

命令参考-安全

本分册介绍命令参考相关内容，包括以下章节：

1. AAA
2. RADIUS
3. TACACS+
4. 802.1x
5. SCC
6. 全局 IP+MAC 绑定
7. PASSWORD-POLICY
8. 端口安全
9. STORM-CONTROL
10. SSH
11. URPF
12. CPP
13. DHCP Snooping
14. ARP-CHECK
15. DAI
16. IP Source Guard
17. 防网关 ARP 欺骗
18. NFPP
19. DOS 保护

1 AAA

命令	作用
<u>aaa accounting commands</u>	对登录到 NAS 上的用户所执行的命令活动进行记账。
<u>aaa accounting exec</u>	对用户登录 NAS 的访问活动进行记账。
<u>aaa accounting network</u>	对用户的访问活动进行记账。
<u>aaa accounting update</u>	启用记账更新功能。
<u>aaa accounting update periodic</u>	设置已经启用记账更新功能的记账更新间隔。
<u>aaa authentication dot1x</u>	配置 802.1X 用户认证的方法列表。
<u>aaa authentication enable</u>	配置 Enable 认证的方法列表。
<u>aaa authentication login</u>	配置 Login 认证的方法列表。
<u>aaa authentication web-auth</u>	配置设备二代 Portal Web 用户认证的方法列表。
<u>aaa authorization commands</u>	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。
<u>aaa authorization config-commands</u>	对配置模式（包括全局配置模式及其子模式）下的命令进行授权的功能。
<u>aaa authorization console</u>	对通过控制台登录的用户所执行命令的授权功能。
<u>aaa authorization exec</u>	在使用 AAA 时对登录到 NAS 的 CLI 界面的用户进行 Exec 授权 赋予其权限级别。
<u>aaa authorization network</u>	在使用 AAA 时对访问网络用户的服务请求（包括 PPP、SLIP 等协议）进行授权。
<u>aaa domain</u>	进入域配置模式，配置域的属性。
<u>aaa domain enable</u>	设置基于域名的 AAA 服务总开关。
<u>aaa local authentication attempts</u>	配置 login 登录用户尝试登录失败次数。
<u>aaa local authentication lockout-time</u>	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。
<u>aaa log enable</u>	使能 AAA 用户认证通过的 syslog 打印功能。
<u>aaa log rate-limit</u>	配置 AAA 用户认证通过的 syslog 的打印速率。
<u>aaa new-model</u>	使能 RGOS 的 AAA 安全服务功能。
<u>access-limit</u>	设置域的用户数量限制，只对 IEEE802.1x 用户有效。
<u>accounting network</u>	在域配置模式下配置 Network 记账列表。
<u>authentication dot1x</u>	在域配置模式下配置 IEEE802.1x 认证列表。
<u>authorization network</u>	在域配置模式下配置 Network 授权列表。
<u>clear aaa local user lockout</u>	清除被锁定的用户列表。
<u>show aaa accounting update</u>	显示记账更新相关的信息。
<u>show aaa domain</u>	显示当前所有配置域信息。
<u>show aaa lockout</u>	显示当前 login 的锁定配置参数。
<u>show aaa group</u>	显示 AAA 配置的所有服务器组。
<u>show aaa method-list</u>	显示 AAA 所有的方法列表。
<u>show aaa user</u>	显示 AAA 用户相关信息。
<u>state</u>	设置域是否有效。
<u>username-format</u>	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。

1.1 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
<i>level</i>	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。
<i>list-name</i>	定义一个命令记账的方法列表，可以是任何字符串。
<i>method</i>	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】 -

1.2 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。
<i>list-name</i>	定义一个 Exec 记账的方法列表，可以是任何字符串。
<i>method</i>	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】 -

1.3 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。
<i>list-name</i>	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。
<i>method</i>	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】 -

1.4 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】 -

1.5 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
	<i>interval</i>	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】 -

1.6 aaa authentication dot1x

要使用 AAA 进行 802.1X 用户认证，请执行全局配置命令 **aaa authentication dot1x** 配置 802.1X 用户认证的方法列表。

aaa authentication dot1x { **default** | *list-name* } *method1* [*method2...*]

删除 802.1X 用户认证的方法列表。

no aaa authentication dot1x { 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 802.1X 用户认证的默认方法。
	<i>list-name</i>	定义一个 802.1X 用户认证的方法列表，可以是任何字符串。
	<i>method</i>	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
【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 802.1X 安全服务，用户就必须使用 AAA 进行 802.1X 用户认证协商。您必须使用 aaa authentication dot1x 命令配置默认的或可选的方法列表用于 802.1X 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】	下面的示例定义一个名为 rds_d1x 的 AAA 802.1X 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。 <pre>Ruijie(config)# aaa authentication dot1x rds_d1x group radius local</pre>	
【检验方法】	使用 show aaa method-list 命令可以查看已配置的 802.1X 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。 <pre>%Group XXX is not existed</pre>	
	2：如果 group 类型不支持此认证类型，则提示错误。 <pre>The authentication does not support this type of group</pre>	
	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】	-	

1.7 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。
<i>method</i>	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】 -

1.8 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。
<i>list-name</i>	定义一个 Login 认证的方法列表，可以是任何字符串。
<i>method</i>	必须是“local、none、group”所列关键字之一，一个方法列表最多有 4 个方法
local	使用本地用户名数据库进行身份认证
none	不进行身份认证
group	使用服务器组进行身份认证，目前支持 RADIUS 和 TACACS+服务器组

【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】 -

1.9 aaa authentication web-auth

要使用 AAA 进行二代 Web 认证，请执行全局配置命令 **aaa authentication web-auth** 配置设备二代 Web 认证的方法列表。

```
aaa authentication web-auth { default | list-name } method1 [ method2...]
```

删除认证的方法列表。

```
no aaa authentication web-auth { 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二代 Web 认证的默认方法。
	<i>list-name</i>	定义一个设备二代 Web 认证的方法列表，可以是任何字符串。
	<i>method</i>	必须是“none、group”所列关键字之一，一个方法列表最多有 4 个方法
	none	不进行身份认证
	group	使用服务器组进行认证，目前支持 RADIUS 服务器组

【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 设备二代 Web 安全服务，用户就必须使用 AAA 进行设备二代 Web 用户认证协商。您必须使用 **aaa authentication web-auth** 命令配置默认的或可选的方法列表用于设备二代 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 设备二代 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，则直接放行，认证通过。

```
Ruijie(config)# aaa authentication web-auth rds_web group radius none
```

【检验方法】 使用 **show aaa method-list** 命令可以查看已配置的 web-auth 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】 -

1.10 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	描述
<i>level</i>	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
<i>list-name</i>	定义一个命令授权的方法列表，可以是任何字符串。
<i>method</i>	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】 -

1.11 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】 -

1.12 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】 -

1.13 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。
<i>list-name</i>	定义一个 Exec 授权的方法列表，可以是任何字符串。
<i>method</i>	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】 -

1.14 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。
<i>method</i>	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】 -

1.15 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
	<i>domain-name</i>	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】 -

1.16 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】 -

1.17 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
	<i>max-attempts</i> :	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	
	<pre>Ruijie# configure terminal Ruijie(config)# aaa local authentication attempts 6</pre>	
【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】	-	

1.18 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
	<i>lockout-time</i>	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	
	<pre>Ruijie# configure terminal</pre>	

```
Ruijie(config)# aaa local authentication logout-time 5
```

【检验方法】 使用 **show aaa logout** 命令查看锁定配置信息。

【提示信息】 -

【常见错误】 -

【平台说明】 -

1.19 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】 不打印 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。因特殊需要时，通过配置本命令来使能打印功能。

【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】 -

1.20 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
	<i>num</i>	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】 -

1.21 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。	
	<pre>Ruijie(config)# aaa new-model</pre>	
【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】	-	

1.22 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
	<i>num</i>	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】 -

1.23 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】 -

1.24 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
<i>list-name</i>	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】 -

1.25 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
<i>list-name</i>	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】 -

1.26 clear aaa local user logout

清除被锁定的用户列表。

clear aaa local user logout { 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 logout 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】 -

1.27 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】 -

1.28 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
<i>domain-name</i>	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】 -

1.29 show aaa logout

显示当前 login 的锁定配置参数。

show aaa logout

【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 logout
Lock tries:      3
Lock timeout:   15 minutes
```

【提示信息】 -

【平台说明】 -

1.30 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】 -

1.31 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 authorizing network default group radius
```

【提示信息】 -

【平台说明】 -

1.32 show aaa user

显示 aaa 用户相关信息。

show aaa user { all | logout | 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
	logout	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 logout

Name                                     Tries      Lock      Timeout (min)
-----
Ruijie#
```

【提示信息】 -

【平台说明】 -

1.33 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】 -

1.34 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：	
	<pre>Ruijie(config)# aaa domain ruijie.com Ruijie(config-aaa-domain)# username-domain without-domain</pre>	
【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】	-	

2 RADIUS

命令	作用
aaa group server radius	配置 RADIUS 类型的 AAA 服务器组。
ip radius source-interface	指定 RADIUS 报文的源地址。
ip vrf forwarding	为 AAA 服务器组选择 vrf。
radius attribute	配置私有属性类型值。
radius vendor-specific extend	扩展为不区别私有厂商 id 。
radius-server account update retransmit	配置二代 Web 认证用户的记账更新报文进行重传的功能
radius-server attribute 31	指定 RADIUS Calling-Station-ID 属性（基于 MAC）的格式。
radius-server dead-criteria	配置设备判定 RADIUS 安全服务器不可达的标准。
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 host	指定 RADIUS 安全服务器主机。
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 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 source-port	配置设备发送 RADIUS 报文的源端口。
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 set qos cos	设置 radius 下发的 qos 值为接口 cos 值。
radius support cui	设置 radius 支持 cui 属性
server auth-port acct-port	添加 AAA 服务器组的服务器。
show radius parameter	显示 RADIUS 服务器全局参数。
show radius acct statistics	显示 RADIUS 计费相关统计信息。
show radius auth statistics	显示 RADIUS 认证相关统计信息。
show radius group	显示 RADIUS 服务器组的配置。
show radius parameter	显示 RADIUS 服务器全局参数。
show radius server	显示 RADIUS 服务器配置情况。
show radius vendor-specific	显示 RADIUS 私有属性类型配置。

2.1 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

<i>name</i>	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】 -

2.2 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
	<i>interface-name</i>	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。如果被指定的接口在某个 vrf 域中，则发送报文时使用这个 vrf 域的路由寻路。
【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】	-

2.3 ip vrf forwarding

为 AAA 服务器组选择 vrf。 ip vrf forwarding vrf_name		
删除 AAA 服务器组选择的 vrf no ip vrf forwarding		
【参数说明】	参数	描述
	vrf_name	vrf 名字
【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】	为指定服务器组选择 vrf。	
【配置举例】	1：下面示例为服务器组 ss 选择 vrf 为 vrf_name。 Ruijie(config)# aaa group server radius ss	

```
Ruijie(config-gs-radius)# server 192.168.4.12
Ruijie(config-gs-radius)# server 192.168.4.13
Ruijie(config-gs-radius)# ip vrf forwarding vrf_name
Ruijie(config-gs-radius)# end
```

【检验方法】 使用 **show radius group** 命令查看 RADIUS 类型服务器组的 vrf 配置信息。

【提示信息】 -

【常见错误】 -

【平台说明】 -

2.4 radius attribute

配置私有属性类型值。

radius attribute { *id* | **down-rate-limit** | **dscp** | **mac-limit** | **up-rate-limit** } **vendor-type** *type*

恢复默认私有属性类型值。

no radius attribute { *id* | **down-rate-limit** | **dscp** | **mac-limit** | **up-rate-limit** } **vendor-type**

【参数说明】

参数	描述
<i>id</i>	功能 id <1-255>
<i>type</i>	私有属性 type <1-255>

【缺省配置】 只对我司私有属性识别默认配置：

id	功能	type
1	max down-rate	1
2	q s	2
3	user ip	3
4	vlan id	4
5	ersion to client	5
6	net ip	6
7	user name	7
8	password	8
9	file-directory	9

10	file-count	10
11	file-name-0	11
2	file-name-	12
13	file-name-2	13
14	file-name-3	14
15	file-name-4	15
16	max up-rate	16
17	version to server	17
18	flux-max-high32	18
19	flux-max-low32	19
20	proxy-avoid	20
21	dailup-avoid	21
22	ip privilege	22
23	login privilege	42

扩展情况：

id	功能	type
1	max down-rate	76
2	qos	77
3	user ip	3
4	vlan id	4
5	version to client	5
6	net ip	6
7	user name	7
8	password	8
9	file-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-	15

16	max up-rate	75
17	version to server	17
18	flux-max-high32	18
19	flux-max-low32	19
20	proxy-avoid	20
21	dailup-avoid	21
22	ip privilege	22
23	login privilege	42
24	limit to user number	50

【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私有属性类型值，以适应不同的应用场合。

【配置举例】 1：将 max up-rate 类型值定义为 211。

```
Ruijie(config)# radius attribute 16 vendor-type 211
```

【检验方法】 使用 **show radius vendor-specific** 查看私有属性类型值的配置情况。

【提示信息】 1：如果配置的 id 不在预定义的范围，则提示错误。

```
no application for the id
```

2：如果类型值已经被其他的属性所使用，则提示错误

```
the vendor type had allocated by XXXX
```

【常见错误】 -

【平台说明】 -

2.5 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】	-	

2.6 radius-server account update retransmit

配置二代 Web 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】	配置二代 Web 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：配置二代 Web 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】 -

2.7 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	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】 -

2.8 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】 -

2.9 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
	<i>minutes</i>	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】 -

2.10 radius-server host

指定 RADIUS 安全服务器主机。

```
radius-server host [ oob ] [ via mgmt-name ] { 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 [via mgmt-name]	oob 认证，即向此服务器发送报文时源接口为 mgmt 口。
<i>ipv4-address</i>	RADIUS 安全服务器主机的 IPv4 地址。
<i>ipv6-address</i>	RADIUS 安全服务器主机的 IPv6 地址。
auth-port <i>port-number</i>	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 <i>port-number</i>	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 <i>name</i>	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 <i>time</i>	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] <i>text-string</i>	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，否则使用该 RADIUS 服务器组所对应的 vrf 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】 -

2.11 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
	<i>text-string</i>	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】 -

2.12 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
<i>retries</i>	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】 -

2.13 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
	<i>port</i>	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】 -

2.14 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
	<i>seconds</i>	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】 -

2.15 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】 -

2.16 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】 -

2.17 server auth-port acct-port

添加 AAA 服务器组的服务器，**no** 形式删除。

server { *ipv4-addr* | *ipv6-addr* } [**auth-port** *port1*] [**acct-port** *port2*]

no server { *ipv4-addr* | *ipv6-addr* } [**auth-port** *port1*] [**acct-port** *port2*]

【参数说明】	参数	描述
	<i>ip-addr</i>	服务器 ip 地址
	<i>ipv6-addr</i>	服务器 ipv6 地址
	<i>port1</i>	服务器认证端口
	<i>port2</i>	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】 -

2.18 show radius acct statistics

显示 RADIUS 计费相关统计信息。

show 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】

-

2.19 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
Unknown type Msgs..... 0
Other Drops..... 0
```

【提示信息】 -

【平台说明】 -

2.20 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
```

【提示信息】 -

【平台说明】 -

2.21 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 Timeout: 5 Seconds
Server Deadtime: 0 Minutes
Server Retries: 3
Server Dead Criteria:
Time: 10 Seconds
Tries: 10
```

【提示信息】 -

【平台说明】 -

2.22 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】 -

2.23 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-suppliant-v ersion	17
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
26	ipv6-multicast-addre ss	79
27	ipv4-multicast-addre ss	87

【提示信息】 -

【平台说明】 -

3 TACACS+

命令	作用
<u>aaa group server tacacs+</u>	配置 TACACS+服务器组，将不同的 TACACS+服务器划分到不同的组。
<u>ip tacacs source-interface</u>	指定 TACACS+报文的源地址。
<u>ip oob</u>	为 AAA 服务器组选择管理口
<u>ip vrf forwarding</u>	配置 TACACS+服务器组使用的 vrf 名字(支持 VRF 的设备存在此命令)。
<u>server</u>	添加 TACACS+服务器组的服务器。
<u>show tacacs</u>	显示和各 TACACS+服务器的交互运行情况。
<u>tacacs-server host</u>	配置 TACACS+服务器主机 IP 地址。
<u>tacacs-server key</u>	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口令。
<u>tacacs-server timeout</u>	配置设备与 TACACS+服务器通信时，等待服务器的全局超时时间。

3.1 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
<i>group-name</i>	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】 -

3.2 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
	<i>interface-name</i>	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。如果被指定的接口在某个 vrf 域中，则发送报文时使用这个 vrf 域的路由寻路。
- 【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】 -

3.3 ip vrf forwarding

此命令配置 TACACS+服务器组使用的 VRF 名字(支持 VRF 的设备存在此命令)。

ip vrf forwarding vrf_name

删除 TACACS+服务器组选择 VRF

no ip vrf forwarding

【参数说明】

参数	描述
vrf_name	VRF 名字

【缺省配置】

-

【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 VRF，必须是在全局配置模式下通过 **vrf definition** 命令配置合法 VRF 名字。

【配置举例】

1：为 TACACS+服务器组 ss 选择 VRF 为 vrf_name。

```
Ruijie(config)# aaa group server tacacs+ ss
Ruijie(config-gs-tacacs+)# server 1.1.1.1
Ruijie(config-gs-tacacs+)# ip vrf forwarding vrf_name
```

【检验方法】

使用命令 **show running-config** 可以查看服务器组的 ip vrf 配置信息。

【提示信息】

1：如果指定的 VRF 名超过长度限制，则提示错误。

```
Name is too long
```

2：如果指定的 VRF 尚未配置，则提示错误。

```
Invalid vrf
```

【常见错误】

-

【平台说明】

-

3.4 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
<i>ipv4-address</i>	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】

-

3.5 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】 -

3.6 tacacs-server host

此命令配置 TACACS+服务器的相关信息。

tacacs-server host [*oob*] [*via mgmt-name*] *ipv4-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
	<i>ipv4-address</i>	TACACS+服务器的 IPv4 地址。
	oob [<i>via mgmt-name</i>]	TACACS+通信使用的源接口为 mgmt 口，默认为使用非 mgmt 口进行通信。配置 oob，via 用于指定具体的 mgmt 口，没有指定默认为 mgmt0 口。
	port <i>integer</i>	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 <i>integer</i>	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 <i>string</i>	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】

-

3.7 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
<i>text-string</i>	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】 -

3.8 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
	<i>seconds</i>	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】 -

4 802.1x

命令	作用
<u>aaa authorization ip-auth-mode</u>	配置 ip 授权模式
<u>clear dot1x user all</u>	删除设备上所有的 dot1x 认证用户
<u>clear dot1x user id</u>	删除相应 session id 的 dot1x 认证用户
<u>clear dot1x user mac</u>	删除相应 mac 的 dot1x 认证用户
<u>clear dot1x user name</u>	删除相应用户名的 dot1x 认证用户
<u>dot1x accounting</u>	配置记账方法列表
<u>dot1x auth-mode</u>	配置认证模式(eap/chap/pap)
<u>dot1x auth-address-table address</u>	配置可认证主机列表
<u>dot1x authentication</u>	配置认证方法列表
<u>dot1x auto-reg</u>	配置设备主动发起 802.1x 认证
<u>dot1x auto-reg packet-num</u>	配置设备主动发起认证请求报文的个数
<u>dot1x auto-reg req-interval</u>	配置设备主动发起认证请求报文的间隔
<u>dot1x auto-reg user-detect</u>	配置主动认证检测是否有用户在认证
<u>dot1x client-probe enable</u>	配置锐捷客户端在线检测
<u>dot1x critical</u>	配置服务器失效旁路认证
<u>dot1x critical recovery action reinitialize</u>	配置服务器失效旁路认证恢复处理
<u>dot1x dbg-filter</u>	针对特定的 mac 地址打印调试信息。
<u>dot1x default-user-limit</u>	配置接口下的可认证用户数限制
<u>dot1x dhcp-before-acct enable</u>	配置用户获取 IP 之后发起记账
<u>dot1x dhcp-before-acct timeout</u>	配置用户认证通过之后，允许等待该用户获取 IP 的时间
<u>dot1x mac-auth-bypass</u>	配置单 MAB 认证
<u>dot1x mac-auth-bypass multi-user</u>	配置多 MAB 认证
<u>dot1x mac-auth-bypass timeout-activity</u>	配置 MAB 认证超时时间
<u>dot1x mac-auth-bypass violation</u>	配置 MAB 违例
<u>dot1x mac-auth-bypass vlan</u>	配置 MAB VLAN
<u>dot1x max-reg</u>	配置 request/challenge 报文重传次数
<u>dot1x multi-account enable</u>	配置支持一个 mac 使用多账号认证
<u>dot1x multi-mab quiet-period</u>	配置多 MAB 认证失败后的静默时间
<u>dot1x port-control auto</u>	配置端口上的 802.1x 认证
<u>dot1x probe-timer interval</u>	配置锐捷客户端检测周期
<u>dot1x probe-timer alive</u>	配置锐捷客户端检测时长
<u>dot1x private-supPLICANT-only</u>	配置过滤非锐捷客户端功能
<u>dot1x pseudo source-mac</u>	配置设备使用虚拟 mac 作为设备发出的 802.1x 报文的源 mac 地址
<u>dot1x redirect</u>	配置二代 su 升级功能，通过浏览器重定向到指定的资源网站下载 supplicant 软件

dot1x reauth-max	配置 request/id 报文重传次数
dot1x re-authentication	配置重认证功能
dot1x timeout re-authperiod	配置重认证间隔
dot1x timeout quiet-period	配置认证失败后的静默时间
dot1x timeout supp-timeout	配置 request/challenge 报文重传间隔
dot1x timeout server-timeout	配置服务器超时时间
dot1x timeout tx-period	配置 request/id 报文重传间隔
show dot1x	查看 802.1x 功能状态和协议参数
show dot1x auth-address-table	查看可认证主机列表
show dot1x auto-reg	查看主动认证状态
show dot1x max-reg	查看 request/challenge 报文重传次数
show dot1x port-control	查看受控口信息
show dot1x private-supplicant-only	查看过滤非锐捷客户端开关状态
show dot1x probe-timer	查看客户端探测功能状态和参数
show dot1x re-authentication	查看重认证开关状态
show dot1x reauth-max	查看 request/id 报文重传次数
show dot1x summary	查看认证用户表项信息
show dot1x timeout quiet-period	查看认证失败后的静默时间
show dot1x timeout re-authperiod	查看重认证间隔
show dot1x timeout server-timeout	查看服务器超时时间
show dot1x timeout supp-timeout	查看 request/challenge 报文重传间隔
show dot1x timeout tx-period	查看 request/id 报文重传间隔
show dot1x user id	根据用户 id 查看用户详细信息
show dot1x user mac	根据用户 mac 查看用户详细信息
show dot1x user name	根据用户名查看用户详细信息

4.1 aaa authorization ip-auth-mode

配置 ip 授权模式。

aaa authorization ip-auth-mode { disable | supplicant | radius-server | dhcp-server }

【参数说明】	参数	描述
	disable	关闭授权
	supplicant	Supplicant 提供 ip 地址实现绑定
	radius-server	Radius 服务器下发 ip 地址绑定
	dhcp-server	dhcp 分配 ip 地址绑定
	mixed	混合模式绑定 ip
【缺省配置】	disable。	

【命令模式】 全局模式

- 【缺省级别】

15
- 【使用指导】

supplicant 授权模式仅支持锐捷 supplicant。
radius-server 授权模式需要服务器支持通过 framed-ip 属性下发 ip 地址。
dhcp-server 授权模式需要设备同时开启 dhcp snooping 或者开启 dhcp relay。
同时存在多种授权模式时可以使用 mixed 授权模式
- 【配置举例】

1：配置 supplicant 授权 ip。

Ruijie(config)# aaa authorization ip-auth-mode supplicant
- 【检验方法】

1：使用 **show running-config** 查看配置。
- 【提示信息】

-
- 【常见错误】

对于交换机设备，ip 授权会占用硬件资源，网络中的用户规模以及多种安全功能共用，都有可能导致硬件资源不够，最终的表现就是用户无法使用网络。
- 【平台说明】

-

4.2 clear dot1x user all

删除设备上所有的 dot1x 用户。
clear dot1x user all

- 【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】

使用该命令可以将设备上所有的 dot1x 认证用户删除。
- 【配置举例】

1：删除所有的 dot1x 认证用户。

Ruijie#clear dot1x user all
- 【提示信息】

-

【平台说明】 -

4.3 clear dot1x user id

根据 dot1x 用户的 session id 来删除相应的用户。

clear dot1x user id *session-id*

【参数说明】	参数	描述
	- <i>session-id</i>	-dot1x 认证用户的 session id

【缺省配置】	-
--------	---

【命令模式】 特权模式

【缺省级别】 15

【使用指导】 需要将特定的 session id 的 dot1x 认证用户删除时，可以使用此命令。

【配置举例】 1：删除 session id 为 12345678 的 dot1x 认证用户。

```
Ruijie#clear dot1x user id 12345678
```

【提示信息】 -

【平台说明】 -

4.4 clear dot1x user mac

根据 dot1x 用户的 mac 来删除相应的用户。

clear dot1x user mac *mac-addr*

【参数说明】	参数	描述
	- <i>mac-addr</i>	-dot1x 认证用户的 MAC 地址

【缺省配置】	-
--------	---

【命令模式】 特权模式

【缺省级别】 15

【使用指导】 需要将特定的 mac 地址的的 dot1x 认证用户删除时，可以使用此命令。

【配置举例】 1：删除 mac 地址为 0012.3456.789A 的 dot1x 认证用户。

```
Ruijie#clear dot1x user mac 0012.3456.789A
```

【提示信息】 -

【平台说明】 -

4.5 clear dot1x user name

根据 dot1x 用户的用户名来删除相应的用户。

clear dot1x user name *name-str*

【参数说明】

参数	描述
- <i>name-str</i>	-dot1x 认证用户的用户名

【缺省配置】

-

【命令模式】 特权模式

【缺省级别】 15

【使用指导】 需要将特定的用户名的的 dot1x 认证用户删除时，可以使用此命令。

【配置举例】 1：删除用户名为 dot1x-user 的 dot1x 认证用户。

```
Ruijie#clear dot1x user name dot1x-user
```

【提示信息】 -

【平台说明】 -

4.6 dot1x accounting

配置认证方法列表。

dot1x accounting *list-name*

【参数说明】	参数	描述
	<i>list-name</i>	记账方法列表
【缺省配置】	-	
【命令模式】	全局模式	
【缺省级别】	15	
【使用指导】	如果 aaa 的 dot1x 记账方法不是默认的，需要使用此命令来配置相应的记账方法。	
【配置举例】	1：配置可认证主机列表。	
	<pre>Ruijie(config)# dot1x accounting dot1x-acct</pre>	
【提示信息】	-	
【平台说明】	-	

4.7 dot1x auth-mode

配置认证模式。

dot1x auth-mode { eap | chap | pap }

【参数说明】	参数	描述
	-	默认 eap
【缺省配置】	eap 模式	
【命令模式】	全局模式	
【缺省级别】	15	
【使用指导】	认证模式的选择取决于 supplicant 和认证服务器的支持情况。	
【配置举例】	1：配置 chap 认证模式。	
	<pre>Ruijie(config)# dot1x auth-mode eap</pre>	
【提示信息】	-	
【平台说明】	-	

4.8 dot1x auth-address-table address

配置可认证主机列表。

dot1x auth-address-table address *mac-addr* **interface** *interface*

【参数说明】	参数	描述
	<i>mac-addr</i>	可认证的接入终端的 mac 地址
	<i>interface</i>	接入终端所在的端口

【缺省配置】	-
--------	---

【命令模式】	全局模式
--------	------

【缺省级别】	15
--------	----

【使用指导】	限定指定端口只有指定的 mac 地址的终端才可以进行 802.1x 认证。
--------	---------------------------------------

【配置举例】	1：配置可认证主机列表。
	<pre>Ruijie(config)# dot1x auth-address-table 00d0.f800.0cb2 interface fastethernet 0/1</pre>

【提示信息】	-
--------	---

【平台说明】	-
--------	---

4.9 dot1x authentication

配置认证方法列表。

dot1x authentication *list-name*

【参数说明】	参数	描述
	<i>list-name</i>	认证方法列表

【缺省配置】	-
--------	---

【命令模式】	全局模式
--------	------

【缺省级别】	15
--------	----

【使用指导】	如果 aaa 的 dot1x 认证方法不是默认的，需要使用此命令来配置相应的认证方法。
--------	---

【配置举例】 1：配置可认证主机列表。

```
Ruijie(config)# dot1x authentication dot1x-authen
```

【提示信息】 -

【平台说明】 -

4.10 dot1x auto-req

配置设备主动发起 802.1x 认证。

dot1x auto-req

关闭主动认证

no dot1x auto-req

【参数说明】	参数	描述
	-	默认关闭

【缺省配置】	缺省关闭
--------	------

【命令模式】 全局模式

【缺省级别】 15

【使用指导】 部署 MAB 环境必须开启该功能，终端使用操作系统自带认证客户端可以选择打开该功能。

【配置举例】 1：配置主动认证。

```
Ruijie(config)# dot1x auto-req
```

【提示信息】 -

【平台说明】 -

4.11 dot1x auto-req packet-num

配置设备主动发起认证请求报文的个数。

dot1x auto-req packet-num num

【参数说明】	参数	描述
	num	主动认证发送的报文个数，默认值是 0，表示一直发送，配置范围

	0-1000000
【缺省配置】	0
【命令模式】	全局模式
【缺省级别】	15
【使用指导】	-
【配置举例】	1：配置主动认证报文请求的个数。 Ruijie(config)# dot1x auto-req packet-num 100
【提示信息】	-
【平台说明】	-

4.12 dot1x auto-req req-interval

配置设备主动发起认证请求报文的间隔。

dot1x auto-req req-interval time

【参数说明】	参数	描述
	Time	主动认证发送的报文间隔，默认值是 30 秒，配置范围 10-3600
【缺省配置】	0	
【命令模式】	全局模式	
【缺省级别】	15	
【使用指导】	-	
【配置举例】	1：配置主动认证报文请求间隔。 Ruijie(config)# dot1x auto-req req-interval 50	
【提示信息】	-	
【平台说明】	-	

4.13 dot1x auto-req user-detect

配置主动认证检测是否有用户在认证。

dot1x auto-req user-detect

关闭主动认证检测是否有用户在认证。

no dot1x auto-req user-detect

【参数说明】

参数	描述
-	默认关闭

【缺省配置】

缺省关闭

【命令模式】

全局模式

【缺省级别】

15

【使用指导】

端口下单用户时建议打开该功能，可以减小对服务器造成的认证压力。

【配置举例】

1：配置主动认证检测是否有用户在认证。

```
Ruijie(config)# dot1x auto-req user-detect
```

【提示信息】

-

【平台说明】

-

4.14 dot1x client-probe enable

配置锐捷客户端在线检测。

dot1x client-probe enable

关闭锐捷客户端在线检测。

no dot1x client-probe enable

【参数说明】

参数	描述
-	默认关闭

【缺省配置】

缺省关闭

【命令模式】

全局模式

【缺省级别】 15

【使用指导】 使用锐捷 supplicant 时建议打开该功能。

【配置举例】 1：配置锐捷客户端在线检测。

```
Ruijie(config)# dot1x client-probe enable
```

【提示信息】 -

【平台说明】 -

4.15 dot1x critical

配置服务器失效旁路认证。

dot1x critical

关闭服务器失效旁路认证。

no dot1x critical

【参数说明】

参数	描述
-	

【缺省配置】 缺省关闭

【命令模式】 接口模式

【缺省级别】 15

【使用指导】 RADIUS 需要同时配置检测服务器可达的帐号和判断服务器不可达的标准。

【配置举例】 1：配置服务器失效旁路认证。

```
Ruijie(config-if-GigabitEthernet 0/5)#dot1x critical
```

【提示信息】 -

【平台说明】 -

4.16 dot1x critical recovery action reinitialize

配置服务器失效旁路认证恢复处理。

dot1x critical recovery action reinitialize

关闭服务器失效旁路认证恢复处理。

no dot1x critical recovery action reinitialize

【参数说明】	参数	描述
	-	
【缺省配置】	缺省关闭	
【命令模式】	接口模式	
【缺省级别】	15	
【使用指导】	需要在 RADIUS 服务器恢复可达的时候，重新验证服务器不可达期间授权的用户是否有合法身份，可以使用此命令。	
【配置举例】	1：配置服务器失效旁路认证恢复处理。	
	Ruijie(config-if-GigabitEthernet 0/5)#dot1x critical recovery action reinitialize	
【提示信息】	-	
【平台说明】	-	

4.17 dot1x dbg-filter

针对特定的 mac 地址打印调试信息。

dot1x dbg-filter H.H.H

清除调试过滤器信息。

no dot1x dbg-filter H.H.H

【参数说明】	参数	描述
	H.H.H	需要输出调试信息的用户的 Mac 地址
【缺省配置】	所有认证用户的调试信息均打印	

【命令模式】	全局模式
【缺省级别】	15
【使用指导】	网络中有大量用户且需要在当前网络中定位故障时，可以通过该命令对个别用户打印调试信息，避免设备打印太多调试信息。
【配置举例】	1：配置特定的 mac 地址打印调试信息。 <pre>Ruijie(config)# dot1x dbg-filter 00d0.f800.0001</pre>
【提示信息】	-
【平台说明】	-

4.18 dot1x default-user-limit

	配置接口下的可认证用户数限制。 dot1x default-user-limit num	
	恢复默认值。 no dot1x default-user-limit	
【参数说明】	参数	描述
	num	限制一个接口下有可认证用户数。参数范围 1-1000000。默认 1000000
【缺省配置】	1000000	
【命令模式】	接口模式	
【缺省级别】	15	
【使用指导】	如果要限制一个端口下的可认证用户数，可以通过该命令限制。默认值表示 4 字节可记录的最大用户数。	
【配置举例】	1：配置接口下的可认证用户数。 <pre>Ruijie(config-if)# dot1x default-user-limit 10</pre>	
【提示信息】	-	
【平台说明】	-	

4.19 dot1x mac-auth-bypass

配置单 MAB 认证。

dot1x mac-auth-bypass

关闭单 MAB 认证。

no dot1x mac-auth-bypass

【参数说明】

参数	描述
-	默认关闭

【缺省配置】

缺省单 mab 功能关闭

【命令模式】

接口模式

【缺省级别】

15

【使用指导】

端口下联单个哑终端时使用该功能。

【配置举例】

1：配置单 MAB 认证。

```
Ruijie(config-if-GigabitEthernet 0/0)# dot1x mac-auth-bypass
```

【提示信息】

-

【平台说明】

-

4.20 dot1x mac-auth-bypass multi-user

配置多 MAB 认证。

dot1x mac-auth-bypass multi-user

关闭多 MAB 认证。

no dot1x mac-auth-bypass multi-user

【参数说明】

参数	描述
-	默认关闭

【缺省配置】

缺省多 MAB 功能关闭

【命令模式】

接口模式

【缺省级别】 15

【使用指导】 端口下联多个哑终端时使用该功能。

【配置举例】 1：配置多 MAB 认证。

```
Ruijie(config-if-GigabitEthernet 0/0)# dot1x mac-auth-bypass multi-user
```

【提示信息】 -

【平台说明】 -

4.21 dot1x mac-auth-bypass timeout-activity

配置 MAB 认证超时时间。
dot1x mac-auth-bypass timeout-activity time

【参数说明】	参数	描述
	time	MAB 用户可在线时间，单位秒，默认 0，表示可以一直在线。配置范围 1-65535

【缺省配置】	0 秒
--------	-----

【命令模式】 接口模式

【缺省级别】 15

【使用指导】 限制哑终端可访问网络时间可配置该参数。

【配置举例】 1：配置 MAB 认证超时时间。

```
Ruijie(config-if-GigabitEthernet 0/0)# dot1x mac-auth-bypass timeout-activity 3600
```

【提示信息】 -

【平台说明】 -

4.22 dot1x mac-auth-bypass violation

配置 MAB 违例。
dot1x mac-auth-bypass violation

关闭 MAB 违例

no dot1x mac-auth-bypass violation

【参数说明】	参数	描述
	-	-
【缺省配置】	缺省关闭	
【命令模式】	接口模式	
【缺省级别】	15	
【使用指导】	限制一个端口下哑终端为 1 个时可配置该功能，仅适用于单 MAB 环境。	
【配置举例】	1：配置 MAB 违例。	
	Ruijie(config-if-GigabitEthernet 0/0)# dot1x mac-auth-bypass violation	
【提示信息】	-	
【平台说明】	-	

4.23 dot1x mac-auth-bypass vlan

配置 MAB VLAN。

dot1x mac-auth-bypass vlan *vlan-list*

关闭 MAB VLAN

no dot1x mac-auth-bypass vlan *vlan-list*

【参数说明】	参数	描述
	- <i>vlan-list</i>	-允许进行 MAB 认证的 VLAN 列表
【缺省配置】	缺省关闭	
【命令模式】	接口模式	
【缺省级别】	15	
【使用指导】	仅允许接口上部分 VLAN 内的用户可以进行 MAB 认证时，可以配置此命令。	

【配置举例】 1：配置 MABVLAN。

```
Ruijie(config-if-GigabitEthernet 0/0)# dot1x mac-auth-bypass vlan 5, 8-20
```

【提示信息】 -

【平台说明】 -

4.24 dot1x max-req

配置 request/challenge 报文重传次数。

dot1x max-req num

【参数说明】	参数	描述
	num	request/challenge 报文重传次数，默认 3，配置范围 1-10

【缺省配置】	3
--------	---

【命令模式】 全局模式

【缺省级别】 15

【使用指导】 使用默认值即可。

【配置举例】 1：配置 request/challenge 报文重传次数。

```
Ruijie(config)# dot1x max-req 2
```

【提示信息】 -

【平台说明】 -

4.25 dot1x multi-account enable

配置支持一个 mac 使用多账号认证。

dot1x multi-account enable

关闭支持一个 mac 使用多账号认证

no dot1x multi-account 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】 15

【使用指导】 终端在认证过程或者重认证过程中会切换用户名的，需要配置该命令。典型的，在 windows 的域认证中存在这种应用。

【配置举例】 1：配置支持一个 mac 使用多账号认证。

```
Ruijie(config)# dot1x multi-account enable
```

【提示信息】 -

【平台说明】 -

4.26 dot1x multi-mab quiet-period

配置多 MAB 认证失败后的静默时间。

dot1x multi-mab quiet-period time

【参数说明】	参数	描述
	<i>time</i>	多 MAB 认证失败后的静默时间，单位秒，默认 30，表示不静默。配置范围 0-65535，配置为 0 表示不静默

【缺省配置】 0 秒

【命令模式】 全局模式

【缺省级别】 15

【使用指导】 使用默认值即可。

【配置举例】 1：配置多 MAB 认证失败后的静默时间。

```
Ruijie(config)# dot1x multi-mab quiet-period 2
```

【提示信息】 -

【平台说明】 -

4.27 dot1x port-control auto

配置端口上的 802.1x 认证。

dot1x port-control auto

关闭端口上的 802.1x 认证

no dot1x port-control auto

【参数说明】

参数	描述
-	-

【缺省配置】

缺省关闭

【命令模式】

接口模式

【缺省级别】

15

【使用指导】

部署 802.1x 必须配置该命令。

【配置举例】

1：配置端口上的 802.1x 认证。

```
Ruijie(config-if-GigabitEthernet 0/0)# dot1x port-control auto
```

【提示信息】

-

【平台说明】

-

4.28 dot1x probe-timer interval

配置锐捷客户端检测周期。

dot1x probe-timer interval *time*

【参数说明】

参数	描述
<i>time</i>	客户端检测周期，单位秒，默认 20。配置范围 1-65535

【缺省配置】

20 秒

【命令模式】

全局模式

【缺省级别】

15

【使用指导】 使用默认值即可。

【配置举例】 1：配置锐捷客户端检测周期。

```
Ruijie(config)# dot1x probe-timer interval 30
```

【提示信息】 -

【平台说明】 -

4.29 dot1x probe-timer alive

配置锐捷客户端检测时长。

dot1x probe-timer alive *time*

【参数说明】

参数	描述
<i>time</i>	客户端检测时长，单位秒，默认 60。配置范围 1-65535

【缺省配置】 60

【命令模式】 全局模式

【缺省级别】 15

【使用指导】 终端认证上线后，在检测时长内设备没收到终端的任何探测报文响应，则认为终端下线，建议使用默认值即可。

【配置举例】 1：配置锐捷客户端检测时长。

```
Ruijie(config)# dot1x probe-timer alive 120
```

【提示信息】 -

【平台说明】 -

4.30 dot1x private-supPLICANT-only

配置过滤非锐捷客户端功能。

dot1x private-supPLICANT-only

关闭过滤非锐捷客户端功能

no dot1x private-supPLICANT-only

【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】	15	
【使用指导】	部署环境中如果要求必须使用锐捷 supplicant 软件认证，则可以配置该功能。	
【配置举例】	1：配置过滤非锐捷客户端功能。	
	Ruijie(config)# dot1x private-supplicant-only	
【提示信息】	-	
【平台说明】	-	

4.31 dot1x pseudo source-mac

配置使用虚拟 mac 作为设备发出的 802.1x 报文的源 mac 地址。

dot1x pseudo source-mac

关闭使用虚拟 mac 作为设备发出的 802.1x 报文的源 mac 地址

no dot1x pseudo source-mac

【参数说明】	参数	描述
	-	默认关闭
【缺省配置】	缺省关闭	
【命令模式】	全局模式	
【缺省级别】	15	
【使用指导】	默认情况下，设备使用设备本机的 mac 地址作为 802.1x 认证时的 eap 报文源 mac 地址。锐捷 supplicant 的部分版本，会根据 eap 报文的源 mac 地址来判断接入设备是否为锐捷设备，并实施一些私有特性，和这些 supplicant 配合做 802.1x 认证时，如果要使用相关私有特性，可以开启虚拟源 mac 地址功能。	
【配置举例】	1：配置使用虚拟 mac 作为设备发出的 802.1x 报文的源 mac 地址。	
	Ruijie(config)# dot1x pseudo source-mac	

【提示信息】 -

【平台说明】 -

4.32 dot1x redirect

配置二代 su 升级功能。

dot1x redirect

关闭二代 su 升级功能

no dot1x redirect

【参数说明】

参数	描述
-	默认关闭

【缺省配置】

缺省关闭

【命令模式】

全局模式

【缺省级别】

15

【使用指导】

通过浏览器重定向到指定的资源网站下载 supplicant 软件，需要配置好重定向参数，具体参考 web 认证配置手册的说明。

【配置举例】

1：配置二代 su 升级功能。

```
Ruijie(config)# dot1x redirect
```

【提示信息】 -

【平台说明】 -

4.33 dot1x reauth-max

配置 request/id 报文重传次数。

dot1x reauth-max num

【参数说明】

参数	描述
num	request/id 报文重传次数，默认 3，配置范围 1-10

【缺省配置】	3
【命令模式】	全局模式
【缺省级别】	15
【使用指导】	使用默认值即可。
【配置举例】	1：配置 request/id 报文重传次数。 Ruijie(config)# dot1x reauth-max 2
【提示信息】	-
【平台说明】	-

4.34 dot1x re-authentication

配置重认证功能。
dot1x re-authentication

关闭重认证功能
no dot1x re-authentication

【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】	15
--------	----

【使用指导】	重认证功能会给服务器造成压力，在用户量大的环境中，建议关闭该功能。
--------	-----------------------------------

【配置举例】	1：配置重认证功能。 Ruijie(config)# dot1x re-authentication
--------	---

【提示信息】	-
--------	---

【平台说明】	-
--------	---

4.35 dot1x timeout re-authperiod

配置重认证间隔。

dot1x timeout re-authperiod *time*

【参数说明】	参数	描述
	<i>time</i>	重认证间隔，单位秒，默认 3600，配置范围 1-65535
【缺省配置】	3600 秒	
【命令模式】	全局模式	
【缺省级别】	15	
【使用指导】	使用默认值即可。	
【配置举例】	1：配置重认证间隔。	
	Ruijie(config)# dot1x timeout re-authperiod 2400	
【提示信息】	-	
【平台说明】	-	

4.36 dot1x timeout quiet-period

配置认证失败后的静默时间。

dot1x timeout quiet-period *time*

【参数说明】	参数	描述
	<i>time</i>	认证失败后的静默时间，单位秒，默认 10，配置范围 1-65535
【缺省配置】	10	
【命令模式】	全局模式	
【缺省级别】	15	
【使用指导】	使用默认值即可。	
【配置举例】	1：配置认证失败后的静默时间。	

```
Ruijie(config)# dot1x timeout quiet-period 60
```

【提示信息】 -

【平台说明】 -

4.37 dot1x timeout supp-timeout

配置 request/challenge 报文重传间隔。

dot1x timeout supp-timeout *time*

【参数说明】	参数	描述
	<i>time</i>	request/challenge 报文重传间隔，单位秒，默认 3，配置范围 1-65535

【缺省配置】	3 秒
--------	-----

【命令模式】	全局模式
--------	------

【缺省级别】	15
--------	----

【使用指导】	使用默认值即可。
--------	----------

【配置举例】	1：配置 request/challenge 报文重传间隔。
	<pre>Ruijie(config)# dot1x timeout supp-timeout 10</pre>

【提示信息】	-
--------	---

【平台说明】	-
--------	---

4.38 dot1x timeout server-timeout

配置服务器超时时间。

dot1x timeout server-timeout *time*

【参数说明】	参数	描述
	<i>time</i>	服务器超时时间，单位秒，默认 5，配置范围 1-65535

【缺省配置】	5 秒
--------	-----

【命令模式】	全局模式
--------	------

【缺省级别】 15

【使用指导】 必须保证 802.1x 的服务器超时值大于 radius 的超时值，默认情况下，802.1x 的超时值是小于 radius 的超时值的，因此实际使用中主要是将 radius 的服务器超时值调小，具体可参考 radius 的配置手册。

【配置举例】 1：配置服务器超时时间。

```
Ruijie(config)# dot1x timeout server-timeout 10
```

【提示信息】 -

【平台说明】 -

4.39 dot1x timeout tx-period

配置 request/id 报文重传间隔。

dot1x timeout tx-period time

【参数说明】

参数	描述
time	request/id 报文重传间隔，单位秒，默认 3，配置范围 1-65535

【缺省配置】 3 秒

【命令模式】 全局模式

【缺省级别】 15

【使用指导】 使用默认值即可。

【配置举例】 1：配置服务器超时时间。

```
Ruijie(config)# dot1x timeout tx-period 5
```

【提示信息】 -

【平台说明】 -

4.40 dot1x valid-ip-acct enable

配置用户获取 IP 之后发起记账的功能。

dot1x valid-ip-acct enable

关闭用户获取 IP 之后发起记账的功能。

no dot1x valid-ip-acct enable

【参数说明】	参数	描述
		默认关闭

【缺省配置】	缺省关闭
--------	------

【命令模式】	全局模式
--------	------

【缺省级别】	15
--------	----

【使用指导】	服务器要求认证用户必须在记账报文中携带 IP 地址的可以配置此功能。
--------	------------------------------------

【配置举例】	1：用户获取 IP 之后发起记账。
	<pre>Ruijie(config)# dot1x valid-ip-acct enable</pre>

【提示信息】	-
--------	---

【平台说明】	-
--------	---

4.41 dot1x valid-ip-acct timeout

配置用户认证通过之后，允许等待该用户获取 IP 的时间。

dot1x valid-ip-acct timeout time

恢复默认值。

no dot1x valid-ip-acct timeout

【参数说明】	参数	描述
	<i>time</i>	超时时间，默认为 5 分钟

【缺省配置】	默认为 5 分钟
--------	----------

【命令模式】	全局模式
--------	------

【缺省级别】	15
--------	----

【使用指导】	开启了用户获取 IP 之后才能开始记账的情况下，为避免客户端长时间不获取 IP 而不发起记账，可以根据需要配置此超时时间。
--------	---

【配置举例】 1：用户认证通过之后，允许等待该用户获取 IP 的时间。

```
Ruijie(config)# dot1x valid-ip-acct timeout 10
```

【提示信息】 -

【平台说明】 -

4.42 show dot1x

查看 802.1x 协议参数。

show dot1x

【参数说明】	参数	描述
	-	-

【缺省配置】	-
--------	---

【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 802.1x 当前的协议参数、用户数等信息。

【配置举例】 1：查看 802.1x 协议参数。

```
Ruijie#show dot1x
802.1X Status:          disabled
Authentication Mode:    eap-md5
Total User Number:      0(exclude dynamic user)
Authenticated User Number: 0(exclude dynamic user)
Dynamic User Number:    0
Re-authen Enabled:      disabled
Re-authen Period:       3600 sec
Quiet Timer Period:     10 sec
Tx Timer Period:        3 sec
Supplicant Timeout:     3 sec
Server Timeout:         5 sec
Re-authen Max:          3 times
Maximum Request:        3 times
Private supplicant only: disabled
```

Client Online Probe: disabled
Eapol Tag Enable: disa

字段解释：

字段	说明
802.1X Status	是否有配置 802.1x 功能
Authentication Mode	认证模式
Total User Number	当前认证用户总数，含正在认证和已经认证
Authed User Number	当前已认证用户数
Dynamic User Number	端口模式下的动态用户数量

【提示信息】 -

【平台说明】 -

4.43 show dot1x auth-address-table

查看可认证主机列表。

show dot1x auth-address-table [address addr] [interface interface]

【参数说明】	参数	描述
	addr	指定终端 mac 地址显示
	Interface	指定端口显示列表

【缺省配置】 -

【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】 使用可认证主机列表。

【配置举例】 1：查看可认证主机列表。

```
Ruijie #show dot1x auth-address-table
Interface      Address
-----
Fa0/1          00d0.f800.0c0e
Fa0/2          001a.c800.0102

Ruijie #show dot1x auth-address-table interface fastEthernet 0/1
```

```

Interface      Address
-----
Fa0/1          00d0.f800.0c0e

Ruijie #show dot1x auth-address-table address 00d0.f8.00.0c0e
Interface      Address
-----
Fa0/1          00d0.f800.0c0e

```

字段解释：

字段	说明
Interface	端口
Address	可认证主机的 mac 地址

【提示信息】 -

【平台说明】 -

4.44 show dot1x auto-req

查看主动认证状态和参数。

show dot1x auto-req

【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 802.1x 主动认证功能的状态和参数。

【配置举例】 1：查看主动认证的功能状态和参数。

```

Ruijie# show dot1x auto-req
Auto-Req: Enabled
User-Detect : Enabled
Packet-Num   : 0
Req-Interval: 30 Seconds

```

字段解释：

字段	说明
----	----

Auto-Req	主动认证功能状态
User-Detect	用户检测功能状态
Req-Interval	主动认证报文发送间隔

【提示信息】 -

【平台说明】 -

4.45 show dot1x max-req

查看 request/challenge 报文重传次数。

show dot1x max-req

【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 request/challenge 报文重传次数。

【配置举例】 1：查看 request/challenge 报文重传次数

```
Ruijie#show dot1x max-req
```

```
Max-Req: 3 Times
```

字段解释：

字段	说明
Max-Req	request/challenge 报文重传次数

【提示信息】 -

【平台说明】 -

4.46 show dot1x port-control

查看受控口信息。

show dot1x port-control [interface interface-type interface-number]

【参数说明】	参数	描述

<i>interface-type</i>	接口类型
<i>interface-number</i>	接口编号

【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受控口信息。

【配置举例】 1：查看受控口信息

```
Ruijie#show dot1x port-control
```

Interface	Mode	Dynamic-User	Static-User	Max-User	Authened	MAB
Gi0/5	mac-based	0	0	unlimited	no	disable

字段解释：

字段	说明
Interface	受控口名称
Mode	端口模式
Dynamic-User	端口动态用户数量
Static-User	端口静态用户数量
Max-User	端口最大用户数
Authened	端口是否认证通过的状态
MAB	端口配置 MAB 认证的状态

【提示信息】 -

【平台说明】 -

4.47 show dot1x private-supPLICANT-only

查看过滤非锐捷客户端开关的状态。

show dot1x private-supPLICANT-only

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过滤非锐捷客户端开关的状态。

【配置举例】 1：查看过滤非锐捷客户端开关的状态

```
Ruijie#show dot1x private-supPLICANT-only
```

```
private-supPLICANT-only: Disabled
```

字段解释：

字段	说明
private-supPLICANT-only	过滤非锐捷客户端开关的状态

【提示信息】 -

【平台说明】 -

4.48 show dot1x probe-timer

查看客户端探测的参数。

show dot1x probe-timer

【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客户端探测功能的参数。

【配置举例】 1：查看客户端探测功能的参数

```
Ruijie#show dot1x probe-timer
```

```
Hello Interval : 20
```

```
Hello Alive : 60
```

字段解释：

字段	说明
Hello Interval	探测周期
Hello Alive	探测时长

【提示信息】 -

【平台说明】 -

4.49 show dot1x re-authentication

查看重认证开关状态。

show dot1x re-authentication

【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重认证开关状态。

【配置举例】 1：查看重认证开关状态

```
Ruijie#show dot1x re-authentication
```

```
Reauth-Enabled: Disabled
```

字段解释：

字段	说明
Reauth-Enabled	重认证开关状态

【提示信息】 -

【平台说明】 -

4.50 show dot1x reauth-max

查看 request/id 报文重传次数。

show dot1x reauth-max

【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 request/id 报文重传次数。

【配置举例】 1：查看 request/id 报文重传次数

```
Ruijie#show dot1x reauth-max
```

```
Reauth-Max: 3 Times
```

字段解释：

字段	说明
Reauth-Max	request/id 报文重传次数

【提示信息】 -

【平台说明】 -

4.51 show dot1x summary

查看认证用户表项信息。

show dot1x 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】 15

【使用指导】 查看认证用户表项信息，通过该信息，可以知道认证终端当前处于什么阶段，比如正在认证、已经认证或者静默。

【配置举例】 1：查看认证用户表项信息

```
Ruijie#show dot1x summary
```

```
ID      User      MAC      Interface 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

Interface0	认证终端所在端口
VLAN	认证终端所在 vlan id
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】 -

4.52 show dot1x timeout quiet-period

查看认证失败后的静默时间。
show dot1x timeout quiet-period

【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】 查看认证失败后的静默时间。

【配置举例】 1：查看认证失败后的静默时间

```
Ruijie#show dot1x timeout quiet-period
```

```
Quiet-Period: 10 Seconds
```

字段解释：

字段	说明
Quiet-Period	认证失败后的静默时间

【提示信息】 -

【平台说明】 -

4.53 show dot1x timeout re-authperiod

查看重认证间隔。

show dot1x timeout re-authperiod

【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】 查看重认证间隔。

【配置举例】 1：查看重认证间隔

```
Ruijie#show dot1x timeout re-authperiod
```

```
Reauth-Period: 3600 Seconds
```

字段解释：

字段	说明
Reauth-Period	重认证间隔

【提示信息】 -

【平台说明】 -

4.54 show dot1x timeout server-timeout

查看服务器超时时间。

show dot1x timeout server-timeout

【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】 查看服务器超时时间。

【配置举例】 1：查看服务器超时时间

```
Ruijie#show dot1x timeout server-timeout
```

```
Server-Timeout: 5 Seconds
```

字段解释：

字段	说明
Server-Period	服务器超时时间

【提示信息】 -

【平台说明】 -

4.55 show dot1x timeout supp-timeout

查看 request/challenge 报文重传间隔。

show dot1x timeout supp-timeout

【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】 查看 request/challenge 报文重传间隔。

【配置举例】 1：查看 request/challenge 报文重传间隔

```
Ruijie#show dot1x timeout supp-timeout
```

```
Supp-Timeout: 3 Seconds
```

字段解释：

字段	说明
Supp-Timeout	request/challenge 报文重传间隔

【提示信息】 -

【平台说明】 -

4.56 show dot1x timeout tx-period

查看 request/id 报文重传间隔。

show dot1x timeout tx-period

【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】 查看 request/id 报文重传间隔。

【配置举例】 1：查看 request/id 报文重传间隔

```
Ruijie#show dot1x timeout tx-period
```

```
Tx-Period: 30 Seconds
```

字段解释：

字段	说明
Tx-Period	request/id 报文重传间隔

【提示信息】 -

【平台说明】 -

4.57 show dot1x user id

根据用户 id 查看用户的详细信息。

show dot1x dot1x user id id

【参数说明】

参数	描述
-id	-认证用户的 id

【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 show dot1x summary 查看用户概要信息，从中选择用户的 id，使用此命令进一步查看用户信息。

【配置举例】 1：查看认证用户的详细信息

```
Ruijie#show dot1x user id 16777225

User name: ts-user
User id: 16777225
Type: static
Mac address is 0023.aeea.4286
Vlan id is 2
Access from port Gi0/5
Time online: 0days 0h 0m17s
User ip address is 192.168.3.21
Max user number on this port is 0
Authorization session time is 1000 seconds
Supplicant is private
Start accounting
Permit proxy user
Permit dial user
IP privilege is 0
user acl-name ts-user_6_0_0 :
```

字段解释：

字段	说明
User name	用户名称
User id	用户 id
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
Supplicant is private	该用户的客户端是否是我司 su
Start accounting	该用户使用了记账
Permit proxy user	允许该用户代理
Permit dial user	允许该用户拨号
IP privilege	该用户 IP 权限级别
user acl-name	该用户的下发 ACL 信息

【提示信息】 -

【平台说明】 -

4.58 show dot1x user mac

根据用户 mac 查看用户的详细信息。

show dot1x dot1x user mac mac-addr

【参数说明】	参数	描述
	-mac-addr	-认证用户的 mac 地址

【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 show dot1x summary 查看用户概要信息，从中选择用户的 mac，使用此命令进一步查看用户信息。

【配置举例】 1：查看认证用户的详细信息

```
Ruijie#show dot1x user mac 0023.aaaa.4286
```

```
User name: ts-user
User id: 16777225
Type: static
Mac address is 0023.aaaa.4286
Vlan id is 2
Access from port Gi0/5
Time online: 0days 0h 0m17s
User ip address is 192.168.3.21
Max user number on this port is 0
Authorization session time is 1000 seconds
Supplicant is private
Start accounting
Permit proxy user
Permit dial user
IP privilege is 0
user acl-name ts-user_6_0_0 :
```

字段解释：

字段	说明
User name	用户名称
User id	用户 id
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
Supplicant is private	该用户的客户端是否是我司 su
Start accounting	该用户使用了记账
Permit proxy user	允许该用户代理
Permit dial user	允许该用户拨号
IP privilege	该用户 IP 权限级别
user acl-name	该用户的下发 ACL 信息

【提示信息】 -

【平台说明】 -

4.59 show dot1x user name

根据用户 mac 查看用户的详细信息。

show dot1x dot1x user name name

参数	描述
-name	-认证用户的用户名字符串

【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 show dot1x summary 查看用户概要信息，从中选择用户的用户，使用此命令进一步查看用户信息。

【配置举例】 1：查看认证用户的详细信息

```
Ruijie#show dot1x user name ts-user
```

```
User name: ts-user
```

```
User id: 16777225
```

```
Type: static
```

```
Mac address is 0023.aeaa.4286
```

```
Vlan id is 2
```



```
Access from port Gi0/5
Time online: 0days 0h 0m17s
User ip address is 192.168.3.21
Max user number on this port is 0
Authorization session time is 1000 seconds
Supplicant is private
Start accounting
Permit proxy user
Permit dial user
IP privilege is 0
user acl-name ts-user_6_0_0 :
```

字段解释：

字段	说明
User name	用户名称
User id	用户 id
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
Supplicant is private	该用户的客户端是否是我司 su
Start accounting	该用户使用了记账
Permit proxy user	允许该用户代理
Permit dial user	允许该用户拨号
IP privilege	该用户 IP 权限级别
user acl-name	该用户的下发 ACL 信息

【提示信息】 -

【平台说明】 -

5 SCC

命令	作用
auth-mode gateway	将认证模式切换到网关认证模式。
direct-vlan	配置免认证 VLAN。
nac-author-user maximum	配置 IPv4 用户容量。
offline-detect interval threshold	配置在线认证用户检测功能
show direct-vlan	显示免认证 VLAN 信息。
show nac-author-user interface	显示指定接口 IPv4 当前用户数和用户容量。
station-move permit	配置认证用户可迁移。

5.1 命令标识符表

在以下命令中用到的标识符可参见以下命令标识符表：

标识符	含义
vlanlist	免认证 VLAN 列表
interval	在线认证用户检测周期
threshold	在线认证用户检测的流量门限

5.2 auth-mode gateway

将设备的认证模式从接入认证模式切换到网关认证模式。

auth-mode gateway

将设备的认证模式从网关认证模式切换到接入认证模式

no auth-mode gateway

【参数说明】	参数	描述
	-	-

【缺省配置】 接入认证模式

【命令模式】 全局模式

【缺省级别】 14

【使用指导】 在核心网关设备上进行接入控制时，需要在核心设备上将认证模式切换到网关认证模式。

【配置举例】 1：将设备的认证模式切换到网关认证模式：

```
Ruijie(config)# auth-mode gateway
Please save config and reload system.
```

【检验方法】 1：使用 **running** 命令可以查看到设备的认证模式。

【提示信息】 -

【常见错误】 认证模式切换需要重启设备，切换前如果忘了保存配置，会导致配置丢失。

【平台说明】 -

5.3 direct-vlan

配置免认证 VLAN。

```
direct-vlan vlanlist
```

删除免认证 VLAN 配置

```
no direct-vlan vlanlist
```

【参数说明】	参数	描述
	<i>vlanlist</i>	VLAN 列表，可以是一个 vlan，也可以是一组 VLAN

【缺省配置】 没有免认证 VLAN

【命令模式】 全局模式

【缺省级别】 14

【使用指导】 为了让某个特殊 VLAN 内的用户免于进行 dot1x 或 web 认证就能上网，可以配置免认证 VLAN。

【配置举例】 1：将 VLAN 2 配置为免认证 VLAN：

```
Ruijie(config)# direct-vlan 2
```

【检验方法】 1：使用 **show direct-vlan** 命令可以查看到所有的免认证 VLAN 信息。

【提示信息】 -

【常见错误】 -

【平台说明】 -

5.4 nac-author-user maximum

配置端口下 IPv4 用户容量限制。

nac-author-user maximum *max-user-num*

取消端口下的 IPv4 用户容量限制

no nac-author-user maximum

【参数说明】

参数	描述
<i>max-user-num</i>	IPv4 用户最大容量限制，取值范围[1,1024]。

【缺省配置】 端口下的 IPv4 用户容量无限制

【命令模式】 接口模式

【缺省级别】 14

【使用指导】 为了限制一个端口下的 IPv4 用户数，可以使用本命令进行配置。

【配置举例】 1：限制端口 Gi 0/1 下的 IPv4 最大用户数为 100：

```
Ruijie(config)#int gigabitEthernet 0/1
Ruijie(config-if-GigabitEthernet 0/1)#nac-author-user maximum 100
```

【检验方法】 1：使用 **show nac-author-user** 命令可以查看到所有接口上当前的 IPv4 用户数和容量限制。
2：使用 **show nac-author-user interface interface-name** 命令可以查看到指定接口上当前的 IPv4 用户数和容量限制。

【提示信息】 -

【常见错误】 -

【平台说明】 -

5.5 offline-detect interval thredshold

配置认证用户在线检测功能，在指定的时间周期内低流量下线或无流量下线。

offline-detect interval *interval* **thredshold** *thredshold*

恢复认证用户在线检测至默认配置

default offline-detect

关闭认证用户在线检测功能

no offline-detect

【参数说明】

参数	描述
<i>interval</i>	流量检测周期，单位分钟，非交换机产品上，取值范围为[1, 65535]；交换机产品上取值范围为[6, 65535]。
<i>thredshold</i>	流量，单位字节，取值范围[0, 4294967294]。0 表示无流量检测。

【缺省配置】 8 小时无流量检测下线

【命令模式】 全局模式

【缺省级别】 14

【使用指导】 认证用户在流量低于某一特定值时就认为该用户没在使用网络，将用户下线，不再对该用户进行计费。要实现这样的功能，可以配置认证用户的在线检测功能。

【配置举例】 1：配置 5 分钟内如果用户的流量低于 5kBytes 时就将用户下线：

```
Ruijie(config)#offline-detect interval 5 threshold 5120
```

【检验方法】 1：使用 **show running** 命令可以查看认证用户在线检测的相关配置。

【提示信息】 -

【常见错误】 -

【平台说明】 -

5.6 show direct-vlan

显示免认证 VLAN 配置信息

show direct-vlan

【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】 显示设备上配置的免认证 VLAN 信息
- 【配置举例】 1：查看免认证 VLAN 配置信息：
Ruijie #show direct-vlan
direct-vlan 5,7,100
- 【提示信息】 -
- 【平台说明】 -

5.7 show nac-author-user interface

显示所有接口或指定接口上的 IPv4 用户容量限制和当前 IPv4 用户数
show nac-author-user [interface interface-name]

- | | | |
|--------|----------------|------|
| 【参数说明】 | 参数 | 描述 |
| | interface-name | 接口名称 |
- 【命令模式】 特权模式
 - 【缺省级别】 14
 - 【使用指导】 如果要查看设备上的 IPv4 用户数限制，可以使用本使命查看。
 - 【配置举例】 1：查看接口 Gi 0/1 上的当前 IPv4 用户数和 IPv4 用户容量限制：
Ruijie#show nac-author-user interface gi 0/1
Port Cur_num Max_num

Gi0/1 0 100
 - 【提示信息】 -
 - 【平台说明】 -

5.8 station-move permit

配置认证用户可迁移。

station-move permit

取消认证用户可迁移功能

no station-move permit

【参数说明】

参数	描述
-	-

【缺省配置】

认证用户不可迁移

【命令模式】

全局模式

【缺省级别】

14

【使用指导】

如果想让已在线认证用户在不下线的情况下，迁移到网络中的另一个物理位置(端口或 vlan 不一样)可以重新认证上线，可以配置认证用户可迁移功能。

【配置举例】

1：配置认证用户可迁移：

```
Ruijie(config)#station-move permit
```

【检验方法】

1：使用 **show running** 命令可以查看认证用户可迁移功能是否开启。

【提示信息】

-

【常见错误】

-

【平台说明】

-

6 全局 IP+MAC 绑定

命令	作用
<u>address-bind</u>	配置全局 IPv4+MAC 地址绑定
<u>address-bind install</u>	开启地址绑定功能
<u>address-bind ipv6-mode</u>	配置 IPv6 地址绑定模式
<u>address-bind uplink</u>	配置地址绑定例外端口
<u>show address-bind</u>	显示全局 IP+MAC 地址绑定
<u>show address-bind uplink</u>	显示地址绑定例外端口

6.1 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
<i>ip-address</i>	绑定的 IPv4 地址
<i>ipv6-address</i>	绑定的 IPv6 地址
<i>mac-address</i>	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】 -

6.2 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】 -

6.3 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】 -

6.4 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
	<i>interface-id</i>	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】 -

6.5 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】 -

6.6 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】 -

7 PASSWORD-POLICY

命令	作用
password policy life-cycle	设置口令生存周期。
password policy min-size	限制用户口令的最小长度。
password policy no-repeat-times	限制重复使用最近几次已配置过的口令。
password policy strong	打开强口令检测功能。
service password-encryption	设置口令加密存储。
show password policy	查看用户设置的口令安全策略信息。

7.1 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
	<i>days</i>	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】 -

7.2 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
	<i>length</i>	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】 -

7.3 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】 -

7.4 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】 -

7.5 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】 -

7.6 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 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 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】 -

8 端口安全

命令	作用
switchport port-security	设置端口安全功能，端口安全的违例处理等。
switchport port-security aging	为一个端口上的所有安全地址配置老化时间。
switchport port-security binding	接口配置模式下手工配置安全地址绑定。
switchport port-security interface binding	特权模式下手工配置安全地址绑定。
switchport port-security mac-address	接口配置模式下手工配置静态安全地址。
switchport port-security interface mac-address	特权模式下手工配置静态安全地址。
switchport port-security maximum	设置端口最大安全地址个数。
switchport port-security mac-address sticky	配置 Sticky MAC 安全地址。
show port-security	显示端口安全的设置信息和安全地址。

8.1 switchport port-security

设置端口安全功能，端口安全的违例处理等。

switchport port-security [violation { protect | restrict | shutdown }]

关闭端口安全的设置，或者将安全违例处理方式恢复成缺省值。

no switchport port-security [violation]

【参数说明】

参数	描述
protect	发现违例，则丢弃违例的报文。
restrict	发现违例，则丢弃违例的报文并且发送 trap。
shutdown	发现违例，则丢弃报文、发送 Trap 并且关闭接口。

【缺省配置】

接口的安全缺省是关闭的。

【命令模式】

接口配置模式

【缺省级别】

14

【使用指导】

利用端口安全这个特性，可以通过限制允许访问设备上某个接口的 MAC 地址以及 IP(可选)来实现严格控制对该接口的输入。当为安全端口(打开了端口安全功能的端口)配置了一些安全地址后，则除了源地址为这些安全地址的包外，这个端口将不转发其它任何报文。此外，还可以限制一个端口上能包含的安全地址最大个数，如果将最大个数设置为 1 并且为该端口配置一个安全地址，则连接到这个口的工作站(其地址为配置的安全 M 地址)将独享该端口的全部带宽。



如果在违例后修改端口的违例模式，新的违例模式必须在安全端口恢复成非违例状态后，再次违例，才会

生效。。

【配置举例】 下面的例子是在接口 Gigabitethernet 1/1 上打开端口安全功能，并设置违例处理为 shutdown：

```
Ruijie(config)# interface gigabitethernet 1/1
Ruijie(config-if)# switchport port-security
Ruijie(config-if)# switchport port-security violation shutdown
```

【检验方法】 1：使用 **show port-security** 命令，可以查看端口安全的设置信息和安全地址。

【提示信息】 -

【常见错误】 -

【平台说明】 -

8.2 switchport port-security aging

为一个端口上的所有安全地址配置老化时间。

```
switchport port-security aging { static | time time }
```

设置老化时间只应用于自动学习的地址，或者关闭老化功能。

```
no switchport port-security aging { static | time }
```

【参数说明】	参数	描述
	static	表示老化时间将同时应用于手工配置的安全地址和自动学习的地址，否则只应用于自动学习的地址。
	time time	表示这个端口上安全地址的老化时间，范围是 0 - 1440，单位是分钟。如果设置为 0，则老化功能实际上被关闭。

【缺省配置】 不老化任何安全地址。

【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使用命令 no switchport port-security aging time 关闭一个接口的安全地址老化功能，使用命令 no switchport port-security aging static 来是老化时间仅应用于动态学习到的安全地址。

 端口安全和 DOT1X 同时开启时，如果安全地址老化，则 DOT1X 对应的用户必须重新认证才可以继续通信。

 此功能与设置端口最大安全地址个数功能配合，可以让设备自动添加和删除接口上的安全地址。

【配置举例】 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
Ruijie(config)# interface gigabitethernet 1/1
Ruijie(config-if)# switchport port-security aging time 8
Ruijie(config-if)# switchport port-security aging static
Ruijie(config-if)# end
```

【检验方法】 1：使用 **show port-security** 命令，可以查看端口安全的设置信息和安全地址。

【提示信息】 -

【常见错误】 -

【平台说明】 -

8.3 switchport port-security binding

手工配置安全地址绑定，对安全地址进行源 IP+源 MAC 绑定，绑定之后，必须是符合绑定的安全地址的报文才可以进入交换机，不符合绑定的报文将被丢弃。

switchport port-security binding [*mac-address* **vlan** *vlan_id*] { *ipv4-address* | *ipv6-address* }

删除绑定的地址。

no switchport port-security binding [*mac-address* **vlan** *vlan_id*] { *ipv4-address* | *ipv6-address* }

手工配置安全地址绑定，对安全地址进行源 IP 绑定，绑定之后，必须是符合绑定的安全地址的报文才可以进入交换机，不符合绑定的报文将被丢弃。

switchport port-security binding { *ipv4-address* | *ipv6-address* }

删除绑定的地址。

no switchport port-security binding { *ipv4-address* | *ipv6-address* }

【参数说明】

参数	描述
<i>mac-address</i>	绑定的源 MAC 地址
<i>vlan_id</i>	绑定源 MAC 的 VID
<i>ipv4-address</i>	绑定 Ipv4 的 Ip 地址
<i>ipv6-address</i>	绑定 Ipv6 的 Ip 地址

【缺省配置】 -

【命令模式】 接口配置模式

【缺省级别】 14

【使用指导】 1：符合端口安全 IP+MAC，或者仅 IP 绑定的报文，其源 MAC 地址必须同时是端口安全地址才可以被转发；
2：对于动态安全地址来说，在安全地址添加到安全地址表之前，符合安全地址绑定或者仅 IP 绑定的任何报文不能被转发。

 静态端口安全地址不需要认证即可上网，如果存在授权，则必须同时符合授权绑定才可以上网。

【配置举例】 1：绑定 192.168.1.100 到接口 10：

```
Ruijie# configure terminal
Ruijie(config)#interface gigabitethernet 0/10
Ruijie(config-if)# switchport port-security binding 192.168.1.100
Ruijie(config-if)# end
```

2：绑定 192.168.1.100 MAC 地址 00d0.f800.5555, VID= 1 到接口 10：

```
Ruijie# configure terminal
Ruijie(config)#interface gigabitethernet 0/10
Ruijie(config-if)# switchport port-security binding 00d0.f800.5555 vlan 1 192.168.1.100
Ruijie(config-if)# end
```

【检验方法】 1：使用 **show port-security** 命令，可以查看端口安全的设置信息和安全地址。

【提示信息】 -

【常见错误】 -

【平台说明】 -

8.4 switchport port-security interface binding

手工配置安全地址绑定，对安全地址进行源 IP+源 MAC 绑定，绑定之后，必须是符合绑定的安全地址的报文才可以进入交换机，不符合绑定的报文将被丢弃。

switchport port-security interface interface-id binding [mac-address vlan vlan_id] { ipv4-address | ipv6-address }

删除绑定的地址。

no switchport port-security interface interface-id binding [mac-address vlan vlan_id] { ipv4-address | ipv6-address }

手工配置安全地址绑定，对安全地址进行源 IP 绑定，绑定之后，必须是符合绑定的安全地址的报文才可以进入交换机，不符合绑定的报文将被丢弃。

switchport port-security binding interface *interface-id* { *ipv4-address* | *ipv6-address* }

删除绑定的地址。

no switchport port-security binding interface *interface-id* { *ipv4-address* | *ipv6-address* }

【参数说明】

参数	描述
<i>interface-id</i>	绑定的接口 ID
<i>mac-address</i>	绑定的源 MAC 地址
<i>vlan_id</i>	绑定源 MAC 的 VID
<i>ipv4-address</i>	绑定 Ipv4 的 Ip 地址
<i>ipv6-address</i>	绑定 Ipv6 的 Ip 地址

【缺省配置】

-

【命令模式】

特权模式

【缺省级别】

14

【使用指导】

1：符合端口安全 IP+MAC，或者仅 IP 绑定的报文，其源 MAC 地址必须同时是端口安全地址才可以被转发；
2：对于动态安全地址来说，在安全地址添加到安全地址表之前，符合安全地址绑定或者仅 IP 绑定的任何报文不能被转发。

【配置举例】

1：绑定 192.168.1.100 到接口 10：

```
Ruijie# configure terminal
Ruijie(config)# switchport port-security binding interface g0/10 192.168.1.100
Ruijie(config)# end
```

2：绑定 192.168.1.100 MAC 地址 00d0.f800.5555, VID= 1 到接口 10：

```
Ruijie# configure terminal
Ruijie(config)# switchport port-security binding interface g0/10 00d0.f800.5555 vlan 1
Ruijie(config)# end
```

【检验方法】

1：使用 **show port-security** 命令，可以查看端口安全的设置信息和安全地址。

【提示信息】

-

【常见错误】

-

【平台说明】

-

8.5 switchport port-security mac-address

手工配置静态安全地址。

switchport port-security mac-address *mac-address* [**vlan** *vlan-id*]

删除配置的地址

no switchport port-security mac-address *mac-address* [**vlan** *vlan-id*]

【参数说明】	参数	描述
	<i>mac-address</i>	静态安全地址
	<i>vlan-id</i>	MAC 地址的 VID。  仅在 TRUNK 口下才支持设置 <i>vlan-id</i> 的设置。
【缺省配置】	-	
【命令模式】	接口配置模式	
【缺省级别】	14	
【使用指导】	-	
【配置举例】	设置 TRUNK 接口 10 的静态安全地址 00d0.f800.5555 VID=2：	
	<pre>Ruijie# configure terminal Ruijie(config)#interface gigabitethernet 0/10 Ruijie(config-if)# switchport port-security mac-address 00d0.f800.5555 vlan 2 Ruijie(config-if)# end</pre>	
【检验方法】	1：使用 show port-security 命令，可以查看端口安全的设置信息和安全地址。	
【提示信息】	-	
【常见错误】	-	
【平台说明】	-	

8.6 switchport port-security interface mac-address

手工配置静态安全地址。

switchport port-security interface *interface-id* **mac-address** *mac-address* [**vlan** *vlan-id*]

删除配置的安全地址。

no switchport port-security interface *interface-id* **mac-address** *mac-address* [**vlan** *vlan-id*]

【参数说明】

参数	描述
<i>interface-id</i>	接口 ID。
<i>mac-address</i>	静态安全地址。
<i>vlan-id</i>	MAC 地址的 VID，取值范围为 1~4094。  仅在 TRUNK 口下才支持设置 <i>vlan-id</i> 的设置。

【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】

设置 TRUNK 端口 10 的静态安全地址 00d0.f800.5555 VID=2：

```
Ruijie# configure terminal
Ruijie(config)# switchport port-security interface g0/10 mac-address 00d0.f800.5555 vlan 2
Ruijie(config)# end
```

【检验方法】

1：使用 **show port-security** 命令，可以查看端口安全的设置信息和安全地址。

【提示信息】

-

【常见错误】

-

【平台说明】

-

8.7 switchport port-security maximum

设置端口最大安全地址个数。

switchport port-security maximum *value*

恢复缺省个数。

no switchport port-security maximum

【参数说明】

参数	描述
----	----

	value 安全地址个数 1-128
【缺省配置】	128
【命令模式】	接口配置模式
【缺省级别】	14
【使用指导】	安全地址个数包含静态配置和动态学习的安全地址个数的总和，缺省为 128 个，如果设置的安全地址个数小于当前已有的安全地址个数，将提示设置失效。 如果端口 DOT1X 开启并且已认证的用户数大于端口安全的最大用户数,此时开启端口安全将会提示失败。
【配置举例】	设置接口 10 的端口安全地址个数为 2： Ruijie# configure terminal Ruijie(config)#interface gigabitethernet 0/10 Ruijie(config-if)# switchport port-security maximum 2 Ruijie(config-if)# end
【检验方法】	1：使用 show port-security 命令，可以查看端口安全的设置信息和安全地址。
【提示信息】	1：设置最大允许值小于当前值时，则提示错误。 Setting value is less than the current maximum.
【常见错误】	1：设置的最大允许值，小于当前值。
【平台说明】	-

8.8 switchport port-security mac-address sticky

配置 Stickk MAC 安全地址。

switchport port-security mac-address sticky mac-address [vlan vlan-id]

删除配置的地址。

no switchport port-security mac-address sticky mac-address [vlan vlan-id]

使能 Sticky MAC 地址学习功能。

switchport port-security mac-address sticky

关闭 Sticky MAC 地址学习功能

no switchport port-security mac-address sticky

【参数说明】	参数	描述
	mac-address	MAC 地址。
	vlan-id	MAC 地址的 VID。  仅在 TRUNK 口下才支持设置 vlan-id 的设置。
【缺省配置】	Sticky MAC 学习功能缺省情况下关闭。	
【命令模式】	接口配置模式	
【缺省级别】	14	
【使用指导】	Sticky MAC 地址是一种特殊的 MAC 地址，不受老化机制影响，无论是配置了动态的老化还是静态的老化，Sticky MAC 地址均不会老化。	
【配置举例】	1：设置 TRUNK 接口 10 的静态安全地址 00d0.f800.5555 VID=2：	
	<pre>Ruijie# configure terminal Ruijie(config)#interface gigabitethernet 0/10 Ruijie(config-if)# switchport port-security mac-address 00d0.f800.5555 vlan 2 Ruijie(config-if)# end</pre>	
	2：设置接口 10 的 Sticky MAC 地址学习打开：	
	<pre>Ruijie# configure terminal Ruijie(config)#interface gigabitethernet 0/10 Ruijie(config-if)# switchport port-security sticky mac-address Ruijie(config-if)# end</pre>	
【检验方法】	1：使用 show port-security 命令，可以查看端口安全的设置信息和安全地址。	
【提示信息】	-	
【常见错误】	-	
【平台说明】	-	

8.9 show port-security

显示端口安全的设置信息和安全地址。

show port-security [**address** [**interface** *interface-id*] | **binding** [**interface** *interface-id*] | **interface** *interface-id* | **all**]

【参数说明】

参数	描述
address	显示所有的安全地址，或者是指定接口的所有安全地址。
binding	显示所有的安全绑定，或者是指定接口的所有安全绑定。
interface <i>interface-id</i>	显示指定接口的端口安全设置信息。
all	显示所有生效的端口安全地址和端口安全绑定记录。

【命令模式】

特权模式

【缺省级别】

14

【使用指导】

如果使用该命令时不加参数，则显示所有接口的安全设置状态、违例处理等信息。若需要查看具体接口的端口安全配置、安全地址、安全绑定，分别使用参数 *interface*、*address*、*binding*。

【配置举例】

1：下面的例子显示的是端口安全的统计信息

```
Ruijie#show port-security
NO.   SecurePort  MaxSecureAddr  CurrentAddr  CurrentIpBind  CurrentIpMacBind  SecurityAction
      (Count)      (Count)      (Count)      (Count)
-----
1     Gi0/1      128           2            2              1                protect

Total secure addresses in System : 2
Total secure bindings in System : 3
```

字段解释：

字段	说明
NO.	记录序号。
Secure Port	设备端口名称。
MaxSecureAddr(count)	端口允许的最大安全地址数。
CurrentAddr(count)	端口当前的安全地址数。
CurrentIpBind (count)	端口当前的仅 IP 安全绑定个数。
CurrentIpMacBind (count)	端口当前的 IP+MAC 绑定个数。
Security Action	端口对违例行为的处理方式。
Total secure addresses in System	当前设备上配置的安全地址总个数。
Total secure bindings in System	当前设备上配置的安全绑定总个数。

2：下面的例子显示了接口 GigabitEthernet 0/1 上的端口安全配置

```
Ruijie#show port-security interface gigabitEthernet 0/1
Interface           : GigabitEthernet 0/1
Port status         : down
Port Security       : enabled
SecureStatic address aging : disabled
Sticky dynamic address : disabled
```

```

Violation mode           : protect
Maximum MAC Addresses    : 128
Total MAC Addresses      : 2
Configured MAC Addresses : 2
Dynamic MAC Addresses     : 0
Sticky MAC Addresses     : 0
Total security binding   : 3
IPv4-ONLY Binding Addresses : 1
IPv6-ONLY Binding Addresses : 1
IPv4-MAC Binding Addresses : 1
IPv6-MAC Binding Addresses : 0
Aging time(min)         : 0

```

字段解释：

字段	说明
Interface	设备端口名称。
Port status	设备端口状态。
Port Security	设备端口上的端口安全开关状态。
SecureStatic address aging	端口上静态配置的安全地址是否进行老化。
Sticky dynamic address	端口上动态学习的安全地址是否转化为 sticky 类型。
Violation mode	端口对违例行为的处理方式。
Maximum MAC Addresses	端口允许的最大安全地址数。
Total MAC Addresses	当前端口上生效的安全地址个数。
Configured MAC Addresses	静态配置的安全地址个数。
Dynamic MAC Addresses	动态配置的安全地址个数。
Sticky MAC Addresses	Sticky 类型的安全地址个数。
Total security binding	当前端口上生效的安全绑定个数。
IPv4-ONLY Binding Addresses	仅 IPv4 匹配的安全绑定个数。
IPv6-ONLY Binding Addresses	仅 IPv6 匹配的安全绑定个数。
IPv4-MAC Binding Addresses	IPv4+MAC 匹配的安全绑定个数。
IPv6-MAC Binding Addresses	IPv6+MAC 匹配的安全绑定个数。
Aging time(min)	端口上安全地址的老化时间。

3：下面的例子显示了系统中的所有安全地址

```
Ruijie#show port-security address
```

NO.	VLAN	MacAddress	PORT	TYPE	RemainingAge(mins)	STATUS
1	1	00d0.f800.073c	GigabitEthernet 0/1	Configured	--	active
2	1	00d0.f800.073d	GigabitEthernet 0/1	Configured	--	active

字段解释：

字段	说明
NO.	记录序号。

Vlan	VLAN 编号。
Mac Address	MAC 地址。
Port	端口名称。
Type	安全地址生成类型。
Remaining Age(mins)	地址老化时间。
STATUS	安全地址生效状态

4：下面的例子显示了系统中的所有安全绑定

```
Ruijie#show port-security binding
```

NO.	VLAN	MacAddress	PORT	IpAddress	FilterType	FilterStatus
1	1	00d0.f800.073c	Gi0/1	192.168.12.202	ipv4-mac	active
2	--	--	Gi0/1	192.168.0.1	ipv4-only	active
3	--	--	Gi0/1	ffaa:ddcc::1	ipv6-only	active

字段解释：

字段	说明
NO.	记录序号。
Vlan	VLAN 编号。
Mac Address	MAC 地址。
Port	端口名称。
IpAddress	IP 地址
FilterType	安全绑定过滤类型。
FilterStatus	安全绑定生效状态

【提示信息】 -

【平台说明】 -

9 STORM-CONTROL

命令	作用
show storm-control	显示风暴控制信息
storm-control	设置接口的风暴控制开关

9.1 show storm-control

显示风暴控制信息

show storm-control [*interface-type interface-number*]

【参数说明】	参数	描述
	<i>interface-type interface-number</i>	指定接口。缺省为所有接口。

【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】 使用该命令可以显示风暴控制信息

【配置举例】 1：使用 **show storm-control** 命令查看 FastEthernet 0/1 口的风暴控制信息。

```
Ruijie# show storm-control fastEthernet 0/1
```

Interface	Broadcast Control	Multicast Control	Unicast Control	Action
-----	-----	-----	-----	-----
FastEthernet 0/1	1%	50%	1%	none

【提示信息】 -

【平台说明】 -

9.2 storm-control

开启未知单播报文风暴控制开关

storm-control unicast [{ **level percent** | **pps packets** | **rate-bps** }]

开启组播报文风暴控制开关

storm-control multicast [{ **level percent** | **pps packets** | **rate-bps** }]

开启广播报文风暴控制开关

storm-control broadcast [{ *level percent* | *pps packets* | *rate-bps* }]

关闭未知名单播报文风暴控制开关
no storm-control unicast

关闭组播报文风暴控制开关
no storm-control multicast

关闭广播报文风暴控制开关
no storm-control broadcast

恢复未知名单播报文风暴控制缺省配置
default storm-control unicast

恢复组播报文风暴控制缺省配置
default storm-control multicast

恢复广播报文缺省配置
default storm-control broadcast

【参数说明】	参数	描述
	level percent	以带宽的百分比进行设置，如 20 表示 20%。
	pps packets	以 PPS 为单位进行设置，即 packets per second。
	rate-bps	允许的通过速率。

【缺省配置】 未知名单播、组播、广播报文风暴控制关闭

【命令模式】 接口配置模式。

【缺省级别】 14

【使用指导】 当一个端口上接收到过量的广播、多播或未知名单播包时，一个数据包的风暴就会产生，这会导致网络变慢和超时增加。协议栈的执行错误或对网络中一些错误配置都有可能产生导致风暴的产生。
设备可以分别广播、多播和未知名单播数据流进行风暴控制。当接收到的广播、多播或未知名单播包过量时，设备将暂时禁止相应类型的包的转发直到数据流恢复正常（这时包的转发将恢复正常）。

【配置举例】 1： 下面的例子说明了打开物理端口 FastEthernet 0/1 口的多播风暴控制功能，并且设置允许的通过速 率为 4M。

```
Ruijie(config)# int fastEthernet 0/1
Ruijie(config-if-FastEthernet 0/1)# storm-control multicast 4096
```

【检验方法】 1：使用 **show storm-control** 命令查看 FastEthernet 0/1 口的风暴控制信息。

```
Ruijie# show storm-control fastEthernet 0/1
```

Interface	Broadcast Control	Multicast Control	Unicast Control	Action
FastEthernet 0/1	1%	4%	1%	none

【提示信息】 -

【常见错误】 -

【平台说明】 -

10 SSH

命令	作用
crypto key generate	生成服务器端的公共密钥
crypto key zeroize	删除 SSH 服务器端的公共密钥
disconnect ssh	断开已经建立的 SSH 连接会话
ip scp server enable	在网络设备上打开 SCP 服务器功能。
ip ssh authentication-retries	设置 SSH Server 用户认证的重认证次数
ip ssh peer	将客户端的公钥文件和用户名关联
ip ssh time-out	设置 SSH Server 的用户认证超时时间
ip ssh version	设置 SSH Server 的版本
show crypto key mypubkey	显示 SSH Server 公共密钥的公开密钥部分的信息
show ip ssh	显示 SSH Server 的当前生效的配置信息
show ssh	显示已经建立的 SSH 连接的每个连接信息
ssh	建立一个到远程网络设备的 SSH 连接会话

10.1 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】 -

10.2 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 /rsal_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】 -

10.3 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
	vtty	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】 -

10.4 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】 -

10.5 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
	<i>retry times</i>	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】 -

10.6 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
	<i>username</i>	用户名
	<i>filename</i>	公钥文件名
	<i>rsa</i>	public-key 类型为 rsa
	<i>dsa</i>	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 <i>test</i> 关联的 RSA 和 DSA 公钥文件。	
	<pre>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</pre>	
【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。	
	<pre>Ruijie(config)# ip ssh peer test public-key rsa flash:rsa.pub %% Too many public-keys, system support max public key 1024</pre>	
	2：如果为输入关联的公钥文件名，则提示公钥文件名无效。	
	<pre>Ruijie(config)#ip ssh peer test public-key rsa flash: % Invalid file name</pre>	
【常见错误】	-	
【平台说明】	-	

10.7 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
	<i>time</i>	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： <pre>Ruijie# configure terminal Ruijie(config)# ip ssh time-out 100</pre>	
【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】	-	

10.8 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】 -

10.9 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 AQAAAEAA 2m6H/J+2 xOMLW5MR 8tOmpW1I XU1QItVN mLdR+G7O Q10kz+4/
```

```
/IgYR0ge 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 AAAAAEEA 0E5w2H0k v744uTIR yZBd/7AM 8pLItnW3 XH3LhEEi BbZGZvn3
      LEYYfQ9s pgYLOZQf S0s/GY0X gJOMsc6z i80AkQ==
```

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】 -

10.10 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】 -

10.11 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】 -

10.12 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 } ] [ -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 }	（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）算法依据密钥长度不同，可以支持三种类型：aes128-cbc（128 位密钥），aes192-cbc（192 位密钥）、aes256-cbc（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 <i>port-num</i>	(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。
<i>ip-addr</i> <i>hostname</i>	(必选) 指定远程服务器的 IPv4/IPv6 地址或主机名。
via <i>mgmt-name</i>	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 <i>interface-name</i>	指定 SSH Client 使用的源接口
/vrf <i>vrf-name</i>	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: aes128-cbc、aes192-cbc 和 aes256-cbc。
-  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】 -

11 URPF

命令	作用
clear ip urpf	清除 IPv4 URPF 检查丢弃报文数量的统计信息。
ip verify urpf drop-rate compute interval	全局配置 URPF IPv4 丢包率的计算时间间隔。
show ip urpf	查看 IPv4 URPF 配置及统计信息。

11.1 clear ip urpf

清除 IPv4 URPF 检查丢弃报文数量的统计信息。

clear ip urpf [interface *interface-name*]

【参数说明】

参数	描述
interface <i>interface-name</i>	清除指定接口的统计信息。缺省时，删除所有接口的统计信息。

【命令模式】

特权模式

【缺省级别】

1

【使用指导】

如果没有配置指定接口，将清除所有接口的统计信息。

【配置举例】

1：清除指定接口 GigabitEthernet 0/1 上的 IPv4 URPF 丢包统计信息。

```
Ruijie# clear ip urpf interface gigabitEthernet0/1
```

2：清除设备上所有接口的 IPv4 URPF 丢包统计信息。

```
Ruijie# clear ip urpf
```

【提示信息】

1：如果指定的接口没有启动 IPv4 URPF 功能，则提示错误。

```
% Interface GigabitEthernet 0/1 does not enable URPF function.
```

2：如果没有指定接口且设备都没有启动 IPv4 URPF 功能，则提示错误。

```
% Device does not enable URPF function.
```

【平台说明】

-

11.2 ip verify unicast source reachable-via (接口配置模式)

接口配置模式下，启动 IPv4 URPF 功能。

ip verify unicast source reachable-via { rx | any } [allow-default] [*acl-id*]

关闭 URPF 功能。
no ip verify unicast

【参数说明】	参数	描述
	rx	使用严格模式进行 URPF 检查。严格模式要求通过接收的 IP 报文的源地址在转发表中查找到的转发表项的出接口要与该报文的入接口匹配。
	any	使用宽松模式进行 URPF 检查。宽松模式只要求通过接收的 IP 报文的源地址能够在转发表中查找到转发表项即可。
	allow-default	(可选) 允许使用缺省路由进行 URPF 检查。缺省时，不使用缺省路由进行 URPF 检查。
	acl-id	(可选) ACL 号，支持： 1 to 99 (IP standard access list) 100 to 199 (IP extended access list) 1300 to 1999 (IP standard access list, expanded range) 2000 to 2699 (IP extended access list, expanded range) 缺省时，不继续匹配 ACL。

【缺省配置】 缺省 URPF 功能关闭。

【命令模式】 接口配置模式

【缺省级别】 14

【使用指导】 URPF 特性通过检查接收到的 IP 报文的源地址，判断在转发表中是否存在到达源地址的路由，来判断报文的合法性，如果匹配不到转发表项，则认为报文非法。

在接口配置模式下启动 URPF 特性，能对在该接口上接收到的报文启动 URPF 检查。

缺省情况下，不使用缺省路由进行 URPF 检查，如果用户需要，可以使用 **allow-default** 关键字启动该功能。

缺省情况下，URPF 检查失败的报文将被丢弃。如果配置了 ACL (*acl-name*)，在选路失败的情况下将继续匹配 ACL。如果 ACL 不存在或者匹配到 deny 的 ACE，报文将被丢弃；否则，如果匹配到 permit 的 ACE，报文将被转发。

-  启用本命令后，交换机产品将同时对 IPv4 报文启动 URPF 检查。
-  交换机产品只在 Routed Port 和 L3 AP 口上支持 URPF 特性，并且存在如下限制：
1. URPF 特性不支持关联 ACL 选项。
 2. URPF 特性不支持使用 65 ~ 127 位前缀的 IPv6 路由进行 URPF 检查。
 3. 启动 URPF 特性后，在这些接口对应的物理口上接收到的所有报文都将启动 URPF 检查，会扩大 URPF 检查报文的范围。典型的应用场景为，如果一个 Tunnel 口接收的报文从上述物理口上收到，该报文也将进行 URPF 检查，如果存在这样的应用场景，建议谨慎启动 URPF 检查。
 4. 启动 URPF 特性后，设备路由转发容量将减半。
 5. 启动 URPF 严格模式后，接口接收的报文在 URPF 检查时如果匹配等价路由，将转换为宽松模式处理。

【配置举例】 1：对从接口 GigabitEthernet 0/1 接收到的报文进行 URPF 严格检查，不需要使用缺省路由进行检查。

```
Ruijie(config)# interface gigabitEthernet0/1
Ruijie(config-if-GigabitEthernet 0/1)# ip verify unicast source reachable-via rx
```

【检验方法】 1：使用 **show ip urpf** 命令，可以查看接口接口是否启动 URPF 功能。

【提示信息】 -

【常见错误】 -

【平台说明】 -

11.3 ip verify urpf drop-rate compute interval

全局配置 URPF IPv4/IPv6 丢包率的计算时间间隔。
ip verify urpf drop-rate compute interval seconds

恢复缺省配置。
no ip verify urpf drop-rate compute interval

【参数说明】	参数	描述
	interval seconds	URPF 丢包率的计算时间间隔。单位为秒，范围[30, 300]，缺省值 30s。

【缺省配置】 缺省值为 30s。

【命令模式】 全局模式

【缺省级别】 14

【使用指导】 URPF 丢包率的计算时间间隔基于全局配置模式进行配置，将应用于全局的 URPF 丢包率计算和基于每个启动 URPF 特性的接口的 URPF 丢包率计算，并且同时对 IPv4 URPF 和 IPv6 URPF 生效。

【配置举例】 1：配置 URPF 丢包率的计算时间间隔为 1 分钟。
Ruijie(config)# ip verify urpf drop-rate compute interval 60

【检验方法】 1：使用 **show ip urpf** 或者 **show ipv6 urpf** 命令，可以查看当前配置的丢包率的计算间隔。

【提示信息】 -

【常见错误】 -

【平台说明】 -

11.4 ip verify urpf drop-rate notify

启动 URPF 丢包信息监控。

ip verify urpf drop-rate notify

关闭 URPF 丢包信息监控。

no ip verify urpf drop-rate notify

恢复缺省配置。

default ip verify urpf drop-rate notify

【参数说明】	参数	描述
	-	-

【缺省配置】 缺省没有启动 URPF 丢包信息监控。

【命令模式】 接口配置模式

【缺省级别】 14

【使用指导】 通过启动 URPF 丢包信息监控，能够通过 Syslog 或者 Trap 的方式主动告知用户 URPF 检查丢包的信息，方便用户对网络状况进行监控。

【配置举例】 1：配置接口 GigabitEthernet 0/1 上启动 URPF 丢包信息监控。

```
Ruijie(config)# interface gigabitEthernet0/1
Ruijie(config-if-GigabitEthernet 0/1)# ip verify urpf drop-rate notify
```

【检验方法】 1：使用 **show ip urpf** 命令，可以查看接口是否启动 URPF 丢包信息监控。

【提示信息】 -

【常见错误】 -

【平台说明】 -

11.5 ip verify urpf drop-rate notify hold-down

全局配置 URPF IPv4 丢包率的告警时间间隔。

ip verify urpf drop-rate notify hold-down *seconds*

恢复缺省配置。

no ip verify urpf drop-rate notify hold-down

【参数说明】

参数	描述
hold-down <i>seconds</i>	URPF 丢包率的告警时间间隔。 单位为秒，范围[30, 300]，缺省值 300s。

【缺省配置】 缺省值为 300s。

【命令模式】 全局配置模式

【缺省级别】 14

【使用指导】 URPF 丢包率的告警时间间隔基于全局配置模式进行配置，将应用于全局的 URPF 丢包率告警和基于每个启动 URPF 特性的接口的 URPF 丢包率告警，并且同时对 IPv4 URPF 生效。

【配置举例】 1：配置 URPF 丢包率的告警时间间隔为 1 分钟。

```
Ruijie(config)# ip verify urpf drop-rate notify hold-down 60
```

【检验方法】 1：使用 **show ip urpf** 命令，可以查看 URPF 丢包率的告警时间间隔。

【提示信息】 -

【常见错误】 -

【平台说明】 -

11.6 ip verify urpf notification threshold

配置 URPF 丢包率的水线值。

ip verify urpf notification threshold *rate-value*

恢复缺省配置。

no ip verify urpf notification threshold

【参数说明】	参数	描述
	threshold <i>rate-value</i>	URPF 丢包率的水线值。 单位为 pps(packets per second) ,范围[0, 4294967295] ,缺省值 1000pps。
【缺省配置】	缺省值为 1000pps。	
【命令模式】	接口配置模式	
【缺省级别】	14	
【使用指导】	如果水线值为 0，表示监测到任何一个因 URPF 检查而丢弃的报文就会发送通告。 用户可以根据网络实际情况调整丢包率水线值。	
【配置举例】	1：配置接口 GigabitEthernet 0/1 上 URPF 丢包率的水线值为每秒 10 个报文。 <pre>Ruijie(config)# interface gigabitEthernet0/1 Ruijie(config-if-GigabitEthernet 0/1)# ip verify urpf drop-rate notify Ruijie(config-if-GigabitEthernet 0/1)# ip verify urpf notification threshold 10</pre>	
【检验方法】	1：使用 show ip urpf 命令，可以查看接口配置的 URPF 丢包率的水线值。	
【提示信息】	-	
【常见错误】	-	
【平台说明】	-	

11.7 show ip urpf

查看 IPv4 URPF 配置及统计信息。

show ip urpf [**interface** *interface-name*]

【参数说明】	参数	描述
	interface <i>interface-name</i>	查看指定接口的配置及统计信息。
【命令模式】	特权模式、全局模式、接口模式	
【缺省级别】	1	

【使用指导】 如果没有配置指定接口，将显示全局和所有接口的配置及统计信息。

【配置举例】 1：显示指定接口 GigabitEthernet 0/1 上的 URPF 配置及统计信息

```
Ruijie# show ip urpf interface gigabitEthernet0/1
IP verify source reachable-via RX
IP verify URPF drop-rate notify disabled
IP verify URPF notification threshold is 1000pps
Number of drop packets in this interface is 124
Number of drop-rate notification counts in this interface is 2
```

字段解释：

字段	说明
IP verify source reachable-via xx	如果是严格模式，则 xx 是 RX；如果是宽松模式，则 xx 是 ANY。
IP verify URPF drop-rate notify xx	如果开启丢报信息监控，则 xx 是 enabled，否则 xx 是 disabled。
IP verify URPF notification threshold is xxpps	URPF 丢包率的水线值。 单位为 pps (packets per second)，范围 [0, 4294967295]，缺省值 1000pps。
Number of drop packets in this interface is x	丢包数。
Number of drop-rate notification counts in this interface is x	URPF 丢包信息监控通告次数。

2：查看设备的 IPv4 URPF 配置及统计信息

```
Ruijie# show ip urpf
IP verify URPF drop-rate compute interval is 30s
IP verify URPF drop-rate notify hold-down is 300s

Interface GigabitEthernet 0/1
IP verify source reachable-via RX
IP verify URPF drop-rate notify disabled
IP verify URPF notification threshold is 1000pps
Number of drop packets in this interface is 124
Number of drop-rate notification counts in this interface is 2
```

字段解释：

字段	说明
IP verify URPF drop-rate compute interval is x	丢包率的计算时间间隔。
IP verify URPF drop-rate notify hold-down is x	丢包率的告警时间间隔。
Interface interface-name	interface-name 是应用 URPF 的接口名称 ,在此字段下显示的是此接口的配置及统计信息。

【提示信息】 -

【平台说明】 -

12 CPP

命令	作用
<u>clear cpu-protect counters</u>	清除 CPP 的统计信息
<u>clear cpu-protect mboard</u>	清除主设备的 CPP 的统计信息
<u>cpu-protect cpu bandwidth</u>	配置 CPU 端口的带宽。
<u>cpu-protect traffic-class traffic-class-num bandwidth</u>	配置某个优先级队列的带宽。
<u>cpu-protect type packet-type bandwidth</u>	配置某个报文类型对应的带宽。
<u>cpu-protect type packet-type traffic-class</u>	配置某个报文类型对应的优先级队列。
<u>show cpu-protect</u>	显示 CPP 所有信息。
<u>show cpu-protect cpu</u>	显示 CPU 端口相关信息。
<u>show cpu-protect mboard</u>	显示主设备上 CPP 所有信息。
<u>show cpu-protect summary</u>	显示主设备上 CPP 所有信息。
<u>show cpu-protect traffic-class</u>	显示优先级队列相关信息。
<u>show cpu-protect type</u>	显示报文类型相关信息。

12.1 clear cpu-protect counters

清除 CPP 的统计信息。

clear cpu-protect counters [*device device_num*]

【参数说明】

参数	描述
<i>device_num</i>	在单机情况下， device 关键字不可见；在 VSU 情况下， <i>device</i> 用于表示对应机箱或者盒式设备，若未输入 device 关键字，表示主机箱或者主设备。

【命令模式】 特权模式

【缺省级别】 14

【使用指导】 -

【配置举例】 1：清除 cpp 的统计信息。

```
Ruijie(config)#show cpu-protect type bpdu
Packet Type      Traffic-class  Bandwidth(pps)  Rate(pps)  Drop(pps)  Total  Total Drop
-----
bpdu              6              200              0           0           600    50
Ruijie#clear cpu-protect counters
Ruijie(config)#show cpu-protect type bpdu
Packet Type      Traffic-class  Bandwidth(pps)  Rate(pps)  Drop(pps)  Total  Total Drop
```

-----	-----	-----	-----	-----	-----	-----
bpdu	6	200	0	0	0	0

【提示信息】 -

【平台说明】 -

12.2 clear cpu-protect counters mboard

清除主设备的 CPP 的统计信息。

clear cpu-protect counters mboard

【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：清除主设备的 cpp 的统计信息。

Ruijie(config)#show cpu-protect type bpdu						
Packet Type	Traffic-class	Bandwidth(pps)	Rate(pps)	Drop(pps)	Total	Total Drop
-----	-----	-----	-----	-----	-----	-----
bpdu	6	200	0	0	600	50
Ruijie#clear cpu-protect counters mboard						
Ruijie(config)#show cpu-protect type bpdu						
Packet Type	Traffic-class	Bandwidth(pps)	Rate(pps)	Drop(pps)	Total	Total Drop
-----	-----	-----	-----	-----	-----	-----
bpdu	6	200	0	0	0	0

【提示信息】 -

【平台说明】 -

12.3 cpu-protect cpu bandwidth

配置 cpu 端口对应的带宽。

cpu-protect cpu bandwidth *bandwidth_value*

将 cpu 端口的带宽恢复为缺省值。

no cpu-protect cpu bandwidth

【参数说明】	参数	描述
	<i>bandwidth_value</i>	整数，取值范围 0-100000（pps），表示配置的具体带宽值。

【缺省配置】 CPU 端口的缺省带宽与产品相关，具体参见产品特性文档。

【命令模式】 全局模式

【缺省级别】 14

【使用指导】 -

【配置举例】 1：配置 CPU 端口的带宽为 32000 pps。

```
Ruijie# configure terminal
Ruijie(config)# cpu-protect cpu bandwidth 32000
Ruijie#show cpu-protect cpu
%cpu port bandwidth: 32000(pps)
```

【检验方法】 可以通过 **show cpu-protect cpu** 命令查看设置的 CPU 端口的带宽。

【提示信息】 -

【常见错误】 -

【平台说明】 -

12.4 cpu-protect traffic-class *traffic-class-num* bandwidth

配置某个优先级队列对应的带宽。

cpu-protect traffic-class *traffic-class-num* **bandwidth** *bandwidth_value*

将某个优先级队列的带宽恢复为缺省值。

no cpu-protect traffic-class *traffic-class-num* **bandwidth**

【参数说明】	参数	描述
	<i>traffic-class-num</i>	整数，取值范围不同产品存在差异，具体参见产品特性文档，表示具体的优先级队列。
	<i>bandwidth_value</i>	整数，取值范围 0-100000（pps），表示配置的具体带宽值。
【缺省配置】	各优先级队列的缺省带宽与产品相关，具体参见产品特性文档。	
【命令模式】	全局模式	
【缺省级别】	14	
【使用指导】	-	
【配置举例】	1：配置优先级队列 5 的带宽为 3500 pps。 <pre> Ruijie# configure terminal Ruijie(config)# cpu-protect traffic-class 5 bandwidth 3500 Ruijie#show cpu-protect traffic-class 5 Traffic-class Bandwidth(pps) Rate(pps) Drop(pps) ----- 5 3500 0 0 </pre>	
【检验方法】	可以通过 show cpu-protect traffic-class <i>traffic-class-num</i> 命令查看设置的优先级队列的带宽。	
【提示信息】	-	
【常见错误】	-	
【平台说明】	-	

12.5 cpu-proctect type *packet-type* bandwidth

配置某个报文类型对应的带宽。

cpu-protect type *packet-type* bandwidth *bandwidth_value*

将某个报文类型对应的带宽恢复为缺省值。

no cpu-protect type *packet-type* bandwidth

【参数说明】	参数	描述
	<i>packet-type</i>	交换机固定划分的报文类型，不同产品存在差异，具体参见产品特性文档。
	<i>bandwidth_value</i>	整数，取值范围 0-32000（pps），表示配置的具体带宽值。

【缺省配置】 各报文类型的缺省带宽配置与产品相关，具体参见产品特性文档。

【命令模式】 全局模式

【缺省级别】 14

【使用指导】

【配置举例】 1：配置报文 bpu 的带宽为 200 pps。

```
Ruijie# configure terminal
Ruijie(config)# cpu-protect type bpu bandwidth 200
Ruijie(config)# show cpu-protect type bpu
```

Packet Type	Traffic-class	Bandwidth(pps)	Rate(pps)	Drop(pps)	Total	Total Drop
bpu	6	200	0	0	0	0

【检验方法】 使用 **show cpu-protect type packet-type** 命令查看设置的报文对应带宽。

【提示信息】 -

【常见错误】 -

【平台说明】 -

12.6 cpu-protect type packet-type traffic-class

配置某个报文类型对应的优先级队列。

cpu-protect type packet-type traffic-class traffic-class-num

将某个报文类型对应的优先级队列恢复为缺省值。

no cpu-protect type packet-type traffic-class

【参数说明】	参数	描述
	packet-type	交换机固定划分的报文类型，不同产品存在差异，具体参见产品特性文档。
	traffic-class-num	整数，取值范围不同产品存在差异，具体参见产品特性文档，表示具体的优先级队列。

【缺省配置】 各报文类型的缺省优先级队列与产品相关，具体参见产品特性文档。

【命令模式】 全局模式

【缺省级别】 14

【使用指导】 -

【配置举例】 1：配置报文 bpu 的优先级队列为 5。

```
Ruijie# configure terminal
Ruijie(config)# cpu-protect type bpu traffic-class 5
Ruijie(config)#show cpu-protect type bpu
```

Packet Type	Traffic-class	Bandwidth(pps)	Rate(pps)	Drop(pps)	Total	Total Drop
bpu	5	200	0	0	0	0

【检验方法】 使用 **show cpu-protect type packet-type** 命令查看设置的报文对应优先级队列。

【提示信息】 -

【常见错误】 -

【平台说明】 -

12.7 show cpu-protect

显示 CPP 相关的所有配置及统计信息。

show cpu-protect [**device** *device_num*]

【参数说明】

参数	描述
<i>device_num</i>	在单机情况下， device 关键字不可见；在 VSU 情况下， <i>device</i> 用于表示对应机箱或者盒式设备，若未输入 device 关键字，表示主机箱或者主设备。

【命令模式】 各模式均可执行。

【缺省级别】 14

【使用指导】 -

【配置举例】 1：查看某线卡的 CPP 所有配置及统计信息。

```
Ruijie#show cpu-protect
%cpu port bandwidth: 80000(pps)
Traffic-class  Bandwidth(pps)  Rate(pps)      Drop(pps)
-----
```

0	8000	0	0			
1	8000	0	0			
2	8000	0	0			
3	8000	0	0			
4	8000	0	0			
5	8000	0	0			
6	8000	0	0			
7	8000	0	0			
Packet Type	Traffic-class	Bandwidth(pps)	Rate(pps)	Drop(pps)	Total	Total Drop
bpdu	6	128	0	0	0	0
arp	3	10000	0	0	0	0
arp-dai	3	10000	0	0	0	0
arp-proxy	3	10000	0	0	0	0
tpp	7	128	0	0	0	0
dot1x	4	128	0	0	0	0
gvrp	5	128	0	0	0	0
rldp	6	128	0	0	0	0
lacp	6	128	0	0	0	0
rerp	6	128	0	0	0	0
reup	6	128	0	0	0	0
lldp	5	128	0	0	0	0
cdp	5	128	0	0	0	0
dhcps	4	128	0	0	0	0
dhcps6	4	128	0	0	0	0
dhcp6-client	4	128	0	0	0	0
dhcp6-server	4	128	0	0	0	0
dhcp-relay-c	4	128	0	0	0	0
dhcp-relay-s	4	128	0	0	0	0
option82	4	128	0	0	0	0
tunnel-bpdu	5	128	0	0	0	0
tunnel-gvrp	5	128	0	0	0	0
unknown-v6mc	3	128	0	0	0	0
known-v6mc	3	128	0	0	0	0
xgv6-ipmc	3	128	0	0	0	0
stargv6-ipmc	3	128	0	0	0	0
unknown-v4mc	3	128	0	0	0	0
known-v4mc	3	128	0	0	0	0
xgv-ipmc	3	128	0	0	0	0
sgv-ipmc	3	128	0	0	0	0
udp-helper	4	128	0	0	0	0

dvmp	5	128	0	0	0	0
igmp	4	128	0	0	0	0
icmp	4	128	0	0	0	0
ospf	5	128	0	0	0	0
ospf3	5	128	0	0	0	0
pim	6	128	0	0	0	0
pimv6	6	128	0	0	0	0
rip	6	128	0	0	0	0
ripng	6	128	0	0	0	0
vrrp	6	128	0	0	0	0
vrrp6	6	128	0	0	0	0
ttl0	6	128	0	0	0	0
ttl1	6	128	0	0	0	0
err_hop_limit	1	800	0	0	0	0
local-ipv4	6	128	0	0	0	0
local-ipv6	6	128	0	0	0	0
route-host-v4	0	4096	0	0	0	0
route-host-v6	0	4096	0	0	0	0
mld	0	1000	0	0	0	0
nd-snp-ns-na	6	128	0	0	0	0
nd-snp-rs	6	128	0	0	0	0
nd-snp-ra-redirect	6	128	0	0	0	0
nd-non-snp	6	128	0	0	0	0
erps	4	128	0	0	0	0
mpls-ttl0	6	128	0	0	0	0
mpls-ttl1	6	128	0	0	0	0
mpls-ctrl	6	128	0	0	0	0
isis	5	2000	0	0	0	0
bgp	1	128	0	0	0	0
cfm	0	128	0	0	0	0
fcoe-fip	6	128	0	0	0	0
fcoe-local	6	128	0	0	0	0
bfd-echo	6	5120	0	0	0	0
bfd-ctrl	6	5120	0	0	0	0
madp	7	1000	0	0	0	0
ip4-other	6	128	0	0	0	0
ip6-other	6	128	0	0	0	0
non-ip-other	6	20000	0	0	0	0
trill	2	1000	0	0	0	0
trill-oam	2	1000	0	0	0	0
efm	2	1000	0	0	0	0

【提示信息】 -

【平台说明】 -

12.8 show cpu-protect cpu

显示 cpu 端口的配置信息。

show cpu-protect cpu

【参数说明】

参数	描述
-	-

【命令模式】 各模式均可执行。

【缺省级别】 14

【使用指导】 -

【配置举例】 1：查看 cpu 端口的配置信息。

```
Ruijie#show cpu-protect cpu
%cpu port bandwidth: 32000(pps)
```

【提示信息】 -

【平台说明】 -

12.9 show cpu-protect mboard

显示主设备上 CPP 相关的所有配置及统计信息。

show cpu-protect mboard

【参数说明】

参数	描述
-	-

【命令模式】 各模式均可执行。

【缺省级别】 14

【使用指导】 -

【配置举例】 1：查看主设备上的 CPP 所有配置及统计信息。

```
Ruijie#show cpu-protect mboard
```

```
%cpu port bandwidth: 80000(pps)
```

Traffic-class	Bandwidth(pps)	Rate(pps)	Drop(pps)
0	8000	0	0
1	8000	0	0
2	8000	0	0
3	8000	0	0
4	8000	0	0
5	8000	0	0
6	8000	0	0
7	8000	0	0

Packet Type	Traffic-class	Bandwidth(pps)	Rate(pps)	Drop(pps)	Total	Total Drop
bpdu	6	128	0	0	0	0
arp	3	10000	0	0	0	0
arp-dai	3	10000	0	0	0	0
arp-proxy	3	10000	0	0	0	0
tpp	7	128	0	0	0	0
dot1x	4	128	0	0	0	0
gvrp	5	128	0	0	0	0
rldp	6	128	0	0	0	0
lacp	6	128	0	0	0	0
rerp	6	128	0	0	0	0
reup	6	128	0	0	0	0
lldp	5	128	0	0	0	0
cdp	5	128	0	0	0	0
dhcps	4	128	0	0	0	0
dhcps6	4	128	0	0	0	0
dhcp6-client	4	128	0	0	0	0
dhcp6-server	4	128	0	0	0	0
dhcp-relay-c	4	128	0	0	0	0
dhcp-relay-s	4	128	0	0	0	0
option82	4	128	0	0	0	0
tunnel-bpdu	5	128	0	0	0	0
tunnel-gvrp	5	128	0	0	0	0
unknown-v6mc	3	128	0	0	0	0
known-v6mc	3	128	0	0	0	0
xgv6-ipmc	3	128	0	0	0	0

stargv6-ipmc	3	128	0	0	0	0
unknown-v4mc	3	128	0	0	0	0
known-v4mc	3	128	0	0	0	0
xgv-ipmc	3	128	0	0	0	0
sgv-ipmc	3	128	0	0	0	0
udp-helper	4	128	0	0	0	0
dvmrp	5	128	0	0	0	0
igmp	4	128	0	0	0	0
icmp	4	128	0	0	0	0
ospf	5	128	0	0	0	0
ospf3	5	128	0	0	0	0
pim	6	128	0	0	0	0
pimv6	6	128	0	0	0	0
rip	6	128	0	0	0	0
ripng	6	128	0	0	0	0
vrrp	6	128	0	0	0	0
vrrp6	6	128	0	0	0	0
ttl0	6	128	0	0	0	0
ttl1	6	128	0	0	0	0
err_hop_limit	1	800	0	0	0	0
local-ipv4	6	128	0	0	0	0
local-ipv6	6	128	0	0	0	0
route-host-v4	0	4096	0	0	0	0
route-host-v6	0	4096	0	0	0	0
mld	0	1000	0	0	0	0
nd-snp-ns-na	6	128	0	0	0	0
nd-snp-rs	6	128	0	0	0	0
nd-snp-ra-redirect	6	128	0	0	0	0
nd-non-snp	6	128	0	0	0	0
erps	4	128	0	0	0	0
mpls-ttl0	6	128	0	0	0	0
mpls-ttl1	6	128	0	0	0	0
mpls-ctrl	6	128	0	0	0	0
isis	5	2000	0	0	0	0
bgp	1	128	0	0	0	0
cfm	0	128	0	0	0	0
fcoe-fip	6	128	0	0	0	0
fcoe-local	6	128	0	0	0	0
bfd-echo	6	5120	0	0	0	0
bfd-ctrl	6	5120	0	0	0	0
madp	7	1000	0	0	0	0

ip4-other	6	128	0	0	0	0
ip6-other	6	128	0	0	0	0
non-ip-other	6	20000	0	0	0	0
trill	2	1000	0	0	0	0
trill-oam	2	1000	0	0	0	0
efm	2	1000	0	0	0	0

【提示信息】 -

【平台说明】 -

12.10 show cpu-protect summary

显示主设备上 CPP 相关的所有配置及统计信息。

show cpu-protect summary

【参数说明】

参数	描述
-	-

【命令模式】 各模式均可执行。

【缺省级别】 14

【使用指导】 -

【配置举例】 1：查看主设备上的 CPP 所有配置及统计信息。

```
Ruijie#show cpu-protect summary
```

```
%cpu port bandwidth: 80000(pps)
```

Traffic-class	Bandwidth(pps)	Rate(pps)	Drop(pps)
0	8000	0	0
1	8000	0	0
2	8000	0	0
3	8000	0	0
4	8000	0	0
5	8000	0	0
6	8000	0	0
7	8000	0	0

Packet Type	Traffic-class	Bandwidth(pps)	Rate(pps)	Drop(pps)	Total	Total Drop
-----	-----	-----	-----	-----	-----	-----

bpdv	6	128	0	0	0	0
arp	3	10000	0	0	0	0
arp-dai	3	10000	0	0	0	0
arp-proxy	3	10000	0	0	0	0
tpp	7	128	0	0	0	0
dot1x	4	128	0	0	0	0
gvrp	5	128	0	0	0	0
rldp	6	128	0	0	0	0
larp	6	128	0	0	0	0
rerp	6	128	0	0	0	0
reup	6	128	0	0	0	0
lldp	5	128	0	0	0	0
cdp	5	128	0	0	0	0
dhcps	4	128	0	0	0	0
dhcps6	4	128	0	0	0	0
dhcp6-client	4	128	0	0	0	0
dhcp6-server	4	128	0	0	0	0
dhcp-relay-c	4	128	0	0	0	0
dhcp-relay-s	4	128	0	0	0	0
option82	4	128	0	0	0	0
tunnel-bpdu	5	128	0	0	0	0
tunnel-gvrp	5	128	0	0	0	0
unknown-v6mc	3	128	0	0	0	0
known-v6mc	3	128	0	0	0	0
xgv6-ipmc	3	128	0	0	0	0
stargv6-ipmc	3	128	0	0	0	0
unknown-v4mc	3	128	0	0	0	0
known-v4mc	3	128	0	0	0	0
xgv-ipmc	3	128	0	0	0	0
sgv-ipmc	3	128	0	0	0	0
udp-helper	4	128	0	0	0	0
dvmrp	5	128	0	0	0	0
igmp	4	128	0	0	0	0
icmp	4	128	0	0	0	0
ospf	5	128	0	0	0	0
ospf3	5	128	0	0	0	0
pim	6	128	0	0	0	0
pimv6	6	128	0	0	0	0
rip	6	128	0	0	0	0
ripng	6	128	0	0	0	0
vrrp	6	128	0	0	0	0

vrrp6	6	128	0	0	0	0
ttl0	6	128	0	0	0	0
ttl1	6	128	0	0	0	0
err_hop_limit	1	800	0	0	0	0
local-ipv4	6	128	0	0	0	0
local-ipv6	6	128	0	0	0	0
route-host-v4	0	4096	0	0	0	0
route-host-v6	0	4096	0	0	0	0
mld	0	1000	0	0	0	0
nd-snp-ns-na	6	128	0	0	0	0
nd-snp-rs	6	128	0	0	0	0
nd-snp-ra-redirect	6	128	0	0	0	0
nd-non-snp	6	128	0	0	0	0
erps	4	128	0	0	0	0
mpls-ttl0	6	128	0	0	0	0
mpls-ttl1	6	128	0	0	0	0
mpls-ctrl	6	128	0	0	0	0
isis	5	2000	0	0	0	0
bgp	1	128	0	0	0	0
cfm	0	128	0	0	0	0
fcoe-fip	6	128	0	0	0	0
fcoe-local	6	128	0	0	0	0
bfd-echo	6	5120	0	0	0	0
bfd-ctrl	6	5120	0	0	0	0
madp	7	1000	0	0	0	0
ip4-other	6	128	0	0	0	0
ip6-other	6	128	0	0	0	0
non-ip-other	6	20000	0	0	0	0
trill	2	1000	0	0	0	0
trill-oam	2	1000	0	0	0	0
efm	2	1000	0	0	0	0

【提示信息】 -

【平台说明】 -

12.11 show cpu-protect traffic-class

显示优先级队列的配置及统计信息。

show cpu-protect traffic-class {*traffic-class-num* | **all**} [**device** *device_num*]

【参数说明】

参数	描述
<i>traffic-class-num</i>	整数，取值范围不同产品存在差异，具体参见产品特性文档，表示具体的优先级队列。
<i>all</i>	显示所有的优先级队列对应配置及统计信息。
<i>device_num</i>	在单机情况下， device 关键字不可见；在 VSU 情况下， <i>device</i> 用于表示对应机箱或者盒式设备，若未输入 device 关键字，表示主机箱或者主设备。

【命令模式】 各模式均可执行。

【缺省级别】 14

【使用指导】 -

【配置举例】 1：查看主设备上的所有优先级队列的配置及统计信息。

```
Ruijie#show cpu-protect traffic-class all
```

Traffic-class	Bandwidth(pps)	Rate(pps)	Drop(pps)
0	8000	0	0
1	8000	0	0
2	8000	0	0
3	8000	0	0
4	8000	0	0
5	3200	0	0
6	8000	0	0
7	8000	0	0

【提示信息】 -

【平台说明】 -

12.12 show cpu-protect type

显示报文类型的配置及统计信息。

show cpu-protect type *packet-type* [**device** *device_num*]

【参数说明】

参数	描述
<i>packt-type</i>	交换机固定划分的报文类型，不同产品存在差异，具体参见产品特性文档。
<i>all</i>	显示所有的报文类型对应配置及统计信息。
<i>device_num</i>	在单机情况下， device 关键字不可见；在 VSU 情况下， <i>device</i> 用于表示对应机箱或者盒式设备，若未输入 device 关键字，表示主机箱或者主设备。

【命令模式】 各模式均可执行。

【缺省级别】 14

【使用指导】 -

【配置举例】 1：查看主设备上的 icmp 报文的配置及统计信息。

```
Ruijie(config)#show cpu-protect type icmp
```

Packet Type	Traffic-class	Bandwidth(pps)	Rate(pps)	Drop(pps)	Total	Total Drop
icmp	5	1500	50	0	10000	100

【提示信息】 -

【平台说明】 -

13 DHCP Snooping

命令	作用
clear ip dhcp snooping binding	删除 DHCP Snooping 数据库中的所有动态用户。
ip dhcp snooping	启动全局 DHCP Snooping 功能。
ip dhcp snooping bootp-bind	启动 DHCP Snooping 支持 Bootp 绑定功能。
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-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 information option	在 DHCP 请求报文中加入 option82 选项。
ip dhcp snooping information option format remote-id	设置 option82 选项的子选项 remote-id 为自定义字符串。
ip dhcp snooping suppression	配置接口为 suppression 状态。
ip dhcp snooping trust	配置接口的 DHCP snooping 信任状态为 TRUST 口。
ip dhcp snooping verify mac-address	打开源 MAC 地址校验功能。
ip dhcp snooping vlan	打开指定 VLAN 的 DHCP Snooping 功能。
ip dhcp snooping vlan vlan-id information option change-vlan-to vlan	打开 option82 选项的子选项 circuit-id，修改 circuit-id 中的 VLAN 为指定 VLAN。
ip dhcp snooping vlan vlan-id information option format-type circuit-id string	配置 option 82 选项的子选项 circuit-id 为用户自定义的内容(存储格式为 ASCII) 并进行转发。
ip dhcp snooping vlan max-user	配置接口下指定 VLAN 上最大允许生成的绑定用户个数。
renew ip dhcp snooping database	手动地把当前 flash 中的信息导入 DHCP Snooping 绑定数据库。
show ip dhcp snooping	查看 DHCP Snooping 当前的配置情况。
show ip dhcp snooping binding	查看 DHCP Snooping 数据库中的用户信息。

13.1 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*]

【参数说明】

参数	描述
<i>mac</i>	指定删除的用户的 MAC 地址。
<i>vlan-id</i>	指定删除的用户的 vlan id。
<i>ip</i>	指定删除的用户的 IP 地址。
<i>interface-id</i>	指定删除的用户所属的接口。

【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】 -

13.2 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】 -

【常见错误】 -

【平台说明】 -

13.3 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】 -

13.4 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】 -

13.5 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。

【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】 -

13.6 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]

【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。
- 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】

-

13.7 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 <i>ascii-string</i>	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】-

13.8 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
- 【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 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
```

【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】 -

13.9 ip dhcp snooping trust

配置接口的 DHCP snooping 信任状态为 TRUST 口。

ip dhcp snooping trust

配置接口的 DHCP snooping 信任状态为 UNTRUST 口。

no ip dhcp snooping trust

【参数说明】	参数	描述
	-	-

【缺省配置】 缺省情况下，所有接口为 UNTRUST 口。

【命令模式】 接口配置模式

【缺省级别】 14

【使用指导】 1：通过配置该命令，将连接合法 DHCP 服务器的接口配置为 TRUST 口。TRUST 接口收到的所有 DHCP 响应报文被正常转发，UNTRUST 接口收到的所有 DHCP 响应报文将被丢弃。
2：该命令配置在二层交换口、AP 口或者封装子接口上会立刻生效。其他接口上配置该命令将会失败。

 通常将上链口，即连接信任 DHCP 服务器的接口设置为 TRUST 口。

【配置举例】 1：下面是配置接口 GigabitEthernet 0/1 为 TRUST 口的例子：

```
Ruijie# configure terminal
```



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

【检验方法】 1：使用 **show ip dhcp snooping** 命令，可以查看接口的信任状态。

【提示信息】 1：如果接口上配置了其他接入安全控制选项，无法设置成 TRUST 口。

```
% Failed to execute command, because of "Security config conflict".
```

2：当不是在 2 层交换口、AP 口或者封装子接口上执行该命令时，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】 -

13.10 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】 -

13.11 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
<i>vlan-rng</i>	dhcp snooping 功能生效的 vlan 范围。
<i>vlan-min</i>	dhcp snooping 功能生效的 vlan 下限。
<i>vlan-max</i>	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】 -

13.12 ip dhcp snooping vlan vlan-id information option change-vlan-to vlan

设置 option82 选项处于扩展模式时，子选项 circuit-id 中的 VLAN 为指定 VLAN。

ip dhcp snooping vlan *vlan-id* information option change-vlan-to vlan *vlan-id*

关闭该功能。

no ip dhcp snooping vlan *vlan-id* information option change-vlan-to vlan *vlan-id*

【参数说明】	参数	描述
	<i>vlan-id</i>	指定进行替换的 VLAN 编号

【缺省配置】 该功能缺省关闭。

【命令模式】 接口配置模式

【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 的子选项 circuit-id 填充的 VLAN 修改为指定的 VLAN。

【配置举例】 1：下面是配置在 DHCP 请求报文中添加 option82 选项，其中 option82 的子选项 circuit-id 中的 VLAN4094 修改为 VLAN4093 的例子：

```
Ruijie# configure terminal
Ruijie(config)# interface GigabitEthernet 0/1
Ruijie(config-if-GigabitEthernet 0/1)# ip dhcp snooping vlan 4094 information option change-vlan-to vlan 4093
```

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

【检验方法】 1：使用 **show run** 命令，可以查看功能是否开启。

【提示信息】 1：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】 -

13.13 ip dhcp snooping vlan vlan-id information option format-type circuit-id string

设置 option82 选项处于扩展模式时，子选项 circuit-id 为用户自定义的内容（存储格式为 ASCII）并进行转发。

ip dhcp snooping vlan *vlan-id* information option format-type circuit-id string *ascii-string*

关闭此功能。

no ip dhcp snooping vlan *vlan-id* information option format-type circuit-id string *ascii-string*

【参数说明】	参数	描述
	<i>vlan-id</i>	DHCP 请求报文所在 VLAN
	<i>ascii-string</i>	Circuit ID 要填充的用户自定义的内容

【缺省配置】 该功能缺省关闭。

【命令模式】 接口配置模式

【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 的子选项 circuit-id 内容设置为自定义内容。该内容为长度 3 到 63 字节的字符串。

【配置举例】 1：下面是配置在 DHCP 请求报文中加入 option82 选项，其中 option82 的子选项 circuit-id 内容为 port-name 的例子：

```
Ruijie# configure terminal
Ruijie(config)# interface GigabitEthernet 0/1
Ruijie(config-if-GigabitEthernet 0/1)# ip dhcp snooping vlan 4094 information option format-type
circuit-id string port-name
Ruijie(config-if-GigabitEthernet 0/1)# end
```

【检验方法】 1：使用 **show run** 命令，可以查看功能是否开启。

【提示信息】 1：若指定的 VLAN 不存在，则提示错误。

% Failed to execute command, because of "VLAN not exist".

2：若指定的自定义字符串不是 3 到 63 个字符，则提示错误。

% Failed to execute command, because of "Circuit-ID string must be 3 to 63 characters".

【常见错误】 -

【平台说明】 -

13.14 ip dhcp snooping vlan max-user

设置接口上指定 vlan 下最大允许生成的绑定用户个数。

ip dhcp snooping vlan *vlan-word* **max-user** *user-number*

关闭此功能。

no ip dhcp snooping vlan *vlan-word* **max-user** *user-number*

【参数说明】	参数	描述
	<i>vlan-word</i>	功能生效的 vlan 范围
	<i>user-number</i>	允许的最大用户数量

【缺省配置】 该功能缺省关闭。

【命令模式】 接口配置模式

【缺省级别】 14

【使用指导】 通过配置该命令,开启基于接口和 VLAN 的绑定用户限制,配合相应的网络拓扑结构,可以起到防止伪造 DHCP 报文攻击的作用。

【配置举例】 1：下面是配置在接口 1 的 VLAN 1~10 及 VLAN 20 上面开启绑定用户数目限制，最多允许 30 个用户：

```
Ruijie# configure terminal
Ruijie(config)# interface GigabitEthernet 0/1
Ruijie(config-if-GigabitEthernet 0/1)# ip dhcp snooping vlan 1-10,20 max-user 30
Ruijie(config-if-GigabitEthernet 0/1)# end
```

【检验方法】 1：使用 **show run** 命令，可以查看功能是否开启。

- 【提示信息】

1：若接口为 DHCP snooping TRUST 口，则提示错误。
% Failed to execute command, because of "Security configuration conflict in interface GigabitEthernet 0/1".

2：若指定接口 VLAN 上面已经生成的绑定数大于命令中配置的最大用户数，则提示错误。
% Failed to execute command, because of "New max address number little more than the current".
- 【常见错误】

-
- 【平台说明】

-

13.15 renew ip dhcp snooping database

手动地把当前 flash 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 flash 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 flash 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】

-

13.16 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 flash 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】 -

13.17 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

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。
Interface	用户连接端口，有线接入接口

【提示信息】

-

【平台说明】

-

14 ARP Check

命令	作用
arp-check	开启 ARP 报文检查。
show interface arp-check list	查看接口下实际生效的 ARP Check 表项。

14.1 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

【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。

【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
```

【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】 -

14.2 show interface arp-check list

查看接口下实际生效的 ARP Check 表项。

show interface [*interface-type interface-number*] **arp-check list**

【参数说明】

参数	描述
<i>interface-type</i>	接口类型；
<i>interface-number</i>	接口编号；

【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 interface 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

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】

-

15 DAI

命令	作用
ip arp inspection trust	配置二层端口为 DAI 可信任口。
ip arp inspection vlan	配置 VLAN 启用 DAI 功能。
show ip arp inspection vlan	显示 VLAN 是否打开 DAI 检查功能。
show ip arp inspection interface	查看端口是否配置成功信任状态。

15.1 ip arp inspection trust

配置二层端口为 DAI 可信任口。

ip arp inspection trust

配置二层端口为 DAI 不可信任口。

no ip arp inspection trust

【参数说明】	参数	描述
	-	-

【缺省配置】 端口处于不信任状态。

【命令模式】 接口配置模式

【缺省级别】 14

【使用指导】 当需要使某个接口收到的 ARP 报文无条件的通过 DAI 的检查时， 可以将该接口设置成受信任状态，表示我们不需要检查此接口收到的 ARP 报文，它们是合法的。

【配置举例】 以下的配置例子，将 gigabitEthernet 0/19 接口设置成受信任：

```
Ruijie# configure terminal
Ruijie(config)# interface gigabitEthernet 0/19
Ruijie(config-if-GigabitEthernet 0/19)# ip arp inspection trust
Ruijie(config-if-GigabitEthernet 0/19)# end
```

【检验方法】 1：使用 **show ip arp inspection interface** 命令，可以查看端口是否配置成功。

【提示信息】 -

【常见错误】 -

【平台说明】 -

15.2 ip arp inspection vlan

配置 VLAN 启用 DAI 功能。

ip arp inspection vlan { *vlan-id* | *word* }

配置 VLAN 关闭 DAI 功能。

no ip arp inspection vlan { *vlan-id* | *word* }

【参数说明】

参数	描述
<i>vlan-id</i>	表示 vlan 编号，取值范围为 1~4094。
<i>word</i>	vlan 范围字符串，如 1,3-5,7,9-11

【缺省配置】 所有 VLAN 上关闭 DAI 报文检查功能。

【命令模式】 全局配置模式

【缺省级别】 14

【使用指导】 要使命令发挥作用，首先需要启用 ARP-Check 功能。

 并非 VLAN 上所有接口都能开启 ARP 报文检查，当接口为 DHCP Snooping TRUST 口时，不允许在接口上配置任何安全检查规则。

【配置举例】 以下配置，为检查 VLAN 1 上接收到的 ARP 报文。：

```
Ruijie# configure terminal
Ruijie(config)# ip arp inspection
Ruijie(config)# ip arp inspection vlan 1
Ruijie(config)# end
```

【检验方法】 1：使用 **show ip arp inspection vlan** 命令，可以显示 VLAN 是否打开 DAI 检查功能。

【提示信息】 -

【常见错误】 -

【平台说明】 -

15.3 show ip arp inspection vlan

显示 VLAN 是否打开 DAI 检查功能。

show ip arp inspection vlan [*vlan-id* | *word*]

【参数说明】

参数	描述
<i>vlan-id</i>	表示 vlan 编号，取值范围为 1~4094。
<i>word</i>	vlan 范围字符串，如 1,3-5,7,9-11

【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所有 VLAN 上的 DAI 开关。

【配置举例】

1：查看所有 VLAN 的 DAI 开关

```
Ruijie# show ip arp inspection vlan
Vlan      Configuration
-----
1         Active
```

字段解释：

字段	说明
Vlan	VLAN 编号
Configuration	开关状态（打开/关闭）

【提示信息】

-

【平台说明】

-

15.4 show ip arp inspection interface

查看端口是否配置成功信任状态。

show ip arp inspection interface

【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的端口是否配置成 DAI 信任口。

【配置举例】 1：查看所有端口的 DAI 信任状态：

```
Ruijie#show ip arp inspection interface
Interface          Trust State
-----
GigabitEthernet 0/1    Untrusted
GigabitEthernet 0/2    Untrusted
GigabitEthernet 0/3    Untrusted
GigabitEthernet 0/4    Untrusted
Default              Untrusted
```

字段解释：

字段	说明
Interface	接口名称
Trust State	信任状态

【提示信息】 -

【平台说明】 -

16 IP Source Guard

命令	作用
ip source binding	在 IP 源地址绑定数据库中添加静态用户信息。
ip verify source	打开接口上的 IP Source Guard 功能。
ip verify source exclude-vlan	指定接口上 IP Source Guard 的例外 VLAN
show ip source binding	查看 IP 源地址绑定数据库的信息。
show ip verify source	查看 IP Source Guard 用户过滤表项。

16.1 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* | **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* | **ip-mac** | **ip-only** }

【参数说明】

参数	描述
<i>mac-address</i>	静态添加的用户的 MAC 地址。
<i>vlan-id</i>	静态添加的用户的 vlan id。
<i>ip-address</i>	静态添加的用户的 IP 地址。
<i>interface-id</i>	静态添加的用户所属的端口。
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 2 层交换口及 AP 口上使用该命令进行配置。其他类型的接口将配置失败。
- 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接口上通过 IP Source Guard 的检测。

 一条配置的绑定记录要么在接口上生效，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端口 1 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)# 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
```

【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 interface 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，若输入的接口不是二层交换口或者是 AP 口，则提示错误。

```
% Failed to execute command, because of "Interface name is not switch port".
```

【常见错误】 -

【平台说明】 -

16.2 ip verify source

打开接口上的 IP Source Guard 功能。

```
ip verify source [ port-security ]
```

关闭接口上的 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

【缺省级别】 14

【使用指导】 1：通过该命令打开接口的 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 2 层交换口及 AP 口上配置该命令。其他类型的接口上将配置失败。



目前锐捷设备 IP Source Guard 功能依赖的合法用户数量来源于 DHCP Snooping 与用户静态配置。若接口上仅仅开启了 IP Source Guard 功能，但是没有配置合法数据来源，会导致连接到该接口的用户无法正常使用网络。

【配置举例】 1：下面是配置接口 1 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
```

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
```

【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 Guard，而不配置合法用户记录的来源。

【平台说明】 -

16.3 Ip verify source exclude-vlan

接口上指定 IP Source Guard 的例外 VLAN 功能。

ip verify source exclude-vlan *vlan-id*

删除接口上 IP Source Guard 的例外 VLAN 功能。

no ip verify source exclude-vlan *vlan-id*

【参数说明】	<table><tr><th>参数</th><th>描述</th></tr><tr><td>vlan-id</td><td>不受接口上 IP Source Guard 控制的 vlan id</td></tr></table>	参数	描述	vlan-id	不受接口上 IP Source Guard 控制的 vlan id
参数	描述				
vlan-id	不受接口上 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				
【缺省级别】	14				
【使用指导】	1：启动 IP Source Guard 的接口上，通过该命令可以控制该接口的某些 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：接口上关闭 IP Source Guard 后，指定的例外 VLAN 也会被自动清除。  接口下必须先启动 IP Source Guard 才可以指定例外 VLAN。				
【配置举例】	1：下面是配置接口 1 上的 IP Source Guard 功能并指定例外 VLAN： <pre>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</pre>				
【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】	1：开启 IP Source Gourd，而不配置合法用户记录的来源。				
【平台说明】	-				

16.4 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*]

【参数说明】

参数	描述
<i>ip-address</i>	显示对应 ip 的用户绑定信息；
<i>mac-address</i>	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；
<i>vlan-id</i>	显示对应 vlan 的用户绑定信息；
<i>interface-id</i>	显示对应接口的用户绑定信息。

【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
```

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

Total number of bindings: 4

字段解释：

字段	说明
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	接口名称
Total number of bindings	当前 Binding 数据库中绑定的个数

【提示信息】 -

【平台说明】 -

16.5 show ip verify source

查看 IP Source Guard 用户过滤表项。

show ip verify source [**interface** *interface-id*]

【参数说明】

参数	描述
<i>interface-id</i>	显示对应接口的用户过滤表项

【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-system-error，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
```

NO.	INTERFACE	FILTERTYPE	FILTERSTATUS	IPADDRESS	MACADDRESS	
VLAN	TYPE					
1	Global	IP+MAC	Inactive-system-error	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		
Total number of bindings: 6						

字段解释：

字段	说明
----	----

NO.	记录序号
INTERFACE	用户连接端口
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

【提示信息】 -

【平台说明】 -

17 防网关 ARP 欺骗

命令	作用
anti-arp-spoofing ip	设置防网关 arp 欺骗
show anti-arp-spoofing	显示所有接口下的防网关 arp 欺骗信息

17.1 anti-arp-spoofing ip

设置防网关 arp 欺骗。

anti-arp-spoofing ip *ip-address*

删除防网关 arp 欺骗。

no anti-arp-spoofing ip *ip-address*

【参数说明】	参数	描述
	<i>ip-address</i>	网关 IP 地址

【缺省配置】 该功能缺省不生效

【命令模式】 接口配置模式

【缺省级别】 14

【使用指导】 1、 该命令为设置防网关 arp 欺骗，使用 show anti-arp-spoofing 命令查看设置。
2、 该命令仅支持二层口配置。

【配置举例】 1：设置防网关 arp 欺骗功能。

```
Ruijie(config)#interface fastEthernet 0/1
Ruijie(config-if)#anti-arp-spoofing ip 192.168.1.1
```

【检验方法】 **show run** 查看配置，存在所配置的命令。
show anti-arp-spoofing 显示接口下的防网关 arp 欺骗信息。

【提示信息】 -

【常见错误】 -

【平台说明】 -

17.2 show anti-arp-spoofing

显示所有接口下的防网关 arp 欺骗信息。

show anti-arp-spoofing

【参数说明】

参数	描述
-	-

【命令模式】

全局模式

【缺省级别】

14

【使用指导】

显示所有接口下的防网关 arp 欺骗信息

【配置举例】

1：显示所有接口下的防网关 arp 欺骗信息

```
Ruijie#show anti-arp-spoofing
```

NO	PORT	IP	STATUS
1	Gi0/1	192.168.1.1	active

字段解释：

字段	说明
NO	序号
PORT	端口信息
IP	网关 IP 地址
STATUS	表项生效状态

【提示信息】

-

【平台说明】

-

18 NFPP

命令	作用
<u>arp-guard attack-threshold</u>	配置 ARP 抗攻击全局攻击水线
<u>arp-guard enable</u>	配置 ARP 抗攻击全局打开抗攻击功能
<u>arp-guard isolate-period</u>	配置 ARP 抗攻击全局隔离时间
<u>arp-guard isolate-forwarding enable</u>	配置允许隔离转发功能
<u>arp-guard monitored-host-limit</u>	配置 ARP 抗攻击支持的最大受监控主机数
<u>arp-guard monitor-period</u>	配置 ARP 抗攻击监控时间
<u>arp-guard rate-limit</u>	配置 ARP 抗攻击全局抗攻击限速水线
<u>arp-guard ratelimit-forwarding enable</u>	配置 ARP 抗攻击基于端口的隔离转发限速功能
<u>arp-guard scan-threshold</u>	配置 ARP 抗攻击全局扫描水线
<u>clear nfpp arp-guard hosts</u>	清除 ARP 抗攻击受监控主机
<u>clear nfpp arp-guard scan</u>	清除 ARP 抗攻击扫描表。
<u>clear nfpp define name hosts</u>	清除自定义抗攻击受监控主机。
<u>clear nfpp dhcp-guard hosts</u>	清除 DHCP 抗攻击受监控主机
<u>clear nfpp dhcpv6-guard hosts</u>	清除 DHCPV6 抗攻击受监控主机
<u>clear nfpp icmp-guard hosts</u>	清除 ICMP 抗攻击受监控主机
<u>clear nfpp ip-guard hosts</u>	清除 IP 抗攻击受监控主机
<u>clear nfpp nd-guard hosts</u>	清除 ND 抗攻击受监控主机
<u>clear nfpp log</u>	清除 NFPP 日志缓冲区
<u>cpu-protect sub-interface {manage protocol route} percent</u>	配置每种类型报文占用队列的百分比
<u>cpu-protect sub-interface {manage protocol route} pps</u>	配置每种类型报文的流量带宽
<u>define</u>	配置创建自定义抗攻击类型
<u>define name enable</u>	配置自定义抗攻击全局打开抗攻击功能
<u>dhcp-guard attack-threshold</u>	配置 DHCP 抗攻击全局攻击水线
<u>dhcp-guard enable</u>	配置 DHCP 抗攻击全局打开抗攻击功能
<u>dhcp-guard isolate-period</u>	配置 DHCP 抗攻击全局隔离时间
<u>dhcp-guard monitored-host-limit</u>	配置 DHCP 抗攻击支持的最大受监控主机数
<u>dhcp-guard monitor-period</u>	配置 DHCP 抗攻击监控时间
<u>dhcp-guard rate-limit</u>	配置 DHCP 抗攻击全局限速水线
<u>dhcpv6-guard attack-threshold</u>	配置 DHCPV6 抗攻击全局攻击水线
<u>dhcpv6-guard enable</u>	配置 DHCPV6 抗攻击全打开抗攻击功能
<u>dhcpv6-guard monitored-host-limit</u>	配置 DHCPV6 抗攻击支持的最大受监控主机数
<u>dhcpv6-guard monitor-period</u>	配置 DHCPV6 抗攻击监控时间
<u>dhcpv6-guard rate-limit</u>	配置 DHCPV6 抗攻击全局限速水线
<u>global-policy</u>	配置自定义抗攻击全局基于主机或者端口限速水线和攻击水线
<u>icmp-guard attack-threshold</u>	配置 ICMP 抗攻击全局攻击水线

<u>icmp-guard enable</u>	配置 ICMP 抗攻击全局打开抗攻击功能
<u>icmp-guard isolate-period</u>	配置 ICMP 抗攻击全局隔离时间
<u>icmp-guard monitored-host-limit</u>	配置 ICMP 抗攻击支持的最大受监控主机数
<u>icmp-guard monitor-period</u>	配置 ICMP 抗攻击监控时间
<u>icmp-guard rate-limit</u>	配置 ICMP 抗攻击全局限速水线
<u>icmp-guard trusted-host</u>	配置 ICMP 抗攻击不监控的可信主机
<u>ip-guard attack-threshold</u>	配置 IP 抗攻击全局攻击水线
<u>ip-guard enable</u>	配置 IP 抗攻击全局打开 IP 防扫描功能
<u>ip-guard isolate-period</u>	配置 IP 抗攻击全局隔离时间
<u>ip-guard monitor-period</u>	配置 IP 抗攻击监控时间
<u>ip-guard monitored-host-limit</u>	配置 IP 抗攻击支持的最大受监控主机数
<u>ip-guard rate-limit</u>	配置 IP 抗攻击全局限速水线
<u>ip-guard scan-threshold</u>	配置 IP 抗攻击全局扫描水线
<u>ip-guard trusted-host</u>	配置 IP 抗攻击不监控的可信主机
<u>log-buffer enable</u>	配置日志打印到屏幕
<u>log-buffer entries</u>	配置 NFPP 日志缓冲区大小
<u>log-buffer logs</u>	配置 NFPP 从日志缓冲区取日志生成系统消息的速率
<u>logging</u>	配置 NFPP 记录哪些 VLAN 或端口的日志
<u>match</u>	配置自定义抗攻击匹配的报文类型
<u>monitored-host-limit</u>	配置自定义抗攻击支持的最大受监控主机数
<u>monitor-period</u>	配置自定义抗攻击监控时间
<u>nd-guard attack-threshold</u>	配置 ND 抗攻击全局攻击水线
<u>nd-guard enable</u>	配置 ND 抗攻击全局打开抗攻击功能
<u>nd-guard rate-limit</u>	配置 ND 抗攻击全局限速水线
<u>nd-guard ratelimit-forwarding enable</u>	配置 ND 抗攻击基于端口的隔离转发限速功能
<u>nfpp</u>	该命令用于进入 nfpp 配置模式。
<u>nfpp arp-guard enable</u>	配置 ARP 抗攻击在端口上打开 ARP 抗攻击功能
<u>nfpp arp-guard isolate-period</u>	配置 ARP 抗攻击在端口上配置局部隔离时间
<u>nfpp arp-guard policy</u>	配置 ARP 抗攻击在端口上配置局部的限速水线和攻击水线
<u>nfpp arp-guard scan-threshold</u>	配置 ARP 抗攻击在端口上配置局部扫描水线
<u>nfpp define name enable</u>	配置自定义抗攻击在端口上打开局部的攻击功能
<u>nfpp define name policy</u>	配置自定义抗攻击在端口上配置局部的限速水线和攻击水线
<u>nfpp dhcp-guard enable</u>	配置 DHCP 抗攻击在端口上打开局部的抗攻击功能
<u>nfpp dhcp-guard isolate-period</u>	配置 DHCP 抗攻击在端口上配置局部隔离时间
<u>nfpp dhcp-guard policy</u>	配置 DHCP 抗攻击在端口上配置局部的限速水线和攻击水线
<u>nfpp dhcpv6-guard enable</u>	配置 DHCPV6 抗攻击在端口上打开局部的抗攻击功能
<u>nfpp dhcpv6-guard policy</u>	配置 DHCPV6 抗攻击在端口上配置局部的限速水线和攻击水线
<u>nfpp icmp-guard enable</u>	配置 ICMP 抗攻击在端口上打开局部的抗攻击功能
<u>nfpp icmp-guard isolate-period</u>	配置 ICMP 抗攻击在端口上配置局部隔离时间
<u>nfpp icmp-guard policy</u>	配置 ICMP 抗攻击在端口上配置局部的限速水线和攻击水线

<u>nfpp ip-guard enable</u>	配置 IP 抗攻击在端口上打开局部的 IP 防扫描功能
<u>nfpp ip-guard isolate-period</u>	在配置 IP 抗攻击端口上配置局部隔离时间
<u>nfpp ip-guard policy</u>	配置 IP 抗攻击在端口上配置局部的限速水线和攻击水线
<u>nfpp ip-guard scan-threshold</u>	配置 IP 抗攻击在端口上配置局部扫描水线
<u>nfpp nd-guard enable</u>	配置 ND 抗攻击在端口上打开局部的抗攻击功能
<u>nfpp nd-guard policy</u>	配置 ND 抗攻击在端口上配置局部的限速水线和攻击水线
<u>show nfpp arp-guard hosts</u>	查看 ARP 抗攻击受监控主机
<u>show nfpp arp-guard scan</u>	查看 ARP 抗攻击扫描表
<u>show nfpp arp-guard summary</u>	查看 ARP 抗攻击配置信息
<u>show nfpp define hosts</u>	查看自定义抗攻击受监控主机
<u>show nfpp define summary</u>	查看自定义抗攻击配置信息
<u>show nfpp define trusted-host</u>	查看自定义抗攻击不监控的可信主机
<u>show nfpp dhcp-guard hosts</u>	查看 DHCP 抗攻击受监控主机
<u>show nfpp dhcp-guard summary</u>	查看 DHCP 抗攻击配置信息
<u>show nfpp dhcpv6-guard hosts</u>	查看 DHCPV6 抗攻击受监控主机
<u>show nfpp dhcpv6-guard summary</u>	查看 DHCPV6 抗攻击配置信息
<u>show nfpp icmp-guard hosts</u>	查看 ICMP 抗攻击受监控主机
<u>show nfpp icmp-guard summary</u>	查看 ICMP 抗攻击配置信息
<u>show nfpp icmp-guard trusted-host</u>	查看 ICMP 抗攻击不监控的可信主机
<u>show nfpp ip-guard hosts</u>	查看 IP 抗攻击受监控主机
<u>show nfpp ip-guard summary</u>	查看 IP 抗攻击配置信息
<u>show nfpp ip-guard trusted-host</u>	查看 IP 抗攻击不监控的可信主机
<u>show nfpp log</u>	查看 NFPP 日志配置/日志缓冲区内容
<u>show nfpp nd-guard summary</u>	查看 ND 抗攻击配置信息
<u>show nfpp nd-guard hosts</u>	查看 ND 抗攻击受监控端口
<u>trusted-host</u>	配置自定义抗攻击不监控的可信主机

18.1 arp-guard attack-threshold

配置全局攻击水线，即当报文速度超过攻击水线的时候，认为存在攻击行为。

arp-guard attack-threshold {per-src-ip | per-src-mac | per-port} pps

删除攻击水线配置，恢复到缺省配置。

no arp-guard attack-threshold {per-src-ip | per-src-mac | per-port}

恢复缺省配置。

default arp-guard attack-threshold {per-src-ip | per-src-mac | per-port}

【参数说明】

参数	描述
per-src-ip	配置每个源 IP 地址的攻击水线。

per-src-mac	配置每个源 MAC 地址的攻击水线。
per-port	配置每个端口的攻击水线。
<i>pps</i>	攻击水线，单位是每秒报文数，取值范围是[1,19999]。

- 【缺省配置】 缺省配置与产品相关，具体参见《配置指南》中关于产品相关的章节描述。
- 【命令模式】 NFPP 配置模式
- 【缺省级别】 14
- 【使用指导】 攻击水线不能小于限速水线。
- 【配置举例】 1：配置 ARP 抗攻击全局攻击水线，基于源 IP 攻击水线 2pps，基于源 MAC 攻击水线 3pps,基于源端口攻击水线 50pps。

Ruijie(config)# nfpp
Ruijie(config-nfpp)# arp-guard attack-threshold per-src-ip 2
Ruijie(config-nfpp)# arp-guard attack-threshold per-src-mac 3
Ruijie(config-nfpp)# arp-guard attack-threshold per-port 50
- 【检验方法】 使用 **show nfpp arp-guard summary** 查看配置信息
- 【提示信息】 -
- 【常见错误】 -
- 【平台说明】 -

18.2 arp-guard enable

该命令用来全局打开 ARP 抗攻击功能。

arp-guard enable

关闭 ARP 抗攻击功能。

no arp-guard enable

恢复缺省配置。

default arp-guard enable

【参数说明】

参数	描述
-	-

【缺省配置】 默认 ARP 抗攻击功能打开。

【命令模式】 NFPP 配置模式

【缺省级别】 14

【使用指导】 -

【配置举例】 1：配置全局打开 ARP 抗攻击功能。

```
Ruijie(config)# nfpp
Ruijie(config-nfpp)# arp-guard enable
```

【检验方法】 使用 **show nfpp arp-guard summary** 查看配置信息。

【提示信息】 -

【常见错误】 -

【平台说明】 -

18.3 arp-guard isolate-period

该命令用来配置全局隔离时间。

arp-guard isolate-period {*seconds* | **permanent**}

删除隔离时间配置，恢复到缺省配置。

no arp-guard isolate-period

恢复缺省配置。

default arp-guard isolate-period

【参数说明】	参数	描述
	<i>seconds</i>	隔离时间，单位是秒，取值范围是 0 或者[30, 86400]。
	permanent	永久隔离。

【缺省配置】 全局隔离时间的缺省值是 0，即不隔离。

【命令模式】 NFPP 配置模式

【缺省级别】 14

【使用指导】 -

【配置举例】 1：配置 ARP 抗攻击全局隔离时间为 180 秒。

```
Ruijie(config)# nfpp
Ruijie(config-nfpp)# arp-guard isolate-period 180
```

【检验方法】 使用 **show nfpp arp-guard summary** 查看配置信息。

【提示信息】 -

【常见错误】 -

【平台说明】 -

18.4 arp-guard isolate-forwarding enable

该命令用来配置允许隔离转发功能，恢复到缺省配置。
arp-guard isolate-forwarding enable

关闭隔离转发功能。
no arp-guard isolate-forwarding enable

恢复缺省配置。
default arp-guard isolate-forwarding enable

【参数说明】	参数	描述
	-	-

【缺省配置】 默认允许隔离转发。

【命令模式】 NFPP 配置模式

【缺省级别】 14

【使用指导】 -

【配置举例】 1：配置允许隔离转发。

```
Ruijie(config)# nfpp
Ruijie(config-nfpp)# arp-guard isolate-forwarding enable
```

【检验方法】 -

【提示信息】 -

【常见错误】 -

【平台说明】 -

18.5 arp-guard monitored-host-limit

该命令用来配置支持的最大受监控主机数。

arp-guard monitored-host-limit *number*

删除最大受监控主机数配置，恢复到缺省配置。

no arp-guard monitored-host-limit

恢复缺省配置。

default arp-guard monitored-host-limit

【参数说明】

参数	描述
<i>number</i>	支持的最大受监控主机数，取值范围为 1 到 4294967295。

【缺省配置】 最大受监控主机数默认 20000 个。

【命令模式】 NFPP 配置模式

【缺省级别】 14

【使用指导】 如果受监控主机数已经达到默认的 20000 个，此时管理员把受监控主机的最大数目设置成小于 20000，不会删除已有的受监控主机，而是打印信息 “%ERROR: The value that you configured is smaller than current monitored hosts 20000（配置的受监控主机数），please clear a part of monitored hosts.” 来提醒管理员配置没有生效，需要删除部分已经被监控的主机。

当受监控主机表满时，打印日志 “% NFPP_ARP_GUARD-4-SESSION_LIMIT: Attempt to exceed limit of ARP 20000（配置的受监控主机数） monitored hosts.” 提醒管理员。

【配置举例】 1：配置 ARP 抗攻击最大受监控主机数为 200 个。

```
Ruijie(config)# nfpp
Ruijie(config-nfpp)# arp-guard monitored-host-limit 200
```

【检验方法】 使用 **show nfpp arp-guard summary** 查看配置信息。

【提示信息】 -

【常见错误】 -

【平台说明】 -

18.6 arp-guard monitor-period

该命令用来配置监控时间。

arp-guard monitor-period *seconds*

删除置监控时间配置，恢复到缺省配置。

no arp-guard monitor-period

恢复缺省配置。

default arp-guard monitor-period

【参数说明】

参数	描述
<i>seconds</i>	监控时间，单位是秒，取值范围是[180, 86400]。

【缺省配置】 监控时间的缺省值是 600 秒。

【命令模式】 NFPP 配置模式

【缺省级别】 14

【使用指导】 检测出攻击者的时候，如果隔离时间为 0，将对攻击者进行软件监控，超时为监控时间。在软件监控过程中，当隔离时间被配置为非零值时，将自动对软件监控的攻击者采取硬件隔离，并且把超时设置为隔离时间。监控时间在隔离时间为 0 的情况下才有意义。
如果把隔离时间从非零值改成零，将直接把相关端口的攻击者删除，而不是进行软件监控。

【配置举例】 1：配置 ARP 抗攻击监控时间 180 秒。

```
Ruijie(config)# nfpp
Ruijie(config-nfpp)# arp-guard monitor-period 180
```

【检验方法】 使用 **show nfpp arp-guard summary** 查看配置信息。

【提示信息】 -

【常见错误】 -

【平台说明】 -

18.7 arp-guard rate-limit

配置全局限速水线。

arp-guard rate-limit {per-src-ip | per-src-mac | per-port} pps

删除限速水线配置，恢复到缺省配置。

no arp-guard rate-limit {per-src-ip | per-src-mac | per-port}

恢复缺省配置。

default arp-guard rate-limit {per-src-ip | per-src-mac | per-port}

【参数说明】

参数	描述
per-src-ip	对每个源 IP 地址进行限速。
per-src-mac	对每个源 MAC 地址进行限速。
per-port	对每个端口进行限速。
<i>pps</i>	限速水线值，单位是每秒报文数，取值范围是[1,19999]。

【缺省配置】 缺省配置与产品相关，具体参见《配置指南》中关于产品相关的章节描述。。

【命令模式】 NFPP 配置模式

【缺省级别】 14

【使用指导】 -

【配置举例】 1：配置 ARP 抗攻击全局限速水线，基于源 IP 限速水线 2pps，基于源 MAC 限速水线 3pps,基于源端口限速水线 50pps。

```
Ruijie(config)# nfpp
Ruijie(config-nfpp)# arp-guard rate-limit per-src-ip 2
Ruijie(config-nfpp)# arp-guard rate-limit per-src-mac 3
Ruijie(config-nfpp)# arp-guard rate-limit per-port 50
```

【检验方法】 使用 **show nfpp arp-guard summary** 查看配置信息。

【提示信息】 -

【常见错误】 -

【平台说明】 -

18.8 arp-guard ratelimit-forwarding enable

配置 ARP 抗攻击基于端口的隔离转发限速功能，恢复到缺省配置。

arp-guard ratelimit-forwarding enable

关闭隔离转发限速功能。

no arp-guard ratelimit-forwarding enable

恢复缺省配置。

default arp-guard ratelimit-forwarding enable

【参数说明】	参数	描述
	-	-

【缺省配置】 缺省打开基于端口的隔离转发限速功能。

【命令模式】 NFPP 配置模式

【缺省级别】 14

【使用指导】 -

【配置举例】 1：配置使 ARP 抗攻击基于端口的隔离转发限速功能。

```
Ruijie(config)# nfpp
```

```
Ruijie(config-nfpp)# arp-guard ratelimit-forwarding enable
```

【检验方法】 -

【提示信息】 -

【常见错误】 -

【平台说明】 -

18.9 arp-guard scan-threshold

配置全局扫描水线。

arp-guard scan-threshold *pkt-cnt*

删除扫描水线配置，恢复到缺省配置。

no arp-guard scan-threshold

恢复缺省配置。

default arp-guard scan-threshold

【参数说明】	参数	描述
	<i>pkt-cnt</i>	扫描水线值，单位是每秒报文数，取值范围是[1,19999]。

【缺省配置】 缺省扫描水线与产品相关，具体参见产品差异信息文档。时间单位是 10 秒。

【命令模式】 NFPP 配置模式

【缺省级别】 14

【使用指导】 如果 10 秒钟收到对应配置扫描水线个以上 ARP 报文，链路层源 MAC 地址固定而源 IP 地址变化，或者链路层源 MAC 地址和源 IP 地址固定而目标 IP 地址不断变化，就认为有扫描嫌疑。

【配置举例】 1：配置 ARP 抗攻击全扫描水线为 20pps。

```
Ruijie(config)# nfpp
Ruijie(config-nfpp)# arp-guard scan-threshold 20
```

【检验方法】 使用 **show nfpp arp-guard summary** 查看配置信息。

【提示信息】 -

【常见错误】 -

【平台说明】 -

18.10 clear nfpp arp-guard hosts

清除受监控主机，如果主机被隔离，需要解除隔离。

clear nfpp arp-guard hosts [*vlan vid*] [*interface interface-id*] [*ip-address* | *mac-address*]

【参数说明】	参数	描述
	<i>vid</i>	虚拟局域网号。
	<i>interface-id</i>	端口名称。
	<i>ip-address</i>	IP 地址。
	<i>mac-address</i>	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：把 VLAN 1 端口 g 0/1 的 ARP 抗攻击主机解除隔离。

```
Ruijie# clear nfpp arp-guard hosts vlan 1 interface g0/1
```

【提示信息】 -

【平台说明】 -

18.11 clear nfpp arp-guard scan

清除 ARP 扫描表。

clear nfpp arp-guard scan

【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 ARP 抗攻击的扫描表。

```
Ruijie# clear nfpp arp-guard scan
```

【提示信息】 -

【平台说明】 -

18.12 clear nfpp define name hosts

清除受监控主机，如果主机被隔离，需要解除隔离。

clear nfpp define name hosts [vlan vid] [interface interface-id] [ip-address] [mac-address] [ipv6-address]

【参数说明】

参数	描述
----	----

<i>name</i>	自定义抗攻击类型名称。
<i>vid</i>	虚拟局域网号。
<i>interface-id</i>	端口名称。
<i>ip-address</i>	IP 地址。
<i>mac-address</i>	MAC 地址。
<i>ipv6-address</i>	IPv6 地址。

【命令模式】 特权模式

【缺省级别】 14

【使用指导】 如果不带参数，表示清除该自定义分类下所有被监控的主机。

【配置举例】 1：清除自定义类型 tcp 的 VLAN 1 端口 g 0/1 的受监控的主机。

```
Ruijie# clear nfpp define tcp hosts vlan 1 interface g 0/1
```

【提示信息】 -

【平台说明】 -

18.13 clear nfpp dhcp-guard hosts

清除用户，即把用户解除隔离。

clear nfpp dhcp-guard hosts [*vlan vid*] [**interface** *interface-id*] [*mac-address*]

【参数说明】	参数	描述
	<i>vid</i>	虚拟局域网号。
	<i>interface-id</i>	端口名称。
	<i>mac-address</i>	MAC 地址。

【命令模式】 特权模式

【缺省级别】 14

【使用指导】 如果不带参数，表示清除所有被隔离的用户。

【配置举例】 1：把 VLAN 1 端口 g 0/1 的 DHCP 抗攻击用户解除隔离。

```
Ruijie# clear nfpp dhcp-guard hosts vlan 1 interface g0/1
```

【提示信息】 -

【平台说明】 -

18.14 clear nfpp dhcp-guard hosts

清除用户，即把用户解除隔离。

clear nfpp dhcp-guard hosts [*vlan vid*] [**interface** *interface-id*] [*mac-address*]

【参数说明】

参数	描述
<i>vid</i>	虚拟局域网号。
<i>interface-id</i>	端口名称。
<i>mac-address</i>	MAC 地址。

【命令模式】 特权模式

【缺省级别】 14

【使用指导】 如果不带参数，表示清除所有被隔离的用户。

【配置举例】 1：把 VLAN 1 端口 g 0/1 的 DHCP 抗攻击用户解除隔离。

```
Ruijie# clear nfpp dhcp-guard hosts vlan 1 interface g0/1
```

【提示信息】 -

【平台说明】 -

18.15 clear nfpp dhcpv6-guard hosts

清除用户，即把用户解除隔离。

clear nfpp dhcpv6-guard hosts [*vlan vid*] [**interface** *interface-id*] [*mac-address*]

【参数说明】

参数	描述
<i>vid</i>	虚拟局域网号
<i>interface-id</i>	端口名称
<i>mac-address</i>	MAC 地址

【命令模式】 特权模式

【缺省级别】 14

【使用指导】 如果不带参数，表示清除所有被隔离的用户。

【配置举例】 1：把 VLAN 1 端口 g 0/1 的 DHCPv6 抗攻击用户解除隔离。

```
Ruijie# clear nfpp dhcpv6-guard hosts vlan 1 interface g0/1
```

【提示信息】 -

【平台说明】 -

18.16 clear nfpp icmp-guard hosts

清除受监控主机，如果主机被隔离，需要解除隔离。

clear nfpp icmp-guard hosts [*vlan vid*] [**interface** *interface-id*] [*ip-address*]

【参数说明】

参数	描述
<i>vid</i>	虚拟局域网号。
<i>interface-id</i>	端口名称。
<i>ip-address</i>	IP 地址。

【命令模式】 特权模式

【缺省级别】 14

【使用指导】 如果不带参数，表示清除所有被监控的主机。

【配置举例】 1：清除 VLAN 1 端口 g 0/1 的 ICMP 抗攻击受监控主机。

```
Ruijie# clear nfpp icmp-guard hosts vlan 1 interface g 0/1
```

【提示信息】 -

【平台说明】 -

18.17 clear nfpp ip-guard hosts

清除受监控主机，如果主机被隔离，需要解除隔离。

clear nfpp ip-guard hosts [*vlan vid*] [**interface** *interface-id*] [*ip-address*]

【参数说明】

参数	描述
<i>vid</i>	虚拟局域网号。
<i>interface-id</i>	端口名称。

<i>ip-address</i>	IP 地址。
-------------------	--------

【命令模式】 特权模式

【缺省级别】 14

【使用指导】 如果不带参数，表示清除所有被监控的主机。

【配置举例】 1：把 VLAN 1 端口 g 0/1 的 IP 抗攻击主机解除隔离。

```
Ruijie# clear nfpp ip-guard hosts vlan 1 interface g0/1
```

【提示信息】 -

【平台说明】 -

18.18 clear nfpp nd-guard hosts

清除受监控主机，如果主机已被硬件限速，需要解除限速。

clear nfpp nd-guard hosts [*vlan vid*] [*interface interface-id*]

【参数说明】	参数	描述
	<i>vid</i>	虚拟局域网号。
	<i>interface-id</i>	端口名称。

【命令模式】 特权模式

【缺省级别】 14

【使用指导】 如果不带参数，表示清除所有被监控的主机。

【配置举例】 1：把 VLAN 1 端口 g 0/1 的 IP 抗攻击主机解除隔离。

```
Ruijie# clear nfpp nd-guard hosts vlan 1 interface g0/1
```

【提示信息】 -

【平台说明】 -

18.19 clear nfpp log

清空 NFPP 日志缓冲区。

clear nfpp 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】

1：清空 NFPP 的日志缓冲区。

```
Ruijie# clear nfpp log
```

.

【提示信息】

-

【平台说明】

-

18.20 cpu-protect sub-interface {manage|protocol|route} percent

该命令用来配置每种类型报文占用队列的百分比。

cpu-protect sub-interface {*manage|protocol|route*} **percent** *percent_vaule*

删除每种类型报文占用队列的百分比配置，恢复到缺省配置

no cpu-protect sub-interface {*manage|protocol|route*} **percent**

恢复缺省配置

default cpu-protect sub-interface {*manage|protocol|route*} **percent**

【参数说明】

参数	描述
<i>percent_vaule</i>	百分比，取值范围是 1 到 30。

【缺省配置】

管理类(Manage)占用缓冲区百分比为 30。

转发类(Route)占用缓冲区百分比为 25。

协议类(Protocol)占用缓冲区百分比为 45。

【命令模式】

全局配置模式

【缺省级别】

14

【使用指导】 -

【配置举例】 1：配置管理类报文占用缓冲区百分比为 60。

```
Ruijie(config)# cpu-protect sub-interface manage percent 30
```

【检验方法】 -

【提示信息】 -

【常见错误】 -

【平台说明】 -

18.21 cpu-protect sub-interface {manage|protocol|route} pps

该命令用来配置每种类型报文的流量带宽。

cpu-protect sub-interface {manage|protocol|route} pps pps_vaule

删除每种类型报文的流量带宽配置，恢复到缺省配置。

no cpu-protect sub-interface {manage|protocol|route} pps

恢复缺省配置。

default cpu-protect sub-interface {manage|protocol|route} pps

【参数说明】	参数	描述
	pps_vaule	限速水线，单位是每秒报文数，取值范围是 1-100000。

【缺省配置】 缺省配置与产品相关，具体参见《配置指南》中关于产品相关的章节描述。

【命令模式】 全局配置模式

【缺省级别】 14

【使用指导】 -

【配置举例】 1：配置管理类报文流量带宽为 2000pps。

```
Ruijie(config)# cpu-protect sub-interface manage pps 2000
```

【检验方法】 -

【提示信息】 -

【常见错误】 -

【平台说明】 -

18.22 define

该命令用来创建自定义抗攻击类型。

define *name*

删除自定义抗攻击类型。

no define *name*

恢复缺省配置。

default define *name*

【参数说明】	参数	描述
	<i>name</i>	自定义的抗攻击类型名称。

【缺省配置】 -

【命令模式】 NFPP 配置模式

【缺省级别】 14

【使用指导】 创建新的自定义抗攻击类型。

【配置举例】 1:创建自定义抗攻击 tcp

```
Ruijie(config)# nfpp
Ruijie(config-nfpp)# define tcp
Ruijie(config-nfpp-define)#
```

【检验方法】 使用 **show nfpp define summary** *name* 查看配置信息。

【提示信息】 -

【常见错误】 -

【平台说明】 -

18.23 define name enable

该命令用来全局开启自定义类型抗攻击功能。

define name enable

关闭自定义类型抗攻击功能。

no define name enable

恢复缺省配置。

default define name enable

【参数说明】	参数	描述
	name	自定义的抗攻击类型名称。
【缺省配置】	关闭自定义类型抗攻击功能。	
【命令模式】	NFPP 配置模式	
【缺省级别】	14	
【使用指导】	必须配置了 match 、 rate-limit 和 attack-threshold 之后，配置才能生效，否则配置失败。	
【配置举例】	1：配置自定义抗攻击 tcp 全局开启抗攻击功能。	
	Ruijie(config)# nfpp Ruijie(config-nfpp)#define tcp enable	
【检验方法】	使用 show nfpp define summary 查看配置信息。	
【提示信息】	-	
【常见错误】	-	
【平台说明】	-	

18.24 dhcp-guard attack-threshold

配置全局攻击水线，即当报文速度超过攻击水线的时候，认为存在攻击行为。

dhcp-guard attack-threshold { per-src-mac | per-port} pps

删除攻击水线配置，恢复到缺省配置。

no dhcp-guard attack-threshold { per-src-mac | per-port}

恢复缺省配置。

default dhcp-guard attack-threshold { per-src-mac | per-port}

【参数说明】

参数	描述
per-src-mac	配置每个源 MAC 地址的攻击水线。
per-port	配置每个端口的攻击水线。
<i>pps</i>	攻击水线，单位是每秒报文数，取值范围是[1,19999]。

【缺省配置】 缺省配置与产品相关，具体参见《配置指南》中关于产品相关的章节描述。

【命令模式】 NFPP 配置模式

【缺省级别】 14

【使用指导】 -

【配置举例】 1：配置 DHCP 抗攻击全局攻击水线，基于源 MAC 攻击水线 15pps,基于源端口攻击水线 200pps。

```
Ruijie(config)# nfpp
Ruijie(config-nfpp)# dhcp-guard attack-threshold per-src-mac 15
Ruijie(config-nfpp)# dhcp-guard attack-threshold per-port 200
```

【检验方法】 使用 **show nfpp dhcp-guard summary** 查看配置信息

【提示信息】 -

【常见错误】 -

【平台说明】 -

18.25 dhcp-guard enable

该命令用来打开 DHCP 防攻击功能。

dhcp-guard enable

关闭 DHCP 抗攻击功能

no dhcp-guard enable

恢复缺省配置

default dhcp-guard enable

【参数说明】	参数	描述
	-	-
【缺省配置】	端口没有配置 DHCP 抗攻击开关，采用全局开关。	
【命令模式】	NFPP 配置模式	
【缺省级别】	14	
【使用指导】	-	
【配置举例】	1：配置全局打开 DHCP 抗攻击功能。	
	<pre>Ruijie(config)# nfpp Ruijie(config-nfpp)# dhcp-guard enable</pre>	
【检验方法】	使用 show nfpp dhcp-guard summary 查看配置信息	
【提示信息】	-	
【常见错误】	-	
【平台说明】	-	

18.26 dhcp-guard isolate-period

该命令用来配置全局隔离时间。

dhcp-guard isolate-period {seconds | permanent}

删除隔离时间配置，恢复到缺省配置。

no dhcp-guard isolate-period

恢复缺省配置。

default dhcp-guard isolate-period

【参数说明】	参数	描述
	seconds	隔离时间，单位是秒，取值范围是 0 或者[30, 86400]，0 表示不隔离。
	permanent	永久隔离。

【缺省配置】 全局隔离时间的缺省值是 0，即不隔离。

- 【命令模式】 NFPP 配置模式
- 【缺省级别】 14
- 【使用指导】 对攻击者的隔离时间分为全局隔离时间和基于端口的隔离时间（即局部隔离时间）。对于某个端口，如果没有配置基于端口的隔离时间，那么采用全局隔离时间；否则，采用基于端口的隔离时间。
- 【配置举例】 1：配置 DHCP 抗攻击全局隔离时间为 180 秒。
- ```
Ruijie(config)# nfpp
Ruijie(config-nfpp)# dhcp-guard isolate timeout 180
```
- 【检验方法】 使用 **show nfpp dhcp-guard summary** 查看配置信息。
- 【提示信息】 -
- 【常见错误】 -
- 【平台说明】 -

## 18.27 dhcp-guard monitored-host-limit

该命令用来配置支持的最大受监控主机数。

**dhcp-guard monitored-host-limit** *number*

删除最大受监控主机数配置，恢复到缺省配置。

**no dhcp-guard monitored-host-limit**

恢复缺省配置。

**default dhcp-guard monitored-host-limit**

| 【参数说明】 | 参数            | 描述                                  |
|--------|---------------|-------------------------------------|
|        | <i>number</i> | 支持的最大最大受监控主机数，取值范围为 1 到 4294967295。 |

- 【缺省配置】 最大受监控主机数默认 20000 个。
- 【命令模式】 NFPP 配置模式
- 【缺省级别】 14
- 【使用指导】 如果受监控主机数已经达到默认的 20000 个，此时管理员把受监控主机的最大数目设置成小于 20000，不会删

除已有的受监控主机，而是打印信息 “%ERROR : The value that you configured is smaller than current monitored hosts 20000（配置的受监控主机数），please clear a part of monitored hosts.” 来提醒管理员配置没有生效，需要删除部分已经被监控的主机。  
当受监控主机表满时，打印日志 “% NFPP\_DHCP\_GUARD-4-SESSION\_LIMIT: Attempt to exceed limit of DHCP 20000（配置受监控主机数） monitored hosts.” 提醒管理员。

- 【配置举例】1：配置 DHCP 抗攻击最大受监控主机数为 200 个。

Ruijie(config)# nfpp  
Ruijie(config-nfpp)# dhcp-guard monitored-host-limit 200
- 【检验方法】使用 show nfpp dhcp-guard summary 查看配置信息。
- 【提示信息】-
- 【常见错误】-
- 【平台说明】-

18.28 dhcp-guard monitor-period

该命令用来配置监控时间。  
**dhcp-guard monitor-period seconds**  
  
删除置监控时间配置，恢复到缺省配置。  
**no dhcp-guard monitor-period**  
  
恢复缺省配置。  
**default dhcp-guard monitor-period**

- 【参数说明】

| 参数      | 描述                           |
|---------|------------------------------|
| seconds | 监控时间，单位是秒，取值范围是[180, 86400]。 |
- 【缺省配置】全局监控时间的缺省值是 600 秒。
- 【命令模式】NFPP 配置模式
- 【缺省级别】14
- 【使用指导】检测出攻击者的时候，如果隔离时间为 0，将对攻击者进行软件监控，超时为监控时间。在软件监控过程中，当隔离时间被配置为非零值时，将自动对软件监控的攻击者采取硬件隔离，并且把超时设置为隔离时间。监控时间在隔离时间为 0 的情况下才有意义。

如果把隔离时间从非零值改成零，将直接把相关端口的攻击者删除，而不是进行软件监控。

【配置举例】 1：配置 DHCP 抗攻击监控时间 180 秒。

```
Ruijie(config)# nfpp
Ruijie(config-nfpp)# dhcp-guard monitor-period 180
```

【检验方法】 使用 **show nfpp dhcp-guard summary** 查看配置信息。

【提示信息】 -

【常见错误】 -

【平台说明】 -

## 18.29 dhcp-guard rate-limit

配置全局限速水线。

**dhcp-guard rate-limit { per-src-mac | per-port} pps**

删除限速水线配置，恢复到缺省配置。

**no dhcp-guard rate-limit {per-src-mac | per-port}**

恢复缺省配置。

**default dhcp-guard rate-limit { per-src-mac | per-port}**

【参数说明】

| 参数                 | 描述                             |
|--------------------|--------------------------------|
| <b>per-src-mac</b> | 对每个源 MAC 地址进行限速。               |
| <b>per-port</b>    | 对每个端口进行限速。                     |
| <i>pps</i>         | 限速水线值，单位是每秒报文数，取值范围是[1,19999]。 |

【缺省配置】 缺省配置与产品相关，具体参见《配置指南》中关于产品相关的章节描述。

【命令模式】 NFPP 配置模式

【缺省级别】 14

【使用指导】 -

【配置举例】 1：配置 DHCP 抗攻击全局限速水线，基于源 MAC 限速水线 8pps,基于源端口限速水线 100pps。

```
Ruijie(config)# nfpp
Ruijie(config-nfpp)# dhcp-guard rate-limit per-src-mac 8
```



```
Ruijie(config-nfpp)# dhcp-guard rate-limit per-port 100
```

【检验方法】 使用 **show nfpp dhcp-guard summary** 查看配置信息。

【提示信息】 -

【常见错误】 -

【平台说明】 -

## 18.30 dhcpv6-guard attack-threshold

配置全局攻击水线，即当报文速度超过攻击水线的时候，认为存在攻击行为。

**dhcpv6-guard attack-threshold { per-src-mac | per-port} pps**

删除攻击水线配置，恢复到缺省配置。

**no dhcpv6-guard attack-threshold {per-src-mac | per-port}**

恢复缺省配置。

**default dhcpv6-guard attack-threshold { per-src-mac | per-port}**

| 参数                 | 描述                            |
|--------------------|-------------------------------|
| <b>per-src-mac</b> | 配置每个源 MAC 地址的攻击水线。            |
| <b>per-port</b>    | 配置每个端口的攻击水线。                  |
| <i>pps</i>         | 攻击水线，单位是每秒报文数，取值范围是[1,19999]。 |

【缺省配置】 缺省配置与产品相关，具体参见《配置指南》中关于产品相关的章节描述。

【命令模式】 NFPP 配置模式

【缺省级别】 14

【使用指导】 -

【配置举例】 1：配置 DHCPv6 抗攻击全局攻击水线，基于源 MAC 攻击水线 15pps,基于源端口攻击水线 200pps。

```
Ruijie(config)# nfpp
```

```
Ruijie(config-nfpp)# dhcpv6-guard attack-threshold per-src-mac 15
```

```
Ruijie(config-nfpp)# dhcpv6-guard attack-threshold per-port 200
```

【检验方法】 使用 **show nfpp dhcpv6-guard summary** 查看配置信息。

【提示信息】 -

【常见错误】 -

【平台说明】 -

## 18.31 dhcpv6-guard enable

该命令用来打开 DHCPv6 防攻击功能。

**dhcpv6-guard enable**

关闭 DHCPv6 抗攻击功能。

**no dhcpv6-guard enable**

恢复缺省配置。

**default dhcpv6-guard enable**

【参数说明】

| 参数 | 描述 |
|----|----|
| -  | -  |

【缺省配置】 端口没有配置 DHCPv6 抗攻击开关，采用全局开关。

【命令模式】 NFPP 配置模式

【缺省级别】 14

【使用指导】 -

【配置举例】 1：配置全局打开 DHCPv6 抗攻击功能。

```
Ruijie(config)# nfpp
Ruijie(config-nfpp)# dhcpv6-guard enable
```

【检验方法】 使用 **show nfpp dhcpv6-guard summary** 查看配置信息。

【提示信息】 -

【常见错误】 -

【平台说明】 -

## 18.32 dhcpv6-guard monitored-host-limit

该命令用来配置支持的最大受监控主机数。

**dhcpv6-guard monitored-host-limit** *number*

删除最大受监控主机数配置，恢复到缺省配置。

**no dhcpv6-guard monitored-host-limit**

恢复缺省配置。

**default dhcpv6-guard monitored-host-limit**

| 【参数说明】 | 参数            | 描述                                  |
|--------|---------------|-------------------------------------|
|        | <i>number</i> | 支持的最大最大受监控主机数，取值范围为 1 到 4294967295。 |

【缺省配置】 最大受监控主机数默认 20000 个。

【命令模式】 NFPP 配置模式

【缺省级别】 14

【使用指导】 如果受监控主机数已经达到默认的 20000 个，此时管理员把受监控主机的最大数目设置成小于 20000，不会删除已有的受监控主机，而是打印信息 “%ERROR : The value that you configured is smaller than current monitored hosts 20000（配置的受监控主机数），please clear a part of monitored hosts.” 来提醒管理员配置没有生效，需要删除部分已经被监控的主机。

当受监控主机表满时，打印日志 “% NFPP\_DHCPV6\_GUARD -4-SESSION\_LIMIT: Attempt to exceed limit of DHCPv6 20000（配置受监控主机数） monitored hosts.” 提醒管理员。

【配置举例】 1：配置 DHCPv6 抗攻击最大受监控主机数为 200 个。

```
Ruijie(config)# nfpp
Ruijie(config-nfpp)# dhcp-guard monitored-host-limit 200
```

【检验方法】 使用 **show nfpp dhcpv6-guard summary** 查看配置信息

【提示信息】 -

【常见错误】 -

【平台说明】 -

## 18.33 dhcpv6-guard monitor-period

该命令用来配置监控时间。

**dhcpv6-guard monitor-period** *seconds*

删除置监控时间配置，恢复到缺省配置。

**no dhcpv6-guard monitor-period**

恢复缺省配置。

**default dhcpv6-guard monitor-period**

【参数说明】

| 参数             | 描述                           |
|----------------|------------------------------|
| <i>seconds</i> | 监控时间，单位是秒，取值范围是[180, 86400]。 |

【缺省配置】 全局监控时间的缺省值是 600 秒。

【命令模式】 NFPP 配置模式

【缺省级别】 14

【使用指导】 检测出攻击者的时候，如果隔离时间为 0，将对攻击者进行软件监控，超时为监控时间。在软件监控过程中，当隔离时间被配置为非零值时，将自动对软件监控的攻击者采取硬件隔离，并且把超时设置为隔离时间。监控时间在隔离时间为 0 的情况下才有意义。

如果把隔离时间从非零值改成零，将直接把相关端口的攻击者删除，而不是进行软件监控。

【配置举例】 1：配置 DHCPv6 抗攻击监控时间 180 秒。

```
Ruijie(config)# nfpp
Ruijie(config-nfpp)# dhcpv6-guard monitor-period 180
```

【检验方法】 使用 **show nfpp dhcpv6-guard summary** 查看配置信息。

【提示信息】 -

【常见错误】 -

【平台说明】 -

## 18.34 dhcpv6-guard rate-limit

配置全局限速水线。

**dhcpv6-guard rate-limit { per-src-mac | per-port} pps**

删除限速水线配置，恢复到缺省配置。

**no dhcpv6-guard rate-limit {per-src-mac | per-port}**

恢复缺省配置。

**default dhcpv6-guard rate-limit { per-src-mac | per-port}**

【参数说明】

| 参数                 | 描述                             |
|--------------------|--------------------------------|
| <b>per-src-mac</b> | 对每个源 MAC 地址进行限速。               |
| <b>per-port</b>    | 对每个端口进行限速。                     |
| <i>pps</i>         | 限速水线值，单位是每秒报文数，取值范围是[1,19999]。 |

【缺省配置】 缺省配置与产品相关，具体参见《配置指南》中关于产品相关的章节描述。

【命令模式】 NFPP 配置模式

【缺省级别】 14

【使用指导】 -

【配置举例】 1：配置 DHCPv6 抗攻击全局限速水线，基于源 MAC 限速水线 8pps,基于源端口限速水线 100pps。

```
Ruijie(config)# nfpp
Ruijie(config-nfpp)# dhcpv6-guard rate-limit per-src-mac 8
Ruijie(config-nfpp)# dhcpv6-guard rate-limit per-port 100
```

【检验方法】 使用 **show nfpp dhcpv6-guard summary** 查看配置信息。

【提示信息】 -

【常见错误】 -

【平台说明】 -

## 18.35 global-policy

该命令用来配置自定义抗攻击类型的基于主机或者端口限速水线和攻击水线。

**global-policy {per-src-mac | per-src-ip | per-port} rate-limit-pps attack-threshold-pps**

删除限速水线和攻击水线配置，恢复到缺省配置。

**no global-policy {per-src-mac | per-src-ip | per-port}**

恢复缺省配置。

**default global-policy {per-src-mac | per-src-ip | per-port}**

【参数说明】

| 参数                          | 描述                            |
|-----------------------------|-------------------------------|
| <b>per-src-ip</b>           | 基于源 IP/VID/端口识别主机进行速率统计。      |
| <b>per-src-mac</b>          | 基于源 MAC/VID/端口识别主机进行速率统计。     |
| <b>per-port</b>             | 基于每个报文接收的物理端口进行速率统计。          |
| <i>rate-limit-pps</i>       | 限速水线，单位是每秒报文数，取值范围是[1,19999]。 |
| <i>attack-threshold-pps</i> | 攻击水线，单位是每秒报文数，取值范围是[1,19999]。 |

【缺省配置】 缺省没有限速水线和攻击水线配置，所以自定义抗攻击要生效，必须明确进行限速水线和攻击水线的配置。

【命令模式】 NFPP 自定义类型配置模式

【缺省级别】 14

【使用指导】 创建一个自定义抗攻击类型，必须为该类型指定速率统计的分类原则，即基于源 IP 识别用户、基于源 MAC 识别用户，进行基于用户的自定义报文速率统计，或者基于端口的速率统计，并且指定各分类的限速水线及攻击水线。限速水线不能高于攻击水线。当速率超过限速水线时，满足该分类的自定义类型报文将被丢弃。当速率超过攻击水线时，将被视为攻击，打印 log，并且发送 trap。

【配置举例】 1：创建自定义抗攻击 tcp，配置基于源 IP 的全局限速和攻击水线，限速水线 10pps，攻击水线 20pps；配置基于源端口的全局限速和攻击水线，限速水线 100pps，攻击水线 200pps。

```
Ruijie(config)# nfpp
Ruijie(config-nfpp)# nfpp define tcp
Ruijie(config-nfpp-define)# global-policy per-src-ip 10 20
Ruijie(config-nfpp-define)# global-policy per-port 100 200
```

【检验方法】 使用 **show nfpp define summary name** 查看配置信息。

【提示信息】 -

【常见错误】 -

【平台说明】 -

## 18.36 icmp-guard attack-threshold

配置全局攻击水线，即当报文速度超过攻击水线的时候，认为存在攻击行为。

**icmp-guard attack-threshold { per-src-ip | per-port } pps**

删除攻击水线配置，恢复到缺省配置。

**no icmp-guard attack-threshold { per-src-ip | per-port }**

恢复缺省配置。

**default icmp-guard attack-threshold { per-src-ip | per-port }**

### 【参数说明】

| 参数                | 描述                            |
|-------------------|-------------------------------|
| <b>per-src-ip</b> | 配置每个源 IP 地址的攻击水线。             |
| <b>per-port</b>   | 配置每个端口的攻击水线。                  |
| <i>pps</i>        | 攻击水线，单位是每秒报文数，取值范围是[1,19999]。 |

【缺省配置】 缺省配置与产品相关，具体参见《配置指南》中关于产品相关的章节描述。

【命令模式】 NFPP 配置模式

【缺省级别】 14

【使用指导】 -

【配置举例】 1：配置 ICMP 抗攻击全局攻击水线，基于源 IP 攻击水线 600pps,基于源端口攻击水线 1200pps。

```
Ruijie(config)# nfpp
Ruijie(config-nfpp)# icmp-guard attack-threshold per-src-ip 600
Ruijie(config-nfpp)# icmp-guard attack-threshold per-port 1200
```

【检验方法】 使用 **show nfpp icmp-guard summary** 查看配置信息。

【提示信息】 -

【常见错误】 -

【平台说明】 -

## 18.37 icmp-guard enable

该命令用来打开 ICMP 防攻击功能。

**icmp-guard enable**

关闭 ICMP 抗攻击功能。

**no icmp-guard enable**

恢复缺省配置。

**default icmp-guard enable****【参数说明】**

| 参数 | 描述 |
|----|----|
| -  | -  |

**【缺省配置】** 默认 ICMP 防攻击功能打开。

**【命令模式】** NFPP 配置模式

**【缺省级别】** 14

**【使用指导】** -

**【配置举例】** 1：配置全局打开 ICMP 抗攻击功能。

```
Ruijie(config)# nfpp
Ruijie(config-nfpp)# icmp-guard enable
```

**【检验方法】** 使用 **show nfpp icmp-guard summary** 查看配置信息。

**【提示信息】** -

**【常见错误】** -

**【平台说明】** -

## 18.38 icmp-guard isolate-period

该命令用来配置全局隔离时间。

**icmp-guard isolate-period {seconds | permanent}**

删除隔离时间配置，恢复到缺省配置。

**no icmp-guard isolate-period**

恢复缺省配置。

**default icmp-guard isolate-period**



|        |                                                                                                                   |                                          |
|--------|-------------------------------------------------------------------------------------------------------------------|------------------------------------------|
| 【参数说明】 | 参数                                                                                                                | 描述                                       |
|        | <i>seconds</i>                                                                                                    | 隔离时间，单位是秒，取值范围是 0 或者[30, 86400]，0 表示不隔离。 |
|        | <b>permanent</b>                                                                                                  | 永久隔离。                                    |
| 【缺省配置】 | 全局隔离时间的缺省值是 0，即不隔离。                                                                                               |                                          |
| 【命令模式】 | NFPP 配置模式                                                                                                         |                                          |
| 【缺省级别】 | 14                                                                                                                |                                          |
| 【使用指导】 | 对攻击者的隔离时间分为全局隔离时间和基于端口的隔离时间（即局部隔离时间）。对于某个端口，如果没有配置基于端口的隔离时间，那么采用全局隔离时间；否则，采用基于端口的隔离时间。                            |                                          |
| 【配置举例】 | 1：配置 ICMP 抗攻击全局隔离时间为 180 秒。<br><pre>Ruijie(config)# nfpp Ruijie(config-nfpp)# icmp-guard isolate-period 180</pre> |                                          |
| 【检验方法】 | 使用 <b>show nfpp icmp-guard summary</b> 查看配置信息。                                                                    |                                          |
| 【提示信息】 | -                                                                                                                 |                                          |
| 【常见错误】 | -                                                                                                                 |                                          |
| 【平台说明】 | -                                                                                                                 |                                          |

## 18.39 icmp-guard monitored-host-limit

该命令用来配置支持的最大受监控主机数。

**icmp-guard monitored-host-limit** *number*

删除最大受监控主机数配置，恢复到缺省配置。

**no icmp-guard monitored-host-limit**

恢复缺省配置。

**default icmp-guard monitored-host-limit**

|        |               |                                   |
|--------|---------------|-----------------------------------|
| 【参数说明】 | 参数            | 描述                                |
|        | <i>number</i> | 支持的最大受监控主机数，取值范围为 1 到 4294967295。 |

- 【缺省配置】 最大受监控主机数默认 20000 个。
- 【命令模式】 NFPP 配置模式
- 【缺省级别】 14
- 【使用指导】 如果受监控主机数已经达到默认的 20000 个，此时管理员把受监控主机的最大数目设置成小于 20000，不会删除已有的受监控主机，而是打印信息 “%ERROR : The value that you configured is smaller than current monitored hosts 20000（配置的受监控主机数），please clear a part of monitored hosts.” 来提醒管理员配置没有生效，需要删除部分已经被监控的主机。  
当受监控主机满时，打印日志 “% NFPP\_ICMP\_GUARD-4-SESSION\_LIMIT: Attempt to exceed limit of ICMP 20000（配置的受监控主机数） monitored hosts.” 提醒管理员。
- 【配置举例】 1：配置 ICMP 抗攻击最大受监控主机数为 200 个。
- ```
Ruijie(config)# nfpp
Ruijie(config-nfpp)# icmp-guard monitored-host-limit 200
```
- 【检验方法】 使用 **show nfpp icmp-guard summary** 查看配置信息。
- 【提示信息】 -
- 【常见错误】 -
- 【平台说明】 -

18.40 icmp-guard monitor-period

该命令用来配置监控时间。

icmp-guard monitor-period *seconds*

删除置监控时间配置，恢复到缺省配置。

no icmp-guard monitor-period

恢复缺省配置。

default icmp-guard monitor-period

【参数说明】	参数	描述
	<i>seconds</i>	监控时间，单位是秒，取值范围是[180, 86400]。

【缺省配置】 全局监控时间的缺省值是 600 秒。

- 【命令模式】 NFPP 配置模式
- 【缺省级别】 14
- 【使用指导】 检测出攻击者的时候，如果隔离时间为 0，将对攻击者进行软件监控，超时为监控时间。在软件监控过程中，当隔离时间被配置为非零值时，将自动对软件监控的攻击者采取硬件隔离，并且把超时设置为隔离时间。监控时间在隔离时间为 0 的情况下才有意义。
如果把隔离时间从非零值改成零，将直接把相关端口的攻击者删除，而不是进行软件监控。
- 【配置举例】 1：配置 ICMP 抗攻击监控时间 180 秒。
- ```
Ruijie(config)# nfpp
Ruijie(config-nfpp)# icmp-guard monitor-period 180
```
- 【检验方法】 使用 **show nfpp icmp-guard summary** 查看配置信息。
- 【提示信息】 -
- 【常见错误】 -
- 【平台说明】 -

## 18.41 icmp-guard rate-limit

配置全局限速水线。

**icmp-guard rate-limit { per-src-ip | per-port} pps**

删除限速水线配置，恢复到缺省配置。

**no icmp-guard rate-limit {per-src-ip | per-port}**

恢复缺省配置。

**default icmp-guard rate-limit { per-src-ip | per-port}**

| 参数                | 描述                             |
|-------------------|--------------------------------|
| <b>per-src-ip</b> | 对每个源 IP 地址进行限速。                |
| <b>per-port</b>   | 对每个端口进行限速。                     |
| <i>pps</i>        | 限速水线值，单位是每秒报文数，取值范围是[1,19999]。 |

- 【缺省配置】 缺省配置与产品相关，具体参见《配置指南》中关于产品相关的章节描述。
- 【命令模式】 NFPP 配置模式

【缺省级别】 14

【使用指导】 -

【配置举例】 1：配置 ICMP 抗攻击全局限速水线，基于源 IP 限速水线 500pps，基于源端口限速水线 800pps。

```
Ruijie(config)# nfpp
Ruijie(config-nfpp)# icmp-guard rate-limit per-src-ip 500
Ruijie(config-nfpp)# icmp-guard rate-limit per-port 800
```

【检验方法】 使用 **show nfpp icmp-guard summary** 查看配置信息。

【提示信息】 -

【常见错误】 -

【平台说明】 -

## 18.42 icmp-guard trusted-host

配置不监控的可信主机。

**icmp-guard trusted-host** *ip mask*

删除不监控可信主机。

**no icmp-guard trusted-host** {all | *ip mask*}

清除不监控可信主机。

**default icmp-guard trusted-host**

【参数说明】

| 参数          | 描述                           |
|-------------|------------------------------|
| <i>ip</i>   | IP 地址。                       |
| <i>mask</i> | IP 地址的掩码。                    |
| <b>all</b>  | 和 <b>no</b> 一起使用，删除所有可信主机配置。 |

【缺省配置】 缺省没有设置任何可信主机。

【命令模式】 NFPP 配置模式

【缺省级别】 14

【使用指导】 如果管理员希望对某台主机不进行监控，即对该主机表示信任，则可以通过该命令配置。该可信主机发往 CPU 的 ICMP 报文将被允许发往 CPU，不做任何的限速和告警处理。通过配置掩码可以达到对某一个网段的所有主

机都不进行监控。

最多支持设置 500 条可信主机。

【配置举例】 1：把 1.1.1.0/24 网段的所有主机配置为 ICMP 抗攻击的可信主机。

```
Ruijie(config)# nfpp
Ruijie(config-nfpp)# icmp-guard trusted-host 1.1.1.0 255.255.255.0
```

【检验方法】 使用 **show nfpp icmp-guard summary** 查看配置信息。

【提示信息】 -

【常见错误】 -

【平台说明】 -

## 18.43 ip-guard attack-threshold

配置全局攻击水线，即当报文速度超过攻击水线的时候，认为存在攻击行为。

**ip-guard attack-threshold {per-src-ip | per-port} pps**

删除攻击水线配置，恢复到缺省配置。

**no ip-guard attack-threshold { per-src-ip | per-port }**

恢复缺省配置。

**default ip-guard attack-threshold { per-src-ip | per-port }**

|        |                   |                               |
|--------|-------------------|-------------------------------|
| 【参数说明】 | 参数                | 描述                            |
|        | <b>per-src-ip</b> | 配置每个源 IP 地址的攻击水线。             |
|        | <b>per-port</b>   | 配置每个端口的攻击水线。                  |
|        | <i>pps</i>        | 攻击水线，单位是每秒报文数，取值范围是[1,19999]。 |

【缺省配置】 缺省配置与产品相关，具体参见《配置指南》中关于产品相关的章节描述。

【命令模式】 NFPP 配置模式

【缺省级别】 14

【使用指导】 攻击水线不能小于限速水线。  
IP 防扫描针对的是目的 IP 地址不是本机 IP 地址的 IP 报文攻击。对于目的 IP 地址是本机 IP 地址的 IP 报文，则由 CPP（CPU Protect Policy）限速。

【配置举例】 1：配置 IP 抗攻击全局攻击水线，基于源 IP 攻击水线 2pps,基于源端口攻击水线 50pps。

```
Ruijie(config)# nfpp
Ruijie(config-nfpp)# ip-guard attack-threshold per-src-ip 2
Ruijie(config-nfpp)# ip-guard attack-threshold per-port 50
```

【检验方法】 使用 **show nfpp ip-guard summary** 查看配置信息。

【提示信息】 -

【常见错误】 -

【平台说明】 -

18.44 ip-guard enable

该命令用来全局打开 IP 防扫描功能。

**ip-guard enable**

关闭 IP 防扫描功能。

**no ip-guard enable**

恢复缺省配置。

**default ip-guard enable**

| 【参数说明】 | 参数 | 描述 |
|--------|----|----|
|        | -  | -  |

【缺省配置】 默认 IP 防扫描功能打开。

【命令模式】 NFPP 配置模式

【缺省级别】 14

【使用指导】 -

【配置举例】 1：配置全局打开 IP 防扫描功能

```
Ruijie(config)# nfpp
Ruijie(config-nfpp)# ip-guard enable
```

【检验方法】 使用 **show nfpp ip-guard summary** 查看配置信息。

【提示信息】 -

【常见错误】 -

【平台说明】 -

## 18.45 ip-guard isolate-period

该命令用来配置全局隔离时间。

**ip-guard isolate-period** {seconds | permanent}

删除隔离时间配置，恢复到缺省配置。

**no ip-guard isolate-period**

恢复缺省配置。

**default ip-guard isolate-period**

【参数说明】

| 参数        | 描述                               |
|-----------|----------------------------------|
| seconds   | 隔离时间，单位是秒，取值范围是 0 或者[30, 86400]。 |
| permanent | 永久隔离。                            |

【缺省配置】 全局隔离时间的缺省值是 0，即不隔离。

【命令模式】 NFPP 配置模式

【缺省级别】 14

【使用指导】 -

【配置举例】 1：配置 IP 抗攻击全局隔离时间为 180 秒。

```
Ruijie(config)# nfpp
Ruijie(config-nfpp)# ip-guard isolate-period 180
```

【检验方法】 使用 **show nfpp ip-guard summary** 查看配置信息。

【提示信息】 -

【常见错误】 -

【平台说明】 -

## 18.46 ip-guard monitor-period

该命令用来配置监控时间。

**ip-guard monitor-period** *seconds*

删除置监控时间配置，恢复到缺省配置。

**no ip-guard monitor-period**

恢复缺省配置。

**default ip-guard monitor-period**

|        |                |                              |
|--------|----------------|------------------------------|
| 【参数说明】 | 参数             | 描述                           |
|        | <i>seconds</i> | 监控时间，单位是秒，取值范围是[180, 86400]。 |

【缺省配置】 监控时间的缺省值是 600 秒。

【命令模式】 NFPP 配置模式

【缺省级别】 14

【使用指导】 检测出攻击者的时候，如果隔离时间为 0，将对攻击者进行软件监控，超时为监控时间。在软件监控过程中，当隔离时间被配置为非零值时，将自动对软件监控的攻击者采取硬件隔离，并且把超时设置为隔离时间。监控时间在隔离时间为 0 的情况下才有意义。  
如果把隔离时间从非零值改成零，将直接把相关端口的攻击者删除，而不是进行软件监控。

【配置举例】 1：配置 IP 抗攻击监控时间 180 秒。

```
Ruijie(config)# nfpp
Ruijie(config-nfpp)# ip-guard monitor-period 180
```

【检验方法】 使用 **show nfpp ip-guard summary** 查看配置信息。

【提示信息】 -

【常见错误】 -

【平台说明】 -

## 18.47 ip-guard monitored-host-limit

该命令用来配置支持的最大受监控主机数。



**ip-guard monitored-host-limit** *number*

删除最大受监控主机数配置，恢复到缺省配置。

**no ip-guard monitored-host-limit**

恢复缺省配置。

**default ip-guard monitored-host-limit**

【参数说明】

| 参数            | 描述                                |
|---------------|-----------------------------------|
| <i>number</i> | 支持的最大受监控主机数，取值范围为 1 到 4294967295。 |

【缺省配置】

最大受监控主机数默认 20000 个。

【命令模式】

NFPP 配置模式

【缺省级别】

14

【使用指导】

如果受监控主机数已经达到默认的 20000 个，此时管理员把受监控主机的最大数目设置成小于 20000，不会删除已有的受监控主机，而是打印信息“%ERROR: The value that you configured is smaller than current monitored hosts 20000 (配置的受监控主机数)，please clear a part of monitored hosts.”来提醒管理员配置没有生效，需要删除部分已经被监控的主机。

当受监控主机表满时，打印日志 “% NFPP\_IP\_GUARD-4-SESSION\_LIMIT: Attempt to exceed limit of IP 20000 (配置的受监控主机数) monitored hosts.” 提醒管理员。

【配置举例】

1：配置 IP 抗攻击最大受监控主机数为 200 个。

```
Ruijie(config)# nfpp
```

```
Ruijie(config-nfpp)# ip-guard monitored-host-limit 200
```

【检验方法】

使用 **show nfpp ip-guard summary** 查看配置信息。

【提示信息】

-

【常见错误】

-

【平台说明】

-

## 18.48 ip-guard rate-limit

配置全局限速水线。

**ip-guard rate-limit** {per-src-ip | per-port} *pps*

删除限速水线配置，恢复到缺省配置。

**no ip-guard rate-limit {per-src-ip | per-port}**

恢复缺省配置。

**default ip-guard rate-limit {per-src-ip | per-port}**

|        |                   |                                |
|--------|-------------------|--------------------------------|
| 【参数说明】 | 参数                | 描述                             |
|        | <b>per-src-ip</b> | 对每个源 IP 地址进行限速。                |
|        | <b>per-port</b>   | 对每个端口进行限速。                     |
|        | <i>pps</i>        | 限速水线值，单位是每秒报文数，取值范围是[1,19999]。 |

【缺省配置】 缺省配置与产品相关，具体参见《配置指南》中关于产品相关的章节描述。

【命令模式】 NFPP 配置模式

【缺省级别】 14

【使用指导】 -

【配置举例】 1：配置 IP 抗攻击全局限速水线，基于源 IP 限速水线 2pps，基于源端口限速水线 50pps。

```
Ruijie(config)# nfpp
Ruijie(config-nfpp)# ip-guard rate-limit per-src-ip 2
Ruijie(config-nfpp)# ip-guard rate-limit per-port 50
```

【检验方法】 使用 **show nfpp ip-guard summary** 查看配置信息。

【提示信息】 -

【常见错误】 -

【平台说明】 -

## 18.49 ip-guard scan-threshold

配置全局扫描水线。

**ip-guard scan-threshold pkt-cnt**

删除扫描水线配置，恢复到缺省配置。

**no ip-guard scan-threshold**

恢复缺省配置。

**default ip-guard scan-threshold**

| 【参数说明】 | 参数             | 描述                             |
|--------|----------------|--------------------------------|
|        | <i>pkt-cnt</i> | 扫描水线值，单位是每秒报文数，取值范围是[1,19999]。 |

【缺省配置】 缺省扫描水线与产品相关，具体参见《配置指南》中关于产品相关的章节描述。时间单位是 10 秒。

【命令模式】 NFPP 配置模式

【缺省级别】 14

【使用指导】 -

【配置举例】 1：配置 IP 抗攻击全扫描水线为 20pps。

```
Ruijie(config)# nfpp
Ruijie(config-nfpp)# ip-guard scan-threshold 20
```

【检验方法】 使用 **show nfpp ip-guard summary** 查看配置信息。

【提示信息】 -

【常见错误】 -

【平台说明】 -

## 18.50 ip-guard trusted-host

如果管理员希望对某台主机不进行监控，即对该主机表示信任，则可以通过该命令配置。

**ip-guard trusted-host *ip mask***

删除不监控可信主机。

**no ip-guard trusted-host {all | *ip mask*}**

清除不监控可信主机。

**default ip-guard trusted-host**

| 【参数说明】 | 参数          | 描述        |
|--------|-------------|-----------|
|        | <i>ip</i>   | IP 地址。    |
|        | <i>mask</i> | IP 地址的掩码。 |

|            |                              |
|------------|------------------------------|
| <b>all</b> | 和 <b>no</b> 一起使用，删除所有可信主机配置。 |
|------------|------------------------------|

- 【缺省配置】 -
- 【命令模式】 NFPP 配置模式
- 【缺省级别】 14
- 【使用指导】 如果管理员希望对某台主机不进行监控，即对该主机表示信任，则可以通过该命令配置。该可信主机发往 CPU 的 IP 报文将被允许发往 CPU，不做任何的限速和告警处理。  
最多支持设置 500 条可信主机。
- 【配置举例】 1：把 1.1.1.0/24 网段的所有主机配置为 IP 抗攻击的可信主机。
- ```
Ruijie(config)# nfpp
Ruijie(config-nfpp)#ip-guard trusted-host 1.1.1.0 255.255.255.0
```
- 【检验方法】 使用 **show nfpp ip-guard trusted-host** 查看配置信息
- 【提示信息】 -
- 【常见错误】 -
- 【平台说明】 -

18.51 log-buffer enable

配置日志打印到屏幕。

log-buffer enable

日志不打印到屏幕，保存在缓存中，恢复到缺省配置。

no log-buffer enable

恢复缺省配置。

default log-buffer enable

【参数说明】	参数	描述
	-	-

【缺省配置】 默认日志保存在缓存。

【命令模式】 NFPP 配置模式

【缺省级别】 14

【使用指导】 -

【配置举例】 1：日志输出到屏幕。

```
Ruijie(config)# nfpp
Ruijie(config-nfpp)# log-buffer enable
```

【检验方法】 -

【提示信息】 -

【常见错误】 -

【平台说明】 -

18.52 log-buffer entries

配置 NFPP 日志缓冲区大小。

log-buffer entries *number*

删除日志缓冲区大小配置，恢复到缺省配置。

no log-buffer entries

恢复缺省配置。

default log-buffer entries

【参数说明】	参数	描述
	<i>number</i>	缓冲区大小，单位是日志条数，取值范围是[0,1024]。

【缺省配置】 默认缓冲区大小为 256。

【命令模式】 NFPP 配置模式

【缺省级别】 14

【使用指导】 -

【配置举例】 1：把 NFPP 日志缓冲区大小配置为 50 条日志。

```
Ruijie(config)# nfpp
```

```
Ruijie(config-nfpp)# log-buffer entries 50
```

- 【检验方法】 使用 **show nfpp log summary** 查看配置信息。
- 【提示信息】 -
- 【常见错误】 -
- 【平台说明】 -

18.53 log-buffer logs

配置 NFPP 从日志缓冲区取日志生成系统消息的速率。

log-buffer logs *number_of_message interval length_in_seconds*

删除从日志缓冲区取日志生成系统消息的速率配置，恢复到缺省配置。

no log-buffer logs

恢复缺省配置。

default log-buffer logs

【参数说明】	参数	描述
	<i>number_of_message</i>	范围为 0-1024，0 表示日志全部记录在专用缓冲区，不生成系统消息。
	<i>length_in_seconds</i>	范围为 0-86400(1 天)，0 表示不把日志写到缓冲区，而是立即生成系统消息。 <i>number_of_message</i> 和 <i>length_in_seconds</i> 都为 0 表示不把日志写到缓冲区，而是立即生成系统消息。 <i>number_of_message /length_in_second</i> 表示取日志生成系统消息的速率。

- 【缺省配置】 *number_of_message* 缺省为 0，*length_in_seconds* 缺省值为 0。
- 【命令模式】 NFPP 配置模式
- 【缺省级别】 14
- 【使用指导】 -
- 【配置举例】 1：配置日志生成速率为每 12 秒输出 2 条日志信息。

```
Ruijie(config)# nfpp
Ruijie(config-nfpp)# log-buffer logs 2 interval 12
```
- 【检验方法】 使用 **show nfpp log summary** 查看配置信息。

【提示信息】 -

【常见错误】 -

【平台说明】 -

18.54 logging

配置 NFPP 记录哪些 VLAN 或端口的日志。

logging vlan *vlan-range*

logging interface *interface-id*

删除 P 记录哪些 VLAN 或端口的日志的配置

no logging vlan *vlan-range*

no logging interface *interface-id*

恢复缺省配置

default logging

【参数说明】	参数	描述
	<i>vlan-range</i>	需要记录指定 VLAN 范围内的日志信息，输入格式如 “1-3,5” 。
	<i>interface-id</i>	需要记录指定端口的日志信息。

【缺省配置】 所有日志都记录。

【命令模式】 NFPP 配置模式

【缺省级别】 14

【使用指导】 通过该命令可以对日志进行过滤，只记录指定 VLAN 范围或者指定端口的日志信息。两条日志过滤配置是或的关系，即只需要满足其中一条日志过滤规则，就应该记录到日志缓冲区中。

【配置举例】 1：管理员要求只记录 VLAN 1、VLAN 2、VLAN 3 和 VLAN 5 的日志。

```
Ruijie(config)# nfpp
```

```
Ruijie(config-nfpp)# logging vlan 1-3,5
```

2：管理员要求只记录端口 G 0/1 的日志。

```
Ruijie(config)# nfpp
```

```
Ruijie(config-nfpp)# logging interface G 0/1
```

【检验方法】 使用 **show nfpp log summary** 查看配置信息。

【提示信息】 -

【常见错误】 -

【平台说明】 -

18.55 match

该命令用来指定自定义抗攻击匹配的报文类型。

match [*etype type*] [*src-mac smac* [*src-mac-mask smac_mask*]] [*dst-mac dmac* [*dst-mac-mask dst_mask*]] [*protocol protocol*] [*src-ip sip* [*src-ip-mask sip-mask*]] [*src-ipv6 sipv6* [*src-ipv6-masklen sipv6-masklen*]] [*dst-ip dip* [*dst-ip-mask dip-mask*]] [*dst-ipv6 dipv6* [*dst-ipv6-masklen dipv6-masklen*]][*src-port sport*] [*dst-port dport*]

【参数说明】

参数	描述
<i>type</i>	以太网链路层报文类型。
<i>smac</i>	源 mac 地址。
<i>smac_mask</i>	源 mac 地址掩码。
<i>dmac</i>	目的 mac 地址。
<i>dmac_mask</i>	目的 mac 地址掩码。
<i>protocol</i>	IPv4/v6 报文协议号。
<i>sip</i>	源 IPv4 地址。
<i>sip_mask</i>	源 IPv4 地址掩码。
<i>sipv6</i>	源 IPv6 地址。
<i>sipv6_masklen</i>	源 IPv6 地址掩码长度。
<i>dip</i>	目的 IPv4 地址。
<i>dip_mask</i>	目的 IPv4 地址掩码。
<i>dipv6</i>	目的 IPv6 地址。
<i>dipv6_masklen</i>	目的 IPv6 地址掩码长度。
<i>sport</i>	源传输层端口号。
<i>dport</i>	目的传输层端口号。

【缺省配置】 -

【命令模式】 NFPP 配置模式

【缺省级别】 14

【使用指导】 创建新的自定义抗攻击类型。指定该类型所要匹配的报文字段。

【配置举例】 1：创建自定义抗攻击 tcp，其匹配关键字段为 etype 0x0800，protocol 0x06 的报文。

```
Ruijie(config)# nfpp
Ruijie(config-nfpp)#define tcp
Ruijie(config-nfpp-define)#match etype 0x0800 protocol 0x06
```

【检验方法】 使用 **show nfpp define summary name** 查看配置信息。

【提示信息】 -

【常见错误】 -

【平台说明】 -

18.56 monitored-host-limit

该命令用来配置支持的最大受监控主机数。

monitored-host-limit *number*

删除最大受监控主机数配置，恢复到缺省配置。

no monitored-host-limit

恢复缺省配置。

default monitored-host-limit

【参数说明】	参数	描述
	<i>number</i>	支持的最大受监控主机数，取值范围为 1 到 4294967295。

【缺省配置】 最大受监控主机数默认 1000 个。

【命令模式】 NFPP 自定义类型配置模式

【缺省级别】 14

【使用指导】 如果受监控主机数已经达到默认的 20000 个，此时管理员把受监控主机的最大数目设置成小于 20000，不会删除已有的受监控主机，而是打印信息 “%ERROR: The value that you configured is smaller than current monitored hosts 20000 (配置的受监控主机数) ， please clear a part of monitored hosts.” 来提醒管理员配置没有生效，需要删除部分已经被监控的主机。
当受监控主机满时，打印日志 “% NFPP_DEFINE_GUARD -4-SESSION_LIMIT: Attempt to exceed limit of name(自定义抗攻击类型名)'s 20000 (配置的受监控主机数) monitored hosts.” 提醒管理员。

【配置举例】 1：配置自定义抗攻击 tcp，最大受监控主机数为 500 个。

```
Ruijie(config)# nfpp
Ruijie(config-nfpp)# define tcp
Ruijie(config-nfpp-define)#monitored-host-limit 500
```

【检验方法】 使用 **show nfpp define summary name** 查看配置信息。

【提示信息】 -

【常见错误】 -

【平台说明】 -

18.57 monitor-period

该命令用来配置监控时间。

monitor-period seconds

删除置监控时间配置，恢复到缺省配置。

no monitor-period

恢复缺省配置。

default monitor-period

【参数说明】	参数	描述
	seconds	监控时间，单位是秒，取值范围是[180, 86400]。

【缺省配置】 全局监控时间的缺省值是 600 秒。

【命令模式】 NFPP 自定义类型配置模式

【缺省级别】 14

【使用指导】 检测出攻击者的时候，如果隔离时间为 0，将对攻击者进行软件监控，超时为监控时间。在软件监控过程中，当隔离时间被配置为非零值时，将自动对软件监控的攻击者采取硬件隔离，并且把超时设置为隔离时间。监控时间在隔离时间为 0 的情况下才有意义。
如果把隔离时间从非零值改成零，将直接把相关端口的攻击者删除，而不是进行软件监控。

【配置举例】 1：配置自定义抗攻击 tcp，监控时间 180 秒。

```
Ruijie(config)# nfpp
Ruijie(config-nfpp)# define tcp
```

```
Ruijie(config-nfpp-define)#monitor-period 180
```

命令	描述
show nfpp define summary <i>name</i>	显示自定义抗攻击类型配置信息。

【平台说明】 -

18.58 nd-guard attack-threshold

配置全局攻击水线，即当报文速度超过攻击水线的时候，认为存在攻击行为。

nd-guard attack-threshold per-port {ns-na | rs | ra-redirect} pps

删除攻击水线配置，恢复到缺省配置。

no nd-guard attack-threshold per-port {ns-na | rs | ra-redirect}

恢复缺省配置。

default nd-guard attack-threshold per-port {ns-na | rs | ra-redirect}

参数	描述
ns-na	邻居请求和邻居公告。
rs	路由器请求。
ra-redirect	路由器公告和重定向报文。
<i>pps</i>	攻击水线，单位是每秒报文数，取值范围是[1,19999]。

【缺省配置】 缺省配置与产品相关，具体参见《配置指南》中关于产品相关的章节描述。

【命令模式】 NFPP 配置模式

【缺省级别】 14

【使用指导】 攻击水线不能小于限速水线。

【配置举例】 1：配置 ND 抗攻击全局攻击水线，基于源端口的 ns-na 攻击水线 20pps,基于源端口的 rs 攻击水线 10pps，基于源端口的 ra-redirect 攻击水线 10pps。

```
Ruijie(config)# nfpp
Ruijie(config-nfpp)# nd-guard attack-threshold per-port ns-na 20
Ruijie(config-nfpp)# nd-guard attack-threshold per-port rs 10
Ruijie(config-nfpp)# nd-guard attack-threshold per-port ra-redirect 10
```

【检验方法】 使用 **show nfpp nd-guard summary** 查看配置信息。

【提示信息】 -

【常见错误】 -

【平台说明】 -

18.59 nd-guard enable

该命令用来全局打开 ND 抗攻击功能。

nd-guard enable

关闭 ND 抗攻击功能。

no nd-guard enable

恢复缺省配置。

default nd-guard enable

【参数说明】

参数	描述
-	-

【缺省配置】 默认 ND 抗攻击功能打开。

【命令模式】 NFPP 配置模式

【缺省级别】 14

【使用指导】 -

【配置举例】 1：配置全局打开 ND 抗攻击功能

```
Ruijie(config)# nfpp
```

```
Ruijie(config-nfpp)# nd-guard enable
```

【检验方法】 使用 **show nfpp nd-guard summary** 查看配置信息。

【提示信息】 -

【常见错误】 -

【平台说明】 -

18.60 nd-guard rate-limit

配置全局限速水线。

nd-guard rate-limit per-port {ns-na | rs | ra-redirect} pps

删除限速水线配置，恢复到缺省配置。

no nd-guard rate-limit per-port {ns-na | rs | ra-redirect}

恢复缺省配置。

default nd-guard rate-limit per-port {ns-na | rs | ra-redirect}

【参数说明】	参数	描述
	ns-na	邻居请求和邻居公告。
	rs	路由器请求。
	ra-redirect	路由器公告和重定向报文。
	<i>pps</i>	限速水线值，单位是每秒报文数，取值范围是[1,19999]。

【缺省配置】 缺省配置与产品相关，具体参见《配置指南》中关于产品相关的章节描述。

【命令模式】 NFPP 配置模式

【缺省级别】 14

【使用指导】 -

【配置举例】 1：配置 ND 抗攻击全局限速水线，基于源端口 ns-na 限速水线 10pps，基于源端口 rs 限速水线 5pps,基于源端口 ra-redirect 限速水线 5pps。

```
Ruijie(config)# nfpp
Ruijie(config-nfpp)# nd-guard rate-limit per-port ns-na 10
Ruijie(config-nfpp)# nd-guard rate-limit per-port rs 5
Ruijie(config-nfpp)# nd-guard rate-limit per-port ra-redirect 5
```

【检验方法】 使用 **show nfpp nd-guard summary** 查看配置信息。

【提示信息】 -

【常见错误】 -

【平台说明】 -

18.61 nd-guard ratelimit-forwarding enable

配置 ND 抗攻击基于端口的隔离转发限速功能，恢复到缺省配置。

nd-guard ratelimit-forwarding enable

关闭隔离转发限速功能。

no nd-guard ratelimit-forwarding enable

恢复缺省配置。

default nd-guard ratelimit-forwarding enable

【参数说明】	参数	描述
	-	-

【缺省配置】 缺省打开基于端口的隔离转发限速功能。

【命令模式】 NFPP 配置模式

【缺省级别】 14

【使用指导】 -

【配置举例】 1：配置使 ND 抗攻击基于端口的隔离转发限速功能。

```
Ruijie(config)# nfpp
```

```
Ruijie(config-nfpp)# nd-guard ratelimit-forwarding enable
```

【检验方法】 -

【提示信息】 -

【常见错误】 -

【平台说明】 -

18.62 nfpp

该命令用于进入 nfpp 配置模式。

nfpp

【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】 通过此命令进入 nfpp 配置模式，进行 nfpp 的相关配置

【配置举例】 Ruijie(config)# nfpp

【检验方法】 -

【提示信息】 -

【常见错误】 -

【平台说明】 -

18.63 nfpp arp-guard enable

该命令用来在端口上打开 ARP 抗攻击功能。

nfpp arp-guard enable

关闭端口上的 ARP 抗攻击功能。

no nfpp arp-guard enable

恢复缺省配置。

default nfpp arp-guard enable

【参数说明】	参数	描述
	-	-

【缺省配置】 端口没有配置 ARP 抗攻击开关，采用全局开关。

【命令模式】 接口配置模式

【缺省级别】 14

【使用指导】 端口的 ARP 抗攻击开关优先于全局 ARP 抗攻击开关。

【配置举例】 1 打开接口 G0/1 上 ARP 抗攻击抗攻击能力。

```
Ruijie(config)# interface G0/1
Ruijie(config-if)# nfpp arp-guard enable
```

【检验方法】 使用 **show nfpp arp-guard summary** 查看配置信息。

【提示信息】 -

【常见错误】 -

【平台说明】 -

18.64 nfpp arp-guard isolate-period

该命令用来在端口上配置局部隔离时间。

```
nfpp arp-guard isolate-period {seconds | permanent}
```

删除端口上隔离时间配置，恢复到缺省配置。

```
no nfpp arp-guard isolate-period
```

恢复缺省配置。

```
default nfpp arp-guard isolate-period
```

【参数说明】	参数	描述
	seconds	隔离时间，单位是秒，取值范围是 0 或者[30, 86400]，0 表示不隔离。
	permanent	永久隔离。

【缺省配置】 缺省情况是没有配置局部隔离时间，采用全局隔离时间。

【命令模式】 接口配置模式

【缺省级别】 14

【使用指导】 -

【配置举例】 1：配置接口 G0/1 上 ARP 抗攻击隔离时间为 180 秒。

```
Ruijie(config)# interface G 0/1
Ruijie(config-if)# nfpp arp-guard isolate-period 180
```

【检验方法】 使用 **show nfpp arp-guard summary** 查看配置信息。

【提示信息】 -

【常见错误】 -

【平台说明】 -

18.65 nfpp arp-guard policy

在端口上配置局部的限速水线和攻击水线。

nfpp arp-guard policy {per-src-ip | per-src-mac | per-port} rate-limit-pps attack-threshold-pps

删除端口上限速水线和攻击水线配置，恢复到缺省配置。

no nfpp arp-guard policy {per-src-ip | per-src-mac | per-port}

恢复缺省配置。

default nfpp arp-guard policy {per-src-ip | per-src-mac | per-port}

【参数说明】

参数	描述
per-src-ip	配置每个源 IP 地址的限速水线和攻击水线。
per-src-mac	配置每个源 MAC 地址的限速水线和攻击水线。
per-port	配置每个端口的限速水线和攻击水线。
<i>rate-limit-pps</i>	限速水线，单位是每秒报文数，取值范围是 1 到 19999。
<i>attack-threshold-pps</i>	攻击水线，单位是每秒报文数，取值范围是 1 到 19999。

【缺省配置】 端口没有自己的限速水线和攻击水线，采用全局的限速水线和限速水线。

【命令模式】 接口配置模式

【缺省级别】 14

【使用指导】 攻击水线不能小于限速水线。

【配置举例】 1：配置接口 G0/1 上 ARP 抗攻击限速水线和攻击水线，配置基于 IP 限速水线 2pps，攻击水线 10pps；配置基于 MAC 限速水线 3pps，攻击水线 10pps；配置基于端口限速水线 50pps，攻击水线 100pps。

```
Ruijie(config)# interface G 0/1
Ruijie(config-if)# nfpp arp-guard policy per-src-ip 2 10
Ruijie(config-if)# nfpp arp-guard policy per-src-mac 3 10
Ruijie(config-if)# nfpp arp-guard policy per-port 50 100
```

- 【检验方法】 使用 **show nfpp arp-guard summary** 查看配置信息。
- 【提示信息】 -
- 【常见错误】 -
- 【平台说明】 -

18.66 nfpp arp-guard scan-threshold

在端口上配置局部扫描水线。
nfpp arp-guard scan-threshold *pkt-cnt*

删除端口上扫描水线配置，恢复到缺省配置。
no nfpp arp-guard scan-threshold

恢复缺省配置。
default nfpp arp-guard scan-threshold

【参数说明】	参数	描述
	<i>pkt-cnt</i>	扫描水线值，单位是每秒报文数，取值范围是[1,19999]。

【缺省配置】 没配置基于端口的 ARP 扫描阈值，采用全局 ARP 扫描阈值。

【命令模式】 接口配置模式

【缺省级别】 14

【使用指导】 -

【配置举例】 1：配置接口 G0/1 上 ARP 抗攻击描水线为 20pps。
Ruijie(config)# interface G 0/1
Ruijie(config-if)# nfpp arp-guard scan-threshold 20

【检验方法】 使用 **show nfpp arp-guard summary** 查看配置信息。

【提示信息】 -

【常见错误】 -

【平台说明】 -

18.67 nfpp define *name* enable

该命令用来开启端口上的自定义类型抗攻击功能。

nfpp define *name* enable

关闭端口上的自定义类型抗攻击功能。

no nfpp define *name* enable

恢复缺省配置。

default nfpp define *name* enable

【参数说明】

参数	描述
<i>name</i>	自定义的抗攻击类型名称。

【缺省配置】 -

【命令模式】 接口配置模式

【缺省级别】 14

【使用指导】 必须存在该自定义名字，并且配置了 match、global-policy 之后，配置才能生效，否则配置失败。

【配置举例】 1 打开接口 G0/1 上自定义抗攻击 tcp 抗攻击能力。

```
Ruijie(config)# interface G0/1
Ruijie(config-if)# nfpp define tcp enable
```

【检验方法】 使用 **show nfpp define summary *name*** 查看配置信息。

【提示信息】 -

【常见错误】 -

【平台说明】 -

18.68 nfpp define *name* policy

在端口上配置局部的限速水线和攻击水线。

nfpp define *name* policy {per-src-ip | per-src-mac | per-port} rate-limit-pps attack-threshold-pps

删除端口上限速水线和攻击水线配置，恢复到缺省配置。

no nfpp define *name* policy {per-src-ip | per-src-mac | per-port}

恢复缺省配置。

default nfpp define *name* policy {per-src-ip | per-src-mac | per-port}

【参数说明】

参数	描述
per-src-ip	配置每个源 IP 地址的攻击水线。
per-src-mac	配置每个源 MAC 地址的攻击水线。
per-port	配置每个端口的攻击水线。
<i>rate-limit-pps</i>	限速水线，单位是每秒报文数，取值范围是 1 到 19999。
<i>attack-threshold-pps</i>	攻击水线，单位是每秒报文数，取值范围是 1 到 19999。

【缺省配置】 端口没有自己的限速水线和攻击水线，采用全局的限速水线和攻击水线。

【命令模式】 接口配置模式

【缺省级别】 14

【使用指导】 攻击水线不能小于限速水线。

【配置举例】 1：配置接口 G0/1 上自定义抗攻击 tcp 限速水线和攻击水线，配置基于 IP 限速水线 2pps，攻击水线 10pps；配置基于端口限速水线 50pps，攻击水线 100pps。

```
Ruijie(config)# interface G 0/1
Ruijie(config-if)# nfpp define tcp policy per-src-ip 2 10
Ruijie(config-if)# nfpp define tcp policy per-port 50 100
```

【检验方法】 使用 **show nfpp define summary *name*** 查看配置信息。

【提示信息】 -

【常见错误】 -

【平台说明】 -

18.69 nfpp dhcp-guard enable

该命令用来在端口上打开 DHCP 抗攻击功能。

nfpp dhcp-guard enable

关闭端口上的 DHCP 抗攻击功能。

no nfpp dhcp-guard enable

恢复缺省配置。

default nfpp dhcp-guard enable

【参数说明】	参数	描述
	-	-

【缺省配置】 端口没有配置 DHCP 抗攻击开关，采用全局开关。

【命令模式】 接口配置模式

【缺省级别】 14

【使用指导】 端口的 DHCP 抗攻击开关优先于全局 DHCP 抗攻击开关。

【配置举例】 1 打开接口 G0/1 上 DHCP 抗攻击抗攻击能力。

```
Ruijie(config)# interface G0/1
Ruijie(config-if)# nfpp dhcp-guard enable
```

【检验方法】 使用 **show nfpp dhcp-guard summary** 查看配置信息。

【提示信息】 -

【常见错误】 -

【平台说明】 -

18.70 nfpp dhcp-guard isolate-period

该命令用来在端口上配置局部隔离时间。

nfpp dhcp-guard isolate-period {seconds | permanent}

删除端口上隔离时间配置，恢复到缺省配置。

no nfpp dhcp-guard isolate-period

恢复缺省配置。

default nfpp dhcp-guard isolate-period

【参数说明】	参数	描述
	<i>seconds</i>	隔离时间，单位是秒，取值范围是 0 或者[30, 86400]，0 表示不隔离。
	permanent	永久隔离。
【缺省配置】	缺省情况是没有配置局部隔离时间，采用全局隔离时间。	
【命令模式】	接口配置模式	
【缺省级别】	14	
【使用指导】	-	
【配置举例】	1：配置接口 G0/1 上 DHCP 抗攻击隔离时间为 180 秒。 <pre>Ruijie(config)# interface G 0/1 Ruijie(config-if)# nfpp dhcp-guard isolate-period 180</pre>	
【检验方法】	使用 show nfpp dhcp-guard summary 查看配置信息。	
【提示信息】	-	
【常见错误】	-	
【平台说明】	-	

18.71 nfpp dhcp-guard policy

在端口上配置局部的限速水线和攻击水线。

nfpp dhcp-guard policy { per-src-mac | per-port} rate-limit-pps attack-threshold-pps

删除端口上限速水线和攻击水线配置，恢复到缺省配置。

no nfpp dhcp-guard policy { per-src-mac | per-port}

恢复缺省配置。

default nfpp dhcp-guard policy { per-src-mac | per-port}

【参数说明】	参数	描述
	per-src-mac	配置每个源 MAC 地址的限速水线和攻击水线。
	per-port	配置每个端口的限速水线和攻击水线。
	<i>rate-limit-pps</i>	限速水线，单位是每秒报文数，取值范围是 1 到 19999。
	<i>attack-threshold-pps</i>	攻击水线，单位是每秒报文数，取值范围是 1 到 19999。

【缺省配置】	端口没有自己的限速水线和攻击水线，采用全局的限速水线和限速水线。
【命令模式】	接口配置模式
【缺省级别】	14
【使用指导】	攻击水线不能小于限速水线。
【配置举例】	1：配置接口 G0/1 上 DHCP 抗攻击限速水线和攻击水线，配置基于 MAC 限速水线 3pps，攻击水线 10pps；配置基于端口限速水线 50pps，攻击水线 100pps。 Ruijie(config)# interface G 0/1 Ruijie(config-if)# nfpp dhcp-guard policy per-src-mac 3 10 Ruijie(config-if)# nfpp dhcp-guard policy per-port 50 100
【检验方法】	使用 show nfpp dhcp-guard summary 查看配置信息。
【提示信息】	-
【常见错误】	-
【平台说明】	-

18.72 nfpp dhcpv6-guard enable

该命令用来在端口上打开 DHCPv6 抗攻击功能。

nfpp dhcpv6-guard enable

关闭端口上的 DHCPv6 抗攻击功能。

no nfpp dhcpv6-guard enable

恢复缺省配置。

default nfpp dhcpv6-guard enable

【参数说明】	参数	描述
	-	-

【缺省配置】	端口没有配置 DHCPv6 抗攻击开关，采用全局开关。
【命令模式】	接口配置模式

- 【缺省级别】 14
- 【使用指导】 端口的 DHCPv6 抗攻击开关优先于全局 DHCP 抗攻击开关。
- 【配置举例】 1 打开接口 G0/1 上 DHCPv6 抗攻击抗攻击能力。
- ```
Ruijie(config)# interface G0/1
Ruijie(config-if)# nfpp dhcpv6-guard enable
```
- 【检验方法】 使用 **show nfpp dhcpv6-guard summary** 查看配置信息。
- 【提示信息】 -
- 【常见错误】 -
- 【平台说明】 -

## 18.73 nfpp dhcpv6-guard policy

在端口上配置局部的限速水线和攻击水线。

**nfpp dhcpv6-guard policy { per-src-mac | per-port} rate-limit-pps attack-threshold-pps**

删除端口上限速水线和攻击水线配置，恢复到缺省配置。

**no nfpp dhcpv6-guard policy { per-src-mac | per-port}**

恢复缺省配置。

**default nfpp dhcpv6-guard policy { per-src-mac | per-port}**

|        |                             |                                |
|--------|-----------------------------|--------------------------------|
| 【参数说明】 | 参数                          | 描述                             |
|        | <b>per-src-mac</b>          | 配置每个源 MAC 地址的限速水线和攻击水线。        |
|        | <b>per-port</b>             | 配置每个端口的限速水线和攻击水线。              |
|        | <i>rate-limit-pps</i>       | 限速水线，单位是每秒报文数，取值范围是 1 到 19999。 |
|        | <i>attack-threshold-pps</i> | 攻击水线，单位是每秒报文数，取值范围是 1 到 19999。 |

- 【缺省配置】 端口没有自己的限速水线和攻击水线，采用全局的限速水线和限速水线。
- 【命令模式】 接口配置模式
- 【缺省级别】 14
- 【使用指导】 攻击水线不能小于限速水线。



【配置举例】 1：配置接口 G0/1 上 DHCPv6 抗攻击限速水线和攻击水线，配置基于 IP 限速水线 2pps，攻击水线 10pps；配置基于 MAC 限速水线 3pps，攻击水线 10pps；配置基于端口限速水线 50pps，攻击水线 100pps。

```
Ruijie(config)# interface G 0/1
Ruijie(config-if)# nfpp dhcpv6-guard policy per-src-mac 3 10
Ruijie(config-if)# nfpp dhcpv6-guard policy per-port 50 100
```

【检验方法】 使用 **show nfpp dhcpv6-guard summary** 查看配置信息。

【提示信息】 -

【常见错误】 -

【平台说明】 -

18.74 nfpp icmp-guard enable

该命令用来在端口上打开 ICMP 抗攻击功能。

**nfpp icmp-guard enable**

关闭端口上的 ICMP 抗攻击功能。

**no nfpp icmp-guard enable**

恢复缺省配置。

**default nfpp icmp-guard enable**

| 【参数说明】 | 参数 | 描述 |
|--------|----|----|
|        | -  | -  |

【缺省配置】 端口没有配置 ICMP 抗攻击开关，采用全局开关。

【命令模式】 接口配置模式

【缺省级别】 14

【使用指导】 端口的 ICMP 抗攻击开关优先于全局 ICMP 抗攻击开关。

【配置举例】 1 打开接口 G0/1 上 ICMP 抗攻击能力。

```
Ruijie(config)# interface G0/1
Ruijie(config-if)# nfpp icmp-guard enable
```

【检验方法】 使用 **show nfpp icmp-guard summary** 查看配置信息。

【提示信息】 -

【常见错误】 -

【平台说明】 -

## 18.75 nfpp icmp-guard isolate-period

该命令用来在端口上配置局部隔离时间。

**nfpp icmp-guard isolate-period** {seconds | permanent}

删除端口上隔离时间配置，恢复到缺省配置。

**no nfpp icmp-guard isolate-period**

恢复缺省配置。

**default nfpp icmp-guard isolate-period**

|        |           |                                          |
|--------|-----------|------------------------------------------|
| 【参数说明】 | 参数        | 描述                                       |
|        | seconds   | 隔离时间，单位是秒，取值范围是 0 或者[30, 86400]，0 表示不隔离。 |
|        | permanent | 永久隔离。                                    |

【缺省配置】 缺省情况是没有配置局部隔离时间，采用全局隔离时间。

【命令模式】 接口配置模式

【缺省级别】 14

【使用指导】 -

【配置举例】 1：配置接口 G0/1 上 ICMP 抗攻击隔离时间为 180 秒。

```
Ruijie(config)# interface G 0/1
Ruijie(config-if)# nfpp icmp-guard isolate-period 180
```

【检验方法】 使用 **show nfpp icmp-guard summary** 查看配置信息。

【提示信息】 -

【常见错误】 -

【平台说明】 -

18.76 nfpp icmp-guard policy

在端口上配置局部的限速水线和攻击水线。

**nfpp icmp-guard policy { per-src-ip | per-port} rate-limit-pps attack-threshold-pps**

删除端口上限速水线和攻击水线配置，恢复到缺省配置。

**no nfpp icmp-guard policy {per-src-ip | per-port}**

恢复缺省配置。

**default nfpp icmp-guard policy {per-src-ip | per-port}**

【参数说明】

| 参数                          | 描述                             |
|-----------------------------|--------------------------------|
| <b>per-src-ip</b>           | 配置每个源 IP 地址的限速水线和攻击水线。         |
| <b>per-port</b>             | 配置每个端口的限速水线和攻击水线。              |
| <i>rate-limit-pps</i>       | 限速水线，单位是每秒报文数，取值范围是 1 到 19999。 |
| <i>attack-threshold-pps</i> | 攻击水线，单位是每秒报文数，取值范围是 1 到 19999。 |

【缺省配置】 端口没有自己的限速水线和攻击水线，采用全局的限速水线和限速水线。

【命令模式】 接口配置模式

【缺省级别】 14

【使用指导】 攻击水线不能小于限速水线。

【配置举例】 1：配置接口 G0/1 上 ICMP 抗攻击限速水线和攻击水线，配置基于 IP 限速水线 5pps，攻击水线 10pps；配置基于端口限速水线 100pps，攻击水线 200pps。

```
Ruijie(config)# interface G 0/1
Ruijie(config-if)# nfpp icmp-guard policy per-src-ip 5 10
Ruijie(config-if)# nfpp icmp-guard policy per-port 100 200
```

【检验方法】 使用 **show nfpp icmp-guard summary** 查看配置信息。

【提示信息】 -

【常见错误】 -

【平台说明】 -

## 18.77 nfpp ip-guard enable

该命令用来在端口上打开 IP 防扫描功能。

**nfpp ip-guard enable**

关闭端口上的 IP 防扫描功能。

**no nfpp ip-guard enable**

恢复缺省配置。

**default nfpp ip-guard enable**

| 【参数说明】 | 参数 | 描述 |
|--------|----|----|
|        | -  | -  |

【缺省配置】 端口没有配置 IP 防扫描开关，采用全局开关。

【命令模式】 接口配置模式

【缺省级别】 14

【使用指导】 端口的 IP 防扫描开关优先于全局防扫描开关。

【配置举例】 1 打开接口 G0/1 上 IP 防扫描能力。

```
Ruijie(config)# interface G0/1
Ruijie(config-if)# nfpp ip-guard enable
```

【检验方法】 使用 **show nfpp ip-guard summary** 查看配置信息。

【提示信息】 -

【常见错误】 -

【平台说明】 -

## 18.78 nfpp ip-guard isolate-period

该命令用来在端口上配置局部隔离时间。

**nfpp ip-guard isolate-period {seconds | permanent}**

删除端口上隔离时间配置，恢复到缺省配置。

**no nfpp ip-guard isolate-period**

恢复缺省配置。

**default nfpp ip-guard isolate-period**

【参数说明】

| 参数               | 描述                                       |
|------------------|------------------------------------------|
| <i>seconds</i>   | 隔离时间，单位是秒，取值范围是 0 或者[30, 86400]，0 表示不隔离。 |
| <b>permanent</b> | 永久隔离。                                    |

【缺省配置】 缺省情况是没有配置局部隔离时间，采用全局隔离时间。

【命令模式】 接口配置模式

【缺省级别】 14

【使用指导】 -

【配置举例】 1：配置接口 G0/1 上 IP 抗攻击隔离时间为 180 秒。

```
Ruijie(config)# interface G 0/1
Ruijie(config-if)# nfpp ip-guard isolate-period 180
```

【检验方法】 使用 **show nfpp ip-guard summary** 查看配置信息。

【提示信息】 -

【常见错误】 -

【平台说明】 -

## 18.79 nfpp ip-guard policy

在端口上配置局部的限速水线和攻击水线。

**nfpp ip-guard policy {per-src-ip | per-port} rate-limit-pps attack-threshold-pps**

删除端口上限速水线和攻击水线配置，恢复到缺省配置。

**no nfpp ip-guard policy {per-src-ip | per-port}**

恢复缺省配置。

**default nfpp ip-guard policy {per-src-ip | per-port}**

| 【参数说明】 | 参数                          | 描述                             |
|--------|-----------------------------|--------------------------------|
|        | <b>per-src-ip</b>           | 配置每个源 IP 地址的攻击水线。              |
|        | <b>per-port</b>             | 配置每个端口的攻击水线。                   |
|        | <i>rate-limit-pps</i>       | 限速水线，单位是每秒报文数，取值范围是 1 到 19999。 |
|        | <i>attack-threshold-pps</i> | 攻击水线，单位是每秒报文数，取值范围是 1 到 19999。 |

【缺省配置】 端口没有自己的限速水线和攻击水线，采用全局的限速水线和攻击水线。

【命令模式】 接口配置模式

【缺省级别】 14

【使用指导】 攻击水线不能小于限速水线。

【配置举例】 1：配置接口 G0/1 上 IP 抗攻击限速水线和攻击水线，配置基于 IP 限速水线 2pps，攻击水线 10pps；配置基于端口限速水线 50pps，攻击水线 100pps。

```
Ruijie(config)# interface G 0/1
Ruijie(config-if)# nfpp ip-guard policy per-src-ip 2 10
Ruijie(config-if)# nfpp ip-guard policy per-port 50 100
```

【检验方法】 使用 **show nfpp ip-guard summary** 查看配置信息。

【提示信息】 -

【常见错误】 -

【平台说明】 -

## 18.80 nfpp ip-guard scan-threshold

在端口上配置局部扫描水线。

**nfpp ip-guard scan-threshold** *pkt-cnt*

删除端口上扫描水线配置，恢复到缺省配置。

**no nfpp ip-guard scan-threshold**

恢复缺省配置。

**default nfpp ip-guard scan-threshold**

| 【参数说明】 | 参数 | 描述 |
|--------|----|----|
|--------|----|----|

|                |                                |
|----------------|--------------------------------|
| <i>pkt-cnt</i> | 扫描水线值，单位是每秒报文数，取值范围是[1,19999]。 |
|----------------|--------------------------------|

【缺省配置】 没配置基于端口的 IP 扫描水线，采用全局 ARP 扫描水线。

【命令模式】 接口配置模式

【缺省级别】 14

【使用指导】 -

【配置举例】 1：配置接口 G0/1 上 IP 抗攻击扫描水线为 20pps。

```
Ruijie(config)# interface G 0/1
Ruijie(config-if)# nfpp ip-guard scan-threshold 20
```

【检验方法】 使用 **show nfpp ip-guard summary** 查看配置信息。

【提示信息】 -

【常见错误】 -

【平台说明】 -

## 18.81 nfpp nd-guard enable

该命令用来在端口上打开 ND 抗攻击功能。

**nfpp nd-guard enable**

关闭端口上的 ND 抗攻击功能。

**no nfpp nd-guard enable**

恢复缺省配置。

**default nfpp nd-guard enable**

| 【参数说明】 | 参数 | 描述 |
|--------|----|----|
|        | -  | -  |

【缺省配置】 端口没有配置 ND 抗攻击开关，采用全局开关。

【命令模式】 接口配置模式

【缺省级别】 14

【使用指导】 端口的 ND 抗攻击开关优先于全局开关。

【配置举例】 1：配置使能 G0/1 口的 ND 抗攻击。

```
Ruijie(config)# interface G0/1
Ruijie(config-if)# nfpp nd-guard enable
```

【检验方法】 使用 **show nfpp nd-guard summary** 查看配置信息。

【提示信息】 -

【常见错误】 -

【平台说明】 -

## 18.82 nfpp nd-guard policy

在端口上配置局部的限速水线和攻击水线。

**nfpp nd-guard policy per-port {ns-na | rs | ra-redirect} *rate-limit-pps attack-threshold-pps***

删除端口上限速水线和攻击水线配置，恢复到缺省配置。

**no nfpp nd-guard policy per-port {ns-na | rs | ra-redirect}**

恢复缺省配置。

**default nfpp nd-guard policy per-port {ns-na | rs | ra-redirect}**

【参数说明】

| 参数                          | 描述                             |
|-----------------------------|--------------------------------|
| <b>ns-na</b>                | 邻居请求和邻居公告。                     |
| <b>rs</b>                   | 路由器请求。                         |
| <b>ra-redirect</b>          | 路由器公告和重定向报文。                   |
| <i>rate-limit-pps</i>       | 限速水线，单位是每秒报文数，取值范围是 1 到 19999。 |
| <i>attack-threshold-pps</i> | 攻击水线，单位是每秒报文数，取值范围是 1 到 19999。 |

【缺省配置】 端口没有自己的限速水线和攻击水线，采用全局的限速水线和攻击水线。

【命令模式】 接口配置模式

【缺省级别】 14

【使用指导】 攻击水线不能小于限速水线。



【配置举例】 1 :配置接口 G0/1 上 ND 抗攻击限速水线和攻击水线 ,配置基于端口 ns-na 限速水线 50pps ,攻击水线 100pps ;配置基于端口 rs 限速水线 10pps ,攻击水线 20pps;配置基于端口 ra-redirect 限速水线 10pps,gongji 水线 20pps。

```
Ruijie(config)# interface G 0/1
Ruijie(config-if)# nfpp nd-guard policy per-port ns-na 50 100
Ruijie(config-if)# nfpp nd-guard policy per-port rs 10 20
Ruijie(config-if)# nfpp nd-guard policy per-port ra-redirect 10 20
```

【检验方法】 使用 **show nfpp nd-guard summary** 查看配置信息。

【提示信息】 -

【常见错误】 -

【平台说明】 -

## 18.83 show nfpp arp-guard hosts

查看受监控主机。

**show nfpp arp-guard hosts** [**statistics** | [[*vlan vid*] [*interface interface-id*] [*ip-address* | *mac-address*]]]

| 参数                  | 描述            |
|---------------------|---------------|
| <b>statistics</b>   | 查看受监控主机的统计信息。 |
| <i>vid</i>          | 虚拟局域网号。       |
| <i>interface-id</i> | 端口名称。         |
| <i>ip-address</i>   | IP 地址。        |
| <i>mac-address</i>  | 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 ARP 抗攻击受监控主机的统计信息。当前有 120 台主机被监控，其中 100 台主机被硬件成功地隔离，20 台主机硬件隔离失败（通常引起的原因有内存不足，或者硬件资源不足）。

```
Ruijie# show nfpp arp-guard hosts statistics
success fail total

```

100          20          120

2：查看 ARP 抗攻击受监控主机，第四列 “remain-time(s)” 是指剩余的隔离时间。

```
Ruijie# show nfpp arp-guard hosts
```

If column 1 shows '\*', it means "hardware do not isolate user".

| VLAN            | interface | IP address | MAC address    | remain-time(s) |
|-----------------|-----------|------------|----------------|----------------|
| 1               | Gi0/1     | 1.1.1.1    | -              | 110            |
| 2               | Gi0/2     | 1.1.2.1    | -              | 61             |
| *3              | Gi0/3     | -          | 0000.0000.1111 | 110            |
| 4               | Gi0/4     | -          | 0000.0000.2222 | 61             |
| Total : 4 hosts |           |            |                |                |

【提示信息】 -

【平台说明】 -

## 18.84 show nfpp arp-guard scan

查看 ARP 扫描表。

**show nfpp arp-guard scan** [**statistics** | **[[vlan vid] [interface interface-id] [ip-address] [mac-address]]**]

【参数说明】

| 参数                  | 描述               |
|---------------------|------------------|
| <b>statistics</b>   | 查看 ARP 扫描表的记录条数。 |
| <i>vid</i>          | 虚拟局域网号。          |
| <i>interface-id</i> | 端口名称。            |
| <i>mac-address</i>  | 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 ARP 抗攻击扫描用户统计信息，当前扫描表总共有 4 条记录。

```
Ruijie# show nfpp arp-guard scan statistics
```

arp-guard scan table has 4 record(s).

2：查看 ARP 抗攻击扫描用户信息，“timestamp” 记录的是检测出 ARP 扫描的时间，如 “2008-01-23 16:23:10” 表示在 2008 年 1 月 23 日 16 点 23 分 10 秒检测出 ARP 扫描。

```
Ruijie# show nfpp arp-guard scan
```

| VLAN | interface | IP address | MAC address    | timestamp           |
|------|-----------|------------|----------------|---------------------|
| 1    | Gi0/1     | -          | 0000.0000.0001 | 2008-01-23 16:23:10 |
| 2    | Gi0/2     | 1.1.1.1    | 0000.0000.0002 | 2008-01-23 16:24:10 |
| 3    | Gi0/3     | -          | 0000.0000.0003 | 2008-01-23 16:25:10 |
| 4    | Gi0/4     | -          | 0000.0000.0004 | 2008-01-23 16:26:10 |

Total : 4 record(s)

3 : 仅查看 vlan 1, G0/1 口, 符合 MAC 为 0000.0000.0001 的扫描用户信息。

```
Ruijie# show nfpp arp-guard scan vlan 1 interface G 0/1 0000.0000.0001
```

| VLAN | interface | IP address | MAC address    | timestamp           |
|------|-----------|------------|----------------|---------------------|
| 1    | Gi0/1     | -          | 0000.0000.0001 | 2008-01-23 16:23:10 |

Total : 1 record(s)

【提示信息】 -

【平台说明】 -

## 18.85 show nfpp arp-guard summary

查看配置信息。

**show nfpp arp-guard summary**

| 【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】 通过该命令可以查看配置信息。

【配置举例】 1 : 查看 ARP 抗攻击的配置信息, 包括全局配置信息以及接口上的配置信息。

```
Ruijie# show nfpp arp-guard summary
```

(Format of column Rate-limit and Attack-threshold is per-src-ip/per-src-mac/per-port. )

| Interface | Status  | Isolate-period | Rate-limit | Attack-threshold | Scan-threshold |
|-----------|---------|----------------|------------|------------------|----------------|
| Global    | Enable  | 300            | 4/5/60     | 8/10/100         | 15             |
| Gi 0/1    | Enable  | 180            | 5/-/-      | 8/-/-            | -              |
| Gi 0/2    | Disable | 200            | 4/5/60     | 8/10/100         | 20             |

Maximum count of monitored hosts: 1000

Monitor period : 300s

字段解释：

| 字段               | 说明                                       |
|------------------|------------------------------------------|
| Interface        | 表示对应接口，Global 表示对应行为全局配置。                |
| Status           | 表示是否打开抗攻击功能。                             |
| Isolat-period    | 表示对应策略配置的隔离周期。                           |
| Rate-limit       | 分别对应源 IP 地址的限速水线/源 MAC 地址的限速水线/端口的限速水线值。 |
| Attack-threshold | 分别对应源 IP 地址的攻击水线/源 MAC 地址的攻击水线/端口的攻击水线值。 |
| Scan-threshold   | 表示扫描水线。                                  |

【提示信息】 -

【平台说明】 -

## 18.86 show nfpp define hosts

查看受监控主机。

**show nfpp define hosts** *name* [**statistics** | [[**vlan** *vid*] [**interface** *interface-id*] [*ip-address*] [*mac-address*] [*ipv6-address*]]]

【参数说明】

| 参数                  | 描述            |
|---------------------|---------------|
| <i>name</i>         | 自定义抗攻击类型名称。   |
| <b>statistics</b>   | 查看受监控主机的统计信息。 |
| <i>vid</i>          | 虚拟局域网号。       |
| <i>interface-id</i> | 端口名称。         |
| <i>ip-address</i>   | IP 地址。        |
| <i>mac-address</i>  | MAC 地址。       |
| <i>ipv6-address</i> | IPv6 地址。      |

【命令模式】 特权模式

【缺省级别】 14

【使用指导】 可以携带参数进行过滤。

【配置举例】 查看自定义抗攻击 tcp 受监控主机，第四列 “remain-time(s)” 是指剩余的隔离时间。

```
Ruijie#show nfpp define hosts abc
```

```
If col_filter 1 shows '*', it means "hardware do not isolate host".
```

| VLAN          | interface | MAC address    | remain-time(s) |
|---------------|-----------|----------------|----------------|
| *1            | Gi4/2     | 00d0.f822.33e5 | 592            |
| Total: 1 host |           |                |                |

【提示信息】 -

【平台说明】 -

## 18.87 show nfpp define summary

查看配置信息。

**show nfpp define summary** [*name*]

【参数说明】

| 参数          | 描述         |
|-------------|------------|
| <i>name</i> | 自定义抗攻击类型名称 |

【命令模式】 特权模式

【缺省级别】 14

【使用指导】 通过该命令可以查看配置信息。不带 name 表示显示所有的自定义抗攻击类型

【配置举例】 1：查看自定义抗攻击 tcp 的配置信息，包括全局配置信息以及接口上的配置信息。

```
Ruijie#show nfpp define summary abc
Define abc summary:
match etype 0x800 src-ip 1.1.1.1 src-ip-mask 255.255.255.255
Maximum count of monitored hosts: 20000
Monitor period:600s
(Format of column Rate-limit and Attack-threshold is per-src-ip/per-src-mac/per-port.)
Interface Status Rate-limit Attack-threshold
Global Disable -/10/- -/20/-
Gi4/1 Enable -/-/ -/-/
```

字段解释：

| 字段               | 说明                                       |
|------------------|------------------------------------------|
| Interface        | 表示对应接口，Global 表示对应行为全局配置。                |
| Status           | 表示是否打开抗攻击功能。                             |
| Rate-limit       | 分别对应源 IP 地址的限速水线/源 MAC 地址的限速水线/端口的限速水线值。 |
| Attack-threshold | 分别对应源 IP 地址的攻击水线/源 MAC 地址的攻击水线/端口的攻击水线值。 |

【提示信息】 -

【平台说明】 -

## 18.88 show nfpp define trusted-host

查看不监控的可信主机

**show nfpp define trusted-host** *name*

| 【参数说明】 | 参数          | 描述         |
|--------|-------------|------------|
|        | <i>name</i> | 自定义抗攻击类型名称 |

【命令模式】 特权模式

【缺省级别】 14

【使用指导】 -

【配置举例】 1：查看自定义抗攻击 tcp 可信主机配置。

```
Ruijie# show nfpp define trusted-host tcp
Define tcp:
IP address mask

1. 1. 1. 0 255. 255. 255. 0
1. 1. 2. 0 255. 255. 255. 0
Total : 2 record(s)
```

【提示信息】 -

【平台说明】 -

## 18.89 show nfpp dhcp-guard hosts

查看受监控主机。

**show nfpp dhcp-guard hosts** [**statistics** | [[**vlan** *vid*] [**interface** *interface-id*] [*mac-address*]]]

| 【参数说明】 | 参数                | 描述            |
|--------|-------------------|---------------|
|        | <b>statistics</b> | 查看受监控主机的统计信息。 |
|        | <i>vid</i>        | 虚拟局域网号。       |

|                     |         |
|---------------------|---------|
| <i>interface-id</i> | 端口名称。   |
| <i>mac-address</i>  | 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 DHCP 抗攻击受监控主机的统计信息。当前有 120 台主机被监控，其中 100 台主机被硬件成功地隔离，20 台主机硬件隔离失败（通常引起的原因有内存不足，或者硬件资源不足）。

```
Ruijie# show nfpp dhcp-guard hosts statistics
```

```
success fail total

100 20 120
```

2：查看 DHCP 抗攻击受监控主机，第四列 “remain-time(s)” 是指剩余的隔离时间。

```
Ruijie# show nfpp dhcp-guard hosts
```

If column 1 shows '\*', it means "hardware failed to isolate host".

```
VLAN interface MAC address remain-time(seconds)
```

```

1 gi0/2 0000.0000.0001 10
*2 gi0/1 0000.0000.0002 20
```

```
Total : 2 host(s)
```

【提示信息】 -

【平台说明】 -

## 18.90 show nfpp dhcp-guard summary

查看配置信息。

**show nfpp dhcp-guard summary**

| 【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】 通过该命令可以查看配置信息。

【配置举例】 1：查看 DHCP 抗攻击的配置信息，包括全局配置信息以及接口上的配置信息。

```
Ruijie# show nfpp dhcp-guard summary
(Format of column Rate-limit and Attack-threshold is per-src-ip/per-src-mac/per-port.)
Interface Status Isolate-period Rate-limit Attack-threshold
Global Enable 300 -/5/150 -/10/300
Gi 0/1 Enable 180 -/6/- -/8/-
Gi 0/2 Disable 200 -/5/30 -/10/50

Maximum count of monitored hosts: 1000
Monitor period : 300s
```

字段解释：

| 字段               | 说明                                       |
|------------------|------------------------------------------|
| Interface        | 表示对应接口，Global 表示对应行为全局配置。                |
| Status           | 表示是否打开抗攻击功能。                             |
| Isolate-period   | 表示对应配置策略的隔离周期。                           |
| Rate-limit       | 分别对应源 IP 地址的限速水线/源 MAC 地址的限速水线/端口的限速水线值。 |
| Attack-threshold | 分别对应源 IP 地址的攻击水线/源 MAC 地址的攻击水线/端口的攻击水线值。 |

【提示信息】 -

【平台说明】 -

## 18.91 show nfpp dhcpv6-guard hosts

查看受监控主机。

**show nfpp dhcpv6-guard hosts** [**statistics** | [[**vlan** *vid*] [**interface** *interface-id*] [*mac-address*]]]

【参数说明】

| 参数                  | 描述           |
|---------------------|--------------|
| <b>statistics</b>   | 查看受监控主机的统计信息 |
| <i>vid</i>          | 虚拟局域网号       |
| <i>interface-id</i> | 端口名称         |
| <i>mac-address</i>  | MAC 地址       |

【命令模式】 特权模式



【缺省级别】 14

【使用指导】 -

【配置举例】 查看 DHCPv6 抗攻击受监控主机，第四列 “remain-time(s)” 是指剩余的隔离时间。

```
Ruijie# show nfpp dhcpv6-guard hosts
If column 1 shows '*', it means "hardware failed to isolate host".
VLAN interface MAC address remain-time(seconds)

*1 gi0/2 0000.0000.0001 10
*2 gi0/1 0000.0000.0002 20
Total : 2 host(s)
```

【提示信息】 -

【平台说明】 -

18.92 show nfpp dhcpv6-guard summary

查看配置信息  
show nfpp dhcpv6-guard summary

| 【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】 通过该命令可以查看配置信息。

【配置举例】 1：查看 DHCPv6 抗攻击的配置信息，包括全局配置信息以及接口上的配置信息。

```
Ruijie#show nfpp dhcpv6-guard summary

(Format of column Rate-limit and Attack-threshold is per-src-ip/per-src-mac/per-port.)
Interface Status Rate-limit Attack-threshold
Global Enable -/5/1200 -/10/1500

Maximum count of monitored hosts: 20000
Monitor period: 600s

字段解释：
```

| 字段               | 说明                                       |
|------------------|------------------------------------------|
| Interface        | 表示对应接口，Global 表示对应行为全局配置。                |
| Status           | 表示是否打开抗攻击功能。                             |
| Rate-limit       | 分别对应源 IP 地址的限速水线/源 MAC 地址的限速水线/端口的限速水线值。 |
| Attack-threshold | 分别对应源 IP 地址的攻击水线/源 MAC 地址的攻击水线/端口的攻击水线值。 |

【提示信息】 -

【平台说明】 -

## 18.93 show nfpp icmp-guard hosts

查看受监控主机。

**show nfpp icmp-guard hosts** [**statistics** | [[**vlan** *vid*] [**interface** *interface-id*] [*ip-address*]]]

【参数说明】

| 参数                  | 描述           |
|---------------------|--------------|
| <b>statistics</b>   | 查看受监控主机的统计信息 |
| <i>vid</i>          | 虚拟局域网号       |
| <i>interface-id</i> | 端口名称         |
| <i>ip-address</i>   | 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：查看 ICMP 抗攻击受监控主机的统计信息。当前有 120 台主机被监控，其中 100 台主机被硬件成功地隔离，20 台主机硬件隔离失败（通常引起的原因有内存不足，或者硬件资源不足）。

```
Ruijie#show nfpp icmp-guard hosts statistics
```

```
success fail total

100 20 120
```

2：查看 ICMP 抗攻击受监控主机，第四列 “remain-time(s)” 是指剩余的隔离时间。

```
Ruijie# show nfpp icmp-guard hosts
```

If column 1 shows '\*', it means "hardware failed to isolate host".

```
VLAN interface IP address remain-time(s)

```

|                   |       |         |     |
|-------------------|-------|---------|-----|
| 1                 | Gi0/1 | 1.1.1.1 | 110 |
| 2                 | Gi0/2 | 1.1.2.1 | 61  |
| Total : 2 host(s) |       |         |     |

【提示信息】 -

【平台说明】 -

18.94 show nfpp icmp-guard summary

查看配置信息。  
**show nfpp icmp-guard summary**

| 【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】 通过该命令可以查看配置信息。

【配置举例】 1：查看 ICMP 抗攻击的配置信息，包括全局配置信息以及接口上的配置信息。

```
Ruijie# show nfpp icmp-guard summary
(Format of column Rate-limit and Attack-threshold is per-src-ip/per-src-mac/per-port.)
Interface Status Isolate-period Rate-limit Attack-threshold
Global Enable 300 4/-/60 8/-/100
Gi 0/1 Enable 180 5/-/- 8/-/-
Gi 0/2 Disable 200 4/-/60 8/-/100
```

```
Maximum count of monitored hosts: 1000
Monitor period : 300s
```

字段解释：

| 字段               | 说明                                       |
|------------------|------------------------------------------|
| Interface        | 表示对应接口，Global 表示对应行为全局配置。                |
| Status           | 表示是否打开抗攻击功能。                             |
| Isolate-period   | 表示对应配置策略的隔离周期。                           |
| Rate-limit       | 分别对应源 IP 地址的限速水线/源 MAC 地址的限速水线/端口的限速水线值。 |
| Attack-threshold | 分别对应源 IP 地址的攻击水线/源 MAC 地址的攻击             |

|  |              |
|--|--------------|
|  | 水线/端口的攻击水线值。 |
|--|--------------|

【提示信息】 -

【平台说明】 -

## 18.95 show nfpp icmp-guard trusted-host

查看不监控的可信主机。

**show nfpp icmp-guard trusted-host**

| 【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 ICMP 抗攻击可信主机配置。

```
Ruijie# show nfpp icmp-guard trusted-host
IP address mask

1. 1. 1. 0 255. 255. 255. 0
1. 1. 2. 0 255. 255. 255. 0
Total : 2 record(s)
```

【提示信息】 -

【平台说明】 -

## 18.96 show nfpp ip-guard hosts

查看受监控主机。

**show nfpp ip-guard hosts** [**statistics** | **[[vlan vid] [interface interface-id] [ip-address]]**]

| 【参数说明】 | 参数                | 描述           |
|--------|-------------------|--------------|
|        | <b>statistics</b> | 查看受监控主机的统计信息 |
|        | <i>vid</i>        | 虚拟局域网号       |

|                     |       |
|---------------------|-------|
| <i>interface-id</i> | 端口名称  |
| <i>ip-address</i>   | 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：查看 IP 抗攻击受监控主机的统计信息。当前有 120 台主机被监控，其中 100 台主机被硬件成功地隔离，20 台主机硬件隔离失败（通常引起的原因有内存不足，或者硬件资源不足）。

```
Ruijie#show nfpp ip-guard hosts statistics
```

```
success fail total
```

```

100 20 120
```

2：查看 IP 抗攻击受监控主机，第四列 “remain-time(s)” 是指剩余的隔离时间。

```
Ruijie#show nfpp ip-guard hosts
```

If column 1 shows '\*', it means "hardware do not isolate host".

```
VLAN interface IP address Reason remain-time(s)
```

```

1 Gi0/1 1.1.1.1 ATTACK 110
2 Gi0/2 1.1.2.1 SCAN 61
```

```
Total : 2 host(s)
```

第四个字段 “Reason” 描述主机被监控的原因，“ATTACK” 表示主机发送 IP 报文的速度超过攻击水线，“SCAN” 表示主机在扫描某个网段。

【提示信息】 -

【平台说明】 -

## 18.97 show nfpp ip-guard summary

查看配置信息

**show nfpp ip-guard summary**

| 【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】 通过该命令可以查看配置信息。

【配置举例】 1：查看 IP 抗攻击的配置信息，包括全局配置信息以及接口上的配置信息。

```
Ruijie# show nfpp ip-guard summary
(Format of column Rate-limit and Attack-threshold is per-src-ip/per-src-mac/per-port.)
Interface Status Isolate-period Rate-limit Attack-threshold Scan-threshold
Global Enable 300 4-/60 8-/100 15
Gi 0/1 Enable 180 5/-/- 8/-/- -
Gi 0/2 Disable 200 4-/60 8-/100 20

Maximum count of monitored hosts: 1000
Monitor period : 300s
```

字段解释：

| 字段               | 说明                                       |
|------------------|------------------------------------------|
| Interface        | 表示对应接口，Global 表示对应行为全局配置。                |
| Status           | 表示是否打开抗攻击功能。                             |
| Isolate-period   | 表示对应配置策略的隔离周期。                           |
| Rate-limit       | 分别对应源 IP 地址的限速水线/源 MAC 地址的限速水线/端口的限速水线值。 |
| Attack-threshold | 分别对应源 IP 地址的攻击水线/源 MAC 地址的攻击水线/端口的攻击水线值。 |
| Scan-threshold   | 表示扫描水线。                                  |

【提示信息】 -

【平台说明】 -

## 18.98 show nfpp ip-guard trusted-host

查看不监控的可信主机。

**show nfpp ip-guard trusted-host**

| 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 IP 抗攻击可信主机配置。

```
Ruijie# show nfpp ip-guard trusted-host
IP address mask

1.1.1.0 255.255.255.0
1.1.2.0 255.255.255.0
Total : 2 record(s)
```

【提示信息】 -

【平台说明】 -

## 18.99 show nfpp log

显示 NFPP 日志配置。

**show nfpp log summary**

显示 NFPP 日志缓冲区内容。

**show nfpp log buffer [statistics]**

| 【参数说明】 | 参数                | 描述                 |
|--------|-------------------|--------------------|
|        | <b>statistics</b> | 显示 NFPP 日志缓冲区的统计信息 |

【命令模式】 特权模式

【缺省级别】 14

【使用指导】 当日志缓冲区溢出时，后续的日志将被丢弃，同时在日志缓冲区中显示一条所有属性都为“-”的表项。管理员需要增加日志缓冲区容量或者提高生成系统消息的速率。

从日志缓冲区取日志生成的系统消息带有事件发生的时间戳，如下所示：

```
%NFPP_ARP_GUARD-4-DOS_DETECTED: Host<IP=N/A,MAC=0000.0000.0004,port=Gi4/1,VLAN=1> was
detected.(2009-07-01 13:00:00)
```

【配置举例】 1：查看 NFPP 日志信息配置。

```
Ruijie#show nfpp log summary
Total log buffer size : 10
Syslog rate : 1 entry per 2 seconds
Logging:
```

```
VLAN 1-3, 5
interface Gi 0/1
interface Gi 0/2
```

## 2：查看 NFPP 日志缓冲区中日志条数。

```
Ruijie#show nfpp log buffer statistics
There are 6 logs in buffer.
```

## 3：查看 NFPP 的日志缓冲区。

```
Ruijie#show nfpp log buffer
```

| Protocol | VLAN | Interface | IP address | MAC address    | Reason         | Timestamp           |
|----------|------|-----------|------------|----------------|----------------|---------------------|
| ARP      | 1    | Gi0/1     | 1.1.1.1    | -              | DoS            | 2009-05-30 16:23:10 |
| ARP      | 1    | Gi0/1     | 1.1.1.1    | -              | ISOLATED       | 2009-05-30 16:23:10 |
| ARP      | 1    | Gi0/1     | 1.1.1.2    | -              | DoS            | 2009-05-30 16:23:15 |
| ARP      | 1    | Gi0/1     | 1.1.1.2    | -              | ISOLATE_FAILED | 2009-05-30 16:23:15 |
| ARP      | 1    | Gi0/1     | -          | 0000.0000.0001 | SCAN           | 2009-05-30 16:30:10 |
| ARP      | -    | Gi0/2     | -          | -              | PORT_ATTACKED  | 2009-05-30 16:30:10 |

Protocol 有以下取值：

| Protocol    | 说明                      |
|-------------|-------------------------|
| ARP         | 对应 ARP 抗攻击。             |
| IP          | 对应 IP 防扫描。              |
| ICMP        | 对应 ICMP 抗攻击。            |
| DHCP        | 对应 DHCP 抗攻击。            |
| DHCPv6      | 对应 DHCPv6 抗攻击。          |
| NS-NA       | 对应 ND 抗攻击中的邻居请求和邻居公告。   |
| RS          | 对应 ND 抗攻击中的路由器请求。       |
| RA-REDIRECT | 对应 ND 抗攻击中的路由器公告和重定向报文。 |

Reason 表示原因，有 5 种取值：

| Reason         | 说明            |
|----------------|---------------|
| DoS            | 表示检测到拒绝服务攻击   |
| ISOLATED       | 表示攻击者被硬件成功地隔离 |
| ISOLATE_FAILED | 表示隔离攻击者失败     |
| SCAN           | 表示检测到扫描       |
| PORT_ATTACKED  | 表示端口被攻击       |

【提示信息】 -

【平台说明】 -



## 18.100 show nfpp nd-guard summary

查看配置信息。

**show nfpp nd-guard summary**

【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】

通过该命令可以查看配置信息。

【配置举例】

1：查看 ND 抗攻击的配置信息，包括全局配置信息以及接口上的配置信息。

```
Ruijie# show nfpp nd-guard summary
(Format of column Rate-limit and Attack-threshold is NS-NA/RS/RA-REDIRECT.)
Interface Status Rate-limit Attack-threshold
Global Enable 20/5/10 40/10/20
Gi 0/1 Enable 15/15/15 30/30/30
Gi 0/2 Disable -/5/30 -/10/50
```

字段解释：

| 字段               | 说明                                       |
|------------------|------------------------------------------|
| Interface        | 表示对应接口，Global 表示对应行为全局配置。                |
| Status           | 表示是否打开抗攻击功能。                             |
| Rate-limit       | 分别对应源 IP 地址的限速水线/源 MAC 地址的限速水线/端口的限速水线值。 |
| Attack-threshold | 分别对应源 IP 地址的攻击水线/源 MAC 地址的攻击水线/端口的攻击水线值。 |

【提示信息】

-

【平台说明】

-

## 18.101 show nfpp nd-guard hosts

查看受监控主机。

**show nfpp nd-guard hosts [statistics | [[vlan vid] [interface interface-id]]]**

【参数说明】

| 参数 | 描述 |
|----|----|
|----|----|

|                     |              |
|---------------------|--------------|
| <b>statistics</b>   | 查看受监控主机的统计信息 |
| <i>vid</i>          | 虚拟局域网号       |
| <i>interface-id</i> | 端口名称         |

【命令模式】 特权模式

【缺省级别】 14

【使用指导】 -

【配置举例】 1：查看 ND 抗攻击受监控主机的统计信息。当前有 12 个端口被监控，其中 10 台主机被硬件成功地限速，2 台主机硬件限速失败（通常引起的原因有内存不足，或者硬件资源不足）。

```
Ruijie#show nfpp nd-guard hosts statistics
```

```
success fail total
```

```

```

```
10 2 12
```

2：查看 ND 抗攻击受监控主机，第四列 “remain-time(s)” 是指剩余的隔离时间。

```
Ruijie#show nfpp nd-guard hosts
```

If col\_filter 1 shows '\*', it means "hardware do not isolate host".

```
VLAN interface ND-guard remain-time(s)
```

```

```

```
- Gi4/2 ns-na-guard 174
```

```
- Gi4/2 rs-guard 98
```

```
- Gi4/2 ra-redirect-guard 127
```

```
Total: 3 hosts
```

【提示信息】 -

【平台说明】 -

## 18.102 trusted-host

配置不监控的可信主机。

**trusted-host** {*mac mac\_mask* | *ip mask* | *IPv6/prefixlen*}

删除不监控可信主机。

**no trusted-host** {**all** | *mac mac\_mask* | *ip mask* | *IPv6/prefixlen*}

清除不监控可信主机。

**default trusted-host**

| 【参数说明】 | 参数                    | 描述                           |
|--------|-----------------------|------------------------------|
|        | <i>mac</i>            | mac 地址。                      |
|        | <i>mac_mask</i>       | mac 地址的掩码。                   |
|        | <i>ip</i>             | IP 地址。                       |
|        | <i>mask</i>           | IP 地址的掩码。                    |
|        | <i>IPv6/prefixlen</i> | IPv6 地址和掩码长度。                |
|        | <b>all</b>            | 和 <b>no</b> 一起使用，删除所有可信主机配置。 |

【缺省配置】 缺省没有设置任何可信主机。

【命令模式】 NFPP 自定义类型配置模式

【缺省级别】 14

【使用指导】 如果管理员希望对某台主机不进行监控，即对该主机表示信任，则可以通过该命令配置。该可信主机发往 CPU 的 ICMP 报文将被允许发往 CPU，不做任何的限速和告警处理。通过配置掩码可以达到对某一个网段的所有主机都不进行监控。

最多支持设置 500 条可信主机。

必须先配置 match 类型后后才能配置 trusted-host。若 match 配置的报文类型为 IPv4，则不允许配置 IPv6 信任地址；同理若 match 配置的报文类型为 IPv6，则不允许配置 IPv4 信任地址。

【配置举例】 1：把主机 1.1.1.1 配置为自定义抗攻击 tcp 的可信主机。

```
Ruijie(config)# nfpp
Ruijie(config-nfpp)# define tcp
Ruijie(config-nfpp-define)#trusted-host 1.1.1.1 255.255.255.255
```

【检验方法】 使用 **show nfpp define trusted-host name** 查看配置信息。

【提示信息】 -

【常见错误】 -

## 19 DOS 保护

| 命令                                          | 作用                |
|---------------------------------------------|-------------------|
| <a href="#">ip deny invalid-l4port</a>      | 开启防自身消耗攻击功能。      |
| <a href="#">ip deny invalid-tcp</a>         | 开启防非法 TCP 报文攻击功能。 |
| <a href="#">ip deny land</a>                | 开启防 Land 攻击功能。    |
| <a href="#">show ip deny</a>                | 显示所有防 DOS 攻击的状态   |
| <a href="#">show ip deny invalid-l4port</a> | 显示防自身消耗攻击的状态。     |
| <a href="#">show ip deny invalid-tcp</a>    | 显示防非法 TCP 报文攻击的状态 |
| <a href="#">show ip deny land</a>           | 显示防 Land 攻击的状态    |

### 19.1 ip deny invalid-l4port

开启防自身消耗攻击功能。

**ip deny invalid-l4port**

关闭防自身消耗攻击功能。

**no ip deny invalid-l4port**

#### 【参数说明】

| 参数 | 描述 |
|----|----|
| -  | -  |

【缺省配置】 缺省情况下，设备的防自身消耗攻击功能是关闭的。

【命令模式】 全局模式

【缺省级别】 14

【使用指导】 -

【配置举例】 1：在设备上开启防自身消耗攻击功能。

```
Ruijie(config)# ip deny invalid-l4port
```

2：在设备上关闭防自身消耗攻击功能。

```
Ruijie(config)# no ip deny invalid-l4port
```

【检验方法】 使用 **show ip deny invalid-l4port** 命令，可以查看防自身消耗攻击是启用还是关闭。

【提示信息】 -

【常见错误】 -

【平台说明】 -

## 19.2 ip deny invalid-tcp

开启防非法 TCP 报文攻击功能。

**ip deny invalid-tcp**

关闭防非法 TCP 报文攻击功能。

**no ip deny invalid-tcp**

【参数说明】

| 参数 | 描述 |
|----|----|
| -  | -  |

【缺省配置】 缺省情况下，设备的防非法 TCP 报文攻击功能是关闭的。

【命令模式】 全局模式

【缺省级别】 14

【使用指导】 -

【配置举例】 1：在设备上开启防非法 TCP 报文攻击功能。

```
Ruijie(config)# ip deny invalid-tcp
```

2：在设备上关闭防非法 TCP 报文攻击功能。

```
Ruijie(config)# no ip deny invalid-tcp
```

【检验方法】 使用 **show ip deny invalid-tcp** 命令，可以查看防非法 TCP 报文攻击是启用还是关闭。

【提示信息】 -

【常见错误】 -

【平台说明】 -

## 19.3 ip deny land

开启防 Land 攻击功能。

**ip deny land**

关闭防 Land 攻击功能。

**no ip deny land**

| 【参数说明】 | 参数                                                   | 描述 |
|--------|------------------------------------------------------|----|
|        | -                                                    | -  |
| 【缺省配置】 | 缺省情况下，设备的防 Land 攻击功能是关闭的。                            |    |
| 【命令模式】 | 全局模式                                                 |    |
| 【缺省级别】 | 14                                                   |    |
| 【使用指导】 | -                                                    |    |
| 【配置举例】 | 1：在设备上开启防 Land 攻击功能。                                 |    |
|        | Ruijie(config)# ip deny land                         |    |
|        | 2：在设备上关闭防 Land 攻击功能。                                 |    |
|        | Ruijie(config)# no ip deny land                      |    |
| 【检验方法】 | 使用 <b>show ip deny land</b> 命令，可以查看防 Land 攻击是启用还是关闭。 |    |
| 【提示信息】 | -                                                    |    |
| 【常见错误】 | -                                                    |    |
| 【平台说明】 | -                                                    |    |

19.4 show ip deny

显示所有防 DOS 攻击的状态。

**show ip deny**

| 【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：查看所有防 DOS 攻击的状态。

```
ruijie#show ip deny
Protect against Land attack On
Protect against invalid L4port attack Off
Protect against invalid TCP attack Off
```

【提示信息】 -

【平台说明】 -

## 19.5 show ip deny invalid-l4port

显示防自身消耗攻击的状态。

**show ip deny invalid-l4port**

【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：查看防自身消耗攻击的状态。

```
Ruijie# show ip deny invalid-l4port
DoS Protection Mode State

protect against invalid l4port attack Off
```

【提示信息】 -

【平台说明】 -

## 19.6 show ip deny invalid-tcp

显示防非法 TCP 报文攻击的状态。

**show ip deny invalid-tcp**

【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：查看防非法 TCP 报文攻击的状态。

```
Ruijie# show ip deny invalid-tcp
```

| DoS Protection Mode | State |
|---------------------|-------|
|---------------------|-------|

|       |       |
|-------|-------|
| ----- | ----- |
|-------|-------|

|                                    |    |
|------------------------------------|----|
| protect against invalid tcp attack | On |
|------------------------------------|----|

【提示信息】 -

【平台说明】 -

## 19.7 show ip deny land

显示防 Land 攻击的状态。

**show ip deny land**

【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：查看防 Land 攻击的状态。



```
Ruijie# show ip deny land
```

| DoS Protection Mode | State |
|---------------------|-------|
|---------------------|-------|

|       |       |
|-------|-------|
| ----- | ----- |
|-------|-------|

|                             |    |
|-----------------------------|----|
| protect against land attack | On |
|-----------------------------|----|

【提示信息】 -

【平台说明】 -