast ip	因目的 ip 是广播或组播而允许通过
Allowed for the desitination ip is to local	因目的 ip 是本机而允许通过
Allowed for the source ip is a local ip	因源 ip 是本机而允许通过
Allowed for hitting a security zone rule	因命中一条安全域策略而允许通过
Allowed for permitted by inner zone accessing control	因安全域内部允许访问而允许通过
Allowed for the level of src_zone is greater than dst_zone’s	因源安全域的优先级高于目的安全域的优先级而允许通过
Allowed for the level of dst_zone is equal to src_zone’s	因源安全域的优先级等于目的安全域的优先级而允许通过

【提示信息】 -

【平台说明】 -

命令参考-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-TRACK

1 VRRP

1.1 ipv6 vrrp enable

全局启用 IPv6 VRRP
ipv6 vrrp enable

全局关闭 IPv6 VRRP
no ipv6 vrrp enable

【参数说明】

参数	描述
-	-

【缺省配置】 缺省情况下，系统全局没有启用 IPv6 的 VRRP 功能。

【命令模式】 全局模式

【缺省级别】 14

【使用指导】 只在插入了 CB 线卡的 N18K 设备上才支持本命令。
配置本命令后，系统只支持在 SVI 口 1~255 上配置 IPv4 VRRP 和 IPv6 VRRP。配置 no ipv6 vrrp enable 后，系统支持在路由口、L3AP、SVI 口上配置 IPv4 VRRP。

【配置举例】 全局启用 IPv6 VRRP

```
Ruijie#configure terminal
Ruijie(config)#ipv6 vrrp enable
```

【检验方法】 1：使用 **show run** 命令，可以查看全局 IPv6 的 VRRP 功能是启用还是关闭。

【提示信息】 -

【常见错误】 -

【平台说明】 -

1.2 show vrrp

查看 IPv4 VRRP 或者 IPv6 VRRP 的概况或者细节。
show [**ipv6**] **vrrp** [**brief** | *group*]

【参数说明】

参数	描述
ipv6	应用于 IPv6。缺省为 IPv4。
brief	显示 VRRP 的概况。缺省显示完整信息。
group	待显示的 VRRP 组号。缺省显示所有 VRRP 备份组的信息。

【命令模式】 特权模式、全局模式、接口模式

【缺省级别】 14

【使用指导】 如果不使用可选参数，将显示所有的 VRRP 组的情况。

【配置举例】 1：查看所有的 VRRP 组情况

```
Ruijie# 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
Ruijie#show ipv6 vrrp
GigabitEthernet 0/13 - Group 1
  State is Master
  Virtual IPv6 address is as follows:
    FE80::2
```

```
  1::2
 Virtual MAC address is 0000.5e00.0201
 Advertisement interval is 1 sec
 Accept_Mode is enabled
 Preemption is enabled
   min delay is 0 sec
 Priority is 100
 Master Router is FE80::1 (local), priority is 100
 Master Advertisement interval is 1 sec
 Master Down interval is 3.60 sec
```

字段解释：

字段	说明
State	备份组状态
Virtual IP address	备份组虚拟 IP 地址
Virtual MAC address	备份组虚拟 MAC 地址
Advertisement interval	备份组 VRRP 通告间隔
Preemption	备份组抢占方式
min delay	备份组抢占延迟时间
Priority	备份组优先级
Master Router	Master 路由设备 IP 地址和优先级
Master Advertisement interval	Master 路由设备通告间隔
Master Down interval	Master 路由设备失效判断间隔
Accept_Mode	IPv6 VRRP 备份组 Accept_Mode 模式

2：查看 VRRP 组的概况

```
Ruijie# show vrrp brief
Interface   Grp Pri timer  Own Pre State   Master addr     Group addr
Gi 0/0     1 100  10.82    -   P  Backup  192.168.201.213 192.168.201.1
Gi 0/0     2 120  10.59    -   P  Master  192.168.201.217 192.168.201.2
Ruijie#show ipv6 vrrp brief
Interface      Grp Pri timer Own Pre State Master addr  Group addr
Gi0/13          1 100 3.60 -  P  Master FE80::1               FE80::2
```

字段解释：

字段	说明
Interface	以太网口名称
Grp	接口上设置的 VRRP 备份组号
Pri	备份组优先级
timer	备份组计算的 Master 路由设备失效判断间隔
Own	备份组 Owner 状态
Pre	备份组抢占方式
State	备份组状态

Master addr	Master 路由设备 IP 地址
Group addr	备份组主虚拟 IP 地址

【提示信息】 -

【平台说明】 -

1.3 show vrrp interface

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**]

【参数说明】

参数	描述
ipv6	应用于 IPv6。缺省为 IPv4。
type	接口的类型
number	接口的序号
brief	显示概要信息。缺省显示完整信息。

【命令模式】 特权模式、全局模式、接口模式

【缺省级别】 14

【使用指导】 -

【配置举例】 1：显示以太网口 GigabitEthernet 0/0 上的 IPv4 VRRP 情况

```
Ruijie# show vrrp interface GigabitEthernet 0/0
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
```

字段解释：

字段	说明
State	备份组状态
Virtual IP address	备份组虚拟 IP 地址
Virtual MAC address	备份组虚拟 MAC 地址
Advertisement interval	备份组 VRRP 通告间隔
Preemption	备份组抢占方式
min delay	备份组抢占延迟时间
Priority	备份组优先级
Master Router	Master 路由设备 IP 地址和优先级
Master Advertisement interval	Master 路由设备通告间隔
Master Down interval	Master 路由设备失效判断间隔

【提示信息】 -

【平台说明】 -

1.4 show vrrp packet statistics

查看 VRRP 报文收发的统计信息。

show vrrp packet statistics [*interface-type interface-number*]

【参数说明】

参数	描述
interface-type interface-number	接口类型和接口编号。缺省显示所有接口的 VRRP 报文收发统计信息。

【命令模式】 特权模式、全局模式、接口模式

【缺省级别】 14

【使用指导】 -

【配置举例】 1：查看所有接口上的 VRRP 报文统计信息

```
Ruijie# show vrrp packet statistics
```

```
Total
   InReceives: 966043 packets, InOctets: 38641824, InErrors: 38826
   OutTransmits: 306079, OutOctets: 7798564
GigabitEthernet 3/0/1
   InReceives: 799665 packets, InOctets: 31986600, InErrors: 19657
   OutTransmits: 272931, OutOctets: 6675320
GigabitEthernet 3/0/2
   InReceives: 0 packets, InOctets: 0, InErrors: 0
   OutTransmits: 681, OutOctets: 16344
```

字段解释：

字段	说明
Total	所有接口上的 VRRP 报文统计信息。
InReceives	所有接口上接收到 VRRP 报文的数目。
InOctets	所有接口上接收到 VRRP 报文的字节数。
InErrors	所有接口上接收到 VRRP 错误报文的数目。
OutTransmits	所有接口上发送 VRRP 报文的数目。
OutOctets	所有接口上发送 VRRP 报文的字节数。

2：查看接口 gigabitEthernet 3/0/1 的 VRRP 报文统计信息

```
Ruijie#show vrrp packet statistics gigabitEthernet 3/0/1
GigabitEthernet 3/0/1
   InReceives: 799911 packets, InOctets: 31996440, InErrors: 19657
   OutTransmits: 273053, OutOctets: 6677760
```

字段解释：

字段	说明
InReceives	某接口上所有接收到 VRRP 报文的数目。
InOctets	某接口上所有接收到 VRRP 报文的字节数。
InErrors	某接口上所有接收到 VRRP 错误报文的数目。
OutTransmits	某接口上所有发送 VRRP 报文的数目。
OutOctets	某接口上所有发送 VRRP 报文的字节数。

【提示信息】 -

【平台说明】 -

1.5 vrrp accept_mode

启用 IPv6 VRRP 虚拟路由器的报文接收功能。

vrrp ipv6 *group* **accept_mode**

关闭 IPv6 VRRP 虚拟路由器的报文接收功能。

no vrrp ipv6 *group* **accept_mode**

【参数说明】

参数	描述
group	VRRP 组号

【缺省配置】 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。

【命令模式】 接口模式

【缺省级别】 14

【使用指导】 在网络接口配置，对配置的处于 Master 状态的虚拟路由器生效。

只有 IPv6 VRRP 才有此配置模式。

【配置举例】 1：在接口 GigabitEthernet 0/0 上启用 IPv6 VRRP 功能。该 IPv6 VRRP 组号为 1，在 IPv6 VRRP 组 1 上启用 IPv6 VRRP 虚拟路由器的报文接收功能。

```
Ruijie#configure terminal
Ruijie(config)#interface GigabitEthernet 0/0
// ‘no switchport’命令在交换机上使用
Ruijie(config-if-GigabitEthernet 0/0)#no switchport
Ruijie(config-if-GigabitEthernet 0/0)#ipv6 enable
Ruijie(config-if-GigabitEthernet 0/0)#ipv6 address 2001::2/64
Ruijie(config-if-GigabitEthernet 0/0)#vrrp 1 ipv6 FE80::1
Ruijie(config-if-GigabitEthernet 0/0)#vrrp 1 ipv6 2001::1
Ruijie(config-if-GigabitEthernet 0/0)# vrrp ipv6 1 accept_mode
```

【检验方法】 1：使用 **show ipv6 vrrp** 命令，可以查看 IPv6 VRRP 虚拟路由器的报文接收功能是启用还是关闭。

【提示信息】 -

【常见错误】 -

【平台说明】 -

1.6 vrrp authentication

启用 VRRP 数据包验证功能。
vrrp *group* **authentication** *string*

关闭 VRRP 数据包验证功能。
no vrrp *group* **authentication**

【参数说明】

参数	描述
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)

【缺省配置】 缺省情况下，系统在接口上没有启用 VRRP 功能。即便启用 VRRP 功能，系统没有缺省设置任何验证口令。

【命令模式】 接口模式

【缺省级别】 14

【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。

【配置举例】 1：在接口 GigabitEthernet 0/0 上启用 IPv4 VRRP 功能。该 IPv4 VRRP 组号为 1，在 IPv4 VRRP 组 1 上设置验证口令。

```
Ruijie#configure terminal
Ruijie(config)#interface GigabitEthernet 0/0
// ‘no switchport’在交换机上使用
Ruijie(config-if-GigabitEthernet 0/0)#no switchport
Ruijie(config-if-GigabitEthernet 0/0)#ip address 10.0.1.1 255.255.255.0
Ruijie(config-if-GigabitEthernet 0/0)#vrrp 1 ip 10.0.1.20
Ruijie(config-if-GigabitEthernet 0/0)# vrrp 1 authentication x30dn78k
```

【检验方法】 1：使用 **show vrrp** 命令，可以查看数据包验证功能是启用还是关闭。

【提示信息】 1：如果输入验证口令长度大于 8，则提示错误。

```
VRRP: Maximum authentication string length is 8.
```

【常见错误】 1 :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。
2：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。

【平台说明】 -

1.7 vrrp delay

启用配置某个接口上 VRRP 备份组的延迟启动时间。
vrrp delay { **minimum** *min-seconds* | **reload** *reload-seconds* }

关闭配置某个接口上 VRRP 备份组的延迟启动时间。
no vrrp delay

【参数说明】

参数	描述
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

【缺省配置】 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。缺省状态下，接口没有配置 VRRP 备份组延迟启动。两种 VRRP 备份组延迟启动时间的取值范围均为 0~60 秒。

【命令模式】 接口模式

【缺省级别】 14

【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。网络接口配置此命令，将对 IPv4 VRRP 和 IPv6 VRRP 同时生效。

【配置举例】 1：在接口 GigabitEthernet 0/0 上启用 IPv4 VRRP 功能。该 IPv4 VRRP 组号为 1，在接口 GigabitEthernet 0/0 上启动 VRRP 备份组的延迟启动。

```
Ruijie#configure terminal
Ruijie(config)#interface GigabitEthernet 0/0
// 'no switchport'在交换机上使用
Ruijie(config-if-GigabitEthernet 0/0)#no switchport
Ruijie(config-if-GigabitEthernet 0/0)#vrrp delay minimum 10 reload 10
Ruijie(config-if-GigabitEthernet 0/0)#ip address 10.0.1.1 255.255.255.0
Ruijie(config-if-GigabitEthernet 0/0)#vrrp 1 ip 10.0.1.20
```

【检验方法】 1：使用 **show vrrp** 或 **show ipv6 vrrp** 命令，可以查看 VRRP 备份组延迟启动剩余时间。

【提示信息】 -

【常见错误】 -

【平台说明】 -

1.8 vrrp description

为 IPv4 VRRP 或者 IPv6 VRRP 指定一个描述符。
vrrp [**ipv6**] *group* **description** *text*

恢复系统缺省设置。
no vrrp [**ipv6**] *group* **description**

【参数说明】

参数	描述
ipv6	应用于 IPv6。缺省为 IPv4。
group	VRRP 组号
text	VRRP 组描述符

【缺省配置】 缺省情况下，系统在接口上没有启用 VRRP 功能。即便启用了 VRRP 功能，系统也没有缺省设置任何 VRRP 组描述符。

【命令模式】 接口模式

【缺省级别】 14

【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。

【配置举例】 1 :在接口 GigabitEthernet 0/0 上启用 VRRP 功能。该备份组号为 1 ,在接口 GigabitEthernet 0/0 上的 IPv4 VRRP 组 1 为 Building A – Marketing and Administration，IPv6 VRRP 组 1 为 Building B – Marketing and Administration。

```
Ruijie#configure terminal
Ruijie(config)#interface GigabitEthernet 0/0
Ruijie(config-if-GigabitEthernet 0/0)#ip address 10.0.1.1 255.255.255.0
Ruijie(config-if-GigabitEthernet 0/0)#vrrp 1 ip 10.0.1.20
Ruijie(config-if-GigabitEthernet 0/0)#vrrp 1 description “Building A - Marketing and Administration”
Ruijie(config-if-GigabitEthernet 0/0)#vrrp 1 ipv6 fe80::1
Ruijie(config-if-GigabitEthernet 0/0)#vrrp ipv6 1 description “Building B - Marketing and Administration”
```

【检验方法】 1：使用 **show vrrp** 或 **show ipv6 vrrp** 命令，可以查看 VRRP 组是否设置描述符。

【提示信息】 1：如果设置的描述符超过 80 个字节，提示配置错误。

```
% The length of description is up to 80!
```

【常见错误】 -

【平台说明】 -

1.9 vrrp ip

在接口上启用 VRRP 并设置对应的虚拟 IP 地址。

vrrp *group* **ip** *ipaddress* [**secondary**]

禁止该接口上的 VRRP 功能并取消虚拟 IP 地址的设置。

no vrrp *group* **ip** *ipaddress* [**secondary**]

【参数说明】

参数	描述
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

【缺省配置】 缺省情况下，系统在接口上没有启用 VRRP 功能。

【命令模式】 接口模式

【缺省级别】 14

【使用指导】 如果不使用 secondary 参数，那么设置的 IP 地址将成为虚拟设备的主 IP 地址。

【配置举例】 1：在接口 GigabitEthernet 0/0 上启用 VRRP 功能。该 VRRP 组号为 1，虚拟设备的主 IP 地址为 10.0.1.20，次 IP 地址为 10.0.2.20。

```
Ruijie#configure terminal
Ruijie(config)#interface GigabitEthernet 0/0
// ‘no switchport’在交换机上使用
Ruijie(config-if-GigabitEthernet 0/0)#no switchport
Ruijie(config-if-GigabitEthernet 0/0)#ip address 10.0.1.1 255.255.255.0
Ruijie(config-if-GigabitEthernet 0/0)#ip address 10.0.2.1 255.255.255.0 secondary
Ruijie(config-if-GigabitEthernet 0/0)#vrrp 1 ip 10.0.1.20
Ruijie(config-if-GigabitEthernet 0/0)#vrrp 1 ip 10.0.2.20 secondary
```

【检验方法】 1：使用 **show vrrp** 命令，可以查看接口上 VRRP 功能是启用还是关闭。

【提示信息】 1：如果是 no 命令且该接口上不存在该备份组号的备份组，则提示信息。

```
VRRP:there is not ipv4 group 1 on interface Vl10.
```

2：如果设置的虚拟 IP 地址不是有效的地址，则提示错误。

```
VRRP:127.0.0.1 is not a valid host address.
```

3：如果配置的虚拟 IP 地址是接口上的子网地址或广播地址，则提示错误。

```
VRRP: IP address 192.168.23.0 cannot be equal to interface broadcast or subnet address.
```

4：如果备份组配置未配置主虚拟 IP 地址，直接配置从虚拟 IP 地址，则提示信息。

```
VRRP: the first address assigned to IPv4 virtual router must be primary address!
```

5：如果 no 命令删除从虚拟 IP 地址，但该备份组不存在该从虚拟 IP 地址，则提示错误。

```
VRRP: 192.168.23.162 is not secondary virtual IP address of ipv4 group 1 on interface vl2.
```

6：如果 no 命令删除主虚拟 IP 地址，但该备份组不存在该主虚拟 IP 地址，则提示错误。

```
VRRP: 192.168.23.160 is not primary virtual IP address of ipv4 group 2 on interface vl2.
```

7：如果 no 命令删除主虚拟 IP 地址，但该备份组还存在从虚拟 IP 地址，则提示错误。

```
VRRP: all secondary addresses must be deleted before deleting primary address.
```

【常见错误】 1 :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。

【平台说明】 -

1.10 vrrp ipv6

在接口上启用 IPv6 的 VRRP 并设置对应的虚拟 IPv6 地址。
vrrp *group* **ipv6** *ipv6-address*

禁止该接口上的 VRRP 功能并取消虚拟 IPv6 地址的设置。
no vrrp *group* **ipv6** *ipv6-address*

【参数说明】

参数	描述
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

【缺省配置】 缺省情况下，系统在接口上没有启用 IPv6 的 VRRP 功能。

【命令模式】 接口模式

【缺省级别】 14

【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。

【配置举例】 1：在接口 Fa0/0 上启用 IPv6 的 VRRP 功能。该 VRRP 组号为 1，虚拟 IPv6 地址为 FE80::1 和 2001::1。

```
Ruijie#configure terminal
Ruijie(config)#interface GigabitEthernet 0/0
// ‘no switchport’命令在交换机上使用
Ruijie(config-if-GigabitEthernet 0/0)#no switchport
Ruijie(config-if-GigabitEthernet 0/0)#ipv6 enable
Ruijie(config-if-GigabitEthernet 0/0)#ipv6 address 2001::2/64
Ruijie(config-if-GigabitEthernet 0/0)#vrrp 1 ipv6 FE80::1
Ruijie(config-if-GigabitEthernet 0/0)#vrrp 1 ipv6 2001::1
```

【检验方法】 1：使用 **show ipv6 vrrp** 命令，可以查看接口上 IPv6 的 VRRP 功能是启用还是关闭。

【提示信息】 1：如果是 no 命令且该接口上不存在该备份组号的备份组，则提示信息。

```
VRRP:there is not ipv6 group 1 on interface vl2.
```

2：如果设置的虚拟 IP 地址不是有效的 IPv6 地址，则提示错误。

```
VRRP:::1 is not a valid host address.
```

3：如果配置虚拟 IP 地址时，接口被绑定到多协议 VRF，但该 VRF 没有配置 IPv6 地址族，则提示错误。

```
VRRP: VLAN 2 is linked to a VRF. Enable IPv6 on that VRF first.
```

4：如果配置的虚拟 IP 地址和同一个 VRF 实例中其他接口的 IP 地址重叠，则提示错误。

```
VRRP: 2001::66 overlaps with other interface's address.
```

6：如果备份组配置的第一个虚拟 IP 地址不是链路本地地址，则提示信息。

```
VRRP: the first address assigned to IPv6 virtual router must be link-local address.
```

7：如果 no 命令删除虚拟 IP 地址，但该备份组不存在该虚拟 IP 地址，则提示错误。

```
VRRP: FE80::66 is not virtual IPv6 address of ipv6 group 1 on interface vl2.
```

8：如果 no 命令删除的是链路本地地址，但还存在非链路本地地址，则提示信息。

```
VRRP: link-local address must be deleted at last.
```

【常见错误】 1：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。

【平台说明】 -

1.11 vrrp preempt

设置 IPv4 VRRP 组或者 IPv6 VRRP 处于抢占模式。
vrrp [**ipv6**] *group* **preempt** [**delay** *seconds*]

禁止 VRRP 抢占功能。
no vrrp [**ipv6**] *group* **preempt** [**delay**]

【参数说明】

参数	描述
ipv6	应用于 IPv6。缺省为 IPv4。
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。

【缺省配置】 缺省情况下，系统在接口上没有启用 VRRP 功能。
一旦启用 VRRP 功能，VRRP 组默认工作在抢占模式下。

【命令模式】 接口模式

【缺省级别】 14

【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。

【配置举例】 1：在接口 GigabitEthernet 0/0 上启用 IPv4 VRRP 功能。该 IPv4 VRRP 组号为 1，一旦 IPv4 VRRP 组发现自己的优先级(200)高于当前主设备的优先级，它会在等待 15 秒后宣告自己抢占为主设备。

```
Ruijie#configure terminal
Ruijie(config)#interface GigabitEthernet 0/0
// ‘no switchport’在交换机上使用
Ruijie(config-if-GigabitEthernet 0/0)#no switchport
Ruijie(config-if-GigabitEthernet 0/0)#ip address 10.0.1.1 255.255.255.0
Ruijie(config-if-GigabitEthernet 0/0)#vrrp 1 ip 10.0.1.20
Ruijie(config-if-GigabitEthernet 0/0)#vrrp 1 preempt delay 15
Ruijie(config-if-GigabitEthernet 0/0)#vrrp 1 priority 200
```

2：在接口 GigabitEthernet 0/0 上启用 IPv6 VRRP 功能。该 IPv6 VRRP 组号为 1，一旦 IPv6 VRRP 组发现自己的优先级(200)高于当前主设备的优先级，它会在等待 15 秒后宣告自己抢占为主设备。

```
Ruijie#configure terminal
Ruijie(config)#interface GigabitEthernet 0/0
// ‘no switchport’命令在交换机上使用
Ruijie(config-if-GigabitEthernet 0/0)#no switchport
Ruijie(config-if-GigabitEthernet 0/0)#ipv6 enable
Ruijie(config-if-GigabitEthernet 0/0)#ipv6 address 2001::2/64
Ruijie(config-if-GigabitEthernet 0/0)#vrrp 1 ipv6 FE80::1
Ruijie(config-if-GigabitEthernet 0/0)#vrrp 1 ipv6 2001::1
Ruijie(config-if-GigabitEthernet 0/0)#vrrp ipv6 1 preempt delay 15
Ruijie(config-if-GigabitEthernet 0/0)#vrrp ipv6 1 priority 200
```

【检验方法】 1：使用 **show vrrp** 或 **show ipv6 vrrp** 命令，可以查看抢占模式是启用还是关闭。

【提示信息】 -

【常见错误】 -

【平台说明】 -

1.12 vrrp priority

设置 IPv4 VRRP 组或者 IPv6 VRRP 组的优先级。
vrrp [**ipv6**] *group* **priority** *level*

恢复系统默认设置。
no vrrp [**ipv6**] *group* **priority**

【参数说明】

参数	描述
ipv6	应用于 IPv6。缺省为 IPv4。
group	VRRP 组号
level	VRRP 组的优先级

【缺省配置】 缺省情况下，系统在接口上没有启用 VRRP 功能。一旦启用 VRRP 功能，VRRP 组默认其优先级为 100。

【命令模式】 接口模式

【缺省级别】 14

【使用指导】 该命令将手动设置 VRRP 组的优先级。

【配置举例】 1：在接口 GigabitEthernet 0/0 上启用 IPv4 VRRP 功能。该 IPv4 VRRP 组号为 1，设置 IPv4 VRRP 组 1 的优先级为 254。

```
Ruijie#configure terminal
Ruijie(config)#interface GigabitEthernet 0/0
// ‘no switchport’在交换机上使用
Ruijie(config-if-GigabitEthernet 0/0)#no switchport
Ruijie(config-if-GigabitEthernet 0/0)#ip address 10.0.1.1 255.255.255.0
Ruijie(config-if-GigabitEthernet 0/0)#vrrp 1 ip 10.0.1.20
Ruijie(config-if-GigabitEthernet 0/0)#vrrp 1 priority 254
```

2：在接口 GigabitEthernet 0/0 上启用 IPv6 VRRP 功能。该 IPv6 VRRP 组号为 1，设置 IPv6 VRRP 组 1 的优先级为 254。

```
Ruijie#configure terminal
Ruijie(config)#interface GigabitEthernet 0/0
// ‘no switchport’命令在交换机上使用
Ruijie(config-if-GigabitEthernet 0/0)#no switchport
Ruijie(config-if-GigabitEthernet 0/0)#ipv6 enable
Ruijie(config-if-GigabitEthernet 0/0)#ipv6 address 2001::2/64
Ruijie(config-if-GigabitEthernet 0/0)#vrrp 1 ipv6 FE80::1
Ruijie(config-if-GigabitEthernet 0/0)#vrrp 1 ipv6 2001::1
Ruijie(config-if-GigabitEthernet 0/0)#vrrp ipv6 1 priority 254
```

【检验方法】 1：使用 **show vrrp** 或 **show ipv6 vrrp** 命令，可以查看 VRRP 组的优先级。

【提示信息】 1：如果当前备份组处于 Owner 状态，则提示信息。

```
VRRP: Priority change will have no effect while interface is VRRP address owner.
```

【常见错误】 -

【平台说明】 -

1.13 vrrp timers advertise

设置 IPv4 VRRP 组或者 IPv6 VRRP 组主设备发送 VRRP 通告的间隔。

vrrp [**ipv6**] *group* **timers advertise** { *advertise-interval* | **csec** *centisecond-interval* }

恢复系统默认设置。

no vrrp [**ipv6**] *group* **timers advertise**

【参数说明】

参数	描述
ipv6	应用于 IPv6。缺省为 IPv4。
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。

【缺省配置】 缺省情况下，系统在接口上没有启用 VRRP 功能。一旦启用 VRRP 功能，系统默认主设备的通告发送间隔为 1 秒。

【命令模式】 接口模式

【缺省级别】 14

【使用指导】 如果当前设备成 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，配置了组播报文发送标准为 VRRPv3 的 IPv4 VRRP 组或者 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。

【配置举例】 1：在接口 GigabitEthernet 0/0 上启用 VRRP 功能。该备份组号为 1，设置 IPv4 VRRP 通告发送间隔为 4 秒。

```
Ruijie#configure terminal
Ruijie(config)#interface GigabitEthernet 0/0
// ‘no switchport’在交换机上使用
Ruijie(config-if-GigabitEthernet 0/0)#no switchport
Ruijie(config-if-GigabitEthernet 0/0)#ip address 10.0.1.1 255.255.255.0
Ruijie(config-if-GigabitEthernet 0/0)#vrrp 1 ip 10.0.1.20
Ruijie(config-if-GigabitEthernet 0/0)#vrrp 1 timers advertise 4
```

2：在接口 GigabitEthernet 0/0 上启用 IPv6 VRRP 功能。该 IPv6 VRRP 组号为 1，设置 IPv6 VRRP 通告发送间隔为 4 秒。

```
Ruijie#configure terminal
Ruijie(config)#interface GigabitEthernet 0/0
// ‘no switchport’命令在交换机上使用
Ruijie(config-if-GigabitEthernet 0/0)#no switchport
Ruijie(config-if-GigabitEthernet 0/0)#ipv6 enable
Ruijie(config-if-GigabitEthernet 0/0)#ipv6 address 2001::2/64
Ruijie(config-if-GigabitEthernet 0/0)#vrrp 1 ipv6 FE80::1
```

```
Ruijie(config-if-GigabitEthernet 0/0)#vrrp 1 ipv6 2001::1
Ruijie(config-if-GigabitEthernet 0/0)#vrrp ipv6 1 timers advertise 4
```

3：在接口 GigabitEthernet 0/0 上启用 VRRP 功能。该备份组号为 1，设置 IPv4 VRRP 通告发送间隔为 50 厘秒。

```
Ruijie#configure terminal
Ruijie(config)#interface GigabitEthernet 0/0
// 'no switchport'在交换机上使用
Ruijie(config-if-GigabitEthernet 0/0)#no switchport
Ruijie(config-if-GigabitEthernet 0/0)#ip address 10.0.1.1 255.255.255.0
Ruijie(config-if-GigabitEthernet 0/0)#vrrp 1 ip 10.0.1.20
Ruijie(config-if-GigabitEthernet 0/0)#vrrp 1 timers advertise csec 50
```

4：在接口 GigabitEthernet 0/0 上启用 IPv6 VRRP 功能。该 IPv6 VRRP 组号为 1，设置 IPv6 VRRP 通告发送间隔为 50 厘秒。

```
Ruijie#configure terminal
Ruijie(config)#interface GigabitEthernet 0/0
// 'no switchport'命令在交换机上使用
Ruijie(config-if-GigabitEthernet 0/0)#no switchport
Ruijie(config-if-GigabitEthernet 0/0)#ipv6 enable
Ruijie(config-if-GigabitEthernet 0/0)#ipv6 address 2001::2/64
Ruijie(config-if-GigabitEthernet 0/0)#vrrp 1 ipv6 FE80::1
Ruijie(config-if-GigabitEthernet 0/0)#vrrp 1 ipv6 2001::1
Ruijie(config-if-GigabitEthernet 0/0)#vrrp ipv6 1 timers advertise csec 50
```

【检验方法】 1：使用 **show vrrp** 或 **show ipv6 vrrp** 命令，可以查看 VRRP 组的通告发送间隔。

2：配置了组播报文发送标准为 VRRPv3 的 IPv4 VRRP 组或者 IPv6 VRRP 备份组，如果配置的报文通告间隔超过 40 秒，通过 show vrrp 或 show ipv6 vrrp 命令查看的 VRRP 组的通告发送间隔为 40 秒。

配置了组播报文发送标准为 VRRPv3 的 IPv4 VRRP 组或者 IPv6 VRRP 备份组，如果配置的报文通告间隔为 50-99 厘秒，通过 show vrrp 或 show ipv6 vrrp 命令查看的 VRRP 组的通告发送间隔为配置的厘秒时间；如果组播报文发送标准为 VRRPv2 的 IPv4 VRRP 组配置的报文通告间隔为 50-99 厘秒，通过 show vrrp 命令查看的 VRRP 组的通告发送间隔为默认的 1s。

【提示信息】 1：配置了组播报文发送标准为 VRRPv3 的 IPv4 VRRP 组或者 IPv6 VRRP 备份组，如果配置的报文通告间隔超过 40 秒，则提示错误：

```
VRRP: The Maximum adver time of VRRPv3 Packet is 40s.
```

【常见错误】 -

【平台说明】 -

1.14 vrrp timers learn

启用 IPv4 VRRP 或者 IPv6 VRRP 的定时器学习功能。
vrrp [**ipv6**] *group* **timers learn**

关闭 IPv4 VRRP 或者 IPv6 VRRP 的定时器学习功能。
no vrrp [**ipv6**] *group* **timers learn**

【参数说明】

参数	描述
ipv6	应用于 IPv6。缺省为 IPv4。
group	VRRP 组号

【缺省配置】 缺省情况下，系统在接口上没有启用 VRRP 功能。即便启用 VRRP 功能，系统默认情况下还是关闭了定时器学习功能。

【命令模式】 接口模式

【缺省级别】 14

【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。

【配置举例】 1：在接口 GigabitEthernet 0/0 上启用 IPv4 VRRP 功能。该 IPv4 VRRP 组号为 1，在 IPv4 VRRP 组 1 上启用了定时器学习功能。

```
Ruijie#configure terminal
Ruijie(config)#interface GigabitEthernet 0/0
// ‘no switchport’在交换机上使用
Ruijie(config-if-GigabitEthernet 0/0)#no switchport
Ruijie(config-if-GigabitEthernet 0/0)#ip address 10.0.1.1 255.255.255.0
Ruijie(config-if-GigabitEthernet 0/0)#vrrp 1 ip 10.0.1.20
Ruijie(config-if-GigabitEthernet 0/0)#vrrp 1 timers learn
```

2：在接口 GigabitEthernet 0/0 上启用 IPv6 VRRP 功能。该 IPv6 VRRP 组号为 1，在 IPv6 VRRP 组 1 上启用了定时器学习功能。

```
Ruijie#configure terminal
Ruijie(config)#interface GigabitEthernet 0/0
// ‘no switchport’命令在交换机上使用
Ruijie(config-if-GigabitEthernet 0/0)#no switchport
Ruijie(config-if-GigabitEthernet 0/0)#ipv6 enable
Ruijie(config-if-GigabitEthernet 0/0)#ipv6 address 2001::2/64
```

```
Ruijie(config-if-GigabitEthernet 0/0)#vrrp 1 ipv6 FE80::1
Ruijie(config-if-GigabitEthernet 0/0)#vrrp 1 ipv6 2001::1
Ruijie(config-if-GigabitEthernet 0/0)#vrrp ipv6 1 timers learn
```

【检验方法】 -

【提示信息】 -

【常见错误】 1：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。

【平台说明】 -

1.15 vrrp track

启用 IPv4 VRRP 的链路跟踪功能。
vrrp *group* **track** { *interface-type interface-number* } [*priority*]

启用 Ipv6 VRRP 的链路跟踪功能。
vrrp ipv6 *group* **track** { *interface-type interface-number* } [*priority*]

关闭 VRRP 的接口跟踪功能。
no vrrp *group* **track** *interface-type interface-number*

关闭 Ipv6 VRRP 的接口跟踪功能。
no vrrp ipv6 *group* **track** *interface-type interface-number*

启用 IPv4 VRRP 的 IP 地址跟踪功能。
vrrp *group* **track** *ipv4-address* [**interval** *interval-value*] [**timeout** *timeout-value*] [**retry** *retry-value*] [*priority*]

启用 Ipv6 VRRP 的 Ipv6 地址跟踪功能。
vrrp ipv6 *group* **track** *ipv6-address* [**interval** *interval-value*] [**timeout** *timeout-value*] [**retry** *retry-value*] [*priority*]

关闭 IPv4 VRRP 的 IP 地址跟踪功能。
no vrrp *group* **track** *ipv4-address*

关闭 Ipv6 VRRP 的 Ipv6 地址跟踪功能。
no vrrp ipv6 *group* **track** *ipv6-address*

【参数说明】

参数	描述

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。
ipv6	应用于 IPv6。缺省为 IPv4。
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。

【缺省配置】 缺省情况下，系统在接口上没有启用 VRRP 功能。
即便启用 VRRP 功能，系统没有缺省指定监视的接口、IPv4 地址或者 IPv6 地址。

【命令模式】 接口模式

【缺省级别】 14

【使用指导】

- 可以使用本命令监视出口链路，需要注意的是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)。
- 如果是监视主机，对于 IPv4 虚拟路由器，指定主机的 IPv4 地址；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，可以配置监视 IP 地址或者监视接口，但此时不改变 VRRP 组的优先级。

【配置举例】 1 .在接口 GigabitEthernet 0/0 上启用 IPv4 VRRP 功能。该 IPv4 VRRP 组号为 1 ,VRRP 组 1 对 GigabitEthernet 1/1 进行监视。如果 GigabitEthernet 1/1 链路断开，VRRP 组的优先级就减少 30；在 GigabitEthernet 1/1 的链路恢复后，VRRP 组 1 的优先级恢复。

```
Ruijie#configure terminal
Ruijie(config)#interface  GigabitEthernet 0/0
// ‘no switchport’在交换机上使用
Ruijie(config-if-GigabitEthernet 0/0)#no switchport
Ruijie(config-if-GigabitEthernet 0/0)#ip address 10.0.1.1 255.255.255.0
Ruijie(config-if-GigabitEthernet 0/0)#vrrp 1 ip 10.0.1.20
Ruijie(config-if-GigabitEthernet 0/0)#vrrp 1 priority 254
Ruijie(config-if-GigabitEthernet 0/0)#vrrp 1 track GigabitEthernet 1/1 30
```

2 :在接口 GigabitEthernet 0/0 上启用 IPv6 VRRP 功能。该 IPv6 VRRP 组号为 1 ,VRRP 组 1 跟踪主机 1000::1 是否可到达。

```
Ruijie#configure terminal
Ruijie(config)#interface GigabitEthernet 0/0
// 'no switchport'命令在交换机上使用
Ruijie(config-if-GigabitEthernet 0/0)#no switchport
Ruijie(config-if-GigabitEthernet 0/0)#ipv6 enable
Ruijie(config-if-GigabitEthernet 0/0)#ipv6 address 2001::2/64
Ruijie(config-if-GigabitEthernet 0/0)#vrrp 1 ipv6 FE80::1
Ruijie(config-if-GigabitEthernet 0/0)#vrrp 1 ipv6 2001::1
Ruijie(config-if-GigabitEthernet 0/0)#vrrp ipv6 1 priority 254
Ruijie(config-if-GigabitEthernet 0/0)#vrrp ipv6 1 track 1000::1
```

3：在接口 GigabitEthernet 0/0 上启用 IPv6 VRRP 功能。该 IPv6 VRRP 组号为 1，VRRP 组 1 跟踪网络接口 VLAN 1 上的主机 FE80::2 是否可到达，注意必须指定网络接口。

```
Ruijie#configure terminal
Ruijie(config)#interface GigabitEthernet 0/0
// 'no switchport'命令在交换机上使用
Ruijie(config-if-GigabitEthernet 0/0)#no switchport
Ruijie(config-if-GigabitEthernet 0/0)#ipv6 enable
Ruijie(config-if-GigabitEthernet 0/0)#ipv6 address 2001::2/64
Ruijie(config-if-GigabitEthernet 0/0)#vrrp 1 ipv6 FE80::1
Ruijie(config-if-GigabitEthernet 0/0)#vrrp 1 ipv6 2001::1
Ruijie(config-if-GigabitEthernet 0/0)#vrrp ipv6 1 priority 254
Ruijie(config-if-GigabitEthernet 0/0)#vrrp ipv6 1 track FE80::2 vlan 1
```

【检验方法】 1：使用 **show vrrp** 命令，可以查看 VRRP 组监视的接口或者地址。

【提示信息】 1：如果监视的接口不是三层接口，则提示错误。

```
VRRP: tracked interface must be a Layer 3 interface.
```

2：如果监控的地址不是有效的地址，则提示错误。

```
VRRP: 127.0.0.1 is not a valid host address.
```

3：如果配置监控地址的 interval-value 小于 timeout-value，则提示错误。

```
VRRP: interval must not be less than timeout.
```

【常见错误】 -

【平台说明】 -

1.16 vrrp version

配置 IPv4 VRRP 的 VRRP 组播报文的发送标准 ,对于 IPv4 VRRP ,VRRP 组播报文的发送标准有两种 VRRPv2 和 VRRPv3。

vrrp *group* **version** { **2** | **3** }

恢复默认 IPv4 VRRP 的 VRRP 组播报文的发送标准。

no vrrp *group* **version**

【参数说明】

参数	描述
2	使用 VRRPv2 报文发送标准
3	使用 VRRPv3 报文发送标准

【缺省配置】 缺省状态下，接口配置 IPv4 VRRP 的报文发送标准为 VRRPv2。

【命令模式】 接口模式

【缺省级别】 14

【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】 1：在接口 GigabitEthernet 0/0 上启用 IPv4 VRRP 功能。该 IPv4 VRRP 组号为 1，在 IPv4 VRRP 组 1 上配置 IPv4 VRRP 使用 VRRPv3 报文发送标准。

```
Ruijie#configure terminal
Ruijie(config)#interface GigabitEthernet 0/0
// 'no switchport'在交换机上使用
Ruijie(config-if-GigabitEthernet 0/0)#no switchport
Ruijie(config-if-GigabitEthernet 0/0)#ip address 10.0.1.1 255.255.255.0
Ruijie(config-if-GigabitEthernet 0/0)#vrrp 1 ip 10.0.1.20
Ruijie(config-if-GigabitEthernet 0/0)# vrrp 1 version 3
```

【检验方法】 1：使用 **show vrrp** 命令，可以查看接口上配置 IPv4 VRRP 报文的发送标准。

【提示信息】 -

【常见错误】 -

【平台说明】 -

2 RNS-TRACK

2.1 delay

配置 track 状态变化的通告延迟时间。
delay { **up** *seconds* [**down** *seconds*] **|** [**up** *seconds*] **down** *seconds* }

删除 delay 设置，恢复缺省值。
no delay

【参数说明】

参数	描述
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。

【缺省配置】 缺省没有延迟。

【命令模式】 track 配置模式

【缺省级别】 1

【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。

【配置举例】 1：配置 track 对象，当 track 对象状态由 down 变为 up 时，延迟 30 秒再通告。

```
Ruijie(config)# track 5 rns 10
Ruijie(config-track)# delay up 30
Ruijie(config-track)# end
```

【检验方法】 使用 **show track** 命令，可以查看 track 对象状态变化的通告延迟时间。

【提示信息】 若 track 对象未配置或配置失败，则配置该 delay 命令时会出错。
set delay error.

【常见错误】 -

【平台说明】 -

2.2 dns

创建一个 DNS 类型的 RNS 探测。

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】

参数	描述
oob	MGMT 口探测
name-server *a.b.c.d*	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 *A.B.C.D*	指定出接口时，下一跳 ip 地址。

【缺省配置】 -

【命令模式】 IP RNS 配置模式(config-ip-rns)

【缺省级别】 1

【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。

必须先配置 RNS 探测的类型（如 icmp-echo、dns），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。

【配置举例】

1：配置 DNS 类型的 RNS 探测，，请求域名 www.ruijie.com.cn 的 ip 地址。

```
Ruijie(config)# ip rns 1
Ruijie(config-ip-rns)# dns www.ruijie.com.cn name-server 61.154.22.41
Ruijie(config-ip-rns-dns)# exit
Ruijie(config)# ip rns schedule 1 start-time now
```

【检验方法】 使用 **show ip rns configuration** 命令，可以查看 RNS 探测的配置信息。

【提示信息】 1 :创建一个 DNS 类型的 RNS 探测时 ,如果内存分配失败 ,则配置失败并提示错误信息。rns object dns create fail

【常见错误】

1：创建一个 DNS 类型的 RNS 探测时，内存分配失败。

2：创建一个 DNS 类型的 RNS 探测时，目的主机名最长为 127 个字符，超出自动截断。

【平台说明】 NBR6205-E、NBR6135-E、NBR6210-E、NBR6215-E 支持 MGMT 口；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 MGMT 口。

2.3 frequency

配置一个 RNS 探测的重复时间间隔。
frequency *milliseconds*

恢复缺省值。
no frequency

【参数说明】

参数	描述
milliseconds	报文的发送时间间隔（毫秒），范围<10-604800000>，最长一周时间。

【缺省配置】 探测的重复时间间隔为 60s。

【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)

【缺省级别】 1

【使用指导】 在一个 RNS 探测的生命期内，会进行周期性的探测处理。通过配置 **frequency** 命令，可以指定该重复间隔。配置上必须满足下面的公式，以保证探测的计算正确性。
(**frequency** *milliseconds*) > (**timeout** *milliseconds*) >= (**threshold** *milliseconds*)

【配置举例】 1：配置一个 ICMP-ECHO 类型的 IP RNS 探测，目的 IP 为 192.168.21.1；设置探测频率为 30 秒，超时时间为 8000 毫秒，阈值为 6000 毫秒。

```
Ruijie(config)# ip rns 1
Ruijie(config-ip-rns)#icmp-echo 192.168.21.1
Ruijie(config-ip-rns-icmp-echo)#frequency 30000
Ruijie(config-ip-rns-icmp-echo)#timeout 8000
Ruijie(config-ip-rns-icmp-echo)#threshold 6000
```

【检验方法】 使用 **show ip rns configuration** 命令，可以查看 RNS 对象的配置信息。

【提示信息】 1：配置探测重复时间时，如果配置的重复时间小于超时时间，则配置失败并提示错误信息

Illegal Value: Cannot set Frequency to be less than Timeout

【常见错误】 1：配置探测重复时间时，配置的重复时间小于超时时间

【平台说明】 -

2.4 icmp-echo

创建一个 ICMP-Echo 类型的 RNS 探测。

icmp-echo { { *destination-ip-address* | *destination-hostname* [**name-server** *ip-address*] } [**source-ipaddr** *ip-address*] } | { { *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】

参数	描述
oob	MGMT 口探测
destination-ip-address	目的 IP 地址。
destination-hostname	目的主机名，最长允许输入 127 字符，超出部分自动截断。
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*	指定出接口时，下一跳 ip 地址。

【缺省配置】 -

【命令模式】 IP RNS 配置模式(config-ip-rns)

【缺省级别】 1

【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。必须先配置 RNS 探测的类型（如 icmp-echo、dns），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。

【配置举例】 1：配置一个 ICMP-ECHO 类型的 IP RNS 探测，目的 IP 为 10.1.1.1。

```
Ruijie(config)# ip rns 1
Ruijie(config-ip-rns)# icmp-echo 10.1.1.1
Ruijie(config-ip-rns-icmp-echo)# exit
```

```
Ruijie(config)# ip rns schedule 1 start-time now life forever
```

【检验方法】 使用 **show ip rns configuration** 命令，可以查看 RNS 对象的配置信息。

【提示信息】 1：创建一个 ICMP-ECHO 类型的 RNS 探测时，如果内存分配失败，则配置失败并提示错误信息。rns object icmp-echo create fail.

【常见错误】 -

【平台说明】 NBR6205-E、NBR6135-E、NBR6210-E、NBR6215-E 支持 MGMT 口；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 MGMT 口。

2.5 ip rns

定义一个 RNS 操作对象。

ip rns *operation-number* [{ **dns** *destination-hostname* **name-server** *a.b.c.d* **| icmp-echo** *destination-ip-address* **| tcp-connect** *destination-ip-address port-number* } [**frequency** *seconds*] [**timeout** *milliseconds*] [**threshold** *milliseconds*]]

删除一个 RNS 操作对象。

no ip rns *operation-number*

【参数说明】

参数	描述
operation-number	RNS 操作索引，取值范围<1-500>。
dns *destination-hostname* **name-server** *a.b.c.d*	简洁配置 dns 探测： *destination-hostname：*目的主机名，最长允许输入 127 字符，超出部分自动截断。 **name-server** *a.b.c.d* ：dns 服务器 ip 地址。
icmp-echo *destination-ip-address*	简洁配置 icmp-echo 探测： *destination-ip-address：*目的 IP 地址。
tcp-connect *destination-ip-address port-number*	简洁配置 tcp-connect 探测： *destination-ip-address：*目的 IP 地址。 *port-number：*要探测的 tcp 端口。
frequency *seconds*	设置探测的重复时间间隔。详见 1.3 frequency 配置
timeout *milliseconds*	配置一个 IP RNS 探测的超时时间。详见 1.26 timeout 配置
threshold *milliseconds*	配置一个 IP RNS 探测的上限阈值。详见 1.25 threshold 配置

【缺省配置】 -

【命令模式】 全局模式

【缺省级别】 1

【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 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 对象不会被创建；在配置完一个 RNS 探测后，还必须通过 **ip rns schedule** 命令配置它的调度启动策略，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配置模式，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。

简洁配置（执行 ip rns 后续的可选探测项）：执行可选项后，相当于详细配置的 ip rns operation-number、ip rns schedule、具体探测配置（如：icmp-echo 探测等）、frequency、timeout、threshold 等多条命令按照逻辑顺序执行。其中 ip rns schedule 按照参数 start-time now life forever 默认启动探测。其余配置项的限制可参考详细配置下的各参数的限制。

同样，需要修改一个通过简洁配置的探测，需要先先删除该 RNS 探测（通过全局模式下输入 no ip rns 命令），再重新进行配置。

【配置举例】

1：详细配置：配置操作索引为 1 的 RNS 探测。

```
Ruijie(config)# ip rns 1
Ruijie(config-ip-rns)# icmp-echo 10.1.1.1
Ruijie(config-ip-rns-icmp-echo)# threshold 10000
Ruijie(config-ip-rns-icmp-echo)# timeout 20000
Ruijie(config-ip-rns-icmp-echo)# frequency 30000
Ruijie(config)# ip rns schedule 1 start-time now life forever
```

2：简洁配置：配置操作索引为 1 的 RNS 探测。

```
Ruijie(config)# ip rns 1 icmp-echo 10.1.1.1 threshold 10000 timeout 20000 frequency 30000
```

【检验方法】 1：使用 **show ip rns statistics** 命令，显示 RNS 探测的统计数据。

【提示信息】

1：定义一个 RNS 操作对象时，如果该操作对像 ID 已存在，且正在运行，则进入 IP RNSI 模式失败并提示错误。

```
Entry already running and cannot be modified
(only can delete (no) and start over)
(check to see if the probe has finished exiting)
```

【常见错误】 1：执行 ip rns 命令时，若对应 RNS 探测已存在并且正在运行，则无法进入该 RNS 探测类型对应的模式。如果需要修改 RNS 探测配置，必须先通过 **no ip rns schedule** 命令删除调度配置，然后再进行修改。

【平台说明】 -

2.6 ip rns reaction-configuration

配置一个 RNS 探测的主动阈值监控和触发机制。

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]

删除该阈值监控机制。

no ip rns reaction-configuration operation-number [**react** monitored-element]

【参数说明】

参数	描述
operation-number	操作索引号，取值范围<1-500>。
monitored-element	指定被监视的探测信息元素。 可带参数有： **allfail**：监控所有失败，动作类型默认为 track，当前供 track 模块交互使用； **rtt**：报文往返时间不在阈值范围时； **timeout**：任一方向超时时。
action-type option	触发后联动的动作。 可带参数有： **none**：不采取任何动作，这是缺省值； **trigger：**仅支持 trigger 联动。 **track：**仅支持 track 联动，仅当 monitored-element 为 allfail 时才可配该动作，且只有该动作类型。
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。例如设置 number-of-measurements 值=3，阈值上限 5000，下限 4000。连续三次探测的值分别为 6000，6000，5000，则他们的平均值为(6000+6000+5000)/3=5667 超过阈值上限 5000。number-of-measures 的缺省值为 5，可选范围 1-16。
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 缺省值为 5，可选范围为 1-16；y 缺省值为 5，可选范围为 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。

【缺省配置】 -

【命令模式】 全局模式

【缺省级别】 1.

【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，支持的监控对象不尽相同，对应关系见下表：

monitored-element	icmp-echo	dns	udp-echo
timeout	✓	✓	✓
rtt	✓	✓	✓

各监控元素的默认阈值如下表:

Monitored Element	Upper Threshold	Lower Threshold
timeout	-	-
rtt	5000 ms	0 ms

【配置举例】 1：配置 rns 1 及其阈值监控处理。

```
Ruijie(config)# ip rns 1
Ruijie(config-ip-rns)# icmp-echo 192.168.23.1
Ruijie(config-ip-rns-icmp-echo)# exit
Ruijie(config)# ip rns schedule 1 start-time now life forever
Ruijie(config)#ip rns reaction-configuration 1 react timeout threshold-type immediate action-type triggerOnly
```

【检验方法】 1：使用 **show ip rns reaction-configuration** 命令，可以查看 RNS 探测的阈值监控配置。

【提示信息】 1：配置 RNS 实例探测的主动阈值时，如果创建 react 变量内存创建失败，配置失败并提示错误信息。
rns react malloc fail
2: 配置监视探测元素信息类型不支持，则配置失败并提示错误信息。
rns entry %d detect not support this react_type %s [react 类型名称]

【常见错误】 1：配置监视探测元素信息类型不支持。

【平台说明】 -

2.7 ip rns reaction-trigger

配置一个 RNS 探测在发生监控阈值超过预期时，触发另一个处于 pending 状态的 IP RNS 探测激活探测。
ip rns reaction-trigger *operation-number target-operatio*n

删除配置。

no ip rns reaction-trigger *operation-number target-operation*

【参数说明】

参数	描述
operation-number	触发动作的源操作号，取值范围<1-500>。
target-operation	被触发的目的操作号，取值范围<1-500>。

【缺省配置】 -

【命令模式】 全局模式

【缺省级别】 1

【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。

【配置举例】 1：配置 ip rns 1 触发 ip rns 2 的联动动作。

```
Ruijie(config)# ip rns 1
Ruijie(config-ip-rns)# icmp-echo www.baidu.com
Ruijie(config-ip-rns-icmp-echo)# exit
Ruijie(config)#ip rns schedule 1 start-time now life forever
Ruijie(config)#ip rns reaction-configuration 1 react timeout threshold-type immediate action-type
trigger
Ruijie(config)# ip rns 2
Ruijie(config-ip-rns)# dns www.baidu.com name-server 8.8.8.8
Ruijie(config-ip-rns-dns)# exit
Ruijie(config)#ip rns reaction-trigger 1 2
```

【检验方法】 1：使用 **show ip rns reaction-trigger** 命令，可以显示 rns 探测的阈值监控配置。

【提示信息】 1：配置 RNS 探测 trigger 对象时，如果 trigger 对象内存分配失败，则配置失败并提示错误信息。

rns trigger malloc fail

【常见错误】 -

【平台说明】 -

2.8 ip rns reset

清除所有 RNS 探测的配置。

ip rns reset

【参数说明】

参数	描述
-	-

【缺省配置】 -

【命令模式】 全局模式

【缺省级别】 1

【使用指导】 该命令清除所有 RNS 配置。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，但发现配置有误）。

【配置举例】 1：清除所有 ip rns 的配置。

```
Ruijie(config)# ip rns reset
```

【检验方法】 1：ip rns reset 执行后，**show ip rns configuation** 查看配置信息，此时显示应该为空。

```
Ruijie(config)#sh ip rns configuration
```

【提示信息】 1：提示 ip rns reset 会清空所有 RNS 配置，确认是否执行，默认为[no]。
WARNING: rns reset will remove all rns configurations, continue? (y/n) [no]
2：如果某个 rns 实例正在探测，则提示是否确认删除，默认为[no]。
rns 1 schedule is running, confirm to delete?(y/n) [no]

【常见错误】 -

【平台说明】 -

2.9 ip rns restart

重新启动一个 RNS 探测。

ip rns restart *operation-number*

【参数说明】

参数	描述
operation-number	RNS 操作索引，取值范围<1-500>。

【缺省配置】 -

【命令模式】 全局模式

【缺省级别】 1

【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 ip rns 探测重新启动。对于未配置调度的 RNS 探测，该命令无效。

【配置举例】 1：重新启动 ip rns 1。

```
Ruijie(config)# ip rns restart 1
```

【检验方法】 -

【提示信息】 1：指定 RNS 探测不存在，则重启探测失败并提示错误信息。

```
rns operate has not define
```

2、指定 RNS 探测 rns schedule 配置不存在，则重启探测失败并提示错误信息。

```
% rns 2 schedule is not configured.
```

3、指定 RNS 探测正在运行，则重启探测失败并提示错误信息。

rns 1 schedule is active state.

【常见错误】 1：指定 RNS 探测不存在。

2:：rns schedule 配置不存在。

3：指定 RNS 探测正在运行。

【平台说明】 -

2.10 ip rns schedule

配置一个 RNS 探测的调度策略。

ip rns schedule operation-number [**life** { **forever** | seconds }] [**start-time** { hh:mm [:ss] [month day | day month] | **pending** | **now** | **after** hh:mm:ss }] [**recurring**]

删除配置。

no ip rns schedule operation-number

【参数说明】

参数	描述
operation-number	Rns 操作索引，取值范围<1-500>。
life forever	rns 的操作生存时间永远有效。
life seconds	rns 的生存时间秒数。
hh:mm [:ss]	精确定义操作开始时间，24 小时制。
month	操作启动的月份，默认是本月，格式为 1-12 月的英文缩写或全称。

day	操作启动的日期，默认是当日，取值范围为<1-31>。
pending	操作启动时间未定，这是默认值。
now	操作启动时间是现在，马上开始。
after hh:mm:ss	延迟 hh:mm:ss 的时间后启动操作。
recurring	是否自动在每天的相同时间启动。

【缺省配置】 默认情况下， RNS 探测处于 pending 状态。即探测不会运行，除非其他 RNS 探测通过 trigger 将其触发执行。

【命令模式】 全局模式

【缺省级别】 1

【使用指导】 已经通过 **ip rns schedule** 命令配置了调度策略的 RNS 探测，如果探测已经开始，其探测参数无法进行修改，如果要修改配置，必须先通过 **no ip rns schedule** 命令删除调度配置，然后再进行修改。

Life{seconds} 是指 ip rns 探测的生命周期 ,即在配置的 start-time 启动探测后 ,经过 seconds 时间将停止探测。

【配置举例】 1：配置探测类型的 RNS 探测，并配置该探测的调度策略。

```
Ruijie(config)# ip rns 1
Ruijie(config-ip-rns)# icmp-echo 10.1.1.1
Ruijie(config-ip-rns-icmp-echo)# exit
Ruijie(config)#ip rns schedule 1 start-time now life forever
```

2：配置完调度策略后，该探测将无法修改。删除调度后，可以修改。

```
Ruijie(config)# ip rns 1
Entry already running and cannot be modified
        (only can delete (no) and start over)
        (check to see if the probe has finished exiting)
Ruijie(config)# no ip rns schedule 1
Ruijie(config)# ip rns 1
Ruijie(config-ip-rns-icmp-echo)# exit
```

【检验方法】 1：使用 **show ip rns configuration** 命令，可以查看 RNS 对象的配置信息。

【提示信息】 1：配置一个 RNS 探测的调度策略时，如果内存分配失败，则配置调度策略失败并提示错误信息

ip rns malloc rns schedule fail

2：如果 schedule 对象已存在并且正在探测，则配置失败并提示错误信息。
Cannot modify schedule. Operation may have started.

【常见错误】 1：ip rns schedule 对象已存在并且正在运行

【平台说明】 -

2.11 object

设置一个 track 跟踪的 list 对象的成员对象。
object *object-number* [**not**]

删除 track 成员。
no object *object-number*

【参数说明】

参数	描述
object-number	track 对象的编号，有效值为 1 到 700。

【缺省配置】 无成员对象。

【命令模式】 track 配置模式

【缺省级别】 1

【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。
object *object-number*:track 对象的状态与成员对象的状态一致，只有当成员对象满足 up，track 对象才有可能为 up；
object *object-number* not:track 对象的状态与成员对象的状态相反，只有当成员对象满足 down，track 对象才有可能为 up；
需要注意的是：
该命令只能在跟踪对象为 list 的 track 模式下进行配置；
track 不能跟踪自己本身；
track 不能互相跟踪。如 track A 跟踪 track B ,track B 不能反过来跟踪 track A。否则可能会造成 track A 和 track B 一直处于震荡状态。

【配置举例】 1：配置一个 track 对象 4，当 track 对象 1 为 up，2 为 down，3 为 up 同时满足时，track 对象 4 为 up。

```
Ruijie(config)# track 4 list boolean and
Ruijie(config-track)# object 1
Ruijie(config-track)# object 2 not
Ruijie(config-track)# object 3
Ruijie(config-track)# end
```

【检验方法】 使用 **show track** 命令，可以查看 track 对象的统计信息。

【提示信息】 1、若 track 对象未配置或配置失败，则配置该 object 命令时会出错。

set object error.

2、若配置成员对象为 track 本身，则配置不成功，提示不能跟踪自己本身。
track can not track itself.

3、若配置的成员对象已经跟踪该 track 对象，则配置不成功。
object xx is already tracking track yy.

【常见错误】 -

【平台说明】 -

2.12 request-data-size

配置一个 RNS 探测的协议载荷大小。
request-data-size *bytes*

恢复默认值。
no request-data-size

【参数说明】

参数	描述
bytes	探测包 payload 的字节数，不同探测的最小/最大字节数不同，具体依据不同探测的子模式下输入命令的提示进行配置。

【缺省配置】 不同探测类型的缺省值不同，默认都是该种类型探测 payload 必须的最小值。

【命令模式】 IP RNS ICMP echo 配置模式 (config-ip-rns-icmp-echo)
IP RNS UDP echo 配置模式 (config-ip-rns-udp-echo)

【缺省级别】 1

【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。
当前 ICMP-ECHO 类型支持的载荷大小取值情况如下表：

探测类型	取值范围	默认值
ICMP-ECHO	[36, 1472]	36
UDP-ECHO	[36, 1472]	36

【配置举例】 1：配置 RNS 探测的协议载荷大小为 50。

```
Ruijie(config)# ip rns 1
Ruijie(config-ip-rns)# icmp-echo 10.1.1.1
Ruijie(config-ip-rns-icmp-echo)# request-data-size 50
```

```
Ruijie(config-ip-rns-icmp-echo)# exit
```

【检验方法】 1：使用 **show ip rns configuration** 命令，可以查看 RNS 对象的配置信息。

【提示信息】 -

【常见错误】 -

【平台说明】 -

2.13 show ip rns collection-statistics

显示 RNS 对象探测的详细统计信息。

show ip rns collection-statistics [*operation-number*]

【参数说明】

参数	描述
operation-number	ip rns 操作对象的编号 ,取值范围<1-500>。缺省为所有的 rns 操作对象。

【命令模式】 特权模式

【缺省级别】 1

【使用指导】 通过该命令，用户可以显示某一个 RNS 对象探测的结果统计信息。

【配置举例】 1：查看所有 RNS 对象探测的结果统计信息（以 icmp-echo 探测类型说明）。

```
Ruijie#show ip rns collection-statistics 1
Entry number: 1
Start Time Index: *2014-03-20 19:53:51
Number of successful operations: 919
Number of operations over threshold: 0
Number of failed operations due to a Disconnect: 0
Number of failed operations due to a Timeout: 2
Number of failed operations due to a Busy: 0
Number of failed operations due to a No Connection: 0
Number of failed operations due to an Internal Error: 2
Number of failed operations due to a Sequence Error: 0
Number of failed operations due to a Verify Error: 0
RTT Values:
RTTAvg: 18       RTTMin: 16       RTTMax: 37
NumOfRTT: 919     RTTSum: 16654       RTTSum2: 302786
```

字段解释：

字段	说明
Entry number	IP RNS 操作索引
Start Time Index:	探测实际启动时刻(调度启动时刻)
Number of successful operations:	成功探测次数
Number of operations over threshold:	超过配置阈值次数
Number of failed operations due to a Disconnect:	断开连接次数
Number of failed operations due to a Timeout:	超时次数
Number of failed operations due to a Busy:	探测目的发送报文，返回对方忙的次数
Number of failed operations due to a No Connection:	因为没有连接上的失败次数
Number of failed operations due to an Internal Error:	因为内部错误探测失败次数
Number of failed operations due to a Sequence Error:	接收顺序错误次数
Number of failed operations due to a Verify Error:	验证接收数据错误次数
RTT Values	往返时间值说明
RTTAvg:	探测往返时间平均值
RTTMin:	探测往返时间最小值
RTTMax:	探测往返时间最大值
NumOfRTT:	统计往返时间的次数
RTTSum:	探测往返时间之和
RTTSum2:	探测往返时间平方和

【提示信息】 1：ip rns 实例不存在
rns operate has not define

【平台说明】 -

2.14 show ip rns configuration

显示 RNS 对象的配置信息。

show ip rns configuration [*operation-number*]

【参数说明】

参数	描述
operation-number	RNS 操作索引，取值范围<1-500>。缺省为所有的 RNS 探测。

【命令模式】 特权模式

【缺省级别】 1

【使用指导】 通过该命令，用户可以显示一个 RNS 探测的配置信息。对于不同的报文类型，配置信息不相同。

【配置举例】 1：查看 ip rns 1 的配置信息。

```
Ruijie# show ip rns configuration 1
Entry number: 1
Tag: ruijie555
Type of operation to perform: icmp-echo
Operation timeout (milliseconds): 5000
Operation frequency (milliseconds): 10000
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
```

字段解释：

字段	说明
Entry number	RNS 操作索引
Tag	实例标签
Type of operation to perform	探测类型
Operation timeout (milliseconds)	超时时间
Operation frequency (milliseconds)	探测的重复时间间隔
Threshold (milliseconds)	阈值
Recurring (Starting Everyday)	是否重复启动标识
Life (seconds)	生存时间
Next Scheduled Start Time	下一次探测调度的启动时间
Target address/Source address	目的地址/源地址
Request size (ARR data portion)	请求报文数据的大小

【提示信息】 1：ip rns 实例不存在
rns operate has not define

【平台说明】 -

2.15 show ip rns operational-state

显示 RNS 探测的当前状态信息。

show ip rns operational-state [*operation-number*]

【参数说明】

参数	描述

operation-number	RNS 操作索引，取值范围<1-500>。缺省为所有的 rns 操作对象。

【命令模式】 特权模式

【缺省级别】 1

【使用指导】 通过该命令，用户可以显示某一个 RNS 探测的当前状态信息。

【配置举例】 1：查看所有 RNS 探测的当前状态信息。

```
Ruijie# show ip rns operational-state
Entry number: 1
Modification time: *2014-01-10 10:26:14
Current seconds left in Life: Forever
Operational state of entry: Active
Number of Octets Used by this Entry: 2272
Number of operations attempted: 232
Number of operations skipped: 0
Connection loss occurred: FALSE
Timeout occurred: FALSE
Over thresholds occurred: FALSE
Latest RTT (milliseconds): 4
Latest operation start time: 2014-01-10 10:26:55
Latest operation return code: OK
```

字段解释：

字段	说明
Entry number	RNS 操作索引
Modification time	探测结果重新统计时间（一次调度启动重新统计结果）
Number of Octets Used by this Entry	该实例探测发送报文字节总数
Number of operations attempted	发送探测总数
Number of operations skipped	发送探测失败总数
Current seconds left in Life	探测剩余生命期
Operational state of entry	探测当前所处状态（Active,Disactive）
Connection loss occurred	是否发送断开连接
Timeout occurred	是否发送超时
Over thresholds occurred	是否超过阈值
Latest RTT (milliseconds)	最近一次探测往返时间
Latest operation start time	最近一次探测发送时间
Latest operation return code	最近一次探测返回值

【提示信息】 1：ip rns 实例不存在

rns operate has not define

【平台说明】 -

2.16 show ip rns reaction-configuration

显示 RNS 探测的主动阈值监控信息。

show ip rns reaction-configuration [*operation-number*]

【参数说明】

参数	描述
operation-numbe	RNS 操作索引，取值范围<1-500>。缺省为所有的 RNS 探测。

【命令模式】 特权模式

【缺省级别】 1

【使用指导】 通过该命令，用户可以显示某一个 RNS 探测的主动阈值监控信息。

【配置举例】 1：查看所有 RNS 探测的主动阈值监控信息

```
Ruijie#show ip rns reaction-configuration
Entry number: 1
Reaction: rtt
Threshold Type: Never
Rising (milliseconds): 5000
Falling (milliseconds): 3000
Threshold Count: 5
Threshold Count2: 5
Action Type: trigger

Reaction: timeout
Threshold Type: Never
Threshold Count: 5
Threshold Count2: 5
Action Type: trigger
```

字段解释：

字段	说明
Entry number	RNS 操作索引
Reaction	阈值监控对象
Threshold Type	阈值触发动作类型
Rising (milliseconds)	阈值上限

Falling (milliseconds)	阈值下限
Threshold Count	当 threshold-type 为 xofy 时的 x 值 或 threshold-type 为 average 时的平均次数
Threshold Count2	当 threshold-type 为 xofy 时的 y 值 或 threshold-type 为 consecutive 时的连续次数
Action Type	动作类型

【提示信息】 1：ip rns 实例不存在
rns operate has not define.

【平台说明】 -

2.17 show ip rns reaction-trigger

显示 RNS 探测的触发探测信息。

show ip rns reaction-trigger [*operation-number*]

【参数说明】

参数	描述
operation-number	ip rns 操作对象的编号 ,取值范围<1-500>。缺省为所有的 rns 操作对象。

【命令模式】 特权模式

【缺省级别】 1

【使用指导】 通过该命令，用户可以显示某一个 RNS 探测的触发探测信息。

【配置举例】 1：查看所有 RNS 探测的触发探测信息。

```
Ruijie#show ip rns reaction-trigger
Entry number: 1
Target rns index: 2
Status of Entry (SNMP RowStatus): active
Operational State: pending
```

字段解释：

字段	说明
Entry number	RNS 操作索引
Target rns index	被触发 RNS 索引值
Status of Entry (SNMP RowStatus)	Rns_entry 状态
Operational State	当前触发状态

【提示信息】 1：ip rns 实例不存在

rns operate has not define

【平台说明】 -

2.18 show ip rns statistics

显示 RNS 对象的简单统计信息。

show ip rns statistics [*operation-number*]

【参数说明】

参数	描述
operation-number	ip rns 操作对象的编号 ,取值范围<1-500>。缺省为所有的 rns 操作对象。

【命令模式】 特权模式

【缺省级别】 1

【使用指导】 通过该命令，用户可以显示某一个 RNS 对象的统计信息。对于不同的报文类型，统计信息不相同。

【配置举例】 1：查看 ip rns 1 的简单统计信息

```
Ruijie#show ip rns statistics 1
Round trip time(RTT) Index 1
Operation time to live: Forever
Latest RTT: 1 ms
Latest operation start time: 2014-01-20 10:21:38
Latest operation return code: OK
Number of successes: 386
Number of failures: 12
```

字段解释：

字段	说明
Round trip time(RTT) Index	Rns 索引 id
Operation time to live	当前探测剩余生命周期
Latest RTT	最近一次探测往返时间
Latest operation start time	最近一次探测开始时间
Latest operation return code	最近一次探测返回值（ok,timeout,noconnection 等）
Number of successes	探测成功次数
Number of failures	探测失败次数

【提示信息】 1：ip rns 实例不存在

rns operate has not define

【平台说明】 -

2.19 show track

查看 track 对象的统计信息。

show track [*object-number*]

【参数说明】

参数	描述
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

【缺省级别】 1

【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】 1：查看所有 track 对象的统计信息

```
Ruijie#show track
Track 1
  Reliable Network Service 5
  The state is Up
    1 change, current state last: 120 secs
  Delay up 30 secs, down 50 secs
Track 3
  Interface FastEthernet 1/0
  The state is Down, delayed Up (5 secs remaining)
    3 change, current state last: 300 secs
  Delay up 60 secs, down 60 secs
Track 4
  List boolean and
Object 1
Object 2 not
  The state is Up
1 change, current state last: 100 secs
  Delay up 0 secs, down 0 secs
```

字段解释：

字段	说明
Track x	Track 对象编号
Reliable Network Service x	跟踪的 rns 对象
The state is x	Track 对象状态
x change	Track 对象状态变化的次数

current state last：x secs	当前 track 对象状态持续的时间
Delay up x secs, down x secs	Track 对象的延迟属性
Interface x x	跟踪的接口信息
The state is x, delayed y (c secs remaining)	当前 track 对象状态为 x，经过 c 秒后将变为 y
List boolean and	Track 对象的结果取所有成员“与”的结果
Object x	成员 x 的满足条件为其状态 up
Object x not	成员 x 的满足条件为其状态 down

【提示信息】 1：指定显示的 track 对象不存在，则提示错误。
Illegal Value: the track object does not exist.

【平台说明】 -

2.20 show track client

查看 track 客户端的统计信息。
show track client

【参数说明】

参数	描述
-	-

【命令模式】 特权模式

【缺省级别】 1

【使用指导】 使用该命令可以查看当前连接到 track 的客户端的统计信息。

【配置举例】 1：查看当前连接到 track 的客户端的统计信息

```
Ruijie# show track client
Track client 2: socket 4
client_path: /tmp/vsd/0/track/.client_nsm
Connection time: Fri Dec 28 17:04:43 2012
```

字段解释：

字段	说明
Track client x: socket x	Track 客户端编号及套接字
client_path: /tmp/vsd/0/track/.client_nsm	客户端连接到 track 的路径
Connection time: xx xx xx xx:xx:xx xx	客户端连接到 track 的时间

【提示信息】 -

【平台说明】 -

2.21 tag

为一个 IP RNS 探测设置一个标签。
tag *text*

删除标签。
no tag

【参数说明】

参数	描述
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。

【缺省配置】 -

【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)

【缺省级别】 1

【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。当标签字符长度超过 79 时自动截断。

【配置举例】 1：配置 ip rns 探测的标签为 telecom_gateway。

```
Ruijie(config)# ip rns 1
Ruijie(config-ip-rns)# icmp-echo 10.1.1.1
Ruijie(config-ip-rns-icmp-echo)# tag telecom_gateway
Ruijie(config-ip-rns-icmp-echo)# exit
```

【检验方法】 1：使用 **show ip rns configuration** 命令，可以查看 RNS 对象的配置信息。

【提示信息】 -

【常见错误】 -

【平台说明】 -

2.22 threshold

配置一个 RNS 探测的上限阈值。
threshold *milliseconds*

恢复缺省值。
no threshold

【参数说明】

参数	描述
milliseconds	探测的上限阈值，取值范围为 0-60000，单位 ms，默认值 5000。

【缺省配置】 5000ms。

【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)

【缺省级别】 1

【使用指导】 threshold 配置必须小于等于 timeout。timeout，frequency，threshold 三者在配置上的关系，请参见 frequency 的使用指导。

【配置举例】 1：配置 RNS 探测的上限阈值为 8000ms。

```
Ruijie(config)# ip rns 1
Ruijie(config-ip-rns)# icmp-echo 10.1.1.1
Ruijie(config-ip-rns-icmp-echo)# threshold 8000
Ruijie(config-ip-rns-icmp-echo)# exit
```

【检验方法】 1：使用 **show ip rns configuration** 命令，可以查看 RNS 对象的配置信息。

【提示信息】 1：配置 threshold 大于 timeout 时，提示参数无效信息。
Illegal Value: Cannot set Threshold to be greater than Timeout.

【常见错误】 -

【平台说明】 -

2.23 timeout

配置一个 RNS 探测的超时时间。
timeout *millisecond*

恢复缺省值。
no timeout

【参数说明】

参数	描述
millisecond	探测超时时间 ,取值范围为 10 - 604800000 ,单位 ms ,默认值均为 5000ms。

【缺省配置】 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。

【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)

【缺省级别】 1

【使用指导】 timeout 的配置必须大于等于 threshold 配置。timeout，frequency，threshold 三者在配置上的关系，请参见 frequency 的使用指导。

【配置举例】 1：配置 IP RNS 探测的超时时间为 10000ms。

```
Ruijie(config)# ip rns 1
Ruijie(config-ip-rns)# icmp-echo 10.1.1.1
Ruijie(config-ip-rns-icmp-echo)# timeout 10000
Ruijie(config-ip-rns-icmp-echo)# exit
```

【检验方法】 1：使用 **show ip rns configuration** 命令，可以查看 RNS 对象的配置信息。

【提示信息】 1：配置 timeout 值时，如果 timeout 值大于 frequency 数值，则配置失败并提示错误信息
Illegal Value: Cannot set Timeout to be greater than Frequency.
2：配置 timeout 值时，如果 timeout 小于 threshold 数值时，提示错误信息。
Illegal Value: Cannot set Timeout to be less than Threshold.

【常见错误】 1：配置 timeout 值时，timeout 大于 frequency。
2：配置 timeout 值时，timeout 小于 threshold。

【平台说明】 -

2.24 tos

配置一个 RNS 探测的 IPv4 报文 tos 字段。

tos *number*

删除配置。

no tos

【参数说明】

参数	描述
number	设置探测报文 IPv4 的 tos 字段，取值范围 0-255。默认为 0。

【缺省配置】 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)

【缺省级别】 1

【使用指导】 tos 是 IPv4 报文头中的一个 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】

```
1：配置 RNS 探测包的 IPv4 报文头中的 tos 字段为 128。Ruijie(config)# ip rns 1
Ruijie(config-ip-rns)# icmp-echo 10.1.1.1
Ruijie(config-ip-rns-icmp-echo)# tos 128
Ruijie(config-ip-rns-icmp-echo)# exit
```

【检验方法】 1：使用 **show ip rns configuration** 命令，可以查看 RNS 对象的配置信息。

【提示信息】 -

【常见错误】 -

【平台说明】 -

2.25 track interface line-protocol

配置 track 对象，跟踪一个接口的链路状态。

track *object-number* **interface** *interface-type interface-number* **line-protocol**

删除 track 对象。
no track *object-number*

【参数说明】

参数	描述
object-number	Track 对象的编号，取值范围为 1-700。
Interface-type *interface-number*	接口类型、接口编号。

【缺省配置】 -

【命令模式】 全局模式

【缺省级别】 1

【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。

【配置举例】 1：配置一个 track 对象，其编号为 3，且用来跟踪接口 ethernet 0/1 的链路状态。

```
Ruijie(config)# track 5 interface ethernet 0/1 line-protocol
```

【检验方法】 使用 **show track** 命令，可以查看 track 对象的统计信息。

【提示信息】 1：配置 track 对象时，如果设备上资源不足，则提示错误。
Failed to create track obj, no resource.

2：使用 **no track** 删除指定 track 对象时，如果设备上没有配置该 track 对象，则提示错误。
the track object does not exist.

【常见错误】 1：配置了跟踪接口链路状态的 track，但未配置相应的接口。

【平台说明】 -

2.26 track list

配置 track 对象，跟踪一个 track 列表的状态。
track *object-number* **list boolean** { **and** | **or** }

删除 track 对象。
no track *object-number*

【参数说明】

参数	描述
object-number	track 对象的编号，取值范围为 1-700。

【缺省配置】 -

【命令模式】 全局模式

【缺省级别】 1

【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。

track *object-number* **list boolean and**：配置 track 对象用来跟踪 track 列表的状态，其结果为所有成员状态取“与”的结果；

track *object-number* **list boolean or：**配置 track 对象用来跟踪 track 列表的状态，其结果为所有成员状态取“或”的结果；

【配置举例】 配置一个 track 对象，其编号为 4，且用来跟踪一个 track 列表的状态，其结果是所有成员状态取“与”的结果。

```
Ruijie(config)# track 4 list boolean and
```

【检验方法】 使用 **show track** 命令，可以查看 track 对象的统计信息。

【提示信息】 1：配置 track 对象时，如果设备上资源不足，则提示错误。
Failed to create track obj, no resource.

2：使用 **no track** 删除指定 track 对象时，如果设备上没有配置该 track 对象，则提示错误。
the track object does not exist.

【常见错误】 1：配置了跟踪 track 列表状态的 track，但未配置相应的 track 列表成员。

【平台说明】 -

2.27 track rns

配置 track 对象，跟踪一个 rns 实例的探测结果。
track *object-number* **rns** *entry-number*

删除 track 对象。
no track *object-number*

【参数说明】

参数	描述
object-number	track 对象的编号，取值范围为 1-700。

entry-number	RNS 操作索引，取值范围为 1-500。

【缺省配置】 -

【命令模式】 全局模式

【缺省级别】 1

【使用指导】 使用该命令配置一个 track 对象 ,用来跟踪一个 rns 实例的探测结果。当 rns 实例的探测结果成功时 ,相应的 track 对象状态为 up。

【配置举例】 1：配置一个 track 对象，其编号为 5，且用来跟踪编号为 7 的 rns 实例。

```
Ruijie(config)# track 5 rns 7
```

【检验方法】 使用 **show track** 命令，可以查看 track 对象的统计信息。

【提示信息】 1：配置 track 对象时，如果设备上资源不足，则提示错误。
Failed to create track obj, no resource.

2：使用 **no track** 删除指定 track 对象时，如果设备上没有配置该 track 对象，则提示错误。
the track object does not exist.

【常见错误】 1：配置了跟踪 rns 的 track，但未配置相应的 rns 实例。

【平台说明】 -

命令参考-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. SYS
4. USER-TASK
5. SERVICE-MANAGER

1 DEV-AUDIT

1.1 dev-audit enable

开启设备审计功能。

dev-audit enable

关闭设备审计功能。

no dev-audit enable

【参数说明】

参数	描述
-	-

【缺省配置】 开启设备审计功能。

【命令模式】 全局配置模式

【缺省级别】 15

【使用指导】 设备审计的数据记录到设备本地数据库。

⚠ 如果记录的数据未保存在设备本地，则只发送日志，本地无法查看记录。

【配置举例】 1：开启设备审计功能。

```
Ruijie(config)# dev-audit enable
```

【检验方法】 1：使用 **show run** 命令，可以查看是启用还是关闭。

【提示信息】 无

【常见错误】 -

【平台说明】 -

1.2 show dev-audit

查看设备审计记录。

show dev-audit {**cpu** | **memory** | **flash** | **buffer** | **flow** | **interface** *interface-name*} **from** *year* [*month* [*mday* [*hh:mm:ss*]]] [**to** *year* [*month* [*mday* [*hh:mm:ss*]]]]

【参数说明】

参数	描述
cpu	cpu 使用率
memory	内存使用率
flash	flash 记录，包含了 flash、sata 硬盘或 U 盘空间使用情况
buffer	可用 buffer 数
flow	ipv4 连接数
interface *interface-name*	指定接口收发速率和 no buffer 数
from *year* [*month* [*mday* [*hh:mm:ss*]]]	指定显示信息的时间范围，从什么时候开始。
to *year* [*month* [*mday* [*hh:mm:ss*]]]	指定显示信息的时间范围，到什么时候为止。

【命令模式】 特权模式、全局模式、接口模式

【缺省级别】 15

【使用指导】 使用该命令可以查看设备审计的记录。

【配置举例】 1：查看 cpu 记录

```
Ruijie#show dev-audit cpu from 2013 9 2
Date & Time             CPU
2013-09-02 12:03:11     2%
2013-09-02 12:08:11     2%
2013-09-02 12:13:11     3%
2013-09-02 12:18:11     2%
2013-09-02 12:23:11     2%
2013-09-02 12:28:11     2%
```

字段解释：

字段	说明
Date & Time	记录时间
CPU	cpu 利用率

2：查看 flash 记录

```
Ruijie#show dev-audit flash from 2013 9 2 12:00:00
Date & Time         Flash-Total(KB)      Flash-Free (KB)    SATA-Total(MB) SATA-Free(MB)
2013-09-02 12:12:11         523776    454592    143372    140859
2013-09-02 13:11:11         523776    454592    143372    140858
2013-09-02 14:10:11         523776    454592    143372    140858
2013-09-02 15:09:11         523776    454592    143372    140857
```

字段解释：

字段	说明
Date & Time	记录时间
CPU	cpu 利用率
Flash-Total (KB)	flash 总空间
Flash-Free (KB)	flash 可用空间硬盘数据
SATA-Total(MB)	sata 硬盘总空间
SATA-Free(MB)	sata 硬盘可用空间
USB-Total(MB)	U 盘总空间
USB-Free(MB)	U 盘可用空间
Avail-Buff	可用 buffer 数
v4-Flow	当前 ipv4 流数量
Input-Rate	接口接收速率
Output-Rate	接口发送速率
No-Buffer	接口 no buffer 数

【提示信息】 1：如果数据未保存在设备本地数据库，则提示错误。

```
Data is not stored in the local !
```

【平台说明】 show dev-audit ｛ cpu | memory | flash ｝:网关全系列产品支持。NBR2500D-E、NBR3000D-E、NBR3000D-UE 出厂带 SATA 硬盘。NBR108G-P 、NBR800G、NBR950G、NBR1500G、NBR2000G、NBR1000G-C、NBR2000G-C、NBR3000G-S、NBR1000G-E、NBR6120-E、NBR1300G-E、NBR1700G-E、NBR2100G-E、NBR6205-E、NBR6135-E、NBR6210-E、NBR6215-E 出厂无 SATA 硬盘。其中 NBR6205-E、NBR6135-E、NBR6210-E、NBR6215-E 可自行购买 SATA 硬盘使用。

2 USB

2.1 show usb

查看已插入的 USB 设备信息。

show usb

【参数说明】

参数	描述
-	-

【命令模式】 特权模式

【缺省级别】 2

【使用指导】 如果有 USB 设备，则显示设备信息，否则无输出。如果 U 盘直接插在设备的 USB 端口，show usb 显示的 ID 格式为 X，其中 X 是数字，表示 USB 端口号；如果 U 盘接在 HUB 上，HUB 插在设备的 USB 端口，show usb 显示的 ID 格式为 X-Y，其中 X、Y 都是数字，X 表示设备 USB 端口号，Y 表示 HUB 的槽号。

【配置举例】 1：直接将 U 盘插在设备的 USB 端口上，下面是显示 USB 的信息：

```
Ruijie# show usb
Device: Mass Storage
ID: 0
URL prefix: usb0
Disk Partitions:
usb0(type:FAT32)
Size : 131,072,000B(125MB)
Available size： 1,260,020B(1.2MB)

Device: Mass Storage
ID: 1
URL prefix: usb1
Disk Partitions:
usb1(type:FAT32)
Size : 131,072,000B(125MB)
Available size： 1,260,020B(1.2MB)
```

字段解释：

字段	说明
ID	设备号。
URL prefix	表示该 U 盘的访问前缀。

Size	表示 U 盘上可访问的空间。
Available size	表示 U 盘上的剩余空间。

2：U 盘插在 HUB 端口上，HUB 插在设备的 USB 端口，下面是显示 USB 的信息：

```
Ruijie# show usb
Device: Mass Storage
ID: 0-3
URL prefix: usb0-3
Disk Partitions:
usb0-3(type:vfat)
Size:15789711360B(15789.7MB)
Available size:15789694976B(15789.6MB)

Device: Mass Storage
ID: 0-4
URL prefix: usb0-4
Disk Partitions:
usb0-4(type:vfat)
Size:15922782208B(15922.7MB)
Available size:14861926400B(14861.9MB)
```

字段解释：

字段	说明
ID	设备号。0 表示设备的 0 号 USB 端口 ,3、4 表示 HUB 的插槽号。
URL prefix	表示该 U 盘的访问前缀。
Size	表示 U 盘上可访问的空间。
Available size	表示 U 盘上的剩余空间。

【提示信息】 -

【平台说明】 -

2.2 usb remove

移除 USB 设备。

usb remove *device-id*

【参数说明】

参数	描述
device-id	设备号，它是 USB 显示信息中的 ID 号。该设备号可以通过 **show usb** 来获取。

【命令模式】 特权模式

【缺省级别】 2

【使用指导】 在拔出 USB 设备之前，需要用命令移除设备，以防系统正在使用设备而导致错误。如果设备移除成功，系统会打印出提示，这时方可拔出设备。如果移除失败，说明该时刻系统有使用该 USB 设备，则须等待一会再执行移除操作。

【配置举例】 1：下面为移除上面例子所示中的 USB 设备：

```
Ruijie# usb remove 0
OK, now you can pull out the device 0.
```

这时候就可以将 USB 设备拔出了。

【检验方法】 命令执行成功后，show usb 将看不到 usb 设备的相关信息。若命令执行失败，show usb 还可以看到 usb 设备的相关信息。

【提示信息】 1.执行了卸载命令后，如果执行成功，系统会打印出如下信息：

```
OK, now you can pull out the device 0
```

2.执行了卸载命令后，如果执行失败，系统会打印出如下信息：

```
Device is busy now, try again few minutes later.
```

【常见错误】 打印 Device is busy now, try again few minutes later. 说明设备正在被使用，请先关闭所有使用设备的操作。比方说之前 cd usb0:/ 操作后，没有退出，执行 usb remove 0 时就会提示失败，这时请执行 cd flash:/操作，将当前路径切换到 flash，然后再执行 usb remove 0。

【平台说明】 -

3 SYS

3.1 calendar set

设置系统硬件时间。

calendar set { *hour* [:*minute* [:*second*]] } [*month* [*day* [*year*]]]

【参数说明】

参数	描述
hour [:*minute* [:*second*]]	设置系统硬件时间，时：分：秒，只会重置指定的小时，分钟，秒，省略的部分使用系统当前的设置值。
month	设置月份，取值范围 1~12。
day	设置日期，取值范围 1~31，若当月不存在这一天，则日期会向后推算
year	设置年份，取值范围 1970~2069

【缺省配置】 -

【命令模式】 特权模式

【缺省级别】 -

【使用指导】

1. 时间参数必须要输入，然后按照月份 *month*，日期 *day*，年 *year* 参数的顺序，根据需要可省略后面的参数。被省略的参数，为系统当前的设置值。例如，当前硬件时间为“2012-02-29 09:33:44”，只改月份和小时，而其它保持不变，可输入命令 **calendar set** *12 5*，则当前时间变为“2012-05-29 12:33:44”。
2. 如果输入的 *day* 参数在 1~31 内，但该月不存在这一天，则日期会往后推算。例如，2012 年 2 月共 29 天，若设置了日期为 2 月 31 日，**calendar set** *11:30 2 31 2012*，则系统会默认往后加两天，当前硬件时间则为“2012-03-02 11:30:23”。

设置的系统硬件时间即充当 UTC 时间，而系统软件时间是指设备本地时间。

只有设备在 vsd0 下才具有该条命令，不支持多 vsd。

【配置举例】 1：将当前系统硬件时间（假设 2012-02-01 18:23:06），更改为 6 小时，其它参数不变。

```
Ruijie# calendar set 6
06:41:39 UTC Fri, Jul 6, 2012
```

2：将当前系统硬件时间（假设 2012-02-01 18:23:06），更改为 6 小时 42 分钟，其它参数不变。

```
Ruijie# calendar set 6:42
06:42:27 UTC Fri, Jul 6, 2012
```

3：将当前系统硬件时间（假设 2012-02-01 18:23:06），更改月份和日期为 3 月 2 日，其它参数不变。

```
Ruijie# calendar set 18 3 2
18:43:05 UTC Fri, Mar 2, 2012
```

⚠ 由于命令中 *hour* 参数是必选字段，如果该参数无需变更，输入与当前小时一致的时钟值即可，如上例所示：输入时钟值 18，再输入月份和日期“3 2”。

【检验方法】 -

【提示信息】 -

【常见错误】 -

【平台说明】 -

3.2 clock read-calendar

设置系统根据硬件时间同步软件时间。

clock read-calendar

【参数说明】

参数	描述
-	-

【缺省配置】 -

【命令模式】 特权模式

【缺省级别】 -

【使用指导】 只有设备在 vsd0 下才具有该条命令，不支持多 vsd。

通过该命令，系统会根据设备时区、夏令时的设置情况，将当前硬件系统时间生成相应的软件时间。

【配置举例】 1：配置系统根据硬件时间同步软件时间。

```
Ruijie# clock read-calendar
Set the system clock from the hardware time.
```

【检验方法】 -

【提示信息】 -

【常见错误】 -

【平台说明】 -

3.3 clock set

设置系统软件时间。

clock set { *hour* [:*minute* [:*second*]] } [*month* [*day* [*year*]]]

【参数说明】

参数	描述
hour [:*minute* [:*second*]]	设置系统软件时间，时：分：秒，只会重置指定的小时，分钟，秒，省略的部分使用系统当前的设置值。
month	设置月份，取值范围 1~12。
day	设置日期，取值范围 1~31，若当月不存在这一天，则日期会向后推算。
year	设置年份，取值范围 1970~2069。

【缺省配置】 -

【命令模式】 特权模式

【缺省级别】 -

【使用指导】

3. 时间参数必须要输入，然后按照月份 *month*，日期 *day*，年 *year* 参数的顺序，根据需要可省略后面的参数。被省略的参数，为系统当前的设置值。

例如，当前系统软件时间为“2012-02-29 09:33:44”，只改月份和小时，而其它保持不变，可输入命令 **clock set** *12 5*，则当前时间变为“2012-05-29 12:33:44”

4. 如果输入的 *day* 参数在 1~31 内，但该月不存在这一天，则日期会往后推算。

例如，2012 年 2 月共 29 天，若设置了日期为 2 月 31 日，**clock set** *11:30 2 31 2012*，则系统会默认往后加两天，当前系统软件时间则为“2012-03-02 11:30:23”。

只有设备在 vsd0 下才具有该条命令，不支持多 vsd。

【配置举例】

1：将当前系统软件时间（假设 2012-02-01 18:23:06），更改为 6 小时，其它参数不变。

```
Ruijie# clock set 6
06:48:13 CST Fri, Mar 2, 2012
```

2：将当前系统软件时间（假设 2012-02-01 18:23:06），更改为 6 小时 42 分钟，其它参数不变。

```
Ruijie# clock set 6:42
06:42:31 CST Fri, Mar 2, 2012
```

3：将当前系统软件时间（假设 2012-02-01 18:23:06），，更改月份和日期为 3 月 2 日，其它参数不变。

```
Ruijie# clock set 18 3 2
18:42:48 CST Fri, Mar 2, 2012
```

⚠ 由于命令中 *hour* 参数是必选字段，如果该参数无需变更，输入与当前小时一致的时钟值即可，如上例所示：输入时钟值 18，再输入月份和日期“3 2”。

【检验方法】 -

【提示信息】 -

【常见错误】 -

【平台说明】 -

3.4 clock summer-time

设置夏令时。

clock summer-time *zone* **start** *start-month* [*week*|**last**] *start-date hh:mm* **end** *end-month* [*week*| **last**] *end-date hh:mm* [**ahead** *hours-offset* [*minutes-offset*]

关闭夏令时。

no clock summer-time

【参数说明】

参数	描述
zone	夏令时的名称，只能为[A~Z][a~z]，大小写无限制。名字长度为 3~31。
start	夏令时生效的起始时间关键字
start-month	起始月份，取值范围：January、February、March、April、May、June、July、August、September、October、November、December。大小写不限制，也可不用输入完整单词，如：Febr、FebRu 等。
week	起始月份的起始星期数。取值范围 1~5。
last	指定为某月的最后个星期。
start-date	起始月份的起始星期的星期几，取值范围：Sunday、Monday、Tuesday、Wednesday、Thursday、Friday、Saturday。大小写不限制，也可不输入完整单词。比如：Wed、WeDne 等。
hh:mm	时间，小时、分钟。
end	夏令时生效的结束时间关键字
end-month	结束月份，取值范围：January、February、March、April、May、June、July、August、September、October、November、December。大小写不限制，也可不用输入完整单词，如：Febr、FebRu 等。
ahead	夏令时生效期间，夏令时时间比标准时间快多少时间的关键字。。若不设置，则默认为快 1 小时。
hours-offset	比标准时间提前的小时数。取值范围 0~12。不允许把夏令时提前的时间设置为 00:00。

minutes-offset	比标准时间提前的分钟数。取值范围 0~59。若 *hours-offset* 已经设置为 0，则不允许 *minutes-offset* 也设置 0

【缺省配置】 -

【命令模式】 配置模式

【缺省级别】 -

【使用指导】

只有设备在 vsd0 下才具有该条命令，不支持多 vsd。

【配置举例】 1：如果你居住在一个地方，时区名称为 ABC，标准时间比 UTC 时间快 8:15，即 GMT+08:15。夏令时时间段从 2 月的第一个星期六到 5 月的第三个星期 1，夏令时时段比标准时间提前 01:20。则夏令时时段的时间比 UTC 时间快 09:35，但非夏令时时段的时间仍为比 UTC 时间快 08:15。

```
Ruijie(config)# clock timezone ABC 8 15
Set time zone name: ABC (GMT+08:15)
Ruijie(config)#show clock
16:39:16 ABC Wed, Feb 29, 2012
Ruijie(config)#show calendar
08:24:35 GMT Wed, Feb 29, 2012

Ruijie(config)# clock summer-time TZA start Feb 1 sat 2:00 end May 3 Monday 18:30 ahead 1 20
*May 10 03:45:58: %SYS-5-CLOCKUPDATE: Set summer-time: TZA from February the 1st Saturday at 2:00
TO May the 3rd Monday at 18:30, ahead 1 hour 20 minute
Set summer-time: TZA from February the 1st Saturday at 2:00 TO May the 3rd Monday at 18:30, ahead
1 hour 20 minute

Ruijie# show clock
18:00:08 TZA Wed, Feb 29, 2012

# 如果将时间设置为非夏令时期间，时区名称又转换回 ABC
Ruijie#clo set 18 1 1
*Jan  1 18:00:09: %SYS-5-CLOCKUPDATE: Set system clock: 18:00:09 ABC Sun, Jan  1, 2012
Set system clock: 18:00:09 ABC Sun, Jan  1, 2012
Ruijie#show clock
18:00:12 ABC Sun, Jan  1, 2012
```

2：采用默认的夏令时时段时间比标准时间快 1 小时，可省略 ahead 及 ahead 后面的参数。例如，设置夏令时从 4 月的第一个星期日的凌晨 2:00 起，至 10 月的最后一个星期日的凌晨 2:00，比标准时间快 1 小时。

```
Ruijie(config)#clo summer-time PDT start April 1 sunday 2:00 end October last Sunday 2:00
```

```
*May 10 03:15:05: %SYS-5-CLOCKUPDATE: Set summer-time: PDT from April the 1st Sunday at 2:00 TO October the last Sunday at 2:00, ahead 1 hour
Set summer-time: PDT from April the 1st Sunday at 2:00 TO October the last Sunday at 2:00, ahead 1 hour
```

3：关闭夏令时。

```
Ruijie(config)#no clock summer-time
*Jan  1 18:01:09: %SYS-5-CLOCKUPDATE: Set no summer time.
Set no summer time.
```

【检验方法】 -

【提示信息】 -

【常见错误】 -

【平台说明】 -

3.5 clock timezone

设置时区。

clock timezone [*name hours-offset* [*minutes-offset*]]

关闭时区设置。

no clock timezone

【参数说明】

参数	描述
name	时区名称，只能为[A~Z][a~z]，大小写无限制。名字长度为 3~31。
hours-offset	时差的小时值。表示与硬件时间 UTC 时间快或慢 *hours-offset*，取值范围为 [-12, 12]，负数表示比硬件时间慢，正数表示比硬件时间快。 若比 UTC 时间慢，则 *hours-offset* 参数前要加“-”。
minutes-offset	时差的分钟值。取值范围为 0~59。

【缺省配置】 -

【命令模式】 配置模式

【缺省级别】 -

【使用指导】 只有设备在 vsd0 下才具有该条命令，不支持多 vsd。

【配置举例】 1：设置时区名称为 CST，软件时间比硬件时间快 8 小时整。

```
Ruijie(config)# clock timezone CST 8
Set time zone name: CST (GMT+08:00)

Ruijie# show clock
18:00:17 CST Wed, Dec 5, 2012
```

2：设置时区名称 TZA，软件时间比硬件时间慢 06:13。

```
Ruijie(config)# clock timezone TZA -6 13
Set time zone name: TZA (GMT-06:13)
```

3：关闭时区设置。

```
Ruijie(config)# no clock timezone
Set no clock timezone.
```

【检验方法】 -

【提示信息】 -

【常见错误】 -

【平台说明】 -

3.6 clock update-calendar

设置系统根据软件时间同步硬件时间。

clock update-calendar

【参数说明】

参数	描述
-	-

【缺省配置】 -

【命令模式】 特权模式

【缺省级别】 -

【使用指导】 只有设备在 vsd0 下才具有该条命令，不支持多 vsd。
通过该命令，系统会根据设备时区、夏令时的设置情况，将当前软件系统时间生成相应的硬件时间。

【配置举例】 1：设置系统根据软件时间同步硬件时间。

```
Ruijie# clock update-calendar
Set the hardware time from the system clock.
```

2：设置硬件时间，时区设置为 GMT+5:10，无夏令时设置，即硬件时间比软件时间慢 5:10。

```
Ruijie# show clock
09:30:21 TSZ Wed, Feb 29, 2012

Ruijie# clock update-calendar
Set the hardware time from the system clock.

Ruijie#show calendar
04:20:25 UTC Wed, Feb 29, 2012
```

3：设置硬件时间，若时间设置为 GMT+5:10，夏令时设置为从 2 月 1 日第 1 个星期一至 6 月 1 日第 2 个星期日，快 1 小时 15 分钟，即在夏令时期间，硬件时间比软件时间慢 6:25。

```
Ruijie# show clock
09:30:02 TSZ Wed, Feb 29, 2012

Ruijie# clock update-calendar
Set the hardware time from the system clock.

Ruijie#show calendar
03:05:08 UTC Wed, Feb 29, 2012
```

【检验方法】 -

【提示信息】 -

【常见错误】 -

【平台说明】 -

3.7 cpu high-watermark set

显示和设置控制核上总的 CPU 使用率的最高水线，并开启监控。
cpu high-watermark set [[**high** *high-value*] [**range** *range-value*]]

关闭 CPU 使用率监控。

no cpu high-watermark set

恢复缺省配置。

default cpu high-watermark set

【参数说明】

参数	描述
high *high-value*	设置 CPU 使用率的最高水线，取值范围 2~99。
range *range-value*	设置水线波动范围，取值范围 1~20。

【缺省配置】 CPU 水线的默认值 80%，波动范围为 5%（即 75%~85%）。

【命令模式】 配置模式

【缺省级别】 -

【使用指导】 只有设备在 vsd0 下才具有该条命令，不支持多 vsd。

通过设置 CPU 使用率最高水线，并开启监控。当系统监测到 CPU 使用率超出最高水线允许的波动范围，将会打印相应的提示信息。

【配置举例】 1：设置 CPU 水线为默认值，若监控关闭则开启。

```
Ruijie(config)# default cpu high-watermark set
Reset default cpu watermark monitor
set system cpu watermark high 80%(75%~85%)
```

2：关闭 CPU 水线监控。

```
Ruijie(config)# no cpu high-watermark set
Close cpu watermark monitor
```

3：开启监控，水线值保持关闭前已设置的值。

```
Ruijie(config)# cpu high-watermark set
Open cpu watermark monitor
set system cpu watermark high 80%(75%~85%)
```

4：开启监控，并设置最高水线值为 88%、波动范围为 3%。

```
Ruijie(config)# cpu high-watermark set high 88 range 3
Open cpu watermark monitor
set system cpu watermark high 88%(85%~91%)
```

此时，设置了高水线值为 88%，高水线上限值为 91%（88%+3%），下限值为 85%（88%-3%）。

【检验方法】 -

【提示信息】 如果 CPU 使用率最高水线的允许波动范围是 85%~91%，当 CPU 使用率超过最高水线上限值时，会打印如下的报警信息：

```
*Jan 19 16:23:01: %RG_SYSMON-4-CPU_WATERMARK_HIGH: warning! system cpu usage above high watermark(85%),current cpu usage 100%
```

当 CPU 使用率低于最高水线下限值时，会打印如下的解除报警信息：

```
*Jan 20 07:02:52:  %RG_SYSMON-5- CPU_WATERMARK:withdraw warning! system cpu usage below high watermark(85%), current cpu usage 36%
```

【常见错误】 -

【平台说明】 -

3.8 memory history clear

清除内存使用记录的历史条目。

memory history clear [**one-forth | half | all**]

【参数说明】

参数	描述
one-forth	清除四分之一的条目。
half	清除一半的条目。
all	清除全部的条目。

【缺省配置】 -

【命令模式】 全局模式

【缺省级别】 -

【使用指导】 -

【配置举例】 1：清除一半的内存使用记录的历史条目。

```
Ruijie# show memory history

Time Thu Jan  1 00:24:45 1970
Used(k) 148516
Maxinum memory users for this period
Process Name    Holding
tcpip.elf       270028
cli-memory      60600
rg_syslogd      36640
```

```
Time Thu Jan  1 00:24:41 1970
Used(k) 148492
Maxinum memory users for this period
Process Name    Holding
tcpip.elf       270028
cli-memory      52408
rg_syslogd      36640

Time Thu Jan  1 00:24:41 1970
Used(k) 148444
Maxinum memory users for this period
Process Name    Holding
tcpip.elf       270028
cli-memory      44088
rg_syslogd      36640

Ruijie(config)#memory history clear half
2 out of 5 records in the history table to be cleared...
Clear done !
```

【检验方法】 -

【提示信息】 -

【常见错误】 -

【平台说明】 -

3.9 memory low-watermark set

配置内存利用率水线，并开启监控。
memory low-watermark set *mem-rate*

关闭内存利用率检测功能。
no memory low-watermark set

恢复缺省配置。
default memory low-watermark set

【参数说明】

参数	描述

mem-rate	内存利用率水线，取值范围 1~100，单位为%。

【缺省配置】 缺省内存利用率水线为 90%。

【命令模式】 全局模式

【缺省级别】 -

【使用指导】 开启内存利用率检测功能，并设置内存利用率水线。

【配置举例】 1：配置内存利用率水线为 80%，并开启检测功能。

```
Ruijie(config)#memory low-watermark set 80
```

【检验方法】 -

【提示信息】

【常见错误】 -

【平台说明】 -

3.10 reload

重启设备。

reload [**at** { *hour* [:*minute* [:*second*]] } [*month* [*day* [*year*]]]]

【参数说明】

参数	描述
hour [:*minute* [:*second*]]	设置重启的时：分：秒，省略的部分使用系统当前的设置值
month	设置月份，取值范围 1~12。
day	设置日期，取值范围 1~31，若当月不存在这一天，则日期会向后推算
year	设置年份，取值范围 1970~2069

【缺省配置】 -

【命令模式】 特权模式

【缺省级别】 -

【使用指导】 -

【配置举例】 1：重启设置

```
Ruijie# reload
Reload system?(Y/N) Y
Sending all processes the TERM signal...                              [  OK  ]
Sending all processes the KILL signal...                              [  OK  ]
Restarting system...
```

【检验方法】 -

【提示信息】 -

【常见错误】 -

【平台说明】 -

3.11 show calendar

显示系统硬件时间。

show calendar

【参数说明】

参数	描述
-	-

【命令模式】 特权模式或全局模式

【缺省级别】 -

【使用指导】 -

【配置举例】 1：显示系统硬件时间。

```
Ruijie# show calendar
21:57:48 GMT Sun, Feb 28, 2012
```

【提示信息】 -

【平台说明】 -

3.12 show clock

显示系统软件时间。

show clock

【参数说明】

参数	描述
-	-

【命令模式】 特权模式或全局模式

【缺省级别】 -

【使用指导】 -

【配置举例】 1：当关闭时区设置时，显示系统软件时间。

```
Ruijie# show clock
18:22:20 UTC Tue, Dec 11, 2012
```

2：当开启时区设置，显示系统软件时间。

```
Ruijie# show clock
03:07:49 TSZ Wed, Feb 29, 2012
```

【提示信息】 -

【平台说明】 -

3.13 show cpu

显示系统任务在控制核和非虚拟核上的信息。

show cpu

【参数说明】

参数	描述
-	-

【命令模式】 特权模式或全局模式

【缺省级别】 -

【使用指导】 只有设备在 vsd0 下才具有该条命令，不支持多 vsd。
如果系统存在虚拟核，需要查看虚拟核的 cpu 利用率信息，参见 show processes cpu 的相关命令。

【配置举例】 1：显示系统任务在控制核和非虚拟核上的信息。

```
Ruijie#show cpu
================================================
CPU Using Rate Information
```

```
CPU utilization in five seconds:  4.80%
CPU utilization in one minute:  4.10%
CPU utilization in five minutes:  4.00%

 NO       5Sec     1Min     5Min Process
    1    0.00%    0.00%    0.00% init
    2    0.00%    0.00%    0.00% kthreadd
    3    0.00%    0.00%    0.00% ksoftirqd/0
    4    0.00%    0.00%    0.00% events/0
--More--
```

【提示信息】 -

【平台说明】 -

3.14 show memory

显示内存的相关信息。

show memory [**sorted total | history | low-watermark |** *process-id* **|** *process-name*]

【参数说明】

参数	描述
sorted total	根据内存使用量来排序
history	显示内存使用情况的历史记录
low-watermark	显示系统内存低水线值
process-id	显示 *process-id* 指定的特定任务的内存使用量
process-name	显示 *process-name* 指定的特定任务的内存使用量

【命令模式】 特权模式或全局模式

【缺省级别】 -

【使用指导】 **show memory history** 每执行一次，显示的条目就会多一个，最多显示 10 个，可以用 **memory history clear** 命令清除历史条目。

【配置举例】 1：显示当前各任务内存使用情况并按总量大小排序。

```
Ruijie# show memory sorted
System Memory: 508324K total, 481560K used, 26764K free, 31.5% used rate
Used detail:   149112K active, 247776K inactive, 30460K mapped, 50460K slab, 3752K others

PID     Text(K) Rss(K)  Data(K)         Stack(K) Total(K)        Process
807     1568    4584    264728          84       270028          tcpip.elf
```

```
854     40      1436    246076          84      248840          cli-filesystem
1237    52      1492    123260          84      126036          cli-memory
803     56      1104    74064           84      76920           ping.elf
727     84      1276    33812           84      36640           rg_syslogd
733     84      796     33536           84      36364           rg_syslogd
776     224     1416    16896           84      19800           lsmdemo
858     40      1324    16844           84      19612           rg-tty-admin
769     40      3600    11052           84      13812           skbdemo
--More--
```

该命令显示的一些关键字信息描述表：

关建字	说明
total	系统总的内存
used	已使用的内存
free	剩余内存
used rate	内存使用百分比
Active	活动的页
inactive	非活动的页
mapped	映射的内存
slab	Slab 消耗的内存
others	Used 中除了 active，inactive，mapped，slab 之外的内存量

当前各任务的显示信息描述表：

字段	说明
PID	进程号
Text	代码段大小
Rss	驻留内存大小
Data	数据段大小
Stack	栈大小
Total	总消耗内存
Process	任务名

【提示信息】 -

【平台说明】 -

3.15 show pci-bus

显示挂在 PCI 总线上的设备相关信息。

show pci-bus

【参数说明】

参数	描述
-	-

【命令模式】 特权模式或全局模式

【缺省级别】 -

【使用指导】 -

【配置举例】 1：显示挂在 PCI 总线上的设备相关信息。

```
Ruijie# show pci-bus
NO:0
Vendor ID              : 0x1131
Device ID              : 0x1561
Domain:bus:dev.func    : 0000:00:05.0
Status / Command       : 0x2100000
Class / Revision       : 0xc031030
Latency                : 0x0
first 64 bytes of configuration address space:
00: 31 11 61 15 00 00 10 02 30 10 03 0c 20 00 80 00
10: 00 00 00 f0 00 00 00 00 00 00 00 00 00 00 00 00
20: 00 00 00 00 00 00 00 00 00 00 00 00 31 11 61 15
30: 00 00 00 00 dc 00 00 00 00 00 00 00 29 01 01 2a

NO:1
Vendor ID              : 0x1131
Device ID              : 0x1562
Domain:bus:dev.func    : 0000:00:05.1
Status / Command       : 0x2100156
Class / Revision       : 0xc032030
Latency                : 0x30
First 64 bytes of configuration address space:
00: 31 11 62 15 56 01 10 02 30 20 03 0c 20 30 80 00
10: 00 10 00 f0 00 00 00 00 00 00 00 00 00 00 00 00
20: 00 00 00 00 00 00 00 00 00 00 00 00 31 11 62 15
30: 00 00 00 00 dc 00 00 00 00 00 00 00 29 01 02 10
```

【提示信息】 -

【平台说明】 -

3.16 show processes cpu

显示系统任务信息。

show processes cpu [**history** [**table**] | [**5sec | 1min | 5min | 15min**] [**nonzero**] [**record**]]

【参数说明】

参数	描述
**5sec	1min	5min	15min**	按最近 5 秒钟，1 分钟，5 分钟，15 分钟时间段内 CPU 利用率的降序排列的任务信息列表
nonzero	不显示 CPU 利用率为零的任务的信息
history	以直方图的形式 ,分别显示在过去 60 秒、60 分钟、72 小时的时间段内，系统控制核上的 cpu 利用率
table	以表格的形式，分别显示在过去 60 秒、60 分钟、72 小时的时间段内，系统控制核上的 cpu 利用率
record	显示最近一周控制核上 5 分钟内的 cpu 利用率超过 cpu 使用率最高水线时的 CPU 利用率信息（分别显示控制核 5 分钟内的 cpu 利用率和 5 分钟内的 cpu 利用率 top5 的任务信息）

【命令模式】 特权模式或全局模式

【缺省级别】 -

【使用指导】 只有设备在 vsd0 下才具有该条命令，不支持多 vsd。

【配置举例】 1：按系统所有任务的 ID 号升序排列的任务信息

```
Ruijie# show processes cpu
System Uptime: 19:08.6
CPU utilization for five seconds:1.2%; one minute:0.8%; five minutes:0.8%
set system cpu watermark (open): high 80%(85%~75%)

Tasks Statistics: 375 total, 10 running, 365 sleeping, 0 stopped, 0 zombie
  Pid Vsd S   PRI  P       5Sec       1Min       5Min      15Min Process
    1   0 S    20  0   0.0(0.0)   0.0(0.0)   0.0(0.0)   0.0(0.0) init
    2   0 S    20  1   0.0(0.0)   0.0(0.0)   0.0(0.0)   0.0(0.0) kthreadd
    3   0 S  -100  0   0.0(0.0)   0.0(0.0)   0.0(0.0)   0.0(0.0) migration/0
    4   0 S    20  0   0.0(0.0)   0.0(0.0)   0.0(0.0)   0.0(0.0) ksoftirqd/0
    5   0 S  -100  1   0.0(0.0)   0.0(0.0)   0.0(0.0)   0.0(0.0) migration/1

 --More--
```

2：按系统所有任务的 ID 号升序排列，且不显示 15 分钟内 CPU 利用率为 0 的任务的信息。

```
Ruijie# show processes cpu nonzero
```

该命令显示开头显示的信息描述表：

字段	说明
System Uptime	设备总的运行时间，精确到秒
CPU Utilization	最近 5 秒钟，1 分钟，5 分钟控制核总的 CPU 利用率
Virtual CPU usage	虚拟核上，最近 5 秒钟，1 分钟，5 分钟控制核总的 CPU 利用率
Tasks Statistics	任务统计信息，统计总任务数和任务状态
set system cpu watermark	控制核总的 cpu 水线设置值及状态

系统中的任务运行状态有如下几种：

任务运行状态计	说明
running	正在运行的任务
sleeping	挂起的任务
stopped	暂停的任务
zombie	终止且未被系统回收的任务

显示的各任务的信息描述表：

字段	说明
Pid	任务 ID 号
Vsd	所属的 vsd 号
S	任务状态，共 5 种，R(running)，T(stopped)，S(sleeping)，D(waiting)，Z(zombie)
PRI	任务运行优先级
P	任务运行在 cpu 的哪个核上
5sec/1min/5min/15min	任务过去 5 秒钟，1 分钟，5 分钟，15 分钟内的 CPU 使用率。圆括号里的值是未除以当前该任务所在核的总核数的 cpu 利用率。
Process	任务名称 最多只显示前 15 个字符，超过的字符会被截断

3：按任务的 ID 号升序排列，并且只显示 15 分钟内 CPU 利用率为非零的线程信息.

```
Ruijie #show processes cpu nonzero
```

4：按在 5 秒钟内 CPU 利用率的降序排列，并且不显示 1sec 内 CPU 利用率为零的任务信息。

```
Ruijie #show processes cpu 5sec nonzero
```

5：以直方图的方式显示系统的控制核 cpu 利用率，在过去的 60 秒钟，60 分钟、72 小时内使用情况信息。
其中，第一个图表为 300 秒内，系统的控制核 cpu 利用率情况，横坐标每一小格为 5 秒，纵坐标每格为 5%，
“*” 表示最近某秒时 cpu 利用率的值 ,即横坐标最靠近 0 的第一个标格为最近 5 秒的 cpu 利用率值 ,单位为%。
第二个图表，为最近 60 分钟内，系统的控制核 cpu 利用率值，单位为%，横坐标每一小格为 1 分钟。
第三个图表，为最近 72 小时内，系统的控制核 cpu 利用率值，单位为%，横坐标每一小格为 1 小时。
示例如下：

```
Ruijie#show processes cpu history
```

```
            system cpu percent usage(%) [last 300 second]

    -
  100|
   95|
   90|
   85|
   80|
   75|
   70|
   65|
   60|
   55|
   50|
   45|
   40|*********
   35|||||||||||
   30|||||||||||*
   25|||||||||||
   20|||||||||||
   15|||||||||||
   10|||||||||||
    5|||||||||||***************
    0|||||||||||||||||||||||||||
     #=========#=========#=====*==>
     0          50         100       second
         system cpu percent usage(%) per 5second (last 125 second)
--------------------------------------------------------------------------------


            system cpu percent usage(%) [last 60 minute]

    -
  100|
   95|
   90|
   85|
   80|
   75|
   70|
   65|
   60|
```

```
  55|
  50|
  45|
  40|
  35|
  30|*
  25||
  20||
  15||
  10||
   5||*
   0|||
    #==*==>
    0     minute
        system cpu percent usage(%) per 1minute (last 2 minute)
--------------------------------------------------------------------------------
```

6：以表格的方式显示系统 cpu（0 核）在过去的 60 秒钟，60 分钟、72 小时内使用情况信息。
其中，第一个大表格为 300 秒内，系统的 cpu 利用率情况，第一个格子为最近的 5 秒的 cpu 利用率的值，单位为%，每个小格子间隔 5 秒。
第二个大表格，为最近 60 分钟的 cpu 利用率值，单位为%，每个小格子间隔 1 分钟。
第三个大表格，为最近 72 小时的 cpu 利用率值，单位为%，每个小格子间隔 1 小时。
示例如下

```
Ruijie #show processes cpu history table
              system cpu percent usage(%) [last 300 second]
#-------------------------------------------------------------------------------#
|         |     1|     2|     3|     4|     5|     6|     7|     8|     9|    10|
#-------------------------------------------------------------------------------#
#-------------------------------------------------------------------------------#
|       0|   2.0|   2.4|   2.3|   2.3|   2.8|   3.0|   2.7|   3.2|   2.6|   2.4|
#-------------------------------------------------------------------------------#
|       1|   2.7|   2.5|   2.7|   2.2|   2.4|   2.6|   2.2|   2.7|   2.3|   2.5|
#-------------------------------------------------------------------------------#
|       2|   2.9|   2.0|   2.4|   2.5|   2.7|   2.4|   2.4|   2.6|   2.6|   2.5|
#-------------------------------------------------------------------------------#
|       3|   2.7|   2.8|   2.8|   3.2|   2.5|   3.2|   3.1|   4.0|   2.7|   2.7|
#-------------------------------------------------------------------------------#
|       4|   4.0|   2.3|   2.1|   2.2|   2.7|   2.4|   2.5|   2.6|   2.4|   2.6|
#-------------------------------------------------------------------------------#
|       5|   2.4|   3.2|   2.5|   2.3|   2.3|   3.6|   2.8|   2.5|   2.2|   2.4|
#-------------------------------------------------------------------------------#
```

```
              system cpu percent usage(%) [last 60 minute]
#-------------------------------------------------------------------------------#
|         |     1|     2|     3|     4|     5|     6|     7|     8|     9|    10|
#-------------------------------------------------------------------------------#
#-------------------------------------------------------------------------------#
|       0|   2.6|   2.5|   3.0|   2.4|   2.6|
#-------------------------------------------------------------------------------#
```

7：按一周内时间的前后顺序进行排序，显示过去一周 5 分钟内控制核上 cpu 利用率超过 CPU 使用率最高水线时 CPU 利用率信息（5 分钟内控制核上 cpu 利用率和 5 分钟内 CPU 利用率 TOP5 的任务信息）。CPU 使用率最高水线设置参考 cpu high-watermark set 命令。

```
Ruijie#show processes cpu record
CPU watermark high up 9%, down 6%

 1970-01-07 01:20:13     system(11.0%)   ssa_process(9.1%)  ssd_process(0.6%)  ssc_process(0.3%)
ham(0.3%)  rl-con/0(0.2%)
 1970-01-07 01:25:26     system(10.8%)   ssa_process(9.1%)  ssd_process(0.6%)  ham(0.3%)
ssc_process(0.3%)  lsm.elf(0.2%)
 1970-01-07 01:30:39     system(10.5%)   ssa_process(9.0%)  ssd_process(0.6%)  ssc_process(0.3%)
ham(0.3%)  rg-sysmon(0.2%)
 1970-01-07 01:35:52     system(10.5%)   ssa_process(9.0%)  ssd_process(0.6%)  ham(0.3%)
ssc_process(0.3%)  rg-sysmon(0.2%)
 1970-01-07 01:41:05     system(10.7%)   ssa_process(9.1%)  ssd_process(0.6%)  ssc_process(0.3%)
ham(0.3%)  lsm.elf(0.2%)
 1970-01-07 01:46:18     system(10.7%)   ssa_process(9.1%)  ssd_process(0.6%)  ham(0.3%)
ssc_process(0.3%)  rg-sysmon(0.2%)
 1970-01-07 01:51:31     system(10.8%)   ssa_process(9.1%)  ssd_process(0.6%)  rg-sysmon(0.3%)
ssc_process(0.3%)  ham(0.3%)
 1970-01-07 01:56:45     system(10.9%)   ssa_process(9.1%)  ssd_process(0.6%)  ham(0.3%)
ssc_process(0.3%)  rg-sysmon(0.3%)
 1970-01-07 02:01:58     system(11.0%)   ssa_process(9.1%)  ssd_process(0.7%)  rg-sysmon(0.4%)
ssc_process(0.3%)  ham(0.3%)
 1970-01-07 02:07:11     system(11.0%)   ssa_process(9.1%)  ssd_process(0.7%)  rg-sysmon(0.4%)
ham(0.3%)  ssc_process(0.3%)
 1970-01-07 02:12:24     system(11.0%)   ssa_process(9.1%)  ssd_process(0.7%)  rg-sysmon(0.4%)
ssc_process(0.3%)  ham(0.3%)
 1970-01-07 02:17:37     system(11.0%)   ssa_process(9.0%)  ssd_process(0.6%)  rg-sysmon(0.4%)
ham(0.3%)  ssc_process(0.3%)
```

【提示信息】 -

【平台说明】 -

3.17 show processes cpu detailed

显示指定任务的详细信息。

show processes cpu detailed { *process-id* | process-*name* }

【参数说明】

参数	描述
process-id	查看指定任务 ID 号的任务信息。
process-name	查看指定任务名的任务信息。

【命令模式】 特权模式或全局模式

【缺省级别】 -

【使用指导】 只有设备在 vsd0 下才具有该条命令，不支持多 vsd。

【配置举例】 1：查看指定任务名的任务信息。

```
Ruijie# show processes cpu detailed demo
Process Id    : 1820
Process Name  : demo
Vsdid         : 0
Process Ppid  : 1

State         : R(running)
On CPU        : 0
Priority      : 20
Age Time      : 24:06.5
Run Time      : 00:01.0
Cpu Usage     :
    Lass  5 sec    0.3%(0.6%)
    Lass  1 min    0.3%(0.6%)
    Lass  5 min    0.3%(0.6%)
    Lass 15 min    0.3%(0.6%)
Tty           : ?
```

Code Usage ：209.6KB.若指定的任务名不唯一，则如下所示：

```
Ruijie# show processes cpu detailed demo
duplicate process, choose one by id not name.
name: demo, id: 1089, state: S(sleeping)
```

```
name: demo, id: 1091, state: R(running)
process name: monitor_procps, do NOT exist, or NOT only one.
```

显示信息描述表：

字段	说明
Process Id	任务 ID 号
Vsdid	任务所属的 vsd 号
Process Name	任务名称
Process Ppid	父进程任务的 ID 号
State	任务运行状态
On CPU	任务所运行的 CPU
Priority	任务优先级
Age Time	任务自启动到现在持续的时间
Run Time	任务自启动到现在被调度执行的时间
Cpu Usage	任务在过去 5 秒钟，1 分钟，5 分钟，15 分钟时间段内的 CPU 使用率。圆括号里的值是未除以当前该任务所在核的总核数的 cpu 利用率。如 ,demo 任务当前在 0 核上，0 核是控制核，系统总共有两个控制核，则显示 0.3%（0.6%）。
Tty	Tty 号。“主设备号，次设备号”，如果 0 为“?”
Code Usage	任务代码段占用的大小

2：查看指定任务 ID 的任务信息。

```
Ruijie# show process cpu detailed 1715
```

【提示信息】 -

【平台说明】 -

3.18 show usb-bus

显示挂在 USB 总线上的设备相关信息。

show usb-bus

【参数说明】

参数	描述
-	-

【命令模式】 特权模式或全局模式

【缺省级别】 -

【使用指导】 -

【配置举例】 1：显示挂在 USB 总线上的设备相关信息。

```
Ruijie# show usb-bus
Device: Linux Foundation 2.0 root hub
  Bus 001 Device 001: ID 1d6b:0002
```

【提示信息】 -

【平台说明】 -

3.19 show version

显示系统版本信息

show version

【参数说明】

参数	描述
-	-

【命令模式】 特权模式或全局模式

【缺省级别】 -

【使用指导】 -

【配置举例】 1：显示系统版本信息。

```
Ruijie# show version
System description      : Ruijie Indoor AP320-I (802.11a/n and 802.11b/g/n) By Ruijie Networks
System start time       : 2012-12-06 00:00:00
System uptime           : 0:03:20:07
System hardware version : 1.0.0
System software version : AP_RGOS11.0(1B1)
System serial number    : 1234942570018
System boot version     : 1.0.0
```

【提示信息】 -

【平台说明】 -

4 USER-TASK

4.1 clear user-task

清除用户任务日志。

clear user-task

【参数说明】

参数	描述
-	-

【命令模式】 特权模式

【缺省级别】 15

【使用指导】 此命令用来清除用户任务的任务日志。

【配置举例】 1：清除用户任务日志。

```
Ruijie# clear user-task
```

【提示信息】 无

【平台说明】 -

4.2 show user-task

查看用户任务信息。

show user-task [**log**]

【参数说明】

参数	描述
log	查看用户任务日志。

【命令模式】 特权模式、全局配置模式

【缺省级别】 15

【使用指导】 使用该命令可以查看用户任务列表以及用户任务日志。

【配置举例】 1：查看所有用户任务列表

```
Ruijie#sh user-task
User-task: enable
User-task log: enable
Time              Name              Mode    Loop Command-sequence
2014-09-22 15:00 删除静态绑定      config --    ip dhcp pool my_pool
                                               no host
```

字段解释：

字段	说明
Time	任务时间
Name	任务名
Mode	命令模式
Loop	是否循环任务，循环时间
Command-sequence	待执行 CLI 命令序列

2：查看用户任务日志

【提示信息】

```
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
```

【平台说明】 -

4.3 user-task

添加用户任务

user-task add *task-name* **command** *cli-string* **mode** { **exec** | **config** } [**date** *YYYY MM DD*] **time** *hh:mm* [**every** { *mmm* | *hhh:mm* }]

删除用户任务

user-task delete *task-name*

修改用户任务

user-task modify *task-name* { **mode** { **exec** | **config** } | **date** *YYYY MM DD* | **time** *hh:mm* | **every** { *mmm* | *hhh:mm* } }

【参数说明】

参数	描述
task-name	任务名，最长不能超过 16 字节。
command *cli-string*	待执行 CLI 命令序列，序列总长不能超过 512 字节。 ⚠ 命令中间有空格的情况下，命令前后要用双引号包括 ⚠ 子命令之间使用“@”符号间隔 ℹ 支持命令缩写，例如”sh ip int br” ℹ 命令中带有”@”字符时，使用”\@”代替
mode { **exec**	**config** }	命令模式，exec 为特权模式，config 为全局配置模式。
date *YYYY MM DD*	任务执行年月日，如未指定日期则默认为当日。 ℹ 若未配置任务日期并且任务时间比当前时间早，则任务日期默认为次日
time *hh:mm*	任务执行时间，从 00:00 到 23:59。 ❗ 注意：若配置的日期+时间小于当前的日期+时间，则配置的命令会立即执行，包括 reload 命令！
every { *mmm*	*hhh:mm* }	任务循环时间，支持 1 分钟-168 小时（即 1 分钟-1 周）。配置了任务循环时间后，任务会根据循环时间重复执行。若不配置则不循环。 ℹ 时间格式为：1-3 位分钟数即 1 分钟-999 分钟，或者是 1-3 位小时数加上 1-2 位分钟数即 0:1（0 小时 1 分钟）-167:59（167 小时 59 分钟），注意中间有冒号

【命令模式】 特权模式

该命令是在特权模式下执行，需要注意

【缺省级别】 15

【使用指导】 该命令用于添加、删除与修改用户任务，添加成功后任务将存在于任务库中，系统将根据任务执行时间来定时执行所配置的任务。删除与修改任务需要指定任务名。修改任务时如果需要修改多项属性必须进行多次修改配置，一次修改一个属性。

【配置举例】 1：添加用户任务，在 2014 年 9 月 2 日下午 4 点 30 分重启设备。

```
Ruijie# user-task add reload-task command “reload@y” mode exec date 2014 9 2 time 16:30
```

2：删除一条名为 test 的任务。

```
Ruijie# user-task delete test
```

2：将一条名为 aa 的非循环任务修改为每天中午 12 点执行。

```
Ruijie# user-task modify aa every 24
Ruijie# user-task modify aa time 12:00
```

【提示信息】 1：输入的任务名过长，则配置失败

```
USER-TASK: Task name len 22 is more than 16 bytes!
```

2：输入的命令过长，则配置失败

```
USER-TASK: Command len 567 is more than 512 bytes!
```

3：输入的任务名已存在，则添加任务失败

```
USER-TASK: Task name exists!
```

4：输入的任务名不存在，则删除/修改任务失败

```
USER-TASK: No such task named test!
```

5：修改任务时间/日期时，如果输入的总时间日期小于当前时间日期则修改失败。

```
USER-TASK: New time is less than current time!
```

6：如果数据库异常将导致配置失败。

```
USER-TASK: Unexpected database error!
```

7：如果任务数超过 1000 则新增任务失败。

```
USER-TASK: Too more tasks!(Not support more than %d tasks)
```

【常见错误】 1：command 参数没加引号，导致配置失败

【平台说明】 -

4.4 user-task enable

启动用户任务功能
user-task enable

关闭用户任务功能
no user-task enable

【参数说明】

参数	描述
-	-

【缺省配置】 开启用户任务功能

【命令模式】 全局配置模式

【缺省级别】 15

【使用指导】 开启用户任务功能后才可以执行任务库中的自定义命令。

⚠ 若设备重启/用户任务被关闭等原因导致任务没有及时执行，任务库中有任务时间早于当前时间的任务的情况，则在功能开启后第一次执行任务会将所有已超时的任务全部执行一遍，如果是循环任务则按照任务计划时间与循环间隔进行下一次的任务时间的计算。

【配置举例】 1：开启用户任务功能

```
Ruijie(config)# user-task enable
```

【检验方法】 1：使用 **show user-task** 命令，可以查看用户任务开启还是关闭。
2：使用 **show run** 命令，可以查看用户任务开启还是关闭。

【提示信息】 无

【常见错误】 -

【平台说明】 -

4.5 user-task log

启动用户任务日志功能
user-task log enable

关闭用户任务日志功能
no user-task log enable

【参数说明】

参数	描述
-	-

【缺省配置】 关闭任务日志功能

【命令模式】 全局配置模式

【缺省级别】 15

【使用指导】 待配置执行的任务若包括 show 命令等需要关注任务执行结果，则必须开启任务日志功能，用于记录任务执行结果。

⚠ 设备最多保存 30 天的日志

⚠ 设备日志最多保存 20MB

【配置举例】 1：开启用户任务日志功能

```
Ruijie(config)# user-task log enable
```

【检验方法】 1：使用 **show user-task** 命令，可以查看用户任务开启还是关闭。
2：使用 **show run** 命令，可以查看用户任务开启还是关闭。

【提示信息】 无

【常见错误】 -

【平台说明】 -

5 SERVICE-MANAGER

5.1 servctl service

设置服务状态。

servctl service *name* { **on** | **off** }

恢复服务默认状态。

no servctl service *name*

【参数说明】

参数	描述
name	指定服务名称。
on	设置服务状态为运行。
off	设置服务状态为停止。

【命令模式】 全局配置模式

【缺省级别】 14

【使用指导】 此命令用来设置设备上服务的运行状态，同步控制相关业务模块是否启机加载、WEB 对应的页面是否显示。

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。

【配置举例】 1：启动服务 was 的功能，允许启机自动运行。

```
Ruijie(config)#servctl service was on
```

【提示信息】 1：根据服务加卸载执行状态，给出提示。部分业务要求重启设备才能生效。

```
You must reload the system to enable service was.
```

【平台说明】 网关系列产品

5.2 show servctl

查看支持服务管理控制的服务，以及服务状态。

show servctl { **all | service** *name* }

【参数说明】

参数	描述

all	显示所有服务的状态。
service *name*	显示指定服务的状态。

【命令模式】 特权模式、全局模式

【缺省级别】 14

【使用指导】 使用该命令可以查看设备上支持服务管理控制的服务，以及服务状态。

【配置举例】 1：查看服务 was 的状态

```
Ruijie#show servctl service was
service             controllable startup   running
------------------- ------------ --------- ---------
was                 true         true      true
```

字段解释：

字段	说明
service	服务名称
controllable	服务是否允许控制加卸载
startup	服务当前是否设置为启机运行
running	服务当前是否在运行

【提示信息】 1：如果服务名称不存在，则只显示标题。

```
Ruijie#show servctl service foo
service             controllable startup   running
------------------- ------------ --------- ---------
```

【平台说明】 网关系列产品

命令参考-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
8. UPNP-PROXY

1 RLOG

1.1 ip nat-log on

启用只记录本地 NAT 日志
ip nat-log on

关闭 SSM。
no ip nat-log on

【参数说明】

参数	描述
-	-

【缺省配置】 关闭只记录本地 NAT 日志。

【命令模式】 配置模式

【缺省级别】 14

【使用指导】 开启该命令，则只记录 NAT 日志。关闭后，则记录所有流日志。

【配置举例】 1：启动只记录本地 NAT 日志。

```
Ruijie(config)# ip nat-log on
```

【检验方法】 1：使用 **show nat-log status** 命令，可以查看该功能打开情况。

【提示信息】 -

【常见错误】 -

【平台说明】 -

1.2 nat-log data-store

设置本地日志存储的天数
nat-log data-store *days*

恢复默认配置。
no nat-log data-store

【参数说明】

参数	描述
days	日志存储天数，取值范围：10~90

【缺省配置】 默认保存 30 天

【命令模式】 配置模式

【缺省级别】 14

【使用指导】 根据磁盘容量和查询需求，可适当调整日志存储的天数

【配置举例】 1：启动本地日志记录。

```
Ruijie(config)# nat-log data-store 60
```

【检验方法】 1：使用 **show run** 命令，查看当前配置的的天数。默认为 30 天。

【提示信息】 -

【常见错误】 -

【平台说明】 -

1.3 nat-log enable

启动本地日志功能
nat-log enable

关闭 nat log。
no nat-log enable

【参数说明】

参数	描述
-	-

【缺省配置】 关闭 nat-log 功能

【命令模式】 配置模式

【缺省级别】 14

【使用指导】 如果要在本地记录流日志，则需要执行本命令。

【配置举例】 1：启动本地日志记录。

```
Ruijie(config)# nat-log enable
```

【检验方法】 1：使用 **show nat-log status** 命令，可以查看 NAT_LOG 打开情况。

【提示信息】 -

【常见错误】 -

【平台说明】 -

1.4 rlog dev-ip

设置 RLOG 本地 IP

rlog dev-ip *ip*

取消设置 RLOG 本地 IP。

no rlog dev-ip

【参数说明】

参数	描述
ip	指定的 RLOG 本地 IP

【缺省配置】 -

【命令模式】 配置模式

【缺省级别】 14

【使用指导】 部分日志中需要本地 IP 字段，因此设备需要根据本地对外 IP，设置该值。

⚠ 该值主要传给日志服务器使用，未配置可能导致服务器解析出信息有误。

【配置举例】 1：配置本地 IP 为 10.10.10.2。

```
Ruijie(config)# rlog dev-ip 10.10.10.2
```

【检验方法】 1：使用 **show rlog** 命令，可以查看 dev-ip 的取值。

【提示信息】 -

【常见错误】 -

【平台说明】 -

1.5 rlog export-rate

配置 RLOG 发送速率
rlog export-rate *val*

取消发送速率配置
no rlog export-rate

【参数说明】

参数	描述
val	每秒发送日志数，取值范围为 10-100000

【缺省配置】 每秒发送 1000 条日志。

【命令模式】 配置模式

【缺省级别】 14

【使用指导】 发送速率要根据设备性能和设备产生日志数量来决定。

⚠ 配置太大，容易使得设备 CPU 偏高，太小，则容易使得日志丢失。

【配置举例】 1：配置 RLOG 日志发送速率为 10000 每秒。

```
rlog export-rate 10000
```

【检验方法】 1：使用 **show rlog** 命令，可以查看当前 RLOG 日志发送速率。

【提示信息】

```
-
```

【常见错误】 -

【平台说明】 -

1.6 rlog filter

设置流日志、本地日志的过滤条件
rlog filter *aclid*

取消设置流日志、本地日志的过滤条件
no rlog filter

【参数说明】

参数	描述
aclid	指定的过滤 ACL 条件，取值范围：2000-2699

【缺省配置】 -

【命令模式】 配置模式

【缺省级别】 14

【使用指导】 该配置同时对流日志和本地日志生效，在流日志量过大或者不需要记录全部的流日志时，使用该配置。

该配置需要有预先配置对应的 acl。

【配置举例】 1：配置按照 ACL 2000 的条件来过滤流日志。

```
Ruijie(config)# access-list 2000 permit udp any any
Ruijie(config)# rlog filter 2000
```

【检验方法】 1：使用 **show run** 命令，可以查看命令是否配置。

【提示信息】 -

【常见错误】 未配置对应的 ACL
配置的 ACL ID 超出指定范围

【平台说明】 -

1.7 rlog server

配置 RLOG 服务器
rlog server *ip-address* [**oob**] [**port** *port-num*]

关闭 RLOG 服务器。
no rlog server *ip-address*

【参数说明】

参数	描述
Ip-address	服务器 ip
port-num	服务器端口
oob	oob 接口

【缺省配置】 -

【命令模式】 配置模式

【缺省级别】 14

【使用指导】 要将日志发往服务器，首先要配置一个服务器的 ip，端口等信息。

【配置举例】 1：配置一台服务器，地址为 10.10.10.10，端口为 20000。

```
Ruijie(config)# rlog server 10.10.10.10 port 20000
```

【检验方法】 1：使用 **show rlog** 命令，可以查看服务器是否已生效。

【提示信息】 -

【常见错误】 -

【平台说明】 NBR6205-E、NBR6135-E、NBR6210-E、NBR6215-E 支持 MGMT 口；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 MGMT 口。

1.8 rlog set

设置 RLOG 可合并多条日志到一个报文
rlog set log-com

关闭日志合并的功能。
no rlog set log-com

【参数说明】

参数	描述
-	-

【缺省配置】 -

【命令模式】 配置模式

【缺省级别】 14

【使用指导】 开启该命令，可以一定程度上提高日志发送效率，但是需要日志服务器支持。

⚠ 如果日志服务器不支持多条日志合并在同一个报文中的功能，则可能导致日志丢失或无法解析。

【配置举例】 -

【检验方法】 1：使用 **show rlog** 命令，可以查看该设置是否开启。

【提示信息】 -

【常见错误】 -

【平台说明】 -

1.9 rlog sn-mac-on

设置流日志中包含 sn 和 mac 信息
rlog sn-mac-on

取消设置流日志中包含 sn 和 mac 信息
no rlog sn-mac-on

【参数说明】

参数	描述

【缺省配置】 未开启

【命令模式】 配置模式

【缺省级别】 14

【使用指导】 该配置开启时，发给日志服务器的流日志将带有 sn 和 mac 信息，服务器要能够解析该信息。

⚠ 该配置需要有预先确认服务器是否兼容。

【配置举例】 1：打开流日志带 sn 和 mac 信息开关。

```
Ruijie(config)# rlog sn-mac-on
```

【检验方法】 1：使用 **show run** 命令，可以查看命令是否配置。

【提示信息】 -

【常见错误】 -

【平台说明】 -

1.10 rlog type

配置指定类型的日志发送或生成文件
rlog type *n* **server** *server-ip* **priority** *prio*
rlog type *n* **file**

取消指定的日志发送
no rlog type *n* **server** *server-ip*
no rlog type *n* **file**

【参数说明】

参数	描述
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

【缺省配置】 -

【命令模式】 配置全局模式

【缺省级别】 14

【使用指导】 该配置是发送日志的必须配置，每个需要发送的日志都必须配置一条此命令。如果日志要使用文件方式发送，则需要配合 rlog-file 使用。

【配置举例】 1：配置流日志发送到服务器 10.10.10.10。

```
Ruijie(config)# rlog type 16 server 10.10.10.10 priority 1
```

【检验方法】 1：使用 **show rlog-status** 命令，当前服务器开了哪些日志。

【提示信息】 1：如果指定的 RLOG 服务器不存在，则报错，配置不生效。

【平台说明】 -

1.11 rlog-file local-path

设置 RLOG 本地文件存储目录
rlog-file local-path *path-string*

取消设置 RLOG 本地文件存储目录。

no rlog-file local-path

【参数说明】

参数	描述
path-string	指定的 RLOG 文件本地存储目录

【缺省配置】 实时方式默认路径为：/tmp/rlog-file，定时方式默认路径为/mnt/sata0/rlog-file

【命令模式】 配置模式

【缺省级别】 14

【使用指导】 文件实时发送方式和定时发送方式对日志的存储要求不一样，如果是定时发送，需要较大的日志存储空间，应该存储在硬盘中。

⚠ 如果定时发送方式选择了 tmp 目录保存文件，可能把内存耗光，导致系统异常。

【配置举例】 1：配置本地存储目录为硬盘目录。

```
Ruijie(config)# rlog-file local-path /mnt/sata0/rlog-file
```

【检验方法】 1：使用 **show rlog-file** 命令，可以查看取值。

【提示信息】 -

【常见错误】 -

【平台说明】 NBR2500D-E、NBR3000D-E、NBR3000D-UE 出厂带 SATA 硬盘。NBR108G-P 、NBR800G、NBR950G、NBR1500G、NBR2000G、NBR1000G-C、NBR2000G-C、NBR3000G-S、NBR1000G-E、NBR6120-E、NBR1300G-E、NBR1700G-E、NBR2100G-E、NBR6205-E、NBR6135-E、NBR6210-E、NBR6215-E 出厂无 SATA 硬盘。其中 NBR6205-E、NBR6135-E、NBR6210-E、NBR6215-E 可自行购买 SATA 硬盘使用。

1.12 rlog-file send

设置 RLOG 文件上传参数

rlog-file send time-range from *from-hour* **to** *to-hour*

rlog-file send compress { zip | none }

rlog-file send format {elog | macc }

取消设置 RLOG 文件上传参数。

no rlog-file send time-range

no rlog-file send compress
no rlog-file send format

【参数说明】

参数	描述
from-hour	指定文件定时上传的开始时间，为 24 小时制的小时
to-hour	指定文件定时上传的结束时间，为24小时制的小时，可以比from-hour小，表示跨天

【缺省配置】 实时上传，ftp 方式，zip 压缩，**key-val** 格式

【命令模式】 配置模式

【缺省级别】 14

【使用指导】 使用文件方式上传日志，需要配置日志上传的参数。

⚠ 该值需要和日志服务器约定好，未配置可能导致日志无法正常上传。

【配置举例】 1：配置定时发送日志，从 22 点到凌晨 6 点。

```
Ruijie(config)# rlog-file send time-range from 22 to 6
2：配置上传压缩方式为 zip
Ruijie(config)# rlog-file send compress zip
3：配置文件日志格式为 json 格式
Ruijie(config)# rlog-file send format elog
```

【检验方法】 1：使用 **show rlog-file** 命令，可以查看取值。

【提示信息】 -

【常见错误】 -

【平台说明】 -

1.13 rlog-file server

设置 RLOG 文件服务器信息
rlog-file server *protocal ip-address* [**port** *port-num*] [**oob**] [**path** *server-path-string*] [**username** *username-string* **passwd** *passwd-string*]

取消设置 RLOG 文件服务器。
no rlog-file server

【参数说明】

参数	描述
protocal	协议，FTP 或 HTTP
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
oob	指定 oob 参数，当前仅 HTTP 方式有效
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”

【缺省配置】 -

【命令模式】 配置模式

【缺省级别】 14

【使用指导】 当需要配置文件方式上传时，需要配置一个文件服务器。
目前只支持一个文件服务器，多次配置将覆盖已配置的内容。

【配置举例】 1：配置一个 FTP 服务器。

```
Ruijie(config)# rlog-file server 10.10.10.2 path rlog/ username test passwd test
```

【检验方法】 1：使用 **show rlog-file** 命令，可以服务器信息是否一致。

【提示信息】 -

【常见错误】 -

【平台说明】 NBR6205-E、NBR6135-E、NBR6210-E、NBR6215-E 支持 MGMT 口；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 MGMT 口。

1.14 rlog-file storage

设置 RLOG 本地文件存储大小限制
rlog-file storage *storage-size*

恢复设置 RLOG 本地文件存储大小默认限制。
no rlog-file storage

【参数说明】

参数	描述
storage-size	指定的 RLOG 文件本地存储大小，单位 K

【缺省配置】 实时发送目录默认为 64M，定时发送目录默认为 1G。

【命令模式】 配置模式

【缺省级别】 14

【使用指导】 根据设备实际需要调整最大存储空间，设置该值。

⚠ 配置值要根据设备实际存储空间的大小而定。

【配置举例】 1：配置本地存储大小为 2G。

```
Ruijie(config)# rlog-file storage 2097152
```

【检验方法】 1：使用 **show rlog** 命令，可以查看取值。

【提示信息】 -

【常见错误】 -

【平台说明】

1.15 rlog-file type

设置 RLOG 文件上传的日志类型

rlog-file type *type-num*

取消设置 RLOG 文件上传参数。

no rlog-file type *type-num*

【参数说明】

参数	描述
type-num	日志类型

【缺省配置】 -

【命令模式】 配置模式

【缺省级别】 14

【使用指导】 需要开启日志文件上传时，设置该值。

⚠ 未开启该命令，日志不会上传。

【配置举例】 1：配置以文件方式发送 URL 审计日志。

```
Ruijie(config)# rlog-file type 20
```

【检验方法】 1：使用 **show rlog** 命令，可以查看取值。

【提示信息】 -

【常见错误】 -

【平台说明】

1.16 show nat-log

查看本地日志信息

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*

【参数说明】

参数	描述
user_name	用户名
ip-protocol	协议号
source-ip	源 ip
dst-ip	目的 ip
src-port	源端口，取值范围：0-65535
dst-port	目的端口，取值范围：0-65535
begin-year	开始时间年，取值范围：1993-2035
begin-mon	开始时间月，取值范围：1-12
begin-day	开始时间日，取值范围：1-31
begin-hour	开始时间小时，取值范围：0-23
end-year	结束时间年，，取值范围：1993-2035
end-mon	结束时间月，取值范围：1-12
end-day	结束时间日，取值范围：1-31
end-hour	结束时间小时，取值范围：0-23

【命令模式】 特权模式

【缺省级别】 14

【使用指导】 该命令用于查询一段时间内记录的流/NAT 日志,，可以根据用户名，协议号，源 ip，目的 ip，源端口，目的端口过滤。

【配置举例】 1：下面的示例查看 2010 年 10 月 6 号 3 点到 5 点的日志记录

```
Ruijie#show nat-log time-interval 2010 10 6 3 t 2010 10 6 5
count:427
Pr  SrcAddr                         DstAddr                         UserName
SrcPort      DstPort      Vrf        SendBytes  RecvBytes  time
17  192.168.122.62 (0.0.0.0)        192.168.122.255(0.0.0.0)        192.168.122.62
138  (0)     138  (0)     0          2028       0          2010-10-6 3:1
17  192.168.100.55 (0.0.0.0)        192.168.100.255(0.0.0.0)        192.168.100.55
138  (0)     138  (0)     0          732        0          2010-10-6 3:1
17  192.168.122.54 (0.0.0.0)        192.168.122.255(0.0.0.0)        192.168.122.54
137  (0)     137  (0)     0          864        0          2010-10-6 3:1
138  (0)     138  (0)     0          714        0          2010-10-6 3:3
```

字段解释：

字段	说明
Pr	协议
SrcAddr	源地址
DstAddr	目的地址
UserName	用户名
SrcPort	源端口
DstPort	目的端口
Vrf	VRF 名称
RecvBytes	接收字节数
time	流时间

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。

【提示信息】 -

【平台说明】 -

1.17 show rlog

查看 RLOG 配置信息

show rlog

【参数说明】

参数	描述
-	-

【命令模式】 特权模式

【缺省级别】 14

【使用指导】 使用该命令可以查看 RLOG 的服务器，本地设备 IP，发送速率，以发送日志统计，日志合并功能等。

【配置举例】 1：查看 RLOG 配置信息

```
Ruijie#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 1000 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
```

字段解释：

字段	说明
rlog server is enable	配置了服务器，以下 N 行为具体的服务器端口和 IP
rlog dev-ip	设备本地 IP
rlog export-rate	日志发送速率
rlog queue remain	日志缓存剩余节点数
send log count	已发送的日志个数
error count	发送失败的日志个数
errorno	最后一次发送失败的错误码
recv buf	RLOG 接收到的日志个数
poll buf err	日志缓存空间不足的次数
local buf	本地日志输出个数
recv err cnt	接收消息发生错误的次数
depatch err cnt	接收到的没有对应服务器的消息，或者该消息的服务器以失效
enable log combination	是否进行日志合并发送

【提示信息】 如果未配置任何服务器，则该命令不显示任何东西。

【平台说明】 -

1.18 show rlog-file

查看 RLOG 文件方式的配置信息

show rlog-file

【参数说明】

参数	描述
-	-

【命令模式】 特权模式

【缺省级别】 14

【使用指导】 使用该命令可以查看 RLOG 文件的服务器信息，日志存储路径，日志目录大小现在，日志发送类型和发送参数等等。

【配置举例】 1：查看 RLOG 配置信息

```
Ruijie#show rlog-file
rlog file server ftp:
     ip:10.10.10.2, port:21 oob
     path: rlog/
     username:ftp  passwd:ftp
local path: /tmp/rlog-file
local storage: 65536 K
send time-rage: from 22 to 6
send compress: zip; format: json
total proc files: 99
client count: 2
log          total  tar|err  send|err  lasterr
LOG          100    100|0    100|0     0
MAIL_BODY    100    100|0    100|0     0
MAIL_ATTACH  100    100|0    100|0     0
WEBMAIL      100    100|0    100|0     0
BSS_BODY      100    100|0    100|0     0

send log type:
RLOG_FILE_TYPE_URL_AUDIT  20
```

字段解释：

字段	说明
ip	服务器 IP
port	服务器端口
oob	通过管理口发送

path	服务器上传目录
username	服务器用户名
passwd	服务器密码
local path	本地存储路径
local storage	本地存储大小上限
send time-rage	定时发送时间范围
send protocal	日志发送协议
total proc files	已处理日志文件数
client count	客户端个数
tar file error	打包文件错误次数和最后一次错误代码
put file error	上传文件错误次数和最后一次错误代码
send log type	发送日志类型

网关产品不支持 oob，配置举例仅作为配置参考，实际请以具体设备配置为准。

【提示信息】 -

【平台说明】 NBR6205-E、NBR6135-E、NBR6210-E、NBR6215-E 支持 MGMT 口；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 MGMT 口。

1.19 show rlog-status

查看 RLOG 服务器状态

show rlog-status { [**server** *ip*] | [**client**] | [**log**] }

【参数说明】

参数	描述
Ip	指定具体服务器的 IP

【命令模式】 特权模式

【缺省级别】 14

【使用指导】 使用该命令可以查看 RLOG 服务器状态。

【配置举例】 1：查看所有 RLOG 服务器信息

```
Ruijie#show rlog-status
============================================================
server:192.168.1.100      port:20000
type                            prio
```

```
=======================================================
server:10.10.10.10       port:20000
type                              prio
RLOG_TYPE_FLOW        16          1
```

字段解释：

字段	说明
server	服务器地址
port	服务器端口
type	服务器开通的日志类型
prio	服务器开通的日志优先级

2：查看连接到 RLOG 功能模块个数

```
Ruijie#show rlog-status client
rlog client count: 0
```

字段解释：

字段	说明
rlog client count	接到 RLOG 功能模块个数

3：查看 RLOG 已接收的日志个数

```
Ruijie#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
```

字段解释：

字段	说明
local rlog message	接到 RLOG 本地日志个数信息
remote rlog message	接收到的 RLOG 远程日志个数信息，按日志类型区分

【提示信息】 1：如果设备上没有配置任何服务器，则该命令不显示任何东西。

【平台说明】 -

1.20 show rlog-type

查看 RLOG 有哪些日志类型

show rlog-type

【参数说明】

参数	描述
-	-

【命令模式】 特权模式

【缺省级别】 14

【使用指导】 使用该命令可以查看 RLOG 有哪些日志类型。

【配置举例】 1：查看 RLOG 日志类型

```
Ruijie#show rlog-type
RLOG_TYPE_FLOW                16
RLOG_TYPE_CPU_MEM             17
RLOG_TYPE_DISC                18
RLOG_TYPE_DEV_LOG             19
RLOG_TYPE_URL_AUDIT           20
RLOG_TYPE_SESSION             21
RLOG_TYPE_IP_APP              22
RLOG_TYPE_IP                  23
RLOG_TYPE_CHANNEL             24
```

```
RLOG_TYPE_INTERFACE          25
RLOG_TYPE_IP_OFFLINE         26
RLOG_TYPE_MAIL_AUDIT         27
RLOG_TYPE_TELNET_AUDIT       28
RLOG_TYPE_WEB_SEARCH_AUDIT   29
RLOG_TYPE_WEB_BBS_AUDIT      30
RLOG_TYPE_IM_AUDIT           31
RLOG_TYPE_FTP_AUDIT          32
RLOG_TYPE_WEB_AUDIT          33
RLOG_TYPE_APP_AUDIT          34
RLOG_TYPE_FLOOD              35
RLOG_TYPE_FLOOD_CEASEm       36
RLOG_TYPE_SCAN               37
RLOG_TYPE_SCAN_CEASE         38
RLOG_TYPE_ATTACK_FRAG        39
```

字段解释：

字段	说明
-	格式为日志类型名称，日志类型取值

【提示信息】 1：如果设备上没有配置任何服务器，则该命令不显示任何东西。

【平台说明】 -

2 POLICE-LOG

2.1 content-audit write-plog

开启内容审计第三方日志

[no] content-audit write-plog {*im* | *mail* | *url* | *vid* | *web-bbs* | *web-mail* | *web-search***}**

关闭内容审计第三方日志

[no] 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】 缺省为关闭状态。

【命令模式】 全局模式

【缺省级别】 15

【使用指导】 该命令用户开启内容审计日志发送第三方日志模块

【配置举例】 1：开启内容审计日志发送第三方日志模块

```
Ruijie(config)#content-audit write-plog ?
  im          Im audit information
  mail        Mail audit information
  url         Url audit information
  vid         Vid audit information
  web-bbs     Web-bbs audit information
  web-mail    Web-mail audit information
  web-search  Web-search audit information

Ruijie(config)#content-audit write-plog
```

【检验方法】 使用 **show content-audit plog config** 命令可以查看配置状态。

【提示信息】 -

【常见错误】 -

【平台说明】 -

2.2 debug police-log

开启指定日志级别的调试日志。

debug police-log {*auth* | *common* | *mail* | *nat* | *setdev* | *url* | *vid* | *webbbs* | *websearch***}**

默认日志级别

no debug police-log {*auth* | *common* | *mail* | *nat* | *setdev* | *url* | *vid* | *webbbs* | *websearch***}**

或者

undebug police-log {*auth* | *common* | *mail* | *nat* | *setdev* | *url* | *vid* | *webbbs* | *websearch***}**

【参数说明】

参数	描述
-auth	开启认证日志 debug 信息
-common	开启 5 种内容审计日志 debug 信息
-getdev	开启场所信息获取 debug 信息
-mail	开启 mail 日志 debug 信息
-nat	开启 nat 日志 debug 信息
-setdev	开启获取心跳 debug 信息
-url	开启 http 日志 debug 信息
-vid	开启虚拟身份日志 debug 信息
-webbbs	开启论坛日志 debug 信息
-websearch	开启搜索日志 debug 信息

【缺省配置】 无

【命令模式】 特权模式

【缺省级别】 15

【使用指导】 该命令为调试开关，用于排除故障，比如 MACC 显示设备离线，此时可开启日志，查看第三方日志模块与 MACC 的交互详细信息。

⚠ 该模块的调试日志是使用 rg_syslog 模块输出，需要开启 log on 和 log console 命令

【配置举例】 1：开启调试日志

```
Ruijie#debug police-log ?
  auth       Open auth police log debug
  common     Open all common police log debug
  getdev     Open get dev status debug
  mail       Open mail police log debug
  nat        Open nat police log debug
  setdev     Open set dev status debug
  url        Open url police log debug
  vid        Open vid police log debug
  webbbs     Open webbbs police log debug
  websearch  Open websearch police log debug
```

2：关闭调试日志

```
Ruijie#no debug police-log ?
  auth       Open auth police log debug
  common     Open all common police log debug
  getdev     Open get dev status debug
  mail       Open mail police log debug
  nat        Open nat police log debug
  setdev     Open set dev status debug
  url        Open url police log debug
  vid        Open vid police log debug
  webbbs     Open webbbs police log debug
  websearch  Open websearch police log debug
```

【调试信息】 1：向 MACC 请求场所信息

调试信息	https://192.168.23.206/specification/service/dc/getDevConf post data:{"device_sn":"1234842571023", "device_mac":"00-D0-F8-22-35-35", "device_type":0}
信息解释	本设备向 MACC 请求场所信息
产生原因	设备开机，以及间隔更新场所信息触发
处理建议	-无

2：MACC 心跳请求

调试信息	https://192.168.23.206/specification/service/ds/setDevStatus post data:{"netbar_wacode":"35011110341520","collection_equipment_id":"75496176400D0F8223535", "device_status":"00"} {"code":0,"msg":"ok"}
信息解释	本设备向 MACC 发送心跳请求包，MACC 放回心跳成功

产生原因	与 MACC 的定时间隔心跳
处理建议	-无

3、向 MACC 上报日志文件

调试信息	https://120.35.11.138:4433/specification/service/fileUpload?collection_equipment_id=754961764FFFFFFFFFFF&line_count=31 /tmp/log//145-010000-1456709687-00000-WA_SOURCE_FJ_0001-0.xml {"code":"0","msg":"ok"}
信息解释	发送日志文件到 MACC，MACC 返回接收成功
产生原因	设备上场所的日志需要上传給 MACC
处理建议	无

【检验方法】 使用 show debuging 命令可以查看配置状态。

【提示信息】 -

【常见错误】 -

【平台说明】 -

2.3 nat-log police

开启 NAT 流日志审计

nat-log police

关闭 NAT 流日志审计

no nat-log police

【参数说明】

参数	描述
-	-

【缺省配置】 缺省为关闭状态。

【命令模式】 全局模式

【缺省级别】 15

【使用指导】 该命令用户开启 NAT 流日志的监听

【配置举例】 1：开启第三方日志模块

```
Ruijie# configure
```

```
Ruijie(config)# nat-log police
Ruijie(config)# exit
Ruijie# wr
```

【检验方法】 使用 show nat-log status 命令可以查看配置状态。

【提示信息】 -

【常见错误】 -

【平台说明】 -

2.4 police-log enable

开启 police-log

police-log enable

关闭 police-log

no police-log enable

【参数说明】

参数	描述
-	-

【缺省配置】 缺省为关闭状态。

【命令模式】 全局模式

【缺省级别】 15

【使用指导】 该命令用户开启第三方日志模块程序，与 MACC 对接，发送相应的日志

【配置举例】 1：开启第三方日志模块

```
Ruijie# configure
Ruijie(config)# police-log enable
Ruijie(config)# exit
Ruijie# wr
```

【检验方法】 使用 show police-log config 命令可以查看配置状态。

【提示信息】 -

【常见错误】 -

【平台说明】 -

2.5 police-log file-sender compress

开启 police-log 压缩日志功能
police-log file-sender compress

关闭 police-log 压缩日志功能
no police-log file-sender compress

【参数说明】

参数	描述
-	-

【缺省配置】 缺省为关闭状态。

【命令模式】 全局模式

【缺省级别】 15

【使用指导】 该命令用于对发送 MACC/ELOG 的日志进行压缩或者非压缩

【配置举例】 1：开启第三方日志压缩功能

```
Ruijie#config
Enter configuration commands, one per line.  End with CNTL/Z.
Ruijie(config)#police-log file-sender compress
Ruijie(config)#
Ruijie# wr
```

【检验方法】 使用 **show police-log config** 命令可以查看配置状态。

【提示信息】 -

【常见错误】 -

【平台说明】 -

2.6 police-log set url

设置 MACC/ELOG 对接地址

police-log set url *url* **source** [**interface** *interface-name* | *addr*]

清除 MACC/ELOG 对接地址

no police-log set url

【参数说明】

参数	描述
url	MACC/ELOG 完整的 URL 访问主页，注意 MACC/ELOG 是否在一个服务器的子目录中。
interface-name	本地接口名称
addr	本地 IP 地址

【缺省配置】 缺省情况下，地址为空及没有指定第三方日志模块使用的本地(源)接口

【命令模式】 全局模式

【缺省级别】 15

【使用指导】 该命令是用来配置 MACC/ELOG 服务器的 url，请注意，是完整的 MACC/ELOG 服务主机地址，有些主机上会部署多套的 WEB 服务

【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
```

【检验方法】 使用 show police-log config 命令可以查看配置状态。

【提示信息】 -

【常见错误】 -

【平台说明】 -

2.7 police-log set platform

设置 police-log 对接平台

police-log set platform { elog | { *platform-type* [**name** *plat-name*] } }

清除 police-log 对接配置

no police-log set platform { elog | { *platform-type* [**name** *plat-name*] } }

子命令：

[no] { **data-gather | send-para** } *key-string value*

【参数说明】

参数	描述
platform-type	第三方日志类型。通过如下命令获取： **show plog platform** 如 surfilter：表示对接任子行
plat-name	第三方日志平台名称
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】 如果没有配置该命令，则缺省为 elog

【命令模式】 全局模式

【缺省级别】 15

【使用指导】 该命令设置对接平台。

【配置举例】 1：配置对接平台为 elog

```
Ruijie# configure
Ruijie(config)# police-log set platform elog
Ruijie(config)# end
Ruijie# wr
```

2：配置对接平台为任子行

```
Ruijie# configure
Ruijie(config)# police-log set platform surfilter name renzixing
Ruijie(config)# end
Ruijie# wr
```

【检验方法】 使用 **show plog config platform** 命令可以查看配置状态。

【提示信息】 -

【常见错误】 -

【平台说明】 EG、NBR 系列（除 CS 系列）系列产品均支持，MSC、NBR-C/S、AG、ACE 产品不支持

2.8 police-log-ap

设置 AP 设备信息
police-log-ap *index*

删除 AP 设备信息
no police-log-ap *index*

子命令：

[no] set service-code *code-value* **platform** *name*

[no] set *key-string value*

【参数说明】

参数	描述
index	AP 设备索引
code-value	AP 设备所属的场所编号
keystring	场所参数名，通过 **show plog para-list ap { platform** *plat-name* | **netsite** *id* }获取参数
value	参数值

【缺省配置】 缺省为关闭状态。

【命令模式】 全局模式

【缺省级别】 15

【使用指导】 该命令设置场所资料

【配置举例】 1：配置 AP 设备信息

```
Ruijie# configure
Ruijie(config)# police-log-ap 1
Ruijie(config-plog-netsite)# set service-code 12345678901234 platform surfilter
Ruijie(config-plog-netsite)# set ap-mac 00d0.00f8.1122
Ruijie(config-plog-netsite)# end
Ruijie# wr
```

【检验方法】 使用命令 **show plog config ap [** *ap-id* **| netsite** *netsite-id* **| platform** *plat-name* **]**可以查看配置状态。

【提示信息】 -

【常见错误】 -

【平台说明】 EG、NBR 系列（除 CS 系列）系列产品均支持，MSC、NBR-C/S、AG、ACE 产品不支持

2.9 police-log-netsite

设置第三方日志场所资料
police-log-netsite *index*

清除第三方日志 场所资料
no police-log-netsite

子命令：

[no] set platform *plat-name*
[no] **set** *key-string value*

【参数说明】

参数	描述
index	场所索引
palt-name	场所所属的第三方日志平台
keystring	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】 缺省为关闭状态。

【命令模式】 全局模式

【缺省级别】 15

【使用指导】 该命令设置场所资料

【配置举例】 1：配置场所名称

```
Ruijie# configure
```

```
Ruijie(config)# police-log-netsite 1
Ruijie(config-plog-netsite)# set platform renzixing
Ruijie(config-plog-netsite)# set service-code 12345678901234
Ruijie(config-plog-netsite)#
Ruijie# wr
```

【检验方法】 使用 **show plog config netsite [** *netsite-id* **| platform** *plat-name* **]**命令可以查看配置状态。

【提示信息】 -

【常见错误】 -

【平台说明】 EG、NBR 系列（除 CS 系列）系列产品均支持，MSC、NBR-C/S、AG、ACE 产品不支持

2.10 show plog config ap

显示已配置的 AP 设备信息

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】

参数	描述
ap-id	配置的 ap 索引
netsite-id	配置的场所索引
plat-name	配置的第三方日志平台名称
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】 查看所有配置的 AP 信息：

```
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" }] }

字段解释：（不同第三方日志对应的参数不一样，这里罗列常见的）

字段	说明
platform-name	第三方日志平台名称
platform-type	第三方日志平台类型
service-code	上网服务场所的编号
mac	ap 的 mac 地址
aptype	ap 的类型，如移动 AP、固定 AP，这里为对应的代码
apfloor	ap 所在的楼层
create-time	创建日期

【提示信息】 -

【平台说明】 EG、NBR 系列（除 CS 系列）系列产品均支持，MSC、NBR-C/S、AG、ACE 产品不支持

2.11 show plog config data-gather

显示已配置第三方日志的数据采集参数

show plog config data-gather platform *plat-name*

【参数说明】

参数	描述
plat-name	配置的第三方日志平台名称

【命令模式】 特权模式、全局模式

【使用指导】

【配置举例】 查看指定第三方日志平台的数据采集参数：

```
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" } ] }
```

字段解释：（不同第三方日志对应的参数不一样，这里罗列常见的）

字段	说明
security-org-code	厂商组织机构代码（9 位数字）
collection-type	数据采集系统类型，通常为 145
source-wacode	数据产生源标识，为地方区号
destination-wacode	数据传输目的标识，为地区区号
org-name	厂商名称

【提示信息】 -

【平台说明】 EG、NBR 系列（除 CS 系列）系列产品均支持，MSC、NBR-C/S、AG、ACE 产品不支持

2.12 show plog config netsite

显示已配置场所信息

show plog config netsite [*netsite-id* **| platform** *plat-name* **]**

【参数说明】

参数	描述
netsite-id	场所索引
plat-name	配置的第三方日志平台名称

【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】 查看指定场所的配置信息

```
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" } ] }
```

字段解释：（不同第三方日志对应的参数不一样，这里罗列几个参数说明）

字段	说明
service-code	上网服务场所编码（14 位）
service-type	上网服务场所类型，如网吧等，这里填写的是第三方日志提供的代码

【提示信息】 -

【平台说明】 EG、NBR 系列（除 CS 系列）系列产品均支持，MSC、NBR-C/S、AG、ACE 产品不支持

2.13 show plog config platform

显示已配置场所信息

show plog config platform

【参数说明】

参数	描述
-	-

【命令模式】 特权模式、全局模式

【使用指导】

【配置举例】 查看已经配置的第三方日志列表

```
Ruijie#sh plog config platform
{"code": 0, "msg": "", "list": [{"platform-type": "surfilter", "platform-name": "surfilter"}]}
```

字段解释：（不同第三方日志对应的参数不一样，这里罗列几个参数说明）

字段	说明
Platform-type	第三方日志平台类型
Platform-name	第三方日志平台名称

【提示信息】 -

【平台说明】 EG、NBR 系列（除 CS 系列）系列产品均支持，MSC、NBR-C/S、AG、ACE 产品不支持

2.14 show plog config send-para

显示已配置第三方日志的发送参数

show plog config send-para platform *plat-name*

【参数说明】

参数	描述
plat-name	配置的第三方日志平台名称

【命令模式】 特权模式、全局模式

【使用指导】

【配置举例】 查看指定第三方日志平台的发送参数：

```
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"}]}
```

字段解释：（不同第三方日志对应的参数不一样，这里罗列常见的）

字段	说明
server	服务器地址

【提示信息】 -

【平台说明】 EG、NBR 系列（除 CS 系列）系列产品均支持，MSC、NBR-C/S、AG、ACE 产品不支持

2.15 show plog para-list ap

显示 AP 配置的参数列表

show plog para-list ap { platform *plat-name* **| netsite** *id* **}**

【参数说明】

参数	描述
plat-name	配置的第三方日志平台名称
id	场所的索引

【命令模式】 特权模式、全局模式

【使用指导】

【配置举例】 查看指定第三方日志平台 AP 可配置参数：（非固定，不同第三方日志可能不一样）

```
Ruijie#sh plog para-list ap platform surfilter
{ "code": 0, "msg": 6, "list": [ { "key": "service-code", "description": "上网服务场所编号",
"required":"0", "help_string":"(14 位数字)(*)", "value_size":"0", "index":"0" }, { "key":"mac",
"description": "MAC 地址", "required": "0", "help_string": "(例：AA-BB-CC-DD-EE-FF)(*)",
"value_size": "0", "index": "1" }, { "key": "apname", "description": "AP 名称", "required": "0",
"help_string": "(*)", "value_size": "0", "index": "2" }, { "key": "aptype", "description": "AP 类
型", "required": "0", "help_string": "(0-固定 AP、1-移动 AP、10-固定围栏、11-移动围栏、12-单兵设备
围栏、20-H 系列、22-RT 系列)(*)", "value_size":"0","index":"3"},{"key":"apfloor","description":
"AP 所在楼层", "required": "0", "help_string": "(*)", "value_size": "0", "index": "4" }, { "key":
"create-time","description":"AP 创建时间","required":"0","help_string":"(例：2018-01-10)(*)",
"value_size": "0", "index": "5" } ] }
```

字段解释：（不同第三方日志对应的参数不一样）

字段	说明
key-string	参数名，配置命令用
required	是否必填，1 表示必填，0 表示非必填
description	参数中文描述
help-string	参数的帮助信息，为空表示不限制

【提示信息】 -

【平台说明】 EG、NBR 系列（除 CS 系列）系列产品均支持，MSC、NBR-C/S、AG、ACE 产品不支持

2.16 show plog para-list data-gather

显示第三方日志数据采集可配置的参数

show plog para-list data-gather *plat-name*

【参数说明】

参数	描述
plat-name	配置的第三方日志平台名称

【命令模式】 特权模式、全局模式

【使用指导】

【配置举例】 查看指定第三方日志平台的数据采集可配置参数列表（非固定，不同第三方日志可能不一样）

```
Ruijie#sh plog para-list data-gather surfilter
{ "code": 0, "msg": 5, "list": [ { "key": "org-name", "description": "厂商名称", "required": "0", "help_string": "", "value_size": "0", "index": "0" }, { "key": "security-org-code", "description": "厂商组织机构代码", "required": "0", "help_string": "", "value_size": "0", "index": "1" }, { "key": "collection-type", "description": "数据采集系统类型", "required": "0", "help_string": "", "value_size": "0", "index": "2" }, { "key": "source-wacode", "description": "数据产生源标识", "required": "0", "help_string": "", "value_size": "0", "index": "3" }, { "key": "destination-wacode", "description": "数据传输目的标识", "required": "0", "help_string": "", "value_size": "0", "index": "4" } ] }
```

字段解释：（不同第三方日志对应的参数不一样）

字段	说明
key-string	参数名，配置命令用
required	是否必填，1 表示必填，0 表示非必填
description	参数中文描述
help-string	参数的帮助信息，为空表示不限制

【提示信息】 -

【平台说明】 EG、NBR 系列（除 CS 系列）系列产品均支持，MSC、NBR-C/S、AG、ACE 产品不支持

2.17 show plog para-list netsite

显示第三方日志数据采集可配置的参数

show plog para-list netsite *palt-name*

【参数说明】

参数	描述
plat-name	配置的第三方日志平台名称

【命令模式】 特权模式、全局模式

【使用指导】

【配置举例】 查看指定第三方日志平台的场所信息可配置参数列表（非固定，不同第三方日志可能不一样）

```
Ruijie#sh plog para-list netsite surfilter
{ "code": 0, "msg": 23, "list": [ { "key": "service-code", "description": "上网服务场所编号",
"required": "0", "help_string": "(14 位数字)(*)", "value_size": "0", "index": "0" }, { "key":
"service-name", "description": "上网服务场所名称", "required": "0", "help_string": "(*)",
"value_size":"0", "index":"1" }, {"key":"principal-name","description":"经营法人","required":
"0", "help_string": "(*)", "value_size": "0", "index": "2" }, { "key": "principal-cert-type",
"description": "经营法人有效证件类型", "required":"0", "help_string": "(1021111-身份证、1021133-
学生证、1021335-驾驶证、1021114-军官证、1021123-警官证、1021113-户口簿、1021414-护照、1021511-台
胞证、1021516-回乡证、1021159-社保卡、1021233-士兵证\/军人证、1021990-其他证件)(*)","value_size":
"0", "index": "3" }, { "key": "principal-cert-code", "description": "经营法人有效证件号码",
"required": "0", "help_string": "(*)", "value_size": "0", "index": "4" }, { "key": "person-name",
"description": "场所负责人", "required": "0", "help_string": "(*)", "value_size": "0", "index":
"5" }, { "key": "person-phone", "description": "联系电话", "required": "0", "help_string": "(*)",
"value_size": "0", "index": "6" }, {"key": "cap-type", "description": "采集类型", "required": "0",
"help_string": "(1-围栏、2-WIFI、3-车载、9-其他)(*)", "value_size": "0", "index": "7" }, { "key":
"service-type", "description": "场所服务类型", "required": "0", "help_string": "(1-旅店宾馆类（住
宿服务场所）、2-图书馆阅览室、3-电脑培训中心类、4-娱乐场所类、5-交通枢纽、6-公共交通工具、7-餐饮服
务场所、8-金融服务场所、10-购物场所、11-公共服务场所、12-文化服务场所、13-公共休闲场所、9-其他)(*)",
"value_size": "0", "index": "8" }, { "key": "business-nature", "description": "场所经营性质",
"required": "0", "help_string": "(1-经营、2-非经营、3-围栏采集、9-其他)(*)", "value_size": "0",
"index": "9" }, { "key": "status", "description": "营业状态", "required": "0", "help_string": "(1-
装机开业在线、2-装机开业离线、6-勒令停业、12-暂停营业、14-预约安装、10-其他)(*)","value_size":"0",
"index": "10" }, { "key":"address", "description": "场所详细地址", "required": "0", "help_string":
"(*)", "value_size": "0", "index": "11" }, { "key": "create-time", "description": "场所安装时间",
"required":"0", "help_string": "(例：2018-01-10)(*)", "value_size": "0", "index": "12" }, {"key":
"province-code", "description": "所属省编码", "required": "0", "help_string": "6 位数编码",
"value_size":"0", "index":"13" }, {"key":"city-code","description":"所属城市编码","required":
"0", "help_string": "6 位数编码", "value_size": "0", "index": "14" }, { "key": "area-code",
"description": "所属分区编码", "required": "0", "help_string": "6 位数编码", "value_size": "0",
"index": "15" }, { "key": "police-code", "description": "所属派出所编码", "required": "0",
"help_string": "(8 位数编码)(*)", "value_size": "0", "index": "16" }, { "key": "longitude",
```

"description":"场所经度","required":"0","help_string":"(*)","value_size":"0","index":"17"},{"key":"latitude","description":"场所纬度","required":"0","help_string":"(*)","value_size":"0","index":"18"},{"key":"start-time","description":"营业开始时间","required":"0","help_string":"(例：14:00)","value_size":"0","index":"19"},{"key":"end-time","description":"营业结束时间","required":"0","help_string":"(例：14:00)","value_size":"0","index":"20"},{"key":"producer-code","description":"接入服务商","required":"0","help_string":"(1-中国电信、2-中国网通、3-中国联通、4-中国长城宽带、5-中国铁通、6-中国移动、8-教育部门、9-中科院、11-广电部门、99-其他)","value_size":"0","index":"21"},{"key":"producer-type","description":"接入方式","required":"0","help_string":"(1-专网、真实 IP 地址、2-专线、3-ADSL 拨号、4-ISDN、5-普通拨号、6-Cable modem 拨号、7-电力线、8-无线上网、99-其他)","value_size":"0","index":"22"}]}

字段解释：（不同第三方日志对应的参数不一样）

字段	说明
key-string	参数名，配置命令用
required	是否必填，1 表示必填，0 表示非必填
description	参数中文描述
help-string	参数的帮助信息，为空表示不限制

【提示信息】 -

【平台说明】 EG、NBR 系列（除 CS 系列）系列产品均支持，MSC、NBR-C/S、AG、ACE 产品不支持

2.18 show plog para-list send-para

显示第三方日志发送可配置的参数

show plog para-list send-para *palt-name*

【参数说明】

参数	描述
plat-name	配置的第三方日志平台名称

【命令模式】 特权模式、全局模式

【使用指导】

【配置举例】 查看指定第三方日志平台的场所信息可配置参数列表（非固定，不同第三方日志可能不一样）

```
Ruijie#sh plog para-list send-para surfilter
{ "code": 0, "msg": 18, "list": [ { "key": "server", "description": "服务器 IP", "required": "0", "help_string": "", "value_size": "0", "index": "0" }, { "key": "ftp-server-port", "description": "服务器端口(FTP)", "required": "0", "help_string": "", "value_size": "0", "index": "7" }, { "key": "username", "description": "FTP 用户名", "required": "0", "help_string": "", "value_size": "0", "index": "12" }, { "key": "password", "description": "FTP 密码", "required": "0", "help_string": "", "value_size": "0", "index": "13" } ] }
```

字段解释：（不同第三方日志对应的参数不一样）

字段	说明
key-string	参数名，配置命令用
required	是否必填，1 表示必填，0 表示非必填
description	参数中文描述
help-string	参数的帮助信息，为空表示不限制

【提示信息】 -

【平台说明】 EG、NBR 系列（除 CS 系列）系列产品均支持，MSC、NBR-C/S、AG、ACE 产品不支持

2.19 show plog platform

显示第三方日志发送可配置的参数

show plog platform

【参数说明】

参数	描述
-	-

【命令模式】 特权模式、全局模式

【使用指导】

【配置举例】 查看当前支持的第三方日志类型

```
Ruijie#sh plog platform
{ "code": 0, "msg": "", "list": [ { "platform-type": "surfilter", "description": "任子行" },
{"platform-type":"test","description":"万能测试模板"},{"platform-type":"myp","description":
"美亚柏科" }, { "platform-type": "yitaiwangke", "description": "以太网科" }, { "platform-type":
"xinwangcheng", "description": "新网程" }, { "platform-type": "wuhanhongxu", "description": "武汉
宏旭" }, { "platform-type": "shandongzhaowu", "description": "山东兆物" }, { "platform-type":
"ruian_beijing", "description": "北京锐安" }, { "platform-type": "ruian_baoji", "description": "
宝鸡锐安" }, { "platform-type": "anhuizhongxin", "description": "安徽中新" }, { "platform-type":
"baian", "description": "佰安" }, {"platform-type": "chongqingaisi", "description": "重庆爱思" },
{ "platform-type": "wangjixingchen", "description": "网际星辰" }, { "platform-type": "paibo",
"description": "派博" }, { "platform-type": "fenghuo", "description": "烽火" }, { "platform-type":
"wangbo", "description": "网博" }, { "platform-type": "hunanbubiao", "description": "湖南部标" },
{"platform-type":"quanguobubiao","description":"全国部标"},{"platform-type":"youmachuangda",
"description": "优码创达" }, { "platform-type": "zhongxinwangan", "description": "中新网安" },
{"platform-type":"zhili","description":"芝立软件"},{"platform-type":"boyi","description":
"博艺" } ] }
```

字段解释：（不同第三方日志对应的参数不一样）

字段	说明
platform-type	第三方日志类型
description	描述，一般为中文名称

【提示信息】 -

【平台说明】 EG、NBR 系列（除 CS 系列）系列产品均支持，MSC、NBR-C/S、AG、ACE 产品不支持

2.20 show police-log config

显示第三方日志模块的配置信息

show police-log config

【参数说明】

参数	描述
-	-

【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配置信息

```
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】 -

【平台说明】 -

2.21 show police-log status

显示第三方日志模块的运行状态

show police-log status

【参数说明】

参数	描述
-	-

【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 status
------------police-log status--------------
>police-log:     enable
>server status:  connected
>log total deal: 2626   speed:0
>file total send:184    failed:16       waitting:0
>compress:       disable
------------AUTH LOG---------------
in>   rcv:2,    deal:2,  fail:0
out>  rcv:2,    deal:2,  fail:0
file> send:1,    fail:3,         drop:1
------------NAT LOG---------------
in>   rcv:2568, deal:2568,       fail:0
out>  rcv:2568, deal:2568,       fail:0
file> send:141,  fail:50,        drop:13
------------VID LOG---------------
in>   rcv(vid):0,       deal:0,  fail:0
out>  rcv(vid+im):19,   deal:19,         fail:0
file> send:15,   fail:5,         drop:1
------------URL LOG---------------
out>  rcv:37,   deal:37,         fail:0
```

```
file> send:11,    fail:7,          drop:1

-------------MAIL LOG---------------

out>  rcv:0,     deal:0,   fail:0

file> send:0,     fail:0,          drop:0

-------------WEBBBS LOG---------------

out>  rcv:0,     deal:0,   fail:0

file> send:0,     fail:0,          drop:0

-------------WEBSEARCH LOG---------------

out>  rcv:0,     deal:0,   fail:0

file> send:0,     fail:0,          drop:0
```

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 status	MACC 的通信是否联通，connected 表示已连接，disconect 表示未连接
log total deal	总共处理日志个数及速度
file total send	总共发送日志文件个数及失败个数
compress	文件压缩开关：enable 压缩，disable 不压缩
AUTH LOG	认证日志统计信息
NAT LOG	nat 日志统计信息
VID LOG	虚拟身份日志统计信息
URL LOG	http 日志统计信息
MAIL LOG	邮件日志统计信息
WEBBBS LOG	bbs 论坛日志统计信息
WEBSEARCH LOG	搜索日志统计信息

【提示信息】 -

【平台说明】 -

3 LOG-POLICY

命令	作用
log-policy	创建日志策略
log-policy-relate	设置日志策略的关联用户
log-policy-config	配置日志策略
show log-policy	查询日志策略信息
clear log-policy	删除所有的日志策略

3.1 log-policy

配置基于用户的日志策略

log-policy *policy-name* { **netlog | 82log | none** }

删除日志策略。

no log-policy *policy-name*

【参数说明】

参数	描述
policy-name	日志策略名称，允许最大长度为 64 个字节

【缺省配置】 缺省无配置

【命令模式】 全局模式

【缺省级别】 14

【使用指导】 1：不能配置同名的日志策略

2：日志策略最多 1000 条

【配置举例】 1：添加日志策略。

```
Ruijie# configure terminal
Ruijie(config)# log-policy eg 82log
Ruijie(config)#end
```

2：删除日志策略

```
Ruijie# configure terminal
Ruijie(config)#no log-policy eg
Ruijie(config)# end
```

【检验方法】 使用 show running-config 命令可以查看配置状态。

【提示信息】 1：如果用户策略名称超过最大长度，则给出提示。

```
Ruijie(config)#log-policy      kkkk
```

【命令模式】 全局模式

【缺省级别】 14

【使用指导】 1：对同策略名的策略进行配置，表示修改。
2：配置地址范围时，起始地址必须小于结束地址
3：基于 ip 信息的日志策略只能关联一个对象
4：基于用户的日志策略最多只能关联 10 用户

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。

用户管理模块和营销认证模块重启时，这期间将无认证日志。

【配置举例】 1：关联静态用户

```
Ruijie# configure terminal
Ruijie(config)# log-policy-relate relate policyname sub-any subscriber any
Ruijie(config)#end
```

2：关联动态用户

```
Ruijie# configure terminal
Ruijie(config)# log-policy-relate relate policyname auth auth-subscribe any
Ruijie(config)#end
```

3：关联 ip 地址

```
Ruijie# configure terminal
Ruijie(config)# log-policy-relate relate policyname ip ip-host 192.168.3.11
Ruijie(config)# end
```

4：关联 ip 子网

```
Ruijie# configure terminal
Ruijie(config)# log-policy-relate relate policyname subnet ip-subnet 192.168.5.0 255.255.255.0
Ruijie(config)#end
```

5：关联 ip 范围

```
Ruijie# configure terminal
Ruijie(config)# log-policy-relate relate policyname range ip-range 192.168.3.1 192.168.5.1
Ruijie(config)# end
```

【检验方法】 使用 show running-config 命令可以查看配置状态。

【提示信息】 1：如果策略超过最大容量，则给出提示。

```
Ruijie(config)#log-policy k1001 netlog
The maximum capacity has been reached, the max number of log policy is 1000!
```

2：如果基于 ip 的范围配置的起始地址大于结束地址，则给出提示。

```
Ruijie(config)#log-policy policyname kk netlog ip-range 192.168.2.1 192.168.1.1 2
invalid param, 192.168.2.1 must greater than 192.168.1.1
```

【常见错误】 -

【平台说明】 MSC 产品不支持，其他网关系列产品均支持

3.3 log-policy-config

日志策略顺序交换

log-policy-config priority-swap *policy-name1 policy-name2*

【参数说明】

参数	描述
policy-name1	日志策略名称，允许最大长度为 64 个字节
policy-name2	日志策略名称，允许最大长度为 64 个字节

【缺省配置】 缺省无配置

【命令模式】 全局模式

【缺省级别】 14

【使用指导】 1：交换的策略一定要存在。

2：交换的策略必须是前后关系

【配置举例】 1：日志策略优先级调换。

```
Ruijie# configure terminal
Ruijie(config)# log-policy-config priority-swap subnet range
Ruijie(config)# end
```

【检验方法】 使用 show running-config 命令可以查看配置状态。

【提示信息】 1：如果交换的策略不存在

```
Ruijie(config)# log-policy-config priority-swap subnet xx
swap failed
```

【常见错误】 -

【平台说明】 MSC 产品不支持，其他网关系列产品均支持

3.4 show log-policy

显示日志策略信息

show log-policy [**policyname** *policy-name*]

【参数说明】

参数	描述
policy-name	日志策略名称，允许最大长度为 64 个字节

【命令模式】 特权模式

【缺省级别】 14

【使用指导】 1：没有策略名时，显示所有的日志策略信息，有策略名只显示指定日志策略的信息。

【配置举例】 1：查看所有的日志策略。

```
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
```

2：基于策略名称查询日志策略。

```
Ruijie# show log-policy policyname ip
  log-policy ip none
      log-policy-relate relate policyname ip ip-host 192.168.3.11
```

【提示信息】 如果用户策略名称超过最大长度，则给出提示。

```
Ruijie(config)#show log-policy kkkk
```

【平台说明】 MSC 产品不支持，其他网关系列产品均支持

3.5 clear log-policy

删除所有的日志策略

clear log-policy

【参数说明】

参数	描述
-	-

【命令模式】 特权模式

【缺省级别】 14

【使用指导】 无

【配置举例】 1：删除所有的日志策略。

```
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# clear log-policy
Ruijie# show log-policy

Ruijie#
```

【提示信息】 如果用户策略名称超过最大长度，则给出提示。

【平台说明】 MSC 产品不支持，其他网关系列产品均支持

4 SNMP

4.1 clear snmp locked-ip

要清除 SNMP 连续认证失败后被锁定的源 IP 地址表，请执行特权模式命令 **clear snmp locked-ip**。

clear snmp locked-ip [**ipv4** *ipv4-address* | **ipv6** *ipv6-address*]

【参数说明】

参数	描述
ipv4 *ipv4-address*	清除某个特定的源 IPv4 地址
ipv6 *ipv6-address*	清除某个特定的源 IPv6 地址

【命令模式】 特权模式

【缺省级别】 14

【使用指导】 该命令用于手工清除 SNMP 连续认证失败后被锁定的源 IP 地址，可以清除整个源 IP 地址表，也可以清除某个特定的源 IP 地址。

源 IP 地址被清除后，来自于此源 IP 地址的 SNMP 访问报文，又可以重新尝试认证。

【配置举例】 下面的示例清除整个 SNMP 连续认证失败后被锁定的源 IP 地址表：

```
Ruijie# clear snmp locked-ip
```

【提示信息】 -

【平台说明】

4.2 no snmp-server

配置屏蔽设备 SNMP 代理功能。

no snmp-server

【参数说明】

参数	描述
-	-

【缺省配置】 启动 SNMP 代理功能

【命令模式】 全局配置模式

【缺省级别】 14

【使用指导】 SNMP 代理功能服务默认开启，另外在设置 SNMP 代理参数(例如 NMS 主机地址、认证名和访问权限等)时，同时也会自动打开 SNMP 代理服务，使用该命令可以关闭设备支持的所有版本 SNMP 的代理服务。
该命令必须与服务开关命令 **enable service snmp-agent** 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。

【配置举例】 1：屏蔽 SNMP 代理服务。

```
Ruijie(config)# no snmp-server
```

【检验方法】 执行 **no snmp-server** 命令，然后执行 **show running-config** 命令查看配置，可以发现除了该命令以外，所有 SNMP 代理的配置命令都被屏蔽。此时使用 NMS 无法访问 MIB。

【提示信息】 -

【常见错误】 -

【平台说明】 -

4.3 show snmp

显示 SNMP 的状态信息。
show snmp [**mib** | **user** | **view** | **group| host | locked-ip | process-mib-time**]

【参数说明】

参数	描述
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	显示 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。

【命令模式】 特权用户模式

【缺省级别】 14

【使用指导】 -

【配置举例】 1：显示是 SNMP 的统计信息。

```
Ruijie# show snmp
```

```
Chassis: 60FF60
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: disabled
SNMP logging: disabled
SNMP agent: enabled
```

字段解释：

字段	说明
Chassis	系统序列码。
SNMP packets input	输入报文计数：输入报文总数
Bad SNMP version errors	输入报文计数：版本错误的报文总数
Unknown community name	输入报文计数：使用未知团体名进行访问的报文总数
Illegal operation for community name supplied	输入报文计数：使用团体名进行越权操作的报文总数
Encoding errors	输入报文计数：编码错误的报文总数
Number of requested variables	输入报文计数：读取的 MIB 对象总数
Number of altered variables	输入报文计数：设置的 MIB 对象总数
Get-request PDUs	输入报文计数：Get 请求报文总数
Get-next PDUs	输入报文计数：Get-next 请求报文总数
Set-request PDUs	输入报文计数：Set 请求报文总数
SNMP packets output	输出报文计数：输出报文总数
Too big errors (Maximum packet size 1472)	输出报文计数：超长（超过 1472 字节）报文总数

No such name errors	输出报文计数：返回 No such name 错误的报文总数
Bad values errors	输出报文计数：返回 Bad values 错误的报文总数
General errors	输出报文计数：返回 General error 错误的报文总数
Response PDU	输出报文计数：正常返回的报文总数
Trap PDUs	输出报文计数：发出的 Trap 报文总数
SNMP global trap	全局 Trap 开关状态
SNMP logging	全局 SNMP 日志开关状态
SNMP agent	全局 SNMP 代理开关状态

【提示信息】 -

【平台说明】 -

4.4 snmp trap link-status

打开接口发送 Link Trap 功能。

snmp trap link-status

关闭接口发送 Link Trap 功能。

no snmp trap link-status

【参数说明】

参数	描述
-	-

【缺省配置】 缺省情况下，该功能打开，如果接口发生 Link 状态变化，SNMP 将发出 LinkTrap。

【命令模式】 接口配置模式

【缺省级别】 14

【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。

【配置举例】 1：关闭接口发送 Link Trap 功能。

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

2：打开接口发送 Link Trap 功能。

```
Ruijie(config)# interface gigabitEthernet 1/1
Ruijie(config-if-GigabitEthernet 1/1)# snmp trap link-status
```

【检验方法】 -

【提示信息】 -

【常见错误】 -

【平台说明】 -

4.5 snmp-server authentication attempt

本命令用于限制 SNMP 连续认证失败次数，并指定连续认证失败后的处理策略。该命令的 **no** 形式清除连续认证失败次数限制及相关处理策略。

snmp-server authentication attempt *times* **exceed** { **lock** | **lock-time** *minutes* | **unlock** }

清除连续认证失败次数限制及相关处理策略。

no snmp-server authentication attempt *times* **exceed** { **lock** | **lock-time** *minutes* | **unlock** }

【参数说明】

参数	描述
times	SNMP 认证失败的最大次数，范围：1~10。
exceed	对 SNMP 尝试认证后失败次数超过最大限制值所采取的处理策略。
lock	表示永久禁止该源 IP 地址进行认证，一直列入黑名单，需要管理员手工进行解除。
lock-time *minutes*	表示禁止该源 IP 地址一段时间后，再允许其重新认证 其中，*minutes* 为禁止该源 IP 地址的时间，范围：1～65535，单位：分钟。
unlock	表示对认证失败的用户不做限制处理，允许其继续登录。

【缺省配置】 默认关闭 SNMP 攻击防护检测功能

【命令模式】 全局配置模式

【缺省级别】 14

【使用指导】 SNMP 认证失败后，系统会将其加入 SNMP 源 IP 地址管理的黑名单。当认证失败次数超过限定值时，系统将会根据设备设置的处理措施对其之后的访问认证行为进行相应的限制：

- 对于被永久禁止认证的源 IP 地址，只有管理员进行手工解除后，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 地址才可以重新认证；

对于不受限制的源 IP 地址，只要用户重新访问认证时，使用了正确的 community（针对 SNMPv1 和 SNMPv2c）或 username（针对 SNMPv3），就可以重新认证成功。

【配置举例】 1：下面的示例设置 SNMP 连续认证失败次数为 4，连续 4 次认证失败后锁定 30 分钟:

```
Ruijie(config)# snmp-server authentication attempt 4 exceed lock-time 30
```

【检验方法】 打开 SNMP 攻击防护检测功能后，用错误的团体名或错误的用户名进行访问认证，连续认证失败后会锁定该源 IP 地址，再次访问认证的时候会有 log 该 IP 已经被锁定。用 show snmp locked-ip 可以查看到锁定列表中有该 IP 地址。

【提示信息】 -

【常见错误】 -

【平台说明】 -

4.6 snmp-server chassis-id

配置系统序列码。

snmp-server chassis-id *text*

恢复缺省值。

no snmp-server chassis-id

【参数说明】

参数	描述
text	系统序列号的文本，可以是数字或字符。

【缺省配置】 序列号缺省值是 60FF60

【命令模式】 全局配置模式

【缺省级别】 14

【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。系统序列号可以通过 **show snmp** 命令查看。

【配置举例】 1：配置 SNMP 的系统序列号为 123456。

```
Ruijie(config)# snmp-server chassis-id 123456
```

【检验方法】 -

【提示信息】 -

【常见错误】 -

【平台说明】 -

4.7 snmp-server community

配置认证名和访问权限。

snmp-server community [0 | 7] *string* [**view** *view-name*] [[**ro** | **rw**] [**host** *ipaddr*]] [**ipv6** *ipv6-aclname*] [*aclnum* | *aclname*]

删除认证名。

no snmp-server community [0 | 7] *string*

【参数说明】

参数	描述
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(1-199 及 1300-2699)，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。
ipaddr	关联 NMS 地址，指定访问 MIB 的 NMS 地址。

【缺省配置】 所有团体缺省为只读。

【命令模式】 全局配置模式

【缺省级别】 14

【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。

【配置举例】 1：配置允许 NMS 使用 public 的 SNMP 团体访问字符对 MIB 的访问，权限为只读。

```
Ruijie(config)# snmp-server community public ro
```

【检验方法】 -

【提示信息】 -

【常见错误】 -

【平台说明】 -

4.8 snmp-server contact

配置系统的联系方式。
snmp-server contact *text*

删除指定的联系方式。
no snmp-server contact

【参数说明】

参数	描述
text	描述系统联系方式的字符串

【缺省配置】 系统联系方式为空。

【命令模式】 全局配置模式

【缺省级别】 14

【使用指导】 -

【配置举例】 1：配置 SNMP 的系统联系方式为 i-net800@i-net.com.cn。

```
Ruijie(config)# snmp-server contact i-net800@i-net.com.cn
```

【检验方法】 -

【提示信息】 -

【常见错误】 -

【平台说明】 -

4.9 snmp-server enable secret-dictionary-check

配置对 community 和 user 进行密码字典检查。
snmp-server enable secret-dictionary-check

撤销对 community 和 user 进行密码字典检查。
no snmp-server enable secret-dictionary-check

【参数说明】

参数	描述
-	-

【缺省配置】 缺省下，不对 community 和 user 进行密码字典检查。

【命令模式】 全局配置模式

【缺省级别】 14

【使用指导】 该命令必须与全局配置命令 **password policy** 一起使用。

【配置举例】 1：配置密码长度不小于 6 个字符。

```
Ruijie(config)# password policy min-size 6
Ruijie(config)# snmp-server enable secret-dictionary-check
Ruijie(config)#snmp-server community abc12
% The community(abc12) is a weak community!
```

【检验方法】 -

【提示信息】 -

【常见错误】 -

【平台说明】 -

4.10 snmp-server enable traps

配置 Agent 主动向 NMS 发送 Trap 消息。
snmp-server enable traps [*notification-type*]

禁止 SNMP 向 NMS 主动发送 Trap 消息。
no snmp-server enable traps

【参数说明】

参数	描述
notification-type	主动发送的 Trap 类型，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。

【缺省配置】 缺省下，禁止 SNMP 向 NMS 主动发送 Trap 消息。。

【命令模式】 全局配置模式

【缺省级别】 14

【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。
如果没有指定 Trap 类型，则包括所有 Trap 类型。

【配置举例】 1：配置主动发送 SNMP 事件 Trap 消息。

```
Ruijie(config)# snmp-server enable traps snmp
Ruijie(config)# snmp-server host 192.168.12.219 public snmp
```

【检验方法】 -

【提示信息】 -

【常见错误】 -

【平台说明】 -

4.11 snmp-server flow-control

配置 SNMP 流控。
snmp-server flow-control pps [*count*]

恢复 SNMP 流控的默认值。
no snmp-server flow-control pps

【参数说明】

参数	描述

count	每秒处理的 SNMP 请求报文数量，范围<50-65535>

【缺省配置】 缺省配置 *count* 为 300。

【命令模式】 全局配置模式

【缺省级别】 14

【使用指导】 -

【配置举例】 1：配置每秒处理 200 个 SNMP 请求报文。

```
Ruijie(config)# snmp-server flow-control pps 200
```

【检验方法】 -

【提示信息】 -

【常见错误】 -

【平台说明】 -

4.12 snmp-server group

配置 SNMP 用户组。

snmp-server group *groupname* { **v1** | **v2c** | **v3** { **auth** | **noauth** | **priv** } } [**read** *readview*] [**write** *writeview*] [**access** { **ipv6** *ipv6-aclname aclnum* | *aclname* }]

删除用户组。

no snmp-server group *groupname* { **v1** | **v2c** | **v3** {**auth** | **noauth** | **priv**} }

【参数说明】

参数	描述
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。

【缺省配置】 缺省没有配置用户组。

【命令模式】 全局配置模式

【缺省级别】 14

【使用指导】 -

【配置举例】 1：配置一个用户组 mib2user。

```
Ruijie(config)# snmp-server group mib2user v3 priv read mib2
```

【检验方法】 -

【提示信息】 -

【常见错误】 -

【平台说明】 -

4.13 snmp-server host

配置 Agent 主动发送消息的 NMS 主机地址。

snmp-server host [**oob**] { *host-addr* | **ipv6** *ipv6-addr* } [**traps | informs**] [**version** { **1** | **2c** | **3** { **auth** | **noauth** | **priv** }] *community-string* [**udp-port** *port-num*] [*notification-type*]

删除指定 SNMP 主机地址。

no snmp-server host [**oob**] { *host-addr* | **ipv6** *ipv6-addr* } [**traps | informs**] [**version** { **1** | **2c** | **3** { **auth** | **noauth** | **priv** }] *community-string* [**udp-port** *port-num*]

【参数说明】

参数	描述
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），只有在设备具备 MGMT 管理口的时候才会有该选项
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。

【缺省配置】 缺省情况下，没有 SNMP 主机。

【命令模式】 全局配置模式

【缺省级别】 14

【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。

【配置举例】 1：指定一个 SNMP 主机，接收 SNMP 事件 Trap。

```
Ruijie(config)# snmp-server host 192.168.12.219 public snmp
```

【检验方法】 -

【提示信息】 -

【常见错误】 -

【平台说明】 NBR6205-E、NBR6135-E、NBR6210-E、NBR6215-E 支持 MGMT 口；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 MGMT 口。

4.14 snmp-server inform

配置 inform 尝试发送次数与超时发送时间。
snmp-server inform [retries *retry-num* | timeout *time*]

恢复 inform 报文尝试重发次数和超时发送时间。
no snmp-server inform

【参数说明】

参数	描述
retry-num	Inform 报文尝试重发次数，范围是<0-255>。

time	Inform 报文超时发送时间，范围是<0-21474836>。

【缺省配置】 缺省配置 *retry-num 为 3，time 为 15s*。

【命令模式】 全局配置模式

【缺省级别】 14

【使用指导】 -

【配置举例】 1：配置 inform 报文尝试重发次数为 5。

```
Ruijie(config)# snmp-server inform retries 5
```

1：配置 inform 报文超时发送时间为 20s。

```
Ruijie(config)# snmp-server inform timeout 20
```

【检验方法】 -

【提示信息】 -

【常见错误】 -

【平台说明】 -

4.15 snmp-server location

配置系统位置。

snmp-server location *text*

删除系统位置。

no snmp-server location

【参数说明】

参数	描述
text	描述系统信息的字符串。

【缺省配置】 系统信息为空

【命令模式】 全局配置模式

【缺省级别】 14

【使用指导】 -

【配置举例】 1：配置系统位置。

```
Ruijie(config)# snmp-server location start-technology-city 4F of A Building
```

【检验方法】 -

【提示信息】 -

【常见错误】 -

【平台说明】 -

4.16 snmp-server logging

SNMP 日志功能将记录 NMS 对 SNMP Agent 的 GET、GET-NEXT 和 SET 操作

snmp-server logging { **get-operation | set-operation** }

关闭打开的开关

no snmp-server logging { **get-operation | set-operation** }

【参数说明】

参数	描述
get-operation	记录 GET、GET-NEXT 操作的开关
set-operation	记录 SET 操作的开关

【缺省配置】 缺省情况下，SNMP 日志功能处于关闭状态

【命令模式】 全局配置模式

【缺省级别】 14

【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。

【配置举例】 1：打开 get、set 操作记录开关

```
ruijie(config)#snmp-server logging get-operation
ruijie(config)#snmp-server logging set-operation
```

通过 NMS 对 sysname 节点（.1.3.6.1.2.1.1.5.0）进行 GET、GET-NEXT 和 SET 操作，控制台会打印下面的日志信息

```
ruijie#*Feb  7 15:31:16: %SNMP-6-GET_OPER: NMS source-ip(13.12.11.7) operation(GET)
object(id=1.3.6.1.2.1.1.5.0)

ruijie#*Feb  7 15:32:16:%SNMP-6-GETN_OPER: NMS source-ip(13.12.11.7) operation(GET-NEXT)
object(id=1.3.6.1.2.1.1.5.0)

ruijie#*Feb  7 15:33:23: %SNMP-6-SET_OPER: NMS source-ip(13.12.11.7) operation(SET)
object(id=1.3.6.1.2.1.1.5.0, value=ruijie)
```

2：关闭 get 或者 set 开关

```
ruijie(config)#no snmp-server logging get-operation
ruijie(config)#no snmp-server logging set-operation
```

【检验方法】 -

【提示信息】 -

【常见错误】 -

【平台说明】 -

4.17 snmp-server net-id

配置设备网元编码信息。
snmp-server net-id *text*

删除设备网元编码信息。
no snmp-server net-id

【参数说明】

参数	描述
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。

【缺省配置】 设备网元编码信息为空

【命令模式】 全局配置模式

【缺省级别】 14

【使用指导】 -

【配置举例】 1：配置设备网元编码信息。

```
Ruijie(config)# snmp-server net-id FZ_CDMA_MSC1
```

【检验方法】 -

【提示信息】 -

【常见错误】 -

【平台说明】 -

4.18 snmp-server packetsize

配置 SNMP 代理最大数据报文长度。

snmp-server packetsize *byte-count*

恢复缺省值。

no snmp-server packetsize

【参数说明】

参数	描述
byte-count	数据包大小，从 484 字节到 17876 字节。

【缺省配置】 1472 字节

【命令模式】 全局模式

【缺省级别】 14

【使用指导】 -

【配置举例】 1：配置 SNMP 最大数据包大小为 1492。

```
Ruijie(config)# snmp-server packetsize 1492
```

【检验方法】 -

【提示信息】 -

【常见错误】 -

【平台说明】 -

4.19 snmp-server queue-length

配置 Trap 消息报文的队列长度。
snmp-server queue-length *length*

恢复缺省值。
no snmp-server queue-length

【参数说明】

参数	描述
length	队列长度，大小从 1 到 1000。

【缺省配置】 10

【命令模式】 全局配置模式

【缺省级别】 14

【使用指导】 通过调整消息队列大小来控制消息发送速度。

【配置举例】 1：配置 Trap 消息队列长度为 100。

```
Ruijie(config)# snmp-server queue-length 100
```

【检验方法】 -

【提示信息】 -

【常见错误】 -

【平台说明】 -

4.20 snmp-server system-shutdown

打开 SNMP 系统重启通知功能。
snmp-server system-shutdown

关闭 SNMP 系统重启通知功能。
no snmp-server system-shutdown

【参数说明】

参数	描述
-	-

【缺省配置】 关闭 SNMP 系统重启通知功能。

【命令模式】 全局配置模式

【缺省级别】 14

【使用指导】 打开 SNMP 系统重启通知功能，RGOS 会在设备 **reload/reboot** 以前给 NMS 发送 Trap 消息通知系统重启。

【配置举例】 1：打开 SNMP 系统重启功通知功能。

```
Ruijie(config)# snmp-server system-shutdown
```

【检验方法】 -

【提示信息】 -

【常见错误】 -

【平台说明】 -

4.21 snmp-server trap-format private

配置 SNMP Trap 消息携带私有字段。

snmp-server trap-format private

恢复缺省配置。

no snmp-server trap-format private

【参数说明】

参数	描述
-	-

【缺省配置】 不携带私有字段。

【命令模式】 全局配置模式

【缺省级别】 14

【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。

⚠ 当使用 SNMP v1 的版本发送 Trap 消息时，该配置不生效。

【配置举例】 1：指定 Trap 消息携带私有字段。

```
Ruijie(config)# snmp-server trap-format private
```

【检验方法】 -

【提示信息】 -

【常见错误】 -

【平台说明】 -

4.22 snmp-server trap-source

指定发送 Trap 消息的源地址。

snmp-server trap-source *interface*

恢复缺省配置。

no snmp-server trap-source

【参数说明】

参数	描述
interface	用于作为 SNMP 源地址的接口

【缺省配置】 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。

【命令模式】 全局配置模式

【缺省级别】 14

【使用指导】 缺省情况下，SNMP 报文从哪个接口出去，就使用哪个接口的 IP 地址作为源地址，为了便于管理和识别，可以使用该命令固定使用一个本地 IP 地址作为 SNMP 的源地址。

【配置举例】 1：指定以太网口 0/1 的 IP 地址作为发送 Trap 消息的源地址。

```
Ruijie(config)# snmp-server trap-source fastethernet 0/1
```

【检验方法】 -

【提示信息】 -

【常见错误】 -

【平台说明】 -

4.23 snmp-server trap-timeout

配置发送 Trap 消息重发的超时时间。

snmp-server trap-timeout *seconds*

恢复缺省配置。

no snmp-server trap-timeout

【参数说明】

参数	描述
seconds	超时时间，单位为秒，取值范围：1 – 1000。

【缺省配置】 30 秒

【命令模式】 全局配置模式

【缺省级别】 14

【使用指导】 -

【配置举例】 1：配置发送 Trap 消息重发的超时时间为 60 秒。

```
Ruijie(config)# snmp-server trap-timeout 60
```

【检验方法】 -

【提示信息】 -

【常见错误】 -

【平台说明】 -

4.24 snmp-server udp-port

指定接收 SNMP 报文的协议端口号。

snmp-server udp-port *port-num*

恢复缺省配置。

no snmp-server udp-port

【参数说明】

参数	描述
port-num	指定接收 SNMP 报文的协议端口号。

【缺省配置】 缺省情况下，使用 161 协议端口接收 SNMP 报文。

【命令模式】 全局配置模式

【缺省级别】 14

【使用指导】 -

【配置举例】 1：指定 15000 协议端口接收 SNMP 报文。

```
Ruijie(config)# snmp-server udp-port 15000
```

【检验方法】 -

【提示信息】 -

【常见错误】 -

【平台说明】 -

4.25 snmp-server user

配置 SNMP 用户。

snmp-server user *username groupname* {**v1** | **v2c** | **v3** [**encrypted**] [**auth** {**md5** | **sha**} *auth-password*] [**priv des56** *priv-password*]} [**access** { **ipv6** *ipv6-aclname* | *aclnum* | *aclname*}]

删除 SNMP 用户。

no snmp-server user *username groupname* {**v1** | **v2c** | **v3** }

【参数说明】

参数	描述
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。

【缺省配置】 缺省没有配置用户。

【命令模式】 全局配置模式

【缺省级别】 14

【使用指导】 -

【配置举例】 1：配置一个 SNMPv3 用户，使用 MD5 认证，和使用 DES 加密。

```
Ruijie(config)# snmp-server user user-2 mib2user v3 auth md5 authpassstr priv des56 despassstr
```

【检验方法】 -

【提示信息】 -

【常见错误】 -

【平台说明】 -

4.26 snmp-server view

配置 SNMP 视图。

snmp-server view *view-name oid-tree* {**include** | **exclude**}

删除 SNMP 视图。

no snmp-server view *view-name* [*oid-tree*]

【参数说明】

参数	描述
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。

【缺省配置】 缺省配置一个 default 视图，允许访问所有的 MIB 对象。

【命令模式】 全局配置模式

【缺省级别】 14

【使用指导】 -

【配置举例】 1：配置一个视图，包括所有的 MIB-2 子树（oid 为 1.3.6.1）。

```
Ruijie(config)# snmp-server view mib2 1.3.6.1 include
```

【检验方法】 -

【提示信息】 -

【常见错误】 -

【平台说明】 -

5 CM-APM

5.1 apm conference-system access-list

通过 ACL 指定哪些数据流需要进行视频会议质量监控。
apm conference-system access-list *acl_id* **alias** *name*

删除某一个 ACL 的指定
no apm conference-system access-list *acl_id*

删除所有 ACL 的指定
no apm conference-system access-list all

【参数说明】

参数	描述
acl_id	acl 的 id，取值范围 1~199
name	符合规则的数据流的别名

【缺省配置】 缺省无相关配置。

【命令模式】 全局模式

【缺省级别】 14

【使用指导】 通过配置本命令可以指定哪些数据流需要进行视频会议质量监控。

【配置举例】 1：监控 IP：172.18.3.3 和 IP:172.18.3.8 之间的所有 UDP 流 。

```
Ruijie(config)# access-list 150 permit udp 172.18.3.3 0.0.0.0 172.18.3.8 0.0.0
Ruijie(config)# apm conference-system access-list 150 alias kkk
```

2：删除上述 ACL 的指定。

```
Ruijie(config)#no apm conference-system access-list 150
```

3：删除所有 ACL 指定。

```
Ruijie(config)# no apm conference-system access-list all
```

【检验方法】 通过 show run | include apm conference-system access-list 可以查看配置了哪些监控 acl。

【提示信息】 -

【常见错误】 1. 配置的 ACL 不存在。
2. 如果视频会议是 UDP 数据流，则需要在视频会议的两端都部署网关设备，否则无法进行质量监控。

【平台说明】 -

5.2 apm conference-system application

通过应用名指定哪些数据流需要进行视频会议质量监控。
apm conference-system application *app_name*

删除某一个应用的配置
no apm conference-system application *app_name*

删除所有应用的配置
no apm conference-system application all

【参数说明】

参数	描述
app_name	应用名称，不能为 all

【缺省配置】 无相关配置。

【命令模式】 全局模式

【缺省级别】 14

【使用指导】 通过配置本命令可以指定哪些数据流需要进行视频会议质量监控。

【配置举例】 1：指定监控红杉树会议系统的视频会议。

```
Ruijie(config)# apm conference-system application 红杉树会议系统
```

2：删除指定监控红杉树会议系统。

```
Ruijie(config)#no apm conference-system application 红杉树会议系统
```

3：删除所有应用指定。

```
Ruijie(config)# no apm conference-system application all
```

【检验方法】 通过 show run | include apm conference-system application 可以查看配置了哪些监控应用。

【提示信息】 1：应用名不存在，则提示错误

```
% Configuration fail: application is not exist!
```

【常见错误】 1、配置的应用名不存在。
2、如果视频会议是 UDP 数据流，则需要在视频会议的两端都部署网关设备，否则无法进行质量监控。

【平台说明】 -

5.3 apm conference-system enable

开启视频会议质量监控功能。
apm conference-system enable

关闭视频会议质量监控功能
no apm conference-system enable

【参数说明】

参数	描述
-	-

【缺省配置】 缺省情况下，视频会议质量监控功能是开启。

【命令模式】 全局模式

【缺省级别】 14

【使用指导】 通过配置本命令启动视频会议质量监控功能。可以在不删除 application 和 access-list 的情况下，通过 no apm conference-system enable 暂时关闭视频会议监控功能。

【配置举例】 1：开启视频会议质量监控功能。

```
Ruijie(config)# apm conference-system enable
```

2：关闭视频会议质量监控功能。

```
Ruijie(config)# no apm conference-system enable
```

【检验方法】 show run 里头看不到该命令，即为开启状态。

【提示信息】 -

【常见错误】 -

【平台说明】 -

5.4 apm conference-system measure-period

设置视频会议质量采用周期。

apm conference-system measure-period *time*

删除采用周期设置

no apm conference-system measure-period

【参数说明】

参数	描述
time	采用周期时间，单位为秒，取值范围 30~120

【缺省配置】 缺省值为 60。

【命令模式】 配置模式

【缺省级别】 14

【使用指导】 通过配置本命令可以设置视频会议质量采用周期。

【配置举例】 1：设置采用周期为 30 秒。

```
Ruijie(config)# apm conference-system measure-period 30
```

2：恢复采样周期。

```
Ruijie(config)#no apm conference-system measure-period
```

【检验方法】 -

【提示信息】 -

【常见错误】 采样范围超过限制区间，导致配置失败

【平台说明】 -

5.5 apm export-length

设置 APM 日志报文有效数据的最大长度

apm export-length *value*

恢复默认配置
no apm export-length

【参数说明】

参数	描述
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

【缺省配置】 缺省最大长度为 1400。

【命令模式】 全局模式

【缺省级别】 14

【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。

【配置举例】 1：设置 APM 日志报文有效数据的最大长度为 1000

```
Ruijie(config)#apm export-length 1000
```

2、恢复系统默认的 ipfix 报文长度

```
Ruijie(config)#no apm export-length
```

【检验方法】 通过 show apm server info 可以查看。

【提示信息】 -

【常见错误】 长度配置太小，导致额外浪费了更多的带宽。

【平台说明】 -

5.6 apm export-rate

设置 APM 日志发送速率
apm export-rate *rate*

恢复 APM 日志发送默认速率
no apm export-rate

【参数说明】

参数	描述
rate	每秒发送多少个 APM 信息，取值范围 10~100000 之间

【缺省配置】 缺省速率为 1000。

【命令模式】 全局模式

【缺省级别】 14

【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。

【配置举例】 1、配置每秒钟发送 100 个 ipfix 数据，即节点，而非报文数

```
Ruijie(config)# apm export-rate 100
```

2、将每秒发送节点数恢复到默认值

```
Ruijie(config)# no apm export-rate
```

【检验方法】 通过 show apm server info 可以查看。

【提示信息】 -

【常见错误】 速率配置过大，导致 CPU 持续偏高。

【平台说明】 -

5.7 apm log-type

设置 APM 日志往哪个服务器发送

apm log-type {*type* | **default**} **priority** *prio* **server** *name*

删除相关配置

no apm log-type { type | **default** | **all** }

【参数说明】

参数	描述
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
name	消息类型发往那个服务器

【缺省配置】 无相关配置。

【缺省级别】 14

【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 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。

【配置举例】 1、默认将所有消息类型都发到服务器 rac 中，优先级为 0

```
Ruijie(config)# apm log-type default priority 0 server rac
```

2、删除默认消息类型的配置

```
Ruijie(config)# no apm log-type default
```

3、删除所有消息类型对应服务器的配置

```
Ruijie(config)# no apm log-type all
```

4、将 log-type 为 1 的消息类型发到服务器 ruijie 中，优先级为 1

```
Ruijie(config)#apm  log-type 1 priority 1 server ruijie
```

5、将 log-tye 为 1 的消息类型的特殊配置删除

```
Ruijie(config)# no apm log-type 1
```

【检验方法】 使用 show apm server info 查看配置的服务器和优先级是否正确

【提示信息】 如果服务器“ruijie”不存在，则提示错误

```
% The item is not exist！
```

【常见错误】 0 的优先级最高，而不是最低

【平台说明】 -

5.8 apm sample business application

设置需要监控哪些业务的数据加载速率
apm sample business application *app-name*

删除某一个被监控的业务
no apm sample business application *app-name*

删除对所有业务数据加载速率的监控
no apm sample business application all

【参数说明】

参数	描述
app-name	应用名称，具体参考应用识别

【缺省配置】 缺省无相关配置。

【缺省级别】 14

【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。

【配置举例】 1、监控 BQQ 数据加载速率

```
Ruijie(config)# apm sample business application BQQ
```

2、删除对 BQQ 数据加载速率的监控

```
Ruijie(config)# no apm sample business application BQQ
```

3、删除对所有业务数据加载速率的监控

```
Ruijie(config)# no apm sample business application all
```

【检验方法】 使用 Ruijie#show apm sample business info 查看是否成功。

【提示信息】 1、如果配置数目达到上限，则提示错误

```
% The capacity is full, you can't configure any more!
```

2、如果配置的应用设备不支持识别，则提示错误。

```
% Configuration fail: application is not exist!
```

【常见错误】 -

【平台说明】 -

5.9 apm sample disable

关闭指定的 APM 监控日志

apm sample { **cpu-mem** | **sata-flash** | **vpn | vpn-detail** | **ip-session** | **intf-flowrate** | **app-type-flowrate** | **app-flowrate** | **user-flowrate** | **ping-detect** | **url-topn** | **business** } **disable**

删除指定 APM 日志的 disable

no apm sample{ **cpu-mem** | **sata-flash** | **vpn | vpn-detail** | **ip-session** | **intf-flowrate** | **app-type-flowrate** | **app-flowrate** | **user-flowrate** | **ping-detect** | **url-topn** | **business** } **disable**

删除所有 disable 配置

apm sample del-all-disable

【参数说明】

参数	描述
-	-

【缺省配置】 所有 APM 监控日志都没有 disable。

【缺省级别】 14

【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 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。

【配置举例】 1、关闭 cpu、内存信息采样

```
Ruijie(config)# apm sample cpu-mem disable
```

2、关闭应用流量采样

```
Ruijie(config)# apm sample app-flowrate disable
```

3、开启应用流量采样

```
Ruijie(config)# no apm sample app-flowrate disable
```

【检验方法】 使用 Ruijie#show running-config | include apm sample 查看是否开启、关闭

【提示信息】 -

【常见错误】 -

【平台说明】 NBR2500D-E、NBR3000D-E、NBR3000D-UE 出厂带 SATA 硬盘。NBR108G-P 、NBR800G、NBR950G、NBR1500G、NBR2000G、NBR1000G-C、NBR2000G-C、NBR3000G-S、NBR1000G-E、NBR6120-E、

NBR1300G-E、NBR1700G-E、NBR2100G-E、NBR6205-E、NBR6135-E、NBR6210-E、NBR6215-E 出厂无 SATA 硬盘。其中 NBR6205-E、NBR6135-E、NBR6210-E、NBR6215-E 可自行购买 SATA 硬盘使用。

5.10 apm sample enable

开启全局 APM 采样开关
apm sample enable

关闭全局 APM 采样开关
no apm sample enable

【参数说明】

参数	描述
-	-

【缺省配置】 默认关闭状态

【缺省级别】 14

【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

【配置举例】 1、开启全局 APM 采样开关

```
Ruijie(config)# apm sample enable
```

2、关闭全局 APM 采样开关

```
Ruijie(config)# no apm sample enable
```

【检验方法】 使用 show running-config | include apm sample 查看是否开启

【提示信息】 -

【常见错误】 -

【平台说明】 -

5.11 apm sample interval

设置全局 APM 采样周期
apm sample default interval *second*

恢复全局 APM 采样周期默认值
no apm sample default interval

单独设置各 APM 信息的采样周期
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*

将指定 APM 信息的采样周期恢复到默认值
no apm sample { **cpu-mem** | **sata-flash** | **vpn | vpn-detail** | **ip-session** | **intf-flowrate** | **app-type-flowrate** | **app-flowrate** | **user-flowrate** | **ping-detect** | **business** } **interval**

【参数说明】

参数	描述
second	采样周期，单位为秒，取值范围为 10~3600

【缺省配置】 全局 APM 采样周期默认为 5 分钟，默认无单独设置。

【命令模式】 全局模式

【缺省级别】 14

【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。

【配置举例】 1、配置 cpu、内存信息采集时间为 10s

```
Ruijie(config)# apm sample cpu-mem interval 10
```

2、配置应用流量采样周期为 10s

```
Ruijie(config)# apm sample app-flowrate interval 10
```

3、将应用流量采样周期时间恢复为默认时间

```
Ruijie(config)# no apm sample app-flowrate interval
```

【检验方法】 使用 show apm sample log-sends 查看是否正确

【提示信息】 -

【常见错误】 -

【平台说明】 NBR2500D-E、NBR3000D-E、NBR3000D-UE 出厂带 SATA 硬盘。NBR108G-P 、NBR800G、NBR950G、NBR1500G、NBR2000G、NBR1000G-C、NBR2000G-C、NBR3000G-S、NBR1000G-E、NBR6120-E、NBR1300G-E、NBR1700G-E、NBR2100G-E、NBR6205-E、NBR6135-E、NBR6210-E、NBR6215-E 出厂

无 SATA 硬盘。其中 NBR6205-E、NBR6135-E、NBR6210-E、NBR6215-E 可自行购买 SATA 硬盘使用。

5.12 apm sample ping-detect server

设置 PING 检测的检测地址

apm sample ping-detect server { *ip-address* | *host* } [**ntimes** *times*] [**length** *len*] [**source** {**lan** | *so-ip-address* | *interface-name* }]

删除指定 PING 服务器

no apm sample ping-detect server { *ip-address* | *host* }

删除所有服务器

no apm sample ping-detect server all

【参数说明】

参数	描述
ip-address	*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

【缺省配置】 times 默认为 5，len 默认值为 100

【缺省级别】 14

【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。

【配置举例】 1、配置服务器 172.18.3.1，PING 包次数 10 次，包长 100 个字节

```
Ruijie(config)# apm sample ping-detect server 172.18.3.1 ntimes 10 length 100
```

2、删除服务器 172.18.3.1

```
Ruijie(config)# no apm sample ping-detect server 172.18.3.1
```

3、删除所有服务器

```
Ruijie(config)# no apm sample ping-detect server all
```

【检验方法】 使用 show apm sample ping-detect info 查看是否正确

【提示信息】 -

【常见错误】 1. 输入的 ip 地址错误。
2. PING 检测的服务器没有经过 IPSECVPN，却配置了 source lan 的参数。

【平台说明】 -

5.13 apm sample url-topn send-time

设置行为报表 URL-TOPN 的发送时间点
apm sample url-topn send-time *hour*

将发送时间恢复到默认时间
no apm sample url-topn send-time

【参数说明】

参数	描述
hour	URL-TOPN 发送的时间。取值范围 0~23

【缺省配置】 默认发送日志时间为 1 点

【命令模式】 全局模式

【缺省级别】 14

【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。

【配置举例】 1、配置 URL-TOPN 发送时间为 0 点

```
Ruijie(config)# apm sample url-topn send-time 0
```

2、将发送时间恢复到默认时间

```
Ruijie(config)# no apm sample url-topn send-time
```

【检验方法】 使用 show apm sample url-topn info 查看是否正确

【提示信息】 -

【常见错误】 将时间设置在设备繁忙的时间段，导致设备 CPU 偏高。

【平台说明】 -

5.14 apm sample url-topn top

设置行为报表 URL-TOPN

apm sample url-topn top *num*

将 topn 值恢复到默认

no apm sample url-topn top

【参数说明】

参数	描述
num	收集 url 访问量 top 多少的值，取值范围是 1~100

【缺省配置】 默认发送 top50 的 url

【缺省级别】 14

【使用指导】 设置发送 top 几的 url 信息

【配置举例】 1、配置每次发送 top80 的 url

```
Ruijie(config)# apm sample url-topn top 80
```

2、将 topn 值恢复到默认

```
Ruijie(config)# no apm sample url-topn top
```

【检验方法】 使用 show apm sample url-topn info 查看是否正确

【提示信息】 -

【常见错误】 -

【平台说明】 -

5.15 apm server

设置 APM 日志服务器

apm server *name* { *ip-address* } [source *ip-address*] [*port*] [**tcp** | **udp**] [oob]

删除指定服务器

no apm server *name*

删除所有服务器

no apm server all

【参数说明】

参数	描述
name	*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

【缺省配置】 port 默认值为 30000，协议默认使用 tcp

【缺省级别】 14

【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。最多配置 10 个服务器。

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。

要删除一个服务器，使用 **no apm server** *name* 命令。

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。

【配置举例】 1、配置服务器 rac，端口 20000，udp 协议

```
Ruijie(config)# apm server rac 172.18.3.51 20000 udp
```

2、配置服务器 rac，source 192.168.1.1

```
Ruijie(config)# apm server rac 172.18.3.51 source 192.168.1.1
```

在 2 的基础上修改服务器 rac 的 ip，其余不变

```
Ruijie(config)# apm server rac 172.18.3.52
```

在上述的基础上，删除 source 配置（即不绑定任何源 ip），其余不变

Ruijie(config)# apm server rac 172.18.3.52 source 0.0.0.0

3、删除服务器 rac

```
Ruijie(config)# no apm server rac
```

4、删除所有服务器

```
Ruijie(config)# no apm server all
```

【检验方法】 1：使用 show apm server info 查看配置是否正确，socket 值是否不为 0

2、查看对应的服务器是否有收到消息

【提示信息】 如果服务器个数达到上限，提示错误信息

```
% The capacity is full, you can't configure any more!
```

如果要删除的服务器不存在提示错误

```
% The item is no exist!
```

【常见错误】 1 配置的服务器 IP、端口与服务器不符，导致无法建立连接。

【平台说明】 NBR6205-E、NBR6135-E、NBR6210-E、NBR6215-E 支持 MGMT 口；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 MGMT 口。

5.16 apm template send-period

设置 APM 日志模板的发送周期
apm template send-period *seconds*

将模板发送时间恢复到默认
no apm template send-period

【参数说明】

参数	描述
seconds	定时发送模板时长，单位为秒，取值范围为 60~3600

【缺省配置】 默认发送时间为 300s

【命令模式】 全局模式

【缺省级别】 14

【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】 1、配置模板发送时间为 60s

```
Ruijie(config)# apm template send-period 60
```

2、将模板发送时间恢复到默认

```
Ruijie(config)# no apm template send-period
```

【检验方法】 1、使用 show apm server info 查看配置的时间是否正确
2、仅配置一个可用的服务器，该服务器下不关联任何消息类型，然后执行 clear apm server log-count 命令清除计数。一段时间后查看是否有数据发出，并统计两次之间的时间差是否为所配置的时间。

【提示信息】 -

【常见错误】 -

【平台说明】 -

5.17 apm user-log filter

配置设备审计日志的过滤字段
apm user-log filter *words*

取消配置设备审计日志过滤字段。
no apm user-log filter *words*

【参数说明】

参数	描述
words	需要过滤的字段

【缺省配置】 -

【命令模式】 配置模式

【缺省级别】 14

【使用指导】 不需要记录的设备审计日志，可以通过该命令指定关键字

【配置举例】 1：配置不记录含有“登录”的设备审计日志。

```
Ruijie(config)# apm user-log filter 登录
```

2：取消过滤配置。

```
Ruijie(config)# no apm user-log filter 登录
```

【检验方法】 使用 show apm user-log filter 查看已配置的内容

【提示信息】 -

【常见错误】 -

【平台说明】 -

5.18 apm webpage enable

启动网页加载耗时统计的功能

apm webpage enable

关闭网页加载耗时统计的功能。
no apm webpage enable

【参数说明】

参数	描述
-	-

【缺省配置】 打开网页加载耗时统计的功能。

【命令模式】 配置模式

【缺省级别】 14

【使用指导】 该功能默认打开，在没有配置需要监控的网页的情况下，对性能没有影响。
如果配置了若干个监控的网页，想停止监控功能，则可以适用关闭的命令。

【配置举例】 1：打开网页加载耗时统计的功能。

```
Ruijie(config)# apm webpage enable
```

2：关闭网页加载耗时统计的功能。

```
Ruijie(config)# no apm webpage enable
```

【检验方法】 1：使用 show apm webpage statistics 命令，可以查看网页加载耗时监控功能是启用还是关闭。

【提示信息】 -

【常见错误】 -

【平台说明】 -

5.19 apm webpage url

配置需要监控的网页
apm webpage url *url-string*

取消配置监控的网页。
no apm webpage url [**all** | *url-string*]

【参数说明】

参数	描述
url-string	需要监控的网页地址

【缺省配置】 -

【命令模式】 全局模式

【缺省级别】 14

【使用指导】 如果要监控某个网页的加载耗时，通过则可以通过该命令添加。
如果要取消对某个网页的监控，则使用对应的 no 命令。
no apm webpage url all 是删除所有的网址配置。
这里的 URL 是精确匹配。

【配置举例】 1：配置一个监控的网页，如 www.ietf.com。

```
Ruijie(config)# apm webpage url www.ietf.com/
```

2：取消一个监控的网页。

```
Ruijie(config)# no apm webpage url www.ietf.com/
```

3：取消所有监控的网页。
Ruijie(config)# no apm webpage url all

【检验方法】 1：使用 **show apm webpage url** 命令，可以查看当前配置的监控网页。

【提示信息】 1：如果配置的网页地址长度超过 200 个字节，则提示出错。

```
% The URL length must be shorter than 200！
```

处理建议：重新配置，保证 URL 长度不超过 200。

2：如果配置的网页地址已满，则提示出错。

```
% The capacity is full, you can’t configure anymore!
```

处理建议：删除不需要的配置，重新配置。

3：如果配置的网页地址已经配置过了，则提示出错。

```
% The item has been configured!
```

处理建议：检查配置的内容是否有误，如已配置，不需要再进行配置。

4：如果要取消的网页地址尚未配置，则提示出错。

```
% The item is not exist!
```

处理建议：检查配置内容是否有误。

5：如果配置的 URL 为关键字，如“all”，则提示出错。

```
% Configuration failed: URL can not be used word “all”!
```

处理建议：更换 URL 名称，重新配置。

【常见错误】 1：配置的网页地址，不是具体的网页如“www.ietf.com/index.html”或者没有以“/”结尾，如“www.ietf.com”。
2：配置的网页地址超过 50 个。
3：配置了超长的网页地址，长度超过 200.
4：配置 URL 时，只截取了 URL 的域名部分导致 URL 无法命中。

【平台说明】 -

5.20 clear apm server log-count

清除 APM 日志发送统计
clear apm server log-count

【参数说明】

参数	描述
-	-

【命令模式】 特权模式

【缺省级别】 14

【使用指导】 清除 APM 日志发送统计，全部清为 0

【配置举例】 1、清除 APM 日志统计值

```
Ruijie#clear apm server log-count
```

【提示信息】 -

【平台说明】 -

5.21 show apm sample business 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

【参数说明】

参数	描述
-	-

【命令模式】 特权模式

【缺省级别】 14

【使用指导】 查看配置了哪些业务（应用）需要监控数据加载速率

【配置举例】 查看配置了哪些业务（应用）需要监控数据加载速率

```
Ruijie#show apm sample business info
其他 TCP
BQQ
QQ-登录|聊天
MAPI
DNS
telnet
NETBIOS-NS
```

字段解释：

字段	说明
	显示被监控的业务名称

【提示信息】 -

【平台说明】 -

5.22 show apm sample log-sends

查看各类采样业务的周期

show apm sample log-sends

【参数说明】

参数	描述
-	-

【命令模式】 特权模式

【缺省级别】 14

【使用指导】 查看各类采样业务的周期

【配置举例】 1、查看各类采样业务的周期

```
Ruijie#show apm sample log-sends
log-name                    interval
cpu-mem                       10
```

```
sata-flash                    10
ip-session                    10
intf-flowrate                 10
app-type-flowrate             10
app-flowrate                  10
user-flowrate                 10
vpn                           10
vpn-detail                    10
business                      10
ping-detect                   10
url-topn                      300
```

字段解释：

字段	说明
log-name	消息类型名称
interval	发送日志周期，单位是秒

【提示信息】 -

【平台说明】 -

5.23 show apm sample ping-detect info

查看用户配置的 PING 检测信息

show apm sample ping-detect info

【参数说明】

参数	描述
-	-

【命令模式】 特权模式

【缺省级别】 14

【使用指导】 查看用户配置的 PING 检测信息

【配置举例】 1、查看用户配置的 PING 检测信息

```
Ruijie#show apm sample ping-detect info
------------------------------------------------------------
server1:172.18.3.1
ntimes:10        length:1400        source:
------------------------------------------------------------
server2:172.18.3.100
```

```
ntimes:10        length:1400        source:
```

字段解释：

字段	说明
server	服务器 IP 地址或域名
ntimes	PING 包次数
length	PING 包长度
source	PING 报文的源 IP 指定，为空的话，表示按设备默认。

【提示信息】 -

【平台说明】 -

5.24 show apm sample url-topn info

查看用户配置的 URL-TOPN 信息

show apm sample url-topn info

【参数说明】

参数	描述
-	-

【命令模式】 特权模式

【缺省级别】 14

【使用指导】 查看用户配置的 URL-TOPN 信息

【配置举例】 1、查看用户配置的 URL-TOPN 信息

```
Ruijie#show apm sample url-topn info
send-clock: 1
send-topn: 50
```

字段解释：

字段	说明
send-clock	日志发送时间
send-topn	发送的 url 的 topn

【提示信息】 -

【平台说明】 -

5.25 show apm server info

查看 APM 日志服务器的设置

show apm server info

【参数说明】

参数	描述
-	-

【命令模式】 特权模式

【缺省级别】 14

【使用指导】 查看 APM 日志服务器的设置

【配置举例】 查看 APM 日志服务器的设置

```
Ruijie#show apm server info
Ipfix server is enable!
================================================================
server:server1                  ip:172.18.181.63   port:30000 protocal:udp
socket : 32857
================================================================
server:server2                  ip:172.18.3.56     port:20000 protocal:tcp
socket : 0
log_type:1    prio:0
================================================================
server:server3               ip:172.18.181.63   port:20000 protocal:udp
socket : 32858
================================================================
Export rate : 1000
Template send period second : 300
Send buffer length : 1400
ipfix queue free node number : 3000
ipfix msg queue node info
prio : 0, msg node number : 0
prio : 1, msg node number : 0
prio : 2, msg node number : 0
Create template error number: 0
Record data error number: 25060
```

字段解释：

字段	说明
show 结果第一行	显示是服务器是否可用

server	显示服务器名称
ip	服务器对应的 ip
port	服务器端口号
protocal	传输报文使用的协议
socket	为 0 表示该服务器不可用，非 0 为 socket 的值
log_type	将 log_type 后的消息类型挂到相对于的服务器中
prio	同一行中 log_type 对应的优先级
Export rate	每秒发送的节点个数
Template send period second	报文发送周期
Send buffer length	Ipfix 报文最大长度
ipfix queue free node number	Ipfix 空闲节点数
ipfix msg queue node info	每个优先级对应的节点数
Create template error number	创建模板失败的个数
Record data error number	业务模块写数据失败次数，clear apm server log-count 可以清除

【提示信息】 -

【平台说明】 -

5.26 show apm server log-count

查看 APM 日志发送情况

show apm server log-count

【参数说明】

参数	描述
-	-

【命令模式】 特权模式

【缺省级别】 14

【使用指导】 查看 apm 日志发送情况

【配置举例】

```
Ruijie#show apm server log-count
Server : server1
Send node num：10 send packet : 24692 error packet : 380
last_error:server socket closed(51)
Drop node num : 0
================================================================
```

```
Server : server2
Send node num：0 send packet : 0 error packet : 0 last_errno : 0
last_error:.....
Drop node num : 200576
=================================================================
Server : server3
Send node num：10 send packet : 24692 error packet : 380 last_errno: 51
last_error:.....
Drop node num : 0
=================================================================
<1>cpu-memory           , send log num: 1
<2>flash-sata           , send log num: 2
<3>ip-session           , send log num: 3
<4>intf-flowrate        , send log num: 4
<5>app-type-flowrate    , send log num: 5
<6>app-flowrate         , send log num: 6
<7>user-flowrate        , send log num: 7
<8>vpn-infomation       , send log num: 8
<9>vpn-detail           , send log num: 9
<10>webpage-time        , send log num: 0
<11>conference-system   , send log num: 10
<12>config-infomation   , send log num: 10
<13>business-flowrate   , send log num: 10
<14>ping-detect         , send log num: 10
<15>url-top-n           , send log num: 10
<16>tcp-performance     , send log num: 10
<17>udp-performance     , send log num: 10
```

字段解释：

字段	说明
Server	服务器名称
Send node num	发送的节点个数
send packet	往该服务器发送了多个报文
error packet	发送错误的报文个数
last_error	最后一次发送失败原因，括号中记录的是错误码。
Drop node num	由于节点队列已满，无法写入的节点数
send log num	对应类型发送的消息个数

【提示信息】 -

【平台说明】 -

5.27 show apm tcp-measure info

查看 tcp-measure 的运行信息。

show apm tcp-measure info

【参数说明】

参数	描述
-	-

【命令模式】 特权模式

【缺省级别】 14

【使用指导】 使用该命令可以查看 tcp 协议性能测量概况，包括正在测量的流个数，重包统计数，输出日志数等。

【配置举例】 1：查看 tcp-measure 运行信息

```
Ruijie#show apm tcp-measure info
Flow capacity: 2000, used num:0
Duplicate capacity: 8000, used num:0
Send Logs: 988
```

字段解释：

字段	说明
Flow capacity	当前统计的流节点，分别含系统最大节点数和已适用节点数
Duplicate capacity	当前用于统计重包的节点，分别含系统最大节点数和已适用节点数
Send Logs	当前已发送的日志数

【提示信息】 -

【平台说明】 -

5.28 show apm udp-measure info

查看当前视频会议监控的 UDP 流情况。

show apm udp-measure info

【参数说明】

参数	描述
-	-

【缺省配置】 无。

【命令模式】 特权模式

【缺省级别】 14

【使用指导】 通过此命令可以查看查看当前视频会议监控的 UDP 流情况。

【配置举例】 1：查看当前视频会议监控的 UDP 流情况。

```
Ruijie# show apm udp-measure info
the udp monitor buffer is : 5112
the udp monitor bank: 248
the sector head num  :111
dst_ip             src_ip          dst _port     src_port        direct     packet_code
172.18.3.8         172.18.3.3       8000          1863            2          24e551a1
172.18.3.3         172.18.3.8       1863          8000            1          e61d5c16
```

字段解释：

字段	说明
udp monitor buffer	空闲的组装 BUF 的个数
udp monitor bank	空闲的窗口个数
sector head	空闲的监控五元组个数
dst_ip	目的 IP
src_ip	源 IP
dst_port	目的端口
src_port	源端口
direct	报文的方向，1 为下行，2 为上行
packet_code	首个报文的特征码

【提示信息】 -

【平台说明】 -

5.29 show apm webpage statistics

查看网页加载耗时统计的运行信息。

show apm webpage statistics

【参数说明】

参数	描述
-	-

【命令模式】 特权模式

【缺省级别】 14

【使用指导】 使用该命令可以网页加载耗时的运行信息，包括在统计的网页个数，连接个数，已发送的日志数，以及当前模块是否在运行。

【配置举例】 1：查看网页加载耗时的运行情况

```
Ruijie#show apm webpage statistics
apm webpage info:
    export log num:0
    webpage capacity: 1000; used:     0
    connection capacity: 2000; used:     0
webpage : disable
```

字段解释：

字段	说明
export log num	已发送的网页耗时日志条数
webpage capacity	网页统计节点最大个数和已使用个数
connection capacity	网页连接的最大个数和已使用个数
webpage	当前模块是否在运行（处理报文）

【提示信息】 -

【平台说明】 -

5.30 show apm webpage url

查看已配置的监控网页的地址。

show apm webpage url

【参数说明】

参数	描述
-	-

【命令模式】 特权模式

【缺省级别】 14

【使用指导】 使用该命令可以查看设备上配置的监控网页的详细信息。

【配置举例】 1：查看设备上配置的监控网页的详细信息

```
Ruijie#show apm webpage url
```

```
www.ietf.com/
www.ietf.com/index.html
```

字段解释：

字段	说明
www.ietf.com/	配置的网页地址

【提示信息】 -

【平台说明】 -

6 ANTI-SNIPER

命令	作用
anti-sniper interface	开启某个接口的防网络尖兵功能。
http-modify off	关闭 HTTP 报文拆分功能
http-modify mode	配置 HTTP 报文拆分方式
ip-id off	关闭修改 IP 报文的 IPID 值功能
ip-id random	设定 ipid 值为随机
ip-ttl off	关闭修改 IP 报文 TTL 值的功能
ip-ttl value	设置 IP 报文的 TTL 值
tcp-port off	关闭修改 tcp 端口的功能
tcp-port continuous	设置 TCP 端口为连续的
tcp-port range	设置 TCP 端口值的范围
tcp-timestamp off	关闭抹掉 tcp 报文中时间戳选项的功能
tcp-win-size off	关闭修改 TCP 窗口大小的功能
tcp-win-size value	设置 TCP 窗口大小的值
show anti-sniper policy	查看防网络尖兵的配置

6.1 anti-sniper interface

开启某个接口的防网络尖兵功能。

anti-sniper interface *intf-name*

关闭某个接口的防网络尖兵功能。

no anti-sniper interface *intf-name*

【参数说明】

参数	描述
intf-name	接口名

【缺省配置】 缺省情况下，功能是关闭的。

【命令模式】 全局配置模式

【缺省级别】 14

【使用指导】 通过配置本命令启动某个接口下的防网络尖兵功能。

【配置举例】 1：开启设备的 GI0/5 下防网络尖兵功能

```
Ruijie#config
```

```
Ruijie(config)#anti-sniper interface gigabitEthernet 0/5
```

2：关闭设备的 GI0/5 下防网络尖兵功能

```
Ruijie#config
Ruijie(config)# no anti-sniper interface gigabitEthernet 0/5
```

【检验方法】 1：使用 **show run** 命令，可以查看 GI0/5 下防网络尖兵功能是不是开着

2：使用 **show anti-sniper policy** 命令，也可以查看功能是否配置成功。

【提示信息】 -

【常见错误】 -

【平台说明】 EG 系列、NBR 系列

6.2 http-modify off

关闭 HTTP 报文拆分功能。

http-modify off

打开 HTTP 报文拆分功能。

no http-modify off

【参数说明】

参数	描述
-	-

【缺省配置】 缺省情况下，此功能是打开的

【命令模式】 防网络尖兵模式

【缺省级别】 14

【使用指导】 通过本命令配置打开或关闭 HTTP 报文拆分功能。

【配置举例】 1：设置打开 HTTP 报文拆分功能

```
Ruijie#config
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
```

【检验方法】 1：使用 **show anti-sniper policy** 命令，可以查看功能开关是否打开。

【提示信息】 -

【常见错误】 -

【平台说明】 EG 系列、NBR 系列

6.3 http-modify mode

配置 HTTP 报文拆分方式
http-modify mode *num*

删除相关配置。
no http-modify mode

【参数说明】

参数	描述
num	方式，取值范围 1-4

【缺省配置】 缺省情况下，默认为 1。

【命令模式】 防网络尖兵模式

【缺省级别】 14

【使用指导】 通过本命令配置 HTTP 报文拆分方式。

【配置举例】 1：设置 HTTP 报文拆分方式为 3

```
Ruijie#config
Enter configuration commands, one per line.  End with CNTL/Z.
Ruijie(config)# anti-sniper interface gigabitEthernet 0/5
Ruijie(config-anti-sniper)# http-modify mode 3
```

【检验方法】 1：使用 **show anti-sniper policy** 命令，可以查看模式配置情况。

【提示信息】 -

【常见错误】 -

【平台说明】 EG 系列、NBR 系列

6.4 ip-id off

关闭修改 IP 报文的 IPID 功能。

ip-id off

打开修改 IP 报文的 IPID 功能。

no ip-id off

【参数说明】

参数	描述
-	-

【缺省配置】 缺省情况下，此功能是开启的。

【命令模式】 防网络尖兵模式

【缺省级别】 14

【使用指导】 通过本命令配置启用或关闭修改 IP 报文的 IPID 功能。

【配置举例】 1：打开修改 IP 报文的 IPID 功能

```
Ruijie#config
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
```

【检验方法】 1：使用 **show anti-sniper policy** 命令，可以查看模式配置情况。

【提示信息】 -

【常见错误】 -

【平台说明】 EG 系列、NBR 系列

6.5 ip-id random

设置 IP 报文的 IPID 值为随机方式

ip-id random

设置 IP 报文的 IPID 值为递增方式

no ip-id random

【参数说明】

参数	描述

-	-

【缺省配置】 缺省情况下，为随机方式

【命令模式】 防网络尖兵模式

【缺省级别】 14

【使用指导】 通过本命令配置 IP 报文的 IPID 值方式。

【配置举例】 1：设置 IP 报文的 IPID 值为随机方式。

```
Ruijie#config
Enter configuration commands, one per line.  End with CNTL/Z.
Ruijie(config)# anti-sniper interface gigabitEthernet 0/5
Ruijie(config-anti-sniper)#ip-id random
```

【检验方法】 1：使用 **show anti-sniper policy** 命令，可以查看模式配置情况。

【提示信息】 -

【常见错误】 -

【平台说明】 EG 系列、NBR 系列

6.6 ip-ttl off

关闭修改 IP 报文 TTL 值的功能。
ip-ttl off

开启修改 IP 报文 TTL 值的功能。
no ip-ttl off

【参数说明】

参数	描述
-	-

【缺省配置】 缺省情况下，此功能是开启的。

【命令模式】 防网络尖兵模式

【缺省级别】 14

【使用指导】 通过本命令配置启动或关闭修改 IP 报文 TTL 值的功能

【配置举例】 1：打开修改 IP 报文 TTL 值的功能。

```
Ruijie#config
Enter configuration commands, one per line.  End with CNTL/Z.
Ruijie(config)# anti-sniper interface gigabitEthernet 0/5
Ruijie(config-anti-sniper)# no ip-ttl off
```

【检验方法】 1：使用 **show anti-sniper policy** 命令，可以查看模式配置情况。

【提示信息】 -

【常见错误】 -

【平台说明】 EG 系列、NBR 系列

6.7 ip-ttl value

设置 IP 报文的 TTL 值

ip-ttl value *num*

删除相关配置。

no ip-ttl value

【参数说明】

参数	描述
num	设置 TTL 的值，取值范围 1~255

【缺省配置】 缺省情况下，默认值为 128

【命令模式】 防网络尖兵模式

【缺省级别】 14

【使用指导】 通过本命令设置 IP 报文的 TTL 值。

【配置举例】 1：设置 IP 报文的 TTL 值为 127

```
Ruijie#config
Enter configuration commands, one per line.  End with CNTL/Z.
Ruijie(config)# anti-sniper interface gigabitEthernet 0/5
Ruijie(config-anti-sniper)# ip-ttl value 127
```

【检验方法】 1：使用 **show anti-sniper policy** 命令，可以查看模式配置情况。

【提示信息】 -

【常见错误】 -

【平台说明】 EG 系列、NBR 系列

6.8 tcp-port off

关闭修改 tcp 端口的功能。
tcp-port off

打开修改 tcp 端口的功能。
no tcp-port off

【参数说明】

参数	描述
-	-

【缺省配置】 缺省情况下，此功能是关闭的。

【命令模式】 防网络尖兵模式

【缺省级别】 14

【使用指导】 通过本命令配置启动或关闭修改 tcp 端口的功能。

【配置举例】 1：打开修改 tcp 端口的功能。

```
Ruijie#config
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
```

【检验方法】 1：使用 **show anti-sniper policy** 命令，可以查看模式配置情况。

【提示信息】 -

【常见错误】 -

【平台说明】 EG 系列、NBR 系列

6.9 tcp-port continuous

配置 TCP 端口值为连续的
tcp-port continuous

配置 TCP 端口为奇偶交替
no tcp-port continuous

【参数说明】

参数	描述
-	-

【缺省配置】 缺省情况下，TCP 端口值为连续的

【命令模式】 防网络尖兵模式

【缺省级别】 14

【使用指导】 通过本命令可以配置 TCP 端口值为连续或奇偶交替

【配置举例】 1：配置 TCP 端口为奇偶交替

```
Ruijie#config
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 continuous
```

【检验方法】 1：使用 **show anti-sniper policy** 命令，可以查看模式配置情况。

【提示信息】 -

【常见错误】 -

【平台说明】 EG 系列、NBR 系列

6.10 tcp-port range

配置 TCP 端口值的范围
tcp-port range *min-port max-port*

删除配置
no tcp-port range

【参数说明】

参数	描述
min-port	端口值范围的最小值，范围为 1-65535，默认为 1054
max-port	端口值范围的最大值，范围为 1-65535，默认为 9000

【缺省配置】 缺省情况下，TCP 端口值的范围为 1054~9000

【命令模式】 防网络尖兵模式

【缺省级别】 14

【使用指导】 通过本命令配置可以配置 TCP 端口范围的值

【配置举例】 1：配置 TCP 端口值范围为 2000~8000

```
Ruijie#config
Enter configuration commands, one per line.  End with CNTL/Z.
Ruijie(config)# anti-sniper interface gigabitEthernet 0/5
Ruijie(config-anti-sniper)# tcp-port range 2000 8000
```

【检验方法】 1：使用 **show anti-sniper policy** 命令，可以查看模式配置情况。

【提示信息】 -

【常见错误】 -

【平台说明】 EG 系列、NBR 系列

6.11 tcp-timestamp off

关闭抹掉 tcp 报文中时间戳选项的功能
tcp-timestamp off

开启抹掉 tcp 报文中时间戳选项的功能
no tcp-timestamp off

【参数说明】

参数	描述
-	-

【缺省配置】 缺省情况下，此功能是打开的

【命令模式】 防网络尖兵模式

【缺省级别】 14

【使用指导】 通过本命令可以关闭和开启抹掉 tcp 报文中时间戳选项的功能。

【配置举例】 1：开启抹掉 tcp 报文中时间戳选项的功能

```
Ruijie#config
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】 1：使用 **show anti-sniper policy** 命令，可以查看模式配置情况。

【提示信息】 -

【常见错误】 -

【平台说明】 EG 系列、NBR 系列

6.12 tcp-win-size off

关闭修改 TCP 窗口大小的功能
tcp-win-size off

开启修改 TCP 窗口大小的功能
no tcp-win-size off

【参数说明】

参数	描述
-	-

【缺省配置】 缺省情况下，此功能是打开的

【命令模式】 防网络尖兵模式

【缺省级别】 14

【使用指导】 通过本命令可以关闭和开启修改 TCP 窗口大小的功能。

【配置举例】 1：开启修改 TCP 窗口大小的功能

```
Ruijie#config
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
```

【检验方法】 1：使用 **show anti-sniper policy** 命令，可以查看模式配置情况。

【提示信息】 -

【常见错误】 -

【平台说明】 EG 系列、NBR 系列

6.13 tcp-win-size value

设置 TCP 窗口大小的值

tcp-win-size value *num*

删除配置

no tcp-win-size value

【参数说明】

参数	描述
num	窗口大小的值，默认为 65535，范围为 1~65535

【缺省配置】 缺省情况下，窗口大小值为 65535

【命令模式】 防网络尖兵模式

【缺省级别】 14

【使用指导】 通过本命令可以设置 TCP 窗口大小的值。

【配置举例】 1：设置 TCP 窗口大小的值为 65535

```
Ruijie#config
Enter configuration commands, one per line.  End with CNTL/Z.
Ruijie(config)# anti-sniper interface gigabitEthernet 0/5
Ruijie(config-anti-sniper)# tcp-win-size value 65535
```

【检验方法】 1：使用 **show anti-sniper policy** 命令，可以查看模式配置情况。

【提示信息】 -

【常见错误】 -

【平台说明】 EG 系列、NBR 系列

6.14 show anti-sniper policy

显示当前防网络尖兵的配置

show anti-sniper policy

【参数说明】

参数	描述
-	-

【缺省配置】 无。

【命令模式】 特权模式

【缺省级别】 14

【使用指导】 -

【配置举例】 1：显示防网络尖兵配置

```
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     : FALSE
tcp-port range          : 1054-9000
tcp-win-size            : ON
tcp-win-size value      : 65535
tcp-timestamp           : ON
http-modify             : ON
http-modify mode        : 1
```

【提示信息】 -

【平台说明】 EG 系列、NBR 系列

7 IPMAC-SNIFF

7.1 clear ipmac-sniff

清除通过嗅探绑定的 ipmac 信息。

clear ipmac-sniff all

【参数说明】

参数	描述
all	清除通过嗅探模块绑定的所有 mac 信息

【命令模式】 特权模式

【缺省级别】 15

【使用指导】 此命令用于删除嗅探中绑定的 mac 信息

【配置举例】

1：清除通过嗅探绑定的 mac 信息

```
Ruijie# clear ipmac-sniff all
```

【提示信息】 -

【平台说明】 EG3000 系列，EG3200 系列、NBR6200 系列产品均支持

7.2 ipmac-sniff enable

开启嗅探功能总开关

ipmac-sniff enable

关闭嗅探功能总开关

no ipmac-sniff enable

【参数说明】

参数	描述
-	-

【缺省配置】 关闭嗅探功能

【命令模式】 全局模式

【缺省级别】 15

【使用指导】 开启 IPMAC 嗅探功能的总开关

【配置举例】 1：打开嗅探总开关

```
Ruijie(config)# ipmac-sniff enable
```

2：关闭嗅探总开关

```
Ruijie(config)# no ipmac-sniff enable
```

【检验方法】 1：使用 **show run** 命令，查看对应的配置是否存在。

【提示信息】 -

【常见错误】 -

【平台说明】 EG3000 系列，EG3200 系列、NBR6200 系列产品均支持

7.3 ipmac-sniff ipv6 enable

开启 ipv6-mac 嗅探功能开关

ipmac-sniff ipv6 enable

关闭 ipv6-mac 嗅探功能开关

no ipmac-sniff ipv6 enable

【参数说明】

参数	描述
-	-

【缺省配置】 开启 ipv6-mac 嗅探功能

【命令模式】 全局模式

【缺省级别】 15

【使用指导】 开启 IPV6-MAC 嗅探功能的开关

【配置举例】 1：打开 ipv6-mac 嗅探开关

```
Ruijie(config)# ipmac-sniff ipv6 enable
```

2：关闭 ipv6-mac 嗅探开关

```
Ruijie(config)# no ipmac-sniff ipv6 enable
```

【检验方法】 1：使用 **show run** 命令，查看对应的配置是否存在。

【提示信息】 -

【常见错误】 -

【平台说明】 EG3000 系列，EG3200 系列、NBR6200 系列产品均支持

7.4 ipmac-sniff ipv4 enable

开启 ipv4-mac 嗅探功能开关

ipmac-sniff ipv4 enable

关闭 ipv4-mac 嗅探功能开关

no ipmac-sniff ipv4 enable

【参数说明】

参数	描述
-	-

【缺省配置】 开启 ipv4-mac 嗅探功能

【命令模式】 全局模式

【缺省级别】 15

【使用指导】 开启 IPV4-MAC 嗅探功能的开关

【配置举例】 1：打开 ipv4-mac 嗅探开关

```
Ruijie(config)# ipmac-sniff ipv4 enable
```

2：关闭 ipv4-mac 嗅探开关

```
Ruijie(config)# no ipmac-sniff ipv4 enable
```

【检验方法】 1：使用 **show run** 命令，查看对应的配置是否存在。

【提示信息】 -

【常见错误】 -

【平台说明】 EG3000 系列，EG3200 系列、NBR6200 系列产品均支持

7.5 ipmac-sniff flow-detect

设置 ipmac 节点老化参数

ipmac-sniff flow-detect flowrate *flow-val*

ipmac-sniff flow-detect time-interval *time-val*

恢复 ipmac 节点老化参数默认值

no ipmac-sniff flow-detect flowrate

no ipmac-sniff flow-detect time-interval

【参数说明】

参数	描述
flow-val	流量阀值
time-val	时间阀值，在该时间内，没有超过流量阀值的流量，则老化该 ipmac 节点

【缺省配置】 流量阀值为 0，时间阀值为 15 分钟

【命令模式】 全局模式

【缺省级别】 15

【使用指导】 设置 ipmac 节点老化参数

【配置举例】 1：设置 ipmac 老化时间为 20 分钟

```
Ruijie(config)# ipmac-sniff flow-detect time-interval 20
```

2：恢复 ipmac 老化时间为 15 分钟

```
Ruijie(config)# no ipmac-sniff flow-detect time-interval
```

【检验方法】 1：使用 **show run** 命令，查看对应的配置是否存在。

【提示信息】 -

【常见错误】 -

【平台说明】 EG3000 系列，EG3200 系列、NBR6200 系列产品均支持

7.6 show ipmac-sniff

查看 ipv6/ipv4-mac 绑定情况，以及配置信息

show ipmac-sniff { ipv6 | ipv4 | stat }

【参数说明】

参数	描述
-	-

【命令模式】 特权模式、全局模式

【缺省级别】 15

【使用指导】 查看 ipv4\ipv6-mac 绑定情况

【配置举例】 1：查看 ipv6-mac 绑定情况

```
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
```

2：查看 ipv4-mac 绑定情况

```
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
```

3.查看嗅探功能的配置情况

```
Ruijie# show ipmac-sniff stat
ipmac-sniff           : enable
ipv4-mac              : enable
ipv6-mac              : enable
flow-detect flow(bps) : 0
flow-detect time(min) : 15
```

【检验方法】 -

【提示信息】 -

【常见错误】 -

【平台说明】 EG3000 系列，EG3200 系列、NBR6200 系列产品均支持

8 UPNP-PROXY

8.1 bonjour

设置 bonjour 协议的投屏报文伪造 ip 地址。
投屏报文转发过程中，若报文目的端口是 5353（mDNS），因为 Bonjour 协议要求代理的源 IP 需要与目的 IP 在同一 VLAN 下。默认使用对应目的 IP 的网关子接口 IP 作为代理的源 IP，目的 IP 为映射客户端的 IP。
upnp-proxy bonjour lastip *lastip_num*

删除 bonjour 协议的投屏报文伪造 ip 地址。采用接口地址伪造。
no upnp-proxy bonjour

【参数说明】

参数	描述
lastip_num	1-254

【缺省配置】 缺省为关闭状态。

【命令模式】 全局模式

【缺省级别】 15

【使用指导】 若关闭，则针对 bonjour 协议的投屏报文的伪造，采用映射表对端 IP 节点的接口地址来进行伪造，。

【配置举例】 1：设置 bonjour 协议的投屏报文伪造 ip 地址的最后一位是 100。如果映射表对端 IP 节点是 192.168.10.0 网段，则投屏报文的伪造 IP 地址为 192.168.10.100.

```
Ruijie# configure terminal
Ruijie(config)# upnp-proxy bonjour last-ip 100
Ruijie(config)# end
```

2：关闭 bonjour 协议的投屏报文伪造 ip 地址。

```
Ruijie# configure terminal
Ruijie(config)# no upnp-proxy bonjour
Ruijie(config)# end
```

【检验方法】 使用 show running-config 命令可以查看配置状态。

【提示信息】 -

【常见错误】 -

【平台说明】 -

8.2 child

设置每个房间投屏允许的电视数量，终端数量。
upnp-proxy child length *child_num* *tvip_num* *tvmac_num*

恢复每个房间投屏允许的电视数量，终端数量为缺省值。缺省值都是 8。
no upnp-proxy child

【参数说明】

参数	描述
child_num	1-255 (缺省值是 8)
tvip_num	1-8 (缺省值是 8)
tvmac_num	1-8 (缺省值是 8)

【缺省配置】 缺省为关闭状态。每个房间最大允许的终端数量是 8 个，电视 IP 数量是 8 个，电视 MAC 数量是 8 个。

【命令模式】 全局模式

【缺省级别】 15

【使用指导】 设置每个房间投屏允许的电视数量，终端数量。

【配置举例】 1：设置每个房间投屏允许的绑定的客户终端最大为 2 个，电视 ip 为 2 个，电视 mac 为 2 个。
这种情况下，upnp-proxy map key 最大允许配置的电视 ip 或者电视 mac 也只能是 2 个，超过的配置不成功。

```
Ruijie# configure terminal
Ruijie(config)# upnp-proxy child length 2 2 2
Ruijie(config)# end
```

2：恢复 upnp-proxy 每个房间绑定的终端数量，电视数量为缺省值。

```
Ruijie# configure terminal
Ruijie(config)# no upnp-proxy child
Ruijie(config)# end
```

【检验方法】 使用 show running-config 命令可以查看配置状态。

【提示信息】 -

【常见错误】 -

【平台说明】 -

8.3 enable

开启 upnp-proxy。
upnp-proxy enable

关闭 upnp-proxy。
no upnp-proxy enable

【参数说明】

参数	描述
-	-

【缺省配置】 缺省为关闭状态。

【命令模式】 全局模式

【缺省级别】 15

【使用指导】 若关闭，相关配置并不会删除， 并且仍可以进行配置，但服务并不会启用。

【配置举例】 1：开启 upnp-proxy。采用 mac 匹配模式。

```
Ruijie# configure terminal
Ruijie(config)# upnp-proxy enable
Ruijie(config)# end
```

2：关闭 upnp-proxy。

```
Ruijie# configure terminal
Ruijie(config)# no upnp-proxy enable
Ruijie(config)# end
```

【检验方法】 使用 show running-config 命令可以查看配置状态。

【提示信息】 -

【常见错误】 -

【平台说明】 -

8.4 isolate-region

添加限制网段。

upnp-proxy isolate-region { server | station } *ip_addr1 ip_addr2*

删除限制网段。

no upnp-proxy isolate-region { server | station } *ip_addr1 ip_addr2*

【参数说明】

参数	描述
ip_addr1	IP 网段起始地址
ip_addr2	IP 网段结束地址

【缺省配置】 缺省无配置。

【命令模式】 全局模式

【缺省级别】 15

【使用指导】 无

【配置举例】 1：添加服务器网段。

```
Ruijie# configure terminal
Ruijie(config)# upnp-proxy isolate-region server 20.20.20.1 20.20.20.254
```

2：添加终端网段。

```
Ruijie# configure terminal
Ruijie(config)# upnp-proxy isolate-region station 10.10.10.1 10.10.10.254
```

【检验方法】 使用 show running-config 命令可以查看配置状态。

【提示信息】 1：区间不正确——isolation region error !

2：区间重叠——isolation region overlap !

3：区间已满——isolation region full!

【常见错误】 -

【平台说明】 -

8.5 map

添加 key 与服务器的映射。

upnp-proxy map key *key_string* { [**sip1** *ip_addr1* **sip2** *ip_addr2 …***sip8** *ip_addr8*] | [**smac1** *mac_addr1* **smac2** *mac_addr2 …***smac8** *mac_addr8*] }

删除 key 与服务器的映射。

no upnp-proxy map key *key_string* [[**sip** *ip_addr*] | [**smac** *mac_addr*]]

【参数说明】

参数	描述
key_string	key 的字符串。
ip_addr	服务端的 IP 地址。
mac_addr	服务端的 mac 地址

【缺省配置】 缺省无配置。

【命令模式】 全局模式

【缺省级别】 15

【使用指导】 1：添加映射可以使用服务端的 IP 和 mac，如果配置了服务端 IP，就不能配置服务端 MAC。反之亦然。

2：一条 key 映射命令一次最多可以配置 8 个 IP 地址，可以选择配置 1 个到 8 个。

3：一条 key 映射命令一次最多可以配置 8 个 MAC 地址，可以选择配置 1 个到 8 个。

4：如果 key 重叠，则认为是更新当前的 key 与服务器的映射表项，则用本次的配置命令替换覆盖上次的配置命令。

5：删除 key 映射表项，可以选择删除 key 表项下的一个服务器 IP 映射，也可以选择删除整个 key 表项。但是不能选择删除 key 表项下的多个服务器 IP 映射

【配置举例】 1：添加 key 与服务器 IP 的映射。

```
Ruijie# configure terminal
Ruijie(config)# upnp-proxy map key 123 sip1 192.168.2.2
```

2：添加 key 与服务器多个 IP 的映射。

```
Ruijie# configure terminal
Ruijie(config)# upnp-proxy map key 123 sip1 192.168.2.2 sip2 192.168.2.3
```

3：添加 key 与服务器 MAC 的映射。

```
Ruijie# configure terminal
Ruijie(config)# upnp-proxy map key 123 smac1 f48e.388f.f50d
```

3：删除 key 与服务器 IP 的映射。

```
Ruijie# configure terminal
Ruijie(config)# no upnp-proxy map key 123 sip 192.168.2.2
```

4：删除 key 与服务器 mac 的映射。

```
Ruijie# configure terminal
Ruijie(config)# no upnp-proxy map key 123 smac f48e.388f.f50d
```

5：删除 key 下的全部服务器映射。

```
Ruijie# configure terminal
Ruijie(config)# no upnp-proxy map key 123
```

【检验方法】 使用 show running-config 命令可以查看配置状态。

【提示信息】 1：key 下映射已满——map full !
2：key 已满——key full !
3：输入参数错误——para error !

【常见错误】 -

【平台说明】 -

8.6 mode

配置 upnp-proxy 代理的匹配模式。
upnp-proxy mode mac

恢复缺省 upnp-proxy 代理的匹配模式，则匹配模式改为 ip 模式。
no upnp-proxy mode

【参数说明】

参数	描述
-	-

【缺省配置】 缺省为关闭状态。

【命令模式】 全局模式

【缺省级别】 15

【使用指导】 配置 upnp-proxy 代理的匹配模式为 mac 模式或者 ip 模式。
缺省模式为 IP 模式。如果配置 no upup_proxy mode，则恢复缺省模式。

在模式切换的时候，如果存在着和模式不匹配的映射表项，这些映射表项都将被删除。

【配置举例】 1：upnp-proxy 采用 mac 匹配模式。

```
Ruijie# configure terminal
Ruijie(config)# upnp-proxy mode mac
Ruijie(config)# end
```

2：关闭 upnp-proxy 匹配模式。该命令会恢复匹配模式为缺省的 ip 模式。

```
Ruijie# configure terminal
Ruijie(config)# no upnp-proxy mode
Ruijie(config)# end
```

【检验方法】 使用 show running-config 命令可以查看配置状态。

【提示信息】 -

【常见错误】 -

【平台说明】 -

8.7 offline-detect

设置投屏绑定的无流量解绑的时间，无流量解绑的流量阀值。
upnp-proxy offline-detect time-interval *time_value* **flowrate** *flowrate _value*

恢复缺省的投屏绑定的无流量解绑的时间参数(60 分钟)，无流量解绑的流量阀值参数（0 流量）。
upnp-proxy offline-detect

关闭投屏绑定的无流量解绑的功能。
no upnp-proxy offline-detect

【参数说明】

参数	描述
time_value	1-65535 投屏无流量解绑的最大时间，单位分钟，缺省是 60 分钟。
flowrate _value	1-81920 投屏无流量解绑的流量阀值，单位 bit/s，缺省是 0bit/s。

【缺省配置】 缺省为关闭状态。

【命令模式】 全局模式

【缺省级别】 15

【使用指导】 投屏如果没有和认证用户绑定，则需要通过无流量解绑来把已经绑定房间的投屏终端定期解绑掉，否则已经绑定房间的投屏终端会占用这个房间的投屏名额，导致后续进入这个房间的用户无法进行投屏，。
因此投屏在没有和认证用户绑定的情况下，缺省要配置 **upnp-proxy offline-detect。**这种情况下投屏绑定的终端如果 60 分钟都没有任何流量，就会被解除绑定。
投屏如果有和认证用户绑定，则可以通过认证用户的下线动作解除投屏绑定关系，因此这种情况下可以配置 **no upnp-proxy offline-detect** 关闭投屏无流量解绑的功能。

【配置举例】 1：设置投屏无流量解绑的最大时间为 120 分钟，无流量解绑的流量阀值是 0 bit/s

```
Ruijie# configure terminal
Ruijie(config)# upnp-proxy offline-detect time-interval 120 flowrate 0
Ruijie(config)# end
```

2：恢复缺省的投屏绑定的无流量解绑的时间参数(60 分钟)，无流量解绑的流量阀值参数（0 流量）。

```
Ruijie# configure terminal
Ruijie(config)# upnp-proxy offline-detect
Ruijie(config)# end
```

3：关闭投屏绑定的无流量解绑的功能。

```
Ruijie# configure terminal
Ruijie(config)# no upnp-proxy offline-detect
Ruijie(config)# end
```

【检验方法】 使用 show running-config 命令可以查看配置状态。

【提示信息】 -

【常见错误】 -

【平台说明】 -

8.8 unicast

配置 upnp-proxy 代理放行客户终端投屏软件的单播报文。
upnp-proxy unicast permit

恢复缺省 upnp-proxy 代理的处理方式，不放行客户终端投屏软件的单播报文。
no upnp-proxy unicast permit

【参数说明】

参数	描述
-	-

【缺省配置】 缺省为关闭状态。

【命令模式】 全局模式

【缺省级别】 15

【使用指导】 目前很多投屏软件，在完成了投屏发现过程，就会把投屏电视的 IP 地址记录下来，下次开启投屏软件的时候，就会不进行投屏发现，直接向电视发起投屏的单播请求。这样就会导致之前已经解除投屏绑定关系的客户终端，还是能够看到曾经投屏过的电视，无法达到投屏隔离电视的效果。
因此投屏代理缺省处理方式，对于已经解除绑定关系的客户终端，是会阻断该客户终端和之前绑定的电视的单播请求报文。
当然在某些特殊场合，可能客户希望不阻断这种单播报文，因此可以通过该命令开关来设置不阻断。

【配置举例】 1：配置 upnp-proxy 代理放行客户终端投屏软件的单播报文。

```
Ruijie# configure terminal
Ruijie(config)# upnp-proxy unicast permit
Ruijie(config)# end
```

2：恢复缺省 upnp-proxy 代理的处理方式，不放行客户终端投屏软件的单播报文。

```
Ruijie# configure terminal
Ruijie(config)# no upnp-proxy unicast permit
Ruijie(config)# end
```

【检验方法】 使用 show running-config 命令可以查看配置状态。

【提示信息】 -

【常见错误】 -

【平台说明】 -

8.9 set

设置投屏报文处理的单 IP 最大处理速率，缺省是每 5 秒最多处理 20 个报文。
upnp-proxy set { time *time_value* | **volume** *volume _value* **}**

恢复缺省的投屏报文处理的单 IP 最大处理速率，缺省是每 5 秒最多处理 20 个报文。
no upnp-proxy set

【参数说明】

参数	描述
time_value	1-255 投屏报文处理的最大时间间隔，缺省是 5 秒

volume _value	1-255　投屏报文处理的最大时间间隔内的最大报文个数，缺省是 20 个

【缺省配置】 缺省为关闭状态。

【命令模式】 全局模式

【缺省级别】 15

【使用指导】 若关闭，则恢复缺省的投屏报文处理的单 IP 最大处理速率，。

【配置举例】 1：设置每 10 秒最多处理 40 个报文.

```
Ruijie# configure terminal
Ruijie(config)# upnp-proxy set time 10
Ruijie(config)# upnp-proxy set volume 40
Ruijie(config)# end
```

2：恢复缺省的投屏报文处理的单 IP 最大处理速率。

```
Ruijie# configure terminal
Ruijie(config)# no upnp-proxy set
Ruijie(config)# end
```

【检验方法】 使用 show running-config 命令可以查看配置状态。

【提示信息】 -

【常见错误】 -

【平台说明】 -

8.10 show upnp-proxy config

显示 upnp-proxy 相关配置信息。

show upnp-proxy config

【参数说明】

参数	描述
-	-

【缺省配置】 -

【命令模式】 特权模式

【缺省级别】 15

【使用指导】 可以查看服务是否开启，以及当前配置的服务端映射。

【配置举例】 显示配置信息。采用 json 格式呈现。

```
Ruijie# show upnp-proxy status
{ "data": { "enable": 1, "service_list": [ { "id": "102", "ipmac": [ "bc1c.81b8.ae12",
"bc1c.81b8.ef4a", "bc1c.81b8.ef35", "bc1c.81b8.ea4d", "bc1c.81b8.e123" ] } ] }, "mode": 1, "msg":
0, "total": 1, "max": 500 }
```

【检验方法】 -

【提示信息】 -

【常见错误】 -

【平台说明】 -

8.11 show upnp-proxy isolate-region

显示配置的互访限制网段信息。

show upnp-proxy isolate-region

【参数说明】

参数	描述
-	-

【缺省配置】 -

【命令模式】 特权模式

【缺省级别】 15

【使用指导】 可以查看服务是否开启，以及当前配置的服务端、客户端映射。

【配置举例】 显示状态信息。采用 json 格式呈现。

```
Ruijie# show upnp-proxy isolate-region
{ "data": { "region_list": [ { "type": "server", "start": "20.20.20.1", "end": "20.20.20.254" },
{ "type": "station", "start": "10.10.10.1", "end": "10.10.10.254" } ] }, "msg": 0, "code": 0,
"server_total": 1, "station_total": 1, "server_max": 5, "station_max": 5 }
```

【检验方法】 -

【提示信息】 -

【常见错误】 -

【平台说明】 -

8.12 show upnp-proxy status

显示 upnp-proxy 相关状态信息，只会显示已经建立投屏绑定关系的客户终端和电视的映射关系。这个命令是采用 json 格式显示。

show upnp-proxy status

【参数说明】

参数	描述
-	-

【缺省配置】 -

【命令模式】 特权模式

【缺省级别】 15

【使用指导】 可以查看服务是否开启，以及当前配置的服务端、客户端映射。

【配置举例】 显示状态信息。采用 json 格式呈现。

```
Ruijie# show upnp-proxy status
{ "data": { "enable": 1, "service_list": [ { "id": "123", "service_ip": [ "192.168.2.3" ], "sta":
[ { "ip": "192.168.1.2", "name": "test" }, { "ip": "10.10.10.15", "name": "user" }, { "ip":
"20.20.20.4", "name": "ipad" } ] } ] }, "code": 0, "msg": 0, "total": 1, "max": 500 }
```

【检验方法】 -

【提示信息】 -

【常见错误】 -

【平台说明】 -

8.13 show upnp-proxy vty

显示 upnp-proxy 相关状态信息，只会显示已经建立投屏绑定关系的客户终端和电视的映射关系。这个命令是采用 cli 格式显示。

show upnp-proxy vty

【参数说明】

参数	描述
-	-

【缺省配置】 -

【命令模式】 特权模式

【缺省级别】 15

【使用指导】 detect_num 是表示这个客户终端的解绑的老化计时器，单位颗粒度是 30 秒，1 表示 30 秒，2 表示 60 秒。在这里客户终端老化计时器达到 120，也就是 60 分钟，就会被解除绑定，从绑定关系表中删除。

【配置举例】 显示状态信息。采用 cli 格式呈现。

```
Ruijie#show upnp-proxy vty
keymax: 500    keynum: 4    mode: 0        detectlimit:120
child length: 2    tvip length: 2    tvip length: 2
keyid                          ip/mac                          sta
detect_num
704                            20.20.20.4                      10.10.10.3                      1
703                            20.20.20.3                      10.10.10.2                      1
705                            20.20.20.5                      10.10.10.4                      0
705                            20.20.20.6                      10.10.10.4                      0
```

【检验方法】 -

【提示信息】 -

【常见错误】 -

【平台说明】 -

命令参考-IPV6

本分册介绍 IPV6 相关内容，包括以下章节：

1. IPV6

1 IPv6

命令	作用
clear ipv6 neighbors	清除动态学习到的邻居。
clear ipv6 path-mtu	清除动态路径 MTU
ipv6 address	配置 IPV6 地址。
ipv6 address autoconfig	开启接口 IPv6 无状态自动配置地址。
ipv6 icmp error-interval	配置 ICMPv6 差错报文的发送速率。
ipv6 enable	开启接口 IPv6 协议。
Ipv6 gateway	配置 MGMT 接口的缺省网关
ipv6 general-prefix	配置 IPv6 通用前缀。
ipv6 hop-limit	配置发送单播报文的跳数。
ipv6 mtu	配置 IPv6 包最大传输单元（MTU）。
ipv6 nd cache interface-limit	配置限制接口的邻居学习最大数量
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。
ipv6 nd dad retry	配置重复地址冲突检测的间隔。
ipv6 nd managed-config-flag	配置路由器公告报文中的“**managed address configuration**”标志位。
ipv6 nd max-opt	配置 ND 支持的扩展首部支持限制。
ipv6 nd ns-interval	配置接口上邻居请求(NS)的重传间隔。
ipv6 nd other-config-flag	配置路由器公告报文中的“**other stateful configuration**”标志位。
ipv6 nd prefix	配置路由器公告报文(RA)中所包含的地址前缀。
ipv6 nd ra-hoplimit	配置接口上发送的路由器公告(RA)报文的跳数。
ipv6 nd ra-interval	配置接口上邻居请求(NS)的重传间隔。
ipv6 nd ra-lifetime	配置接口上发送的路由器公告(RA)报文中的 “路由器生存期” 。
ipv6 nd ra-mtu	配置接口上发送的路由器公告(RA)报文的 MTU。
ipv6 nd reachable-time	配置邻居被认为可到达的时间。
ipv6 nd stale-time	配置邻居 stale 状态的执行时间。
Ipv6 nd suppress-auth-vlan-ns	抑制在 SVI 口上往认证 vlan 发送广播邻居请求（NS）报文。
ipv6 nd suppress-ra	抑制在接口上发送路由器公告(RA)报文。
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
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
Ipv6 nd unresolved	配置未解析的邻居表项的最大数量
ipv6 neighbor	配置一个静态邻居。
ipv6 ns-linklocal-src	发送邻居请求时将强制使用链路本地地址作为源地址。
ipv6 path-mtu	配置静态路径 MTU。
ipv6 path-mtu age	配置动态路径 MTU 的老化时间
ipv6 redirects	开启 ICMPv6 重定向。
ipv6 source-route	配置设备转发带有路由首部的 IPv6 报文。
ipv6 unnumbered	配置接口借用特定接口的 ipv6 地址作为本地发包的源地址。

peer default ipv6 pool	配置设备送路由器公告(RA)报文能从前缀池获取一个前缀来公告
show ipv6 address	显示 IPv6 地址的信息。
show ipv6 general-prefix	显示通用前缀中的前缀信息。
show ipv6 interface	显示 IPV6 接口的信息。
show ipv6 neighbors	显示 IPV6 的邻居表。
show ipv6 neighbors statistics	显示 IPv6 报文的统计信息。
show ipv6 neighbor statistics per-mac	查看每个 MAC 地址的邻居表项的数量
show ipv6 packet statistics	显示 IPv6 报文的统计信息。
show ipv6 path-mtu	显示路径 MTU 的信息。
show ipv6 path-mtu statistics	显示路径 MTU 的统计信息。
show ipv6 raw-socket	显示 IPv6 原始套接字。
show ipv6 routers	显示邻居路由器和路由公告信息。
show ipv6 sockets	显示所有 IPv6 套接字。
show ipv6 udp	显示 IPv6 UDP 套接字。

1.1 clear ipv6 neighbors

清除动态学习到的邻居。

clear ipv6 neighbors [**vrf** *vrf-name*] [**oob**] [*interface-id*]

【参数说明】

参数	描述
vrf-name	VRF 名称。缺省不指定 vrf 名称，代表清除全局的 ipv6 邻居表项
oob	带 oob 关键字清除 MGMT 口上所有通过邻居发现动态学习到的邻居
interface-id	接口名称，表示删除指定接口的动态邻居

【命令模式】 特权模式

【缺省级别】 14

【使用指导】

⚠ 静态配置的不会被清除；网关认证模式下，认证 vlan 下的动态邻居不会被删除。

【配置举例】 1：清除所有通过动态学习到的邻居。

```
Ruijie# clear ipv6 neighbors
```

2：清除 MGMT 口上所有通过动态学习的邻居。

```
Ruijie# clear ipv6 neighbors oob
```

3：清除 gigabitEthernet 0/1 口上所有动态学习的邻居。

```
Ruijie# clear ipv6 neighbors gigabitEthernet 0/1
```

【提示信息】 -

【平台说明】 NBR6205-E、NBR6135-E、NBR6210-E、NBR6215-E 支持 MGMT 口；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 MGMT 口。

1.2 clear ipv6 path-mtu

清除动态路径 MTU。

clear ipv6 path-mtu [**vrf** *vrf-name*] [*ipv6-address*]

清除所有动态路径 MTU，包括全局和所有 VRF。

clear ipv6 path-mtu all

【参数说明】

参数	描述
vrf *vrf-name*	VRF 名称。如果不输入 VRF 名称，表示清除全局的动态路径 MTU
ipv6-address	IPv6 地址，可以是单播或者组播地址

【命令模式】 特权模式

【缺省级别】 14

【使用指导】 -

【配置举例】 1：清除全局的所有动态路径 MTU。

```
Ruijie# clear ipv6 path-mtu
```

2：清除全局和所有 VRF 的动态路径 MTU。

```
Ruijie# clear ipv6 path-mtu all
```

【检验方法】 使用 **show ipv6 path-mtu dynamic** 查看动态路径 MTU。

【提示信息】 -

【平台说明】 -

1.3 ipv6 address

配置 IPv6 地址，不使用通用前缀。

ipv6 address *ipv6-address* | *prefix-length*

删除指定 IPv6 地址。
no ipv6 address *ipv6-address* | *prefix-length*

配置 eui-64 格式的 IPv6 地址。
ipv6 address *ipv6-prefix* | *prefix-length* **eui-64**

删除指定的 eui-64 格式的 IPv6 地址。
no ipv6 address *ipv6-prefix* | *prefix-length* **eui-64**

使用通用前缀来配置 IPv6 地址，包括 eui-64 格式的地址。
ipv6 address *prefix-name sub-bits* | *prefix-length* [**eui-64**]

删除指定的使用通用前缀配置的 IPv6 地址，包括 eui-64 格式的地址。
no ipv6 address *prefix-name sub-bits*| *prefix-length* [**eui-64**]

删除接口所有 IPv6 地址
no ipv6 address

【参数说明】

参数	描述
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。

【缺省配置】 无地址

【命令模式】 接口模式

【缺省级别】 14

【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。

【配置举例】 1：下面的例子是在 GigabitEthernet 0/1 口手工配置 IPv6 地址。

```
Ruijie(config-if-GigabitEthernet 0/1)# ipv6 address 2001:1::1/64
Ruijie(config-if-GigabitEthernet 0/1)# no ipv6 address 2001:1::1/64
Ruijie(config-if-GigabitEthernet 0/1)# ipv6 address 2002:1::/64 eui-64
Ruijie(config-if-GigabitEthernet 0/1)# no ipv6 address 2002:1::/64 eui-64
```

2：下面的例子是在 GigabitEthernet 0/1 口使用通用前缀配置地址。

```
Ruijie(config-if-GigabitEthernet 0/1)# ipv6 address my-prefix 0:0:0:7272::72/64
```

假设通用前缀 my-prefix 配置的前缀是 2001:1111:2222::/48，那么生成的接口 IPv6 地址是 2001:1111:2222:7272::72/64。

【检验方法】 使用 **show ipv6 address** 和 **show ipv6 interface** 查看已经成功配置的 IPv6 地址。

【提示信息】 -

【常见错误】 -

【平台说明】 -

1.4 ipv6 address autoconfig

开启接口 IPv6 无状态自动配置地址。
ipv6 address autoconfig [**default**]

删除接口 IPv6 无状态自动配置地址。
no ipv6 address autoconfig

【参数说明】

参数	描述
default	可选参数。为无状态自动配置地址生成一条缺省路由。注意整台设备只允许一个三层接口使用 **default** 关键字。缺省情况下，不生成缺省路由。

【缺省配置】 关闭

【命令模式】 接口模式

【缺省级别】 14

【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，那么不允许在接口上开启 IPv6 无状态地址自动配置功能，必须先给多协议 VRF 配置 IPv6 地址族，然后才能开启 IPv6 无状态地址自动配置功能。

无状态自动地址配置是指当设备收到 RA(路由公告)报文时 ,可以使用 RA 报文中的前缀信息自动生成 EUI-64 格式的接口地址。
如果收到的 RA 报文中含有“其它配置”的标志，那么该接口将通过 DHCPv6 获取这些“其它配置”。 “其它配置”通常指 DNS 服务器的 IPv6 地址、NTP 服务器的 IPv6 地址等。

【配置举例】 1：在 GigabitEthernet 0/1 接口上开启接口 IPV6 无状态自动配置地址并生成一条缺省路由。

```
Ruijie(config-if-GigabitEthernet 0/1)# ipv6 address autoconfig default
```

2：删除 GigabitEthernet 0/1 接口 IPV6 无状态自动配置地址。

```
Ruijie(config-if-GigabitEthernet 0/1)# no ipv6 address autoconfig
```

【检验方法】 通过 **show ipv6 address** 和 **show ipv6 interface** 查看成功获取到的 IPv6 地址。

【提示信息】 -

【常见错误】 -

【平台说明】 -

1.5 ipv6 icmp error-interval

配置 ICMPv6 报文太大消息的发送速率。
ipv6 icmp error-interval too-big *milliseconds* [*bucket-size*]

配置其它 ICMPv6 差错报文的发送速率。
ipv6 icmp error-interval *milliseconds* [*bucket-size*]

把 ICMPv6 报文太大消息的发送速率恢复成缺省值。
no ipv6 icmp error-interval too-big *milliseconds* [*bucket-size*]

把其它 ICMPv6 差错报文的发送速率恢复成缺省值。
no ipv6 icmp error-interval *milliseconds* [*bucket-size*]

【参数说明】

参数	描述

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。

【缺省配置】 100 毫秒发送 10 个。

【命令模式】 全局模式

【缺省级别】 14

【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。注意：ICMPv6 重定向报文不属于 ICMPv6 差错报文，我司把其它 ICMPv6 差错报文和 ICMPv6 重定向报文一起限速。
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。

【配置举例】 1：配置 ICMPv6 报文太大消息的发送速率为 1 秒 100 个。

```
Ruijie(config)# ipv6 icmp error-interval too-big 1000 100
```

2：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 1000 10
```

【检验方法】 使用 **show running-config** 查看配置。

【提示信息】 -

【常见错误】 -

【平台说明】 -

1.6 ipv6 enable

开启接口 IPv6 协议。
ipv6 enable

关闭接口 IPv6 协议。

no ipv6 enable

【参数说明】

参数	描述
-	-

【缺省配置】 关闭

【命令模式】 接口模式

【缺省级别】 14

【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。

【配置举例】 1：在 GigabitEthernet 0/1 接口上开启 IPV6 协议功能。

```
Ruijie(config-if-GigabitEthernet 0/1)# ipv6 enable
```

【检验方法】 使用 **show ipv6 address** 和 **show ipv6 interface**,如果存在链路本地地址，表明成功部署了 ipv6 enable。

【提示信息】 -

【常见错误】 -

【平台说明】 -

1.7 ipv6 gateway

使用该命令配置 MGMT 接口的缺省网关

ipv6 gateway *ipv6-address*

【参数说明】

参数	描述
ipv6-address	MGMT 接口 IPv6 通信的缺省网关地址

【缺省配置】 无缺省配置

【命令模式】 接口模式

【缺省级别】 14

【使用指导】 MGMT 接口的类型是 MGMT，编号固定为 0。

【配置举例】 下例是配置 MGMT 接口的缺省网关地址

```
Ruijie(config)# interface mgmt 0
Ruijie(config-int)# ipv6 gateway 2001:1::1
Ruijie(config-int)# exit
Ruijie(config)#
```

【检验方法】 使用 **show run** 查看配置是否成功。

【提示信息】 -

【常见错误】 -

【平台说明】 -

1.8 ipv6 general-prefix

配置 IPv6 通用前缀。
ipv6 general-prefix *prefix-name ipv6-prefix* | *prefix-length*

删除 IPv6 通用前缀。
no ipv6 general-prefix *prefix-name ipv6-prefix* | *prefix-length*

【参数说明】

参数	描述
prefix-name	通用前缀的名字。
ipv6-prefix	通用前缀的网络前缀值。这个值的表示法要遵循 RFC4291 描述的冒号表示法。
prefix-length	通用前缀的长度。

【缺省配置】 未配置

【命令模式】 全局配置模式

【缺省级别】 14

【使用指导】 使用通用前缀可以方便网络编号。因为通用前缀定义出一个前缀，很多更长的特定前缀可以引用它。当通用前

缀变化时，这些引用通用前缀的特定前缀就会跟着变化。网络编号变化时，只要修改一下通用前缀即可。
一个通用前缀可以包含多个前缀。
这些更长的特定前缀通常用在接口的 IPv6 地址配置上。

【配置举例】 1：配置一个通用前缀叫 my-prefix。

```
Ruijie(config)# ipv6 general-prefix my-prefix 2001:1111:2222::/48
```

【检验方法】 通过 **show ipv6 general-prefix** 可以观察到已经成功配置的通用前缀。

【提示信息】 -

【常见错误】 -

【平台说明】 -

1.9 ipv6 hop-limit

配置发送单播报文的跳数。
ipv6 hop-limit *value*

恢复缺省配置。
no ipv6 hop-limit

【参数说明】

参数	描述
value	跳数值，范围是 1 --- 255。

【缺省配置】 默认值是 64。

【命令模式】 全局模式

【缺省级别】 14

【使用指导】 该命令只对单播报文生效，对多播报文无效。

【配置举例】 1：配置发送单播报文的跳数为 100。

```
Ruijie(config)# ipv6 hop-limit 100
```

【检验方法】 -

【提示信息】 -

【常见错误】 -

【平台说明】 -

1.10 ipv6 mtu

配置 IPv6 包最大传输单元（MTU）。
ipv6 mtu *bytes*

恢复缺省配置。
no ipv6 mtu

【参数说明】

参数	描述
bytes	IPv6 包最大传输单元，以字节为单位，范围 1280~1500(最大值受接口 mtu 限制，不同接口类型最大值不同)。

【缺省配置】 缺省与接口命令 mtu 配置的值相同。

【命令模式】 接口模式

【缺省级别】 14

【使用指导】 如果一个 IPv6 报文超过 IPv6 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 IPv6 MTU 一定要一致。

【配置举例】 1：将 GigabitEthernet 0/1 接口的 IPv6 MTU 值设为 1400 字节。

```
Ruijie(config)# interface GigabitEthernet 0/1
Ruijie(config-if-GigabitEthernet 0/1)# ipv6 mtu 1400
```

【检验方法】 通过 **show ipv6 interface** 查看接口上配置的 mtu 的值。

【提示信息】 -

【常见错误】 -

【平台说明】 -

1.11 ipv6 nd cache interface-limit

配置限制接口学习的邻居数量。
ipv6 nd cache interface-limit *value*

恢复缺省配置。
no ipv6 nd cache interface-limit

【参数说明】

参数	描述
value	特定接口所能学习的邻居最大限制，包括静态配置和动态学习的邻居，取值范围为 0-设备支持的邻居表项容量，0 表示不限制接口学习邻居数量。

【缺省配置】 缺省为 0，表示不限制接口学习邻居数量。

【命令模式】 接口模式

【缺省级别】 14

【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】 1：将 GigabitEthernet 0/1 接口邻居学习数量限制为 100。

```
Ruijie(config)# interface GigabitEthernet 0/1
Ruijie(config-if-GigabitEthernet 0/1)# ipv6 nd cache interface-limit 100
```

【检验方法】 通过 **show run** 查看配置是否生效。

【提示信息】 -

【常见错误】 -

【平台说明】 -

1.12 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。
ipv6 nd dad attempts *value*

恢复缺省配置。
no ipv6 nd dad attempts

【参数说明】

参数	描述
value	邻居请求(NS)报文的数量。当设置的值为 0 时表示阻止为该接口上的 Ipv6 地址启动地址冲突检测。范围：0-600。缺省为 1。

【缺省配置】 1

【命令模式】 接口模式

【缺省级别】 14

【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。

【配置举例】 1：在 GigabitEthernet 0/1 接口上配置冲突检测时连续发送 3 个邻居请求报文。

```
Ruijie(config-if-GigabitEthernet 0/1)# ipv6 nd dad attempts 3
```

【检验方法】 通过 **show ipv6 interface** 查看接口上配置的 DAD 重传次数。

【提示信息】 -

【常见错误】 -

【平台说明】 -

1.13 ipv6 nd dad retry

配置重复地址冲突检测间隔。
ipv6 nd dad retry *value*

恢复缺省配置。
no ipv6 nd dad retry

【参数说明】

参数	描述
value	地址冲突后，重新进行冲突检测的时间间隔，默认为 60s，配置成 0，关闭重新进行冲突检测功能。

【缺省配置】 1

【命令模式】 全局模式

【缺省级别】 14

【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，如果检测到冲突了，那么设备将不能接收目的地址为该地址的 ipv6 报文。该命令在配置的时间到期后会对已冲突的地址重新进行一遍地址冲突检测，如果重新检测没有冲突，该地址将可以正常使用。

【配置举例】 1：修改重复地址冲入检测间隔为 10s。

```
Ruijie(config)# ipv6 nd dad retry 10
```

【检验方法】 通过 **show run** 可以看到配置是否生效。

【提示信息】 -

【常见错误】 -

【平台说明】 -

1.14 ipv6 nd managed-config-flag

配置路由器公告报文中的“**managed address configuration**”标志位。
ipv6 nd managed-config-flag

删除该标志位。
no ipv6 nd managed-config-flag

【参数说明】

参数	描述
-	-

【缺省配置】 缺省无配置。

【命令模式】 接口模式

【缺省级别】 14

【使用指导】 该标志位的设置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。如果配置了该标志位，

将使用全状态自动配置来获得地址，否则不使用。

【配置举例】 1：在 GigabitEthernet 0/1 接口上配置路由器公告报文中的“**managed address configuration**”标志位。

```
Ruijie(config-if-GigabitEthernet 0/1)# ipv6 nd managed-config-flag
```

【检验方法】 通过 **show ipv6 interface** 查看接口上配置的有状态地址配置标志。

【提示信息】 -

【常见错误】 -

【平台说明】 -

1.15 ipv6 nd max-opt

配置设备处理 ND 选项数量限制。
ipv6 nd max-opt *value*

恢复缺省配置。
no ipv6 nd max-opt

【参数说明】

参数	描述
value	支持的选项个数，值的范围： 1-100。

【缺省配置】 缺省处理的选项个数为 10。

【命令模式】 全局配置模式

【缺省级别】 14

【使用指导】 配置设备处理 ND 选项数量限制，比如源链路层地址选项，MTU 选项，重定向选项，前缀选项。

【配置举例】 1：配置设备处理 ND 选项限制为 20。

```
Ruijie(config)# ipv6 nd max-opt 20
```

【检验方法】 通过 **show run** 查看配置是否生效。

【提示信息】 -

【常见错误】 -

【平台说明】 -

1.16 ipv6 nd ns-interval

配置接口上邻居请求(NS)的重传间隔。
ipv6 nd ns-interval *milliseconds*

恢复缺省配置。
no ipv6 nd ns-interval

【参数说明】

参数	描述
milliseconds	邻居请求的重传间隔，以毫秒为单位，值的范围： 1000-4294967295。

【缺省配置】 用于填入设备发送的路由器公告报文(RA)中时，缺省值为 0（表示未指定）；
用于控制设备自身发送邻居请求的重传间隔时，缺省值为 1000 毫秒。

【命令模式】 接口模式

【缺省级别】 14

【使用指导】 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。建议不要将该值设置得太小。

【配置举例】 1：在 GigabitEthernet 0/1 接口上配置邻居请求的重传间隔为 2 秒。

```
Ruijie(config-if-GigabitEthernet 0/1)# ipv6 nd ns-interval 2000
```

【检验方法】 通过 **show ipv6 interface** 查看接口上配置的 NS 重传时间间隔。

【提示信息】 -

【常见错误】 -

【平台说明】 -

1.17 ipv6 nd other-config-flag

配置路由器公告报文中的“**other stateful configuration**”标志位。
ipv6 nd other-config-flag

删除该标志位。

no ipv6 nd other-config-flag

【参数说明】

参数	描述
-	-

【缺省配置】 缺省无配置

【命令模式】 接口模式

【缺省级别】 14

【使用指导】 设置了此标志位后，设备发出的路由器公告报文的这个标志位被置位。主机收到这个标志位后，将使用 dhcpv6 来获取除 IPv6 地址以外的其他信息进行自动配置。当 managed address configuration 被设置时，默认 other stateful configuration 也被设置。

【配置举例】 1：在 GigabitEthernet 0/1 接口上配置路由器公告报文中的“**other stateful configuration**”标志位。

```
Ruijie(config-if-GigabitEthernet 0/1)# ipv6 nd other-config-flag
```

【检验方法】 通过 **show ipv6 interface** 查看到接口上是否配置了有状态配置标志（除地址外的其它配置）。

【提示信息】 -

【常见错误】 -

【平台说明】 -

1.18 ipv6 nd prefix

配置路由器公告报文(RA)中所包含的地址前缀。

ipv6 nd prefix { *ipv6-prefix*/*prefix-length* | **default** } [[*valid-lifetime* { **infinite** | *preferred-lifetime* }] | [**at** *valid-date preferred-date*] | [**infinite { infinite** | *preferred-lifetime* }]] [**no-advertise**] | [[**off-link**] [**no-autoconfig**] | [**pool** *pool-name*]]

删除所配置的前缀或者恢复前缀配置参数的缺省值。

no ipv6 nd prefix { *ipv6-prefix/prefix-length* | **default** }

【参数说明】

参数	描述
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。
pool *pool-name*	接口绑定的前缀池，用于为不同的用户分配不同的 IPv6 前缀

【缺省配置】 缺省公告的前缀是在该接口上通过 IPV6 address 命令配置的前缀。配置的前缀在路由器公告报文中的缺省参数如下：

valid-lifetime：2592000 秒 (30 天)

preferred-lifetime：604800 秒 (7 天),

前缀被公告，并且可以用于 on-link 判断，可以用于地址自动配置。

【命令模式】 接口模式

【缺省级别】 14

【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-date preferred-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。

【配置举例】 1：在接口 SVI 1 上增加一个前缀。

```
Ruijie(config)#interface vlan 1
Ruijie(config-if)# ipv6 nd prefix 2001::/64 infinite 2592000
```

2：设置接口 SVI 1 上的前缀的缺省参数（不可用于地址自动配置）。

```
Ruijie(config)# interface vlan 1
Ruijie(config-if)# ipv6 nd default no-autoconfig
```

在该情况下如果增加一个前缀，不指定任何参数，那么将使用缺省的配置参数即该前缀也是不可用于地址自动配置的。

【检验方法】 通过 **show ipv6 interface** [*interface-id*] **ra-info** 查看路由器公告报文中的前缀信息

【提示信息】 -

【常见错误】 -

【平台说明】 -

1.19 ipv6 nd ra-hoplimit

配置接口上发送的路由器公告(RA)报文的跳数。
ipv6 nd ra-hoplimit *value*

恢复缺省配置。
no ipv6 nd ra-hoplimit

【参数说明】

参数	描述
value	路由器公告(RA)报文跳数的值，取值范围 0-255。 缺省是 64 跳。

【缺省配置】 缺省值是 64。

【命令模式】 接口模式

【缺省级别】 14

【使用指导】 -

【配置举例】 1：在 GigabitEthernet 0/1 接口上配置发送路由器公告报文的跳数为 110。

```
Ruijie(config-if-GigabitEthernet 0/1)# ipv6 nd ra-hoplimit 110
```

【检验方法】 通过 **show ipv6 interface** [*interface-id*] **ra-info** 查看路由器公告报文中的跳数限制信息。

【提示信息】 -

【常见错误】 -

【平台说明】 -

1.20 ipv6 nd ra-interval

配置接口上发送的路由器公告(RA)报文的间隔。
ipv6 nd ra-interval { *seconds* | **min-max** *min_value max_value* }

恢复缺省配置。
no ipv6 nd ra-interval

【参数说明】

参数	描述
seconds	路由器公告(RA)公告报文的发送间隔。以秒为单位。缺省是 200 秒。
min-max	设置通告报文发送间隔的最小值和最大值。
min_value	设置通告报文发送间隔的最小值。
max_value	设置通告报文发送间隔的最大值。

【缺省配置】 200 秒，实际发送报文的间隔在 200 秒上下浮动 20%。

【命令模式】 接口模式

【缺省级别】 14

【使用指导】 如果该设备充当缺省路由设备时，那么设置的间隔值不能够大于路由器生存期的时间。另外，为了防止链路上的其它设备同时发送路由器公告报文而占用网络带宽，所以实际发送报文的间隔将在该值上浮动百分之二十。如果指定关键字 **min-max**，那么实际发送报文的间隔将在最小值和最大值之间随机选择一个值。

【配置举例】 1：在 GigabitEthernet 0/1 接口上配置路由器公告报文的发送间隔为 110 秒。

```
Ruijie(config-if-GigabitEthernet 0/1)# ipv6 nd ra-interval 110
```

2：在 GigabitEthernet 0/1 接口上配置路由器公告后文的发送间隔在 110 秒到 120 秒之间。

```
Ruijie(config-if-GigabitEthernet 0/1)# ipv6 nd ra-interval min-max 110 120
```

【检验方法】 通过 **show ipv6 interface** [*interface-id*] **ra-info** 查看接口发送 RA 报文的时间间隔

【提示信息】 -

【常见错误】 -

【平台说明】 -

1.21 ipv6 nd ra-lifetime

配置接口上发送的路由器公告(RA)报文中的“路由器生存期”。
ipv6 nd ra-lifetime *seconds*

恢复缺省配置。
no ipv6 nd ra-lifetime

【参数说明】

参数	描述
seconds	该设备作为该接口上的缺省设备的有效时间，取值范围 0-9000。 缺省是 1800 秒。

【缺省配置】 1800 秒

【命令模式】 接口模式

【缺省级别】 14

【使用指导】 “路由器生存期”字段存在于每个路由器公告(RA)报文中，该值指明了该接口所在的链路上主机可以将该设备作为缺省设备的时间。如果设置的值为 0 表示不再被当作缺省设备。当设置非 0 值时要注意该值必须大于等于设备发送路由器公告(RA)报文的间隔(ra-interval)。

【配置举例】 1：在 GigabitEthernet 0/1 接口上配置发送路由器公告报文的生存期为 2000 秒。

```
Ruijie(config-if-GigabitEthernet 0/1)# ipv6 nd ra-lifetime 2000
```

【检验方法】 通过 **show ipv6 interface** [*interface-id*] **ra-info** 查看路由器公告报文中的此路由器的生命期。

【提示信息】 -

【常见错误】 -

【平台说明】 -

1.22 ipv6 nd ra-mtu

配置接口上发送的路由器公告(RA)报文的 MTU。
ipv6 nd ra-mtu *value*

恢复缺省配置。
no ipv6 nd ra-mtu

【参数说明】

参数	描述
value	路由器公告(RA)报文的 MTU 字段的值，取值范围 0-4294967295。缺省与 IPv6 MTU 保持一致。

【缺省配置】 网络接口的 IPv6 MTU 值。

【命令模式】 接口模式

【缺省级别】 14

【使用指导】 如果指定为 0，路由器公告就不会带 MTU 选项。

【配置举例】 1：在接口上配置发送路由器公告报文的 MTU 为 1400 字节。

```
Ruijie(config -if)# ipv6 nd ra-mtu 1400
```

【检验方法】 通过 **show ipv6 interface** [*interface-id*] **ra-info** 查看路由器公告报文中的 mtu 信息。

【提示信息】 -

【常见错误】 -

【平台说明】 -

1.23 ipv6 nd reachable-time

配置邻居被认为可到达的时间。
ipv6 nd reachable-time *milliseconds*

恢复缺省配置
no ipv6 nd reachable-time

【参数说明】

参数	描述
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。

【缺省配置】 在路由器公告报文(RA)中缺省值为 0（表示未指定），设备自己在邻居发现行为中邻居被认为可到达的持续时间为 30000ms(30 秒)。

【命令模式】 接口模式

【缺省级别】 14

【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。

【配置举例】 1：在 GigabitEthernet 0/1 接口上配置邻居被认为可到达的时间为 1000 秒。

```
Ruijie(config-if-GigabitEthernet 0/1)# ipv6 nd reachable-time 1000000
```

【检验方法】 通过 **show ipv6 interface** 查看路由器公告报文中的路由器可达时间值

【提示信息】 -

【常见错误】 -

【平台说明】 -

1.24 ipv6 nd stale-time

配置邻居保持 stale 状态的时间。
ipv6 nd stale-time *seconds*

恢复缺省配置
no ipv6 nd stale-time

【参数说明】

参数	描述
seconds	邻居 stale 状态保持的时间，以秒为单位，范围： 0-86400。 缺省为 3600 秒。

【缺省配置】 邻居状态迁移到 stale 状态的持续时间，默认为 1h。

【命令模式】 全局模式

【缺省级别】 14

【使用指导】 该配置可修改 stale 状态的持续时间，该时间过期后进行邻居不可达检测。配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。

【配置举例】 1：配置设备邻居的 stale 执行时间为 600s。

```
Ruijie(config)# ipv6 nd stale-time 600
```

【检验方法】 通过 **show run** 可以查看配置是否生效

【提示信息】 -

【常见错误】 -

【平台说明】 -

1.25 ipv6 nd suppress-auth-vlan-ns

抑制在 SVI 口上往认证 vlan 发送广播邻居请求（NS）报文。
ipv6 nd suppress-auth-vlan-ns

允许往认证 vlan 发送广播邻居请求报文。
no ipv6 nd suppress-auth-vlan-ns

【参数说明】

参数	描述
-	-

【缺省配置】 在支持 IPv6 的 Supervlan 接口上将不会往认证子网发送广播邻居请求报文。

【命令模式】 接口模式

【缺省级别】 14

【使用指导】 该命令只在 SVI 口支持，在开启网关认证模式情况下生效。

【配置举例】 1：在 vlan2 接口上关闭抑制往认证 vlan 发送广播邻居请求报文。

```
Ruijie(config-if-VLAN 2)# no ipv6 nd suppress-auth-vlan-ns
```

【检验方法】 使用 show run interface <name> 命令查看是否配置成功

【提示信息】 -

【常见错误】 -

【平台说明】 -

1.26 ipv6 nd suppress-ra

抑制在接口上发送路由器公告(RA)报文。
ipv6 nd suppress-ra

在接口上发送 RA 报文。
no ipv6 nd suppress-ra

【参数说明】

参数	描述
-	-

【缺省配置】 在 IPv6 的接口上将不会发送路由器公告报文。

【命令模式】 接口模式

【缺省级别】 14

【使用指导】 -

【配置举例】 1：在 GigabitEthernet 0/1 接口上抑制发送路由器公告报文。

```
Ruijie(config-if-GigabitEthernet 0/1)# ipv6 nd suppress-ra
```

【检验方法】 通过 **show ipv6 interface** 查看 RA 报文发送功能是否被抑制。

【提示信息】 -

【常见错误】 -

【平台说明】 -

1.27 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
ipv6 nd threshold *percent_value*

恢复缺省配置。
no ipv6 nd threshold

【参数说明】

参数	描述
percent_value	邻居表容量的百分比，取值范围是 50 到 100，默认值是 70。

【缺省配置】 默认值为 70。

【命令模式】 全局模式

【缺省级别】 14

【使用指导】 这里的占比是指当前邻居表项数与设备所能支持的邻居表项数之比。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。

【配置举例】 1：配置 IPv6 邻居表项数目达到容量的 80%时，启用 ND 拒绝服务攻击。

```
Ruijie(config)# ipv6 nd threshold 80
```

【检验方法】 通告 **show run** 查看配置是否一致

【提示信息】 -

【常见错误】 -

【平台说明】 -

1.28 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
ipv6 nd threshold per-mac *value*

恢复缺省配置。
no ipv6 nd threshold per-mac

【参数说明】

参数	描述
value	单个用户对应的邻居表项数目，取值范围是 4 到 256，默认值是 16

【缺省配置】 默认值为 16。

【命令模式】 全局模式

【缺省级别】 14

【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。其它 IPv6 邻居表项数目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】 1：配置单个用户的邻居表项数量达到 100 时，启用 ND 拒绝服务攻击。

```
Ruijie(config)# ipv6 nd threshold per-mac 100
```

【检验方法】 通告 **show run** 查看配置是否一致

【提示信息】 -

【常见错误】 -

【平台说明】 -

1.29 ipv6 nd unresolved

配置未解析的邻居表项的最大数量。
ipv6 nd unresolved *number*

恢复缺省配置。
no ipv6 nd unresolved

【参数说明】

参数	描述
number	未解析邻居表项限制数，最小取值 1，最大取值为设备支持的邻居表项容量。

【缺省配置】 默认值为 0，表示不限制，即受限于设备支持的邻居表项容量。

【命令模式】 全局模式

【缺省级别】 14

【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。

【配置举例】 1：配置未解析邻居表项限制数 200。

```
Ruijie(config)# ipv6 nd unresolved 200
```

【检验方法】 通告 **show run** 查看配置是否一致

【提示信息】 -

【常见错误】 -

【平台说明】 -

1.30 ipv6 neighbor

配置一个静态邻居。
ipv6 neighbor *ipv6-address interface-id hardware-address*

删除一个静态邻居。
no ipv6 neighbor *ipv6-address interface-id*

【参数说明】

参数	描述
ipv6-address	邻居的 IPV6 地址，必须遵循 RFC4291 定义的地址表示形式。
interface-id	指定该邻居所在的网络接口（包括 Routed Port,L3 AP 口和 SVI 接口）。
hardware-address	邻居的链路地址，即以 XXXX.XXXX.XXXX 表示的 48 位的 MAC 地址，'X' 表示十六进制数。

【缺省配置】 没有配置任何静态邻居。

【命令模式】 全局配置模式

【缺省级别】 14

【使用指导】 该命令类似 ARP 命令，静态的邻居只能配置在开启 IPv6 协议的接口上，
如果要配置的邻居已经通过 NDP 学到并存储在邻居表中，那么该动态生成的邻居将自动转换为静态的。配置的静态邻居如果有效，将总是处于 Reachable 状态。无效的静态邻居，是指配置的静态邻居 IPV6 地址，与接口上配置的地址不匹配（不在该接口的任一 IPV6 地址的网段内，或与该接口地址冲突），此时数据包不会按静态邻居指定的 mac 地址转发。无效的静态邻居，处于 inactive 状态，可以通过 **show ipv6 neighbor static** 命令查看该静态邻居的有效性状态。
使用 **clear ipv6 neighbors** 命令将清除所有动态学到的(即通过 NDP)邻居。

【配置举例】 1：在 SVI 1 上配置一个静态邻居。

```
Ruijie(config)# ipv6 neighbor 2001::1 vlan 1 00d0.f811.1111
```

【检验方法】 使用 **show ipv6 neighbors** 命令查看邻居信息。

【提示信息】 -

【常见错误】 -

【平台说明】 -

1.31 ipv6 ns-linklocal-src

发送邻居请求时将强制使用链路本地地址作为源地址。

ipv6 ns-linklocal-src

发送邻居请求时不强制使用链路本地地址作为源地址，而是根据目的 IPv6 地址按 RFC3484 选择使用链路本地地址或者全球单播地址。

no ipv6 ns-linklocal-src

【参数说明】

参数	描述
-	-

【缺省配置】 发送邻居请求时，总是以链路本地地址作为源地址。

【命令模式】 全局配置模式

【缺省级别】 14

【使用指导】 -

【配置举例】 1：在发送邻居请求时不强制使用链路本地地址作为源地址。

```
Ruijie(config)# no ipv6 ns-linklocal-src
```

【检验方法】 -

【提示信息】 -

【常见错误】 -

【平台说明】 -

1.32 ipv6 path-mtu

配置静态路径 MTU。

ipv6 path-mtu [**vrf** *vrf-name*] *ipv6-address value*

删除静态路径 MTU。

no ipv6 path-mtu [**vrf** *vrf-name*] *ipv6-address*

删除所有静态路径 MTU。

no ipv6 path-mtu all

【参数说明】

参数	描述
vrf *vrf-name*	VRF 名称，如果不输入该参数，表示全局。
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。

【缺省配置】 -

【命令模式】 全局模式

【缺省级别】 14

【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。

【配置举例】 1：配置 IPv6 地址 A000::1 的路径 MTU 为 1400 字节。

```
Ruijie(config)# ipv6 path-mtu A000::1 1400
```

【检验方法】 通过 **show ipv6 path-mtu** 查看配置是否生效。

【提示信息】 -

【常见错误】 -

【平台说明】 -

1.33 ipv6 path-mtu age

配置动态路径 MTU 的老化时间。
ipv6 path-mtu age { *age-time* | **infinity** }

把动态路径 MTU 的老化时间恢复为缺省值。
no ipv6 path-mtu age
或者 **default ipv6 path-mtu age**

【参数说明】

参数	描述
age-time	老化时间，单位是分钟，取值范围是 10 到（30 * 24 * 60），缺省值是 10 分钟。
infinity	老化时间无穷大，即永远不老化。

【缺省配置】 缺省老化时间是 10 分钟。

【命令模式】 全局模式

【缺省级别】 14

【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】 1：把动态路径 MTU 的老化时间配置为 20 分钟。

```
Ruijie(config)#ipv6 path-mtu age 20
```

【检验方法】 通过 **show run** 查看配置是否生效。

【提示信息】 -

【常见错误】 -

【平台说明】 -

1.34 ipv6 redirects

开启 ICMPv6 重定向。
ipv6 redirects

关闭 ICMPv6 重定向。
no ipv6 redirects

【参数说明】

参数	描述
-	-

【缺省配置】 缺省开启 ICMPv6 重定向。

【命令模式】 接口模式

【缺省级别】 14

【使用指导】 -

【配置举例】 1：在 GigabitEthernet 0/1 接口上开启 ICMPv6 重定向。

```
Ruijie(config-if-GigabitEthernet 0/1)# ipv6 redirects
```

【检验方法】 通过 **show ipv6 interface** 查看接口是否允许发送 ICMPv6 重定向。

【提示信息】 -

【常见错误】 -

【平台说明】 -

1.35 ipv6 source-route

配置设备转发带有路由首部的 IPv6 报文。
ipv6 source-route

禁止转发带有路由首部的 IPv6 报文。
no ipv6 source-route

【参数说明】

参数	描述
-	-

【缺省配置】 禁止转发带有路由首部的 IPv6 报文

【命令模式】 全局模式

【缺省级别】 14

【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】 1：配置设备转发带有路由首部的 IPv6 报文。

```
Ruijie(config)# ipv6 source-route
```

【检验方法】 -

【提示信息】 -

【常见错误】 -

【平台说明】 -

1.36 ipv6 unnumbered

配置接口借用某个特定接口的地址作为本地往外发送的报文的源地址。
ipv6 unnumbered *interface-id*

取消接口借用某个特定接口的地址作为本地往外发送的报文的源地址。
no ipv6 unnumbered

【参数说明】

参数	描述
interface-id	接口（包括以太网接口、aggregateport 接口、SVI 接口）。

【缺省配置】 不借用特定接口的地址作为源地址

【命令模式】 接口配置模式

【缺省级别】 14

【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。

【配置举例】 1：配置 Virtual-Template 1 借用 loopback 1 的接口地址。

```
Ruijie(config-if-Virtual-Template 1)#ipv6 unnumbered loopback 1
```

【检验方法】 show ipv6 interface brief

Virtual-Template 1 [down/down]

FE80::2A9:15FF:FE36:5413

unnumbered (Loopback 1)

【提示信息】 -

【常见错误】 -

【平台说明】 只有路由器支持

1.37 peer default ipv6 pool

使用该命令使设备发送路由器公告(RA)报文能从前缀池获取一个前缀来公告。

peer default ipv6 pool *pool-name*

禁止发送路由器公告(RA)报文从前缀池获取一个前缀来公告。

no peer default ipv6 pool

【参数说明】

参数	描述
pool-name	本地前缀池，通过 **ipv6 local pool** 命令配置。

【缺省配置】 禁止发送路由器公告(RA)报文从前缀池获取一个前缀来公告。

【命令模式】 接口配置模式

【缺省级别】 14

【使用指导】 用于 IPv6 over vpdn 环境，使设备发送路由器公告(RA)报文能从前缀池获取一个前缀来公告。

【配置举例】 1：配置 Virtual-Template 1 发送 RA 时从前缀池 rapool 获取前缀进行公告。

```
Ruijie(config-if-Virtual-Template 1)# peer default ipv6 pool rapool
```

【检验方法】 通过 **show run** 可以查看配置是否生效

【提示信息】 -

【常见错误】 -

【平台说明】 只有路由器支持

1.38 show ipv6 address

显示 IPv6 地址的信息。

show ipv6 address [*interface-name*]

【参数说明】

参数	描述
interface-name	接口名称，缺省显示所有的 IPv6 地址。

【命令模式】 特权模式

【缺省级别】 14

【使用指导】 -

【配置举例】 1：查看本设备配置的所有 IPv6 地址。

```
 Ruijie#show ipv6 addr
Global unicast address limit: 1024, Global unicast address count: 2
Tentative address count: 3,Duplicate address count: 0
Preferred address count: 0,Deprecated address count: 0
  GigabitEthernet 0/5
    2003:1::23/64                              Tentative
  Preferred lifetime: INFINITE, Valid lifetime: INFINITE
    fe80::2d0:f8ff:fefb:deb2/64                  Tentative
  Preferred lifetime: INFINITE, Valid lifetime: INFINITE
    2005:1::1111/64                            Tentative
  Preferred lifetime: INFINITE, Valid lifetime: INFINITE
Ruijie#
```

2：查看本设备接口 GigabitEthernet 0/1 上配置的 IPv6 地址。

```
 Ruijie#show ipv6 addr gi 0/5
Global unicast address count: 2
Tentative address count: 3,Duplicate address count: 0
Preferred address count: 0,Deprecated address count: 0
    2003:1::23/64                             Tentative
  Preferred lifetime: INFINITE, Valid lifetime: INFINITE
    fe80::2d0:f8ff:fefb:deb2/64                  Tentative
  Preferred lifetime: INFINITE, Valid lifetime: INFINITE
```

```
    2005:1::1111/64                              Tentative
  Preferred lifetime: INFINITE, Valid lifetime: INFINITE
Ruijie#
```

字段解释：

字段	说明
Global unicast address count	此接口配置的全球单播 IPv6 地址个数
Tentative address count	临时地址个数
Duplicate address count	发生冲突的地址个数
Preferred address count	首选的地址个数
Deprecated address count	过期的地址个数
Preferred lifetime	首选生命期
Valid lifetime	有效生命期

【提示信息】 -

【平台说明】 -

1.39 show ipv6 general-prefix

显示通用前缀中的前缀信息。

show ipv6 general-prefix

【参数说明】

参数	描述
-	-

【命令模式】 特权模式

【缺省级别】 14

【使用指导】 手工配置的通用前缀，与 DHCPv6 客户端学习到通用前缀，都会显示出来。

【配置举例】 1：显示通用前缀信息。

```
Ruijie# show ipv6 general-prefix
There is 1 general prefix.
IPv6 general prefix my-prefix, acquired via Manual configuration
        2001:1111:2222::/48
        2001:1111:3333::/48
```

字段解释：

字段	说明
There is	当前存在的通用前缀的个数
IPv6 general prefix	通用前缀的名称
acquired via	取得方式
Prefix/len	具体的前缀列表

【提示信息】 -

【平台说明】 -

1.40 show ipv6 interface

显示 IPV6 接口的信息。

show ipv6 interface [[*interface-id*] [**ra-info**]] [brief [*interface-id*]]

【参数说明】

参数	描述
interface-id	接口（包括以太网接口、aggregateport 接口、SVI 接口），缺省显示所有接口。
ra-info	查看该接口上关于发送的 RA 报文的参数信息。
brief	显示接口的简要信息（接口状态和地址信息）

【命令模式】

【缺省级别】 14

【使用指导】 通过该命令可以查看 IPV6 接口上的地址配置、ND 配置以及相关的统计信息。

【配置举例】 1：显示 IPV6 接口的信息。

```
Ruijie# show ipv6 interface vlan 1
Interface vlan 1 is Up, ifindex: 2001
address(es):
Mac Address: 00:00:00:00:00:01
INET6: fe80::200:ff:fe00:1 , subnet is fe80::/64
INET6: 2001::1 , subnet is 2001::/64 [TENTATIVE]
Joined group address(es):
ff01:1::1
ff02:1::1
```

```
ff02:1::2
ff02:1::1:ff00:1
MTU is 1500 bytes
ICMP error messages limited to one every 10 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<240--160>
ND router advertisements live for 1800 seconds
```

在上面显示中可以看到 INET6: 2001::1，subnet is 2001::/64

[TENTATIVE]这一行，关于：INET6 地址后 [ ] 内跟的标志位的含义如下

字段	说明
ANYCAST	表示该地址为泛播地址。
TENTATIVE	表示正在为该地址进行地址冲突检测(DAD)，检测还未结束该地址是个临时的地址。
DUPLICATED	表示该地址已经被检测到有重复的地址存在。
DEPRECATED	表示该地址的首选有效期已经到了，该地址变为不赞成被使用的地址了。
NODAD	表示不对该地址进行地址冲突检测。
AUTOIFID	表示该地址的接口标识符由系统自动生成的，通常就是 EUI-64 标识符。
PRE	表示无状态自动配置的地址。
GEN	表示由通用前缀生成的地址。

2：查看 IPV6 接口上关于发送的 RA 报文的参数信息。

```
Ruijie# show ipv6 interface vlan 1 ra-info
vlan 1: DOWN
RA timer is stopped
waits: 0, initcount: 3
statistics: RA(out/in/inconsistent): 4/0/0, RS(input): 0
Link-layer address: 00:00:00:00:00:01
Physical MTU: 1500
ND router advertisements live for 1800 seconds
ND router advertisements are sent every 200 seconds<240--160>
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)
fec0:1:1:1::/64(Def,Auto,vltime:2592000,pltime:604800, flags: LA)
```

关于 **ra-info** 中的各个字段含义：

字段	说明
RA timer is stopped (on)	表示定时发送路由器公告报文的定时器是否打开。
waits	表示已经收到路由器请求报文但还没有为其应答的个数。
initcount	表示 RA 定时器重新启动时初始发出的路由器公告报文个数。
RA(out/in/inconsistent)	Out：表示发出的路由器公告报文的个数。 in：表示收到的路由器公告报文的个数。 inconsistent 表示收到的路由器公告报文中和路由器自身公告的报文的参数不一致的报文的个数。
RS(input)	表示收到的路由器请求报文的个数。
Link-layer address	该接口的链路层地址。
Physical MTU	该接口的链路 MTU。
!M | M	!M 表示路由器公告报文中的。 managed-config-flag 标志位没有置上。 M: 意思与上面相反。
!O | O	!O 表示路由器公告报文中的。 other-config-flag 标志位没有置上。 O：意思与上面相反。

关于 **ra-info** 中的前缀表(Prefix)的各个字段的介绍：

字段	说明
total	表示该接口的前缀的个数。
fec0:1:1:1::/64	具体的前缀。
Def	该标志表示该前缀使用接口的缺省前缀参数配置。
Auto | CFG	Auto 标志表示该前缀是由于在接口配置了相应的 IPV6 地址而自动生成的前缀, CFG 标志表示该前缀是手工配置的。
!Adv	该标志表示该前缀不被公告。
vltime	表示该前缀的有效时间(秒)。
pltime	表示该前缀的首选有效时间(秒)。
L | !L	L 标志表示该前缀的 on-link 位置上。 !L 意思与上面相反。
A | !A	A 标志表示该前缀的 auto-config 位置上, !A 意思与上面相反。

3：显示 IPV6 接口的简要信息。

```
Ruijie#show ipv6 interface brief

GigabitEthernet 0/1           [down/down]
        2222::2
        FE80::1614:4BFF:FE5C:ED3A
```

【提示信息】 -

【平台说明】 -

1.41 show ipv6 neighbors

显示 IPV6 的邻居表。

show ipv6 neighbors [**vrf** *vrf-name*] [**verbose**] [*interface-id*] [*ipv6-address*] [**static**] [**oob**]

【参数说明】

参数	描述
vrf-name	VRF 名称，缺省显示全局的 IPv6 邻居。
verbose	显示邻居的详细信息
interface-id	显示某个接口上的邻居表 缺省显示所有接口的邻居
ipv6-addres	显示指定邻居的信息
static	显示静态邻居有效性状态
oob	显示 mgmt 口的 IPv6 邻居

【命令模式】 特权模式

【缺省级别】 14

【使用指导】 -

【配置举例】 1：显示 SVI 1 接口上的邻居信息

```
Ruijie# show ipv6 neighbors vlan 1
IPv6 Address Linklayer Addr   Interface
fa::1          00d0.0000.0002   vlan 1
fe80::200:ff:fe00:2  00d0.0000.0002  vlan 1
```

2：显示邻居的详细信息

```
Ruijie# show ipv6 neighbors verbose
```

```
IPv6 Address  Linklayer Addr Interface
2001::1       00d0.f800.0001 vlan 1
       State: Reach/H Age: - asked: 0
fe80::200:ff:fe00:1     00d0.f800.0001 vlan 1
       State: Reach/H Age: - asked: 0
```

字段解释：

字段	说明
IPv6 Address	邻居的 IPV6 地址
Linklayer Addr	链路地址即 Mac 地址，如果还未得到则显示 incomplete
Interface	该邻居所在的接口
State	邻居的状态： state/H(R) STATE 的值如下： INCMP(Incomplete)—该邻居的地址解析正在进行中，邻居请求(NS)报文已经发送但是还没有收到邻居的应答报文(NA)。 REACH(Reachable) —表示从设备到邻居是连通的，在该状态向邻居发送报文时不需要额外的动作。STALE — 表示邻居被认为可到达的时间已经到期，处在该状态时设备不需要额外的动作直到有报文发送到该邻居上，此时即将启动 NUD (Neighbor Unreachability Detection) 。 DELAY—表示有报文向处于STALE状态的邻居发送 此时状态由STALE转换为DELAY状态 ,在 DELAY_FIRST_PROBE_TIME seconds(5 秒)内如果没有收到邻居可达性的通知信息，那么状态将由 DELAY 转换为 PROBE，同时向该邻居发送邻居请求报文(NS)，正式启动 NUD。 PROBE—表示 NUD 已经启动，检测邻居的可达性，每隔 RetransTimer milliseconds 向邻居发送邻居请求(NS)报文直到收到了邻居的应答或者发送的邻居请求报文数量已达到上限值 MAX_UNICAST_SOLICIT(3 个) ?—表示未知状态 /R—表示认为邻居是一个设备 /H—表示认为邻居是一个主机
Age	表示邻居被认为可到达的时间，'-'表示永远是可达的，注意对静态配置的邻居表项将依赖于实际是否可达。'expired'表示邻居被认为可达的时间已经到期 ,等待触发 NUD 检测。
Asked	表示在解析邻居的链路地址时已经向邻居发送的邻居请求(NS)的数量。

3：显示静态邻居状态

```
Ruijie# show ipv6 neighbors static
IPv6 Address     Linklayer Addr  Interface                State
2001:1::1         00d0.f822.33ab   GigabitEthernet 0/14   ACTIVE
2001:2::2         00d0.f822.33ac   VLAN 1                    INACTIVE
```

字段解释：

字段	说明
IPv6 Address	静态邻居的 IPV6 地址
Linklayer Addr	配置的链路地址即 Mac 地址
Interface	该邻居所在的接口
State	静态邻居的状态： STATE 的值如下： ACTIVE—活动的 INACTIVE—不活动的，当配置的静态邻居 IPV6 地址，与接口上配置的地址不匹配（不在任一接口地址的网段内，或与接口地址本身冲突），该静态邻居配置不活动，即数据包不会按静态邻居指定的 mac 地址转发。

【提示信息】 -

【平台说明】 NBR6205-E、NBR6135-E、NBR6210-E、NBR6215-E 支持 MGMT 口；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 MGMT 口。

1.42 show ipv6 neighbors statistics

显示 IPv6 邻居表的统计信息

show ipv6 neighbors [**vrf** *vrf-name*] **statistics** [**all**]

【参数说明】

参数	描述
vrf-name	VRF 名称，缺省显示全局的 IPv6 邻居表统计信息。
all	显示所有 IPv6 邻居表的统计信息

【命令模式】 特权用户模式

【缺省级别】 14

【使用指导】 -

【配置举例】 1：查看全局邻居表的统计信息。

```
Ruijie#show ipv6 neighbor statistics

Memory: 0 bytes
Entries: 0
  Static: 0,Dynamic: 0,Local: 0
```

```
  Incomplete:0, Reachable:0, Stale:0, Delay:0, Probe:0
Ruijie#
```

2：查看所有邻居表的统计信息

```
 Ruijie#show ipv6 neighbor statistics all

IPv6 neighbor table count: 1
Static neighbor count: 0(0 active, 0 inactive)
Total
Memory: 0 bytes
Entries: 0
  Static: 0,Dynamic: 0,Local: 0
  Incomplete:0, Reachable:0, Stale:0, Delay:0, Probe:0;

Global
Memory: 0 bytes
Entries: 0
  Static: 0,Dynamic: 0,Local: 0
  Incomplete:0, Reachable:0, Stale:0, Delay:0, Probe:0;
Ruijie#
```

字段解释：

字段	说明
IPv6 neighbor table count	邻居表的个数
Static neighbor count	静态邻居表项数
active	活动邻居表项个数
inactive	不活动邻居表项个数
Memory	内存占用量
Entries	邻居表项数
Static	静态表项数目
Dynamic	动态表项数目
Local	本地 IPv6 地址对应的表项数目
Incomplete	未解析表项数目
Reachable	可达的邻居表项数目
Stale	Stale 状态的表项数目
Delay	Delay 状态的表项数目

Probe	Probe 状态的表项数目

【提示信息】 -

【平台说明】 -

1.43 show ipv6 neighobr statistics per-mac

显示每个 MAC 地址的邻居表项的数量。

show ipv6 neighbor statistics per-mac [*interface-name*] [*mac-address*]

【参数说明】

参数	描述
interface-name	接口名称
mac-address	Mac 地址

【命令模式】 特权模式

【缺省级别】 14

【使用指导】 -

【配置举例】 1：查看每个 MAC 地址的邻居表项的数量

```
Ruijie# show ipv6 neighbor statistics per-mac
Interface  MAC address     Statistics
-----------------------------------------------
VLAN 1  0000:0000:0001   3
VLAN 1  0000:0000:0002   5
VLAN 2  0000:0000:0003   10
```

字段解释：

字段	说明
Interface	接口名称
MAC address	mac 地址
Statistics	ND 表项数目

【提示信息】 -

【平台说明】 -

1.44 show ipv6 packet statistics

显示 IPv6 报文的统计信息。

show ipv6 packet statistics [**total |** *interface-name*]

【参数说明】

参数	描述
total	所有接口的统计信息总和 缺省既显示所有接口的统计之和，也显示每一个接口的统计值。
interface-name	接口名称

【命令模式】 特权模式

【缺省级别】 14

【使用指导】 -

【配置举例】 1：查看 IPv6 报文统计信息总和和每个接口上的统计信息

```
Ruijie#show ipv6 pack statistics
Total
  Received 0 packets, 0 bytes
    Unicast:0,Multicast:0
    Discards:0
      HdrErrors:0(HoplimitExceeded:0,Others:0)
      NoRoutes:0
      Others:0
  Sent 0 packets, 0 bytes
    Unicast:0,Multicast:0
  GigabitEthernet 0/5
  Received 0 packets, 0 bytes
    Unicast:0,Multicast:0
    Discards:0
      HdrErrors:0(HoplimitExceeded:0,Others:0)
      NoRoutes:0
      Others:0
  Sent 0 packets, 0 bytes
    Unicast:0,Multicast:0
Ruijie#
```

2：查看 IPv6 报文统计信息总和

```
 Ruijie#show ipv6 pack statistics total
```

```
Total
  Received 0 packets, 0 bytes
    Unicast:0,Multicast:0
    Discards:0
      HdrErrors:0(HoplimitExceeded:0,Others:0)
      NoRoutes:0
      Others:0
  Sent 0 packets, 0 bytes
    Unicast:0,Multicast:0
Ruijie#
```

字段解释：

字段	说明
Total	下面几行表示所有接口的 IPv6 报文统计之和 GigabitEthernet 0/5 下面几行表示的是此接口的报文统计
Received	接收到的 IPv6 报文数目，字节数目
Unicast	IPv6 单播报文数目
Multicast	IPv6 组播报文数目
Discards	丢弃的 IPv6 报文数目
HdrErrors	IPv6 首部错误丢弃的报文数目
HoplimitExceeded	报文转发过程中，超过了跳数限制而丢弃的报文数目
Others	其他 IPv6 首部错误，导致丢弃的报文数目
NoRoutes	由于没有路由，而丢弃的 IPv6 报文数目
Others	其它原因丢弃的 IPv6 报文数目
Sent	发送的 IPv6 报文数目，字节数目。 单播报文数目，组播报文数目。

【提示信息】 -

【平台说明】 -

1.45 show ipv6 path-mtu

显示路径 MTU 的信息。

show ipv6 path-mtu [**vrf** *vrf-name*] [ipv6-address | **dynamic** | **static**]

【参数说明】

参数	描述
vrf *vrf-name*	VRF 名称。如果不指定该参数，表示显示全局的路径 MTU。

ipv6-address	IPv6 地址。
dynamic	只显示动态路径 MTU。
static	只显示静态路径 MTU。

【命令模式】 特权模式

【缺省级别】 14

【使用指导】 -

【配置举例】 1：查看全局的路径 MTU。

```
Ruijie#show ipv6 path-mtu
IPv6 Address   MTU   Age   Type
A000::1        1400  --    Static
A000::2        1300  1     Dynamic
```

字段解释：

字段	说明
IPv6 Address	IPv6 地址
MTU	路径 MTU 的值
Age	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	路径 MTU 的类型：动态或者静态。

【提示信息】 -

【平台说明】 -

1.46 show ipv6 path-mtu statistics

显示路径 MTU 的统计信息。

show ipv6 path-mtu statistics

【参数说明】

参数	描述
-	-

【命令模式】 特权模式

【缺省级别】 14

【使用指导】 -

【配置举例】 1：查看路径 MTU 的统计信息。

```
Ruijie#show ipv6 path-mtu statistics

Maximum count: static 8192, dynamic 8192

VRF      Static   Dynamic    Sum

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

Global   10       20         30

AAA      20       30         50

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

Total    30       50         80
```

字段解释：

字段	说明
Maximum count: static 8192, dynamic 8192	最大数量，即容量，静态路径 MTU 的容量是 8192，动态路径 MTU 的容量是 8192。
VRF	VRF 名称，Global 表示全局
Static	静态路径 MTU 的数量
Dynamic	动态路径 MTU 的数量
Sum	静态路径 MTU 和动态路径 MTU 的数量总和
Total	全局和所有 VRF 的路径 MTU 的数量总和

【提示信息】 -

【平台说明】 -

1.47 show ipv6 raw-socket

显示所有 IPv6 原始套接字。

show ipv6 raw-socket [*num*]

【参数说明】

参数	描述
num	协议号

【命令模式】 特权模式

【缺省级别】 14

【使用指导】 -

【配置举例】 1：查看所有 IPv6 原始套接字。

```
Ruijie# show ipv6 raw-socket
Number Protocol Process name
1      ICMPv6   vrrp.elf
2      ICMPv6   tcpip.elf
3      VRRP     vrrp.elf
Total: 3
```

字段解释：

字段	说明
Number	序号
Protocol	协议号
Process name	进程名称
Total	总数

【提示信息】 -

【平台说明】 -

1.48 show ipv6 routers

显示邻居路由器和路由公告信息。

show ipv6 routers [*interface-type interface-number*]

【参数说明】

参数	描述
interface-type interface-number	可选参数。显示指定接口收到的路由公告信息。 缺省显示所有接口收到的路由公告。

【命令模式】 特权模式

【缺省级别】 14

【使用指导】 如果没有指定接口，则显示本设备收到的所有路由公告的信息。

【配置举例】 1：显示邻居路由器和路由公告信息。

```
Ruijie# show ipv6 routers
```

```
Router FE80::2D0:F8FF:FEC1:C6E1 on VLAN 2, last update 62 sec
  Hops 64, Lifetime 1800 sec, ManagedFlag=0, OtherFlag=0, MTU=1500
  Preference=MEDIUM
  Reachable time 0 msec, Retransmit time 0 msec
  Prefix 6001:3::/64 onlink autoconfig
    Valid lifetime 2592000 sec, preferred lifetime 604800 sec
  Prefix 6001:2::/64 onlink autoconfig
    Valid lifetime 2592000 sec, preferred lifetime 604800 sec
```

字段解释：

字段	说明
Router	表明一个邻居路由器，由 IPv6 地址和收到 RA 公告的网络接口描述
last update	上一次收到 RA 公告多久了
Hops	RA 公告通知的跳数
Lifetime	此路由器的生存期
ManagedFlag	此路由器的管理配置标志
OtherFlag	此路由器的其它标志
MTU	此路由器发送 RA 公告接口的 MTU
Reachable time	此路由器的可达时间
Retransmit time	此路由器对应的 RA 公告的重传时间
Prefix	此路由器公告的前缀
Valid lifetime	对应前缀的生存期
preferred lifetime	对应前缀的首选生命期

【提示信息】 -

【平台说明】 -

1.49 show ipv6 sockets

显示所有 IPv6 套接字，可以知道哪些 UDP 端口和 TCP 端口对外提供服务。

show ipv6 sockets

【参数说明】

参数	描述
-	-

【命令模式】 特权模式

【缺省级别】 14

【使用指导】 -

【配置举例】 1：查看所有 IPv6 套接字。

```
Ruijie# show ipv6 sockets
Number Process name     Type   Protocol  LocalIP:Port  ForeignIP:Port  State
1      vrrp.elf         RAW    ICMPv6    :::58         :::0            *
2      tcpip.elf        RAW    ICMPv6    :::58         :::0            *
3      vrrp.elf         RAW    VRRP      :::112        :::0            *
4      rg-snmpd         DGRAM  UDP       :::161        :::0            *
5      rg-snmpd         DGRAM  UDP       :::162        :::0            *
6      dhcp6.elf        DGRAM  UDP       :::547        :::0            *
7      rg-sshd          STREAM TCP       :::22         :::0            LISTEN
8      rg-telnetd       STREAM TCP       :::23         :::0            LISTEN
Total: 8
```

字段解释：

字段	说明
Number	序号
Process name	进程名称
Type	套接字类型，RAW 表示原始套接字，DGRAM 表示数据包类型，STREAM 表示流类型。
Protocol	协议号
LocalIP:Port	本地 IPv6 地址和端口
ForeignIP:Port	对端 IPv6 地址和端口
State	状态，只对 IPv6 TCP 套接字有意义。
Total	套接字总数

【提示信息】 -

【平台说明】 -

1.50 show ipv6 udp

显示所有 IPv6 UDP 套接字，可以知道哪些 UDP 端口对外提供服务。

show ipv6 udp [**local-port** *num*] [**peer-port** *num*]

显示 IPv6 UDP 套接字的统计值。

show ipv6 udp statistics

【参数说明】

参数	描述
local-port *num*	本地端口号
peer-port *num*	对端端口号

【命令模式】 特权模式

【缺省级别】 14

【使用指导】 -

【配置举例】 1：查看所有 IPv6 UDP 套接字。

```
Ruijie# show ipv6 udp
Number Local Address   Peer Address   Process name
1      :::161           :::0          rg-snmpd
2      :::162           :::0          rg-snmpd
3      :::547           :::0          dhcp6.elf
```

字段解释：

字段	说明
Number	序号
Local Address	本地 IPv6 地址和端口
Peer Address	对端 IPv6 地址和端口
Process name	进程名称

【提示信息】 -

【平台说明】 -

命令参考-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 in-path rule auto-discovery dstport port 80 accelerate http rulenum start

配置基于 80 端口的 TCP 代理规则

in-path rule auto-discovery dstport port 80 accelerate http rulenum start

删除 TCP 代理规则

no in-path rule all

【参数说明】

参数	描述
-	-

【缺省配置】 -

【命令模式】 全局模式

【缺省级别】 14

【使用指导】 开启 80 端口的 TCP 代理

【配置举例】 1：开启 80 端口的 TCP 代理

```
Ruijie(config)# in-path rule auto-discovery dstport port 80 accelerate http rulenum start
```

【检验方法】 1. 使用 **show in-path rules** 命令查看 TCP 代理规则。

【提示信息】 -

【常见错误】 -

【平台说明】 网关系列产品

1.2 show in-path rules

查看 TCP 代理规则。

show in-path rules

【参数说明】

参数	描述
-	-

【命令模式】 全局模式、特权模式、接口模式

【缺省级别】 14

【使用指导】 查看 TCP 代理规则

【配置举例】 1：显示 TCP 代理规则。

```
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
```

【提示信息】 -

【平台说明】 网关系列产品

1.3 show was http ad config

显示悬浮广告当前配置

show was http ad config

【参数说明】

参数	描述
-	-

【命令模式】 全局模式、特权模式、接口模式

【缺省级别】 14

【使用指导】 查看悬浮广告配置信息。

【配置举例】 1：显示悬浮广告的配置信息

```
Ruijie#show was http ad config
ad   status : on
ad   url    : http://rujie.com.cn/ad.js
```

【提示信息】 -

【平台说明】 网关系列产品

1.4 show was http ad status

显示悬浮广告当前运行状态。

show was http ad status

【参数说明】

参数	描述
-	-

【命令模式】 全局模式、特权模式、接口模式

【缺省级别】 14

【使用指导】 查看悬浮广告当前运行状态

【配置举例】 1：显示悬浮广告当前运行状态。

```
Ruijie# show was http ad status
ad   status : on
Http request count           : 9
Http insert ad count         : 0
Http insert html count       : 0
Http insert ad rate          : 0%
Http no 200 response         : 0
Http exceed memory count     : 0
Http no html feature         : 0
Http other fail count        : 0
Http decprs count            : 0
Http decprs success count    : 0
Http decprs gzip off count   : 0
Http decprs fail count       : 0
Http decprs no html count    : 0
Http decprs abnor   count    : 0
Http avg memory              : 0
```

【提示信息】 -

【平台说明】 网关系列产品

1.5 show was status

显示 was 模块状态。

show was status

【参数说明】

参数	描述
-	-

【命令模式】 全局模式、特权模式、接口模式

【缺省级别】 14

【使用指导】 查看 was 模块运行状态

【配置举例】 1：显示 was 模块运行状态。

```
Ruijie# show was status
was:on
```

【提示信息】 -

【平台说明】 网关系列产品

1.6 was enable

启用 was 模块功能

was enable

禁用 was 模块功能

no was enable

【参数说明】

参数	描述
-	-

【缺省配置】 开启 was 模块功能

【命令模式】 全局模式

【缺省级别】 14

【使用指导】 此命令用来开启 was 模块功能

【配置举例】 1：开启 was 模块功能

```
Ruijie(config)# was enable
```

【检验方法】 1：使用 **show was status** 命令可以查看 was 模块是开启还是关闭。

【提示信息】 -

【常见错误】 -

【平台说明】 网关系列产品

1.7 was http ad enable

启用 ad 广告功能

was http ad enable

禁用 ad 广告

no was http ad enable

【参数说明】

参数	描述
-	-

【缺省配置】 开启 ad 广告功能

【命令模式】 全局模式

【缺省级别】 14

【使用指导】 此命令用来开启 ad 广告功能

【配置举例】 1：开启 ad 广告功能

```
Ruijie(config)# was http ad enable
```

【检验方法】 1：使用 **show was http ad config** 命令可以查看 ad 广告是开启还是关闭。

【提示信息】 -

【常见错误】 依赖于 was 模块的总开关，需要先开启 was enable 后此配置才生效

【平台说明】 网关系列产品

1.8 was http ad url

配置插入的广告脚本链接

was http ad url *string*

删除广告脚本链接

no was http ad url

【参数说明】

参数	描述
string	广告脚本的链接

【缺省配置】 -

【命令模式】 全局模式

【缺省级别】 14

【使用指导】 广告脚本由网络运营者提供

有些脚本编写，可能存在部分页面上显示异常或不显示的问题。

【配置举例】 1：运营者的广告脚本链接

```
Ruijie(config)# was http ad url http://rujie.com.cn/ad.js
```

【检验方法】 1. 使用 **show was http ad config** 命令查看脚本链接。

【提示信息】 -

【常见错误】 -

【平台说明】 网关系列产品

2 APP-CACHE

2.1 was http app-cache enable

启用 app 缓存

was http app-cache enable

停止 app 缓存

no was http app-cache enable

【参数说明】

参数	描述
-	-

【缺省配置】 -

【命令模式】 全局模式

【缺省级别】 14

【使用指导】

开启 app 缓存功能

【配置举例】 -

【检验方法】 1：使用 **show was http app-cache config** 查看配置是否生效

```
Ruijie#show was http app-cache config
app-cache : on
```

【提示信息】 -

【常见错误】 依赖于 was 模块的总开关，需要先开启 was enable 后此配置才生效

【平台说明】 网关 EG，NBR 系列产品

2.2 was http app-cache rule

配置 app 缓存的匹配规则。

was http app-cache rule { **type | key** } *string*

删除 app 缓存匹配规则配置。

no was http app-cache rule { **type | key** } *string*

【参数说明】

参数	描述
type *string*	匹配的文件类型，默认为 apk|ipa,支持正则表达式
key *string*	url 匹配规则, url 可分解为$host$path$name$args 等项目,可进行组合

【缺省配置】 rule type 缺省值为 “ipa|apk”
rule key 的缺省值为 “$path$name”

【命令模式】 全局模式

【缺省级别】 14

【使用指导】 根据配置的规则来决定是否对 http 报文进行缓存处理
1. 默认规则下文件名为 apk|ipa 的才缓存
2. 缓存文件的索引值算法为 URL 的 path 和 name 部分
对于规则不匹配的文件下载，不缓存

【配置举例】 1：配置为只缓存 apple 应用 ipa, (默认缓存 ipa 和 apk)

```
Ruijie(config)# was http app-cache rule type ipa
```

2：配置为只比较文件名，不管 url 中的路径及其它

```
Ruijie(config)# was http app-cache rule key $name
```

【检验方法】 1：使用 show was http app-cache config 查看配置
2：进行应用下载测试，查看缓存规则是否生效

【提示信息】 -

【常见错误】 -

【平台说明】 网关 EG，NBR 系列产品

2.3 was http inpath domain

设置域名，根据域名来生成 tcp 代理的动态 inpath 规则。
was http inpath domain *string*
删除配置
no was http inpath domain *string*

【参数说明】

参数	描述
string	域名或者 ip 地址

【缺省配置】 -

【命令模式】 全局模式

【缺省级别】 14

【使用指导】 配置后,访问此服务器的 tcp 流量才会进入 tcp 代理,从而进入应用缓存模块

如果配置为域名，则需要配置设备 dns。

【配置举例】 1：配置访问 apple store 的流量进入应用缓存。

```
Ruijie(config)# was http inpath domain ituns.apple.com
```

2：配置访问 10.0.0.10 的流量进入应用缓存。

```
Ruijie(config)# was http inpath domain 10.0.0.10
```

【检验方法】 1. show was http inpath domain

2. 进行下载测试，对应服务器的流量能进 tcp 代理

【提示信息】 -

【常见错误】 -

【平台说明】 网关 EG，NBR 系列产品

2.4 was http app-cache url

配置 app 缓存指定应用的跳转链接

was http app-cache url *string*

删除 app 缓存指定应用的跳转链接

no was http app-cache url *num*

no was http app-cache url *all*

【参数说明】

参数	描述
string	指定应用的跳转链接,配置后如果用户访问此页面，则其后 10 分钟内的应用下载动作才会触发应用缓存功能
num	删除序号
all	删除全部

【缺省配置】 -

【命令模式】 全局模式

【缺省级别】 14

【使用指导】 配置后,访问此服务器的 tcp 流量会进入 tcp 代理,从而进入应用缓存模块

用户访问此 url 后，接下来 10 分钟如果有进行应用下载，会触发应用缓存

如果 url 中 host 部分为域名，则需要配置设备 dns。

【配置举例】 1：指定厂家应用的下载页面

```
Ruijie(config)# was http app-cache url http://rujie.com.cn/appdownload.html
```

【检验方法】 1. 使用 **show was http app-cache config** 命令查看
2. 访问配置的 url，并下载应用

【提示信息】 -

【常见错误】 -

【平台说明】 网关 EG，NBR 系列产品

2.5 was http app-cache match url

配置 app 缓存指定应用 url 特征字符串
was http app-cache match url *string*
删除 app 缓存指定应用 url 特征字符串
no was http app-cache match url *string*
no was http app-cache match url *all*

【参数说明】

参数	描述
string	特征字符串，用于与 url 进行匹配

【缺省配置】 -

【命令模式】 全局模式

【缺省级别】 14

【使用指导】 配置后,在访问资源时，会将 url 与特征字符串进行比较，匹配时才会缓存

如果 url 中 host 部分为域名，则需要配置设备 dns。

【配置举例】 1：指定应用的 url 匹配特征字符串

```
Ruijie(config)# was http app-cache match test.com
Ruijie(config)# was http app-cache match qq
Ruijie(config)# was http app-cache match 360
```

【检验方法】 1. 使用 **show was http app-cache conig** 命令查看
2. 下载应用,验证指定缓存是否有根据特征字符串进行匹配生效

【提示信息】 -

【常见错误】 -

【平台说明】 网关 EG，NBR 系列产品

2.6 was http app-cache match app-name

配置 app 缓存指定应用的特征字符串
was http app-cache match app-name *string*
删除 app 缓存指定应用的特征字符串
no was http app-cache match app-name

【参数说明】

参数	描述
string	特征字符串，用于与应用名进行匹配

【缺省配置】 -

【命令模式】 全局模式

【缺省级别】 14

【使用指导】 配置后,在访问资源时，会将应用名与特征字符串进行比较，匹配时才会缓存

如果 url 中 host 部分为域名，则需要配置设备 dns。

【配置举例】 1：指定厂家应用的下载页面

```
Ruijie(config)# was http app-cache match app-name abc.app
Ruijie(config)# was http app-cache match app-name abc.apk
```

【检验方法】 1. 使用 **show was http app-cache config** 命令查看
2. 下载应用，会根据配置的特征字符串进行缓存

【提示信息】 -

【常见错误】 -

【平台说明】 网关 EG，NBR 系列产品

2.7 clear was http app-cache database

清除已缓存的文件

clear was http app-cache database

【参数说明】

参数	描述
-	

【缺省配置】 -

【命令模式】 全局模式

【缺省级别】 14

【使用指导】 清除已下载的缓存文件，空出磁盘空间

【配置举例】 1：清除已下载的缓存文件，空出磁盘空间

```
Ruijie(config)# clear was http app-cache database
```

【检验方法】 **show was http app-cache status** 查看磁盘空间

【提示信息】 -

【常见错误】 -

【平台说明】 网关 EG，NBR 系列产品

2.8 show was http app-cache database

显示应用缓存当前已缓存的文件信息

show was http app-cache database num

【参数说明】

参数	描述
num	显示条目数

【命令模式】 全局模式、特权模式、接口模式

【缺省级别】 14

【使用指导】 显示应用缓存当前已缓存的文件信息。

【配置举例】 -

【提示信息】 -

【平台说明】 网关 EG，NBR 系列产品

2.9 show was http app-cache config

显示应用缓存当前配置

show was http app-cache config

【参数说明】

参数	描述
-	-

【命令模式】 全局模式、特权模式、接口模式

【缺省级别】 14

【使用指导】 显示 app 缓存配置信息。

【配置举例】 -

【提示信息】 -

【平台说明】 网关 EG，NBR 系列产品

2.10 show was http app-cache status

显示所有应用缓存当前运行状态。

show was http app-cache status

【参数说明】

参数	描述
-	-

【命令模式】 全局模式、特权模式、接口模式

【缺省级别】 14

【使用指导】

【配置举例】 1：显示所有应用缓存当前运行状态.。

```
Ruijie#show was http app-cache status
app-cache : on

Http request count       : 1021
Http Cache hit count     : 0
Http Cache hit rate      : 0%
Http is_cacheable count  : 1
Http is_cacheble rate    : 0%
Http Cache count         : 787

Http app_cache cache total size   : 100.00GB
Http app_cache cache used  size   : 14.73MB
Http app_cache cache left  size   : 99.99GB



Cache disk space info:
Total_size              : 300452.93MB
Disk_available          : 283145.84MB
```

【提示信息】 -

【平台说明】 网关 EG，NBR 系列产品

2.11 show was http app-cache muldownload status

显示多线程下载文件的信息。

show was http app-cache muldownload status

【参数说明】

参数	描述
-	-

【命令模式】 全局模式、特权模式、接口模式

【缺省级别】 14

【使用指导】

【配置举例】 1：显示所有应用缓存当前运行状态.。

```
Ruijie#show was http app-cache muldownload status
filename                                size
  0b668ba1018def125c15f3760b2aa347     7804576
0b668ba1018def125c15f3760b2aa347-tmp:
  s138-23792520-41878397-133826528     9223807
  s141-41878398-75311012-133826528     7093886
  s140-75311013-131729375-133826528     9868573
  s139-112418973-131729375-133826528     6274685
  e139-131729376-132777951-133826528     1048576
  e138-132777952-133826527-133826528     1048576
```

【提示信息】 -

【平台说明】 网关 EG，NBR 系列产品

2.12 show was http inpath domain

显示应用缓存的域名解析状态。
show was http inpath domain

【参数说明】

参数	描述
-	-

【命令模式】 全局模式、特权模式、接口模式

【缺省级别】 14

【使用指导】 **show was http inpath domain** 查看当前配置及 dns 解析出的 ip 结果

【配置举例】 1：显示应用缓存的域名解析状态。

```
Ruijie# show was http inpath domain
0    domain: www.baidu.com
     0       14.215.177.37
     1       14.215.177.38
Ruijie#
```

【提示信息】 -

【平台说明】 网关 EG，NBR 系列产品

2.13 was httpd enable

启用 app 缓存文件本机下载服务

was httpd enable

停止 app 缓存文件本机下载服务

no was httpd enable

【参数说明】

参数	描述
-	-

【缺省配置】 -

【命令模式】 全局模式

【缺省级别】 14

【使用指导】 开启 app 缓存文件本机下载服务

【配置举例】 -

【检验方法】 1：使用 **show was httpd config** 查看配置是否生效

```
Ruijie# show was httpd config
was httpd enable                  : on
was httpd port                    : 6080
```

【提示信息】 -

【常见错误】 依赖于 was 模块的总开关，需要先开启 was enable 后此配置才生效

【平台说明】 网关 EG，NBR 系列产品

2.14 was httpd hot-html-generate app-cahce

生成资源列表文件

was httpd hot-html-generate app-cahce filter *string1* **filename** *string2*

【参数说明】

参数	描述
string1	过滤条件，例: ipa|apk
string2	文件名

【命令模式】 特权模式

【缺省级别】 14

【使用指导】 **1. show was httpd hot-html database** *num* 可以查看当前已生成的文件

【配置举例】 1：显示应用缓存的域名解析状态。

```
Ruijie# was http hot-html-generate app-cache
Create hot html succ url: http://127.0.0.1:6080/hot_html/appc-cache-hot.html
```

【提示信息】 -

【平台说明】 网关 EG，NBR 系列产品

2.15 show was httpd config

显示 app 缓存文件下载服务的配置

show was httpd config

【参数说明】

参数	描述
-	-

【命令模式】 全局模式、特权模式、接口模式

【缺省级别】 14

【使用指导】 显示 app 缓存配置信息。

【配置举例】 -

【提示信息】 -

【平台说明】 网关 EG，NBR 系列产品

2.16 show was httpd hot-html database

显示已生成的缓存资源列表文件

show was httpd hot-html database *num*

【参数说明】

参数	描述
num	显示条目数

【命令模式】 全局模式、特权模式、接口模式

【缺省级别】 14

【使用指导】 显示已生成的缓存资源列表文件

【配置举例】 -

【提示信息】 -

【平台说明】 网关 EG，NBR 系列产品

2.17 clear was httpd hot-html database

清除已缓存的文件

clear was http hot-html database

【参数说明】

参数	描述
-	

【缺省配置】 -

【命令模式】 特权模式

【缺省级别】 14

【使用指导】 清除所有资源列表文件

【配置举例】 1：清除资源列表文件，空出磁盘空间

```
Ruijie# clear was http hot-html database
```

【检验方法】 show was httpd hot-html database

【提示信息】 -

【常见错误】 -

【平台说明】 网关 EG，NBR 系列产品

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

命令	作用
ac-controller	进入 AC 配置模式
acctrl-trap	配置 AC 上相关 trap 的开关
ac-name	配置 AC 的名称
ap-auth	配置指定 AP 进行接入认证功能
ap-auth enable	配置 AP 开启指定的接入认证功能
ap-auth serial-update	配置所有在线 AP 更新认证序列号
ap-backup group	配置 AP 备份组
ap-backup-group	配置 AP 加入 AP 备份组
ap-config	进入指定 AP 的配置模式
ap-group	创建新的 AP 组，或者进入一个 AP 组的配置模式
ap-group（AP 配置模式）	配置 AP 属于指定的 AP 组
ap-mac	绑定 AP 的 MAC 地址
ap-name	配置 AP 的名称
ap-priority	开启/关闭对 AP 的 Failover 优先级的支持
bind-ap-mac	配置开启 AP 合规性检查
credential	配置 AP 的用户名和密码
enable-broad-ssid	开启 SSID 广播
factory-reset	配置将指定的 AP 恢复出厂设置
interface-mapping	配置映射
logging on	配置允许显示系统日志信息
logging server	配置日志服务器地址
nas-id	配置用户接入地编号
priority	配置设备 Failover 的优先级
reload at	配置指定 AP 每天定时重启
reset	配置所有的 AP、有更新过软件版本的 AP、指定 AP 复位
show ac-config	显示本 AC 的基本配置信息
show ac-config ap-backup-group	显示 AP 备份组信息
show ap-config bssid	显示所有 AP 的 BSSID 列表
show ap-config cb	显示 AP 的状态信息
show ap-config inherit-wlan	显示 AP 从 AP 备份组的主 AP 集成而来的 wlan 信息
show ap-config product	显示 AP 产品统计列表
show ap-config summary	显示 AP 列表
show ap-config summary ap-auth	显示所有 AP 认证相关信息
show ap-config summary deny-ap	显示尝试关联但是被 AC 拒绝的 AP 列表
show ap-group aps	显示连接到指定 AP 组的 AP 列表
show ap-group aps summary	显示所有 AP 组的 AP 列表
show ap-group cb	显示指定 AP 组的基本配置信息

show ap-group intf-wlan-map	显示 AP 组的 WLAN-VLAN 映射信息
show ap-group summary	显示本 AC 配置的所有 AP 组列表
show wlan-config cb	显示指定 WLAN 信息
show wlan-config summary	该命令用于查看 AC 上的 WLAN 配置列表
ssid	修改 WLAN 的 ssid 名字
statistics-timer	设置指定 AP 或指定 AP 组内的所有 AP 的定时上传统计信息的时间间隔
wlan-config	创建 WLAN 并且进入 WLAN 配置模式
wtp-limit	配置 AP 上支持的最大 AP 数量

1.1 ac-controller

在全局配置模式下通过该命令进入 AC 配置模式。

ac-controller

【参数说明】

参数	描述
-	-

【缺省配置】 无

【命令模式】 全局配置模式

【缺省级别】 15

【使用指导】 无。

【配置举例】 1：进入 AC 配置模式。

```
Ruijie(config)# ac-controller
Ruijie(config-ac)#
```

【检验方法】 -

【提示信息】 -

【常见错误】 -

【平台说明】 仅 AC 支持

1.2 acctrl-trap

在 AC 配置模式下，通过 **acctrl-trap** 来控制 AC 上相关 trap 的开关。

acctrl-trap [**acap-updown-ctrl** | **acap-joinfail-ctrl** | **acap-decryeroreport-ctrl** | **acap-imageupdt-ctrl** | **acap-timestamp-ctrl** | **acsta-oper-ctrl**]

恢复至缺省配置。
no acctrl-trap [**acap-updown-ctrl** | **acap-joinfail-ctrl** | **acap-decryeroreport-ctrl** | **acap-imageupdt-ctrl** | **acap-timestamp-ctrl** | **acsta-oper-ctrl**]

【参数说明】

参数	描述
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。

【命令模式】 AC 配置模式

【缺省级别】 15

【使用指导】 用来控制 AC 上相关 trap 的开关。

【配置举例】 1：配置 AC 开启 AP 加入 AC 失败的 trap 消息的发送。

```
Ruijie(config)#ac-controller
Ruijie(config-ac)#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

【提示信息】 -

【常见错误】 -

【平台说明】 仅 AC 支持

1.3 ac-name

在 AC 配置模式下，通过 **ac-name** 来配置 AC 的名称，便于用户识别。
ac-name *ac-name*

恢复至缺省配置。

no ac-name

【参数说明】

参数	描述
ac-name	配置 AC 的名称，最多可配置 63 个字符，不能包含空格。

【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

【命令模式】 AC 配置模式

【缺省级别】 15

【使用指导】 可以给不同的 AC 配置不同的名称便于用户管理。

【配置举例】 1：配置 AC 名称为 ruijie-ac。

```
Ruijie(config-ac)# ac-name ruijie-ac
```

【检验方法】 通过 **show ac-config** 命令可以查看当前 AC 名称。

【提示信息】 -

【常见错误】 -

【平台说明】 仅 AC 支持

1.4 ap-auth

在 AP 配置模式下，通过 **ap-auth** 命令配置指定 AP 进行接入认证功能。可以使用的方法有：基于 AP 的序列号，基于 AP 的密码，基于 AP 的证书。

ap-auth { **serial** *serial-string* | **password** *password* | **ac-cert** *ac-cert-name* | **ap-cert** *ap-cert-name* }

通过 **no** 命令删除相关配置。

no ap-auth { **serial** | **password** | **ac-cert** | **ap-cert** }

【参数说明】

参数	描述
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 配置模式

【缺省级别】 15

【使用指导】 AP 上线时的认证，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。

【配置举例】 1：配置 AP1 的认证序列号。

```
Ruijie# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Ruijie(config)# ap-config AP1
Ruijie(config-ap)# ap-auth serial 123456
```

2：删除 AP1 的认证序列号

```
Ruijie# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Ruijie(config)# ap-config AP1
Ruijie(config-ap)# no ap-auth serial
```

【检验方法】 **show ap-config running** 显示 AP 的各配置情况

【提示信息】 -

【常见错误】 -

【平台说明】 本命令在 WLAN AC 系列产品上支持

1.5 ap-auth enable

在 AC 配置模式下，通过 **ap-auth enable** 命令配置 AP 开启指定的接入认证功能。可以开启使用的方法有：基于 AP 的序列号，基于 AP 的密码，基于 AP 的证书。
ap-auth [**serial** | **password** | **certificate**] **enable**

关闭 AP 的接入认证。
no ap-auth [**serial** | **password** | **certificate**] **enable**

【参数说明】

参数	描述
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

【缺省级别】 15

【使用指导】 无。

【配置举例】 1：开启基于 AP 接入序列号的认证功能。

```
Ruijie(config)# ac-controller
Ruijie(config-ac)# ap-auth serial enable
```

2: 关闭基于 AP 接入序列号的认证功能

```
Ruijie(config)# ac-controller
Ruijie(config-ac)# no ap-auth serial enable
```

【检验方法】 -

【提示信息】 -

【常见错误】 -

【平台说明】 本命令在 WLAN AC 系列产品上支持

1.6 ap-auth serial-update

在 AC 配置模式下，通过 **ap-auth serial-update** 命令配置所有在线 AP 更新认证序列号。

ap-auth serial-update

【参数说明】

参数	描述
-	-

【缺省配置】 缺省为不配置。

【命令模式】 AC 配置模式

【缺省级别】 15

【使用指导】 该配置将使得所有在线 AP 以当前 AP 的序列号作为认证的序列号配置

【配置举例】 1：配置所有在线 AP 更新认证序列号。

```
Ruijie(config)# ac-controller
Ruijie(config-ac)# ap-auth serial-update
```

【检验方法】 -

【提示信息】 -

【常见错误】 -

【平台说明】 本命令在 WLAN AC 系列产品上支持

1.7 ap-backup group

在 AC 配置模式下，通过 **ap-backup group** 命令创建 AP 备份组。
ap-backup group *name*

删除 AP 备份组
no ap-backup group *name*

【参数说明】

参数	描述
name	AP 备份组名称，default 系统保留，即不允许配置 default 作为组名字

【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

【缺省级别】 15

【使用指导】 使用 no 命令删除 AP 备份组时，如果组内有 AP 成员，组内 AP 加入到 default 组，default 组的 AP 备份功能不生效

【配置举例】 1：创建一个 AP 备份组，组名为 apbackup-test-group。

```
Ruijie(config)# ac-controller
Ruijie(config-ac)# ap-backup group apbackup-test-group
```

2：删除一个 AP 备份组，组名为 apbackup-test-group。

```
Ruijie(config)# ac-controller
Ruijie(config-ac)# no ap-backup group apbackup-test-group
```

【检验方法】 **show ac-config ap-backup-group** 查看创建的 AP 备份组

【提示信息】 -

【常见错误】 -

【平台说明】 本命令在 WLAN AC 系列产品上支持

1.8 ap-backup-group

可以通过 AP 配置模式下的 ap-**backup group** 命令来配置 AP 属于指定的 AP 备份组。
ap-backup-group *name* [**master**]

通过 **no** 前缀将 AP 移出 AP 备份组或者取消其主 AP 角色。
no ap-backup-group [*name*] [**master**]

【参数说明】

参数	描述
name	AP 备份组名称
master	可选关键字，用于指定该 AP 作为主 AP 加入到 AP 备份组

【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

【缺省级别】 15

【使用指导】 把 AP 加入 AP 备份组之前，备份组需要已经存在。命令加上 master 关键字则表示把该 AP 设置为 AP 备份组的主 AP，如果 AP 组已存在一个主 AP，不允许第二个以主 AP 角色的 AP 加入到 AP 备份组，如果需要变更 AP 备份组的主 AP，需要先使用 no 命令取消之前的主 AP。

【配置举例】 1：配置 AP 加入 backup-test-group 组，并设置为该组的主 AP

```
Ruijie(config)# ap-config AP0001
Ruijie(config-ap)# ap-backup-group backup-test-group master
```

2：设置已经在 AP 备份组的 AP 取消其主 AP 角色

```
Ruijie(config-ap)# no ap-backup-group backup-test-group master
```

3：配置 AP 移出 AP 备份组

```
Ruijie(config)# ap-config AP0001
Ruijie(config-ap)# no ap-backup-group
```

【检验方法】 **show ap-config running** 和 **show ac-config ap-backup-group** 查看配置

【提示信息】 -

【常见错误】 -

【平台说明】 仅 AC 支持

1.9 ap-config

通过 **ap-config** 命令可以创建 AP 配置，或者进入 AP 配置模式。
ap-config *ap-name*

该命令可以通过 **no** 前缀将一个已经存在的 AP 组删除。
no ap-config *ap-name*

【参数说明】

参数	描述
ap-name	要配置的 AP 的名称。

【缺省配置】 无。

【命令模式】 全局配置模式

【缺省级别】 15

【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。

【配置举例】 1：创建名称为 Ruijie_AP 的 AP 配置

```
Ruijie(config)#ap-config Ruijie_AP
You are going to config AP(Ruijie_AP), which is not on line now.
Ruijie(config-ap)#
```

2：配置删除名称为 Ruijie_AP 的 AP 配置

```
Ruijie(config)# no ap-config Ruijie_AP
```

【检验方法】 通过 **show ap-config running** 命令可以查看所有 AP 配置。

【提示信息】 -

【常见错误】 -

【平台说明】 仅 AC 支持

1.10 ap-group

所有加入 AC 的 AP 在一个时刻都会属于且仅属于某个特定的 AP 组。新加入的 AP 都属于默认 AP 组 :default。可以通过 **ap-group** 来创建新的 AP 组，或者进入一个 AP 组的配置模式。如果是创建 AP 组，则在创建后会进入该 AP 组的配置模式。。

ap-group *ap-group-name*

该命令可以通过 **no** 前缀将一个已经存在的 AP 组删除。

no ap-group *ap-group-name*

【参数说明】

参数	描述
ap-group-name	AP 组名称，长度最大 63 字节，不能有空格。

【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

【缺省级别】 15

【使用指导】 删除 AP 组时，属于该 AP 组的 AP 将自动切换到 default 组。

【配置举例】 1：创建一个 AP 组，AP 组名为 test-group。

```
Ruijie(config)# ap-group test-group
Ruieji(config-ap-group)#
```

2：删除一个 AP 组，AP 组名为 test-group

```
Ruijie(config)#no ap-group test-group
```

3：进入一个 AP 组，例子中进入默认 AP 组，AP 组名为 default

```
Ruijie(config)# ap-group default
```

【检验方法】 -

【提示信息】 -

【常见错误】 -

【平台说明】 仅 AC 支持

1.11 ap-group（AP 配置模式）

所有加入 AC 的 AP 在一个时刻都会属于且仅属于某个特定的 AP 组。新加入的 AP 都属于默认 AP 组 :default。可以通过 AP 配置模式下的 **ap-group** 命令来配置 AP 属于指定的 AP 组。

ap-group *ap-group-name*

通过 **no** 前缀将 AP 恢复到 default 组。

no ap-group

【参数说明】

参数	描述
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

【缺省级别】 15

【使用指导】 删除 AP 组时，属于该 AP 组的 AP 将自动切换到 default 组

【配置举例】 1：配置 AP 加入 test-group 组。

```
Ruijie(config)# ap-group test-group
Ruieji(config-ap-group)#
Ruijie(config)# ap-config AP0001
Ruijie(config-ap)# ap-group test-group
```

2：配置 AP 恢复到 default 组

```
Ruijie(config)# ap-config AP0001
Ruijie(config-ap)# no ap-group test-group
```

【检验方法】 -

【提示信息】 -

【常见错误】 -

【平台说明】 仅 AC 支持

1.12 ap-mac

在 AP 配置模式上可以通过 **ap-mac** 来绑定 AP 的 MAC 地址。
ap-mac *ap-mac*

no 命令删除 **ap-mac** 的绑定。
no ap-mac

【参数说明】

参数	描述
ap-mac	AP 的 MAC 地址。

【缺省配置】 无

【命令模式】 AP 配置模式

【缺省级别】 15

【使用指导】

- 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。
- 在热备环境中，通过绑定 AP 的 MAC 地址，保证两台 AC 之间配置的一致性。

【配置举例】 1：绑定 ap test 的 AMC 地址为 00ff.ffff.1111

```
Ruijie(config)# ap-config test
Ruijie(config-ap)# ap-mac 00ff.ffff.1111
```

【检验方法】 通过 **show ap-config running** 命令查看当前 AP 的 ap-mac 配置。

【提示信息】 -

【常见错误】 -

【平台说明】 仅 AC 支持

1.13 ap-name

AC 设备在 AP 的配置模式下，或者 AP 设备上的配置模式下，通过 **ap-name** 来配置 AP 的名称。
ap-name *ap-name*

删除 AP 名称配置。
no ap-name

【参数说明】

参数	描述
ap-name	配置 AP 的名称，最多可配置 63 个字符，不能包含空格。

【缺省配置】 无。

【命令模式】 AP 配置模式

【缺省级别】 15

【使用指导】

- **AC 上配置**：

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。

最多可配置 63 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 上配置**：

如果 AP 在线，那么配置名字后，断开隧道，重新建立连接，如果 AC 上没有修订 AP 的名字，即 AC 上是默认

的名字，那么就采用 AP 修订的名字接入，否则已 AC 上配置的名字为准。

如果 AP 不在线，AP 接入 AC，如果 AC 上没有离线配置，那么就以 AP 的配置为准，如果 AC 有离线配置那么以 AC 配置为准。

如果 AP 配置的名字和 AC 上的其他 AP 的名字配置冲突，那么 AP 接入不成功。

最多可配置 63 个字符，不能包含空格。

不能配置 AP 名称为 “all”。

【配置举例】 1：AC 上配置 AP0001 的新名称为 AP_NEW。

```
Ruijie(config)# ap-config AP0001
Ruijie(config-ap)# ap-name AP_NEW
```

2：AP 上配置名字为 AP_TEST。

Ruijie(config)# ap-name AP_ TEST

【检验方法】 1：**AC 上**

通过 **show ap-config running** 命令查看当前 AP 配置情况。

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。

2：**AP 上**

通过 show running 命令查看当前 AP 名字的配置情况。

【提示信息】 -

【常见错误】 -

【平台说明】 AC 和瘦 AP 支持

1.14 ap-priority

在 AC 配置模式下，通过 **ap-priority** 命令上开启/关闭对 AP 的 Failover 优先级的支持。

ap-priority { **enable** | **disable** }

【参数说明】

参数	描述
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

【缺省级别】 15

【使用指导】 无。

【配置举例】 1：AP0001 同 AC1 建立连接。配置该 AP（AP0001）的 Failover 优先级为 3，并打开 AC1 的 Failover 优先级功能支持开关。

```
Ruijie(config)# ap-config AP0001
Ruijie(config-ap)# priority 3
Ruijie(config-ap)# exit
Ruijie(config)# ac-controller
Ruijie(config-ac)# ap-priority enable
```

【检验方法】 -

【提示信息】 -

【常见错误】 -

【平台说明】 仅 AC 支持

1.15 bind-ap-mac

通过 **bind-ap-mac** 命令配置开启 AP 合规性检查。
bind-ap-mac

关闭 AP 合规性检查。
no bind-ap-mac

【参数说明】

参数	描述
-	–

【缺省配置】 关闭。

【命令模式】 AC 配置模式

【缺省级别】 15

【使用指导】

- 通过 AC 配置模式下 **bind-ap-mac** 命令开启 AP 合规性检查。
- **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

【配置举例】 1：配置开启 AP 合规性检查

```
Ruijie(config)# ac-controller
Ruijie(config-ac)# bind-ap-mac
```

2：配置关闭 AP 合规性检查

```
Ruijie(config)# ac-controller
Ruijie(config-ac)# no bind-ap-mac
```

【检验方法】 -

【提示信息】 -

【常见错误】 -

【平台说明】 仅 AC 支持

1.16 credential

用户可以通过 **credential** 来配置 AP 的用户名和密码。
credential *user-name password*

取消该配置。
no credential

【参数说明】

参数	描述
user-name	AP 上要使用的用户名，不允许带空格
password	AP 上要使用的密码，不允许带空格

【缺省配置】 该命令没有缺省配置。

【命令模式】 AP 配置模式或 AP 组配置模式

【缺省级别】 15

【使用指导】 无

【配置举例】 1：配置 AP0001 的用户名为：first-ap，密码为：123456

```
Ruijie(config)# ap-config AP0001
Ruijie(config-ap)# credential first-ap 123456
```

2：配置 AP 组（Default）下所有 AP 的用户名为：first-ap，密码为：123456

```
Ruijie(config)# ap-group default
Ruijie(config-ap-group)# credential first-ap 123456
```

【检验方法】 -

【提示信息】 -

【常见错误】 -

【平台说明】 仅 AC 支持

1.17 enable-broad-ssid

在 WLAN 配置模式下通过 **enable-broad-ssid** 来开启 SSID 广播
enable-broad-ssid

禁止 SSID 广播
no enable-broad-ssid

【参数说明】

参数	描述
-	-

【缺省配置】 缺省情况下，为 enable

【命令模式】 WLAN 配置模式

【缺省级别】 15

【使用指导】 配置该 WLAN 的 Suppress SSID 信息，该配置仅在 WLAN 应用前配置生效。
如果 WLAN 已经部署，该命令将导致当前关联该 WLAN 的用户下线。

【配置举例】 1：开启该 WLAN 上的 SSID 广播

```
Ruijie(config-wlan)#enable-broad-ssid
```

2：禁用该 WLAN 上的 SSID 广播。

```
Ruijie(config-wlan)#no enable-broad-ssid
```

【检验方法】 -

【提示信息】 -

【常见错误】 -

【平台说明】 仅 AC 支持

1.18 factory-reset

通过 **factory-reset** 命令配置将指定的 AP 恢复出厂设置，该操作会引起该 AP 复位。

factory-reset *ap-name*

【参数说明】

参数	描述
ap-name	要恢复出厂设置的 AP 名称

【缺省配置】 无

【命令模式】 AC 配置模式

【缺省级别】 15

【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。

【配置举例】 1：配置 AP0001 恢复出厂设置

```
Ruijie(config-ac)# factory-reset AP0001
```

【检验方法】 -

【提示信息】 -

【常见错误】 -

【平台说明】 仅 AC 支持

1.19 interface-mapping

在 AP 组配置模式下通过 **interface-mapping** 来将 wlan-vlan 或者 wlan-vlan-group mapping (本命令各项说明中的 mapping 即指 wlan-vlan 或者 wlan-vlan-group mapping) 映射到 AP 组内的所有 AP 的 radio 上。通过该映射可以将 wlan 的相关配置信息应用到指定的 radio 上。

interface-mapping *wlan-id* [*vlan-id* | **group** *vlan-group-id*] [**radio** {*radio-id* | [*802.11b* | *802.11a*]}] [**ap-wlan-id** *ap-wlan-id*]

将相关的 mapping 配置删除。

no interface-mapping *wlan-id* [*vlan-id* I **group** *vlan-group-id*] [**radio** {*radio-id* | [*802.11b* | *802.11a*]}] [**ap-wlan-id** *ap-wlan-id*]

【参数说明】

参数	描述
wlan-id	要被映射的 wlan 的 ID，该 wlan 必须已经创建，取值范围为 1~4094
vlan-id	要被映射的 vlan 的 ID，取值范围为 1~4094
vlan-group-id	要被映射的 vlan-group 的 ID，取值范围为 1~128
radio-id	要应用指定 mapping 的 AP 的 radio，取值范围预留标准定义的 1~48 若不指定 radio-id 参数，则该 mapping 会被应用到该 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 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。

【缺省配置】 无。

【命令模式】 AP 组配置模式

【缺省级别】 15

【使用指导】 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。由于 AP 的 VLAN 是由接入交换机决定的，当 STA 的 VLAN 和接入交换机的 Native VLAN 相同时，也需要 ap-vlan 和接入交换机的 Native VLAN 相同，否则 STA 将无法通讯(上行要求和 AP 属于不同 VLAN，而下行又要求使用相同 VLAN，两者冲突)。

【配置举例】 1：创建 vlan 2，创建一个 ID 为 4094 的 wlan，并将 wlan4094-vlan2 的 mapping 应用到默认 AP 组内所有 AP 的 radio 1 上

```
Ruijie(config)#vlan 2
Ruijie(config)#wlan-config 4094 pro-4094 ssid-4094
Ruijie(config-wlan)#exit
Ruijie(config)#ap-group default
Ruijie(config-ap-group)#interface-mapping 4094 2 radio 1
```

2：创建 vlan-group 3，创建一个 ID 为 4094 的 wlan，并将 wlan4094-vlan-group3 的 mapping 应用到默认 AP 组内所有 AP 的所有 radio 上

```
Ruijie(config)#vlan-group 3
Ruijie(config)#wlan-config 4094 pro-4094 ssid-4094
Ruijie(config-wlan)#exit
```

```
Ruijie(config)#ap-group default
Ruijie(config-ap-group)#interface-mapping 4094 group 3
```

3：进入默认 AP 组，删除已经配置过的 wlan4094-vlan2 mapping

```
Ruijie(config)# ap-group default
Ruieji(config-ap-group)# no interface-mapping 4094 2 radio 1
```

【检验方法】 -

【提示信息】 -

【常见错误】 -

【平台说明】 仅 AC 支持

1.20 logging on

配置 AP 打开系统日志显示。
logging on

使用该命令的 **no** 选项禁止 AP 显示系统日志信息
no logging on

【参数说明】

参数	描述
-	-

【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

【缺省级别】 15

【使用指导】 无

【配置举例】 1：配置 AP 禁止打印系统日志

```
Ruijie(config-ap)#no logging on
```

【检验方法】 -

【提示信息】 -

【常见错误】 -

【平台说明】 仅 AC 支持

1.21 logging server

配置 AP 将系统日志信息记录到执行服务器。
logging server *ip-address* **[udp-port** *num***]**

使用该命令的 no 选项删除指定服务器
no logging server *ip-address*

【参数说明】

参数	描述
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）。

【缺省配置】 无

【命令模式】 AP 配置模式/所有 AP 配置模式

【缺省级别】 15

【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。

【配置举例】 1：配置日志服务器的地址为 1.1.1.1

```
Ruijie(config-ap)# logging server 1.1.1.1
```

【检验方法】 -

【提示信息】 -

【常见错误】 -

【平台说明】 仅 AC 支持

1.22 nas-id

配置 WLAN 用户或 AC 接入地编号。
nas-id *nas-id*

使用该命令的 **no** 选项可以恢复至缺省配置

no nas-id

【参数说明】

参数	描述
nas-id	接入地编号，包含 32 个字符，不能带空格

【缺省配置】 WLAN 用户接入地编码缺省空字符串

AC 接入地编码缺省 AC MAC 地址点分形式字符串

【命令模式】 WLAN 配置模式或 AC 配置模式

【缺省级别】 15

【使用指导】 无

【配置举例】 1：配置 WLAN 接入用户地编号为 0000059159100460

```
Ruijie(config-wlan)# nas-id 0000059159100460
```

2：恢复 WLAN 接入用户地编号为默认值

```
Ruijie(config-wlan)# no nas-id
```

3：配置 AC 接入地编号为 123456789

```
Ruijie(config-ac)#nas-id 123456789
```

2：恢复 AC 接入地编号为默认值

```
Ruijie(config-ac)# no nas-id
```

【检验方法】 通过 show wlan-config cb 命令查看指定 WLAN 用户接入地编码

```
Ruijie(config)#show wlan-config cb 1
WLAN ID..................................... 1
SSID........................................ 1-leichen-test-wlan
Profile.....................................
MAC Mode.................................... Local
Tunnel Mode................................. 802.3 Tunnel
Suppress SSID............................... Disable
Sta-limit................................... 0
NAS ID...................................... 0000059159100460
Band Select................................. Disable
SSID Code...................................
```

通过 show ac-config 命令查看 AC 接入地编码

```
Ruijie(config)# show ac-config
AC Configuration info:
max_wtp          :10
sta_limit        :81920
license wtp max  :2560
license sta max  :81920
serial auth      :Disable
password auth    :Disable
certificate auth :Disable
Bind AP MAC      :Disable
AP Priority      :Enable
supp_psk_cer     :Disable
ac_name          :Ruijie_Ac_050607
ac location      :Ruijie_COM

AC State info:
sta_num          :1
act_wtp          :1
localIpAddr      :10.10.10.10
localIpAddr6     :::
used wtp         :1.0(0 four 1 normal 0 half)
remain wtp       :2 four 9 normal 18 half
HW Ver           :1.00
SW Ver           :AC_RGOS 11.1(5)B6, Release(02193103)
Mac address      :00d0.0405.0607
Product ID       :WS6816
NET ID           :9876543210012345
NAS ID           :123456789
```

【提示信息】 -

【常见错误】 -

【平台说明】 仅 AC 支持

1.23 priority

该命令用于设置 AP 的 Failover 优先级，在 AC 上开启对 AP 的 Failover 优先级的支持后， AC 可以按照 AP 的优先级顺序来接受 AP 的接入。

priority *priority-value*

【参数说明】

参数	描述

priority-value	配置 AP 的 Failover 的优先级。 允许的取值为 1~4，其中 1 为最低优先级，4 为最高优先级

【缺省配置】 AP 的 Failover 的缺省优先级为 1

【命令模式】 AP 配置模式

【缺省级别】 15

【使用指导】 配置设备 Failover 的优先级。1 的优先级最低，4 的优先级最高。这里配置的 AP 加入 AC 顺序（即 AP 的优先级），在配置后就会保存在 AP 中，当 AP 下次进行关联的时候生效。

【配置举例】 1：配置 AP 组 apgroup 的 Failover 优先级为 3

```
Ruijie#config terminal
Ruijie(config)#ap-config ap001
Ruijie(config-ap)#priority 3
```

【检验方法】 -

【提示信息】 -

【常见错误】 -

【平台说明】 仅 AC 支持

1.24 reload at

可以在 AP 配置模式下通过 **reload at** 命令配置指定 AP 每天定时重启。
reload at *time*

删除每天定时重启配置
no reload at

【参数说明】

参数	描述
time	以 hh:mm:ss 形式定义的每天定时重启的时间点。

【缺省配置】 无

【命令模式】 AP 配置模式

【缺省级别】 15

【使用指导】 无

【配置举例】 1：配置 Ruijie-AP1 在每天的 1:00:00 定时重启

```
Ruijie(config)#ap-config Ruijie-AP1
Ruijie(config-ap)#reload at 1:00:00
```

【检验方法】 -

【提示信息】 -

【常见错误】 -

【平台说明】 仅 AC 支持

1.25 reset

可以在 AC 配置模式下通过 **reset** 命令配置所有的 AP 或者指定 AP 复位。

reset { **all** | **single** *ap-name* }

【参数说明】

参数	描述
all	复位所有的 AP。
single *ap-name*	复位指定的 AP

【缺省配置】 无

【命令模式】 AC 配置模式

【缺省级别】 15

【使用指导】 无

【配置举例】 1：配置所有的 AP 复位

```
Ruijie(config-ac)# reset all
```

2：配置名称为 AP0001 的 AP 复位

```
Ruijie(config-ac)# reset AP0001
```

【检验方法】 -

【提示信息】 -

【常见错误】 -

【平台说明】 仅 AC 支持

1.26 show ac-config

显示本 AC 的基本配置信息

show ac-config

【参数说明】

参数	描述
-	-

【命令模式】 任意模式

【缺省级别】 1

【使用指导】 无

【配置举例】 1：本 AC 的基本配置信息

```
Ruijie(config)#show ac-config
AC Configuration info:
max_wtp          :128
sta_limit        :4096
license wtp max  :128
license sta max  :4096
serial auth      :Disable
password auth    :Disable
certificate auth :Disable
Bind AP MAC      :Disable
AP Priority      :Disable
ac_name          :Ruijie_Ac_231455
ac location      :Ruijie_COM

AC State info:
sta_num          :0
act_wtp          :12
used wtp          :8( 4 normal 8 half)
remain wtp        :120 normal 240 half
HW Ver           :1.0
SW Ver           :AC_RGOS 11.1(1)B1
```

```
Mac address       :001a.9923.1455
Product ID        :WS5708
NET ID            :9876543210012345
NAS ID            :001a.9923.1455
```

【提示信息】 -

【平台说明】 仅 AC 支持

1.27 show ac-config ap-backup-group

显示本 AC 的 AP 备份组信息

show ac-config ap-backup-group [*group-name*]

【参数说明】

参数	描述
group-name	创建的 AP 备份组名称，可选，不显示 default 组的信息

【命令模式】 任意模式

【缺省级别】 1

【使用指导】 无

【配置举例】 1：显示本 AC 的 AP 备份组信息

```
Ruijie#show ac-config ap-backup-group
Cnt    Group-Name                  Master-AP cnt   Standby-AP cnt    Master-AP-Name     Working
------ ----------------------------------- ------------ ----------- ------------  -----------
1      AP-BACKUP-GROUP1            1               2                 AP4210-1            false
```

2：显示 AP 备份组 AP-BACKUP-GROUP1 的详细信息

```
Ruijie#show ac-config ap-backup-group AP-BACKUP-GROUP1
Cnt     Ap-Name                    Ap-Mac              Online    Is-Master   Inherit-Wlan Cnt
------- ------------------------- -------------------- -------- ------------ ------------------
1      AP4210-1                   8832.0000.1111      true       Yes        0
2      APD-M-1                         -              false      No         0
3      APD-M-2                    0011.4477.8833      true       No         0
```

【提示信息】 -

【平台说明】 仅 AC 支持

1.28 show ap-config bssid

显示所有 AP 的 BSSID 列表

show ap-config bssid

【参数说明】

参数	描述
-	-

【命令模式】 任意模式

【缺省级别】 1

【使用指导】 无

【配置举例】 1：查看所有 AP 的 BSSID 列表

```
Ruijie(config)#show ap-config bssid
AP Mac          Radio ID WLAN ID  BSSID
--------------- -------- -------- --------------
5869.6c75.7677         1        2 0669.6c75.7679
5869.6c75.7677         2        2 0669.6c75.767a
```

【提示信息】 -

【平台说明】 仅 AC 支持

1.29 show ap-config cb

显示 AP 的状态信息

show ap-config cb *ap-name*

【参数说明】

参数	描述
ap-name	要查询的 AP 的名称

【命令模式】 特权模式

【缺省级别】 1

【使用指导】 无

【配置举例】 1：显示 AP 的状态信息

```
ac#show ap-config cb wlan-ap-0001
Configuration:
ap name             :wlan-ap-0001
ap fallback         :1
group name          :default

Status:
local ipv4          :192.168.120.2
WTP Name            :wlan-ap-0001
```

【提示信息】 -

【平台说明】 仅 AC 支持

1.30 show ap-config inherit-wlan

显示 AP 备份组的备份 AP 继承的 WLAN 信息

show ap-config inherit-wlan *ap-name*

【参数说明】

参数	描述
ap-name	要查询的 AP 的名称

【命令模式】 特权模式

【缺省级别】 1

【使用指导】 无

【配置举例】 1：显示备份 AP 继承的 WLAN 信息

```
ac#show ap-config inherit-wlan wlan-ap-0001
WLAN ID  SSID                  VLAN-Id/VLAN-Group ID     Radio ID                    AP WLAN ID
-------- --------------------- ------------------------- --------------------------- -----------
1        ruijie-wifi            1100                      ALL                         1
```

【提示信息】 -

【平台说明】 仅 AC 支持

1.31 show ap-config product

显示 AP 产品统计列表

show ap-config product

【参数说明】

参数	描述
-	-

【命令模式】 特权模式

【缺省级别】 1

【使用指导】 无

【配置举例】 1：显示 AP 产品统计列表

```
Ruijie#show ap-config product
Product ID           Hardware Version Count    Used Wtp
-------------------- ---------------- -------- --------
AP120                              1.0       10      5.0
AP220-E                            1.0        5      5.0
AP320                              2.0        8      8.0
AP530-PPC                          1.5        2      2.0
```

【提示信息】 -

【平台说明】 仅 AC 支持

1.32 show ap-config summary

显示 AP 列表

show ap-config summary

【参数说明】

参数	描述
-	-

【命令模式】 特权模式

【缺省级别】 1

【使用指导】 无

【配置举例】 1：显示 AP 列表

```
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
       Channel: * = Global
       Power Level = Percent

Online AP number: 2
Offline AP number: 1

AP Name                                IP Address       Mac Address     Radio               Radio
Up/Off time   State
---------------------------------------- --------------- -------------- --------------------
------------------- ------------- -----
AP220E-2                               22.22.22.11      00d0.1414.3f67 1  E   0   11*  100 2  E
0  153*  100    0:00:37:34 Run
xh-ap                                  10.21.121.4      00d0.f822.33d6 1# N   0    -     - 2# N
0    -     -    0:23:56:05 Run
AP220E_V2.0_19                               -          1414.4b13.96f7 1  N   -    -     - 2  N
-    -     -    0:00:14:07 Quit
```

【提示信息】 -

【平台说明】 仅 AC 支持

1.33 show ap-config summary ap-auth

显示所有 AP 的认证相关信息

show ap-config summary ap-auth

【参数说明】

参数	描述
-	-

【命令模式】 特权模式

【缺省级别】 1

【使用指导】 -

【配置举例】 1：显示所有 AP 的认证相关信息:

```
Ruijie#sh ap-config summary ap-auth
AP Name                    Mac Address    Bind  bind-ap-serial   Bind  bind-ap-cert
Bind  bind-ap-password Bind  State
-------------------------- -------------- ----- ---------------- ----- -------------------------
----- ---------------- ----- -----
ap220                      1414.4b13.9ff3 FALSE                  TRUE
FALSE                 TRUE  Run
0011.0000.0101                            FALSE                  TRUE
FALSE                 TRUE  Quit
0011.0000.0201                            FALSE                  TRUE
FALSE                 TRUE  Quit
```

【提示信息】 -

【平台说明】 仅 AC 支持

1.34 show ap-config summary deny-ap

显示尝试关联但是被 AC 拒绝的 AP 列表

show ap-config summary deny-ap

【参数说明】

参数	描述
-	-

【命令模式】 特权模式

【缺省级别】 1

【使用指导】 列表条目容量与 AC 支持的在线 AP 数容量一致。

【配置举例】 1：显示尝试关联但是被 AC 拒绝的 AP 列表

其中包含 AP 名称、AP IP 地址、AP MAC 地址、被拒绝原因信息。

```
Ruijie#sh ap-config summary deny-ap
AP Name       IP Address          Mac Address     Reason
-----------  -----------------  -------------- --------------
AP1            192.168.10.10     1414.4b13.9ff3  By bind-ap-mac
AP2            192.168.10.11     00d0.f822.33b0  By bind-ap-mac
```

【提示信息】 -

【平台说明】 仅 AC 支持

1.35 show ap-group aps

显示连接到指定 AP 组的 AP 列表

show ap-group aps *ap-group-name*

【参数说明】

参数	描述
ap-group-name	AP 组名称

【命令模式】 特权模式

【缺省级别】 1

【使用指导】 无

【配置举例】 1：本 AC 的基本配置信息

```
Ruijie(config)#show ap-group aps default
Ap Name              Mac Addr        Pid
-------------------- --------------- --------------------

rrm-ap               0011.1122.3333 AP220E
```

【提示信息】 -

【平台说明】 仅 AC 支持

1.36 show ap-group aps summary

显示所有 AP 组的 AP 列表

show ap-group aps summary

【参数说明】

参数	描述
-	-

【命令模式】 特权模式

【缺省级别】 1

【使用指导】 无

【配置举例】 1：查看所有 AP 组的 AP 列表

```
Ruijie(config)#show ap-group aps summary
AP Group Name        AP Name              Mac Addr
-------------------- -------------------- ---------------
default              rrm-ap               0011.1122.3333
default              ap0001               0011.1122.4444
apg-10               ap0001               0011.1122.4455
```

【提示信息】 -

【平台说明】 仅 AC 支持

1.37 show ap-group cb

显示指定 AP 组的基本配置信息

show ap-group cb *ap-group-name*

【参数说明】

参数	描述
ap-group-name	AP 组名称

【命令模式】 特权模式

【缺省级别】 1

【使用指导】 无

【配置举例】 1：显示默认 AP 组的基本配置信息

```
Ruijie(config)#show ap-group cb default

Ap Group info:
apg_name            :default
ap_fallback         :Enable
hb_ctx_id           :2
```

【提示信息】 -

【平台说明】 仅 AC 支持

1.38 show ap-group intf-wlan-map

显示指定 AP 组的 WLAN-VLAN 映射

show ap-group intf-wlan-map *ap-group-name*

【参数说明】

参数	描述
ap-group-name	AP 组名称

【命令模式】 特权模式

【缺省级别】 1

【使用指导】 无

【配置举例】 1：显示 AP 组的 WLAN-VLAN 映射

```
Ruijie#show ap-group intf-wlan-map apg-1

WLAN ID   SSID                              VLAN-Id/VLAN-Group ID     Radio ID
AP WLAN ID       Enable
--------- --------------------------------- ------------------------
----------------------------------- ---------------- ----------
1         test-web-11                       110                       ALL
1                True
2         test-802.1x-11                    111                       ALL
2                True
3         test-iphone-11                    112                       ALL
3                True
4         test-guest-11                     113                       ALL
4                True
```

【提示信息】 -

【平台说明】 仅 AC 支持

1.39 show ap-group summary

显示本 AC 配置的所有 AP 组列表

show ap-group summary

【参数说明】

参数	描述

-	-

【命令模式】 特权模式

【缺省级别】 1

【使用指导】 无

【配置举例】 1：显示本 AC 配置的所有 AP 组列表

```
Ruijie(config)#show ap-group summary
Total Ap Group Num : 2
Ap Group Name
1. default
2. test-group
```

【提示信息】 -

【平台说明】 仅 AC 支持

1.40 show wlan-config cb

该命令用于查看 AC 上的 WLAN 详细信息。

show wlan-config cb

【参数说明】

参数	描述
-	-

【命令模式】 特权模式

【缺省级别】 1

【使用指导】 无

【配置举例】 1：查看 AC 上的 WLAN 配置列表

```
Ruijie(config)#show wlan-config cb  512
WLAN ID.................................. 512
SSID..................................... ssid-512
Profile.................................. <NULL>
Short Preamble........................... Disable
Spectrum Management...................... Disable
QoS...................................... Disable
```

```
Short Slot Time..... Disable
APSD..... Disable
Delayed Block ACK..... Disable
Immediate Block ACK..... Disable
MAC Mode..... Local
Tunnel Mode..... 802.3 Tunnel
Suppress SSID..... Enable
RTS Threshold..... 2347
Long Retry..... 4
Short Retry..... 7
```

【提示信息】 -

【平台说明】 仅 AC 支持

1.41 show wlan-config summary

该命令用于查看 AC 上的 WLAN 配置列表。

show wlan-config summary

【参数说明】

参数	描述
-	-

【命令模式】 特权模式

【缺省级别】 1

【使用指导】 无

【配置举例】 1：查看 AC 上的 WLAN 配置列表

```
Ruijie(config)#show wlan-config summary
Total Wlan Num : 3
Wlan id  Profile Name         SSID                STA NUM
-------- -------------------- -------------------- --------
1        pro-1                ssid-1              0
2        pro-2                ssid-2              0
4095     <NULL>               ssid-4095           0
```

【提示信息】 -

【平台说明】 仅 AC 支持

1.42 ssid

在 WLAN 配置模式下通过 **ssid** 来修改 SSID 名字

ssid *ssid-string*

【参数说明】

参数	描述
ssid-string	ssid 字符串，最大长度为 32 个字符

【缺省配置】 -

【命令模式】 WLAN 配置模式

【缺省级别】 15

【使用指导】 如果 WLAN 已经部署，该命令将导致当前关联该 WLAN 的用户下线。

【配置举例】 1：修改 ID 为 1 的 WLAN 的 SSID 名字为 ruijie

```
Ruijie(config)#wlan-config 1
Ruijie(config-wlan)#ssid ruijie
```

【检验方法】 使用 show wlan-config summary 查看所有 wlan 信息

```
Ruijie(config)#show wlan-config summary
Total Wlan Num : 2
Wlan id  Profile Name         SSID                STA NUM
-------- -------------------- ------------------- --------
1        pro-1                ruijie              0
2        pro-2                ssid-2              0
```

【提示信息】 -

【常见错误】 -

【平台说明】 仅 AC 支持

1.43 statistics-timer

在配置模式下通过 **statistics-timer** 来设置指定 AP 或指定 AP 组内的所有 AP 的定时上传统计信息的时间间隔。

statistics-timer *timer-num*

恢复至默认值。

no statistics-timer

【参数说明】

参数	描述
timer-num	要设置的定时器间隔，单位秒，取值范围：1~65535

【缺省配置】 缺省情况下，该定时器为 120s。

【命令模式】 AP 配置模式或 AP 组配置模式

【缺省级别】 15

【使用指导】 设置指定 AP 的 statistics timer。该命令可以通过 **no** 前缀将 statistics timer 恢复默认值。

【配置举例】 1：进入 AP0001 的配置模式，并且配置其 statistics timer 时间为 200s

```
Ruijie(config)# ap-config AP0001
Ruieji(config-ap)# statistics-timer 200
```

2：进入 AP0001 的配置模式，并且配置其 statistics timer 时间恢复为默认值 120s

```
Ruijie(config)# ap-config AP0001
Ruieji(config-ap)# no statistics-timer
```

*3：*进入默认 AP 组，并且配置其 statistics timer 时间为 200s

```
Ruijie(config)# ap-group default
Ruieji(config-ap-group)# statistics-timer 200
```

4：进入默认 AP 组，并且配置其 statistics timer 时间恢复为默认值 120s

```
Ruijie(config)# ap-group default
Ruieji(config-ap-group)# no statistics-timer
```

【检验方法】 -

【提示信息】 -

【常见错误】 -

【平台说明】 仅 AC 支持

1.44 wlan-config

在配置模式下通过 **wlan-config** 创建 WLAN 并且进入 WLAN 配置模式。

wlan-config *wlan-id* [*profile-string*] [*ssid-string*]

删除 WLAN
no wlan-config *wlan-id*

【参数说明】

参数	描述
wlan-id	要创建的 WLAN 的 ID，取值范围 1~4094
profile-string	该 WLAN 的描述符，可省略，最大长度为 32 个字符
ssid-string	该 WLAN 对应的 ssid 字符串，最大长度为 32 个字符

【缺省配置】 无

【命令模式】 全局配置模式

【缺省级别】 15

【使用指导】

- 创建一个 WLAN，如命令描述，必须要指定 ssid-string，profile-string 可以省略；创建完一个 WLAN 后，cli 会自动进入该 WLAN 的配置模式；
- 进入一个 WLAN 的配置模式，只需要指定已存在的 WLAN ID，就可以进入该 WLAN 对应的配置模式。
- 一个 SSID 可以对应多个 WLAN，但一个 WLAN 不能同时关联多个 SSID

【配置举例】 1：创建一个 ID 为 2048 的 WLAN，该 WLAN 的 ssid 为 ssid-test

```
Ruijie(config)# wlan-config 2048 profile-test ssid-test
Ruijie(config-wlan)# exit
Ruijie(config)#
```

2：进入已经创建 ID 为 2048 的 WLAN 配置模式

```
Ruijie(config)# wlan-config 2048
Ruijie(config-wlan)# exit
```

【检验方法】 -

【提示信息】 -

【常见错误】 -

【平台说明】 仅 AC 支持

1.45 wtp-limit

通过 **wtp-limit** 配置 AP 上支持的最大 AP 数量。

wtp-limit *wtp-num*

恢复默认值。

no wtp-limit

【参数说明】

参数	描述
wtp-num	AC 可以连接的最大 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

【缺省级别】 15

【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，也不能超过 license 允许的最大值。

⚠ 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。该命令和 license 控制的是权重的 AP 数而非实际的 AP 数。

【配置举例】 1：用户配置该 AC 最大可连接 100 台 AP

```
Ruijie(config-ac)# wtp-limit 100
```

2：用户配置该 AC 最大可连接 AP 数为默认值

```
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。

【提示信息】 -

【常见错误】 -

【平台说明】 仅 AC 支持

2 STAMG

命令	作用
ap	配置该域中的 AP 信息。
assoc-control	开启关联控制功能
client-kick	配置指定无线用户的 MAC 地址。
control-zone	创建关联控制域
flow-balance-group add	添加指定 AP 到指定负载均衡组。
flow-balance-group base	配置流量负载均衡所使用的流量基准值
flow-balance-group create	创建基于流量的负载均衡组
flow-balance-group del	配置从指定负载均衡组删除指定 AP。
flow-balance-group enable	配置均衡组的启动门限值
flow-balance-group flow	配置均衡组的负载阈值。
flow-balance-group radio-flow	配置均衡组切换为使用 AP 定时上传来的流量作负载均衡判断
inter-radio-balance flow-balance dual-band	配置 AP 或 AP 组的不同频（2.4G 和 5G）radio 间流量负载均衡启动门限值和阈值
inter-radio-balance flow-balance enable	开启 AP 或 AP 组的 radio 间流量负载均衡
inter-radio-balance flow-balance same-band	配置 AP 或 AP 组的同频（同为 2.4G 或 5G）radio 间流量负载均衡启动门限值和阈值
inter-radio-balance num-balance dual-band	配置 AP 或 AP 组的不同频（2.4G 和 5G）radio 间数量负载均衡启动门限值和阈值
inter-radio-balance num-balance enable	开启 AP 或 AP 组的 radio 间数量负载均衡
inter-radio-balance num-balance same-band	配置 AP 或 AP 组的同频（同为 2.4G 或 5G）radio 间数量负载均衡启动门限值和阈值
num-balance-group add	配置添加指定 AP 到指定负载均衡组。
num-balance-group create	命令配置创建基于数量的负载均衡组。
num-balance-group del	配置从指定负载均衡组删除指定 AP。
num-balance-group enable	配置均衡组的启动门限值
num-balance-group mode	配置均衡组的负载均衡模式。
num-balance-group num	配置均衡组的负载阈值。
package	创建终端包并进入终端包配置模式。
primary-sta	在一个终端包中配置主 STA。
secondary-sta	在一个终端包中配置从 STA。
show ac-config client	显示本 AC 上所有连接的 STA 的信息
show ac-config client detail	显示指定无线用户的详细信息
show ac-config client statistic	显示所有无线用户的在过去一个小时内的上下线次数
show ac-config flow-balance summary	查看基于流量的负载均衡组的详细配置信息。
show ac-config num-balance summary	查看基于数量的负载均衡组的详细配置信息。
show assoc-control	显示关联控制当前运行状态。

show control-zone	显示关联控制域配置信息。
show package	显示终端包配置信息。
show sta-blacklist	显示 STA 黑名单
sta-blacklist	配置 STA 黑名单功能的开启和关闭
sta-idle-timeout	设置指定 AP 或 AP 组中无线用户的老化时间
sta-limit	配置可连接的最大无线用户数
sta-limit per-ap	配置 WLAN 下每个 AP 可连接的最大用户数
sta-limit radio	配置可连接的最大无线用户数
sta-logging rate-limit	配置 STA syslog 的限速

2.1 ap

在关联控制域配置模式下中配置该域中的 AP 信息。

ap *WORD*

用户可以用该命令的 **no** 选项从关联控制域中删除指定的 AP。

no ap [*WORD*]

【参数说明】

参数	描述
WORD	AP 名称。 长度[1-64]

【缺省配置】 关联控制域中无任何 AP 信息

【命令模式】 关联控制域配置模式

【缺省级别】 15

【使用指导】 一个关联控制域中最多允许配置 5 台 AP 信息，超过了系统会给出相应的错误提示。另外，给关联控制域配置 AP 信息时，不要求 AP 是在线的。

【配置举例】 1：为名为”一年级(1)班”的关联控制域配置一台 MAC 地址为 00d0.f800.1001 的 AP 信息

```
Ruijie(config)#control-zone 一年级(1)班
Ruijie(config- cznoe)# ap 00d0.f800.1001
```

【检验方法】 -

【提示信息】 -

【常见错误】 -

【平台说明】 AC、胖 AP

2.2 assoc-control

开启关联控制功能
assoc-control

用户可以用该命令的 **no** 选项关闭关联控制功能
no assoc-control

【参数说明】

参数	描述
-	-

【缺省配置】 缺省关联控制功能关闭。

【命令模式】 全局配置模式

【缺省级别】 15

【使用指导】 不开启关联控制功能时，关联控制的相关命令仍然可配置，只不过功能不起作用。

【配置举例】 1：开启关联控制功能：

```
Ruijie(config)#assoc-control
```

2：关闭关联控制功能：

```
Ruijie (config)#no assoc-control
```

【检验方法】 -

【提示信息】 -

【常见错误】 -

【平台说明】 AC、胖 AP

2.3 client-kick

通过 **client-kick** 命令配置删除指定无线用户的 MAC 地址。
client-kick *sta-mac*

【参数说明】

参数	描述
sta-mac	无线用户的 MAC 地址。

【缺省配置】 无

【命令模式】 AC 配置模式

【缺省级别】 15

【使用指导】 无

【配置举例】 1：删除 MAC 地址为 aaaa.bbbb.cccc 的无线用户

```
Ruijie(config)# ac-controller
Ruijie(config-ac)# client-kick aaaaa.bbbbb.ccccc
```

【检验方法】 -

【提示信息】 -

【常见错误】 -

【平台说明】 AC

2.4 control-zone

创建关联控制域并进入关联控制域配置模式。
control-zone *czone-name*

用户可以用该命令的 **no** 选项删除指定的关联控制域配置。
no control-zone *czone-name*

【参数说明】

参数	描述
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

【缺省级别】 15

【使用指导】 AC 上最多允许配置 300 个关联控制域，胖 AP 上只允许配置一个关联控制域，超过上限，将会得出一个错误

提示。

【配置举例】 1：配置一个名为”一年级(1)班”的关联控制域

```
Ruijie(config)#control-zone 一年级(1)班
Ruijie(config- czone)#
```

2：删除名为” 一年级(1)班”的关联控制域

```
Ruijie(config)# no control-zone 一年级(1)班
The opreration will clear the control zone configuration, which may cause corresponding STAs offline .
Continue? [no] y
Ruijie(config)#
```

【检验方法】 -

【提示信息】 -

【常见错误】 -

【平台说明】 AC、胖 AP

2.5 flow-balance-group add

通过 **flow-balance-group add** 命令配置添加指定 AP 到指定负载均衡组。

flow-balance-group add *group-name ap-name*

【参数说明】

参数	描述
group-name	指定均衡组名称，每个流量均衡组最多支持 10 个 AP
ap-name	要添加的 AP 的名称

【缺省配置】 负载均衡组中无 AP

【命令模式】 AC 配置模式

【缺省级别】 15

【使用指导】 无

【配置举例】 1：将名称为 ap1，ap2 的两个 AP 加入均衡组 test-group

```
Ruijie(config)# ac-controller
Ruijie(config-ac)# flow-balance-group add test-group ap1
Ruijie(config-ac)# flow-balance-group add test-group ap2
```

【检验方法】 -

【提示信息】 -

【常见错误】 -

【平台说明】 AC

2.6 flow-balance-group base

通过 **flow-balance-group base** 命令配置流量负载均衡所使用的流量基准值。

flow-balance-group base *number*

恢复基准值为缺省配置（10Mbps）。

no flow-balance-group base

【参数说明】

参数	描述
number	流量基准值，默认 10Mbps，范围 1-100。

【缺省配置】 基准值为 10Mbps

【命令模式】 AC 配置模式

【缺省级别】 15

【使用指导】 无

【配置举例】 1：配置流量负载均衡的流量基准值为 50Mbps

```
Ruijie(config)# ac-controller
Ruijie(config-ac)# flow-balance-group base 50
```

【检验方法】 -

【提示信息】 -

【常见错误】 -

【平台说明】 AC

2.7 flow-balance-group create

通过 **flow-balance-group create** 命令配置创建基于流量的负载均衡组。
flow-balance-group create *group-name*

删除基于流量的负载均衡组。
no flow-balance-group create *group-name*

【参数说明】

参数	描述
group-name	负载均衡组的名称，最多可配置 55 个字符，不能包含空格。最多支持创建 80 个流量均衡组

【缺省配置】 没有创建负载均衡组

【命令模式】 AC 配置模式

【缺省级别】 15

【使用指导】 **no** 操作用于删除指定均衡组配置

【配置举例】 1：创建名称为 test-group 的负载均衡组

```
Ruijie(config)# ac-controller
Ruijie(config-ac)# flow-balance-group create test-group
```

2：删除名称为 test-group 的负载均衡组

```
Ruijie(config)# ac-controller
Ruijie(config-ac)# no flow-balance-group create test-group
```

【检验方法】 -

【提示信息】 -

【常见错误】 -

【平台说明】 AC

2.8 flow-balance-group del

通过 **flow-balance-group del** 命令配置从指定负载均衡组删除指定 AP。
flow-balance-group del *group-name ap-name*

【参数说明】

参数	描述
group-name	要操作的负载均衡组
ap-name	要从均衡组中移除的 AP 的名称

【缺省配置】 无

【命令模式】 全局配置模式

【缺省级别】 15

【使用指导】 无

【配置举例】 1：将名称为 ap1 的 AP 从均衡组 test-group 中移除

```
Ruijie(config)# ac-controller
Ruijie(config-ac)# flow-balance-group del test-group ap1
```

【检验方法】 -

【提示信息】 -

【常见错误】 -

【平台说明】 AC

2.9 flow-balance-group enable

通过 **flow-balance-group enable** 命令配置均衡组的启动门限值。仅在当前关联 AP 的流量达到该门限值时，才启动流量负载均衡功能。

flow-balance-group enable *group-name number*

恢复均衡组的负载阈值为缺省配置。

no flow-balance-group enable *group-name number*

【参数说明】

参数	描述
group-name	要操作的负载均衡组名称
number	均衡组的启动门限值，单位是%，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是 10Mbps。

【缺省配置】 启动门限值 5%

【命令模式】 AC 配置模式

【缺省级别】 15

【使用指导】 无

【配置举例】 1：配置名称为 test-group 的均衡组的门限值为 100kbps

```
Ruijie(config)# ac-controller
Ruijie(config-ac)# flow-balance-group enable test-group 1
```

【检验方法】 -

【提示信息】 -

【常见错误】 -

【平台说明】 AC

2.10 flow-balance-group flow

通过 **flow-balance-group flow** 命令配置均衡组的负载阈值。
flow-balance-group flow *group-name number*

恢复均衡组的负载阈值为缺省配置。
no flow-balance-group flow *group-name number*

【参数说明】

参数	描述
group-name	要操作的负载均衡组名称
number	均衡组的阈值，单位是%，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是 10Mbps。

【缺省配置】 流量阈值 5%

【命令模式】 AC 配置模式

【缺省级别】 15

【使用指导】 无

【配置举例】 1：配置名称为 test-group 的均衡组的阈值为 100kbps

```
Ruijie(config)# ac-controller
```

```
Ruijie(config-ac)# flow-balance-group flow test-group 1
```

【检验方法】 -

【提示信息】 -

【常见错误】 -

【平台说明】 AC

2.11 flow-balance-group radio-flow

通过 **flow-balance-group radio-flow** 命令配置均衡组支持本地转发下的负载均衡。均衡组将使用 AP 定时上传的流量，代替 AC 上实时统计的流量进行均衡判断。

flow-balance-group radio-flow *group-name*

恢复使用 AC 实时统计的流量进行负载均衡判断。

no flow-balance-group radio-flow *group-name*

【参数说明】

参数	描述
group-name	要操作的负载均衡组名称

【缺省配置】 使用 AC 上 CAPWAP 数据通道统计的流量

【命令模式】 AC 配置模式

【缺省级别】 15

【使用指导】 无

【配置举例】 1：配置名称为 test-group 的均衡组切换为使用 AP 定时发送来的流量

```
Ruijie(config)# ac-controller
Ruijie(config-ac)# flow-balance-group radio-flow test-group
```

【检验方法】 -

【提示信息】 -

【常见错误】 -

【平台说明】 AC

2.12 inter-radio-balance flow-balance dual-band

配置 AP 或 AP 组的不同频（2.4G 和 5G）radio 间流量负载均衡启动门限值和阈值
inter-radio-balance flow-balance dual-band enable-load *en-num* **threshold** *thrs-num*

将 AP 或 AP 组中不同频 radio 间流量负载均衡参数恢复为默认值
no inter-radio-balance flow-balance dual-band

【参数说明】

参数	描述
en-num	启动门限值，即当前关联 radio 上的流量超过此值才启动负载均衡。单位为 100Kbps，取值范围为 1-1000
thrs-num	均衡阈值 ,即当前关联 radio 上的流量与负载最低的 radio 的流量之差超过此值时，拒绝 STA 关联到此 radio。单位为 100Kbps，取值范围为 1-1000

【缺省配置】 缺省情况下，启动门限值为 10（1Mbps），均衡阈值为 10（1Mbps）

【命令模式】 AP 配置模式或 AP 组配置模式

【缺省级别】 15

【使用指导】 若指定 AP 的 radio 间流量负载均衡使能 ,STA 意图关联的 radio 的负载超出启动门限值 ,且与最低负载之差超出阈值，STA 将被拒绝关联，以引导到负载较低的 radio 上。该配置仅当最低负载 radio 与意图关联的 radio 不同频时生效，若同频，则 **inter-radio-balance flow-balance same-band** 的配置生效。

【配置举例】 1：配置 AP0001 的不同频 radio 间流量负载均衡启动门限值和阈值为 800Kbps

```
Ruijie(config)# ap-config AP0001
Ruijie(config-ap)# inter-radio-balance flow-balance dual-band enable-load 8 threshold 8
```

2：将 AP0001 的不同频 radio 间流量负载均衡配置恢复到默认值

```
Ruijie(config)# ap-config AP0001
Ruijie(config-ap)# no inter-radio-balance flow-balance dual-band
```

3：配置默认 AP 组内 AP 的不同频 radio 间流量负载均衡启动门限值为 300Kbps，阈值为 500Kbps

```
Ruijie(config)# ap-group default
Ruijie(config-group)# inter-radio-balance flow-balance dual-band enable-load 3 threshold 5
```

4：配置所有 AP 的不同频 radio 间流量负载均衡启动门限值和阈值为 3Mbps

```
Ruijie(config)# ap-config all
Ruijie(config-ap)# inter-radio-balance flow-balance dual-band enable-load 30 threshold 30
```

【检验方法】 -

【提示信息】 -

【常见错误】 -

【平台说明】 AC

2.13 inter-radio-balance flow-balance enable

开启 AP 或 AP 组的 radio 间流量负载均衡
inter-radio-balance flow-balance enable

关闭 AP 或 AP 组的 radio 间流量负载均衡
no inter-radio-balance flow-balance enable

【参数说明】

参数	描述
-	-

【缺省配置】 缺省情况下，radio 间流量负载均衡关闭。

【命令模式】 AP 配置模式或 AP 组配置模式

【缺省级别】 15

【使用指导】 开启指定 AP 的 radio 间流量负载均衡后，AC 将尽可能保证该 AP 的各个 radio 间用户流量差值不超过阈值

【配置举例】 1：开启 AP0001 的 radio 间流量负载均衡

```
Ruijie(config)# ap-config AP0001
Ruijie(config-ap)# inter-radio-balance flow-balance enable
```

2：关闭 AP0001 的 radio 间流量负载均衡

```
Ruijie(config)# ap-config AP0001
Ruijie(config-ap)# no inter-radio-balance flow-balance enable
```

3：开启默认 AP 组内 AP 的 radio 间流量负载均衡

```
Ruijie(config)# ap-group default
Ruijie(config-group)# inter-radio-balance flow-balance enable
```

4：开启所有 AP 的 radio 间流量负载均衡

```
Ruijie(config)# ap-config all
Ruijie(config-ap)# inter-radio-balance flow-balance enable
```

【检验方法】 -

【提示信息】 -

【常见错误】 -

【平台说明】 AC

2.14 inter-radio-balance flow-balance same-band

配置 AP 或 AP 组的同频（同为 2.4G 或 5G）radio 间流量负载均衡启动门限值和阈值
inter-radio-balance flow-balance same-band enable-load *en-num* **threshold** *thrs-num*

将 AP 或 AP 组中同频 radio 间流量负载均衡参数恢复为默认值
no inter-radio-balance flow-balance same-band

【参数说明】

参数	描述
en-num	启动门限值，即当前关联 radio 上的流量超过此值才启动负载均衡。单位为 100kbps，取值范围为 1-1000
thrs-num	均衡阈值 ,即当前关联 radio 上的流量与负载最低的 radio 的流量之差超过此值时，拒绝 STA 关联到此 radio。单位为 100kbps，取值范围为 1-1000

【缺省配置】 缺省情况下，启动门限值为 5（500Kbps），均衡阈值为 5（500Kbps）

【命令模式】 AP 配置模式或 AP 组配置模式

【缺省级别】 15

【使用指导】 若指定 AP 的 radio 间流量负载均衡使能 ,STA 意图关联的 radio 的负载超出启动门限值 ,且与最低负载之差超出阈值，STA 将被拒绝关联，以引导到负载较低的 radio 上。该配置仅当最低负载 radio 与意图关联的 radio 同频时生效，若不同频，则 **inter-radio-balance flow-balance dual-band** 的配置生效。

【配置举例】 1：配置 AP0001 的同频 radio 间流量负载均衡启动门限值和阈值为 800kbps

```
Ruijie(config)# ap-config AP0001
Ruijie(config-ap)# inter-radio-balance flow-balance same-band enable-load 10 threshold 10
```

2：将 AP0001 的同频 radio 间流量负载均衡配置恢复到默认值

```
Ruijie(config)# ap-config AP0001
Ruijie(config-ap)# no inter-radio-balance flow-balance same-band
```

3：配置默认 AP 组内 AP 的同频 radio 间流量负载均衡启动门限值为 300kbps，阈值为 500kbps

```
Ruijie(config)# ap-group default
Ruijie(config-group)# inter-radio-balance flow-balance same-band enable-load 3 threshold 5
```

4：配置所有 AP 的同频 radio 间流量负载均衡启动门限值和阈值为 3Mbps

```
Ruijie(config)# ap-config all
Ruijie(config-ap)# inter-radio-balance flow-balance same-band enable-load 30 threshold 30
```

【检验方法】 -

【提示信息】 -

【常见错误】 -

【平台说明】 AC

2.15 inter-radio-balance num-balance dual-band

配置 AP 或 AP 组的不同频（2.4G 和 5G）radio 间数量负载均衡启动门限值和阈值
inter-radio-balance num-balance dual-band enable-load *en-num* **threshold** *thrs-num*

将 AP 或 AP 组中不同频 radio 间数量负载均衡参数恢复为默认值
no inter-radio-balance num-balance dual-band

【参数说明】

参数	描述
en-num	启动门限值，即当前关联 radio 上的用户数量超过此值才启动负载均衡。取值范围为 1-20 个用户
thrs-num	均衡阈值 ,即当前关联 radio 上的用户数量与负载最低的 radio 的用户数量之差超过此值时，拒绝 STA 关联到此 radio。取值范围为 1-20 个用户

【缺省配置】 缺省情况下，启动门限值为 8，均衡阈值为 8

【命令模式】 AP 配置模式或 AP 组配置模式

【缺省级别】 15

【使用指导】 若指定 AP 的 radio 间数量负载均衡使能 ,STA 意图关联的 radio 的负载超出启动门限值 ,且与最低负载之差超出阈值 , STA 将被拒绝关联 , 以引导到负载较低的 radio 上。该配置仅当最低负载 radio 与意图关联的 radio 不同频时生效，若同频，则 **inter-radio-balance num-balance same-band** 的配置生效。

【配置举例】 1：配置 AP0001 的不同频 radio 间数量负载均衡启动门限值和阈值为 10

```
Ruijie(config)# ap-config AP0001
Ruijie(config-ap)# inter-radio-balance num-balance dual-band enable-load 10 threshold 10
```

2：将 AP0001 的不同频 radio 间数量负载均衡配置恢复到默认值

```
Ruijie(config)# ap-config AP0001
Ruijie(config-ap)# no inter-radio-balance num-balance dual-band
```

3：配置默认 AP 组内 AP 的不同频 radio 间数量负载均衡启动门限值为 4，阈值为 5

```
Ruijie(config)# ap-group default
Ruijie(config-group)# inter-radio-balance num-balance dual-band enable-load 4 threshold 5
```

4：配置所有 AP 的不同频 radio 间数量负载均衡启动门限值和阈值为 5

```
Ruijie(config)# ap-config all
Ruijie(config-ap)# inter-radio-balance num-balance dual-band enable-load 5 threshold 5
```

【检验方法】 -

【提示信息】 -

【常见错误】 -

【平台说明】 AC

2.16 inter-radio-balance num-balance enable

开启 AP 或 AP 组的 radio 间数量负载均衡
inter-radio-balance num-balance enable

关闭 AP 或 AP 组的 radio 间数量负载均衡
no inter-radio-balance num-balance enable

【参数说明】

参数	描述
-	-

【缺省配置】 缺省情况下，radio 间数量负载均衡关闭。

【命令模式】 AP 配置模式或 AP 组配置模式

【缺省级别】 15

【使用指导】 开启指定 AP 的 radio 间数量负载均衡后，AC 将尽可能保证该 AP 的各个 radio 间用户数量差值不超过阈值

【配置举例】 1：开启 AP0001 的 radio 间数量负载均衡

```
Ruijie(config)# ap-config AP0001
Ruijie(config-ap)# inter-radio-balance num-balance enable
```

2：关闭 AP0001 的 radio 间数量负载均衡

```
Ruijie(config)# ap-config AP0001
Ruijie(config-ap)# no inter-radio-balance num-balance enable
```

3：开启默认 AP 组内 AP 的 radio 间数量负载均衡

```
Ruijie(config)# ap-group default
Ruijie(config-group)# inter-radio-balance num-balance enable
```

4：开启所有 AP 的 radio 间数量负载均衡

```
Ruijie(config)# ap-config all
Ruijie(config-ap)# inter-radio-balance num-balance enable
```

【检验方法】 -

【提示信息】 -

【常见错误】 -

【平台说明】 AC

2.17 inter-radio-balance num-balance same-band

配置 AP 或 AP 组的同频（同为 2.4G 或 5G）radio 间数量负载均衡启动门限值和阈值
inter-radio-balance num-balance same-band enable-load *en-num* **threshold** *thrs-num*

将 AP 或 AP 组中同频 radio 间数量负载均衡参数恢复为默认值
no inter-radio-balance num-balance same-band

【参数说明】

参数	描述
en-num	启动门限值，即当前关联 radio 上的数量超过此值才启动负载均衡。取值范围为 1-20 个用户
thrs-num	均衡阈值 ,即当前关联 radio 上的数量与负载最低的 radio 的数量之差超过此值时，拒绝 STA 关联到此 radio。取值范围为 1-20 个用户

【缺省配置】 缺省情况下，启动门限值为 2，均衡阈值为 2

【命令模式】 AP 配置模式或 AP 组配置模式

【缺省级别】 15

【使用指导】 若指定 AP 的 radio 间数量负载均衡使能，STA 意图关联的 radio 的负载超出启动门限值，且与最低负载之差超出阈值，STA 将被拒绝关联，以引导到负载较低的 radio 上。该配置仅当最低负载 radio 与意图关联的 radio 同频时生效，若不同频，则 **inter-radio-balance num-balance dual-band** 的配置生效。

【配置举例】 1：配置 AP0001 的同频 radio 间数量负载均衡启动门限值和阈值为 3

```
Ruijie(config)# ap-config AP0001
Ruijie(config-ap)# inter-radio-balance num-balance same-band enable-load 3 threshold 3
```

2：将 AP0001 的同频 radio 间数量负载均衡配置恢复到默认值

```
Ruijie(config)# ap-config AP0001
Ruijie(config-ap)# no inter-radio-balance num-balance same-band
```

3：配置默认 AP 组内 AP 的同频 radio 间数量负载均衡启动门限值为 3，阈值为 5

```
Ruijie(config)# ap-group default
Ruijie(config-group)# inter-radio-balance num-balance same-band enable-load 3 threshold 5
```

4：配置所有 AP 的同频 radio 间数量负载均衡启动门限值和阈值为 5

```
Ruijie(config)# ap-config all
Ruijie(config-ap)# inter-radio-balance num-balance same-band enable-load 5 threshold 5
```

【检验方法】 -

【提示信息】 -

【常见错误】 -

【平台说明】 AC

2.18 num-balance-group add

通过 **num-balance-group add** 命令配置添加指定 AP 到指定负载均衡组。

num-balance-group add *group-name ap-name*

【参数说明】

参数	描述
group-name	指定均衡组名称，每个数量均衡组最多支持 10 个 AP

ap-name	要添加的 AP 的名称

【缺省配置】 负载均衡组中无 AP

【命令模式】 AC 配置模式

【缺省级别】 15

【使用指导】 无

【配置举例】 1：将名称为 ap1 的 AP 加入均衡组 test-group

```
Ruijie(config)# ac-controller
Ruijie(config-ac)# num-balance-group add test-group ap1
```

【检验方法】 -

【提示信息】 -

【常见错误】 -

【平台说明】 AC

2.19 num-balance-group create

通过 **num-balance-group create** 命令配置创建基于数量的负载均衡组。
num-balance-group create *group-name*

删除基于数量的负载均衡组。
no num-balance-group create *group-name*

【参数说明】

参数	描述
group-name	负载均衡组的名称，最多可配置 55 个字符，不能包含空格。最多支持创建 80 个数量均衡组

【缺省配置】 没有创建负载均衡组

【命令模式】 AC 配置模式

【缺省级别】 15

【使用指导】 无

【配置举例】 1：创建名称为 test-group 的负载均衡组

```
Ruijie(config)# ac-controller
Ruijie(config-ac)# num-balance-group create test-group
```

2：删除名称为 test-group 的负载均衡组

```
Ruijie(config)# ac-controller
Ruijie(config-ac)# no num-balance-group create test-group
```

【检验方法】 -

【提示信息】 -

【常见错误】 -

【平台说明】 AC

2.20 num-balance-group del

通过 **num-balance-group del** 命令配置从指定负载均衡组删除指定 AP。

num-balance-group del *group-name ap-name*

【参数说明】

参数	描述
group-name	要操作的负载均衡组
ap-name	要从均衡组中移除的 AP 的名称

【缺省配置】 无

【命令模式】 AC 配置模式

【缺省级别】 15

【使用指导】 无

【配置举例】 1：将名称为 ap1 的 AP 从均衡组 test-group 中移除

```
Ruijie(config)# ac-controller
Ruijie(config-ac)# num-balance-group del test-group ap1
```

【检验方法】 -

【提示信息】 -

【常见错误】 -

【平台说明】 AC

2.21 num-balance-group enable

通过 **num-balance-group enable** 命令配置均衡组的启动门限值。仅在当前关联 AP 的用户数达到该门限值时，才启动数量负载均衡功能。

num-balance-group enable *group-name number*

恢复均衡组的负载阈值为缺省配置。

no num-balance-group enable *group-name number*

【参数说明】

参数	描述
group-name	要操作的负载均衡组名称
number	均衡组的启动门限值，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】 启动门限值为 3

【命令模式】 AC 配置模式

【缺省级别】 15

【使用指导】 无

【配置举例】 1：配置名称为 test-group 的均衡组的门限值为 1

```
Ruijie(config)# ac-controller
Ruijie(config-ac)# num-balance-group enable test-group 1
```

【检验方法】 -

【提示信息】 -

【常见错误】 -

【平台说明】 AC

2.22 num-balance-group mode

通过 **num-balance-group mode** 命令配置均衡组的负载均衡模式。

num-balance-group mode *group-name* { **radio-mode** | **ap-mode** }

使用 **no** 命令恢复成缺省配置。

no num-balance-group mode *group-name*

【参数说明】

参数	描述
group-name	要操作的负载均衡组名称
radio-mode	配置均衡组为基于 radio 的负载均衡
ap-mode	配置均衡组为基于 ap 的负载均衡

【缺省配置】 缺省是基于 AP 的负载均衡。

【命令模式】 AC 配置模式

【缺省级别】 15

【使用指导】 无

【配置举例】 1：配置名称为 test-group 的均衡组的负载均衡模式为基于 radio 的负载均衡：

```
Ruijie(config)# ac-controller
Ruijie(config-ac)# num-balance-group mode test-group radio-mode
```

【检验方法】 -

【提示信息】 -

【常见错误】 -

【平台说明】 AC

2.23 num-balance-group num

配置均衡组的负载阈值。

num-balance-group num *group-name number*

恢复均衡组的负载阈值为缺省值。

no num-balance-group num *group-name number*

【参数说明】

参数	描述
group-name	要操作的负载均衡组名称
number	均衡组的阈值，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】 阈值为 3

【命令模式】 AC 配置模式

【缺省级别】 15

【使用指导】 无

【配置举例】 1：配置名称为 test-group 的均衡组的阈值为 1

```
Ruijie(config)# ac-controller
Ruijie(config-ac)# num-balance-group num test-group 1
```

【检验方法】 -

【提示信息】 -

【常见错误】 -

【平台说明】 AC

2.24 package

创建终端包并进入终端包配置模式。
package *pkg-name*

用户可以用该命令的 **no** 选项删除指定的终端包配置。
no package [*pkg-name*]

【参数说明】

参数	描述
pkg-name	终端包名称，长度[1,32]

【缺省配置】 无终端包配置

【命令模式】 全局配置模式

【缺省级别】 15

【使用指导】 AC 上最多允许配置 300 个终端包，胖 AP 上最多允许配置 50 个终端包，超过上限，将会得出一个错误提示。

【配置举例】 1：配置一个名为”AAA”的终端包

```
Ruijie(config)#package AAA
Ruijie(config-package)#
```

2：删除名为”AAA”的终端包

```
Ruijie(config)# no package AAA
The opreration will clear package(s) configuration, which may cause corresponding STAs offline .
Continue? [no]y
Ruijie(config)#
```

【检验方法】 -

【提示信息】 -

【常见错误】 -

【平台说明】 AC、胖 AP

2.25 primary-sta

在一个终端包中配置主 STA。
primary-sta *mac-address*

用户可以用该命令的 **no** 选项删除指定终端包中的主 STA 配置。
no primary-sta

【参数说明】

参数	描述
mac-address	主 STA 的 MAC 地址，格式形如 H.H.H

【缺省配置】 无

【命令模式】 终端包配置模式

【缺省级别】 15

【使用指导】 一个终端包只允许配置一个主 STA，因此，使用该命令来配置终端包中的主 STA 时，如果终端包中的主 STA 已经存在，则直接覆盖。

【配置举例】 1：为终端包”AAA”配置 MAC 地址为 00d0.f800.0001 的主 STA

```
Ruijie(config)#package AAA
Ruijie(config- package)#primary-sta 00d0.f800.0001
```

【检验方法】 -

【提示信息】 -

【常见错误】 -

【平台说明】 AC、胖 AP

2.26 secondary-sta

在一个终端包中配置从 STA。

secondary-sta *mac-address*

用户可以用该命令的 **no** 选项删除指定终端包中的从 STA 配置。

no secondary-sta [*mac-address*]

【参数说明】

参数	描述
mac-address	从 STA 的 MAC 地址，格式形如 H.H.H

【缺省配置】 无

【命令模式】 终端包配置模式

【缺省级别】 15

【使用指导】 一个终端包最多允许配置 100 台从 STA。使用该命令来配置从 STA 时，如果指定的从 STA 已经存在，则会提示错误信息; 如果终端包中的从 STA 总数已经达到 100 台，也会给出相应的错误提示。

【配置举例】 1：在终端包”推车 1”中配置 MAC 地址为从 00d0.f800.0002 的 STA

```
Ruijie(config)#package 推车 1
Ruijie(config- package)#secondary-sta 00d0.f800.0002
```

【检验方法】 -

【提示信息】 -

【常见错误】 -

【平台说明】 AC、胖 AP

2.27 show ac-config client

显示本 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**]

【参数说明】

参数	描述
by-ap-name	按照 AP 的命名排序
802.11a	显示 802.11a 用户信息
802.11b	显示 802.11b 用户信息
802.11n	显示 802.11n 用户信息
802.11g	显示 802.11g 用户信息
802.11ac	显示 802.11ac 用户信息
other	显示未知用户信息

【命令模式】 特权模式

【缺省级别】 1

【使用指导】 无

【配置举例】 1：显示本 AC 上所有连接的 STA 的信息

```
AC#show ac-config client
========= show sta status =========
AP    : ap name/radio id
Status: Speed/Power Save/Work Mode/Roaming State, E = enable power save, D = disable power save

Total Sta Num : 1
STA MAC        IP Address      AP                                        Wlan Vlan Status
Asso Auth Link Auth Up time
-------------- --------------- ----------------------------------------- ---- ---- -----------
--------- --------- -------------
78e4.00d3.1183 192.168.248.2   te/1                                      1    1    65.0M/D/bn
Open      Open        0:00:08:10
```

【提示信息】 -

【平台说明】 AC

2.28 show ac-config client detail

显示指定无线用户的详细信息

show ac-config client detail *mac-address*

【参数说明】

参数	描述
mac-address	无线用户的 MAC 地址

【命令模式】 特权模式

【缺省级别】 1

【使用指导】 无

【配置举例】 1：显示指定无线用户的详细信息

```
AC#show ac-config client detail 0023.cdae.5260
Mac Address          :0023.cdae.5260
IP Address           :0.0.0.0
Wlan Id              :123
Vlan Id              :2
Roam State           :Local
Association ID       :0

Associated Ap Information:
AP Name              :youzt
AP IP                :10.1.1.2
```

【提示信息】 -

【平台说明】 AC

2.29 show ac-config client statistic

显示无线用户在过去不同时间段内的上下线次数以及漫游次数。

show ac-config client statistic

【参数说明】

参数	描述
-	-

【命令模式】 特权模式

【缺省级别】 1

【使用指导】 无

【配置举例】 1：显示指定无线用户的统计信息

```
AC# #show ac-config client statistic
========= show sta statistic =========
STA online  times in 5 second: 13
STA offline times in 5 second: 10
STA roaming times in 5 second: 2

STA online  times in 1 minute: 30
STA offline times in 1 minute: 25
STA roaming times in 1 minute: 10

STA online  times in 1 hour:   200
STA offline times in 1 hour:   300
STA roaming times in 1 hour:   100

Maxinum rate of STA-online in 1 hour: 20/s
```

【提示信息】 -

【平台说明】 AC

2.30 show ac-config flow-balance summary

该命令用于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

【参数说明】

参数	描述
-	-

【命令模式】 特权模式

【缺省级别】 1

【使用指导】 无

【配置举例】 1：查看基于流量的负载均衡组的详细配置信息：

```
Ruijie(config)#show ac-config flow-balance summary
Group            Threshold      AP NAME
---------------- --------------
--------------------------------------------------------------------------------
test-group1           5*100kbps ap1,ap2,ap3
test-group2           6*200kbps ap4,ap5,ap6
```

【提示信息】 -

【平台说明】 AC

2.31 show ac-config num-balance summary

该命令用于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

【参数说明】

参数	描述
-	-

【命令模式】 特权模式

【缺省级别】 1

【使用指导】 无

【配置举例】 1：查看基于数量的负载均衡组的详细配置信息：

```
Ruijie(config)#show ac-config num-balance summary
Group            Threshold AP NAME
---------------- --------- -------------------------
test-group1      1         ap1,ap2,ap3
test-group2      2         ap4,ap5,ap6
```

【提示信息】 -

【平台说明】 AC

2.32 show assoc-control

显示关联控制当前运行状态。

show assoc-control

【参数说明】

参数	描述
-	-

【命令模式】 特权模式

【缺省级别】 1

【使用指导】 无

【配置举例】 1：显示关联控制当前运行状态

```
Ruijie# show assoc-control
Association control is enabled.
```

2：显示关联控制当前运行状态

```
Ruijie# show assoc-control
Association control is disabled.
```

【提示信息】 -

【平台说明】 AC、胖 AP

2.33 show control-zone

显示关联控制域配置信息。

show control-zone [**summary** | *czone-name*]

【参数说明】

参数	描述
summary	显示摘要信息
czone-name	所要查看的关联控制域名称，长度[1,64]

【命令模式】 特权模式

【缺省级别】 1

【使用指导】 使用 **show control-zone summary** 命令查看配置的关联控制域信息，使用 **show control-zone** 或 **show**

control-zone *czone-name* 除了可查看到关联控制域信息，还可以查看到控制域中的 AP 信息。

【配置举例】 1：显示所有关联控制域信息

```
Ruijie# show control-zone summary
control zone num : 4
一年级 1 班
一年级 2 班
一年级 3 班
二年级 1 班
```

2：显示所有关联控制域信息

```
Ruijie# show control-zone summary
No control zone configuration.
```

3：显示所有关联控制域的详细配置信息

```
Ruijie# show control-zone
control zone num : 3
control-znoe        AP
-------------       ------------------------
一年级 1 班           AP1(1)-1  00d0.f800.889f
                    AP1(1)-2  00d0.f800.7869
二年级 2 班           AP2(2)-1  00d0.f800.889f
二年级 3 班           AP2(3)-1  offline
二年级 3 班           n/a
```

4：显示所有关联控制域的详细配置信息

```
Ruijie# show control-zone
No control zone configuration.
```

5：显示名为“1 年级 1 班”的关联控制域的详细配置信息

```
Ruijie# show control-zone 1 年级 1 班
control-zone        AP
-------------       ------------------------
一年级 1 班           AP1(1)-1  00d0.f800.889f
                    AP1(1)-2  00d0.f800.7869
二年级 2 班           AP2(2)-1  00d0.f800.889f
二年级 3 班           AP2(3)-1  offline
二年级 3 班           n/a
```

6：显示名为“5 年级 1 班”的关联控制域的详细配置信息

```
Ruijie# show control-zone 5 年级 1 班
```

```
No such control zone configuration.
```

【提示信息】 -

【平台说明】 AC、胖 AP

2.34 show package

显示终端包配置信息。

show package [*pkg-name*]

【参数说明】

参数	描述
pkg-name	所要查看的终端包名称，长度[1,32]

【命令模式】 特权模式

【缺省级别】 1

【使用指导】 无

【配置举例】 1：显示所有终端包配置

```
Ruijie# show package
total package num : 2
========= package_1 =========
primary STA : none
secondary STA num : 0
========= package_2 =========
primary STA : 00d0.f809.0092
secondary STA num : 4
00d0.f809.0096
00d0.f809.0097
00d0.f809.0098
00d0.f809.0099
```

2：显示所有终端包配置

```
Ruijie# show package
No package configuration.
```

【提示信息】 -

【平台说明】 AC、胖 AP

2.35 show sta-blacklist

显示 STA 黑名单

show sta-blacklist

【参数说明】

参数	描述
-	-

【命令模式】 特权模式

【缺省级别】 1

【使用指导】 无

【配置举例】 1：当前 STA 黑名单中的 STA

```
Ruijie#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
```

【提示信息】 -

【平台说明】 AC

2.36 sta-balance num-limit enable

配置开启 STA 在多次关联失败后自动停止负载均衡功能。

sta-balance num-limit enable

可以通过该命令的 **no** 前缀将自动停止负载均衡功能关闭。

no sta-balance num-limit enable

【参数说明】

参数	描述
-	-

【缺省配置】 缺省情况下，该功能关闭。

【命令模式】 AC 配置模式

【缺省级别】 15

【使用指导】 默认模式下，STA 在负载均衡下会一直尝试与负载均衡结果得到的 AP 进行连接。开启了 sta-balance 功能，STA 在负载均衡下最多尝试连接同一个 AP 5 次。如果 5 次全部连接失败，那么下一次连接 STA 将不受到负载均衡限制。

【配置举例】 1：开启 sta-balance 功能。

```
Ruijie(config)# ac-controller
Ruijie(config-ap)# sta-balance num-limit enable
```

【检验方法】 -

【提示信息】 -

【常见错误】 -

【平台说明】 AC

2.37 sta-blacklist

sta-blacklist 命令可以用于配置 STA 黑名单功能的开启和关闭，同时可以配置黑名单中 STA 的老化时间，并且可以通过配置 detect-time 和 fail-limit 来界定 STA 是否为攻击源。
sta-blacklist { **enable** | **lifetime** | **detect-time** | **fail-limit** } [*seconds* | *number*]

sta-blacklist 命令可以通过 **no** 参数用于配置 STA 黑名单功能的关闭，同时可以配置黑名单中 STA 的老化时间，并且可以通过配置 **detect-time 和 fail-limit** 来界定 STA 是否为攻击源。
no sta-blacklist { **enable** | **lifetime** | **detect-time** | **fail-limit** } [*seconds* | *number*]

【参数说明】

参数	描述
enable	开启 STA 黑名单功能
lifetime	表示 STA 在黑名单中的老化时间
detect-time	表示检测时间，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 关联失败次数达到上限次数(即 fail-limit)则把该 sta 加入黑名单；
fail-limit	表示在 detect-time 时间内，STA 关联失败次数上限。
seconds	表示时间，lifetime | detect-time 选项的参数，单位为秒，表示 lifetime 时取值范围 60-1200，表示 detect-time 时取值范围 5-60。
number	表示 STA 上线失败次数，fail-limit 选项参数，配置范围为 1-100。

【缺省配置】 黑名单功能默认关闭，lifetime 默认为 300 秒，detect-time 默认为 60 秒，number 默认值为 5。

【命令模式】 AC 配置模式

【缺省级别】 15

【使用指导】 无

【配置举例】 1：开启 STA 黑名单功能。

```
Ruijie(config)# ac-controller
Ruijie(config-ac)# sta-blacklist enable
```

2: 关闭 STA 黑名单功能。

```
Ruijie(config)# ac-controller
Ruijie(config-ac)# no sta-blacklist enable
```

3: 配置黑名单老化时间

```
Ruijie(config)# ac-controller
Ruijie(config-ac)# sta-blacklist lifetime 60
```

4: 配置检测时间

```
Ruijie(config)# ac-controller
Ruijie(config-ac)# sta-blacklist detect-time 10
```

5: 配置关联失败上限

```
Ruijie(config)# ac-controller
Ruijie(config-ac)# sta-blacklist fail-limit 20
```

【检验方法】 -

【提示信息】 -

【常见错误】 -

【平台说明】 AC

2.38 sta-idle-timeout

用户可以通过 **sta-idle-timeout** 来设置指定 AP 或 AP 组中无线用户的老化时间
sta-idle-timeout *timer-num*

可以通过该命令的 **no** 前缀将 client timeout timer 属性恢复默认值。
no sta-idle-timeout

【参数说明】

参数	描述
timer-num	要设置老化时间值，单位秒，取值范围：60~86400 说明：该值以 15 秒步进，配置值如果不是 15 整数倍，则自动向下取整。

【缺省配置】 缺省情况下，该定时器为 300s。

【命令模式】 AP 配置模式或 AP 组配置模式

【缺省级别】 15

【使用指导】 如果在设置的时间内，没有收到无线用户发来的信息，将认为该无线用户离开 WLAN 网络，系统将其从网络中删除

【配置举例】 1：进入 AP0001 的配置模式，并且配置其 client timeout timer 时间为 *600s*

```
Ruijie(config)# ap-config AP0001
Ruijie(config-ap)# sta-idle-timeout 600
```

2：进入 AP0001 的配置模式，并且配置其 client timeout timer 时间恢复为默认值 300s

```
Ruijie(config)# ap-config AP0001
Ruijie(config-ap)# no sta-idle-timeout-timer
```

3: 进入默认 AP 组，并且配置其 client timeout timer 时间为 *600s*

```
Ruijie(config)# ap-group default
Ruijie(config-group)# sta-idle-timeout 600
```

4：进入默认 AP 组，并且配置其 client timeout timer 时间恢复为默认值 300s

```
Ruijie(config)# ap-group default
Ruijie(config-group)# no sta-idle-timeout-timer
```

【检验方法】 -

【提示信息】 -

【常见错误】 -

【平台说明】 AC

2.39 sta-limit

通过 **sta-limit** 可以配置可连接的最大无线用户数，可以在 AC 配置模式下全局配置或在 AP 组和 AP 配置模式

下指定某个 AP 可连接的最大无线用户数，或在 WLAN 配置模式下指定某个 WLAN 可连接的最大无线用户数。
sta-limit *client-num*

通过 **no** 形式可以恢复默认值。
no sta-limit

【参数说明】

参数	描述
client-num	可连接的最大无线用户数 在 AC 配置模式下：最大值为 32 乘以 AC 可支持的 AP 数量（受 license 限制） 在 AP 组配置模式下：最大值为 1536 在 AP 配置模式下：离线 AP 或 ap-config all 的最大值为 1536，在线 AP 最大值根据 AP 的型号决定 在 WLAN 配置模式下：最大值与 AC 配置模式相同

【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
AP 组配置模式
AP 配置模式
WLAN 配置模式

【缺省级别】 15

【使用指导】 配置设备最多给多少 client 提供服务，该值不应该超过 AC 最大支持数和 license 限制的最大值。不同的 AC 产品支持的最大无线用户数不同。
对于 ap-config all、ap-group 和离线 AP 的配置，允许用户的配置范围为 1~512。如果用户配置的值超过 AP 实际可以支持的 STA 数目，当 AP 上线之后，会自动调整为实际可支持的最大 STA 数。
对于在线 AP 的配置，该命令可配置的最大值为 AP 实际支持的最大值。

【配置举例】 1：配置该 AC 最多给 2400 个 client 提供服务

```
Ruijie(config-ac)# sta-limit 2400
```

2：配置 AP 组（Default）内所有 AP 允许加入的最大无线用户数为 20

```
Ruijie(config)# ap-group default
Ruijie(config-group)# sta-limit 20
```

【检验方法】 -

【提示信息】 -

【常见错误】 -

【平台说明】 AC

2.40 sta-limit per-ap

通过 **sta-limit per-ap** 可以配置 WLAN 下每台 AP 可连接的最大无线用户数。
sta-limit per-ap *client-num*

通过 **no** 形式可以恢复默认值。
no sta-limit per-ap

【参数说明】

参数	描述
client-num	可连接的最大无线用户数。取值范围：1-1536

【缺省配置】 缺省不做限制。

【命令模式】 WLAN 配置模式

【缺省级别】 15

【使用指导】 配置每台 AP 在该 WLAN 下可支持多少用户。若配置值超过 AP 的最大限制，则以最大限制为准。

【配置举例】 1：配置每台 AP 的 WLAN 1 下仅允许 10 个用户关联

```
Ruijie(config)# wlan-config 1
Ruijie(config-wlan)# sta-limit per-ap 10
```

【检验方法】 -

【提示信息】 -

【常见错误】 -

【平台说明】 AC

2.41 sta-limit radio

通过 **sta-limit** 可以配置可连接的最大无线用户数，可以在 AP 组和 AP 配置模式下指定 AP 上某个 radio 可连接的最大无线用户数。
sta-limit *client-num* **radio** *radio-id*

通过 **no** 形式可以恢复默认值。
no sta-limit radio *radio-id*

【参数说明】

参数	描述
client-num	可连接的最大无线用户数，取值范围：1-156（或 AP 能力上限）
radio-id	radio 标识

【缺省配置】 缺省不做限制

【命令模式】 AP 组配置模式
AP 配置模式

【缺省级别】 15

【使用指导】 **sta-limit radio** 命令中的用户数限制与 sta-limit 中的用户数限制没有依赖关系。也就是说，**sta-limit radio** 中的用户数限制可以大于 sta-limit 中配置的用户数限制。
对于 ap-config all、ap-group 和离线 AP 的配置，允许用户的配置范围为 1~156。如果用户配置的值超过 AP 上该 radio 实际可以支持的 STA 数目，当 AP 上线之后，会自动调整为实际可支持的最大 STA 数。
对于在线 AP 的配置，该命令可配置的最大值为 AP 上该 radio 实际支持的最大值。

【配置举例】 1：配置 AP 的 radio 1 上允许加入的最大无线用户数为 20

```
Ruijie(config)# ap-config ap1
Ruijie(config-ap)# sta-limit 20 radio 1
```

【检验方法】 -

【提示信息】 -

【常见错误】 -

【平台说明】 AC

2.42 sta-logging rate-limit

通过 **sta-logging rate-limit** 可以配置每秒最多输出的 syslog 条数，这个 syslog 包括 STA 上下线以及 STA 信息变更的 syslog。

sta-logging rate-limit *limit-num*

通过 **no** 形式可以恢复默认的每秒 syslog 输出条数。

no sta-logging rate-limit

【参数说明】

参数	描述
limit-num	对于 STA 上下线的 syslog，每秒输出的最大条数。取值范围：0-10000

【缺省配置】 缺省每秒最多输出 5 条

【命令模式】 AC 配置模式

【缺省级别】 15

【使用指导】 无

【配置举例】 1：配置每秒输出 syslog 的最大条数为 100

```
Ruijie(config)# ac-controller
Ruijie(config-ac)# sta-logging rate-limit 100
```

【检验方法】 -

【提示信息】 -

【常见错误】 -

【平台说明】 AC

3 CAPWAP

命令	作用
ac-domain-name	配置 AP 发现 AC 的域名。
acip ipv4	配置 AP 加入指定 AC。
active-bin-file	配置激活一个 AP 软件版本。
ap-image	配置 AC 升级使用指定的文件升级指定系列的 AP。
ap-image	配置指定 AP 使用指定的文件升级。
apip	配置指定的 AP 的静态地址。
apip pppoe	配置 AP 使用 PPPoE 拨号方式获取地址
ap-serial	AC 上配置一个 AP 系列。
ap-subif	创建 WAN 口的子接口
ap-vlan	配置 AP 的 Native VLAN
ap-upgrade band-width	配置 AP 升级带宽
ap-upgrade group	配置 AP 添加到升级组
capwap ctrl-ip	配置 AC 与 AP 建立 CAPWAP 隧道的控制 IPv4 地址。
capwap dtls enable	配置 CAPWAP 控制通道 dtls 加密功能。
capwap fragment enable	开启 CAPWAP 分片功能。
capwap max-concurrent	配置 AC 允许的 AP 并发上线的最大个数。
capwap max-retransmit	配置 CAPWAP 报文的最大重传次数。
capwap mtu	配置 CAPWAP 隧道的路径 mtu。
capwap upgrade group	配置 AP 升级组
capwap upgrade max-concurrent	配置 AC 允许的 AP 并发升级的最大个数
echo-interval	配置 CAPWAP 的心跳保活间隔。
exec-cmd	在 AC 上配置 AP 执行命令或者配置某个 AP 组下 AP 执行命令
ip address	配置指定 AP 的静态 IP 地址。
link-latency	配置检测 AC 与指定 AP 组内 AP 之间的链路状态。
location	配置 AC 和 AP 的位置信息。
set-version	配置定制版本号
show ac-config active-file	显示本 AC 已经激活的文件列表。
show ac-config serial-product	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 upgrade-group	显示 AC 上升级组以及组内 AP 成员
show ap-config board-data	显示 AP 的主板数据信息。
show ap-config inventory	显示 AP 的厂商信息。
show ap-config link-latency	显示 AC 与 AP 之间的链路状态。
show ap-config reboot	查询 AP 的重启数据统计。
show ap-config static-ip	显示 AP 的静态地址
show ap-config summary location	显示所有 AP 的位置信息

show ap-config updating-list	显示 AP 升级状态信息
show ap-config wtp-descriptor	显示 AP 的状态描述信息。
show ap-config wtp-info	显示 AP 的状态信息
show capwap detail	显示 CAPWAP 隧道的详细信息。
show capwap state	显示 CAPWAP 隧道的状态信息。
show capwap statistics	显示 CAPWAP 隧道的报文统计信息。
show version	显示 AP 的版本信息
timestamp	配置指定 AP 或 AP 组内所有 AP 同步本 AC 的时间。
tran-data-show	显示指定 AP 最近传输到 AC 的各种日志信息。
tran-data-start	获取指定 AP 的各种日志信息。
wired-interface	配置 AP 关闭有线网络接口
wired-vlan	配置 AP 有线网络接口使用的 VLAN。

3.1 ac-domain-name

配置 AP 发现 AC 的域名。

ac-domain-name *ac-domain-name*

恢复缺省配置。

no ac-domain-name

【参数说明】

参数	描述
ac-domain-name	配置 AP 发现 AC 的域名，最多可配置 64 个字符，不能包含空格。

【缺省配置】 缺省情况下，ac.ruijie.com.cn

【命令模式】 AP 配置模式或 AP 组配置模式。

【缺省级别】 15

【使用指导】 AP 可以通过 DNS 域名来发现 AC。通过这条命令可以修订 AP 发现 AC 的域名，使得不同 AP 可以通过不同域名来发现不同的 AC。

【配置举例】 1：配置 AP 发现 AC 的域名为 ruijie-ac。

```
Ruijie(config-ap)# ac-domain-name ruijie-ac
```

【检验方法】 1： 使用 **show ap-config cb** *ap-name* 命令，可以查看配置是否成功

【提示信息】 -

【常见错误】 -

【平台说明】 仅 AC 支持该命令。

3.2 acip ipv4

配置 AP 加入指定 AC。
acip ipv4 *ip-address* [*ip-address…*]

删除指定 AC 配置。
no acip ipv4

【参数说明】

参数	描述
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。

【缺省级别】 15

【使用指导】 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。通过配置该命令 ,AP 将向这些 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。

⚠ 若瘦 AP 与所连接的 AC 都配置了该命令，则最终配置为 AC 的配置。

【配置举例】 1：为瘦 AP 配置加入 AC 的静态地址列表为 192.168.1.1，192.168.2.1。

```
Ruijie(config)# acip ipv4 192.168.1.1 192.168.2.1
```

2：配置 AP0001 加入 AC 的静态地址列表为 192.168.1.1，192.168.2.1。

```
Ruijie(config)# ap-config AP0001
Ruijie(config-ap)# acip ipv4 192.168.1.1 192.168.2.1
```

【检验方法】 1：瘦 AP 使用 **show running-config** 命令，AC 使用 **show ap-config running**，可以查看配置是否成功。

【提示信息】 -

【常见错误】 -

【平台说明】 仅瘦 AP 和 AC 支持该命令。

3.3 active-bin-file

在 AC 上激活一个 AP 软件版本，只有被激活的 AP 软件版本才可以用于升级。
active-bin-file *filename* [**rgos10**]

删除相关配置。
no active-bin-file *filename* [**rgos10**]

【参数说明】

参数	描述
filename	文件名，可以包含路径前缀，路径前缀包括 **flash:**， **tmp:**， **usb0:**，**sata0:**，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 rgos10 系统到 rgos11 系统的中间版本 ,只适用于 AP 的软件版本。

【缺省配置】 -

【命令模式】 AC 配置模式。

【缺省级别】 15

【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。

⚠ 激活版本文件后若要删除版本文件，需要先删除该配置去掉版本文件的占用，否则删除文件时会出错。

⚠ 直接覆盖版本文件无法触发 AP 升级，需要重新激活版本文件。

【配置举例】 1：在 AC 上激活一个 AP 软件版本文件：ap.bin。

```
Ruijie(config-ac)# active-bin-file ap.bin
```

2：在 AC 上激活一个 AP 软件版本文件：ap.bin，该软件版本在 usb0:文件系统中。

```
Ruijie(config-ac)# active-bin-file usb0:ap.bin
```

3：删除在 AC 上激活的一个 AP 软件版本文件：ap.bin。

```
Ruijie(config-ac)# no active-bin-file ap.bin
```

【检验方法】 1： 使用 **show ac-config active-file**，查看已激活的软件版本。

【提示信息】 -

【常见错误】 -

【平台说明】 NBR2500D-E、NBR3000D-E、NBR3000D-UE 出厂带 SATA 硬盘。NBR108G-P 、NBR800G、NBR950G、NBR1500G、NBR2000G、NBR1000G-C、NBR2000G-C、NBR3000G-S、NBR1000G-E、NBR6120-E、NBR1300G-E、NBR1700G-E、NBR2100G-E、NBR6205-E、NBR6135-E、NBR6210-E、NBR6215-E 出厂无 SATA 硬盘。其中 NBR6205-E、NBR6135-E、NBR6210-E、NBR6215-E 可自行购买 SATA 硬盘使用。

3.4 ap-image

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。
ap-image { **auto-upgrade** | *filename serial-name* }

取消配置
no ap-image { **auto-upgrade** | *filename serial-name* }

【参数说明】

参数	描述
auto-upgrade	自动匹配软件版本适用的 AP 型号进行升级
filename	指定的软件版本名称，包括后缀。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。

【缺省级别】 15

【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。

⚠ 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。

【配置举例】 1：配置产品系列名为 test-serial 使用 ap.bin 文件进行升级。

```
Ruijie(config-ac)# active-bin-file ap.bin
Ruijie(config-ac)# ap-serial test-serial AP220-E hw-ver 1.0
Ruijie(config-ac)# ap-image ap.bin test-serial
```

【检验方法】 1：使用 **show ac-config serial-product** 命令，查看产品系列、产品型号、升级版本之间的对应关系。

【提示信息】 -

【常见错误】 -

【平台说明】 仅 AC 支持该命令。

3.5 ap-image

配置指定 AP 使用指定的文件升级。该命令不支持 ap-config all 模式。
ap-image *filename*

取消配置
no ap-image

【参数说明】

参数	描述
filename	用于升级的 AP 软件版本文件名，包括后缀。

【缺省配置】 -

【命令模式】 AP 配置模式

【缺省级别】 15

【使用指导】 无

【配置举例】 1：配置 AP0001 使用 ap.bin 文件进行升级。

```
Ruijie(config-ac)# active-bin-file ap.bin
Ruijie(config-ac)# exit
Ruijie(config)# ap-config AP0001
Ruijie(config-ap)# ap-image ap.bin
```

【检验方法】 1：使用 **show ap-config running** 命令，可以查看配置是否成功。

【提示信息】 -

【常见错误】 -

【平台说明】 仅 AC 支持该命令

3.6 apip ipv4

配置指定的 AP 的静态地址。

apip ipv4 *ip-address network-mask gateway*

删除配置

no apip ipv4

【参数说明】

参数	描述
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 全局配置模式。

【缺省级别】 15

【使用指导】 瘦 AP 一般都是零配置的，其自身的 IP 地址和网关可以通过 DHCP 动态获取。当 AP 和 AC 建立 CAPWAP 隧道后，还可以通过 AC 下发 AP 的静态 IP 地址，以便 AP 重启后，其地址保持不变。在某些特殊的应用场合，期望手动设置瘦 AP 的静态 IP 地址，可以通过在 AP 的全局配置模式下配置该命令实现。

1.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，因此配置该命令后还需要在 AP 上通过“acip”命令配置 AC 的地址，以便 AP 和 AC 不在同一个子网时能发现并加入 AC。

2.该命令在 AP 配置后将自动保存，无需再执行配置保存命令。

3.该命令与 AC 上的 AP 配置模式的“ip address”命令作用相同，该命令不会影响 AC 上的配置。但是 AP 加入 AC 时，若 AC 的 AP 配置模式存在“ip address”命令且与“apip”命令冲突，将更新 AP 的静态地址并重建 CAPWAP 隧道。

【配置举例】 1：为瘦 AP 配置静态地址为 192.168.1.2，子网掩码为 255.255.255.0，网关地址为 192.168.1.1

```
Ruijie(config)# apip 192.168.1.2 255.255.255.0 192.168.1.1
```

【检验方法】 1：使用 **show running-config** 命令，可以查看配置是否成功

【提示信息】 -

【常见错误】 -

【平台说明】 仅瘦 AP 支持该命令

3.7 apip pppoe

配置 AP 使用 PPPoE 拨号方式获取地址。
apip pppoe

取消配置
no apip pppoe

【参数说明】

参数	描述
-	-

【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 全局配置模式。

【缺省级别】 15

【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。

【配置举例】 1：为瘦 AP 配置使用 PPPoE 拨号方式获取地址。

```
Ruijie(config)# apip pppoe
```

【检验方法】 1：使用 **show running-config** 命令，可以查看配置是否成功

【提示信息】 -

【常见错误】 -

【平台说明】 仅瘦 AP 支持该命令

3.8 ap-serial

在 AC 上配置一个 AP 系列，只有把 AP 硬件版本、产品型号配置到某个系列中才有可能通过 AC 升级 AP 软件版本。

ap-serial *serial-name ap-pid1 ap-pid2 ... ap-pidn* [**hw-ver** *hardware-versio*n]

取消配置

no ap-serial *serial-name*

【参数说明】

参数	描述
serial-name	要创建的 AP 系列名称，最多可配置 64 个字符，不能包含空格。
ap-pid1 ap-pid2 ... ap-pidn	要加入该 AP 系列的产品型号列表。ap-pidn 表示第 n 个产品型号。多个产品型号用英文逗号隔开
hardware-version	指定 AP 的硬件版本，最多可配置 64 个字符，不能包含空格。硬件版本格式为小数格式，符号‘x’或‘X’可用于通配后面的字符。

【缺省配置】 -

【命令模式】 AC 配置模式。

【缺省级别】 15

【使用指导】 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，激活软件版本，这三个步骤缺一不可，且在配置前需要确保 AC 系统文件中已存有该软件版本。

【配置举例】 1：在 AC 上创建一个 AP 系列，该系列的名称为 test-serial，其中指定 AP 硬件版本为 1.0，包含的 AP 型号有 AP220-SE、AP220-SH、AP220-E：

```
Ruijie(config-ac)# ap-serial test-serial AP220-SE AP220-SH AP220-E hw-ver 1.0
Ruijie(config-ac)# active-bin-file ap.bin
Ruijie(config-ac)# ap-iamge test-serial ap.bin
```

2：删除 AC 上的配置，使得属于产品系列名为 test-serial 的 AP 不再使用 ap.bin 文件进行升级：

```
Ruijie(config-ac)# no ap-image test-serial ap.bin
```

【检验方法】 1：使用 **show ac-config serial-product** 命令，查看产品系列、产品型号、升级版本之间的对应关系。

【提示信息】 -

【常见错误】 --

【平台说明】 仅 AC 支持该命令

3.9 ap-subif

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。

ap-subif enable

取消配置

no ap-subif enable

【参数说明】

参数	描述
-	-

【缺省配置】 -

【命令模式】 AP 配置模式/所有 AP 配置模式

【缺省级别】 15

【使用指导】 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。

【配置举例】 1：配置 AP1 去掉 WAN 口的子接口

```
Ruijie(config)# ap-config AP1
Ruijie(config-ap)# no ap-subif enable
```

【检验方法】 1：使用使用 **show ap-config running** 命令，可以查看配置是否成功。

【提示信息】 -

【常见错误】 -

【平台说明】 仅 AC 支持该命令

3.10 ap-vlan

配置 AP 的 Native VLAN，AP 将在该 VLAN 下的帧以 UNTAG 形式传输。

ap-vlan *vlan-id*

恢复默认值

no ap-vlan

【参数说明】

参数	描述
vlan-id	配置有线网络接口使用的 VLAN。 *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

【缺省级别】 15

【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。

⚠ 1.配置该命令将使已经在线的 AP 断开重建。

⚠ 2.在 WDS 部署中，ROOT-BRIDGE 和 NONROOT-BRIDGE 设备都部署本地转发时，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。

⚠ 3.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。

⚠ 4.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。

【配置举例】 1：配置 AP1 的 Native VLAN 的 VLAN ID 为 20。

```
Ruijie(config)# ap-config AP1
Ruijie(config-ap)# ap-vlan 20
```

【检验方法】 1：使用 **show ap-config running** 命令，可以查看配置是否成功。

【提示信息】 -

【常见错误】 -

【平台说明】 AC 支持该命令

3.11 ap-upgrade band-width

配置 AP 的集中升级带宽。
ap-upgrade band-width *num*

取消配置
no ap-upgrade band-width

【参数说明】

参数	描述
num	AP 升级的带宽，AP 集中升级的文件下发速率，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

【缺省级别】 15

【使用指导】 AC 给 AP 升级时，总是尽可能占用传输带宽以便减少升级时间。在一些带宽较小的网络中，在 AP 升级时可能需要保障有线业务的带宽，避免 AP 升级影响对其他业务造成影响。这时可以通过配置升级带宽限制来控制 AC 给 AP 发送版本文件的速率，从而达到控制 AP 升级的带宽占比。。

⚠ 1.配置只限制 AP 从 AC 集中升级的带宽控制，分布式升级不直接受该配置影响，但是分布式升级数据来源是根 AP 通过集中升级而来，所以分布式升级间接受该配置影响。

⚠ 2.单位为 1KB，如，AP 与 AC 链路上的最小可用带宽为 1Mbps，则配置 128

【配置举例】 1：为 AP 配置升级带宽，其中 128 转化为带宽就是 1Mbps,即 AP 集中升级占用最大带宽为 1M。

```
Ruijie(config-ac)# ap-upgrade band-width 128
```

【检验方法】 1：使用 **show ap-config running-config** 命令，可以查看配置是否成功。

【提示信息】 -

【常见错误】 -

【平台说明】 仅 AC 支持该命令

3.12 ap-upgrade group

配置 AP 加入到升级组。
ap-upgrade group *group-name*

取消配置
no ap-upgrade group

【参数说明】

参数	描述
group-name	AP 的升级组名字

【缺省配置】 -

【命令模式】 AP 配置模式

【缺省级别】 15

【使用指导】 AP 加入到升级组，将受到该升级组的配置约束。

⚠ 1.加入到同一个升级组的 AP 应该都要配置 ap-grade band-width，以达到以升级组为单位的带宽控制

⚠ 2.配置提前是升级组已通过 capwap upgrade group 命令创建

⚠ 3.no 配置时，如果组内存在 ap，则不允许删除组

【配置举例】 1：为 AP 加入到升级组 UPGRADE-GROUP1 中。

```
Ruijie(config-ac)# ap-upgrade group UPGRADE-GROUP1
```

【检验方法】 1：使用 **show ap-config running-config** 命令，可以查看配置是否成功。

【提示信息】 -

【常见错误】 -

【平台说明】 仅 AC 支持该命令

3.13 capwap ctrl-ip

配置 AC 与 AP 建立 CAPWAP 隧道的控制 IPv4 地址，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。

capwap ctrl-ip *ip-address*

取消配置

no capwap ctrl-ip

【参数说明】

参数	描述
ip-address	指定与 AP 建立隧道的 CAPWAP 隧道控制 IP 地址，需要为本 AC 设备的某个接口的 IP 地址。

【缺省配置】 -

【命令模式】 AC 配置模式

【缺省级别】 15

【使用指导】 AC 一般是通过 Loopback 地址来建立 CAPWAP 隧道的，该命令可以使得 AC 能够用其它三层接口的地址来建立 CAPWAP 隧道。

⚠ 1.配置有可能使已经在线的 AP 断开。

⚠ 2.配置一个在 AC 上不存在的地址，会使得 CAPWAP 隧道不能建立

⚠ 3.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)。

⚠ 4.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。

【配置举例】 1：为 AC 配置用于建立 CAPWAP 隧道的地址为 10.0.0.1，其中 10.0.0.1 是一个 SVI 地址。

```
Ruijie(config-ac)# capwap ctrl-ip 10.0.0.1
```

【检验方法】 1：使用 **show running-config** 命令，可以查看配置是否成功。

【提示信息】 -

【常见错误】 -

【平台说明】 仅 AC 支持该命令

3.14 capwap dtls enable

配置 CAPWAP 控制通道 dtls 加密功能。
capwap dtls enable

配置 CAPWAP 控制通道不加密。
no capwap dtls enable

【参数说明】

参数	描述
-	-

【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

【缺省级别】 15

【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。

【配置举例】 1：开启配置 CAPWAP 控制通道 dtls 加密功能。

```
Ruijie(config)# ac-controller

Ruijie(config-ac)# capwap dtls enable
```

【检验方法】 1：使用 **show running-config** 命令，可以查看配置是否成功。

【提示信息】 -

【常见错误】 -

【平台说明】 仅 AC 支持该命令

3.15 capwap fragment enable

开启 CAPWAP 分片功能。
capwap fragment enable

关闭 CAPWAP 分片功能。
no capwap fragment enable

【参数说明】

参数	描述
-	-

【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。

【缺省级别】 15

【使用指导】 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。

【配置举例】 1：开启配置 AP1 的 CAPWAP 分片功能

```
Ruijie(config)# ap-config AP1

Ruijie(config-ap)# capwap fragment enable
```

【检验方法】 1：使用 **show ap-config running** 命令，可以查看配置是否成功。

【提示信息】 -

【常见错误】 -

【平台说明】 仅 AC 支持该命令

3.16 capwap max-concurrent

配置 AC 允许的 AP 并发上线的最大个数。
capwap max-concurrent *num*

取消配置
no capwap max-concurrent

【参数说明】

参数	描述
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

【缺省级别】 15

【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。

⚠ 当配置的值较小时，会使该 AC 下所有 AP 上线的总时间偏长。

【配置举例】 1：为 AC 配置允许的最大 AP 并发上线数

```
Ruijie(config-ac)#capwap max-concurrent 100
```

【检验方法】 1：使用 **show running-config** 命令，可以查看配置是否成功。

【提示信息】 -

【常见错误】 -

【平台说明】 仅 AC 支持该命令

3.17 capwap max-retransmit

配置 CAPWAP 报文的最大重传次数。
capwap max-retransmit *num*

取消配置
no capwap max-retransmit

【参数说明】

参数	描述
num	最大重传次数，默认值为 5，范围为 3~60

【缺省配置】 重传次数为 5

【命令模式】 AP 配置模式或 AP 组配置模式

【缺省级别】 15

【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。

【配置举例】 1：配置 AP1 的最大重传次数为 20

```
Ruijie(config)# ap-config AP1
Ruijie(config-ap)#capwap max-retransmit 20
```

【检验方法】 1：使用 **show ap-config running-config** 命令，可以查看配置是否成功。

【提示信息】 -

【常见错误】 -

【平台说明】 仅 AC 支持该命令

3.18 capwap upgrade group

配置 AP 升级组。

capwap upgrade group *group-name* [**max-concurrent** *num*]

取消配置

no capwap upgrade group *group-name* [**max-concurrent**]

【参数说明】

参数	描述
group-name	升级组名字
num	该升级组允许并发的集中升级 AP 个数，默认为 5，范围 1~200

【缺省配置】 -

【命令模式】 AC 配置模式

【缺省级别】 15

【使用指导】 配置 AP 升级组，带宽控制的集中升级以升级组为调度单位，AC 集中升级并发数均衡的分配到所有升级组中。

⚠ 1.默认每个升级组最大集中并发数为 5，该数字应该为该组最大可用带宽/每个 ap 可用最大带宽比。

【配置举例】 1：配置 AP 升级组 Upgrade-Group1，最大并发数 10 个。

```
Ruijie(config-ac)# capwap upgrade group Upgrade-Group1 max-current 10
```

【检验方法】 1：使用 **show running-config** 命令，可以查看配置是否成功。

【提示信息】 -

【常见错误】 -

【平台说明】 仅 AC 支持该命令

3.19 capwap mtu

配置 CAPWAP 隧道的路径 mtu。
capwap mtu *num*

恢复缺省值
no capwap mtu

【参数说明】

参数	描述
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

【缺省级别】 15

【使用指导】 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。

⚠ 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。

【配置举例】 1：配置 AP1 的路径 MTU 为 1200 字节

```
Ruijie(config)# ap-config AP1

Ruijie(config-ap)# capwap mtu 1200
```

【检验方法】 1：使用 **show ap-config running** 命令，可以查看配置是否成功。

【提示信息】 -

【常见错误】 -

【平台说明】 仅 AC 支持该命令

3.20 capwap upgrade max-concurrent

配置 AC 允许的 AP 并发升级的最大个数。
capwap upgrade max-concurrent *num*

取消配置
no capwap upgrade max-concurrent

【参数说明】

参数	描述
num	AP 并发升级的最大个数，范围为 1~200

【缺省配置】 AP 并发上线的最大个数默认值为 15

【命令模式】 AC 配置模式

【缺省级别】 15

【使用指导】 大量 AP 并发升级时，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 并发升级的最大个数。

【配置举例】 1：为 AC 配置允许的最大 AP 并发升级数

```
Ruijie(config-ac)#capwap upgrade max-concurrent 10
```

【检验方法】 1：使用 **show running-config** 命令，可以查看配置是否成功。

【提示信息】 -

【常见错误】 -

【平台说明】 仅 AC 支持该命令

3.21 echo-interval

配置 CAPWAP 的心跳保活间隔。
echo-interval *seconds*

恢复缺省值

no echo-interval

【参数说明】

参数	描述
seconds	CAPWAP 心跳保活间隔，范围为 5~255，单位为秒。

【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。

【缺省级别】 15

【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。

⚠ 无线网络部署时可以根据网络规模调整 echo-interval 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。

【配置举例】 1：配置 AP0001 的心跳间隔为 10s

```
Ruijie(config)# ap-config AP0001
Ruijie(config-ap)# echo-interval 10
```

2：配置所有 AP 的心跳间隔为 10s

```
Ruijie(config)# ap-config all
Ruijie(config-ap)# echo-interval 10
```

3：配置 AP 组（default）下所有 AP 的心跳间隔为 10s

```
Ruijie(config)# ap-group default
Ruijie(config-ap-group)# echo-interval 10
```

【检验方法】 1：使用 **show ap-config running** 命令，可以查看配置是否成功。

【提示信息】 -

【常见错误】 -

【平台说明】 仅 AC 支持该命令

3.22 exec-cmd

配置 AP 执行某条命令

exec-cmd mode *exec-mode* **cmd** *exec-cmd* **once**

配置 AP 组内 AP 执行某条命令

exec-cmd *exec-cmd*

取消配置

no exec-cmd mode *exec-mode* **cmd** *exec-cmd*

【参数说明】

参数	描述
exec-mode	命令在 AP 上执行所在的模式
exec-cmd	在 AP 上或者对应 ap-config 上执行的命令
once	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 配置模式或 AP 组配置模式。

【缺省级别】 15

【使用指导】 一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 ap-config 下的 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；

一些配置命令只有 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。

【配置举例】 1：配置 AC 上关闭 AP 的 EWEB 功能

```
Ruijie(config)#ap-config AP1
Ruijie(config-ap)# exec-cmd mode configure cmd "no enable service web-server all"
```

2：配置 AC 上重新开启 AP 的 EWEB 功能

```
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"
```

3：配置 AP 组内所有 AP 蓝牙 ibeacon 配置

```
Ruijie(config)#ap-group default
Ruijie(config-group)#exec-cmd ibeacon uuid ffffffffffffffffffffffffffffffff major ffff minor ffff
```

4：配置 AP 组内所有 AP 关闭 AP 的 EWEB 功能

```
Ruijie(config-group)#exec-cmd exec-cmd mode configure cmd "no enable service web-server all"
```

【检验方法】 1：使用 **show ap-config running** 命令，可以查看配置是否成功。

【提示信息】 -

【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

【平台说明】 仅 AC 支持该命令

3.23 ip address

配置指定 AP 的静态 IP 地址。

ip address *ip-address network-mask gateway*

恢复为缺省配置。

no ip address

【参数说明】

参数	描述
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

【缺省级别】 15

【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。

⚠ 1.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 配置模式下通过“acip”命令配置连接的 AC 地址，以便 AP 和 AC 不在同一个子网时能发现并加入 AC。

⚠ 2.若 AP 当前的地址与该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。

【配置举例】 1：配置 AP0001 的地址为 1.1.1.1，掩码为 255.255.255.0，下一跳为 1.1.1.2。

```
Ruijie(config)# ap-config AP0001

Ruijie(config-ap)# ip address 1.1.1.1 255.255.255.0 1.1.1.2
```

【检验方法】 1：使用 **show ap-config running** 命令，可以查看配置是否成功。

【提示信息】 -

【常见错误】 -

【平台说明】 仅 AC 支持该命令

3.24 link-latency

配置检测 AC 与指定 AP 组内 AP 之间的链路状态。

link-latency

取消配置

no link-latency

【参数说明】

参数	描述
-	-

【缺省配置】 -

【命令模式】 AP 配置模式或 AP 组配置模式

【缺省级别】 15

【使用指导】 无

【配置举例】 1：开启检测指定 AP-0001 与 AC 之间的链路状态，并查看对应的链路状态信息。

```
Ruijie(config)# ap-config AP-0001
Ruijie(config-ap)# link-latency
```

2：开启 AP 组“default”检测 AC 与 AP 的链路状态，并查看指定 AP-0001 的链路状态信息。

```
Ruijie(config)# ap-group default
Ruijie(config-ap-group)# link-latency
```

【检验方法】 1：使用 **show ap-config link-latency** 命令查看 AC 与 AP 之间的链路状态信息。

【提示信息】 -

【常见错误】 -

【平台说明】 仅 AC 支持该命令

3.25 location

配置 AC 或 AP 的位置信息。

location *location-string*

恢复至缺省配置。
no location

【参数说明】

参数	描述
location-string	AC 或 AP 的位置信息，最多可配置 255 字符,不能带空格。

【缺省配置】 缺省情况下，AC 的位置信息为 Ruijie_COM，AP 的位置信息为空。

【命令模式】 AC 配置模式或 AP 配置模式。

【缺省级别】 15

【使用指导】 无

【配置举例】 1：配置特定 AC 的位置为计算机系 2 楼（computer-layer2）

```
Ruijie(config-ac)# location computer-layer2
```

2：配置 AP0001 的位置信息为 AP-company

```
Ruijie(config)# ap-config AP0001
Ruijie(config-ap)# location AP-company
```

【检验方法】 1：使用 **show ac-config running** 命令，查看 AC 位置信息。
2：使用 **show ap-config running** 命令，查看 AP 位置信息。

【提示信息】 -

【常见错误】 -

【平台说明】 仅 AC 支持该命令

3.26 set-version

配置定制版本号。
set-version *string*

【参数说明】

参数	描述
string	定制的版本号

【缺省配置】 -

【命令模式】 AC 配置模式。

【缺省级别】 15

【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。

【配置举例】 1：配置定制软件版本号为 RGOS 10.4(2B17)-SP2

```
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。

【提示信息】 -

【常见错误】 -

【平台说明】 仅 AC 支持该命令

3.27 show ac-config active-file

显示本 AC 已经激活的文件列表。

show ac-config active-file

【参数说明】

参数	描述
-	-

【命令模式】 特权模式

【缺省级别】 15

【使用指导】 无

【配置举例】 1：显示本 AC 已经激活的文件列表

```
Ruijie#show ac-config active-file
Cnt    File Name                          Image Id            Software number      Type
Used Cnt   DL Cnt Ready
```

```
------ -------------------------------- ------------------- ------------------- ----------
---------- ---------- --------

1      ap220ev1.1-mid(6-3).bin          RGOS 10.X-UPG       NA                  rgos10     0
0          Init

2      ap220.bin                        1.0.0.017ed304      M09092708272014     main
0          0          Init
```

字段解释：

字段	说明
Cnt	激活的文件列表编号
File Name	激活的文件名
Image Id	激活的文件版本
Software number	激活的文件编译日期
Used Cnt	代表当前有多少 AP 正在使用这个文件
DL Cnt	代表该升级文件已经给多少 AP 下载了
Ready	代表该文件是否已经完全激活.

【提示信息】 -

【平台说明】 -

3.28 show ac-config serial-product

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

【参数说明】

参数	描述
-	-

【命令模式】 特权模式

【缺省级别】 15

【使用指导】 无

【配置举例】 1：本 AC 配置的 AP 产品系列和产品型号

```
Ruijie#show ac-config serial-product


Cnt    Serial Name     Hardware Version File Name    AP Product ID
```

```
------ --------------- ---------------- ------------ ---------------
1      ap-ser1.x       1.x              ap220-1.bin  AP220-E
                                                     AP220-SE
                                                     AP220-SH
                                                     AP620-H
                                                     AP220-E(M)
2      ap-ser2.x       2.x              ap220.bin    AP220-E
                                                     AP220-SH
                                                     AP220-E(M)
```

字段解释：

字段	说明
Cnt	显示编号
Serial Name	AP 产品系列
Hardware Version	硬件版本号
File Name	AP 产品系列对应的升级文件
AP Product ID	AP 产品型号

【提示信息】 -

【平台说明】 -

3.29 show ac-config upgrade-group

显示 AC 上配置的升级组和升级组内 AP 信息。

show ap-config upgrade-group [*group-name***]**

【参数说明】

参数	描述
group-name	要查询的 AP 升级组的名字

【命令模式】 特权模式

【缺省级别】 15

【使用指导】 无

【配置举例】 1：显示 AC 配置的升级组信息。

```
Ruijie#show ac-config upgrade-group
```

```
Cnt    Group-Name                Max-Concurrent    Token cnt    Upgrading cnt
------ --------------------------------- ------------ ----------- ------------
1      UPGRADE-GROUP1              10               2          1
```

字段解释：

字段	说明
Cnt	显示编号
Group-Name	AP 升级组名字
Max-Concurrent	本组最大升级并发数
Token cnt	当前分配的升级数
Upgrading cnt	正在升级的 AP 数

2：显示升级组内部的 AP 信息。

```
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
```

字段解释：

字段	说明
Cnt	显示编号
Ap-Name	AP 名字
Ap-Mac	AP 的 MAC 地址
Online	是否在线
Upgrade	是否正在升级
Band-width	该 AP 的带宽配置

【提示信息】 -

【平台说明】 -

3.30 show ap-config board-data

显示 AP 的主板数据信息。

show ap-config board-data *ap-name*

【参数说明】

参数	描述
ap-name	要查询的 AP 的名称

【命令模式】 特权模式

【缺省级别】 15

【使用指导】 无

【配置举例】 1：显示 AP 的主板数据信息。

```
ac#show ap-config board-data ap330
Ap(ap330)'s board data:
  wtp model num     :30090020
  wtp serial num    :G1GD111000864
  board id           :AP330-I
  board reversion   :1.00
  base address       :1414.4b62.7f77
```

字段解释：

字段	说明
wtp model num	产品型号
wtp serial num	AP 序列号
board id	主板 id
board reversion	主板版本
base address	系统 mac

【提示信息】 -

【平台说明】 -

3.31 show ap-config inventory

显示 AP 的厂商信息。

show ap-config inventory *ap-name*

【参数说明】

参数	描述
ap-name	要查询的 AP 的名称

【命令模式】 特权模式

【缺省级别】 15

【使用指导】 无

【配置举例】 1：显示 AP 的厂商信息

```
ac#show ap-config inventory wlan-ap-0001

AP Name: wlan-ap-0001

Location:

Product Id: AP220E

Vendor Id: 31762

SN: 1531991320
```

字段解释：

字段	说明
AP Name	AP 名字
Location	AP 位置
Product Id	产品 id
Vendor Id	厂商 id
SN	序列号

【提示信息】 -

【平台说明】 -

3.32 show ap-config link-latency

显示 AC 与 AP 之间的链路状态。

show ap-config link-latency { **all** | **single** *ap-name* }

【参数说明】

参数	描述
all	查询所有 AP
single	查询单个 AP
ap-name	要查询的 AP 的名称

【命令模式】 特权模式

【缺省级别】 15

【使用指导】 无

【配置举例】 1：查看单个 AP 与 AC 之间的链路状态。

```
ac#show ap-config link-latency single ap330

AP Name                                  Status      Current    Maximum   Minimum   Number

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

ap330                                    Disabled     0ms        0ms       0ms       0
```

字段解释：

字段	说明
AP Name	AP 名字
Status	链路状态
Current	当前链路延
Maximum	最大链路延迟
Minimum	最小链路延迟
Number	最大链路延迟，上传的次数

【提示信息】 -

【平台说明】 -

3.33 show ap-config reboot

查询 AP 的重启数据统计。

show ap-config reboot *ap-name*

【参数说明】

参数	描述
ap-name	要查询的 AP 的名称。

【命令模式】 特权模式

【缺省级别】 15

【使用指导】 无

【配置举例】 1：查询 AP 的重启数据统计

```
Ruijie#show ap-config reboot ap330

Ap(ap330)'s reboot statistic:

Reboot Cnt          :67

AC Init Cnt         :0
```

```
Link Fail Cnt       :0
SW Fail Cnt         :0
HW Fail Cnt         :0
Other Fail Cnt      :67
Unknow Fail Cnt     :0
Last Fail Type      :0
```

字段解释：

字段	说明
Reboot Cnt	重启次数
AC Init Cnt	AC 初始化次数
Link Fail Cnt	链路失败次数
SW Fail Cnt	软件失败次数
HW Fail Cnt	硬件失败次数
Other Fail Cnt	其他原因失败次数
Unknow Fail Cnt	未知原因失败次数
Last Fail Type	上次失败类型

【提示信息】 -

【平台说明】 -

3.34 show ap-config static-ip

显示所有 AP 的位置信息。

show ap-config static-ip { **all** | **single** *ap-name* }

【参数说明】

参数	描述
all	查询所有 AP
single	查询单个 AP
ap-name	要查询的 AP 的名称

【命令模式】 特权模式

【缺省级别】 15

【使用指导】 无

【配置举例】 1：显示 AP 的静态地址

其中包含 AP 名称、AP ip 地址、掩码和网关。

```
Ruijie#show ap-config static-ip single 0034.5612.78a0
AP Name                     Static    IP              Net Mask         Getway
--------------------------- --------- --------------- ---------------- ----------------
0034.5612.78a0              Enabled  22.22.22.22      255.255.255.0    22.22.22.53
```

【提示信息】 -

【平台说明】 仅 AC 支持

3.35 show ap-config summary location

显示所有 AP 的位置信息。

show ap-config summary location

【参数说明】

参数	描述
-	-

【命令模式】 特权模式

【缺省级别】 15

【使用指导】 无

【配置举例】 1：显示 AP 的位置信息

其中包含 AP 名称、AP ip 地址、AP mac 地址、AP 位置信息和 AP 状态即在线或离线。

```
Ruijie#show ap-config summary location
AP Name                                 IP Address      Mac Address    Location
State
--------------------------------------- --------------- --------------
--------------------------------------- -----
ap220                                   172.18.100.4    1414.4b13.9ff3  Bangongshi_4#
Run
ap3                                     172.18.100.16   001a.a94e.d40d  教学楼 20#3F
Run
```

【提示信息】 -

【平台说明】 仅 AC 支持

3.36 show ap-config updating-list

显示 AP 升级状态信息。

show ap-config updating-list

【参数说明】

参数	描述
-	-

【命令模式】 特权模式

【缺省级别】 15

【使用指导】 无

【配置举例】 1：显示 AP 的升级状态信息

```
Ruijie#show ap-config updating-list
AP NAME                    AP PID          File Tx  Time      AP Reset Ready
-------------------------- --------------- -------- --------- ---------------
AP220-I                    AP220-I          100%     00:00:45  Y
00d0.1414.3f67             AP220-E          98 %     00:00:48  N
```

字段解释：

字段	说明
AP NAME	AP 名字
AP PID	AP 产品 ID
File Tx	文件传输进度
Time	升级耗时
AP Reset Ready	升级完成可以重启

【提示信息】 -

【平台说明】 仅 AC 支持

3.37 show ap-config wtp-descriptor

显示 AP 的状态描述信息。

Show ap-config wtp-descriptor *ap-name*

【参数说明】

参数	描述
ap-name	要查询的 AP 的名称。

【命令模式】 特权模式

【缺省级别】 15

【使用指导】 无

【配置举例】 1：显示 AP 的状态描述信息。

```
Ruijie#show ap-config wtp-descriptor AP220E-0
Ap(AP220E-0)'s wtp descriptor:
max radio           :2
radio in used       :2

encrypt num         :1
Cnt  WBID    Encry Cap
1    0x1     0xc

sub descriptor num  :3
Cnt  vendor id version type   version len    version
1    0x7c12    BOOT Ver       21             1.1.5.0a2945e(140830)
2    0x7c12    ACT SW Ver     14             1.0.0.6b94c319
3    0x7c12    HW Ver         4              2.00
```

字段解释：

字段	说明
max radio	最多射频口数目。
radio in used	正在使用的射频口数目。
encrypt num	无线口支持的加密能力：我司支持 ccmp 和 tkip。

【提示信息】 -

【平台说明】 -

3.38 show ap-config wtp-info

显示 AP 的状态信息。

show ap-config wtp-info *ap-name*

【参数说明】

参数	描述
ap-name	要查询的 AP 的名称。

【命令模式】 特权模式

【缺省级别】 15

【使用指导】 无

【配置举例】 1：显示 AP 的状态信息。

```
Ruijie#show ap-config wtp-info ap220e

Ap(ap220e)'s status:

AC IP(status):      :101.101.101.101

AP IP(status):      :10.10.10.8 255.255.255.0 10.10.10.2

AP IPV4 ENABLE:     :enable

Location Data:      :

Session ID:         :88320000,111163fb,5c3b3cb3,2cac585a

mac type            :full support

WTP Name:           :ap220e

AP Domain Name:     :ac.ruijie.com.cn

wired vlan          :0 port id 1

wired vlan          :0 port id 2

wired vlan          :0 port id 3

wired vlan          :0 port id 4

Cw_interface_name   :BVI 1

Cw_wan_interface_ifx::1

Cw_wan_interface_ifx::0

Upgrading State     :Init

AP Image file       :NA

Real version        :1.0.0.641d31e6

Custom version      :AP_RGOS 11.1(2)B1

Upgrade version     :NA

Upgrade from AP     :FALSE
```

```
Upgrade for other AP:FALSE

Upgrade from AC     :FALSE

Wait for upgrade    :FALSE

Support distr-upg   :TRUE

Upgrade-banfwidth   :128

Upgrade group       :Upgrade-group1
```

字段解释：

AC IP(status)	AP 的 acip ipv4 状态
AP IP(status)	AP 的 apip ipv4 状态
AP IPV4 ENABLE	AP 的 apip ipv4 enable 配置
Location Data	AP 上报的位置信息
Session ID	AP 与 AC 建立 CAPWAP 使用的会话 ID
mac type	MACTYPE 类型
WTP Name	AP 名字
AC Domain Name	AP 上报的 AC 域名
wired vlan	AP LAN 口 1 上的 wired-vlan 配置
wired vlan	AP LAN 口 2 上的 wired-vlan 配置
wired vlan	AP LAN 口 3 上的 wired-vlan 配置
wired vlan	AP LAN 口 4 上的 wired-vlan 配置
Cw_interface_name	AP 上选择的接口名字
Cw_wan_interface_ifx	AP 上 WAN 口 1 索引
Cw_wan_interface_ifx	AP 上 WAN 口 2 索引
Upgrading State	AP 升级状态
AP Image file	AP 升级的 bin 名字
Real version	AP 运行的真实版本
Custom version	AP 运行的软件定制版本
Upgrade version	AP 升级的版本
Upgrade from AP	是否从 AP 分布式升级
Upgrade for other AP	是否为其他 AP 进行分布式升级
Upgrade from AC	是否从 AC 集中升级
Wait for upgrade	是否等待升级
Support distr-upg	是否支持分布式升级
Upgrade-banfwidth	集中升级带宽
Upgrade group	集中升级组

【提示信息】 -

【平台说明】 -

3.39 show capwap detail

显示 CAPWAP 隧道的详细信息。

show capwap [*index* | [*ip-address* [*port*]]] **detail**

【参数说明】

参数	描述
index	隧道索引
ip-address	隧道的 IP 地址
port	隧道的端口号

【命令模式】 特权模式

【缺省级别】 15

【使用指导】 无

【配置举例】 1：显示地址为 1.1.1.1 的 CAPWAP 隧道信息：

```
Ruijie#show capwap 1.1.1.1 detail
CAPWAP process “capwap 1” with state Run
  Process uptime is 3 days 0 hour 41 minutes
  Echo interval is 30 secs, Dead interval is 81 secs
  Current timers echo-interval
  Peer address is 172.18.59.5
  Peer control port is 10000, data port is 10001
  My address is 55.55.55.60
  The MAC of AP is 001a.a94e.d773
  The Session ID of AP is 001a.a94e.d773.53e1.0801.53e1.0801.53e1
  The Path MTU is 1500
  Recent recieved request's sequence number 39
  Recent recieved response's sequence number 11
  Recent send request's sequence number 11
  Retransmit Count 0, Discovery Count 0, Failed DTLS Session Count 0
  Sending queue length 0, Receive queue length 0
```

【提示信息】 -

【平台说明】 -

3.40 show capwap state

显示 CAPWAP 隧道的状态信息。

show capwap state

【参数说明】

参数	描述
-	-

【命令模式】 特权模式

【缺省级别】 15

【使用指导】 无

【配置举例】 1：显示 CAPWAP 隧道的状态信息：

```
Ruijie#show capwap state

CAPWAP tunnel state, 3 peers, 2 is run:

Index  Peer IP                Peer Port  State          Mac Address

1      192.168.0.1            10000      Run             001a.a900.0001

2      192.168.0.2            10000      Run             001a.a900.0002

3      192.168.0.3            10000      DTLS Teardown   001a.a900.0003
```

字段解释：

字段	说明
Index	隧道索引
Peer IP	隧道对端的 IP 地址
Peer Port	端口号
State	隧道的状态信息
Mac Address	AP 的 mac 地址，仅 AC 上才显示该信息

【提示信息】 -

【平台说明】 -

3.41 show capwap statistics

显示 CAPWAP 隧道的报文统计信息。

show capwap [*index* | [*ip-address* [*port*]]] **statistics**

【参数说明】

参数	描述
index	隧道索引
ip-address	隧道的 IP 地址
port	隧道的端口号

【命令模式】 特权模式

【缺省级别】 15

【使用指导】 无

【配置举例】 1：显示地址为 1.1.1.1 的 CAPWAP 隧道报文统计信息。

```
Ruijie#show capwap 1.1.1.1 statistics
```

【提示信息】 -

【平台说明】 -

3.42 show version

显示 AP 的版本信息。

show version { **all** | *ap-name* }

【参数说明】

参数	描述
all	所有 AP
ap-name	指定 AP 名称

【命令模式】 特权模式

【缺省级别】 15

【使用指导】 无

【配置举例】 1：显示所有 AP 的版本信息。

```
Ruijie#show version all

AP(AP220E-0)'s version:

  Product ID          : AP220-E
```

```
  System uptime       : 0:3:9:32
  Hardware version    : 2.00
  Software version    : AP_RGOS 11.1(2)B1
  Patch number        : SP2
  Software number     : M05563609152014
  Serial number       : 1234942570005
  MAC address         : 00d0.f822.33b0

AP(AP220E-2)'s version:
  Product ID          : AP220-E
  System uptime       : 0:6:11:53
  Hardware version    : 2.00
  Software version    : AP_RGOS 11.1(2)B1
  Patch number        : SP2
  Software number     : M05563609152014
  Serial number       : 1234942570018
  MAC address         : 001a.a9bd.0c1b
```

【提示信息】 -

【平台说明】 -

3.43 timestamp

配置指定 AP 或 AP 组内所有 AP 同步本 AC 的时间。

timestamp

【参数说明】

参数	描述
-	-

【缺省配置】 -

【命令模式】 AP 配置模式或 AP 组配置模式

【缺省级别】 15

【使用指导】 无

【配置举例】 1：配置 AP0001 同步本 AC 的时间

```
Ruijie(config)# ap-config AP0001
Ruijie(config-ap)# timestamp
```

2：配置 AP 组（Default）内所有 AP 同步本 AC 的时间

```
Ruijie(config)# ap-group default
Ruijie(config-ap-group)# timestamp
```

【检验方法】 1： 查看 AP 和 AC 的时间是否一致

【提示信息】 -

【常见错误】 -

【平台说明】 仅 AC 支持该命令

3.44 tran-data-show

显示指定 AP 最近传输到 AC 的各种日志信息。

tran-data-show *ap-name* { **exception** | **cpuinfo** | **memory** | **syslog** | **tech-support** }

【参数说明】

参数	描述
ap-name	指定的 AP 的名称
exception	指定 AP 的死机日志信息
cpuinfo	指定 AP 的 CPU 信息
memory	指定 AP 的内存信息
syslog	指定 AP 的普通信息
tech-support	指定 AP 的一键收集 console 信息

【缺省配置】 -

【命令模式】 AC 配置模式

【缺省级别】 15

【使用指导】 无

【配置举例】 1：显示 AP0001 的死机日志

```
Ruijie(config-ac)# tran-data-show AP0001 exception
```

2：显示 AP0001 的 cpu 信息

```
Ruijie(config-ac)# tran-data-show AP0001 cpuinfo
```

3：显示 AP0001 的内存信息

```
Ruijie(config-ac)# tran-data-show AP0001 memory
```

4：显示 AP0001 的普通日志信息

```
Ruijie(config-ac)# tran-data-show AP0001 syslog
```

5：显示 AP0001 的一键收集 console 信息

```
Ruijie(config-ac)# tran-data-show AP0001 tech-support
```

【检验方法】 1：查看是否显示指定的日志信息。

【提示信息】 -

【常见错误】 -

【平台说明】 AC 支持该命令

3.45 tran-data-start

获取指定 AP 的各种日志信息。

tran-data-start *ap-name* { **exception** | **memory** | **tech-support** | **tech-package** }

【参数说明】

参数	描述
ap-name	指定的 AP 的名称。
exception	指定 AP 发送死机日志信息。
memory	指定 AP 发送设备状态信息，包括：CPU 信息、内存信息、普通日志信息（如端口 UP/DOWN 等信息）。
tech-support	指定 AP 收集并发送一键收集 console 信息
tech-package	指定 AP 收集并发送一键收集 package 信息

【缺省配置】 -

【命令模式】 AC 配置模式

【缺省级别】 15

【使用指导】 无

【配置举例】 名为 AP0001 的 MAC 地址为 8832.0000.1111

1：获取 AP0001 的死机日志信息，在 AC 文件系统中保存为 ap_8832.0000.1111_exception.log

```
Ruijie(config-ac)# tran-data-start AP0001 exception
```

2：获取 AP0001 的普通日志信息，在 AC 文件系统中保存为 ap_8832.0000.1111_syslog.log、ap_8832.0000.1111_memory.log、ap_8832.0000.1111_cpuinfo.log。

```
Ruijie(config-ac)# tran-data-start AP0001 memory
```

3：获取 AP0001 的一键收集 console 信息，在 AC 文件系统中保存为 ap_AP0001_8832.0000.1111_tech-console.log。

```
Ruijie(config-ac)# tran-data-start AP0001 tech-support
```

4：获取 AP0001 的一键收集 package 信息，在 AC 文件系统中保存为 ap_AP0001_8832.0000.1111_tech-package.tar.gz。

```
Ruijie(config-ac)# tran-data-start AP0001 tech-package
```

【检验方法】 1： 使用 **tran-data-show ap-name** 命令，查看从指定 AP 上获取的相关信息。tech-package 命令收集的文件需要通过 tftp 等方式传输到 PC 解压后再查看。

【提示信息】 -

【常见错误】 -

【平台说明】 仅 AC 支持该命令

3.46 wired-interface

对于我司具有有线网络接口的 AP（例如墙面式 RG-AP110-W 型号的 AP 在产品正面提供了以太网口用于有线网络用户接入），通过 wired-interface 命令可以配置关闭上述有线网络接口。缺省情况下，有线网络接口是开启的

wired-interface [**slot** *slot-id*] [**port** *port-id*] **enable**

关闭有线网络接口：

no wired-interface [**slot** *slot-id*] [**port** *port-id*] **enable**

恢复有线网络接口开启关闭默认配置：

default wired-interface [**slot** *slot-id*] [**port** *port-id*] **enable**

【参数说明】

参数	描述
slot	微 AP 接入的槽位
slot-id	槽位号，范围 1~24
port	设置有线网络接口。
port-id	指定有线网络接口，取值范围为 1~4。
enable	开启有线网络接口

【缺省配置】 缺省配置，有线网络接口开启。

【命令模式】 AP 配置模式/所有 AP 配置模式/AP 组配置模式

【缺省级别】 15

【使用指导】 1. 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。

2. 配置该命令不带 port 参数时，将设置所有有线网络接口配置相同。当配置四个 port 都关闭时，则配置显示不带 port 参数。slot 参数仅对智分+AP 有效，不指定 slot 参数时，对 24 个槽位的微 AP 应用相同的配置。

3. 瘦 AP 是零配置启机的，其配置从 AC 下发。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，如果配置了关闭有线口，则 AP 重启后有线口还是关闭的。

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。

【配置举例】 1：配置 AP1 关闭有线网络接口

```
Ruijie(config)# ap-config AP1

Ruijie(config-ap)# no wired-interface
```

【检验方法】 1：使用 **show ap-config running** 命令，可以查看配置是否成功。

【提示信息】 -

【常见错误】 -

【平台说明】 AC 支持该命令

3.47 wired-vlan

对于我司具有有线网络接口的 AP（例如墙面式 RG-AP110-W 型号的 AP 在产品正面提供了以太网口用于有线网络用户接入），通过 wired-vlan 命令可以配置上述有线网络接口使用的 VLAN。缺省情况下，有线网络接口使用的 VLAN 与 AP 相同

wired-vlan *vlan-id* [**slot** *slot-id*] [**port** *port-id*]**auto-save**

恢复默认值

no wired-vlan [*vlan-id* [**slot** *slot-id*] [**port** *port-id*]] **auto-save**

【参数说明】

参数	描述
vlan-id	配置有线网络接口使用的 VLAN。 *vlan-id*：指定的 VLAN，取值范围为 1~4094。
slot	微 AP 接入的槽位
slot-id	槽位号，范围 1~24
port	设置有线网络接口。
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

【缺省级别】 15

【使用指导】

1. 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。
2. 配置该命令不带 port 参数时，将设置所有有线网络接口为相同的 VLAN。当配置四个 port 属于相同 VLAN，则配置显示不带 port 参数。slot 参数仅对智分+AP 有效，不指定 slot 参数时，对 24 个槽位的微 AP 应用相同的配置。
3. 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。
4. 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。
5. 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。

⚠ 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。

【配置举例】 1：配置 AP1 的有线网络接口使用 VLAN 20

```
Ruijie(config)# ap-config AP1
Ruijie(config-ap)# wired-vlan 20
```

【检验方法】 1：使用 **show ap-config running** 命令，可以查看配置是否成功。

【提示信息】 -

【常见错误】 -

【平台说明】 AC 支持该命令

4 WBS

命令	作用
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
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
{802.11a | 802.11b} network {enable | disable}	配置 2.4GHZ 或 5GHZ 网络的开关情况
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 最大支持的 MCS
802.11ac mcs support	配置指定 AP 指定 radio 最大支持的 11AC 的 MCS
ampdu-retries	配置指定 AP 指定 radio 的 AMPDU 软件重传次数
ampdu-rts	配置指定 AP 指定 radio 开启 AMPDU 聚合报文的 RTS 保护
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
antenna receive	配置指定 AP 或指定 AP 组内的所有 AP 指定 radio 的天线接收类型
antenna transmit	配置指定 AP 或指定 AP 组内的所有 AP 指定 radio 的天线发送类型
apsd	配置指定 AP 指定 radio 是否启用 U-APSD 节电模式
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
autowifi	在空配置上一键配置 WLAN
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-width	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 支持的国家或地区代码集合或 AP Radio 使用的国家码
coverage-area-control	配置 AP 管理帧功率选择
ebag	一键配置电子书包网优
enable-radio	设置指定 AP 的 radio 或全部 radio 的使能状态为开启
eth-schd	配置 AP 以太网单次收包数
external-antenna enable	配置 AP 启用外置天线，并禁用内置天线
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
ldpc	配置指定 AP 指定 radio 支持低密度奇偶校验编码
link-check	配置链路完整性检测功能
linktest	显示无线用户链路信息
mcast-rate	配置 WLAN 的组播速率
mu-mimo enable	配置 radio 的多用户多入多出功能
peer-distance	配置指定 AP 指定 radio 与无线传输对端之间允许的最远距离
power local	配置指定 AP 或指定 AP 组内的所有 AP 指定 radio 发射功率
preamble	配置指定 AP 指定 radio 开启 short preamable 功能
radio-type	配置指定 AP 指定 radio 的工作频段
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
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
short-slot-time	配置指定 AP 使能短时隙功能
stbc	配置指定 AP 指定 radio 使能接收发送空时分组码
show ac-config {802.11a | 802.11b} summary	显示本 AC 的 802.11a 或 802.11b 网络中的 AP 列表
show antenna all	查看所有 AP 的天线馈线状态
show antenna single	查看指定 AP 的天线馈线状态
show ap-config radio	查看所有 AP 的 radio 信息
show ap-config radio config	查看指定 AP 指定 radio 的配置信息
show ap-config radio info	查看知道 AP 的 radio 一些特性配置状态
show ap-config radio radio-id **status**	查看 AP 指定 radio 的详细状态信息
show ap-config radio status	查看 AP 的 radio 列表
show client details	查看指定 MAC 用户信息
show smart bad radio	在 AC 上查看 ap5280 的坏卡情况
update-key-tsc enable	配置 AP 在进行 1X 重认证的时候更新加密 TSC

4.1 11asupport enable

配置指定 AP 指定 radio 在 5G 下支持 11A。

11asupport enable radio *radio-id*

配置指定 AP 指定 radio 在 5G 下不支持 11A。

no 11asupport enable radio *radio-id*

【参数说明】

参数	描述
radio-id	要配置的 radio 的 id，范围为 1~48

【缺省配置】 支持 11A

【命令模式】 AP 配置模式

【缺省级别】 14

【使用指导】 配置仅在 AP 的 Radio 工作在 5G 下生效。

【配置举例】 1：进入 AP0001 的配置模式，并且配置 Radio 1 在 5G 下支持 11A。

```
Ruijie(config)# ap-config AP0001
Ruijie(config-ap)# 11asupport enable radio 1
```

【检验方法】 1：使用 **show ap-config running** *ap-name* 命令，可以查看指定 AP 是否配置支持 11A。

【提示信息】 -

【常见错误】 -

【平台说明】 -

4.2 11bsupport enable

配置指定 AP 指定 radio 在 2.4G 下支持 11 B。
11bsupport enable radio *radio-id*

配置指定 AP 指定 radio 在 2.4G 下不支持 11 B。
no 11bsupport enable radio *radio-id*

【参数说明】

参数	描述
radio-id	要配置的 radio 的 id，范围为 1~48

【缺省配置】 支持 11B

【命令模式】 AP 配置模式

【缺省级别】 14

【使用指导】 配置仅在 AP 的 Radio 工作在 2.4G 下生效。

【配置举例】 1：进入 AP0001 的配置模式，并且配置 Radio 1 在 2.4G 下支持 11B。

```
Ruijie(config)# ap-config AP0001
Ruijie(config-ap)# 11bsupport enable radio 1
```

【检验方法】 1：使用 **show ap-config running** *ap-name* 命令，可以查看指定 AP 是否配置支持 11B。

【提示信息】 -

【常见错误】 -

【平台说明】 -

4.3 11gsupport enable

配置指定 AP 指定 radio 在 2.4G 下支持 11G。
11gsupport enable radio *radio-id*

配置指定 AP 指定 radio 在 2.4G 下不支持 11G。
no 11gsupport enable radio *radio-id*

【参数说明】

参数	描述
radio-id	要配置的 radio 的 id，范围为 1~48

【缺省配置】 支持 11G

【命令模式】 AP 配置模式

【缺省级别】 14

【使用指导】 配置仅在 AP 的 Radio 工作在 2.4G 下生效。

【配置举例】 1：进入 AP0001 的配置模式，并且配置 Radio 1 在 2.4G 下支持 11G。

```
Ruijie(config)# ap-config AP0001
Ruijie(config-ap)# 11gsupport enable radio 1
```

【检验方法】 1：使用 **show ap-config running** *ap-name* 命令，可以查看指定 AP 是否配置支持 11G。

【提示信息】 -

【常见错误】 -

【平台说明】 -

4.4 11nasupport enable

配置指定 AP 指定 radio 在 5G 下支持 11N。

11nasupport enable radio *radio-id*

配置指定 AP 指定 radio 在 5G 下不支持 11N。

no 11nasupport enable radio *radio-id*

【参数说明】

参数	描述
radio-id	要配置的 radio 的 id，范围为 1~48

【缺省配置】 支持 11N

【命令模式】 AP 配置模式

【缺省级别】 14

【使用指导】 配置仅在 AP 的 Radio 工作在 5G 下生效。

【配置举例】 1：进入 AP0001 的配置模式，并且配置 Radio 1 在 5G 下支持 11N。

```
Ruijie(config)# ap-config AP0001
Ruijie(config-ap)# 11nasupport enable radio 1
```

【检验方法】 1：使用 **show ap-config running** *ap-name* 命令，可以查看指定 AP 是否配置支持 11N。

【提示信息】 -

【常见错误】 -

【平台说明】 -

4.5 11ngsupport enable

配置指定 AP 指定 radio 在 2.4G 下支持 11N。

11ngsupport enable radio *radio-id*

配置指定 AP 指定 radio 在 2.4G 下不支持 11N。

no 11ngsupport enable radio *radio-id*

【参数说明】

参数	描述

	radio-id	要配置的 radio 的 id，范围为 1~48

【缺省配置】 支持 11N

【命令模式】 AP 配置模式

【缺省级别】 14

【使用指导】 配置仅在 AP 的 Radio 工作在 2.4G 下生效。

【配置举例】 1：进入 AP0001 的配置模式，并且配置 Radio 1 在 2.4G 下支持 11N。

```
Ruijie(config)# ap-config AP0001
Ruijie(config-ap)# 11ngsupport enable radio 1
```

【检验方法】 1：使用 **show ap-config running** *ap-name* 命令，可以查看指定 AP 是否配置支持 11N。

【提示信息】 -

【常见错误】 -

【平台说明】 -

4.6 11acsupport enable

配置指定 AP 指定 radio 支持 11AC。
11acsupport enable radio *radio-id*

配置指定 AP 指定 radio 不支持 11AC。
no 11acsupport enable radio *radio-id*

【参数说明】

参数	描述
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，Radio ID 为偶数的 Radio 支持 11AC

【命令模式】 AP 配置模式

【缺省级别】 14

【使用指导】 -

【配置举例】 1：进入 AP0001 的配置模式，并且配置 Radio 1 支持 11AC。

```
Ruijie(config)# ap-config AP0001
Ruijie(config-ap)# 11acsupport enable radio 1
```

【检验方法】 1：使用 **show ap-config running** *ap-name* 命令，可以查看指定 AP 是否配置支持 11AC。

【提示信息】 -

【常见错误】 -

【平台说明】 -

4.7 802.11a network rate

配置 802.11a 用户支持的速率集。

802.11a network rate { **6** | **9** | **12** | **18** | **24** | **36** | **48** | **54** } { **disabled** | **mandatory** | **supported** }

【参数说明】

参数	描述
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】 缺省情况下，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

【缺省级别】 14

【使用指导】 -

【配置举例】 1：802.11a 用户禁用 6Mbps 速率。

```
Ruijie(config)# ac-controller
```

```
Ruijie(config-ac)# 802.11a network rate 6 disabled
```

2：配置 AP0001 上的 802.11a 用户禁用 6Mbps 速率。

```
Ruijie(config)# ap-config AP001
Ruijie(config-ap)# 802.11a network rate 6 disabled
```

3：配置 default 组上的 802.11a 用户禁用 6Mbps 速率。

```
Ruijie(config)# ap-group default
Ruijie(config-group)# 802.11a network rate 6 disabled
```

【检验方法】 1：使用 **show running** 命令，可以查看该配置。

2： 使用 **show ap-config running** *ap-name* 命令，可以查看指定 AP 的配置。

【提示信息】 -

【常见错误】 -

【平台说明】 -

4.8 802.11b network rate

配置 802.11b 用户支持的速率集。

802.11b network rate { **1** | **2** | **5** | **11** } { **disabled** | **mandatory** | **supported** }

【参数说明】

参数	描述
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】 缺省情况下，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

【缺省级别】 14

【使用指导】 -

【配置举例】 1：802.11b 用户禁用 1Mbps 速率。

```
Ruijie(config)# ac-controller
Ruijie(config-ac)# 802.11b network rate 1 disabled
```

2：配置 AP0001 上的 802.11b 用户禁用 1Mbps 速率。

```
Ruijie(config)# ap-config AP001
Ruijie(config-ap)# 802.11b network rate 1 disabled
```

3：配置 default 组上的 802.11b 用户禁用 1Mbps 速率。

```
Ruijie(config)# ap-group default
Ruijie(config-group)# 802.11b network rate 1 disabled
```

【检验方法】 1：使用 **show running** 命令，可以查看该配置。

2： 使用 **show ap-config running** *ap-name* 命令，可以查看指定 AP 的配置。

【提示信息】 -

【常见错误】 -

【平台说明】 -

4.9 802.11g network rate

配置 802.11g 用户支持的速率集。

802.11g network rate { **1** | **2** | **5** | **6** | **9** | **11** | **12** | **18** | **24** | **36** | **48** | **54** } { **disabled** | **mandatory** | **supported** }

【参数说明】

参数	描述
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】 缺省情况下，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、AP 配置模式、AP 组配置模式

【缺省级别】 14

【使用指导】 -

【配置举例】 1：802.11g 用户禁用 1Mbps 速率。

```
Ruijie(config)# ac-controller
Ruijie(config-ac)# 802.11g network rate 1 disabled
```

2：配置 AP0001 上的 802.11g 用户禁用 1Mbps 速率。

```
Ruijie(config)# ap-config AP001
Ruijie(config-ap)# 802.11g network rate 1 disabled
```

3：配置 default 组上的 802.11g 用户禁用 1Mbps 速率。

```
Ruijie(config)# ap-group default
Ruijie(config-group)# 802.11g network rate 1 disabled
```

【检验方法】 1：使用 **show running** 命令，可以查看该配置。

2： 使用 **show ap-config running** *ap-name* 命令，可以查看指定 AP 的配置。

【提示信息】 -

【常见错误】 -

【平台说明】 -

4.10 {802.11a | 802.11b} network {enable | disable}

通过{ **802.11a** | **802.11b** } **network** { **disable** | **enable** }命令配置 2.4GHZ 或 5GHZ 网络的开关情况，配置 disable 将导致该无线网络中所有连接 2.4GHZ 或 5GHZ 网络的无线用户离线。

{ **802.11a** | **802.11b** } **network** { **enable** | **disable** }

【参数说明】

参数	描述
-	-

【缺省配置】 缺省情况为 enable

【命令模式】 AC 配置模式

【缺省级别】 14

【使用指导】 -

【配置举例】 1：配置 802.11a 网络 disable。

```
Ruijie(config)# ac-controller
Ruijie(config-ac)# 802.11a network disable
```

【检验方法】 1：使用 **show running** 命令，可以查看该配置。

【提示信息】 -

【常见错误】 -

【平台说明】 -

4.11 802.11n a-mpdu enable

配置指定 AP 指定 radio 支持 AMPDU。
802.11n a-mpdu enable radio *radio-id*

配置指定 AP 指定 radio 不支持 AMPDU。
no 802.11n a-mpdu enable radio *radio-id*

【参数说明】

参数	描述
radio-id	要配置的 radio 的 id，范围为 1~48

【缺省配置】 支持 AMPDU

【命令模式】 AP 配置模式

【缺省级别】 14

【使用指导】 配置仅在 AP 的 Radio 工作在 11N 模式或 11AC 模式下生效。

【配置举例】 1：进入 AP0001 的配置模式，并且配置 Radio 1 支持 AMPDU。

```
Ruijie(config)# ap-config AP0001
Ruijie(config-ap)# 802.11n a-mpdu enable radio 1
```

【检验方法】 1：使用 **show ap-config running** *ap-name* 命令，可以查看指定 AP 是否配置支持 AMPDU。

【提示信息】 -

【常见错误】 -

【平台说明】 -

4.12 802.11n mcs support

配置指定 AP 指定 radio 最大支持的 11N 的 MCS。
802.11n mcs support *num* **radio** *radio-id*

恢复指定 AP 指定 radio 最大支持的 11N 的 MCS。
no 802.11n mcs support radio *radio-id*

【参数说明】

参数	描述
num	MCS 开始序号，范围 0~31
radio-id	要配置的 radio 的 id，范围为 1~48

【缺省配置】 11N 的 mcs 最大支持缺省值为 31

【命令模式】 AP 配置模式

【缺省级别】 14

【使用指导】 配置仅在 AP 的 Radio 工作在 11N 模式或 11AC 模式下生效。

【配置举例】 1：进入 AP0001 的配置模式，并且配置 Radio 1 最大支持的 11N 的 MCS 为 15。

```
Ruijie(config)# ap-config AP0001
Ruijie(config-ap)# 802.11n mcs support 15 radio 1
```

【检验方法】 1：使用 **show ap-config running** *ap-name* 命令，可以查看指定 AP 是否配置最大支持的 11N 的 MCS。

【提示信息】 -

【常见错误】 -

【平台说明】 该命令对 AP220-E(M) v1.5/AP220-SH 产品不生效

4.13 802.11ac mcs support

配置指定 AP 指定 radio 最大支持的 11AC 的 MCS。
802.11ac mcs support *num* **radio** *radio-id*

恢复指定 AP 指定 radio 最大支持的 11AC 的 MCS。
no 802.11ac mcs support radio *radio-id*

【参数说明】

参数	描述
num	MCS 开始序号，范围 0~39
radio-id	要配置的 radio 的 id，范围为 1~48

【缺省配置】 11AC 的 mcs 最大支持缺省值为 39

【命令模式】 AP 配置模式

【缺省级别】 14

【使用指导】 配置仅在 AP 的 Radio 工作在 11AC 模式下生效。

【配置举例】 1：进入 AP0001 的配置模式，并且配置 Radio 1 最大支持的 11AC 的 MCS 为 19。

```
Ruijie(config)# ap-config AP0001
Ruijie(config-ap)# 802.11ac mcs support 19 radio 1
```

【检验方法】 1：使用 **show ap-config running** *ap-name* 命令，可以查看指定 AP 是否配置最大支持的 11AC 的 MCS。

【提示信息】 -

【常见错误】 -

【平台说明】 -

4.14 ampdu-retries

配置指定 AP 指定 radio 的 AMPDU 软件重传次数。

ampdu-retries *times* **radio** *radio-id*

【参数说明】

参数	描述
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】 AMPDU 软件重传次数为 10

【命令模式】 AP 配置模式

【缺省级别】 14

【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。

【配置举例】 1：进入 AP0001 的配置模式，并且配置 Radio 1 的 AMPDU 软件重传次数为 2。

```
Ruijie(config)# ap-config AP0001
Ruijie(config-ap)# ampdu-retries 2 radio 1
```

【检验方法】 1：使用 **show ap-config running** *ap-name* 命令，可以查看指定 AP 是否配置 AMPDU 软件重传次数。

【提示信息】 -

【常见错误】 -

【平台说明】 -

4.15 ampdu-rts

配置指定 AP 指定 radio 开启 AMPDU 聚合报文的 RTS 保护机制。
ampdu-rts radio {*radio-id* | *[802.11b* | *802.11a*]}

配置指定 AP 指定 radio 关闭 AMPDU 聚合报文的 RTS 保护机制。
no ampdu-rts radio {*radio-id* | *[802.11b* | *802.11a*]}

【参数说明】

参数	描述
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】 关闭

【命令模式】 AP 配置模式

【缺省级别】 14

【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。

【配置举例】 1：进入 AP0001 的配置模式，并且配置 Radio 1 开启 AMPDU 聚合报文的 RTS 保护机制。

```
Ruijie(config)# ap-config AP0001
Ruijie(config-ap)# ampdu-rts radio 1
```

【检验方法】 1：使用 **show ap-config running** *ap-name* 命令，可以查看指定 AP 是否配置开启 AMPDU 聚合报文的 RTS

保护机制。

【提示信息】 -

【常见错误】 -

【平台说明】 -

4.16 antdetect enable

开启馈线链路状态检测功能。
antdetect enable

关闭馈线链路状态检测功能。
no antdetect enable

【参数说明】

参数	描述
-	-

【缺省配置】 关闭馈线链路状态检测功能。

【命令模式】 AP 配置模式

【缺省级别】 14

【使用指导】 如果需要智分天线馈线链路检测功能，可以开启此命令。

如果对离线 AP 配置该命令，则在该离线 AP 上线后检查产品型号。如果不支持，则该配置命令将失效。

【配置举例】 1：以下的例子为示范配置，开启智分天线馈线链路检测功能。

```
Ruijie(config-ap)# antdetect enable
```

【检验方法】 1：使用 **show ap-config running** *ap-name* 命令，可以查看指定 AP 是否开启智分天线馈线链路检测功能。

【提示信息】 -

【常见错误】 1：对非 AP220-E(M) v3.0 产品配置该命令。

【平台说明】 该命令仅在 AP220-E(M) v3.0 上支持。

4.17 antdetect interval

配置馈线状态检测时间间隔，单位是分钟。
antdetect interval *interval*

恢复馈线状态检测时间间隔为默认值。
no antdetect interval

【参数说明】

参数	描述
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

【缺省级别】 14

【使用指导】 馈线状态检测时间间隔。

该命令仅在 AP220-E(M) v3.0 上支持。

【配置举例】 1：以下的例子为示范配置，1 分钟检测一次馈线状态。

```
Ruijie(config-ap)# antdetect enable
Ruijie(config-ap)# antdetect interval 1
```

【检验方法】 1：使用 **show ap-config running** *ap-name* 命令，可以查看指定 AP 馈线状态检测时间间隔配置。

【提示信息】 -

【常见错误】 1：配置馈线状态检测时间间隔，但未开启馈线链路状态检测功能。

【平台说明】 该命令仅在 AP220-E(M) v3.0 上支持。

4.18 antenna receive

配置指定 AP 或指定 AP 组内的所有 AP 指定 radio 的天线接收类型。
antenna receive *value* **radio** *radio-id*

【参数说明】

参数	描述
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

【缺省级别】 14

【使用指导】 配置仅在 AP 的 Radio 工作在 11N 模式或 11AC 模式下生效。

【配置举例】 1：进入 AP0001 的配置模式，并且配置 Radio 1 的接收天线设置为 5。

```
Ruijie(config)# ap-config AP0001
Ruijie(config-ap)# antenna receive 5 radio 1
```

2：进入 AP 组（default）的配置模式，并且配置 Radio 1 的接收天线设置为 5。

```
Ruijie(config)# ap-group default
Ruijie(config-group)# antenna receive 5 radio 1
```

【检验方法】 1：使用 **show ap-config running** *ap-name* 命令，可以查看指定 AP Radio 的接收天线配置。
2：使用 **show running-config** 命令，可以查看 AP 组 Radio 的接收天线配置。

【提示信息】 -

【常见错误】 -

【平台说明】 -

4.19 antenna transmit

配置指定 AP 或指定 AP 组内的所有 AP 指定 radio 的天线发送类型。
antenna transmit *value* **radio** *radio-id*

【参数说明】

参数	描述
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

【缺省级别】 14

【使用指导】 配置仅在 AP 的 Radio 工作在 11N 模式或 11AC 模式下生效。

【配置举例】 1：进入 AP0001 的配置模式，并且配置 Radio 1 的发送天线设置为 7。

```
Ruijie(config)# ap-config AP0001
Ruijie(config-ap)# antenna transmit 7 radio 1
```

2：进入 AP 组（default）的配置模式，并且配置 Radio 1 的发送天线设置为 7。

```
Ruijie(config)# ap-group default
Ruijie(config-group)# antenna transmit 7 radio 1
```

【检验方法】 1：使用 **show ap-config running** *ap-name* 命令，可以查看指定 AP Radio 的发送天线配置。
2：使用 **show running-config** 命令，可以查看 AP 组 Radio 的发送天线配置。

【提示信息】 -

【常见错误】 -

【平台说明】 -

4.20 apsd

配置指定 AP 指定 radio 是否启用 U-APSD 节电模式。
apsd { **enable** | **disable** } **radio** *radio-id*

【参数说明】

参数	描述
enable	启用 U-APSD 节电模式
disable	禁用 U-APSD 节电模式
radio-id	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

【缺省级别】 14

【使用指导】 不支持对所有 AP 进行配置。

【配置举例】 1：进入 AP0001 的配置模式，并且配置 Radio 1 启用 U-APSD 节电模式。

```
Ruijie(config)# ap-config AP0001
Ruijie(config-ap)#apsd enable radio 1
```

【检验方法】 1：使用 **show ap-config running** *ap-name* 命令，可以查看该命令配置。

【提示信息】 -

【常见错误】 -

【平台说明】 -

4.21 autowifi

在空配置上一键配置 WLAN。
autowifi

取消一键配置 WLAN。
no autowifi

【参数说明】

参数	描述
-	-

【缺省配置】 无

【命令模式】 AC 的全局配置模式

【缺省级别】 14

【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。

【配置举例】 1：进入 AC 的全局配置模式，并且一键配置 WLAN。

```
Ruijie(config)# autowifi
```

【检验方法】 1：使用 **show running** 命令，可以查看一键配置 WLAN。

【提示信息】 -

【常见错误】 -

【平台说明】 -

4.22 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。
assoc-rssi *rssi* **radio** *radio-id*

恢复指定 AP 指定 radio 的无线用户保持接入的最小信号强度为默认值。
no assoc-rssi radio *radio-id*

【参数说明】

参数	描述
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】 缺省情况下，为 0，即所有信号强度的无线用户都保持接入

【命令模式】 AP 配置模式

【缺省级别】 14

【使用指导】 一般应用于漫游粘滞场景。这时，建议 rssi 在 15 至 30 之间取值，小于 15 基本不会有效果。

【配置举例】 1：进入 AP0001 的配置模式，并且配置 Radio 1 的无线用户保持接入的最小信号强度为 15。

```
Ruijie(config)# ap-config AP0001
Ruijie(config-ap)# assoc-rssi 15 radio 1
```

【检验方法】 1：使用 **show ap-config running** *ap-name* 命令，可以查看指定 AP 该配置情况。

【提示信息】 -

【常见错误】 -

【平台说明】 -

4.23 beacon dtim-period

配置指定 AP 指定 radio 的 DTIM 周期。
beacon dtim-period *period-num* **radio** *radio-id*

【参数说明】

参数	描述
period-num	DTIM 的周期，表示 beacon 周期数，取值范围为：1~255
radio-id	要配置的 radio 的 id，范围为 1~48

【缺省配置】 DTIM 缺省配置为 1

【命令模式】 AP 配置模式

【缺省级别】 14

【使用指导】 不支持对所有 AP 进行配置。

【配置举例】 1：进入 AP0001 的配置模式，并且配置 Radio 1 的 DTIM 周期为 30 个 Beacon 周期。

```
Ruijie(config)# ap-config AP0001
Ruijie(config-ap)# beacon dtim-period 30 radio 1
```

【检验方法】 1：使用 **show ap-config running** *ap-name* 命令，可以查看该命令配置。

【提示信息】 -

【常见错误】 -

【平台说明】 -

4.24 beacon period

配置指定 AP 指定 radio 的 beacon 帧发送周期。

beacon period *milliseconds* **radio** *radio-id*

【参数说明】

参数	描述
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】 Beacon 周期缺省值为 100ms

【命令模式】 AP 配置模式

【缺省级别】 14

【使用指导】 不支持对所有 AP 进行配置。

【配置举例】 1：进入 AP0001 的配置模式，并且配置 Radio 1 的 beacon 发送周期为 200ms。

```
Ruijie(config)# ap-config AP0001
Ruijie(config-ap)# beacon period 200 radio 1
```

【检验方法】 1：使用 **show ap-config running** *ap-name* 命令，可以查看指定 AP 是否配置 beacon 帧发送周期。

【提示信息】 -

【常见错误】 -

【平台说明】 -

4.25 beacon rate

配置指定 AP 指定 radio 的 beacon 帧发送速率。

beacon rate *rate-Mbps* **radio** {*radio-id* | [*802.11b* | *802.11a*]}

恢复指定 AP 指定 radio 的 beacon 帧发送速率为默认发送速率。

no beacon rate radio {*radio-id* | [*802.11b* | *802.11a*]}

【参数说明】

参数	描述
rate_Mbps	beacon 帧发送速率，需要注意的是： 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；
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】 缺省不配置当前命令

【命令模式】 AP 配置模式

【缺省级别】 14

【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。

【配置举例】 1：进入 AP0001 的配置模式，并且配置 Radio 1 的 beacon 发送速率为 12Mbps。

```
Ruijie(config)# ap-config AP0001
Ruijie(config-ap)# beacon rate 12.0 radio 1
```

【检验方法】 1：使用 **show ap-config running** *ap-name* 命令，可以查看指定 AP 是否配置 beacon 帧发送速率。

【提示信息】 -

【常见错误】 -

【平台说明】 -

4.26 chan-width

配置指定 AP 指定 radio 的带宽。

chan-width { **20** | **40** | **80|160** } **radio** {*radio-id* | *[802.11b* | *802.11a*]}

【参数说明】

参数	描述
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】 缺省为 20M

【命令模式】 AP 配置模式

【缺省级别】 14

【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。

【配置举例】 1：进入 AP0001 的配置模式，并且配置 Radio 1 带宽为 40M。

```
Ruijie(config)# ap-config AP0001
Ruijie(config-ap)# chan-width 40 radio 1
```

【检验方法】 1：使用 **show ap-config running** *ap-name* 命令，可以查看指定 AP 该配置信息。

【提示信息】 -

【常见错误】 -

【平台说明】 -

4.27 channel

配置指定 AP 指定 radio 的信道。
channel { **global** | *channel-id* } **radio** *radio-id*

【参数说明】

参数	描述
global	配置指定 AP 指定 radio 由 RRM 自动调整信道
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】 缺省情况下，由 RRM 自动调整信道

【命令模式】 AP 配置模式

【缺省级别】 14

【使用指导】 不支持对所有 AP 进行配置。

【配置举例】 1：进入 AP0001 的配置模式，并且配置 Radio 1 工作信道为 6。

```
Ruijie(config)# ap-config AP0001
Ruijie(config-ap)# channel 6 radio 1
```

【检验方法】 1：使用 **show ap-config running** *ap-name* 命令，可以查看指定 AP 该配置信息。

【提示信息】 -

【常见错误】 -

【平台说明】 -

4.28 country

用户可以通过 **country** 命令给指定 AC 支持的国家或地区代码集合。
country *country-code*

用户可以通过 **country** 命令删除 AC 支持的国家或地区代码。
no country *country-code*

配置指定 AP 指定 radio 使用的国家或地区代码。
country *country-code* **radio** {*radio-id* | [*802.11b* | *802.11a*]}

【参数说明】

参数	描述
country-code	国家或地区代码
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】 缺省情况下，AC 支持的国家或地区代码为“CN”，AP 使用的国家或地区代码为“CN”

【命令模式】 AC 配置模式、AP 配置模式

【缺省级别】 14

【使用指导】

1. AC 支持的国家或地区代码“CN”不允许删除。
2. 不支持对所有 AP 进行配置。
3. 当前支持的国家或地区代码有： “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，在配置国家或地区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 可支持的国家或地区代码集合。如果配置该 AP 所使用的国家或地区代码发生变化，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。

【配置举例】 1：配置 AC 支持的国家或地区代码为 US，配置 AP0001 的 radio 1 国家或地区代码为 US。

```
Ruijie(config)# ac-controller
Ruijie(config-ac)# country US
Ruijie(config-ac)# exit
Ruijie(config)# ap-config AP0001
Ruijie(config-ap)# country US radio 1
```

【检验方法】 1：使用 **show running** 命令，可以查看 AC 支持的国家码配置。
2：使用 **show ap-config running** *ap-name* 命令，可以查看指定 AP 是否配置国家码。

【提示信息】 -

【常见错误】 1：未配置 AC 支持的国家码，直接配置 AP Radio 使用该国家码。

```
Ruijie(config-ap)#country JP radio 1
The Country-code(JP) is invalid, please check.
```

【平台说明】 -

4.29 coverage-area-control

配置 AP 管理帧功率选择。
coverage-area-control *power*

恢复 AP 管理帧功率选择。
no coverage-area-control

【参数说明】

参数	描述
power	管理帧功率，单位：dbm，范围 0~32

【缺省配置】 0

【命令模式】 AP 配置模式、AP 组配置模式

【缺省级别】 14

【使用指导】 -

【配置举例】 1：进入 AP0001 的配置模式，并且配置 AP 管理帧功率为 20。

```
Ruijie(config)# ap-config AP0001
Ruijie(config-ap)# coverage-area-control 20
```

2：进入 AP 组(default)的配置模式，并且配置 AP 管理帧功率为 20。

```
Ruijie(config)# ap-group default
Ruijie(config-group)# coverage-area-control 20
```

【检验方法】 1：使用 **show ap-config running** *ap-name* 命令，可以查看指定 AP 是否配置管理帧功率选择。
1：使用 **show running-config** 命令，可以查看 AP 组管理帧功率配置。

【提示信息】 -

【常见错误】 -

【平台说明】 以下产品不支持该命令配置：AP220-I V1.X, AP220-SI V1.X, AP220-E V2.X, AP220-E V3.X, AP220-E(M) V2.X, AP220-SH V2.X, AP220-SH V3.X, AP620-H(C) V2.X, AP530-I V1.0。

4.30 ebag

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。提供一键电子书包网优命令，来实现快速配置。

ebag

取消一键配置电子书包网优。
no ebag

【参数说明】

参数	描述
-	-

【缺省配置】 无

【命令模式】 AP 配置模式

【缺省级别】 14

【使用指导】 一般用于电子书包场景中，其他场景慎用！

【配置举例】 1：进入 AP0001 的配置模式，并且配置一键电子书包网优。

```
Ruijie(config)# ap-config AP0001
Ruijie(config-ap)# ebag
```

【检验方法】 1：使用 **show ap-config running** *ap-name* 命令，可以查看指定 AP 是否配置一键电子书包网优。

【提示信息】 -

【常见错误】 -

【平台说明】 -

4.31 enable-radio

设置指定 AP 的 radio 或全部 radio 的使能状态为开启。
enable-radio { *radio-id* | **all** }

设置指定 AP 的 radio 或全部 radio 的使能状态为关闭。
no enable-radio { *radio-id* | **all** }

【参数说明】

参数	描述
radio-id	要配置的 radio 的 id，范围为 1~48
all	指所有 radio

【缺省配置】 缺省情况下，所有 AP 的所有 radio 都是使能开启的。

【命令模式】 AP 配置模式

【缺省级别】 14

【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。

【配置举例】 1：进入 AP0001 的配置模式，并且配置 Radio 1 状态为关闭。

```
Ruijie(config)# ap-config AP0001
Ruijie(config-ap)# no enable-radio 1
```

【检验方法】 1：使用 **show ap-config running** *ap-name* 命令，可以查看指定 AP Radio 使能配置。

【提示信息】 -

【常见错误】 -

【平台说明】 -

4.32 eth-schd

配置 AP 以太网单次收包数。
eth-schd *limit*

恢复 AP 以太网单次收包数。
no eth-schd

【参数说明】

参数	描述
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

【缺省级别】 14

【使用指导】 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。

【配置举例】 1：进入 AP0001 的配置模式，并且配置 AP 以太网单次收包数为 50。

```
Ruijie(config)# ap-config AP0001
Ruijie(config-ap)# eth-schd 50
```

【检验方法】 1：使用 **show ap-config running** *ap-name* 命令，可以查看指定 AP 是否配置以太网单次收包数。

【提示信息】 -

【常见错误】 -

【平台说明】 -

4.33 external-antenna enable

配置指定 AP 指定 radio 启用外置天线，并禁用内置天线。
external-antenna enable radio *radio-id*

恢复指定 AP 指定 radio 启用内置天线，并禁用外置天线。
no external-antenna enable radio *radio-id*

【参数说明】

参数	描述
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

【缺省级别】 14

【使用指导】 -

【配置举例】 1：进入 AP0001 的配置模式，并且配置 Radio 1 启用外置天线，并禁用内置天线。

```
Ruijie(config)# ap-config AP0001
Ruijie(config-ap)# external-antenna enable radio 1
```

【检验方法】 1：使用 **show ap-config running** *ap-name* 命令，可以查看指定 AP Radio 是否配置启用外置天线，并禁用内置天线。

【提示信息】 -

【常见错误】 -

【平台说明】 -

4.34 fragment-threshold

配置指定 AP 指定 radio 的分片阈值。
fragment-threshold *value* **radio** *radio-id*

恢复指定 AP 指定 radio 的分片阈值为默认值。
no fragment-threshold radio *radio-id*

【参数说明】

参数	描述
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】 缺省情况下分片阈值为 2346

【命令模式】 AP 配置模式

【缺省级别】 14

【使用指导】 不支持对所有 AP 进行配置。

【配置举例】 1：进入 AP0001 的配置模式，并且配置 Radio 1 的分片阈值为 1538。

```
Ruijie(config)# ap-config AP0001
Ruijie(config-ap)# fragment-threshold 1538  radio 1
```

【检验方法】 1：使用 **show ap-config running** *ap-name* 命令，可以查看指定 AP 分片阈值配置。

【提示信息】 -

【常见错误】 -

【平台说明】 -

4.35 green-field enable

配置指定 AP 指定 radio 的保护模式。
green-field enable radio *radio-id*

恢复指定 AP 指定 radio 的保护模式为 disable。

no green-field enable radio *radio-id*

【参数说明】

参数	描述
radio-id	要配置的 radio 的 id，范围为 1~48

【缺省配置】 缺省情况下为 disable

【命令模式】 AP 配置模式

【缺省级别】 14

【使用指导】 仅支持 2.4G Radio

【配置举例】 1：进入 AP0001 的配置模式，并且配置 Radio 1 的 green-field 保护模式。

```
Ruijie(config)# ap-config AP0001
Ruijie(config-ap)# green-field enable radio 1
```

【检验方法】 1：使用 **show ap-config running** *ap-name* 命令，可以查看指定 AP Radio 的 green-field 配置。

【提示信息】 -

【常见错误】 -

【平台说明】 -

4.36 ldpc

配置指定 AP 指定 radio 支持低密度奇偶校验编码。

ldpc radio *radio-id*

配置指定 AP 指定 radio 不支持低密度奇偶校验编码。

no ldpc radio *radio-id*

【参数说明】

参数	描述
radio-id	要配置的 radio 的 id，范围为 1~48

【缺省配置】 支持

【命令模式】 AP 配置模式

【缺省级别】 14

【使用指导】 -

【配置举例】 1：进入 AP0001 的配置模式，并且配置 Radio 1 支持低密度奇偶校验编码。

```
Ruijie(config)# ap-config AP0001
Ruijie(config-ap)# ldpc radio 1
```

【检验方法】 1：使用 **show ap-config running** *ap-name* 命令，可以查看指定 AP 是否配置支持低密度奇偶校验编码。

【提示信息】 -

【常见错误】 -

【平台说明】 -

4.37 link-check

打开或关闭链路完整性检测功能。

link-check { **enable** | **disable** }

打开或关闭链路完整性检测功能。

no link-check { **enable** | **disable** }

【参数说明】

参数	描述
no	反操作

【缺省配置】 关闭

【命令模式】 全局配置模式

【缺省级别】 14

【使用指导】 -

【配置举例】 1：打开链路完整性检测功能。

```
Ruijie(config)# link-check enable
```

2：关闭链路完整性检测功能。

```
Ruijie(config)# link-check disable
```

或者

```
Ruijie(config)# no link-check enable
```

【检验方法】 1：使用 **show running-config** 命令，可以查看链路完整性检测功能的开启情况。

【提示信息】 -

【常见错误】 -

【平台说明】 -

4.38 linktest

显示无线用户链路信息。

linktest *H.H.H*

【参数说明】

参数	描述
H.H.H	Client 的 MAC 地址

【命令模式】 特权模式

【缺省级别】 1

【使用指导】 -

【配置举例】 1：显示无线用户（MAC 地址：cca2.2352.768d）链路信息

```
Ruijie# linktest cca2.2352.768d
Link test station(cca2.2352.768d):
    Signal strength in the form of RSSI :           55
    Signal quality in the form of SNR:              -37
    Total number of packets that are retried:       9
    Maximum retry count for a single packet:        16
    Number of lost packets:                         0
    Data rate of a successfully transmitted packet: 0
```

字段解释：

字段	说明
Signal strength in the form of RSSI	以接收信号强度指示的形式表示的信号强度
Signal quality in the form of SNR	以信噪比的形式表示的信号质量
Total number of packets that are retried	重传帧总数
Maximum retry count for a single packet	单个报文最大重传次数
Number of lost packets	总丢包数
Data rate of a successfully transmitted packet	成功传输报文的速率

【提示信息】 -

【平台说明】 -

4.39 mcast-rate

配置 WLAN 的组播速率。
mcast-rate *mcast-num*

恢复 WLAN 的组播速率为默认值。
no mcast-rate

【参数说明】

参数	描述
mcast-num	WLAN 组播速率，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】 WLAN 默认组播速率为 24Mbps

【命令模式】 WLAN 配置模式

【缺省级别】 14

【使用指导】 -

【配置举例】 1：进入 WLAN 2048 的配置模式，并且配置组播速率为 11Mbps。

```
Ruijie(config)# wlan-config 2048
Ruijie(config-wlan)# mcast-rate 11
```

【检验方法】 1：使用 **show running-config** 命令，可以查看组播速率配置。

【提示信息】 -

【常见错误】 -

【平台说明】 -

4.40 mu-mimo enable

配置指定 radio 开启 MU-MIMO 功能。

mu-mimo enable radio *radio-id*

配置指定 radio 关闭 MU-MIMO 功能。
no mu-mimo enable radio *radio-id*

恢复指定 radio 的 MU-MIMO 功能。
default mu-mimo enable radio *radio-id*

【参数说明】

参数	描述
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

【缺省级别】 14

【使用指导】 -

【配置举例】 1：进入 AP0001 的配置模式，并且配置 Radio 1 开启 MU-MIMO。

```
Ruijie(config)# ap-config AP0001
Ruijie(config-ap)# mu-mimo enable radio 1
```

2：进入 AP0001 的配置模式，并且配置 Radio 2 关闭 MU-MIMO。

```
Ruijie(config)# ap-config AP0001
```

```
Ruijie(config-ap)# no mu-mimo enable radio 2
```

3：进入 AP0001 的配置模式，恢复 Radio 3 默认 MU-MIMO。

```
Ruijie(config)# ap-config AP0001
```

```
Ruijie(config-ap)# default mu-mimo enable radio 3
```

4：进入 AP all 的配置模式，配置 Radio 1 开启 MU-MIMO。

```
Ruijie(config)# ap-config all
```

```
Ruijie(config-ap)# mu-mimo enable radio 1
```

4：进入 AP 默认 default 的配置模式，配置 Radio 1 开启 MU-MIMO。

```
Ruijie(config)# ap-group default
Ruijie(config-group)# mu-mimo enable radio 1
```

【检验方法】 1：使用 **show ap-config running** *ap-name* 命令，可以查看指定 AP Radio 的 MU-MIMO 配置。

2：使用 **show running-config** 命令，可以查看 AP 组 Radio 的 MU-MIMO 配置。

【提示信息】 -

【常见错误】 -

【平台说明】 -

4.41 peer-distance

配置指定 AP 指定 radio 与无线传输对端之间允许的最远距离。

peer-distance *val* **radio** *radio-id*

【参数说明】

参数	描述
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】 缺省情况下，1000m

【命令模式】 AP 配置模式

【缺省级别】 14

【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。

【配置举例】 1：进入 AP0001 的配置模式，并且配置 Radio 1 与无线传输对端之间允许的最远距离为 3000m。

```
Ruijie(config)# ap-config AP0001
Ruijie(config-ap)# peer-distance 3000 radio 1
```

【检验方法】 1：使用 **show ap-config running** *ap-name* 命令，可以查看指定 AP Radio 与无线传输对端之间允许的最远距离配置。

【提示信息】 -

【常见错误】 -

【平台说明】 -

4.42 power local

配置指定 AP 或指定 AP 组内的所有 AP 指定 radio 发射功率。

power local { **global** | *power* } **radio** {*radio-id* | [*802.11b* | *802.11a*]}

【参数说明】

参数	描述
global	配置指定 AP 或指定 AP 组内所有 AP 指定 radio 由 RRM 自动调整发射功率
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】 缺省情况下，由 RRM 自动调整发射功率

【命令模式】 AP 配置模式或 AP 组配置模式

【缺省级别】 14

【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。

【配置举例】 1：进入 AP0001 的配置模式，并且配置 Radio 1 发射功率为最大功率的 50%。

```
Ruijie(config)# ap-config AP0001
Ruijie(config-ap)# power local 50 radio 1
```

2：进入 AP 组（default）的配置模式，并且配置 Radio 1 发射功率为最大功率的 50%。

```
Ruijie(config)# ap-group default
Ruijie(config-group)# power local 50 radio 1
```

【检验方法】 1：使用 **show ap-config running** *ap-name* 命令，可以查看指定 AP Radio 发射功率配置。

2：使用 **show running-config** 命令，可以查看 AP 组 Radio 发射功率配置。

【提示信息】 -

【常见错误】 -

【平台说明】 -

4.43 preamble

配置指定 AP 指定 radio 的 preamable 属性。

preamble { **long** | **short** } **radio** *radio-id*

【参数说明】

参数	描述
radio-id	要配置的 radio 的 id，范围为 1~48
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

【缺省配置】 缺省情况下，为 short，即使用短前导码

【命令模式】 AP 配置模式

【缺省级别】 14

【使用指导】 不支持对所有 AP 进行配置。

【配置举例】 1：进入 AP0001 的配置模式，并且配置 Radio 1 关闭 short preamable 功能。

```
Ruijie(config)# ap-config AP0001
Ruijie(config-ap)# preamble long radio 1
```

【检验方法】 1：使用 **show ap-config running** *ap-name* 命令，可以查看指定 AP Radio 的 short preamable 配置。

【提示信息】 -

【常见错误】 -

【平台说明】 -

4.44 radio-type

配置指定 AP 指定 radio 的工作频段。

radio-type *radio-id* { **802.11a** | **802.11b** }

【参数说明】

参数	描述
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】 缺省情况下 ,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

【缺省级别】 14

【使用指导】 不支持对所有 AP 进行配置。

【配置举例】 1：进入 AP0001 的配置模式，并且配置 Radio 1 工作在 2.4G 频段。

```
Ruijie(config)# ap-config AP0001
Ruijie(config-ap)# radio-type 1 802.11a
```

【检验方法】 1：使用 **show ap-config running** *ap-name* 命令，可以查看指定 AP Radio 的工作频段配置。

【提示信息】 -

【常见错误】 -

【平台说明】 -

4.45 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。
response-rssi *rssi* **radio** {*radio-id* | [*802.11b* | *802.11a*]}

恢复指定 AP 指定 radio 允许接入无线用户的最小信号强度为默认值。
no response-rssi radio {*radio-id* | [*802.11b* | *802.11a*]}

【参数说明】

参数	描述
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】 缺省情况下，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

【缺省级别】 14

【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。

【配置举例】 1：进入 AP0001 的配置模式，并且配置 Radio 1 允许接入无线用户的最小信号强度为 20。

```
Ruijie(config)# ap-config AP0001
Ruijie(config-ap)# response-rssi 20 radio 1
```

【检验方法】 1：使用 **show ap-config running** *ap-name* 命令，可以查看指定 AP 该配置情况。

【提示信息】 -

【常见错误】 -

【平台说明】 -

4.46 rts-threshold

配置指定 AP 指定 radio 的 RTS 阈值。
rts-threshold *value* **radio** *radio-id*

恢复指定 AP 指定 radio 的 RTS 阈值为默认值。
no rts-threshold radio *radio-id*

【参数说明】

参数	描述
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】 缺省情况下，为 2347

【命令模式】 AP 配置模式

【缺省级别】 14

【使用指导】 -

【配置举例】 1：进入 AP0001 的配置模式，并且配置 Radio 1 的 RTS 阈值为 1539。

```
Ruijie(config)# ap-config AP0001
Ruijie(config-ap)# rts-threshold 1539 radio 1
```

【检验方法】 1：使用 **show ap-config running** *ap-name* 命令，可以查看指定 AP Radio 的 RTS 阈值配置。

【提示信息】 -

【常见错误】 -

【平台说明】 -

4.47 short-gi

配置指定 AP 指定 radio 支持 short-gi。
short-gi enable radio *radio-id* **chan-width** { **20** | **40** | **80|160** }

配置指定 AP 指定 radio 不支持 short-gi。
no short-gi enable radio *radio-id* **chan-width** { **20** | **40** | **80|160** }

【参数说明】

参数	描述
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】 缺省情况下，20M、40M、80M、160M 带宽都使能

【命令模式】 AP 配置模式

【缺省级别】 14

【使用指导】 -

【配置举例】 1：进入 AP0001 的配置模式，并且配置 Radio 1 支持 20M 带宽的 short-gi。

```
Ruijie(config)# ap-config AP0001
Ruijie(config-ap)# short-gi enable radio 1 chan-width 20
```

2：进入 AP0001 的配置模式，并且配置 Radio 2 不支持 40M 带宽的 short-gi。

```
Ruijie(config)# ap-config AP0001
Ruijie(config-ap)# no short-gi enable radio 2 chan-width 40
```

【检验方法】 1：使用 **show ap-config running** *ap-name* 命令，可以查看指定 AP Radio 的 short-gi 配置。

【提示信息】 -

【常见错误】 -

【平台说明】 -

4.48 short-slot-time

配置指定 AP 使能短时隙功能。
short-slot-time radio *radio-id*

配置指定 AP 禁用短时隙功能。
no short-slot-time radio *radio-id*

【参数说明】

参数	描述
radio-id	要配置的 radio 的 id，范围为 1~48

【缺省配置】 缺省情况下，为 enable

【命令模式】 AP 配置模式

【缺省级别】 14

【使用指导】 long slot time 在 AP 的 Radio 工作在 5G 下不生效。

【配置举例】 1：进入 AP0001 的配置模式，并且配置 Radio 1 支持 short slot time 功能。

```
Ruijie(config)# ap-config AP0001
Ruijie(config-ap)# short-slot-time radio 1
```

【检验方法】 1：使用 **show ap-config running** *ap-name* 命令，可以查看指定 AP Radio 的 short-slot-time 配置。

【提示信息】 -

【常见错误】 -

【平台说明】 -

4.49 stbc

配置指定 AP 指定 radio 使能接收发送空时分组码。

stbc radio *radio-id*

配置指定 AP 指定 radio 禁止接收发送空时分组码。
no stbc radio *radio-id*

【参数说明】

参数	描述
radio-id	要配置的 radio 的 id，范围为 1~48

【缺省配置】 使能

【命令模式】 AP 配置模式

【缺省级别】 14

【使用指导】 -

【配置举例】 1：进入 AP0001 的配置模式，并且配置 Radio 1 使能接收发送空时分组码。

```
Ruijie(config)# ap-config AP0001
Ruijie(config-ap)# stbc radio 1
```

【检验方法】 1：使用 **show ap-config running** *ap-name* 命令，可以查看指定 AP 是否配置使能接收发送空时分组码。

【提示信息】 -

【常见错误】 -

【平台说明】 -

4.50 show ac-config {802.11a | 802.11b} summary

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**

【参数说明】

参数	描述
-	-

【命令模式】 特权模式

【缺省级别】 1

【使用指导】 -

【配置举例】 1：显示本 AC 的 802.11a 网络中的 AP 列表

```
Ruijie#show ac-config 802.11a summary
Index  Ap name                                slot id  Radio Base MAC  state    load(%)
noise(dBm) interfere(%)
------ -------------------------------------- -------- --------------- -------- --------
---------- ---------------
1      ap320v1.0                              2        0000.0000.0000  Enable   0        -110
0
2      00d0.fb88.7812                         2        00d0.fb88.7815  Enable   0        -110
0
```

字段解释：

字段	说明
Index	序号
Ap name	AP 名字
slot id	radio id
Radio Base MAC	radio MAC 地址
state	使能/禁止状态
load(%)	信道负载
noise(dBm)	基底噪声
interfere(%)	同频干扰

【提示信息】 -

【平台说明】 -

4.51 show antenna all

显示所有 AP 的天线馈线状态。

show antenna all

【参数说明】

参数	描述
-	-

【命令模式】 特权模式

【缺省级别】 1

【使用指导】 使用该命令可以查看设备上所有关联 AP 的馈线状态。

【配置举例】 1：查看所有 AP 的天线馈线状态

```
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
-------------------------------------------------------------   -------   -------   -------
-------   -------   -------
APD-M4                                                            - N N -   - N Y -   - N N -   -
N N -   - - - -   - - - -
```

字段解释：

字段	说明
ap	AP 名字

【提示信息】 -

【平台说明】 -

4.52 show antenna single

显示指定 AP 的天线馈线状态。

show antenna single *ap-name*

【参数说明】

参数	描述
ap-name	指定待查询 AP 名字

【命令模式】 特权模式

【缺省级别】 1

【使用指导】 使用该命令可以查看指定关联 AP 名字的馈线状态。

【配置举例】 1：查看指定 AP 的天线馈线状态

```
Ruijie# show antenna single APD-M4
ap[APD-M4] antenna state
R1-1: N
R1-2: N
R2-1: N
R2-2: N
R3-1: N
R3-2: N
```

```
R4-1: N
R4-2: N
```

【提示信息】 -

【平台说明】 -

4.53 show ap-config radio

查看所有 AP 的 radio 信息。

show ap-config radio

【参数说明】

参数	描述
-	-

【命令模式】 特权模式

【缺省级别】 1

【使用指导】 -

【配置举例】 1：查看所有 AP 的 radio 信息

```
Ruijie#show ap-config radio
Show all AP radios:
AP Name                                 MAC Address         Radio MAC          Radio MAC
---------------------------------------- ------------------- -------------------
-------------------
AP0001                                  N/A                 N/A                 N/A
```

字段解释：

字段	说明
AP Name	AP 名字
MAC Address	AP MAC 地址
Radio MAC	Radio ID 为奇数的 Radio MAC 地址
Radio MAC	Radio ID 为偶数的 Radio MAC 地址

【提示信息】 -

【平台说明】 -

4.54 show ap-config radio ap-name

查看所有 AP 的 radio 信息。

show ap-config radio ap-name *ap-name*

【参数说明】

参数	描述
ap-name	指定待查询 AP 名字

【命令模式】 特权模式

【缺省级别】 1

【使用指导】 -

【配置举例】 1：查看所有 AP 的 radio 信息

```
Ruijie#show ap-config radio ap-name
Radio ID Radio Type   STA NUM  Channel  Power  Radio Base MAC  Status
-------- ------------ -------- -------- ------ --------------- -------
1        802.11b/g/n  10       6*        100    000c.3067.fbd7  Enable
2        802.11a/n/ac  0       149*      100    000c.3067.fbd8  Disable
```

字段解释：

字段	说明
Radio ID	射频接口 ID
Radio Type	工作频段
STA NUM	STA 个数
Channel	信道
Power	功率
Radio Base MAC	射频口的 mac 地址
Status	射频口状态

【提示信息】 -

【平台说明】 -

4.55 show ap-config radio config

查看指定 AP 指定 radio 的配置信息。

show ap-config radio *radio-id* **config** *ap-name*

【参数说明】

参数	描述
radio-id	要配置的 radio 的 id，范围为 1~48
ap-name	指定待查询 AP 名字

【命令模式】 特权模式

【缺省级别】 1

【使用指导】 -

【配置举例】 1：查看指定 AP 指定 radio 的配置信息

```
Ruijie# show ap-config radio 1 config 220em
Admin State.............................. Enable
Current Tx Power......................... Global
Num of BSSIDs............................ 1
DTIM Period.............................. 1
Beacon Period(milliseconds)............... 100
Country Code............................. CN
Current Channel.......................... Global
```

字段解释：

字段	说明
Admin State	Radio 使能状态
Current Tx Power	当前发射功率
Num of BSSIDs	BSSID 个数
DTIM Period	DTIM 周期
Beacon Period	Beacon 周期
Country Code	国家码
Current Channel	使用信道

【提示信息】 -

【平台说明】 -

4.56 show ap-config radio info

查看指定 AP 的 radio 信息。

show ap-config radio info *ap-name*

【参数说明】

参数	描述
ap-name	指定待查询 AP 名字

【命令模式】 特权模式

【缺省级别】 1

【使用指导】 -

【配置举例】 1：查看所有 AP 的 radio 信息

```
Ruijie#show ap-config radio info ap-name
Radio ID Radio Type   MU-MIMO    Radio Base MAC  Status
-------- ------------ ---------- --------------- -------
1        802.11b/g/n  Nonsupport 000c.3067.fbd7  Enable
2        802.11a/n/ac Enable     000c.3067.fbd8  Disable
```

字段解释：

字段	说明
Radio ID	射频接口 ID
Radio Type	工作频段
MU-MIMO	射频口的多用户多入多出配置情况
Radio Base MAC	射频口的 mac 地址
Status	射频口状态

【提示信息】 -

【平台说明】 -

4.57 show ap-config radio *radio-id* status

查看 AP 指定 radio 的详细状态信息。

show ap-config radio *radio-id* **status** *ap-name*

【参数说明】

参数	描述
radio-id	要配置的 radio 的 id，范围为 1~48
ap-name	指定待查询 AP 名字

【命令模式】 特权模式

【缺省级别】 1

【使用指导】 -

【配置举例】 1：查看 AP 指定 radio 的详细状态信息

```
Ruijie# show ap-config radio 1 s 220em
Admin State.............................. Enable
Oper State............................... Normal
WTP Radio Statistics
 Last Fail Type.......................... Statistic Not Supported
 Reset Count............................. 0
 SW Failure Count........................ 0
 HW Failure Count........................ 0
 Other Failure Count..................... 0
 Unknown Failure Count................... 0
 Config Update Count..................... 0
 Channel Change Count.................... 2
 Band Change Count....................... 197
 Current Noise Floor..................... -102
Assigned WTP BSSID
 WLAN ID................................. 0
 MAC Address............................. 0000.0000.0000
MIC Countermeasures
 WLAN ID................................. 0
 MAC Address............................. 0000.0000.0000
RSNA Error Report From Station
 Client MAC Address...................... 0000.0000.0000
 Radio Base MAC.......................... 0000.0000.0000
 Radio ID................................ 1
 WLAN ID................................. 0
 TKIP ICV Errors......................... 0
 TKIP Local MIC Failures................. 0
 TKIP Remote MIC Failures................ 0
 CCMP Replays............................ 0
 CCMP Decrypt Errors..................... 0
 TKIP Replays............................ 0
Statistics
 Tx Fragment Count....................... 0
 Multicast Tx Count...................... 0
 Failed Count............................ 0
 Retry Count............................. 0
 Multiple Retry Count.................... 0
 Frame Duplicate Count................... 0
 RTS Success Count....................... 0
```

```
 RTS Failure Count..................... 0
 ACK Failure Count..................... 0
 Rx Fragment Count..................... 0
 Multicast RX Count.................... 0
 FCS Error Count....................... 0
 Tx Frame Count ....................... 0
 Decryption Errors..................... 0
 Discarded QoS Fragment Count.......... 0
 Associated Station Count.............. 0
 QoS CF Polls Received Count........... 0
 QoS CF Polls Unused Count............. 0
 QoS CF Polls Unusable Count........... 0
Current Tx Power...................... 100
Current Tx Power Value................ 28
Tx Power Level Num.................... 0
WebAuth online sta Count.................0
DOT1x online sta Count..................0
Security sta Count......................0
WTP Radio Fail Alarm Indication
 Type.................................. Unknown
 Status................................ 0
 Pad................................... 0
WTP Radio Information
Radio Type............................ 802.11b
WTP Radio Config
 Short Preamble........................ 0
 Number of BSSIDs...................... 1
 DTIM Period........................... 0
 Radio Base MAC........................ 00d0.f822.33da
 Beacon Period(milliseconds)........... 100
 Country String........................ CNI
Direct Sequence Control
 Current Channel....................... 11
 Current CCA........................... 1
 Energy Detect Threshold............... 1
MAC Operation
 RTS Threshold......................... 2347
 Short Retry........................... 7
 Long Retry............................ 4
 Fragmentation Threshold............... 2346
 Tx MSDU Lifetime...................... 0
```

```
 Rx MSDU Lifetime..................... 0
Multi-Domain Capability
 First Channel........................ 0
 Number of Channels................... 0
 Max Tx Power Level................... 0
OFDM Control
 Current Channel...................... 0
 Band Supported....................... 0
 TI Threshold......................... 0
Capability
 Power Default........................ 28
 Power Max............................ 28
 Power Min............................ 1
 Power Per Default.................... 100
 Power Per Max........................ 100
 Power Per Min........................ 4
```

字段解释：

字段	说明
WTP Radio Statistics	Radio 统计信息
Assigned WTP BSSID	BSSID 信息
MIC Countermeasures	MIC 记数
RSNA Error Report From Station	RSNA 错误报告
Statistics	统计信息
WTP Radio Information	Radio 信息
WTP Radio Config	Radio 配置
Direct Sequence Control	DSC 控制
MAC Operation	MAC 属性
Multi-Domain Capability	多域容量
OFDM Control	OFDM 控制
Capability	功率容量

【提示信息】 -

【平台说明】 -

4.58 show ap-config radio status

显示 AP 的 radio 列表。

show ap-config radio status *ap-name*

【参数说明】

参数	描述
ap-name	指定待查询 AP 名字

【命令模式】 特权模式

【缺省级别】 1

【使用指导】 -

【配置举例】 1：显示 AP 的 radio 列表

```
Ruijie# show ap-config radio status 220em
Radio Slot  Radio Type      Sub Band   Admin Status    Oper Status     Regulary Domain      Radio
Base MAC
----------- --------------- ---------- --------------- --------------- --------------------
--------------------
1           802.11b/g/n     -          Enable          -               Supported
00d0.f822.33da
2           802.11a/n       -          Enable          -               Supported
00d0.f822.33db
```

字段解释：

字段	说明
Radio Slot	Radio 槽号
Radio Type	Radio 类型
Sub Band	子带宽
Admin Status	管理状态
Oper Status	操作状态
Regulary Domain	规则域
Radio Base MAC	Radio MAC 地址

【提示信息】 -

【平台说明】 -

4.59 show ap-config summary radio

查看所有 AP 在 radio 下的相关信息

show ap-config summary radio [*radio-id*]

【参数说明】

参数	描述
radio-id	要指定的 radio 的 id，范围为 1~48

【命令模式】 特权模式

【缺省级别】 1

【使用指导】 无

【配置举例】 1：查看所有 AP 在 radio 1 下的相关信息
其中包含 AP 名称、AP IP 地址、Radio 的 MAC 地址、Radio 类型和用户数。

```
Ruijie#sh ap-config summary radio 1
Ap Name                                  Radio Base MAC  STA NUM  Radio Type AP IP
---------------------------------------- --------------- -------- ---------- ---------------
AP530-I1.01                              0014.4b74.d427  0        802.11b    172.18.57.195
AP330-I1.1                               0014.4b6d.e18f  8        802.11b    172.18.57.227
```

【提示信息】 -

【平台说明】 仅 AC 支持

4.60 show client details

查看指定 MAC 用户信息。
show client details *sta-mac*

【参数说明】

参数	描述
sta-mac	指定 STA MAC 地址，格式为 H.H.H

【命令模式】 特权模式

【缺省级别】 1

【使用指导】 -

【配置举例】 1：查看 0025.9c9b.aeb5 用户统计信息

```
Ruijie# show client details 0025.9c9b.aeb5
The Details of Client 0025.9c9b.aeb5:
    RSSI..................... 28
    SNR...................... -67
    AID...................... 1
    RX Data.................. 51
    RX Management........... 0
```

```
RX Control.............. 0
RX Unicast.............. 25
RX Multicast............ 0
RX Bytes................ 6174
TX Data................. 3
TX Management........... 0
TX Unicast.............. 3
TX Multicast............ 0
TX Bytes................ 228
TX Probe................ 0
TX Assoc................ 0
TX Assoc Fail........... 0
TX Auth................. 0
TX Auth Fail............ 0
TX Deauth............... 0
TX Disassoc............. 0
Packet Load............. 51216
```

字段解释：

字段	说明
RSSI	接收的信号强度指示
SNR	信噪比
AID	标识 ID
RX Data	接收数据帧数
RX Management	接收管理帧数
RX Control	接收控制帧数
RX Unicast	接收单播帧数
RX Multicast	接收组播帧数
RX Bytes	接收字节数
TX Data	发送数据帧数
TX Management	发送管理帧数
TX Unicast	发送单播帧数
TX Multicast	发送组播帧数
TX Bytes	发送字节数
TX Probe	发送 probe 帧
TX Assoc	发送关联帧
TX Assoc Fail	发送关联帧失败数
TX Auth	发送认证帧数
TX Auth Fail	发送认证帧失败数
TX Deauth	发送解认证帧数
TX Disassoc	发送解关联帧数
Packet Load	吞吐量

【提示信息】 -

【平台说明】 -

4.61 show smart bad radio

显示本 AC 下的 AP5280 的坏卡情况。

show smart bad radio

【参数说明】

参数	描述
-	-

【命令模式】 特权模式

【缺省级别】 1

【使用指导】 -

【配置举例】 1：显示本 AC 的 AP5280 的坏卡情况

```
AC#show smart bad radio
Ap-name                  ap-mac                radio
-------------------      ---------------       ----------------
AP5280-1                 00d0.1234.4565        1,2,3,4,
AP5280-2                 00d0.1234.4568        7,8,
```

字段解释：

字段	说明
Ap name	AP 名字
Ap-mac	AP MAC 地址
radio	坏卡的 radio 号

【提示信息】 -

【平台说明】 仅能在 AC 上显示 AP5280 的坏卡信息

4.62 update-key-tsc enable

配置 AP 在进行 1X 重认证的时候更新加密 TSC。

update-key-tsc enable

配置 AP 在进行 1X 重认证的时候不更新加密 TSC。

no update-key-tsc enable

【参数说明】

参数	描述
-	-

【缺省配置】 不更新。

【命令模式】 AP 配置模式、AP 组配置模式

【缺省级别】 14

【使用指导】 -

【配置举例】 1：进入 AP0001 的配置模式，并且配置在进行 1X 重认证的时候更新加密 TSC。

```
Ruijie(config)# ap-config AP0001
Ruijie(config-ap)# update-key-tsc enable
```

【检验方法】 1：使用 **show ap-config running** *ap-name* 命令，可以查看指定 AP 是否配置更新加密 TSC。

【提示信息】 -

【常见错误】 -

【平台说明】 -

5 ETH-MNG

命令	作用
wired-rate	配置各个 LAN 口带宽限制的命令。

5.1 wired-rate

配置各个 LAN 口带宽限制的命令：

1) **瘦 AP 配置：wired-rate** *value* [**port** *port-id*]

2) **胖 AP 配置：wired-rate** *value*

【参数说明】

参数	描述
value	指定限速值，单位为 1Mbps。默认缺省为不限速。AP 各自以最大能力值生效。
port-id	指定接口。port-id 可配置 1-4，无默认值，在胖 AP 模式下无此参数。

【缺省配置】 默认缺省为不限速，AP 以 AP 本身的最大能力值生效。

【命令模式】 瘦 AP 下在 AP 配置模式或者 AP-GROUP 配置模式，胖 AP 下在接口配置模式。

【缺省级别】 14

【使用指导】 命令支持产品详见配置手册。命令不指定 port 时，表示配置 AP 上的所有 LAN 口速率。

【配置举例】 1：配置单 AP 的 port 2 限速 50。

```
Ruijie(config)# ap-config [ap-name]
Ruijie(config-ap)# wired-rate 50 port 2
```

2：配置所有 AP 的 port 3 限速 30。

```
Ruijie(config)# ap-config all
Ruijie(config-ap)# wired-rate 30 port 3
```

3：配置胖 AP 的 interface FastEthernet 0/4 或 GigabitEthernet 0/4 限速 40。

```
Ruijie(config-if-FastEthernet 0/4)#wired-rate 40
```

或

```
Ruijie(config-if-GigabitEthernet 0/4)#wired-rate 40
```

4：配置组 AP 的 port 1 限速 80。

```
Ruijie(config)#ap-group default
Ruijie(config-group)#wired-rate 80 port 1
```

5：配置组 AP 的所有 LAN 口速率为 90 。

```
Ruijie(config)#ap-group default
Ruijie(config-group)#wired-rate 90
```

【检验方法】 1：使用 **show run** 命令，可以查看当前配置的命令，默认配置时不显示。

【提示信息】 无。

【常见错误】 无

【平台说明】 命令支持差异详见配置手册

6 DATA-PLANE

命令	作用
data-plane	配置无线广播转发设置。

6.1 data-plane

配置广播转发比重。

data-plane queue-weight *unicast-packet-weight multicast-packet-weight broadcast-packet-weight unknown-multicast-packet-weight unknown-unicast-packet-weight*

用户可以用该命令的 **no** 选项还原参数为缺省值。

no data-plane queue-weight

配置广播转发令牌桶的更新周期和倍数。

data-plane token *token-interval token-base-rate*

用户可以用该命令的 **no** 选项还原参数为缺省值

no data-plane token

配置广播无线转发策略。

data-plane wireless-broadcast { **enable** | **disable** }

用户可以用该命令的 **no** 选项取消将所有广播向空口转发。

no data-plane wireless-broadcast

【参数说明】

参数	描述
queue-weight	配置不同类型报文广播转发比重。
wireless-broadcast	配置是否将所有广播报文转发到空口。
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
token	配置广播转发令牌桶的更新周期和倍数
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】 默认开启不同类型报文广播转发的比重控制；默认不开启向空口转发所有广播报文。

【命令模式】 全局配置模式。

【缺省级别】 15

【使用指导】 -

【配置举例】 1：设置不同类型报文广播转发权重，同时开启向空口转发所有广播报文。

```
Ruijie(config)#data-plane queue-weight 100 50 50 25 25
Ruijie(config)#data-plane token 10 10
Ruijie(config)#data-plane wireless-broadcast enable
```

【检验方法】 -

【提示信息】 -

【常见错误】 -

【平台说明】 AC/AP

7 WLOG

命令	作用
show wlan diag ap	查看 AP 记录信息
show wlan diag network	查看整网概况记录信息
show wlan diag sta	查看终端信息
wlan diag enable	配置 WLOG 功能使能。
web-server enable api-path assoc-sta url	配置与 Elog 服务器对接的 url

7.1 show wlan diag ap

AC 上查看 AP 记录信息的命令

show wlan diag ap [**ap-mac** *ap-mac*] [**number** *number*]

【参数说明】

参数	描述
ap-mac	指定要显示的 AP 的 MAC 地址
number	显示的最大条目数

【命令模式】 特权模式

【缺省级别】 1

【使用指导】 无

【配置举例】 1：显示 AP 记录信息：

```
Ruijie# show wlan diag ap ap-mac 00d0.f822.33b0 number 10

ap_record: ruijieAP[00d0.f822.33b0/1.1.1.2],down/up:2

IP Address:1.1.1.2
2012-05-28 09:30:00  [TIMER]      AP UP Time：00:00:18:54
Wired port five in rate/out rate stat:612kbits/sec(in) 1208kbits/sec(out)
   Unicast:    84595   bytes(in) 86625   bytes(out)
   Multicast:  7       bytes(in) 4       bytes(out)
   Broadcast:  2145    bytes(in) 117     bytes(out)
   Error Frame:0       bytes(in) 0       bytes(out)
Radio    channel power       Active STA WEB_Auth   DOT1X       Rssi     ErrorPkt   RetryPkt
-------- ------- ----------- ---------- ---------- ----------  -------- ---------- ----------
1        11      100         2          1          0           0        0          0
```

```
2        157     100         0          0          0          0        0          0

IP Address:1.1.1.2
2012-05-28 09:49:18  [CW-DOWN]    AP UP Time：00:00:38:12
Wired port five in rate/out rate stat:187kbits/sec(in) 905kbits/sec(out)
   Unicast:    84789   bytes(in) 86810   bytes(out)
   Multicast:  7       bytes(in) 5       bytes(out)
   Broadcast:  2148    bytes(in) 133     bytes(out)
   Error Frame:0       bytes(in) 0       bytes(out)
Radio    channel power       Active STA WEB_Auth   DOT1X       Rssi     ErrorPkt   RetryCnt
-------- ------- ----------- ---------- ---------- ----------  -------- ---------- ----------
1        11      100         2          1          0           0        0          0
2        157     100         0          0          0           0        0          0
CAPWAP DOWN REASON:echo expired
```

字段解释：

字段	说明
ap_record	AP 记录标识
IP Address	采集信息时 AP 的 IP 地址
TIMER	定时器采集信息记录标识
CW-DOWN	CAPWAP 断开时采集信息记录标识
Wired port five in rate/out rate stat	有线口最近 5 分钟的输入输出速率
Unicast	有线口单播帧统计信息
Multicast	有线口组播帧统计信息
Broadcast	有线口广播帧统计信息
Error Frame	有线口错帧统计信息
Radio	Radio id
channel	该 radio 的工作信道
power	该 radio 的发射功率
Active STA	关联该 radio 的 STA 数
WEB_AUTH	关联该 radio 通过 WEB 认证上线的 STA 数
DOT1X	关联该 radio 通过 1X 认证上线的 STA 数
ErrorPkt	该 radio 收到的错帧数量
RetryCnt	该 radio 报文重传次
CAPWAP DOWN REASON	CAPWAP 断开原因(只有 CW_DOWN)类型的记录有该项

【提示信息】 -

【平台说明】 AC

7.2 show wlan diag network

查看整网概况记录信息。

show wlan diag network

【参数说明】

参数	描述
-	-

【命令模式】 特权模式

【缺省级别】 1

【使用指导】 无

【配置举例】 1：显示当前整网概况记录信息：

```
Ruijie# show wlan diag network
     Time：2012-05-28 09:10:00
     AC uptime: 1 h
     Online AP：1
     Online AP Version:
         PID[AP220-E]:hwver[2.00] AP Number:1
     Offline AP:7
     ssid                              Active STA WEB Auth   Dot1x      Free STA
     ------------------------------ ---------- ---------- ---------- ----------
     1T17-wlog-test1                    0          0          0          0
     1T17-wlog-test2                    0          0          0
```

字段解释：

字段	说明
Time	该条记录采集的时间
AC Running Time	AC 连接运行的时间长度
Current Online Number of AP	当前在线 AP 数
Online AP Version	当前在线 AP 中各版本情况
Offline Number of AP	预配置但是不在线的 AP 数
ssid	WLAN 的 SSID
Active STA	在线 STA 总数
WEB Auth	Web 认证上线的 STA 数
Dot1x	Dot1X 认证上线的 STA 数
Free STA	免认证上线的 STA 数

【提示信息】 -

【平台说明】 AC

7.3 show wlan diag sta

在 AC 上查看终端信息的命令如下：

show wlan diag sta [**sta-mac** *sta-mac*] [**ip-range** *ip-prefix*] [**action** *action* [**result** *result*]] [**number** *number*]

在 AP 上查看终端信息的命令如下：

show wlan diag sta [**sta-mac** *sta-mac*] [**number** *number*]

【参数说明】

参数	描述
sta-mac	STA MAC 地址
ip-prefix	STA 的 IP 地址范围，以 IP 前缀的方式限定
action	STA 的行为记录类型
result	STA 的行为记录的结果类型
number	STA 的行为记录的个数

【命令模式】 特权模式

【缺省级别】 1

【使用指导】 无

【配置举例】 1：在 AC 上查看终端信息：

```
Ruijie# show wlan diag sta
sta_record: c83a.35c6.0c72
TIME             IP Address      Rssi    Link Rate   AP MAC         SSID
RADIO     Action                          Result   Reason
-------------------  ---------------- -------- ----------- --------------
---------------------------------- --------- ------------------------------  ------
------------------------------
09:59:28  192.168.248.2   0       0           00d0.f822.33b0 lxh-ssid
1         STA UP BY APMG                 SUCCESS
10:12:07  192.168.248.2   21      5500        00d0.f822.33b0 lxh-ssid
1         STA DOWN BY RSNA               SUCCESS  AP circular AC user is offline
```

2：在 AP 上查看终端信息：

```
Ruijie# show wlan diag sta
sta mac: c83a.35c6.0c72
```

```
==========================================================================================
=======================================
2012-05-28 19:31:08
wlan id  state    rssi_rt  rs_rate_mcs tx_frm_cnts rx_frm_cnts tx_frm_flow rx_frm_flow
tx_cnts_error tx_flow_error mgmt_cnts mgmt_flow
-------- -------- -------- ---------- ---------- ---------- ---------- ----------
---------- --------- ---------
1        3        23       80          18          59          4384        5967        0
0             3         381

tx/rxmcs      mcs0, mcs1    mcs2, mcs3    mcs4, mcs5    mcs6, mcs7    mcs8, mcs9    mcs10, mcs11
mcs12, mcs13 mcs14, mcs15
---------- ---------- ---------- ---------- ---------- ---------- ----------
---------- ----------
txmcspercent : 0             0             0             0             0             0
0             0
rxmcspercent : 0             0             0             0             0             0
0             0

tx/rxrate     1, 2    5.5, 11 6, 9    12, 18  24, 36  48, 54   --      --
---------- ------- ------- ------- ------- ------- ------- ------- -------
txratepercent: 16      0       0       7       50      27      0       0
rxratepercent: 57      3       0       5       13      22      0       0
```

字段解释：

字段	说明
sta_record	STA 记录标识
TIME	STA 记录采集的时间
IP Address	STA 记录采集时 IP 地址
Rssi	STA 信号强度
Link Rate	STA 连接速率
AP MAC	STA 关联的 AP 的 MAC 地址
SSID	STA 关联的 WLAN 的 SSID
RADIO	STA 关联的 radio ID
Action	STA 行为记录类型
Result	STA 行为记录结果
Reason	STA 行为记录原因

【提示信息】 -

【平台说明】 AC、胖 AP

7.4 wlan diag enable

配置 WLOG 功能使能
wlan diag enable

关闭 WLOG 功能。
no wlan diag enable

【参数说明】

参数	描述
-	-

【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

【缺省级别】 15

【使用指导】 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。

【配置举例】 1：配置 WLOG 功能开启与关闭

```
Ruijie# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Ruijie(config)#wlan diag enable
Ruijie(config)#no wlan diag enable
```

【检验方法】 -

【提示信息】 -

【常见错误】 -

【平台说明】 AC、胖 AP

7.5 web-server enable api-path assoc-sta url

配置对接的 Elog 服务器地址
web-server enable api-path assoc-sta url *url*

删除对接的 Elog 服务器地址。

no web-server enable api-path assoc-sta url

【参数说明】

参数	描述
url	Elog 服务器的完整地址

【缺省配置】 缺省不与 Elog 服务器对接。

【命令模式】 全局配置模式

【缺省级别】 15

【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 ,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。

【配置举例】 1：STA 上下线信息对接的 Elog 服务器地址的配置与删除

```
Ruijie# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Ruijie(config)#web-server enable api-path assoc-sta url
http://172.18.155.14:8080/elog/service/dc/updateSta
Ruijie(config)#no web-server enable api-path assoc-sta url
```

【检验方法】 -

【提示信息】 -

【常见错误】 -

【平台说明】 AC

WLAN 射频

本分册介绍 WLAN 射频相关内容，包括以下章节：

1. 频谱导航

1 频谱导航

命令	作用
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 enable	开启或关闭频谱导航功能
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
show band-select configuration	查看频谱导航相关配置
show band-select statistics	查看频谱导航运行统计信息

1.1 band-select acceptable-rssi

配置频谱导航可以接受的 STA 信号强度下限。

band-select acceptable-rssi *value*

恢复频谱导航可以接受的 STA 信号强度下限为默认值。

no band-select acceptable-rssi

【参数说明】

参数	描述
value	配置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】 全局配置模式

【缺省级别】 14

【使用指导】 频谱导航可接受的信号强度，用于区分“有可能关联上”和“不可能关联上”的 STA，RSSI 大于这个值的被认为是潜在的可能关联上的 STA，STA 的信息会被关注；相反，RSSI 小于这个值的 STA 的信息将被忽略。

⚠ 2.4G 频段的覆盖范围一般要超过相同信号强度的 5G 频段覆盖范围，如果因为双频 STA 距离 AP 较远，信号强度较弱而不希望接入 5G 频段，那么可以适当调高这个阀值。

【配置举例】 1：配置频谱导航可接受的信号强度为-70 dBm。

```
Ruijie(config)# band-select acceptable-rssi -70
```

【检验方法】 1：使用 **show running-config** 命令，可以查看频谱导航可接受的信号强度配置。

2：使用 **show band-select configuration** 命令，可以查看频谱导航可接受的信号强度配置。

【提示信息】 -

【常见错误】 -

【平台说明】 -

1.2 band-select access-denial

配置拒绝双频 STA 接入 2.4G 频段的次数。
band-select access-denial *value*

恢复拒绝双频 STA 接入 2.4G 频段的次数为默认值。
no band-select access-denial

【参数说明】

参数	描述
value	配置拒绝双频 STA 接入 2.4G 频段的次数，范围[0，10]。

【缺省配置】 2

【命令模式】 全局配置模式

【缺省级别】 14

【使用指导】 频谱导航拒绝双频 STA 接入 2.4G 频段的次数决定了频谱导航对双频 STA 接入 2.4G 频段行为的抑制程度：值为 n，表示 AP 收到双频 STA 在 2.4G 频段上连续发出的 n 个链路认证请求后才开始回应。

⚠ 配置这个值能提高频谱导航成功率，但是有可能导致某些双频 STA 接入困难。

【配置举例】 1：配置频谱导航拒绝双频 STA 接入 2.4G 频段的次数为 4 次。

```
Ruijie(config)# band-select access-denial 4
```

【检验方法】 1：使用 **show running-config** 命令，可以查看频谱导航拒绝双频 STA 接入 2.4G 频段的次数。
2：使用 **show band-select configuration** 命令，可以查看频谱导航拒绝双频 STA 接入 2.4G 频段的次数。

【提示信息】 -

【常见错误】 -

【平台说明】 -

1.3 band-select age-out

配置 STA 信息的老化时间。

band-select age-out { **dual-band** *value* **| suppression** *value* }

恢复 STA 信息的老化时间为默认值。

no band-select age-out { **dual-band | suppression** }

【参数说明】

参数	描述
dual-band *value*	配置双频 STA 信息的老化时间，范围[20，120]，单位秒。
suppression *value*	配置抑制 STA 信息的老化时间，范围[10，60]，单位秒。

【缺省配置】 dual-band：60 秒

suppression：20 秒

【命令模式】 全局配置模式

【缺省级别】 14

【使用指导】 STA 的信息老化时间，即 STA 的信息生命周期，周期越长，AP 对 STA 的频段切换越不敏感。

如果无线用户的网卡经常在 2.4G 和 5G 频段之间切换（用户禁用、启用无线网卡的频段支持），可以配置较小的值；反之，如果无线用户的网卡不经常在 2.4G 和 5G 频段之间切换，可以配置较大的值。

⚠ 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。

【配置举例】 1：配置双频 STA 信息的老化时间为 120 秒。

```
Ruijie(config)# band-select age-out dual-band 120
```

2：配置抑制 STA 信息的老化时间为 60 秒。

```
Ruijie(config)# band-select age-out suppression 60
```

【检验方法】 1：使用 **show running-config** 命令，可以查看频谱导航 STA 信息老化时间配置。

2：使用 **show band-select configuration** 命令，可以查看频谱导航 STA 信息老化时间配置。

【提示信息】 -

【常见错误】 -

【平台说明】 -

1.4 band-select enable

开启频谱导航功能。
band-select enable

关闭频谱导航功能。
no band-select enable

【参数说明】

参数	描述
-	-

【缺省配置】 关闭频谱导航功能。

【命令模式】 WLAN 配置模式

【缺省级别】 14

【使用指导】 开启频谱导航需要满足两个条件：
1：WLAN 映射的 AP 是双频 AP。
2：WLAN 同时映射到双频 AP 的两个 Radio 上。
如果应用场景不满足这两个条件，建议不要开启该 WLAN 的频谱导航功能。

⚠ 如果开启频谱导航功能的 WLAN 映射到单频 2.4G 的 AP 上，那么该 AP 覆盖范围内的双频 STA 将不能导航到 5G 频段。

【配置举例】 1：开启 WLAN 1 的频谱导航功能

```
Ruijie(config)# wlan-config 1
Ruijie(config-wlan)# band-select enable
```

2：关闭 WLAN 1 的频谱导航功能。

```
Ruijie(config)# wlan-config 1
Ruijie(config-wlan)# no band-select enable
```

【检验方法】 1：使用 **show running-config** 命令，可以查看所有 WLAN 的频谱导航功能是启用还是关闭。
2：使用 **show wlan-config cb** *wlan-id* 命令，可以查看某 WLAN 的频谱导航功能是启用还是关闭。

【提示信息】 -

【常见错误】 -

【平台说明】 -

1.5 band-select probe-count

配置抑制 STA 的探测周期计数值。
band-select probe-count *value*

恢复抑制 STA 的探测周期计数值为默认值。
no band-select probe-count

【参数说明】

参数	描述
value	配置抑制 STA 的探测周期计数值，范围[1，10]。

【缺省配置】 2

【命令模式】 全局配置模式

【缺省级别】 14

【使用指导】 这个配置项决定了对抑制 STA 的“抑制”程度：值为 n 表示如果 AP 回应了抑制 STA 一次探测请求，然后直到 n 个探测周期后才会再次回应。

如果发现有单频 2.4G 的 STA 很难发现 WLAN，应该调低抑制 STA 的探测周期计数值。

【配置举例】 1：配置抑制 STA 的探测周期计数值为 1。

```
Ruijie(config)# band-select probe-count 1
```

【检验方法】 1：使用 **show running-config** 命令，可以查看抑制 STA 的探测周期计数值配置。
2：使用 **show band-select configuration** 命令，可以查看抑制 STA 的探测周期计数值配置。

【提示信息】 -

【常见错误】 -

【平台说明】 -

1.6 band-select scan-cycle

配置 STA 探测扫描周期门限。
band-select scan-cycle *value*

恢复 STA 探测扫描周期门限为默认值。

no band-select scan-cycle

【参数说明】

参数	描述
value	配置 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】 全局配置模式

【缺省级别】 14

【使用指导】 STA 在所有支持的信道上主动探测扫描 WLAN 的周期，也是在同一信道上连续两次探测扫描的间隔，和 STA 的驱动有关。如果清楚知道使用的 STA 的扫描周期，那么最好配置成相同的值，可以提高识别成功率；否则，使用默认配置即可。

如果发现有单频 2.4G 的 STA 很难发现 WLAN，应该调低 STA 探测扫描周期门限。

【配置举例】 1：配置 STA 探测扫描周期门限为 1 毫秒。

```
Ruijie(config)# band-select scan-cycle 1
```

【检验方法】 1：使用 **show running-config** 命令，可以查看 STA 探测扫描周期门限配置。
2：使用 **show band-select configuration** 命令，可以查看 STA 探测扫描周期门限配置。

【提示信息】 -

【常见错误】 -

【平台说明】 -

1.7 show band-select configuration

查看频谱导航相关配置。

show band-select configuration

【参数说明】

参数	描述
-	-

【命令模式】 特权模式

【缺省级别】 1

【使用指导】 使用该命令可以查看频谱导航相关的配置，包括：可以接受的 STA 信号强度下限，拒绝双频 STA 接入 2.4G 频段的次数，STA 信息的老化时间，抑制 STA 的探测周期计数值，STA 探测扫描周期门限。

【配置举例】 1：查看频谱导航相关的配置。

```
Ruijie# show band-select configuration
Band Select Configuration
  Acceptable Client RSSI (dBm)............................ -80
  Access Denial Count..................................... 0
  Age Out Dual Band (seconds)............................. 60
  Age Out Suppression (seconds)........................... 20
  Probe Cycle Count....................................... 2
  Scan Cycle Period Threshold (milliseconds).............. 200
```

字段解释：

字段	说明
Acceptable Client RSSI	可以接受的 STA 信号强度下限
Access Denial Count	拒绝双频 STA 接入 2.4G 频段的次数
Age Out Dual Band	双频 STA 信息的老化时间
Age Out Suppression	抑制 STA 信息的老化时间
Probe Cycle Count	抑制 STA 的探测周期计数值
Scan Cycle Period Threshold	STA 探测扫描周期门限

【提示信息】 -

【平台说明】 -

1.8 show band-select statistics

查看频谱导航运行统计信息。

show band-select statistics

【参数说明】

参数	描述
-	-

【命令模式】 特权模式

【缺省级别】 1

【使用指导】 使用该命令可以查看频谱导航运行的统计信息。

【配置举例】 1：查看频谱导航相关的配置。

```
Ruijie# show band-select statistics
Band Select Statistics
  Number of dual band client.............................. 4
  Number of dual band client added........................ 132
  Number of dual band client expired...................... 128
  Number of suppressed client............................. 6
  Number of suppressed client added....................... 234
  Number of suppressed client expired..................... 228
```

字段解释：

字段	说明
Number of dual band client	当前双频 STA 的数量
Number of dual band client added	所有识别出的双频 STA 数量
Number of dual band client expired	已经老化掉的双频 STA 数量
Number of suppressed client	当前抑制 STA 的数量
Number of suppressed client added	所有识别出的抑制 STA 数量
Number of suppressed client expired	已经老化掉的抑制 STA 数量

【提示信息】 -

【平台说明】 -

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

命令	作用
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。
security rsn	配置 WLAN 的认证模式为 RSN 认证模式。
security rsn akm	配置 RSN 认证模式的接入认证方式。
security rsn akm psk set-key	配置 RSN PSK 认证方式的共享密码。
security rsn ciphers	配置 RSN 认证模式的加密方式。
security static-wep-key authentication	配置静态 WEP 模式的链路验证方式。
security static-wep-key encryption	配置 WLAN 启用静态 WEP 模式，同时配置静态 WEP 密钥。
security wpa	配置 WLAN 的认证模式为 WPA 认证模式。
security wpa akm	配置 WPA 认证模式的接入认证方式。
security wpa akm psk set-key	配置 WPA PSK 认证方式的共享密码。
security wpa ciphers	配置 WPA 认证模式的加密方式。
show wclient security	显示 STA 的安全配置信息。
show wlan security	显示 WLAN 的安全配置信息。
webauth prevent-jitter	配置 WEB 认证防抖时间。
wlansec	进入 WLAN 的无线安全配置模式。

1.1 authtimeout forbidcount

配置四次握手 key 交互失败后，禁止关联的次数。

authtimeout forbidcount *count*

删除配置。

no authtimeout forbidcount

恢复缺省配置。

default authtimeout forbidcount

【参数说明】

参数	描述
count	四次握手 key 交互失败后，禁止关联的次数。

【缺省配置】 四次握手 key 交互失败后，禁止关联的次数为 10 次。

【命令模式】 WLAN 安全配置模式

【缺省级别】 14

【使用指导】 -

【配置举例】 1：配置四次握手 key 交互失败后，禁止关联的次数为 5 次。

```
Ruijie(config-wlansec)#authtimeout forbidcount 5
```

【检验方法】 1：使用 **show running-config** 命令，可以查看配置是否生效。

【提示信息】 -

【常见错误】 -

【平台说明】 -

1.2 authtimeout forbidtime

配置四次握手 key 交互失败后，禁止关联的时间间隔，以秒为单位。

authtimeout forbidtime *time*

删除配置。
no authtimeout forbidtime

恢复缺省配置。
default authtimeout forbidtime

【参数说明】

参数	描述
time	四次握手 key 交互失败后，禁止关联的时间间隔。

【缺省配置】 四次握手 key 交互失败后，禁止关联的时间间隔为 5 秒。

【命令模式】 WLAN 安全配置模式

【缺省级别】 14

【使用指导】 -

【配置举例】 1：配置四次握手 key 交互失败后，禁止关联的时间间隔为 6 秒。

```
Ruijie(config-wlansec)#authtimeout forbidtime 6
```

【检验方法】 1：使用 **show running-config** 命令，可以查看配置是否生效。

【提示信息】 -

【常见错误】 -

【平台说明】 -

1.3 authtimeout groupcount

配置组播密钥协商报文重传次数。
authtimeout groupcount *count*

删除配置。
no authtimeout groupcount

恢复缺省配置。
default authtimeout groupcount

【参数说明】

参数	描述
count	组播密钥协商报文重传次数。

【缺省配置】 7 次。

【命令模式】 WLAN 安全配置模式

【缺省级别】 14

【使用指导】 -

【配置举例】 1：配置组播密钥协商报文重传次数为 5 次。

```
Ruijie(config-wlansec)#authtimeout groupcount 5
```

【检验方法】 1：使用 **show running-config** 命令，可以查看配置是否生效。

【提示信息】 -

【常见错误】 -

【平台说明】 -

1.4 authtimeout grouptime

配置组播密钥协商报文超时时间，以毫秒为单位。
authtimeout grouptime *timeout*

删除配置。
no authtimeout grouptime

恢复缺省配置。
default authtimeout grouptime

【参数说明】

参数	描述
timeout	组播密钥协商报文超时时间。

【缺省配置】 1200ms。

【命令模式】 WLAN 安全配置模式

【缺省级别】 14

【使用指导】 -

【配置举例】 1：配置组播密钥协商报文超时时间为 100ms。

```
Ruijie(config-wlansec)#authtimeout grouptime 100
```

【检验方法】 1：使用 **show running-config** 命令，可以查看配置是否生效。

【提示信息】 -

【常见错误】 -

【平台说明】 -

1.5 authtimeout paircount

配置单播密钥协商报文重传次数。
authtimeout paircount *count*

删除配置。
no authtimeout paircount

恢复缺省配置。
default authtimeout paircount

【参数说明】

参数	描述
count	单播密钥协商报文重传次数。

【缺省配置】 7 次。

【命令模式】 WLAN 安全配置模式

【缺省级别】 14

【使用指导】 -

【配置举例】 1：配置单播密钥协商报文重传次数为 5 次。

```
Ruijie(config-wlansec)#authtimeout paircount 5
```

【检验方法】 1：使用 **show running-config** 命令，可以查看配置是否生效。

【提示信息】 -

【常见错误】 -

【平台说明】 -

1.6 authtimeout pairtime

配置单播密钥协商报文超时时间，以毫秒为单位。
authtimeout pairtime *timeout*

删除配置。
no authtimeout pairtime

恢复缺省配置。
default authtimeout pairtime

【参数说明】

参数	描述

timeout	单播密钥协商报文超时时间。

【缺省配置】 1200ms。

【命令模式】 WLAN 安全配置模式

【缺省级别】 14

【使用指导】 -

【配置举例】 1：配置单播密钥协商报文超时时间为 100ms。

```
Ruijie(config-wlansec)#authtimeout pairtime 100
```

【检验方法】 1：使用 **show running-config** 命令，可以查看配置是否生效。

【提示信息】 -

【常见错误】 -

【平台说明】 -

1.7 security rsn

配置 WLAN 的认证模式为 RSN 认证模式。
security rsn enable

关闭 RSN 认证模式。
security rsn disable

【参数说明】

参数	描述
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

【缺省级别】 14

【使用指导】 这个命令是用来启用 RSN 认证模式。
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进行配置，否则配置无效。

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。
RSN 认证模式，即是通常所说的 WPA2 认证模式。如果一个 WLAN 同时开启了 WPA 认证模式和 RSN 认证模式，那么这两种认证模式下的加密方式和接入认证方式是一样的，新配置的加密方式和接入认证方式将覆盖之前的加密方式和接入认证方式。

【配置举例】 1：配置 WLAN 1 的认证模式为 RSN 认证模式。

```
Ruijie(config)#wlansec 1
Ruijie(config-wlansec)#security rsn enable
```

【检验方法】 1：使用 **show running-config** 命令，可以查看配置是否生效。

【提示信息】 1：如果 WLAN 已经启用了其他的加密方式（如 WEP），则无法配置 RSN 认证模式，提示错误。

```
wlan security is static wep, can't config other security mode
```

【常见错误】 1：WLAN 已经启用了其他的加密认证方式（如 WEP）。

【平台说明】 -

1.8 security rsn akm

配置 RSN 认证模式下的接入认证方式为 PSK 认证。
security rsn akm psk enable

关闭 RSN 认证模式下的 PSK 接入认证方式。
security rsn akm psk disable

【参数说明】

参数	描述
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】 无接入认证方式。

【命令模式】 WLAN 安全配置模式

【缺省级别】 14

【使用指导】 这个命令是用来启用 RSN 认证模式下的认证方式，有 PSK 接入认证方式。
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。

【配置举例】 1：配置 WLAN 1 RSN 认证模式下的接入认证方式为预共享密钥认证。

```
Ruijie(config-wlansec)#security rsn akm psk enable
```

【检验方法】 1：使用 **show running-config** 命令，可以查看配置是否生效。

【提示信息】 1：如果 WLAN 安全配置模式下未启用 RSN 认证，则开启 RSN 模式的接入认证方式时提示错误。

```
Ruijie(config)#wlansec 1
Ruijie(config-wlansec)#security rsn akm psk enable
WLAN 1 rsn is disable.
```

2：如果 WLAN 安全配置模式下已经开启了一种接入认证方式，则开启另一种接入认证方式时提示错误。

```
Ruijie(config-wlansec)#security rsn akm psk enable
Wlan 1 has config psk, can not config 1x.
```

【常见错误】 1：WLAN 安全配置模式下未启用 RSN 认证就配置接入认证方式。
2：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。

【平台说明】 -

1.9 security rsn akm psk set-key

配置 RSN PSK 认证方式下的共享密码。
security rsn akm psk set-key { **ascii** *ascii-key* | **hex** *hex-key* }

【参数说明】

参数	描述
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

【缺省级别】 14

【使用指导】 只有开启了 PSK 认证方式时，这个共享密码才生效。
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。

【配置举例】 1：配置 WLAN 1 RSN 的共享密码为 12345678。

```
Ruijie(config)#wlansec 1
Ruijie(config-wlansec)#security rsn enable
Ruijie(config-wlansec)#security rsn akm psk enable
Ruijie(config-wlansec)#security rsn akm psk set-key ascii 12345678
```

【检验方法】 1：使用 **show running-config** 命令，可以查看配置是否生效。

【提示信息】 1：如果 ASCII 码形式的密码长度不足 8 个字符，则提示错误。

```
Ruijie(config-wlansec)#security rsn akm psk set-key ascii 1234567
ASCII PSK length must be not less than 8 (7).
```

2：如果十六进制形式的密码长度不是 64 个十六进制字符，则提示错误。

```
Ruijie(config-wlansec)# security rsn akm psk set-key hex
0123456789abcdef0123456789abcdef0123456789abcdef0123456789abcde
Hex PSK length must be 64.
```

【常见错误】 1：未启用 RSN 认证模式，就配置 RSN PSK 密码。
2：ASCII 码形式的密码长度不足 8 个字符或超过 63 个字符。
3：十六进制形式的密码长度不是 64 个十六进制字符。

【平台说明】 -

1.10 security rsn ciphers

配置 RSN 认证模式下的加密方式为 AES。
security rsn ciphers aes enable

关闭 RSN 认证模式下的 AES 加密方式。
security rsn ciphers aes disable

配置 RSN 认证模式下的加密方式为 TKIP。
security rsn ciphers tkip enable

关闭 RSN 认证模式下的 TKIP 加密方式。
security rsn ciphers tkip disable

【参数说明】

参数	描述
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】 无。

【命令模式】 WLAN 安全配置模式

【缺省级别】 14

【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。

【配置举例】 1：配置 WLAN 1 RSN 认证模式下的加密方式为 AES。

```
Ruijie(config)#wlansec 1
Ruijie(config-wlansec)#security rsn enable
Ruijie(config-wlansec)#security rsn ciphers aes enable
```

【检验方法】 1：使用 **show running-config** 命令，可以查看配置是否生效。

【提示信息】 1：如果 WLAN 安全配置模式下未启用 RSN 认证，则配置 RSN 模式的加密方式时提示错误。

```
Ruijie(config)#wlansec 1
Ruijie(config-wlansec)#security rsn ciphers aes enable
WLAN 1 rsn is disable.
```

【常见错误】 1：WLAN 安全配置模式下未启用 RSN 认证就配置 RSN 加密方式。
2：WLAN 安全配置模式启用 RSN 认证，却没有配置加密方式，导致终端无法关联无线网络。

【平台说明】 -

1.11 security static-wep-key authentication

配置 WLAN 在静态 WEP 模式下的链路验证方式。
security static-wep-key authentication { **open** | **share-key** }

【参数说明】

参数	描述
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】 缺省为开放系统链路验证方式。

【命令模式】 WLAN 安全配置模式

【缺省级别】 14

【使用指导】 这个命令要和 **security static-wep-key encryption** 一起使用，且先配置完静态 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。

【配置举例】 1：配置 WLAN 1 的链路验证方式为共享密钥。

```
Ruijie(config-wlansec)#security static-wep-key authentication share-key
```

【检验方法】 1：使用 **show running-config** 命令，可以查看配置是否生效。

【提示信息】 1：如果未配置启用 WEP 就配置链路验证方式，则提示错误。

```
Fail to setup WEP authmode, not in static WEP security mode (1).
```

【常见错误】 1：未配置启用静态 WEP 模式就配置链路验证方式。

【平台说明】 -

1.12 security static-wep-key encryption

配置 WLAN 启用静态 WEP 模式，同时配置静态 WEP 密码。
security static-wep-key encryption *key-length* { **ascii** | **hex** } *key-index key*

【参数说明】

参数	描述
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

【缺省级别】 14

【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。

⚠ 设备上只有 1 个 WLAN 可配置静态 WEP 加密模式。

需通过删除 WLAN 的安全配置模式删除静态 WEP 模式。

【配置举例】 配置 WLAN 1 的静态 WEP 密钥为 12345。

```
Ruijie(config)#wlansec 1
Ruijie(config-wlansec)#security static-wep-key encryption 40 ascii 1 12345
```

【检验方法】 1：使用 **show running-config** 命令，可以查看配置是否生效。

【提示信息】 1：如果配置的密码字符数与指定的密码长度不一致，则提示错误。

```
Ruijie(config-wlansec)#security static-wep-key encryption 40 ascii 1 123456
password Must be 5 ASCII characters.
```

2：如果设备上已经有一个 WLAN 配置了静态 WEP 模式，配置另一个 WLAN 为静态 WEP 模式时提示错误。

```
Fail to setup static WEP key, because another wlan has configed static WEP.
```

【常见错误】 1：配置的密码字符数与指定的密码长度不一致。
2：配置多个 WLAN 为静态 WEP 模式。

【平台说明】 -

1.13 security wpa

配置 WLAN 的认证模式为 WPA 认证模式。
security wpa enable

关闭 WPA 认证模式。
security wpa disable

【参数说明】

参数	描述
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

【缺省级别】 14

【使用指导】 这个命令是用来启用 WPA 认证模式。
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进行配置，否则配置无效。

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。
如果一个 WLAN 同时开启了 WPA 认证模式和 RSN 认证模式，那么这两种认证模式下的加密方式和接入认证方式是一样的，新配置的加密方式和接入认证方式将覆盖之前的加密方式和接入认证方式。

【配置举例】 1：配置 WLAN 1 的认证模式为 WPA 认证模式。

```
Ruijie(config)#wlansec 1
Ruijie(config-wlansec)#security wpa enable
```

【检验方法】 1：使用 **show running-config** 命令，可以查看配置是否生效。

【提示信息】 1：如果 WLAN 已经启用了其他的加密方式（如 WEP），则无法配置 WPA 认证模式，提示错误。

```
wlan security is static wep, can't config other security mode
```

【常见错误】 1：WLAN 已经启用了其他的加密认证方式（如 WEP）。

【平台说明】 -

1.14 security wpa akm

配置 WPA 认证模式下的接入认证方式为 PSK 认证。
security wpa akm psk enable

关闭 WPA 认证模式下的 PSK 接入认证方式。
security wpa akm psk disable

【参数说明】

参数	描述
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】 无接入认证方式。

【命令模式】 WLAN 安全配置模式

【缺省级别】 14

【使用指导】 这个命令是用来启用 WPA 认证模式下的认证方式，有 PSK 接入认证方式。
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。

【配置举例】 1：配置 WLAN 1 WPA 认证模式下的接入认证方式为预共享密钥认证。

```
Ruijie(config-wlansec)#security wpa akm psk enable
```

【检验方法】 1：使用 **show running-config** 命令，可以查看配置是否生效。

【提示信息】 1：如果 WLAN 安全配置模式下未启用 WPA 认证，则开启 WPA 模式的接入认证方式时提示错误。

```
Ruijie(config)#wlansec 1
Ruijie(config-wlansec)#security wpa akm psk enable
WLAN 1 wpa is disable.
```

2：如果 WLAN 安全配置模式下已经开启了一种接入认证方式，则开启另一种接入认证方式时提示错误。

```
Ruijie(config-wlansec)#security wpa akm psk enable
Wlan 1 has config psk, can not config 1x.
```

【常见错误】 1：WLAN 安全配置模式下未启用 WPA 认证就配置接入认证方式。
2：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。

【平台说明】 -

1.15 security wpa akm psk set-key

配置 WPA PSK 认证方式下的共享密码。
security wpa akm psk set-key { **ascii** *ascii-key* | **hex** *hex-key* }

【参数说明】

参数	描述
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

【缺省级别】 14

【使用指导】 只有开启了 PSK 认证方式时，这个共享密码才生效。
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。

【配置举例】 1：配置 WLAN 1 WPA 的共享密码为 12345678。

```
Ruijie(config)#wlansec 1
Ruijie(config-wlansec)#security wpa enable
Ruijie(config-wlansec)#security wpa akm psk enable
Ruijie(config-wlansec)#security wpa akm psk set-key ascii 12345678
```

【检验方法】 1：使用 **show running-config** 命令，可以查看配置是否生效。

【提示信息】 1：如果 ASCII 码形式的密码长度不足 8 个字符，则提示错误。

```
Ruijie(config-wlansec)#security wpa akm psk set-key ascii 1234567
ASCII PSK length must be not less than 8 (7).
```

2：如果十六进制形式的密码长度不是 64 个十六进制字符，则提示错误。

```
Ruijie(config-wlansec)# security wpa akm psk set-key hex
0123456789abcdef0123456789abcdef0123456789abcdef0123456789abcde
Hex PSK length must be 64.
```

【常见错误】 1：未启用 WPA 认证模式，就配置 WPA PSK 密码。
2：ASCII 码形式的密码长度不足 8 个字符或超过 63 个字符。
3：十六进制形式的密码长度不是 64 个十六进制字符。

【平台说明】 -

1.16 security wpa ciphers

配置 WPA 认证模式下的加密方式为 AES。
security wpa ciphers aes enable

关闭 WPA 认证模式下的 AES 加密方式。
security wpa ciphers aes disable

配置 WPA 认证模式下的加密方式为 TKIP。
security wpa ciphers tkip enable

关闭 WPA 认证模式下的 TKIP 加密方式。
security wpa ciphers tkip disable

【参数说明】

参数	描述
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】 无。

【命令模式】 WLAN 安全配置模式

【缺省级别】 14

【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。

【配置举例】 1：配置 WLAN 1 WPA 认证模式下的加密方式为 AES。

```
Ruijie(config)#wlansec 1
Ruijie(config-wlansec)#security wpa enable
Ruijie(config-wlansec)#security wpa ciphers aes enable
```

【检验方法】 1：使用 **show running-config** 命令，可以查看配置是否生效。

【提示信息】 1：如果 WLAN 安全配置模式下未启用 WPA 认证，则配置 WPA 模式的加密方式时提示错误。

```
Ruijie(config)#wlansec 1
Ruijie(config-wlansec)#security wpa ciphers aes enable
WLAN 1 wpa is disable.
```

【常见错误】 1：WLAN 安全配置模式下未启用 WPA 认证就配置 WPA 加密方式。
2：WLAN 安全配置模式启用 WPA 认证，却没有配置加密方式，导致终端无法关联无线网络。

【平台说明】 -

1.17 show wclient security

查看 STA 的安全配置信息。
show wclient security *mac-address*

【参数说明】

参数	描述
mac-address	所要查看的 STA 的 MAC 地址。

【命令模式】 特权模式、全局模式、WLAN 安全配置模式

【缺省级别】 1

【使用指导】 使用该命令可以查看 STA 的认证是否完成、安全策略、WPA 版本、单播加密套件、EAP 类型等信息。

【配置举例】 1：查看 STA(3848.4c48.d953)的安全配置信息。

```
Ruijie# show wclient security 3848.4c48.d953
Security policy finished      :TRUE
Security policy type          :PSK
Security WPA version          :WPA2
Security Ucast cipher         :CCMP
Security EAP type             :NONE
```

字段解释：

字段	说明
Security policy finished	认证是否完成
Security policy type	安全策略
Security PA v rsion	WPA 版本
Security Ucast cipher	单播加密套件
Security EAP type	EAP 类型

【提示信息】 1：如果设备上没有 STA 的信息，提示错误。

```
Ruijie#show wclient security 3848.4c48.d953
No station info for this MAC  :3848.4c48.d953
```

【平台说明】 -

1.18 show wlan security

显示 WLAN 的安全配置信息。

show wlan security *wlan-id*

【参数说明】

参数	描述
wlan-id	所要查看的 WLAN 的 ID。

【命令模式】 特权模式、全局模式、WLAN 安全配置模式

【缺省级别】 1

【使用指导】 使用该命令可以查看 WLAN 的安全配置信息，包括 WPA 版本、认证方式、单播加密套件、组播加密套件、组播密钥等信息。

【配置举例】 1：查看 WLAN 1 的安全配置信息。

```
Ruijie#show wlan security 1
WLAN SSID           : ruijie-psk
Security Policy     : PSK
WPA version         : RSN(WPA2)
```

```
AKM type            : preshare key
pairwise cipher type: AES
group cipher type   : AES
wpa_passphrase_len  : 8
wpa_passphrase      : 31 32 33 34 35 36 37 38
group key           : 39 de c7 57 5c 58 9a af 84 84 cf 18 3e ce ff 5c
```

字段解释：

字段	说明
WLAN SSID	WLAN 的 SSID
Security Policy	WLAN 的安全策略
WPA version	WPA 版本
AKM type	AKM 套件，即接入认证方式
pairwise cipher type	单播密钥套件
group cipher type	组播密钥套件
wpa_passphrase_len	配置的密码长度
wpa_passphrase	配置的 PSK 密码
group key	WLAN 的组播密钥

【提示信息】 1：如果对应的 WLAN 没有启用任何安全策略，则提示错误。

```
Ruijie#show wlan security 2
No wlan config for this wlanid (2).
```

【平台说明】 -

1.19 webauth prevent-jitter

配置 WLAN 的 WEB 认证防抖时间。
webauth prevent-jitter *timeout*

删除 WEB 认证防抖时间配置。
no webauth prevent-jitter

恢复缺省配置。
default webauth prevent-jitter

【参数说明】

参数	描述
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

【缺省级别】 14

【使用指导】 这个命令是用来在 WLAN 安全配置模式下配置 WEB 认证防抖时间。
必须先启用 WEB 认证，才可以配置 WEB 认证防抖时间。

【配置举例】 1：配置 WLAN 1 的 WEB 认证防抖时间为 900 秒。

```
Ruijie(config)#wlansec 1
Ruijie(config-wlansec)#webauth
Ruijie(config-wlansec)#webauth prevent-jitter 900
```

【检验方法】 1：使用 **show running-config** 命令，可以查看配置是否生效。

【提示信息】 1：如果未启用 WEB 认证就配置 WEB 认证防抖时间参数，则提示错误。

```
Ruijie(config-wlansec)#webauth prevent-jitter 900
Please config webauth first!
```

【常见错误】 1：未启用 WEB 认证就配置 WEB 认证防抖时间。

【平台说明】 -

1.20 wlansec

通过 wlansec 命令进入指定 WLAN 的安全配置模式。
wlansec *wlan-id*

删除安全配置模式。
no wlansec *wlan-id*

恢复缺省配置。
default wlansec *wlan-id*

【参数说明】

参数	描述
wlan-id	配置 WLAN 的 ID。

【缺省配置】 未创建 WLAN 的安全配置模式。

【命令模式】 全局模式

【缺省级别】 14

【使用指导】 进入指定 WLAN 的安全配置模式，该 WLAN 必须已经创建。用户可以通过 **no wlansec** *wlan-id* 命令删除本 WLAN 的安全配置。

【配置举例】 1：配置创建 WLAN 1 的安全配置模式。

```
Ruijie(config)#wlansec 1
```

【检验方法】 1：使用 **show wlan security** 1 命令，可以查看 WLAN 1 的安全配置模式是否创建成功。

【提示信息】 1：如果所要配置安全配置模式的 WLAN 未创建，则提示错误。

```
Ruijie(config)#wlansec 2
Ruijie(config)#No wlan or no ssid for this wlanid(2).
```

【常见错误】 1：所要配置安全配置模式的 WLAN 未创建。

【平台说明】 -

2 WIDS

命令	作用
attack-detection enable	配置使能无线入侵攻击检测功能的检测类型
attack-detection ddos	配置 ddos 攻击的指定种类型报文检测阙值和周期时长
attack-detection flood multi-mac	配置多用户的 flood 攻击的指定类型报文阙值和周期时长
attack-detection flood single-mac	配置单用户的 flood 攻击的指定类型报文阙值和周期时长
attack-detection spoof	配置 spoof 攻击的指定类型报文检测阙值和周期时长。
attack-detection weak-iv	配置 weak-iv 攻击的报文检测阙值和周期时长。
attack-detection statistics ac-max	配置 IDS 攻击检测列表 AC 端的长度限制
attack-detection statistics ap-max	置 IDS 攻击检测列表 AP 端的长度限制
countermeasures ap-max	配置反制设备最大个数
countermeasures enable	配置使能 Rogue 设备反制功能
countermeasures channel-match	配置使能基于信道反制功能
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	配置检测到的设备超时时间
device attack mac-address	配置静态攻击名单的名单 mac 地址
device attack max	配置静态攻击名单的长度限制
device black-ssid	配置 SSID 黑名单列表表项
device channel-bind	配置互通 AP 扫描信道信息
device detected-ap-max	配置扫描 AP 检测链表的最大个数
device friendly-flags	配置设备友好标志位
device max-black-ssid	配置 SSID 黑名单列表表项长度
device mode	配置 AP 工作模式
device permit mac-address	配置允许 MAC 列表表项名单
device permit mac-address max	配置允许 MAC 列表表项长度
device permit ssid	配置允许 SSID 列表表项名单
device permit max-ssid	配置允许 SSID 列表表项长度
device permit vendor bssid	配置允许产商列表表项名单
device permit vendor bssid max	配置允许产商列表表项长度
device scan-para	配置互通 AP 扫描参数信息
device unknown-sta dynamic-enable	配置开启或者关闭未知名 STA 功能
device unknown-sta mac-address	配置未知名 STA 列表表项名单 MAC
device unknown-sta mac-address max	配置未知名 STA 列表表项长度
dos-detection	互通防 dos 攻击检测配置
dynamic-blacklist enable	配置开启或者关闭动态黑名单功能
dynamic-blacklist lifetime	配置动态黑名单列表表项的生存时间
dynamic-blacklist ac-max	配置动态黑名单列表在 AC 端的长度
dynamic-blacklist ap-max	配置动态黑名单列表在 AP 端的长度

dynamic-blacklist mac-address	配置动态黑名单 MAC
hybrid-scan radio	配置 radio 扫描开关
kickout client	配置剔除指定关联用户
kickout threshold	配置剔除低速用户过滤阈值
reset attack-list all	配置清空静态攻击列表表项
reset black-ssid all	配置清空 SSID 黑名单列表
reset detected	配置清除检测到的指定类型设备信息
reset dos-detected	配置清空互通防 dos 攻击检测
reset dynamic-blacklist	配置清空动态黑名单列表表项配置信息
reset permit-mac all	配置清空允许 MAC 列表表项表项配置信息
reset permit-ssid all	配置清空允许 SSID 列表表项表项配置信息
reset permit-vendor all	配置清空允许产商列表表项配置信息
reset rogue-ap detected	配置清空互通非法 AP 检测
reset ssid-filter	清空所有的或者指定的基于 SSID 的黑、白名单列表表项信息
reset ssid-filter blacklist all	清空所有的基于 SSID 的黑名单列表表项
reset ssid-filter blacklist all in-ssid	配置清空基于指定 SSID 的所有黑名单配置信息
reset ssid-filter whitelist all	清空所有的基于 SSID 的白名单列表表项
reset ssid-filter whitelist all in-ssid	配置清空基于指定 SSID 的所有白名单配置信息
reset static-blacklist all	配置清空静态黑名单列表表项配置信息
reset statistic all	配置清空攻击统计列表表项检测信息
reset unknown-sta all	配置清空未知名 STA 列表表项信息
reset user-isolation-permit-list all	配置清空用户隔离允许列表表项配置信息
reset whitelist all	配置清空白名单列表表项配置信息
scan-channels {802.11a | 802.11b} channels	配置设备检测扫描信道信息
rogue-ap countermeasures enable	互通非法 AP 反制功能配置
show wids attacklist	显示静态攻击链表配置信息
show wids blacklist	显示静态或者动态黑名单列表表项信息
show wids black-ssid	显示 SSID 黑名单列表表项信息
show wids detected	显示 WIDS 检测到的指定类型设备信息
show wids dos-detected	显示互通的防 dos 攻击的检测信息
show wids ssid-filter	显示基于 SSID 的黑白名单配置信息
show wids permitted	显示 WIDS 的允许 mac、允许 SSID 和允许产商列表表项配置信息
show wids rogue-ap detected	显示互通的非法 AP 检测信息
show wids statistics	显示 WIDS 的 IDS 攻击检测信息
show wids unknown-sta	显示未知名 STA 列表表项信息
show wids user-isolation permit-mac	显示用户隔离允许 MAC 列表表项信息
show wids whitelist	显示白名单列表表项配置信息
ssid-fitter max	配置基于 ssid 的黑、白名单的 ssid 列表长度
ssid-filter blacklist mac-address in-ssid	配置指定 SSID 的黑名单列表表项
ssid-filter blacklist max	配置基于 SSID 的黑名单列表表项长度

ssid-filter whiteist ssid mac-address in-ssid	配置指定 SSID 的白名单列表表项
ssid-filter whitelist max	配置基于 SSID 的白名单列表表项长度
static-blacklist mac-address	配置静态黑名单列表表项配置信息
static-blacklist max	配置静态黑名单列表表项长度
user-isolation enable	配置用户隔离功能的隔离模式
user-isolation permit-mac	配置用户隔离允许 MAC 列表表项
user-isolation permit-mac max	配置用户隔离允许 MAC 列表表项长度
whitelist mac-address	配置白名单列表表项
whitelist max	配置白名单列表表项长度
wids	配置进入 WIDS 模式

2.1 attack-detection enable

配置开启 IDS 攻击检测功能的检测类型。

attack-detection enable { **all** | **flood** | **ddos** | **spoof** | **weak-iv** }

配置关闭 IDS 攻击检测功能的检测类型。

no attack-detection enable { **all** | **flood** | **ddos** | **spoof** | **weak-iv** }

【参数说明】

参数	描述
all	表示所有 IDS 攻击检测类型
flood	表示 Flooding IDS 攻击检测类型
ddos	表示 DDOS IDS 攻击检测类型
spoof	表示 Spoof IDS 攻击检测类型
weak-iv	表示 Weak-Iv 攻击检测类型

【缺省配置】 默认关闭。

【命令模式】 WIDS 配置模式。

【缺省级别】 14

【使用指导】 此命令用来使能 IDS 攻击检测功能。

【配置举例】 1：开启 Flooding IDS 攻击检测功能。

```
Ruijie(config-wids)# attack-detection enable flood
```

2：关闭 Flooding IDS 攻击检测功能。

```
Ruijie(config-wids)#no attack-detection enable flood
```

【检验方法】 1：使用 **show running-config** 命令，查看 IDS 攻击检测类型配置信息

【提示信息】 -

【常见错误】 -

【平台说明】 -

2.2 attack-detection ddos

配置 ddos 攻击的指定类型报文检测阈值和周期时长

attack-detection ddos { **arp-threshold** *num* | **icmp-threshold** *num* | **syn-threshold** *num* | **interval** *time* }

恢复 ddos 攻击的指定类型报文阈值和周期时长为默认值。

no attack-detection ddos { **arp-threshold** | **icmp-threshold** | **syn-threshold** | **interval** }

【参数说明】

参数	描述
interval *time*	ddos 检测周期,范围为 10~60s
arp-threshold *num*	arp 报文阈值，范围为 1~10000pps
icmp-threshold *num*	icmp 报文阈值，范围为 1~10000pps
syn-threshold *num*	syn 报文阈值，范围为 1~10000pps

【缺省配置】 arp 默认阈值为 5pps，icmp 默认阈值为 100pps，syn 默认阈值为 5pps，ddos 默认检测周期为 30s。

【命令模式】 WIDS 配置模式。

【缺省级别】 14

【使用指导】 -

【配置举例】 1：配置 ddos 攻击 arp 报文的阈值为 200pps。

```
Ruijie(config-wids)# attack-detection ddos arp-threshold 200
```

2：恢复 ddos 攻击 arp 报文的阈值为默认值。

```
Ruijie(config-wids)#no attack-detection ddos arp-threshold
```

【检验方法】 1：使用 **show running-config** 命令，查看 ddos 攻击检测的各类报文阈值和周期时长。

【提示信息】 -

【常见错误】 -

【平台说明】 -

2.3 attack-detection flood multi-mac

配置多用户的 flood 攻击的指定类型报文阈值和周期时长。

attack-detection flood multi-mac { **assoc** | **reassoc** | **disassoc** | **probe** | **action** | **auth** | **deauth** | **null-data** } **threshold** *num* **interval** *time*

恢复多用户的 flood 攻击的指定类型报文阈值和周期时长为默认值。

no attack-detection flood multi-mac { **assoc** | **reassoc** | **disassoc** | **probe** | **action** | **auth** | **deauth** | **null-data** }

【参数说明】

参数	描述
assoc	association 报文
reassoc	reassocation 报文
disassoc	disassocation 报文
probe	probe request 报文
action	action 报文
auth	authentication 报文
deauth	deauthentication 报文
null-data	null data 报文
threshold *num*	攻击报文阈值，范围为 1~5000
interval *time*	统计周期报文阈值，周期为 10~60s

【缺省配置】 所有 flood 攻击检测的报文阈值默认均为 500，统计周期默认 10s。

【命令模式】 WIDS 配置模式。

【缺省级别】 14

【使用指导】 -

【配置举例】 1：配置多用户的 flood 攻击检测的 assoc 报文阈值为 200,统计周期为 20000ms。

```
Ruijie(config-wids)# attack-detection flood multi-mac assoc threshld 200 interval 20000
```

2：恢复多用户的 flood 攻击检测的 assoc 报文阈值和统计周期为默认值。

```
Ruijie(config-wids)#no attack-detection flood multi-mac assoc
```

【检验方法】 1：使用 **show running-config** 命令，多用户的 flood 攻击检测的报文配置检测值

【提示信息】 -

【常见错误】 -

【平台说明】 -

2.4 attack-detection flood single-mac

配置单用户用户的 flood 攻击的指定类型报文阈值和周期时长

attack-detection flood single-mac { **total** | **assoc** | **reassoc** | **disassoc** | **probe** | **action** | **auth** | **deauth** | **null-data** } **threshold** *num* **interval** *time*

恢复单用户的 flood 攻击的指定类型报文阈值和周期时长为默认值。

no attack-detection flood single-mac { **tota** | **assoc** | **reassoc** | **disassoc** | **probe** | **action** | **auth** | **deauth** | **null-data** }

【参数说明】

参数	描述
total	全部报文
assoc	association 报文
reassoc	reassocation 报文
disassoc	disassocation 报文
probe	probe request 报文
action	action 报文
auth	authentication 报文
deauth	deauthentication 报文
null-data	null data 报文
threshold *num*	攻击报文阈值，范围为 1~5000
interval *time*	统计周期报文阈值，周期为 10~60s

【缺省配置】 所有 flood 攻击检测的报文阈值默认均为 300，统计周期默认 10s。

【命令模式】 WIDS 配置模式。

【缺省级别】 14

【使用指导】 -

【配置举例】 1：配置单用户的 flood 攻击检测的 assoc 报文阈值为 200,统计周期为 20000ms。

```
Ruijie(config-wids)# attack-detection flood single-mac assoc threshld 200 interval 20000
```

2：恢复单用户的 flood 攻击检测的 asso 报文阈值和统计周期为默认值。

```
Ruijie(config-wids)#no attack-detection flood single-mac assoc
```

【检验方法】 1：使用 **show running-config** 命令，单用户的 flood 攻击检测的报文检测配置值

【提示信息】 -

【常见错误】 -

【平台说明】 -

2.5 attack-detection spoof

配置 spoof 攻击报文阈值

attack-detection spoof { **threshold** *num* **| interval** *time* }

恢复 spoof 攻击报文阈值为默认值。

no attack-detection spoof { **threshold** | **interval** }

【参数说明】

参数	描述
threshold *num*	报文阈值，范围为 1~1000
interval *time*	检测周期，范围为 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。

【缺省级别】 14

【使用指导】 -

【配置举例】 1：配置 spoof 攻击报文阈值阈值为 20。

```
Ruijie(config-wids)# attack-detection spoof threshold 20
```

2：恢复 spoof 攻击 arp 报文的阈值为默认值。

```
Ruijie(config-wids)#no attack-detection spoof threshold
```

【检验方法】 1：使用 **show runnin-config** 命令，查看 spoof 攻击各种类型报文的检测配置。

【提示信息】 -

【常见错误】 -

【平台说明】 -

2.6 attack-detection weak-iv

配置 weak-iv 攻击的报文检测阈值和周期时长。
attack-detection weak-iv { **threshold** *num* | **interval** *time* }

恢复 weak-iv 攻击的报文检测阈值和周期时长。
no attack-detection weak-iv { **threshold** | **interval** }

【参数说明】

参数	描述
threshold *num*	weak-iv 检测报文阈值，范围为 1~10000
interval *time*	weak-iv 检测周期时长,范围为 1~60s

【缺省配置】 weak-iv 检测报文默认阈值为 10，默认检测周期为 15s。

【命令模式】 WIDS 配置模式。

【缺省级别】 14

【使用指导】 -

【配置举例】 1：配置 weak-iv 检测报文阈值为 200。

```
Ruijie(config-wids)# attack-detection weak-iv threshold 200
```

2：恢复 weak-iv 检测报文阈值为默认值。

```
Ruijie(config-wids)#no attack-detection weak-iv threshold
```

【检验方法】 1：使用 **show runnin-config** 命令，查看 weak-iv 的报文检测配置值和周期

【提示信息】 -

【常见错误】 -

【平台说明】 -

2.7 attack-detection statistics ac-max

配置 IDS 攻击检测列表 AC 端的长度。
attack-detection statistics ac-max *num*

恢复 IDS 攻击检测列表 AC 端的长度为默认值。
no attack-detection statistics ac-max

【参数说明】

参数	描述
num	表示 ids 攻击检测列表 AC 端的个数限制，范围为 1~4096

【缺省配置】 默认为 2048。

【命令模式】 WIDS 配置模式。

【缺省级别】 14

【使用指导】 -

【配置举例】 1：配置 IDS 攻击检测列表 AC 端的长度为 2000。

```
Ruijie(config-wids)# attack-detection statistics ac-max 2000
```

2：恢复 IDS 攻击检测列表 AC 端的长度为默认值。

```
Ruijie(config-wids)#no attack-detection statistics ac-max
```

【检验方法】 1：使用 **show runnin-config** 命令，查看 IDS 攻击检测列表 AC 端的长度。

【提示信息】 -

【常见错误】 -

【平台说明】 -

2.8 attack-detection statistics ap-max

配置 IDS 攻击检测列表 AP 端的长度。
attack-detection statistics ap-max *num*

恢复 IDS 攻击检测列表 AP 端的长度为默认值。
no attack-detection statistics ap-max

【参数说明】

参数	描述
num	表示 ids 攻击检测列表 AP 端的个数限制，范围为 1~1024

【缺省配置】 默认为 512。

【命令模式】 WIDS 配置模式。

【缺省级别】 14

【使用指导】 -

【配置举例】 1：配置 IDS 攻击检测列表 AP 端的长度为 1000。

```
Ruijie(config-wids)# attack-detection statistics ap-max 1000
```

2：恢复 IDS 攻击检测列表 AP 端的长度为默认值。

```
Ruijie(config-wids)#no attack-detection statistics ap-max
```

【检验方法】 1：使用 **show running-config** 命令，查看 IDS 攻击检测列表 AP 端的长度

【提示信息】 -

【常见错误】 -

【平台说明】 -

2.9 countermeasures ap-max

配置每次设备反制的设备最大数量。

countermeasures ap-max *ap-num*

恢复每次设备反制的设备最大数量为默认数量。

no countermeasures ap-max

【参数说明】

参数	描述
ap-num	每次设备反制的设备最大数量，范围为 1~256

【缺省配置】 默认数量为 30。

【命令模式】 WIDS 配置模式。

【缺省级别】 14

【使用指导】 此命令用来配置每次设备反制的设备最大数量，该功能需要设备反制功能开启。

【配置举例】 1：配置设备反制的设备最大数量值为 22。

```
Ruijie(config-wids)# countermeasures ap-max 22
```

2：恢复设备反制的设备最大数量值为默认值。

```
Ruijie(config-wids)#no countermeasures ap-max
```

【检验方法】 1：使用 **show running-config** 命令，查看每次反制设备的最大数量值

【提示信息】 -

【常见错误】 -

【平台说明】 -

2.10 countermeasures enable

配置开启设备反制功能。
countermeasures enable

配置关闭设备反制功能。
no countermeasures enable

【参数说明】

参数	描述
-	-

【缺省配置】 默认关闭。

【命令模式】 WIDS 配置模式。

【缺省级别】 14

【使用指导】 此命令用来使能设备反制功能，设备反制功能在 AP 工作模式 normal 的时候不生效。

【配置举例】 1：开启设备反制功能。

```
Ruijie(config-wids)#countermeasures enable
```

2：关闭设备反制功能。

```
Ruijie(config-wids)#no countermeasures enable
```

【检验方法】 1：使用 **show running-config** 命令，查看设备反制功能是否开启

【提示信息】 -

【常见错误】 -

【平台说明】 -

2.11 countermeasures channel-match

配置使能基于信道反制功能。
countermeasures channel-match

配置关闭基于信道反制功能。
no countermeasures channel-match

【参数说明】

参数	描述
-	-

【缺省配置】 默认关闭。

【命令模式】 WIDS 配置模式。

【缺省级别】 14

【使用指导】 此命令用来配置基于信道反制功能，该功能需要设备反制功能开启。

【配置举例】 1：开启基于信道反制功能。

```
Ruijie(config-wids)# countermeasures channel-matah
```

2：关闭基于信道反制功能。

```
Ruijie(config-wids)#no countermeasures channel-match
```

【检验方法】 1：使用 **show running-config** 命令，查看基于信道反制功能开启状态。

【提示信息】 -

【常见错误】 -

【平台说明】 -

2.12 countermeasures interval

配置设备反制功能的周期时长。
countermeasures interval *time*

恢复设备反制功能的周期时长为默认时长。
no countermeasures interval

【参数说明】

参数	描述
time	设备反制功能的周期时长，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。

【缺省级别】 14

【使用指导】 此命令用来配置设备反制功能的时长。

【配置举例】 1：配置设备反制功能的时长为 2000ms。

```
Ruijie(config-wids)# countermeasures interval 2000
```

2：恢复设备反制功能的时长为默认值。

```
Ruijie(config-wids)#no countermeasures interval
```

【检验方法】 1：使用 **show running-config** 命令，查看设备反制功能的时长。

【提示信息】 -

【常见错误】 -

【平台说明】 -

2.13 countermeasures mode

配置开启设备反制功能。
countermeasures mode { **all** | **adhoc** | **config** | **rogue** | **ssid** }

配置关闭设备反制功能。

no countermeasures mode { **all** | **adhoc** | **config** | **rogue** | **ssid** }

【参数说明】

参数	描述
all	表示所有反制模式都使能
adhoc	表示反制检测到的非法 adhoc 设备
config	表示反制攻击列表表项里面或者 ssid 黑名单里面的设备
rogue	表示反制检测到的非法 ap 设备（信号值超过反制信号值）
ssid	表示反制与 AP 上的 ssid 一样的检测设备

【缺省配置】 默认关闭。

【命令模式】 WIDS 配置模式。

【缺省级别】 14

【使用指导】 此命令用来配置设备反制模式，该模式需要反制功能开启配置才有效。

【配置举例】 1：开启设备反制模式 adhoc。

```
Ruijie(config-wids)#countermeasures mode adhoc
```

2：关闭设备反制模式为 adhoc 的功能。

```
Ruijie(config-wids)#no countermeasures mode adhoc
```

【检验方法】 1：使用 **show running-config** 命令，查看开启的设备反制模式

【提示信息】 1：如果反制功能未开启就配置反制模式，会提示错误。

```
Countermeasures has not been enabled!
```

【常见错误】 -

【平台说明】 -

2.14 countermeasures rssi-min

配置设备反制功能的反制信号强度下限。

countermeasures rssi-min *num*

恢复设备反制功能的反制信号强度下限为默认值。

no countermeasures rssi-min

【参数说明】

参数	描述
num	设备反制功能的反制信号强度下限，范围为 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。

【缺省级别】 14

【使用指导】 此命令用来配置设备反制功能的反制信号强度下限，反制功能未开启时配置该功能无效。

【配置举例】 1：配置设备反制功能的反制信号强度下限为 40。

```
Ruijie(config-wids)# countermeasures rssi-min 40
```

2：恢复设备反制功能的反制信号强度下限为默认值。

```
Ruijie(config-wids)#no countermeasures rssi-min
```

【检验方法】 1：使用 **show running-config** 命令，查看设备反制功能的反制信号强度下限

【提示信息】 -

【常见错误】 -

【平台说明】 -

2.15 device aging duration

配置检测到的设备超时时间。

device aging duration *time*

恢复检测到的设备超时时间为默认值。

no device aging duration

【参数说明】

参数	描述
time	检测到的设备超时时间，范围为 500~5000s

【缺省配置】 默认检测到的设备超时时间为 1200s。

【命令模式】 WIDS 配置模式。

【缺省级别】 14

【使用指导】 此命令用来配置检测到的设备超时时间。

【配置举例】 1：配置检测到的设备超时时间为 1000。

```
Ruijie(config-wids)# device aging duration 1000
```

2：恢复检测到的设备超时时间为默认值。

```
Ruijie(config-wids)#no device aging duration
```

【检验方法】 1：使用 **show running-config** 命令，查看检测到的设备超时时间

【提示信息】 -

【常见错误】 -

【平台说明】 -

2.16 device attack mac-address

配置静态攻击列表表项名单。
device attack mac-address *H.H.H*

删除静态攻击列表表项名单。
no device attack mac-address *H.H.H*

【参数说明】

参数	描述
H.H.H	静态攻击列表表项名单 MAC 地址，表示 bssid 是静态攻击列表表项 MAC 的检测设备在 config 模式下会被反制

【缺省配置】 缺省为空。

【命令模式】 WIDS 配置模式。

【缺省级别】 14

【使用指导】 此命令用来配置静态攻击列表表项名单，是反制 Rogue 设备的策略之一。

【配置举例】 1：设置静态攻击源 MAC 地址为 0000.0000.0001 的设备。

```
Ruijie(config-wids)# device attack mac-address 0000.0000.0001
```

2：删除 MAC 地址为 0000.0000.0001 的静态攻击攻击列表表项名单。

```
Ruijie(config-wids)#no device attack mac-address 0000.0000.0001
```

【检验方法】 1：使用 **show wids attack-list** 命令，查看配置的静态攻击列表表项名单信息

【提示信息】 1：如果允许 MAC 已经在允许 MAC 列表中，会有错误提示。

```
The mac address has been permitted!
```

【常见错误】 -

【平台说明】 -

2.17 device attack max

配置静态攻击列表长度。
device attack max *num*

恢复静态攻击列表长度为默认值。
no device attack max

【参数说明】

参数	描述
num	静态攻击列表长度，范围 1~1024

【缺省配置】 缺省为 512。

【命令模式】 WIDS 配置模式。

【缺省级别】 14

【使用指导】 -。

【配置举例】 1：设置静态攻击列表长度为 900。

```
Ruijie(config-wids)# device attack max 900
```

2：恢复静态攻击列表长度为 512。

```
Ruijie(config-wids)#no device attack max
```

【检验方法】 1：使用 **show running-config** 命令，查看配置的静态攻击列表长度。

【提示信息】 -

【常见错误】 -

【平台说明】 -

2.18 device black-ssid

配置 SSID 黑名单列表表项。
device black-ssid *ssid*

清除 SSID 黑名单列表表项的指定 ssid。
no device black-ssid *ssid*

【参数说明】

参数	描述
ssid	配置该*ssid*为黑名单 ,表示SSID为该*ssid*的的检测设备在反制模式为config时会被反制，

【缺省配置】 缺省为空。

【命令模式】 WIDS 配置模式。

【缺省级别】 14

【使用指导】 此命令用来配置 ssid 黑名单。

【配置举例】 1：配置 SSID：my-wlan 黑名单 SSID 。

```
Ruijie(config-wids)# device black-ssid my-wlan
```

2：从黑名单 SSID 列表表项中删除 SSID：my-wlan。

```
Ruijie(config-wids)#no device black-ssid my-wlan
```

【检验方法】 1：使用 **show wids blacklist** 命令，查看配置的 SSID 黑名单列表信息

【提示信息】 1：SSID 如果长度超过 32，会有错误提示。

```
SSID not more than 32 characters!
```

【常见错误】 -

【平台说明】 -

2.19 device channel-bind

配置指定 radio 扫描信道信息。

device channel-bind radio *radio-id* { **channel** *num* | **max-cycles** *value* }

配置恢复指定 radio 扫描信道为默认值。

no device channel-bind radio *radio-id*

【参数说明】

参数	描述
radio *radio-id*	表示 radio id 值
channel *num*	表示信道值，默认为中国信道开启，可配置范围 1~255
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】 缺省值详见参数说明。

【命令模式】 AP 配置模式。

【缺省级别】 14

【使用指导】 -

【配置举例】 1：配置互通扫描信道扫描次数为 20。

```
Ruijie#configure
Ruijie(config)#ap-config ap1
Ruijie(config-ap)#device channel-bind radio 1 max-cycles 20
```

【检验方法】 通过 **show ap-config running** *ap-name* 查看指定 AP 的互通扫描信道信息。

【提示信息】 -

【常见错误】 -

【平台说明】 -

2.20 device detected-ap-max

配置扫描 AP 链表的最大成员个数。

device detected-ap-max *num*

配置恢复扫描 AP 链表的最大成员个数为默认值。

no device detected-ap-max *num*

【参数说明】

参数	描述
detected-ap-max *num*	表示扫描 AP 的个数上限值，默认 2048。

【缺省配置】 缺省值详见参数说明。

【命令模式】 WIDS 配置模式。

【缺省级别】 14

【使用指导】 -

【配置举例】 1：配置 AP 检测链表的最大个数为 1000。

```
Ruijie#configure
Ruijie(config)#wids
Ruijie(config-wids)#device detected-ap-max 1000
```

【检验方法】 通过 **show running** 查看配置信息。

【提示信息】 -

【常见错误】 -

【平台说明】 -

2.21 device friendly-flags

配置设备友好标识。
device friendly-flags *value*

恢复设备友好标识为默认值。
no device friendly-flags

【参数说明】

参数	描述
value	配置的设备友好标识值，范围在 1 ~ 4294967295

【缺省配置】 默认值为 0。

【命令模式】 WIDS 配置模式。

【缺省级别】 14

【使用指导】 通过配置设备友好标识，使得 AC/AP 可以识别友好 AP。默认值的时候采用 AC/AP 产生的随机友好标识值。

【配置举例】 1：配置设备友好标识为 4294967295。

```
Ruijie(config-wids)# device friendly-flags 4294967295
```

2：恢复设备友好标识值为默认值。

```
Ruijie(config-wids)#no device friendly-flags
```

【检验方法】 1：使用 **show running-config** 命令，查看用户友好标识值

【提示信息】 -

【常见错误】 -

【平台说明】 -

2.22 device max-black-ssid

配置 SSID 黑名单列表长度。
device max-black-ssid *num*

恢复 SSID 黑名单列表长度为默认值。
no device max-black-ssid

【参数说明】

参数	描述
num	SSID 黑名单列表长度，范围 1～1024

【缺省配置】 缺省为 512。

【命令模式】 WIDS 配置模式。

【缺省级别】 14

【使用指导】 -

【配置举例】 1：设置 SSID 黑名单列表长度为 900。

```
Ruijie(config-wids)# device max-black-ssid 900
```

2：恢复 SSID 黑名单列表长度为默认值。

```
Ruijie(config-wids)#no device max-black-ssid
```

【检验方法】 1：使用 **show running-config** 命令，查看配置的 SSID 黑名单列表长度。

【提示信息】 -

【常见错误】 -

【平台说明】 -

2.23 device mode

配置 AP 工作模式。

device mode { **hybrid** | **monitor** | **normal** }

配置恢复 AP 工作模式。

no countermeasures mode

【参数说明】

参数	描述
hybrid	表示混合模式，既做接入设备，又做监测设备
monitor	表示监测模式，只做监测设备
normal	表示普通模式，只做接入设备

【缺省配置】 默认工作模式为 normal。

【命令模式】 AP 配置模式。

【缺省级别】 14

【使用指导】 -

【配置举例】 1：配置工作模式为 hybrid。

```
Ruijie#configure
Enter configuration commands, one per line.  End with CNTL/Z.
Ruijie(config)#ap-config ap1
Ruijie(config-ap)#device mode hybrid
```

【检验方法】 通过 **show ap-config running** *ap-name* 查看指定 AP 的工作模式。

【提示信息】 -

【常见错误】 -

【平台说明】 -

2.24 device permit mac-address

配置允许 MAC 列表表项名单。
device permit mac-address *H.H.H*

删除允许 MAC 列表表项名单。
no device permit mac-address *H.H.H*

【参数说明】

参数	描述
H.H.H	允许 MAC 列表表项名单 MAC 地址，表示 bssid 是允许 MAC 地址列表里面的检测设备是合法设备

【缺省配置】 缺省为空。

【命令模式】 WIDS 配置模式。

【缺省级别】 14

【使用指导】 此命令用来配置允许 MAC 列表表项名单，用来反制 Rogue 设备的策略之一。

【配置举例】 1：设置 MAC 地址为 0000.0000.0001 的允许 MAC 列表表项名单。

```
Ruijie(config-wids)# device permit mac-address 0000.0000.0001
```

2：删除 MAC 地址为 0000.0000.0001 的允许 MAC 列表表项名单。

```
Ruijie(config-wids)#no device permit mac-address 0000.0000.0001
```

【检验方法】 1：使用 **show wids permitted mac-address** 命令，查看配置的允许 MAC 列表表项名单信息

【提示信息】 1：如果允许 MAC 已经在攻击统计列表中，会有错误提示。

```
The mac address has been attacked!
```

【常见错误】 -

【平台说明】 -

2.25 device permit mac-address max

配置允许 MAC 列表长度。
device permit mac-address max *num*

恢复允许 MAC 列表长度为默认值。
no device permit mac-address max

【参数说明】

参数	描述
num	表示允许 MAC 列表长度，范围(1~2048)

【缺省配置】 默认允许 MAC 列表长度为 1024。

【命令模式】 WIDS 配置模式。

【缺省级别】 14

【使用指导】 -

【配置举例】 1：设置允许 MAC 列表长度为 1000。

```
Ruijie(config-wids)# device permit mac-address max 1000
```

2：恢复允许 MAC 列表长度为默认值。

```
Ruijie(config-wids)#no device permit mac-address max
```

【检验方法】 1：使用 **show running-config** 命令，查看配置的允许 MAC 列表长度。

【提示信息】 -

【常见错误】 -

【平台说明】 -

2.26 device permit ssid

配置允许 SSID 列表表项名单。
device permit ssid *ssid*

删除允许 SSID 列表表项名单。
no device permit ssid *ssid*

【参数说明】

参数	描述
ssid	配置该 *ssid* 为允许 SSID 列表表项名单

【缺省配置】 缺省为空。

【命令模式】 WIDS 配置模式。

【缺省级别】 14

【使用指导】 此命令用来配置允许 SSID 列表表项名单，此名单做为设备反制的策略之一。

【配置举例】 1：配置 SSID：my-wlan 为允许 SSID 名单 。

```
Ruijie(config-wids)# device permit ssid my-wlan
```

2：从允许 SSID 列表表项名单中删除 SSID：my-wlan。

```
Ruijie(config-wids)#no device permit ssid my-wlan
```

【检验方法】 1：使用 **show wids permitted ssid** 命令查看配置的允许 SSID 信息

【提示信息】 1：如果配置的 ssid 长度超过 32，会提示配置错误

```
SSID not more than 32 characters!
```

【常见错误】 -

【平台说明】 -

2.27 device permit max-ssid

配置允许 SSID 列表长度。
device permit max-ssid *num*

恢复允许 SSID 列表长度。
no device permit max-ssid

【参数说明】

参数	描述
num	允许 SSID 列表长度，范围 1～1024

【缺省配置】 缺省为 512。

【命令模式】 WIDS 配置模式。

【缺省级别】 14

【使用指导】 -

【配置举例】 1：设置允许 SSID 列表长度为 900。

```
Ruijie(config-wids)# device permit max-ssid 900
```

2：恢复允许 SSID 列表长度为默认值。

```
Ruijie(config-wids)#no device permit max-ssid
```

【检验方法】 1：使用 **show running-config** 命令，查看配置的允许 SSID 列表长度。

【提示信息】 -

【常见错误】 -

【平台说明】 -

2.28 device permit vendor bssid

配置允许产商列表表项名单。
device permit vendor bssid *H.H.H*

删除允许产商列表表项名单。
no device permit vendor bssid *H.H.H*

【参数说明】

参数	描述
H.H.H	允许产商 MAC 地址

【缺省配置】 缺省为空。

【命令模式】 WIDS 配置模式。

【缺省级别】 14

【使用指导】 厂商号是配置 MAC 地址的前 3 字节，不允许配置多条同一厂商的 MAC 地址。此配置是用来反制 Rogue 设备的策略之一。

【配置举例】 1：设置 MAC 地址为 0000.0000.0001 的允许产商列表表项。

```
Ruijie(config-wids)# device permit vendor bssid 0000.0000.0001
```

2：删除 MAC 地址为 0000.0000.0001 的允许产商列表表项。

```
Ruijie(config-wids)#no device permit vendor bssid 0000.0000.0001
```

【检验方法】 1：使用 **show wids permitted vendor** 命令，查看已经配置的允许产商列表表项

【提示信息】 1：如果允许产商重复配置，会有错误提示。

```
The permitted vendor[vendor-mac] already exists!
```

【常见错误】 -

【平台说明】 -

2.29 device permit vendor bssid max

配置允许产商列表长度。

device permit vendor bssid max *num*

恢复允许产商列表长度为默认值。

no device permit vendor bssid max

【参数说明】

参数	描述
num	表示允许产商列表长度，范围(1~1024)

【缺省配置】 默认允许产商列表长度为 512。

【命令模式】 WIDS 配置模式。

【缺省级别】 14

【使用指导】 -

【配置举例】 1：设置允许产商列表长度为 1000。

```
Ruijie(config-wids)# device permit vendor bssid max 1000
```

2：恢复允许产商列表长度为默认值。

```
Ruijie(config-wids)#no device permit vendor bssid max
```

【检验方法】 1：使用 **show running-config** 命令，查看配置的允许产商列表长度。

【提示信息】 -

【常见错误】 -

【平台说明】 -

2.30 device scan-para

配置互通非法 AP 检测扫描参数。

device scan-para { **radio** *radio-id* **scan-type** { **active** | **passive** } **device-detect** { **enable** | **disable** } | **ap-mode** { **normal** | **monitor** } | **detect-rpt-time** *time* }

配置恢复互通非法 AP 检测扫描参数为默认值。

no device scan-para { radio *radio-id* | **ap-mode** | **detect-rpt-time }**

【参数说明】

参数	描述
radio *radio-id*	表示 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。

【缺省级别】 14

【使用指导】 -

【配置举例】 1：配置恢复指定 radio：1 的互通 AP 扫描类型和扫描开关为默认值。

```
Ruijie#configure
Enter configuration commands, one per line.  End with CNTL/Z.
Ruijie(config)#ap-config ap1
Ruijie(config-ap)#no device scan-para radio 1
```

【检验方法】 通过 **show ap-config running** *ap-name* 查看指定互通 AP 的扫描信息。

【提示信息】 -

【常见错误】 -

【平台说明】 -

2.31 device unknown-sta dynamic-enable

配置使能动态未知名 STA 检测功能。
device unknown-sta dynamic-enable

配置关闭动态未知名 STA 检测功能。
no device unknown-sta dynamic-enable

【参数说明】

参数	描述
-	-

【缺省配置】 默认关闭。

【命令模式】 WIDS 配置模式。

【缺省级别】 14

【使用指导】 该功能仅在 AP 工作在非 normal 模式下有效。

【配置举例】 1：配置开启动态未知名 STA 检测功能。

```
Ruijie(config-wids)# device unknown-sta dynamic-enable
```

2：配置关闭动态未知名 STA 检测功能。

```
Ruijie(config-wids)#no device unknown-sta dynamic-enable
```

【检验方法】 1：使用 **show running-config** 命令，查看动态未知名 STA 检测配置情况

【提示信息】 -

【常见错误】 -

【平台说明】 -

2.32 device unknown-sta mac-address

配置静态未知名 STA 列表表项名单。
device unknown-sta mac-address *H.H.H*

删除静态未知名 STA 列表表项名单。
no device unknown-sta mac-address *H.H.H*

【参数说明】

参数	描述
H.H.H	表示该 MAC 地址的用户是未知名 STA

【缺省配置】 缺省为空。

【命令模式】 WIDS 配置模式。

【缺省级别】 14

【使用指导】 此命令用来配置静态未知名 STA 列表表项名单，用来反制未知名 STA 设备的策略。

【配置举例】 1：设置 MAC 地址为 0000.0000.0001 的设备为未知名 STA。

```
Ruijie(config-wids)# device unknown-sta mac-address 0000.0000.0001
```

2：删除 MAC 地址为 0000.0000.0001 的未知名 STA。

```
Ruijie(config-wids)#no device unknown-sta mac-address 0000.0000.0001
```

【检验方法】 1：使用 **show wids unknown-sta** 命令，查看配置的未知名 STA 列表表项名单信息

【提示信息】 -

【常见错误】 -

【平台说明】 -

2.33 device unknown-sta mac-address max

配置未知名 STA 列表长度。
device unknown-sta mac-address max *num*

恢复未知名 STA 列表长度为默认值。
no device unknown-sta mac-address max

【参数说明】

参数	描述
num	未知名 STA 列表长度，范围(1~256)

【缺省配置】 默认未知名 STA 列表长度为 128。

【命令模式】 WIDS 配置模式。

【缺省级别】 14

【使用指导】 -

【配置举例】 1：设置未知名 STA 列表长度为 200。

```
Ruijie(config-wids)# device unknown-sta mac-address max 200
```

2：恢复未知名 STA 列表长度为默认值。

```
Ruijie(config-wids)#no device unknown-sta mac-address max
```

【检验方法】 1：使用 **show running-config** 命令，查看配置的未知名 STA 列表长度。

【提示信息】 -

【常见错误】 -

【平台说明】 -

2.34 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。
dos-detection { **enable** | **threshold** *num* | **interval** *time* }

配置恢复互通防 dos 攻击检测为默认值。
no dos-detection { **enable** | **threshold** | **interva** }

【参数说明】

参数	描述
enable	表示互通防 dos 攻击检测开关
threshold *num*	表示互通防 dos 攻击检测报文阈值，范围为 1~5000
time	表示互通防 dos 攻击检测周期时长 1~60000ms

【缺省配置】 默认关闭互通防 dos 攻击功能 默认防 dos 攻击检测报文阈值为 30 默认防 dos 攻击检测周期时间为 1000ms。

【命令模式】 WIDS 配置模式。

【缺省级别】 14

【使用指导】 -

【配置举例】 1：配置开启互通防 dos 攻击功能。

```
Ruijie(config-wids)#dos-detection enable
```

【检验方法】 1：使用 **show running-config** 命令，查看互通防 dos 攻击功能相关配置。

【提示信息】 -

【常见错误】 -

【平台说明】 -

2.35 dynamic-blacklist enable

配置开启动态黑名单功能。
dynamic-blacklist enable

配置关闭动态黑名单功能。
no dynamic-blacklist enable

【参数说明】

参数	描述
-	-

【缺省配置】 默认关闭。

【命令模式】 WIDS 配置模式。

【缺省级别】 14

【使用指导】 -

【配置举例】 1：开启动态黑名单功能。

```
Ruijie(config-wids)# dynamic-blacklist enable
```

2：关闭动态黑名单功能。

```
Ruijie(config-wids)#no dynamic-blacklist enable
```

【检验方法】 1：使用 **show running-config** 命令，查看动态黑名单功能开启状态。

【提示信息】 -

【常见错误】 -

【平台说明】 -

2.36 dynamic-blacklist lifetime

配置动态黑名单生存时间。
dynamic-blacklist lifetime *time*

恢复动态黑名单生存时间为默认值。
no dynamic-blacklist lifetime

【参数说明】

参数	描述
time	动态黑名单的生存时间，范围为 60~86400s

【缺省配置】 默认动态黑名单的生存时间为 300s。

【命令模式】 WIDS 配置模式。

【缺省级别】 14

【使用指导】 -

【配置举例】 1：配置动态黑名单的生存时间为 600s。

```
Ruijie(config-wids)# dynamic-blacklist lifetime 600
```

2：恢复动态黑名单生存时间为默认值。

```
Ruijie(config-wids)#no dynamic-blacklist lifetime
```

【检验方法】 1：使用 **show running-config** 命令，查看动态黑名单的生存时间

【提示信息】 -

【常见错误】 -

【平台说明】 -

2.37 dynamic-blacklist ac-max

配置 AC 端动态黑名单列表长度。
dynamic-blacklist ac-max *num*

恢复 AC 端动态黑名单列表长度为默认值。
no dynamic-blacklist ac-max

【参数说明】

参数	描述
num	AC 端动态黑名单列表 AC 端长度，范围 1～4096

【缺省配置】 缺省为 2048。

【命令模式】 WIDS 配置模式。

【缺省级别】 14

【使用指导】 -

【配置举例】 1：设置 AC 端动态黑名单列表长度为 2000。

```
Ruijie(config-wids)# dynamic-blacklist ac-max 2000
```

2：恢复 AC 端动态黑名单列表长度为默认值。

```
Ruijie(config-wids)#no dynamic-blacklist ac-max
```

【检验方法】 1：使用 **show running-config** 命令，查看配置的 AC 端动态黑名单列表长度。

【提示信息】 -

【常见错误】 -

【平台说明】 -

2.38 dynamic-blacklist ap-max

配置 AP 端动态黑名单列表长度。
dynamic-blacklist ap-max *num*

恢复 AP 端动态黑名单列表长度为默认值。
no dynamic-blacklist ap-max

【参数说明】

参数	描述
num	AP 端动态黑名单列表长度，范围 1～4096

【缺省配置】 缺省为 2048。

【命令模式】 WIDS 配置模式。

【缺省级别】 14

【使用指导】 -

【配置举例】 1：设置 AP 端动态黑名单列表长度为 1000。

```
Ruijie(config-wids)# dynamic-blacklist ap-max 1000
```

2：恢复 AP 端动态黑名单列表长度为默认值。

```
Ruijie(config-wids)#no dynamic-blacklist ap-max
```

【检验方法】 1：使用 **show running-config** 命令，查看配置的 AP 端动态黑名单列表长度。

【提示信息】 -

【常见错误】 -

【平台说明】 -

2.39 dynamic-blacklist mac-address

配置动态黑名单列表表项名单。

dynamic-blacklist mac-address *H.H.H*

删除动态黑名单 STA 列表表项名单。

no dynamic-blacklist mac-address *H.H.H*

【参数说明】

参数	描述
H.H.H	表示该 MAC 地址的用户是动态黑名单列表

【缺省配置】 缺省为空。

【命令模式】 WIDS 配置模式。

【缺省级别】 14

【使用指导】 此命令用来配置动态黑名单列表表项名单，用来动态控制 STA 接入和通信的策略。

【配置举例】 1：设置 MAC 地址为 0000.0000.0001 的设备为动态黑名单。

```
Ruijie(config-wids)#dynamic-blacklist mac-address 0000.0000.0001
```

2：删除 MAC 地址为 0000.0000.0001 的动态黑名单。

```
Ruijie(config-wids)#no dynamic-blacklist mac-address 0000.0000.0001
```

【检验方法】 1：使用 **show wids blacklist dynamic** 命令，查看配置的未知名 STA 列表表项名单信息

【提示信息】 -

【常见错误】 -

【平台说明】 -

2.40 hybrid-scan radio

配置开启 radio 扫描开关状态信息。
hybrid-scan radio *num* **enable**

配置关闭 radio 扫描开关关状态信息。
hybrid-scan radio *num* **disable**

【参数说明】

参数	描述
radio *num*	表示指定 radio，默认开启

【缺省配置】 缺省值详见参数说明。

【命令模式】 AP 配置模式。

【缺省级别】 14

【使用指导】 -

【配置举例】 1：配置关闭 radio1 的扫描。

```
Ruijie#configure
Ruijie(config)#ap-config ap1
Ruijie(config-ap)#hybrid-scan radio 1 disable
```

【检验方法】 通过 **show ap-config running** *ap-name* 查看指定 AP 的扫描信道配置信息。

【提示信息】 -

【常见错误】 -

【平台说明】 -

2.41 kickout client

配置剔除当前关联用户。

kickout client *H.H.H*

【参数说明】

参数	描述
H.H.H	剔除用户的 MAC 地址

【缺省配置】 缺省为空。

【命令模式】 WIDS 配置模式。

【缺省级别】 14

【使用指导】 此命令用来解除已经关联的 STA，通过此命令，可以断开指定 STA 的关联

【配置举例】 1：配置剔除 MAC 地址为 0000.0000.0001 的用户。

```
Ruijie(config-wids)# kickout client 0000.0000.0001
```

【检验方法】 -

【提示信息】 -

【常见错误】 -

【平台说明】 -

2.42 kickout threshold

配置低速用户过滤阈值。

kickout threshold *rate*

关闭低速用户过滤功能。

no kickout threshold

【参数说明】

参数	描述
rate	报文收发速率，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。

【缺省级别】 14

【使用指导】 当 STA 的速率小于指定的阈值时，AP 设备将断开 STA 的关联。

【配置举例】 1：配置低速用户过滤阈值为 20Mbps。

```
Ruijie(config-wids)# kickout threshold 20
```

2：关闭低速用户过滤功能。

```
Ruijie(config-wids)#no kickout threshold
```

【检验方法】 1：使用 **show running-config** 命令，查看低速用户过滤阈值。

【提示信息】 -

【常见错误】 -

【平台说明】 -

2.43 reset attack-list all

配置清空静态攻击列表表项配置信息。

reset attack-list all

【参数说明】

参数	描述
-	-

【缺省配置】 无。

【命令模式】 WIDS 配置模式。

【缺省级别】 14

【使用指导】 此命令用来清空静态攻击列表表项配置信息。

【配置举例】 1：清空静态攻击列表表项配置信息。

```
Ruijie(config-wids)#reset attack-list all
```

【检验方法】 1：使用命令 **show wids attacklist** 可以查看是否清空成功。

【提示信息】 -

【常见错误】 -

【平台说明】 -

2.44 reset black-ssid all

配置清空 SSID 黑名单列表表项配置信息。

reset black-ssid all

【参数说明】

参数	描述
-	-

【缺省配置】 无。

【命令模式】 WIDS 配置模式。

【缺省级别】 14

【使用指导】 此命令用来清空 SSID 黑名单列表表项配置信息。

【配置举例】 1：清空 SSID 黑名单列表表项配置信息。

```
Ruijie(config-wids)#reset black-ssid all
```

【检验方法】 1：使用 **show wids black-ssid** 查看是否成功清空。

【提示信息】 -

【常见错误】 -

【平台说明】 -

2.45 reset detected

配置清除检测到的指定类型设备信息。

reset detected { **all** | **adhoc** | **rogue** { **ap** | **client** } | **mac-address** *H.H.H* }

【参数说明】

参数	描述
all	表示清空检测到的所有设备
adhoc	表示清空检测到的 adhoc 设备
rogue ap	表示清空检测到的 rogue ap 设备
rogue client	表示清空检测到的 rogue client 设备
mac-address *H.H.H*	表示需要清除的设备 MAC 地址

【缺省配置】 无。

【命令模式】 WIDS 配置模式。

【缺省级别】 14

【使用指导】 无

【配置举例】 1： 清空检测到的 rogue ap 信息

```
Ruijie(config-wids)#reset detected rogue ap
```

2： 清除 MAC 地址为 0000.0000.0001 的设备检测信息

```
Ruijie(config-wids)#reset detected mac-address 0000.0000.0001
```

【检验方法】 使用命令 **show wids detected** 查看是否已经清空。

【提示信息】 -

【常见错误】 -

【平台说明】 -

2.46 reset dos-detected

配置清除互通防 dos 攻击检测到的信息。

reset dos-detected

【参数说明】

参数	描述

-	-

【缺省配置】 无。

【命令模式】 WIDS 配置模式。

【缺省级别】 14

【使用指导】 无

【配置举例】 1： 清空互通防 dos 攻击检测到的信

```
Ruijie(config-wids)#reset dos-detected
```

【检验方法】 使用命令 **show wids dos-detected** 查看是否已经清空。

【提示信息】 -

【常见错误】 -

【平台说明】 -

2.47 reset dynamic-blacklist

配置清除动态黑名单列表表项信息。

reset dynamic-blacklist { **all** | **mac-address** *H.H.H* }

【参数说明】

参数	描述
all	表示清除所有动态黑名单列表表项。
mac-address *H.H.H*	表示清除源 MAC 为 H.H.H 的动态黑名单列表表项。

【缺省配置】 无。

【命令模式】 WIDS 配置模式。

【缺省级别】 14

【使用指导】 -

【配置举例】 1：清除源 MAC 为 0000.0000.0001 的动态黑名单列表表项。

```
Ruijie(config-wids)# reset dynamic-blacklist mac-addres 0000.0000.0001
```

【检验方法】 使用命令 **show wids blacklist dynamic** 查看是否已经清除。

【提示信息】 -

【常见错误】 -

【平台说明】 -

2.48 reset permit-mac all

配置清空允许 MAC 列表表项配置信息。

reset permit-mac all

【参数说明】

参数	描述
-	-

【缺省配置】 无。

【命令模式】 WIDS 配置模式。

【缺省级别】 14

【使用指导】 -

【配置举例】 1：清空允许 MAC 列表表项配置信息。

```
Ruijie(config-wids)#reset permit-mac all
```

【检验方法】 使用命令 **show wids permitted mac-address** 查看是否已经清空。

【提示信息】 -

【常见错误】 -

【平台说明】 -

2.49 reset permit-ssid all

配置清空允许 SSID 列表表项配置信息。

reset permit-ssid all

【参数说明】

参数	描述
-	-

【缺省配置】 无。

【命令模式】 WIDS 配置模式。

【缺省级别】 14

【使用指导】 -

【配置举例】 1：清空允许 SSID 列表表项配置信息。

```
Ruijie(config-wids)#reset permit-ssid all
```

【检验方法】 使用命令 **show wids permitted ssid** 查看是否已经成功清除。

【提示信息】 -

【常见错误】 -

【平台说明】 -

2.50 reset permit-vendor all

配置清空允许产商列表表项配置信息。

reset permit-vendor all

【参数说明】

参数	描述
-	-

【缺省配置】 无。

【命令模式】 WIDS 配置模式。

【缺省级别】 14

【使用指导】 -

【配置举例】 1：清空允许产商列表表项配置信息。

```
Ruijie(config-wids)#reset permit-vendor all
```

【检验方法】 使用命令 **show wids permitted vendo**r 查看是否已经成功清除。

【提示信息】 -

【常见错误】 -

【平台说明】 -

2.51 reset rogue-ap detected

配置清除互通非法 AP 检测到的信息。

reset rogue-ap detected

【参数说明】

参数	描述
-	-

【缺省配置】 无。

【命令模式】 WIDS 配置模式。

【缺省级别】 14

【使用指导】 无

【配置举例】 1： 清空互通非法 AP 检测到的信

```
Ruijie(config-wids)#reset rogue-ap detected
```

【检验方法】 使用命令 **show wids rogue-ap detected** 查看是否已经清空。

【提示信息】 -

【常见错误】 -

【平台说明】 -

2.52 reset ssid-filter

配置清空所有或者指定 SSID 的黑、白名单配置信息。

reset ssid-filter { **ssid all** | **in-ssid** *ssid* }

【参数说明】

参数	描述
ssid all	所有 ssid
in-ssid *ssid*	指定 ssid

【缺省配置】 无。

【命令模式】 WIDS 配置模式。

【缺省级别】 14

【使用指导】 -

【配置举例】 1：清空所有的基于 SSID 的黑、白名单配置信息。

```
Ruijie(config-wids)#reset ssid-filter ssid all
```

【检验方法】 使用命令 **show wids ssid-filter** 查看是否已经清空。

【提示信息】 1：如果指定的 SSID 不存在，会有错误提示。

```
There is no SSID[ssid] to filter!
```

【常见错误】 -

【平台说明】 -

2.53 reset ssid-filter blacklist all

配置清空所有的基于 SSID 的黑、白名单的黑名单配置信息。

reset ssid-filter blacklist all

【参数说明】

参数	描述
-	-

【缺省配置】 无。

【命令模式】 WIDS 配置模式。

【缺省级别】 14

【使用指导】 -

【配置举例】 1：清空所有的基于 SSID 的黑、白名单的黑名单配置信息。

```
Ruijie(config-wids)#reset ssid-filter blacklist all
```

【检验方法】 使用命令 **show wids ssid-filter blacklist all** 查看是否已经清空。

【提示信息】 -

【常见错误】 -

【平台说明】 -

2.54 reset ssid-filter blacklist all in-ssid

配置清空基于指定 SSID 的所有黑名单配置信息。

reset ssid-filter blacklist all in-ssid *string*

【参数说明】

参数	描述
string	表示清楚基于 SSID:string 下的所有黑名单信息

【缺省配置】 无。

【命令模式】 WIDS 配置模式。

【缺省级别】 14

【使用指导】 -

【配置举例】 1：清空清空基于 SSID:my-wlan 的所有黑名单配置信息。

```
Ruijie(config-wids)#reset ssid-filter blacklist all in-ssid my-wlan
```

【检验方法】 使用命令 **show wids ssid-filter blacklist all in-ssid** *string* 查看是否已经清空。

【提示信息】 1：如果 SSID 不存在，会有错误提示。

```
There is no SSID[ssid] to filter!
```

【常见错误】 -

【平台说明】 -

2.55 reset ssid-filter whitelist all

配置清空所有的基于 SSID 的黑、白名单的白名单配置信息。

reset ssid-filter whitelist all

【参数说明】

参数	描述
-	-

【缺省配置】 无。

【命令模式】 WIDS 配置模式。

【缺省级别】 14

【使用指导】 -

【配置举例】 1：清空所有的基于 SSID 的黑、白名单的白名单配置信息。

```
Ruijie(config-wids)#reset ssid-filter whitelist all
```

【检验方法】 使用命令 **show wids ssid-filter whitelist all** 查看是否已经清空。

【提示信息】 -

【常见错误】 -

【平台说明】 -

2.56 reset ssid-filter whitelist all in-ssid

配置清空基于指定 SSID 的所有白名单配置信息。

reset ssid-filter whitelist all in-ssid *string*

【参数说明】

参数	描述
string	表示清楚基于 SSID:string 下的所有白名单信息

【缺省配置】 无。

【命令模式】 WIDS 配置模式。

【缺省级别】 14

【使用指导】 -

【配置举例】 1：清空清空基于 SSID:my-wlan 的所有白名单配置信息。

```
Ruijie(config-wids)#reset ssid-filter whitelist all in-ssid my-wlan
```

【检验方法】 使用命令 **show wids ssid-filter whitelist all in-ssid** *string* 查看是否已经清空。

【提示信息】 1：如果 SSID 不存在，会有错误提示。

```
There is no SSID[ssid] to filter!
```

【常见错误】 -

【平台说明】 -

2.57 reset static-blacklist all

配置清空静态黑名单列表表项配置信息。

reset static-blacklist all

【参数说明】

参数	描述
-	-

【缺省配置】 无。

【命令模式】 WIDS 配置模式。

【缺省级别】 14

【使用指导】 -

【配置举例】 1：清空静态黑名单列表表项配置信息。

```
Ruijie(config-wids)# reset static-blacklist all
```

【检验方法】 使用命令 **show wids blacklist static** 查看是否已经清空。

【提示信息】 -

【常见错误】 -

【平台说明】 -

2.58 reset statistic all

配置清空攻击统计列表表项检测信息。

reset statistic all

【参数说明】

参数	描述
-	-

【缺省配置】 无。

【命令模式】 WIDS 配置模式。

【缺省级别】 14

【使用指导】 -

【配置举例】 1：清空攻击统计列表表项检测信息。

```
Ruijie(config-wids)# reset statistic all
```

【检验方法】 -

【提示信息】 -

【常见错误】 -

【平台说明】 -

2.59 reset unknown-sta all

配置清空未知名 STA 列表表项信息。

reset unknown-sta all

【参数说明】

参数	描述
-	-

【缺省配置】 无。

【命令模式】 WIDS 配置模式。

【缺省级别】 14

【使用指导】 -

【配置举例】 1：清空未知名 STA 列表表项信息。

```
Ruijie(config-wids)#reset unknown-sta all
```

【检验方法】 使用命令 **show wids unknown-sta** 查看是否已经清空。

【提示信息】 -

【常见错误】 -

【平台说明】 -

2.60 reset user-isolation-permit-list all

配置清空用户隔离允许列表表项配置信息。

reset user-isolation-permit-list all

【参数说明】

参数	描述
-	-

【缺省配置】 无。

【命令模式】 WIDS 配置模式。

【缺省级别】 14

【使用指导】 -

【配置举例】 1：清空用户隔离允许列表表项信息。

```
Ruijie(config-wids)#reset user-isolation-permit-list all
```

【检验方法】 使用命令 **show wids user-isolation permit-mac** 查看是否已经清除。

【提示信息】 -

【常见错误】 -

【平台说明】 -

2.61 reset whitelist all

配置清空白名单列表表项配置信息。
reset whitelist all

【参数说明】

参数	描述
-	-

【缺省配置】 无。

【命令模式】 WIDS 配置模式。

【缺省级别】 14

【使用指导】 -

【配置举例】 1：清空白名单列表表项配置信息。

```
Ruijie(config-wids)#reset whitelist all
```

【检验方法】 使用命令 **show wids whitelist** 查看是否已经清除。

【提示信息】 -

【常见错误】 -

【平台说明】 -

2.62 rogue-ap countermeasures enable

配置开启互通非法 AP 反制功能。
rogue-ap countermeasures enable

配置关闭互通非法 AP 反制功能。
no rogue-ap countermeasures enable

【参数说明】

参数	描述
-	-

【缺省配置】 默认关闭。

【命令模式】 WIDS 配置模式。

【缺省级别】 14

【使用指导】 -

【配置举例】 1：开启互通非法 AP 反制功能。

```
Ruijie(config-wids)#rogue-ap countermeasures enable
```

2：关闭互通非法 AP 反制功能。

```
Ruijie(config-wids)#no rogue-ap countermeasures enable
```

【检验方法】 1：使用 **show running-config** 命令，查看互通反制功能配置。

【提示信息】 -

【常见错误】 -

【平台说明】 -

2.63 scan-channels { 802.11a | 802.11b } channels

配置扫描信道。

scan-channels { 802.11a | 802.11b } channels *nuim1 num2…num13*

配置恢复扫描信道为默认值。

no scan-channels { 802.11a | 802.11b }

【参数说明】

参数	描述
802.11a	表示配置 5G 信道，默认扫描信道为空。
802.11b	表示配置 2.4G 信道，默认扫描信道为空。
channels *num*	表示配置的信道值

【缺省配置】 缺省值详见参数说明。

【命令模式】 AP 配置模式。

【缺省级别】 14

【使用指导】 -

【配置举例】 1：配置 5g 的扫描信道 149 153 157。

```
Ruijie#configure
Ruijie(config)#ap-config ap1
Ruijie(config-ap)#scan-channels 802.11a channels 149 153 157
```

【检验方法】 通过 **show ap-config running** *ap-name* 查看指定 AP 的扫描信道配置信息。

【提示信息】 -

【常见错误】 -

【平台说明】 -

2.64 show wids attacklist

显示 WIDS 的静态攻击列表表项配置信息。

show wids attack-list

【参数说明】

参数	描述
-	-

【命令模式】 特权模式。

【缺省级别】 1

【使用指导】 -

【配置举例】 1：显示 WIDS 的静态列表表项配置信息。

```
Ruijie# show wids attack-list
```

【提示信息】 -

【平台说明】 -

2.65 show wids blacklist

显示 WIDS 的动态/静态黑名单列表表项信息。

show wids blacklist { **dynamic** | **static** }

【参数说明】

参数	描述

dynamic	表示显示动态黑名单列表表项信息
static	表示显示静态黑名单列表表项信息

【命令模式】 特权模式。

【缺省级别】 1

【使用指导】 -

【配置举例】 1：显示 WIDS 的静态黑名单列表表项信息。

```
Ruijie# show wids blacklist static
```

2：显示 WIDS 的动态黑名单列表表项信息。

```
Ruijie# show wids blacklist dynamic
```

【提示信息】 -

【平台说明】 -

2.66 show wids black-ssid

显示 WIDS 的 SSID 黑名单列表表项配置信息。

show wids black-ssid

【参数说明】

参数	描述
-	-

【命令模式】 特权模式。

【缺省级别】 1

【使用指导】 -

【配置举例】 1：显示 WIDS 的 SSID 黑名单列表表项配置信息。

```
Ruijie# show wids black-ssid
```

【提示信息】 -

【平台说明】 -

2.67 show wids detected

显示 WIDS 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* **}**

【参数说明】

参数	描述
adhoc	表示显示检测到的 adhoc 网络。
all	表示显示所有 WLAN 检测到的设备。
friendly ap	表示显示检测到的友好 AP。
interfering ap	表示显示检测到的干扰 AP。
rogue adhoc-ap	表示显示检测到符合反制模式 adhoc 的设备。
rogue ap	表示显示检测到符合反制模式 rogue 的设备。
rogue client	表示显示检测到的 Rogue client 设备。
rogue config-ap	表示显示检测到的符合反制模式 config 的设备。
rogue ssid-ap	表示显示检测到的符合反制模式 ssid 的设备。
mac-address *H.H.H*	表示显示检测到的源 MAC 为 H.H.H 的设备。

【命令模式】 特权模式。

【缺省级别】 1

【使用指导】 -

【配置举例】 1：显示检测到的 Rogue AP 设备信息。

```
Ruijie# show wids detected rogue ap
```

【提示信息】 -

【平台说明】 -

2.68 show wids dos-detected

显示互通的防 dos 攻击检测信息。

show wids dos-detected

【参数说明】

参数	描述
-	-

【命令模式】 特权模式。

【缺省级别】 1

【使用指导】 -

【配置举例】 1：显示互通的防 dos 攻击检测信息。

```
Ruijie# show wids dos-detected
```

【提示信息】 -

【平台说明】 -

2.69 show wids ssid-filter

显示基于 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*] }

【参数说明】

参数	描述
blacklist all	表示显示所有基于 SSID 的黑名单列表表项信息
blacklist all in-ssid *string*	表示显示指定 SSID 的所有基于 SSID 的黑名单列表表项信息
ssid all	表示显示所有基于 SSID 的黑白名单的 SSID 信息
whitelist all	表示显示所有基于 SSID 的白名单列表表项信息
whitelist all in-ssid *string*	表示显示指定 SSID 的所有基于 SSID 的白名单列表表项信息

【命令模式】 特权模式。

【缺省级别】 1

【使用指导】 -

【配置举例】 1：显示 WIDS 的所有基于 SSID 的黑名单列表表项信息

```
Ruijie# show wids ssid-filter blacklist all
```

【提示信息】 -

【平台说明】 -

2.70 show wids permitted

显示 WIDS 的允许 MAC、允许 SSID 和允许产商列表表项配置信息。

show wids permitted { **mac-address** | **ssid** | **vendor** }

【参数说明】

参数	描述
mac-address	表示允许的 MAC 地址列表表项信息
ssid	表示允许的 SSID 列表表项信息
vendor	表示允许的产商列表表项信息

【命令模式】 特权模式。

【缺省级别】 1

【使用指导】 -

【配置举例】 1：显示 WIDS 的允许 SSID 列表表项信息。

```
Ruijie# show wids permitted ssid
```

【提示信息】 -

【平台说明】 -

2.71 show wids rogue-ap detected

显示互通的非法 AP 检测信息。

show wids rogue-ap detected

【参数说明】

参数	描述
-	-

【命令模式】 特权模式。

【缺省级别】 1

【使用指导】 -

【配置举例】 1：显示互通的非法 AP 检测信息。

```
Ruijie# show wids rogue-ap detected
```

【提示信息】 -

【平台说明】 -

2.72 show wids statistics

显示 WIDS 的 IDS 攻击检测信息。

show wids statistics

【参数说明】

参数	描述
-	-

【命令模式】 特权模式。

【缺省级别】 1

【使用指导】 -

【配置举例】 1：显示 WIDS 的 IDS 攻击检测信息。

```
Ruijie# show wids statistics
```

【提示信息】 -

【平台说明】 -

2.73 show wids unknown-sta

显示未知名 STA 列表表项信息。

show wids unknown-sta

【参数说明】

参数	描述
-	-

【命令模式】 特权模式。

【缺省级别】 1

【使用指导】 -

【配置举例】 1：显示 WIDS 的未知名 STA 列表表项信息。

```
Ruijie# show wids unknown-sta
```

【提示信息】 -

【平台说明】 -

2.74 show wids user-isolation permit-mac

显示 WIDS 的用户隔离允许列表表项信息。

show wids user-isolation permit-mac

【参数说明】

参数	描述
-	-

【命令模式】 特权模式。

【缺省级别】 1

【使用指导】 -

【配置举例】 1：显示 WIDS 的用户隔离允许列表表项信息。

```
Ruijie# show wids user-isolation permit-mac
```

【提示信息】 -

【平台说明】 -

2.75 show wids whitelist

显示 WIDS 的白名单列表表项信息。

show wids whitelist

【参数说明】

参数	描述
-	-

【命令模式】 特权模式。

【缺省级别】 1

【使用指导】 -

【配置举例】 1：显示 WIDS 的白名单列表表项信息。

```
Ruijie# show wids whitelist
```

【提示信息】 -

【平台说明】 -

2.76 ssid-filter max

配置基于 ssid 的黑、白名单的 ssid 列表长度。
ssid-filter max *num*

恢复基于 ssid 的黑、白名单的 ssid 列表长度为默认值。
no ssid-filter max

【参数说明】

参数	描述
num	基于 ssid 的黑、白名单的 ssid 列表长度，范围(1~128)

【缺省配置】 默认 ssid 列表长度为 64。

【命令模式】 WIDS 配置模式。

【缺省级别】 14

【使用指导】 -

【配置举例】 1：设置基于 ssid 的黑、白名单的 ssid 列表长度为 40。

```
Ruijie(config-wids)# ssid-filter max 40
```

2：恢复基于 ssid 的黑、白名单的 ssid 列表长度为默认值。

```
Ruijie(config-wids)#no ssid-filter max
```

【检验方法】 通过 **show running-config** 命令查看

【提示信息】 -

【常见错误】 -

【平台说明】 -

2.77 ssid-filter blacklist mac-address in-ssid

配置指定 SSID 的黑名单列表表项。

ssid-filter blacklist mac-address *H.H.H* **in-ssid** *string*

删除指定 SSID 的指定 MAC 地址的黑名单列表表项。
no ssid-filter blacklist mac-address *H.H.H* **in-ssid** *string*

【参数说明】

参数	描述
H.H.H	表示基于 ssid 的黑名单列表表项名单 MAC 地址
string	表示 ssid 值

【缺省配置】 缺省为空。

【命令模式】 WIDS 配置模式。

【缺省级别】 14

【使用指导】 如果基于 SSID 的白名单列表中已经有该信息，则不允许配置。

【配置举例】 1：设置 MAC 地址为 0000.0000.0001 的设备为 SSID: my-wlan 的黑名单。

```
Ruijie(config-wids)# ssid-filter blacklist mac-address 0000.0000.0001 in-ssid my-wlan
```

2：从 SSID: my-wlan 删除 MAC 地址为 0000.0000.0001 的黑名单列表表项。

```
Ruijie(config-wids)# no ssid-filter blacklist mac-address 0000.0000.0001 in-ssid my-wlan
```

【检验方法】 通过 **show wids ssid-filter** 命令查看

【提示信息】 1：如果基于 SSID 的白名单列表中已经有该配置信息，则有错误提示。

```
The mac[H.H.H] was filtered by white-list of SSID[string].
```

【常见错误】 -

【平台说明】 -

2.78 ssid-filter blacklist max

配置基于 SSID 的黑名单列长度。
ssid-filter blacklist max *num*

恢复基于 SSID 的黑名单列表长度为默认值。
no ssid-filter blacklist max

【参数说明】

参数	描述

num	基于 SSID 的黑名单列表长度，范围(1~256)

【缺省配置】 默认基于 SSID 的黑名单列表长度为 256。

【命令模式】 WIDS 配置模式。

【缺省级别】 14

【使用指导】 -

【配置举例】 1：配置基于黑名单列表长度为 50。

```
Ruijie(config-wids)#ssid-filter blacklist max 50
```

2：恢复基于 SSID 的黑名单列表长度为默认值。

```
Ruijie(config-wids)#no sid-filter blacklist max
```

【检验方法】 通过 **show running-config** 命令查看

【提示信息】 -

【常见错误】 -

【平台说明】 -

2.79 ssid-filter whitelist mac-address in-ssid

配置指定 SSID 的白名单列表表项。

ssid-filter whitelist mac-address *H.H.H* **in-ssid** *string*

删除指定 SSID 的指定 MAC 地址的白名单列表表项。

no ssid-filter whitelist mac-address *H.H.H* **in-ssid** *string*

【参数说明】

参数	描述
H.H.H	表示基于 ssid 的白名单列表表项名单 MAC 地址
string	表示 ssid 值

【缺省配置】 缺省为空。

【命令模式】 WIDS 配置模式。

【缺省级别】 14

【使用指导】 如果基于 SSID 的黑名单中已经有该信息，则不允许配置。

【配置举例】 1：设置 MAC 地址为 0000.0000.0001 的设备为 SSID: my-wlan 的白名单。

```
Ruijie(config-wids)# ssid-filter whitelist mac-address 0000.0000.0001 in-ssid my-wlan
```

2：从 SSID: my-wlan 删除 MAC 地址为 0000.0000.0001 的白名单列表表项。

```
Ruijie(config-wids)# no ssid-filter whitelist mac-address 0000.0000.0001 in-ssid my-wlan
```

【检验方法】 **show wids ssid-filter** 命令查看

【提示信息】 1：如果基于 SSID 的黑名单列表中已经有该表项，则会有错误提示。

```
The mac[H.H.H] was filtered by black-list of SSID[string].
```

【常见错误】 -

【平台说明】 -

2.80 ssid-filter whitelist max

配置基于 SSID 的白名单列表长度。
ssid-filter whitelist max *num*

恢复基于 SSID 的白名单列表长度为默认值。
no ssid-filter whitelist max

【参数说明】

参数	描述
num	基于 SSID 的白名单列表长度限，范围(1~256)

【缺省配置】 默认基于 SSID 的白名单列表长度为 256。

【命令模式】 WIDS 配置模式。

【缺省级别】 14

【使用指导】 -

【配置举例】 1：配置基于白名单列表长度为 50。

```
Ruijie(config-wids)#ssid-filter whitelist max 50
```

2：恢复基于 SSID 的白名单列表长度为默认值。

```
Ruijie(config-wids)#no sid-filter whitelist max
```

【检验方法】 通过 **show running-config** 命令查看

【提示信息】 -

【常见错误】 -

【平台说明】 -

2.81 static-blacklist mac-address

配置静态黑名单列表表项。
static-blacklist mac-address *H.H.H*

删除指定 MAC 地址的静态黑名单列表表项。
no static-blacklist mac-address *H.H.H*

【参数说明】

参数	描述
H.H.H	表示静态黑名单列表表项名单 MAC 地址

【缺省配置】 缺省为空。

【命令模式】 WIDS 配置模式。

【缺省级别】 14

【使用指导】 如果白名单列表中已经有该配置信息，则不允许配置。

【配置举例】 1：设置 MAC 地址为 0000.0000.0001 的设备为静态黑名单。

```
Ruijie(config-wids)# static-blacklist mac-address 0000.0000.0001
```

2：删除 MAC 地址为 0000.0000.0001 的静态黑名单列表表项。

```
Ruijie(config-wids)# no static-blacklist mac-address 0000.0000.0001
```

【检验方法】 -

【提示信息】 1：静态黑名单配置信息已经在白名单中，会有错误提示。

```
The mac address has existed in white list！
```

【常见错误】 -

【平台说明】 -

2.82 static-blacklist max

配置静态黑名单列表长度。
static-blacklist max *num*

恢复允许静态黑名单列表长度为默认值。
no static-blacklist max

【参数说明】

参数	描述
num	静态黑名单列表长度，范围(1~2048)

【缺省配置】 默认静态黑名单列表长度为 1024。

【命令模式】 WIDS 配置模式。

【缺省级别】 14

【使用指导】 -

【配置举例】 1：设置静态黑名单列表长度为 1000。

```
Ruijie(config-wids)# static-blacklist max 1000
```

2：恢复静态黑名单列表长度为默认值。

```
Ruijie(config-wids)#no static-blacklist max
```

【检验方法】 -

【提示信息】 -

【常见错误】 -

【平台说明】 -

2.83 user-isolation enable

配置使能 AP 上的二层用户隔离功能
user-isolation { **ap** | **ssid-ap** | **wlan-id** *num* } **enable**

配置关闭 AP 上的二层用户隔离功能。

no user-isolation { **ap** | **ssid-ap** | **wlan-id** *num* } **enable**

【参数说明】

参数	描述
ap	表示使能基于 ap 的二层用户隔离功能。
ssid-ap	表示使能基于 ap-ssid 的二层用户隔离功能。
wlan-id *num*	表示使能指定 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。

【缺省级别】 14

【使用指导】 -

【配置举例】 **-**

【检验方法】 通过 **show ruuning-config** 命令查看

【提示信息】 -

【常见错误】 -

【平台说明】 -

2.84 user-isolation permit-mac

配置隔离允许 MAC 列表表项名单。

user-isolation permit-mac *H.H.H*

删除隔离允许 MAC 列表表项名单。

no user-isolation permit-mac *H.H.H*

【参数说明】

参数	描述
H.H.H	表示隔离允许 MAC 名单的 MAC 地址

【缺省配置】 缺省为空。

【命令模式】 WIDS 配置模式。

【缺省级别】 14

【使用指导】 -

【配置举例】 1：设置 MAC 地址为 0000.0000.0001 的隔离允许 MAC 列表表项名单。

```
Ruijie(config-wids)# user-isolation permit-mac 0000.0000.0001
```

2：删除 MAC 地址为 0000.0000.0001 的允许 MAC 列表表项名单。

```
Ruijie(config-wids)#no user-isolation permit-mac 0000.0000.0001
```

【检验方法】 通过 **show wids user-isolation permit-mac** 命令查看

【提示信息】 -

【常见错误】 -

【平台说明】 -

2.85 user-isolation permit-mac max

配置隔离允许 MAC 列表长度。
user-isolation permit-mac max *num*

恢复隔离允许 MAC 列表长度为默认值。
no user-isolation permit-mac max

【参数说明】

参数	描述
num	隔离允许 MAC 列表长度，范围(1~2048)

【缺省配置】 默认隔离允许 MAC 列表长度为 1024。

【命令模式】 WIDS 配置模式。

【缺省级别】 14

【使用指导】 -

【配置举例】 1：设置隔离允许 MAC 列表长度为 1000。

```
Ruijie(config-wids)# user-isolation permit-mac max 1000
```

2：恢复隔离允许 MAC 列表长度为默认值。

```
Ruijie(config-wids)#no user-isolation permit-mac max
```

【检验方法】 通过 **show ruuning-config** 命令查看

【提示信息】 -

【常见错误】 -

【平台说明】 -

2.86 whitelist mac-address

配置白名单列表表项。
whitelist mac-address *H.H.H*

删除指定 MAC 地址的白名单列表表项。
no whitelist mac-address *H.H.H*

【参数说明】

参数	描述
H.H.H	表示白名单列表表项名单 MAC 地址

【缺省配置】 缺省为空。

【命令模式】 WIDS 配置模式。

【缺省级别】 14

【使用指导】 -。

【配置举例】 1：设置 MAC 地址为 0000.0000.0001 的设备为白名单。

```
Ruijie(config-wids)# whitelist mac-address 0000.0000.0001
```

2：删除 MAC 地址为 0000.0000.0001 的白名单列表表项。

```
Ruijie(config-wids)# no whitelistmac-address 0000.0000.0001
```

【检验方法】 通过 **show wids whitelist** 命令查看

【提示信息】 1：如果白名单配置信息已经在静态黑名单列表中，会有错误提示。

```
The mac address has existed in black list.
```

【常见错误】 -

【平台说明】 -

2.87 whitelist max

配置白名单列表长度。
whitelist max *num*

恢复白名单列表长度。
no whitelist max

【参数说明】

参数	描述
num	白名单列表长度，范围(1~2048)

【缺省配置】 默认白名单列表长度为 1024。

【命令模式】 WIDS 配置模式。

【缺省级别】 14

【使用指导】 -

【配置举例】 1：设置白名单列表长度为 1000。

```
Ruijie(config-wids)# whitelist max 1000
```

2：恢复白名单列表长度为默认值。

```
Ruijie(config-wids)#no whitelist max
```

【检验方法】 通过 **show running-config** 命令查看

【提示信息】 -

【常见错误】 -

【平台说明】 -

2.88 wids

配置进入 WIDS 配置模式。
wids

【参数说明】

参数	描述

-	-

【缺省配置】 无缺省配置。

【命令模式】 全局配置模式。

【缺省级别】 14

【使用指导】 此命令用来进入 WIDS 配置模式。

【配置举例】 1：进入 wids 配置模式。

```
Ruijie(config)#wids
Ruijie(config-wids)#
```

【检验方法】 -

【提示信息】 -

【常见错误】 -

【平台说明】 -

3 WAPI

命令	作用
security wapi	配置 WAPI 安全模式。
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 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 asu cert	配置认证服务器 WAPI 证书。
security wapi ca cert	配置颁发者证书。
security wapi psk	配置预共享密钥认证方式。
security wapi psk set-key	配置 WAPI 预共享密钥。
show wapi-sta summary	查看 WAPI 用户状态信息。

3.1 security wapi

配置 WAPI 安全模式。

security wapi enable

关闭 WAPI 安全模式。

security wapi disable

【参数说明】

参数	描述
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

【缺省级别】 14

【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。

【配置举例】 1：配置 WLAN 1 启用 WAPI 安全模式。

```
Ruijie(config)#wlansec 1
Ruijie(config-wlansec)#security wapi enable
```

【检验方法】 1：使用 **show running-config** 命令，可以查看配置是否生效。

【提示信息】 1：如果 WLAN 已经启用了其他的加密方式（如 WPA），则无法启用 WAPI 安全模式，提示错误。

```
Ruijie(config)#wlansec 1
Ruijie(config-wlansec)#security wapi enable
WLAN 1 WPA has been enabled, can not config wapi.
```

【常见错误】 1：WLAN 已经启用了其他的加密认证方式（如 WEP/RSN/WPA）。

【平台说明】 -

3.2 security wapi 2-cert

配置二证书认证方式。
security wapi 2-cert enable

关闭二证书认证方式。
security wapi 2-cert disable

【参数说明】

参数	参数
enable	启用二证书认证方式。
disable	关闭二证书认证方式。

【缺省配置】 关闭。

【命令模式】 WLAN 安全配置模式

【缺省级别】 14

【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模式不可同时启用。

【配置举例】 1：启用二证书认证方式。

```
Ruijie(config-wlansec)#security wapi 2-cert enable
```

【检验方法】 1：使用 **show running-config** 命令，可以查看配置是否生效。

【提示信息】 1：如果 WLAN 未启用 WAPI 安全模式就配置二证书认证方式，提示错误。

```
Ruijie(config)#wlansec 1
Ruijie(config-wlansec)#security wapi 2-cert enable
Wapi is disabled, can not config!
```

【常见错误】 1：WLAN 未启用 WAPI 安全模式就配置二证书认证方式。

【平台说明】 -

3.3 security wapi 3-cert

配置三证书认证方式。
security wapi 3-cert enable

关闭三证书认证方式。
security wapi 3-cert disable

【参数说明】

参数	参数
enable	启用三证书认证方式。
disable	关闭三证书认证方式。

【缺省配置】 关闭。

【命令模式】 WLAN 安全配置模式

【缺省级别】 14

【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模式不可同时启用。

【配置举例】 1：启用三证书认证方式。

```
Ruijie(config-wlansec)#security wapi 3-cert enable
```

【检验方法】 1：使用 **show running-config** 命令，可以查看配置是否生效。

【提示信息】 1：如果 WLAN 未启用 WAPI 安全模式就配置三证书认证方式，提示错误。

```
Ruijie(config)#wlansec 1
Ruijie(config-wlansec)#security wapi 3-cert enable
Wapi is disabled, can not config!
```

【常见错误】 1：WLAN 未启用 WAPI 安全模式就配置三证书认证方式。

【平台说明】 -

3.4 security wapi ae cert

配置 AE 设备的 WAPI 证书。

security wapi ae cert *ae_certfile*

【参数说明】

参数	描述
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

【缺省级别】 14

【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。

【配置举例】 1：配置设备 AE 证书文件为 AE.cer。

```
Ruijie(config-wlansec)#security wapi ae cert AE.cer
```

【检验方法】 1：使用 **show running-config** 命令，可以查看配置是否生效。

【提示信息】 1：如果设备上找不到配置的证书文件，提示错误。

```
Ruijie(config)#wlansec 1
Ruijie(config-wlansec)#security wapi enable
Ruijie(config-wlansec)#security wapi ae cert AE.cer
Failed to set wapi AE cert!
```

【常见错误】 -

【平台说明】 -

3.5 security wapi asu address

在证书认证模式下，配置认证服务器的 IP 地址。

security wapi asu address *ip_address*

【参数说明】

参数	描述
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

【缺省级别】 14

【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。

【配置举例】 1：配置认证服务器 IP 地址为 192.168.1.123。

```
Ruijie(config-wlansec)#security wapi asu address 192.168.1.123
```

【检验方法】 1：使用 **show running-config** 命令，可以查看配置是否生效。

【提示信息】 -

【常见错误】 -

【平台说明】 -

3.6 security wapi asu cert

WAPI 三证书认证模式下，配置 ASU 证书。

security wapi asu cert *asu_certfile*

【参数说明】

参数	描述
asu_certfile	ASU 证书文件名。

【缺省配置】 无。

【命令模式】 WLAN 安全配置模式

【缺省级别】 14

【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。

【配置举例】 1：配置 ASU 证书文件为 ASU.cer。

```
Ruijie(config-wlansec)#security wapi asu cert ASU.cer
```

【检验方法】 1：使用 **show running-config** 命令，可以查看配置是否生效。

【提示信息】 1：如果设备上找不到配置的证书文件，提示错误。

```
Ruijie(config)#wlansec 1
Ruijie(config-wlansec)#security wapi enable
Ruijie(config-wlansec)#security wapi asu cert ASU.cer
Failed to set wapi ASU cert!
```

【常见错误】 -

【平台说明】 -

3.7 security wapi ca cert

配置颁发者证书。

security wapi ca cert *ca_certfile*

【参数说明】

参数	描述
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

【缺省级别】 14

【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。

【配置举例】 1：配置颁发者证书文件为 CA.cer。

```
Ruijie(config-wlansec)#security wapi ca cert CA.cer
```

【检验方法】 1：使用 **show running-config** 命令，可以查看配置是否生效。

【提示信息】 1：如果设备上找不到配置的证书文件，提示错误。

```
Ruijie(config)#wlansec 1
Ruijie(config-wlansec)#security wapi enable
Ruijie(config-wlansec)#security wapi ca cert CA.cer
Failed to set wapi CA cert!
```

【常见错误】 -

【平台说明】 -

3.8 security wapi psk

配置 WAPI 预共享密钥认证方式。
security wapi psk enable

关闭 WAPI 预共享密钥认证方式。
security wapi psk disable

【参数说明】

参数	描述
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

【缺省级别】 14

【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。

【配置举例】 1：配置 WLAN 1 的 WAPI 接入方式为预共享密钥认证。

```
Ruijie(config-wlansec)#security wapi psk enable
```

【检验方法】 1：使用 **show running-config** 命令，可以查看配置是否生效。

【提示信息】 -

【常见错误】 -

【平台说明】 -

3.9 security wapi psk set-key

配置 WAPI 预共享密钥。
security wapi psk set-key { **ascii** *ascii-key* | **hex** *hex-key* }

【参数说明】

参数	描述

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

【缺省级别】 14

【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。

【配置举例】 1：配置 WLAN 1 WAPI 预共享密钥为 12345678。

```
Ruijie(config-wlansec)#security wapi psk set-key ascii 12345678
```

【检验方法】 1：使用 **show running-config** 命令，可以查看配置是否生效。

【提示信息】 1：如果 WAPI 预共享密钥长度不足 8 个字符，则提示错误。

```
Ruijie(config-wlansec)#security wapi psk set-key ascii 1234567
Length of password should be 8-32
Failed to set wapi password!
```

【常见错误】 1：WAPI 预共享密钥长度不足 8 个或超过 32 个 ASCII 码字符。

【平台说明】 -

3.10 show wapi-sta summary

查看 WAPI 用户状态信息。
show wapi-sta summary

【参数说明】

参数	描述
-	-

【命令模式】 特权模式、全局模式、WLAN 安全配置模式

【缺省级别】 1

【使用指导】 -

【配置举例】 1：查看 WAPI 用户状态信息。

```
Ruijie#show wapi-sta summary
In the authenticated list:
authenticated sta number: 1
INDEX     STA-MAC-addr          AP-MAC-addr           WLAN ID     MODE        CUR-STATE
1         000b.c002.9cbe        021b.b120.687e        1           CERT        AUTHENTICATED
In the authenticating list:
authenticating sta number: 0
INDEX     STA-MAC-addr          AP-MAC-addr           WLAN ID     MODE        CUR-STATE
```

字段解释：

字段	说明
INDEX	序号
STA-MAC-addr	STA 的 MAC 地址
AP-MAC-addr	STA 关联的 BSSID
WLAN ID	STA 关联的 WLAN ID
MODE	STA 接入认证方式
CUR-STATE	STA 当前认证状态

【提示信息】 -

【平台说明】 -

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

命令	作用
ap-based	配置当前 AP 的上行和下行流量限速参数。
fair-schedule	开启无线 AP 的公平调度功能。
illegal-sta-check	使用 illegal-check 开启防代理检测功能。
netuser	配置基于指定用户的上行和下行流量限速参数。
show dot11 ratelimit	显示 WLAN 的限速信息。
sta-fair	配置指定用户的公平调度优先级。
wlan-based	配置当前 WLAN 的上行和下行流量限速参数。
wlan-qos ap-based	配置当前 AP 的上行和下行流量限速参数。
wlan-qos netuser	配置基于指定用户的上行和下行流量限速参数。
wlan-qos wlan-based	配置当前 WLAN 的上行和下行流量限速参数。
wqos fs enable	开启 wqos 流量统计功能
wqos radio rate-guarante	配置智能带宽保障功能

1.1 ap-based

配置当前 AP 的上行和下行流量限速参数。

ap-based { **per-user-limit** | **total-user-limit** } { **down-streams** | **up-streams** } **average-data-rate** *average-data-rate* **burst-data-rate** *burst-data-rate*

用户可以用该命令的 **no** 选项还原参数为缺省值。

no ap-based { **per-user-limit** | **total-user-limit** } { **down-streams** | **up-streams** }

配置当前 AP 的 total-user-limit 智能限速。

ap-based total-user-limit { **down-streams** | **up-streams** } **intelligent**

用户可以用该命令的 **no** 选项取消智能限速。

no ap-based total-user-limit { **down-streams** | **up-streams** } **intelligent**

【参数说明】

参数	描述
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。
down-streams	表示设置 AP 的下行流量限速参数。
up-streams	表示设置 AP 的上行流量限速参数。
intelligent	表示是否对 total-user-limit 进行智能限速。
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】 AP 配置模式。

【缺省级别】 15

【使用指导】 开启智能限速的前提是配置了 total-user-limit 限速，否者单独配置智能限速开关不会生效。。

【配置举例】 1：设置 AP wlan-ap-001 上的每个用户的下行平均速率为 800KB/s，突发速率为 1600KB/s。

```
Ruijie(config)# ap-config wlan-ap-001
Ruijie(config-ap)# ap-based per-user-limit down-streams average-data-rate 800 burst-data-rate 1600
```

【检验方法】 -

【提示信息】 -

【常见错误】 -

【平台说明】 AC

1.2 fair-schedule

开启无线 AP 的公平调度功能。
fair-schedule

用户可以用该命令的 **no** 选项关闭该功能。
no fair-schedule

【参数说明】

参数	描述
-	-

【缺省配置】 缺省开启。

【命令模式】 AC 上，AP 配置模式。
AP 配置模式。

【缺省级别】 15

【使用指导】 在胖 AP 上，配置公平调度的命令位于(config)模式下，使用 **show run** 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。

【配置举例】 1：关闭 AP 的公平调度功能。

```
Ruijie(config)# ap-config ap-name
Ruijie(ap-config)# no fair-schedule
```

【检验方法】 -

【提示信息】 -

【常见错误】 -

【平台说明】 AC、胖 AP

1.3 illegal-sta-check

使用 illegal-check 开启防代理检测功能。

illegal-sta-check ip ttl

illegal-sta-check tcp source-ports [*port-num*]

用户可以使用该命令的 **no** 命令关闭防代理检测功能。

no illegal-sta-check ip ttl

no illegal-sta-check tcp source-ports

【参数说明】

参数	描述
port-num	设置端口检测数量的上限，范围为 1 到 512，缺省 512。

【缺省配置】 缺省关闭。

【命令模式】 AP 配置模式。

【缺省级别】 15

【使用指导】 无。

【配置举例】 1：设置 ap1 开启防代理检测功能，使用 TTL 作为策略。

```
Ruijie(config)# ap-config ap1
Ruijie(config-ap)#illegal-sta-check ip ttl
```

2：设置 ap2 开启防代理检测功能，使用源端口检测作为策略，默认端口数为 512。

```
Ruijie(config)# ap-config ap2
Ruijie(config-ap)#illegal-sta-check tcp source-ports
```

【检验方法】 -

【提示信息】 -

【常见错误】 -

【平台说明】 AC、胖 AP

1.4 netuser

配置基于指定用户的上行和下行流量限速参数。

netuser *mac-address* { **inbound** | **outbound** } **average-data-rate** *average-data-rate* **burst-data-rate** *burst-data-rate*

用户可以用该命令的 **no** 选项还原参数为缺省值。

no netuser *mac-address* { **inbound** | **outbound** }

【参数说明】

参数	描述
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参数。
outbound	表示设置用户的下行流量限速参数。
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 配置模式。

【缺省级别】 15

【使用指导】 无。

【配置举例】 1：设置用户 0000.0000.0001 的上行平均速率为 800KB/s，突发速率为 1600KB/s。

```
Ruijie(config)# ac-controller
Ruijie(ac-config)# netuser 0000.0000.0001 inbound average-data-rate 800 burst-data-rate 1600
```

【检验方法】 -

【提示信息】 -

【常见错误】 -

【平台说明】 AC

1.5 show dot11 ratelimit

显示 WLAN 的限速信息。

show dot11 ratelimit { **wlan** | **ap** | **user** }

show dot11 ratelimit wlan perap

【参数说明】

参数	描述
wlan	表示显示所有 WLAN 的限速信息。
ap	表示显示所有 AP 的限速信息。
user	表示显示所有 user 的限速信息。
perap	表示限速所有 AP 的 wlan total 限速

【命令模式】 特权模式

【缺省级别】 1

【使用指导】 无。

【配置举例】 1：显示所有 AP 的限速信息。

```
Ruijie# show dot11 ratelimit ap
```

【提示信息】 -

【平台说明】 AC

1.6 sta-fair

配置指定用户的公平调度优先级。

sta-fair *mac-address* **priority** *priority*

用户可以使用该命令的 **no** 命令还原参数为缺省值。

no sta-fair *mac-address*

【参数说明】

参数	描述
mac-address	表示需要设置的用户 MAC 地址。

priority	表示优先级的数值，范围为 1-6

【缺省配置】 缺省所有的 STA 优先级为 1。

【命令模式】 AP 上，全局配置模式。
AC 上，AC 配置模式。

【缺省级别】 15

【使用指导】 无。

【配置举例】 1：在 ac 上设置用户 0000.0000.0001 的公平调度优先级为 3

```
Ruijie(config)# ac-controller
Ruijie(config-ac)# sta-fair 0000.0000.0001 priority 3
```

【检验方法】 -

【提示信息】 -

【常见错误】 -

【平台说明】 AC、胖 AP

1.7 wlan-based

配置当前 WLAN 的上行和下行流量限速参数。
wlan-based { **per-user-limit** | **total-user-limit** | **per-ap-limit** } { **down-streams** | **up-streams** } **average-data-rate** *average-data-rate* **burst-data-rate** *burst-data-rate*

用户可以用该命令的 **no** 选项还原参数为缺省值。
no wlan-based { **per-user-limit** | **total-user-limit** | **per-ap-limit** } { **down-streams** | **up-streams }**

配置当前 WLAN 的 per-ap-limit 智能限速。
wlan-based per-ap-limit { **down-streams** | **up-streams** } **intelligent**
用户可以用该命令的 **no** 选项取消智能限速。
no wlan-based per-ap-limit { **down-streams** | **up-streams }** **intelligent**

【参数说明】

参数	描述
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。

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。
intelligent	表示是否对 per-ap-limit 进行智能限速。
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 per-ap-limit 缺省不开启智能限速。

【命令模式】 WLAN 配置模式。

【缺省级别】 15

【使用指导】 开启智能限速的前提是配置了 per-ap-limit 限速，否者单独配置智能限速开关不会生效。

【配置举例】 1：设置 WLAN 1 上的每个用户的下行平均速率为 800KB/s，突发速率为 1600KB/s。

```
Ruijie(config)# wlan-config 1
Ruijie(config-ap)# wlan-based per-user-limit down-streams average-data-rate 800 burst-data-rate 1600
```

【检验方法】 -

【提示信息】 -

【常见错误】 -

【平台说明】 AC

1.8 wlan-qos ap-based

配置当前 AP 的上行和下行流量限速参数。
wlan-qos ap-based { **per-user-limit** | **total-user-limit** } { **down-streams** | **up-streams** } **average-data-rate** *average-data-rate* **burst-data-rate** *burst-data-rate*

用户可以用该命令的 **no** 选项还原参数为缺省值。
no wlan-qos ap-based { **per-user-limit** | **total-user-limit** } { **down-streams** | **up-streams** }

开启当前 AP 的 total-user-limit 智能限速。
wlan-qos ap-based total-user-limit { **down-streams** | **up-streams** } **intelligent**
用户可以用该命令的 **no** 选项取消智能限速。
no wlan-qos ap-based total-user-limit { **down-streams** | **up-streams** } **intelligent**

【参数说明】

参数	描述
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。
down-streams	表示设置 AP 的下行流量限速参数。
up-streams	表示设置 AP 的上行流量限速参数。
Intelligent	表示是否对 total-user-limit 进行智能限速。
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】 全局配置模式。

【缺省级别】 15

【使用指导】 开启智能限速的前提是配置了 total-user-limit 限速，否者单独配置智能限速开关不会生效。

【配置举例】 1：设置 AP wlan-ap-001 上的每个用户的下行平均速率为 800KB/s，突发速率为 1600KB/s。

```
Ruijie(config-ap)# wlan-qos ap-based per-user-limit down-streams average-data-rate 800
burst-data-rate 1600
```

【检验方法】 -

【提示信息】 -

【常见错误】 -

【平台说明】 胖 AP

1.9 wlan-qos netuser

配置基于指定用户的上行和下行流量限速参数。

wlan-qos netuser *mac-address* { **inbound** | **outbound** } **average-data-rate** *average-data-rate* **burst-data-rate** *burst-data-rate*

用户可以用该命令的 **no** 选项还原参数为缺省值。

no wlan-qos netuser *mac-address* { **inbound** | **outbound** }

【参数说明】

参数	描述
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参数。
outbound	表示设置用户的下行流量限速参数。
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】 全局配置模式。

【缺省级别】 15

【使用指导】 无。

【配置举例】 1：设置用户 0000.0000.0001 的上行平均速率为 800KB/s，突发速率为 1600KB/s。

```
Ruijie(ac-config)# wlan-qos netuser 0000.0000.0001 inbound average-data-rate 800 burst-data-rate 1600
```

【检验方法】 -

【提示信息】 -

【常见错误】 -

【平台说明】 胖 AP

1.10 wlan-qos wlan-based

配置当前 WLAN 的上行和下行流量限速参数。

wlan-qos wlan-based { *wlan-id* | *ssid* } { **per-user-limit** | **total-user-limit** } { **down-streams** | **up-streams** } **average-data-rate** *average-data-rate* **burst-data-rate** *burst-data-rate*

用户可以用该命令的 **no** 选项还原参数为缺省值。

no wlan-qos wlan-based { *wlan-id* | *ssid* } { **per-user-limit** | **total-user-limit**} { **down-streams** | **up-streams** }

配置当前 WLAN 的 total-user-limit 智能限速。

Wlan-qos wlan-based { *wlan-id* | *ssid* } **total-user-limit** { **down-streams** | **up-streams** } **intelligent**

用户可以用该命令的 **no** 选项取消智能限速。

no wlan-qos wlan-based { *wlan-id* | *ssid* } **total-user-limit** { **down-streams** | **up-streams }** **intelligent**

【参数说明】

参数	描述
wlan-id	WLAN 的标识。
ssid	WLAN 配置的 SSID 标识
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。
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。
Intelligent	表示是否对 total-user-limit 进行智能限速。
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】 全局配置模式。

【缺省级别】 15

【使用指导】 开启智能限速的前提是配置了 total-user-limit 限速，否者单独配置智能限速开关不会生效。

【配置举例】 1：设置 WLAN 1 上的每个用户的下行平均速率为 800KB/s，突发速率为 1600KB/s。

```
Ruijie(config-ap)# wlan-based 1 per-user-limit down-streams average-data-rate 800 burst-data-rate 1600
```

【检验方法】 -

【提示信息】 -

【常见错误】 -

【平台说明】 胖 AP

1.11 wqos fs enable

使能开启 wqos 流量统计功能。

wqos fs enable

关闭 wqos 流量统计功能。

no wqos fs enable

【参数说明】

参数	描述

【缺省配置】 缺省为不开启 wqos 流量统计功能。

【命令模式】 AC 上为 AC 配置模式， AP 上为全局配置模式。

【缺省级别】 15

【使用指导】 该命令用于补充非 WEB 认证/1X 认证环境下，开启 wqos 流量统计功能。如果已经有配置了 WEB 认证/1X 认证，则默认为开启 wqos 流量统计功能，因此通过该命令开启或者关闭 wqos 流量统计功能都无效。

【配置举例】 1：AC 上开启所关联的所有 AP 开启 WQOS 流量统计功能。

```
Ruijie(config-ac)#wqos fs enable
```

【检验方法】 -

【提示信息】 -

【常见错误】 -

【平台说明】 瘦 AP，胖 AP

1.12 wqos radio rate-guarantee

配置在 AP 组下指定 radio 开启智能带宽保障。
wqos radio *radio_id* **rate-guarantee enable**

用户可以用该命令的 **no** 选项还原参数为缺省值。
no wqos radio *radio_id* **rate-guarantee enable**

配置在 AP 组下指定 radio 在 802.11a/802.11b/802.11g/802.11n/802.11ac 射频模式下的总带宽。
wqos radio *radio_id* **rate-guarantee** { **802.11a** | **802.11b** | **802.11g** | **802.11n** | **802.11ac** } **bandwidth** *average-data-rate*

用户可以用该命令的 **no** 选项还原参数为缺省值。
no wqos radio *radio_id* **rate-guarantee** { **802.11a** | **802.11b** | **802.11g** | **802.11n** | **802.11ac** } **bandwidth**

配置 AP 组下指定 radio 关联的 wlan 保障的带宽百分比。

wqos radio *radio_id* **rate-guarantee wlan** *wlan_id* **percent** *percnet*

【参数说明】

参数	描述
radio_id	AP 的 radio id，范围 1-16
802.11a	设置 radio 在 802.11a 射频模式下的总带宽
802.11b	设置 radio 在 802.11b 射频模式下的总带宽
802.11g	设置 radio 在 802.11g 射频模式下的总带宽
802.11n	设置 radio 在 802.11n 射频模式下的总带宽
802.11ac	设置 radio 在 802.11ac 射频模式下的总带宽
average-data-rate	指定该 radio 下的总带宽，单位 KBps 802.11n 范围为 2-31250 802.11a 范围为 2-3750 802.11b 范围为 2-875 802.11g 范围为 2-3750 802.11ac 范围为 2-93750
wlan_id	该 AP 组中 radio 映射的 wlan id，AC 上范围 1-4094， 胖 AP 上范围 1-32
percnet	保障带宽百分比，范围 1-100

【缺省配置】 缺省 radio 不开启智能带宽保障，
radio 下 802.11n 默认总带宽为 31250，
radio 下 802.11a 默认总带宽为 3750，
radio 下 802.11b 默认总带宽为 875，
radio 下 802.11g 默认总带宽为 3750，
radio 下 802.11ac 默认总带宽为 93750，
radio 下的 wlan 保障带宽百分比为 0%。

【命令模式】 AC 上为 AP 组配置模式， 胖 AP 为全局配置模式。

【缺省级别】 15

【使用指导】 只有 radio 开启了智能带宽保障，之后的总带宽和带宽保障百分比才会生效。
Radio 下一旦配置了总带宽，并且开启智能带宽保障，那么 radio 的实际带宽将不超过总带宽。
配置时要求 radio 下所有 wlan 配置的带宽保障百分比之和不能超过 100%。
Radio 下的所有 wlan 会根据当前的射频模式下的总带宽和保障百分比计算出保障的绝对带宽。Radio 下带宽拥塞时该 wlan 会得到该绝对带宽的保障，不拥塞时按照 wlan 按照需要占用 radio 下的带宽资源。

【配置举例】 1：AC 上设置 ap-group1 的 radio 1 在射频模式为 802.11n 的总带宽为 5000KBps。

```
Ruijie(config)# ap-group ap-group1
Ruijie(config-group)# wqos radio 1 rate-guarantee 802.11n bandwidth 5000
```

2：AC 上设置 ap-group1 的 radio 1 下 wlan 1 的带宽保障百分比为 50%

```
Ruijie(config)# ap-group ap-group1
Ruijie(config-group)# wqos radio 1 rate-guarantee wlan 1 percent 50
```

3：AC 上设置开启 ap-group1 的 radio 1 的智能带宽保障

```
Ruijie(config)# ap-group ap-group1
```

Ruijie(config-group)# wqos radio 1 rate-guarantee enable

【检验方法】

1. AP 连接到 ap-group 上，AP 上 radio 下的总带宽不超过对应射频模式设置的额定总带宽
2. 当 radio 带宽不拥塞时，radio 下的 wlan 按照各自需要的带宽进行分配，当 radio 带宽出现拥塞时，radio 下的 wlan 严格按照配置的保障百分比进行分配。

【提示信息】

1 提示 wlan 配置的带宽百分比导致 radio 下的所以百分比之和超过 100%

```
Sum of percent in radio 1(假设 radio id 为 1) will more 100%，configure failed！
```

【常见错误】 -

【平台说明】 -

2 WMM

命令	作用
wlan-qos map-table	配置当前 WLAN 的报文优先级映射关系
wmm dot1p enable	开启 802.11p QoS 映射策略机制
wmm dot1p policy	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
wmm dscp enable	开启 dscp QoS 映射策略机制
wmm dscp policy	配置 AP 如何应用 dscp QoS 映射策略机制
wmm dscp tag	配置 dscp 标识
wmm edca-client	配置客户端的 EDCA 参数。
wmm edca-radio	配置 AP 使用的 EDCA 参数。
wmm enable	配置 AP 上开启/关闭 WMM 服务。

2.1 wlan-qos map-table

配置当前 WLAN 的报文优先级映射关系。

wlan-qos map-table { **dot11e-inner-dscp** | **dot11e-tunnel-dscp** | **dscp-dot11e** } **import** *import-tag-value* **export** *export-tag-value*

恢复默认 WLAN 的报文优先级映射关系。

no wlan-qos map-table { **dot11e-inner-dscp** | **dot11e-tunnel-dscp** | **dscp-dot11e** } **import** *import-tag-value*

【参数说明】

参数	描述
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。 WMM(dot11e)--为 802.11 无线协议头中 QOS 字段的一部分 ,表示无线的优先级，取值范围 0-7； dscp--为 IP 协议头中的优先级字段，取值范围 0-63，默认值为 0。
export *export-tag-value*	表示设置输出的报文优先级。 WMM(dot11e)--为 802.11 无线协议头中 QOS 字段的一部分 ,表示无线的优先级，取值范围 0-7； dscp--为 IP 协议头中的优先级字段，取值范围 0-63，默认值为 0。
no	表示还原报文映射关系为默认值。

【缺省配置】 dscp 到 dot11e 映射表：

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

dot11e 到 dscp 映射表：

802.11e	dscp
0	0
3	8
1	16
2	24
4	32
5	40
6	48
7	56

【命令模式】 WLAN 配置模式。

【缺省级别】 14

【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。

【配置举例】 1：设置有线报文下行映射关系为 dscp-dot11e，进入原始报文的优先级为 1，输出报文的优先级为 10。

```
Ruijie# configure terminal
Ruijie(config)# wlan-config 1
Ruijie(config-wlan)# wlan-qos map-table dscp-dot11e import 1 export 10
```

【检验方法】 1：使用 **show run** 命令，可以查看当前生效的优先级映射，默认配置时不显示。

【提示信息】 -

【常见错误】 -

【平台说明】 -

2.2 wmm dot1p enable

开启 802.11p QoS 映射策略机制。
wmm dot1p enable radio *radio-id*

关闭 802.11p QoS 映射策略机制。
no wmm dot1p enable radio *radio-id*

【参数说明】

参数	描述
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】 默认为关闭 802.11p QoS 映射策略机制。

【命令模式】 瘦 AP 下在 AP 配置模式，胖 AP 下在接口配置模式。

【缺省级别】 14

【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。

【配置举例】 1：设置开启 VOICE-AP 的 radio 1 下的 802.11p QoS 映射策略机制。

```
Ruijie# configure terminal
Ruijie(config)# ap-config VOICE-AP
Ruijie(config-ap)# wmm dot1p enable radio 1
```

【检验方法】 1：使用 **show running** 或 **show ap-config running** 命令，可以查看 802.11p QoS 映射策略是否开启，默认配置时不显示。

【提示信息】 -

【常见错误】 -

【平台说明】 -

2.3 wmm dot1p policy

配置 AP 如何应用 802.11p QoS 映射策略机制。
wmm dot1p policy 1q [*1q-policy-value*] **radio** *radio-id*

恢复默认 AP 如何应用 802.11p QoS 映射策略机制。

no wmm dot1p policy radio *radio-id*

【参数说明】

参数	描述
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。 Q=1：AP 根据下发的 802.1p 标记 802.1Q 头里面的优先级域； Q=0：AP 根据 IEEE 802.11 头的 QoS Control field 的用户优先级值标记 802.1Q 头里面的优先级域；如果 QoS Control field 在 IEEE 802.11 头没有出现，则采用‘Q=1’的方式描述处理；
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。

【命令模式】 瘦 AP 下在 AP 配置模式，胖 AP 下在接口配置模式。

【缺省级别】 14

【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。

【配置举例】 1：设置 VOICE-AP 的 radio 1 根据下发的 802.1p 标记 802.1Q 头里面的优先级域。

```
Ruijie# configure terminal
Ruijie(config)# ap-config VOICE-AP
Ruijie(config-ap)# wmm dot1p 1q 1 radio 1
```

【检验方法】 1：使用 **show running** 或 **show ap-config running**，可以查看当前应用 802.11p QoS 映射策略机制，默认配置时不显示。

【提示信息】 -

【常见错误】 -

【平台说明】 -

2.4 wmm dot1p tag

配置 802.1p 优先级。

wmm dot1p tag [*tag-value*] { **back-ground** | **best-effort** | **video** | **voice** } **radio** *radio-id*

恢复默认 802.1p 优先级。

no wmm dot1p tag { **back-ground** | **best-effort** | **video** | **voice** } **radio** *radio-id*

【参数说明】

参数	描述
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*	表示设置 802.1p 优先级的 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。

【命令模式】 瘦 AP 下在 AP 配置模式，胖 AP 下在接口配置模式。

【缺省级别】 14

【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。

【配置举例】 1：设置 VOICE-AP 的 radio 1 下的 voice 队列的 802.1p 优先级为 5。

```
Ruijie# configure terminal
Ruijie(config)# ap-config VOICE-AP
Ruijie(config-ap)# wmm dot1p tag 5 voice radio 1
```

【检验方法】 1：使用 **show running** 或 **show ap-config running**，可以查看 802.1p 优先级，默认配置时不显示。

【提示信息】 -

【常见错误】 -

【平台说明】 -

2.5 wmm dscp enable

开启 dscp QoS 映射策略机制。
wmm dscp enable radio *radio-id*

关闭 dscp QoS 映射策略机制。
no wmm dscp enable radio *radio-id*

【参数说明】

参数	描述
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】 默认为关闭 dscp QoS 策略机制。

【命令模式】 瘦 AP 下在 AP 配置模式，胖 AP 下在接口配置模式。

【缺省级别】 14

【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。

【配置举例】 1：设置开启 VOICE-AP 的 radio 1 下的 dscp QoS 映射策略机制。

```
Ruijie# configure terminal
Ruijie(config)# ap-config VOICE-AP
Ruijie(config-ap)# wmm dscp enable radio 1
```

【检验方法】 1：使用 **show running** 或 **show ap-config running**，可以查看 dscp QoS 映射策略是否开启，默认配置时不显示。

【提示信息】 -

【常见错误】 -

【平台说明】 -

2.6 wmm dscp policy

配置 AP 如何应用 dscp QoS 映射策略机制。
wmm dscp policy outer-tunnel [*outer-tunnel-value*] **inner-tunnel** [*inner-tunnel-value*] **radio** *radio-id*

恢复默认 AP 如何应用 dscp QoS 映射策略机制。

no wmm dscp policy radio *radio-id*

【参数说明】

参数	描述
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。 在集中转发模式下： O=1：AP 根据下发配置策略设置 tunnel 头 DSCP 域； O=0：AP 根据隧道内（inner）报文的 DSCP 域设置 tunnel 头 DSCP 域；如果隧道内（inner）报文被加密或不是 IPv4 报文，则采用 ‘O=1’ 描述的方式执行； 在本地转发模式下： O=1：无效值； O=0：无效值；
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。 在集中转发模式下: I=1：AP 根据下发的策略设置隧道内（inner）用户报文的 DSCP 域；如果隧道内（inner）用户报文被加密或不是 IPv4 报文，则采用 ‘I=0’ 描述的方式执行； I=0：AP 不能修改用户报文的 DSCP 域； 在本地转发模式下： I=1：AP 根据下发的策略设置用户报文的 DSCP 域； I=0：AP 不能修改用户报文的 DSCP 域；
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。

【命令模式】 瘦 AP 下在 AP 配置模式，胖 AP 下在接口配置模式。

【缺省级别】 14

【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。

【配置举例】 1：设置 VOICE-AP 的 radio 1 的 dscp 映射策略机制 outer tunnel 头为 0，inner tunnel 头为 0。

```
Ruijie# configure terminal
```

```
Ruijie(config)# ap-config VOICE-AP
Ruijie(config-ap)# wmm dscp outer-tunnel 0 inner-tunnel 0 radio 1
```

【检验方法】 1：使用 **show running** 或 **show ap-config running**，可以查看当前应用 dscp QoS 映射策略机制，默认配置时不显示。

【提示信息】 -

【常见错误】 -

【平台说明】 -

2.7 wmm dscp tag

配置 dscp 标识。
wmm dscp tag [*tag-value*] { **back-ground** | **best-effort** | **video** | **voice** } **radio** *radio-id*

恢复默认 dscp 标识。
no wmm dscp tag { **back-ground** | **best-effort** | **video** | **voice** } **radio** *radio-id*

【参数说明】

参数	描述
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。

【命令模式】 瘦 AP 下在 AP 配置模式，胖 AP 下在接口配置模式。

【缺省级别】 14

【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。

【配置举例】 1：设置 VOICE-AP 的 radio 1 下的 voice 队列的 dscp 标识为 5。

```
Ruijie# configure terminal
Ruijie(config)# ap-config VOICE-AP
Ruijie(config-ap)# wmm dscp tag 5 voice radio 1
```

【检验方法】 1：使用 **show running** 或 **show ap-config running**，可以查看 dscp 标识，默认配置时不显示。

【提示信息】 -

【常见错误】 -

【平台说明】 -

2.8 wmm edca-client

配置客户端的 EDCA 参数。

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*

恢复客户端默认 EDCA 参数。

no wmm edca-client { **back-ground** | **best-effort** | **video** | **voice** } [**length**] **radio** *radio-id*

【参数说明】

参数	描述
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】

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】 瘦 AP 下在 AP 配置模式，胖 AP 下在接口配置模式。

【缺省级别】 14

【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。

【配置举例】 1：设置 VOICE-AP 的 radio 1 下的客户端的 voice 队列 EDCA 参数为 aifsn 2 cwmin 2 cwmax 3 txop 50。

```
Ruijie# configure terminal
Ruijie(config)# ap-config VOICE-AP
Ruijie(config-ap)# wmm edca-client voice aifsn 2 cwmin 2 cwmax 3 txop 50 radio 1
```

【检验方法】 1：使用 **show running** 或 **show ap-config running**，可以查看当前生效的客户端的 EDCA 参数，默认配置时不显示。

【提示信息】 1：如果 radio 不存在，则提示错误。

```
This radio is not exist.
```

2：如果 cwmax 值小于 cwmin 值，则提示错误。

```
Cwmax must be greater than cwmin!
```

【常见错误】 1：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。

【平台说明】 -

2.9 wmm edca-radio

配置 AP 使用的 EDCA 参数。

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*

恢复 AP 使用的默认 EDCA 参数。

no wmm edca-radio { **back-groud** | **best-effort** | **video** | **voice** } [**noack**] **radio** *radio-id*

【参数说明】

参数	描述
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 AP 使用的 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】

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】 瘦 AP 下在 AP 配置模式，胖 AP 下在接口配置模式。

【缺省级别】 14

【使用指导】 wmm 服务开启时，配置的参数才能生效。

IEEE 802.11 标准规定组播、广播帧不回复 ACK。

cwmax 值必须大于 cwmin 值。否则提示配置失败。

【配置举例】 1：设置 VOICE-AP 的 radio 1 下的 AP 使用的 voice 队列 EDCA 参数为 aifsn 1 cwmin 1 cwmax 3 txop 50。

```
Ruijie# configure terminal
Ruijie(config)# ap-config VOICE-AP
Ruijie(config-ap)# wmm edca-radio voice aifsn 1 cwmin 1 cwmax 3 txop 50 radio 1
```

【检验方法】 1：使用 **show running** 或 **show ap-config running**，可以查看当前生效的 AP 使用的 EDCA 参数，默认配置时不显示。

【提示信息】 1：如果 radio 不存在，则提示错误。

```
This radio is not exist.
```

2：如果参数设置错误，则提示错误。

```
Cwmax must be greater than cwmin!
```

【常见错误】 1：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。

【平台说明】 -

2.10 wmm enable

配置 AP 上开启 WMM 服务。
wmm enable radio *radio-id*

配置 AP 上关闭 WMM 服务。
no wmm enable radio *radio-id*

【参数说明】

参数	描述
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。
no	no 表示关闭。

【缺省配置】 默认开启 WMM 服务

【命令模式】 瘦 AP 下在 AP 配置模式，胖 AP 下在接口配置模式。

【缺省级别】 14

【使用指导】 wmm 服务关闭，采用默认的优先级队列接收与映射。

【配置举例】 1：开启 VOICE-AP 的 radio1 的 wmm 服务。

```
Ruijie# configure terminal
Ruijie(config)# ap-config VOICE-AP
Ruijie(config-ap)# wmm enable radio 1
```

【检验方法】 1：使用 **show running** 或 **show ap-config running**，可以查看当前 wmm 服务是否开启，默认配置时不显示。

【提示信息】 1：如果 radio 不存在，则提示错误。

```
This radio is not exist.
```

【常见错误】 -

【平台说明】 -