

H3C S5130S-SI[LI]&S5120V2-SI[LI]&S5110V2-SI& S5000V3-EI&S5000E-X&S3100V3-SI 系列以太网交换机

安全命令参考

新华三技术有限公司
<http://www.h3c.com>

资料版本：6W103-20190822
产品版本：Release 612x 系列

Copyright © 2019 新华三技术有限公司及其许可者 版权所有，保留一切权利。

未经本公司书面许可，任何单位和个人不得擅自摘抄、复制本书内容的部分或全部，并不得以任何形式传播。

除新华三技术有限公司的商标外，本手册中出现的其它公司的商标、产品标识及商品名称，由各自权利人拥有。

前言

本命令参考主要介绍各种安全业务特性的配置命令，包括 AAA、PKI 等身份认证特性配置命令，802.1X、MAC 地址认证、Portal、端口安全等接入安全特性配置命令，公钥管理、IPsec、SSH、SSL 等数据安全特性配置命令，以及 IP Source Guard、ARP 攻击防御、MFF 等安全防御特性配置命令。

前言部分包含如下内容：

- [读者对象](#)
- [本书约定](#)
- [资料意见反馈](#)

读者对象

本手册主要适用于如下工程师：

- 网络规划人员
- 现场技术支持与维护人员
- 负责网络配置和维护的网络管理员

本书约定

1. 命令行格式约定

格 式	意 义
粗体	命令行关键字（命令中保持不变、必须照输的部分）采用 加粗 字体表示。
<i>斜体</i>	命令行参数（命令中必须由实际值进行替代的部分）采用 <i>斜体</i> 表示。
[]	表示用“[]”括起来的部分在命令配置时是可选的。
{ x y ... }	表示从多个选项中仅选取一个。
[x y ...]	表示从多个选项选取一个或者不选。
{ x y ... } *	表示从多个选项中至少选取一个。
[x y ...] *	表示从多个选项选取一个、多个或者不选。
&<1-n>	表示符号&前面的参数可以重复输入1~n次。
#	由“#”号开始的行表示为注释行。






2. 图形界面格式约定

格 式	意 义
< >	带尖括号“< >”表示按钮名，如“单击<确定>按钮”。
[]	带方括号“[]”表示窗口名、菜单名和数据表，如“弹出[新建用户]窗口”。

格 式	意 义
/	多级菜单用“/”隔开。如[文件/新建/文件夹]多级菜单表示[文件]菜单下的[新建]子菜单下的[文件夹]菜单项。

3. 各类标志

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

 警告	该标志后的注释需给予格外关注，不当的操作可能会对人身造成伤害。
 注意	提醒操作中应注意的事项，不当的操作可能会导致数据丢失或者设备损坏。
 提示	为确保设备配置成功或者正常工作而需要特别关注的操作或信息。
 说明	对操作内容的描述进行必要的补充和说明。
 窍门	配置、操作、或使用设备的技巧、小窍门。

4. 图标约定

本书使用的图标及其含义如下：

	该图标及其相关描述文字代表一般网络设备，如路由器、交换机、防火墙等。
	该图标及其相关描述文字代表一般意义下的路由器，以及其他运行了路由协议的设备。
	该图标及其相关描述文字代表二、三层以太网交换机，以及运行了二层协议的设备。
	该图标及其相关描述文字代表无线控制器、无线控制器业务板和有线无线一体化交换机的无线控制引擎设备。
	该图标及其相关描述文字代表无线接入点设备。
	该图标及其相关描述文字代表无线终结单元。
	该图标及其相关描述文字代表无线终结者。
	该图标及其相关描述文字代表无线Mesh设备。
	该图标代表发散的无线射频信号。
	该图标代表点到点的无线射频信号。
	该图标及其相关描述文字代表防火墙、UTM、多业务安全网关、负载均衡等安全设备。



该图标及其相关描述文字代表防火墙插卡、负载均衡插卡、NetStream插卡、SSL VPN插卡、IPS插卡、ACG插卡等安全插卡。

5. 示例约定

由于设备型号不同、配置不同、版本升级等原因，可能造成本手册中的内容与用户使用的设备显示信息不一致。实际使用中请以设备显示的内容为准。

本手册中出现的端口编号仅作参考，并不代表设备上实际具有此编号的端口，实际使用中请以设备上存在的端口编号为准。

资料意见反馈

如果您在使用过程中发现产品资料的任何问题，可以通过以下方式反馈：

E-mail: info@h3c.com

感谢您的反馈，让我们做得更好！

目 录

1 AAA.....	1-1
1.1 ISP域中实现AAA配置命令.....	1-1
1.1.1 aaa nas-id profile.....	1-1
1.1.2 aaa session-limit.....	1-2
1.1.3 accounting command	1-3
1.1.4 accounting default.....	1-3
1.1.5 accounting lan-access	1-5
1.1.6 accounting login	1-6
1.1.7 accounting portal	1-8
1.1.8 accounting quota-out.....	1-9
1.1.9 accounting start-fail.....	1-10
1.1.10 accounting update-fail.....	1-10
1.1.11 authentication default.....	1-11
1.1.12 authentication lan-access	1-12
1.1.13 authentication login	1-14
1.1.14 authentication portal	1-15
1.1.15 authentication super	1-16
1.1.16 authorization command	1-17
1.1.17 authorization default	1-18
1.1.18 authorization lan-access.....	1-20
1.1.19 authorization login.....	1-21
1.1.20 authorization portal.....	1-22
1.1.21 authorization-attribute (ISP domain view)	1-23
1.1.22 display domain	1-25
1.1.23 domain	1-29
1.1.24 domain default enable.....	1-30
1.1.25 domain if-unknown	1-30
1.1.26 nas-id bind vlan	1-31
1.1.27 session-time include-idle-time.....	1-32
1.1.28 state (ISP domain view).....	1-33
1.2 本地用户配置命令.....	1-34
1.2.1 access-limit	1-34
1.2.2 authorization-attribute (Local user view/user group view).....	1-34

1.2.3 bind-attribute	1-37
1.2.4 description	1-38
1.2.5 display local-user	1-39
1.2.6 display user-group	1-42
1.2.7 group	1-43
1.2.8 local-user	1-44
1.2.9 local-user auto-delete enable	1-45
1.2.10 password (Device management user view)	1-46
1.2.11 password (Network access user view)	1-47
1.2.12 service-type	1-48
1.2.13 state (Local user view)	1-49
1.2.14 user-group	1-49
1.2.15 validity-datetime	1-50
1.3 RADIUS配置命令	1-51
1.3.1 aaa device-id	1-51
1.3.2 accounting-on enable	1-52
1.3.3 accounting-on extended	1-53
1.3.4 attribute 15 check-mode	1-54
1.3.5 attribute 25 car	1-55
1.3.6 attribute 31 mac-format	1-55
1.3.7 attribute convert (RADIUS DAE server view)	1-56
1.3.8 attribute convert (RADIUS scheme view)	1-57
1.3.9 attribute reject (RADIUS DAE server view)	1-58
1.3.10 attribute reject (RADIUS scheme view)	1-59
1.3.11 attribute remanent-volume	1-61
1.3.12 attribute translate	1-61
1.3.13 client	1-62
1.3.14 data-flow-format (RADIUS scheme view)	1-63
1.3.15 display radius scheme	1-64
1.3.16 display radius statistics	1-67
1.3.17 display stop-accounting-buffer (for RADIUS)	1-69
1.3.18 key (RADIUS scheme view)	1-70
1.3.19 nas-ip (RADIUS scheme view)	1-71
1.3.20 port	1-72
1.3.21 primary accounting (RADIUS scheme view)	1-73
1.3.22 primary authentication (RADIUS scheme view)	1-74

1.3.23 radius attribute extended	1-76
1.3.24 radius dscp	1-77
1.3.25 radius dynamic-author server	1-78
1.3.26 radius nas-ip	1-78
1.3.27 radius scheme	1-79
1.3.28 radius session-control client	1-80
1.3.29 radius session-control enable	1-81
1.3.30 radius-server test-profile	1-82
1.3.31 reset radius statistics	1-83
1.3.32 reset stop-accounting-buffer (for RADIUS)	1-83
1.3.33 retry	1-84
1.3.34 retry realtime-accounting	1-85
1.3.35 retry stop-accounting (RADIUS scheme view)	1-86
1.3.36 secondary accounting (RADIUS scheme view)	1-87
1.3.37 secondary authentication (RADIUS scheme view)	1-89
1.3.38 server-load-sharing enable	1-90
1.3.39 snmp-agent trap enable radius	1-91
1.3.40 state primary	1-92
1.3.41 state secondary	1-94
1.3.42 stop-accounting-buffer enable (RADIUS scheme view)	1-95
1.3.43 stop-accounting-packet send-force	1-96
1.3.44 timer quiet (RADIUS scheme view)	1-96
1.3.45 timer realtime-accounting (RADIUS scheme view)	1-97
1.3.46 timer response-timeout (RADIUS scheme view)	1-98
1.3.47 user-name-format (RADIUS scheme view)	1-99
1.4 HWTACACS配置命令	1-100
1.4.1 data-flow-format (HWTACACS scheme view)	1-100
1.4.2 display hwtacacs scheme	1-101
1.4.3 display stop-accounting-buffer (for HWTACACS)	1-106
1.4.4 hwtacacs nas-ip	1-107
1.4.5 hwtacacs scheme	1-108
1.4.6 key (HWTACACS scheme view)	1-109
1.4.7 nas-ip (HWTACACS scheme view)	1-110
1.4.8 primary accounting (HWTACACS scheme view)	1-111
1.4.9 primary authentication (HWTACACS scheme view)	1-112
1.4.10 primary authorization	1-113

1.4.11 reset hwtacacs statistics	1-114
1.4.12 reset stop-accounting-buffer (for HWTACACS)	1-115
1.4.13 retry stop-accounting (HWTACACS scheme view)	1-116
1.4.14 secondary accounting (HWTACACS scheme view)	1-116
1.4.15 secondary authentication (HWTACACS scheme view)	1-118
1.4.16 secondary authorization	1-119
1.4.17 stop-accounting-buffer enable (HWTACACS scheme view)	1-120
1.4.18 timer quiet (HWTACACS scheme view)	1-121
1.4.19 timer realtime-accounting (HWTACACS scheme view)	1-122
1.4.20 timer response-timeout (HWTACACS scheme view)	1-123
1.4.21 user-name-format (HWTACACS scheme view)	1-123
1.5 LDAP配置命令	1-124
1.5.1 attribute-map	1-124
1.5.2 authentication-server	1-125
1.5.3 authorization-server	1-126
1.5.4 display ldap scheme	1-127
1.5.5 ip	1-129
1.5.6 ipv6	1-129
1.5.7 ldap attribute-map	1-130
1.5.8 ldap scheme	1-131
1.5.9 ldap server	1-132
1.5.10 login-dn	1-132
1.5.11 login-password	1-133
1.5.12 map	1-134
1.5.13 protocol-version	1-135
1.5.14 search-base-dn	1-136
1.5.15 search-scope	1-136
1.5.16 server-timeout	1-137
1.5.17 user-parameters	1-138
1.6 RADIUS服务器配置命令	1-139
1.6.1 display radius-server active-client	1-139
1.6.2 display radius-server active-user	1-139
1.6.3 radius-server activate	1-141
1.6.4 radius-server client	1-141
1.7 连接记录策略配置命令	1-142
1.7.1 aaa connection-recording policy	1-142

1.7.2 accounting hwtacacs-scheme.....	1-143
1.7.3 display aaa connection-recording policy.....	1-144

1 AAA



说明

设备运行于 FIPS 模式时，本特性部分配置相对于非 FIPS 模式有所变化，具体差异请见本文相关描述。有关 FIPS 模式的详细介绍请参见“安全配置指导”中的“FIPS”。

1.1 ISP域中实现AAA配置命令

1.1.1 aaa nas-id profile

aaa nas-id profile 命令用来创建 NAS-ID Profile，并进入 NAS-ID-Profile 视图。如果指定的 NAS-ID Profile 已经存在，则直接进入 NAS-ID-Profile 视图。

undo aaa nas-id profile 命令用来删除指定的 NAS-ID Profile。

【命令】

```
aaa nas-id profile profile-name  
undo aaa nas-id profile profile-name
```

【缺省情况】

不存在 NAS-ID Profile。

【视图】

系统视图

【缺省用户角色】

network-admin

【参数】

profile-name：Profile 名称，为 1~31 个字符的字符串，不区分大小写。

【使用指导】

在某些应用环境中，网络运营商需要使用接入设备发送给 RADIUS 服务器的 NAS-Identifier 属性值来获知用户的接入位置，而用户的接入 VLAN 可标识用户的接入位置，因此接入设备上可通过建立用户接入 VLAN 与指定的 NAS-ID 之间的绑定关系来实现接入位置信息的映射。NAS-ID Profile 用于保存 NAS-ID 和 VLAN 的绑定关系。这样，当用户上线时，设备会将与用户接入 VLAN 匹配的 NAS-ID 填充在 RADIUS 请求报文中的 NAS-Identifier 属性中发送给 RADIUS 服务器。

若以上配置都不存在，则使用设备的名称作为 NAS-ID。

【举例】

创建一个名称为 aaa 的 NAS-ID Profile，并进入 NAS-ID-Profile 视图。

```
<Sysname> system-view  
[Sysname] aaa nas-id profile aaa
```

[Sysname-nas-id-prof-aaa]

【相关命令】

- **nas-id bind vlan**
- **port-security nas-id-profile**（安全命令参考/端口安全）
- **portal nas-id-profile**（安全命令参考/Portal）

1.1.2 aaa session-limit

aaa session-limit 命令用来配置同时在线的最大用户连接数，即采用指定登录方式登录设备并同时在线的用户数。

undo aaa session-limit 命令用来将指定登录方式的同时在线的最大用户连接数恢复为缺省情况。

【命令】

非 FIPS 模式下：

```
aaa session-limit { ftp | http | https | ssh | telnet } max-sessions  
undo aaa session-limit { ftp | http | https | ssh | telnet }
```

FIPS 模式下：

```
aaa session-limit { https | ssh } max-sessions  
undo aaa session-limit { https | ssh }
```

【缺省情况】

同时在线的各类型最大用户连接数均为 32。

【视图】

系统视图

【缺省用户角色】

network-admin

【参数】

ftp：表示 FTP 用户。

http：表示 HTTP 用户。

https：表示 HTTPS 用户。

ssh：表示 SSH 用户。

telnet：表示 Telnet 用户。

max-sessions：允许同时在线的最大用户连接数，FTP/SSH/Telnet 用户的取值范围为 1~32，HTTP/HTTPS 用户的取值范围为 1~64。

【使用指导】

配置本命令后，当指定类型的接入用户的用户数超过当前配置的最大连接数后，新的接入请求将被拒绝。

【举例】

设置同时在线的最大 FTP 用户连接数为 4。

```
<Sysname> system-view
[Sysname] aaa session-limit ftp 4
```

1.1.3 accounting command

accounting command 命令用来配置命令行计费方法。

undo accounting command 命令用来恢复缺省情况。

【命令】

```
accounting command hwtacacs-scheme hwtacacs-scheme-name
undo accounting command
```

【缺省情况】

命令行计费采用当前 ISP 域的缺省计费方法。

【视图】

ISP 域视图

【缺省用户角色】

network-admin

【参数】

hwtacacs-scheme *hwtacacs-scheme-name* : 指定 HWTACACS 方案。其中，*hwtacacs-scheme-name* 表示 HWTACACS 方案名，为 1~32 个字符的字符串，不区分大小写。

【使用指导】

命令行计费过程是指，用户执行过的合法命令会被发送给计费服务器进行记录。若未开启命令行授权功能，则计费服务器对用户执行过的所有合法命令进行记录；若开启了命令行授权功能，则计费服务器仅对授权通过的命令进行记录。

目前，仅支持使用远程 HWTACACS 服务器完成命令行计费功能。

【举例】

在 ISP 域 test 下，配置使用 HWTACACS 计费方案 hwtac 进行命令行计费。

```
<Sysname> system-view
[Sysname] domain test
[Sysname-isp-test] accounting command hwtacacs-scheme hwtac
```

【相关命令】

- **accounting default**
- **command accounting**（基础命令参考/登录设备）
- **hwtacacs scheme**

1.1.4 accounting default

accounting default 命令用来为当前 ISP 域配置缺省的计费方法。

undo accounting default 命令用来恢复缺省情况。

【命令】

非 FIPS 模式下:

```
accounting default { hwtacacs-scheme hwtacacs-scheme-name [ radius-scheme  
radius-scheme-name ] [ local ] [ none ] | local [ none ] | none | radius-scheme  
radius-scheme-name [ hwtacacs-scheme hwtacacs-scheme-name ] [ local ]  
[ none ] }  
undo accounting default
```

FIPS 模式下:

```
accounting default { hwtacacs-scheme hwtacacs-scheme-name [ radius-scheme  
radius-scheme-name ] [ local ] | local | radius-scheme radius-scheme-name  
[ hwtacacs-scheme hwtacacs-scheme-name ] [ local ] }  
undo accounting default
```

【缺省情况】

当前 ISP 域的缺省计费方法为 **local**。

【视图】

ISP 域视图

【缺省用户角色】

network-admin

【参数】

hwtacacs-scheme *hwtacacs-scheme-name* : 指定 HWTACACS 方案。其中，*hwtacacs-scheme-name* 表示 HWTACACS 方案名，为 1~32 个字符的字符串，不区分大小写。

local: 本地计费。

none: 不计费。

radius-scheme *radius-scheme-name*: 指定 RADIUS 方案。其中，*radius-scheme-name* 表示 RADIUS 方案名，为 1~32 个字符的字符串，不区分大小写。

【使用指导】

当前 ISP 域的缺省计费方法对于该域中未指定具体计费方法的所有接入用户都起作用，但是如果某类型的用户不支持指定的计费方法，则该计费方法对于这类用户不能生效。

本地计费只是为了支持本地用户的连接数管理，没有实际的计费相关的统计功能。

可以指定多个备选的计费方法，在当前的计费方法无效时按照配置顺序尝试使用备选的方法完成计费。例如，**radius-scheme radius-scheme-name local none** 表示，先进行 RADIUS 计费，若 RADIUS 计费无效则进行本地计费，若本地计费也无效则不进行计费。

【举例】

在 ISP 域 **test** 下，配置缺省计费方法为使用 RADIUS 方案 **rd** 进行计费，并且使用 **local** 作为备选计费方法。

```
<Sysname> system-view  
[Sysname] domain test  
[Sysname-isp-test] accounting default radius-scheme rd local
```

【相关命令】

- `hwtacacs scheme`
- `local-user`
- `radius scheme`

1.1.5 accounting lan-access

`accounting lan-access` 命令用来为 lan-access 用户配置计费方法。

`undo accounting lan-access` 命令用来恢复缺省情况。

【命令】

非 FIPS 模式下:

```
accounting lan-access { broadcast radius-scheme radius-scheme-name1  
radius-scheme radius-scheme-name2 [ local ] [ none ] | local [ none ] | none  
| radius-scheme radius-scheme-name [ local ] [ none ] }
```

`undo accounting lan-access`

FIPS 模式下:

```
accounting lan-access { broadcast radius-scheme radius-scheme-name1  
radius-scheme radius-scheme-name2 [ local ] | local | radius-scheme  
radius-scheme-name [ local ] }
```

`undo accounting lan-access`

【缺省情况】

lan-access 用户采用当前 ISP 域的缺省计费方法。

【视图】

ISP 域视图

【缺省用户角色】

network-admin

【参数】

broadcast: 指定广播 RADIUS 方案，即同时向指定的两个 RADIUS 方案中的计费服务器发送计费请求。

radius-scheme radius-scheme-name1: 表示主送计费 RADIUS 方案名，为 1~32 个字符的字符串，不区分大小写；

radius-scheme radius-scheme-name2: 表示抄送计费 RADIUS 方案名，为 1~32 个字符的字符串，不区分大小写。

local: 本地计费。

none: 不计费。

radius-scheme radius-scheme-name: 指定 RADIUS 方案。其中，*radius-scheme-name* 表示 RADIUS 方案名，为 1~32 个字符的字符串，不区分大小写。

【使用指导】

可以指定多个备选的计费方法。在当前的计费方法无效时按照配置顺序尝试使用备选的方法完成计费。例如，**radius-scheme radius-scheme-name local none** 表示，先进行 RADIUS 计费，若 RADIUS 计费无效则进行本地计费，若本地计费也无效则不进行计费。

当指定 **broadcast** 关键字时，将以主送 RADIUS 方案中的实时计费间隔同时向指定的两个 RADIUS 方案里的主计费服务器发送计费请求，若某 RADIUS 方案里的主计费服务器不可达，则按照配置顺序依次尝试向该 RADIUS 方案里的从计费服务器发送计费请求。主送计费方案计费成功时，表示用户计费成功；抄送计费方案的计费结果对用户无影响。

【举例】

在 ISP 域 test 下，为 lan-access 用户配置计费方法为 **local**。

```
<Sysname> system-view
[Sysname] domain test
[Sysname-isp-test] accounting lan-access local
```

在 ISP 域 test 下，配置 lan-access 用户使用 RADIUS 方案 rd 进行计费，并且使用 **local** 作为备选计费方法。

```
<Sysname> system-view
[Sysname] domain test
[Sysname-isp-test] accounting lan-access radius-scheme rd local
```

在 ISP 域 test 下，配置 lan-access 用户使用 RADIUS 方案 rd1 和 rd2 进行广播计费，并且使用 **local** 作为备选计费方法。

```
<Sysname> system-view
[Sysname] domain test
[Sysname-isp-test] accounting lan-access broadcast radius-scheme rd1 radius-scheme rd2 local
```

【相关命令】

- **accounting default**
- **local-user**
- **radius scheme**
- **timer realtime-accounting**

1.1.6 accounting login

accounting login 命令用来为 login 用户配置计费方法。

undo accounting login 命令用来恢复缺省情况。

【命令】

非 FIPS 模式下：

```
accounting login { hwtacacs-scheme hwtacacs-scheme-name [ radius-scheme radius-scheme-name ] [ local ] [ none ] | local [ none ] | none | radius-scheme radius-scheme-name [ hwtacacs-scheme hwtacacs-scheme-name ] [ local ] [ none ] }
```

```
undo accounting login
```

FIPS 模式下：


```

accounting login { hwtacacs-scheme hwtacacs-scheme-name [ radius-scheme
radius-scheme-name ] [ local ] | local | radius-scheme radius-scheme-name
[ hwtacacs-scheme hwtacacs-scheme-name ] [ local ] }
undo accounting login

```

【缺省情况】

login 用户采用当前 ISP 域的缺省计费方法。

【视图】

ISP 域视图

【缺省用户角色】

network-admin

【参数】

hwtacacs-scheme *hwtacacs-scheme-name* : 指定 HWTACACS 方案。其中，*hwtacacs-scheme-name* 表示 HWTACACS 方案名，为 1~32 个字符的字符串，不区分大小写。

local: 本地计费。

none: 不计费。

radius-scheme *radius-scheme-name*: 指定 RADIUS 方案。其中，*radius-scheme-name* 表示 RADIUS 方案名，为 1~32 个字符的字符串，不区分大小写。

【使用指导】

不支持对 FTP、SFTP 以及 SCP 类型的 login 用户进行计费。

可以指定多个备选的计费方法。在当前的计费方法无效时按照配置顺序尝试使用备选的方法完成计费。例如，**radius-scheme** *radius-scheme-name* **local** **none** 表示，先进行 RADIUS 计费，若 RADIUS 计费无效则进行本地计费，若本地计费也无效则不进行计费。

【举例】

在 ISP 域 test 下，为 login 用户配置计费方法为 **local**。

```

<Sysname> system-view
[Sysname] domain test
[Sysname-isp-test] accounting login local

```

在 ISP 域 test 下，配置 login 用户使用 RADIUS 方案 rd 进行计费，并且使用 **local** 作为备选计费方法。

```

<Sysname> system-view
[Sysname] domain test
[Sysname-isp-test] accounting login radius-scheme rd local

```

【相关命令】

- **accounting default**
- **hwtacacs scheme**
- **local-user**
- **radius scheme**

1.1.7 accounting portal

accounting portal 命令用来为 Portal 用户配置计费方法。

undo accounting portal 命令用来恢复缺省情况。

【命令】

非 FIPS 模式下:

```
accounting portal { broadcast radius-scheme radius-scheme-name1
radius-scheme radius-scheme-name2 [ local ] [ none ] | local [ none ] | none
| radius-scheme radius-scheme-name [ local ] [ none ] }
undo accounting portal
```

FIPS 模式下:

```
accounting portal { broadcast radius-scheme radius-scheme-name1
radius-scheme radius-scheme-name2 [ local ] | local | radius-scheme
radius-scheme-name [ local ] }
undo accounting portal
```

【缺省情况】

Portal 用户采用当前 ISP 域的缺省计费方法。

【视图】

ISP 域视图

【缺省用户角色】

network-admin

【参数】

broadcast: 指定广播 RADIUS 方案，即同时向指定的两个 RADIUS 方案中的计费服务器发送计费请求。

radius-scheme radius-scheme-name1: 表示主送计费 RADIUS 方案名，为 1~32 个字符的字符串，不区分大小写；

radius-scheme radius-scheme-name2: 表示抄送计费 RADIUS 方案名，为 1~32 个字符的字符串，不区分大小写。

local: 本地计费。

none: 不计费。

radius-scheme radius-scheme-name: 指定 RADIUS 方案。其中，*radius-scheme-name* 表示 RADIUS 方案名，为 1~32 个字符的字符串，不区分大小写。

【使用指导】

可以指定多个备选的计费方法，在当前的计费方法无效时按照配置顺序尝试使用备选的方法完成计费。例如，**radius-scheme radius-scheme-name local none** 表示，先进行 RADIUS 计费，若 RADIUS 计费无效则进行本地计费，若本地计费也无效则不进行计费。

当指定 **broadcast** 关键字时，将以主送 RADIUS 方案中的实时计费间隔同时向指定的两个 RADIUS 方案里的主计费服务器发送计费请求，若某 RADIUS 方案里的主计费服务器不可达，则按

照配置顺序依次尝试向该 RADIUS 方案里的从计费服务器发送计费请求。主送计费方案计费成功时，表示用户计费成功；抄送计费方案的计费结果对用户无影响。

【举例】

在 ISP 域 test 下，为 Portal 用户配置计费方法为 local。

```
<Sysname> system-view
[Sysname] domain test
[Sysname-isp-test] accounting portal local
```

在 ISP 域 test 下，配置 Portal 用户使用 RADIUS 方案 rd 进行计费，并且使用 local 作为备选计费方法。

```
<Sysname> system-view
[Sysname] domain test
[Sysname-isp-test] accounting portal radius-scheme rd local
```

在 ISP 域 test 下，配置 Portal 用户使用 RADIUS 方案 rd1 和 rd2 进行广播计费，并且使用 local 作为备选计费方法。

```
<Sysname> system-view
[Sysname] domain test
[Sysname-isp-test] accounting portal broadcast radius-scheme rd1 radius-scheme rd2 local
```

【相关命令】

- **accounting default**
- **local-user**
- **radius scheme**
- **timer realtime-accounting**

1.1.8 accounting quota-out

accounting quota-out 命令用来配置用户计费流量配额耗尽策略。

undo accounting quota-out 命令用来恢复缺省情况。

【命令】

```
accounting quota-out { offline | online }
undo accounting quota-out
```

【缺省情况】

用户的计费流量配额耗尽后将被强制下线。

【视图】

ISP 域视图

【缺省用户角色】

network-admin

【参数】

offline: 当用户的整体流量配额耗尽后，强制用户下线。

online: 当用户的整体流量配额耗尽后，允许用户保持在线状态。

【使用指导】

需要注意的是，如果配置的用户计费流量配额耗尽策略为 **offline**，则当服务器为 Portal 用户授权了剩余流量时，强制该类用户下线的时间可能会不准确。

【举例】

在 ISP 域 test 下，配置用户计费流量配额耗尽策略为：当流量配额耗尽后用户仍能保持在线状态。

```
<Sysname> system-view
[Sysname] domain test
[Sysname-isp-test] accounting quota-out online
```

1.1.9 accounting start-fail

accounting start-fail 命令用来配置用户计费开始失败策略，即设备向计费服务器发送计费开始请求失败后，是否允许用户接入网络。

undo accounting start-fail 命令用来恢复缺省情况。

【命令】

```
accounting start-fail { offline | online }
undo accounting start-fail
```

【缺省情况】

如果用户计费开始失败，允许用户保持在线状态。

【视图】

ISP 域视图

【缺省用户角色】

network-admin

【参数】

offline：强制用户下线。

online：允许用户保持在线状态。

【举例】

在 ISP 域 test 下，配置计费开始失败策略为：用户计费开始失败时允许用户保持在线状态。

```
<Sysname> system-view
[Sysname] domain test
[Sysname-isp-test] accounting start-fail online
```

1.1.10 accounting update-fail

accounting update-fail 命令用来配置用户计费更新失败策略，即设备向计费服务器发送用户的计费更新报文失败时，是否允许用户接入网络。

undo accounting update-fail 命令用来恢复缺省情况。

【命令】

```
accounting update-fail { [ max-times max-times ] offline | online }
undo accounting update-fail
```

【缺省情况】

如果用户计费更新失败，允许用户保持在线状态。

【视图】

ISP 域视图

【缺省用户角色】

network-admin

【参数】

max-times *max-times*: 允许用户连续计费更新失败的次数，取值范围 1~255，缺省值为 1。

offline: 如果用户连续计费更新失败的次数达到了指定的次数，则强制用户下线。

online: 如果用户计费更新失败，允许用户保持在线状态。

【举例】

在 ISP 域 test 下，配置计费更新失败策略为：用户计费更新失败时允许用户保持在线状态。

```
<Sysname> system-view
[Sysname] domain test
[Sysname-isp-test] accounting update-fail online
```

1.1.11 authentication default

authentication default 命令用来为当前 ISP 域配置缺省的认证方法。

undo authentication default 命令用来为恢复缺省情况。

【命令】

非 FIPS 模式下：

```
authentication default { hwtacacs-scheme hwtacacs-scheme-name
[ radius-scheme radius-scheme-name ] [ local ] [ none ] | ldap-scheme
ldap-scheme-name [ local ] [ none ] | local [ none ] | none | radius-scheme
radius-scheme-name [ hwtacacs-scheme hwtacacs-scheme-name ] [ local ]
[ none ] }
```

undo authentication default

FIPS 模式下：

```
authentication default { hwtacacs-scheme hwtacacs-scheme-name
[ radius-scheme radius-scheme-name ] [ local ] | ldap-scheme
ldap-scheme-name [ local ] | local | radius-scheme radius-scheme-name
[ hwtacacs-scheme hwtacacs-scheme-name ] [ local ] }
```

undo authentication default

【缺省情况】

当前 ISP 域的缺省认证方法为 **local**。

【视图】

ISP 域视图

【缺省用户角色】

network-admin

【参数】

hwtacacs-scheme *hwtacacs-scheme-name* : 指定 HWTACACS 方案。其中, *hwtacacs-scheme-name* 表示 HWTACACS 方案名, 为 1~32 个字符的字符串, 不区分大小写。

ldap-scheme *ldap-scheme-name*: 指定 LDAP 方案。其中 *ldap-scheme-name* 表示 LDAP 方案名, 为 1~32 个字符的字符串, 不区分大小写。

local: 本地认证。

none: 不进行认证。

radius-scheme *radius-scheme-name*: 指定 RADIUS 方案。其中, *radius-scheme-name* 表示 RADIUS 方案名, 为 1~32 个字符的字符串, 不区分大小写。

【使用指导】

当前 ISP 域的缺省的认证方法对于该域中未指定具体认证方法的所有接入用户都起作用, 但是如果某类型的用户不支持指定的认证方法, 则该认证方法对于这类用户不能生效。

可以指定多个备选的认证方法, 在当前的认证方法无效时按照配置顺序尝试使用备选的方法完成认证。例如, **radius-scheme radius-scheme-name local none** 表示, 先进行 RADIUS 认证, 若 RADIUS 认证无效则进行本地认证, 若本地认证也无效则不进行认证。

【举例】

在 ISP 域 test 下, 配置缺省认证方法为使用 RADIUS 方案 rd 进行认证, 并且使用 **local** 作为备选认证方法。

```
<Sysname> system-view
[Sysname] domain test
[Sysname-isp-test] authentication default radius-scheme rd local
```

【相关命令】

- **hwtacacs scheme**
- **ldap scheme**
- **local-user**
- **radius scheme**

1.1.12 authentication lan-access

authentication lan-access 命令用来为 lan-access 用户配置认证方法。

undo authentication lan-access 命令用来恢复缺省情况。

【命令】

非 FIPS 模式下:

```
authentication lan-access { ldap-scheme ldap-scheme-name [ local ] [ none ]
| local [ none ] | none | radius-scheme radius-scheme-name [ local ] [ none ] }
undo authentication lan-access
```

FIPS 模式下:

```
authentication lan-access { ldap-scheme ldap-scheme-name [ local ] | local |  
radius-scheme radius-scheme-name [ local ] }  
undo authentication lan-access
```

【缺省情况】

lan-access 用户采用当前 ISP 域的缺省认证方法。

【视图】

ISP 域视图

【缺省用户角色】

network-admin

【参数】

ldap-scheme *ldap-scheme-name*: 指定 LDAP 方案。其中 *ldap-scheme-name* 表示 LDAP 方案名，为 1~32 个字符的字符串，不区分大小写。

local: 本地认证。

none: 不进行认证。

radius-scheme *radius-scheme-name*: 指定 RADIUS 方案。其中，*radius-scheme-name* 表示 RADIUS 方案名，为 1~32 个字符的字符串，不区分大小写。

【使用指导】

可以指定多个备选的认证方法，在当前的认证方法无效时按照配置顺序尝试使用备选的方法完成认证。例如，**radius-scheme radius-scheme-name local none** 表示，先进行 RADIUS 认证，若 RADIUS 认证无效则进行本地认证，若本地认证也无效则不进行认证。

【举例】

在 ISP 域 test 下，为 lan-access 用户配置认证方法为 local。

```
<Sysname> system-view  
[Sysname] domain test  
[Sysname-isp-test] authentication lan-access local
```

在 ISP 域 test 下，配置 lan-access 用户使用 RADIUS 方案 rd 进行认证，并且使用 local 作为备选认证方法。

```
<Sysname> system-view  
[Sysname] domain test  
[Sysname-isp-test] authentication lan-access radius-scheme rd local
```

【相关命令】

- authentication default
- hwtacacs scheme
- ldap scheme
- local-user
- radius scheme

1.1.13 authentication login

authentication login 命令用来为 login 用户配置认证方法。

undo authentication login 命令用来恢复缺省情况。

【命令】

非 FIPS 模式下:

```
authentication login { hwtacacs-scheme hwtacacs-scheme-name [ radius-scheme radius-scheme-name ] [ local ] [ none ] | ldap-scheme ldap-scheme-name [ local ] [ none ] | local [ none ] | none | radius-scheme radius-scheme-name [ hwtacacs-scheme hwtacacs-scheme-name ] [ local ] [ none ] }
```

undo authentication login

FIPS 模式下:

```
authentication login { hwtacacs-scheme hwtacacs-scheme-name [ radius-scheme radius-scheme-name ] [ local ] | ldap-scheme ldap-scheme-name [ local ] | local | radius-scheme radius-scheme-name [ hwtacacs-scheme hwtacacs-scheme-name ] [ local ] }
```

undo authentication login

【缺省情况】

login 用户采用当前 ISP 域的缺省认证方法。

【视图】

ISP 域视图

【缺省用户角色】

network-admin

【参数】

hwtacacs-scheme *hwtacacs-scheme-name* : 指定 HWTACACS 方案。其中, *hwtacacs-scheme-name* 表示 HWTACACS 方案名, 为 1~32 个字符的字符串, 不区分大小写。

ldap-scheme *ldap-scheme-name*: 指定 LDAP 方案。其中 *ldap-scheme-name* 表示 LDAP 方案名, 为 1~32 个字符的字符串, 不区分大小写。

local: 本地认证。

none: 不进行认证。

radius-scheme *radius-scheme-name*: 指定 RADIUS 方案。其中, *radius-scheme-name* 表示 RADIUS 方案名, 为 1~32 个字符的字符串, 不区分大小写。

【使用指导】

可以指定多个备选的认证方法, 在当前的认证方法无效时按照配置顺序尝试使用备选的方法完成认证。例如, **radius-scheme radius-scheme-name local none** 表示, 先进行 RADIUS 认证, 若 RADIUS 认证无效则进行本地认证, 若本地认证也无效则不进行认证。

【举例】

在 ISP 域 test 下, 为 login 用户配置认证方法为 **local**。


```

<Sysname> system-view
[Sysname] domain test
[Sysname-isp-test] authentication login local
# 在 ISP 域 test 下，配置 login 用户使用 RADIUS 方案 rd 进行认证，并且使用 local 作为备选认证方法。

<Sysname> system-view
[Sysname] domain test
[Sysname-isp-test] authentication login radius-scheme rd local

```

【相关命令】

- **authentication default**
- **hwtaacacs scheme**
- **ldap scheme**
- **local-user**
- **radius scheme**

1.1.14 authentication portal

authentication portal 命令用来为 Portal 用户配置认证方法。

undo authentication portal 命令用来恢复缺省情况。

【命令】

非 FIPS 模式下：

```

authentication portal { ldap-scheme ldap-scheme-name [ local ] [ none ] |
local [ none ] | none | radius-scheme radius-scheme-name [ local ] [ none ] }
undo authentication portal

```

FIPS 模式下：

```

authentication portal { ldap-scheme ldap-scheme-name [ local ] | local |
radius-scheme radius-scheme-name [ local ] }
undo authentication portal

```

【缺省情况】

Portal 用户采用当前 ISP 域的缺省认证方法。

【视图】

ISP 域视图

【缺省用户角色】

network-admin

【参数】

ldap-scheme *ldap-scheme-name*：指定 LDAP 方案。其中 *ldap-scheme-name* 表示 LDAP 方案名，为 1~32 个字符的字符串，不区分大小写。

local：本地认证。

none：不进行认证。

radius-scheme *radius-scheme-name*: 指定 RADIUS 方案。其中, *radius-scheme-name* 表示 RADIUS 方案名, 为 1~32 个字符的字符串, 不区分大小写。

【使用指导】

可以指定多个备选认证方法, 在当前的认证方法无效时按照配置顺序尝试使用备选的方法完成认证。例如, **radius-scheme radius-scheme-name local none** 表示, 先进行 RADIUS 认证, 若 RADIUS 认证无效则进行本地认证, 若本地认证也无效则不进行认证。

【举例】

在 ISP 域 test 下, 为 Portal 用户配置认证方法为 local。

```
<Sysname> system-view
[Sysname] domain test
[Sysname-isp-test] authentication portal local
```

在 ISP 域 test 下, 配置 Portal 用户使用 RADIUS 方案 rd 进行认证, 并且使用 local 作为备选认证方法。

```
<Sysname> system-view
[Sysname] domain test
[Sysname-isp-test] authentication portal radius-scheme rd local
```

【相关命令】

- **authentication default**
- **ldap scheme**
- **local-user**
- **radius scheme**

1.1.15 authentication super

authentication super 命令用来配置用户角色切换认证方法。

undo authentication super 命令用来恢复缺省情况。

【命令】

```
authentication super { hwtacacs-scheme hwtacacs-scheme-name | radius-scheme radius-scheme-name } *
undo authentication super
```

【缺省情况】

用户角色切换认证采用当前 ISP 域的缺省认证方法。

【视图】

ISP 域视图

【缺省用户角色】

network-admin

【参数】

hwtacacs-scheme *hwtacacs-scheme-name* : 指定 HWTACACS 方案。其中, *hwtacacs-scheme-name* 表示 HWTACACS 方案名, 为 1~32 个字符的字符串, 不区分大小写。

radius-scheme radius-scheme-name: 指定 RADIUS 方案。其中, *radius-scheme-name* 表示 RADIUS 方案名, 为 1~32 个字符的字符串, 不区分大小写。

【使用指导】

切换用户角色是指在不退出当前登录、不断开当前连接的前提下修改用户的用户角色, 改变用户所拥有的命令行权限。为了保证切换操作的安全性, 需要在用户执行用户角色切换时进行身份认证。设备支持本地和远程两种认证方式, 关于用户角色切换的详细介绍请参见“基础配置指导”中的“RBAC”。

可以指定一个备选的认证方法, 在当前的认证方法无效时尝试使用备选的方法完成认证。

【举例】

在 ISP 域 test 下, 配置使用 HWTACACS 方案 tac 进行用户角色切换认证。

```
<Sysname> system-view
[Sysname] super authentication-mode scheme
[Sysname] domain test
[Sysname-isp-test] authentication super hwtacacs-scheme tac
```

【相关命令】

- **authentication default**
- **hwtacacs scheme**
- **radius scheme**

1.1.16 authorization command

authorization command 命令用来配置命令行授权方法。

undo authorization command 命令用来恢复缺省情况。

【命令】

非 FIPS 模式下:

```
authorization command { hwtacacs-scheme hwtacacs-scheme-name [ local ]
[ none ] | local [ none ] | none }
undo authorization command
```

FIPS 模式下:

```
authorization command { hwtacacs-scheme hwtacacs-scheme-name [ local ] |
local }
undo authorization command
```

【缺省情况】

命令行授权采用当前 ISP 域的缺省授权方法。

【视图】

ISP 域视图

【缺省用户角色】

network-admin

【参数】

hwtacacs-scheme *hwtacacs-scheme-name* : 指定 HWTACACS 方案。其中，*hwtacacs-scheme-name* 表示 HWTACACS 方案名，为 1~32 个字符的字符串，不区分大小写。

local: 本地授权。

none: 不授权。用户执行角色所允许的命令时，无须接受授权服务器的检查。

【使用指导】

命令行授权是指，用户执行的每一条命令都需要接受授权服务器的检查，只有授权成功的命令才被允许执行。用户登录后可以执行的命令受登录授权的用户角色和命令行授权的用户角色的双重限制，即，仅登录授权的用户角色和命令行授权的用户角色均允许执行的命令行，才能被执行。需要注意的是，命令行授权功能只利用角色中的权限规则对命令行执行权限检查，不进行其它方面的权限检查，例如资源控制策略等。

对用户采用本地命令行授权时，设备将根据用户登录设备时输入的用户名对应的本地用户配置来对用户输入的命令进行检查，只有本地用户中配置的授权用户角色所允许的命令才被允许执行。

可以指定多个备选的命令授权方法，在当前的授权方法无效时按照配置顺序尝试使用备选的方法完成命令授权。例如，**hwtacacs-scheme hwtacacs-scheme-name local none** 表示，先进行 HWTACACS 授权，若 HWTACACS 授权无效则进行本地授权，若本地授权也无效则不进行授权。

【举例】

在 ISP 域 test 下，配置命令行授权方法为 **local**。

```
<Sysname> system-view
[Sysname] domain test
[Sysname-isp-test] authorization command local
```

在 ISP 域 test 下，配置使用 HWTACACS 方案 hwtac 进行命令行授权，并且使用 **local** 作为备选授权方法。

```
<Sysname> system-view
[Sysname] domain test
[Sysname-isp-test] authorization command hwtacacs-scheme hwtac local
```

【相关命令】

- **command authorization** (基础命令参考/登录设备)
- **hwtacacs scheme**
- **local-user**

1.1.17 authorization default

authorization default 命令用来为当前 ISP 域配置缺省的授权方法。

undo authorization default 命令用来恢复缺省情况。

【命令】

非 FIPS 模式下：

```
authorization default { hwtacacs-scheme hwtacacs-scheme-name
[ radius-scheme radius-scheme-name ] [ local ] [ none ] | local [ none ] | none
| radius-scheme radius-scheme-name [ hwtacacs-scheme hwtacacs-scheme-name ]
[ local ] [ none ] }
```

```
undo authorization default
```

FIPS 模式下:

```
authorization default { hwtacacs-scheme hwtacacs-scheme-name  
[ radius-scheme radius-scheme-name ] [ local ] | local | radius-scheme  
radius-scheme-name [ hwtacacs-scheme hwtacacs-scheme-name ] [ local ] }  
undo authorization default
```

【缺省情况】

当前 ISP 域的缺省授权方法为 **local**。

【视图】

ISP 域视图

【缺省用户角色】

network-admin

【参数】

hwtacacs-scheme *hwtacacs-scheme-name* : 指定 HWTACACS 方案。其中，*hwtacacs-scheme-name* 表示 HWTACACS 方案名，为 1~32 个字符的字符串，不区分大小写。

local: 本地授权。

none: 不授权。接入设备不请求授权信息，不对用户可以使用的操作以及用户允许使用的网络服务进行授权。此时，认证通过的 Login 用户（通过 Console 口或者 Telnet、FTP/SFTP/SCP 访问设备的用户）只有系统给予的缺省用户角色 **level-0**，其中 FTP/SFTP/SCP 用户的工作目录是设备的根目录，但并无访问权限；认证通过的非 Login 用户可直接访问网络。关于用户角色 **level-0** 的详细介绍请参见“基础配置指导”中的“RBAC”。

radius-scheme *radius-scheme-name*: 指定 RADIUS 方案。其中，*radius-scheme-name* 表示 RADIUS 方案名，为 1~32 个字符的字符串，不区分大小写。

【使用指导】

当前 ISP 域的缺省的授权方法对于该域中未指定具体授权方法的所有接入用户都起作用，但是如果某类型的用户不支持指定的授权方法，则该授权方法对于这类用户不能生效。

在一个 ISP 域中，只有配置的认证和授权方法中引用了相同的 RADIUS 方案时，RADIUS 授权过程才能生效。

可以指定多个备选的授权方法，在当前的授权方法无效时按照配置顺序尝试使用备选的方法完成授权。例如，**radius-scheme radius-scheme-name local none** 表示，先进行 RADIUS 授权，若 RADIUS 授权无效则进行本地授权，若本地授权也无效则不进行授权。

【举例】

在 ISP 域 **test** 下，配置缺省授权方法为使用 RADIUS 方案 **rd** 进行授权，并且使用 **local** 作为备选授权方法。

```
<Sysname> system-view  
[Sysname] domain test  
[Sysname-isp-test] authorization default radius-scheme rd local
```

【相关命令】

- `hwtaacs scheme`
- `local-user`
- `radius scheme`

1.1.18 authorization lan-access

`authorization lan-access` 命令用来为 lan-access 用户配置授权方法。

`undo authorization lan-access` 命令用来恢复缺省情况。

【命令】

非 FIPS 模式下：

```
authorization lan-access { local [ none ] | none | radius-scheme  
radius-scheme-name [ local ] [ none ] }  
undo authorization lan-access
```

FIPS 模式下：

```
authorization lan-access { local | radius-scheme radius-scheme-name  
[ local ] }  
undo authorization lan-access
```

【缺省情况】

lan-access 用户采用当前 ISP 域的缺省授权方法。

【视图】

ISP 域视图

【缺省用户角色】

network-admin

【参数】

local：本地授权。

none：不授权。接入设备不请求授权信息，不对用户可以使用的操作以及用户允许使用的网络服务进行授权，认证通过的 lan-access 用户可直接访问网络。

radius-scheme radius-scheme-name：指定 RADIUS 方案。其中，*radius-scheme-name* 表示 RADIUS 方案名，为 1~32 个字符的字符串，不区分大小写。

【使用指导】

在一个 ISP 域中，只有配置的认证和授权方法中引用了相同的 RADIUS 方案时，RADIUS 授权过程才能生效。

可以指定多个备选的授权方法，在当前的授权方法无效时按照配置顺序尝试使用备选的方法完成授权。例如，**radius-scheme radius-scheme-name local none** 表示，先进行 RADIUS 授权，若 RADIUS 授权无效则进行本地授权，若本地授权也无效则不进行授权。

【举例】

在 ISP 域 test 下，为 lan-access 用户配置授权方法为 local。

```

<Sysname> system-view
[Sysname] domain test
[Sysname-isp-test] authorization lan-access local
# 在 ISP 域 test 下，配置 lan-access 用户使用 RADIUS 方案 rd 进行授权，并且使用 local 作为备选授权方法。
<Sysname> system-view
[Sysname] domain test
[Sysname-isp-test] authorization lan-access radius-scheme rd local

```

【相关命令】

- **authorization default**
- **local-user**
- **radius scheme**

1.1.19 authorization login

authorization login 命令用来为 login 用户配置授权方法。

undo authorization login 命令用来恢复缺省情况。

【命令】

非 FIPS 模式下：

```

authorization login { hwtacacs-scheme hwtacacs-scheme-name [ radius-scheme
radius-scheme-name ] [ local ] [ none ] | local [ none ] | none | radius-scheme
radius-scheme-name [ hwtacacs-scheme hwtacacs-scheme-name ] [ local ]
[ none ] }

```

```

undo authorization login

```

FIPS 模式下：

```

authorization login { hwtacacs-scheme hwtacacs-scheme-name [ radius-scheme
radius-scheme-name ] [ local ] | local | radius-scheme radius-scheme-name
[ hwtacacs-scheme hwtacacs-scheme-name ] [ local ] }

```

```

undo authorization login

```

【缺省情况】

login 用户采用当前 ISP 域的缺省授权方法。

【视图】

ISP 域视图

【缺省用户角色】

network-admin

【参数】

hwtacacs-scheme *hwtacacs-scheme-name*：指定 HWTACACS 方案。其中，*hwtacacs-scheme-name* 表示 HWTACACS 方案名，为 1~32 个字符的字符串，不区分大小写。
local：本地授权。

none: 不授权。接入设备不请求授权信息，不对用户可以使用的操作以及用户允许使用的网络服务进行授权。此时，认证通过的 Login 用户（通过 Console 口或者 Telnet、FTP/SFTP/SCP 访问设备的用户）只有系统给予的缺省用户角色 **level-0**，其中 FTP/SFTP/SCP 用户的工作目录是设备的根目录，但并无访问权限。关于用户角色 **level-0** 的详细介绍请参见“基础配置指导”中的“RBAC”。

radius-scheme radius-scheme-name: 指定 RADIUS 方案。其中，*radius-scheme-name* 表示 RADIUS 方案名，为 1~32 个字符的字符串，不区分大小写。

【使用指导】

在一个 ISP 域中，只有配置的认证和授权方法中引用了相同的 RADIUS 方案时，RADIUS 授权过程才能生效。

可以指定多个备选的授权方法，在当前的授权方法无效时按照配置顺序尝试使用备选的方法完成授权。例如，**radius-scheme radius-scheme-name local none** 表示，先进行 RADIUS 授权，若 RADIUS 授权无效则进行本地授权，若本地授权也无效则不进行授权。

【举例】

在 ISP 域 **test** 下，为 login 用户配置授权方法为 **local**。

```
<Sysname> system-view
[Sysname] domain test
[Sysname-isp-test] authorization login local
```

在 ISP 域 **test** 下，配置 login 用户使用 RADIUS 方案 **rd** 进行授权，并且使用 **local** 作为备选授权方法。

```
<Sysname> system-view
[Sysname] domain test
[Sysname-isp-test] authorization login radius-scheme rd local
```

【相关命令】

- **authorization default**
- **hwtaacs scheme**
- **local-user**
- **radius scheme**

1.1.20 authorization portal

authorization portal 命令用来为 Portal 用户配置授权方法。

undo authorization portal 命令用来恢复缺省情况。

【命令】

非 FIPS 模式下:

```
authorization portal { local [ none ] | none | radius-scheme
radius-scheme-name [ local ] [ none ] }
undo authorization portal
```

FIPS 模式下:

```
authorization portal { local | radius-scheme radius-scheme-name [ local ] }
undo authorization portal
```


【缺省情况】

Portal 用户采用当前 ISP 域的缺省授权方法。

【视图】

ISP 域视图

【缺省用户角色】

network-admin

【参数】

local: 本地授权。

none: 不授权。接入设备不请求授权信息，不对用户可以使用的操作以及用户允许使用的网络服务进行授权，认证通过的 Portal 用户可直接访问网络。

radius-scheme radius-scheme-name: 指定 RADIUS 方案。其中，*radius-scheme-name* 表示 RADIUS 方案名，为 1~32 个字符的字符串，不区分大小写。

【使用指导】

在一个 ISP 域中，只有配置的认证和授权方法中引用了相同的 RADIUS 方案时，RADIUS 授权过程才能生效。

可以指定多个备选的授权方法，在当前的授权方法无效时按照配置顺序尝试使用备选的方法完成授权。例如，**radius-scheme radius-scheme-name local none** 表示，先进行 RADIUS 授权，若 RADIUS 授权无效则进行本地授权，若本地授权也无效则不进行授权。

【举例】

在 ISP 域 test 下，为 Portal 用户配置授权方法为 **local**。

```
<Sysname> system-view
[Sysname] domain test
[Sysname-isp-test] authorization portal local
```

在 ISP 域 test 下，配置 Portal 用户使用 RADIUS 方案 rd 进行授权，并且使用 **local** 作为备选授权方法。

```
<Sysname> system-view
[Sysname] domain test
[Sysname-isp-test] authorization portal radius-scheme rd local
```

【相关命令】

- **authorization default**
- **local-user**
- **radius scheme**

1.1.21 authorization-attribute (ISP domain view)

authorization-attribute 命令用来设置当前 ISP 域下的用户授权属性。

undo authorization-attribute 命令用来删除指定的授权属性，恢复用户具有的缺省访问权限。

【命令】

```
authorization-attribute { acl acl-number | car inbound cir  
committed-information-rate [ pir peak-information-rate ] outbound cir  
committed-information-rate [ pir peak-information-rate ] | igmp  
max-access-number max-access-number | ip-pool ipv4-pool-name | ipv6-pool  
ipv6-pool-name | mld max-access-number max-access-number | url url-string |  
user-group user-group-name | user-profile profile-name }  
undo authorization-attribute { acl | car | igmp | ip-pool | ipv6-pool | mld  
| url | user-group | user-profile }
```

【缺省情况】

IPv4 用户可以同时点播的最大节目数为 4，IPv6 用户可以同时点播的最大节目数为 4，无其它授权属性。

【视图】

ISP 域视图

【缺省用户角色】

network-admin

【参数】

acl *acl-number*: 指定用于匹配用户流量的 ACL。其中 *acl-number* 表示 ACL 编号，取值范围 2000~4999。与授权 ACL 规则匹配的流量，将按照规则中指定的 **permit** 或 **deny** 动作进行处理。此属性只对 **Portal**、**lan-access** 用户生效。

car: 指定授权用户的流量监管动作。**Portal** 用户在认证前，若被授权认证域，则其流量将受到指定的流量监管动作控制。此属性只对 **Portal** 用户生效。

inbound: 表示用户的上传速率。

outbound: 表示用户的下载速率。

cir *committed-information-rate*: 承诺信息速率，取值范围为 1~4194303，单位为 kbps。

pir *peak-information-rate*: 峰值信息速率，取值范围为 1~4194303，单位为 kbps。若不指定该参数，则表示不对峰值信息速率进行限制。

igmp **max-access-number** *max-access-number*: 指定 IPv4 用户可以同时点播的最大节目数。其中，*max-access-number* 的取值范围为 1~64。此属性只对 **Portal** 用户生效。

ip-pool *ipv4-pool-name*: 指定为用户分配 IPv4 地址的地址池。其中，*ipv4-pool-name* 表示地址池名称，为 1~63 个字符的字符串，不区分大小写。此属性只对 **Portal** 用户生效。

ipv6-pool *ipv6-pool-name*: 指定为用户分配 IPv6 地址的地址池。其中，*ipv6-pool-name* 表示地址池名称，为 1~63 个字符的字符串，不区分大小写。此属性只对 **Portal** 用户生效。

mld **max-access-number** *max-access-number*: 指定 IPv6 用户可以同时点播的最大节目数。其中，*max-access-number* 的取值范围为 1~64。此属性只对 **Portal** 用户生效。

url *url-string*: 指定用户的重定向 URL，为 1~255 个字符的字符串，区分大小写。用户认证成功，首次访问网络时将被推送此 URL 提供的 Web 页面。此属性只对 **lan-access** 用户生效。

user-group *user-group-name*: 表示用户所属用户组。其中，*user-group-name* 表示用户组名，为 1~32 个字符的字符串，不区分大小写。用户认证成功后，将继承该用户组中的所有属性。

user-profile profile-name: 指定用户的授权 User Profile。其中, *profile-name* 为 User Profile 名称, 为 1~31 个字符的字符串, 区分大小写。Portal 用户在认证前, 若被授权认证域, 则其访问行为将受到该域中的 User Profile 配置的限制。此属性只对 Portal、lan-access 用户生效。

【使用指导】

如果当前 ISP 域的用户认证成功, 但认证服务器 (包括本地认证下的接入设备) 未对该 ISP 域下发授权属性, 则系统使用当前 ISP 下指定的授权属性为用户授权。

需要注意的是, 可通过多次执行本命令配置多个授权属性, 但对于相同授权属性, 最后一次执行的命令生效。

授权给 Portal 用户的 ACL 中不能配置携带用户源 IP 地址和源 MAC 地址信息的规则, 否则会导致用户上线失败。

【举例】

设置 ISP 域 test 的用户授权组为 abc。

```
<Sysname> system-view
[Sysname] domain test
[Sysname-isp-test] authorization-attribute user-group abc
```

【相关命令】

- **display domain**

1.1.22 display domain

display domain 命令用来显示所有或指定 ISP 域的配置信息。

【命令】

```
display domain [ isp-name ]
```

【视图】

任意视图

【缺省用户角色】

```
network-admin
network-operator
```

【参数】

isp-name: ISP 域名, 为 1~255 个字符的字符串, 不区分大小写。如果不指定该参数, 则表示所有 ISP 域。

【举例】

显示系统中所有 ISP 域的配置信息。

```
<Sysname> display domain
Total 2 domains

Domain: system
  State: Active
  Default authentication scheme: Local
  Default authorization scheme: Local
```

```

Default accounting      scheme: Local
Accounting start failure action: Online
Accounting update failure action: Online
Accounting quota out policy: Offline
Service type: HSI
Session time: Exclude idle time
Dual-stack accounting method: Merge
Authorization attributes:
    Idle cut: Disabled
    IGMP access number: 4
    MLD access number: 4

Domain: dm
State: Active
Login authentication scheme: RADIUS=rad
Login authorization scheme: HWTACACS=hw
Super authentication scheme: RADIUS=rad
Command authorization scheme: HWTACACS=hw
LAN access authentication scheme: RADIUS=r4
Portal authentication scheme: LDAP=ldp
Default authentication scheme: RADIUS=rad, Local, None
Default authorization scheme: Local
Default accounting      scheme: None
Accounting start failure action: Online
Accounting update failure action: Online
Accounting quota out policy: Offline
Service type: HSI
Session time: Include idle time
Dual-stack accounting method: Merge
Authorization attributes:
    Idle cut : Disabled
    IP pool: appy
    User profile: test
    Inbound CAR: CIR 64000 bps PIR 640000 bps
    Outbound CAR: CIR 64000 bps PIR 640000 bps
    ACL number: 3000
    User group: ugg
    IPv6 pool: ipv6pool
    URL: http://test
    IGMP access number: 4
    MLD access number: 4

Default domain name: system

```

表1-1 display domain 命令显示信息描述表

字段	描述
Total 2 domains	总计2个ISP域

字段	描述
Domain	ISP域名
State	ISP域的状态
Default authentication scheme	缺省的认证方案
Default authorization scheme	缺省的授权方案
Default accounting scheme	缺省的计费方案
Login authentication scheme	Login用户认证方案
Login authorization scheme	Login用户授权方案
Login accounting scheme	Login用户计费方案
Super authentication scheme	用户角色切换认证方案
Command authorization scheme	命令行授权方案
Command accounting scheme	命令行计费方案
LAN access authentication scheme	lan-access用户认证方案
LAN access authorization scheme	lan-access用户授权方案
LAN access accounting scheme	lan-access用户计费方案
Portal authentication scheme	Portal用户认证方案
Portal authorization scheme	Portal用户授权方案
Portal accounting scheme	Portal用户计费方案
RADIUS	RADIUS方案
HWTACACS	HWTACACS方案
LDAP	LDAP方案
Local	本地方案
None	不认证、不授权和不计费
Accounting start failure action	用户计费开始失败的动作，包括以下取值： <ul style="list-style-type: none"> Online: 如果用户计费开始失败，则保持用户在线 Offline: 如果用户计费开始失败，则强制用户下线
Accounting update failure max-times	允许用户连续计费更新失败的次数
Accounting update failure action	用户计费更新失败的动作，包括以下取值： <ul style="list-style-type: none"> Online: 如果用户计费更新失败，则保持用户在线 Offline: 如果用户计费更新失败，则强制用户下线
Accounting quota out policy	用户计费流量配额耗尽策略，包括以下取值： <ul style="list-style-type: none"> Online: 如果用户计费流量配额耗尽，则保持用户在线 Offline: 如果用户计费流量配额耗尽，则强制用户下线

字段	描述
Service type	（暂不支持）ISP域的业务类型，取值为HSI，STB和VoIP
Session time	<p>当用户异常下线时，设备上传到服务器的用户在线时间情况：</p> <ul style="list-style-type: none"> • Include idle time: 保留用户闲置切断时间 • Exclude idle time: 扣除用户闲置切断时间
Dual-stack accounting method	<p>（暂不支持）双协议栈用户的计费方式，包括以下取值：</p> <ul style="list-style-type: none"> • Merge: 统一计费，即将双协议栈用户的 IPv4 流量和 IPv6 流量统一汇总后上送给计费服务器 • Separate: 分别计费，即将双协议栈用户的 IPv4 流量和 IPv6 流量分别上送给计费服务器
Authorization attributes	ISP的用户授权属性
Idle cut	<p>（暂不支持）用户闲置切断功能，包括以下取值：</p> <ul style="list-style-type: none"> • Enabled: 处于开启状态，表示当 ISP 域中的用户在指定的最大闲置切断时间内产生的流量小于指定的最小数据流量时，会被强制下线 • Disabled: 处于关闭状态，表示不对用户进行闲置切断控制，它为缺省状态
Idle timeout	用户闲置切断时间（单位为分钟）
Flow	用户数据流量阈值（单位为字节）
Traffic direction	<p>用户数据流量的统计方向，包括以下取值：</p> <ul style="list-style-type: none"> • Both: 表示用户双向数据流量 • Inbound: 表示用户上行数据流量 • Outbound: 表示用户下行数据流量
IP pool	授权IPv4地址池的名称
User profile	授权User Profile的名称
Inbound CAR	授权的入方向CAR（CIR: 承诺信息速率，单位为bps；PIR: 峰值信息速率，单位为bps）。若未授权入方向CAR，则显示为N/A
Outbound CAR	授权的出方向CAR（CIR: 承诺信息速率，单位为bps；PIR: 峰值信息速率，单位为bps）。若未授权出方向CAR，则显示为N/A
ACL number	授权ACL编号
User group	授权User group的名称
IPv6 pool	授权IPv6地址池的名称
URL	授权重定向URL
IGMP max access number	授权IPv4用户可以同时点播的最大节目数
MLD max access number	授权IPv6用户可以同时点播的最大节目数
Default domain name	缺省ISP域名

1.1.23 domain

domain 命令用来创建 ISP 域，并进入 ISP 域视图。如果指定的 ISP 域已经存在，则直接进入 ISP 域视图。

undo domain 命令用来删除指定的 ISP 域。

【命令】

```
domain isp-name
undo domain isp-name
```

【缺省情况】

存在一个 ISP 域，名称为 **system**。

【视图】

系统视图

【缺省用户角色】

network-admin

【参数】

isp-name: ISP 域名，为 1~255 个字符的字符串，不区分大小写，不能包括 “/”、“\”、“|”、“”、“.”、“*”、“?”、“<”、“>” 以及 “@” 字符，且不能为字符串 “d”、“de”、“def”、“defa”、“defau”、“default”、“default”、“i”、“if”、“if-”、“if-u”、“if-un”、“if-unk”、“if-unkn”、“if-unkno”、“if-unknown” 和 “if-unknown”。

【使用指导】

所有的 ISP 域在创建后即处于 **active** 状态。

不能删除系统中预定义的 ISP 域 **system**，只能修改该域的配置。

不能删除作为系统缺省 ISP 域的 ISP 域。如需删除一个系统缺省 ISP 域，请先使用 **undo domain default enable** 命令将其恢复为非缺省的 ISP 域。

建议设备上配置的 ISP 域名尽量短，避免用户输入的包含域名的用户名长度超过客户端可支持的最大用户名长度。

【举例】

创建一个名称为 **test** 的 ISP 域，并进入其视图。

```
<Sysname> system-view
[Sysname] domain test
[Sysname-isp-test]
```

【相关命令】

- **display domain**
- **domain default enable**
- **domain if-unknown**
- **state (ISP domain view)**

1.1.24 domain default enable

domain default enable 命令用来配置系统缺省的 ISP 域，所有在登录时没有提供 ISP 域名的用户都属于这个域。

undo domain default enable 命令用来恢复缺省情况。

【命令】

```
domain default enable isp-name  
undo domain default enable
```

【缺省情况】

存在一个系统缺省的 ISP 域，名称为 system。

【视图】

系统视图

【缺省用户角色】

network-admin

【参数】

isp-name: ISP 域名，为 1~255 个字符的字符串，不区分大小写，且必须已经存在。

【使用指导】

系统中只能存在一个缺省的 ISP 域。

配置为缺省的 ISP 域不能被删除。如需删除一个系统缺省 ISP 域，请先使用 **undo domain default enable** 命令将其恢复为非缺省的 ISP 域。

【举例】

创建一个新的 ISP 域 test，并设置为系统缺省的 ISP 域。

```
<Sysname> system-view  
[Sysname] domain test  
[Sysname-isp-test] quit  
[Sysname] domain default enable test
```

【相关命令】

- **display domain**
- **domain**

1.1.25 domain if-unknown

domain if-unknown 命令用来为未知域名的用户指定 ISP 域。

undo domain if-unknown 命令用来恢复缺省情况。

【命令】

```
domain if-unknown isp-name  
undo domain if-unknown
```


【缺省情况】

没有为未知域名的用户指定 ISP 域。

【视图】

系统视图

【缺省用户角色】

network-admin

【参数】

isp-name: ISP 域名。为 1~255 个字符的字符串，不区分大小写，不能包括 “/”、“\”、“|”、“”、“:”、“*”、“?”、“<”、“>” 以及 “@” 字符，且不能为字符串 “d”、“de”、“def”、“defa”、“defau”、“default”、“i”、“if”、“if-”、“if-u”、“if-un”、“if-unk”、“if-unkn”、“if-unkno”、“if-unknow” 和 “if-unknown”。

【使用指导】

设备将按照如下先后顺序选择认证域：接入模块指定的认证域-->用户名中指定的 ISP 域-->系统缺省的 ISP 域。其中，仅部分接入模块支持指定认证域。

如果根据以上原则决定的认证域在设备上不存在，但设备上为未知域名的用户指定了 ISP 域，则最终使用该指定的 ISP 域认证，否则，用户将无法认证。

【举例】

为未知域名的用户指定 ISP 域为 test。

```
<Sysname> system-view
[Sysname] domain if-unknown test
```

【相关命令】

- **display domain**

1.1.26 nas-id bind vlan

nas-id bind vlan 命令用来设置 NAS-ID 与 VLAN 的绑定关系。

undo nas-id bind vlan 命令用来删除指定的 NAS-ID 和 VLAN 的绑定关系。

【命令】

```
nas-id nas-identifier bind vlan vlan-id
undo nas-id nas-identifier bind vlan vlan-id
```

【缺省情况】

不存在 NAS-ID 与 VLAN 的绑定关系。

【视图】

NAS-ID Profile 视图

【缺省用户角色】

network-admin

【参数】

nas-identifier: NAS-ID 名称, 为 1~31 个字符的字符串, 区分大小写。
vlan-id: 与 NAS-ID 绑定的 VLAN ID, 取值范围为 1~4094。

【使用指导】

一个 NAS-ID Profile 视图下, 可以指定多个 NAS-ID 与 VLAN 的绑定关系。

一个 NAS-ID 可以与多个 VLAN 绑定, 但是一个 VLAN 只能与一个 NAS-ID 绑定。若多次将一个 VLAN 与不同的 NAS-ID 进行绑定, 则最后的绑定关系生效。

【举例】

在名称为 aaa 的 NAS-ID Profile 视图下, 配置 NAS-ID 222 与 VLAN 2 的绑定关系。

```
<Sysname> system-view
[Sysname] aaa nas-id profile aaa
[Sysname-nas-id-prof-aaa] nas-id 222 bind vlan 2
```

【相关命令】

- **aaa nas-id profile**

1.1.27 session-time include-idle-time

session-time include-idle-time 命令用来配置设备上传到服务器的用户在线时间中保留闲置切断时间。

undo session-time include-idle-time 命令用来恢复缺省情况。

【命令】

```
session-time include-idle-time
undo session-time include-idle-time
```

【缺省情况】

设备上传到服务器的用户在线时间中扣除闲置切断时间。

【视图】

ISP 域视图

【缺省用户角色】

network-admin

【使用指导】

请根据实际的计费策略决定是否在用户在线时间中保留闲置切断时间。该闲置切断时间在用户认证成功由 AAA 授权, 对于 Portal 认证用户, 若接入接口上开启了 Portal 用户在线探测功能, 则 Portal 在线探测闲置时长为闲置切断时间。

当用户正常下线时, 设备上传到服务器上的用户在线时间为实际在线时间; 当用户异常下线时, 上传到服务器的用户在线时间具体如下:

- 若配置为保留闲置切断时间, 则上传到服务器上的用户在线时间中包含了一定的闲置切断时间。此时, 服务器上记录的用户时长将大于用户实际在线时长。

- 若配置为扣除闲置切断时间，则上传到服务器上的用户在线时间为，闲置切断检测机制计算出的用户已在线时长扣除掉一个闲置切断时间。此时，服务器上记录的用户时长将小于用户实际在线时长。

【举例】

在 ISP 域 test 下，配置设备上传到服务器的用户在线时间中保留闲置切断时间。

```
<Sysname> system-view
[Sysname] domain test
[Sysname-isp-test] session-time include-idle-time
```

【相关命令】

- **display domain**

1.1.28 state (ISP domain view)

state 命令用来设置当前 ISP 域的状态。

undo state 命令用来恢复缺省情况。

【命令】

```
state { active | block }
undo state
```

【缺省情况】

当前 ISP 域处于活动状态。

【视图】

ISP 域视图

【缺省用户角色】

network-admin

【参数】

active: 指定当前 ISP 域处于活动状态，即系统允许该域下的用户请求网络服务。

block: 指定当前 ISP 域处于阻塞状态，即系统不允许该域下的用户请求网络服务。

【使用指导】

当某个 ISP 域处于阻塞状态时，将不允许该域下的用户请求网络服务，但不影响已经在线的用户。

【举例】

设置当前 ISP 域 test 处于阻塞状态。

```
<Sysname> system-view
[Sysname] domain test
[Sysname-isp-test] state block
```

【相关命令】

- **display domain**

1.2 本地用户配置命令

1.2.1 access-limit

access-limit 命令用来设置使用当前本地用户名接入设备的最大用户数。

undo access-limit 命令用来恢复缺省情况。

【命令】

```
access-limit max-user-number  
undo access-limit
```

【缺省情况】

不限制使用当前本地用户名接入的用户数。

【视图】

本地用户视图

【缺省用户角色】

network-admin

【参数】

max-user-number: 表示使用当前本地用户名接入设备的最大用户数，取值范围为 1~1024。

【使用指导】

本地用户视图下的 **access-limit** 命令只在该用户采用了本地计费方法的情况下生效。

对于网络接入类本地用户，还需要在用户接入的 ISP 域视图下配置 **accounting start-fail offline** 命令，否则使用当前用户名接入的用户数并不受 **access-limit** 命令的限制。

由于 FTP/SFTP/SCP 用户不支持计费，因此 FTP/SFTP/SCP 用户不受此属性限制。

【举例】

允许同时以本地用户名 abc 在线的用户数为 5。

```
<Sysname> system-view  
[Sysname] local-user abc  
[Sysname-luser-manage-abc] access-limit 5
```

【相关命令】

- **accounting start-fail offline**
- **display local-user**

1.2.2 authorization-attribute (Local user view/user group view)

authorization-attribute 命令用来设置本地用户或用户组的授权属性，该属性在本地用户认证通过之后，由设备下发给用户。

undo authorization-attribute 命令用来删除指定的授权属性，恢复用户具有的缺省访问权限。

【命令】

```
authorization-attribute { acl acl-number | idle-cut minutes | ip-pool  
ipv4-pool-name | ipv6-pool ipv6-pool-name | session-timeout minutes |  
user-profile profile-name | user-role role-name | vlan vlan-id |  
work-directory directory-name } *  
  
undo authorization-attribute { acl | idle-cut | ip-pool | ipv6-pool |  
session-timeout | user-profile | user-role role-name | vlan | work-directory }  
*
```

【缺省情况】

授权 FTP/SFTP/SCP 用户可以访问的目录为设备的根目录，但无访问权限。

由用户角色为 **network-admin** 或 **level-15** 的用户创建的本地用户被授权用户角色 **network-operator**。

【视图】

本地用户视图

用户组视图

【缺省用户角色】

network-admin

【参数】

acl acl-number: 指定本地用户的授权 ACL。其中，*acl-number* 为授权 ACL 的编号，取值范围为 2000～4999。与授权 ACL 规则匹配的流量，将按照规则中指定的 **permit** 或 **deny** 动作进行处理。

idle-cut minutes: 设置本地用户的闲置切断时间。其中，*minutes* 为设定的闲置切断时间，取值范围为 1～120，单位为分钟。如果用户在线后连续闲置的时长超过该值，设备会强制该用户下线。

ip-pool ipv4-pool-name: 指定本地用户的 IPv4 地址池信息。本地用户认证成功后，将允许使用该 IPv4 地址池分配地址。其中，*ipv4-pool-name* 表示地址池名称，为 1～63 个字符的字符串，不区分大小写。

ipv6-pool ipv6-pool-name: 指定本地用户的 IPv6 地址池信息。本地用户认证成功后，将允许使用该 IPv6 地址池分配地址。其中，*ipv6-pool-name* 表示地址池名称，为 1～63 个字符的字符串，不区分大小写。

session-timeout minutes: 设置本地用户的会话超时时间。其中，*minutes* 为设定的会话超时时间，取值范围为 1～1440，单位为分钟。如果用户在线时长超过该值，设备会强制该用户下线。

user-profile profile-name: 指定本地用户的授权 User Profile。其中，*profile-name* 表示 User Profile 名称，为 1～31 个字符的字符串，只能包含英文字母、数字、下划线，区分大小写。当用户认证成功后，其访问行为将受到 User Profile 中的预配置的限制。关于 User Profile 的详细介绍请参见“安全配置指导”中的“User Profile”。

user-role role-name: 指定本地用户的授权用户角色。其中，*role-name* 表示用户角色名称，为 1～63 个字符的字符串，区分大小写。可以为每个用户最多指定 64 个用户角色。本地用户角色的相关命令请参见“基础命令参考”中的“RBAC”。该授权属性只能在本地用户视图下配置，不能在本地用户组视图下配置。

vlan *vlan-id*: 指定本地用户的授权 VLAN。其中, *vlan-id* 为 VLAN 编号, 取值范围为 1~4094。本地用户认证成功后, 将被授权仅可以访问指定 VLAN 内的网络资源。

work-directory *directory-name*: 授权 FTP/SFTP/SCP 用户可以访问的目录。其中, *directory-name* 表示 FTP/SFTP/SCP 用户可以访问的目录, 为 1~255 个字符的字符串, 不区分大小写, 且该目录必须已经存在。

【使用指导】

可配置的授权属性都有其明确的使用环境和用途, 请针对用户的服务类型配置对应的授权属性:

- 对于 Portal 用户, 仅授权属性 **ip-pool**、**ipv6-pool**、**session-timeout**、**user-profile**、**acl** 有效。
- 对于 Lan-access 用户, 仅授权属性 **acl**、**session-timeout**、**user-profile**、**vlan** 有效。
- 对于 Telnet、Terminal、SSH 用户, 仅授权属性 **idle-cut**、**user-role** 有效。
- 对于 http、https 用户, 仅授权属性 **user-role** 有效。
- 对于 FTP 用户, 仅授权属性 **user-role**、**work-directory** 有效。
- 对于其它类型的本地用户, 所有授权属性均无效。

用户组的授权属性对于组内的所有本地用户生效, 因此具有相同属性的用户可通过加入相同的用户组来统一配置和管理。

本地用户视图下未配置的授权属性继承所属用户组的授权属性配置, 但是如果本地用户视图与所属的用户组视图下都配置了某授权属性, 则本地用户视图下的授权属性生效。

授权给 Portal 用户的 ACL 中不能配置携带用户源 IP 地址和源 MAC 地址信息的规则, 否则会导致用户上线失败。

在多台设备组成 IRF 的环境下, 为了避免 IRF 系统进行主从倒换后 FTP/SFTP/SCP 用户无法正常登录, 建议用户在指定工作目录时不要携带 slot 信息。

为确保本地用户仅使用本命令指定的授权用户角色, 请先使用 **undo authorization-attribute user-role** 命令删除该用户已有的缺省用户角色。

被授权安全日志管理员的本地用户登录设备后, 仅可执行安全日志文件管理相关的命令以及安全日志文件操作相关的命令, 具体命令可通过 **display role name security-audit** 命令查看。安全日志文件管理相关命令的介绍, 请参见“网络管理与监控”中的“信息中心”。文件系统管理相关命令的介绍, 请参见“基础配置命令参考”中的“文件系统管理”。

为本地用户授权安全日志管理员角色时, 需要注意的是:

- 安全日志管理员角色和其它用户角色互斥:
 - 为一个用户授权安全日志管理员角色时, 系统会通过提示信息请求确认是否删除当前用户的所有其它他用户角色;
 - 如果已经授权当前用户安全日志管理员角色, 再授权其它的用户角色时, 系统会通过提示信息请求确认是否删除当前用户的安全日志管理员角色。
- 系统中的最后一个安全日志管理员角色的本地用户不可被删除。

【举例】

配置网络接入类本地用户 abc 的授权 VLAN 为 VLAN 2。

```
<Sysname> system-view
[Sysname] local-user abc class network
```

```
[Sysname-luser-network-abc] authorization-attribute vlan 2
# 配置用户组 abc 的授权 VLAN 为 VLAN 3。
<Sysname> system-view
[Sysname] user-group abc
[Sysname-ugroup-abc] authorization-attribute vlan 3
# 配置设备管理类本地用户 xyz 的授权用户角色为 security-audit（安全日志管理员）。
<Sysname> system-view
[Sysname] local-user xyz class manage
[Sysname-luser-manage-xyz] authorization-attribute user-role security-audit
This operation will delete all other roles of the user. Are you sure? [Y/N]:y
```

【相关命令】

- **display local-user**
- **display user-group**

1.2.3 bind-attribute

bind-attribute 命令用来设置用户的绑定属性。

undo bind-attribute 命令用来删除指定的用户绑定属性。

【命令】

```
bind-attribute { ip ip-address | location interface interface-type
interface-number | mac mac-address | vlan vlan-id } *
undo bind-attribute { ip | location | mac | vlan } *
```

【缺省情况】

未设置用户的绑定属性。

【视图】

本地用户视图

【缺省用户角色】

network-admin

【参数】

ip *ip-address*: 指定用户的 IP 地址。该绑定属性仅适用于 lan-access 类型中的 802.1X 用户。

location interface *interface-type interface-number*: 指定用户绑定的接口。其中 *interface-type interface-number* 表示接口类型和接口编号。如果用户接入的接口与此处绑定的接口不一致，则认证失败。该绑定属性仅适用于 lan-access、Portal 类型的用户。

mac *mac-address*: 指定用户的 MAC 地址。其中，*mac-address* 为 H-H-H 格式。该绑定属性仅适用于 lan-access、Portal 类型的用户。

vlan *vlan-id*: 指定用户所属于的 VLAN。其中，*vlan-id* 为 VLAN 编号，取值范围为 1~4094。该绑定属性仅适用于 lan-access、Portal 类型的用户。

【使用指导】

设备对用户进行本地认证时，会检查用户的实际属性与配置的绑定属性是否一致，如果不一致或用户未携带该绑定属性则认证失败。

绑定属性的检测不区分用户的接入服务类型，因此在配置绑定属性时要考虑某接入类型的用户是否需要绑定某些属性。例如，只有支持 IP 地址上传功能的 802.1X 认证用户才可以配置绑定 IP 地址；对于不支持 IP 地址上传功能的 MAC 地址认证用户，如果配置了绑定 IP 地址，则会导致该用户的本地认证失败。

在绑定接口属性时要考虑绑定接口类型是否合理。对于不同接入类型的用户，请按照如下方式进行绑定接口属性的配置：

- 802.1X 用户：配置绑定的接口为开启 802.1X 的二层以太网接口。
- MAC 地址认证用户：配置绑定的接口为开启 MAC 地址认证的二层以太网接口。
- Web 认证用户：配置绑定的接口为开启 Web 认证的二层以太网接口。
- Portal 用户：若使能 Portal 的接口为 VLAN 接口，且没有通过 **portal roaming enable** 命令配置 Portal 用户漫游功能，则配置绑定的接口为用户实际接入的二层以太网接口；其它情况下，配置绑定的接口均为使能 Portal 的接口。

【举例】

配置网络接入类本地用户 abc 的绑定 MAC 地址为 11-11-11。

```
<Sysname> system-view
[Sysname] local-user abc class network
[Sysname-luser-network-abc] bind-attribute mac 11-11-11
```

【相关命令】

- **display local-user**

1.2.4 description

description 命令用来配置网络接入类本地用户的描述信息。

undo description 命令用来恢复缺省情况。

【命令】

```
description text
undo description
```

【缺省情况】

未配置网络接入类本地用户的描述信息。

【视图】

网络接入类本地用户视图

【缺省用户角色】

network-admin

【参数】

text：用户的描述信息，为 1~255 个字符的字符串，区分大小写。

【举例】

配置网络接入类本地用户 123 的描述信息为 Manager of MSC company。

```
<Sysname> system-view
[Sysname] local-user 123 class network
```


[Sysname-luser-network-123] description Manager of MSC company

【相关命令】

- **display local-user**

1.2.5 display local-user

display local-user 命令用来显示本地用户的配置信息和在线用户数的统计信息。

【命令】

```
display local-user [ class { manage | network } | idle-cut { disable | enable }  
| service-type { ftp | http | https | lan-access | portal | ssh | telnet |  
terminal } | state { active | block } | user-name user-name class { manage |  
network } | vlan vlan-id ]
```

【视图】

任意视图

【缺省用户角色】

network-admin
network-operator

【参数】

class: 显示指定用户类别的本地用户信息。

manage: 设备管理类用户。

network: 网络接入类用户。

idle-cut { disable | enable }: 显示开启或关闭闲置切断功能的本地用户信息。其中，**disable** 表示未启用闲置切断功能的本地用户；**enable** 表示启用了闲置切断功能并配置了闲置切断时间的本地用户。

service-type: 显示指定用户类型的本地用户信息。

- **ftp:** FTP 用户。
- **http:** HTTP 用户。
- **https:** HTTPS 用户。
- **lan-access:** lan-access 类型用户（主要指以太网接入用户，比如 802.1X 用户）。
- **portal:** Portal 用户。
- **ssh:** SSH 用户。
- **telnet:** Telnet 用户。
- **terminal:** 从 Console 口登录的终端用户。

state { active | block }: 显示处于指定状态的本地用户信息。其中，**active** 表示用户处于活动状态，即系统允许该用户请求网络服务；**block** 表示用户处于阻塞状态，即系统不允许用户请求网络服务。

user-name user-name: 显示指定用户名的本地用户信息。其中，*user-name* 表示本地用户名，为 1~55 个字符的字符串，区分大小写，不能携带域名，不能包括符号“\”、“|”、“/”、“:”、“*”、“?”、“<”、“>”和“@”，且不能为“a”、“al”或“all”。

vlan vlan-id: 显示指定 VLAN 内的所有本地用户信息。其中, *vlan-id* 为 VLAN 编号, 取值范围为 1~4094。

【使用指导】

如果不指定任何参数, 则显示所有本地用户信息。

【举例】

显示所有本地用户的相关信息。

```
<Sysname> display local-user
```

```
Device management user root:
```

```
State: Active
Service type: SSH/Telnet/Terminal
Access limit: Enabled Max access number: 3
Current access number: 1
User group: system
Bind attributes:
Authorization attributes:
  Work directory: flash:
  User role list: network-admin
Password control configurations:
  Password aging: 3 days
```

```
Network access user jj:
```

```
State: Active
Service type: LAN-access
User group: system
Bind attributes:
  IP address: 2.2.2.2
  Location bound: GigabitEthernet1/0/1
  MAC address: 0001-0001-0001
  VLAN ID: 2
Authorization attributes:
  Idle timeout: 33 minutes
  Work directory: flash:
  ACL number: 2000
  User profile: pp
  User role list: network-operator, level-0, level-3
Description: A network access user from company cc
Validity period:
  Start date and time: 2016/01/01-00:01:01
  Expiration date and time: 2017/01/01-01:01:01
```

```
Total 2 local users matched.
```

表1-2 display local-user 命令显示信息描述表

字段	描述
State	本地用户状态 <ul style="list-style-type: none"> • Active: 活动状态 • Block: 阻塞状态
Service type	本地用户使用的服务类型
Access limit	是否对使用该用户名的接入用户数进行限制
Max access number	最大接入用户数
Current access number	使用该用户名的当前接入用户数
User group	本地用户所属的用户组
Bind attributes	本地用户的绑定属性
IP address	本地用户的IP地址
Location bound	本地用户绑定的端口
MAC address	本地用户的MAC地址
VLAN ID	本地用户绑定的VLAN
Authorization attributes	本地用户的授权属性
Idle timeout	本地用户闲置切断时间（单位为分钟）
Session-timeout	本地用户的会话超时时间（单位为分钟）
Work directory	FTP/SFTP/SCP用户可以访问的目录
ACL number	本地用户授权ACL
VLAN ID	本地用户授权VLAN
User profile	本地用户授权User Profile
User role list	本地用户的授权用户角色列表
IP pool	本地用户的授权IPv4地址池
IPv6 pool	本地用户的授权IPv6地址池
Password control configurations	本地用户的密码控制属性
Password aging	密码老化时间
Password length	密码最小长度
Password composition	密码组合策略（密码元素的组合类型、至少要包含每种元素的个数）
Password complexity	密码复杂度检查策略（是否包含用户名或者颠倒的用户名；是否包含三个或以上相同字符）
Maximum login attempts	用户最大登录尝试次数
Action for exceeding login attempts	登录尝试次数达到设定次数后的用户帐户锁定行为
Description	网络接入类本地用户的描述信息

字段	描述
Validity period	网络接入类本地用户有效期
Start date and time	网络接入类本地用户开始生效的日期和时间
Expiration date and time	网络接入类本地用户的失效日期和时间
Total x local users matched.	总计有x个本地用户匹配

1.2.6 display user-group

display user-group 命令用来显示用户组的配置信息。

【命令】

```
display user-group { all | name group-name }
```

【视图】

任意视图

【缺省用户角色】

network-admin
network-operator

【参数】

all: 显示所有用户组的配置信息。

name group-name: 显示指定用户组的配置。*group-name* 表示用户组名称，为 1~32 个字符的字符串，不区分大小写。

【举例】

显示所有用户组的相关配置。

```
<Sysname> display user-group all
Total 2 user groups matched.
```

```
User group: system
  Authorization attributes:
    Work directory:      flash:
User group: jj
  Authorization attributes:
    Idle timeout:        2 minutes
    Work directory:      flash:/
    ACL number:          2000
    VLAN ID:             2
    User profile:         pp
  Password control configurations:
    Password aging:      2 days
```

表1-3 display user-group 命令显示信息描述表

字段	描述
Total 2 user groups matched.	总计有2个用户组匹配
User group	用户组名称
Authorization attributes	授权属性信息
Idle timeout	闲置切断时间（单位：分钟）
Session-timeout	会话超时时间（单位：分钟）
Work directory	FTP/SFTP/SCP用户可以访问的目录
ACL number	授权ACL号
VLAN ID	授权VLAN ID
User profile	授权User Profile名称
IP pool	授权IPv4地址池
IPv6 pool	授权IPv6地址池
Password control configurations	用户组的密码控制属性
Password aging	密码老化时间
Password length	密码最小长度
Password composition	密码组合策略（密码元素的组合类型、至少要包含每种元素的个数）
Password complexity	密码复杂度检查策略（是否包含用户名或者颠倒的用户名；是否包含三个或以上相同字符）
Maximum login attempts	用户最大登录尝试次数
Action for exceeding login attempts	登录尝试次数达到设定次数后的用户帐户锁定行为

1.2.7 group

group 命令用来设置本地用户所属的用户组。

undo group 命令用来恢复缺省配置。

【命令】

group *group-name*

undo group

【缺省情况】

本地用户属于用户组 **system**。

【视图】

本地用户视图

【缺省用户角色】

network-admin

【参数】

group-name: 用户组名称，为 1~32 个字符的字符串，不区分大小写。

【举例】

设置设备管理类本地用户 111 所属的用户组为 abc。

```
<Sysname> system-view
[Sysname] local-user 111 class manage
[Sysname-luser-manage-111] group abc
```

【相关命令】

- **display local-user**

1.2.8 local-user

local-user 命令用来添加本地用户，并进入本地用户视图。如果指定的本地用户已经存在，则直接进入本地用户视图。

undo local-user 命令用来删除指定的本地用户。

【命令】

```
local-user user-name [ class { manage | network } ]
undo local-user { user-name class { manage | network } | all [ service-type
{ ftp | http | https | lan-access | portal | ssh | telnet | terminal } | class
{ manage | network } ] }
```

【缺省情况】

不存在本地用户。

【视图】

系统视图

【缺省用户角色】

network-admin

【参数】

user-name: 表示本地用户名，为 1~55 个字符的字符串，区分大小写。用户名不能携带域名，不能包括符号“\”、“|”、“/”、“:”、“*”、“?”、“<”、“>”和“@”，且不能为“a”、“al”或“all”。

class: 指定本地用户的类别。若不指定本参数，则表示设备管理类用户。

manage: 设备管理类用户，用于登录设备，对设备进行配置和监控。此类用户可以提供 **ftp**、**http**、**https**、**telnet**、**ssh**、**terminal** 服务。

network: 网络接入类用户，用于通过设备接入网络，访问网络资源。此类用户可以提供 **lan-access** 和 **portal** 服务。

all: 所有的用户。

service-type: 指定用户的类型。

- **ftp**: 表示 FTP 类型用户。
- **http**: 表示 HTTP 类型用户。
- **https**: 表示 HTTPS 类型用户。
- **lan-access**: 表示 lan-access 类型用户（主要指以太网接入用户，比如 802.1X 用户）。
- **portal**: 表示 Portal 用户。
- **ssh**: 表示 SSH 用户。
- **telnet**: 表示 Telnet 用户。
- **terminal**: 表示从 Console 口登录的终端用户。

【举例】

添加名称为 **user1** 的设备管理类本地用户。

```
<Sysname> system-view
[Sysname] local-user user1 class manage
[Sysname-luser-manage-user1]
```

添加名称为 **user2** 的网络接入类本地用户。

```
<Sysname> system-view
[Sysname] local-user user2 class network
[Sysname-luser-network-user2]
```

【相关命令】

- **display local-user**
- **service-type**

1.2.9 local-user auto-delete enable

local-user auto-delete enable 命令用来开启本地用户过期自动删除功能。

undo local-user auto-delete enable 命令用来恢复缺省情况。

【命令】

```
local-user auto-delete enable
undo local-user auto-delete enable
```

【缺省情况】

本地用户过期自动删除功能处于关闭状态。

【视图】

系统视图

【缺省用户角色】

network-admin

【使用指导】

本地用户过期自动删除功能处于开启状态时，设备将定时（10 分钟，不可配）检查网络接入类本地用户是否过期并自动删除过期的本地用户。

【举例】

开启本地用户过期自动删除功能。

```
<Sysname> system-view
[Sysname] local-user auto-delete enable
```

【相关命令】

- **validity-datetime**

1.2.10 password (Device management user view)

password 命令用来设置本地用户的密码。

undo password 命令用来恢复缺省情况。

【命令】

非 FIPS 模式下：

```
password [ { hash | simple } string ]
```

```
undo password
```

FIPS 模式下：

```
password
```

【缺省情况】

非 FIPS 模式下：

不存在本地用户密码，即本地用户认证时无需输入密码，只要用户名有效且其它属性验证通过即可认证成功。

FIPS 模式下：

不存在本地用户密码，但本地用户认证时不能成功。

【视图】

设备管理类本地用户视图

【缺省用户角色】

network-admin

【参数】

hash：表示以哈希方式设置密码。

simple：表示以明文方式设置密码，该密码将以密文形式存储。

string：密码字符串，区分大小写。非 FIPS 模式下，明文密码为 1~63 个字符的字符串；哈希密码为 1~110 个字符的字符串。FIPS 模式下，明文密码为 15~63 个字符的字符串，密码元素的最少组合类型为 4（必须包括数字、大写字母、小写字母以及特殊字符）。

【使用指导】

如果不指定任何参数，则表示以交互式设置明文形式的密码。

在非 FIPS 模式下，可以不为本地用户设置密码。若不为本地用户设置密码，则该用户认证时无需输入密码，只要用户名有效且其它属性验证通过即可认证成功。为提高用户帐户的安全性，建议设置本地用户密码。

在 FIPS 模式下，必须且只能通过交互式方式设置明文密码，否则用户的本地认证不能成功。

【举例】

设置设备管理类本地用户 **user1** 的密码为明文 123456TESTplat&!

```
<Sysname> system-view
[Sysname] local-user user1 class manage
[Sysname-luser-manage-user1] password simple 123456TESTplat&!
```

以交互式方式设置设备管理类本地用户 **test** 的密码。

```
<Sysname> system-view
[Sysname] local-user test class manage
[Sysname-luser-manage-test] password
Password:
confirm :
```

【相关命令】

- **display local-user**

1.2.11 password (Network access user view)

password 命令用来设置本地用户的密码。

undo password 命令用来恢复缺省情况。

【命令】

```
password { cipher | simple } string
undo password
```

【缺省情况】

不存在本地用户密码，即本地用户认证时无需输入密码，只要用户名有效且其它属性验证通过即可认证成功。

【视图】

网络接入类本地用户视图

【缺省用户角色】

network-admin

【参数】

cipher: 表示以密文方式设置密码。

simple: 表示以明文方式设置密码，该密码将以密文形式存储。

string: 密码字符串，区分大小写。明文密码为 1~63 个字符的字符串；密文密码为 1~117 个字符的字符串。

【使用指导】

为提高用户帐户的安全性，建议设置本地用户密码。

【举例】

设置网络接入类本地用户 **user1** 的密码为明文 123456TESTuser&!

```
<Sysname> system-view
[Sysname] local-user user1 class network
[Sysname-luser-network-user1] password simple 123456TESTuser&!
```

【相关命令】

- `display local-user`

1.2.12 service-type

service-type 命令用来设置用户可以使用的服务类型。

undo service-type 命令用来删除用户可以使用的服务类型。

【命令】

非 FIPS 模式下：

```
service-type { ftp | lan-access | { http | https | ssh | telnet | terminal }  
* | portal }  
undo service-type { ftp | lan-access | { http | https | ssh | telnet | terminal }  
* | portal }
```

FIPS 模式下：

```
service-type { lan-access | { https | ssh | terminal } * | portal }  
undo service-type { lan-access | { https | ssh | terminal } * | portal }
```

【缺省情况】

系统不对用户授权任何服务，即用户不能使用任何服务。

【视图】

本地用户视图

【缺省用户角色】

network-admin

【参数】

ftp：指定用户可以使用 FTP 服务。若授权 FTP 服务，授权目录可以通过 **authorization-attribute work-directory** 命令来设置。

http：指定用户可以使用 HTTP 服务。

https：指定用户可以使用 HTTPS 服务。

lan-access：指定用户可以使用 lan-access 服务。主要指以太网接入，比如用户可以通过 802.1X 认证接入。

ssh：指定用户可以使用 SSH 服务。

telnet：指定用户可以使用 Telnet 服务。

terminal：指定用户可以使用 terminal 服务（即从 Console 口登录）。

portal：指定用户可以使用 Portal 服务。

【使用指导】

可以通过多次执行本命令，设置用户可以使用多种服务类型。

【举例】

指定设备管理类用户可以使用 Telnet 服务和 FTP 服务。

```
<Sysname> system-view
```

```
[Sysname] local-user user1 class manage
[Sysname-luser-manage-user1] service-type telnet
[Sysname-luser-manage-user1] service-type ftp
```

【相关命令】

- **display local-user**

1.2.13 state (Local user view)

state 命令用来设置当前本地用户的状态。

undo state 命令用来恢复缺省情况。

【命令】

```
state { active | block }
undo state
```

【缺省情况】

本地用户处于活动状态。

【视图】

本地用户视图

【缺省用户角色】

network-admin

【参数】

active: 指定当前本地用户处于活动状态，即系统允许当前本地用户请求网络服务。

block: 指定当前本地用户处于“阻塞”状态，即系统不允许当前本地用户请求网络服务。

【举例】

设置设备管理类本地用户 **user1** 处于“阻塞”状态。

```
<Sysname> system-view
[Sysname] local-user user1 class manage
[Sysname-luser-manage-user1] state block
```

【相关命令】

- **display local-user**

1.2.14 user-group

user-group 命令用来创建用户组，并进入用户组视图。如果指定的用户组已经存在，则直接进入用户组视图。

undo user-group 命令用来删除指定的用户组。

【命令】

```
user-group group-name
undo user-group group-name
```

【缺省情况】

存在一个用户组，名称为 **system**。

【视图】

系统视图

【缺省用户角色】

network-admin

【参数】

group-name：用户组名称，为 1～32 个字符的字符串，不区分大小写。

【使用指导】

用户组是一个本地用户的集合，某些需要集中管理的属性可在用户组中统一配置和管理。

不允许删除一个包含本地用户的用户组。

不能删除系统中存在的默认用户组 **system**，但可以修改该用户组的配置。

【举例】

创建名称为 **abc** 的用户组并进入其视图。

```
<Sysname> system-view
[Sysname] user-group abc
[Sysname-ugroup-abc]
```

【相关命令】

- **display user-group**

1.2.15 validity-datetime

validity-datetime 命令用来配置网络接入类本地用户的有效期。

undo validity-datetime 命令用来恢复缺省情况。

【命令】

```
validity-datetime { from start-date start-time to expiration-date
expiration-time | from start-date start-time | to expiration-date
expiration-time }
undo validity-datetime
```

【缺省情况】

未限制本地用户的有效期，该用户始终有效。

【视图】

网络接入类本地用户视图

【缺省用户角色】

network-admin

【参数】

from: 指定用户有效期的开始日期和时间。若不指定该参数，则表示仅限定用户有效期的结束日期和时间。

start-date: 用户有效期的开始日期，格式为 MM/DD/YYYY（月/日/年）或者 YYYY/MM/DD（年/月/日），MM 的取值范围为 1~12，DD 的取值范围与月份有关，YYYY 的取值范围为 2000~2035。

start-time: 用户有效期的开始时间，格式为 HH:MM:SS（小时:分钟:秒），HH 取值范围为 0~23，MM 和 SS 取值范围为 0~59。如果要设置成整分，则可以不输入秒；如果要设置成整点，则可以不输入分和秒。比如将 *start-time* 参数设置为 0 表示零点。

to: 指定用户有效期的结束日期和结束时间。若不指定该参数，则表示仅限定用户有效期的开始日期和时间。

expiration-date: 用户有效期的结束日期，格式为 MM/DD/YYYY（月/日/年）或者 YYYY/MM/DD（年/月/日），MM 的取值范围为 1~12，DD 的取值范围与月份有关，YYYY 的取值范围为 2000~2035。

expiration-time: 用户有效期的结束时间，格式为 HH:MM:SS（小时:分钟:秒），HH 取值范围为 0~23，MM 和 SS 取值范围为 0~59。如果要设置成整分，则可以不输入秒；如果要设置成整点，则可以不输入分和秒。比如将 *expiration-time* 参数设置为 0 表示零点。

【使用指导】

网络接入类本地用户在有效期内才能认证成功。

若同时指定了有效期的开始时间和结束时间，则有效期的结束时间必须晚于起始时间。

如果仅指定了有效期的开始时间，则表示该时间到达后，用户一直有效。

如果仅指定了有效期的结束时间，则表示该时间到达前，用户一直有效。

【举例】

配置网络接入类本地用户 123 的有效期为 2015/10/01 00:00:00 到 2016/10/02 12:00:00。

```
<Sysname> system-view
[Sysname] local-user 123 class network
[Sysname-luser-network-123] validity-datetime from 2015/10/01 00:00:00 to 2016/10/02
12:00:00
```

【相关命令】

- **display local-user**

1.3 RADIUS配置命令

1.3.1 aaa device-id

aaa device-id 命令用来配置设备 ID。

undo aaa device-id 命令用来恢复缺省情况。

【命令】

```
aaa device-id device-id
undo aaa device-id
```

【缺省情况】

设备 ID 为 0。

【视图】

系统视图

【缺省用户角色】

network-admin

【参数】

device-id: 设备 ID，取值范围为 1~255。

【使用指导】

RADIUS 计费过程使用 *Acct-Session-Id* 属性作为用户的计费 ID。设备使用系统时间、随机数以及设备 ID 为每个在线用户生成一个唯一的 *Acct-Session-Id* 值。

修改后的设备 ID 仅对新上线用户生效。

【举例】

```
# 配置设备 ID 为 1。
<Sysname> system-view
[Sysname] aaa device-id 1
```

1.3.2 accounting-on enable

accounting-on enable 命令用来开启 accounting-on 功能。

undo accounting-on enable 命令用来关闭 accounting-on 功能。

【命令】

```
accounting-on enable [ interval interval | send send-times ] *
undo accounting-on enable
```

【缺省情况】

accounting-on 功能处于关闭状态。

【视图】

RADIUS 方案视图

【缺省用户角色】

network-admin

【参数】

interval interval: 指定 accounting-on 报文重发时间间隔，取值范围为 1~15，单位为秒，缺省值为 3。

send send-times: 指定 accounting-on 报文的最大发送次数，取值范围为 1~255，缺省值为 50。

【使用指导】

accounting-on 功能使得整个设备在重启之后通过发送 accounting-on 报文通知该方案所使用的 RADIUS 计费服务器，要求 RADIUS 服务器停止计费且强制该设备的用户下线。

开启 **accounting-on** 功能后，请执行 **save** 命令保证 **accounting-on** 功能在整个设备下次重启后生效。关于命令的详细介绍请参见“基础配置命令参考”中的“配置文件管理”。

本命令设置的 **accounting-on** 参数会立即生效。

【举例】

在 RADIUS 方案 **radius1** 中，开启 **accounting-on** 功能并配置 **accounting-on** 报文重发时间间隔为 5 秒、**accounting-on** 报文的最大发送次数为 15 次。

```
<Sysname> system-view
[Sysname] radius scheme radius1
[Sysname-radius-radius1] accounting-on enable interval 5 send 15
```

【相关命令】

- **display radius scheme**

1.3.3 accounting-on extended

accounting-on extended 命令用来开启 **accounting-on** 扩展功能。

undo accounting-on extended 命令用来关闭 **accounting-on** 扩展功能。

【命令】

```
accounting-on extended
undo accounting-on extended
```

【缺省情况】

accounting-on 扩展功能处于关闭状态。

【视图】

RADIUS 方案视图

【缺省用户角色】

```
network-admin
network-operator
```

【使用指导】

accounting-on 扩展功能是为了适应分布式架构而对 **accounting-on** 功能的增强。只有在 **accounting-on** 功能开启的情况下，**accounting-on** 扩展功能才能生效。

accounting-on 扩展功能适用于 **lan-access** 用户，该类型的用户数据均保存在用户接入的成员设备上。开启 **accounting-on** 扩展功能后，当有用户发起接入认证的成员设备重启时，设备会向 RADIUS 服务器发送携带成员设备标识的 **accounting-on** 报文，用于通知 RADIUS 服务器对该成员设备的用户停止计费且强制用户下线。**accounting-on** 报文的重发间隔时间以及最大发送次数由 **accounting-on enable** 命令指定。如果自上一次重启之后，成员设备上没有用户接入认证的记录，则该成员设备再次重启，并不会触发设备向 RADIUS 服务器发送携带成员设备标识的 **accounting-on** 报文。

开启 **accounting-on** 扩展功能后，请执行 **save** 命令保证 **accounting-on** 扩展功能在成员设备下次重启后生效。关于 **save** 命令的详细介绍请参见“基础配置命令参考”中的“配置文件管理”。

【举例】

在 RADIUS 方案 radius1 中，开启 accounting-on 扩展功能。

```
<Sysname> system-view
[Sysname] radius scheme radius1
[Sysname-radius-radius1] accounting-on extended
```

【相关命令】

- **accounting-on enable**
- **display radius scheme**

1.3.4 attribute 15 check-mode

attribute 15 check-mode 命令用来配置对 RADIUS Attribute 15 的检查方式。

undo attribute 15 check-mode 命令用来恢复缺省情况。

【命令】

```
attribute 15 check-mode { loose | strict }
undo attribute 15 check-mode
```

【缺省情况】

对 RADIUS Attribute 15 的检查方式为 **strict** 方式。

【视图】

RADIUS 方案视图

【缺省用户角色】

network-admin

【参数】

loose: 松散检查方式，设备使用 RADIUS Attribute 15 的标准属性值对用户业务类型进行检查。对于 SSH、FTP、Terminal 用户，在 RADIUS 服务器下发的 Login-Service 属性值为 0（表示用户业务类型为 Telnet）时才，这类用户才能够通过认证。

strict: 严格检查方式，设备使用 RADIUS Attribute 15 的标准属性值以及扩展属性值对用户业务类型进行检查。对于 SSH、FTP、Terminal 用户，当 RADIUS 服务器下发的 Login-Service 属性值为对应的扩展取值时，这类用户才能够通过认证。

【使用指导】

由于某些 RADIUS 服务器不支持自定义的属性，无法下发扩展的 Login-Service 属性，若要使用这类 RADIUS 服务器对 SSH、FTP、Terminal 用户进行认证，建议设备上对 RADIUS 15 号属性值采用松散检查方式。

【举例】

在 RADIUS 方案 radius1 中，配置对 RADIUS Attribute 15 采用松散检查方式。

```
<Sysname> system-view
[Sysname] radius scheme radius1
[Sysname-radius-radius1] attribute 15 check-mode loose
```


【相关命令】

- `display radius scheme`

1.3.5 attribute 25 car

`attribute 25 car` 命令用来开启 RADIUS Attribute 25 的 CAR 参数解析功能。

`undo attribute 25 car` 命令用来关闭 RADIUS Attribute 25 的 CAR 参数解析功能。

【命令】

```
attribute 25 car
undo attribute 25 car
```

【缺省情况】

RADIUS Attribute 25 的 CAR 参数解析功能处于关闭状态。

【视图】

RADIUS 方案视图

【缺省用户角色】

network-admin

【使用指导】

RADIUS 的 25 号属性为 class 属性，该属性由 RADIUS 服务器下发给设备。目前，某些 RADIUS 服务器利用 class 属性来对用户下发 CAR 参数，可以通过本特性来控制设备是否将 RADIUS 25 号属性解析为 CAR 参数，解析出的 CAR 参数可被用来进行基于用户的流量监管控制。

【举例】

在 RADIUS 方案 radius1 中，开启 RADIUS Attribute 25 的 CAR 参数解析功能。

```
<Sysname> system-view
[Sysname] radius scheme radius1
[Sysname-radius-radius1] attribute 25 car
```

【相关命令】

- `display radius scheme`

1.3.6 attribute 31 mac-format

`attribute 31 mac-format` 命令用来配置 RADIUS Attribute 31 中的 MAC 地址格式。

`undo attribute 31 mac-format` 命令用来恢复缺省情况。

【命令】

```
attribute 31 mac-format section { six | three } separator separator-character
{ lowercase | uppercase }
undo attribute 31 mac-format
```

【缺省情况】

RADIUS Attribute 31 中的 MAC 地址为大写字母格式，且被分隔符“-”分成 6 段，即为 HH-HH-HH-HH-HH-HH 的格式。

【视图】

RADIUS 方案视图

【缺省用户角色】

network-admin

【参数】

section: 指定 MAC 地址分段数。

six: 表示 MAC 地址被分为 6 段，格式为 HH-HH-HH-HH-HH-HH。

three: 表示 MAC 地址被分为 3 段，格式为 HHHH-HHHH-HHHH。

separator separator-character: MAC 地址的分隔符，为单个字符，区分大小写。

lowercase: 表示 MAC 地址为小写字母格式。

uppercase: 表示 MAC 地址为大写字母格式。

【使用指导】

不同的 RADIUS 服务器对填充在 RADIUS Attribute 31 中的 MAC 地址有不同的格式要求，为了保证 RADIUS 报文的正常交互，设备发送给服务器的 RADIUS Attribute 31 号属性中 MAC 地址的格式必须与服务器的要求保持一致。

【举例】

在 RADIUS 方案 radius1 中，配置 RADIUS Attribute 31 的 MAC 地址格式为 hh:hh:hh:hh:hh:hh。

```
<Sysname> system-view
```

```
[Sysname] radius scheme radius1
```

```
[Sysname-radius-radius1] attribute 31 mac-format section six separator : lowercase
```

【相关命令】

- **display radius scheme**

1.3.7 attribute convert (RADIUS DAE server view)

attribute convert 命令用来配置 RADIUS 属性转换规则。

undo attribute convert 命令用来删除 RADIUS 属性转换规则。

【命令】

```
attribute convert src-attr-name to dest-attr-name { { coa-ack | coa-request }  
* | { received | sent } * }
```

```
undo attribute convert [ src-attr-name ]
```

【缺省情况】

不存在 RADIUS 属性转换规则，系统按照标准 RADIUS 协议对 RADIUS 属性进行处理。

【视图】

RADIUS DAE 服务器视图

【缺省用户角色】

network-admin

【参数】

src-attr-name: 源属性名称, 为 1~63 个字符的字符串, 不区分大小写。该属性必须为系统支持的属性。

dest-attr-name: 目的属性名称, 为 1~63 个字符的字符串, 不区分大小写。该属性必须为系统支持的属性。

coa-ack: COA 应答报文。

coa-request: COA 请求报文。

received: 接收到的 DAE 报文。

sent: 发送的 DAE 报文。

【使用指导】

RADIUS 属性转换规则中的源属性内容将被按照目的属性的含义来处理。

只有在 RADIUS 属性解释功能开启之后, RADIUS 属性转换规则才能生效。

配置 RADIUS 属性转换规则时, 需要遵循以下原则:

- 源属性内容和目的属性内容的数据类型必须相同。
- 源属性和目的属性的名称不能相同。
- 一个属性只能按照一种方式(按报文类型或报文处理方向)进行转换。
- 一个源属性不能同时转换为多个目的属性。

执行 **undo attribute convert** 命令时, 如果不指定源属性名称, 则表示删除所有 RADIUS 属性转换规则。

【举例】

在 RADIUS DAE 服务器视图下, 配置一条 RADIUS 属性转换规则, 指定将接收到的 DAE 报文中的 Hw-Server-String 属性转换为 H3c-User-Roles 属性。

```
<Sysname> system-view
[Sysname] radius dynamic-author server
[Sysname-radius-da-server] attribute convert Hw-Server-String to H3c-User-Roles received
```

【相关命令】

- **attribute translate**

1.3.8 attribute convert (RADIUS scheme view)

attribute convert 命令用来配置 RADIUS 属性转换规则。

undo attribute convert 命令用来删除 RADIUS 属性转换规则。

【命令】

```
attribute convert src-attr-name to dest-attr-name { { access-accept |
access-request | accounting } * | { received | sent } * }
undo attribute convert [ src-attr-name ]
```

【缺省情况】

不存在 RADIUS 属性转换规则, 系统按照标准 RADIUS 协议对 RADIUS 属性进行处理。

【视图】

RADIUS 方案视图

【缺省用户角色】

network-admin

【参数】

src-attr-name: 源属性名称，为 1~63 个字符的字符串，不区分大小写。该属性必须为系统支持的属性。

dest-attr-name: 目的属性名称，为 1~63 个字符的字符串，不区分大小写。该属性必须为系统支持的属性。

access-accept: RADIUS 认证成功报文。

access-request: RADIUS 认证请求报文。

accounting: RADIUS 计费报文。

received: 接收到的 RADIUS 报文。

sent: 发送的 RADIUS 报文。

【使用指导】

RADIUS 属性转换规则中的源属性内容将被按照目的属性的含义来处理。

只有在 RADIUS 属性解释功能开启之后，RADIUS 属性转换规则才能生效。

配置 RADIUS 属性转换规则时，需要遵循以下原则：

- 源属性内容和目的属性内容的数据类型必须相同。
- 源属性和目的属性的名称不能相同。
- 一个属性只能按照一种方式（按报文类型或报文处理方向）进行转换。
- 一个源属性不能同时转换为多个目的属性。

执行 **undo attribute convert** 命令时，如果不指定源属性名称，则表示删除所有 RADIUS 属性转换规则。

【举例】

在 RADIUS 方案 radius1 中，配置一条 RADIUS 属性转换规则，指定将接收到的 RADIUS 报文中的 Hw-Server-String 属性转换为 H3c-User-Roles 属性。

```
<Sysname> system-view
```

```
[Sysname] radius scheme radius1
```

```
[Sysname-radius-radius1] attribute convert Hw-Server-String to H3c-User-Roles received
```

【相关命令】

- **attribute translate**

1.3.9 attribute reject (RADIUS DAE server view)

attribute reject 命令用来配置 RADIUS 属性禁用。

undo attribute reject 命令用来取消配置的 RADIUS 属性禁用。

【命令】

```
attribute reject attr-name { { coa-ack | coa-request } * | { received | sent } * }
```

undo attribute reject [*attr-name*]

【缺省情况】

不存在 RADIUS 属性禁用规则。

【视图】

RADIUS DAE 服务器视图

【缺省用户角色】

network-admin

【参数】

attr-name: RADIUS 属性名称，为 1~63 个字符的字符串，不区分大小写。该属性必须为系统支持的属性。

coa-ack: COA 应答报文。

coa-request: COA 请求报文。

received: 接收到的 DAE 报文。

sent: 发送的 DAE 报文。

【使用指导】

当设备发送的 RADIUS 报文中携带了 RADIUS 服务器无法识别的属性时，可以定义基于发送方向的属性禁用规则，使得设备发送 RADIUS 报文时，将该属性从报文中删除。

当 RADIUS 服务器发送给设备的某些属性是设备不希望收到的属性时，可以定义基于接收方向的属性禁用规则，使得设备接收 RADIUS 报文时，不处理报文中的该属性。

当某些类型的属性是设备不希望处理的属性时，可以定义基于类型的属性禁用规则。

只有在 RADIUS 属性解释功能开启之后，RADIUS 属性禁用规则才能生效。

一个属性只能按照一种方式（按报文类型或报文处理方向）进行禁用。

执行 **undo attribute reject** 命令时，如果不指定属性名称，则表示删除所有 RADIUS 属性禁用规则。

【举例】

在 RADIUS DAE 服务器视图下，配置一条 RADIUS 属性禁用规则，指定禁用发送的 DAE 报文中的 Connect-Info 属性。

```
<Sysname> system-view
```

```
[Sysname] radius dynamic-author server
```

```
[Sysname-radius-da-server] attribute reject Connect-Info sent
```

【相关命令】

- **attribute translate**

1.3.10 attribute reject (RADIUS scheme view)

attribute reject 命令用来配置 RADIUS 属性禁用规则。

undo attribute reject 命令用来删除 RADIUS 属性禁用规则。

【命令】

```
attribute reject attr-name { { access-accept | access-request | accounting }  
* | { received | sent } * }  
undo attribute reject [ attr-name ]
```

【缺省情况】

不存在 RADIUS 属性禁用规则。

【视图】

RADIUS 方案视图

【缺省用户角色】

network-admin

【参数】

attr-name: RADIUS 属性名称，为 1~63 个字符的字符串，不区分大小写。该属性必须为系统支持的属性。

access-accept: RADIUS 认证成功报文。

access-request: RADIUS 认证请求报文。

accounting: RADIUS 计费报文。

received: 接收到的 RADIUS 报文。

sent: 发送的 RADIUS 报文。

【使用指导】

当设备发送的 RADIUS 报文中携带了 RADIUS 服务器无法识别的属性时，可以定义基于发送方向的属性禁用规则，使得设备发送 RADIUS 报文时，将该属性从报文中删除。

当 RADIUS 服务器发送给设备的某些属性是不希望收到的属性时，可以定义基于接收方向的属性禁用规则，使得设备接收 RADIUS 报文时，不处理报文中的该属性。

当某些类型的属性是设备不希望处理的属性时，可以定义基于类型的属性禁用规则。

只有在 RADIUS 属性解释功能开启之后，RADIUS 属性禁用规则才能生效。

一个属性只能按照一种方式（按报文类型或报文处理方向）进行禁用。

执行 **undo attribute reject** 命令时，如果不指定属性名称，则表示删除所有 RADIUS 属性禁用规则。

【举例】

在 RADIUS 方案 radius1 中，配置一条 RADIUS 属性禁用规则，指定禁用发送的 RADIUS 报文中的 Connect-Info 属性。

```
<Sysname> system-view  
[Sysname] radius scheme radius1  
[Sysname-radius-radius1] attribute reject Connect-Info sent
```

【相关命令】

- **attribute translate**

1.3.11 attribute remanent-volume

attribute remanent-volume 命令用来配置 RADIUS Remanent-Volume 属性的流量单位。

undo attribute remanent-volume 命令用来恢复缺省情况。

【命令】

```
attribute remanent-volume unit { byte | giga-byte | kilo-byte | mega-byte }  
undo attribute remanent-volume unit
```

【缺省情况】

Remanent-Volume 属性的流量单位是千字节。

【视图】

RADIUS 方案视图

【缺省用户角色】

network-admin

【参数】

byte: 表示流量单位为字节。

giga-byte: 表示流量单位为千兆字节。

kilo-byte: 表示流量单位为千字节。

mega-byte: 表示流量单位为兆字节。

【使用指导】

Remanent-Volume 属性为 H3C 自定义 RADIUS 属性，携带在 RADIUS 服务器发送给接入设备的认证响应或实时计费响应报文中，用于向接入设备通知在线用户的剩余流量值。设备管理员通过本命令设置的流量单位应与 RADIUS 服务器上统计用户流量的单位保持一致，否则设备无法正确使用 Remanent-Volume 属性值对用户进行计费。

【举例】

在 RADIUS 方案 radius1 中，设置 RADIUS 服务器下发的 Remanent-Volume 属性的流量单位为千字节。

```
<Sysname> system-view  
[Sysname] radius scheme radius1  
[Sysname-radius-radius1] attribute remanent-volume unit kilo-byte
```

【相关命令】

- **display radius scheme**

1.3.12 attribute translate

attribute translate 命令用来开启 RADIUS 属性解释功能。

undo attribute translate 命令用来关闭 RADIUS 属性解释功能。

【命令】

```
attribute translate  
undo attribute translate
```

【缺省情况】

RADIUS 属性解释功能处于关闭状态。

【视图】

RADIUS 方案视图/RADIUS DAE 服务器视图

【缺省用户角色】

network-admin

【使用指导】

不同厂商的 RADIUS 服务器所支持的 RADIUS 属性集有所不同,而且相同属性的用途也可能不同。为了兼容不同厂商的服务器的 RADIUS 属性,需要开启 RADIUS 属性解释功能,并定义相应的 RADIUS 属性转换规则和 RADIUS 属性禁用规则。

【举例】

在 RADIUS 方案 radius1 中,开启 RADIUS 属性解释功能。

```
<Sysname> system-view
[Sysname] radius scheme radius1
[Sysname-radius-radius1] attribute translate
```

【相关命令】

- **attribute convert**
- **attribute reject**

1.3.13 client

client 命令用来指定 RADIUS DAE 客户端。

undo client 命令用来删除指定的 RADIUS DAE 客户端。

【命令】

```
client { ip ipv4-address | ipv6 ipv6-address } [ key { cipher | simple }
string ]
undo client { ip ipv4-address | ipv6 ipv6-address }
```

【缺省情况】

未指定 RADIUS DAE 客户端。

【视图】

RADIUS DAE 服务器视图

【缺省用户角色】

network-admin

【参数】

ip ipv4-address: RADIUS DAE 客户端 IPv4 地址。

ipv6 ipv6-address: RADIUS DAE 客户端 IPv6 地址。

key: 与 RADIUS DAE 客户端交互 DAE 报文时使用的共享密钥。此共享密钥的设置必须与 RADIUS DAE 客户端的共享密钥设置保持一致。如果此处未指定本参数，则对应的 RADIUS DAE 客户端上也必须未指定。

cipher: 以密文方式设置密钥。

simple: 以明文方式设置密钥，该密钥将以密文形式存储。

string: 密钥字符串，区分大小写。非 FIPS 模式下，明文密钥为 1~64 个字符的字符串；密文密钥为 1~117 个字符的字符串。FIPS 模式下，明文密钥为 15~64 个字符的字符串，密钥元素的最少组合类型为 4（必须包括数字、大写字母、小写字母以及特殊字符）；密文密钥为 15~117 个字符的字符串。

【使用指导】

开启 RADIUS DAE 服务之后，设备会监听并处理指定的 RADIUS DAE 客户端发起的 DAE 请求消息（用于动态授权修改或断开连接），并向其发送应答消息。对于非指定的 RADIUS DAE 客户端的 DAE 报文进行丢弃处理。

可通过多次执行本命令指定多个 RADIUS DAE 客户端。

【举例】

设置 RADIUS DAE 客户端的 IP 地址为 10.110.1.2，与 RADIUS DAE 客户端交互 DAE 报文时使用的共享密钥为明文 123456。

```
<Sysname> system-view
[Sysname] radius dynamic-author server
[Sysname-radius-da-server] client ip 10.110.1.2 key simple 123456
```

【相关命令】

- **radius dynamic-author server**
- **port**

1.3.14 data-flow-format (RADIUS scheme view)

data-flow-format 命令用来配置发送到 RADIUS 服务器的数据流及数据包的单位。

undo data-flow-format 命令用来恢复缺省情况。

【命令】

```
data-flow-format { data { byte | giga-byte | kilo-byte | mega-byte } | packet
{ giga-packet | kilo-packet | mega-packet | one-packet } } *
undo data-flow-format { data | packet }
```

【缺省情况】

数据流的单位为字节，数据包的单位为包。

【视图】

RADIUS 方案视图

【缺省用户角色】

network-admin

【参数】

data: 设置数据流的单位。

- **byte:** 数据流的单位为字节。
- **giga-byte:** 数据流的单位千兆字节。
- **kilo-byte:** 数据流的单位为千字节。
- **mega-byte:** 数据流的单位为兆字节。

packet: 设置数据包的单位。

- **giga-packet:** 数据包的单位为千兆包。
- **kilo-packet:** 数据包的单位为千包。
- **mega-packet:** 数据包的单位为兆包。
- **one-packet:** 数据包的单位为包。

【使用指导】

设备上配置的发送给 RADIUS 服务器的数据流单位及数据包单位应与 RADIUS 服务器上的流量统计单位保持一致，否则无法正确计费。

【举例】

在 RADIUS 方案 radius1 中，设置发往 RADIUS 服务器的数据流单位为千字节、数据包单位为千包。

```
<Sysname> system-view
[Sysname] radius scheme radius1
[Sysname-radius-radius1] data-flow-format data kilo-byte packet kilo-packet
```

【相关命令】

- **display radius scheme**

1.3.15 display radius scheme

display radius scheme 命令用来显示 RADIUS 方案的配置信息。

【命令】

display radius scheme [*radius-scheme-name*]

【视图】

任意视图

【缺省用户角色】

network-admin
network-operator

【参数】

radius-scheme-name: RADIUS 方案名，为 1~32 个字符的字符串，不区分大小写。如果不指定该参数，则表示所有 RADIUS 方案。

【举例】

显示所有 RADIUS 方案的配置信息。

<Sysname> display radius scheme

Total 1 RADIUS schemes

```
-----
RADIUS scheme name: radius1
  Index : 0
  Primary authentication server:
    Host name: Not configured
    IP      : 2.2.2.2                      Port: 1812
    VPN     : Not configured
    State: Active
    Test profile: 132
      Probe username: test
      Probe interval: 60 minutes
    Weight: 40
  Primary accounting server:
    Host name: Not configured
    IP      : 1.1.1.1                      Port: 1813
    VPN     : Not configured
    State: Active
    Weight: 40
  Second authentication server:
    Host name: Not configured
    IP      : 3.3.3.3                      Port: 1812
    VPN     : Not configured
    State: Block
    Test profile: Not configured
    Weight: 40
  Second accounting server:
    Host name: Not configured
    IP      : 3.3.3.3                      Port: 1813
    VPN     : Not configured
    State: Block (Mandatory)
    Weight: 0
  Accounting-On function          : Enabled
    extended function             : Disabled
    retransmission times          : 5
    retransmission interval(seconds) : 2
  Timeout Interval(seconds)      : 3
  Retransmission Times            : 3
  Retransmission Times for Accounting Update : 5
  Server Quiet Period(minutes)    : 5
  Realtime Accounting Interval(seconds) : 22
  Stop-accounting packets buffering : Enabled
    Retransmission times          : 500
  NAS IP Address                  : 1.1.1.1
  VPN                             : Not configured
  User Name Format                  : with-domain
```

```

Data flow unit           : Megabyte
Packet unit             : One
Attribute 15 check-mode : Strict
Attribute 25            : CAR
Attribute Remanent-Volume unit : Mega
server-load-sharing      : loading-share
Attribute 31 MAC format  : hh:hh:hh:hh:hh:hh
Stop-accounting-packet send-force : Disabled

```

表1-4 display radius scheme 命令显示信息描述表

字段	描述
Total 1 RADIUS schemes.	共计1个RADIUS方案
RADIUS scheme name	RADIUS方案的名称
Index	RADIUS方案的索引号
Primary authentication server	主RADIUS认证服务器
Primary accounting server	主RADIUS计费服务器
Second authentication server	从RADIUS认证服务器
Second accounting server	从RADIUS计费服务器
Host name	RADIUS认证/计费服务器主机名 未配置时，显示为Not configured
IP	RADIUS认证/计费服务器IP地址 未配置时，显示为Not configured
Port	RADIUS认证/计费服务器接入端口号 未配置时，显示缺省值
State	RADIUS认证/计费服务器目前状态 <ul style="list-style-type: none"> Active: 激活状态 Block: 自动转换的静默状态 Block(Mandatory): 手工配置的静默状态
VPN	(暂不支持)RADIUS认证/计费服务器或RADIUS方案所在的VPN 未配置时，显示为Not configured
Test profile	探测服务器状态使用的模板名称
Probe username	探测服务器状态使用的用户名
Probe interval	探测服务器状态的周期（单位为分钟）
Weight	RADIUS服务器权重值
Accounting-On function	accounting-on功能的开启情况
extended function	accounting-on扩展功能的开启情况
retransmission times	accounting-on报文的发送尝试次数

字段	描述
retransmission interval(seconds)	accounting-on报文的重发间隔（单位为秒）
Timeout Interval(seconds)	RADIUS服务器超时时间（单位为秒）
Retransmission Times	发送RADIUS报文的最大尝试次数
Retransmission Times for Accounting Update	实时计费更新报文的最大尝试次数
Server Quiet Period(minutes)	RADIUS服务器恢复激活状态的时间（单位为分钟）
Realtime Accounting Interval(seconds)	实时计费更新报文的发送间隔（单位为秒）
Stop-accounting packets buffering	RADIUS停止计费请求报文缓存功能的开启情况
Retransmission times	发起RADIUS停止计费请求的最大尝试次数
NAS IP Address	发送RADIUS报文的源IP地址
User Name Format	发送给RADIUS服务器的用户名格式 <ul style="list-style-type: none"> • with-domain: 携带域名 • without-domain: 不携带域名 • keep-original: 与用户输入保持一致
Data flow unit	数据流的单位
Packet unit	数据包的单位
Attribute 15 check-mode	对RADIUS Attribute 15的检查方式，包括以下两种取值： <ul style="list-style-type: none"> • Strict: 表示使用 RADIUS 标准属性值和私有扩展的属性值进行检查 • Loose: 表示使用 RADIUS 标准属性值进行检查
Attribute 25	对RADIUS Attribute 25的处理，包括以下两种取值： <ul style="list-style-type: none"> • Standard: 表示不对 RADIUS Attribute 25 进行解析 • CAR: 表示将 RADIUS 25 号属性解析为 CAR 参数
Attribute Remanent-Volume unit	RADIUS Remanent-Volume属性的流量单位
server-load-sharing	RADIUS服务器负载分担功能的开启情况 <ul style="list-style-type: none"> • Disabled: 关闭状态，服务器工作于主/从模式 • Enabled: 开启状态，服务器工作于负载分担模式
Attribute 31 MAC format	RADIUS Attribute 31中携带的MAC地址格式
Stop-accounting-packet send-force	用户下线时设备强制发送RADIUS计费停止报文功能的开启情况

1.3.16 display radius statistics

display radius statistics 命令用来显示 RADIUS 报文的统计信息。

【命令】

display radius statistics

【视图】

任意视图

【缺省用户角色】

network-admin
network-operator

【举例】

显示 RADIUS 报文的统计信息。

```
<Sysname> display radius statistics
```

	Auth.	Acct.	SessCtrl.
Request Packet:	0	0	0
Retry Packet:	0	0	-
Timeout Packet:	0	0	-
Access Challenge:	0	-	-
Account Start:	-	0	-
Account Update:	-	0	-
Account Stop:	-	0	-
Terminate Request:	-	-	0
Set Policy:	-	-	0
Packet With Response:	0	0	0
Packet Without Response:	0	0	-
Access Rejects:	0	-	-
Dropped Packet:	0	0	0
Check Failures:	0	0	0

表1-5 display radius statistics 命令显示信息描述表

字段	描述
Auth.	认证报文
Acct.	计费报文
SessCtrl.	Session-control报文
Request Packet	发送的请求报文总数
Retry Packet	重传的请求报文总数
Timeout Packet	超时的请求报文总数
Access Challenge	Access challenge报文数
Account Start	计费开始报文的数目
Account Update	计费更新报文的数目
Account Stop	计费结束报文的数目
Terminate Request	服务器强制下线报文的数目
Set Policy	更新用户授权信息报文的数目
Packet With Response	有回应信息的报文数

字段	描述
Packet Without Response	无响应信息的报文数
Access Rejects	认证拒绝报文的数目
Dropped Packet	丢弃的报文数
Check Failures	报文校验错误的报文数目

【相关命令】

- **reset radius statistics**

1.3.17 display stop-accounting-buffer (for RADIUS)

display stop-accounting-buffer 命令用来显示缓存的 RADIUS 停止计费请求报文的相关信息。

【命令】

```
display stop-accounting-buffer { radius-scheme radius-scheme-name |
session-id session-id | time-range start-time end-time | user-name
user-name }
```

【视图】

任意视图

【缺省用户角色】

network-admin
network-operator

【参数】

radius-scheme *radius-scheme-name*: 表示指定 RADIUS 方案的停止计费请求报文。其中，*radius-scheme-name* 为 RADIUS 方案名，为 1~32 个字符的字符串，不区分大小写。

session-id *session-id*: 表示指定会话的停止计费请求报文。其中，*session-id* 表示会话 ID，为 1~64 个字符的字符串，不包含字母。会话 ID 用于唯一标识当前的在线用户。

time-range *start-time end-time*: 表示指定时间段内发送且被缓存的停止计费请求报文。其中，*start-time* 为请求时间段的起始时间，*end-time* 为请求时间段的结束时间，格式为 hh:mm:ss-mm/dd/yyyy（时:分:秒-月/日/年）或 hh:mm:ss-yyyy/mm/dd（时:分:秒-年/月/日）。

user-name *user-name*: 表示指定用户的停止计费请求报文。其中，*user-name* 表示用户名，为 1~255 个字符的字符串，区分大小写。输入的用户名是否携带 ISP 域名，必须与 RADIUS 方案中的 **user-name-format** 配置保持一致。

【举例】

显示缓存的用户名为 abc 的 RADIUS 停止计费请求报文的相关信息。

```
<Sysname> display stop-accounting-buffer user-name abc
Total entries: 2
Scheme      Session ID      Username      First sending time  Attempts
rad1        1000326232325010  abc          23:27:16-08/31/2015  19
```

表1-6 display stop-accounting-buffer 命令显示信息描述表

字段	描述
Total entries: 2	共有两条记录匹配
Scheme	RADIUS方案名
Session ID	会话ID
Username	用户名
First sending time	首次发送停止计费请求的时间
Attempts	发起停止计费请求的次数

【相关命令】

- **reset stop-accounting-buffer** (for RADIUS)
- **retry**
- **retry stop-accounting** (for RADIUS)
- **stop-accounting-buffer enable** (RADIUS scheme view)
- **user-name-format** (RADIUS scheme view)

1.3.18 key (RADIUS scheme view)

key 命令用来配置 RADIUS 报文的共享密钥。

undo key 命令用来删除 RADIUS 报文的共享密钥。

【命令】

```
key { accounting | authentication } { cipher | simple } string
undo key { accounting | authentication }
```

【缺省情况】

未配置 RADIUS 报文的共享密钥。

【视图】

RADIUS 方案视图

【缺省用户角色】

network-admin

【参数】

accounting: 指定 RADIUS 计费报文的共享密钥。

authentication: 指定 RADIUS 认证报文的共享密钥。

cipher: 以密文方式设置密钥。

simple: 以明文方式设置密钥，该密钥将以密文形式存储。

string: 密钥字符串，区分大小写。非 FIPS 模式下，明文密钥为 1~64 个字符的字符串；密文密钥为 1~117 个字符的字符串。FIPS 模式下，明文密钥为 15~64 个字符的字符串，密钥元素的

最少组合类型为 4（必须包括数字、大写字母、小写字母以及特殊字符）；密文密钥为 15～117 个字符的字符串。

【使用指导】

设备优先采用配置 RADIUS 认证/计费服务器时指定的报文共享密钥，本配置中指定的报文共享密钥仅在配置 RADIUS 认证/计费服务器时未指定相应密钥的情况下使用。

必须保证设备上设置的共享密钥与 RADIUS 服务器上的完全一致。

【举例】

在 RADIUS 方案 radius1 中，配置计费报文的共享密钥为明文 ok。

```
<Sysname> system-view
[Sysname] radius scheme radius1
[Sysname-radius-radius1] key accounting simple ok
```

【相关命令】

- **display radius scheme**

1.3.19 nas-ip (RADIUS scheme view)

nas-ip 命令用来设置设备发送 RADIUS 报文使用的源 IP 地址。

undo nas-ip 命令用来删除指定类型的发送 RADIUS 报文使用的源 IP 地址。

【命令】

```
nas-ip { ipv4-address | ipv6 ipv6-address }
undo nas-ip [ ipv6 ]
```

【缺省情况】

使用系统视图下由命令 **radius nas-ip** 指定的源地址，若系统视图下未指定源地址，则使用发送 RADIUS 报文的接口的主 IP 地址。

【视图】

RADIUS 方案视图

【缺省用户角色】

network-admin

【参数】

ipv4-address: 指定的源 IPv4 地址，应该为本机的地址，禁止配置全 0 地址、全 1 地址、D 类地址、E 类地址和环回地址。

ipv6 ipv6-address: 指定的源 IPv6 地址，应该为本机的地址，必须是单播地址，不能为环回地址与本地链路地址。

【使用指导】

RADIUS 服务器上通过 IP 地址来标识接入设备，并根据收到的 RADIUS 报文的源 IP 地址是否与服务器所管理的接入设备的 IP 地址匹配，来决定是否处理来自该接入设备的认证或计费请求。因此，为保证 RADIUS 报文可被服务器正常接收并处理，接入设备上发送 RADIUS 报文使用的源地址必须与 RADIUS 服务器上指定的接入设备的 IP 地址保持一致。

为避免物理接口故障时从服务器返回的报文不可达，推荐使用 Loopback 接口地址为发送 RADIUS 报文使用的源 IP 地址。

RADIUS 方案视图和系统视图下均可以配置发送 RADIUS 报文使用的源 IP 地址，具体生效情况如下：

- RADIUS 方案视图下配置的源 IP 地址（通过 **nas-ip** 命令）只对本方案有效。
- 系统视图下的配置的源 IP 地址（通过 **radius nas-ip** 命令）对所有 RADIUS 方案有效。
- RADIUS 方案视图下的设置具有更高的优先级。

一个 RADIUS 方案视图下，最多允许指定一个 IPv4 源地址和一个 IPv6 源地址。

如果 **undo nas-ip** 命令中不指定 **ipv6** 参数，则表示删除配置的发送 RADIUS 报文使用的源 IPv4 地址。

【举例】

在 RADIUS 方案 radius1 中，设置设备发送 RADIUS 报文使用的源 IP 地址为 10.1.1.1。

```
<Sysname> system-view
[Sysname] radius scheme radius1
[Sysname-radius-radius1] nas-ip 10.1.1.1
```

【相关命令】

- **display radius scheme**
- **radius nas-ip**

1.3.20 port

port 命令用来指定 RADIUS DAE 服务端口。

undo port 命令用来恢复缺省情况。

【命令】

```
port port-number
undo port
```

【缺省情况】

RADIUS DAE 服务端口为 3799。

【视图】

RADIUS DAE 服务器视图

【缺省用户角色】

network-admin

【参数】

port-number: DAE 服务器接收 DAE 请求消息的 UDP 端口，取值范围为 1~65535。

【使用指导】

必须保证设备上的 RADIUS DAE 服务端口与 RADIUS DAE 客户端发送 DAE 报文的目的 UDP 端口一致。

【举例】

开启 RADIUS DAE 服务后，指定 DAE 服务端口为 3790。

```
<Sysname> system-view
[Sysname] radius dynamic-author server
[Sysname-radius-da-server] port 3790
```

【相关命令】

- **client**
- **radius dynamic-author server**

1.3.21 primary accounting (RADIUS scheme view)

primary accounting 命令用来配置主 RADIUS 计费服务器。

undo primary accounting 命令用来恢复缺省情况。

【命令】

```
primary accounting { host-name | ipv4-address | ipv6 ipv6-address }
[ port-number | key { cipher | simple } string | weight weight-value ] *
undo primary accounting
```

【缺省情况】

未配置主 RADIUS 计费服务器。

【视图】

RADIUS 方案视图

【缺省用户角色】

network-admin

【参数】

host-name: 主 RADIUS 计费服务器的主机名，为 1~253 个字符的字符串，不区分大小写。

ipv4-address: 主 RADIUS 计费服务器的 IPv4 地址。

ipv6 ipv6-address: 主 RADIUS 计费服务器的 IPv6 地址。

port-number: 主 RADIUS 计费服务器的 UDP 端口号，取值范围为 1~65535，缺省值为 1813。

key: 与主 RADIUS 计费服务器交互的计费报文的共享密钥。

cipher: 以密文方式设置密钥。

simple: 以明文方式设置密钥，该密钥将以密文形式存储。

string: 密钥字符串，区分大小写。非 FIPS 模式下，明文密钥为 1~64 个字符的字符串；密文密钥为 1~117 个字符的字符串。FIPS 模式下，明文密钥为 15~64 个字符的字符串，密钥元素的最少组合类型为 4（必须包括数字、大写字母、小写字母以及特殊字符）；密文密钥为 15~117 个字符的字符串。

weight weight-value: RADIUS 服务器负载分担的权重。**weight-value** 表示权重值，取值范围为 0~100，缺省值为 0。0 表示该服务器在负载分担调度时将不被使用。开启服务器负载分担功能后，该参数才能生效，且权重值越大的服务器可以处理的计费请求报文越多。

【使用指导】

配置的主计费服务器的 UDP 端口号以及计费报文的共享密钥必须与服务器的配置保持一致。

在同一个方案中指定的主计费服务器和从计费服务器的主机名、IP 地址、端口号不能完全相同。

设备与主计费服务器通信时优先使用本命令设置的共享密钥，如果此处未设置，则使用 **key accounting** 命令设置的共享密钥。

当 RADIUS 服务器负载分担功能处于关闭状态时，如果在计费开始请求报文发送过程中修改或删除了正在使用的主计费服务器配置，则设备在与当前服务器通信超时后，将会重新按照优先级顺序开始依次查找状态为 **active** 的服务器进行通信；当 RADIUS 服务器负载分担功能处于开启状态时，设备将仅与发起计费开始请求的服务器通信。

如果在线用户正在使用的计费服务器被删除，则设备将无法发送用户的实时计费请求和停止计费请求，且停止计费报文不会被缓存到本地，这将造成对用户计费的不准确。

【举例】

在 RADIUS 方案 radius1 中，配置主计费服务器的 IP 地址为 10.110.1.2，使用 UDP 端口 1813 提供 RADIUS 计费服务，计费报文的共享密钥为明文 123456TESTacct&!。

```
<Sysname> system-view
[Sysname] radius scheme radius1
[Sysname-radius-radius1] primary accounting 10.110.1.2 1813 key simple 123456TESTacct&!
```

【相关命令】

- **display radius scheme**
- **key** (RADIUS scheme view)
- **secondary accounting** (RADIUS scheme view)
- **server-load-sharing enable**

1.3.22 primary authentication (RADIUS scheme view)

primary authentication 命令用来配置主 RADIUS 认证服务器。

undo primary authentication 命令用来恢复缺省情况。

【命令】

```
primary authentication { host-name | ipv4-address | ipv6 ipv6-address }
[ port-number | key { cipher | simple } string | test-profile profile-name |
weight weight-value ] *
undo primary authentication
```

【缺省情况】

未配置 RADIUS 主认证服务器。

【视图】

RADIUS 方案视图

【缺省用户角色】

network-admin

【参数】

host-name: 主 RADIUS 认证服务器的主机名，为 1~253 个字符的字符串，不区分大小写。

ipv4-address: 主 RADIUS 认证服务器的 IPv4 地址。

ipv6 ipv6-address: 主 RADIUS 认证服务器的 IPv6 地址。

port-number: 主 RADIUS 认证服务器的 UDP 端口号，取值范围为 1~65535，缺省值为 1812。此端口号必须与服务器提供认证服务的端口号保持一致。

key: 与主 RADIUS 认证服务器交互的认证报文的共享密钥。此共享密钥必须与服务器上配置的共享密钥保持一致。

cipher: 以密文方式设置密钥。

simple: 以明文方式设置密钥，该密钥将以密文形式存储。

string: 密钥字符串，区分大小写。非 FIPS 模式下，明文密钥为 1~64 个字符的字符串；密文密钥为 1~117 个字符的字符串。FIPS 模式下，明文密钥为 15~64 个字符的字符串，密钥元素的最少组合类型为 4（必须包括数字、大写字母、小写字母以及特殊字符）；密文密钥为 15~117 个字符的字符串。

test-profile profile-name: RADIUS 服务器探测模板名称，为 1~31 个字符的字符串，区分大小写。

weight weight-value: RADIUS 服务器负载分担的权重。**weight-value** 表示权重值，取值范围为 0~100，缺省值为 0。0 表示该服务器在负载分担调度时将不被使用。开启服务器负载分担功能后，该参数才能生效，且权重值越大的服务器可以处理的认证请求报文越多。

【使用指导】

配置的主认证服务器的 UDP 端口号以及认证报文的共享密钥必须与服务器的配置保持一致。

在同一个方案中指定的主认证服务器和从认证服务器的主机名、IP 地址、端口号不能完全相同。

设备与主认证服务器通信时优先使用本命令设置的共享密钥，如果本命令中未设置，则使用 **key authentication** 命令设置的共享密钥。

RADIUS 认证服务器引用了存在的服务器探测模板后，将会触发对该服务器的探测功能。

当 RADIUS 服务器负载分担功能处于关闭状态时，如果在认证过程中修改或删除了正在使用的主认证服务器配置，则设备在与当前服务器通信超时后，将会重新按照优先级顺序开始依次查找状态为 **active** 的服务器进行通信；当 RADIUS 服务器负载分担功能处于开启状态时，如果在认证过程中修改或删除了正在使用的认证服务器配置，则设备在与当前服务器通信超时后，将会根据各服务器的权重以及服务器承载的用户负荷重新选择状态为 **active** 的服务器进行通信。

【举例】

在 RADIUS 方案 radius1 中，配置主认证服务器的 IP 地址为 10.110.1.1，使用 UDP 端口 1812 提供 RADIUS 认证/授权服务，认证报文的共享密钥为明文 123456TESTauth&!

```
<Sysname> system-view
```

```
[Sysname] radius scheme radius1
```

```
[Sysname-radius-radius1] primary authentication 10.110.1.1 1812 key simple 123456TESTauth&!
```

【相关命令】

- **display radius scheme**
- **key** (RADIUS scheme view)

- `radius-server test-profile`
- `secondary authentication` (RADIUS scheme view)
- `server-load-sharing enable`

1.3.23 radius attribute extended

`radius attribute extended` 命令用来定义 RADIUS 扩展属性。

`undo radius attribute extended` 命令用来删除定义的 RADIUS 扩展属性。

【命令】

```
radius attribute extended attribute-name [ vendor vendor-id ] code
attribute-code type { binary | date | integer | interface-id | ip | ipv6 |
ipv6-prefix | octets | string }
undo radius attribute extended [ attribute-name ]
```

【缺省情况】

不存在自定义 RADIUS 扩展属性。

【视图】

系统视图

【缺省用户角色】

network-admin

【参数】

attribute-name: RADIUS 属性名称，为 1~63 个字符的字符串，不区分大小写。该名称不能与系统已支持的（包括标准的以及自定义的）RADIUS 属性名称相同。

vendor vendor-id: RADIUS 属性所属的设备厂商标识。*vendor-id* 为厂商标识号码，取值范围为 1~65535。如果不指定该参数，则表示 RADIUS 属性为标准属性。

code attribute-code: RADIUS 属性在 RADIUS 属性集里的序号，取值范围为 1~255。

type: 属性内容的数据类型，包括以下取值：

- **binary**: 二进制类型。
- **date**: 时间类型。
- **integer**: 整数类型。
- **interface-id**: 接口 ID 类型。
- **ip**: IPv4 地址类型。
- **ipv6**: IPv6 地址类型。
- **ipv6-prefix**: IPv6 地址前缀类型。
- **octets**: 八进制类型。
- **string**: 字符串类型。

【使用指导】

当系统需要支持其他厂商的私有 RADIUS 属性时，可以通过 `radius attribute extended` 命令为其定义为一个扩展属性，并通过 `attribute convert` 命令将其映射到系统可以识别的一个

已知属性。这样，当 RADIUS 服务器发送给设备的 RADIUS 报文中携带了此类不可识别的私有属性时，设备将根据已定义的属性转换规则将其转换为可处理的属性。同理，设备在发送 RADIUS 报文时也可以将自己可识别的属性转换为服务器能识别的属性。

每一个 RADIUS 属性有唯一的属性名称，且该属性的名称、设备厂商标识以及序号的组合必须在设备上唯一。

执行 **undo radius attribute extended** 命令时，如果不指定属性名称，则表示删除所有已定义 RADIUS 扩展属性。

【举例】

配置一个 RADIUS 扩展属性，名称为 Owner-Password，Vendor ID 为 122，属性序号为 80，类型为字符串。

```
<Sysname> system-view
```

```
[Sysname] radius attribute extended Owner-Password vendor 122 code 80 type string
```

【相关命令】

- **attribute convert**
- **attribute reject**
- **attribute translate**

1.3.24 radius dscp

radius dscp 命令用来配置 RADIUS 协议报文的 DSCP 优先级。

undo radius dscp 命令用来恢复缺省情况。

【命令】

```
radius [ ipv6 ] dscp dscp-value
```

```
undo radius [ ipv6 ] dscp
```

【缺省情况】

RADIUS 报文的 DSCP 优先级为 0。

【视图】

系统视图

【缺省用户角色】

network-admin

【参数】

ipv6：表示设置 IPv6 RADIUS 报文。若不指定该参数，则表示设置 IPv4 RADIUS 报文。

dscp-value：RADIUS 报文的 DSCP 优先级，取值范围为 0~63。取值越大，优先级越高。

【使用指导】

DSCP 携带在 IP 报文中的 ToS 字段，用来体现报文自身的优先等级，决定报文传输的优先程度。通过本命令可以指定设备发送的 RADIUS 报文携带的 DSCP 优先级的取值。

【举例】

配置 IPv4 RADIUS 报文的 DSCP 优先级为 10。

```
<Sysname> system-view
[Sysname] radius dscp 10
```

1.3.25 radius dynamic-author server

radius dynamic-author server 命令用来开启 RADIUS DAE 服务，并进入 RADIUS DAE 服务器视图。

undo radius dynamic-author server 命令用来关闭 RADIUS DAE 服务。

【命令】

```
radius dynamic-author server
undo radius dynamic-author server
```

【缺省情况】

RADIUS DAE 服务处于关闭状态。

【视图】

系统视图

【缺省用户角色】

network-admin

【使用指导】

开启 RADIUS DAE 服务后，设备将会监听指定的 RADIUS DAE 客户端发送的 DAE 请求消息，然后根据请求消息修改用户授权信息、断开用户连接请求、关闭/重启用户接入端口或重认证用户。

【举例】

开启 RADIUS DAE 服务，并进入 RADIUS DAE 服务器视图。

```
<Sysname> system-view
[Sysname] radius dynamic-author server
[Sysname-radius-da-server]
```

【相关命令】

- **client**
- **port**

1.3.26 radius nas-ip

radius nas-ip 命令用来设置设备发送 RADIUS 报文使用的源地址。

undo radius nas-ip 命令用来删除指定的发送 RADIUS 报文使用的源地址。

【命令】

```
radius nas-ip { ipv4-address | ipv6 ipv6-address }
undo radius nas-ip { ipv4-address | ipv6 ipv6-address }
```

【缺省情况】

未指定发送 RADIUS 报文使用的源地址，设备将以发送报文的接口的主 IP 地址作为源地址。

【视图】

系统视图

【缺省用户角色】

network-admin

【参数】

ipv4-address: 指定的源 IPv4 地址，应该为本机的地址，不能为全 0 地址、全 1 地址、D 类地址、E 类地址和环回地址。

ipv6 ipv6-address: 指定的源 IPv6 地址，应该为本机的地址，必须是单播地址，不能为环回地址与本地链路地址。

【使用指导】

RADIUS 服务器上通过 IP 地址来标识接入设备，并根据收到的 RADIUS 报文的源 IP 地址是否与服务器所管理的接入设备的 IP 地址匹配，来决定是否处理来自该接入设备的认证或计费请求。为保证 RADIUS 报文可被服务器正常接收并处理，接入设备上发送 RADIUS 报文使用的源地址必须与 RADIUS 服务器上指定的接入设备的 IP 地址保持一致。

为避免物理接口故障时从服务器返回的报文不可达，推荐使用 Loopback 接口地址为发送 RADIUS 报文使用的源 IP 地址。

RADIUS 方案视图和系统视图下均可以配置发送 RADIUS 报文使用的源 IP 地址，具体情况如下：

- RADIUS 方案视图下配置的源 IP 地址（通过 **nas-ip** 命令）只对本 RADIUS 方案有效。
- 系统视图下的配置的源 IP 地址（通过 **radius nas-ip** 命令）对所有 RADIUS 方案有效。
- RADIUS 方案视图下的设置具有更高的优先级。

系统视图下最多允许指定一个 IPv4 源地址和一个 IPv6 源地址。

【举例】

设置设备发送 RADIUS 报文使用的源地址为 129.10.10.1。

```
<Sysname> system-view
[Sysname] radius nas-ip 129.10.10.1
```

【相关命令】

- **nas-ip** (RADIUS scheme view)

1.3.27 radius scheme

radius scheme 命令用来创建 RADIUS 方案，并进入 RADIUS 方案视图。如果指定的 RADIUS 方案已经存在，则直接进入 RADIUS 方案视图。

undo radius scheme 命令用来删除指定的 RADIUS 方案。

【命令】

```
radius scheme radius-scheme-name
undo radius scheme radius-scheme-name
```

【缺省情况】

不存在 RADIUS 方案。

【视图】

系统视图

【缺省用户角色】

network-admin

【参数】

radius-scheme-name: RADIUS 方案的名称，为 1~32 个字符的字符串，不区分大小写。

【使用指导】

一个 RADIUS 方案可以同时被多个 ISP 域引用。

系统最多支持配置 16 个 RADIUS 方案。

【举例】

创建名为 radius1 的 RADIUS 方案并进入其视图。

```
<Sysname> system-view
[Sysname] radius scheme radius1
[Sysname-radius-radius1]
```

【相关命令】

- **display radius scheme**

1.3.28 radius session-control client

radius session-control client 命令用来指定 session control 客户端。

undo radius session-control client 命令用来删除指定的 session control 客户端。

【命令】

```
radius session-control client { ip ipv4-address | ipv6 ipv6-address } [ key
{ cipher | simple } string ]
undo radius session-control client { all | ip ipv4-address | ipv6
ipv6-address }
```

【缺省情况】

未指定 session control 客户端。

【视图】

系统视图

【缺省用户角色】

network-admin

【参数】

ip ipv4-address: session control 客户端的 IPv4 地址。

ipv6 ipv6-address: session control 客户端的 IPv6 地址。

key: 与 session control 客户端交互的计费报文的共享密钥。

cipher: 以密文方式设置密钥。

simple: 以明文方式设置密钥，该密钥将以密文形式存储。

string: 密钥字符串，区分大小写。非 FIPS 模式下，明文密钥为 1~64 个字符的字符串；密文密钥为 1~117 个字符的字符串。FIPS 模式下，明文密钥为 15~64 个字符的字符串，密钥元素的最少组合类型为 4（必须包括数字、大写字母、小写字母以及特殊字符）；密文密钥为 15~117 个字符的字符串。

all: 表示所有 session control 客户端。

【使用指导】

设备和 H3C 的 iMC RADIUS 服务器配合使用时，将作为 session control 服务器端与其交互，因此需要指定 session control 客户端来验证收到的 session control 报文的合法性。当设备收到服务器发送的 session control 报文时，直接根据报文的源 IP 地址与已有的 session control 客户端配置进行匹配，并使用匹配到的客户端共享密钥对报文进行验证。如果报文匹配失败或设备上未配置 session control 客户端，则使用已有的 RADIUS 方案配置进行匹配，并使用匹配到的认证服务器的共享密钥对报文进行验证。

指定的 session control 客户端仅在 RADIUS session control 功能处于开启状态时生效。

配置的 session control 客户端参数必须与服务器的配置保持一致。

系统支持指定多个 session control 客户端。

【举例】

指定一个 session control 客户端 IP 地址为 10.110.1.2，共享密钥为明文 12345。

```
<Sysname> system-view
```

```
[Sysname] radius session-control client ip 10.110.1.2 key simple 12345
```

【相关命令】

- **radius session-control enable**

1.3.29 radius session-control enable

radius session-control enable 命令用来开启 RADIUS session control 功能。

undo radius session-control enable 命令用来关闭 RADIUS session control 功能。

【命令】

```
radius session-control enable
```

```
undo radius session-control enable
```

【缺省情况】

RADIUS session control 功能处于关闭状态。

【视图】

系统视图

【缺省用户角色】

network-admin

【使用指导】

H3C iMC RADIUS 服务器使用 session control 报文向设备发送授权信息的动态修改请求以及断开连接请求。开启 RADIUS session control 功能后，设备会打开知名 UDP 端口 1812 来监听并接收 RADIUS 服务器发送的 session control 报文。

该功能仅能和 H3C iMC 的 RADIUS 服务器配合使用。

【举例】

开启 RADIUS session control 功能。

```
<Sysname> system-view
[Sysname] radius session-control enable
```

1.3.30 radius-server test-profile

radius-server test-profile 命令用来配置 RADIUS 服务器探测模板。

undo radius-server test-profile 命令用来删除指定的 RADIUS 服务器探测模板。

【命令】

```
radius-server test-profile profile-name username name [ password { cipher | simple } string ] [ interval interval ]
undo radius-server test-profile profile-name
```

【缺省情况】

不存在 RADIUS 服务器探测模板。

【视图】

系统视图

【缺省用户角色】

network-admin

【参数】

profile-name: 探测模板名称，为 1~31 个字符的字符串，区分大小写。

username name: 探测报文中的用户名，为 1~253 个字符的字符串，区分大小写。

password: 探测报文中的用户密码。若不指定该参数，则表示探测报文中携带的用户密码为设备生成的随机密码。为避免携带随机密码的探测报文被 RADIUS 服务器判定为攻击报文，建议指定用户密码。

cipher: 以密文方式设置用户密码。

simple: 以明文方式设置用户密码，该密码将以密文形式存储。

string: 密码字符串，区分大小写。明文密码为 1~63 个字符的字符串；密文密码为 1~117 个字符的字符串。

interval interval: 发送探测报文的周期，取值范围为 1~3600，单位为分钟，缺省值为 60。

【使用指导】

系统支持配置多个 RADIUS 服务器探测模板。

RADIUS 方案视图下的 RADIUS 服务器配置成功引用了某探测模板后,若被引用的探测模板不存在,则暂不启动探测功能。之后,当该探测模板被成功配置时,针对该服务器的探测过程将会立即开始。删除一个 RADIUS 服务器探测模板时,引用该探测模板的所有 RADIUS 方案中的 RADIUS 服务器的探测功能也会被关闭。

【举例】

```
# 配置 RADIUS 服务器探测模板 abc, 探测报文中携带的用户名为 admin, 密码为明文 abc123,
探测报文的发送间隔为 10 分钟。

<Sysname> system-view
[Sysname] radius-server test-profile abc username admin password simple abc123 interval 10
```

【相关命令】

- **primary authentication** (RADIUS scheme view)
- **secondary authentication** (RADIUS scheme view)

1.3.31 reset radius statistics

reset radius statistics 命令用来清除 RADIUS 协议的统计信息。

【命令】

```
reset radius statistics
```

【视图】

用户视图

【缺省用户角色】

network-admin

【举例】

```
# 清除 RADIUS 协议的统计信息。

<Sysname> reset radius statistics
```

【相关命令】

- **display radius statistics**

1.3.32 reset stop-accounting-buffer (for RADIUS)

reset stop-accounting-buffer 命令用来清除缓存的 RADIUS 停止计费请求报文。

【命令】

```
reset stop-accounting-buffer { radius-scheme radius-scheme-name |
session-id session-id | time-range start-time end-time | user-name
user-name }
```

【视图】

用户视图

【缺省用户角色】

network-admin

【参数】

radius-scheme *radius-scheme-name*: 表示指定 RADIUS 方案的停止计费响应报文。其中, *radius-scheme-name* 为 RADIUS 方案名, 为 1~32 个字符的字符串, 不区分大小写。

session-id *session-id*: 表示指定会话的停止计费响应报文。其中, *session-id* 表示会话 ID, 为 1~64 个字符的字符串, 不包含字母。会话 ID 用于唯一标识当前的在线用户。

time-range *start-time end-time*: 表示指定时间段内发送且被缓存的停止计费请求报文。其中, *start-time* 为请求时间段的起始时间; *end-time* 为请求时间段的结束时间, 格式为 hh:mm:ss-mm/dd/yyyy (时:分:秒-月/日/年) 或 hh:mm:ss-yyyy/mm/dd (时:分:秒-年/月/日)。

user-name *user-name*: 表示指定用户名的停止计费响应报文。其中, *user-name* 表示用户名, 为 1~255 个字符的字符串, 区分大小写。输入的用户名是否携带 ISP 域名, 必须与 RADIUS 方案中配置的发送给 RADIUS 服务器的用户名格式保持一致。

【举例】

清除缓存的用户 user0001@test 的 RADIUS 停止计费请求报文。

```
<Sysname> reset stop-accounting-buffer user-name user0001@test
```

清除从 2015 年 8 月 31 日 0 点 0 分 0 秒到 2015 年 8 月 31 日 23 点 59 分 59 秒期间内缓存的停止计费请求报文。

```
<Sysname> reset stop-accounting-buffer time-range 00:00:00-08/31/2015 23:59:59-08/31/2015
```

【相关命令】

- **display stop-accounting-buffer** (for RADIUS)
- **stop-accounting-buffer enable** (RADIUS scheme view)

1.3.33 retry

retry 命令用来设置发送 RADIUS 报文的最大尝试次数。

undo retry 命令用来恢复缺省情况。

【命令】

```
retry retries
```

```
undo retry
```

【缺省情况】

发送 RADIUS 报文的最大尝试次数为 3 次。

【视图】

RADIUS 方案视图

【缺省用户角色】

network-admin

【参数】

retries: 发送 RADIUS 报文的最大尝试次数, 取值范围为 1~20。

【使用指导】

由于 RADIUS 协议采用 UDP 报文来承载数据，因此其通信过程是不可靠的。如果设备在应答超时定时器规定的时长内（由 **timer response-timeout** 命令配置）没有收到 RADIUS 服务器的响应，则设备有必要向 RADIUS 服务器重传 RADIUS 请求报文。如果累计的传送次数已达到最大传送次数而 RADIUS 服务器仍旧没有响应，则设备将认为本次请求失败。

需要注意的是：

- 发送 RADIUS 报文的最大尝试次数、RADIUS 服务器响应超时时间以及配置的 RADIUS 服务器总数，三者的乘积不能超过接入模块定义的用户认证超时时间，否则在 RADIUS 认证过程完成之前用户就有可能被强制下线。
- 设备在按照配置顺序尝试与下一个 RADIUS 服务器通信之前，会首先判断当前累计尝试持续时间是否达到或超过 300 秒，如果超过或达到 300 秒，将不再向下一个 RADIUS 服务器发送 RADIUS 请求报文，即认为该 RADIUS 请求发送失败。因此，为了避免某些已部署的 RADIUS 服务器由于此超时机制而无法被使用到，建议基于配置的 RADIUS 服务器总数，合理设置发送 RADIUS 报文的最大尝试次数以及 RADIUS 服务器响应超时时间。

【举例】

在 RADIUS 方案 radius1 中，设置发送 RADIUS 报文的最大尝试次数为 5 次。

```
<Sysname> system-view
[Sysname] radius scheme radius1
[Sysname-radius-radius1] retry 5
```

【相关命令】

- **radius scheme**
- **timer response-timeout** (RADIUS scheme view)

1.3.34 retry realtime-accounting

retry realtime-accounting 命令用来设置允许发起实时计费请求的最大尝试次数。

undo retry realtime-accounting 命令用来恢复缺省情况。

【命令】

```
retry realtime-accounting retries
undo retry realtime-accounting
```

【缺省情况】

设备允许发起实时计费请求的最大尝试次数为 5。

【视图】

RADIUS 方案视图

【缺省用户角色】

network-admin

【参数】

retries：允许发起实时计费请求的最大尝试次数，取值范围为 1～255。

【使用指导】

RADIUS 服务器通常通过连接超时定时器来判断用户是否在线。如果 RADIUS 服务器在连接超时时间之内一直收不到设备传来的实时计费报文，它会认为线路或设备故障并停止对用户记帐。为了配合 RADIUS 服务器的这种特性，有必要在不可预见的故障条件下，尽量保持设备端与 RADIUS 服务器同步切断用户连接。设备提供对实时计费请求连续无响应次数限制的设置，保证设备尽可能得在 RADIUS 服务器的连接超时时长内向 RADIUS 服务器尝试发出实时计费请求。如果设备没有收到响应的次数超过了设定的限度，才会切断用户连接。

假设 RADIUS 服务器的应答超时时长（**timer response-timeout** 命令设置）为 3 秒，发送 RADIUS 报文的最大尝试次数（**retry** 命令设置）为 3，设备的实时计费间隔（**timer realtime-accounting** 命令设置）为 12 分钟，设备允许实时计费无响应的最大次数为 5 次（**retry realtime-accounting** 命令设置），则其含义为：设备每隔 12 分钟发起一次计费请求，如果 3 秒钟得不到回应就重新发起一次请求，如果 3 次发送都没有得到回应就认为该次实时计费失败，然后每隔 12 分钟再发送一次，5 次均失败以后，设备将切断用户连接。

【举例】

在 RADIUS 方案 radius1 中，设置允许发起实时计费请求的最大尝试次数为 10。

```
<Sysname> system-view
[Sysname] radius scheme radius1
[Sysname-radius-radius1] retry realtime-accounting 10
```

【相关命令】

- **retry**
- **timer realtime-accounting** (RADIUS scheme view)
- **timer response-timeout** (RADIUS scheme view)

1.3.35 retry stop-accounting (RADIUS scheme view)

retry stop-accounting 命令用来设置发起 RADIUS 停止计费请求的最大尝试次数。

undo retry stop-accounting 命令用来恢复缺省情况。

【命令】

```
retry stop-accounting retries
undo retry stop-accounting
```

【缺省情况】

发起 RADIUS 停止计费请求的最大尝试次数为 500。

【视图】

RADIUS 方案视图

【缺省用户角色】

network-admin

【参数】

retries：允许停止计费请求无响应的最大次数，取值范围为 10～65535。

【使用指导】

设备通过发起 RADIUS 停止计费请求的最大尝试次数与其它相关参数一起控制停止计费请求报文的发送。假设存在如下配置：

- RADIUS 服务器的应答超时时长（由 **timer response-timeout** 命令设置）为 3 秒；
- 发送 RADIUS 报文的最大尝试次数（由 **retry** 命令设置）为 5；
- 开启了对无响应的 RADIUS 停止计费请求报文的缓存功能；
- 设备发起停止计费请求的最大尝试次数为 20（由 **retry stop-accounting** 命令设置）。

则，如果设备发送停止计费请求报文后的 3 秒内得不到服务器响应就重新发送该报文。如果设备发送 5 次之后仍然没有得到响应，会将该报文缓存在本机上，然后再发起一轮停止计费请求。20 次请求尝试均失败以后，设备将缓存的报文丢弃。

【举例】

在 RADIUS 方案 radius1 中，设置发起 RADIUS 停止计费请求的最大尝试次数为 1000。

```
<Sysname> system-view
[Sysname] radius scheme radius1
[Sysname-radius-radius1] retry stop-accounting 1000
```

【相关命令】

- **display stop-accounting-buffer** (for RADIUS)
- **retry**
- **timer response-timeout** (RADIUS scheme view)

1.3.36 secondary accounting (RADIUS scheme view)

secondary accounting 命令用来配置从 RADIUS 计费服务器。

undo secondary accounting 命令用来删除指定的从 RADIUS 计费服务器。

【命令】

```
secondary accounting { host-name | ipv4-address | ipv6 ipv6-address }
[ port-number | key { cipher | simple } string | weight weight-value ] *
undo secondary accounting [ { host-name | ipv4-address | ipv6 ipv6-address }
[ port-number ] ]
```

【缺省情况】

未配置从 RADIUS 计费服务器。

【视图】

RADIUS 方案视图

【缺省用户角色】

network-admin

【参数】

host-name：从 RADIUS 计费服务器的主机名，为 1~253 个字符的字符串，不区分大小写。

ipv4-address：从 RADIUS 计费服务器的 IPv4 地址。

ipv6 ipv6-address: 从 RADIUS 计费服务器的 IPv6 地址。

port-number: 从 RADIUS 计费服务器的 UDP 端口号，取值范围为 1~65535，缺省值为 1813。

key: 与从 RADIUS 计费服务器交互的计费报文的共享密钥。

cipher: 以密文方式设置密钥。

simple: 以明文方式设置密钥，该密钥将以密文形式存储。

string: 密钥字符串，区分大小写。非 FIPS 模式下，明文密钥为 1~64 个字符的字符串；密文密钥为 1~117 个字符的字符串。FIPS 模式下，明文密钥为 15~64 个字符的字符串，密钥元素的最少组合类型为 4（必须包括数字、大写字母、小写字母以及特殊字符）；密文密钥为 15~117 个字符的字符串。

weight weight-value: RADIUS 服务器负载分担的权重。**weight-value** 表示权重值，取值范围为 0~100，缺省值为 0。0 表示该服务器在负载分担调度时将不被使用。开启服务器负载分担功能后，该参数才能生效，且权重值越大的服务器可以处理的计费请求报文越多。

【使用指导】

配置的从计费服务器的 UDP 端口号以及计费报文的共享密钥必须与服务器的配置保持一致。

每个 RADIUS 方案中最多支持配置 16 个从 RADIUS 计费服务器。当主服务器不可达时，设备根据从服务器的配置顺序由先到后查找状态为 **active** 的从服务器并与之交互。

在同一个方案中指定的主计费服务器和从计费服务器的主机名、IP 地址、端口号不能完全相同，并且各从计费服务器的主机名、IP 地址、端口号也不能完全相同。

设备与从计费服务器通信时优先使用本命令设置的共享密钥，如果此处未设置，则使用命令 **key accounting** 命令设置的共享密钥。

当 RADIUS 服务器负载分担功能处于关闭状态时，如果在计费开始请求报文发送过程中删除了正在使用的从服务器配置，则设备在与当前服务器通信超时后，将会重新按照优先级顺序开始依次查找状态为 **active** 的服务器进行通信；在 RADIUS 服务器负载分担功能处于开启状态时，设备将仅与发起计费开始请求的服务器通信。

如果在线用户正在使用的计费服务器被删除，则设备将无法发送用户的实时计费请求和停止计费请求，且停止计费报文不会被缓存到本地。

【举例】

在 RADIUS 方案 **radius1** 中，配置从计费服务器的 IP 地址为 10.110.1.1，使用 UDP 端口 1813 提供 RADIUS 计费服务。

```
<Sysname> system-view
[Sysname] radius scheme radius1
[Sysname-radius-radius1] secondary accounting 10.110.1.1 1813
```

在 RADIUS 方案 **radius2** 中，配置两个从计费服务器，IP 地址分别为 10.110.1.1、10.110.1.2，且均使用 UDP 端口 1813 提供 RADIUS 计费服务。

```
<Sysname> system-view
[Sysname] radius scheme radius2
[Sysname-radius-radius2] secondary accounting 10.110.1.1 1813
[Sysname-radius-radius2] secondary accounting 10.110.1.2 1813
```

【相关命令】

- **display radius scheme**

- **key** (RADIUS scheme view)
- **primary accounting**

1.3.37 secondary authentication (RADIUS scheme view)

secondary authentication 命令用来配置从 RADIUS 认证服务器。

undo secondary authentication 命令用来删除指定的从 RADIUS 认证服务器。

【命令】

```
secondary authentication { host-name | ipv4-address | ipv6 ipv6-address }
[ port-number | key { cipher | simple } string | test-profile profile-name |
weight weight-value ] *

undo secondary authentication [ { host-name | ipv4-address | ipv6
ipv6-address } [ port-number ] ]
```

【缺省情况】

未配置从 RADIUS 认证服务器。

【视图】

RADIUS 方案视图

【缺省用户角色】

network-admin

【参数】

host-name: 从 RADIUS 认证服务器的主机名，为 1~253 个字符的字符串，不区分大小写。

ipv4-address: 从 RADIUS 认证服务器的 IPv4 地址。

ipv6 ipv6-address: 从 RADIUS 认证服务器的 IPv6 地址。

port-number: 从 RADIUS 认证服务器的 UDP 端口号，取值范围为 1~65535，缺省值为 1812。

key: 与从 RADIUS 认证服务器交互的认证报文的共享密钥。

cipher: 以密文方式设置密钥。

simple: 以明文方式设置密钥，该密钥将以密文形式存储。

string: 密钥字符串，区分大小写。非 FIPS 模式下，明文密钥为 1~64 个字符的字符串；密文密钥为 1~117 个字符的字符串。FIPS 模式下，明文密钥为 15~64 个字符的字符串，密钥元素的最少组合类型为 4（必须包括数字、大写字母、小写字母以及特殊字符）；密文密钥为 15~117 个字符的字符串。

test-profile profile-name: RADIUS 服务器探测模板名称，为 1~31 个字符的字符串，区分大小写。

weight weight-value: RADIUS 服务器负载分担的权重。**weight-value** 表示权重值，取值范围为 0~100，缺省值为 0。0 表示该服务器在负载分担调度时将不被使用。开启服务器负载分担功能后，该参数才能生效，且权重值越大的服务器可以处理的认证请求报文越多。

【使用指导】

配置的从认证服务器的 UDP 端口号以及认证报文的共享密钥必须与服务器的配置保持一致。

每个 RADIUS 方案中最多支持配置 16 个从 RADIUS 认证服务器。当主服务器不可达时，设备根据从服务器的配置顺序由先到后查找状态为 **active** 的从服务器并与之交互。

RADIUS 认证服务器引用了存在的服务器探测模板后，将会触发对该服务器的探测功能。

在同一个方案中指定的主认证服务器和从认证服务器的主机名、IP 地址、端口号不能完全相同，并且各从认证服务器的主机名、IP 地址、端口号也不能完全相同。

设备与从认证服务器通信时优先使用本命令设置的共享密钥，如果此处未设置，则使用命令 **key authentication** 命令设置的共享密钥。

当 RADIUS 服务器负载分担功能处于关闭状态时，如果在认证过程中删除了正在使用的从服务器配置，则设备在与当前服务器通信超时后，将会重新按照优先级顺序开始依次查找状态为 **active** 的服务器进行通信；在 RADIUS 服务器负载分担功能处于开启状态时，如果在认证过程中修改或删除了正在使用的认证服务器配置，则设备在与当前服务器通信超时后，将会根据各服务器的权重以及服务器承载的用户负荷重新选择状态为 **active** 的服务器进行通信。

【举例】

在 RADIUS 方案 radius1 中，配置从认证服务器的 IP 地址为 10.110.1.2，使用 UDP 端口 1812 提供 RADIUS 认证/授权服务。

```
<Sysname> system-view
[Sysname] radius scheme radius1
[Sysname-radius-radius1] secondary authentication 10.110.1.2 1812
```

在 RADIUS 方案 radius2 中，配置两个从认证服务器，IP 地址分别为 10.110.1.1、10.110.1.2，且均使用 UDP 端口 1812 提供 RADIUS 认证/授权服务。

```
<Sysname> system-view
[Sysname] radius scheme radius2
[Sysname-radius-radius2] secondary authentication 10.110.1.1 1812
[Sysname-radius-radius2] secondary authentication 10.110.1.2 1812
```

【相关命令】

- **display radius scheme**
- **key** (RADIUS scheme view)
- **primary authentication** (RADIUS scheme view)
- **radius-server test-profile**

1.3.38 server-load-sharing enable

server-load-sharing enable 命令用来开启 RADIUS 服务器负载分担功能。

undo server-load-sharing enable 命令用来关闭 RADIUS 服务器负载分担功能。

【命令】

```
server-load-sharing enable
undo server-load-sharing enable
```

【缺省情况】

RADIUS 服务器负载分担功能处于关闭状态。

【视图】

RADIUS 方案视图

【缺省用户角色】

network-admin

【使用指导】

缺省情况下，RADIUS 服务器负载分担功能处于关闭状态，RADIUS 服务器的调度采用主/从模式。主/从模式下，设备优先选取状态为 **active** 的主服务器进行交互，若主服务器不可达则尝试与从服务器交互。设备尝试与从服务器交互时，按照从服务器的配置顺序依次选择，先配置的服务器将优先被选取。

在主/从模式下，设备选择服务器的逻辑比较单一。如果 RADIUS 方案中的主服务器或者某一配置顺序靠前的从服务器始终可达，则该服务器将独立承载该方案下所有用户的 AAA 业务。在大用户量下，这类服务器的负荷过重，将会影响处理用户上线的整体性能。

RADIUS 方案中开启服务器负载分担功能后，设备将根据当前各服务器承载的用户负荷调度合适的服务器发送认证/计费请求。考虑到各服务器的性能可能存在差异，设备支持管理员配置服务器时为各个服务器指定适应其性能的权重值（由 **weight** 关键字指定），权重值较大的服务器具备较大的被选取可能性。设备在处理用户认证/计费请求时，将综合各个服务器的权重值及当前用户负荷情况，按比例进行用户负荷分配并选择要交互的服务器。

需要注意的是，负载分担模式下，某台计费服务器开始对某用户计费后，该用户后续计费请求报文均会发往同一计费服务器。如果该计费服务器不可达，则直接返回计费失败。

【举例】

在 RADIUS 方案 radius1 中，开启 RADIUS 服务器负载分担功能。

```
<Sysname> system-view
[Sysname] radius scheme radius1
[Sysname-radius-radius1] server-load-sharing enable
```

【相关命令】

- **primary authentication** (RADIUS scheme view)
- **primary accounting** (RADIUS scheme view)
- **secondary authentication** (RADIUS scheme view)
- **secondary accounting** (RADIUS scheme view)

1.3.39 snmp-agent trap enable radius

snmp-agent trap enable radius 命令用来开启 RADIUS 告警功能。

undo snmp-agent trap enable radius 命令用来关闭指定的 RADIUS 告警功能。

【命令】

```
snmp-agent trap enable radius [ accounting-server-down |
accounting-server-up | authentication-error-threshold |
authentication-server-down | authentication-server-up ] *
```

```
undo snmp-agent trap enable radius [ accounting-server-down |
accounting-server-up | authentication-error-threshold |
authentication-server-down | authentication-server-up ] *
```

【缺省情况】

所有类型的 RADIUS 告警功能处于关闭状态。

【视图】

系统视图

【缺省用户角色】

network-admin

【参数】

accounting-server-down: 表示 RADIUS 计费服务器可达状态变为 down 时发送告警信息。

accounting-server-up: 表示 RADIUS 计费服务器可达状态变为 up 时发送告警信息。

authentication-error-threshold: 表示认证失败次数超过阈值时发送告警信息。该阈值为认证失败次数占认证请求总数的百分比数值，目前仅能通过 MIB 方式配置，取值范围为 1~100，缺省为 30。

authentication-server-down: 表示 RADIUS 认证服务器可达状态变为 down 时发送告警信息。

authentication-server-up: 表示 RADIUS 认证服务器可达状态变为 up 时发送告警信息。

【使用指导】

不指定任何参数时，表示开启或关闭所有类型的 RADIUS 告警功能。

开启 RADIUS 服务器告警功能后，系统将会生成以下几种告警信息：

- **RADIUS 服务器不可达的告警：**当 NAS 向 RADIUS 服务器发送计费或认证请求没有收到响应时，会重传请求，当重传次数达到最大传送次数时仍然没有收到响应时，则发送该告警信息。
- **RADIUS 服务器可达的告警：**当 **timer quiet** 定时器设定的时间到达后，NAS 将服务器的状态置为激活状态并发送该告警信息。
- **认证失败次数超过阈值的告警：**当 NAS 发现认证失败次数与认证请求总数的百分比超过阈值时，会发送该告警信息。

【举例】

开启 RADIUS 计费服务器可达状态变为 down 时的告警功能。

```
<Sysname> system-view
```

```
[Sysname] snmp-agent trap enable radius accounting-server-down
```

1.3.40 state primary

state primary 命令用来设置主 RADIUS 服务器的状态。

【命令】

```
state primary { accounting | authentication } { active | block }
```


【缺省情况】

主 RADIUS 服务器状态为 **active**。

【视图】

RADIUS 方案视图

【缺省用户角色】

network-admin

【参数】

accounting: 主 RADIUS 计费服务器。

authentication: 主 RADIUS 认证服务器。

active: 正常工作状态。

block: 通信中断状态。

【使用指导】

当 RADIUS 服务器负载分担功能处于关闭状态时，每次用户发起认证或计费，如果主服务器状态为 **active**，则设备都会首先尝试与主服务器进行通信，如果主服务器不可达，则将主服务器的状态置为 **block**，同时启动主服务器的 **timer quiet** 定时器，然后设备会严格按照从服务器的配置先后顺序依次查找状态为 **active** 的从服务器。在 **timer quiet** 定时器设定的时间到达之后，主服务器状态将由 **block** 恢复为 **active**。若该定时器超时之前，通过本命令将主服务器的状态手工设置为 **block**，则定时器超时之后主服务器状态不会自动恢复为 **active**，除非通过本命令手工将其设置为 **active**。

当 RADIUS 服务器负载分担功能处于开启状态时，设备仅根据当前各服务器承载的用户负荷调度状态为 **active** 的服务器发送认证或计费请求。

如果主服务器与所有从服务器状态都是 **block**，则采用主服务器进行认证或计费。

认证服务器的状态会影响设备对该服务器可达性探测功能的开启。当指定的服务器状态为 **active**，且该服务器通过 **radius-server test-profile** 命令成功引用了一个已存在的服务器探测模板时，则设备会开启对该服务器的可达性探测功能。当手工将该服务器状态置为 **block** 时，会关闭对该服务器的可达性探测功能。

【举例】

在 RADIUS 方案 radius1 中，设置主认证服务器的状态为 **block**。

```
<Sysname> system-view
[Sysname] radius scheme radius1
[Sysname-radius-radius1] state primary authentication block
```

【相关命令】

- **display radius scheme**
- **radius-server test-profile**
- **server-load-sharing enable**
- **state secondary**

1.3.41 state secondary

state secondary 命令用来设置从 RADIUS 服务器的状态。

【命令】

```
state secondary { accounting | authentication } [ { host-name | ipv4-address |  
ipv6 ipv6-address } [ port-number ] ] { active | block }
```

【缺省情况】

从 RADIUS 服务器状态为 **active**。

【视图】

RADIUS 方案视图

【缺省用户角色】

network-admin

【参数】

accounting: 从 RADIUS 计费服务器。

authentication: 从 RADIUS 认证服务器。

host-name: 从 RADIUS 服务器的主机名，为 1~253 个字符的字符串，不区分大小写。

ipv4-address: 从 RADIUS 服务器的 IPv4 地址。

ipv6 *ipv6-address*: 从 RADIUS 服务器的 IPv6 地址。

port-number: 从 RADIUS 服务器的 UDP 端口号，取值范围为 1~65535，从 RADIUS 计费服务器的缺省 UDP 端口号为 1813，从 RADIUS 认证服务器的缺省 UDP 端口号为 1812。

active: 正常工作状态。

block: 通信中断状态。

【使用指导】

如果不指定从服务器 IP 地址，那么本命令将会修改所有已配置的从认证服务器或从计费服务器的状态。

当 RADIUS 服务器负载分担功能处于关闭状态时，如果设备查找到的状态为 **active** 的从服务器不可达，则设备会将该从服务器的状态置为 **block**，同时启动该服务器的 **timer quiet** 定时器，并继续查找下一个状态为 **active** 的从服务器。在 **timer quiet** 定时器设定的时间到达之后，从服务器状态将由 **block** 恢复为 **active**。若该定时器超时之前，通过本命令将从服务器的状态手工设置为 **block**，则定时器超时之后从服务器状态不会自动恢复为 **active**，除非通过本命令手工将其设置为 **active**。如果所有已配置的从服务器都不可达，则本次认证或计费失败。

当 RADIUS 服务器负载分担功能处于开启状态时，设备仅根据当前各服务器承载的用户负荷调度状态为 **active** 的服务器发送认证或计费请求。

认证服务器的状态会影响设备对该服务器可达性探测功能的开启。当指定的服务器状态为 **active**，且该服务器通过 **radius-server test-profile** 命令成功引用了一个已存在的服务器探测模板时，则设备会开启对该服务器的可达性探测功能。当手工将该服务器状态置为 **block** 时，会关闭对该服务器的可达性探测功能。

【举例】

在 RADIUS 方案 radius1 中，设置从认证服务器的状态设置为 **block**。

```
<Sysname> system-view
[Sysname] radius scheme radius1
[Sysname-radius-radius1] state secondary authentication block
```

【相关命令】

- **display radius scheme**
- **radius-server test-profile**
- **server-load-sharing enable**
- **state primary**

1.3.42 stop-accounting-buffer enable (RADIUS scheme view)

stop-accounting-buffer enable 命令用来开启对无响应的 RADIUS 停止计费请求报文的缓存功能。

undo stop-accounting-buffer enable 命令用来关闭对无响应的 RADIUS 停止计费请求报文的缓存功能。

【命令】

```
stop-accounting-buffer enable
undo stop-accounting-buffer enable
```

【缺省情况】

设备缓存未得到响应的 RADIUS 停止计费请求报文。

【视图】

RADIUS 方案视图

【缺省用户角色】

network-admin

【使用指导】

设备在发送停止计费请求报文而 RADIUS 服务器没有响应时，会尝试重传该报文，最大尝试次数由 **retry** 命令设置。如果设备发送该 RADIUS 报文的最大尝试次数超过最大值后，仍然没有得到响应，则该功能处于开启状态的情况下设备会缓存该报文，然后再发起一次请求，若仍然未得到响应，则重复上述过程，一定次数（由 **retry stop-accounting** 命令设置）之后，设备将其丢弃。如果 RADIUS 方案中的某计费服务器被删除，则设备将会丢弃相应的已缓存停止计费请求报文。

【举例】

开启对无响应的 RADIUS 停止计费请求报文的缓存功能。

```
<Sysname> system-view
[Sysname] radius scheme radius1
[Sysname-radius-radius1] stop-accounting-buffer enable
```

【相关命令】

- **display stop-accounting-buffer (for RADIUS)**

- **reset stop-accounting-buffer** (for RADIUS)

1.3.43 stop-accounting-packet send-force

stop-accounting-packet send-force 命令用来配置用户下线时设备强制发送 RADIUS 计费停止报文。

undo stop-accounting-packet send-force 命令用来恢复缺省情况。

【命令】

```
stop-accounting-packet send-force
undo stop-accounting-packet send-force
```

【缺省情况】

用户下线时设备不会强制发送计费停止报文。

【视图】

RADIUS 方案视图

【缺省用户角色】

network-admin

【使用指导】

通常，RADIUS 服务器在收到用户的计费开始报文后才会生成用户表项，但有一些 RADIUS 服务器在用户认证成功后会立即生成用户表项。如果设备使用该类 RADIUS 服务器进行认证/授权/计费，则在用户认证后，因为一些原因（比如授权失败）并未发送计费开始报文，则在该用户下线时设备也不会发送 RADIUS 计费停止报文，就会导致 RADIUS 服务器上该用户表项不能被及时释放，形成服务器和设备上用户信息不一致的问题。为了解决这个问题，建议开启本功能。

开启本功能后，只要用户使用 RADIUS 服务器进行计费，且设备未向 RADIUS 服务器发送计费开始报文，则在用户下线时设备会强制发送一个 RADIUS 计费停止报文给服务器，使得服务器收到此报文后及时释放用户表项。

【举例】

在 RADIUS 方案 radius1 中，配置用户下线时设备强制发送 RADIUS 计费停止报文。

```
<Sysname> system-view
[Sysname] radius scheme radius1
[Sysname-radius-radius1] stop-accounting-packet send-force
```

【相关命令】

- **display radius scheme**

1.3.44 timer quiet (RADIUS scheme view)

timer quiet 命令用来设置服务器恢复激活状态的时间。

undo timer quiet 命令用来恢复缺省情况。

【命令】

```
timer quiet minutes
undo timer quiet
```

【缺省情况】

服务器恢复激活状态的时间为 5 分钟。

【视图】

RADIUS 方案视图

【缺省用户角色】

network-admin

【参数】

minutes: 恢复激活状态的时间，取值范围为 1~255，单位为分钟。

【使用指导】

建议合理设置服务器恢复激活状态的时间：

- 如果服务器恢复激活状态时间设置的过短，就会出现设备反复尝试与状态 **active** 但实际不可达的服务器通信而导致的认证或计费频繁失败的问题。
- 如果服务器恢复激活状态时间设置的过长，当服务器恢复可达后，设备不能及时与其进行通信，会降低对用户进行认证或计费的效率。

【举例】

在 RADIUS 方案 radius1 中，配置服务器恢复激活状态的时间为 10 分钟。

```
<Sysname> system-view
[Sysname] radius scheme radius1
[Sysname-radius-radius1] timer quiet 10
```

【相关命令】

- **display radius scheme**

1.3.45 timer realtime-accounting (RADIUS scheme view)

timer realtime-accounting 命令用来设置实时计费的时间间隔。

undo timer realtime-accounting 命令用来恢复缺省情况。

【命令】

```
timer realtime-accounting interval [ second ]
undo timer realtime-accounting
```

【缺省情况】

实时计费的时间间隔为 12 分钟。

【视图】

RADIUS 方案视图

【缺省用户角色】

network-admin

【参数】

interval: 实时计费的时间间隔，取值范围为 0~71582。

second: 表示实时计费的时间间隔以秒为单位，缺省以分钟为单位。

【使用指导】

为了对用户实施实时计费，有必要设置实时计费的时间间隔。不同的取值的处理有所不同：

- 若实时计费间隔不为 0，则每隔设定的时间，设备会向 RADIUS 服务器发送一次在线用户的计费信息。
- 若实时计费间隔设置为 0，且服务器上配置了实时计费间隔，则设备按照服务器上配置的实时计费间隔向 RADIUS 服务器发送在线用户的计费信息；如果服务器上没有配置该值，则设备不向 RADIUS 服务器发送在线用户的计费信息。

实时计费间隔的取值小，计费准确性高，但对设备和 RADIUS 服务器的性能要求就高。

表1-7 实时计费间隔与用户量之间的推荐比例关系

用户数	实时计费间隔（分钟）
1~99	3
100~499	6
500~999	12
大于等于1000	大于等于15

【举例】

在 RADIUS 方案 radius1 中，设置实时计费的时间间隔为 51 分钟。

```
<Sysname> system-view
[Sysname] radius scheme radius1
[Sysname-radius-radius1] timer realtime-accounting 51
```

【相关命令】

- **retry realtime-accounting**

1.3.46 timer response-timeout (RADIUS scheme view)

timer response-timeout 命令用来设置 RADIUS 服务器响应超时时间。

undo timer response-timeout 命令用来恢复缺省情况。

【命令】

```
timer response-timeout seconds
undo timer response-timeout
```

【缺省情况】

RADIUS 服务器响应超时时间为 3 秒。

【视图】

RADIUS 方案视图

【缺省用户角色】

network-admin

【参数】

seconds: RADIUS 服务器响应超时时间，取值范围为 1~10，单位为秒。

【使用指导】

如果在 RADIUS 请求报文传送出去一段时间后，设备还没有得到 RADIUS 服务器的响应，则有必要重传 RADIUS 请求报文，以保证用户尽可能地获得 RADIUS 服务，这段时间被称为 RADIUS 服务器响应超时时间，本命令用于调整这个时间。

需要注意的是：

- 发送 RADIUS 报文的最大尝试次数、RADIUS 服务器响应超时时间以及配置的 RADIUS 服务器总数，三者的乘积不能超过接入模块定义的用户认证超时时间，否则在 RADIUS 认证过程完成之前用户就有可能被强制下线。
- 设备在按照配置顺序尝试与下一个 RADIUS 服务器通信之前，会首先判断当前累计尝试持续时间是否达到或超过 300 秒，如果超过或达到 300 秒，将不再向下一个 RADIUS 服务器发送 RADIUS 请求报文，即认为该 RADIUS 请求发送失败。因此，为了避免某些已部署的 RADIUS 服务器由于此超时机制而无法被使用到，建议基于配置的 RADIUS 服务器总数，合理设置发送 RADIUS 报文的最大尝试次数以及 RADIUS 服务器响应超时时间。

【举例】

在 RADIUS 方案 radius1 中，设置服务器响应超时时间设置为 5 秒。

```
<Sysname> system-view
[Sysname] radius scheme radius1
[Sysname-radius-radius1] timer response-timeout 5
```

【相关命令】

- **display radius scheme**
- **retry**

1.3.47 user-name-format (RADIUS scheme view)

user-name-format 命令用来设置发送给 RADIUS 服务器的用户名格式。

undo user-name-format 命令用来恢复缺省情况。

【命令】

```
user-name-format { keep-original | with-domain | without-domain }
undo user-name-format
```

【缺省情况】

发送给 RADIUS 服务器的用户名携带 ISP 域名。

【视图】

RADIUS 方案视图

【缺省用户角色】

network-admin

【参数】

keep-original: 发送给 RADIUS 服务器的用户名与用户的输入保持一致。

with-domain: 发送给 RADIUS 服务器的用户名携带 ISP 域名。

without-domain: 发送给 RADIUS 服务器的用户名不携带 ISP 域名。

【使用指导】

接入用户通常以“*userid@isp-name*”的格式命名，“@”后面的部分为 ISP 域名，设备就是通过该域名来决定将用户归于哪个 ISP 域的。但是，有些较早期的 RADIUS 服务器不能接受携带有 ISP 域名的用户名，在这种情况下，有必要将用户名中携带的域名去除后再传送给 RADIUS 服务器。因此，设备提供此命令以指定发送给 RADIUS 服务器的用户名是否携带有 ISP 域名。

如果指定某个 RADIUS 方案不允许用户名中携带有 ISP 域名，那么请不要在两个或两个以上的 ISP 域中同时设置使用该 RADIUS 方案。否则，会出现虽然实际用户不同（在不同的 ISP 域中），但 RADIUS 服务器认为用户相同（因为传送到它的用户名相同）的错误。

在 802.1X 用户采用 EAP 认证方式的情况下，RADIUS 方案中配置的 **user-name-format** 命令无效，客户端传送给 RADIUS 服务器的用户名与用户输入的用户名保持一致。

【举例】

在 RADIUS 方案 radius1 中，设置发送给 RADIUS 服务器的用户名不得携带域名。

```
<Sysname> system-view
[Sysname] radius scheme radius1
[Sysname-radius-radius1] user-name-format without-domain
```

【相关命令】

- **display radius scheme**

1.4 HWTACACS配置命令

1.4.1 data-flow-format (HWTACACS scheme view)

data-flow-format 命令用来配置发送到 HWTACACS 服务器的数据流或者数据包的单位。

undo data-flow-format 命令用来恢复缺省情况。

【命令】

```
data-flow-format { data { byte | giga-byte | kilo-byte | mega-byte } | packet
{ giga-packet | kilo-packet | mega-packet | one-packet } } *
undo data-flow-format { data | packet }
```

【缺省情况】

数据流的单位为 **byte**，数据包的单位为 **one-packet**。

【视图】

HWTACACS 方案视图

【缺省用户角色】

network-admin

【参数】

data: 设置数据流的单位。

- **byte:** 数据流的单位为字节。

- **giga-byte:** 数据流的单位千兆字节。
- **kilo-byte:** 数据流的单位为千字节。
- **mega-byte:** 数据流的单位为兆字节。

packet: 设置数据包的单位。

- **giga-packet:** 数据包的单位为千兆包。
- **kilo-packet:** 数据包的单位为千包。
- **mega-packet:** 数据包的单位为兆包。
- **one-packet:** 数据包的单位为包。

【使用指导】

设备上配置的发送给 HWTACACS 服务器的数据流单位及数据包单位应与 HWTACACS 服务器上的流量统计单位保持一致，否则无法正确计费。

【举例】

在 HWTACACS 方案 hwt1 中，设置发往 HWTACACS 服务器的数据流的数据单位为千字节、数据包的单位为千包。

```
<Sysname> system-view
[Sysname] hwtacacs scheme hwt1
[Sysname-hwtacacs-hwt1] data-flow-format data kilo-byte packet kilo-packet
```

【相关命令】

- **display hwtacacs scheme**

1.4.2 display hwtacacs scheme

display hwtacacs scheme 命令用来查看 HWTACACS 方案的配置信息或 HWTACACS 服务相关的统计信息。

【命令】

```
display hwtacacs scheme [ hwtacacs-scheme-name [ statistics ] ]
```

【视图】

任意视图

【缺省用户角色】

```
network-admin
network-operator
```

【参数】

hwtacacs-scheme-name: HWTACACS 方案的名称，为 1~32 个字符的字符串，不区分大小写。如果不指定该参数，则显示所有 HWTACACS 方案的配置信息。

statistics: 显示 HWTACACS 服务相关的统计信息。不指定该参数，则显示 HWTACACS 方案的配置信息。

【举例】

查看所有 HWTACACS 方案的配置情况。

```
<Sysname> display hwtacacs scheme
```

Total 1 HWTACACS schemes

```
-----
HWTACACS Scheme Name : hwtac
Index : 0
Primary Auth Server:
  Host name: Not configured
  IP : 2.2.2.2          Port: 49      State: Active
  VPN Instance: Not configured
  Single-connection: Enabled
Primary Author Server:
  Host name: Not configured
  IP : 2.2.2.2          Port: 49      State: Active
  VPN Instance: Not configured
  Single-connection: Disabled
Primary Acct Server:
  Host name: Not configured
  IP : Not Configured   Port: 49      State: Block
  VPN Instance: Not configured
  Single-connection: Disabled

VPN Instance : Not configured
NAS IP Address : 2.2.2.3
Server Quiet Period(minutes) : 5
Realtime Accounting Interval(minutes) : 12
Stop-accounting packets buffering : Enabled
  Retransmission times : 100
Response Timeout Interval(seconds) : 5
Username Format : with-domain
Data flow unit : Byte
Packet unit : one
-----
```

表1-8 display hwtacacs scheme 命令显示信息描述表

字段	描述
Total 1 HWTACACS schemes	共计1个HWTACACS方案
HWTACACS Scheme Name	HWTACACS方案的名称
Index	HWTACACS方案的索引号
Primary Auth Server	主HWTACACS认证服务器
Primary Author Server	主HWTACACS授权服务器
Primary Acct Server	主HWTACACS计费服务器
Secondary Auth Server	从HWTACACS认证服务器
Secondary Author Server	从HWTACACS授权服务器
Secondary Acct Server	从HWTACACS计费服务器

字段	描述
Host name	HWTACACS服务器的主机名 未配置时，显示为Not configured
IP	HWTACACS服务器的IP地址 未配置时，显示为Not configured
Port	HWTACACS服务器的端口号 未配置时，显示缺省值
State	HWTACACS服务器目前状态 <ul style="list-style-type: none"> Active: 激活状态 Block: 静默状态
VPN Instance	（暂不支持）HWTACACS服务器或HWTACACS方案所在的VPN 未配置时，显示为Not configured
Single-connection	单连接状态 <ul style="list-style-type: none"> Enabled: 使用一条 TCP 连接与服务器通信 Disabled: 每次新建 TCP 连接与服务器通信
NAS IP Address	发送HWTACACS报文的源IP地址
Server Quiet Period(minutes)	主HWTACACS服务器恢复激活状态的时间（分钟）
Realtime Accounting Interval(minutes)	实时HWTACACS计费更新报文的发送间隔（分钟）
Stop-accounting packets buffering	HWTACACS停止计费请求报文缓存功能的开启情况
Retransmission times	发起HWTACACS停止计费请求的最大尝试次数
Response Timeout Interval(seconds)	HWTACACS服务器超时时间（秒）
Username Format	用户名格式 <ul style="list-style-type: none"> with-domain: 携带域名 without-domain: 不携带域名 keep-original: 与用户输入保持一致
Data flow unit	数据流的单位
Packet unit	数据包的单位

查看 HWTACACS 方案 tac 的统计信息。

```
<Sysname> display hwtacacs scheme tac statistics
```

```
Primary authentication server : 111.8.0.244
Round trip time:                20 seconds
Request packets:                1
Login request packets:         1
Change-password request packets: 0
Request packets including plaintext passwords: 0
Request packets including ciphertext passwords: 0
```

Response packets:	2
Pass response packets:	1
Failure response packets:	0
Get-data response packets:	0
Get-username response packets:	0
Get-password response packets:	1
Restart response packets:	0
Error response packets:	0
Follow response packets:	0
Malformed response packets:	0
Continue packets:	1
Continue-abort packets:	0
Pending request packets:	0
Timeout packets:	0
Unknown type response packets:	0
Dropped response packets:	0

Primary authorization server :111.8.0.244

Round trip time:	1 seconds
Request packets:	1
Response packets:	1
PassAdd response packets:	1
PassReply response packets:	0
Failure response packets:	0
Error response packets:	0
Follow response packets:	0
Malformed response packets:	0
Pending request packets:	0
Timeout packets:	0
Unknown type response packets:	0
Dropped response packets:	0

Primary accounting server :111.8.0.244

Round trip time:	0 seconds
Request packets:	2
Accounting start request packets:	1
Accounting stop request packets:	1
Accounting update request packets:	0
Pending request packets:	0
Response packets:	2
Success response packets:	2
Error response packets:	0
Follow response packets:	0
Malformed response packets:	0
Timeout response packets:	0
Unknown type response packets:	0
Dropped response packets:	0

表1-9 display hwtacacs scheme statistics 命令显示信息描述表

字段	描述
Primary authentication server	主HWTACACS认证服务器
Primary authorization server	主HWTACACS授权服务器
Primary accounting server	主HWTACACS计费服务器
Secondary authentication server	从HWTACACS认证服务器
Secondary authorization server	从HWTACACS授权服务器
Secondary accounting server	从HWTACACS计费服务器
Round trip time	设备处理最近一组响应报文和请求报文的时间间隔（单位为秒）
Request packets	发送的请求报文个数
Login request packets	登录认证的请求报文个数
Change-password request packets	更改密码的请求报文个数
Request packets including plaintext passwords	发送明文密码的请求报文个数
Request packets including ciphertext passwords	发送密文密码的请求报文个数
Response packets	接收到的响应报文个数
Pass response packets	表示认证通过的响应报文个数
Failure response packets	认证或授权失败的响应报文个数
Get-data response packets	表示获取数据的响应报文个数
Get-username response packets	表示获取用户名的响应报文个数
Get-password response packets	表示获取密码的响应报文个数
Restart response packets	要求重认证的响应报文个数
Error response packets	错误类型的响应报文个数
Follow response packets	Follow类型的响应报文的个数
Malformed response packets	不合法的响应报文个数
Continue packets	发送的Continue报文个数
Continue-abort packets	发送的Continue-abort报文个数
Pending request packets	等待响应的请求报文个数
Timeout response packets	超时的请求报文个数
Unknown type response packets	未知报文类型的响应报文个数
Dropped response packets	被丢弃响应报文个数
PassAdd response packets	接收到的PassAdd类型的响应报文个数。此报文表示同意授权所有请求的属性，并添加其他授权属性

字段	描述
PassReply response packets	接收到的PassReply类型的响应报文个数。此报文表示采用响应报文中指定的授权属性替换请求的授权属性
Accounting start request packets	发送的计费开始请求报文个数
Accounting stop request packets	发送的计费结束请求报文个数
Accounting update request packets	发送的计费更新报文个数
Success response packets	接收到的计费成功的响应报文个数

【相关命令】

- `reset hwtacacs statistics`

1.4.3 display stop-accounting-buffer (for HWTACACS)

display stop-accounting-buffer 命令用来显示缓存的 HWTACACS 停止计费请求报文的相关信息。

【命令】

display stop-accounting-buffer hwtacacs-scheme *hwtacacs-scheme-name*

【视图】

任意视图

【缺省用户角色】

network-admin
network-operator

【参数】

hwtacacs-scheme *hwtacacs-scheme-name*: 表示 HWTACACS 方案名，为 1~32 个字符的字符串，不区分大小写。

【举例】

显示 HWTACACS 方案 hwt1 缓存的 HWTACACS 停止计费请求报文。

```
<Sysname> display stop-accounting-buffer hwtacacs-scheme hwt1
Total entries: 2
Scheme      IP address      Username      First sending time    Attempts
hwt1        192.168.100.1    abc           23:27:16-08/31/2015   19
hwt1        192.168.90.6     bob           23:33:01-08/31/2015   20
```

表1-10 display stop-accounting-buffer 命令显示信息描述表

字段	描述
Total entries: 2	共有两条记录匹配
Scheme	HWTACACS方案名
IP address	用户IP地址

字段	描述
Username	用户名
First sending time	首次发送停止计费请求的时间
Attempts	发送停止计费请求报文的次数

【相关命令】

- **retry stop-accounting** (HWTACACS scheme view)
- **reset stop-accounting-buffer** (for HWTACACS)
- **stop-accounting-buffer enable** (HWTACACS scheme view)
- **user-name-format** (HWTACACS scheme view)

1.4.4 hwtacacs nas-ip

hwtacacs nas-ip 命令用来设置设备发送 HWTACACS 报文使用的源地址。

undo hwtacacs nas-ip 命令用来删除指定的发送 HWTACACS 报文使用的源地址。

【命令】

```
hwtacacs nas-ip { ipv4-address | ipv6 ipv6-address }
undo hwtacacs nas-ip { ipv4-address | ipv6 ipv6-address }
```

【缺省情况】

未设置发送 HWTACACS 报文使用的源地址，设备将以发送报文的接口的主 IP 地址作为源地址。

【视图】

系统视图

【缺省用户角色】

network-admin

【参数】

ipv4-address: 指定的源 IPv4 地址，应该为本机的地址，不能为全 0 地址、全 1 地址、D 类地址、E 类地址和环回地址。

ipv6 ipv6-address: 指定的源 IPv6 地址，应该为本机的地址，必须是单播地址，不能为环回地址与本地链路地址。

【使用指导】

HWTACACS 服务器上通过 IP 地址来标识接入设备，并根据收到的 HWTACACS 报文的源 IP 地址是否与服务器所管理的接入设备的 IP 地址匹配，来决定是否处理来自该接入设备的认证或计费请求。因此，为保证 HWTACACS 报文可被服务器正常接收并处理，接入设备上发送 HWTACACS 报文使用的源地址必须与 HWTACACS 服务器上指定的接入设备的 IP 地址保持一致。

为避免物理接口故障时从服务器返回的报文不可达，推荐使用 Loopback 接口地址为发送 HWTACACS 报文使用的源 IP 地址。

HWTACACS 方案视图和系统视图下均可以配置发送 HWTACACS 报文使用的源 IP 地址, 具体生效情况如下:

- HWTACACS 方案视图下配置的源 IP 地址 (通过 **nas-ip** 命令) 只对本方案有效。
- 系统视图下的配置的源 IP 地址 (通过 **hwtacacs nas-ip** 命令) 对所有 HWTACACS 方案有效。
- HWTACACS 方案视图下的设置具有更高的优先级。

系统视图下最多允许指定一个 IPv4 源地址和一个 IPv6 源地址。

【举例】

设置设备发送 HWTACACS 报文使用的源地址为 129.10.10.1。

```
<Sysname> system-view
[Sysname] hwtacacs nas-ip 129.10.10.1
```

【相关命令】

- **nas-ip** (HWTACACS scheme view)

1.4.5 hwtacacs scheme

hwtacacs scheme 命令用来创建 HWTACACS 方案, 并进入 HWTACACS 方案视图。如果指定的 HWTACACS 方案已经存在, 则直接进入 HWTACACS 方案视图。

undo hwtacacs scheme 命令用来删除指定的 HWTACACS 方案。

【命令】

```
hwtacacs scheme hwtacacs-scheme-name
undo hwtacacs scheme hwtacacs-scheme-name
```

【缺省情况】

不存在 HWTACACS 方案。

【视图】

系统视图

【缺省用户角色】

network-admin

【参数】

hwtacacs-scheme-name: HWTACACS 方案名称, 为 1~32 个字符的字符串, 不区分大小写。

【使用指导】

一个 HWTACACS 方案可以同时被多个 ISP 域引用。

最多可以配置 16 个 HWTACACS 方案。

【举例】

创建名称为 hwt1 的 HWTACACS 方案并进入相应的 HWTACACS 视图。

```
<Sysname> system-view
[Sysname] hwtacacs scheme hwt1
[Sysname-hwtacacs-hwt1]
```

【相关命令】

- `display hwtacacs scheme`

1.4.6 key (HWTACACS scheme view)

key 命令用来配置 HWTACACS 认证、授权、计费报文的共享密钥。

undo key 命令用来删除指定的 HWTACACS 报文的共享密钥。

【命令】

key { **accounting** | **authentication** | **authorization** } { **cipher** | **simple** } *string*

undo key { **accounting** | **authentication** | **authorization** }

【缺省情况】

未配置 HWTACACS 报文的共享密钥。

【视图】

HWTACACS 方案视图

【缺省用户角色】

network-admin

【参数】

accounting: 指定 HWTACACS 计费报文的共享密钥。

authentication: 指定 HWTACACS 认证报文的共享密钥。

authorization: 指定 HWTACACS 授权报文的共享密钥。

cipher: 以密文方式设置密钥。

simple: 以明文方式设置密钥，该密钥将以密文形式存储。

string: 密钥字符串，区分大小写。非 FIPS 模式下，明文密钥为 1~255 个字符的字符串；密文密钥为 1~373 个字符的字符串。FIPS 模式下，明文密钥为 15~255 个字符的字符串，密钥元素的最少组合类型为 4（必须包括数字、大写字母、小写字母以及特殊字符）；密文密钥为 15~373 个字符的字符串。

【使用指导】

必须保证设备上设置的共享密钥与 HWTACACS 服务器上的完全一致。

【举例】

在 HWTACACS 方案 hwt1 中，配置 HWTACACS 认证报文共享密钥为明文 123456TESTauth&!。

```
<Sysname> system-view
```

```
[Sysname] hwtacacs scheme hwt1
```

```
[Sysname-hwtacacs-hwt1] key authentication simple 123456TESTauth&!
```

配置 HWTACACS 授权报文共享密钥为明文 123456TESTautr&!。

```
[Sysname-hwtacacs-hwt1] key authorization simple 123456TESTautr&!
```

配置 HWTACACS 计费报文共享密钥为明文 123456TESTacct&!。

```
[Sysname-hwtacacs-hwt1] key accounting simple 123456TESTacct&!
```

【相关命令】

- `display hwtacacs scheme`

1.4.7 nas-ip (HWTACACS scheme view)

`nas-ip` 命令用来设置设备发送 HWTACACS 报文使用的源 IP 地址。

`undo nas-ip` 命令用来删除指定类型的发送 HWTACACS 报文使用的源 IP 地址。

【命令】

```
nas-ip { ipv4-address | ipv6 ipv6-address }  
undo nas-ip [ ipv6 ]
```

【缺省情况】

使用系统视图下由命令 `hwtacacs nas-ip` 指定的源地址，若系统视图下未指定源地址，则使用发送 HWTACACS 报文的接口的主 IP 地址。

【视图】

HWTACACS 方案视图

【缺省用户角色】

network-admin

【参数】

`ipv4-address`: 指定的源 IPv4 地址，应该为本机的地址，不能为全 0 地址、全 1 地址、D 类地址、E 类地址和环回地址。

`ipv6 ipv6-address`: 指定的源 IPv6 地址，应该为本机的地址，必须是单播地址，不能为环回地址与本地链路地址。

【使用指导】

HWTACACS 服务器上通过 IP 地址来标识接入设备，并根据收到的 HWTACACS 报文的源 IP 地址是否与服务器所管理的接入设备的 IP 地址匹配，来决定是否处理来自该接入设备的认证、授权、计费请求。因此，为保证 HWTACACS 报文可被服务器正常接收并处理，接入设备上发送 HWTACACS 报文使用的源地址必须与 HWTACACS 服务器上指定的接入设备的 IP 地址保持一致。

为避免物理接口故障时从服务器返回的报文不可达，推荐使用 Loopback 接口地址为发送 HWTACACS 报文使用的源 IP 地址。

HWTACACS 方案视图和系统视图下均可以配置发送 HWTACACS 报文使用的源 IP 地址，具体生效情况如下：

- HWTACACS 方案视图下配置的源 IP 地址（通过 `nas-ip` 命令）只对本方案有效。
- 系统视图下的配置的源 IP 地址（通过 `hwtacacs nas-ip` 命令）对所有 HWTACACS 方案有效。
- HWTACACS 方案视图下的设置具有更高的优先级。

一个 HWTACACS 方案视图下，最多允许指定一个 IPv4 源地址和一个 IPv6 源地址。

如果 `undo nas-ip` 命令中不指定 `ipv6` 关键字，则表示删除发送 HWTACACS 报文使用的源 IPv4 地址。

【举例】

在 HWTACACS 方案 hwt1 中，设置设备发送 HWTACACS 报文使用的源 IP 地址为 10.1.1.1。

```
<Sysname> system-view
[Sysname] hwtacacs scheme hwt1
[Sysname-hwtacacs-hwt1] nas-ip 10.1.1.1
```

【相关命令】

- **hwtacacs nas-ip**

1.4.8 primary accounting (HWTACACS scheme view)

primary accounting 命令用来配置主 HWTACACS 计费服务器。

undo primary accounting 命令用来恢复缺省情况。

【命令】

```
primary accounting { host-name | ipv4-address | ipv6 ipv6-address }
[ port-number | key { cipher | simple } string | single-connection ] *
undo primary accounting
```

【缺省情况】

未配置 HWTACACS 主计费服务器。

【视图】

HWTACACS 方案视图

【缺省用户角色】

network-admin

【参数】

host-name: 主 HWTACACS 计费服务器的主机名，为 1~253 个字符的字符串，不区分大小写。

ipv4-address: 主 HWTACACS 计费服务器的 IPv4 地址。

ipv6 *ipv6-address*: 主 HWTACACS 计费服务器的 IPv6 地址。

port-number: 主 HWTACACS 计费服务器的 TCP 端口号，取值范围为 1~65535，缺省值为 49。

key: 与主 HWTACACS 计费服务器交互的计费报文的共享密钥。

cipher: 以密文方式设置密钥。

simple: 以明文方式设置密钥，该密钥将以密文形式存储。

string: 密钥字符串，区分大小写。非 FIPS 模式下，明文密钥为 1~255 个字符的字符串；密文密钥为 1~373 个字符的字符串。FIPS 模式下，明文密钥为 15~255 个字符的字符串，密钥元素的最少组合类型为 4（必须包括数字、大写字母、小写字母以及特殊字符）；密文密钥为 15~373 个字符的字符串。

single-connection: 所有与主 HWTACACS 计费服务器交互的计费报文使用同一个 TCP 连接。如果未指定本参数，则表示每次计费都会使用一个新的 TCP 连接。

【使用指导】

配置的主计费服务器的 TCP 端口号以及计费报文的共享密钥必须与服务器的配置保持一致。

在同一个方案中指定的主计费服务器和从计费服务器的主机名、IP 地址、端口号不能完全相同。只有在设备与计费服务器没有报文交互时，才允许删除该服务器。计费服务器删除后，只对之后的计费过程有影响。

配置 **single-connection** 参数后可节省 TCP 连接资源，但有些 HWTACACS 服务器不支持这种方式，需要根据服务器支持情况进行配置。在服务器支持这种方式的情况下，建议配置 **single-connection** 参数，以提高性能和效率。

【举例】

在 HWTACACS 方案 hwt1 中，配置主 HWTACACS 计费服务器的 IP 地址为 10.163.155.12，使用 TCP 端口 49 与 HWTACACS 计费服务器通信，计费报文的共享密钥为明文 123456TESTacct&！。

```
<Sysname> system-view
[Sysname] hwtacacs scheme hwt1
[Sysname-hwtacacs-hwt1] primary accounting 10.163.155.12 49 key simple 123456TESTacct&！
```

【相关命令】

- **display hwtacacs scheme**
- **key** (HWTACACS scheme view)
- **secondary accounting**

1.4.9 primary authentication (HWTACACS scheme view)

primary authentication 命令用来配置主 HWTACACS 认证服务器。

undo primary authentication 命令用来恢复缺省情况。

【命令】

```
primary authentication { host-name | ipv4-address | ipv6 ipv6-address }
[ port-number | key { cipher | simple } string | single-connection ] *
undo primary authentication
```

【缺省情况】

未配置主 HWTACACS 认证服务器。

【视图】

HWTACACS 方案视图

【缺省用户角色】

network-admin

【参数】

host-name: 主 HWTACACS 认证服务器的主机名，为 1~253 个字符的字符串，不区分大小写。

ipv4-address: 主 HWTACACS 认证服务器的 IPv4 地址。

ipv6 ipv6-address: 主 HWTACACS 认证服务器的 IPv6 地址。

port-number: 主 HWTACACS 认证服务器的 TCP 端口号，取值范围为 1~65535，缺省值为 49。

key: 与主 HWTACACS 认证服务器交互的认证报文的共享密钥。

cipher: 以密文方式设置密钥。

simple: 以明文方式设置密钥，该密钥将以密文形式存储。

string: 密钥字符串，区分大小写。非 FIPS 模式下，明文密钥为 1~255 个字符的字符串；密文密钥为 1~373 个字符的字符串。FIPS 模式下，明文密钥为 15~255 个字符的字符串，密钥元素的最少组合类型为 4（必须包括数字、大写字母、小写字母以及特殊字符）；密文密钥为 15~373 个字符的字符串。

single-connection: 所有与主 HWTACACS 认证服务器交互的计费报文使用同一个 TCP 连接。如果未指定本参数，则表示向主 HWTACACS 计费服务器发送计费报文都会使用一个新的 TCP 连接。

【使用指导】

配置的主认证服务器的 TCP 端口号以及认证报文的共享密钥必须与服务器的配置保持一致。

在同一个方案中指定的主认证服务器和从认证服务器的主机名、IP 地址、端口号不能完全相同。

只有在设备与认证服务器没有报文交互时，才允许删除该服务器。认证服务器删除后，只对之后的认证过程有影响。

配置 **single-connection** 参数后可节省 TCP 连接资源，但有些 HWTACACS 服务器不支持这种方式，需要根据服务器支持情况进行配置。在服务器支持这种方式的情况下，建议配置 **single-connection** 参数，以提高性能和效率。

【举例】

在 HWTACACS 方案 hwt1 中，配置主 HWTACACS 认证服务器的 IP 地址为 10.163.155.13，使用 TCP 端口 49 与 HWTACACS 认证服务器通信，认证报文的共享密钥为明文 123456TESTauth&！。

```
<Sysname> system-view
[Sysname] hwtacacs scheme hwt1
[Sysname-hwtacacs-hwt1] primary authentication 10.163.155.13 49 key simple 123456TESTauth&！
```

【相关命令】

- **display hwtacacs scheme**
- **key** (HWTACACS scheme view)
- **secondary authentication**

1.4.10 primary authorization

primary authorization 命令用来配置主 HWTACACS 授权服务器。

undo primary authorization 命令用来恢复缺省情况。

【命令】

```
primary authorization { host-name | ipv4-address | ipv6 ipv6-address }
[ port-number | key { cipher | simple } string | single-connection ] *
undo primary authorization
```

【缺省情况】

未配置主 HWTACACS 授权服务器。

【视图】

HWTACACS 方案视图

【缺省用户角色】

network-admin

【参数】

host-name: 主 HWTACACS 授权服务器的主机名，为 1~253 个字符的字符串，不区分大小写。

ipv4-address: 主 HWTACACS 授权服务器的 IPv4 地址。

ipv6 ipv6-address: 主 HWTACACS 授权服务器的 IPv6 地址。

port-number: 主 HWTACACS 授权服务器的 TCP 端口号，取值范围为 1~65535，缺省值为 49。

key: 与主 HWTACACS 授权服务器交互的授权报文的共享密钥。

cipher: 以密文方式设置密钥。

simple: 以明文方式设置密钥，该密钥将以密文形式存储。

string: 密钥字符串，区分大小写。非 FIPS 模式下，明文密钥为 1~255 个字符的字符串；密文密钥为 1~373 个字符的字符串。FIPS 模式下，明文密钥为 15~255 个字符的字符串，密钥元素的最少组合类型为 4（必须包括数字、大写字母、小写字母以及特殊字符）；密文密钥为 15~373 个字符的字符串。

single-connection: 所有与主 HWTACACS 授权服务器交互的授权报文使用同一个 TCP 连接。如果未指定本参数，则表示每次授权都会使用一个新的 TCP 连接。

【使用指导】

配置的主授权服务器的 TCP 端口号以及授权报文的共享密钥必须与服务器的配置保持一致。

在同一个方案中指定的主授权服务器和从授权服务器的主机名、IP 地址、端口号不能完全相同。

只有在设备与授权服务器没有报文交互时，才允许删除该服务器。授权服务器删除后，只对之后的授权过程有影响。

配置 **single-connection** 参数后可节省 TCP 连接资源，但有些 HWTACACS 服务器不支持这种方式，需要根据服务器支持情况进行配置。在服务器支持这种方式的情况下，建议配置 **single-connection** 参数，以提高性能和效率。

【举例】

在 HWTACACS 方案 hwt1 中，配置主 HWTACACS 授权服务器的 IP 地址为 10.163.155.13，使用 TCP 端口 49 与 HWTACACS 授权服务器通信，授权报文的共享密钥为明文 123456TESTautr&!

```
<Sysname> system-view
```

```
[Sysname] hwtacacs scheme hwt1
```

```
[Sysname-hwtacacs-hwt1] primary authorization 10.163.155.13 49 key simple 123456TESTautr&!
```

【相关命令】

- **display hwtacacs scheme**
- **key** (HWTACACS scheme view)
- **secondary authorization**

1.4.11 reset hwtacacs statistics

reset hwtacacs statistics 命令用来清除 HWTACACS 协议的统计信息。

【命令】

```
reset hwtacacs statistics { accounting | all | authentication |  
authorization }
```

【视图】

用户视图

【缺省用户角色】

network-admin

【参数】

accounting: 清除 HWTACACS 协议关于计费的统计信息。

all: 清除 HWTACACS 的所有统计信息。

authentication: 清除 HWTACACS 协议关于认证的统计信息。

authorization: 清除 HWTACACS 协议关于授权的统计信息。

【举例】

清除 HWTACACS 协议的所有统计信息。

```
<Sysname> reset hwtacacs statistics all
```

【相关命令】

- **display hwtacacs scheme**

1.4.12 reset stop-accounting-buffer (for HWTACACS)

reset stop-accounting-buffer 命令用来清除缓存的 HWTACACS 停止计费请求报文。

【命令】

```
reset stop-accounting-buffer hwtacacs-scheme hwtacacs-scheme-name
```

【视图】

用户视图

【缺省用户角色】

network-admin

【参数】

hwtacacs-scheme *hwtacacs-scheme-name*: 表示指定 HWTACACS 方案的停止计费请求报文。其中, *hwtacacs-scheme-name* 为 HWTACACS 方案名, 为 1~32 个字符的字符串, 不区分大小写。

【举例】

清除缓存的 HWTACACS 方案 hwt1 的 HWTACACS 停止计费请求报文。

```
<Sysname> reset stop-accounting-buffer hwtacacs scheme hwt1
```

【相关命令】

- **display stop-accounting-buffer (for HWTACACS)**
- **stop-accounting-buffer enable (HWTACACS scheme view)**

1.4.13 retry stop-accounting (HWTACACS scheme view)

retry stop-accounting 命令用来设置发起 HWTACACS 停止计费请求的最大尝试次数。

undo retry stop-accounting 命令用来恢复缺省情况。

【命令】

```
retry stop-accounting retries
undo retry stop-accounting
```

【缺省情况】

发起 HWTACACS 停止计费请求的最大尝试次数为 100。

【视图】

HWTACACS 方案视图

【缺省用户角色】

network-admin

【参数】

retries: 允许停止计费请求无响应的最大次数，取值范围为 1~300。

【使用指导】

设备发送 HWTACACS 停止计费请求报文无响应后，将会缓存该报文并尝试重复发送该报文，当发送的停止计费请求总数达到指定的最大尝试次数之后仍未得到响应时，将其丢弃。

【举例】

在 HWTACACS 方案 hwt1 中，设置发起 HWTACACS 停止计费请求的最大尝试次数为 300。

```
<Sysname> system-view
[Sysname] hwtacacs scheme hwt1
[Sysname-hwtacacs-hwt1] retry stop-accounting 300
```

【相关命令】

- **display stop-accounting-buffer** (for HWTACACS)
- **timer response-timeout** (HWTACACS scheme view)

1.4.14 secondary accounting (HWTACACS scheme view)

secondary accounting 命令用来配置从 HWTACACS 计费服务器。

undo secondary accounting 命令用来删除指定的从 HWTACACS 计费服务器。

【命令】

```
secondary accounting { host-name | ipv4-address | ipv6 ipv6-address }
[ port-number | key { cipher | simple } string | single-connection ] *
undo secondary accounting [ { host-name | ipv4-address | ipv6 ipv6-address }
[ port-number ] ]
```

【缺省情况】

未配置从 HWTACACS 计费服务器。

【视图】

HWTACACS 方案视图

【缺省用户角色】

network-admin

【参数】

host-name: 从 HWTACACS 计费服务器的主机名，为 1~253 个字符的字符串，不区分大小写。

ipv4-address: 从 HWTACACS 计费服务器的 IPv4 地址。

ipv6 ipv6-address: 从 HWTACACS 计费服务器的 IPv6 地址。

port-number: 从 HWTACACS 计费服务器的端口号，取值范围为 1~65535，缺省值为 49。

key: 与从 HWTACACS 计费服务器交互的计费报文的共享密钥。

cipher: 以密文方式设置密钥。

simple: 以明文方式设置密钥，该密钥将以密文形式存储。

string: 密钥字符串，区分大小写。非 FIPS 模式下，明文密钥为 1~255 个字符的字符串；密文密钥为 1~373 个字符的字符串。FIPS 模式下，明文密钥为 15~255 个字符的字符串，密钥元素的最少组合类型为 4（必须包括数字、大写字母、小写字母以及特殊字符）；密文密钥为 15~373 个字符的字符串。

single-connection: 所有与从 HWTACACS 计费服务器交互的计费报文使用同一个 TCP 连接。如果未指定本参数，则表示每次计费都会使用一个新的 TCP 连接。

【使用指导】

配置的从计费服务器的 TCP 端口号以及计费报文的共享密钥必须与服务器的配置保持一致。

每个 HWTACACS 方案中最多支持配置 16 个从 HWTACACS 计费服务器。当主服务器不可达时，设备根据从服务器的配置顺序由先到后查找状态为 **active** 的从服务器并与之交互。

如果不指定任何参数，则 **undo** 命令将删除所有从计费服务器。

在同一个方案中指定的主计费服务器和从计费服务器的主机名、IP 地址、端口号不能完全相同，并且各从计费服务器的主机名、IP 地址、端口号也不能完全相同。

配置 **single-connection** 参数后可节省 TCP 连接资源，但有些 TACACS 服务器不支持这种方式，需要根据服务器支持情况进行配置。在服务器支持这种方式的情况下，建议配置 **single-connection** 参数，以提高性能和效率。

只有在设备与计费服务器没有报文交互时，才允许删除该服务器。计费服务器删除后，只对之后的计费过程有影响。

【举例】

在 HWTACACS 方案 hwt1 中，配置从 HWTACACS 计费服务器的 IP 地址为 10.163.155.12，使用 TCP 端口 49 与 HWTACACS 计费服务器通信，计费报文的共享密钥为明文 123456TESTacct&!

```
<Sysname> system-view
```

```
[Sysname] hwtacacs scheme hwt1
```

```
[Sysname-hwtacacs-hwt1] secondary accounting 10.163.155.12 49 key simple 123456TESTacct&!
```

【相关命令】

- **display hwtacacs scheme**

- **key** (HWTACACS scheme view)
- **primary accounting** (HWTACACS scheme view)

1.4.15 secondary authentication (HWTACACS scheme view)

secondary authentication 命令用来配置从 HWTACACS 认证服务器。

undo secondary authentication 命令用来删除指定的从 HWTACACS 认证服务器。

【命令】

```
secondary authentication { host-name | ipv4-address | ipv6 ipv6-address }
[ port-number | key { cipher | simple } string | single-connection ] *
undo secondary authentication [ { host-name | ipv4-address | ipv6
ipv6-address } [ port-number ] ]
```

【缺省情况】

未配置从 HWTACACS 认证服务器。

【视图】

HWTACACS 方案视图

【缺省用户角色】

network-admin

【参数】

host-name: 从 HWTACACS 认证服务器的主机名，为 1~253 个字符的字符串，不区分大小写。

ipv4-address: 从 HWTACACS 认证服务器的 IPv4 地址。

ipv6 ipv6-address: 从 HWTACACS 认证服务器的 IPv6 地址。

port-number: 从 HWTACACS 认证服务器的 TCP 端口号，取值范围为 1~65535，缺省值为 49。

key: 与从 HWTACACS 认证服务器交互的认证报文的共享密钥。

cipher: 以密文方式设置密钥。

simple: 以明文方式设置密钥，该密钥将以密文形式存储。

string: 密钥字符串，区分大小写。非 FIPS 模式下，明文密钥为 1~255 个字符的字符串；密文密钥为 1~373 个字符的字符串。FIPS 模式下，明文密钥为 15~255 个字符的字符串，密钥元素的最少组合类型为 4（必须包括数字、大写字母、小写字母以及特殊字符）；密文密钥为 15~373 个字符的字符串。

single-connection: 所有与从 HWTACACS 认证服务器交互的认证报文使用同一个 TCP 连接。如果未指定本参数，则表示每次认证都会使用一个新的 TCP 连接。

【使用指导】

配置的从认证服务器的 TCP 端口号以及认证报文的共享密钥必须与服务器的配置保持一致。

每个 HWTACACS 方案中最多支持配置 16 个从 HWTACACS 认证服务器。当主服务器不可达时，设备根据从服务器的配置顺序由先到后查找状态为 **active** 的从服务器并与之交互。

如果不指定任何参数，则 **undo** 命令将删除所有从认证服务器。

在同一个方案中指定的主认证服务器和从认证服务器的主机名、IP 地址、端口号不能完全相同，并且各从认证服务器的主机名、IP 地址、端口号也不能完全相同。

配置 **single-connection** 参数后可节省 TCP 连接资源，但有些 TACACS 服务器不支持这种方式，需要根据服务器支持情况进行配置。在服务器支持这种方式的情况下，建议配置 **single-connection** 参数，以提高性能和效率。

只有在设备与认证服务器没有报文交互时，才允许删除该服务器。认证服务器删除后，只对之后的认证过程有影响。

【举例】

在 HWTACACS 方案 hwt1 中，配置从 HWTACACS 认证服务器的 IP 地址为 10.163.155.13，使用 TCP 端口 49 与 HWTACACS 认证服务器通信，认证报文的共享密钥为明文 123456TESTauth&！。

```
<Sysname> system-view
[Sysname] hwtacacs scheme hwt1
[Sysname-hwtacacs-hwt1] secondary authentication 10.163.155.13 49 key simple
123456TESTauth&！
```

【相关命令】

- **display hwtacacs scheme**
- **key** (HWTACACS scheme view)
- **primary authentication** (HWTACACS scheme view)

1.4.16 secondary authorization

secondary authorization 命令用来配置从 HWTACACS 授权服务器。

undo secondary authorization 命令用来删除指定的从 HWTACACS 授权服务器。

【命令】

```
secondary authorization { host-name | ipv4-address | ipv6 ipv6-address }
[ port-number | key { cipher | simple } string | single-connection ] *
undo secondary authorization [ { host-name | ipv4-address | ipv6
ipv6-address } [ port-number ] ]
```

【缺省情况】

未配置从 HWTACACS 授权服务器。

【视图】

HWTACACS 方案视图

【缺省用户角色】

network-admin

【参数】

host-name: 从 HWTACACS 授权服务器的主机名，为 1~253 个字符的字符串，不区分大小写。

ipv4-address: 从 HWTACACS 授权服务器的 IPv4 地址。

ipv6 ipv6-address: 从 HWTACACS 授权服务器的 IPv6 地址。

port-number: 从 HWTACACS 授权服务器的 TCP 端口号，取值范围为 1~65535，缺省值为 49。

key: 与从 HWTACACS 授权服务器交互的授权报文的共享密钥。

cipher: 以密文方式设置密钥。

simple: 以明文方式设置密钥，该密钥将以密文形式存储。

string: 密钥字符串，区分大小写。非 FIPS 模式下，明文密钥为 1~255 个字符的字符串；密文密钥为 1~373 个字符的字符串。FIPS 模式下，明文密钥为 15~255 个字符的字符串，密钥元素的最少组合类型为 4（必须包括数字、大写字母、小写字母以及特殊字符）；密文密钥为 15~373 个字符的字符串。

single-connection: 所有与从 HWTACACS 授权服务器交互的授权报文使用同一个 TCP 连接。如果未指定本参数，则表示每次授权都会使用一个新的 TCP 连接。

【使用指导】

配置的从授权服务器的 TCP 端口号以及授权报文的共享密钥必须与服务器的配置保持一致。

每个 HWTACACS 方案中最多支持配置 16 个从 HWTACACS 授权服务器。当主服务器不可达时，设备根据从服务器的配置顺序由先到后查找状态为 **active** 的从服务器并与之交互。

如果不指定任何参数，则 **undo** 命令将删除所有从授权服务器。

在同一个方案中指定的主授权服务器和从授权服务器的主机名、IP 地址、端口号不能完全相同，并且各从授权服务器的主机名、IP 地址、端口号也不能完全相同。

配置 **single-connection** 参数后可节省 TCP 连接资源，但有些 TACACS 服务器不支持这种方式，需要根据服务器支持情况进行配置。在服务器支持这种方式的情况下，建议配置 **single-connection** 参数，以提高性能和效率。

只有在设备与授权服务器没有报文交互时，才允许删除该服务器。授权服务器删除后，只对之后的授权过程有影响。

【举例】

在 HWTACACS 方案 hwt1 中，配置从 HWTACACS 授权服务器的 IP 地址为 10.163.155.13，使用 TCP 端口 49 与 HWTACACS 授权服务器通信，授权报文的共享密钥为明文 123456TESTautr&!

```
<Sysname> system-view
[Sysname] hwtacacs scheme hwt1
[Sysname-hwtacacs-hwt1] secondary authorization 10.163.155.13 49 key simple
123456TESTautr&!
```

【相关命令】

- **display hwtacacs scheme**
- **key** (HWTACACS scheme view)
- **primary authorization** (HWTACACS scheme view)

1.4.17 stop-accounting-buffer enable (HWTACACS scheme view)

stop-accounting-buffer enable 命令用来开启对无响应的 HWTACACS 停止计费请求报文的缓存功能。

undo stop-accounting-buffer enable 命令用来关闭对无响应的 HWTACACS 停止计费请求报文的缓存功能。

【命令】

```
stop-accounting-buffer enable
undo stop-accounting-buffer enable
```

【缺省情况】

设备缓存未得到响应的 HWTACACS 计费请求报文。

【视图】

HWTACACS 方案视图

【缺省用户角色】

network-admin

【使用指导】

开启对无响应的 HWTACACS 停止计费请求报文的缓存功能后，设备在发送停止计费请求报文而 HWTACACS 服务器没有响应时，会将其缓存在本机上，然后发送直到 HWTACACS 计费服务器产生响应，或者在发送的次数达到指定的次数限制（由 **retry stop-accounting** 命令设置）后将其丢弃。

如果 HWTACACS 方案中的某计费服务器被删除，则设备将会丢弃相应的已缓存停止计费报文。

【举例】

开启对无响应的 HWTACACS 停止计费请求报文的缓存功能。

```
<Sysname> system-view
[Sysname] hwtacacs scheme hwt1
[Sysname-hwtacacs-hwt1] stop-accounting-buffer enable
```

【相关命令】

- **display stop-accounting-buffer** (for HWTACACS)
- **reset stop-accounting-buffer** (for HWTACACS)

1.4.18 timer quiet (HWTACACS scheme view)

timer quiet 命令用来设置服务器恢复激活状态的时间。

undo timer quiet 命令用来恢复缺省情况。

【命令】

```
timer quiet minutes
undo timer quiet
```

【缺省情况】

服务器恢复激活状态的时间为 5 分钟。

【视图】

HWTACACS 方案视图

【缺省用户角色】

network-admin

【参数】

minutes: 恢复激活状态的时间，取值范围为 1~255，单位为分钟。

【举例】

设置服务器恢复激活状态的时间为 10 分钟。

```
<Sysname> system-view
[Sysname] hwtacacs scheme hwt1
[Sysname-hwtacacs-hwt1] timer quiet 10
```

【相关命令】

- **display hwtacacs scheme**

1.4.19 timer realtime-accounting (HWTACACS scheme view)

timer realtime-accounting 命令用来设置实时计费的时间间隔。

undo timer realtime-accounting 命令用来恢复缺省情况。

【命令】

```
timer realtime-accounting minutes
undo timer realtime-accounting
```

【缺省情况】

实时计费的时间间隔为 12 分钟。

【视图】

HWTACACS 方案视图

【缺省用户角色】

network-admin

【参数】

minutes: 实时计费的时间间隔，取值范围为 0~60，单位为分钟。0 表示设备不向 HWTACACS 服务器发送在线用户的计费信息。

【使用指导】

为了对用户实施实时计费，有必要设置实时计费的时间间隔。在设置了该属性以后，每隔设定的时间，设备会向 HWTACACS 服务器发送一次在线用户的计费信息。

实时计费间隔的取值小，计费准确性高，但对设备和 HWTACACS 服务器的性能要求就高。

表1-11 实时计费间隔与用户量之间的推荐比例关系

用户数	实时计费间隔（分钟）
1~99	3
100~499	6
500~999	12
大于等于1000	大于等于15

【举例】

在 HWTACACS 方案 hwt1 中，设置实时计费的时间间隔为 51 分钟。

```
<Sysname> system-view
[Sysname] hwtacacs scheme hwt1
[Sysname-hwtacacs-hwt1] timer realtime-accounting 51
```

【相关命令】

- **display hwtacacs scheme**

1.4.20 timer response-timeout (HWTACACS scheme view)

timer response-timeout 命令用来设置 HWTACACS 服务器响应超时时间。

undo timer response-timeout 命令用来恢复缺省情况。

【命令】

```
timer response-timeout seconds
undo timer response-timeout
```

【缺省情况】

HWTACACS 服务器响应超时时间为 5 秒。

【视图】

HWTACACS 方案视图

【缺省用户角色】

network-admin

【参数】

seconds: HWTACACS 服务器响应超时时间，取值范围为 1~300，单位为秒。

【使用指导】

由于 HWTACACS 是基于 TCP 实现的，因此，服务器响应超时或 TCP 超时都可能导致与 HWTACACS 服务器的连接断开。

HWTACACS 服务器响应超时时间与配置的 HWTACACS 服务器总数的乘积不能超过接入模块定义的用户认证超时时间，否则在 HWTACACS 认证过程完成之前用户就有可能被强制下线。

【举例】

在 HWTACACS 方案 hwt1 中，设置 HWTACACS 服务器响应超时时间为 30 秒。

```
<Sysname> system-view
[Sysname] hwtacacs scheme hwt1
[Sysname-hwtacacs-hwt1] timer response-timeout 30
```

【相关命令】

- **display hwtacacs scheme**

1.4.21 user-name-format (HWTACACS scheme view)

user-name-format 命令用来设置发送给 HWTACACS 服务器的用户名格式。

undo user-name-format 命令用来恢复缺省情况。

【命令】

```
user-name-format { keep-original | with-domain | without-domain }  
undo user-name-format
```

【缺省情况】

发送给 HWTACACS 服务器的用户名携带 ISP 域名。

【视图】

HWTACACS 方案视图

【缺省用户角色】

network-admin

【参数】

keep-original: 发送给 HWTACACS 服务器的用户名与用户输入的保持一致。

with-domain: 发送给 HWTACACS 服务器的用户名携带 ISP 域名。

without-domain: 发送给 HWTACACS 服务器的用户名不携带 ISP 域名。

【使用指导】

接入用户通常以“userid@isp-name”的格式命名，“@”后面的部分为 ISP 域名，设备就是通过该域名来决定将用户归于哪个 ISP 域的。但是，有些 HWTACACS 服务器不能接受携带有 ISP 域名的用户名，在这种情况下，有必要将用户名中携带的域名去除后再传送给 HWTACACS 服务器。因此，设备提供此命令以指定发送给 HWTACACS 服务器的用户名是否携带有 ISP 域名。

如果指定某个 HWTACACS 方案不允许用户名中携带有 ISP 域名，那么请不要在两个乃至两个以上的 ISP 域中同时设置使用该 HWTACACS 方案。否则，会出现虽然实际用户不同（在不同的 ISP 域中），但 HWTACACS 服务器认为用户相同（因为传送到它的用户名相同）的错误。

【举例】

在 HWTACACS 方案 hwt1 中，设置发送给 HWTACACS 服务器的用户名不携带 ISP 域名。

```
<Sysname> system-view  
[Sysname] hwtacacs scheme hwt1  
[Sysname-hwtacacs-hwt1] user-name-format without-domain
```

【相关命令】

- **display hwtacacs scheme**

1.5 LDAP配置命令

1.5.1 attribute-map

attribute-map 命令用来在 LDAP 方案中引用 LDAP 属性映射表。

undo attribute-map 命令用来恢复缺省情况。

【命令】

```
attribute-map map-name
```

undo attribute-map

【缺省情况】

未引用任何 LDAP 属性映射表。

【视图】

LDAP 方案视图

【缺省用户角色】

network-admin

【参数】

map-name: LDAP 属性映射表的名称，为 1~31 个字符的字符串，不区分大小写。

【使用指导】

在使用 LDAP 授权方案的情况下，可以通过在 LDAP 方案中引用 LDAP 属性映射表，将 LDAP 授权服务器下发给用户的 LDAP 属性映射为 AAA 模块可以解析的某类属性。

一个 LDAP 方案视图中只能引用一个 LDAP 属性映射表，后配置的生效。

如果在 LDAP 授权过程中修改了引用的 LDAP 属性映射表，或者修改了引用的 LDAP 属性映射表的内容，则该修改对当前的授权过程不会生效，只对修改后新的 LDAP 授权过程生效。

【举例】

在 LDAP 方案 ldap1 中，引用名称为 map1 的 LDAP 属性映射表。

```
<Sysname> system-view
[Sysname] ldap scheme test
[Sysname-ldap-test] attribute-map map1
```

【相关命令】

- **display ldap-scheme**
- **ldap attribute-map**

1.5.2 authentication-server

authentication-server 命令用来指定 LDAP 认证服务器。

undo authentication-server 命令用来恢复缺省情况。

【命令】

```
authentication-server server-name
undo authentication-server
```

【缺省情况】

未指定 LDAP 认证服务器。

【视图】

LDAP 方案视图

【缺省用户角色】

network-admin

【参数】

server-name: LDAP 服务器的名称, 为 1~64 个字符的字符串, 不区分大小写。

【使用指导】

一个 LDAP 方案视图下仅能指定一个 LDAP 认证服务器, 多次执行本命令, 最后一次执行的命令生效。

【举例】

在 LDAP 方案 ldap1 中, 指定 LDAP 认证服务器为 ccc。

```
<Sysname> system-view
[Sysname] ldap scheme ldap1
[Sysname-ldap-ldap1] authentication-server ccc
```

【相关命令】

- **display ldap scheme**
- **ldap server**

1.5.3 authorization-server

authorization-server 命令用来指定 LDAP 授权服务器。

undo authorization-server 命令用来恢复缺省情况。

【命令】

```
authorization-server server-name
undo authorization-server
```

【缺省情况】

未指定 LDAP 授权服务器。

【视图】

LDAP 方案视图

【缺省用户角色】

network-admin

【参数】

server-name: LDAP 服务器的名称, 为 1~64 个字符的字符串, 不区分大小写。

【使用指导】

一个 LDAP 方案视图下仅能指定一个 LDAP 授权服务器, 多次执行本命令, 最后一次执行的命令生效。

【举例】

在 LDAP 方案 ldap1 中, 指定 LDAP 授权服务器为 ccc。

```
<Sysname> system-view
[Sysname] ldap scheme ldap1
[Sysname-ldap-ldap1] authorization-server ccc
```


【相关命令】

- `display ldap scheme`
- `ldap server`

1.5.4 display ldap scheme

`display ldap scheme` 命令用来查看 LDAP 方案的配置信息。

【命令】

`display ldap scheme [ldap-scheme-name]`

【视图】

任意视图

【缺省用户角色】

network-admin
network-operator

【参数】

ldap-scheme-name: LDAP 方案的名称，为 1~32 个字符的字符串，不区分大小写。如果不指定该参数，则显示所有 LDAP 方案的配置信息。

【举例】

查看所有 LDAP 方案的配置信息。

```
<Sysname> display ldap scheme
```

```
Total 1 LDAP schemes
```

```
-----
LDAP scheme name           : aaa
Authentication server      : aaa
  IP                        : 1.1.1.1
  Port                      : 111
  VPN instance              : Not configured
LDAP protocol version      : LDAPv3
Server timeout interval    : 10 seconds
Login account DN           : Not configured
Base DN                    : Not configured
Search scope                : all-level
User searching parameters:
  User object class         : Not configured
  Username attribute        : cn
  Username format           : with-domain
Authorization server        : aaa
  IP                        : 1.1.1.1
  Port                      : 111
  VPN instance              : Not configured
LDAP protocol version      : LDAPv3
Server timeout interval    : 10 seconds
```

```

Login account DN      : Not configured
Base DN              : Not configured
Search scope         : all-level
User searching parameters:
  User object class   : Not configured
  Username attribute   : cn
  Username format     : with-domain
Attribute map        : map1

```

表1-12 display ldap scheme 命令显示信息描述表

字段	描述
Total 1 LDAP schemes	总共有1个LDAP方案
LDAP Scheme Name	LDAP方案名称
Authentication Server	LDAP认证服务器名称 未配置时，显示为Not configured
Authorization server	LDAP授权服务器名称 未配置时，显示为Not configured
IP	LDAP认证服务器的IP地址 未配置认证服务器IP时，IP地址显示为Not configured
Port	LDAP认证服务器的端口号 未配置认证服务器IP时，端口号显示为缺省值
VPN Instance	（暂不支持）VPN实例名称 未配置时，显示为Not configured
LDAP Protocol Version	LDAP协议的版本号（LDAPv2、LDAPv3）
Server Timeout Interval	LDAP服务器连接超时时间（单位为秒）
Login Account DN	管理员用户的DN
Base DN	用户DN查询的起始DN
Search Scope	用户DN查询的范围（all-level: 所有子目录查询，single-level: 下级目录查询）
User Searching Parameters	用户查询参数
User Object Class	查询用户DN时使用的用户对象类型 未配置时，显示为Not configured
Username Attribute	用户登录帐号的属性类型
Username Format	发送给服务器的用户名格式
Attribute map	引用的LDAP属性映射表名称 未配置时，显示为Not configured

1.5.5 ip

ip 命令用来配置 LDAP 服务器的 IP 地址。

undo ip 命令用来恢复缺省情况。

【命令】

```
ip ip-address [ port port-number ]  
undo ip
```

【缺省情况】

未配置 LDAP 服务器的 IP 地址。

【视图】

LDAP 服务器视图

【缺省用户角色】

network-admin

【参数】

ip-address: LDAP 服务器的 IP 地址。

port port-number: LDAP 服务器所使用的 TCP 端口号, 取值范围为 1~65535, 缺省值为 389。

【使用指导】

需保证设备上的 LDAP 服务端口与 LDAP 服务器上使用的端口设置一致。

更改后的服务器 IP 地址和端口号, 只对更改之后进行的 LDAP 认证生效。

【举例】

配置 LDAP 服务器 ccc 的 IP 地址为 192.168.0.10、端口号为 4300。

```
<Sysname> system-view  
[Sysname] ldap server ccc  
[Sysname-ldap-server-ccc] ip 192.168.0.10 port 4300
```

【相关命令】

- **ldap server**

1.5.6 ipv6

ipv6 命令用来配置 LDAP 服务器的 IPv6 地址。

undo ipv6 命令用来恢复缺省情况。

【命令】

```
ipv6 ipv6-address [ port port-number ]  
undo ipv6
```

【缺省情况】

未配置 LDAP 服务器的 IP 地址。

【视图】

LDAP 服务器视图

【缺省用户角色】

network-admin

【参数】

ipv6-address: LDAP 服务器的 IPv6 地址。

port *port-number*: LDAP 服务器所使用的 TCP 端口号, 取值范围为 1~65535, 缺省值为 389。

【使用指导】

需保证设备上的 LDAP 服务端口与 LDAP 服务器上使用的端口设置一致。

更改后的服务器 IP 地址和端口号, 只对更改之后的 LDAP 认证生效。

【举例】

配置 LDAP 服务器 ccc 的 IPv6 地址为 1:2::3:4、端口号为 4300。

```
<Sysname> system-view
[Sysname] ldap server ccc
[Sysname-ldap-server-ccc] ipv6 1:2::3:4 port 4300
```

【相关命令】

- **ldap server**

1.5.7 ldap attribute-map

ldap attribute-map 命令用来创建 LDAP 属性映射表, 并进入 LDAP 属性映射表视图。如果指定的 LDAP 属性映射表已经存在, 则直接进入 LDAP 属性映射表视图。

undo ldap attribute-map 命令用来删除指定的 LDAP 属性映射表。

【命令】

```
ldap attribute-map map-name
undo ldap attribute-map map-name
```

【缺省情况】

不存在 LDAP 属性映射表。

【视图】

系统视图

【缺省用户角色】

network-admin

【参数】

map-name: LDAP 属性映射表的名称, 为 1~31 个字符的字符串, 不区分大小写。

【使用指导】

一个 LDAP 的属性映射表中可以添加多个 LDAP 属性映射表项, 每个表项表示一个 LDAP 属性和一个 AAA 属性的映射关系。

可以通过多次执行本命令配置多个 LDAP 的属性映射表。

【举例】

创建名称为 map1 的 LDAP 属性映射表，并进入该属性映射表视图。

```
<Sysname> system-view
[Sysname] ldap attribute-map map1
[Sysname-ldap-map-map1]
```

【相关命令】

- **attribute-map**
- **ldap scheme**
- **map**

1.5.8 ldap scheme

ldap scheme 命令用来创建 LDAP 方案，并进入 LDAP 方案视图。如果指定的 LDAP 方案已经存在，则直接进入 LDAP 方案视图。

undo ldap scheme 命令用来删除指定的 LDAP 方案。

【命令】

```
ldap scheme ldap-scheme-name
undo ldap scheme ldap-scheme-name
```

【缺省情况】

不存在 LDAP 方案。

【视图】

系统视图

【缺省用户角色】

network-admin

【参数】

ldap-scheme-name: LDAP 方案的名称，为 1~32 个字符的字符串，不区分大小写。

【使用指导】

一个 LDAP 方案可以同时被多个 ISP 域引用。

系统最多支持配置 16 个 LDAP 方案。

【举例】

创建名称为 ldap1 的 LDAP 方案并进入其视图。

```
<Sysname> system-view
[Sysname] ldap scheme ldap1
[Sysname-ldap-ldap1]
```

【相关命令】

- **display ldap scheme**

1.5.9 ldap server

ldap server 用来创建 LDAP 服务器，并进入 LDAP 服务器视图。如果指定的 LDAP 服务器已经存在，则直接进入 LDAP 服务器视图。

undo ldap server 命令用来删除指定的 LDAP 服务器。

【命令】

```
ldap server server-name
undo ldap server server-name
```

【缺省情况】

不存在 LDAP 服务器。

【视图】

系统视图

【缺省用户角色】

network-admin

【参数】

server-name: LDAP 服务器的名称，为 1~64 个字符的字符串，不区分大小写。

【举例】

创建 LDAP 服务器 ccc 并进入其视图。

```
<Sysname> system-view
[Sysname] ldap server ccc
[Sysname-ldap-server-ccc]
```

【相关命令】

- **display ldap scheme**

1.5.10 login-dn

login-dn 命令用来配置具有管理员权限的用户 DN。

undo login-dn 命令用来恢复缺省情况。

【命令】

```
login-dn dn-string
undo login-dn
```

【缺省情况】

未配置具有管理员权限的用户 DN。

【视图】

LDAP 服务器视图

【缺省用户角色】

network-admin

【参数】

dn-string: 具有管理员权限的用户 DN，是绑定服务器时使用的用户标识名，为 1~255 个字符的字符串，不区分大小写。

【使用指导】

设备上的管理员 DN 必须与服务器上管理员的 DN 一致。

更改后的管理员 DN，只对更改之后的 LDAP 认证生效。

【举例】

在 LDAP 服务器视图 ccc 下，配置管理员权限的用户 DN 为 uid=test, ou=people, o=example, c=city。

```
<Sysname> system-view
[Sysname] ldap server ccc
[Sysname-ldap-server-ccc] login-dn uid=test,ou=people,o=example,c=city
```

【相关命令】

- **display ldap scheme**

1.5.11 login-password

login-password 命令用来配置 LDAP 认证中，绑定服务器时所使用的具有管理员权限的用户密码。

undo login-password 命令用来恢复缺省情况。

【命令】

```
login-password { cipher | simple } string
undo login-password
```

【缺省情况】

未配置具有管理权限的用户密码。

【视图】

LDAP 服务器视图

【缺省用户角色】

network-admin

【参数】

cipher: 表示以密文方式设置密码。

simple: 表示以明文方式设置密码，该密码将以密文形式存储。

string: 密码字符串，区分大小写。明文密码为 1~128 个字符的字符串，密文密码为 1~201 个字符的字符串。

【使用指导】

该命令只有在配置了 **login-dn** 的情况下生效。当未配置 **login-dn** 时，该命令不生效。

【举例】

在 LDAP 服务器视图 ccc 下，配置具有管理员权限的用户密码为明文 abcdefg。

```
<Sysname> system-view
```

```
[Sysname] ldap server ccc  
[Sysname-ldap-server-ccc] login-password simple abcdefg
```

【相关命令】

- **display ldap scheme**
- **login-dn**

1.5.12 map

map 命令用来配置 LDAP 属性映射表项。

undo map 命令用来删除指定的 LDAP 属性映射表项。

【命令】

```
map ldap-attribute ldap-attribute-name [ prefix prefix-value delimiter  
delimiter-value ] aaa-attribute { user-group | user-profile }  
undo map [ ldap-attribute ldap-attribute-name ]
```

【缺省情况】

未指定 LDAP 属性映射关系。

【视图】

LDAP 属性映射表视图

【缺省用户角色】

network-admin

【参数】

ldap-attribute *ldap-attribute-name*：表示要映射的 LDAP 属性。其中，*ldap-attribute-name* 表示 LDAP 属性名称，为 1~63 个字符的字符串，不区分大小写。

prefix *prefix-value* **delimiter** *delimiter-value*：表示按照一定的格式提取 LDAP 属性字符串中的内容映射为 AAA 属性。其中，*prefix-value* 表示 LDAP 属性字符串中的某内容前缀（例如 cn=），为 1~7 个字符的字符串，不区分大小写；*delimiter-value* 表示 LDAP 属性字符串中的内容分隔符（例如逗号）。若不指定该可选参数，则表示要将一个完整的 LDAP 属性字符串映射为指定的 AAA 属性。

aaa-attribute：表示要映射为的 AAA 属性。

user-group：表示 User group 类型的 AAA 属性。

user-profile：表示 User Profile 类型的 AAA 属性。

【使用指导】

如果某 LDAP 服务器下发给用户的属性不能被 AAA 模块解析，则该属性将被忽略。因此，需要通过本命令指定要获取哪些 LDAP 属性，以及 LDAP 服务器下发的这些属性将被 AAA 模块解析为什么类型的 AAA 属性，具体映射为哪种类型的 AAA 属性由实际应用需求决定。

一个 LDAP 服务器属性只能映射为一个 AAA 属性，但不同的 LDAP 服务器属性可映射为同一个 AAA 属性。

如果 **undo map** 命令中不指定 **ldap-attribute** 参数，则表示删除所有的 LDAP 属性映射表项。

【举例】

在 LDAP 属性映射表视图 map1 下，配置将 LDAP 服务器属性 memberof 按照前缀为 cn=、分隔符为逗号 (,) 的格式提取出的内容映射成 AAA 属性 User group。

```
<Sysname> system-view
[Sysname] ldap attribute-map map1
[Sysname-ldap-map-map1] map ldap-attribute memberof prefix cn= delimiter ; aaa-attribute
user-group
```

【相关命令】

- **ldap attribute-map**
- **user-group**
- **user-profile**（安全命令参考/User Profile）

1.5.13 protocol-version

protocol-version 命令用来配置 LDAP 认证中所支持的 LDAP 协议的版本号。

undo protocol-version 命令用来恢复缺省情况。

【命令】

```
protocol-version { v2 | v3 }
undo protocol-version
```

【缺省情况】

LDAP 版本号为 LDAPv3。

【视图】

LDAP 服务器视图

【缺省用户角色】

network-admin

【参数】

v2：表示 LDAP 协议版本号为 LDAPv2。

v3：表示 LDAP 协议版本号为 LDAPv3。

【使用指导】

为保证 LDAP 认证成功，请保证设备上的 LDAP 版本号与 LDAP 服务器上使用的版本号一致。

更改后的服务器版本号，只对更改之后的 LDAP 认证生效。

Microsoft 的 LDAP 服务器只支持 LDAPv3，配置 LDAP 版本为 v2 时无效。

【举例】

在 LDAP 服务器视图 ccc 下，配置 LDAP 协议版本号为 LDAPv2。

```
<Sysname> system-view
[Sysname] ldap server ccc
[Sysname-ldap-server-ccc] protocol-version v2
```

【相关命令】

- **display ldap scheme**

1.5.14 search-base-dn

search-base-dn 命令用来配置用户查询的起始 DN。

undo search-base-dn 命令用来恢复缺省情况。

【命令】

search-base-dn *base-dn*

undo search-base-dn

【缺省情况】

未指定用户查询的起始 DN。

【视图】

LDAP 服务器视图

【缺省用户角色】

network-admin

【参数】

base-dn: 查询待认证用户的起始 DN 值，为 1~255 个字符的字符串，不区分大小写。

【举例】

在 LDAP 服务器视图 ccc 下，配置用户查询的起始 DN 为 dc=ldap,dc=com。

```
<Sysname> system-view
```

```
[Sysname] ldap server ccc
```

```
[Sysname-ldap-server-ccc] search-base-dn dc=ldap,dc=com
```

【相关命令】

- **display ldap scheme**
- **ldap server**

1.5.15 search-scope

search-scope 命令用来配置用户查询的范围。

undo search-scope 命令用来恢复缺省情况。

【命令】

search-scope { **all-level** | **single-level** }

undo search-scope

【缺省情况】

用户查询的范围为 **all-level**。

【视图】

LDAP 服务器视图

【缺省用户角色】

network-admin

【参数】

all-level: 表示在起始 DN 的所有子目录下进行查询。

single-level: 表示只在起始 DN 的下一级子目录下进行查询。

【举例】

在 LDAP 服务器视图 ccc 下，配置在起始 DN 的所有子目录下查询 LDAP 认证用户。

```
<Sysname> system-view
[Sysname] ldap server ccc
[Sysname-ldap-server-ccc] search-scope all-level
```

【相关命令】

- **display ldap scheme**
- **ldap server**

1.5.16 server-timeout

server-timeout 命令用来配置 LDAP 服务器连接超时时间，即认证、授权时等待 LDAP 服务器回应的最大时间。

undo server-timeout 命令用来恢复缺省情况。

【命令】

```
server-timeout time-interval
undo server-timeout
```

【缺省情况】

LDAP 服务器连接超时时间为 10 秒。

【视图】

LDAP 服务器视图

【缺省用户角色】

network-admin

【参数】

time-interval: LDAP 服务器连接超时时间，取值范围为 5~20，单位为秒。

【使用指导】

更改后的连接超时时间，只对更改之后的 LDAP 认证生效。

【举例】

在 LDAP 服务器视图 ccc 下，配置 LDAP 服务器连接超时时间为 15 秒。

```
<Sysname> system-view
[Sysname] ldap server ccc
[Sysname-ldap-server-ccc] server-timeout 15
```

【相关命令】

- **display ldap scheme**

1.5.17 user-parameters

user-parameters 命令用来配置 LDAP 用户查询的属性参数，包括用户名属性、用户名格式和自定义用户对象类型。

undo user-parameters 命令用来将指定的 LDAP 用户查询的属性参数恢复为缺省值。

【命令】

```
user-parameters { user-name-attribute { name-attribute | cn | uid } |  
user-name-format { with-domain | without-domain } | user-object-class  
object-class-name }  
undo user-parameters { user-name-attribute | user-name-format |  
user-object-class }
```

【缺省情况】

user-name-attribute 为 **cn**；**user-name-format** 为 **without-domain**；未指定自定义 **user-object-class**，根据使用的 LDAP 服务器的类型使用各服务器缺省的用户对象类型。

【视图】

LDAP 服务器视图

【缺省用户角色】

network-admin

【参数】

user-name-attribute { *name-attribute* | **cn** | **uid** }：表示用户名的属性类型。其中，*name-attribute* 表示属性类型值，为 1~64 个字符的字符串，不区分大小写；**cn** 表示用户登录帐号的属性为 **cn**（Common Name）；**uid** 表示用户登录帐号的属性为 **uid**（User ID）。

user-name-format { **with-domain** | **without-domain** }：表示发送给服务器的用户名格式。其中，**with-domain** 表示发送给服务器的用户名带 ISP 域名；**without-domain** 表示发送给服务器的用户名不带 ISP 域名。

user-object-class *object-class-name*：表示查询用户 DN 时使用的用户对象类型。其中，*object-class-name* 表示对象类型值，为 1~64 个字符的字符串，不区分大小写。

【使用指导】

如果 LDAP 服务器上的用户名不包含域名，必须配置 **user-name-format** 为 **without-domain**，将用户名的域名去除后再传送给 LDAP 服务器；如果包含域名则需配置 **user-name-format** 为 **with-domain**。

【举例】

在 LDAP 服务器视图 **ccc** 下，配置用户对象类型为 **person**。

```
<Sysname> system-view  
[Sysname] ldap server ccc  
[Sysname-ldap-server-ccc] user-parameters user-object-class person
```

【相关命令】

- **display ldap scheme**
- **login-dn**

1.6 RADIUS服务器配置命令

1.6.1 display radius-server active-client

display radius-server active-client 命令用来显示处于激活状态的 RADIUS 客户端信息。

【命令】

display radius-server active-client

【视图】

任意视图

【缺省用户角色】

network-admin
network-operator

【使用指导】

可以通过本命令查看设备作为 RADIUS 服务器时，可用于认证的 RADIUS 客户端信息。

【举例】

显示所有处于激活状态的 RADIUS 客户端信息。
<Sysname> display radius-server active-client
Total 2 RADIUS clients.
Client IP: 2.2.2.2
Client IP: 3.3.3.3

表1-13 display radius-server active-client 命令显示信息描述表

字段	描述
Total 2 RADIUS clients	共计2个RADIUS客户端
Client IP	RADIUS客户端IP地址

【相关命令】

- radius-server client

1.6.2 display radius-server active-user

display radius-server active-user 命令用来显示处于激活状态的 RADIUS 用户信息。

【命令】

display radius-server active-user [*user-name*]

【视图】

任意视图

【缺省用户角色】

network-admin

【参数】

user-name: RADIUS 用户名，为 1~55 个字符的字符串，区分大小写，用户名不能携带域名，不能包括符号“\”、“|”、“/”、“:”、“*”、“?”、“<”、“>”和“@”，且不能为“a”、“al”或“all”。若不指定该参数，则显示所有 RADIUS 用户信息。

【使用指导】

可以通过本命令查看设备作为 RADIUS 服务器时，用于验证接入用户身份的 RADIUS 用户信息。

【举例】

显示用户名为 test 的处于激活状态的 RADIUS 用户信息。

```
<Sysname> display radius-server active-user test
Total 1 RADIUS users matched.

Username: test
  Description: A network access user from company cc
  Authorization attributes:
    VLAN ID: 2
    ACL number: 2000
  Validity period:
    Expiration time: 2015/04/03-18:00:00
```

显示所有处于激活状态的 RADIUS 用户信息。

```
<Sysname> display radius-server active-user
Total 2 RADIUS users matched.

Username: 123
  Description: A network access user from company cc
  Authorization attributes:
    VLAN ID: 2
    ACL number: 3000
  Validity period:
    Expiration time: 2016/04/03-18:00:00

Username: 456
  Description: A network access user from company cc
  Authorization attributes:
    VLAN ID: 2
    ACL number: 3000
  Validity period:
    Expiration time: 2016/04/03-18:00:00
```

表1-14 display radius-server active-user 命令显示信息描述表

字段	描述
Username	RADIUS用户名
Description	用户的描述信息
Authorization attributes	用户授权属性

字段	描述
VLAN ID	授权VLAN
ACL number	授权ACL
Validity period	用户有效期
Expiration time	有效期的结束日期和时间

【相关命令】

- `local-user`

1.6.3 radius-server activate

radius-server activate 命令用来激活 RADIUS 服务器配置，即激活当前的 RADIUS 客户端和 RADIUS 用户配置。

【命令】

radius-server activate

【视图】

系统视图

【缺省用户角色】

network-admin

【使用指导】

设备启动后会自动激活已有的 RADIUS 客户端和 RADIUS 用户配置，其中的 RADIUS 用户配置是由设备上的网络接入类本地用户信息直接生成。之后若对 RADIUS 客户端和网络接入类本地用户进行了增加、修改或删除操作，则都需要使用此命令对其进行激活，否则更新后的配置无法生效。

执行此命令后，会导致 RADIUS 服务器进程重启。RADIUS 服务器进程重启期间，设备无法作为 RADIUS 服务器为用户提供认证服务。

【举例】

激活 RADIUS 服务器配置。

```
<Sysname> system-view
```

```
[Sysname] radius-server activate
```

【相关命令】

- `display radius-server active-client`
- `display radius-server active-user`

1.6.4 radius-server client

radius-server client 命令用来指定 RADIUS 客户端。

undo radius-server client 命令用来删除指定的 RADIUS 客户端。

【命令】

```
radius-server client ip ipv4-address key { cipher | simple } string
undo radius-server client { all | ip ipv4-address }
```

【缺省情况】

未指定 RADIUS 客户端。

【视图】

系统视图

【缺省用户角色】

network-admin

【参数】

ip ipv4-address: RADIUS 客户端的 IPv4 地址，不能为 0.X.X.X 和 127.X.X.X，以及 A、B、C 类以外的地址。

key: 指定与 RADIUS 客户端通信的共享密钥。

cipher: 表示以密文方式设置密钥。

simple: 表示以明文方式设置密钥。

string: 密钥字符串，区分大小写。明文密钥为 1~64 个字符的字符串；密文密钥为 1~117 个字符的字符串。

all: 指定所有 RADIUS 客户端。

【使用指导】

RADIUS 服务器上指定的 RADIUS 客户端 IP 地址必须和 RADIUS 客户端上配置的发送 RADIUS 报文的源 IP 地址保持一致。

RADIUS 服务器上指定的共享密钥必须和 RADIUS 客户端上配置的与 RADIUS 服务器通信的共享密钥保持一致。

可通过多次执行本命令，指定多个 RADIUS 客户端。

【举例】

配置 RADIUS 客户端 IP 地址为 2.2.2.2，共享密钥为明文 test。

```
<Sysname> system-view
```

```
[Sysname] radius-server client ip 2.2.2.2 key simple test
```

【相关命令】

- **display radius-server active-client**

1.7 连接记录策略配置命令

1.7.1 aaa connection-recording policy

aaa connection-recording policy 命令用来创建连接记录策略，并进入连接记录策略视图。

如果连接记录策略已经存在，则直接进入连接记录策略视图。

undo aaa connection-recording policy 命令用来删除连接记录策略。

【命令】

```
aaa connection-recording policy
undo aaa connection-recording policy
```

【缺省情况】

不存在连接记录策略。

【视图】

系统视图

【缺省用户角色】

network-admin

【使用指导】

创建连接记录策略后，当设备作为 Telnet 客户端或者 FTP/SSH/SFTP 客户端与服务器端成功建立连接时，系统会按照策略中指定的计费方案向 AAA 服务器发送计费开始报文，断开连接时发送计费结束报文。

【举例】

```
# 创建连接记录策略，并进入其视图。
<Sysname> system-view
[Sysname] aaa connection-recording policy
[sysname-connection-recording-policy]
```

【相关命令】

- **accounting hwtacacs-scheme**
- **display aaa connection-recording policy**

1.7.2 accounting hwtacacs-scheme

accounting hwtacacs-scheme 命令用来指定连接记录策略采用的 HWTACACS 计费方案。
undo accounting 命令用来恢复缺省情况。

【命令】

```
accounting hwtacacs-scheme hwtacacs-scheme-name
undo accounting
```

【缺省情况】

未指定连接记录策略采用的 HWTACACS 计费方案。

【视图】

连接记录策略视图

【缺省用户角色】

network-admin

【参数】

hwtacacs-scheme-name：表示 HWTACACS 方案名，为 1~32 个字符的字符串，不区分大小写。

【使用指导】

修改后的 HWTACACS 计费方案, 仅对设备与远程服务器新建的 Telnet/FTP/SSH/SFTP 连接生效。
对于同一个连接, 若系统已经将计费开始报文成功发送给 HWTACACS 方案中指定的 HWTACACS 服务器, 则后续的计费停止报文也会发送给该服务器。

多次执行本命令, 最后一次执行的命令生效。

连接记录业务处理过程中, 系统发送给 AAA 服务器的计费报文中封装的是用户输入的原始用户名, 因此计费方案中通过 **user-name-format** 命令设置的用户名格式并不生效。

【举例】

创建连接记录策略, 并在其视图下指定连接记录策略采用的 HWTACACS 计费方案为 tac。

```
<Sysname> system-view
[Sysname] aaa connection-recording policy
[sysname-connection-recording-policy] accounting hwtacacs-scheme tac
```

【相关命令】

- **aaa connection-recording policy**
- **display aaa connection-recording policy**

1.7.3 display aaa connection-recording policy

display aaa connection-recording policy 用来显示记录连接策略的配置信息。

【命令】

```
display aaa connection-recording policy
```

【视图】

任意视图

【缺省用户角色】

```
network-admin
network-operator
```

【举例】

显示记录连接策略的配置信息。

```
<Sysname> display aaa connection-recording policy
Connection-recording policy:
  Accounting scheme: HWTACACS=tac1
```

【相关命令】

- **aaa connection-recording policy**
- **accounting hwtacacs-scheme**

目 录

1 802.1X	1-1
1.1 802.1X配置命令	1-1
1.1.1 display dot1x	1-1
1.1.2 display dot1x connection	1-5
1.1.3 display dot1x mac-address	1-8
1.1.4 dot1x	1-9
1.1.5 dot1x access-user log enable	1-10
1.1.6 dot1x after-mac-auth max-attempt	1-11
1.1.7 dot1x authentication-method	1-11
1.1.8 dot1x auth-fail eapol	1-12
1.1.9 dot1x auth-fail vlan	1-13
1.1.10 dot1x critical eapol	1-14
1.1.11 dot1x critical vlan	1-15
1.1.12 dot1x critical-voice-vlan	1-16
1.1.13 dot1x domain-delimiter	1-16
1.1.14 dot1x ead-assistant enable	1-17
1.1.15 dot1x ead-assistant free-ip	1-18
1.1.16 dot1x ead-assistant url	1-19
1.1.17 dot1x eapol untag	1-20
1.1.18 dot1x guest-vlan	1-21
1.1.19 dot1x guest-vlan-delay	1-22
1.1.20 dot1x handshake	1-22
1.1.21 dot1x handshake reply enable	1-23
1.1.22 dot1x handshake secure	1-24
1.1.23 dot1x mac-binding	1-25
1.1.24 dot1x mac-binding enable	1-26
1.1.25 dot1x mandatory-domain	1-26
1.1.26 dot1x max-user	1-27
1.1.27 dot1x multicast-trigger	1-28
1.1.28 dot1x port-control	1-29
1.1.29 dot1x port-method	1-29
1.1.30 dot1x quiet-period	1-30
1.1.31 dot1x re-authenticate	1-31

1.1.32 dot1x re-authenticate manual	1-31
1.1.33 dot1x re-authenticate server-unreachable keep-online	1-32
1.1.34 dot1x retry	1-33
1.1.35 dot1x timer	1-33
1.1.36 dot1x timer reauth-period (interface view).....	1-35
1.1.37 dot1x unicast-trigger	1-36
1.1.38 dot1x user-ip freeze.....	1-37
1.1.39 reset dot1x guest-vlan.....	1-38
1.1.40 reset dot1x statistics	1-38

1 802.1X

1.1 802.1X配置命令

1.1.1 display dot1x

display dot1x 命令用来显示 802.1X 的相关信息。

【命令】

```
display dot1x [ sessions | statistics ] [ interface interface-type
interface-number ]
```

【视图】

任意视图

【缺省用户角色】

network-admin
network-operator

【参数】

sessions: 显示 802.1X 的会话连接信息。

statistics: 显示 802.1X 的相关统计信息。

interface *interface-type* *interface-number*: 显示指定端口的 802.1X 信息。
interface-type *interface-number* 为端口类型和端口编号。

【使用指导】

如果不指定参数 **sessions** 或者 **statistics**，则显示 802.1X 的所有信息，包括会话连接信息、相关统计信息和配置信息等。

如果不指定 **interface** 参数，则显示所有端口上的 802.1X 信息。

【举例】

显示 802.1X 的所有信息。

```
<Sysname> display dot1x
Global 802.1X parameters:
  802.1X authentication    : Enabled
  CHAP authentication      : Enabled
  Max-tx period            : 30 s
  Handshake period        : 15 s
  Quiet timer              : Disabled
    Quiet period           : 60 s
  Supp timeout             : 30 s
  Server timeout          : 100 s
  Reauth period            : 3600 s
  Max auth requests        : 2
  EAD assistant function   : Disabled
```

```

URL                : http://www.dwsoft.com
Free IP            : 6.6.6.0          255.255.255.0
EAD timeout        : 30 min
Domain delimiter   : @
Online 802.1X wired users : 1

```

GigabitEthernet1/0/1 is link-up

```

802.1X authentication : Enabled
Handshake             : Enabled
Handshake reply       : Disabled
Handshake security    : Disabled
Unicast trigger       : Disabled
Periodic reauth       : Disabled
Port role             : Authenticator
Authorization mode     : Auto
Port access control   : Port-based
Multicast trigger     : Enabled
Mandatory auth domain : Not configured
Guest VLAN            : 3
Auth-Fail VLAN        : Not configured
Critical VLAN         : Not configured
Critical voice VLAN   : Disabled
Add Guest VLAN delay  : Disabled
Re-auth server-unreachable : Logoff
Max online users      : 4294967295
User IP freezing      : Disabled
Reauth period         : 0 s
Send Packets Without Tag : Disabled
Max Attempts Fail Number : 0
Guest VSI             : Not configured
Auth-Fail VSI         : Not configured
Critical VSI          : Not configured
Add Guest VSI delay   : Disabled

```

EAPOL packets: Tx 3, Rx 3

Sent EAP Request/Identity packets : 1

EAP Request/Challenge packets: 1

EAP Success packets: 1

EAP Failure packets: 0

Received EAPOL Start packets : 1

EAPOL LogOff packets: 1

EAP Response/Identity packets : 1

EAP Response/Challenge packets: 1

Error packets: 0

Online 802.1X users: 1

MAC address	Auth state
0001-0000-0000	Authenticated

表1-1 display dot1x 命令显示信息描述表

字段	描述
Global 802.1X parameters	全局802.1X参数配置信息
802.1X authentication	全局802.1X的开启状态
CHAP authentication	启用EAP终结方式，并采用CHAP认证方法
EAP authentication	启用EAP中继方式，并支持所有EAP认证方法
PAP authentication	启用EAP终结方式，并采用PAP认证方法
Max-tx period	用户名请求超时定时器的值
Handshake period	握手定时器的值
Quiet timer	静默定时器的开启状态
Quiet period	静默定时器的值
Supp timeout	客户端认证超时定时器的值
Server timeout	认证服务器超时定时器的值
Reauth period	重认证定时器的值
Max auth requests	设备向接入用户发送认证请求报文的最大次数
EAD assistant function	EAD快速部署辅助功能的开启状态 S5000E-X、S5110V2-SI和S5000V3-EI系列交换机不支持该参数
URL	用户HTTP访问的重定向URL S5110V2-SI和S5000V3-EI系列交换机不支持该参数
Free IP	用户通过认证之前可访问的网段 S5110V2-SI和S5000V3-EI系列交换机不支持该参数
EAD timeout	EAD老化定时器超时时间 S5000E-X、S5110V2-SI和S5000V3-EI系列交换机不支持该参数
Domain delimiter	域名分隔符
Online 802.1X wired users	在线802.1X有线用户和正在发起认证的802.1X有线用户的总数
GigabitEthernet1/0/1 is link-up	端口GigabitEthernet1/0/1的链路状态
802.1X authentication	端口上802.1X的开启状态
Handshake	在线用户握手功能的开启状态
Handshake reply	在线用户握手回应功能的开启状态
Handshake security	安全握手功能的开启状态
Unicast trigger	802.1X单播触发功能的开启状态
Periodic reauth	周期性重认证功能的开启状态
Port role	该端口担当认证端的作用，目前仅支持作为认证端

字段	描述
Authorization mode	端口的授权状态 <ul style="list-style-type: none"> • Force-Authorized: 强制授权状态 • Auto: 自动识别状态 • Force-Unauthorized: 强制非授权状态
Port access control	端口接入控制方式 <ul style="list-style-type: none"> • MAC-based: 基于 MAC 地址对接入用户进行认证 • Port-based: 基于端口对接入用户进行认证
Multicast trigger	802.1X组播触发功能的开启状态
Mandatory auth domain	端口上的接入用户使用的强制认证域
Guest VLAN	端口配置的Guest VLAN，若此功能未配置则显示Not configured
Auth-fail VLAN	端口配置的Auth-Fail VLAN，若此功能未配置则显示Not configured
Critical VLAN	端口配置的Critical VLAN，若此功能未配置则显示Not configured
Critical voice VLAN	端口配置802.1X认证的Critical Voice VLAN功能的开启状态，包括如下取值： <ul style="list-style-type: none"> • Enabled: 打开 • Disabled: 关闭 S5110V2-SI和S5000V3-EI系列交换机不支持该参数
Add Guest VLAN delay	端口延迟加入Guest VLAN功能的状态和触发原因： <ul style="list-style-type: none"> • EAPOL: 802.1X 协议报文触发端口延迟加入 802.1X Guest VLAN • NewMac: 源 MAC 地址未知的报文触发端口延迟加入 802.1X Guest VLAN • ALL: 802.1X 协议报文或源 MAC 地址未知的报文触发端口延迟加入 802.1X Guest VLAN • Disabled: 端口延迟加入 802.1X Guest VLAN 功能处于关闭状态
Re-auth server-unreachable	重认证时服务器不可达对802.1X在线用户采取的动作
Max online users	本端口最多可容纳的接入用户数
User IP freezing	802.1X用户IP地址冻结功能的开启状态 <ul style="list-style-type: none"> • Enabled: 打开 • Disabled: 关闭
Reauth period	端口上802.1X周期性重认证定时器的值
Send Packets Without Tag	端口发送802.1X协议报文不携带VLAN Tag的开启状态： <ul style="list-style-type: none"> • Enabled: 打开 • Disabled: 关闭

字段	描述
Max Attempts Fail Number	MAC地址认证成功的用户进行802.1X认证的最大尝试次数
Guest VSI	（暂不支持）端口配置的Guest VSI，若此功能未配置则显示Not configured
Auth-Fail VSI	（暂不支持）端口配置的Auth-Fail VSI，若此功能未配置则显示Not configured
Critical VSI	（暂不支持）端口配置的Critical VSI，若此功能未配置则显示Not configured
Add Guest VSI delay	<p>（暂不支持）端口延迟加入Guest VSI功能的状态和触发原因：</p> <ul style="list-style-type: none"> • EAPOL only: 802.1X 协议报文触发端口延迟加入 802.1X Guest VSI • NewMAC only: 源 MAC 地址未知的报文触发端口延迟加入 802.1X Guest VSI • EAPOL or NewMAC: 802.1X 协议报文或源 MAC 地址未知的报文触发端口延迟加入 802.1X Guest VSI • Disabled: 端口延迟加入 802.1X Guest VSI 功能处于关闭状态
EAPOL packets	EAPOL报文数目。Tx表示发送的报文数目；Rx表示接受的报文数目
Sent EAP Request/Identity packets	发送的EAP Request/Identity报文数
EAP Request/Challenge packets	发送的EAP Request/Challenge报文数
EAP Success packets	发送的EAP Success报文数
EAP Fail packets	发送的EAP Failure报文数
Received EAPOL Start packets	接收的EAPOL Start报文数
EAPOL LogOff packets	接收的EAPOL LogOff报文数
EAP Response/Identity packets	接收的EAP Response/Identity报文数
EAP Response/Challenge packets	接收的EAP Response/Challenge报文数
Error packets	接收的错误报文数
Online 802.1X users	端口上的在线802.1X用户和正在发起认证的802.1X用户的总数
MAC address	802.1X用户的MAC地址
Auth state	802.1X用户的认证状态

1.1.2 display dot1x connection

display dot1x connection 命令用来显示当前 802.1X 在线用户的详细信息。

【命令】

```
display dot1x connection [ open ] [ interface interface-type  
interface-number | slot slot-number | user-mac mac-address | user-name  
name-string ]
```

【视图】

任意视图

【缺省用户角色】

network-admin
network-operator

【参数】

open: 只显示在开放认证模式下使用不存在的用户名或者错误的密码接入的 802.1X 用户信息。若不指定本参数，则显示设备上所有 802.1X 在线用户的信息。

interface interface-type interface-number: 显示指定端口的 802.1X 在线用户信息。其中 *interface-type interface-number* 表示端口类型和端口编号。若不指定本参数，则显示设备上所有 802.1X 在线用户的信息。

slot slot-number: 显示指定成员设备上的 802.1X 在线用户信息。*slot-number* 表示设备在 IRF 中的成员编号。若不指定该参数，则表示所有成员设备上的 802.1X 在线用户信息。

user-mac mac-address: 显示指定 MAC 地址的 802.1X 在线用户信息。其中 *mac-address* 表示用户的 MAC 地址，格式为 H-H-H。若不指定本参数，则显示设备上所有 802.1X 在线用户的信息。

user-name name-string: 显示指定用户名的 802.1X 在线用户信息。其中 *name-string* 表示用户名，为 1~253 个字符的字符串，区分大小写。若不指定本参数，则显示设备上所有 802.1X 在线用户的信息。

【举例】

显示所有 802.1X 在线用户信息。

```
<Sysname> display dot1x connection  
Total connections: 1
```

```
Slot ID: 1  
User MAC address: 0015-e9a6-7cfe  
Access interface: GigabitEthernet1/0/1  
Username: ias  
User access state: Successful  
Authentication domain: aaa  
IPv4 address: 192.168.1.1  
IPv6 address: 2000:0:0:0:1:2345:6789:abcd  
Authentication method: CHAP  
Initial VLAN: 1  
Authorization untagged VLAN: 6  
Authorization tagged VLAN list: 1 to 5 7 9 11 13 15 17 19 21 23 25 27 29 31 33 29 31 33  
                                35 37 40 to 100  
  
Authorization VSI: N/A  
Authorization ACL ID: 3001
```

Authorization user profile: N/A
 Authorization CAR: N/A
 Termination action: Default
 Session timeout period: 2 s
 Online from: 2013/03/02 13:14:15
 Online duration: 0h 2m 15s

表1-2 display dot1x connection 命令显示信息描述表

字段	描述
Total connections	在线802.1X认证用户个数
User MAC address	用户的MAC地址
Access interface	用户的接入接口名称
Username	用户名
User access state	用户的接入状态 <ul style="list-style-type: none"> Successful: 802.1X 认证成功并接入 Open: 使用不存在的用户名或者错误的密码进行开放认证并接入
Authentication domain	认证时使用的ISP域的名称
IPv4 address	用户IP地址 若未获取到用户的IP地址，则不显示该字段
IPv6 address	用户IPv6地址 若未获取到用户的IP地址，则不显示该字段
Authentication method	802.1X系统的认证方法 <ul style="list-style-type: none"> CHAP: 启用 EAP 终结方式，并采用 CHAP 认证方法 EAP: 启用 EAP 中继方式，并支持所有 EAP 认证方法 PAP: 启用 EAP 终结方式，并采用 PAP 认证方法
Initial VLAN	初始的VLAN
Authorization untagged VLAN	授权的untagged VLAN
Authorization tagged VLAN list	授权的tagged VLAN列表
Authorization VSI	（暂不支持）授权的VSI列表
Authorization ACL ID	授权的ACL的编号，若未授权成功，则在ACL编号后显示“(NOT effective)”
Authorization user profile	授权用户的User profile名称
Authorization CAR	（暂不支持）当服务器未授权用户CAR属性时，该字段显示为N/A。
Termination action	服务器下发的终止动作类型： <ul style="list-style-type: none"> Default: 会话超时时长到达后，强制用户下线。但是，如果设备上开启了周期性重认证功能，且设备上配置的重认证定时器值小于用户会话超时时长，则端口会以重认证定时器的值为周期向该端口在线 802.1X 用户发起重认证，而不会强制用户下线 Radius-Request: 会话超时时长到达后，要求 802.1X 用户进行重认证 用户采用本地认证时，该字段显示为Default

字段	描述
Session timeout period	服务器下发的会话超时时长, 该时间到达之后, 用户所在的会话将会被删除, 之后, 对该用户所采取的动作, 由 Terminate action 字段的取值决定
Online from	用户的上线时间
Online duration	用户的在线时长

1.1.3 display dot1x mac-address

display dot1x mac-address 命令用来显示指定类型的 VLAN 中的 802.1X 用户的 MAC 地址信息。

【命令】

```
display dot1x mac-address { auth-fail-vlan | critical-vlan | guest-vlan }
[ interface interface-type interface-number ]
```

【视图】

任意视图

【缺省用户角色】

network-admin
network-operator

【参数】

auth-fail-vlan: 显示 802.1X Auth-Fail VLAN 中的用户 MAC 地址信息。

critical-vlan: 显示 802.1X Critical VLAN 中的用户 MAC 地址信息。

guest-vlan: 显示 802.1X Guest VLAN 中的用户 MAC 地址信息。

interface interface-type interface-number: 显示 VLAN 中指定端口的 802.1X 用户的 MAC 地址信息。其中 *interface-type interface-number* 表示端口类型和端口编号。若不指定本参数, 则显示指定类型的 VLAN 中所有端口的 802.1X 用户的 MAC 地址信息。

【使用指导】

查询到的 MAC 地址数量以及 MAC 地址明细为粗略统计, 当有大量用户频繁进行认证时可能不能完全精准显示。

【举例】

显示所有 802.1X Auth-Fail VLAN 中的用户的 MAC 地址信息。

```
<Sysname> display dot1x mac-address auth-fail-vlan
Total MAC addresses: 10
Interface: GigabitEthernet1/0/1          Auth-Fail VLAN: 3    Aging time: N/A
MAC addresses: 8
    0800-2700-9427    0800-2700-2341    0800-2700-2324    0800-2700-2351
    0800-2700-5627    0800-2700-2251    0800-2700-8624    0800-2700-3f51

Interface: GigabitEthernet1/0/2          Auth-Fail VLAN: 5    Aging time: 30 sec
MAC addresses: 2
```

表1-3 display dot1x mac-address 命令显示信息描述表

字段	描述
Total MAC addresses	指定类型的VLAN中的所有MAC地址总数
Interface	用户的接口名称
Type VLAN	显示802.1X用户所在的VLAN信息，Type包含如下取值： <ul style="list-style-type: none"> Auth-fail VLAN Critical VLAN Guest VLAN
Aging time	MAC地址老化时间，单位秒。N/A表示该地址不老化
MAC addresses	MAC地址数
xxxx-xxxx-xxxx	MAC地址

【相关命令】

- dot1x auth-fail vlan
- dot1x critical vlan
- dot1x guest-vlan

1.1.4 dot1x

dot1x 命令用来开启端口上或全局的 802.1X。

undo dot1x 命令用来关闭端口上或全局的 802.1X。

【命令】

```
dot1x
undo dot1x
```

【缺省情况】

所有端口以及全局的 802.1X 都处于关闭状态。

【视图】

系统视图
二层以太网接口视图

【缺省用户角色】

network-admin

【使用指导】

只有同时开启全局和端口的 802.1X 后，802.1X 的配置才能在端口上生效。

【举例】

开启全局的 802.1X。

```
<Sysname> system-view
[Sysname] dot1x
# 开启端口 GigabitEthernet1/0/1 上的 802.1X。
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] dot1x
[Sysname-GigabitEthernet1/0/1] quit
```

【相关命令】

- **display dot1x**

1.1.5 dot1x access-user log enable

dot1x access-user log enable 命令用来开启 802.1X 接入用户日志信息功能。

undo dot1x access-user log enable 命令用来关闭 802.1X 接入用户日志信息功能。

【命令】

```
dot1x access-user log enable [ abnormal-logoff | failed-login |
normal-logoff | successful-login ] *
undo dot1x access-user log enable [ abnormal-logoff | failed-login |
normal-logoff | successful-login ] *
```

【缺省情况】

802.1X 接入用户日志信息功能处于关闭状态。

【视图】

系统视图

【缺省用户角色】

network-admin

【参数】

abnormal-logoff: 802.1X 接入用户异常下线（例如实时计费失败下线，重认证失败下线等）的日志信息。

failed-login: 802.1X 接入用户上线失败的日志信息。

normal-logoff: 802.1X 接入用户正常下线的日志信息。

successful-login: 802.1X 接入用户上线成功时的日志信息

【使用指导】

为了防止设备输出过多的 802.1X 接入用户日志信息，一般情况下建议关闭此功能。

配置本命令时，如果未指定任何参数，将同时开启或关闭本命令所有参数对应的日志功能。

【举例】

开启 802.1X 接入用户上线失败的日志信息。

```
<Sysname> system-view
[Sysname] dot1x access-user log enable failed-login
```

【相关命令】

- **info-center source dot1x logfile deny**（网络管理和监控/信息中心）

1.1.6 dot1x after-mac-auth max-attempt

dot1x after-mac-auth max-attempt 命令用来配置 MAC 地址认证成功的用户进行 802.1X 认证的最大尝试次数。

undo dot1x after-mac-auth max-attempt 命令用来恢复缺省情况。

【命令】

```
dot1x after-mac-auth max-attempt max-attempts  
undo dot1x after-mac-auth max-attempt
```

【缺省情况】

不限制 MAC 地址认证成功的用户进行 802.1X 认证的最大尝试次数。

【视图】

二层以太网接口视图

【缺省用户角色】

network-admin

【参数】

max-attempts: 表示认证的最大尝试次数，取值范围为 1~50。

【使用指导】

在端口上配置此功能后，MAC 地址认证成功的用户进行 802.1X 认证时，如果用户进行 802.1X 认证的尝试次数超过配置的最大次数，则设备将不再允许此用户进行 802.1X 认证。

如果 MAC 地址认证用户下线或设备重启，则此用户进行 802.1X 认证的尝试次数会重新从零计数。

【举例】

在端口 GigabitEthernet1/0/1 上配置 MAC 地址认证用户进行 802.1X 认证的最大尝试次数为 10 次。

```
<Sysname> system-view  
[Sysname] interface gigabitethernet 1/0/1  
[Sysname-GigabitEthernet1/0/1] dot1x after-mac-auth max-attempt 10
```

【相关命令】

- **display dot1x**

1.1.7 dot1x authentication-method

dot1x authentication-method 命令用来配置 802.1X 系统的认证方法。

undo dot1x authentication-method 命令用来恢复缺省情况。

【命令】

```
dot1x authentication-method { chap | eap | pap }  
undo dot1x authentication-method
```

【缺省情况】

设备启用 EAP 终结方式，并采用 CHAP 认证方法。

【视图】

系统视图

【缺省用户角色】

network-admin

【参数】

chap: 启用 EAP 终结方式，并支持与 RADIUS 服务器之间采用 CHAP 类型的认证方法。

eap: 启用 EAP 中继方式，并支持客户端与 RADIUS 服务器之间所有类型的 EAP 认证方法。

pap: 启用 EAP 终结方式，并支持与 RADIUS 服务器之间采用 PAP 类型的认证方法。

【使用指导】

在 EAP 终结方式下：设备将收到的客户端 EAP 报文中的用户认证信息重新封装在标准的 RADIUS 报文中，然后采用 PAP 或 CHAP 认证方法与 RADIUS 服务器完成认证交互。该方式的优点是，现有的 RADIUS 服务器基本均可支持 PAP 和 CHAP 认证，无需升级服务器，但设备处理较为复杂，且目前仅能支持 MD5-Challenge 类型的 EAP 认证以及 iNode 802.1X 客户端发起的“用户名+密码”方式的 EAP 认证。有关 PAP 和 CHAP 两种认证方法的详细介绍如下：

- PAP（Password Authentication Protocol，密码验证协议）通过用户名和口令来对用户进行验证，其特点是在网络上以明文方式传送用户名和口令，仅适用于对网络安全要求相对较低的环境。目前，H3C iNode 802.1X 客户端支持此认证方法。
- CHAP（Challenge Handshake Authentication Protocol，质询握手验证协议）采用客户端与服务器端交互挑战信息的方式来验证用户身份，其特点是在网络上以明文方式传送用户名，以密文方式传输口令。与 PAP 相比，CHAP 认证保密性较好，更为安全可靠。

在 EAP 中继方式下：设备将收到的客户端 EAP 报文直接封装到 RADIUS 报文的属性字段中，发送给 RADIUS 服务器完成认证。该方式的优点是，设备处理简单，且可支持多种类型的 EAP 认证方法，例如 MD5-Challenge、EAP-TLS、PEAP 等，但要求服务器端支持相应的 EAP 认证方法。

采用远程 RADIUS 认证时，PAP、CHAP、EAP 认证的最终实现，需要 RADIUS 服务器支持相应的 PAP、CHAP、EAP 认证方法。

若采用 EAP 认证方法，则 RADIUS 方案下的 **user-name-format** 配置无效，**user-name-format** 的介绍请参见“安全命令参考”中的“AAA”。

【举例】

启用 EAP 终结方式，并支持与 RADIUS 服务器之间采用 PAP 类型的认证方法。

```
<Sysname> system-view
[Sysname] dot1x authentication-method pap
```

【相关命令】

- **display dot1x**

1.1.8 dot1x auth-fail eapol

dot1x auth-fail eapol 命令用来配置当 802.1X 用户被加入到 Auth-Fail VLAN 后，设备端向客户端发送 EAP-Success 报文。

undo dot1x auth-fail eapol 命令用来恢复缺省情况。



说明

仅 Release 6127 及以上版本支持本命令。

【命令】

```
dot1x auth-fail eapol
undo dot1x auth-fail eapol
```

【缺省情况】

当 802.1X 用户加入到 Auth-Fail VLAN 后，设备端向客户端发送 EAP-Failure 报文。

【视图】

二层以太网接口视图

【缺省用户角色】

network-admin

【使用指导】

某些通过 DHCP 方式获取 IP 地址的 802.1X 客户端进行认证时，在收到 EAP-Failure 报文后，不会发送 DHCP 请求申请 IP 地址，只有在收到 EAP-Success 报文后才会发送 DHCP 请求申请 IP 地址。缺省情况下，当 802.1X 用户因认证失败而被加入 Auth-Fail VLAN 后，设备会向客户端发送一个 EAP-Failure 报文，导致上述客户端获取不到 IP 地址，无法访问 Auth-Fail VLAN 内的资源。为避免这种情况发生，可通过 **dot1x auth-fail eapol** 命令配置当 802.1X 用户被加入到 Auth-Fail VLAN 后，设备向客户端发送 EAP-Success 报文的功能。此类客户端收到 EAP-Success 报文后，认为 802.1X 用户上线成功，会向设备发送 DHCP 请求申请 IP 地址。

【举例】

在端口 GigabitEthernet1/0/1 上配置当 802.1X 用户加入到 Auth-Fail VLAN 后，向客户端发送 EAP-Success 报文。

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] dot1x auth-fail eapol
```

【相关命令】

- **dot1x auth-fail vlan**

1.1.9 dot1x auth-fail vlan

dot1x auth-fail vlan 命令用来配置端口的 802.1X Auth-Fail VLAN。

undo dot1x auth-fail vlan 命令用来恢复缺省情况。

【命令】

```
dot1x auth-fail vlan authfail-vlan-id
undo dot1x auth-fail vlan
```

【缺省情况】

端口上未配置 802.1X Auth-Fail VLAN。

【视图】

二层以太网接口视图

【缺省用户角色】

network-admin

【参数】

authfail-vlan-id: 端口上指定的 Auth-Fail VLAN ID，取值范围为 1~4094。该 VLAN 必须已经创建。

【使用指导】

端口上配置此功能后，认证失败的 802.1X 用户可以继续访问 Auth-Fail VLAN 中的资源。

禁止删除已被配置为 Auth-Fail VLAN 的 VLAN，若要删除该 VLAN，请先通过 **undo dot1x auth-fail vlan** 命令取消 802.1X Auth-Fail VLAN 配置。

【举例】

配置端口 GigabitEthernet1/0/1 的 Auth-Fail VLAN 为 VLAN 100。

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] dot1x auth-fail vlan 100
```

【相关命令】

- **display dot1x**

1.1.10 dot1x critical eapol

dot1x critical eapol 命令用来配置当 802.1X 用户被加入到 Critical VLAN 后，设备端向客户端发送 EAP-Success 报文。

undo dot1x critical eapol 命令用来恢复缺省情况。

【命令】

```
dot1x critical eapol
undo dot1x critical eapol
```

【缺省情况】

当 802.1X 用户加入到 Critical VLAN 后，设备端向客户端发送 EAP-Failure 报文。

【视图】

二层以太网接口视图

【缺省用户角色】

network-admin

【使用指导】

缺省情况下，当 802.1X 用户因认证服务器不可达而被加入 Critical VLAN 后，设备端会向客户端发送一个 EAP-Failure 报文。对于某些 802.1X 客户端（如 Windows 系统的 802.1X 客户端），在收到 EAP-Failure 报文后，不会再响应设备端后继发送的 EAP-Request/Identity 报文。因此当设备端探测到服务器可达并向客户端发送 EAP-Request/Identity 报文进行重认证时，客户端不会进行响应，

该类用户的重认证无法成功。这种情况下,可通过本命令配置当 802.1X 用户被加入到 Critical VLAN 后,设备端向客户端发送一个 EAP-Success 报文。客户端收到该报文后认为 802.1X 用户上线成功,此后可以继续响应设备端发送的 EAP-Request/Identity 报文进行 802.1X 重认证。

【举例】

在端口 GigabitEthernet1/0/1 上配置当 802.1X 用户加入到 Critical VLAN 后,向客户端发送 EAP-Success 报文。

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] dot1x critical eapol
```

【相关命令】

- **dot1x critical vlan**

1.1.11 dot1x critical vlan

dot1x critical vlan 命令用来配置端口的 802.1X Critical VLAN。

undo dot1x critical vlan 命令用来恢复缺省情况。

【命令】

```
dot1x critical vlan critical-vlan-id
undo dot1x critical vlan
```

【缺省情况】

端口上未配置 Critical VLAN。

【视图】

二层以太网接口视图

【缺省用户角色】

network-admin

【参数】

critical-vlan-id: 端口上指定的 Critical VLAN ID, 取值范围为 1~4094。该 VLAN 必须已经创建。

【使用指导】

配置此功能后,当 802.1X 用户认证时对应的 ISP 域下所有认证服务器都不可达的情况下,此 802.1X 用户可以继续访问 Critical VLAN 中的资源。

禁止删除已被配置为 Critical VLAN 的 VLAN,若要删除该 VLAN,请先通过 **undo dot1x critical vlan** 命令取消 802.1X Critical VLAN 配置。

【举例】

配置端口 GigabitEthernet1/0/1 的 Critical VLAN 为 VLAN 100。

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] dot1x critical vlan 100
```

【相关命令】

- **display dot1x**

1.1.12 dot1x critical-voice-vlan

dot1x critical-voice-vlan 命令用来开启 802.1X Critical Voice VLAN 功能。

undo dot1x critical-voice-vlan 命令用来关闭 802.1X Critical Voice VLAN 功能。

【命令】

```
dot1x critical-voice-vlan
undo dot1x critical-voice-vlan
```

【缺省情况】

802.1X Critical Voice VLAN 功能处于关闭状态。

【视图】

二层以太网接口视图

【缺省用户角色】

network-admin

【使用指导】

S5110V2-SI 和 S5000V3-EI 系列交换机不支持配置该命令。

端口上开启 802.1X Critical Voice VLAN 功能后，当语音用户进行 802.1X 认证采用的 ISP 域中的所有认证服务器都不可达时，端口将被加入到此端口上的语音 VLAN 中。有关语音 VLAN 的配置命令请参见“二层技术-以太网交换命令参考”中的“VLAN”。

设备通过 LLDP（Link Layer Discovery Protocol，链路层发现协议）来判断用户是否为语音用户，因此为保证 802.1X Critical Voice VLAN 功能可以正常工作，请在开启此功能之前务必确保全局和相应端口上均已开启 LLDP 功能。有关 LLDP 功能的配置命令请参见“二层技术-以太网交换命令参考”中的“LLDP”。

【举例】

开启端口 GigabitEthernet1/0/1 上的 802.1X Critical Voice VLAN 功能。

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] dot1x critical-voice-vlan
```

【相关命令】

- **display dot1x**
- **lldp enable**（二层技术-以太网交换命令参考/LLDP）
- **lldp global enable**（二层技术-以太网交换命令参考/LLDP）
- **voice-vlan enable**（二层技术-以太网交换命令参考/VLAN）

1.1.13 dot1x domain-delimiter

dot1x domain-delimiter 命令用来配置 802.1X 支持的域名分隔符。

`undo dot1x domain-delimiter` 命令用来恢复缺省情况。

【命令】

```
dot1x domain-delimiter string
undo dot1x domain-delimiter
```

【缺省情况】

802.1X 支持的域名分隔符为@。

【视图】

系统视图

【缺省用户角色】

network-admin

【参数】

string: 多个域名分隔符组成的 1~16 个字符的字符串，且分隔符只能为@、.、/或\。若要指定域名分隔符\，则必须在输入时使用转义操作符\\，即输入\\。

【使用指导】

目前，802.1X 支持的域名分隔符包括@、\、/和.，对应的用户名格式分别为 *username@domain-name*，*domain-name\username*、*username/domain-name* 和 *username.domain-name*，其中 *username* 为纯用户名、*domain-name* 为域名。如果用户名中包含有多个域名分隔符字符，则设备仅将最后一个出现的域名分隔符识别为实际使用的域名分隔符，例如，用户输入的用户名为 121.123/22\@abc，若设备上指定 802.1X 支持的域名分隔符为/、\，则识别出的纯用户名为@abc，域名为 121.123/22。

系统默认支持分隔符@，但如果通过本命令指定的域名分隔符中未包含分隔符@，则 802.1X 仅会支持命令中指定的分隔符。

【举例】

```
# 配置 802.1X 支持的域名分隔符为@和/。
<Sysname> system-view
[Sysname] dot1x domain-delimiter @/
```

【相关命令】

- `display dot1x`

1.1.14 dot1x ead-assistant enable

`dot1x ead-assistant enable` 命令用来开启 EAD 快速部署辅助功能。

`undo dot1x ead-assistant enable` 命令用来关闭 EAD 快速部署辅助功能。

【命令】

```
dot1x ead-assistant enable
undo dot1x ead-assistant enable
```

【缺省情况】

EAD 快速部署辅助功能处于关闭状态。

【视图】

系统视图

【缺省用户角色】

network-admin

【使用指导】

S5000E-X、S5110V2-SI 和 S5000V3-EI 系列交换机不支持配置该命令。

开启 EAD 快速部署辅助功能后，设备允许未通过认证的 802.1X 用户访问一个特定的 IP 地址段，并可以将用户发起的 HTTP 或 HTTPS 访问请求重定向到该 IP 地址段中的一个指定的 URL，实现用户自动下载并安装 EAD 客户端的目的。

为使 EAD 快速部署功能生效，必须保证指定端口的授权模式为 **auto**。

该命令与 MAC 地址认证和端口安全的全局使能命令均互斥，即开启 EAD 快速部署辅助功能时，若全局使能了 MAC 地址认证或端口安全，则该配置将会执行失败，反之亦然。

若要对 802.1X 用户的 HTTPS 访问进行重定向，需要通过 **http-redirect https-port** 命令配置对 HTTPS 报文进行重定向的内部侦听端口号（对于 Release 6127 及以上版本，缺省端口号为 6654），具体介绍请参见“三层技术-IP 业务命令参考”中的“HTTP 重定向”。

【举例】

开启 EAD 快速部署辅助功能。

```
<Sysname> system-view
[Sysname] dot1x ead-assistant enable
```

【相关命令】

- **display dot1x**
- **dot1x ead-assistant free-ip**
- **dot1x ead-assistant url**
- **http-redirect https-port**（三层技术-IP 业务/HTTP 重定向）

1.1.15 dot1x ead-assistant free-ip

dot1x ead-assistant free-ip 命令用来配置 Free IP。

undo dot1x ead-assistant free-ip 命令用来删除指定的 Free IP。

【命令】

```
dot1x ead-assistant free-ip ip-address { mask-address | mask-length }
undo dot1x ead-assistant free-ip { ip-address { mask-address | mask-length }
| all }
```

【缺省情况】

未配置 Free IP，用户在通过 802.1X 认证之前不能够访问任何网段。

【视图】

系统视图

【缺省用户角色】

network-admin

【参数】

ip-address: 指定的 IP 地址。

mask-address: 指定的 IP 掩码地址。

mask-length: 指定的 IP 掩码地址长度，取值范围为 1~32。

all: 所有配置的 IP。

【使用指导】

S5000E-X、S5110V2-SI 和 S5000V3-EI 系列交换机不支持配置该命令。

全局使能 EAD 快速部署功能且配置 Free IP 之后，未通过认证的 802.1X 终端用户可以访问该 IP 地址段中的网络资源。

可通过重复执行此命令来配置多个 Free IP。

【举例】

配置用户在通过 802.1X 认证之前能够访问的网段为 192.168.1.1/16。

```
<Sysname> system-view
```

```
[Sysname] dot1x ead-assistant free-ip 192.168.1.1 255.255.0.0
```

【相关命令】

- **display dot1x**
- **dot1x ead-assistant enable**
- **dot1x ead-assistant url**

1.1.16 dot1x ead-assistant url

dot1x ead-assistant url 命令用来配置 802.1X 用户 HTTP 或 HTTPS 访问的重定向 URL。

undo dot1x ead-assistant url 命令用来恢复缺省情况。

【命令】

```
dot1x ead-assistant url url-string
```

```
undo dot1x ead-assistant url
```

【缺省情况】

未配置 802.1X 用户 HTTP 或 HTTPS 访问的重定向 URL。

【视图】

系统视图

【缺省用户角色】

network-admin

【参数】

url-string: 重定向 URL 地址，为 1~256 个字符的字符串，区分大小写。它以 http://或者 https://开头，如果该 URL 未以 http://或者 https://开头，则缺省认为是以 http://开头。

【使用指导】

S5000E-X、S5110V2-SI 和 S5000V3-EI 系列交换机不支持配置该命令。

用户在 802.1X 认证成功之前，如果使用浏览器访问非 Free IP 网段的其它网络，设备会将用户访问的 URL 重定向到已配置的重定向地址。

802.1X 用户重定向的 URL 和 Free IP 必须在同一个网段内，否则用户无法访问指定的重定向 URL。

多次执行本命令，最后一次执行的命令生效。

若要对 802.1X 用户的 HTTPS 访问进行重定向，需要通过 **http-redirect https-port** 命令配置对 HTTPS 报文进行重定向的内部侦听端口号（对于 Release 6127 及以上版本，缺省端口号为 6654），具体介绍请参见“三层技术-IP 业务命令参考”中的“HTTP 重定向”。

【举例】

配置 802.1X 用户 HTTP 访问的重定向 URL 为 http://test.com。

```
<Sysname> system-view
[Sysname] dot1x ead-assistant url http://test.com
```

【相关命令】

- **display dot1x**
- **dot1x ead-assistant enable**
- **dot1x ead-assistant free-ip**
- **http-redirect https-port**（三层技术-IP 业务/HTTP 重定向）

1.1.17 dot1x eapol untag

dot1x eapol untag 命令用来配置端口发送 802.1X 协议报文不携带 VLAN Tag。

undo dot1x eapol untag 命令用来恢复缺省情况。

【命令】

```
dot1x eapol untag
undo dot1x eapol untag
```

【缺省情况】

端口发送 802.1X 协议报文时携带 VLAN Tag。

【视图】

二层以太网接口视图

【缺省用户角色】

network-admin

【使用指导】

Hybrid 端口开启 802.1X 认证，若该端口上通过 **port hybrid vlan** 命令配置了转发缺省 VLAN 报文携带 VLAN Tag，则端口发送的缺省 VLAN 内的 802.1X 协议报文默认携带 VLAN Tag。这种情况下，当终端发送的是不带 VLAN Tag 的报文进行 802.1X 认证时，由于接收的是带 Tag 的报文，会导致 802.1X 认证失败。为了解决这个问题，设备支持配置端口发送 802.1X 协议报文时不带 VLAN Tag 的功能。

需要注意的是，除了上述应用场景，不要开启本功能，否则端口发送的所有 802.1X 报文都将去除 VLAN Tag，可能导致正常用户无法通过 802.1X 认证。

仅 Hybrid 类型的以太网端口支持本功能。

【举例】

在端口 GigabitEthernet1/0/1 上配置发送 802.1X 协议报文不携带 VLAN Tag。

```
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] dot1x eapol untag
```

【相关命令】

- **display dot1x**

1.1.18 dot1x guest-vlan

dot1x guest-vlan 命令用来配置端口的 802.1X Guest VLAN。

undo dot1x guest-vlan 命令用来恢复缺省情况。

【命令】

```
dot1x guest-vlan guest-vlan-id
undo dot1x guest-vlan
```

【缺省情况】

端口上未配置 802.1X Guest VLAN。

【视图】

二层以太网接口视图

【缺省用户角色】

network-admin

【参数】

guest-vlan-id：端口上指定的 Guest VLAN ID，取值范围为 1～4094。该 VLAN 必须已经创建。

【使用指导】

配置此功能后，在 802.1X 用户在未认证的情况下，其可以访问的 VLAN 资源，该 VLAN 内通常放置一些用于用户下载客户端软件或其他升级程序的服务器。

禁止删除已被配置为 Guest VLAN 的 VLAN，若要删除该 VLAN，请先通过 **undo dot1x guest-vlan** 命令取消 802.1X Guest VLAN 配置。

【举例】

配置端口 GigabitEthernet1/0/1 的 Guest VLAN 为 VLAN 100。

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] dot1x guest-vlan 100
```

【相关命令】

- **display dot1x**

1.1.19 dot1x guest-vlan-delay

dot1x guest-vlan-delay 命令用来开启端口延迟加入 802.1X Guest VLAN 的功能。

undo dot1x guest-vlan-delay 命令用来关闭端口延迟加入 802.1X Guest VLAN 的功能。

【命令】

```
dot1x guest-vlan-delay { eapol | new-mac }  
undo dot1x guest-vlan-delay [ eapol | new-mac ]
```

【缺省情况】

端口延迟加入 802.1X Guest VLAN 的功能处于关闭状态。

【视图】

二层以太网接口视图

【缺省用户角色】

network-admin

【参数】

eapol: 表示 802.1X 协议报文触发端口延迟加入 802.1X Guest VLAN。

new-mac: 表示源 MAC 地址未知的报文触发端口延迟加入 802.1X Guest VLAN。

【使用指导】

开启 802.1X 认证，并且端口的受控方式为 MAC-based 方式时，触发 802.1X 认证后端口会立即被加入到 802.1X Guest VLAN 中。

在这种情况下，如果配置了端口延迟加入 802.1X Guest VLAN 的功能，端口会主动向触发认证的源 MAC 地址单播发送 EAP-Request 报文。若在指定的时间内（通过命令 **dot1x timer tx-period** 设置）没有收到客户端的响应，则重发该报文，直到重发次数达到命令 **dot1x retry** 设置的最大次数时，若仍没有收到客户端的响应，才会加入到 802.1X Guest VLAN 中。

undo dot1x guest-vlan-delay 命令不指定任何参数表示关闭 802.1X 协议报文触发和 MAC 地址未知的报文触发的端口延迟加入 802.1X Guest VLAN 的功能。

【举例】

在端口 GigabitEthernet1/0/1 下配置 802.1X 协议报文触发端口延迟加入 802.1X Guest VLAN 功能。

```
<Sysname> system-view  
[Sysname] interface gigabitethernet 1/0/1  
[Sysname-GigabitEthernet1/0/1] dot1x guest-vlan-delay eapol
```

【相关命令】

- **display dot1x**
- **dot1x retry**
- **dot1x timer tx-period**

1.1.20 dot1x handshake

dot1x handshake 命令用于开启在线用户握手功能。

undo dot1x handshake 命令用于关闭在线用户握手功能。

【命令】

```
dot1x handshake
undo dot1x handshake
```

【缺省情况】

在线用户握手功能处于开启状态。

【视图】

二层以太网接口视图

【缺省用户角色】

network-admin

【使用指导】

开启设备的在线用户握手功能后，设备会定期（时间间隔通过命令 **dot1x timer handshake-period** 设置）向通过 802.1X 认证的在线用户发送握手报文，以定期检测用户的在线情况。如果设备连续多次（通过命令 **dot1x retry** 设置）没有收到客户端的响应报文，则会将用户置为下线状态。

【举例】

在端口 GigabitEthernet1/0/1 上开启在线用户握手功能。

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] dot1x handshake
```

【相关命令】

- **display dot1x**
- **dot1x timer handshake-period**
- **dot1x retry**

1.1.21 dot1x handshake reply enable

dot1x handshake reply enable 命令用来开启端口发送在线握手成功报文功能。

undo dot1x handshake reply enable 命令用来关闭端口发送在线握手成功报文功能。

【命令】

```
dot1x handshake reply enable
undo dot1x handshake reply enable
```

【缺省情况】

端口发送在线握手成功报文功能处于关闭状态。

【视图】

二层以太网接口视图

【缺省用户角色】

network-admin

【使用指导】

端口上开启在线用户握手功能后，缺省情况下，设备收到该端口上 802.1X 在线用户的在线握手应答报文（EAP-Response/Identity 报文）后，则认为该用户在线，并不给客户端回应在线握手成功报文（EAP-Success 报文）。但是，有些 802.1X 客户端如果没有收到设备回应的在线握手成功报文（EAP-Success 报文），就会自动下线。为了避免这种情况发生，需要在端口上开启发送在线握手成功报文功能。

只有当 802.1X 客户端需要收到在线握手成功报文时，才需要开启此功能。

【举例】

在端口 GigabitEthernet1/0/1 上开启的发送在线握手成功报文功能。

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] dot1x handshake reply enable
```

【相关命令】

- **dot1x handshake**

1.1.22 dot1x handshake secure

dot1x handshake secure 命令用来开启在线用户握手安全功能。

undo dot1x handshake secure 命令用来关闭在线用户握手安全功能。

【命令】

```
dot1x handshake secure
undo dot1x handshake secure
```

【缺省情况】

在线用户握手安全功能处于关闭状态。

【视图】

二层以太网接口视图

【缺省用户角色】

network-admin

【使用指导】

开启在线用户握手安全功能后，可以防止在线的 802.1X 认证用户使用非法的客户端与设备进行握手报文的交互，而逃过代理检测、双网卡检测等 iNode 客户端的安全检查功能。

只有设备上的在线用户握手功能处于开启状态时，安全握手功能才会生效。

本功能仅能在 iNode 客户端和 iMC 服务器配合使用的组网环境中生效。

【举例】

在端口 GigabitEthernet1/0/1 上开启在线用户握手安全功能。

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] dot1x handshake secure
```

【相关命令】

- **display dot1x**
- **dot1x handshake**

1.1.23 dot1x mac-binding

dot1x mac-binding 命令用来手工配置 802.1X 认证的 MAC 地址绑定表项。

undo dot1x mac-binding 命令用来删除指定的 802.1X 认证的 MAC 地址绑定表项。

【命令】

```
dot1x mac-binding mac-address  
undo dot1x mac-binding { mac-address | all }
```

【缺省情况】

端口上不存在 802.1X 认证的 MAC 地址绑定表项。

【视图】

二层以太网接口视图

【缺省用户角色】

network-admin

【参数】

mac-address: 表示绑定的 MAC 地址，格式为 H-H-H，取值不能为全 0、全 F（广播 MAC）和组播 MAC。

all: 表示删除接口下所有绑定的 MAC 地址。

【使用指导】

只有 802.1X 认证的 MAC 地址绑定功能处于开启状态，且端口接入控制方式为 MAC-based 方式下，手工配置 802.1X 认证的 MAC 地址绑定表项才能生效。

802.1X 认证的 MAC 地址绑定表项数受端口允许同时接入 802.1X 用户数的最大值（通过 **dot1x max-user** 命令配置）影响，当绑定表项数等于端口允许同时接入 802.1X 用户最大用户数时，MAC 地址绑定表项之外的用户均会认证失败。

手工配置的 802.1X 认证 MAC 地址绑定表项不会老化，即使对应用户下线或设备保存配置重启后也不会删除此绑定表项。只能通过 **undo dot1x mac-binding** 命令删除此表项。绑定用户在线时，不允许删除此表项。

【举例】

在端口 GigabitEthernet1/0/1 下配置 802.1X 认证的 MAC 地址绑定表项，与此端口绑定的 MAC 地址为 000a-eb29-75f1。

```
<Sysname> system-view  
[Sysname] interface gigabitethernet 1/0/1  
[Sysname-GigabitEthernet1/0/1] dot1x mac-binding 000a-eb29-75f1
```

【相关命令】

- **dot1x**

- `dot1x mac-binding enable`
- `dot1x port-method`

1.1.24 dot1x mac-binding enable

`dot1x mac-binding enable` 命令用来开启 802.1X 认证的 MAC 地址绑定功能。

`undo dot1x mac-binding enable` 命令用来关闭 802.1X 认证的 MAC 地址绑定功能。

【命令】

```
dot1x mac-binding enable
undo dot1x mac-binding enable
```

【缺省情况】

802.1X 认证的 MAC 地址绑定功能处于关闭状态。

【视图】

二层以太网接口视图

【缺省用户角色】

network-admin

【使用指导】

802.1X 认证的 MAC 地址绑定功能仅在接入控制方式为 MAC-based 的端口上生效。

802.1X 认证的 MAC 地址绑定表项数受端口允许同时接入 802.1X 用户数的最大值（通过 `dot1x max-user` 命令配置）影响，当绑定表项数等于端口允许同时接入 802.1X 用户最大用户数时，MAC 地址绑定表项之外的用户均会认证失败。

自动生成的端口与 802.1X 认证成功用户的 MAC 地址绑定表项不会老化，即使该用户下线后或设备保存配置重启后也不会删除此绑定表项。只能通过 `undo dot1x mac-binding` 命令删除此表项。绑定用户在线时，不允许删除此表项。

【举例】

在端口 GigabitEthernet1/0/1 上开启 802.1X 认证的 MAC 地址绑定功能。

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] dot1x mac-binding enable
```

【相关命令】

- `dot1x`
- `dot1x mac-binding`
- `dot1x port-method`

1.1.25 dot1x mandatory-domain

`dot1x mandatory-domain` 命令用来指定端口上 802.1X 用户使用的强制认证域。

`undo dot1x mandatory-domain` 命令用来恢复缺省情况。

【命令】

```
dot1x mandatory-domain domain-name
undo dot1x mandatory-domain
```

【缺省情况】

未指定 802.1X 用户使用的强制认证域。

【视图】

二层以太网接口视图

【缺省用户角色】

network-admin

【参数】

domain-name: ISP 域名，为 1~255 个字符的字符串，不区分大小写。

【使用指导】

从指定端口上接入的 802.1X 用户将按照如下先后顺序选择认证域：端口上指定的强制 ISP 域-->用户名中指定的 ISP 域-->系统缺省的 ISP 域。

【举例】

```
# 指定端口 GigabitEthernet1/0/1 上 802.1X 用户使用的强制认证域为 my-domain。
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] dot1x mandatory-domain my-domain
```

【相关命令】

- **display dot1x**

1.1.26 dot1x max-user

dot1x max-user 命令用来配置端口上最多允许同时接入的 802.1X 用户数。

undo dot1x max-user 命令用来恢复缺省情况。

【命令】

```
dot1x max-user max-number
undo dot1x max-user
```

【缺省情况】

端口上最多允许同时接入的 802.1X 用户数为 4294967295。

【视图】

二层以太网接口视图

【缺省用户角色】

network-admin

【参数】

max-number: 端口允许同时接入的 802.1X 用户数的最大值，取值范围为 1~4294967295。

【使用指导】

由于系统资源有限，如果当前端口上接入的用户过多，接入用户之间会发生资源的争用，因此适当地配置该值可以使属于当前端口的用户获得可靠的性能保障。当接入此端口的 802.1X 用户数超过最大值后，新接入的用户将被拒绝。

【举例】

配置端口 GigabitEthernet1/0/1 上最多允许同时接入 32 个 802.1X 用户。

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] dot1x max-user 32
```

【相关命令】

- **display dot1x**

1.1.27 dot1x multicast-trigger

dot1x multicast-trigger 命令用来开启 802.1X 的组播触发功能。

undo dot1x multicast-trigger 命令用来关闭 802.1X 的组播触发功能。

【命令】

```
dot1x multicast-trigger
undo dot1x multicast-trigger
```

【缺省情况】

802.1X 的组播触发功能处于开启状态。

【视图】

二层以太网接口视图

【缺省用户角色】

network-admin

【使用指导】

开启了 802.1X 的组播触发功能的端口会定期（间隔时间通过命令 **dot1x timer tx-period** 设置）向客户端组播发送 EAP-Request/Identity 报文来检测客户端并触发认证。该功能用于支持不能主动发送 EAPOL-Start 报文来发起认证的客户端。

【举例】

在端口 GigabitEthernet1/0/1 上开启 802.1X 的组播触发功能。

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] dot1x multicast-trigger
```

【相关命令】

- **display dot1x**
- **dot1x timer tx-period**
- **dot1x unicast-trigger**

1.1.28 dot1x port-control

dot1x port-control 命令用来设置端口的授权状态。

undo dot1x port-control 命令用来恢复缺省情况。

【命令】

```
dot1x port-control { authorized-force | auto | unauthorized-force }  
undo dot1x port-control
```

【缺省情况】

端口的授权状态为 **auto**。

【视图】

二层以太网接口视图

【缺省用户角色】

network-admin

【参数】

authorized-force: 强制授权状态，表示端口始终处于授权状态，允许用户不经认证授权即可访问网络资源。

auto: 自动识别状态，表示端口初始状态为非授权状态，仅允许 EAPOL 报文收发，不允许用户访问网络资源；如果用户认证通过，则端口切换到授权状态，允许用户访问网络资源。这也是最常用的一种状态。

unauthorized-force: 强制非授权状态，表示端口始终处于非授权状态，不允许用户访问网络资源。

【使用指导】

通过配置端口的授权状态，可以控制端口上接入的用户是否需要通过认证才能访问网络资源。

【举例】

```
# 指定端口 GigabitEthernet1/0/1 处于强制非授权状态。  
<Sysname> system-view  
[Sysname] interface gigabitethernet 1/0/1  
[Sysname-GigabitEthernet1/0/1] dot1x port-control unauthorized-force
```

【相关命令】

- **display dot1x**

1.1.29 dot1x port-method

dot1x port-method 命令用来配置端口的接入控制方式。

undo dot1x port-method 命令用来恢复缺省情况。

【命令】

```
dot1x port-method { machbased | portbased }  
undo dot1x port-method
```

【缺省情况】

端口的接入控制方式为 **macbased**。

【视图】

二层以太网接口视图

【缺省用户角色】

network-admin

【参数】

macbased: 表示基于 MAC 地址对接入用户进行认证，即该端口上的所有接入用户均需要单独认证，当某个用户下线时，也只有该用户无法使用网络。

portbased: 表示基于端口对接入用户进行认证，即只要该端口上的第一个用户认证成功后，其他接入用户无须认证就可使用网络资源，当第一个用户下线后，其它用户也会被拒绝使用网络。

【举例】

在端口 GigabitEthernet1/0/1 上配置对接入用户进行基于端口的 802.1X 认证。

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] dot1x port-method portbased
```

【相关命令】

- **display dot1x**

1.1.30 dot1x quiet-period

dot1x quiet-period 命令用来开启静默定时器功能。

undo dot1x quiet-period 命令用来关闭静默定时器功能。

【命令】

```
dot1x quiet-period
undo dot1x quiet-period
```

【缺省情况】

静默定时器功能处于关闭状态。

【视图】

系统视图

【缺省用户角色】

network-admin

【使用指导】

在静默定时器功能处于开启状态的情况下，设备将在一段时间之内不对 802.1X 认证失败的用户进行 802.1X 认证处理，该时间由 802.1X 静默定时器控制，可通过 **dot1x timer quiet-period** 命令配置。

【举例】

开启静默定时器功能，并配置静默定时器的值为 100 秒。

```
<Sysname> system-view
[Sysname] dot1x quiet-period
[Sysname] dot1x timer quiet-period 100
```

【相关命令】

- **display dot1x**
- **dot1x timer**

1.1.31 dot1x re-authenticate

dot1x re-authenticate 命令用来开启周期性重认证功能。

undo dot1x re-authenticate 命令用来关闭周期性重认证功能。

【命令】

```
dot1x re-authenticate
undo dot1x re-authenticate
```

【缺省情况】

周期性重认证功能处于关闭状态。

【视图】

二层以太网接口视图

【缺省用户角色】

network-admin

【使用指导】

端口开启了 802.1X 的周期性重认证功能后，设备会根据周期性重认证定时器（**dot1x timer reauth-period**）设定的时间间隔定期启动对该端口在线 802.1X 用户的认证，以检测用户连接状态的变化，更新服务器下发的授权属性（例如 ACL、VLAN）。

【举例】

在端口 GigabitEthernet1/0/1 上开启 802.1X 重认证功能，并配置周期性重认证时间间隔为 1800 秒。

```
<Sysname> system-view
[Sysname] dot1x timer reauth-period 1800
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] dot1x re-authenticate
```

【相关命令】

- **display dot1x**
- **dot1x timer**

1.1.32 dot1x re-authenticate manual

dot1x re-authenticate manual 命令用来强制端口上所有 802.1X 在线用户进行重认证。

【命令】

dot1x re-authenticate manual

【视图】

二层以太网接口视图

【缺省用户角色】

network-admin

【使用指导】

强制端口上所有 802.1X 在线用户进行重认证后，不论服务器是否下发重认证或端口下是否开启了周期性重认证，强制重认证都会正常执行，端口上的所有在线 802.1X 用户会依次进行重认证操作。

【举例】

强制 GigabitEthernet1/0/1 端口上所有 802.1X 在线用户进行重认证。

```
[Sysname] interface gigabitethernet 1/0/1
```

```
[Sysname-GigabitEthernet1/0/1] dot1x re-authenticate manual
```

【相关命令】

- **dot1x re-authenticate**

1.1.33 dot1x re-authenticate server-unreachable keep-online

dot1x re-authenticate server-unreachable keep-online 命令用来配置重认证服务器不可达时端口上的用户保持在线状态。

undo dot1x re-authenticate server-unreachable 命令用来恢复缺省情况。

【命令】

dot1x re-authenticate server-unreachable keep-online

undo dot1x re-authenticate server-unreachable

【缺省情况】

端口上的 802.1X 在线用户重认证时，若认证服务器不可达，则会被强制下线。

【视图】

二层以太网接口视图

【缺省用户角色】

network-admin

【使用指导】

若端口上开启了 802.1X 的周期性重认证功能，则设备会定期对端口上的 802.1X 在线用户进行重认证，重认证过程中，若设备发现认证服务器状态不可达，则可以根据本配置，决定是否保持其在线状态。

【举例】

配置端口 GigabitEthernet1/0/1 上的 802.1X 在线用户进行重认证时，若服务器不可达，则保持在线状态。

```
<Sysname> system-view
```

```
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] dot1x re-authenticate server-unreachable keep-online
```

【相关命令】

- **display dot1x**
- **dot1x re-authenticate**

1.1.34 dot1x retry

dot1x retry 命令用来设置设备向接入用户发送认证请求报文的最大次数。

undo dot1x retry 命令用来恢复缺省情况。

【命令】

```
dot1x retry retries
undo dot1x retry
```

【缺省情况】

设备向接入用户发送认证请求报文的最大次数为 2。

【视图】

系统视图

【缺省用户角色】

network-admin

【参数】

retries: 向接入用户发送认证请求报文的最大尝试次数，取值范围为 1~10。

【使用指导】

如果设备向用户发送认证请求报文后，在规定的时间内没有收到用户的响应，则设备将向用户重发该认证请求报文，若设备累计发送认证请求报文的次数达到配置的最大值后，仍然没有得到用户响应，则停止发送认证请求。对于 EAP-Request/Identity 报文，该时间由 **dot1x timer tx-period** 设置；对于 EAP-Request/MD5 Challenge 报文，该时间由 **dot1x timer supp-timeout** 设置。

【举例】

配置设备最多向接入用户发送 9 次认证请求报文。

```
<Sysname> system-view
[Sysname] dot1x retry 9
```

【相关命令】

- **display dot1x**
- **dot1x timer**

1.1.35 dot1x timer

dot1x timer 命令用来配置 802.1X 的定时器参数。

undo dot1x timer 命令用来将指定的定时器恢复为缺省情况。

【命令】

```
dot1x timer { ead-timeout ead-timeout-value | handshake-period handshake-period-value | quiet-period quiet-period-value | reauth-period reauth-period-value | server-timeout server-timeout-value | supp-timeout supp-timeout-value | tx-period tx-period-value }  
undo dot1x timer { ead-timeout | handshake-period | quiet-period | reauth-period | server-timeout | supp-timeout | tx-period }
```

【缺省情况】

握手定时器的值为 15 秒，EAD 超时定时器的值为 30 分钟，静默定时器的值为 60 秒，周期性重认证定时器的值为 3600 秒，认证服务器超时定时器的值为 100 秒，客户端认证超时定时器的值为 30 秒，用户名请求超时定时器的值为 30 秒。

【视图】

系统视图

【缺省用户角色】

network-admin

【参数】

ead-timeout *ead-timeout-value*: EAD 超时定时器的值，取值范围为 1~1440，单位为分钟。S5000E-X、S5110V2-SI 和 S5000V3-EI 系列交换机不支持配置该参数。

handshake-period *handshake-period-value*: 握手定时器的值，取值范围为 5~1024，单位为秒。

quiet-period *quiet-period-value*: 静默定时器的值，取值范围为 10~120，单位为秒。

reauth-period *reauth-period-value*: 周期性重认证定时器的值，取值范围为 60~7200，单位为秒。

server-timeout *server-timeout-value*: 认证服务器超时定时器的值，取值范围为 100~300，单位为秒。

supp-timeout *supp-timeout-value*: 客户端认证超时定时器的值，取值范围为 1~120，单位为秒。

tx-period *tx-period-value*: 用户名请求超时定时器的值，取值范围为 1~120，单位为秒。

【使用指导】

802.1X 认证过程受以下定时器的控制：

- **EAD 超时定时器 (ead-timeout)**: 管理员可以通过配置 EAD 规则的老化时间来控制用户对 ACL 资源的占用，当用户访问网络时该定时器即开始计时，在定时器超时或者用户下载客户端并成功通过认证之后，该用户所占用的 ACL 资源即被删除，这样那些在老化时间内未进行任何操作的用户所占用的 ACL 资源会及时得到释放。
- **握手定时器 (handshake-period)**: 此定时器是在用户认证成功启动的，设备端以此间隔为周期发送握手请求报文，以定期检测用户的在线情况。如果配置发送次数为 N，则当设备端连续 N 次没有收到客户端的响应报文，就认为用户已经下线。
- **静默定时器 (quiet-period)**: 对用户认证失败以后，设备端需要静默一段时间（该时间由静默定时器设置），在静默期间，设备端不对 802.1X 认证失败的用户进行 802.1X 认证处理。

- 周期性重认证定时器(**reauth-period**): 端口上开启了周期性重认证功能(通过命令 **dot1x re-authenticate**) 后, 设备端以此间隔为周期对端口上的在线用户发起重认证。对于已在线的 802.1X 用户, 要等当前重认证周期结束并且认证通过后才按新配置的周期进行后续的重认证。
- 认证服务器超时定时器 (**server-timeout**): 当设备端向认证服务器发送了 RADIUS Access-Request 请求报文后, 设备端启动 **server-timeout** 定时器, 若在该定时器设置的时长内, 设备端没有收到认证服务器的响应, 则 802.1X 认证失败。
建议将 **server-timeout** 的值设定为小于或等于设备发送 RADIUS 报文的最大尝试次数 (**retry**) 与 RADIUS 服务器响应超时时间 (**timer response-timeout**) 之积。如果 **server-timeout** 的值大于 **retry** 与 **timer response-timeout** 之积, 则可能在 **server-timeout** 设定的服务器超时时间到达前, 用户被强制下线。关于发送 RADIUS 报文的最大尝试次数、RADIUS 服务器响应超时时间的具体配置请参见“安全配置指导”中的“AAA”。
- 客户端认证超时定时器 (**supp-timeout**): 当设备端向客户端发送了 EAP-Request/MD5 Challenge 请求报文后, 设备端启动此定时器, 若在该定时器设置的时长内, 设备端没有收到客户端的响应, 设备端将重发该报文。
- 用户名请求超时定时器 (**tx-period**): 当设备端向客户端发送 EAP-Request/Identity 请求报文后, 设备端启动该定时器, 若在该定时器设置的时长内, 设备端没有收到客户端的响应, 则设备端将重发认证请求报文。另外, 为了兼容不主动发送 EAPOL-Start 连接请求报文的客户端, 设备会定期组播 EAP-Request/Identity 请求报文来检测客户端。**tx-period** 定义了该组播报文的发送时间间隔。

一般情况下, 用户无需修改定时器的值, 除非在一些特殊或恶劣的网络环境下, 可以使用该命令调节交互进程。

除周期性重认证定时器外的其他定时器修改后可立即生效。

【举例】

设置认证服务器的超时定时器时长为 150 秒。

```
<Sysname> system-view
[Sysname] dot1x timer server-timeout 150
```

【相关命令】

- **display dot1x**
- **retry** (安全命令参考/AAA)
- **timer response-timeout** (RADIUS scheme view) (安全命令参考/AAA)

1.1.36 dot1x timer reauth-period (interface view)

dot1x timer reauth-period 命令用来在端口上配置 802.1X 周期性重认证定时器。

undo dot1x timer reauth-period 命令用来恢复缺省情况。

【命令】

```
dot1x timer reauth-period reauth-period-value
undo dot1x timer reauth-period
```

【缺省情况】

端口上未配置 802.1X 周期性重认证定时器，端口使用系统视图下配置的 802.1X 周期性重认证定时器的取值。

【视图】

二层以太网接口视图

【缺省用户角色】

network-admin

【参数】

reauth-period-value：周期性重认证定时器的值，取值范围为 60～7200，单位为秒。

【使用指导】

端口上开启了 802.1X 周期性重认证功能后，设备将周期性地对端口上认证成功的 802.1X 用户发起重认证。重认证周期的选择优先级高低顺序为：服务器下发的重认证时间间隔、接口视图下配置的周期性重认证定时器的值、系统视图下配置的周期性重认证定时器的值、设备缺省的周期性重认证定时器的值。

对于已在线的 802.1X 用户，要等当前重认证周期结束并且认证通过后才按新配置的周期性重认证定时器的值进行后续的重认证。

【举例】

在端口 GigabitEthernet1/0/1 上配置 802.1X 周期性重认证定时器的值为 60 秒。

```
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] dot1x timer reauth-period 60
```

【相关命令】

- **dot1x timer**

1.1.37 dot1x unicast-trigger

dot1x unicast-trigger 命令用来开启端口上的 802.1X 的单播触发功能。

undo dot1x unicast-trigger 命令用来关闭 802.1X 的单播触发功能。

【命令】

```
dot1x unicast-trigger
undo dot1x unicast-trigger
```

【缺省情况】

802.1X 的单播触发功能处于关闭状态。

【视图】

二层以太网接口视图

【缺省用户角色】

network-admin

【使用指导】

端口上开启 802.1X 的单播触发功能后，当端口收到源 MAC 未知的报文时，主动向该 MAC 地址发送单播认证报文来触发认证。若设备端在设置的客户端认证超时时间内（该时间由 **dot1x timer supp-timeout** 设置）没有收到客户端的响应，则重发该报文（重发次数由 **dot1x retry** 设置）。

【举例】

在端口 GigabitEthernet1/0/1 上开启 802.1X 的单播触发功能。

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] dot1x unicast-trigger
```

【相关命令】

- **display dot1x**
- **dot1x multicast-trigger**
- **dot1x retry**
- **dot1x timer**

1.1.38 dot1x user-ip freeze

dot1x user-ip freeze 命令用来开启 802.1X 用户 IP 地址冻结功能。

undo dot1x user-ip freeze 命令用来关闭 802.1X 用户 IP 地址冻结功能。

【命令】

```
dot1x user-ip freeze
undo dot1x user-ip freeze
```

【缺省情况】

802.1X 用户 IP 地址冻结功能处于关闭状态。

【视图】

二层以太网接口视图

【缺省用户角色】

network-admin

【使用指导】

开启 802.1X 用户 IP 地址冻结功能后，端口首次获取且保存了 802.1X 上线用户的 IP 地址之后，不会随着该用户 IP 地址的变化而更新 IP Source Guard 表项。有关 IP Source Guard 命令的详细介绍，请参见“安全命令参考”中的“IP Source Guard”。

【举例】

开启端口 GigabitEthernet1/0/1 上的 802.1X 用户 IP 地址冻结功能。

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] dot1x user-ip freeze
```

1.1.39 reset dot1x guest-vlan

reset dot1x guest-vlan 命令用来清除 Guest VLAN 内 802.1X 用户，使其退出 Guest VLAN。

【命令】

```
reset dot1x guest-vlan interface interface-type interface-number  
[ mac-address mac-address ]
```

【视图】

用户视图

【缺省用户角色】

network-admin

【参数】

interface *interface-type interface-number*: 表示使指定端口上的用户退出 Guest VLAN。*interface-type interface-number* 为端口类型和端口编号。

mac-address *mac-address*: 表示使指定 MAC 地址的用户退出 Guest VLAN。若不指定本参数，则表示使指定端口上的所有用户退出 Guest VLAN。

【举例】

在端口 GigabitEthernet1/0/1 上使得 MAC 地址为 1-1-1 的 802.1X 用户退出 Guest VLAN。

```
<Sysname> reset dot1x guest-vlan interface gigabitethernet 1/0/1 mac-address 1-1-1
```

【相关命令】

- **dot1x guest-vlan**

1.1.40 reset dot1x statistics

reset dot1x statistics 命令用来清除 802.1X 的统计信息。

【命令】

```
reset dot1x statistics [ interface interface-type interface-number ]
```

【视图】

用户视图

【缺省用户角色】

network-admin

【参数】

interface *interface-type interface-number*: 清除指定端口上的 802.1X 统计信息。*interface-type interface-number* 为端口类型和端口编号。如果不指定本参数，则清除所有端口上的 802.1X 统计信息。

【举例】

清除端口 GigabitEthernet1/0/1 上的 802.1X 统计信息。

```
<Sysname> reset dot1x statistics interface gigabitethernet 1/0/1
```

【相关命令】

- `display dot1x`

目 录

1 MAC地址认证	1-1
1.1 MAC地址认证配置命令	1-1
1.1.1 display mac-authentication	1-1
1.1.2 display mac-authentication connection	1-4
1.1.3 display mac-authentication mac-address	1-7
1.1.4 mac-authentication	1-8
1.1.5 mac-authentication access-user log enable	1-9
1.1.6 mac-authentication carry user-ip	1-9
1.1.7 mac-authentication critical vlan	1-10
1.1.8 mac-authentication critical-voice-vlan	1-11
1.1.9 mac-authentication domain	1-12
1.1.10 mac-authentication guest-vlan	1-13
1.1.11 mac-authentication guest-vlan auth-period	1-14
1.1.12 mac-authentication host-mode	1-15
1.1.13 mac-authentication max-user	1-15
1.1.14 mac-authentication offline-detect enable	1-16
1.1.15 mac-authentication parallel-with-dot1x	1-17
1.1.16 mac-authentication re-authenticate	1-18
1.1.17 mac-authentication re-authenticate server-unreachable keep-online	1-18
1.1.18 mac-authentication timer (interface view)	1-19
1.1.19 mac-authentication timer (system view)	1-21
1.1.20 mac-authentication user-name-format	1-22
1.1.21 reset mac-authentication critical vlan	1-23
1.1.22 reset mac-authentication critical-voice-vlan	1-24
1.1.23 reset mac-authentication guest-vlan	1-25
1.1.24 reset mac-authentication statistics	1-25

1 MAC地址认证

1.1 MAC地址认证配置命令

1.1.1 display mac-authentication

display mac-authentication 命令用来显示 MAC 地址认证的相关信息。

【命令】

display mac-authentication [**interface** *interface-type interface-number*]

【视图】

任意视图

【缺省用户角色】

network-admin
network-operator

【参数】

interface interface-type interface-number: 显示全局及指定端口的 MAC 地址认证相关信息。*interface-type interface-number* 为端口类型和端口编号。若指定的端口上未使能 MAC 地址认证，则不显示该端口任何信息。

【使用指导】

如果不指定任何参数，则显示所有在线 MAC 地址认证的详细信息，主要包括全局及端口的配置信息、认证报文统计信息以及认证用户信息。

【举例】

显示 MAC 地址认证信息。

```
<Sysname> display mac-authentication
Global MAC authentication parameters:
  MAC authentication      : Enabled
  Username format        : MAC address in lowercase(xxxxxxxxxxxx)
  Username                : mac
  Password                : Not configured
  Offline detect period  : 300 s
  Quiet period            : 60 s
  Server timeout          : 100 s
  Reauth period           : 3600 s
  Authentication domain   : Not configured, use default domain
Online MAC-auth wired users   : 1

Silent MAC users:
  MAC address      VLAN ID  From port      Port index
  0001-0000-0001   100      GE1/0/2        21
```

```
GigabitEthernet1/0/1 is link-up
  MAC authentication          : Enabled
  Carry User-IP              : Disabled
  Authentication domain      : Not configured
  Auth-delay timer           : Enabled
  Auth-delay period          : 60 s
  Periodic reauth            : Enabled
    Reauth period            : 120 s
  Re-auth server-unreachable : Logoff
  Guest VLAN                 : 100
  Guest VLAN auth-period     : 150 s
  Critical VLAN              : Not configured
  Critical voice VLAN        : Disabled
  Host mode                  : Multiple VLAN
  Offline detection          : Enabled
  Authentication order       : Parallel

  Guest VSI                  : Not configured
  Guest VSI auth-period      : 30 s
  Critical VSI               : Not configured
  Auto-tag feature           : Disabled
  VLAN tag configuration ignoring : Disabled
  Max online users           : 4294967295
  Authentication attempts    : successful 2, failed 3
  Current online users       : 1

      MAC address      Auth state
      0001-0000-0001   Unauthenticated
```

表1-1 display mac-authentication 命令显示信息描述表

字段	描述
Global MAC authentication parameters	全局MAC地址认证参数
MAC authentication	MAC地址认证的开启状态
Username format	MAC地址认证使用的账号格式 <ul style="list-style-type: none"> 若采用 MAC 地址账号，则显示具体的用户名格式以及是否带连字符、字母是否大小写，例如本例中“MAC address in lowercase(xxxxxxxxxxxx)”，它表示用户名格式为不带连字符的 MAC 地址，其中字母为小写 若采用固定用户名账号，则显示“Fixed account”
Username	用户名 <ul style="list-style-type: none"> 采用 MAC 地址账号时，该值显示为“mac”，无实际意义，仅表示采用 MAC 地址作为用户名和密码 采用固定用户名账号时，该值为配置的用户名（缺省为 mac）
Password	用户名的密码

字段	描述
	<ul style="list-style-type: none"> 采用 MAC 地址账号时，该值显示为 “Not configured” 采用固定用户名账号时，配置的值将显示为*****
Offline detect period	下线检测定时器的值
Quiet period	静默定时器的值
Server timeout	服务器连接超时定时器的值
Reauth period	重认证定时器的值
Authentication domain	系统视图下指定的MAC地址认证用户使用的认证域，如果没有指定认证域，则显示Not configured, use default domain
Online MAC-auth wired users	在线有线用户和正在发起MAC地址认证的有线用户的总数
Silent MAC users	静默用户信息
MAC address	静默用户的MAC地址
VLAN ID	静默用户所在的VLAN
From port	静默用户接入的端口名称
Port index	静默用户接入的端口索引号
GigabitEthernet1/0/1 is link-up	端口GigabitEthernet1/0/1的链路状态
MAC authentication	当前端口的MAC地址认证开启状态
Carry User-IP	MAC地址认证请求携带用户IP地址关闭状态
Authentication domain	端口上指定的MAC地址认证用户使用的认证域
Auth-delay timer	MAC地址认证延迟功能的开启状态
Auth-delay period	配置的认证延迟时间
Periodic reauth	端口上MAC地址重认证开启状态
Reauth period	端口上配置的MAC地址重认证时间间隔
Re-auth server-unreachable	重认证时服务器不可达对MAC地址认证的在线用户采取的动作 <ul style="list-style-type: none"> Logoff: 重认证服务器不可达，强制 MAC 地址认证在线用户下线 Online: 重认证服务器不可达，保持 MAC 地址认证在线用户在线
Guest VLAN	端口配置的Guest VLAN，如果没有配置，则显示Not configured
Guest VLAN auth-period	进入Guest VLAN后发起重认证的时间间隔
Critical VLAN	端口配置的Critical VLAN，如果没有配置，则显示Not configured
Critical voice VLAN	端口配置MAC地址认证的Critical Voice VLAN功能的开启状态

字段	描述
	<ul style="list-style-type: none"> Enabled: 打开 Disabled: 关闭 S5110V2-SI和S5000V3-EI系列交换机不支持该参数
Host mode	相同MAC地址用户的工作模式 <ul style="list-style-type: none"> 如果配置的是多 VLAN 模式，则显示 Multiple VLAN 如果配置的是单 VLAN 模式，则显示 Single VLAN
Offline detection	MAC地址认证用户下线检测的开启状态 <ul style="list-style-type: none"> Enabled: 处于开启状态 Disabled: 处于关闭状态
Authentication order	MAC地址认证和802.1X认证并行处理 <ul style="list-style-type: none"> Default: 处于关闭状态 Parallel: 处于开启状态
Guest VSI	(暂不支持) 端口配置的Guest VSI，如果没有配置，则显示Not configured
Guest VSI auth-period	(暂不支持) 进入Guest VSI后发起重认证的时间间隔，单位为秒
Critical VSI	(暂不支持) 端口配置的Critical VSI，如果没有配置，则显示Not configured
Auto-tag feature	(暂不支持) 端口上MAC地址认证授权VLAN自动Tag功能 <ul style="list-style-type: none"> Enabled: 处于开启状态 Disabled: 处于关闭状态
VLAN tag configuration ignoring	(暂不支持) 端口上MAC地址认证授权VLAN自动Tag忽略静态VLAN配置功能 <ul style="list-style-type: none"> Enabled: 处于开启状态 Disabled: 处于关闭状态
Max online users	本端口最多可容纳的接入用户数
Authentication attempts: successful 1, failed 0	端口上MAC地址认证的统计信息，包括认证通过的次数和认证失败的次数
MAC address	接入用户的MAC地址
Auth state	接入用户的状态 <ul style="list-style-type: none"> Authenticated: 认证成功 Unauthenticated: 认证失败

1.1.2 display mac-authentication connection

display mac-authentication connection 命令用来显示 MAC 地址认证在线用户的详细信息。

【命令】

```
display mac-authentication connection [ open ] [ interface interface-type  
interface-number | slot slot-number | user-mac mac-addr | user-name  
user-name ]
```

【视图】

任意视图

【缺省用户角色】

network-admin
network-operator

【参数】

open: 只显示在开放认证模式下使用不存在的用户名或者错误的密码接入的 MAC 地址认证的用户信息。若不指定本参数，则显示设备上所有 MAC 地址认证在线用户的信息。

interface interface-type interface-number: 显示指定端口的 MAC 地址认证用户信息。其中 *interface-type interface-number* 表示绑定的端口类型和端口编号。若不指定本参数，则显示设备上所有的 MAC 地址认证用户信息。

slot slot-number: 显示指定成员设备上的 MAC 地址认证用户信息。*slot-number* 表示设备在 IRF 中的成员编号。若不指定本参数，则显示所有成员设备上的 MAC 地址认证用户信息。

user-mac mac-addr: 显示指定 MAC 地址的 MAC 地址认证用户信息。其中 *mac-addr* 表示用户的 MAC 地址，格式为 H-H-H。若不指定本参数，则显示设备上所有的 MAC 地址认证用户信息。

user-name user-name: 显示指定用户名的 MAC 地址认证用户信息。其中 *user-name* 表示用户名（可包含域名），为 1~55 个字符的字符串，区分大小写。若不指定本参数，则显示设备上所有的 MAC 地址认证用户信息。

【举例】

显示所有 MAC 地址认证在线用户信息。

```
<Sysname> display mac-authentication connection  
Total connections: 1  
  
Slot ID: 0  
User MAC address: 0015-e9a6-7cfe  
Access interface: GigabitEthernet1/0/1  
Username: ias  
User access state: Successful  
Authentication domain: macusers  
IPv4 address: 192.168.1.1  
IPv6 address: 2000:0:0:0:1:2345:6789:abcd  
Initial VLAN: 1  
Authorization untagged VLAN: 100  
Authorization tagged VLAN: N/A  
Authorization VSI: N/A  
Authorization ACL ID: 3001  
Authorization user profile: N/A  
Authorization CAR: N/A
```

Termination action: Radius-request

Session timeout period: 2 s

Online from: 2013/03/02 13:14:15

Online duration: 0h 2m 15s

表1-2 display mac-authentication connection 命令显示信息描述表

字段	描述
Total connections	在线MAC地址认证用户个数
User MAC address	用户的MAC地址
Access interface	用户的接入接口名称
Username	用户名
User access state	用户的接入状态 <ul style="list-style-type: none">Successful: MAC 地址认证成功并接入Open: 使用不存在的用户名或者错误的密码进行开放认证并接入
Authentication domain	认证时所用的ISP域的名称
IPv4 address	用户IPv4地址 若未获取到用户的IP地址，则不显示该字段
IPv6 address	用户IPv6地址 若未获取到用户的IP地址，则不显示该字段
Initial VLAN	初始的VLAN
Authorization untagged VLAN	授权的untagged VLAN
Authorization tagged VLAN	授权的tagged VLAN
Authorization VSI	（暂不支持）授权的VSI
Authorization ACL ID	授权ACL编号，若未授权成功，则在ACL编号后显示“(NOT effective)”
Authorization user profile	授权用户的User profile名称
Authorization CAR	（暂不支持）当服务器未授权用户CAR属性时，该字段显示为N/A。
Terminate action	服务器下发的终止动作类型： <ul style="list-style-type: none">Default: 会话超时时间到达后，强制用户下线Radius-Request: 会话超时时间到达后，请求 MAC 地址认证用户进行重认证 用户采用本地认证时，该字段显示为Default
Session timeout period	服务器下发的会话超时时间，该时间到达之后，用户所在的会话将会被删除，之后，对该用户所采取的动作，由Terminate action字段的取值决定
Online from	MAC认证用户的上线时间
Online duration	MAC认证用户的在线时长

1.1.3 display mac-authentication mac-address

display mac-authentication mac-address 命令用来显示指定类型的 VLAN 中的 MAC 地址认证用户的 MAC 地址信息。

【命令】

display mac-authentication mac-address { critical-vlan | guest-vlan }
[**interface** *interface-type interface-number*]

【视图】

任意视图

【缺省用户角色】

network-admin
network-operator

【参数】

critical-vlan: 显示 MAC 地址认证 Critical VLAN 中的用户 MAC 地址信息。
guest-vlan: 显示 MAC 地址认证 Guest VLAN 中的用户 MAC 地址信息。
interface interface-type interface-number: 显示 VLAN 中指定端口的 MAC 地址认证用户的 MAC 地址信息。其中 *interface-type interface-number* 表示端口类型和端口编号。若不指定本参数，则显示指定类型的 VLAN 中所有端口的 MAC 地址认证用户的 MAC 地址信息。

【使用指导】

查询到的 MAC 地址数量以及 MAC 地址明细为粗略统计，当有大量用户频繁进行认证时可能不能完全精准显示。

【举例】

显示所有 MAC 地址认证 Guest VLAN 中的用户的 MAC 地址信息。

```
<Sysname> display mac-authentication mac-address guest-vlan
Total MAC addresses: 10
Interface: GigabitEthernet1/0/1          Guest VLAN: 3          Aging time: N/A
MAC addresses: 8
    0800-2700-9427    0800-2700-2341    0800-2700-2324    0800-2700-2351
    0800-2700-5627    0800-2700-2251    0800-2700-8624    0800-2700-3f51

Interface: GigabitEthernet1/0/2          Guest VLAN: 5          Aging time: 30 sec
MAC addresses: 2
    0801-2700-9427    0801-2700-2341
```

表1-3 display mac-authentication mac-address 命令显示信息描述表

字段	描述
Total MAC addresses	指定类型的VLAN中的所有MAC地址总数
Interface	用户的接口名称

字段	描述
Type VLAN	显示MAC地址认证用户所在的VLAN信息，Type包含如下取值： <ul style="list-style-type: none"> • Critical VLAN • Guest VLAN
Aging time	MAC地址老化时间，单位秒。N/A表示该地址不老化
MAC addresses	MAC地址数
XXXX-XXXX-XXXX	MAC地址

【相关命令】

- `mac-authentication critical vlan`
- `mac-authentication guest-vlan`

1.1.4 mac-authentication

`mac-authentication` 命令用来开启端口上或全局的 MAC 地址认证。

`undo mac-authentication` 命令用来关闭端口上或全局的 MAC 地址认证。

【命令】

```
mac-authentication
undo mac-authentication
```

【缺省情况】

所有端口及全局的 MAC 地址认证都处于关闭状态。

【视图】

系统视图
二层以太网接口视图

【缺省用户角色】

network-admin

【使用指导】

只有全局和端口的 MAC 地址认证均开启后，MAC 地址认证配置才能在端口上生效。

【举例】

```
# 开启全局的 MAC 地址认证。
<Sysname> system-view
[Sysname] mac-authentication
# 开启端口 GigabitEthernet1/0/1 上的 MAC 地址认证。
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] mac-authentication
```

【相关命令】

- `display mac-authentication`

1.1.5 mac-authentication access-user log enable

mac-authentication access-user log enable 命令用来开启 MAC 地址认证接入用户日志信息功能。

undo mac-authentication access-user log enable 命令用来关闭 MAC 地址认证接入用户日志信息功能。

【命令】

```
mac-authentication access-user log enable [ failed-login | logoff |
successful-login ] *
undo mac-authentication access-user log enable [ failed-login | logoff |
successful-login ] *
```

【缺省情况】

MAC 地址认证接入用户日志信息功能处于关闭状态。

【视图】

系统视图

【缺省用户角色】

network-admin

【参数】

failed-login: MAC 地址认证用户上线失败的日志信息。

logoff: MAC 地址认证用户下线的日志信息。

successful-login: MAC 地址认证用户上线成功的日志信息。

【使用指导】

为了防止设备输出过多的 MAC 地址认证接入用户日志信息，一般情况下建议关闭此功能。
配置本命令时，如果未指定任何参数，将同时开启或关闭本命令所有参数对应的日志功能。

【举例】

开启 MAC 地址认证接入用户上线失败的日志信息。

```
<Sysname> system-view
```

```
[Sysname] mac-authentication access-user log enable failed-login
```

【相关命令】

- **info-center source maca logfile deny**（网络管理和监控/信息中心）

1.1.6 mac-authentication carry user-ip

mac-authentication carry user-ip 命令用来配置 MAC 地址认证请求中携带用户 IP 地址。

undo mac-authentication carry user-ip 命令用来恢复缺省情况。

【命令】

```
mac-authentication carry user-ip
undo mac-authentication carry user-ip
```

【缺省情况】

MAC 地址认证请求中不携带用户 IP 地址。

【视图】

二层以太网接口视图

【缺省用户角色】

network-admin

【使用指导】

在终端用户采用静态 IP 地址方式接入的组网环境中，如果终端用户擅自修改自己的 IP 地址，则整个网络环境中可能会出现 IP 地址冲突等问题。

为了解决以上问题，管理员可以在端口上开启 MAC 地址认证请求中携带用户 IP 地址的功能，用户在进行 MAC 地址认证时，设备会把用户的 IP 地址上传到 iMC 服务器。然后 iMC 服务器会把认证用户的 IP 地址和 MAC 地址与服务器上已经存在的 IP 与 MAC 的绑定表项进行匹配，如果匹配成功，则该用户 MAC 地址认证成功；否则，MAC 地址认证失败。

H3C 的 iMC 服务器上 IP 与 MAC 地址信息绑定表项的生成方式如下：

- 如果在 iMC 服务器上创建用户时手工指定了用户的 IP 地址和 MAC 地址信息，则服务器使用手工指定的 IP 和 MAC 信息生成该用户的 IP 与 MAC 地址的绑定表项。
- 如果在 iMC 服务器上创建用户时未手工指定用户的 IP 地址和 MAC 地址信息，则服务器使用用户初次进行 MAC 地址认证时使用的 IP 地址和 MAC 地址生成该用户的 IP 与 MAC 地址的绑定表项。

此功能仅对采用静态 IP 地址方式接入的认证用户才有效。在采用 DHCP 方式获取 IP 地址的情况下，因为用户 MAC 地址认证成功之后才可以进行 IP 地址获取，所以用户在进行 MAC 地址认证时，设备无法上传用户的 IP 地址。

在开启了 MAC 地址认证的端口上，不建议将本命令与 **mac-authentication guest-vlan** 命令同时配置；否则，加入 Guest VLAN 的用户无法再次发起 MAC 地址认证，用户会一直停留在 Guest VLAN 中。

【举例】

在端口 GigabitEthernet1/0/1 上配置 MAC 地址认证请求携带用户 IP 地址功能。

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] mac-authentication carry user-ip
```

【相关命令】

- **mac-authentication**

1.1.7 mac-authentication critical vlan

mac-authentication critical vlan 命令用来配置端口的 MAC 地址认证的 Critical VLAN。

undo mac-authentication critical vlan 命令用来恢复缺省情况。

【命令】

mac-authentication critical vlan critical-vlan-id

undo mac-authentication critical vlan

【缺省情况】

端口上未配置 MAC 地址认证的 Critical VLAN。

【视图】

二层以太网接口视图

【缺省用户角色】

network-admin

【参数】

critical-vlan-id: 端口上指定的 Critical VLAN ID，取值范围为 1~4094。该 VLAN 必须已经创建。

【使用指导】

配置此功能后，当 MAC 用户认证时对应的 ISP 域下所有认证服务器都不可达的情况下被授权访问 Critical VLAN 内的资源。

禁止删除已被配置为 Critical VLAN 的 VLAN，若要删除该 VLAN，请先通过 **undo mac-authentication critical vlan** 命令取消 MAC 地址认证的 Critical VLAN 配置。

【举例】

配置端口 GigabitEthernet1/0/1 的 Critical VLAN 为 VLAN 100。

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] mac-authentication critical vlan 100
```

【相关命令】

- **display mac-authentication**
- **reset mac-authentication critical vlan**

1.1.8 mac-authentication critical-voice-vlan

mac-authentication critical-voice-vlan 命令用来开启端口上 MAC 地址认证的 Critical Voice VLAN 功能。

undo mac-authentication critical-voice-vlan 命令用来关闭端口上 MAC 地址认证的 Critical Voice VLAN 功能。

【命令】

mac-authentication critical-voice-vlan
undo mac-authentication critical-voice-vlan

【缺省情况】

端口下 MAC 地址认证的 Critical Voice VLAN 功能处于关闭状态。

【视图】

二层以太网接口视图

【缺省用户角色】

network-admin

【使用指导】

S5110V2-SI 和 S5000V3-EI 系列交换机不支持配置该命令。

端口上开启 MAC 地址认证 Critical Voice VLAN 功能后，当语音用户进行 MAC 地址认证采用的 ISP 域中的所有认证服务器都不可达时，端口将被加入到此端口上的 Voice VLAN 中。端口上语音 VLAN 的配置命令请参见“二层技术-以太网交换命令参考”中的“VLAN”。

设备通过 LLDP（Link Layer Discovery Protocol，链路层发现协议）来判断用户是否为语音用户，因此为保证 MAC 地址认证 Critical Voice VLAN 功能可以正常工作，请在开启此功能之前务必确保全局和相应端口下均已开启 LLDP 功能。有关 LLDP 功能的配置命令介绍请参见“二层技术-以太网交换命令参考”中的“LLDP”。

【举例】

开启端口 GigabitEthernet1/0/1 上 MAC 地址认证 Critical Voice VLAN 功能。

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] mac-authentication critical-voice-vlan
```

【相关命令】

- **display mac-authentication**
- **lldp enable**（二层技术-以太网交换命令参考/LLDP）
- **lldp global enable**（二层技术-以太网交换命令参考/LLDP）
- **reset mac-authentication critical-voice-vlan**
- **voice-vlan enable**（二层技术-以太网交换命令参考/VLAN）

1.1.9 mac-authentication domain

mac-authentication domain 命令用来指定 MAC 地址认证用户使用的认证域。

undo mac-authentication domain 命令用来恢复缺省情况。

【命令】

```
mac-authentication domain domain-name
undo mac-authentication domain
```

【缺省情况】

未指定 MAC 地址认证用户使用的认证域时，使用系统缺省的认证域。缺省认证域的介绍请参见“安全命令参考/AAA”中的命令 **domain default enable**。

【视图】

系统视图

二层以太网接口视图

【缺省用户角色】

network-admin

【参数】

domain-name: ISP 域名，为 1~255 个字符的字符串，不区分大小写。

【使用指导】

不同视图下指定的认证域的生效范围不同：

- 系统视图下指定的认证域对所有开启了 MAC 地址认证的端口生效。
- 二层以太网接口视图下指定的认证域仅对本端口有效。不同的端口可以指定不同的认证域。

端口上接入的 MAC 地址认证用户将按照如下先后顺序选择认证域：端口上指定的认证域 > 系统视图下指定的认证域 > 系统缺省的认证域。

【举例】

在系统视图下指定 MAC 地址认证用户使用的认证域为 domain1。

```
<Sysname> system-view
```

```
[Sysname] mac-authentication domain domain1
```

指定端口 GigabitEthernet1/0/1 上接入的 MAC 地址认证用户使用的认证域为 aabbcc。

```
[Sysname] interface gigabitethernet 1/0/1
```

```
[Sysname-GigabitEthernet1/0/1] mac-authentication domain aabbcc
```

【相关命令】

- **display mac-authentication**
- **domain default enable**（安全命令参考/AAA）

1.1.10 mac-authentication guest-vlan

mac-authentication guest-vlan 命令用来配置端口的 MAC 地址认证的 Guest VLAN。

undo mac-authentication guest-vlan 命令用来恢复缺省情况。

【命令】

```
mac-authentication guest-vlan guest-vlan-id
```

```
undo mac-authentication guest-vlan
```

【缺省情况】

端口上未配置 MAC 地址认证的 Guest VLAN。

【视图】

二层以太网接口视图

【缺省用户角色】

network-admin

【参数】

guest-vlan-id: 端口上指定的 Guest VLAN ID，取值范围为 1~4094。该 VLAN 必须已经创建。

【使用指导】

配置此功能后，当 MAC 地址认证失败的情况下，用户可以继续被授权访问的 Guest VLAN 内的资源。

禁止删除已被配置为 Guest VLAN 的 VLAN，若要删除该 VLAN，请先通过 **undo mac-authentication guest-vlan** 命令取消 MAC 地址认证的 Guest VLAN 配置。

【举例】

配置端口 GigabitEthernet1/0/1 的 Guest VLAN 为 VLAN 100。

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] mac-authentication guest-vlan 100
```

【相关命令】

- **display mac-authentication**
- **reset mac-authentication guest-vlan**

1.1.11 mac-authentication guest-vlan auth-period

mac-authentication guest-vlan auth-period 命令用来配置设备对 Guest VLAN 中的用户进行重新认证的时间间隔。

undo mac-authentication guest-vlan auth-period 命令用来恢复缺省情况。

【命令】

```
mac-authentication guest-vlan auth-period period-value
undo mac-authentication guest-vlan auth-period
```

【缺省情况】

设备对 Guest VLAN 中的用户进行重新认证的时间间隔为 30 秒。

【视图】

二层以太网接口视图

【缺省用户角色】

network-admin

【参数】

period-value: 表示设备重新发起认证的时间间隔，取值范围为 1~3600，单位为秒。

【举例】

在端口 GigabitEthernet1/0/1 上配置设备对 Guest VLAN 中的用户进行重新认证的时间间隔为 150 秒。

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] mac-authentication guest-vlan auth-period 150
```

【相关命令】

- **display mac-authentication**
- **mac-authentication guest-vlan**

1.1.12 mac-authentication host-mode

mac-authentication host-mode multi-vlan 命令用来指定端口工作在 MAC 地址认证的多 VLAN 模式。

undo mac-authentication host-mode 命令用来恢复缺省情况。

【命令】

```
mac-authentication host-mode multi-vlan
undo mac-authentication host-mode
```

【缺省情况】

端口工作在 MAC 地址认证的单 VLAN 模式。

【视图】

二层以太网接口视图

【缺省用户角色】

network-admin

【使用指导】

端口工作在多 VLAN 模式下时,如果相同 MAC 地址的用户在属于不同 VLAN 的相同端口再次接入,设备将能够允许用户的流量在新的 VLAN 内通过,且允许该用户的报文无需重新认证而在多个 VLAN 中转发。

端口工作在单 VLAN 模式下时,在用户已上线,且没有被下发授权 VLAN 情况下,如果此用户在属于不同 VLAN 的相同端口再次接入,则设备将让原用户下线,使得该用户能够新的 VLAN 内重新开始认证。如果已上线用户被下发了授权 VLAN,则此用户在属于不同 VLAN 的相同端口再次接入时不会被强制下线。

对于接入 IP 电话类用户的端口,指定端口工作在 MAC 地址认证的多 VLAN 模式,可避免 IP 电话终端的报文所携带的 VLAN tag 发生变化后,因用户流量需要重新认证带来语音报文传输质量受干扰的问题。

【举例】

```
# 配置端口 GigabitEthernet1/0/1 工作在 MAC 地址认证的多 VLAN 模式。
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] mac-authentication host-mode multi-vlan
```

【相关命令】

- **display mac-authentication**

1.1.13 mac-authentication max-user

mac-authentication max-user 命令用来配置端口上最多允许同时接入的 MAC 地址认证用户数。**undo mac-authentication max-user** 命令用来恢复缺省情况。

【命令】

```
mac-authentication max-user max-number
```

undo mac-authentication max-user

【缺省情况】

端口上最多允许同时接入的 MAC 地址认证用户数为 4294967295。

【视图】

二层以太网接口视图

【缺省用户角色】

network-admin

【参数】

max-number: 端口允许同时接入的 MAC 地址认证用户数的最大值, 取值范围为 1~4294967295。

【使用指导】

由于系统资源有限, 如果当前端口上接入的用户过多, 接入用户之间会发生资源的争用, 因此适当地配置该值可以使属于当前端口的用户获得可靠的性能保障。当接入此端口的 MAC 地址认证用户数超过最大值后, 新接入的用户将被拒绝。

【举例】

配置端口 GigabitEthernet1/0/1 最多允许同时接入 32 个 MAC 地址认证用户。

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] mac-authentication max-user 32
```

【相关命令】

- **display mac-authentication**

1.1.14 mac-authentication offline-detect enable

mac-authentication offline-detect enable 命令用来开启端口的 MAC 地址认证下线检测功能。

undo mac-authentication offline-detect enable 命令用来关闭端口的 MAC 地址认证下线检测功能。

【命令】

```
mac-authentication offline-detect enable
undo mac-authentication offline-detect enable
```

【缺省情况】

端口的 MAC 地址认证下线检测功能处于开启状态。

【视图】

二层以太网接口视图

【缺省用户角色】

network-admin

【使用指导】

开启端口的 MAC 地址认证下线检测功能后，若设备在一个下线检测定时器间隔之内，未收到此端口下某在线用户的报文，则将切断该用户的连接，同时通知 RADIUS 服务器停止对此用户进行计费。关闭端口的 MAC 地址认证下线检测功能后，设备将不会对在线用户的状态进行检测。

【举例】

关闭端口 GigabitEthernet1/0/1 上的 MAC 地址认证下线检测功能。

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] undo mac-authentication offline-detect enable
```

【相关命令】

- **mac-authentication timer**

1.1.15 mac-authentication parallel-with-dot1x

mac-authentication parallel-with-dot1x 命令用来配置端口 MAC 地址认证和 802.1X 认证并行处理功能。

undo mac-authentication parallel-with-dot1x 命令用来恢复缺省情况。

【命令】

```
mac-authentication parallel-with-dot1x
undo mac-authentication parallel-with-dot1x
```

【缺省情况】

端口在收到源 MAC 地址未知的报文触发认证时，按照 802.1X 认证完成后再进行 MAC 地址认证的顺序进行处理。

【视图】

二层以太网接口视图

【缺省用户角色】

network-admin

【使用指导】

端口采用 802.1X 和 MAC 地址组合认证功能适用于如下情况：

- 端口上同时开启了 802.1X 和 MAC 地址认证功能，并配置了 802.1X 认证的端口的接入控制方式为 macbased。
- 开启了端口安全功能，并配置了端口安全模式为 userlogin-secure-or-mac 或 userlogin-secure-or-mac-ext。端口安全模式的具体配置请参见“安全命令参考”中的“端口安全”。

在端口采用 802.1X 认证和 MAC 地址组合认证的情况下，如果想要在端口加入到 802.1X Guest VLAN 之前进行 MAC 地址认证并下发授权 VLAN，请通过本命令开启端口 MAC 地址认证和 802.1X 认证并行处理功能，并配置端口延迟加入 802.1X Guest VLAN 功能。关于端口延迟加入 802.1X Guest VLAN 配置命令的详细介绍，请参见“安全命令参考”中的“802.1X”。

开启了 MAC 地址认证和 802.1X 认证并行处理功能后，不建议配置端口的 MAC 地址认证延迟功能。

【举例】

在端口 GigabitEthernet1/0/1 上开启 MAC 地址认证和 802.1X 认证并行处理功能。

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] mac-authentication parallel-with-dot1x
```

1.1.16 mac-authentication re-authenticate

mac-authentication re-authenticate 命令用来开启 MAC 地址周期性重认证功能。

undo mac-authentication re-authenticate 命令用来关闭 MAC 地址周期性重认证功能。

【命令】

```
mac-authentication re-authenticate
undo mac-authentication re-authenticate
```

【缺省情况】

MAC 地址周期性重认证功能处于关闭状态。

【视图】

二层以太网接口视图

【缺省用户角色】

network-admin

【使用指导】

端口开启了 MAC 地址认证用户的周期性重认证功能后,设备会周期性对该端口上的 MAC 地址认证在线用户进行重认证,以检测用户连接状态的变化,更新服务器下发的授权属性(例如 ACL、VLAN 等)。

【举例】

在端口 GigabitEthernet1/0/1 上开启 MAC 地址重认证功能,并配置周期性重认证时间间隔为 1800 秒。

```
<Sysname> system-view
[Sysname] mac-authentication timer reauth-period 1800
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] mac-authentication re-authenticate
```

【相关命令】

- **display mac-authentication**
- **mac-authentication timer**

1.1.17 mac-authentication re-authenticate server-unreachable keep-online

mac-authentication re-authenticate server-unreachable keep-online 命令用来配置重认证服务器不可达时端口上的 MAC 地址认证用户保持在线状态。

undo mac-authentication re-authenticate server-unreachable 命令用来恢复缺省情况。

【命令】

```
mac-authentication re-authenticate server-unreachable keep-online
undo mac-authentication re-authenticate server-unreachable
```

【缺省情况】

端口上的 MAC 地址认证在线用户重认证时，若认证服务器不可达，则会被强制下线。

【视图】

二层以太网接口视图

【缺省用户角色】

network-admin

【使用指导】

配置此命令后，在对 MAC 地址认证用户重认证过程中，若设备发现认证服务器状态不可达，则保持 MAC 地址认证用户在线。

是否对 MAC 地址认证在线用户进行周期性重认证由认证服务器授权的属性所决定。认证服务器通过下发 RADIUS 属性（`session-timeout`、`Terminal-Action`）来指定用户会话超时时长以及会话中止的动作类型，它们共同决定了如何对用户进行重认证。

- 当会话中止的动作类型为要求用户进行重认证时，端口会在用户会话超时时长到达后对该用户进行重认证；
- 当会话中止的动作类型为要求用户下线时，端口会在用户会话超时时长到达强制该用户下线；
- 当认证服务器未下发用户会话超时时长时，设备不会对用户进行重认证。

【举例】

配置端口 GigabitEthernet1/0/1 上的 MAC 地址认证在线用户进行重认证时，若服务器不可达，则保持在线状态。

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] mac-authentication re-authenticate server-unreachable
keep-online
```

【相关命令】

- `display mac-authentication`

1.1.18 mac-authentication timer (interface view)

`mac-authentication timer` 命令用来配置端口上的 MAC 地址认证的定时器参数。

`undo mac-authentication timer` 命令用来将端口上指定的 MAC 地址认证定时器恢复为缺省情况。

【命令】

```
mac-authentication timer { auth-delay auth-delay-time | reauth-period
reauth-period-value }
undo mac-authentication timer { auth-delay | reauth-period }
```

【缺省情况】

端口上未配置 MAC 地址认证延迟定时器，表示 MAC 地址认证延迟功能处于关闭状态，如果用户报文触发 MAC 地址认证，认证将会立刻开始；端口上未配置 MAC 地址周期性重认证定时器，端口使用系统视图下配置的 MAC 地址周期性重认证定时器的取值。

【视图】

二层以太网接口视图

【缺省用户角色】

network-admin

【参数】

auth-delay *auth-delay-time*: 表示 MAC 地址认证延迟定时器。其中 *auth-delay-time* 表示 MAC 地址认证延迟定时器的值，取值范围为 1~180，单位为秒。

reauth-period *reauth-period-value*: 表示 MAC 地址认证周期性重认证定时器。其中 *reauth-period-value* 表示周期性重认证定时器的值，取值范围为 60~7200，单位为秒。

【使用指导】

端口同时开启了 MAC 地址认证和 802.1X 认证的情况下，某些组网环境中希望设备对用户报文先进行 802.1X 认证。例如，有些客户端在发送 802.1X 认证请求报文之前，就已经向设备发送了其它报文，比如 DHCP 报文，因而触发了并不期望的 MAC 地址认证。这种情况下，就可以开启端口的 MAC 地址认证延时功能。

开启端口的 MAC 地址认证延时功能之后，端口就不会在收到用户报文时立即触发 MAC 地址认证，而是在等待一定的延迟时间之后，再会对之前收到的用户报文进行 MAC 地址认证。在此认证延迟期间，端口对用户报文的其它认证过程并不受影响。

开启了 MAC 地址认证延迟功能的端口上不建议同时配置端口安全的模式为 **mac-else-userlogin-secure** 或 **mac-else-userlogin-secure-ext**，否则 MAC 地址认证延迟功能不生效。端口安全模式的具体配置请参见“安全命令参考”中的“端口安全”。

对 MAC 地址认证用户进行重认证时，设备将按照如下由高到低的顺序为其选择重认证时间间隔：服务器下发的重认证时间间隔、接口视图下配置的周期性重认证定时器的值、系统视图下配置的周期性重认证定时器的值、设备缺省的周期性重认证定时器的值。

对于已在线的 MAC 地址认证用户，要等当前重认证周期结束并且认证通过后会按新配置的周期进行后续的重认证。

【举例】

开启 MAC 地址延迟认证功能，并指定 MAC 地址认证的延时时间为 10 秒。

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] mac-authentication timer auth-delay 10
```

【相关命令】

- **display mac-authentication**
- **port-security port-mode**（安全命令参考/端口安全）

1.1.19 mac-authentication timer (system view)

mac-authentication timer 命令用来配置 MAC 地址认证的定时器参数。

undo mac-authentication timer 命令用来恢复缺省情况。

【命令】

```
mac-authentication timer { offline-detect offline-detect-value | quiet  
quiet-value | reauth-period reauth-period-value | server-timeout  
server-timeout-value }  
undo mac-authentication timer { offline-detect | quiet | reauth-period |  
server-timeout }
```

【缺省情况】

下线检测定时器的值为 300 秒，静默定时器的值为 60 秒，周期性重认证定时器的值为 3600 秒，服务器超时定时器的值为 100 秒。

【视图】

系统视图

【缺省用户角色】

network-admin

【参数】

offline-detect *offline-detect-value* : 表示下线检测定时器。其中，*offline-detect-value* 表示下线检测定时器的值，取值范围为 60~2147483647，单位为秒。
quiet *quiet-value*: 表示静默定时器。其中 *quiet-value* 表示静默定时器的值，取值范围为 1~3600，单位为秒。

reauth-period *reauth-period-value* : 表示周期性重认证定时器，其中 *reauth-period-value* 表示周期性重认证定时器的值，取值范围为 60~7200，单位为秒。

server-timeout *server-timeout-value* : 表示服务器超时定时器。其中，*server-timeout-value* 表示服务器超时定时器的值，取值范围为 100~300，单位为秒。

【使用指导】

MAC 地址认证过程受以下定时器的控制：

- 下线检测定时器 (**offline-detect**)：用来设置在线用户空闲超时的时间间隔。开启 MAC 地址认证下线检测功能后，若设备在一个下线检测定时器间隔之内，没有收到某在线用户的报文，将切断该用户的连接，同时通知 RADIUS 服务器停止对其计费。配置 **offline-detect** 时，需要将 MAC 地址老化时间配成相同时间，否则会导致用户异常下线。只有当端口的 MAC 地址认证下线检测功能处于开启状态时，该定时器生效。
- 静默定时器 (**quiet**)：用来设置用户认证失败以后，设备需要等待的时间间隔。在静默期间，设备不对来自认证失败用户的报文进行认证处理，直接丢弃。静默期后，如果设备再次收到该用户的报文，则依然可以对其进行认证处理。
- 周期性重认证定时器 (**reauth-period**)：端口下开启了 MAC 地址周期性重认证功能后，设备可以此间隔为周期对端口上的在线用户发起重认证。对于已在线的 MAC 地址认证用户，要等当前重认证周期结束并且认证通过后才按新配置的周期进行后续的重认证。

- 服务器超时定时器 (**server-timeout**): 用来设置设备同 RADIUS 服务器的连接超时时间。在用户的认证过程中, 如果到服务器超时定时器超时时设备一直没有收到 RADIUS 服务器的应答, 则设备将在相应的端口上禁止此用户访问网络。

建议将 **server-timeout** 的值设定为小于或等于设备发送 RADIUS 报文的最大尝试次数 (**retry**) 与 RADIUS 服务器响应超时时间 (**timer response-timeout**) 之积。如果 **server-timeout** 的值大于 **retry** 与 **timer response-timeout** 之积, 则可能在 **server-timeout** 设定的服务器超时时间到达前, 用户被强制下线。

关于发送 RADIUS 报文的最大尝试次数、RADIUS 服务器响应超时时间的具体配置请参见“安全配置指导”中的“AAA”。

【举例】

设置服务器超时定时器时长为 150 秒。

```
<Sysname> system-view
[Sysname] mac-authentication timer server-timeout 150
```

【相关命令】

- **display mac-authentication**
- **retry** (安全命令参考/AAA)
- **timer response-timeout** (RADIUS scheme view) (安全命令参考/AAA)

1.1.20 mac-authentication user-name-format

mac-authentication user-name-format 命令用来配置 MAC 地址认证用户的帐号格式。

undo mac-authentication user-name-format 命令用来恢复缺省情况。

【命令】

```
mac-authentication user-name-format { fixed [ account name ] [ password
{ cipher | simple } string ] | mac-address [ { with-hyphen | without-hyphen }
[ lowercase | uppercase ] ] }
undo mac-authentication user-name-format
```

【缺省情况】

使用用户的 MAC 地址作为用户名和密码, 其中字母为小写, 且不带连字符“-”。

【视图】

系统视图

【缺省用户角色】

network-admin

【参数】

fixed: 表示采用固定用户名账号。

account name: 指定发送给 RADIUS 服务器进行认证或者在本地进行认证的用户名。其中 *name* 为用户名, 为 1~55 个字符的字符串, 区分大小写, 不能包括字符@, 缺省为 mac。

password: 指定固定用户名的密码。

cipher: 以密文方式设置密码。

simple: 以明文方式设置密码，该密码将以密文形式存储。

string: 密码字符串，区分大小写。明文密码为 1~63 个字符的字符串，密文密码为 1~117 个字符的字符串。

mac-address: 表示使用用户的 MAC 地址作为用户名和密码。

with-hyphen: 带连字符“-”的 MAC 地址格式，例如 xx-xx-xx-xx-xx-xx。

without-hyphen: 不带连字符“-”的 MAC 地址格式，例如 xxxxxxxxxxxx。

lowercase: MAC 地址中的字母为小写。

uppercase: MAC 地址中的字母为大写。

【使用指导】

若指定用户的 MAC 地址为用户名，则用户密码也为用户的 MAC 地址。这种情况下，每一个 MAC 地址认证用户都使用唯一的用户名进行认证，安全性高，但要求认证服务器端配置多个 MAC 形式的用户帐户。

若指定一个固定的用户名，则表示不论用户的 MAC 地址为何值，所有用户均使用设备上指定的一个固定用户名和密码作为身份信息进行认证。由于同一个端口下可以有多个用户进行认证，因此这种情况下端口上的所有 MAC 地址认证用户均使用同一个固定用户名账号进行认证，服务器端仅需要配置一个用户帐户即可满足所有认证用户的认证需求，适用于接入客户端比较可信的网络环境。

【举例】

配置 MAC 地址认证的用户名为 abc，密码是明文 xyz。

```
<Sysname> system-view
```

```
[Sysname] mac-authentication user-name-format fixed account abc password simple xyz
```

配置用户的 MAC 地址为用户名和密码，使用带连字符“-”的 MAC 地址格式，其中字母大写。

```
<Sysname> system-view
```

```
[Sysname] mac-authentication user-name-format mac-address with-hyphen uppercase
```

【相关命令】

- **display mac-authentication**

1.1.21 reset mac-authentication critical vlan

reset mac-authentication critical vlan 命令用来清除 Critical VLAN 内的 MAC 地址认证用户。

【命令】

```
reset mac-authentication critical vlan interface interface-type  
interface-number [ mac-address mac-address ]
```

【视图】

用户视图

【缺省用户角色】

network-admin

【参数】

interface *interface-type interface-number*: 表示使指定端口上的用户退出 Critical VLAN。 *interface-type interface-number* 为端口类型和端口编号。

mac-address *mac-address*: 表示使指定 MAC 地址的用户退出 Critical VLAN。若不指定本参数，则表示使指定端口上的所有用户退出 Critical VLAN。

【举例】

在端口 GigabitEthernet1/0/1 上使得 MAC 地址为 1-1-1 的 MAC 地址认证用户退出 Critical VLAN。
<Sysname> reset mac-authentication critical vlan interface gigabitethernet 1/0/1 mac-address 1-1-1

【相关命令】

- **display mac-authentication**
- **mac-authentication critical vlan**

1.1.22 reset mac-authentication critical-voice-vlan

reset mac-authentication critical-voice-vlan 命令用来清除 MAC 地址认证 Critical Voice VLAN 内的 MAC 地址认证用户。

【命令】

reset mac-authentication critical-voice-vlan interface *interface-type interface-number* [**mac-address** *mac-address*]

【视图】

用户视图

【缺省用户角色】

network-admin

【参数】

interface *interface-type interface-number*: 表示使指定端口上的用户退出 MAC 地址认证的 Critical Voice VLAN，其中 *interface-type interface-number* 为端口类型和端口编号。

mac-address *mac-address*: 表示清除指定 MAC 地址的用户退出 MAC 地址认证的 Critical Voice VLAN。若不指定本参数，则表示使指定端口上的所有用户退出 Critical Voice VLAN。

【使用指导】

S5110V2-SI 和 S5000V3-EI 系列交换机不支持配置该命令。

【举例】

在端口 GigabitEthernet1/0/1 上使得 MAC 地址为 1-1-1 的 MAC 地址认证用户退出 Critical Voice VLAN。
<Sysname> reset mac-authentication critical-voice-vlan interface gigabitethernet 1/0/1 mac-address 1-1-1

【相关命令】

- **display mac-authentication**

- **mac-authentication critical-voice-vlan**

1.1.23 reset mac-authentication guest-vlan

reset mac-authentication guest-vlan 命令用来清除 Guest VLAN 内的 MAC 地址认证用户。

【命令】

```
reset      mac-authentication    guest-vlan    interface    interface-type
interface-number [ mac-address mac-address ]
```

【视图】

用户视图

【缺省用户角色】

network-admin

【参数】

interface *interface-type interface-number*: 表示使指定端口上的用户退出 Guest VLAN。*interface-type interface-number* 为端口类型和端口编号。

mac-address *mac-address*: 表示使指定 MAC 地址的用户退出 Guest VLAN。若不指定本参数，则表示使指定端口上的所有用户退出 Guest VLAN。

【举例】

在端口 GigabitEthernet1/0/1 上使得 MAC 地址为 1-1-1 的 MAC 地址认证用户退出 Guest VLAN。

```
<Sysname> reset mac-authentication guest-vlan interface gigabitethernet 1/0/1 mac-address
1-1-1
```

【相关命令】

- **display mac-authentication**
- **mac-authentication guest-vlan**

1.1.24 reset mac-authentication statistics

reset mac-authentication statistics 命令用来清除 MAC 地址认证的统计信息。

【命令】

```
reset      mac-authentication    statistics    [ interface    interface-type
interface-number ]
```

【视图】

用户视图

【缺省用户角色】

network-admin

【参数】

interface *interface-type interface-number*: 清除指定端口的 MAC 地址认证统计信息。
interface-type interface-number 为端口类型和端口编号。如果不指定本参数，则清除所有端口上的 MAC 地址认证统计信息。

【举例】

清除以太网端口 GigabitEthernet1/0/1 上的 MAC 认证统计信息。

```
<Sysname> reset mac-authentication statistics interface gigabitethernet 1/0/1
```

【相关命令】

- **display mac-authentication**

目 录

1 Portal	1-1
1.1 Portal配置命令	1-1
1.1.1 captive-bypass enable	1-1
1.1.2 default-logon-page	1-1
1.1.3 display portal	1-2
1.1.4 display portal packet statistics	1-5
1.1.5 display portal rule	1-7
1.1.6 display portal server	1-11
1.1.7 display portal user	1-12
1.1.8 display portal web-server	1-18
1.1.9 display web-redirect rule	1-20
1.1.10 if-match	1-21
1.1.11 ip (portal authentication server view)	1-23
1.1.12 ipv6	1-24
1.1.13 port (portal authentication server view)	1-25
1.1.14 portal { bas-ip bas-ipv6 } (interface view)	1-25
1.1.15 portal { ipv4-max-user ipv6-max-user } (interface view)	1-26
1.1.16 portal apply web-server (interface view)	1-27
1.1.17 portal authorization strict-checking	1-28
1.1.18 portal delete-user	1-29
1.1.19 portal device-id	1-30
1.1.20 portal domain (interface view)	1-30
1.1.21 portal enable (interface view)	1-31
1.1.22 portal fail-permit server	1-32
1.1.23 portal free-all except destination	1-33
1.1.24 portal free-rule	1-34
1.1.25 portal free-rule destination	1-35
1.1.26 portal free-rule source	1-36
1.1.27 portal ipv6 free-all except destination	1-37
1.1.28 portal ipv6 layer3 source	1-38
1.1.29 portal ipv6 user-detect	1-39
1.1.30 portal layer3 source	1-40
1.1.31 portal local-web-server	1-41

1.1.32 portal log enable	1-43
1.1.33 portal max-user	1-43
1.1.34 portal nas-id-profile.....	1-44
1.1.35 portal nas-port-id format	1-45
1.1.36 portal pre-auth ip-pool.....	1-47
1.1.37 portal refresh enable.....	1-48
1.1.38 portal roaming enable	1-49
1.1.39 portal server.....	1-50
1.1.40 portal user-detect.....	1-51
1.1.41 portal user-dhcp-only (interface view)	1-52
1.1.42 portal web-proxy port	1-53
1.1.43 portal web-server	1-54
1.1.44 reset portal packet statistics	1-54
1.1.45 server-detect (portal authentication server view)	1-55
1.1.46 server-detect (portal web server view)	1-56
1.1.47 server-register.....	1-57
1.1.48 server-type	1-57
1.1.49 tcp-port.....	1-58
1.1.50 url.....	1-59
1.1.51 url-parameter	1-60
1.1.52 user-sync	1-62
1.1.53 web-redirect url.....	1-63

1 Portal

1.1 Portal配置命令

1.1.1 captive-bypass enable

captive-bypass enable 命令用来开启 Portal 被动 Web 认证功能。

undo captive-bypass enable 命令用来关闭 Portal 被动 Web 认证功能。

【命令】

```
captive-bypass enable
undo captive-bypass enable
```

【缺省情况】

Portal 被动 Web 认证功能处于关闭状态，即 iOS 系统和部分 Android 系统的用户接入已开启 Portal 认证的网络后会自动弹出 Portal 认证页面。

【视图】

Portal Web 服务器视图

【缺省用户角色】

network-admin

【使用指导】

iOS 系统或者部分 Android 系统的用户接入已开启 Portal 认证的网络后，设备会主动向这类用户终端推送 Portal 认证页面。开启 Portal 被动 Web 认证功能后，仅在这类用户使用浏览器访问 Internet 时，设备才会为其推送 Portal 认证页面。

【举例】

```
# 开启 Portal 被动 Web 认证功能。
<Sysname> system-view
[Sysname] portal web-server wbs
[Sysname-portal-websvr-wbs] captive-bypass enable
```

【相关命令】

- **display portal web-server**

1.1.2 default-logon-page

default-logon-page 命令用来配置本地 Portal Web 服务提供的缺省认证页面文件。

undo default-logon-page 命令用来恢复缺省情况。

【命令】

```
default-logon-page file-name
undo default-logon-page
```

【缺省情况】

本地 Portal Web 服务提供的缺省认证页面文件为 defaultfile.zip。

【视图】

本地 Portal Web 服务视图

【缺省用户角色】

network-admin

【参数】

file-name: 表示缺省认证页面文件名（不包括文件的保存路径），为 1~91 个字符的字符串，包括字母、数字、点和下划线。

【使用指导】

配置 **default-logon-page** 命令后设备会将指定的压缩文件进行解压缩，并设置为本地 Portal Web 服务为用户进行 Portal 认证提供的缺省认证页面文件。

为了确保本地 Portal Web 服务功能的正常运行，建议使用设备存储介质根目录下自带的认证页面文件。如果用户需要自定义认证页面的内容和样式，请严格遵循自定义认证页面文件规范。

【举例】

配置本地 Portal Web 服务器提供的缺省认证页面文件为 pagefile1.zip。

```
<Sysname> system-view
[Sysname] portal local-web-server http
[Sysname-portal-local-websvr-http] default-logon-page pagefile1.zip
```

【相关命令】

- **portal local-web-server**

1.1.3 display portal

display portal 命令用来显示 Portal 配置信息和 Portal 运行状态信息。

【命令】

display portal interface *interface-type interface-number*

【视图】

任意视图

【缺省用户角色】

network-admin
network-operator

【参数】

interface *interface-type interface-number*: 表示接口类型和接口编号。

【举例】

显示接口 Vlan-interface2 的 Portal 配置信息和 Portal 运行状态信息。

```
<Sysname> display portal interface vlan-interface 2
Portal information of Vlan-interface2
```

```

NAS-ID profile: aaa
Authorization : Strict checking
ACL           : Enabled
User profile  : Disabled
IPv4:
  Portal status: Enabled
  Portal authentication method: Direct
  Portal web server: wbs
  Portal mac-trigger-server: Not configured
  Authentication domain: my-domain
  User-dhcp-only: Enabled
  Pre-auth IP pool: ab
  Max Portal users: Not configured
  Bas-ip: Not configured
  User detection: Type: ICMP Interval: 300s Attempts: 5 Idle time: 180s
  Action for server detection:
    Server type  Server name  Action
    Web server   wbs         fail-permit
    Portal server pts         fail-permit
  Layer3 source network:
    IP address      Mask
    1.1.1.1         255.255.0.0

  Destination authentication subnet:
    IP address      Mask
    2.2.2.2         255.255.255.0

IPv6:
  portal status: Disabled
  Portal authentication method: Disabled
  Portal web server: Not configured
  Portal mac-trigger-server: Not configured
  Authentication domain: Not configured
  User-dhcp-only: Disabled
  Pre-auth IP pool: Not configured
  Max Portal users: Not configured
  Bas-ipv6:Not configured
  User detection: Not configured
  Action for server detection:
    Server type  Server name  Action
    --           --           --
  Layer3 source network:
    IP address      Prefix length
    --             --
  Destination authentication subnet:
    IP address      Prefix length

```

表1-1 display portal interface 命令显示信息描述表

字段	描述
Portal information of interface	接口上的Portal信息
NAS-ID profile	接口上引用的NAS-ID profile
Authorization	服务器下发给Portal用户的授权信息类型，包括ACL和User profile
Strict checking	Portal授权信息的严格检查模式是否开启
IPv4	IPv4 Portal的相关信息
IPv6	IPv6 Portal的相关信息
Portal status	接口上Portal认证的运行状态，包括以下取值： <ul style="list-style-type: none"> Disabled: Portal 认证未开启 Enabled: Portal 认证已开启 Authorized: Portal 认证服务器或者 Portal Web 服务器不可达，端口自动开放
Portal authentication method	接口上配置的认证方式，包括以下取值： <ul style="list-style-type: none"> Direct: 直接认证方式 Redhcp: 二次地址分配认证方式 Layer3: 可跨三层认证方式
Portal Web server	接口上配置的Portal Web服务器的名称
Portal mac-trigger-server	（暂不支持）接口上配置MAC绑定服务器的名称
Authentication domain	接口上的Portal强制认证域
User-dhcp-only	仅允许通过DHCP方式获取IP地址的客户端上线功能 <ul style="list-style-type: none"> Enabled: 仅允许通过 DHCP 方式获取 IP 地址的客户端上线功能处于开启状态，表示仅允许通过 DHCP 方式获取 IP 地址的客户端上线 Disabled: 仅允许通过 DHCP 方式获取 IP 地址的客户端上线功能处于关闭状态，表示通过 DHCP 方式获取 IP 地址的客户端和静态配置 IP 地址的客户端都可以上线
Pre-auth ip-pool	为认证前的Portal用户指定的IP地址池名称
Max Portal users	接口上配置的最大用户数
Bas-ip	发送给Portal认证服务器的Portal报文的BAS-IP属性
Bas-ipv6	发送给Portal认证服务器的Portal报文的BAS-IPv6属性
User detection	接口上配置的用户在线状态探测配置，包括探测的方法（ARP、ICMP、ND、ICMPv6），探测周期和探测尝试次数，用户闲置的时间
Action for server detection	服务器可达性探测功能对应的端口控制配置： <ul style="list-style-type: none"> Server type: 服务器类型，包括 Portal server 和 Web server，分别表示 Portal 认证服务器和 Portal Web 服务器 Server name: 服务器名称 Action: 对应的接口根据服务器探测结果所采取的动作，为不需要认证（fail-permit）

字段	描述
Layer3 source subnet	Portal源认证网段信息
Destination authentication subnet	Portal目的认证网段认证信息
IP address	Portal认证网段的IP地址
Mask	Portal认证网段的子网掩码
Prefix length	Portal IPv6认证网段的地址前缀长度

【相关命令】

- `portal domain`
- `portal enable`
- `portal free-all except destination`
- `portal ipv6 free-all except destination`
- `portal ipv6 layer3 source`
- `portal layer3 source`
- `portal web-server`

1.1.4 display portal packet statistics

`display portal packet statistics` 命令用来显示 Portal 认证服务器的报文统计信息。

【命令】

`display portal packet statistics [server server-name]`

【视图】

任意视图

【缺省用户角色】

network-admin
network-operator

【参数】

server server-name: Portal 认证服务器的名称，为 1~32 个字符的字符串，区分大小写。

【使用指导】

执行此命令后，显示的报文统计信息包括设备接收到 Portal 认证服务器发送的报文以及设备发送给该 Portal 认证服务器的报文的信息。

若不指定参数 **server**，则依次显示所有 Portal 认证服务器的报文统计信息。

【举例】

显示名称为 pts 的 Portal 认证服务器的报文统计信息。

```
<Sysname> display portal packet statistics server pts
Portal server : pts
Invalid packets: 0
```

Pkt-Type	Total	Drops	Errors
REQ_CHALLENGE	3	0	0
ACK_CHALLENGE	3	0	0
REQ_AUTH	3	0	0
ACK_AUTH	3	0	0
REQ_LOGOUT	1	0	0
ACK_LOGOUT	1	0	0
AFF_ACK_AUTH	3	0	0
NTF_LOGOUT	1	0	0
REQ_INFO	6	0	0
ACK_INFO	6	0	0
NTF_USERDISCOVER	0	0	0
NTF_USERIPCHANGE	0	0	0
AFF_NTF_USERIPCHAN	0	0	0
ACK_NTF_LOGOUT	1	0	0
NTF_HEARTBEAT	0	0	0
NTF_USER_HEARTBEAT	2	0	0
ACK_NTF_USER_HEARTBEAT	0	0	0
NTF_CHALLENGE	0	0	0
NTF_USER_NOTIFY	0	0	0
AFF_NTF_USER_NOTIFY	0	0	0

表1-2 display portal server statistics 命令显示信息描述表

字段	描述
Portal server	Portal认证服务器名称
Invalid packets	无效报文的数目
Pkt-Type	报文的名称
Total	报文的总数
Drops	丢弃报文数
Errors	携带错误信息的报文数
REQ_CHALLENGE	Portal认证服务器向接入设备发送的challenge请求报文
ACK_CHALLENGE	接入设备对Portal认证服务器challenge请求的响应报文
REQ_AUTH	Portal认证服务器向接入设备发送的请求认证报文
ACK_AUTH	接入设备对Portal认证服务器认证请求的响应报文
REQ_LOGOUT	Portal认证服务器向接入设备发送的下线请求报文
ACK_LOGOUT	接入设备对Portal认证服务器下线请求的响应报文
AFF_ACK_AUTH	Portal认证服务器收到认证成功响应报文后向接入设备发送的确认报文
NTF_LOGOUT	接入设备发送给Portal认证服务器，用户被强制下线的通知报文
REQ_INFO	信息询问报文
ACK_INFO	信息询问的响应报文
NTF_USERDISCOVER	Portal认证服务器向接入设备发送的发现新用户要求上线的通知报文

字段	描述
NTF_USERIPCHANGE	接入设备向Portal认证服务器发送的通知更改某个用户IP地址的通知报文
AFF_NTF_USERIPCHAN	Portal认证服务器通知接入设备对用户表项的IP切换已成功报文
ACK_NTF_LOGOUT	Portal认证服务器对强制下线通知的响应报文
NTF_HEARTBEAT	Portal认证服务器周期性向接入设备发送的服务器心跳报文
NTF_USER_HEARTBEAT	接入设备收到的从Portal认证服务器发送的用户同步报文
ACK_NTF_USER_HEARTBEAT	接入设备向Portal认证服务器回应的用户同步响应报文
NTF_CHALLENGE	接入设备向Portal认证服务器发送的challenge请求报文
NTF_USER_NOTIFY	接入设备向Portal认证服务器发送的用户消息通知报文
AFF_NTF_USER_NOTIFY	Portal认证服务器向接入设备发送的对NTF_USER_NOTIFY的确认报文

【相关命令】

- `reset portal packet statistics`

1.1.5 display portal rule

`display portal rule` 命令用来显示用于报文匹配的 Portal 过滤规则信息。

【命令】

```
display portal rule { all | dynamic | static } interface interface-type
interface-number [ slot slot-number ]
```

【视图】

任意视图

【缺省用户角色】

network-admin
network-operator

【参数】

all: 显示所有 Portal 规则信息，包括动态 Portal 规则和静态 Portal 规则。

dynamic: 显示动态 Portal 规则信息，即用户通过 Portal 认证后设备上产生的 Portal 规则，这类规则定义了允许指定源 IP 地址的报文通过接口。

static: 显示静态 Portal 规则信息，即开启 Portal 后产生的 Portal 规则，这类规则定义了 Portal 功能开启后对接口上收到的报文的过滤动作。

interface interface-type interface-number: 显示指定接口的 Portal 规则信息。
interface-type interface-number 为接口类型和接口编号。

slot slot-number: 显示指定成员设备上的 Portal 规则信息。*slot-number* 表示设备在 IRF 中的成员编号。若不指定该参数，则表示所有成员设备上的 Portal 过滤规则信息。

【举例】

显示接口 Vlan-interface100 上所有 Portal 过滤规则的信息。

```

<Sysname> display portal rule all interface vlan-interface 100 slot 1
Slot 1:
IPv4 portal rules on Vlan-interface100:
Rule 1
  Type           : Static
  Action          : Permit
  Protocol        : Any
  Status          : Active
  Source:
    IP            : 0.0.0.0
    Mask          : 0.0.0.0
    Port          : Any
    MAC           : 0000-0000-0000
    Interface     : Vlan-interface100
    VLAN          : 100
  Destination:
    IP            : 192.168.0.111
    Mask          : 255.255.255.255
    Port          : Any

Rule 2
  Type           : Dynamic
  Action          : Permit
  Status          : Active
  Source:
    IP            : 2.2.2.2
    MAC           : 000d-88f8-0eab
    Interface     : Vlan-interface100
    VLAN          : 100
  Author ACL:
    Number        : 3001

Rule 3
  Type           : Static
  Action          : Redirect
  Status          : Active
  Source:
    IP            : 0.0.0.0
    Mask          : 0.0.0.0
    Interface     : Vlan-interface100
    VLAN          : 100
    Protocol      : TCP
  Destination:
    IP            : 0.0.0.0
    Mask          : 0.0.0.0
    Port          : 80

Rule 4:

```



```

Type           : Static
Action          : Deny
Status          : Active
Source:
  IP            : 0.0.0.0
  Mask          : 0.0.0.0
  Interface     : Vlan-interface100
  VLAN          : Any
Destination:
  IP            : 0.0.0.0
  Mask          : 0.0.0.0

```

IPv6 portal rules on Vlan-interface100:

Rule 1

```

Type           : Static
Action          : Permit
Protocol        : Any
Status          : Active
Source:
  IP            : ::
  Prefix length : 0
  Port          : Any
  MAC           : 0000-0000-0000
  Interface     : Vlan-interface100
  VLAN          : 100
Destination:
  IP            : 3000::1
  Prefix length : 64
  Port          : Any

```

Rule 2

```

Type           : Dynamic
Action          : Permit
Status          : Active
Source:
  IP            : 3000::1
  MAC           : 0015-e9a6-7cfe
  Interface     : Vlan-interface100
  VLAN          : 100
Author ACL:
  Number        : 3001

```

Rule 3

```

Type           : Static
Action          : Redirect
Status          : Active
Source:
  IP            : ::

```

```

    Prefix length    : 0
    Interface       : Vlan-interface100
    VLAN           : 100
    Protocol        : TCP
Destination:
    IP              : ::
    Prefix length   : 0
    Port            : 80

Rule 4:
    Type            : Static
    Action          : Deny
    Status          : Active
Source:
    IP              : ::
    Prefix length   : 0
    Interface       : Vlan-interface100
    VLAN           : 100
Destination:
    IP              : ::
    Prefix length   : 0
Author ACL:
    Number          : 3001

```

表1-3 display portal rule 命令显示信息描述表

字段	描述
Rule	Portal过滤规则编号。IPv4过滤规则和IPv6过滤规则分别编号
Type	Portal过滤规则的类型，包括以下取值： <ul style="list-style-type: none"> Static: 静态类型 Dynamic: 动态类型
Action	Portal过滤规则的匹配动作，包括以下取值： <ul style="list-style-type: none"> Permit: 允许报文通过 Redirect: 重定向报文 Deny: 拒绝报文通过
Protocol	Portal免认证规则中使用的传输层协议，包括以下取值： <ul style="list-style-type: none"> Any: 不限制传输层协议类型 TCP: TCP 传输类型 UDP: UDP 传输类型
Status	Portal过滤规则下发的状态，包括以下取值： <ul style="list-style-type: none"> Active: 表示规则已生效 Unactuated: 表示规则未生效
Source	Portal过滤规则的源信息
IP	源IP地址

字段	描述
Mask	源IPv4地址子网掩码
Prefix length	源IPv6地址前缀
Port	源传输层端口号
MAC	源MAC地址
Interface	Portal过滤规则应用的二层或三层接口
VLAN	源VLAN
Protocol	Portal重定向规则中使用的传输层协议类型，取值只能为TCP
Destination	Portal规则的目的信息
IP	目的IP地址
Port	目的传输层端口号
Mask	目的IPv4地址子网掩码
Prefix length	目的IPv6地址前缀
Author ACL	Portal用户认证后的授权ACL，即AAA授权给用户的ACL，该字段仅在Type为Dynamic时才显示
Number	授权ACL编号，N/A表示AAA未授权ACL

1.1.6 display portal server

display portal server 命令用来显示 Portal 认证服务器信息。

【命令】

display portal server [*server-name*]

【视图】

任意视图

【缺省用户角色】

network-admin
network-operator

【参数】

server-name: Portal 认证服务器的名称，为 1~32 个字符的字符串，区分大小写。

【使用指导】

若不指定参数 *server-name*，则显示所有 Portal 认证服务器信息。

【举例】

显示 Portal 认证服务器 pts 的信息。

```
<Sysname> display portal server pts
Portal server: pts
```

```

Type           : IMC
IP             : 192.168.0.111
VPN instance   : Not configured
Port          : 50100
Server detection : Timeout 60s Action: log
User synchronization : Timeout 200s
Status         : Up

```

表1-4 display portal server 命令显示信息描述表

字段	描述
Type	Portal认证服务器类型，其取值如下： <ul style="list-style-type: none"> CMCC：符合中国移动标准规范的服务器 iMC：符合 iMC 标准规范的服务器
Portal server	Portal认证服务器名称
IP	Portal认证服务器的IP地址
VPN instance	（暂不支持）Portal认证服务器所属的MPLS L3VPN实例
Port	Portal认证服务器的监听端口
Server detection	Portal认证服务器可达性探测功能的参数，包括超时时间（单位：秒），以及探测到服务器状态变化后触发的动作（log）
User synchronization	Portal用户用户信息同步功能的参数，包括超时时间（单位：秒）
Status	Portal认证服务器当前状态，其取值如下： <ul style="list-style-type: none"> Up：服务器可达性探测功能未开启，或服务器可达性探测功能开启且探测结果为该服务器当前可达 Down：服务器可达性探测功能已开启，探测结果为该服务器当前不可达

【相关命令】

- portal enable
- portal server
- server-detect (portal authentication server view)
- user-sync

1.1.7 display portal user

display portal user 命令用来显示 Portal 用户的信息。

【命令】

```
display portal user { all | interface interface-type interface-number | ip
ipv4-address | ipv6 ipv6-address } [ verbose ]
```

【视图】

任意视图

【缺省用户角色】

network-admin
network-operator

【参数】

all: 显示所有 Portal 用户的信息。

interface *interface-type interface-number*: 显示指定接口上的 Portal 用户信息。
interface-type interface-number 为接口类型和接口编号。

ip *ipv4-address*: 显示指定 IPv4 地址的 Portal 用户信息。

ipv6 *ipv6-address*: 显示指定 IPv6 地址的 Portal 用户信息。

verbose: 显示指定 Portal 用户的详细信息。

【举例】

显示所有 Portal 用户的信息。

```
<Sysname> display portal user all
```

```
Total portal users: 2
```

```
Username: abc
```

```
Portal server: pts
```

```
State: Online
```

```
VPN instance: N/A
```

MAC	IP	VLAN	Interface
000d-88f8-0eab	2.2.2.2	100	Vlan-interface100

```
Authorization information:
```

```
DHCP IP pool: N/A
```

```
User profile: abc (active)
```

```
Session group profile: N/A
```

```
ACL number: N/A
```

```
Inbound CAR: N/A
```

```
Outbound CAR: N/A
```

```
Username: def
```

```
Portal server: pts
```

```
State: Online
```

```
VPN instance: N/A
```

MAC	IP	VLAN	Interface
000d-88f8-0eac	3.3.3.3	200	Vlan-interface200

```
Authorization information:
```

```
DHCP IP pool: N/A
```

```
User profile: N/A
```

```
Session group profile: N/A
```

```
ACL number: 3001
```

```
Inbound CAR: N/A
```

```
Outbound CAR: N/A
```

表1-5 display portal user 命令显示信息描述表

字段	描述
Total portal users	总计的Portal用户数目
Username	用户名
Portal server	用户认证所使用的Portal认证服务器的名称
State	<p>Portal用户的当前状态，包括以下取值：</p> <ul style="list-style-type: none"> • Initialized: 初始化完成后的待认证状态 • Authenticating: 正在认证状态 • Waiting_SetRule: 等待下发用户授权信息 • Authorizing: 正在授权状态 • Online: 在线状态 • Waiting_Traffic: 等待获取用户最后一次流量 • Stop Accounting: 停止计费 • Done: 下线结束
VPN instance	（暂不支持）Portal用户所属的MPLS L3VPN实例。若用户属于公网，则显示为N/A
MAC	Portal用户的MAC地址
IP	Portal用户的IP地址
VLAN	Portal用户所在的VLAN
Interface	Portal用户接入的接口
Authorization information	Portal用户的授权信息
DHCP IP pool	Portal用户的授权地址池名称。若无授权地址池，则显示为N/A
User profile	<p>Portal用户的授权User Profile名称。若未授权User Profile，则显示为N/A。授权状态包括如下：</p> <ul style="list-style-type: none"> • active: AAA 授权 User profile 成功 • inactive: AAA 授权 User profile 失败或者设备上不存在该 User profile
Session group profile	<p>（暂不支持）Portal用户的授权Session Group Profile名称。若未授权Session Group Profile，则显示为N/A。授权状态包括如下：</p> <ul style="list-style-type: none"> • active: AAA 授权 Session group profile 成功 • inactive: AAA 授权 Session group profile 失败或者设备上不存在该 User profile
ACL number	<p>Portal用户的授权ACL编号。若未授权ACL，则显示为N/A。授权状态包括如下：</p> <ul style="list-style-type: none"> • active: AAA 授权 ACL 成功 • inactive: AAA 授权 ACL 失败或者设备上不存在该 ACL
Inbound CAR	（暂不支持）授权的入方向CAR（CIR：平均速率，单位为bps；PIR：峰值速率，单位为bps）。若未授权入方向CAR，则显示为N/A
Outbound CAR	（暂不支持）授权的出方向CAR（CIR：平均速率，单位为bps；PIR：峰值速率，单位为bps）。若未授权出方向CAR，则显示为N/A

显示 IP 地址为 50.50.50.3 的 Portal 用户的详细信息。

```
<Sysname> display portal user ip 50.50.50.3 verbose
```

Basic:

```
Current IP address: 50.50.50.3
Original IP address: 30.30.30.2
Username: user1@hrss
User ID: 0x28000002
Access interface: Vlan-interface20
Service-VLAN/Customer-VLAN: -/-
MAC address: 0000-0000-0001
Domain: hrss
VPN instance: N/A
Status: Online
Portal server: test
Portal authentication method: Direct
```

AAA:

```
Realtime accounting interval: 60s, retry times: 3
Idle cut: 180 sec, 10240 bytes, direction: Inbound
Session duration: 500 sec, remaining: 300 sec
Remaining traffic: 10240000 bytes
Login time: 2014-01-19 2:42:3 UTC
ITA policy name: N/A
DHCP IP pool: abc
```

ACL&QoS&Multicast:

```
Inbound CAR: N/A
Outbound CAR: N/A
ACL number: 3000 (inactive)
User profile: portal (active)
Session group profile: N/A
Max multicast addresses: 4
Multicast address list: 1.2.3.1, 1.34.33.1, 3.123.123.3, 4.5.6.7
                        2.2.2.2, 3.3.3.3, 4.4.4.4
User group: 1 (Id=1)
```

Flow statistic:

```
Uplink   packets/bytes: 7/546
Downlink packets/bytes: 0/0
```

ITA:

```
Accounting merge: Disabled
Traffic separate: Disabled
Quota-out offline: Disabled
```

level-2 Session duration: N/A, remaining: N/A

```
Remaining traffic: N/A
Traffic action: Permit
Inbound CAR: N/A
Outbound CAR: N/A
Uplink packets/bytes: 0/0
Downlink packets/bytes: 0/0
```

表1-6 display portal user verbose 命令显示信息描述表

字段	描述
Current IP address	Portal用户当前的IP地址
Original IP address	Portal用户认证时的IP地址
Username	Portal用户上线时使用的用户名
User ID	Portal用户ID
Access interface	Portal用户接入的接口
Service-VLAN/Customer-VLAN	Portal用户所在的公网VLAN/私网VLAN（“-”表示没有VLAN信息）
MAC address	用户的MAC地址
Domain	用户认证时使用的ISP域名
VPN instance	（暂不支持）用户所属的MPLS L3VPN实例，N/A表示用户属于公网
Status	Portal用户的当前状态，包括以下取值： <ul style="list-style-type: none"> • Authenticating: 正在认证状态 • Authorizing: 正在授权状态 • Waiting_SetRule: 正在下发 Portal 规则状态 • Online: 在线状态 • Waiting_Traffic: 正在等待用户流量状态 • Stop Accounting: 正在停止计费状态 • Done: 用户下线完成状态
Portal server	Portal服务器名称
Portal authentication method	接入接口上的Portal认证方式，包括如下取值： <ul style="list-style-type: none"> • Direct: 直接认证方式 • Redhcp: 二次地址分配认证方式 • Layer3: 可跨三层认证方式
AAA	Portal用户的AAA授权信息
Realtime accounting interval	授权的实时计费间隔和重传次数。若未授权，则显示为N/A
Idle cut	授权的闲置切断时长和流量。若未授权，则显示为N/A
direction	用户数据流量的统计方向，包括以下取值： <ul style="list-style-type: none"> • Both: 表示用户双向数据流量 • Inbound: 表示用户上行数据流量 • Outbound: 表示用户下行数据流量
Session duration	授权的会话时长以及剩余的会话时长。若未授权，则显示为N/A
Remaining traffic	授权的剩余流量。若未授权，则显示为N/A
Login time	用户登录时间，即用户授权成功的时间，格式为设备时间，如：2023-1-19 2:42:30 UTC
ITA policy name	（暂不支持）授权的ITA（Intelligent Target Accounting，智能靶向计费）策略名称

字段	描述
DHCP IP pool	授权的DHCP地址池名称。若未授权DHCP地址池，则显示为N/A
Inbound CAR	（暂不支持）授权的入方向CAR（CIR：平均速率，单位为bps；PIR：峰值速率，单位为bps）。若未授权入方向CAR，则显示为N/A。如果下发成功，显示为active，否则为inactive
Outbound CAR	（暂不支持）授权的出方向CAR（CIR：平均速率，单位为bps；PIR：峰值速率，单位为bps）。若未授权出方向CAR，则显示为N/A。如果下发成功，显示为active，否则为inactive
ACL number	授权的ACL编号。若未授权ACL，则显示为N/A。授权状态包括如下： <ul style="list-style-type: none"> active: AAA 授权 ACL 成功 inactive: AAA 授权 ACL 失败或者设备上不存在该 ACL
User profile	授权的User profile名称。若未授权User profile，则显示为N/A。授权状态包括如下： <ul style="list-style-type: none"> active: AAA 授权 User profile 成功 inactive: AAA 授权 User profile 失败或者设备上不存在该 User profile
Session group profile	（暂不支持）授权的Session group profile名称。若未授权Session group profile，则显示为N/A。授权状态包括如下： <ul style="list-style-type: none"> active: AAA 授权 Session group profile 成功 inactive: AAA 授权 Session group profile 失败或者设备上不存在该 User profile
Max multicast addresses	授权Portal用户可加入的组播组的最大数目
Multicast address list	授权Portal用户可加入的组播组列表。若未授权组播组列表，则显示为N/A
User group	Portal用户所属的用户组的名称。当用户组的ID取值为0xffffffff时无效。
Flow statistic	Portal用户流量统计信息
Uplink packets/bytes	上行流量报文数/字节数
Downlink packets/bytes	下行流量报文数/字节数
ITA	（暂不支持）Portal用户的ITA业务流量统计信息
Accounting merge	（暂不支持）统一计费功能的开启状态，包括以下取值： <ul style="list-style-type: none"> Enabled: 开启了统一计费功能，即系统将 ITA 业务策略下所有级别的流量进行合并，并以该 ITA 业务策略中配置的最低的流量计费级别上报给计费服务器 Disabled: 未开启统一计费功能，即系统将各个级别的流量分别上报给计费服务器
Traffic separate	（暂不支持）ITA业务流量与用户总计费流量分离功能的开启状态，包括以下取值： <ul style="list-style-type: none"> Enabled: 设备上报给计费服务器的用户总计费流量中不包含 ITA 流量 Disabled: 设备上报给计费服务器的用户主计费流量中包含 ITA 流量

字段	描述
Quota-out offline	<p>（暂不支持）ITA业务流量配额耗尽策略，包括以下取值：</p> <ul style="list-style-type: none"> • Enabled: 当用户的指定级别的流量配额耗尽后，用户不能访问授权的IP地址段 • Disabled: 当用户的指定级别的流量配额耗尽后，用户仍能访问授权的IP地址段
level-2 Session duration	（暂不支持）授权指定级别的ITA用户的总在线时长以及剩余的在线时长。若未授权，则显示为N/A
Remaining traffic	（暂不支持）授权ITA用户的剩余流量
Traffic action	<p>（暂不支持）ITA业务流量配额耗尽策略规则的匹配动作，包括以下取值：</p> <ul style="list-style-type: none"> • Permit: 当用户的指定级别的流量配额耗尽后，允许用户访问授权的IP地址段 • Deny: 当用户的指定级别的流量配额耗尽后，禁止用户访问授权的IP地址段
Inbound CAR	（暂不支持）授权ITA用户的入方向CAR（CIR：平均速率，单位为bps；PIR：峰值速率，单位为bps）。若未授权入方向CAR，则显示为N/A。如果下发成功，显示为active，否则为inactive
Outbound CAR	（暂不支持）授权ITA用户的出方向CAR（CIR：平均速率，单位为bps；PIR：峰值速率，单位为bps）。若未授权出方向CAR，则显示为N/A。如果下发成功，显示为active，否则为inactive
Uplink packets/bytes	（暂不支持）ITA用户上行流量报文数/字节数
Downlink packets/bytes	（暂不支持）ITA用户下行流量报文数/字节数

【相关命令】

- `portal enable`

1.1.8 display portal web-server

`display portal web-server` 命令用来显示 Portal Web 服务器信息。

【命令】

`display portal web-server [server-name]`

【视图】

任意视图

【缺省用户角色】

network-admin
network-operator

【参数】

server-name: Portal Web 服务器的名称，为 1~32 个字符的字符串，区分大小写。

【使用指导】

若不指定参数 *server-name*，则显示所有 Portal Web 服务器信息。

【举例】

显示 Portal Web 服务器 wbs 的信息。

```
<Sysname> display portal web-server wbs
```

Portal Web server: wbs

```
Type                : IMC
URL                  : http://www.test.com/portal
URL parameters       : userurl=http://www.test.com/welcome
                      userip=source-address
VPN instance         : Not configured
Server detection     : Interval: 120s  Attempts: 5  Action: log
IPv4 status          : Up
IPv6 status          : Up
Captive-bypass       : Disabled
If-match             : original-url http://2.2.2.2 redirect-url http://192.168.56.2
```

表1-7 display portal web-server 命令显示信息描述表

字段	描述
Type	Portal Web服务器类型，其取值如下： <ul style="list-style-type: none">CMCC：符合中国移动标准规范的服务器iMC：符合 iMC 标准规范的服务器
Portal Web server	Portal Web服务器名称
URL	Portal Web服务器的URL地址以及携带的参数
URL parameters	Portal Web服务器的URL携带的参数信息
VPN instance	（暂不支持）Portal Web服务器所属的MPLS L3VPN实例名称
Server detection	Portal Web服务器可达性探测功能的参数，包括探测间隔时间（单位：秒），探测尝试次数以及探测到服务器状态变化后的动作（log）
IPv4 status	IPv4 Portal Web服务器当前状态，其取值如下： <ul style="list-style-type: none">Up：服务器可达性探测功能未开启，或服务器可达性探测功能开启且探测结果为该服务器当前可达Down：服务器可达性探测功能已开启，且探测结果为该服务器当前不可达
IPv6 status	IPv6 Portal Web服务器当前状态，其取值如下： <ul style="list-style-type: none">Up：服务器可达性探测功能未开启，或服务器可达性探测功能开启且探测结果为该服务器当前可达Down：服务器可达性探测功能已开启，且探测结果为该服务器当前不可达
Captive-bypass	Portal被动Web认证功能状态，其取值如下： <ul style="list-style-type: none">Disabled：未开启Enabled：已开启
If-match	配置的URL重定向匹配规则，未配置时，显示Not configured

【相关命令】

- portal enable

- **portal web-server**
- **server-detect** (portal web-server view)

1.1.9 display web-redirect rule

display web-redirect rule 命令用来显示指定接口上的 Web 重定向过滤规则信息。

【命令】

```
display web-redirect rule interface interface-type interface-number [ slot
slot-number ]
```

【视图】

任意视图

【缺省用户角色】

```
network-admin
network-operator
```

【参数】

interface *interface-type interface-number*: 显示指定接口的 Web 重定向过滤规则信息。*interface-type interface-number* 为接口类型和接口编号。

slot *slot-number*: 显示指定成员设备上指定接口的 Web 重定向过滤规则信息。*slot-number* 表示设备在 IRF 中的成员编号。若不指定该参数, 则显示主用设备上的 Web 重定向过滤规则信息。

【举例】

显示接口 Vlan-interface100 上的所有 Web 重定向过滤规则。

```
<Sysname> display web-redirect rule interface vlan-interface 100
IPv4 web-redirect rules on vlan-interface 100:
```

Rule 1:

```
Type           : Dynamic
Action          : Permit
Status          : Active
Source:
  IP             : 192.168.2.114
  VLAN           : Any
```

Rule 2:

```
Type           : Static
Action          : Redirect
Status          : Active
Source:
  VLAN           : Any
  Protocol       : TCP
Destination:
  Port           : 80
```

```
IPv6 web-redirect rules on vlan-interface 100:
```

Rule 1:

```

Type           : Static
Action         : Redirect
Status         : Active
Source:
    VLAN       : Any
    Protocol    : TCP
Destination:
    Port       : 80

```

表1-8 display web-redirect rule 命令显示信息描述表

字段	描述
Rule	Web重定向规则编号
Type	Web重定向规则的类型，包括以下取值： <ul style="list-style-type: none"> Static: 静态类型。该类型的规则在 Web 重定向功能生效时生成 Dynamic: 动态类型。该类型的规则在用户访问重定向页面时生成
Action	Web重定向规则的匹配动作，包括以下取值： <ul style="list-style-type: none"> Permit: 允许报文通过 Redirect: 重定向报文
Status	Web重定向规则下发的状态，包括以下取值： <ul style="list-style-type: none"> Active: 表示规则已生效 Inactive: 表示规则未生效
Source	Web重定向规则的源信息
IP	源IP地址
Mask	源IPv4地址子网掩码
Prefix length	源IPv6地址前缀
VLAN	源VLAN，如果未指定，显示为Any
Protocol	Web重定向规则中使用的传输层协议类型，取值只能为TCP
Destination	Web重定向规则的目的信息
Port	目的传输层端口号，默认为80

1.1.10 if-match

if-match 命令用来配置重定向 URL 的匹配规则。

undo if-match 命令用来删除配置的重定向 URL 匹配规则。

【命令】

```

if-match { original-url url-string redirect-url url-string
[ url-param-encryption { aes | des } key { cipher | simple } string ] |
user-agent string redirect-url url-string }
undo if-match { original-url url-string | user-agent user-agent }

```

【缺省情况】

不存在重定向 URL 的匹配规则。

【视图】

Portal Web 服务器视图

【缺省用户角色】

network-admin

【参数】

original-url url-string: 根据用户 Web 访问请求的 URL 地址进行匹配, 其中 *url-string* 是用户 Web 访问请求的 URL 地址, 为 1~256 个字符的字符串, 区分大小写。该 URL 地址必须是以 `http://` 或者 `https://` 开头的完整 URL 路径。

redirect-url url-string: Web 访问请求被重定向后的地址, 为 1~256 个字符的字符串, 区分大小写。该 URL 地址必须是以 `http://` 或者 `https://` 开头的完整 URL 路径。

url-param-encryption: 对设备重定向给用户的 Portal Web 服务器 URL 中携带的所有参数信息进行加密。如果未指定本参数, 则表示不对携带的所有参数信息进行加密。

aes: 加密算法为 AES 算法。

des: 加密算法为 DES 算法。

key: 设置密钥。

cipher: 以密文方式设置密钥。

simple: 以明文方式设置密钥, 该密钥将以密文形式存储。

string: 密钥字符串, 区分大小写。密钥的长度范围和选择的加密方式有关。具体关系如下:

- 对于 **des** 加密方式, 明文密钥为 8 个字符的字符串, 密文密钥为 41 个字符的字符串。
- 对于 **aes** 加密方式, 明文密钥为 1~31 个字符的字符串, 密文密钥为 1~73 个字符的字符串。

user-agent user-agent: 根据用户 HTTP/HTTPS 请求报文中的 User Agent 信息进行匹配, 其中 *user-agent* 是 HTTP User Agent 信息内容, 为 1~255 个字符的字符串, 区分大小写。HTTP User Agent 信息包括硬件厂商信息、软件操作系统信息、浏览器信息、搜索引擎信息等内容。

【使用指导】

重定向 URL 匹配规则用于控制重定向用户的 HTTP 或 HTTPS 请求, 该匹配规则可匹配用户的 Web 请求地址或者用户的终端信息。为了让用户能够成功访问重定向后的地址, 需要通过 **portal free-rule** 命令配置免认证规则, 放行去往该地址的 HTTP 或 HTTPS 请求报文。与 **url** 命令不同的是, 重定向匹配规则可以灵活的进行地址的重定向, 而 **url** 命令一般只用于将用户的 HTTP 或 HTTPS 请求重定向到 Portal Web 服务器进行 Portal 认证。在二者同时存在时, **if-match** 命令优先进行地址的重定向。

【举例】

配置 URL 地址为 `http://www.abc.com.cn` 的匹配规则, 访问此地址的报文被重定向到 `http://192.168.0.1`, 对重定向 URL 中携带的参数进行加密。

```
<Sysname> system-view
[Sysname] portal web-server wbs
[Sysname-portal-websvr-wbs] if-match original-url http://www.abc.com.cn redirect-url
http://192.168.0.1 url-param-encryption des key simple 12345678
```

配置用户代理信息为
5.0(WindowsNT6.1)AppleWebKit/537.36(KHTML,likeGecko)Chrome/36.0.1985.125Safari/537.36
的匹配规则，访问此地址的报文被重定向到 http://192.168.0.1。

```
<Sysname> system-view
[Sysname] portal web-server wbs
[Sysname-portal-websvr-wbs] if-match user-agent
5.0(WindowsNT6.1)AppleWebKit/537.36(KHTML,likeGecko)Chrome/36.0.1985.125Safari/537.36
redirect-url http://192.168.0.1
```

【相关命令】

- **display portal web-server**
- **portal free-rule**
- **url**
- **url-parameter**

1.1.11 ip (portal authentication server view)

ip 命令用来指定 Portal 认证服务器的 IPv4 地址。

undo ip 命令用来恢复缺省情况。

【命令】

```
ip ipv4-address [ key { cipher | simple } string ]
undo ip
```

【缺省情况】

未指定 Portal 认证服务器的 IPv4 地址。

【视图】

Portal 认证服务器视图

【缺省用户角色】

network-admin

【参数】

ipv4-address: Portal 认证服务器的 IPv4 地址。

key: 与 Portal 认证服务器通信时使用的共享密钥。设备与 Portal 认证服务器交互的 Portal 报文中会携带一个在该共享密钥参与下生成的验证字，该验证字用于接受方校验收到的 Portal 报文的正确性。

cipher: 以密文方式设置密钥。

simple: 以明文方式设置密钥，该密钥将以密文形式存储。

string: 密码字符串，区分大小写。明文密钥为 1~64 个字符的字符串，密文密钥为 1~117 个字符的字符串。

【使用指导】

一个 Portal 认证服务器对应一个 IPv4 地址，因此一个 Portal 认证服务器视图下只允许存在一个 IPv4 地址。多次执行本命令，最后一次执行的命令生效。

不同的 Portal 认证服务器不允许 IPv4 地址的配置相同。

【举例】

指定 Portal 认证服务器 pts 的 IPv4 地址为 192.168.0.111、共享密钥为明文 portal。

```
<Sysname> system-view
[Sysname] portal server pts
[Sysname-portal-server-pts] ip 192.168.0.111 key simple portal
```

【相关命令】

- **portal server**
- **display portal server**

1.1.12 ipv6

ipv6 命令用来指定 Portal 认证服务器的 IPv6 地址。

undo ipv6 命令用来恢复缺省情况。

【命令】

```
ipv6 ipv6-address [ key { cipher | simple } string ]
undo ipv6
```

【缺省情况】

未指定 Portal 认证服务器的 IPv6 地址。

【视图】

Portal 认证服务器视图

【缺省用户角色】

network-admin

【参数】

ipv6-address: Portal 认证服务器的 IPv6 地址。

key: 与 Portal 认证服务器通信需要的共享密钥。设备与 Portal 认证服务器交互的 Portal 报文中会携带一个在该共享密钥参与下生成的验证字,该验证字用于接受方校验收到的 Portal 报文的正确性。

cipher: 以密文方式设置密钥。

simple: 以明文方式设置密钥,该密钥将以密文形式存储。

string: 密码字符串,区分大小写。明文密钥为 1~64 个字符的字符串,密文密钥为 1~117 个字符的字符串。

【使用指导】

一个 Portal 认证服务器对应一个 IPv6 地址,因此一个 Portal 认证服务器视图下只允许存在一个 IPv6 地址。多次执行本命令,最后一次执行的命令生效。

不同的 Portal 认证服务器不允许 IPv6 地址的配置相同。

【举例】

指定 Portal 认证服务器 pts 的 IPv6 地址为 2000::1、共享密钥为明文 portal。

```
<Sysname> system-view
```



```
[Sysname] portal server pts
[Sysname-portal-server-pts] ipv6 2000::1 key simple portal
```

【相关命令】

- **display portal server**
- **portal server**

1.1.13 port (portal authentication server view)

port 命令用来配置设备主动向 Portal 认证服务器发送 Portal 报文时使用的 UDP 端口号。

undo port 命令用来恢复缺省情况。

【命令】

```
port port-number
undo port
```

【缺省情况】

设备主动发送 Portal 报文时使用的 UDP 端口号为 50100。

【视图】

Portal 认证服务器视图

【缺省用户角色】

network-admin

【参数】

port-number: 设备向 Portal 认证服务器主动发送 Portal 报文时使用的目的 UDP 端口号，取值范围为 1~65534。

【使用指导】

本命令配置的端口号要和 Portal 认证服务器上配置的监听 Portal 报文的端口号保持一致。

【举例】

配置设备向 Portal 认证服务器 pts 主动发送 Portal 报文时使用的目的 UDP 端口号为 50000。

```
<Sysname> system-view
[Sysname] portal server pts
[Sysname-portal-server-pts] port 50000
```

【相关命令】

- **portal server**

1.1.14 portal { bas-ip | bas-ipv6 } (interface view)

portal { bas-ip | bas-ipv6 } 命令用来设置发送给 Portal 认证服务器的 Portal 报文中的 BAS-IP 或 BAS-IPv6 属性。

undo portal { bas-ip | bas-ipv6 } 命令用来恢复缺省情况。

【命令】

```
portal { bas-ip ipv4-address | bas-ipv6 ipv6-address }
```

```
undo portal { bas-ip | bas-ipv6 }
```

【缺省情况】

对于响应类报文 IPv4 Portal 报文中的 BAS-IP 属性为报文的源 IPv4 地址，IPv6 Portal 报文中的 BAS-IPv6 属性为报文源 IPv6 地址。

对于通知类报文 IPv4 Portal 报文中的 BAS-IP 属性为出接口的 IPv4 地址，IPv6 Portal 报文中的 BAS-IPv6 属性为出接口的 IPv6 地址。

【视图】

接口视图

【缺省用户角色】

network-admin

【参数】

ipv4-address: 接口发送 Portal 报文的 BAS-IP 属性值，应该为本机的地址，不能为全 0 地址、全 1 地址、D 类地址、E 类地址和环回地址。

ipv6-address: 接口发送 Portal 报文的 BAS-IPv6 属性值，应该为本机的地址，不能为多播地址、全 0 地址、本地链路地址。

【使用指导】

设备上运行 Portal 协议 2.0 版本时，主动发送给 Portal 认证服务器的报文（例如强制用户下线报文）中必须携带 BAS-IP 属性。设备上运行 Portal 协议 3.0 版本时，主动发送给 Portal 认证服务器必须携带 BAS-IP 或者 BAS-IPv6 属性。

配置此命令后，设备主动发送的通知类 Portal 报文，其源 IP 地址为配置的 BAS-IP，否则为 Portal 报文出接口 IP 地址。

接口上开启了二次地址分配认证方式的 Portal 认证时，如果 Portal 认证服务器上指定的设备 IP 不是 Portal 报文出接口 IP 地址，则必须通过本命令配置相应的 BAS-IP 或 BAS-IPv6 属性，使其值与 Portal 认证服务器上指定的设备 IP 一致，否则 Portal 用户无法认证成功。

使用 H3C iMC 的 Portal 认证服务器的情况下，如果 Portal 服务器上指定的设备 IP 不是设备上 Portal 报文出接口的 IP 地址，则开启了 Portal 认证的接口上必须配置 BAS-IP 或者 BAS-IPv6 属性。

【举例】

配置接口 Vlan-interface100 发送 Portal 报文的 BAS-IP 属性值为 2.2.2.2。

```
<Sysname> system-view
[Sysname] interface vlan-interface 100
[Sysname-Vlan-interface100] portal bas-ip 2.2.2.2
```

【相关命令】

- **display portal**

1.1.15 portal { ipv4-max-user | ipv6-max-user } (interface view)

portal { ipv4-max-user | ipv6-max-user } 命令用来配置接口上的 Portal 最大用户数。

undo portal { ipv4-max-user | ipv6-max-user } 命令用来恢复缺省情况。

【命令】

```
portal { ipv4-max-user | ipv6-max-user } max-number  
undo portal { ipv4-max-user | ipv6-max-user }
```

【缺省情况】

接口上的 Portal 最大用户数不受限制。

【视图】

接口视图

【缺省用户角色】

network-admin

【参数】

max-number: 接口上允许的最大 IPv4 或 IPv6 Portal 用户数，取值范围为 1~4294967295。

【使用指导】

如果接口上配置的 Portal 最大用户数小于当前接口上已经在线的 Portal 用户数，则该配置可以执行成功，且在线 Portal 用户不受影响，但系统将不允许新的 Portal 用户从该接口接入。

【举例】

在接口 Vlan-interface100 上配置 IPv4 Portal 最大用户数为 100。

```
<Sysname> system-view  
[Sysname] interface vlan-interface 100  
[Sysname-Vlan-interface100] portal ipv4-max-user 100
```

【相关命令】

- **display portal**
- **portal max-user**

1.1.16 portal apply web-server (interface view)

portal [ipv6] apply web-server 命令用来引用 Portal Web 服务器，设备会将 Portal 用户的 HTTP 请求报文重定向到该 Web 服务器。

undo portal [ipv6] apply web-server 命令用来取消恢复缺省情况。

【命令】

```
portal [ ipv6 ] apply web-server server-name [ fail-permit ]  
undo portal [ ipv6 ] apply web-server
```

【缺省情况】

未引用 Portal Web 服务器。

【视图】

接口视图

【缺省用户角色】

network-admin

【参数】

ipv6: 表示 IPv6 Portal Web 服务器。若不指定该参数，则表示 IPv4 Portal Web 服务器。

server-name: 被引用的 Portal Web 服务器的名称，为 1~32 个字符的字符串，区分大小写，且必须已经存在。

fail-permit: 开启 Portal Web 服务器不可达时的 Portal 用户逃生功能，即设备检测到 Portal Web 服务器不可达时取消接口上的 Portal 认证功能，允许用户不经过 Portal 认证即可自由访问网络。

【使用指导】

一个接口上可以同时开启 IPv4 Portal 认证和 IPv6 Portal 认证，因此也可以同时引用一个 IPv4 Portal Web 服务器和一个 IPv6 Portal Web 认证服务器。

如果接口上同时开启了 Portal 认证服务器逃生功能和 Portal Web 服务器逃生功能，则当任意一个服务器不可达时，即取消接口 Portal 认证功能，当两个服务器均恢复正常通信后，再重新启动 Portal 认证功能。

【举例】

在接口 Vlan-interface100 上引用名称为 wbs 的 Portal Web 服务器作为用户认证时使用的 Web 服务器。

```
<Sysname> system-view
[Sysname] interface vlan-interface 100
[Sysname-Vlan-interface100] portal apply web-server wbs
```

【相关命令】

- **display portal**
- **portal fail-permit server**
- **portal web-server**

1.1.17 portal authorization strict-checking

portal authorization strict-checking 命令用来开启 Portal 授权信息的严格检查模式。

undo portal authorization strict-checking 命令用来关闭 Portal 授权信息的严格检查模式。

【命令】

```
portal authorization { acl | user-profile } strict-checking
undo portal authorization { acl | user-profile } strict-checking
```

【缺省情况】

缺省为非严格检查授权信息模式，当服务器下发的授权 ACL、User Profile 在设备上不存在或者设备下发 User Profile 失败时，用户保持在线。

【视图】

接口视图

【缺省用户角色】

network-admin

【参数】

acl: 表示开启对授权 ACL 的严格检查。

user-profile: 表示开启对授权 User Profile 的严格检查。

【使用指导】

接口上开启 Portal 授权信息的严格检查模式后，当服务器给用户下发的授权 ACL、User Profile 在设备上不存在或者设备下发 User Profile 失败时，设备将强制该用户下线。

可同时开启对授权 ACL 和授权 User Profile 的严格检查模式。若同时开启了对授权 ACL 和对授权 User Profile 的严格检查模式，则只要其中任意一个授权属性未通过严格授权检查，则用户就会下线。

【举例】

在接口 Vlan-interface100 上开启对授权 ACL 的严格检查模式。

```
<Sysname> system-view
[Sysname] interface vlan-interface 100
[Sysname-Vlan-interface100] portal authorization acl strict-checking
```

【相关命令】

- **display portal**

1.1.18 portal delete-user

portal delete-user 命令用来强制在线 Portal 用户下线。

【命令】

```
portal delete-user { ipv4-address | all | interface interface-type
interface-number | ipv6 ipv6-address }
```

【视图】

系统视图

【缺省用户角色】

network-admin

【参数】

ipv4-address: 在线 Portal 用户的 IPv4 地址。

all: 所有接口下的在线 IPv4 Portal 用户和 IPv6 Portal 用户。

interface interface-type interface-number: 指定接口下的所有在线 Portal 用户，包括 IPv4 Portal 用户和 IPv6 Portal 用户。*interface-type interface-number* 为接口类型和接口编号。

ipv6 ipv6-address: 指定在线 IPv6 Portal 用户的地址。

【举例】

强制 IP 地址为 1.1.1.1 的在线 Portal 用户下线。

```
<Sysname> system-view
[Sysname] portal delete-user 1.1.1.1
```

【相关命令】

- `display portal user`

1.1.19 portal device-id

`portal device-id` 命令用来配置设备 ID。

`undo portal device-id` 命令用来恢复缺省情况。

【命令】

`portal device-id device-id`

`undo portal device-id`

【缺省情况】

未配置任何设备 ID。

【视图】

系统视图

【缺省用户角色】

network-admin

【参数】

device-id: 设备 ID，为 1~63 个字符的字符串，区分大小写。

【使用指导】

通过配置设备 ID，使得设备向 Portal 服务器发送的协议报文中携带一个属性，此属性用于向 Portal 服务器标识发送协议报文的接入设备。

不同设备的设备 ID 不能相同。

【举例】

配置设备的 ID 名为 0002.0010.100.00。

```
<Sysname> system-view
```

```
[Sysname] portal device-id 0002.0010.100.00
```

1.1.20 portal domain (interface view)

`portal [ipv6] domain` 命令用于指定 Portal 用户使用的认证域，使得所有从该接口接入的 Portal 用户强制使用该认证域。

`undo portal [ipv6] domain` 命令用来删除 Portal 用户使用的认证域。

【命令】

`portal [ipv6] domain domain-name`

`undo portal [ipv6] domain`

【缺省情况】

未指定 Portal 用户使用的认证域。

【视图】

接口视图

【缺省用户角色】

network-admin

【参数】

ipv6: 指定 IPv6 Portal 用户使用的认证域。若不指定本参数，则表示指定 IPv4 Portal 用户使用的认证域。

domain-name: ISP 认证域名，为 1~255 个字符的字符串，不区分大小写。

【使用指导】

接口上可以同时指定 IPv4 Portal 用户和 IPv6 Portal 用户的认证域。

如果不指定 **ipv6** 参数，则表示配置或者删除 IPv4 Portal 用户使用的认证域。

【举例】

指定从接口 Vlan-interface100 上接入的 IPv4 Portal 用户使用认证域为 my-domain。

```
<Sysname> system-view
[Sysname] interface vlan-interface 100
[Sysname-Vlan-interface100] portal domain my-domain
```

【相关命令】

- **display portal**

1.1.21 portal enable (interface view)

portal [ipv6] enable 命令用来开启 Portal 认证功能，并指定认证方式。

undo portal [ipv6] enable 命令用来关闭 Portal 认证功能。

【命令】

```
portal enable method { direct | layer3 | redhcp }
portal ipv6 enable method { direct | layer3 }
undo portal [ ipv6 ] enable
```

【缺省情况】

Portal 认证功能处于关闭状态。

【视图】

接口视图

【缺省用户角色】

network-admin

【参数】

ipv6: 表示 IPv6 Portal 认证。若不指定该参数，则表示 IPv4 Portal 认证。

method: 认证方式。

- **direct**: 直接认证方式。

- **layer3**: 可跨三层认证方式。
- **redhcp**: 二次地址分配认证方式。

【使用指导】

不能通过重复执行本命令来修改 Portal 认证方式。如需修改 Portal 的认证方式，请先通过 **undo portal [ipv6] enable** 命令取消 Portal 认证功能，再执行 **portal [ipv6] enable** 命令。

开启 IPv6 Portal 认证功能之前，需要保证设备支持 IPv6 ACL 和 IPv6 转发功能。

IPv6 Portal 认证不支持二次地址分配方式。

允许在接口上同时开启 IPv4 Portal 认证和 IPv6 Portal 认证功能。

【举例】

在接口 Vlan-interface100 上开启 IPv4 Portal 认证，且指定为直接认证方式。

```
<Sysname> system-view
[Sysname] interface vlan-interface 100
[Sysname-Vlan-interface100] portal enable method direct
```

【相关命令】

- **display portal**

1.1.22 portal fail-permit server

portal [ipv6] fail-permit server 命令用来开启 Portal 认证服务器不可达时的 Portal 用户逃生功能。

undo portal [ipv6] fail-permit server 命令用来关闭 Portal 认证服务器不可达时的 Portal 用户逃生功能。

【命令】

```
portal [ ipv6 ] fail-permit server server-name
undo portal [ ipv6 ] fail-permit server
```

【缺省情况】

Portal 认证服务器不可达时的 Portal 用户逃生功能处于关闭状态。

【视图】

接口视图

【缺省用户角色】

network-admin

【参数】

ipv6: 表示 IPv6 Portal 认证服务器。若不指定该参数，则表示 IPv4 Portal 认证服务器。

server-name: Portal 认证服务器名称，为 1~32 个字符的字符串，区分大小写。

【使用指导】

如果接口上同时开启了 Portal 认证服务器不可达时的 Portal 用户逃生功能和 Portal Web 服务器不可达时的 Portal 用户逃生功能，则当任意一个服务器不可达时，立即放开接口控制，允许用户不经过 Portal 认证即可自由访问网络；当两个服务器均恢复可达后，再重新启动接口的 Portal 认证功能。

重新启动接口的 Portal 认证功能之后，未通过认证的用户需要通过认证之后才能访问网络资源，已通过认证的用户可继续访问网络资源。

一个接口上，最多同时可以开启一个 Portal 认证服务器不可达时的 Portal 用户逃生功能和一个 Portal Web 服务器不可达时的 Portal 用户逃生功能。

多次执行本命令，最后一次执行的命令生效。

【举例】

在接口 Vlan-interface100 上启用 Portal 认证服务器 pts1 不可达时的 Portal 用户逃生功能。

```
<Sysname> system-view
[Sysname] interface vlan-interface 100
[Sysname-Vlan-interface100] portal fail-permit server pts1
```

【相关命令】

- **display portal**

1.1.23 portal free-all except destination

portal free-all except destination 命令用来配置 IPv4 Portal 目的认证网段。

undo portal free-all except destination 命令用来删除 IPv4 Portal 目的认证网段。

【命令】

```
portal free-all except destination ipv4-network-address { mask-length | mask }
undo portal free-all except destination [ ipv4-network-address ]
```

【缺省情况】

未配置 IPv4 Portal 目的网段认证，表示对访问任意目的网段的用户都进行 Portal 认证。

【视图】

接口视图

【缺省用户角色】

network-admin

【参数】

ipv4-network-address: IPv4 Portal 认证网段地址。

mask-length: 子网掩码长度，取值范围为 0~32。

mask: 子网掩码，点分十进制格式。

【使用指导】

接口上仅要求 Portal 用户访问指定目的认证网段（除免认证规则中指定的目的 IP 地址或网段）时才需要进行 Portal 认证，访问其它网段访问时不需要进行 Portal 认证。

可以通过多次执行本命令，配置多条目的认证网段。

如果 **undo** 命令中不携带 IP 地址参数，则表示删除所有的 IPv4 Portal 目的认证网段。

目的网段认证对二次地址分配认证方式的 Portal 认证不生效。

如果接口上同时配置了源认证网段和目的认证网段，则源认证网段配置不会生效。

【举例】

在接口 Vlan-interface2 上配置 IPv4 Portal 目的认证网段为 11.11.11.0/24，仅允许访问 11.11.11.0/24 网段的用户触发 Portal 认证，其它目的网段可以直接访问。

```
<Sysname> system-view
[Sysname] interface vlan-interface 2
[Sysname-Vlan-interface2] portal free-all except destination 11.11.11.0 24
```

【相关命令】

- **display portal**

1.1.24 portal free-rule

portal free-rule 命令用来配置基于 IP 地址的 Portal 免认证规则。

undo portal free-rule 命令用来删除指定的或所有 Portal 免认证规则。

【命令】

```
portal free-rule rule-number { destination ip { ipv4-address { mask-length | mask } | any } [ tcp tcp-port-number | udp udp-port-number ] | source ip { ipv4-address { mask-length | mask } | any } [ tcp tcp-port-number | udp udp-port-number ] } * [ interface interface-type interface-number ]
portal free-rule rule-number { destination ipv6 { ipv6-address prefix-length | any } [ tcp tcp-port-number | udp udp-port-number ] | source ipv6 { ipv6-address prefix-length | any } [ tcp tcp-port-number | udp udp-port-number ] } * [ interface interface-type interface-number ]
undo portal free-rule { rule-number | all }
```

【缺省情况】

不存在基于 IP 地址的 Portal 免认证规则。

【视图】

系统视图

【缺省用户角色】

network-admin

【参数】

rule-number: 免认证规则编号。取值范围为 0~4294967295。

destination: 指定目的信息。

source: 指定源信息。

ip ipv4-address: 免认证规则的 IPv4 地址。

{ **mask-length** | **mask** }: 免认证规则的 IP 地址掩码。其中，**mask-length** 为子网掩码长度，取值范围为 0~32；**mask** 为子网掩码，点分十进制格式。

ipv6 ipv6-address: 免认证规则的 IPv6 地址。

prefix-length: 免认证规则的 IPv6 地址前缀长度，取值范围为 0~128。

ip any: 任意 IPv4 地址。

ipv6 any: 任意 IPv6 地址。

tcp tcp-port-number: 免认证规则的 TCP 端口号，取值范围为 0~65535。

udp udp-port-number: 免认证规则的 UDP 端口号，取值范围为 0~65535。

all: 所有免认证规则。

interface interface-type interface-number: 免认证规则生效的三层接口。

【使用指导】

可以同时指定源和目的参数，或者仅指定其中一个参数，后者表示另外一个地址不受限制。

如果免认证规则中同时配置了源端口号和目的端口号，则要求源和目的端口号所属的传输层协议类型保持一致。

未指定三层接口的情况下，免认证规则对所有开启 Portal 的接口生效；指定三层接口的情况下，免认证规则只对指定的三层接口生效。

相同内容的免认证规则不能重复配置，否则提示免认证规则已存在或重复。

【举例】

配置一条基于 IPv4 地址的 Portal 免认证规则：编号为 1、源地址为 10.10.10.1/24、目的地址为 20.20.20.1、目的 TCP 端口号为 23、生效接口为 Vlan-interface1。该规则表示在 Vlan-interface1 接口上，10.10.10.1/24 网段地址的用户不需要经过 Portal 认证即可以访问地址为 20.20.20.1 的主机在 TCP 端口 23 上提供的服务。

```
<Sysname> system-view
```

```
[Sysname] portal free-rule 1 destination ip 20.20.20.1 32 tcp 23 source ip 10.10.10.1 24  
interface vlan-interface 1
```

配置一条基于 IPv6 地址的 Portal 免认证规则：编号为 2、源地址为 2000::1/64、目的地址为 2001::1、目的 TCP 端口号为 23、生效接口为 Vlan-interface1。该规则表示在 Vlan-interface1 接口上，2000::1/64 网段地址的用户不需要经过 Portal 认证即可以访问目的地址为 2001::1 的主机在 TCP 端口 23 上提供的服务。

```
<Sysname> system-view
```

```
[Sysname] portal free-rule 2 destination ipv6 2001::1 128 tcp 23 source ip 2000::1 64 interface  
vlan-interface 1
```

【相关命令】

- **display portal rule**

1.1.25 portal free-rule destination

portal free-rule destination 命令用来配置基于目的的 Portal 免认证规则，这里的目的是指主机名。

undo portal free-rule 命令用来删除指定的或所有 Portal 免认证规则。

【命令】

```
portal free-rule rule-number destination host-name
```

```
undo portal free-rule { rule-number | all }
```

【缺省情况】

不存在基于目的的 Portal 免认证规则。

【视图】

系统视图

【缺省用户角色】

network-admin

【参数】

rule-number: 免认证规则编号。取值范围为 0~4294967295。

destination: 指定目的信息。

host-name: 主机名，为 1~253 个字符的字符串，不区分大小写，字符串中可以包含字母、数字、“-”、“_”、“.” 和通配符“*”，且不能为“i”、“ip”、“ipv” 和 “ipv6”。

all: 所有免认证规则。

【使用指导】

基于目的 Portal 免认证规则支持如下两种配置方式：

- 精确匹配：即完整匹配主机名。例如配置的主机名为 **abc.com.cn**，其含义为只匹配 **abc.com.cn** 的主机名，如果报文中携带的主机名为 **dfabc.com.cn**，则匹配失败。
- 模糊匹配：即使用通配符配置主机名，通配符只能位于主机名字符串之首或末尾，例如配置的主机名为 ***abc.com.cn**、**abc*** 和 ***abc***，其含义分别为匹配所有以 **abc.com.cn** 结尾的主机名、匹配所有以 **abc** 开头的主机名和匹配所有含有 **abc** 字符串的主机名。

配置基于目的 Portal 免认证规则时，需要注意的是：

- 通配符“*”表示任意个数字符，设备会将已配置的多个连续的通配符识别为一个通配符。
- 配置的主机名不能只有通配符。
- 相同内容的免认证规则不能重复配置，否则提示免认证规则已存在或重复。
- 目前，只有用户浏览器发起的 HTTP/HTTPS 请求报文，支持模糊匹配的免认证规则。

【举例】

配置一条基于目的的 Portal 免认证规则：编号为 4、主机名为 **www.h3c.com**。该规则表示用户的 HTTP/HTTPS 请求报文中的主机名必须是 **www.h3c.com** 时，该用户才可以不需要经过 Portal 认证即可以访问网络资源。

```
<Sysname> system-view
```

```
[Sysname] portal free-rule 4 destination www.h3c.com
```

【相关命令】

- **display portal rule**

1.1.26 portal free-rule source

portal free-rule source 命令用来配置基于源的 Portal 免认证规则，这里的源可以是源 MAC 地址、源接口或者源 VLAN。

undo portal free-rule 命令用来删除指定的或所有 Portal 免认证规则。

【命令】

```
portal free-rule rule-number source { interface interface-type  
interface-number | mac mac-address | vlan vlan-id } *
```

```
undo portal free-rule { rule-number | all }
```

【缺省情况】

未配置基于源的 Portal 免认证规则。

【视图】

系统视图

【缺省用户角色】

network-admin

【参数】

rule-number: 免认证规则编号。取值范围为 0~4294967295。

interface interface-type interface-number: 免认证规则的源接口。*interface-type* *interface-number* 为接口类型和接口编号。

mac mac-address: 免认证规则的源 MAC 地址，为 H-H-H 的形式。

vlan vlan-id: 免认证规则的源 VLAN 编号。配置本关键字仅对通过 VLAN 接口接入的 Portal 用户生效。

all: 所有免认证规则。

【使用指导】

如果免认证规则中同时指定了源 VLAN 和二层源接口，则要求该接口属于对应的 VLAN，否则该规则无效。

【举例】

配置一条 Portal 免认证规则：编号为 3、源 MAC 地址为 1-1-1、源 VLAN 为 VLAN 10。该规则表示 MAC 地址为 1-1-1，属于 VLAN 10 的用户不需要经过 Portal 认证即可以访问网络资源。

```
<Sysname> system-view
```

```
[Sysname] portal free-rule 3 source mac 1-1-1 vlan 10
```

【相关命令】

- **display portal rule**

1.1.27 portal ipv6 free-all except destination

portal ipv6 free-all except destination 命令用来配置 IPv6 Portal 目的网段认证。

undo portal ipv6 free-all except destination 命令用来删除 IPv6 Portal 目的认证网段。

【命令】

```
portal ipv6 free-all except destination ipv6-network-address prefix-length
```

```
undo portal ipv6 free-all except destination [ ipv6-network-address ]
```

【缺省情况】

未配置 IPv6 Portal 目的网段认证，表示对访问任意 IPv6 目的网段的用户都进行 Portal 认证。

【视图】

接口视图

【缺省用户角色】

network-admin

【参数】

ipv6-network-address: IPv6 Portal 认证网段地址。

prefix-length: IPv6 地址前缀长度，取值范围为 0~128。

【使用指导】

接口上仅要求在 Portal 用户访问指定目的认证网段（除免认证规则中指定的目的 IP 地址或网段）时才需要进行 Portal 认证，访问其它网段访问时不需要进行 Portal 认证。

可以通过多次执行本命令，配置多条目的认证网段。

如果 **undo** 命令中不携带 IP 地址参数，则表示删除所有的 IPv6 Portal 目的认证网段。

目的网段认证对二次地址分配认证方式的 Portal 认证不生效。

如果接口上同时配置了源认证网段和目的认证网段，则源认证网段配置不会生效。

【举例】

在接口 Vlan-interface2 上配置 IPv6 Portal 目的认证网段为 1::2/16，仅要求访问 1::2/16 网段的用户必须进行 Portal 认证。

```
<Sysname> system-view
```

```
[Sysname] interface vlan-interface 2
```

```
[Sysname-Vlan-interface2] portal ipv6 free-all except destination 1::2 16
```

【相关命令】

- **display portal**

1.1.28 portal ipv6 layer3 source

portal ipv6 layer3 source 命令用来配置 IPv6 Portal 源认证网段。

undo portal ipv6 layer3 source 命令用来删除 IPv6 Portal 源认证网段。

【命令】

portal ipv6 layer3 source *ipv6-network-address* *prefix-length*

undo portal ipv6 layer3 source [*ipv6-network-address*]

【缺省情况】

未配置 IPv6 Portal 源认证网段，表示对来自任意网段的 IPv6 用户都进行 Portal 认证。

【视图】

接口视图

【缺省用户角色】

network-admin

【参数】

ipv6-network-address: IPv6 Portal 源认证网段地址。

prefix-length: IPv6 地址前缀长度，取值范围为 0~128。

【使用指导】

配置此功能后，接口上只允许在源认证网段范围内的 IPv6 用户报文才能触发 Portal 认证，否则丢弃。

如果 **undo** 命令中不携带 IP 地址参数，则表示删除所有的 IPv6 Portal 源认证网段。

源认证网段仅对 Portal 的可跨三层认证方式（**layer3**）生效。

如果接口上同时配置了源认证网段和目的网段认证，则源认证网段配置不会生效。

【举例】

在接口 Vlan-interface2 上配置一条 IPv6 Portal 源认证网段为 1::1/16，仅允许来自 1::1/16 网段的用户触发 Portal 认证。

```
<Sysname> system-view
[Sysname] interface vlan-interface 2
[Sysname-Vlan-interface2] portal ipv6 layer3 source 1::1 16
```

【相关命令】

- **display portal**
- **portal ipv6 free-all except destination**

1.1.29 portal ipv6 user-detect

portal ipv6 user-detect 命令用来开启 IPv6 Portal 用户在线探测功能。

undo portal user-detect 命令用来关闭 IPv6 Portal 用户在线探测功能。

【命令】

```
portal ipv6 user-detect type { icmpv6 | nd } [ retry retries ] [ interval
interval ] [ idle time ]
undo portal ipv6 user-detect
```

【缺省情况】

IPv6 Portal 用户在线探测功能处于关闭状态。

【视图】

接口视图

【缺省用户角色】

network-admin

【参数】

type: 指定探测类型。

- **icmpv6**: 表示探测类型为 ICMPv6。
- **nd**: 表示探测类型为 ND。

retry retries: 探测次数，取值范围为 1~10，缺省值为 3。

interval interval: 探测间隔，取值范围为 1~1200，单位为秒，缺省值为 3。

idle time: 用户在线探测闲置时长，即闲置多长时间后发起探测，取值范围为 60~3600，单位为秒，缺省值为 180。

【使用指导】

根据探测类型的不同，设备有以下两种探测机制：

- 当探测类型为 ICMPv6 时，若设备发现一定时间 (**idle time**) 内接口上未收到某 Portal 用户的报文，则会向该用户定期 (**interval interval**) 发送探测报文。如果在指定探测次数 (**retry retries**) 之内，设备收到了该用户的响应报文，则认为用户在线，且停止发送探测报文，重复这个过程，否则，强制其下线。
- 当探测类型为 ND 时，若设备发现一定时间 (**idle time**) 内接口上未收到某 Portal 用户的报文，则会向该用户发送 ND 请求报文。设备定期 (**interval interval**) 检测用户 ND 表项是否被刷新过，如果在指定探测次数 (**retry retries**) 内用户 ND 表项被刷新过，则认为用户在线，且停止检测用户 ND 表项，重复这个过程，否则，强制其下线。

请根据配置的认证方式选择合适的探测方法，如果配置了直接方式或者二次地址分配方式，则可以使用 ND 或 ICMPv6 探测方式，如果配置了可跨三层认证方式，则可以使用 ICMPv6 探测方式，若配置了 ND 探测方式，则探测功能不生效。

如果用户接入设备上配置了阻止 ICMPv6 报文的防火墙策略，则接口上的 ICMPv6 探测方式可能会失败，从而导致接口上的 Portal 用户非正常下线。因此，若接口上需要使用 ICMPv6 探测方式，请保证用户接入设备不会过滤掉 ICMPv6 报文。

【举例】

在接口 Vlan-interface100 上开启 IPv6 Portal 用户在线探测功能：探测类型为 ND，检测用户 ND 表项的探测次数为 5 次，探测间隔为 10 秒，闲置时间为 300 秒。

```
<Sysname> system-view
[Sysname] interface vlan-interface 100
[Sysname-Vlan-interface100] portal ipv6 user-detect type nd retry 5 interval 10 idle 300
```

【相关命令】

- **display portal**

1.1.30 portal layer3 source

portal layer3 source 命令用来配置 IPv4 Portal 源认证网段。

undo portal layer3 source 命令用来删除 IPv4 Portal 源认证网段。

【命令】

```
portal layer3 source ipv4-network-address { mask-length | mask }
undo portal layer3 source [ ipv4-network-address ]
```

【缺省情况】

未配置 IPv4 Portal 源认证网段，表示对来自任意网段的 IPv4 用户都进行 Portal 认证。

【视图】

接口视图

【缺省用户角色】

network-admin

【参数】

ipv4-network-address: IPv4 Portal 认证网段地址。

mask-length: 子网掩码长度，取值范围为 0~32。

mask: 子网掩码，点分十进制格式。

【使用指导】

配置此功能后，接口上只允许在源认证网段范围内的 IPv4 用户报文才能触发 Portal 认证，否则丢弃。

如果 **undo** 命令中不携带 IP 地址参数，则表示删除所有的 IPv4 Portal 源认证网段。

源认证网段仅对 Portal 的可跨三层认证方式（**layer3**）生效。

如果接口上同时配置了源认证网段和目的网段认证，则源认证网段配置不会生效。

【举例】

在接口 Vlan-interface2 上配置一条 IPv4 Portal 源认证网段为 10.10.10.0/24，仅允许来自 10.10.10.0/24 网段的用户触发 Portal 认证。

```
<Sysname> system-view
[Sysname] interface vlan-interface 2
[Sysname-Vlan-interface2] portal layer3 source 10.10.10.0 24
```

【相关命令】

- **display portal**
- **portal free-all except destination**

1.1.31 portal local-web-server

portal local-web-server 命令用来开启本地 Portal 服务，并进入基于 HTTP/HTTPS 协议的本地 Portal Web 服务视图。

undo portal local-web-server 命令用来关闭本地 Portal 服务功能。

【命令】

```
portal local-web-server { http | https ssl-server-policy policy-name
[ tcp-port port-number ] }
undo portal local-web-server { http | https }
```

【缺省情况】

本地 Portal 服务功能处于关闭状态。

【视图】

系统视图

【缺省用户角色】

network-admin

【参数】

http: 指定本地 Portal Web 服务使用 HTTP 协议和客户端交互认证信息。

https: 指定本地 Portal Web 服务使用 HTTPS 协议和客户端交互认证信息。

ssl-server-policy *policy-name*: 指定 HTTPS 服务关联的 SSL 服务器端策略。
policy-name 为 SSL 服务器端策略的名称, 为 1~31 个字符的字符串, 不区分大小写, 且必须已经存在。

tcp-port *port-number*: 指定本地 Portal Web 服务的 HTTPS 服务侦听的 TCP 端口号, 取值范围为 1~65535, 缺省值为 443。

【使用指导】

本地 Portal 服务功能是指, Portal 认证系统中不采用外部独立的 Portal Web 服务器和 Portal 认证服务器, 而由接入设备实现 Portal Web 服务器和 Portal 认证服务器功能。

只有接口上引用的 Portal Web 服务器中的 URL 同时满足以下两个条件时, 接口上才会使用本地 Portal Web 服务功能。条件如下:

- 该 URL 中的 IP 地址是设备本机上的 IP 地址 (除 127.0.0.1 以外)。
- 该 URL 以 /portal/ 结尾, 例如: http://1.1.1.1/portal/。

配置本地 Portal Web 服务功能时, 需要注意的是:

- 已经被 HTTPS 服务关联的 SSL 服务器端策略不能被删除。
- 不能通过重复执行本命令来修改 HTTPS 服务关联的 SSL 服务器端策略, 如需修改, 请先通过 **undo portal local-web-server https** 命令删除已创建的本地 Portal Web 服务, 再执行 **portal local-web-server https ssl-server-policy** 命令。

配置本地 Portal Web 服务参数时, 需要注意的是:

- 如果本地 Portal Web 服务引用的 SSL 服务器端策略与 HTTPS 服务引用的 SSL 服务器端策略相同, 则本地 Portal Web 服务使用的 TCP 端口号可以与 HTTPS 服务器使用的 TCP 端口号相同, 否则不能使用相同的 TCP 端口号。
- 除了 HTTPS 协议默认的端口号, 本地 Portal Web 服务的 TCP 端口号不能与知名协议使用的端口号或者设备上其它服务已使用的 TCP 端口号配置一致, 如 HTTP 的端口号 80; Telnet 的端口号 23, 否则会造成本地 Portal Web 服务无法向 Portal 用户推送认证页面。
- 使用 HTTP 协议和 HTTPS 协议的本地 Portal Web 服务侦听的 TCP 端口号不能配置一致, 比如不能都配置为 8080, 否则会导致本地 Web 服务无法正常使用。

【举例】

开启本地 Portal 服务, 并进入基于 HTTP 协议的本地 Portal Web 服务视图。

```
<Sysname> system-view
[Sysname] portal local-web-server http
[Sysname-portal-local-websvr-http] quit
```

开启本地 Portal 服务, 并进入基于 HTTP 协议的本地 Portal Web 服务视图, 引用的 SSL 服务器端策略为 policy1。

```
<Sysname> system-view
[Sysname] portal local-web-server https ssl-server-policy policy1
[Sysname-portal-local-websvr-https] quit
```

更改引用的 SSL 服务器端策略为 policy2。

```
[Sysname] undo portal local-web-server https
[Sysname] portal local-web-server https ssl-server-policy policy2
[Sysname-portal-local-websvr-https] quit
```

使用 HTTPS 协议和客户端交互认证信息的方式创建本地 Portal Web 服务，引用的 SSL 服务器端策略为 policy1，指定侦听的端口号为 442。

```
<Sysname> system-view
[Sysname] portal local-web-server https ssl-server-policy policy1 tcp-port 442
[Sysname-portal-local-websvr-https] quit
```

【相关命令】

- **default-logon-page**
- **portal local-web-server**
- **ssl server-policy**（安全命令参考/SSL）

1.1.32 portal log enable

portal log enable 命令用来开启 Portal 用户上/下线日志功能。

undo portal log enable 命令用来关闭 Portal 用户上/下线日志功能。

【命令】

```
portal log enable
undo portal log enable
```

【缺省情况】

Portal 用户上/下线日志功能处于关闭状态。

【视图】

系统视图

【缺省用户角色】

network-admin

【使用指导】

开启本功能后，设备会对用户上线和下线时的信息进行记录，包括用户名、IP 地址、接口名称、VLAN、用户 MAC 地址、上线失败原因等。生成的日志信息将被发送到设备的信息中心，通过设置信息中心的参数，决定日志信息的输出规则（即是否允许输出以及输出方向）。有关信息中心参数的配置请参见“网络管理和监控配置指导”中的“信息中心”。

【举例】

开启 Portal 用户上/下线日志功能。

```
<Sysname> system-view
[Sysname] portal log enable
```

1.1.33 portal max-user

portal max-user 命令用来配置全局 Portal 最大用户数。

undo portal max-user 命令用来恢复缺省情况。

【命令】

```
portal max-user max-number
undo portal max-user
```

【缺省情况】

全局 Portal 最大用户数不受限制。

【视图】

系统视图

【缺省用户角色】

network-admin

【参数】

max-number: 系统中允许同时在线的最大 Portal 用户数。取值范围为 1~4294967295。

【使用指导】

如果配置的全局 Portal 最大用户数小于当前已经在线的 Portal 用户数，则该命令可以执行成功，且在线 Portal 用户不受影响，但系统将不允许新的 Portal 用户接入。

该命令指定的最大用户数是指 IPv4 Portal 和 IPv6 Portal 用户的总数。

建议所有开启 Portal 的接口上的最大 IPv4 Portal 用户数和最大 IPv6 Portal 用户数之和不超过配置的全局最大 Portal 用户数，否则会有部分 Portal 用户因为全局最大用户数已达到上限而无法上线。

【举例】

配置全局 Portal 最大用户数为 100。

```
<Sysname> system-view
[Sysname] portal max-user 100
```

【相关命令】

- **display portal user**
- **portal { ipv4-max-user | ipv6-max-user }**

1.1.34 portal nas-id-profile

portal nas-id-profile 命令用来指定接口引用的 NAS-ID Profile。

undo portal nas-id-profile 命令用来恢复缺省情况。

【命令】

```
portal nas-id-profile profile-name
undo portal nas-id-profile
```

【缺省情况】

未指定引用的 NAS-ID Profile。

【视图】

接口视图

【缺省用户角色】

network-admin

【参数】

profile-name: 标识指定 VLAN 和 NAS-ID 绑定关系的 Profile 名称, 为 1~31 个字符的字符串, 不区分大小写。

【使用指导】

本命令引用的 NAS-ID Profile 由命令 **aaa nas-id profile** 配置, 具体情况请参考“安全命令参考”中的“AAA”。

对于 QinQ 报文, Portal 接入只能匹配内层 VLAN。有关 QinQ 的详细介绍, 请参见“二层技术-以太网交换配置指导”中的“QinQ”。

如果接口上指定了 NAS-ID Profile, 则此 Profile 中定义的绑定关系优先使用; 如果接口上未指定 NAS-ID Profile 或指定的 Profile 中没有找到匹配的绑定关系, 则使用设备名作为 NAS-ID。

【举例】

在接口 Vlan-interface 2 上指定名为 aaa 的 NAS-ID Profile。

```
<Sysname> system-view
[Sysname] interface vlan-interface 2
[Sysname-Vlan-interface2] portal nas-id-profile aaa
```

【相关命令】

- **aaa nas-id profile** (安全命令参考/AAA)

1.1.35 portal nas-port-id format

portal nas-port-id format 命令用来配置 NAS-Port-ID 属性的格式。

undo portal nas-port-id format 命令用来恢复缺省情况。

【命令】

```
portal nas-port-id format { 1 | 2 | 3 | 4 }
undo portal nas-port-id format
```

【缺省情况】

NAS-Port-ID 的消息格式为格式 2。

【视图】

系统视图

【缺省用户角色】

network-admin

【参数】

1: 表示格式 1, 具体为 {atm|eth|trunk} NAS_slot/NAS_subslot/NAS_port:XPI.XCI AccessNodeIdentifier/ANI_rack/ANI_frame/ANI_slot/ANI_subslot/ANI_port[:ANI_XPI.ANI_XCI]。

2: 表示格式 2, 具体为 SlotID00IfNOVlanID。

3: 表示格式 3, 具体为在格式 2 的内容后面添加 Option82 或者 Option18。

4: 表示格式 4, 具体为 slot=**;subslot=**;port=**;vlanid=**;vlanid2=**。

【使用指导】

可通过本命令修改设备为 Portal 用户发送的 RADIUS 报文中填充的 NAS-Port-ID 属性的格式。
不同厂商的 RADIUS 服务器要求不同的格式，通常中国电信的 RADIUS 服务器要求采用格式 1。

1. 格式 1

{atm|eth|trunk} NAS_slot/NAS_subslot/NAS_port:XPI.XCI
AccessNodeIdentifier/ANI_rack/ANI_frame/ANI_slot/ANI_subslot/ANI_port[:ANI_XPI.ANI_XCI]

各项含义如下：

- {atm|eth|trunk}：BRAS 端口类型，包括 ATM 接口、以太网接口或 trunk 类型的以太网接口。
- NAS_slot：BRAS 槽号，取值为 0~31。
- NAS_subslot：BRAS 子槽号，取值为 0~31。
- NAS_Port：BRAS 端口号，取值为 0~63。
- XPI：如果接口类型为 atm，则 XPI 对应 VPI，取值为 0~255；如果接口类型为 eth 或 trunk，则 XPI 对应 PVLAN，XPI 取值为 0~4095。
- XCI：如果接口类型为 atm，则 XCI 对应 VCI，取值为 0~65535；如果接口类型为 eth 或 trunk，XCI 对应于 CVLAN，XCI 取值为 0~4095。
- AccessNodeIdentifier：接入节点标识（例如 DSLAM 设备），为不超过 50 个字符的字符串，字符串中不能包括空格。
- ANI_rack：接入节点机架号（如支持紧耦合的 DSLAM 设备），取值为 0~15。
- ANI_frame：接入节点机框号，取值为 0~31。
- ANI_slot：接入节点槽号，取值为 0~127。
- ANI_subslot：接入节点子槽号，取值为 0~31。
- ANI_port：接入节点端口号，取值为 0~255。
- ANI_XPI.ANI_XCI：可选项，主要用于携带 CPE 侧的业务信息，可用于标识未来的业务类型需求。其中，如果接口类型为 atm，则 ANI_XPI 对应 VPI，取值为 0~255，ANI_XCI 对应 VCI，取值为 0~65535；如果接口类型为 eth 或 trunk，则 ANI_XPI 对应 PVLAN，取值为 0~4095，则 ANI_XCI 对应 CVLAN，取值为 0~4095。

字符串之间用一个空格隔开，要求字符串中间不能有空格。花括号中的内容是必选的，| 表示并列的关系，多选一。[] 表示可选项。对于某些设备没有机架、框、子槽的概念，相应位置应统一填 0，对于无效的 VLAN ID 值都填 4096。

如接口类型为 ATM，则 AccessNodeIdentifier、ANI_rack、ANI_frame、ANI_slot、ANI_subslot、ANI_port 域可统一填 0。

如运营商未使用 SVLAN 技术，则 XPI=4096，XCI=VLAN，取值为 0~4095。

如运营商未使用 VLAN 技术区分用户（用户 PC 直连 BAS 端口），则 XPI=4096，XCI=4096。

对于接入节点设备（如 DSLAM），按如上格式上报本接入节点的接入线路信息，对于与 BRAS 设备相关的接入线路信息可统一填 0，如：“0 0/0/0:4096.1234 guangzhou001/0/31/63/31/127”

其含义是 DSLAM 节点标识为 guangzhou001、DSLAM 的机架号为 0（没有机架）、DSLAM 的框号为 31、DSLAM 的槽号为 63、DSLAM 的子槽号为 31、DSLAM 的端口号为 127、VLAN ID 号为 1234，BRAS 接入线路信息为未知。

对于 BRAS 设备，在获取接入节点设备（如 DSLAM）的接入线路信息后，根据 BRAS 的配置可透传接入线路信息，也可修改添加接入线路信息中与 BRAS 设备相关的线路信息，形成完整的接入线路信息，如：“eth 31/31/7:4096.1234 guangzhou001/0/31/63/31/127”。

格式 1 的解释示例如下：

- 例 1：NAS_PORT_ID = “atm 31/31/7:255.65535 0/0/0/0/0”

含义：BRAS 设备的用户接口类型为 ATM 接口，BRAS 槽号为 31，BRAS 子槽号为 31，BRAS 端口号为 7，VPI 为 255，VCI 为 65535。

- 例 2：NAS_PORT_ID = “eth 31/31/7:1234.2345 0/0/0/0/0”

含义：BRAS 设备的用户接口类型为以太网接口，BRAS 槽号为 31，BRAS 子槽号为 31，BRAS 端口号为 7，PVLAN ID 为 1234，CVLAN ID 为 2345。

- 例 3：NAS_PORT_ID = “eth 31/31/7:4096.2345 0/0/0/0/0”

含义：BRAS 设备的用户接口类型为以太网接口，BRAS 槽号为 31，BRAS 子槽号为 31，BRAS 端口号为 7，VLAN ID 为 2345。

- 例 4：NAS_PORT_ID = “eth 31/31/7:4096.2345 guangzhou001/1/31/63/31/127”

含义：BRAS 设备的用户接口类型为以太网接口，BRAS 槽号为 31，BRAS 子槽号为 31，BRAS 端口号为 7，VLAN ID 为 2345，接入节点 DSLAM 的标识为 guangzhou001，DSLAM 的机架号为 1，DSLAM 的框号为 31，DSLAM 的槽号为 63，DSLAM 的子槽号为 31，DSLAM 的端口号为 127。

2. 格式 2

SlotID00IfNOVlanID

各项含义如下：

- SlotID：用户接入的槽位号，为两个字符的字符串。
- IfNO：用户接入的接口编号，为 3 个字符的字符串。
- VlanID：用户接入的 VLAN ID，为 9 个字符的字符串。

3. 格式 3

其格式为在格式 2 的 NAS-Port-ID 内容后面添加用户 DHCP 报文中指定 Option 的内容：对于 IPv4 用户，此处添加的是 DHCP Option82 的内容。对于 IPv6 用户，此处添加的是 DHCP Option18 的内容。

4. 格式 4

其格式为 slot=**;subslot=**;port=**;vlanid=**;vlanid2=**，具体情况如下：

- 对于非 VLAN 接口，其格式为 slot=**;subslot=**;port=**;vlanid=0。
- 对于只终结了一层 VLAN Tag 的接口，其格式为 slot=**;subslot=**;port=**;vlanid=**。

【举例】

配置 NAS-Port-ID 属性的格式为 format 1。

```
<Sysname> system-view
[Sysname] portal nas-port-id format 1
```

1.1.36 portal pre-auth ip-pool

portal [ipv6] pre-auth ip-pool 命令用来配置 Portal 认证前用户使用的地址池。

undo portal [ipv6] pre-auth ip-pool 命令用来恢复缺省情况。

【命令】

```
portal [ ipv6 ] pre-auth ip-pool pool-name
undo portal [ ipv6 ] pre-auth ip-pool
```

【缺省情况】

未配置 Portal 认证前用户使用的地址池。

【视图】

接口视图

【缺省用户角色】

network-admin

【参数】

ipv6: 表示 IPv6 Portal 用户。若不指定该参数, 则表示 IPv4 Portal 用户。

pool-name: 表示 IP 地址池的名称, 为 1~63 个字符的字符串, 不区分大小写。

【使用指导】

当接口上未配置 IP 地址, 且用户需要通过 DHCP 获取地址时, 就必须通过本命令指定一个地址池, 并在用户进行 Portal 认证之前为其分配一个 IP 地址使其可以进行 Portal 认证。

仅当接口使用直接认证方式的情况下, 接口上为认证前的 Portal 用户指定的 IP 地址池才能生效。

当使用接口上指定的 IP 地址池为认证前的 Portal 用户分配 IP 地址时, 该指定的 IP 地址池必须存在且配置完整, 否则无法为 Portal 用户分配 IP 地址, 并导致用户无法进行 Portal 认证。

【举例】

在接口 Vlan-interface100 上为认证前的 Portal 用户指定 IPv4 地址池为 abc。

```
<Sysname> system-view
[Sysname] interface vlan-interface 100
[Sysname-Vlan-interface100] portal pre-auth ip-pool abc
```

【相关命令】

- **dhcp server ip-pool** (三层技术-IP 业务命令参考/DHCP)
- **display portal**
- **ipv6 dhcp pool** (三层技术-IP 业务命令参考/DHCP)

1.1.37 portal refresh enable

portal refresh { arp | nd } enable 命令用来开启 Portal 客户端 Rule ARP/ND 表项生成功能。

undo portal refresh { arp | nd } enable 命令用来关闭 Portal 客户端 Rule ARP/ND 表项生成功能。

【命令】

```
portal refresh { arp | nd } enable
undo portal refresh { arp | nd } enable
```


【缺省情况】

Portal 客户端 Rule ARP 表项、ND 表项生成功能均处于开启状态。

【视图】

系统视图

【缺省用户角色】

network-admin

【参数】

arp: 表示 ARP 表项。

nd: 表示 ND 表项。

【使用指导】

Portal 客户端的 Rule ARP/ND 表项生成功能处于开启状态时，Portal 客户端上线后，其 ARP/ND 表项为 Rule 表项，在 Portal 客户端下线后会被立即删除，导致 Portal 客户端在短时间内再上线时会因 ARP/ND 表项还未学习到而认证失败。此情况下，需要关闭本功能，使得 Portal 客户端上线后其 ARP/ND 表项仍为动态表项，在 Portal 客户端下线后按老化时间正常老化。

此功能的开启和关闭不影响已经在线的 Portal 客户端的 ARP/ND 表项类型。

【举例】

关闭 Portal 客户端 Rule ARP 表项生成功能。

```
<Sysname> system-view  
[Sysname] undo portal refresh arp enable
```

1.1.38 portal roaming enable

portal roaming enable 命令用来开启 Portal 用户漫游功能。

undo portal roaming enable 命令用来关闭 Portal 用户漫游功能。

【命令】

```
portal roaming enable  
undo portal roaming enable
```

【缺省情况】

Portal 用户漫游功能处于关闭状态，即 Portal 用户上线后不能在所在的 VLAN 内漫游。

【视图】

系统视图

【缺省用户角色】

network-admin

【使用指导】

Portal 用户漫游功能只对通过 VLAN 接口上线的 Portal 用户有效。

设备上有用户在线的情况下，不能配置此命令。

如果开启了 Portal 用户漫游功能，则 Portal 用户上线后可以在开启 Portal 的 VLAN 内漫游，即用户通过 VLAN 内的任何二层端口都可以访问网络资源；否则用户只能通过认证成功的二层端口访问网络资源。

Portal 用户漫游功能需要在关闭 Portal 客户端 Rule ARP/ND 表项生成功能（通过命令 **undo portal refresh { arp | nd } enable**）的情况下才能生效。

【举例】

开启 Portal 用户漫游功能。

```
<Sysname> system-view
[Sysname] portal roaming enable
```

1.1.39 portal server

portal server 命令用来创建 Portal 认证服务器，并进入 Portal 认证服务器视图。如果指定的 Portal 认证服务器已经存在，则直接进入 Portal 认证服务器视图。

undo portal server 命令用来删除指定的 Portal 认证服务器。

【命令】

```
portal server server-name
undo portal server server-name
```

【缺省情况】

不存在 Portal 认证服务器。

【视图】

系统视图

【缺省用户角色】

network-admin

【参数】

server-name: Portal 认证服务器的名称，为 1~32 个字符的字符串，区分大小写。

【使用指导】

Portal 认证服务器视图用于配置 Portal 认证服务器的相关参数，包括服务器的 IP 地址、端口号，设备和服务器间通信的预共享密钥，服务器探测功能等。

可以配置多个 Portal 认证服务器。

【举例】

创建名称为 pts 的 Portal 认证服务器，并进入 Portal 认证服务器视图。

```
<Sysname> system-view
[Sysname] portal server pts
[Sysname-portal-server-pts]
```

【相关命令】

- **display portal server**

1.1.40 portal user-detect

portal user-detect 命令用来开启 IPv4 Portal 用户在线探测功能。

undo portal user-detect 命令用来关闭 IPv4 Portal 用户在线探测功能。

【命令】

```
portal user-detect type { arp | icmp } [ retry retries ] [ interval interval ]  
[ idle time ]  
undo portal user-detect
```

【缺省情况】

IPv4 Portal 用户在线探测功能处于关闭状态。

【视图】

接口视图

【缺省用户角色】

network-admin

【参数】

type: 指定探测类型。

- **arp**: 表示探测类型为 ARP。
- **icmp**: 表示探测类型为 ICMP。

retry retries: 探测次数，取值范围为 1~10，缺省值为 3。

interval interval: 探测间隔，取值范围为 1~1200，单位为秒，缺省值为 3。

idle time: 用户在线探测闲置时长，即闲置多长时间后发起探测，取值范围为 60~3600，单位为秒，缺省值为 180。

【使用指导】

根据探测类型的不同，设备有以下两种探测机制：

- 当探测类型为 ICMP 时，若设备发现一定时间（**idle time**）内接口上未收到某 Portal 用户的报文，则会向该用户定期（**interval interval**）发送探测报文。如果在指定探测次数（**retry retries**）之内，设备收到了该用户的响应报文，则认为用户在线，且停止发送探测报文，重复这个过程，否则，强制其下线。
- 当探测类型为 ARP 时，若设备发现一定时间（**idle time**）内接口上未收到某 Portal 用户的报文，则会向该用户发送 ARP 请求报文。设备定期（**interval interval**）检测用户 ARP 表项是否被刷新过，如果在指定探测次数（**retry retries**）内用户 ARP 表项被刷新过，则认为用户在线，且停止检测用户 ARP 表项，重复这个过程，否则，强制其下线。

请根据配置的认证方式选择合适的探测方法，如果配置了直接方式或者二次地址分配方式，则可以使用 ARP 或 ICMP 探测方式，如果配置了可跨三层认证方式，则仅可以使用 ICMP 探测方式，若配置了 ARP 探测方式，则探测功能不生效。

如果用户接入设备上配置了阻止 ICMP 报文的防火墙策略，则接口上的 ICMP 探测方式可能会失败，从而导致接口上的 Portal 用户非正常下线。因此，若接口上需要使用 ICMP 探测方式，请保证用户接入设备不会过滤掉 ICMP 报文。

【举例】

在接口 Vlan-interface100 上开启 Portal 用户在线探测功能：探测类型为 ARP，检测用户 ARP 表的探测次数为 5 次，探测间隔为 10 秒，闲置时间为 300 秒。

```
<Sysname> system-view
[Sysname] interface vlan-interface 100
[Sysname-Vlan-interface100] portal user-detect type arp retry 5 interval 10 idle 300
```

【相关命令】

- **display portal**

1.1.41 portal user-dhcp-only (interface view)

portal user-dhcp-only 命令用来开启仅允许通过 DHCP 方式获取 IP 地址的客户端上线的功能。

undo portal user-dhcp-only 命令用来关闭仅允许通过 DHCP 方式获取 IP 地址的客户端上线的功能。

【命令】

```
portal [ ipv6 ] user-dhcp-only
undo portal [ ipv6 ] user-dhcp-only
```

【缺省情况】

仅允许通过 DHCP 方式获取 IP 地址的客户端上线的功能处于关闭状态，通过 DHCP 方式获取 IP 地址的客户端和配置静态 IP 地址的客户端都可以上线。

【视图】

接口视图

【缺省用户角色】

network-admin

【参数】

ipv6：表示允许上线的客户端的 IP 地址为 IPv6 地址，如果不指定本参数，则表示允许上线的客户端的 IP 地址为 IPv4 地址。

【使用指导】

配置本命令后，配置静态 IP 地址的 Portal 认证用户不能上线。

在 IPv6 网络中，配置本命令后，终端仍会使用临时 IPv6 地址进行 Portal 认证，从而导致认证失败，所以终端必须关闭临时 IPv6 地址。

【举例】

在接口 Vlan-interface100 上配置仅允许通过 DHCP 获取 IP 地址的客户端上线功能。

```
<Sysname> system-view
[Sysname] interface vlan-interface 100
[Sysname-Vlan-interface100] portal user-dhcp-only
```

【相关命令】

- **display portal**

1.1.42 portal web-proxy port

portal web-proxy port 命令用来配置允许触发 Portal 认证的 Web 代理服务器端口。

undo portal web-proxy port 命令用来删除指定或所有的 Web 代理服务器端口。

【命令】

```
portal web-proxy port port-number
undo portal web-proxy port { port-number | all }
```

【缺省情况】

不存在允许触发 Portal 认证的 Web 代理服务器端口。

【视图】

系统视图

【缺省用户角色】

network-admin

【参数】

port-number: Portal 认证的 Web 代理服务器的 TCP 端口号，取值范围为 1~65535。

all: 指定所有 Portal 认证的 Web 代理服务器的 TCP 端口号。

【使用指导】

设备默认只允许未配置 Web 代理服务器的用户浏览器发起的 HTTP 请求才能触发 Portal 认证。若用户使用配置了 Web 代理服务器的浏览器上网，则用户的这类 HTTP 请求报文将被丢弃，而不能触发 Portal 认证。这种情况下，网络管理员可以通过在设备上添加 Web 代理服务器的 TCP 端口号，来允许使用 Web 代理服务器的用户浏览器发起的 HTTP 请求也可以触发 Portal 认证。

多次配置本命令可以添加多个 Web 代理服务器的 TCP 端口号。

配置 Portal 认证 Web 代理服务器端口号，需要注意的是：

- 如果用户浏览器采用 WPAD（Web Proxy Auto-Discovery，Web 代理服务器自动发现）方式自动配置 Web 代理，则不仅需要网络管理员在设备上添加 Web 代理服务器端口，还需要配置免认证规则，允许目的 IP 为 WPAD 主机 IP 地址的用户报文免认证。
- 除了需要网络管理员在设备上添加指定的 Web 代理服务器端口，还需要用户在浏览器上将 Portal 认证服务器的 IP 地址配置为 Web 代理服务器的例外地址，避免 Portal 用户发送给 Portal 认证服务器的 HTTP 报文被发送到 Web 代理服务器上，从而影响正常的 Portal 认证。
- 目前不支持配置 Portal 认证 Web 代理服务器的端口号为 443。

【举例】

配置允许触发 Portal 认证的 Web 代理服务器端口号为 8080。

```
<Sysname> system-view
[Sysname] portal web-proxy port 8080
```

【相关命令】

- **portal enable method**

1.1.43 portal web-server

portal web-server 命令用来创建 Portal Web 服务器，并进入 Portal Web 服务器视图。如果指定的 Portal Web 服务器已经存在，则直接进入 Portal Web 服务器视图。

undo portal web-server 命令用来删除 Portal Web 服务器。

【命令】

```
portal web-server server-name
undo portal web-server server-name
```

【缺省情况】

不存在 Portal Web 服务器。

【视图】

系统视图

【缺省用户角色】

network-admin

【参数】

server-name: Portal Web 服务器的名称，为 1~32 个字符的字符串，区分大小写。

【使用指导】

Portal Web 服务器是指 Portal 认证过程中向用户推送认证页面的 Web 服务器，也是设备强制重定向用户 HTTP 请求报文时所指的 Web 服务器。Portal Web 服务器视图用于配置该 Web 服务器的 URL 地址及配置设备重定向该 URL 地址给用户时 URL 地址所携带的参数，同时该视图还用于配置 Portal Web 服务器探测等功能。

【举例】

```
# 创建名称为 wbs 的 Portal Web 服务器，并进入 Portal Web 服务器视图。
<Sysname> system-view
[Sysname] portal web-server wbs
[Sysname-portal-websvr-wbs]
```

【相关命令】

- **display portal web-server**
- **portal apply web-server**

1.1.44 reset portal packet statistics

reset portal packet statistics 命令用来清除 Portal 报文的统计信息。

【命令】

```
reset portal packet statistics [ server server-name ]
```

【视图】

用户视图

【缺省用户角色】

network-admin

【参数】

server-name: Portal 认证服务器的名称，为 1~32 个字符的字符串，区分大小写。

【使用指导】

若不指定参数 **server**，则清除所有 Portal 认证服务器的报文统计信息。

【举例】

清除名称为 st 上的 Portal 认证服务器的统计信息。

```
<Sysname> reset portal packet statistics server pts
```

【相关命令】

- **display portal packet statistics**

1.1.45 server-detect (portal authentication server view)

server-detect 命令用来开启 Portal 认证服务器的可达性探测功能。开启 Portal 认证服务器的可达性探测功能后，设备会定期检测 Portal 认证服务器发送的 Portal 报文来判断服务器的可达状态。

undo server-detect 命令用来关闭 Portal 认证服务器的可达性探测功能。

【命令】

```
server-detect [ timeout timeout ] log  
undo server-detect
```

【缺省情况】

Portal 认证服务器的可达性探测功能处于关闭状态。

【视图】

Portal 认证服务器视图

【缺省用户角色】

network-admin

【参数】

timeout *timeout*: 探测超时时间，取值范围为 10~3600，单位为秒，缺省值为 60。

log: Portal 认证服务器可达或者不可达的状态改变时，发送日志信息。日志信息中记录了 Portal 认证服务器名以及该服务器状态改变前后的状态。

【使用指导】

只有当设备上存在开启 Portal 认证的接口时，Portal 认证服务器的可达性探测功能才生效。

只有在支持 Portal 服务器心跳功能（目前仅 iMC 的 Portal 认证服务器支持）的 Portal 认证服务器的配合下，本功能才有效。

若设备在指定的探测超时时间（**timeout** *timeout*）内收到 Portal 报文，且验证其正确，则认为此次探测成功且服务器可达，否则认为此次服务器不可达。

设备配置的探测超时时间（**timeout** *timeout*）必须大于服务器上配置的逃生心跳间隔时间。

【举例】

开启对 Portal 认证服务器 pts 的探测功能, 探测超时时间为 600 秒, 若服务器状态改变, 则发送日志信息。

```
<Sysname> system-view
[Sysname] portal server pts
[Sysname-portal-server-pts] server-detect timeout 600 log
```

【相关命令】

- **portal server**

1.1.46 server-detect (portal web server view)

server-detect 命令用来开启 Portal Web 服务器的可达性探测功能。

undo server-detect 命令用来关闭 Portal Web 服务器的可达性探测功能。

【命令】

```
server-detect [ interval interval ] [ retry retries ] log
undo server-detect
```

【缺省情况】

Portal Web 服务器的可达性探测功能处于关闭状态。

【视图】

Portal Web 服务器视图

【缺省用户角色】

network-admin

【参数】

interval interval: 进行探测尝试的时间间隔, 取值范围为 10~1200, 单位为秒, 缺省值为 20。

retry retries: 连续探测失败的最大次数, 取值范围为 1~10, 缺省值为 3。若连续探测失败数目达到此值, 则认为服务器不可达。

log: Portal Web 服务器可达或者不可达的状态改变时, 发送日志信息。日志信息中记录了 Portal Web 服务器名以及该服务器状态改变前后的状态。

【使用指导】

该探测方法可由设备独立完成, 不需要 Portal Web 服务器端的任何配置来配合。

只有当配置了 Portal Web 服务器的 URL 地址, 且设备上存在开启 Portal 认证接口时, 该 Portal Web 服务器的可达性探测功能才生效。

【举例】

配置对 Portal Web 服务器 wbs 的探测功能, 每次探测间隔时间为 600 秒, 若连续二次探测均失败, 则发送服务器不可达的日志信息。

```
<Sysname> system-view
[Sysname] portal web-server wbs
[Sysname-portal-websvr-wbs] server-detect interval 600 retry 2 log
```


【相关命令】

- `portal web-server`

1.1.47 server-register

`server-register` 命令用来配置设备定期向 Portal 认证服务器发送注册报文。

`undo server-register` 命令用来恢复缺省情况。

【命令】

```
server-register [ interval interval-value ]  
undo server-register
```

【缺省情况】

设备不会定期向 Portal 认证服务器发送注册报文。

【视图】

Portal 认证服务器视图

【缺省用户角色】

network-admin

【参数】

interval interval-value: 设备定期向 Portal 认证服务器发送注册报文的时间间隔，取值范围为 1~3600，单位为秒，缺省值为 600。

【使用指导】

Portal 服务器与接入设备认证交互时，如果二者之间有 NAT 设备，为了使 Portal 服务器能够访问该接入设备，在 NAT 设备上需配置静态 NAT 表项，该静态 NAT 表项中记录了接入设备的 IP 地址以及与 Portal 服务器交互时使用的转换后的 IP 地址。当有大量的接入设备需要与 Portal 服务器进行认证交互时，则需要在 NAT 设备上配置大量的静态 NAT 表项。开启本功能后，接入设备会主动向 Portal 服务器发送注册报文，该报文中携带了接入设备的名称。Portal 服务器收到该注册报文，记录下接入设备的名称、地址转换后的 IP 地址以及端口号等信息后，后续这些信息用于与接入设备进行认证交互。接入设备通过定期发送注册报文更新 Portal 服务器上维护的注册信息。

需要注意的是，本功能仅用于和 CMCC 类型的 Portal 服务器配合使用。

【举例】

配置设备每隔 120 秒向 Portal 认证服务器发送注册报文。

```
<Sysname> system-view  
[Sysname] portal server pts  
[Sysname-portal-server-pts] server-register interval 120
```

【相关命令】

- `server-type`

1.1.48 server-type

`server-type` 命令用来配置 Portal 认证服务器或 Portal Web 服务器的类型。

undo server-type 命令用来恢复缺省情况。

【命令】

```
server-type { cmcc | imc }  
undo server-type
```

【缺省情况】

Portal 认证服务器或 Portal Web 服务器的类型为 iMC 服务器。

【视图】

Portal 认证服务器视图

Portal Web 服务器视图

【缺省用户角色】

network-admin

【参数】

cmcc: 表示 Portal 服务器类型为符合中国移动标准规范的服务器。

imc: 表示 Portal 服务器类型为符合 iMC 标准规范的服务器。

【使用指导】

设备配置的 Portal 服务器类型必须保证与设备所使用的服务器类型保持一致。

【举例】

```
# 配置 Portal 认证服务器类型为 imc。  
<Sysname> system-view  
[Sysname] portal server pts  
[Sysname-portal-server-pts] server-type imc  
# 配置 Portal Web 服务器类型为 imc。  
<Sysname> system-view  
[Sysname] portal web-server pts  
[Sysname-portal-websvr-pts] server-type imc
```

【相关命令】

- **display portal server**

1.1.49 tcp-port

tcp-port 命令用来配置本地 Portal Web 服务的 HTTP/HTTPS 服务侦听的 TCP 端口号。

undo tcp-port 命令用来恢复缺省情况。

【命令】

```
tcp-port port-number  
undo tcp-port
```

【缺省情况】

HTTP 服务侦听的 TCP 端口号为 80，HTTPS 服务侦听的 TCP 端口号为 **portal local-web-serve** 命令指定的 TCP 端口号。

【视图】

本地 Portal Web 服务视图

【缺省用户角色】

network-admin

【参数】

port-number: 表示侦听的 TCP 端口号，取值范围为 1～65535。

【使用指导】

接口上指定的 Portal Web 服务器的 URL 中配置的端口号，应该与本地 Portal Web 服务视图下指定的侦听端口号保持一致。

配置本地 Portal Web 服务的 HTTP/HTTPS 服务侦听的 TCP 端口号时，需要注意的是：

- 除了 HTTP 和 HTTPS 协议默认的端口号，本地 Portal Web 服务的 TCP 端口号不能与知名协议使用的端口号配置一致，如 FTP 的端口号 21；Telnet 的端口号 23，否则会造成本地 Web Server 无法收到用户的认证或下线请求数据。
- 不能把使用 HTTP 协议的本地 Portal Web 服务侦听的 TCP 端口号配置成 HTTPS 的默认端口号 443，反之亦然。
- 使用 HTTP 协议和 HTTPS 协议的本地 Portal Web 服务侦听的 TCP 端口号不能配置一致，比如不能都配置为 8080，否则会导致本地 Web 服务无法正常使用。
- 如果本地 Portal Web 服务引用的 SSL 服务器端策略与 HTTPS 服务引用的 SSL 服务器端策略相同，则本地 Portal Web 服务使用的 TCP 端口号可以与 HTTPS 服务器使用的 TCP 端口号相同；否则使用 TCP 端口号不能相同。

【举例】

配置本地 Portal Web 服务的 HTTP 服务侦听的 TCP 端口号为 2331。

```
<Sysname> system-view
[Sysname] portal local-web-server http
[Sysname-portal-local-websvr-http] tcp-port 2331
```

【相关命令】

- **portal local-web-server**

1.1.50 url

url 命令用来指定 Portal Web 服务器的 URL。

undo url 命令用来恢复缺省情况。

【命令】

```
url url-string
undo url
```

【缺省情况】

未指定 Portal Web 服务器的 URL。

【视图】

Portal Web 服务器视图

【缺省用户角色】

network-admin

【参数】

url-string: Portal Web 服务器的 URL，为 1~256 个字符的字符串，区分大小写。

【使用指导】

本命令指定的 URL 是可用标准 HTTP 或者 HTTPS 协议访问的 URL，它以 `http://` 或者 `https://` 开头。如果该 URL 未以 `http://` 或者 `https://` 开头，则缺省认为是以 `http://` 开头。

若要对用户的 HTTPS 请求进行重定向，需要通过 `http-redirect https-port` 命令配置对 HTTPS 报文进行重定向的内部侦听端口号，具体介绍请参见“三层业务-IP 业务命令参考”中的“HTTP 重定向”。

【举例】

```
# 配置 Portal Web 服务器 wbs 的 URL 为 http://www.test.com/portal。  
<Sysname> system-view  
[Sysname] portal web-server wbs  
[Sysname-portal-websvr-wbs] url http://www.test.com/portal
```

【相关命令】

- `display portal web-server`

1.1.51 url-parameter

`url-parameter` 命令用来配置设备重定向给用户的 Portal Web 服务器的 URL 中携带的参数信息。

`undo url-parameter` 命令用来删除配置的 Portal Web 服务器 URL 携带的参数信息。

【命令】

```
url-parameter param-name { original-url | source-address | source-mac  
[ encryption { aes | des } key { cipher | simple } string ] | value expression }  
undo url-parameter param-name
```

【缺省情况】

未配置设备重定向给用户的 Portal Web 服务器的 URL 中携带的参数信息。

【视图】

Portal Web 服务器视图

【缺省用户角色】

network-admin

【参数】

param-name: URL 参数名，为 1~32 个字符的字符串，区分大小写。URL 参数名对应的参数内容由 *param-name* 后的参数指定。

original-url: 用户初始访问的 Web 页面的 URL。

source-address: 用户的 IP 地址。

source-mac: 用户的 MAC 地址。

encryption: 表示以密文的方式携带用户的 MAC 地址。

aes: 指定加密算法为 AES 算法。

des: 指定加密算法为 DES 算法。

cipher: 以密文方式设置密钥。

key: 指定加密密钥。

simple: 以明文方式设置密钥，该密钥将以密文形式存储。

string: 密钥字符串，区分大小写。密钥的长度范围和选择的加密方式有关。具体关系如下：

- 对于 **des cipher**，密钥为 41 个字符的字符串。
- 对于 **des simple**，密钥为 8 个字符的字符串。
- 对于 **aes cipher**，密钥为 1~73 个字符的字符串。
- 对于 **aes simple**，密钥为 1~31 个字符的字符串。

value expression: 自定义字符串，为 1~256 个字符的字符串，区分大小写。

【使用指导】

可以通过多次执行本命令配置多条参数信息。

对于同一个参数名 *param-name* 后的参数设置，最后配置的生效。

该命令用于配置用户访问 Portal Web 服务器时，要求携带的一些参数，比较常用的是要求携带用户的 IP 地址、MAC 地址、用户原始访问的 URL 信息。用户也可以手工指定，携带一些特定的字符信息。配置完成后，在设备给用户强制重定向 URL 时会携带这些参数，例如配置 Portal Web 服务器的 URL 为：<http://www.test.com/portal>，若同时配置如下两个参数信息：**url-parameter userip source-address** 和 **url-parameter userurl value http://www.abc.com/welcome**，则设备给源 IP 为 1.1.1.1 的用户重定向时回应的 URL 格式即为：<http://www.test.com/portal?userip=1.1.1.1&userurl=http://www.abc.com/welcome>。

param-name 这个 URL 参数名必须与具体应用环境中的 Portal 服务器所支持的 URL 参数名保持一致，不同的 Portal 服务器支持 URL 参数名是不一样的，请根据具体情况配置 URL 参数名。例如 iMC 服务器支持的 URL 参数名如下：

- **userurl:** 表示 **original-url**
- **userip:** 表示 **source-address**
- **usermac:** 表示 **source-mac**

在 Portal 服务器为 H3C 公司的 iMC 服务器的组网环境中，如果设备重定向给用户的 Portal Web 服务器的 URL 中需要携带用户的 IP 地址参数信息时，必须把 *param-name* 参数配置成 **userip**，否则，iMC 服务器不能识别用户的 IP 地址。

如果给某个参数配置了加密方式，则重定向 URL 中携带的将是其加密后的值。例如在上述配置的基础上，再配置 **url-parameter usermac source-mac encryption des key simple 12345678**，则设备给源 MAC 地址为 1111-1111-1111 的用户重定向时回应的 URL 格式即为：<http://www.test.com/portal?usermac=xxxxxxxxx&userip=1.1.1.1&userurl=http://www.test.com/welcome>，其中 xxxxxxxxx 为加密后的用户 mac 地址。

【举例】

为设备重定向给用户的 Portal Web 服务器 wbs 的 URL 中配置两个参数 userip 和 userurl，其值分别为用户 IP 地址和自定义字符串 http://www.abc.com/welcome。

```
<Sysname> system-view
[Sysname] portal web-server wbs
[Sysname-portal-websvr-wbs] url-parameter userip source-address
[Sysname-portal-websvr-wbs] url-parameter userurl value http://www.abc.com/welcome
```

为设备重定向给用户的 Portal Web 服务器 wbs 的 URL 中配置参数 usermac，其值为用户 mac 地址，并使用 des 算法进行加密。

```
<Sysname> system-view
[Sysname] portal web-server wbs
[Sysname-portal-websvr-wbs] url-parameter usermac source-mac encryption des key simple
12345678
```

【相关命令】

- **display portal web-server**
- **url**

1.1.52 user-sync

user-sync 命令用来配置开启 Portal 用户信息同步功能。

undo user-sync 命令用来关闭 Portal 用户信息同步功能。

【命令】

```
user-sync timeout timeout
undo user-sync
```

【缺省情况】

Portal 认证服务器的 Portal 用户信息同步功能处于关闭状态。

【视图】

Portal 认证服务器视图

【缺省用户角色】

network-admin

【参数】

timeout timeout: 检测用户同步报文的时间间隔，取值范围为 60~18000，单位为秒。

【使用指导】

配置此功能后，设备会响应并周期性地检测指定的 Portal 认证服务器发来的用户同步报文，以保持设备与该服务器上在线用户信息的一致性。

只有在支持 Portal 用户心跳功能（目前仅 iMC 的 Portal 认证服务器支持）的 Portal 认证服务器的配合下，本功能才有效。为了实现该功能，还需要在 Portal 认证服务器上选择支持用户心跳功能，且服务器上配置的用户心跳间隔要小于等于设备上配置的检测超时时间。

在设备上删除 Portal 认证服务器时将会同时删除该服务器的用户信息同步功能配置。

对同一服务器多次执行本命令，最后一次执行的命令生效。

对于设备上多余的用户信息，即在检测用户同步报文的时间间隔 *timeout* 到达后被判定为 Portal 认证服务器上已不存在的用户信息，设备会在 *timeout* 后的某时刻将其删除掉。

如果服务器同步过来的用户信息在设备上不存在，则设备会将这些用户的 IP 地址封装在用户心跳回应报文中发送给服务器，由服务器删除多余的用户。

【举例】

配置对 Portal 认证服务器 pts 的 Portal 用户信息同步功能，检测用户同步报文的时间间隔为 600 秒，如果设备中的某用户信息在 600 秒内未在该 Portal 认证服务器发送的同步报文中出现，设备将强制该用户下线。

```
<Sysname> system-view
[Sysname] portal server pts
[Sysname-portal-server-pts] user-sync timeout 600
```

【相关命令】

- `portal server`

1.1.53 web-redirect url

`web-redirect url` 命令用来配置 Web 重定向功能。

`undo web-redirect` 命令用来关闭 Web 重定向功能。

【命令】

```
web-redirect [ ipv6 ] url url-string [ interval interval ]
undo web-redirect [ ipv6 ]
```

【缺省情况】

Web 重定向功能处于关闭状态。

【视图】

接口视图

【缺省用户角色】

network-admin

【参数】

ipv6: 表示 IPv6 Web 重定向功能。若不指定该参数，则表示 IPv4 Web 重定向功能。

url url-string: Web 重定向的地址，即用户的 Web 访问请求被重定向的 URL 地址，为 1~256 个字符的字符串，必须是以 `http://` 或者 `https://` 开头的完整 URL 路径。

interval interval: 对用户访问的 Web 页面进行重定向的周期，取值范围为 60~86400，单位为秒，缺省值为 86400。

【使用指导】

接口上配置了 Web 重定向功能后，当该接口上接入的用户初次通过 Web 页面访问外网时，设备会将用户的初始访问页面重定向到指定的 URL 页面，之后用户才可以正常访问外网，经过一定时长 (*interval*) 后，设备又可以对用户要访问的网页或者正在访问的网页重定向到指定的 URL 页面。不能同时开启 Web 重定向功能和 Portal 功能，否则 Web 重定向功能失效。

Web 重定向功能仅对使用默认端口号 80 的 HTTP 协议报文生效。

【举例】

在接口 Vlan-interface100 上配置 IPv4 Web 重定向功能：Web 重定向地址为 http://192.0.0.1，Web 重定向周期为 3600 秒。

```
<Sysname> system-view
[Sysname] interface vlan-interface 100
[Sysname-Vlan-interface100] web-redirect url http://192.0.0.1 interval 3600
```

【相关命令】

- **display web-redirect rule**

目 录

1 Web认证.....	1-1
1.1 Web认证配置命令	1-1
1.1.1 display web-auth	1-1
1.1.2 display web-auth free-ip	1-2
1.1.3 display web-auth server	1-2
1.1.4 display web-auth user.....	1-3
1.1.5 ip	1-5
1.1.6 redirect-wait-time	1-6
1.1.7 url	1-6
1.1.8 url-parameter.....	1-7
1.1.9 web-auth auth-fail vlan.....	1-8
1.1.10 web-auth domain	1-9
1.1.11 web-auth enable	1-10
1.1.12 web-auth free-ip.....	1-10
1.1.13 web-auth max-user.....	1-11
1.1.14 web-auth offline-detect.....	1-12
1.1.15 web-auth proxy port.....	1-12
1.1.16 web-auth server.....	1-13

1 Web认证

1.1 Web认证配置命令

1.1.1 display web-auth

display web-auth 命令用来显示接口上 Web 认证的配置信息和运行状态信息。

【命令】

display web-auth [**interface** *interface-type interface-number*]

【视图】

任意视图

【缺省用户角色】

network-admin
network-operator

【参数】

interface interface-type interface-number: 显示指定接口上 Web 认证的配置信息。其中 *interface-type interface-number* 表示接口类型和接口编号。若不指定本参数，则显示设备上所有 Web 认证的配置信息。

【举例】

显示接口 GigabitEthernet1/0/1 上 Web 认证的配置信息。

```
<Sysname> display web-auth interface gigabitethernet 1/0/1
Global Web-auth parameters  :
Proxy Port Numbers          : Not configured
Total online web-auth users: 1
GigabitEthernet1/0/1  is link-up
Port role                    : Authenticator
Web-auth domain              : my-domain
Auth-Fail VLAN               : Not configured
Offline-detect               : Not configured
Max online users              : 1024
Web-auth enable               : Enabled

Total online web-auth users: 1
```

表1-1 display web-auth 命令显示信息描述表

字段	描述
Global Web-auth parameters	全局Web认证参数
Proxy Port Numbers	Web代理服务器端口
Total online web-auth users	全局Web认证的在线用户数

字段	描述
GigabitEthernet1/0/1 is link-up	接口GigabitEthernet1/0/1的状态，包括如下取值： <ul style="list-style-type: none"> link-up: 接口管理状态和物理状态均为开启 link-down: 接口处于关闭状态
Port role	该端口担当认证端的作用，目前仅支持作为认证端
Web-auth domain	Web认证用户使用的ISP域
Auth-fail VLAN	Web认证的认证失败VLAN，如果没有配置，则显示Not configured
Offline-detect	Web认证用户在线检测的时间间隔，Not configured表示Web认证用户在线检测功能处于关闭状态
Max online users	允许同时接入的Web认证最大用户数
Web-auth enable	Web认证功能的开启状态，包括如下取值： <ul style="list-style-type: none"> Enabled: 开启 Disabled: 关闭
Total online web-auth users	接口下Web认证的在线用户数

1.1.2 display web-auth free-ip

display web-auth free-ip 命令用来显示所有 Web 认证用户免认证的目的 IP 地址。

【命令】

display web-auth free-ip

【视图】

任意视图

【缺省用户角色】

network-admin
network-operator

【举例】

显示所有 Web 认证用户免认证的目的 IP 地址。

```
<Sysname> display web-auth free-ip
Free IP
      : 1.1.0.0      255.255.0.0
      : 1.2.0.0      255.255.0.0
```

【相关命令】

- web-auth free-ip**

1.1.3 display web-auth server

display web-auth server 命令用来显示 Web 认证服务器信息。

【命令】

display web-auth server [*server-name*]

【视图】

任意视图

【缺省用户角色】

network-admin
network-operator

【参数】

server-name: Web 认证服务器的名称，为 1~32 个字符的字符串，区分大小写。若不指定此参数，则显示设备上所有 Web 认证服务器的信息。

【举例】

显示 Web 认证服务器 aaa 的信息。

```
<Sysname> display web-auth server aaa
Web-auth server: aaa
  IP                : 8.8.8.8
  Port              : 80
  URL               : http://8.8.8.8/portal/
  Redirect-wait-time : 5
  URL parameters    : Not configured
```

表1-2 display web-auth server 命令显示信息描述表

字段	描述
Web-auth server	Web认证服务器名称
IP	Web认证服务器的IP地址
Port	Web认证服务器的端口号
URL	Web认证服务器的重定向URL
Redirect-wait-time	Web认证成功，认证页面跳转的时间间隔
URL parameters	设备重定向给用户的URL中携带的参数信息

1.1.4 display web-auth user

display web-auth user 命令用来显示在线 Web 认证用户的信息。

【命令】

display web-auth user [**interface** *interface-type interface-number* | **slot** *slot-number*]

【视图】

任意视图

【缺省用户角色】

network-admin
network-operator

【参数】

interface *interface-type interface-number*: 显示指定接口上在线 Web 认证用户的信息。其中 *interface-type interface-number* 表示接口类型和接口编号。若不指定该参数，则表示设备上所有接口上在线用户的信息。

slot *slot-number*: 显示指定成员设备上所有接口在线 Web 认证用户的信息。*slot-number* 表示设备在 IRF 中的成员编号。若不指定该参数，则表示所有成员设备上在线 Web 认证用户的信息。

【举例】

```
# 显示接口 GigabitEthernet1/0/1 上在线用户的信息。
<Sysname> display web-auth user interface gigabitethernet 1/0/1
    Total online web-auth users: 1

User name: user1
    MAC address: 0000-2700-b076
    Access interface: GigabitEthernet1/0/1
    Initial VLAN: 1
    Authorization VLAN: N/A
    Authorization ACL ID: N/A
    Authorization user profile: N/A
```

表1-3 display web-auth user 命令显示信息描述表

字段	描述
Total online web-auth users	在线用户总数
User name	在线用户的用户名
MAC address	在线用户的MAC地址
Access interface	在线用户接入的接口
Initial VLAN	初始的VLAN
Authorization VLAN	授权的VLAN
Authorization ACL ID	授权ACL编号
Authorization user profile	Web认证用的授权User profile名称。若未授权User profile，则显示为N/A。授权状态包括如下： <ul style="list-style-type: none">active: AAA 授权 User profile 成功inactive: AAA 授权 User profile 失败或者设备上不存在该 User profile

1.1.5 ip

ip 命令用来配置 Web 认证服务器的 IP 地址。

undo ip 命令用来恢复缺省情况。

【命令】

```
ip ipv4-address port port-number  
undo ip
```

【缺省情况】

不存在 Web 认证服务器的 IP 地址。

【视图】

Web 认证服务器视图

【缺省用户角色】

network-admin

【参数】

ipv4-address: 表示 Web 认证服务器的 IPv4 地址，该地址为接入设备上一个与 Web 认证用户路由可达的三层接口 IP 地址。

port port-number: 指定 Web 认证服务器的端口。**port-number** 是端口号，取值范围为 1～65535。

【使用指导】

配置 Web 认证服务器的 IP 地址，建议使用设备上空闲的 Loopback 接口的 IP 地址，使用 LoopBack 接口有如下优点：

- 状态稳定，可避免因接口故障导致用户无法打开认证页面的问题。
- 由于发送到 LoopBack 接口的报文不会被转发到网络中，当请求上线的用户数目较大时，可减轻对系统性能的影响。

此命令配置的端口号必须与本地 Portal Web 服务中配置的侦听端口号保持一致。有关本地 Portal Web 服务的详细介绍请参见“安全配置指导”中的“Portal”。

同一个 Web 认证服务器视图下多次执行本命令，最后一次执行的命令生效。

【举例】

进入 Web 认证服务器视图。

```
<Sysname> system-view
```

```
[Sysname] web-auth server wbs
```

配置 Web 认证服务器 wbs 的 IP 地址为 192.168.1.1，端口为 8080。

```
[Sysname-web-auth-server-wbs] ip 192.168.1.1 port 8080
```

【相关命令】

- **url**
- **tcp-port**（安全命令参考/Portal）

1.1.6 redirect-wait-time

redirect-wait-time 命令用来配置认证页面跳转的时间间隔。

undo redirect-wait-time 命令用来恢复缺省情况。

【命令】

redirect-wait-time *period*

undo redirect-wait-time

【缺省情况】

Web 认证用户认证成功后认证页面跳转的时间间隔为 5 秒。

【视图】

Web 认证服务器视图

【缺省用户角色】

network-admin

【参数】

period: 表示自 Web 认证用户认证成功后，当前认证页面开始跳转到其他页面的时间间隔，取值范围为 1~90，单位为秒。

【使用指导】

在某些应用环境中，客户端在 Web 认证成功后需要更新 IP 地址，为了避免客户端 IP 地址还未完成更新而无法打开跳转的网站页面，需要适当增加页面跳转的时间间隔，保证认证页面跳转的时间间隔大于客户端更新 IP 地址的时间。

【举例】

配置 Web 认证用户认证成功后认证页面跳转的时间间隔 10 秒。

```
<Sysname> system-view
```

```
[Sysname] web-auth server wbs
```

```
[Sysname-web-auth-server-wbs] redirect-wait-time 10
```

1.1.7 url

url 命令用来配置 Web 认证服务器的重定向 URL。

undo url 命令用来恢复缺省情况。

【命令】

url *url-string*

undo url

【缺省情况】

不存在 Web 认证服务器的重定向 URL。

【视图】

Web 认证服务器视图

【缺省用户角色】

network-admin

【参数】

url-string: 表示 Web 认证服务器的重定向 URL，为 1~256 个字符的字符串，区分大小写。

【使用指导】

本命令配置的 Web 认证服务器重定向 URL 是可以用标准 HTTP 或者 HTTPS 协议访问的 URL，它必须以 http://或者 https://开头。如果该 URL 未以 http://或者 https://开头，则系统默认其以 http://开头。

该 URL 中的 IP 地址和端口号必须与 Web 认证服务器中的 IP 地址和端口号保持一致。

【举例】

配置 Web 认证服务器 wbs 的重定向 URL 为 http://192.168.1.1:80/portal/。

```
<Sysname> system-view
[Sysname] web-auth server wbs
[Sysname-web-auth-server-wbs] url http://192.168.1.1:80/portal/
```

【相关命令】

- **ip**
- **tcp-port**（安全命令参考/Portal）

1.1.8 url-parameter

url-parameter 命令用来配置设备重定向给用户的 URL 中携带的参数信息。

undo url-parameter 命令用来删除配置的设备重定向给用户的 URL 中携带的参数信息。

【命令】

```
url-parameter parameter-name { original-url | source-address | source-mac |  
value expression }  
undo url-parameter parameter-name
```

【缺省情况】

未配置设备重定向给用户的 URL 中携带的参数信息。

【视图】

Web 认证服务器视图

【缺省用户角色】

network-admin

【参数】

parameter-name: 表示 URL 中携带参数的名称，为 1~32 个字符的字符串，区分大小写。URL 参数名对应的参数内容由 **parameter-name** 后的参数指定。

original-url: 用户初始访问的 Web 页面的 URL。

source-address: 用户的 IP 地址。

source-mac: 用户的 MAC 地址。

value expression: 自定义字符串，为 1~256 个字符的字符串，区分大小写。

【使用指导】

可以通过多次执行本命令配置多条参数信息。

多次执行本命令且参数名 *parameter-name* 都相同，则最后一次执行的命令生效

该命令用于配置用户访问 Web 认证服务器时，要求携带的一些参数，比较常用的是要求携带用户的 IP 地址、MAC 地址、用户原始访问的 URL 信息。用户也可以手工指定，携带一些特定的字符信息。配置完成后，在设备给用户强制推送重定向 URL 时会携带这些参数，例如用户的源 IP 地址的 1.1.1.1，配置 Web 认证服务器的 URL 为：http://192.168.1.1/portal，若同时配置如下两个参数信息：**url-parameter userip source-address** 和 **url-parameter userurl value http://www.abc.com/welcome**，则设备给该用户重定向的 URL 格式即为：
http://192.168.1.1/portal?userip=1.1.1.1&userurl=http://www.abc.com/welcome。

param-name 这个 URL 参数名必须与 PC 浏览器所接受的参数名保持一致，请根据具体情况配置 URL 参数名。

【举例】

为设备重定向给用户的 Portal Web 服务器 wbs 的 URL 中配置两个参数 **userip** 和 **userurl**，其值分别为用户 IP 地址和自定义字符串 http://www.abc.com/welcome。

```
<Sysname> system-view
[Sysname] web-auth server wbs
[Sysname-web-auth-server-wbs] url-parameter userip source-address
[Sysname-web-auth-server-wbs] url-parameter userurl value http://www.abc.com/welcome
```

1.1.9 web-auth auth-fail vlan

web-auth auth-fail vlan 命令用来配置 Web 认证的 Auth-Fail VLAN。

undo web-auth auth-fail vlan 命令用来恢复缺省情况。

【命令】

```
web-auth auth-fail vlan authfail-vlan-id
undo web-auth auth-fail vlan
```

【缺省情况】

不存在 Web 认证的 Auth-Fail VLAN。

【视图】

二层以太网接口视图

【缺省用户角色】

network-admin

【参数】

authfail-vlan-id: 表示 Web 认证的 Auth-Fail VLAN ID，取值范围为 1~4094，该 VLAN 必须已经存在。

【使用指导】

接口上配置此功能后，认证失败的 Web 认证用户可以访问 Auth-Fail VLAN 中的资源。

为使此功能生效，必须开启二层以太网接口上的 MAC VLAN 功能，并将 Auth-Fail VLAN 的网段设为 Web 认证用户免认证的目的 IP 地址。

因为 MAC VLAN 功能仅在 Hybrid 端口上生效，所以 Web 认证的 Auth-Fail VLAN 功能也只能在 Hybrid 端口上生效。

当用户认证失败后，设备将 Web 认证用户的 MAC 地址与 Auth-fail VLAN 进行绑定。

禁止删除已被配置为 Web 认证 Auth-Fail VLAN 的 VLAN，若要删除该 VLAN，请先通过 **undo web-auth auth-fail vlan** 命令取消 Web 认证的 Auth-Fail VLAN 配置。

【举例】

配置接口 GigabitEthernet1/0/1 上的 Web 认证的 Auth-Fail VLAN 为 VLAN 5。

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] port link-type hybrid
[Sysname-GigabitEthernet1/0/1] mac-vlan enable
[Sysname-GigabitEthernet1/0/1] web-auth auth-fail vlan 5
```

【相关命令】

- **display web-auth**

1.1.10 web-auth domain

web-auth domain 命令用来指定 Web 认证用户使用的认证域。

undo web-auth domain 命令用来恢复缺省情况。

【命令】

```
web-auth domain domain-name
undo web-auth domain
```

【缺省情况】

未指定 Web 认证用户认证使用的认证域。

【视图】

二层以太网接口视图

【缺省用户角色】

network-admin

【参数】

domain-name: ISP 认证域名，为 1~255 个字符的字符串，不区分大小写。

【使用指导】

在接口上执行此命令后，使得所有从该接口接入的 Web 认证用户强制使用该认证域。

【举例】

指定从接口 GigabitEthernet1/0/1 上接入的 Web 认证用户使用认证域为 my-domain。

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] web-auth domain my-domain
```

1.1.11 web-auth enable

web-auth enable 命令用来开启 Web 认证功能。

undo web-auth enable 命令用来关闭 Web 认证功能。

【命令】

web-auth enable apply server *server-name*

undo web-auth enable

【缺省情况】

Web 认证功能处于关闭状态。

【视图】

二层以太网接口视图

【缺省用户角色】

network-admin

【参数】

server-name: 表示引用的 Web 认证服务器的名称，为 1~32 个字符的字符串，区分大小写。

【使用指导】

此命令用来开启 Web 认证功能，并指定引用的 Web 认证服务器。

为使 Web 认证功正常运行，在接入设备的二层以太网接口上开启 Web 认证功能后，请不要再在此接口上开启端口安全功能和配置端口安全模式。

【举例】

在接口 GigabitEthernet1/0/1 上开启 Web 认证功能，并指定引用的 Web 认证服务器为 wbs。

```
<Sysname> system-view
```

```
[Sysname] interface gigabitethernet 1/0/1
```

```
[Sysname-GigabitEthernet1/0/1] web-auth enable apply server wbs
```

【相关命令】

- **web-auth server**

1.1.12 web-auth free-ip

web-auth free-ip 命令用来配置 Web 认证用户免认证目的 IP 地址。

undo web-auth free-ip 命令用来恢复缺省情况。

【命令】

web-auth free-ip *ip-address* { *mask-length* | *mask* }

undo web-auth free-ip { *ip-address* { *mask-length* | *mask* } | **all** }

【缺省情况】

不存在 Web 认证用户免认证的目的 IP 地址。

【视图】

系统视图

【缺省用户角色】

network-admin

【参数】

ip-address: Web 认证用户免认证目的网段的 IP 地址。

mask-length: Web 认证用户免认证目的网段 IP 地址的掩码长度，取值范围为 1~32。

mask: Web 认证用户免认证目的网段 IP 地址的子网掩码，点分十进制格式。

all: Web 认证用户可免认证访问的所有网段。

【使用指导】

在设备上执行此命令后，Web 认证用户无需认证即可访问此命令指定 IP 地址网段中的资源。

可通过重复执行此命令来配置多个 Web 认证用户免认证的目的 IP 地址。

【举例】

配置 Web 认证用户免认证的目的 IP 地址为 192.168.0.0/24。

```
<Sysname> system-view
```

```
[Sysname] web-auth free-ip 192.168.0.0 24
```

1.1.13 web-auth max-user

web-auth max-user 命令用来配置 Web 认证最大用户数。

undo web-auth max-user 命令用来恢复缺省情况。

【命令】

web-auth max-user *max-number*

undo web-auth max-user

【缺省情况】

接口上同时可接入的 Web 认证最大用户数为 1024。

【视图】

二层以太网接口视图

【缺省用户角色】

network-admin

【参数】

max-number: 表示接口上同时可接入的 Web 认证最大用户数，取值范围为 1~2048。

【使用指导】

若配置的 Web 认证最大用户数小于当前已经在线的 Web 认证用户数，则该命令可以执行成功，且在线 Web 认证用户不受影响，但系统将不允许新的 Web 认证用户接入。

该命令指定的最大用户数仅为 IPv4 Web 认证用户数。

【举例】

在接口 GigabitEthernet1/0/1 上配置 Web 认证最大用户数为 32。

```
<Sysname> system-view
```

```
[Sysname] interface gigabitethernet 1/0/1
```

```
[Sysname-GigabitEthernet1/0/1] web-auth max-user 32
```

【相关命令】

- **display web-auth**

1.1.14 web-auth offline-detect

web-auth offline-detect 命令用来开启 Web 认证用户的在线检测功能。

undo web-auth offline-detect 命令用来关闭 Web 认证用户的在线检测功能。

【命令】

```
web-auth offline-detect interval interval
```

```
undo web-auth offline-detect interval
```

【缺省情况】

Web 认证用户在线检测功能处于关闭状态。

【视图】

二层以太网接口视图

【缺省用户角色】

network-admin

【参数】

interval: 指定用户在线检测时间间隔，取值范围为 60~65535，单位为秒。

【使用指导】

开启端口的 Web 认证用户的在线检测功能后，若设备在一个在线检测时间间隔之内，未收到此端口下某在线用户的报文，则将切断该用户的连接，同时通知 RADIUS 服务器停止对此用户进行计费。配置用户在线检测时间间隔时，需要与 MAC 地址老化时间配成相同时间，否则会导致用户异常下线。

【举例】

在接口 GigabitEthernet1/0/1 上开启 Web 认证用户的在线检测功能，并指定在线检测的时间间隔为 3600 秒。

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] web-auth offline-detect interval 3600
```

1.1.15 web-auth proxy port

web-auth proxy port 命令用来配置允许触发 Web 认证的 Web 代理服务器端口。

undo web-auth proxy port 命令用来删除指定的或所有的 Web 认证的 Web 代理服务器端口。

【命令】

```
web-auth proxy port port-number
```

```
undo web-auth proxy port { port-number | all }
```

【缺省情况】

不存在 Web 认证的 Web 代理服务器端口。

【视图】

系统视图

【缺省用户角色】

network-admin

【参数】

port-number: Web 认证的 Web 代理服务器的 TCP 端口号，取值范围为 1~65535。

all: 指定所有 Web 认证的 Web 代理服务器的 TCP 端口号。

【使用指导】

设备默认只允许未配置 Web 代理服务器的浏览器发起的 HTTP 请求才能触发 Portal 认证。当用户上网使用的浏览器配置了 Web 代理服务器时，用户的 HTTP 请求报文将被丢弃，而不能触发 Web 认证。在这种情况下，网络管理员可以通过在设备上添加 Web 认证的 Web 代理服务器的 TCP 端口号，来允许配置了 Web 代理服务器的浏览器发起的 HTTP 请求也可以触发 Web 认证。

多次配置本命令可以添加多个 Web 认证的 Web 代理服务器的 TCP 端口号。

配置 Web 认证的 Web 代理服务器的 TCP 端口号，需要注意的是：

- 如果用户浏览器采用 WPAD（Web Proxy Auto-Discovery，Web 代理服务器自动发现）方式自动配置 Web 代理，则不仅需要网络管理员在设备上添加 Web 代理服务器端口，还需要将 WPAD 主机的 IP 地址配置为 Web 认证用户免认证的目的 IP 地址。
- 除了网络管理员需要在设备上添加指定的 Web 代理服务器端口，还需要用户在浏览器上将接入设备上 Web 认证服务器的 IP 地址加入到 Web 代理服务器的例外情况中，使 Web 认证服务器的 IP 地址不使用 Web 代理服务器，避免 Web 认证用户发送给 Web 认证页面的 HTTP 报文被发送到 Web 代理服务器上，从而影响正常的 Web 认证。

【举例】

配置 Web 认证的 Web 代理服务器的 TCP 端口号为 7777。

```
<Sysname> system-view  
[Sysname] web-auth proxy port 7777
```

1.1.16 web-auth server

web-auth server 命令用来创建 Web 认证服务器，并进入 Web 认证服务器视图。如果指定的 Web 认证服务器已经存在，则直接进入 Web 认证服务器视图。

undo web-auth server 命令用来删除指定的 Web 认证服务器。

【命令】

```
web-auth server server-name  
undo web-auth server server-name
```

【缺省情况】

不存在 Web 认证服务器。

【视图】

系统视图

【缺省用户角色】

network-admin

【参数】

server-name: 表示 Web 认证服务器的名称，为 1~32 个字符的字符串，区分大小写。

【使用指导】

在 Web 认证服务器视图下可以配置 Web 认证服务器侦听的 IP 地址、重定向 URL 及其重定向 URL 中携带的参数信息。

【举例】

创建名称为 wbs 的 Web 认证服务器，并进入 Web 认证服务器视图。

```
<Sysname> system-view
[Sysname] web-auth server wbs
[Sysname-web-auth-server-wbs]
```

【相关命令】

- **web-auth enable apply server**

目 录

1 端口安全	1-1
1.1 端口安全配置命令	1-1
1.1.1 display port-security	1-1
1.1.2 display port-security mac-address block	1-4
1.1.3 display port-security mac-address security	1-5
1.1.4 port-security access-user log enable	1-6
1.1.5 port-security authentication open	1-7
1.1.6 port-security authentication open global	1-8
1.1.7 port-security authorization ignore	1-9
1.1.8 port-security authorization-fail offline	1-10
1.1.9 port-security enable	1-11
1.1.10 port-security intrusion-mode	1-11
1.1.11 port-security mac-address aging-type inactivity	1-12
1.1.12 port-security mac-address dynamic	1-13
1.1.13 port-security mac-address security	1-14
1.1.14 port-security mac-limit	1-16
1.1.15 port-security mac-move permit	1-17
1.1.16 port-security max-mac-count	1-18
1.1.17 port-security nas-id-profile	1-19
1.1.18 port-security ntk-mode	1-19
1.1.19 port-security oui	1-20
1.1.20 port-security port-mode	1-21
1.1.21 port-security timer autolearn aging	1-23
1.1.22 port-security timer disableport	1-24
1.1.23 snmp-agent trap enable port-security	1-25

1 端口安全

1.1 端口安全配置命令

1.1.1 display port-security

display port-security 命令用来显示端口安全的配置信息、运行情况和统计信息。

【命令】

display port-security [**interface** *interface-type interface-number*]

【视图】

任意视图

【缺省用户角色】

network-admin
network-operator

【参数】

interface interface-type interface-number: 显示指定端口的端口安全相关信息。
interface-type interface-number 表示端口类型和端口编号。若不指定本参数，则显示所有端口的端口安全信息。

【举例】

显示所有端口的端口安全相关状态。

```
<Sysname> display port-security
Global port security parameters:
  Port security           : Enabled
  AutoLearn aging time   : 0 min
  Disableport timeout    : 20 s
  MAC move                : Denied
  Authorization fail      : Online
  NAS-ID profile          : Not configured
  Dot1x-failure trap     : Disabled
  Dot1x-logon trap       : Disabled
  Dot1x-logoff trap      : Enabled
  Intrusion trap         : Disabled
  Address-learned trap   : Enabled
  Mac-auth-failure trap  : Disabled
  Mac-auth-logon trap    : Enabled
  Mac-auth-logoff trap   : Disabled
  Open authentication    : Disabled
  OUI value list         :
    Index : 1           Value : 123401
```

GigabitEthernet1/0/1 is link-up

```

Port mode                : userLogin
NeedToKnow mode          : Disabled
Intrusion protection mode : NoAction
Security MAC address attribute
    Learning mode         : Sticky
    Aging type            : Periodical
Max secure MAC addresses  : 32
Current secure MAC addresses : 0
Authorization             : Permitted
NAS-ID profile            : Not configured
Free VLANs               : Not configured
Open authentication       : Disabled

```

表1-1 display port-security 命令显示信息描述表

字段	描述
Port security	端口安全的开启状态
AutoLearn aging time	Sticky MAC地址的老化时间，单位为分钟或秒
Disableport timeout	收到非法报文的端口暂时被关闭的时间，单位为秒
MAC move	MAC迁移功能的开启状态 <ul style="list-style-type: none"> 如果 MAC 迁移功能处于开启状态，则显示 Permitted 如果 MAC 迁移功能处于关闭状态，则显示 Denied
Authorization fail	授权失败后用户的状态，包括下线（Offline）和保持在线（Online）两种类型
NAS-ID profile	全局引用的NAS-ID Profile
Dot1x-failure trap	802.1X用户认证失败的告警功能开启状态
Dot1x-logon trap	802.1X用户认证成功的告警功能开启状态
Dot1x-logoff trap	802.1X用户认证下线的告警功能开启状态
Intrusion trap	发现非法报文的告警功能开启状态
Address-learned trap	端口学习到新MAC地址的告警功能开启状态
Mac-auth-failure trap	MAC地址认证用户认证失败的告警功能开启状态
Mac-auth-logon trap	MAC地址认证用户认证成功的告警功能开启状态
Mac-auth-logoff trap	MAC地址认证用户认证下线的告警功能开启状态
Open authentication	端口安全全局开放认证模式功能开启状态 <ul style="list-style-type: none"> Enabled: 打开 Disabled: 关闭
OUI value list	允许通过认证的用户的24位OUI值
Index	OUI的索引
Value	OUI值

字段	描述
Port mode	<p>端口安全模式，包括以下几种：</p> <ul style="list-style-type: none"> • noRestriction • autoLearn • macAddressWithRadius • macAddressElseUserLoginSecure • macAddressElseUserLoginSecureExt • secure • userLogin • userLoginSecure • userLoginSecureExt • macAddressOrUserLoginSecure • macAddressOrUserLoginSecureExt • userLoginWithOUI <p>关于各模式的具体涵义，请参考端口安全配置手册</p>
NeedToKnow mode	<p>Need To Know模式，包括以下几种：</p> <ul style="list-style-type: none"> • NeedToKnowOnly: 表示仅允许目的 MAC 地址为已通过认证的 MAC 地址的单播报文通过 • NeedToKnowWithBroadcast: 允许目的 MAC 地址为已通过认证的 MAC 地址的单播报文或广播地址的报文通过 • NeedToKnowWithMulticast: 允许目的 MAC 地址为已通过认证的 MAC 地址的单播报文，广播地址或组播地址的报文通过 • Disabled: 表示不进行 NTK 处理
Intrusion protection mode	<p>入侵检测特性模式，包括以下几种：</p> <ul style="list-style-type: none"> • BlockMacAddress: 表示将非法报文的源 MAC 地址加入阻塞 MAC 地址列表中 • DisablePort: 表示将收到非法报文的端口永久关闭 • DisablePortTemporarily: 表示将收到非法报文的端口暂时关闭一段时间 • NoAction: 表示不进行入侵检测处理
Security MAC address attribute	安全MAC地址的相关属性
Security MAC address learning mode	<p>安全MAC地址的学习方式：</p> <ul style="list-style-type: none"> • Dynamic: 动态类型 • Sticky: Sticky 类型
Security MAC address aging type	<p>安全MAC地址的老化方式：</p> <ul style="list-style-type: none"> • Periodical: 按照配置的老化时间间隔进行老化 • Inactivity: 无流量命中时老化
Max secure MAC addresses	端口安全允许的最大安全MAC地址数目或上线用户数
Current secure MAC addresses	端口下保存的安全MAC地址数目

字段	描述
Authorization	服务器的授权信息是否被忽略 <ul style="list-style-type: none"> Permitted: 表示当前端口应用 RADIUS 服务器或本地设备下发的授权信息 Ignored: 表示当前端口不应用 RADIUS 服务器或本地设备下发的授权信息
NAS-ID profile	端口下引用的 NAS-ID Profile
Free VLANs	(暂不支持) 端口上配置的无需认证的VLAN, 如果没有配置, 则显示 Not configured
Open authentication	端口安全端口开放认证模式功能开启状态 <ul style="list-style-type: none"> Enabled: 打开 Disabled: 关闭

1.1.2 display port-security mac-address block

display port-security mac-address block 命令用来显示阻塞 MAC 地址信息。

【命令】

```
display port-security mac-address block [ interface interface-type
interface-number ] [ vlan vlan-id ] [ count ]
```

【视图】

任意视图

【缺省用户角色】

network-admin
network-operator

【参数】

interface *interface-type* *interface-number*: 显示指定端口的阻塞 MAC 地址信息。
interface-type *interface-number* 表示端口类型和端口编号。

vlan *vlan-id*: 显示指定 VLAN 的阻塞 MAC 地址信息。其中, *vlan-id* 表示 VLAN 编号, 取值范围为 1~4094。

count: 显示阻塞 MAC 地址的个数。

【使用指导】

如果不指定任何参数, 则显示所有阻塞 MAC 地址的信息。

【举例】

显示所有阻塞 MAC 地址。

```
<Sysname> display port-security mac-address block
MAC ADDR          Port          VLAN ID
000f-3d80-0d2d    GE1/0/1      30

--- On slot 1, 1 MAC address(es) found ---
```

```

--- 1 mac address(es) found ---
# 显示所有阻塞 MAC 地址计数。
<Sysname> display port-security mac-address block count

--- On slot 1, 1 MAC address(es) found ---

```

```

--- 1 mac address(es) found ---

```

表1-2 display port-security mac-address block 命令显示信息描述表

字段	描述
MAC ADDR	阻塞MAC地址
Port	阻塞MAC地址所在端口
VLAN ID	端口所属VLAN
<i>number</i> mac address(es) found	当前阻塞MAC地址数目为 <i>number</i> 个

【相关命令】

- **port-security intrusion-mode**

1.1.3 display port-security mac-address security

display port-security mac-address security 命令用来显示安全 MAC 地址信息。

【命令】

```

display port-security mac-address security [ interface interface-type
interface-number ] [ vlan vlan-id ] [ count ]

```

【视图】

任意视图

【缺省用户角色】

```

network-admin
network-operator

```

【参数】

interface interface-type interface-number: 显示指定端口的安全 MAC 地址信息。其中，*interface-type interface-number* 表示端口类型和端口编号。

vlan vlan-id: 显示指定 VLAN 的安全 MAC 地址信息。其中，*vlan-id* 表示 VLAN 编号，取值范围为 1~4094。

count: 统计符合条件的安全 MAC 地址个数。

【使用指导】

当端口工作于 **autoLearn** 模式时，端口上通过自动学习或者静态配置的安全 MAC 地址可通过该命令查看。

如果不指定任何参数，则显示所有安全 MAC 地址的信息。

【举例】

显示所有安全 MAC 地址。

```
<Sysname> display port-security mac-address security
MAC ADDR          VLAN ID  STATE          PORT INDEX          AGING TIME
0002-0002-0002    1        Security       GE1/0/1             Not aged

--- Number of secure MAC addresses: 1 ---
```

显示所有安全 MAC 地址计数。

```
<Sysname> display port-security mac-address security count

--- Number of secure MAC addresses: 1 ---
```

表1-3 display port-security mac-address security 命令显示信息描述表

字段	描述
MAC ADDR	安全MAC地址
VLAN ID	端口所属VLAN
STATE	添加的MAC地址类型 <ul style="list-style-type: none">Security: 表示该项是安全 MAC 地址
Port INDEX	安全MAC地址所在端口
AGING TIME	安全MAC地址的剩余存活时间 <ul style="list-style-type: none">对于静态 MAC 地址，显示为 Not aged对于 Sticky MAC 地址，显示为具体的剩余存活时间，当存活时间小于 60 秒，显示单位为秒；当存活时间大于等于 60 秒时，显示单位为分钟。缺省情况下为不进行老化，显示为 Not aged
Number of secure MAC addresses	当前保存的安全MAC地址数

【相关命令】

- port-security mac-address security

1.1.4 port-security access-user log enable

port-security access-user log enable 命令用来开启端口安全接入用户日志信息功能。
undo port-security access-user log enable 命令用来关闭端口安全接入用户日志信息功能。

【命令】

```
port-security access-user log enable [ failed-authorization | mac-learning  
| violation ] *  
undo port-security access-user log enable [ failed-authorization |  
mac-learning | violation ] *
```

【缺省情况】

端口安全接入用户日志信息功能处于关闭状态。

【视图】

系统视图

【缺省用户角色】

network-admin

【参数】

failed-authorization: 802.1X 或 MAC 地址认证用户授权失败时的日志信息。

mac-learning: 端口自动学习到 MAC 地址时的日志信息。

violation: 端口安全入侵检测功能被触发时的日志信息。

【使用指导】

为了防止设备输出过多的端口安全接入用户日志信息，一般情况下建议关闭此功能。

配置本命令时，如果未指定任何参数，将同时开启或关闭本命令所有参数对应日志功能。

【举例】

开启端口安全入侵检测功能被触发时的日志信息。

```
<Sysname> system-view
```

```
[Sysname] port-security access-user log enable violation
```

【相关命令】

- **info-center source portsec logfile deny**（网络管理和监控/信息中心）

1.1.5 port-security authentication open

port-security authentication open 命令用来开启端口上端口安全的开放认证模式。

undo port-security authentication open 命令用来关闭端口上端口安全的开放认证模式。

【命令】

```
port-security authentication open
```

```
undo port-security authentication open
```

【缺省情况】

端口上的端口安全开放认证模式处于关闭状态。

【视图】

二层以太网接口视图

【缺省用户角色】

network-admin

【使用指导】

开启端口上的端口安全开放认证模式后，端口上的 802.1X、MAC 地址认证用户即使身份信息不正确（包含不存在的用户名或者错误的密码两种情况）也可以正常接入并访问网络。在这种模式下接

入的用户被称为 open 用户，此类用户不支持授权和计费，但可通过 **display dot1x connection open**、**display mac-authentication connection open** 命令查看相关信息。

端口上开启端口安全的开放认证模式后，身份信息正确的用户可正常上线，此类不属于 open 用户。开放认证模式优先级低于 802.1X 的 Auth-Fail VLAN 和 MAC 地址认证的 Guest VLAN，即如果端口上配置了 802.1X 的 Auth-Fail VLAN 或 MAC 地址认证的 Guest VLAN，密码错误的接入用户会加入认证失败 VLAN，开放认证模式不生效。

有关 802.1X、MAC 地址认证的详细介绍，请参见“安全配置指导”中的“802.1X”和“MAC 地址认证”。

【举例】

开启端口 GigabitEthernet1/0/1 上的端口安全的开放认证模式。

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] port-security authentication open
```

【相关命令】

- **display dot1x connection**
- **display mac-authentication connection**
- **port-security authentication open global**

1.1.6 port-security authentication open global

port-security authentication open global 命令用来开启全局端口安全的开放认证模式。

undo port-security authentication open global 命令用来关闭全局端口安全的开放认证模式。

【命令】

```
port-security authentication open global
undo port-security authentication open global
```

【缺省情况】

端口安全的开放认证模式处于关闭状态。

【视图】

系统视图

【缺省用户角色】

network-admin

【使用指导】

开启全局端口安全开放认证模式之后，802.1X、MAC 地址认证用户即使身份信息不正确（包含不存在的用户名或者错误的密码两种情况）也可以正常接入并访问网络。在这种模式下接入的用户被称为 open 用户，此类用户不支持授权和计费，但可通过 **display dot1x connection open**、**display mac-authentication connection open** 命令查看相关信息。

全局开启端口安全的开放认证模式后，身份信息正确的用户可正常上线，此类不属于 open 用户。

开放认证模式优先级低于 802.1X 的 Auth-Fail VLAN 和 MAC 地址认证的 Guest VLAN，即如果端口上配置了 802.1X 的 Auth-Fail VLAN 或 MAC 地址认证的 Guest VLAN，密码错误的接入用户会加入认证失败 VLAN，开放认证模式不生效。

有关 802.1X、MAC 地址认证的详细介绍，请参见“安全”中的“802.1X”和“MAC 地址认证”。

【举例】

开启全局端口安全的开放认证模式。

```
<Sysname> system-view
[Sysname] port-security authentication open global
```

【相关命令】

- **display dot1x connection**
- **display mac-authentication connection**
- **port-security authentication open**

1.1.7 port-security authorization ignore

port-security authorization ignore 命令用来配置端口不应用 RADIUS 服务器或设备本地下发的授权信息。

undo port-security authorization ignore 命令用来恢复缺省情况。

【命令】

```
port-security authorization ignore
undo port-security authorization ignore
```

【缺省情况】

端口应用 RADIUS 服务器或设备本地下发的授权信息。

【视图】

二层以太网接口视图

【缺省用户角色】

network-admin

【使用指导】

当用户通过 RADIUS 认证或本地认证后，RADIUS 服务器或设备会根据用户帐号配置的相关属性进行授权，比如动态下发 VLAN 等。若不希望接受这类动态下发的属性，则可通过配置本命令来忽略。

【举例】

配置端口 GigabitEthernet1/0/1 不应用 RADIUS 服务器或设备本地下发的授权信息。

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] port-security authorization ignore
```

【相关命令】

- **display port-security**

1.1.8 port-security authorization-fail offline

port-security authorization-fail offline 命令用来开启授权失败用户下线功能。

undo port-security authorization-fail offline 命令用来关闭授权失败用户下线功能。

【命令】

```
port-security authorization-fail offline [ quiet-period ]
undo port-security authorization-fail offline
```

【缺省情况】

授权失败用户下线功能处于关闭状态，即授权失败后用户保持在线。

【视图】

系统视图

【缺省用户角色】

network-admin

【参数】

quiet-period: 表示开启用户授权失败下线静默功能。802.1X 认证或 MAC 地址认证用户下线后，设备将其加入对应认证类型的静默队列，并根据对应认证类型的静默定时器的值来确定用户认证失败以后，设备停止对其提供认证服务的时间间隔。在静默期间，设备不对来自认证失败用户的报文进行认证处理，直接丢弃；静默期后，设备再次收到该用户的报文，则对其进行认证处理。若不指定此参数，用户授权下线后，设备再次收到该用户的报文就对其进行认证处理。

【使用指导】

如果配置为授权失败用户下线，当下发的授权 ACL、User Profile 不存在或者 ACL、User Profile 下发失败时，将强制用户下线。

如果配置为授权失败用户保持在线，当下发的授权 ACL、User Profile 不存在或者 ACL、User Profile 下发失败时，用户保持在线，授权 ACL、User Profile 不生效，设备打印日志信息。

若开启本功能时指定了 **quiet-period** 参数则需要先完成如下配置：

- 对于 802.1X 用户，通过 **dot1x quiet-period** 命令开启 802.1X 认证静默定时器功能，并通过 **dot1x timer quiet-period** 命令设置静默定时器的值。
- 对于 MAC 地址认证用户，通过 **mac-authentication timer quiet** 命令配置 MAC 地址认证静默定时器的值。

【举例】

开启授权失败用户下线功能。

```
<Sysname> system-view
[Sysname] port-security authorization-fail offline
```

【相关命令】

- **display port-security**
- **dot1x quiet-period**（安全命令参考/802.1X）
- **dot1x timer quiet-period**（安全命令参考/802.1X）
- **mac-authentication timer**（安全命令参考/MAC 地址认证）

1.1.9 port-security enable

port-security enable 命令用来使能端口安全。

undo port-security enable 命令用来关闭端口安全。

【命令】

```
port-security enable
undo port-security enable
```

【缺省情况】

端口安全功能处于关闭状态。

【视图】

系统视图

【缺省用户角色】

network-admin

【使用指导】

如果已全局开启了 802.1X 或 MAC 地址认证，则无法使能端口安全。

执行使能或关闭端口安全的命令后，端口上的相关配置将会恢复为如下情况：

- 802.1X 端口接入控制方式恢复为 **macbased**；
- 802.1X 端口的授权状态恢复为 **auto**。

端口上有用户在线的情况下，若关闭端口安全，则在线用户将会下线。

【举例】

使能端口安全。

```
<Sysname> system-view
[Sysname] port-security enable
```

【相关命令】

- **display port-security**
- **dot1x**（安全命令参考/802.1X）
- **dot1x port-control**（安全命令参考/802.1X）
- **dot1x port-method**（安全命令参考/802.1X）
- **mac-authentication**（安全命令参考/MAC 地址认证）

1.1.10 port-security intrusion-mode

port-security intrusion-mode 命令用来配置入侵检测特性，对接收到非法报文的端口采取相应的安全策略。

undo port-security intrusion-mode 命令用来恢复缺省情况。

【命令】

```
port-security intrusion-mode { blockmac | disableport |
disableport-temporarily }
```

undo port-security intrusion-mode

【缺省情况】

对接收到非法报文的端口不进行入侵检测处理。

【视图】

二层以太网接口视图

【缺省用户角色】

network-admin

【参数】

blockmac: 表示将非法报文的源 MAC 地址加入阻塞 MAC 地址列表中, 源 MAC 地址为阻塞 MAC 地址的报文将被丢弃, 实现在端口上过滤非法流量的作用。此 MAC 地址在被阻塞 3 分钟 (系统默认, 不可配) 后恢复正常。阻塞 MAC 地址列表可以通过 **display port-security mac-address block** 命令查看。

disableport: 表示将收到非法报文的端口永久关闭。

disableport-temporarily: 表示将收到非法报文的端口暂时关闭一段时间。关闭时长可通过 **port-security timer disableport** 命令配置。

【使用指导】

可以通过执行 **undo shutdown** 命令重新开启被入侵检测特性临时或永久断开的端口。

【举例】

配置端口 GigabitEthernet1/0/1 的入侵检测特性检测到非法报文后, 将非法报文的源 MAC 地址置为阻塞 MAC。

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] port-security intrusion-mode blockmac
```

【相关命令】

- **display port-security**
- **display port-security mac-address block**
- **port-security timer disableport**

1.1.11 port-security mac-address aging-type inactivity

port-security mac-address aging-type inactivity 命令用来配置安全 MAC 地址的老化方式为无流量老化。

undo port-security mac-address aging-type inactivity 命令用来恢复缺省情况。

【命令】

port-security mac-address aging-type inactivity

undo port-security mac-address aging-type inactivity

【缺省情况】

安全 MAC 地址按照配置的老化时间进行老化，即在安全 MAC 地址的老化时间到达后立即老化，不论该安全 MAC 地址是否还有流量产生。

【视图】

二层以太网接口视图

【缺省用户角色】

network-admin

【使用指导】

无流量老化方式下，设备会定期检测端口上的安全 MAC 地址是否有流量产生，若某安全 MAC 地址在配置的老化时间内没有任何流量产生，则才会被老化，否则该安全 MAC 地址不会被老化，并在下一个老化周期内重复该检测过程。下一个周期内若还有流量产生则继续保持该安全 MAC 地址的学习状态，该方式可有效避免非法用户通过仿冒合法用户 MAC 地址乘机在合法用户的安全 MAC 地址老化时间到达之后占用端口资源。

如果通过 **port-security timer autolearn aging** 命令配置的安全 MAC 地址老化时间大于等于 60 秒，则设备以 30 秒为周期，检测端口上的安全 MAC 地址是否有流量产生，当某安全 MAC 地址在配置的老化时间内没有任何流量产生，安全 MAC 地址会被老化。

如果通过 **port-security timer autolearn aging second** 命令配置的安全 MAC 地址老化时间小于 60 秒，则设备以配置的安全 MAC 地址老化时间为周期，检测端口上的安全 MAC 地址是否有流量产生，当某安全 MAC 地址在配置的老化时间内没有任何流量产生，安全 MAC 地址会被老化。

此命令仅对于 Sticky MAC 地址以及动态类型的安全 MAC 地址有效。

【举例】

配置端口 GigabitEthernet1/0/1 的安全 MAC 地址的老化方式为无流量老化。

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] port-security mac-address aging-type inactivity
```

【相关命令】

- **display port-security**

1.1.12 port-security mac-address dynamic

port-security mac-address dynamic 命令用来将 Sticky MAC 地址设置为动态类型的安全 MAC 地址。

undo port-security mac-address dynamic 命令用来恢复缺省情况。

【命令】

```
port-security mac-address dynamic
undo port-security mac-address dynamic
```

【缺省情况】

端口学习到的是 Sticky 类型的安全 MAC，它能够被保存在配置文件中，设备重启后也不会丢失。

【视图】

二层以太网接口视图

【缺省用户角色】

network-admin

【使用指导】

动态类型的安全 MAC 地址不会被保存在配置文件中，可通过执行 **display port-security mac-address security** 命令查看到，设备重启之后会丢失。在不希望设备上保存重启之前端口上已有的 Sticky MAC 地址的情况下，可将其设置为动态类型的安全 MAC 地址。

本命令成功执行后，指定端口上的 Sticky MAC 地址会立即被转换为动态类型的安全 MAC 地址，且将不能手工添加 Sticky MAC 地址。之后，若成功执行对应的 **undo** 命令，该端口上的动态类型的安全 MAC 地址会立即转换为 Sticky MAC 地址，且用户可以手工添加 Sticky MAC 地址。

【举例】

将端口 GigabitEthernet1/0/1 上的 Sticky MAC 地址设置为动态类型的安全 MAC 地址。

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] port-security mac-address dynamic
```

【相关命令】

- **display port-security**
- **display port-security mac-address security**

1.1.13 port-security mac-address security

port-security mac-address security 命令用来添加安全 MAC 地址。

undo port-security mac-address security 命令用来删除指定的安全 MAC 地址。

【命令】

在二层以太网接口视图下：

```
port-security mac-address security [ sticky ] mac-address vlan vlan-id
undo port-security mac-address security [ sticky ] mac-address vlan vlan-id
```

在系统视图下：

```
port-security mac-address security [ sticky ] mac-address interface
interface-type interface-number vlan vlan-id
undo port-security mac-address security [ [ mac-address [ interface
interface-type interface-number ] ] vlan vlan-id ]
```

【缺省情况】

未配置安全 MAC 地址。

【视图】

系统视图

二层以太网接口视图

【缺省用户角色】

network-admin

【参数】

sticky: 表示要添加一个可老化的安全 MAC 地址（Sticky MAC 地址）。若不指定本参数，则表示添加的是一个不老化的静态安全 MAC 地址。

mac-address: 安全 MAC 地址，格式为 H-H-H。

interface interface-type interface-number: 指定添加安全 MAC 地址的接口。其中，*interface-type interface-number* 表示接口类型和接口编号。

vlan vlan-id: 指定安全 MAC 地址所属的 VLAN。其中，*vlan-id* 表示 VLAN 编号，取值范围为 1~4094。

【使用指导】

Sticky MAC 地址的老化时间可通过 **port-security timer autolearn aging** 命令配置。当 Sticky MAC 地址的老化时间到达时，Sticky MAC 地址即被删除。

手工配置添加的安全 MAC 地址在保存配置并设备重启后，不会被删除。因此，可以将网络中一些已知的、固定要接入某端口的主机或设备的 MAC 地址添加为安全 MAC 地址，这样在端口处于 autoLearn 安全模式时，此类源 MAC 地址为安全 MAC 地址的主机或设备的报文将被允许通过指定端口，而且还可避免与其它通过自动方式学习到端口上的 MAC 地址的报文争夺资源而被拒绝接收。成功添加安全 MAC 地址的前提为：端口安全处于开启状态；端口的端口安全模式为 autoLearn；当前的端口允许指定的 VLAN 通过或已加入该 VLAN，且该 VLAN 已存在。

已添加的安全 MAC 地址，除非首先将其删除，否则不能重复添加或者修改其地址类型，例如已经在某端口上添加了一条安全 MAC 地址 **port-security mac-address security 1-1-1 vlan 10**，则不能再添加一条安全 MAC 地址 **port-security mac-address security sticky 1-1-1 vlan 10**。

所有的静态安全 MAC 地址均不老化，除非被管理员通过命令行手工删除，或因为配置的改变（端口的安全模式被改变，或端口安全功能被关闭）而被系统自动删除。

【举例】

使能端口安全，配置端口 GigabitEthernet1/0/1 的安全模式为 autoLearn，并指定端口安全允许的最大 MAC 地址数为 100。

```
<Sysname> system-view
[Sysname] port-security enable
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] port-security max-mac-count 100
[Sysname-GigabitEthernet1/0/1] port-security port-mode autolearn
```

为该端口添加一条 Sticky MAC 地址 0001-0002-0003，该安全 MAC 地址属于 VLAN 4。

```
[Sysname-GigabitEthernet1/0/1] port-security mac-address security sticky 0001-0002-0003
vlan 4
[Sysname-GigabitEthernet1/0/1] quit
```

在系统视图下为端口 GigabitEthernet1/0/1 添加一条安全 MAC 地址 0001-0001-0002，该安全 MAC 地址属于 VLAN 10。

```
[Sysname] port-security mac-address security 0001-0001-0002 interface gigabitethernet 1/0/1
vlan 10
```

【相关命令】

- `display port-security`
- `port-security timer autolearn aging`

1.1.14 port-security mac-limit

`port-security mac-limit` 命令用来设置端口上指定 VLAN 内端口安全功能允许同时接入的最大 MAC 地址数。

`undo port-security mac-limit` 命令用来恢复缺省情况。

【命令】

```
port-security mac-limit max-number per-vlan vlan-id-list
undo port-security mac-limit per-vlan vlan-id-list
```

【缺省情况】

端口上端口安全功能允许同时接入的最大 MAC 地址数为 2147483647。

【视图】

二层以太网接口视图

【缺省用户角色】

network-admin

【参数】

max-number: 端口上端口安全功能允许同时接入的 MAC 地址数的最大值，取值范围为 1～2147483647。

per-vlan vlan-id-list: 指定 VLAN 列表内每个 VLAN 内允许同时接入的 MAC 地址数的最大值。表示方式为 `vlan-id-list = { vlan-id1 [to vlan-id2] } &<1-10>`，`vlan-id` 取值范围为 1～4094，`vlan-id2` 的值要大于或等于 `vlan-id1` 的值，`&<1-10>` 表示前面的参数最多可以重复输入 10 次。

【使用指导】

端口上端口安全功能允许接入的 MAC 地址包括：

- 端口上 MAC 地址认证成功用户的 MAC 地址；MAC 地址认证 Guest VLAN、Critical VLAN 中用户的 MAC 地址。
- 802.1X 认证成功用户的 MAC 地址；802.1X 认证 Guest VLAN、Auth-Fail VLAN、Critical VLAN 中用户的 MAC 地址。

由于系统资源有限，如果当前端口上允许接入的 MAC 地址数过多，接入 MAC 地址之间会发生资源的争用，因此适当地配置该值可以使属于当前端口的用户获得可靠的性能保障。当指定 VLAN 内，端口允许接入的 MAC 地址数超过最大值后，该 VLAN 内新接入的 MAC 地址将被拒绝。

通过本命令配置端口上指定 VLAN 内端口安全功能允许同时接入的最大 MAC 地址数，不能小于当前端口上相应 VLAN 已存在的 MAC 地址数；否则，本次配置不生效。

【举例】

配置端口 GigabitEthernet1/0/1 上, VLAN 1、VLAN 5 和 VLAN 10~VLAN 20 上每个 VLAN 最多允许同时接入 32 个 MAC 地址认证或 802.1X 认证用户。

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] port-security mac-limit 32 per-vlan 1 5 10 to 20
```

【相关命令】

- **display mac-authentication**
- **display dot1x**

1.1.15 port-security mac-move permit

port-security mac-move permit 命令用来开启允许 MAC 迁移功能。

undo port-security mac-move permit 命令用来关闭允许 MAC 迁移功能。

【命令】

```
port-security mac-move permit
undo port-security mac-move permit
```

【缺省情况】

允许 MAC 迁移功能处于关闭状态。

【视图】

系统视图

【缺省用户角色】

network-admin

【使用指导】

该功能对系统中的所有 802.1X 认证用户和 MAC 地址认证用户生效。

MAC 迁移功能处于关闭状态时, 如果用户从某一端口上线成功, 则该用户在未从当前端口下线的情况下无法在设备的其它端口上 (无论该端口是否与当前端口属于同一 VLAN) 发起认证, 也无法上线。

MAC 迁移功能处于开启状态时, 如果用户从某一端口上线成功, 则允许该在线用户在设备的其它端口上 (无论该端口是否与当前端口属于同一 VLAN) 发起认证。如果该用户在后接入的端口上认证成功, 则当前端口会将该用户立即进行下线处理, 保证该用户仅在一个端口上处于上线状态。如果服务器在线用户数已达到上限, 将无法进行 MAC 地址迁移。

【举例】

开启允许 MAC 迁移功能。

```
<Sysname> system-view
[Sysname] port-security mac-move permit
```

【相关命令】

- **display port-security**

1.1.16 port-security max-mac-count

port-security max-mac-count 命令用来设置端口安全允许的最大安全 MAC 地址数。

undo port-security max-mac-count 命令用来恢复缺省情况。

【命令】

```
port-security max-mac-count max-count [ vlan [ vlan-id-list ] ]
undo port-security max-mac-count [ vlan [ vlan-id-list ] ]
```

【缺省情况】

端口安全不限制本端口可保存的最大安全 MAC 地址数。

【视图】

二层以太网接口视图

【缺省用户角色】

network-admin

【参数】

max-count: 端口允许的最大安全 MAC 地址数，取值范围为 1~2147483647。端口安全允许的最大安全 MAC 地址数不能小于当前端口下已保存的 MAC 地址数。

vlan [vlan-id-list]: 指定端口所属 VLAN。**vlan-id-list** 是 VLAN 列表，表示方式为 **vlan-id-list = { vlan-id1 [to vlan-id2] }&<1-10>**，**vlan-id** 取值范围为 1~4094，**&<1-10>** 表示前面的参数最多可以重复输入 10 次。**vlan-id2** 的值必须大于或等于 **vlan-id1** 的值。若不指定 **vlan** 参数，则表示限制当前端口上允许的最大安全 MAC 地址数。若不指定 **vlan-id-list**，则表示限制当前端口上每个 VLAN 内允许通过的最大安全 MAC 地址数。

【使用指导】

对于 **autoLearn** 安全模式，端口允许的最大安全 MAC 地址数由本命令配置，包括端口上学习到的以及手工配置的安全 MAC 地址数；对于采用 **802.1X**、**MAC** 地址认证或者两者组合形式的认证类安全模式，端口允许的最大用户数取本命令配置的值与相应模式下允许认证用户数的最小值。例如，**userLoginSecureExt** 模式下，端口下所允许的最大安全 MAC 地址数为配置的端口安全允许的最大安全 MAC 地址数与 **802.1X** 认证所允许的最大用户数的最小值。

当端口工作于 **autoLearn** 模式时，无法更改端口安全允许的最大安全 MAC 地址数。

vlan [vlan-id-list] 参数配置仅对端口安全的 **autolearn** 模式生效。

端口允许的 VLAN 内最大安全 MAC 地址数不能小于当前 VLAN 内已保存的 MAC 地址数。

对于端口上的同一 VLAN，后配置的最大安全 MAC 地址数覆盖前面配置的最大安全 MAC 地址数。

【举例】

在端口 **GigabitEthernet1/0/1** 上配置端口安全允许的最大安全 MAC 地址数为 100。

```
<Sysname> system-view
```

```
[Sysname] interface gigabitethernet 1/0/1
```

```
[Sysname-GigabitEthernet1/0/1] port-security max-mac-count 100
```

【相关命令】

- **display port-security**

1.1.17 port-security nas-id-profile

port-security nas-id-profile 命令用来指定全局/端口引用的 NAS-ID Profile。

undo port-security nas-id-profile 命令用来恢复缺省情况。

【命令】

port-security nas-id-profile *profile-name*

undo port-security nas-id-profile

【缺省情况】

未指定引用的 NAS-ID Profile。

【视图】

系统视图

二层以太网接口视图

【缺省用户角色】

network-admin

【参数】

profile-name: 标识指定 VLAN 和 NAS-ID 绑定关系的 Profile 名称, 为 1~31 个字符的字符串, 不区分大小写。

【使用指导】

本命令引用的 NAS-ID Profile 由命令 **aaa nas-id profile** 配置, 具体情况请参考“安全命令参考”中的“AAA”。

NAS-ID Profile 可以在系统视图下或者接口视图下进行配置引用, 接口上的配置优先, 若接口上没有配置, 则使用系统视图下的全局配置。

如果指定了 NAS-ID Profile, 则此 Profile 中定义的绑定关系优先使用; 如果未指定 NAS-ID Profile 或指定的 Profile 中没有找到匹配的绑定关系, 则使用设备名作为 NAS-ID。

【举例】

在端口 GigabitEthernet1/0/1 上指定名为 aaa 的 NAS-ID Profile。

```
<Sysname> system-view
```

```
[Sysname] interface gigabitethernet 1/0/1
```

```
[Sysname-GigabitEthernet1/0/1] port-security nas-id-profile aaa
```

在系统视图下指定名为 aaa 的 NAS-ID Profile。

```
<Sysname> system-view
```

```
[Sysname] port-security nas-id-profile aaa
```

【相关命令】

- **aaa nas-id profile** (安全命令参考/AAA)

1.1.18 port-security ntk-mode

port-security ntk-mode 命令用来配置端口 Need To Know 特性。

undo port-security ntk-mode 命令用来恢复缺省情况。

【命令】

```
port-security ntk-mode { ntk-withbroadcasts | ntk-withmulticasts | ntkonly }  
undo port-security ntk-mode
```

【缺省情况】

端口未配置 Need To Know 特性，即所有报文都可成功发送。

【视图】

二层以太网接口视图

【缺省用户角色】

network-admin

【参数】

ntk-withbroadcasts: 允许目的 MAC 地址为已通过认证的 MAC 地址的单播报文或广播地址的报文通过。

ntk-withmulticasts: 允许目的 MAC 地址为已通过认证的 MAC 地址的单播报文，广播地址或组播地址的报文通过。

ntkonly: 仅允许目的 MAC 地址为已通过认证的 MAC 地址的单播报文通过。

【使用指导】

Need To Know 特性通过检测从端口发出的数据帧的目的 MAC 地址，保证数据帧只能被发送到已经通过认证的设备上，从而防止非法设备窃听网络数据。

【举例】

配置端口 GigabitEthernet1/0/1 的 Need To Know 特性为 **ntkonly**，即仅发送目的地址为已认证的 MAC 地址的报文。

```
<Sysname> system-view  
[Sysname] interface gigabitethernet 1/0/1  
[Sysname-GigabitEthernet1/0/1] port-security ntk-mode ntkonly
```

【相关命令】

- **display port-security**

1.1.19 port-security oui

port-security oui 命令用来配置允许通过认证的用户 OUI 值。

undo port-security oui 命令用来删除指定索引的 OUI 值。

【命令】

```
port-security oui index index-value mac-address oui-value  
undo port-security oui index index-value
```

【缺省情况】

不存在允许通过认证的用户 OUI 值。

【视图】

系统视图

【缺省用户角色】

network-admin

【参数】

index-value: 标识此 OUI 的索引值，取值范围为 1~16。

oui-value: OUI 值，输入格式为 H-H-H 的 48 位 MAC 地址。系统会自动取输入的前 24 位作为 OUI 值，忽略后 24 位。

【使用指导】

OUI 是 MAC 地址的前 24 位（二进制），是 IEEE 为不同设备供应商分配的一个全球唯一的标识符。当需要允许某些厂商的设备（如 IP 电话或打印机）无需认证即可接入网络时，则可以通过本命令来指定这些设备的 OUI 值。

可通过多次执行本命令，配置多个 OUI 值。

配置的 OUI 值只在端口安全模式为 userLoginWithOUI 时生效。在 userLoginWithOUI 模式下，端口上除了允许一个 802.1X 认证用户接入之外，还额外允许一个特殊用户接入，该用户报文的源 MAC 地址的 OUI 与设备上配置的某个 OUI 值相符。

【举例】

配置一个允许通过认证的用户 OUI 值为 000d2a，索引为 4。

```
<Sysname> system-view
```

```
[Sysname] port-security oui index 4 mac-address 000d-2a10-0033
```

【相关命令】

- **display port-security**

1.1.20 port-security port-mode

port-security port-mode 命令用来配置端口安全模式。

undo port-security port-mode 命令用来恢复缺省情况。

【命令】

```
port-security port-mode { autolearn | mac-authentication |  
mac-else-userlogin-secure | mac-else-userlogin-secure-ext | secure |  
userlogin | userlogin-secure | userlogin-secure-ext |  
userlogin-secure-or-mac | userlogin-secure-or-mac-ext |  
userlogin-withoui }  
undo port-security port-mode
```

【缺省情况】

端口处于 noRestrictions 模式，此时该端口的安全功能关闭，端口处于不受端口安全限制的状态。

【视图】

二层以太网接口视图

【缺省用户角色】

network-admin

【参数】

表1-4 安全模式的参数解释表

参数	安全模式	说明
autolearn	autoLearn	端口可通过手工配置或自动学习MAC地址。手工配置或自动学习到的MAC地址被称为安全MAC，并被添加到安全MAC地址表中 当端口下的安全MAC地址数超过端口安全允许的最大安全MAC地址数后，端口模式会自动转变为secure模式。之后，该端口停止添加新的安全MAC，只有源MAC地址为安全MAC地址、通过命令 mac-address dynamic 或 mac-address static 手工配置的MAC地址的报文，才能通过该端口
mac-authentication	macAddressWithRadius	对接入用户采用MAC地址认证 此模式下，端口允许多个用户接入
mac-else-userlogin-secure	macAddressElseUserLoginSecure	端口同时处于macAddressWithRadius模式和userLoginSecure模式，但MAC地址认证优先级大于802.1X认证。允许端口下一个802.1X认证用户及多个MAC地址认证用户接入 非802.1X报文直接进行MAC地址认证。802.1X报文先进行MAC地址认证，如果MAC地址认证失败再进行802.1X认证
mac-else-userlogin-secure-ext	macAddressElseUserLoginSecureExt	与macAddressElseUserLoginSecure类似，但允许端口下有多个802.1X和MAC地址认证用户
secure	secure	禁止端口学习MAC地址，只有源MAC地址为端口上的安全MAC地址、手工配置的MAC地址的报文，才能通过该端口
userlogin	userLogin	对接入用户采用基于端口的802.1X认证 此模式下，端口下的第一个802.1X用户认证成功后，其它用户无须认证就可接入
userlogin-secure	userLoginSecure	对接入用户采用基于MAC地址的802.1X认证 此模式下，端口最多只允许一个802.1X认证用户接入
userlogin-secure-ext	userLoginSecureExt	对接入用户采用基于MAC的802.1X认证，且允许端口下有多个802.1X用户
userlogin-secure-or-mac	macAddressOrUserLoginSecure	端口同时处于userLoginSecure模式和macAddressWithRadius模式，且允许一个802.1X认证用户及多个MAC地址认证用户接入 此模式下，802.1X认证优先级大于MAC地址认证：报文首先触发802.1X认证，默认情况下，如果802.1X认证失败再进行MAC地址认证；若开启了端口的MAC地址认证和802.1X认证并行处理功能，则端口配置了802.1X单播触发功能的情况下，当端口收到源MAC地址未知的报文，会向该MAC地址单播发送EAP-Request帧来触发802.1X认证，但不等待802.1X认证处理完成，就同时进行MAC地址认证
userlogin-secure-or-mac-ext	macAddressOrUserLoginSecureExt	与macAddressOrUserLoginSecure类似，但允许端口下有多个802.1X和MAC地址认证用户

参数	安全模式	说明
userlogin-without	userLoginWithOUI	与userLoginSecure模式类似，但端口上除了允许一个802.1X认证用户接入之外，还额外允许一个特殊用户接入，该用户报文的源MAC的OUI与设备上配置的OUI值相符 此模式下，报文首先进行OUI匹配，OUI匹配失败的报文再进行802.1X认证，OUI匹配成功和802.1X认证成功的报文都允许通过端口

【使用指导】

端口安全模式与端口下的 802.1X 认证使能、端口接入控制方式、端口授权状态以及端口下的 MAC 地址认证使能配置互斥。

当端口安全已经使能且当前端口安全模式不是 noRestrictions 时，若要改变端口安全模式，必须首先执行 **undo port-security port-mode** 命令恢复端口安全模式为 noRestrictions 模式。

配置端口安全 autoLearn 模式时，首先需要通过命令 **port-security max-mac-count** 设置端口安全允许的最大安全 MAC 地址数。

端口上有用户在线的情况下，端口安全模式无法改变。

开启了 MAC 地址认证延迟功能的端口上不建议同时配置端口安全的模式为 **mac-else-userlogin-secure** 或 **mac-else-userlogin-secure-ext**，否则 MAC 地址认证延迟功能不生效。MAC 地址认证延迟功能的具体配置请参见“安全命令参考”中的“MAC 地址认证”。

【举例】

使能端口安全，并配置端口 GigabitEthernet1/0/1 的端口安全模式为 secure。

```
<Sysname> system-view
[Sysname] port-security enable
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] port-security port-mode secure
# 将端口 GigabitEthernet1/1 的端口安全模式改变为 userLogin。
[Sysname-GigabitEthernet1/0/1] undo port-security port-mode
[Sysname-GigabitEthernet1/0/1] port-security port-mode userlogin
```

【相关命令】

- **display port-security**
- **port-security max-mac-count**

1.1.21 port-security timer autolearn aging

port-security timer autolearn aging 命令用来配置安全 MAC 地址的老化时间。

undo port-security timer autolearn aging 命令用来恢复缺省情况。

【命令】

```
port-security timer autolearn aging [ second ] time-value
undo port-security timer autolearn aging
```

【缺省情况】

安全 MAC 地址不会老化。

【视图】

系统视图

【缺省用户角色】

network-admin

【参数】

second: 指定安全 MAC 地址老化时间单位为秒。如果未指定本参数，则表示安全 MAC 地址老化时间单位为分钟。

time-value: 安全 MAC 地址的老化时间。若单位为分钟，则取值范围为 0~129600，取值为 0 表示不会老化。若单位为秒，则取值范围 10~7776000。

【使用指导】

安全 MAC 地址的老化时间对所有端口学习到的安全 MAC 地址以及手工添加的 Sticky MAC 地址均有效。

当指定的安全 MAC 地址老化时间单位为秒时，若配置的老化时间大于等于 60 秒，则安全 MAC 地址的实际老化时间会以半分钟向上取整，例如，配置老化时间为 80 秒，则实际老化时间为 90 秒；若配置的老化时间小于 60 秒，则安全 MAC 地址的实际老化时间为用户配置时间。

较短的老化时间可提高端口接入的安全性和端口资源的利用率，但也会影响在线用户的在线稳定性，因此需要结合当前的网络环境和设备的性能合理设置老化时间。

当配置的安全 MAC 地址老化时间小于 60 秒，且安全 MAC 地址老化方式为无流量老化时，建议端口安全允许的最大安全 MAC 地址数不要配置过大，否则可能影响设备性能。

【举例】

```
# 配置安全 MAC 地址的老化时间为 30 分钟。
<Sysname> system-view
[Sysname] port-security timer autolearn aging 30
# 配置安全 MAC 地址的老化时间为 50 秒。
<Sysname> system-view
[Sysname] port-security timer autolearn aging second 50
```

【相关命令】

- **display port-security**
- **port-security mac-address security**

1.1.22 port-security timer disableport

port-security timer disableport 命令用来配置系统暂时关闭端口的时间。

undo port-security timer disableport 命令用来恢复缺省情况。

【命令】

```
port-security timer disableport time-value
undo port-security timer disableport
```


【缺省情况】

系统暂时关闭端口的时间为 20 秒。

【视图】

系统视图

【缺省用户角色】

network-admin

【参数】

time-value: 端口关闭的时间，取值范围为 20~300，单位为秒。

【使用指导】

当 **port-security intrusion-mode** 设置为 **disableport-temporarily** 模式时，系统暂时关闭端口的时间由该命令配置。

【举例】

配置端口 GigabitEthernet1/0/1 的入侵检测特性检测到非法报文后，将收到非法报文的端口暂时关闭 30 秒。

```
<Sysname> system-view
[Sysname] port-security timer disableport 30
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] port-security intrusion-mode disableport-temporarily
```

【相关命令】

- **display port-security**
- **port-security intrusion-mode**

1.1.23 snmp-agent trap enable port-security

snmp-agent trap enable port-security 命令用来开启端口安全告警功能。

undo snmp-agent trap enable port-security 命令用来关闭指定的端口安全告警功能。

【命令】

```
snmp-agent trap enable port-security [ address-learned | dot1x-failure |
dot1x-logoff | dot1x-logon | intrusion | mac-auth-failure | mac-auth-logoff
| mac-auth-logon ] *
undo snmp-agent trap enable port-security [ address-learned | dot1x-failure
| dot1x-logoff | dot1x-logon | intrusion | mac-auth-failure |
mac-auth-logoff | mac-auth-logon ] *
```

【缺省情况】

端口安全的所有告警功能均处于关闭状态。

【视图】

系统视图

【缺省用户角色】

network-admin

【参数】

address-learned: 表示端口学习到新 MAC 地址时的告警功能。

dot1x-failure: 表示 802.1X 用户认证失败时的告警功能。

dot1x-logon: 表示 802.1X 用户认证成功时的告警功能。

dot1x-logoff: 表示 802.1X 用户认证下线时的告警功能。

intrusion: 表示发现非法报文时的告警功能。

mac-auth-failure: 表示 MAC 地址认证用户认证失败时的告警功能。

mac-auth-logoff: 表示 MAC 地址认证用户认证下线时的告警功能。

mac-auth-logon: 表示 MAC 地址认证用户认证成功时的告警功能。

【使用指导】

如果不指定任何参数，则表示开启或关闭所有类型的端口安全告警功能。

只有配置了入侵检测特性（通过命令 **port-security intrusion-mode**），端口安全告警功能才生效。

开启端口安全模块的告警功能后，该模块会生成告警信息，用于报告该模块的重要事件。生成的告警信息将发送到设备的 SNMP 模块，通过设置 SNMP 中告警信息的发送参数，来决定告警信息输出的相关属性。有关告警信息的详细介绍，请参见“网络管理和监控配置指导”中的“SNMP”。

【举例】

开启端口学习到新 MAC 地址时的告警功能。

```
<Sysname> system-view
```

```
[Sysname] snmp-agent trap enable port-security address-learned
```

【相关命令】

- **display port-security**
- **port-security enable**

目 录

1 User Profile	1-1
1.1 User Profile配置命令	1-1
1.1.1 display user-profile	1-1
1.1.2 user-profile	1-2

1 User Profile

1.1 User Profile配置命令

1.1.1 display user-profile

display user-profile 用来显示 User Profile 的配置信息和在线用户信息。

【命令】

display user-profile [**name** *profile-name*] [**slot** *slot-number*]

【视图】

任意视图

【缺省用户角色】

network-admin
network-operator

【参数】

name *profile-name*: 表示 User Profile 的名称，为 1~31 个字符的字符串，只能包含英文字母 [a-z,A-Z]、数字、下划线，且必须以英文字母开始，区分大小写。User Profile 的名称必须全局唯一。如果未指定本参数，将显示所有 User Profile 的配置信息和在线用户信息。

slot *slot-number*: 显示 User Profile 的配置信息和指定成员设备的在线用户信息，*slot-number* 表示设备在 IRF 中的成员编号。如果未指定本参数，将显示 User Profile 的配置信息和所有成员设备的在线用户信息。

【举例】

显示名称为 aaa 的 User Profile 配置信息及被授权该 User Profile 的在线用户信息。

```
<Sysname> display user-profile name aaa
User-Profile: aaa
  Inbound:
    Policy: p1

  User user_1:
    Authentication type: 802.1X
    Network attributes:
      Interface      : GigabitEthernet1/0/1
      MAC address   : 0000-1111-2222
    Failed action list:
      Inbound: Policy p1
```

表1-1 display user-profile 命令显示信息描述表

字段	描述
User-Profile	User Profile名称

字段	描述
Inbound	在入方向上应用的策略
Outbound	在出方向上应用的策略
Policy	策略名
User user_1	与User Profile关联的用户信息
Authentication type	用户认证类型 <ul style="list-style-type: none"> • 802.1X • Portal • MACA
Network attributes	用户特征信息
Failed action list	在该用户上应用失败的动作

1.1.2 user-profile

user-profile 命令用来创建 User Profile，并进入 User Profile 视图。如果指定的 User Profile 已经存在，则直接进入 User Profile 视图。

undo user-profile 命令用来删除指定的 User Profile。

【命令】

```
user-profile profile-name
undo user-profile profile-name
```

【缺省情况】

不存在 User Profile。

【视图】

系统视图

【缺省用户角色】

network-admin

【参数】

profile-name: 表示 User Profile 的名称，为 1~31 个字符的字符串，只能包含英文字母[a-z,A-Z]、数字、下划线，且必须以英文字母开始，区分大小写。User Profile 的名称必须全局唯一。

【使用指导】

User Profile 的名称必须全局唯一。

【举例】

创建名称为 a123 的 User Profile，并进入其视图。

```
<Sysname> system-view
[Sysname] user-profile a123
[Sysname-user-profile-a123]
```

目 录

1 Password Control	1-1
1.1 Password Control 配置命令	1-1
1.1.1 display password-control	1-1
1.1.2 display password-control blacklist	1-2
1.1.3 password-control { aging composition history length } enable	1-3
1.1.4 password-control aging	1-4
1.1.5 password-control alert-before-expire	1-6
1.1.6 password-control complexity	1-6
1.1.7 password-control composition	1-7
1.1.8 password-control enable	1-9
1.1.9 password-control expired-user-login	1-9
1.1.10 password-control history	1-10
1.1.11 password-control length	1-11
1.1.12 password-control login idle-time	1-12
1.1.13 password-control login-attempt	1-13
1.1.14 password-control super aging	1-15
1.1.15 password-control super composition	1-15
1.1.16 password-control super length	1-16
1.1.17 password-control update-interval	1-17
1.1.18 reset password-control blacklist	1-18
1.1.19 reset password-control history-record	1-18

1 Password Control



说明

设备运行于 FIPS 模式时，本特性部分配置相对于非 FIPS 模式有所变化，具体差异请见本文相关描述。有关 FIPS 模式的详细介绍请参见“安全配置指导”中的“FIPS”。

1.1 Password Control 配置命令

1.1.1 display password-control

display password-control 命令用来显示密码管理的配置信息。

【命令】

```
display password-control [ super ]
```

【视图】

任意视图

【缺省用户角色】

```
network-admin
network-operator
```

【参数】

super：显示 super 密码管理的配置信息。如果不指定该参数，将显示全局密码管理的配置信息。

【举例】

显示全局密码管理的配置信息。

```
<Sysname> display password-control
Global password control configurations:
Password control:                Disabled
Password aging:                  Enabled (90 days)
Password length:                 Enabled (10 characters)
Password composition:            Enabled (1 types, 1 characters per type)
Password history:                Enabled (max history records:4)
Early notice on password expiration: 7 days
Maximum login attempts:         3
Action for exceeding login attempts: Lock user for 1 minutes
Minimum interval between two updates: 24 hours
User account idle time:         90 days
Logins with aged password:       3 times in 30 days
Password complexity:            Disabled (username checking)
                                Disabled (repeated characters checking)
```

显示 super 密码管理的配置信息。

```
<Sysname> display password-control super
Super password control configurations:
Password aging:                               Enabled (90 days)
Password length:                             Enabled (10 characters)
Password composition:                         Enabled (1 types, 1 characters per type)
```

表1-1 display password-control 命令显示信息描述表

字段	描述
Global password control configurations	全局密码管理配置
Super password control configurations	Super密码管理配置
Password control	全局密码管理功能的开启状态
Password aging	密码老化功能的开启状态（密码的老化时间）
Password length	密码最小长度功能的开启状态（密码的最小长度）
Password composition	密码组合策略的开启状态（密码元素的组合类型、至少要包含每种元素的个数）
Password history	密码历史记录功能的开启状态（密码历史记录的最大条数）
Early notice on password expiration	密码过期前的提醒时间
Maximum login attempts	用户最大登录尝试次数
Action for exceeding login attempts	登录尝试次数达到设定次数后的用户帐户锁定行为
Minimum interval between two updates	密码更新的最小时间间隔
User account idle time	用户帐号闲置时间
Logins with aged password	密码过期后允许用户登录的次数和时间
Password complexity	密码复杂度检查功能的开启状态（检查是否包含用户名或者颠倒的用户名；检查是否包含三个或以上相同字符）

1.1.2 display password-control blacklist

display password-control blacklist 命令用来显示用户认证失败后，被加入密码管理黑名单中的用户信息。

【命令】

```
display password-control blacklist [ user-name user-name | ip ipv4-address
| ipv6 ipv6-address ]
```

【视图】

任意视图

【缺省用户角色】

- network-admin
- network-operator

【参数】

user-name *user-name*: 显示密码管理黑名单中指定用户名的用户信息。其中，*user-name* 表示用户名，为 1~55 个字符的字符串，区分大小写。

ip *ipv4-address*: 显示密码管理黑名单中指定 IPv4 地址的用户信息。

ipv6 *ipv6-address*: 显示密码管理黑名单中指定 IPv6 地址的用户信息。

【使用指导】

如果不指定任何参数，则显示密码管理黑名单中的所有用户信息。

用户在认证失败后，其 IP 地址和用户名会被加入密码管理的黑名单。通过本命令可以查看被加入密码管理黑名单中的 FTP 用户和通过 Web 或 VTY 方式访问设备的用户。

通过 Console 口连接到设备的用户，由于系统无法获得其 IP 地址，且这类访问设备的用户已经具备了一定的权限和安全性，所以认证失败后不会被加入密码管理的黑名单。

【举例】

显示用户认证失败后，被加入密码管理黑名单中的用户信息。

```
<Sysname> display password-control blacklist
Blacklist items matched: 2.
Username                IP address             Login failures  Lock flag
abcd                    169::168:34:1          4               lock
admin                   192.168.34.1           1               unlock
```

表1-2 display password-control blacklist 命令显示信息描述表

字段	描述
Blacklist items matched	匹配的黑名单表项数目
Username	用户名
IP address	用户的IP地址
Login failures	用户登录失败的次数
Lock flag	该用户是否被锁定 <ul style="list-style-type: none">unlock: 表示未锁定，允许用户再次尝试登录lock: 表示锁定，暂时或永久禁止用户尝试登录（具体由 password-control login-attempt 命令的配置情况决定）

1.1.3 password-control { aging | composition | history | length } enable

password-control { aging | composition | history | length } enable 命令用来使能指定的密码管理功能。

undo password-control { aging | composition | history | length } enable 命令用来关闭指定的密码管理功能。

【命令】

password-control { aging | composition | history | length } enable

undo password-control { aging | composition | history | length } enable

【缺省情况】

各密码管理功能均处于使能状态。

【视图】

系统视图

【缺省用户角色】

network-admin

【参数】

aging: 使能密码老化管理功能。

composition: 使能密码的组合检测管理功能。

history: 使能密码历史记录管理功能。

length: 使能密码最小长度管理功能。

【使用指导】

要使指定的密码管理功能生效，首先必须保证全局密码管理功能处于使能状态，其次要保证对应的密码管理功能处于使能状态。例如，若全局密码管理功能或密码最小长度管理功能处于未使能状态，则 **password-control length** 命令配置的具体长度限制就不会生效。

密码历史记录管理功能关闭后，系统将不再记录历史密码，但之前已经存在的密码历史记录依然保存。

使能了全局密码管理功能，未使能密码最小长度管理功能时：非 **FIPS** 模式下，密码的最小长度为 4 个字符，且至少要有四个字符不同；**FIPS** 模式下，密码的最小长度为 15 个字符，且至少要有四个字符不同。

【举例】

使能全局密码管理功能。

```
<Sysname> system-view
```

```
[Sysname] password-control enable
```

使能密码组合检测管理功能。

```
[Sysname] password-control composition enable
```

使能密码老化功能。

```
[Sysname] password-control aging enable
```

使能密码最小长度功能。

```
[Sysname] password-control length enable
```

使能密码历史记录功能。

```
[Sysname] password-control history enable
```

【相关命令】

- **display password-control**
- **password-control enable**

1.1.4 password-control aging

password-control aging 命令用来配置密码的老化时间。

undo password-control aging 命令用来恢复缺省情况。

【命令】

```
password-control aging aging-time  
undo password-control aging
```

【缺省情况】

全局的密码老化时间为 90 天；用户组的密码老化时间为全局配置的密码老化时间；本地用户的密码老化时间为所属用户组的密码老化时间。

【视图】

系统视图
用户组视图
本地用户视图

【缺省用户角色】

network-admin

【参数】

aging-time：密码的老化时间，取值范围为 1～365，单位为天。

【使用指导】

系统视图下配置具有全局性，对所有用户组有效，用户组视图下的配置对用户组内所有本地用户有效，本地用户视图下的配置只对当前本地用户有效。

该配置的生效优先级顺序由高到低依次为本地用户视图、用户组视图、全局视图。即，系统优先采用本地用户视图下的配置，若本地用户视图下未配置，则采用用户组视图下的配置，若用户组视图下也未配置，则采用全局视图下的配置。

【举例】

```
# 配置全局的密码老化时间为 80 天。  
<Sysname> system-view  
[Sysname] password-control aging 80  
# 配置用户组 test 的密码老化时间为 90 天。  
[Sysname] user-group test  
[Sysname-ugroup-test] password-control aging 90  
[Sysname-ugroup-test] quit  
# 配置设备管理类本地用户 abc 的密码老化时间为 100 天。  
[Sysname] local-user abc class manage  
[Sysname-luser-manage-abc] password-control aging 100
```

【相关命令】

- **display local-user**（安全命令参考/AAA）
- **display password-control**
- **display user-group**（安全命令参考/AAA）
- **password-control aging enable**

1.1.5 password-control alert-before-expire

password-control alert-before-expire 命令用来配置密码过期前的提醒时间。

undo password-control alert-before-expire 命令用来恢复缺省情况。

【命令】

```
password-control alert-before-expire alert-time
undo password-control alert-before-expire
```

【缺省情况】

密码过期前的提醒时间为 7 天，表示在密码过期之前 7 天内，系统会在用户登录时提醒其密码即将过期。

【视图】

系统视图

【缺省用户角色】

network-admin

【参数】

alert-time：密码过期前的提醒时间，取值范围为 1~30，单位为天。

【使用指导】

不允许 FTP 用户更改密码，只能由管理员修改 FTP 用户的密码，因此本命令配置的过期提醒时间仅对非 FTP 类型的 Login 用户有效。

【举例】

设定密码过期前的提醒时间为 10 天。

```
<Sysname> system-view
[Sysname] password-control alert-before-expire 10
```

【相关命令】

- **display password-control**

1.1.6 password-control complexity

password-control complexity 命令用来配置用户密码的复杂度检查策略。

undo password-control complexity 命令用来取消指定的密码复杂度检查策略。

【命令】

```
password-control complexity { same-character | user-name } check
undo password-control complexity { same-character | user-name } check
```

【缺省情况】

全局的密码复杂度检查策略为：不对用户密码进行复杂度检查，允许密码中包含用户名或者字符顺序颠倒的用户名，也允许包含连续三个或以上的相同字符；用户组的密码复杂度检查策略为全局的密码复杂度检查策略；本地用户的密码复杂度检查策略为所属用户组的密码复杂度检查策略。

【视图】

系统视图
用户组视图
本地用户视图

【缺省用户角色】

network-admin

【参数】

same-character: 指定检查密码中是否包含连续三个或以上相同的字符。例如，密码 **aaabc** 就不符合该项复杂度检查。

user-name: 指定检查密码中是否包含用户名或者字符顺序颠倒的用户名。例如，用户名为 **123**，则密码 **abc123**、**321df** 就不符合该项复杂度检查。

【使用指导】

系统视图下配置具有全局性，对所有用户组有效，用户组视图下的配置对用户组内所有本地用户有效，本地用户视图下的配置只对当前本地用户有效。

该配置的生效优先级顺序由高到低依次为本地用户视图、用户组视图、全局视图。即，系统优先采用本地用户视图下的配置，若本地用户视图下未配置，则采用用户组视图下的配置，若用户组视图下也未配置，则采用全局视图下的配置。

可以通过多次执行本命令同时打开用户名检查以及连续字符检查功能。

【举例】

配置密码复杂度检测策略为，检查配置的密码中是否包含用户名或者字符顺序颠倒的用户名。

```
<Sysname> system-view  
[Sysname] password-control complexity user-name check
```

【相关命令】

- **display local-user**（安全命令参考/AAA）
- **display password-control**
- **display user-group**（安全命令参考/AAA）

1.1.7 password-control composition

password-control composition 命令用来配置用户密码的组合策略。

undo password-control composition 命令用来恢复缺省情况。

【命令】

```
password-control composition type-number type-number [ type-length  
type-length ]  
undo password-control composition
```

【缺省情况】

非 FIPS 模式下：

全局的密码元素的最少组合类型为 1 种，至少要包含每种元素的个数为 1 个；用户组的密码组合策略为全局配置的密码组合策略；本地用户的密码组合策略为所属用户组的密码组合策略。

FIPS 模式下：

全局的密码元素的最少组合类型为 4 种，至少要包含每种元素的个数为 1 个；用户组的密码组合策略为全局配置的密码组合策略；本地用户的密码组合策略为所属用户组的密码组合策略。

【视图】

系统视图

用户组视图

本地用户视图

【缺省用户角色】

network-admin

【参数】

type-number *type-number*：密码元素的最少组合类型。其中，*type-number* 表示组合类型的个数，非 FIPS 模式下，取值范围为 1~4；FIPS 模式下，取值为 4。

type-length *type-length*：密码中至少要包含每种元素的个数。其中，*type-length* 表示元素个数，非 FIPS 模式下，取值范围为 1~63；FIPS 模式下，取值范围为 1~15。

【使用指导】

系统视图下配置具有全局性，对所有用户组有效，用户组视图下的配置对用户组内所有本地用户有效，本地用户视图下的配置只对当前本地用户有效。

该配置的生效优先级顺序由高到低依次为本地用户视图、用户组视图、全局视图。即，系统优先采用本地用户视图下的配置，若本地用户视图下未配置，则采用用户组视图下的配置，若用户组视图下也未配置，则采用全局视图下的配置。

密码元素的最少组合类型数以及每种元素的最小个数的乘积应该小于允许的最大密码长度。

【举例】

配置全局的密码元素的最少组合类型为 4 种，至少要包含每种元素的个数为 5 个。

```
<Sysname> system-view
```

```
[Sysname] password-control composition type-number 4 type-length 5
```

配置用户组 test 的密码元素的最少组合类型为 4 种，至少要包含每种元素的个数为 5 个。

```
[Sysname] user-group test
```

```
[Sysname-ugroup-test] password-control composition type-number 4 type-length 5
```

```
[Sysname-ugroup-test] quit
```

配置设备管理类本地用户 abc 的密码元素的最少组合类型为 4 种，至少要包含每种元素的个数为 5 个。

```
[Sysname] local-user abc class manage
```

```
[Sysname-luser-manage-abc] password-control composition type-number 4 type-length 5
```

【相关命令】

- **display local-user**（安全命令参考/AAA）
- **display password-control**
- **display user-group**（安全命令参考/AAA）

- `password-control composition enable`

1.1.8 password-control enable

`password-control enable` 命令用来使能全局密码管理功能。

`undo password-control enable` 命令用来关闭全局密码管理功能。

【命令】

```
password-control enable
undo password-control enable
```

【缺省情况】

非 FIPS 模式下：

全局密码管理功能处于关闭状态。

FIPS 模式下：

全局密码管理功能处于开启状态，且不能关闭。

【视图】

系统视图

【缺省用户角色】

network-admin

【使用指导】

只有在使能了全局密码管理功能的情况下，其它指定的密码管理功能才能生效。

使能全局密码管理功能后，设备管理类本地用户密码以及 **super** 密码的配置将不被显示，即无法通过相应的 **display** 命令查看到设备管理类本地用户密码以及 **super** 密码的配置。网络接入类本地用户密码不受密码管理功能控制，其配置显示也不受影响。

使能全局密码管理功能后，首次设置的设备管理类本地用户密码必须至少由四个不同的字符组成。

【举例】

使能全局密码管理功能。

```
<Sysname> system-view
[Sysname] password-control enable
```

【相关命令】

- `display password-control`
- `password-control { aging | composition | history | length } enable`

1.1.9 password-control expired-user-login

`password-control expired-user-login` 命令用来配置密码过期后允许用户登录的时间和次数。

`undo password-control expired-user-login` 命令用来恢复缺省情况。

【命令】

```
password-control expired-user-login delay delay times times
```

undo password-control expired-user-login

【缺省情况】

密码过期后允许登录的时间为 30 天，允许登录的次数为 3 次，即密码过期后系统还允许用户在 30 天内使用老密码登录 3 次，超过 30 天或登录次数超过 3 次后，系统提示用户设置新密码。

【视图】

系统视图

【缺省用户角色】

network-admin

【参数】

delay *delay*: 密码过期后允许用户登录的时长，取值范围为 1~90，单位为天。

times *times*: 密码过期后允许用户登录的最大次数，取值范围为 0~10。0 表示密码过期后系统直接提示用户设置新密码。

【使用指导】

该配置仅对非 FTP 类型的 Login 用户生效。对于 FTP 用户，密码过期后，系统不允许其继续登录。

【举例】

设定允许用户在密码过期之后的 60 天内登录 5 次。

```
<Sysname> system-view
```

```
[Sysname] password-control expired-user-login delay 60 times 5
```

【相关命令】

- **display password-control**

1.1.10 password-control history

password-control history 命令用来配置每个用户密码历史记录的最大条数。

undo password-control history 命令用来恢复缺省情况。

【命令】

password-control history *max-record-number*

undo password-control history

【缺省情况】

每个用户密码历史记录的最大条数为 4 条。

【视图】

系统视图

【缺省用户角色】

network-admin

【参数】

max-record-number: 每个用户密码历史记录的最大条数，取值范围为 2~15。

【使用指导】

当记录的某用户的历史密码条数达到最大值后，该用户的后续新密码历史记录将覆盖最老的一条密码历史记录。

密码历史记录管理功能关闭后，系统将不再记录历史密码，但之前已经存在的密码历史记录依然保存。只有当关闭全局密码管理功能（**undo password-control enable**）或手动清除历史记录时（**reset password-control history-record**），历史密码记录才会被清除掉。

【举例】

配置每个用户密码历史记录的最大条数为 10 条。

```
<Sysname> system-view
[Sysname] password-control history 10
```

【相关命令】

- **display password-control**
- **password-control history enable**
- **reset password-control blacklist**

1.1.11 password-control length

password-control length 命令用来配置密码的最小长度。

undo password-control length 命令用来恢复缺省情况。

【命令】

```
password-control length length
undo password-control length
```

【缺省情况】

非 FIPS 模式下：

全局的密码最小长度为 10 个字符；用户组的密码最小长度为全局配置的密码最小长度；本地用户的密码最小长度为所属用户组的密码最小长度。

FIPS 模式下：

全局的密码最小长度为 15 个字符；用户组的密码最小长度为全局配置的密码最小长度；本地用户的密码最小长度为所属用户组的密码最小长度。

【视图】

系统视图

用户组视图

本地用户视图

【缺省用户角色】

network-admin

【参数】

length：密码的最小长度，非 FIPS 模式下，取值范围为 4~32；FIPS 模式下，取值范围为 15~32。

【使用指导】

系统视图下配置具有全局性，对所有用户组有效，用户组视图下的配置对用户组内所有本地用户有效，本地用户视图下的配置只对当前本地用户有效。

该配置的生效优先级顺序由高到低依次为本地用户视图、用户组视图、全局视图。即，系统优先采用本地用户视图下的配置，若本地用户视图下未配置，则采用用户组视图下的配置，若用户组视图下也未配置，则采用全局视图下的配置。

【举例】

```
# 配置全局的密码最小长度为 16 个字符。
<Sysname> system-view
[Sysname] password-control length 16
# 配置用户组 test 的密码最小长度为 16 个字符。
[Sysname] user-group test
[Sysname-ugroup-test] password-control length 16
[Sysname-ugroup-test] quit
# 配置设备管理类本地用户 abc 的密码最小长度为 16 个字符。
[Sysname] local-user abc class manage
[Sysname-luser-manage-abc] password-control length 16
```

【相关命令】

- **display local-user**（安全命令参考/AAA）
- **display password-control**
- **display user-group**（安全命令参考/AAA）
- **password-control length enable**

1.1.12 password-control login idle-time

password-control login idle-time 命令用来配置用户帐号的闲置时间。

undo password-control login idle-time 命令用来恢复缺省情况。

【命令】

```
password-control login idle-time idle-time
undo password-control login idle-time
```

【缺省情况】

用户帐号的闲置时间为 90 天。

【视图】

系统视图

【缺省用户角色】

network-admin

【参数】

idle-time：用户帐号的闲置时间，取值范围为 0～365，单位为天。0 表示对用户帐号闲置时间无限制。

【使用指导】

如果用户自最后一次成功登录后，在指定的闲置时间内再未成功登录过设备，那么该用户帐号将会失效。

【举例】

设定用户帐号的闲置时间为 30 天，表示自最后一次成功登录后，若用户在 30 天内再未成功登录过设备，那么该用户帐号将会失效。

```
<Sysname> system-view
[Sysname] password-control login idle-time 30
```

【相关命令】

- **display password-control**

1.1.13 password-control login-attempt

password-control login-attempt 命令用来配置允许用户登录的最大尝试次数以及登录尝试失败后的处理措施。

undo password-control login-attempt 命令用来恢复缺省情况。

【命令】

```
password-control login-attempt login-times [ exceed { lock | lock-time time
| unlock } ]
undo password-control login-attempt
```

【缺省情况】

全局的用户登录尝试次数限制策略为：用户登录尝试的最大次数为 3 次。如果某用户登录尝试失败，则 1 分钟后再允许该用户重新登录；用户组的用户登录尝试次数限制策略为全局配置的用户登录尝试次数限制策略；本地用户的登录尝试次数限制策略为所属用户组的用户登录尝试次数限制策略。

【视图】

系统视图

用户组视图

本地用户视图

【缺省用户角色】

network-admin

【参数】

login-times：用户登录尝试的最大次数，取值范围为 2~10。

exceed：对登录尝试失败次数超过最大值的用户所采取的处理措施。

lock：表示永久禁止该用户登录。

lock-time time：表示禁止该用户一段时间后，再允许该用户重新登录。其中，*time* 为禁止该用户的时间，取值范围为 1~360，单位为分钟。

unlock：表示不禁止该用户，允许其继续登录。

【使用指导】

系统视图下配置具有全局性，对所有用户组有效，用户组视图下的配置对用户组内所有本地用户有效，本地用户视图下的配置只对当前本地用户有效。

该配置的生效优先级顺序由高到低依次为本地用户视图、用户组视图、全局视图。即，系统优先采用本地用户视图下的配置，若本地用户视图下未配置，则采用用户组视图下的配置，若用户组视图下也未配置，则采用全局视图下的配置。

FTP 用户或通过 VTY 方式访问设备的用户登录认证失败后，系统会将其用户名和 IP 地址加入密码管理的黑名单。当登录失败次数超过指定值后，系统将会根据此处配置的处理措施对其之后的登录行为进行相应的限制，并且该用户只能在满足相应的条件后才可重新登录：

- 对于被永久禁止登录的用户，只有管理员使用 **reset password-control blacklist** 命令把该用户从密码管理的黑名单中删除后，该用户才能重新登录。
- 对于被禁止一段时间内登录的用户，当配置的禁止时间超时或者管理员使用 **reset password-control blacklist** 命令将其从密码管理的黑名单中删除，该用户才可以重新登录。
- 对于不禁止登录的用户，只要用户登录成功后，该用户就会从该黑名单中删除。

本命令生效后，会立即影响密码管理黑名单中当前用户的锁定状态以及这些用户后续的登录。

【举例】

管理员设定用户登录尝试次数为 4 次，并且永久禁止该用户登录。

```
<Sysname> system-view
```

```
[Sysname] password-control login-attempt 4 exceed lock
```

之后，若有用户连续尝试认证的失败累加次数达到 4 次，管理员可通过命令查看到被加入密码管理黑名单中的用户锁定状态由之前的 **unlock** 切换为 **lock**，且该用户无法再次成功登录。

```
[Sysname] display password-control blacklist
```

```
Username: test
```

```
IP: 192.168.44.1
```

```
Login failures: 4
```

```
Lock flag: lock
```

```
Blacklist items matched: 1.
```

管理员设定用户登录尝试次数为 2 次，并且限制该用户在 3 分钟后才能重新登录。

```
<Sysname> system-view
```

```
[Sysname] password-control login-attempt 2 exceed lock-time 3
```

之后，若有用户连续尝试认证的失败累加次数达到 2 次，管理员可通过命令查看到被加入密码管理黑名单中的用户锁定状态由之前的 **unlock** 切换为 **lock**。

```
[Sysname] display password-control blacklist
```

```
Username: test
```

```
IP: 192.168.44.1
```

```
Login failures: 2
```

```
Lock flag: lock
```

```
Blacklist items matched: 1.
```

用户被禁止登录 3 分钟后，将被从密码管理黑名单中删除，且可以重新登录。

【相关命令】

- **display local-user**（安全命令参考/AAA）

- `display password-control`
- `display password-control blacklist`
- `display user-group`（安全命令参考/AAA）
- `reset password-control blacklist`

1.1.14 password-control super aging

`password-control super aging` 命令用来配置 super 密码的老化时间。

`undo password-control super aging` 命令用来恢复缺省情况。

【命令】

```
password-control super aging aging-time
undo password-control super aging
```

【缺省情况】

密码的老化时间为 90 天。

【视图】

系统视图

【缺省用户角色】

network-admin

【参数】

aging-time: super 密码的老化时间，取值范围为 1~365，单位为天。

【举例】

设定 super 密码的老化时间为 10 天。

```
<Sysname> system-view
[Sysname] password-control super aging 10
```

【相关命令】

- `display password-control`
- `password-control aging`

1.1.15 password-control super composition

`password-control super composition` 命令用来配置 super 密码的组合策略。

`undo password-control super composition` 命令用来恢复缺省情况。

【命令】

```
password-control super composition type-number type-number [ type-length
type-length ]
undo password-control super composition
```

【缺省情况】

非 FIPS 模式下：

super 密码的最少组合类型为 1 种，每种类型至少包含 1 个字符。

FIPS 模式下：

super 密码的最少组合类型为 4 种，每种类型至少包含 1 个字符。

【视图】

系统视图

【缺省用户角色】

network-admin

【参数】

type-number *type-number*: super 密码的最少组合类型。其中，*type-number* 表示组合类型，非 FIPS 模式下，取值范围为 1~4；FIPS 模式下，取值为 4。

type-length *type-length*: super 密码中每种类型的最少字符个数。其中，*type-length* 表示字符个数，非 FIPS 模式下，取值范围为 1~63；FIPS 模式下，取值范围为 1~15。

【使用指导】

密码元素的最少组合类型数以及每种元素的最小个数的乘积应该小于密码允许的最大长度。

【举例】

配置 super 密码的最少组合类型为 4 种，每种类型的最少字符个数为 5 个。

```
<Sysname> system-view
```

```
[Sysname] password-control super composition type-number 4 type-length 5
```

【相关命令】

- **display password-control**
- **password-control composition**

1.1.16 password-control super length

password-control super length 命令用来配置 super 密码的最小长度。

undo password-control super length 命令用来恢复缺省情况。

【命令】

```
password-control super length length
```

```
undo password-control super length
```

【缺省情况】

非 FIPS 模式下：

super 密码的最小长度为 10 个字符。

FIPS 模式下：

super 密码的最小长度为 15 个字符。

【视图】

系统视图

【缺省用户角色】

network-admin

【参数】

length: **super** 密码的最小字符长度，非 FIPS 模式下，取值范围为 4~63；FIPS 模式下，取值范围为 15~63。

【举例】

设定 **super** 密码的最小长度为 16 个字符。

```
<Sysname> system-view
[Sysname] password-control super length 16
```

【相关命令】

- **display password-control**
- **password-control length**

1.1.17 password-control update-interval

password-control update-interval 命令用来配置密码更新的最小时间间隔。

undo password-control update-interval 命令用来恢复缺省情况。

【命令】

```
password-control update-interval interval
undo password-control update-interval
```

【缺省情况】

密码更新的最小时间间隔为 24 小时。

【视图】

系统视图

【缺省用户角色】

network-admin

【参数】

interval: 密码更新的最小时间间隔，取值范围为 0~168，单位为小时。0 表示对密码更新的时间间隔无限制。

【使用指导】

有两种情况下的密码更新并不受该功能的约束：用户首次登录设备时系统要求用户修改密码；密码老化后系统要求用户修改密码。

【举例】

设定密码更新的最小时间间隔为 36 小时。

```
<Sysname> system-view
[Sysname] password-control update-interval 36
```

【相关命令】

- **display password-control**

1.1.18 reset password-control blacklist

reset password-control blacklist 命令用来清除密码管理黑名单中的用户。

【命令】

```
reset password-control blacklist [ user-name user-name ]
```

【视图】

用户视图

【缺省用户角色】

network-admin

【参数】

user-name *user-name*: 清除密码管理黑名单中指定的用户。其中, *user-name* 表示用户名, 为 1~55 个字符的字符串, 区分大小写。

【使用指导】

对于因为登录认证时密码尝试的失败次数超过最大值而被禁止登录的用户, 管理员可以使用本命令将其从黑名单中删除, 使其可以重新登录。

【举例】

清除密码管理黑名单中的用户 test。

```
<Sysname> reset password-control blacklist user-name test
Are you sure to delete the specified user in blacklist? [Y/N]:
```

【相关命令】

- **display password-control blacklist**

1.1.19 reset password-control history-record

reset password-control history-record 命令用来清除用户的密码历史记录。

【命令】

```
reset password-control history-record [ super [ role role-name ] | user-name
user-name ]
```

【视图】

用户视图

【缺省用户角色】

network-admin

【参数】

super: 删除 super 密码的历史记录。

role *role-name*: 删除指定用户角色的用户密码历史记录。其中, *role-name* 表示用户角色, 为 1~63 个字符的字符串, 区分大小写。如果不指定参数此参数, 将删除所有 super 密码的历史记录。

user-name *user-name*: 删除指定用户名的密码历史记录。其中，*user-name* 表示用户名，为 1~55 个字符的字符串，区分大小写。

【使用指导】

如果不指定任何参数，将删除所有本地用户的密码历史记录。

【举例】

清除所有本地用户的密码历史记录。当用户输入 Y，系统将删除所有本地用户的密码历史记录。

```
<Sysname> reset password-control history-record
```

```
Are you sure to delete all local user's history records? [Y/N]:y
```

【相关命令】

- **password-control history**

目 录

1 公钥管理.....	1-1
1.1 公钥管理配置命令.....	1-1
1.1.1 display public-key local public.....	1-1
1.1.2 display public-key peer	1-5
1.1.3 peer-public-key end.....	1-6
1.1.4 public-key local create	1-7
1.1.5 public-key local destroy.....	1-11
1.1.6 public-key local export dsa.....	1-12
1.1.7 public-key local export ecdsa	1-15
1.1.8 public-key local export rsa	1-16
1.1.9 public-key peer.....	1-18
1.1.10 public-key peer import sshkey.....	1-19

1 公钥管理



说明

设备运行于 FIPS 模式时，本特性部分配置相对于非 FIPS 模式有所变化，具体差异请见本文相关描述。有关 FIPS 模式的详细介绍请参见“安全配置指导”中的“FIPS”。

1.1 公钥管理配置命令

1.1.1 display public-key local public

display public-key local public 命令用来显示本地非对称密钥对中的公钥信息。

【命令】

display public-key local { dsa | ecdsa | rsa } public [name key-name]

【视图】

任意视图

【缺省用户角色】

network-admin
network-operator

【参数】

dsa：显示本地 DSA 密钥对中的公钥信息。

ecdsa：显示本地 ECDSA 密钥对中的公钥信息。

rsa：显示本地 RSA 密钥对中的公钥信息。

name key-name：显示指定的本地非对称密钥对的公钥信息。*key-name* 为本地非对称密钥对的名称，为 1~64 个字符的字符串，不区分大小写，字符串中可以包含字母、数字及“-”。如果不指定本参数，则显示指定类型的所有本地非对称密钥对的公钥信息。

【使用指导】

如果通过手工配置方式将本地的主机公钥保存到远端设备上，则需要事先在本地设备上执行本命令显示主机公钥信息，并记录该信息。

对于默认名称的密钥对，不能通过指定 **name key-name** 参数显示；显示指定类型的所有本地非对称密钥对时会显示默认名称的密钥对。

【举例】

显示所有本地 RSA 密钥对中的公钥信息。

```
<Sysname> display public-key local rsa public
```

```
=====
```

```
Key name: hostkey (default)
Key type: RSA
Time when key pair created: 15:40:48 2011/05/12
Key code:
30819F300D06092A864886F70D010101050003818D0030818902818100DAA4AAFEFE04C2C9
667269BB8226E26331E30F41A8FF922C7338208097E84332610632B49F75DABF6D871B80CE
C1BA2B75020077C74745C933E2F390DC0B39D35B88283D700A163BB309B19F8F87216A44AB
FBF6A3D64DEB33E5CEBF2BCF26296778A26A84F4F4C5DBF8B656ACFA62CD96863474899BC1
2DA4C04EF5AE0835090203010001
```

=====

```
Key name: serverkey (default)
Key type: RSA
Time when key pair created: 15:40:48 2011/05/12
Key code:
307C300D06092A864886F70D0101010500036B003068026100CAB4CACCA16442AD5F453442
762F03897E0D494FEDE69224F5C051A441D290976733A278C9F0C0F5A198E66143EAB54A64
DB608269CAE844B1E7CC64AD7E808972E7CF887F3B657F056E7930FC84FBF1AD83A01CC47E
9D85C13413996ECD093B0203010001
```

=====

```
Key name: rsal
Key type: RSA
Time when key pair created: 15:42:26 2011/05/12
Key code:
30819F300D06092A864886F70D010101050003818D0030818902818100DEBC46F217DDF11D
426E7095AA45CD6BF1F87343D952569AC223A01365E0D8C91D49D347C143C5D8FAADA896AA
1A827E580F2502F1926F52197230E1DE391A64015C43DD79DC4E9E171BAEA1DEB4C71DAED7
9A6EDFD460D8945D27D39B7C9822D56AEA5B7C2CCFF1B6BC524AD498C3B87D4BD6EB36AF03
92D8C6D940890BF4290203010001
```

显示所有本地 DSA 密钥对中的公钥信息。

<Sysname> display public-key local dsa public

=====

```
Key name: dsakey (default)
Key type: DSA
Time when key pair created: 15:41:37 2011/05/12
Key code:
308201B73082012C06072A8648CE3804013082011F02818100D757262C4584C44C211F18BD
96E5F061C4F0A423F7FE6B6B85B34CEF72CE14A0D3A5222FE08CECE65BE6C265854889DC1E
DBD13EC8B274DA9F75BA26CCB987723602787E922BA84421F22C3C89CB9B06FD60FE01941D
DD77FE6B12893DA76EEBC1D128D97F0678D7722B5341C8506F358214B16A2FAC4B36895038
7811C7DA33021500C773218C737EC8EE993B4F2DED30F48EDACE915F0281810082269009E1
4EC474BAF2932E69D3B1F18517AD9594184CCDFCEAE96EC4D5EF93133E84B47093C52B20CD
35D02492B3959EC6499625BC4FA5082E22C5B374E16DD00132CE71B020217091AC717B6123
91C76C1FB2E88317C1BD8171D41ECB83E210C03CC9B32E810561C21621C73D6DAAC028F4B1
585DA7F42519718CC9B09EEF0381840002818041912CE34D12BCD2157E7AB1C2F03B3EF395
100F3DB4A9E2FDFE860C1BD663D676438F7DA40A9406D61CA9079AF13E330489F1C76785DE
52DA649AC8BC04B6D39CD7C52CD0A14F75F7491A91D31D6AC22340B5981B27A915CDEC4F09
887E541EC1E5302D500F68E7AC29A084463C60F9EE266985A502FC92193E1CF4D265C4BA
```

```

=====
Key name: dsal
Key type: DSA
Time when key pair created: 15:35:42 2011/05/12
Key code:
    308201B83082012C06072A8648CE3804013082011F02818100D757262C4584C44C211F18BD
    96E5F061C4F0A423F7FE6B6B85B34CEF72CE14A0D3A5222FE08CECE65BE6C265854889DC1E
    DBD13EC8B274DA9F75BA26CCB987723602787E922BA84421F22C3C89CB9B06FD60FE01941D
    DD77FE6B12893DA76EEBC1D128D97F0678D7722B5341C8506F358214B16A2FAC4B36895038
    7811C7DA33021500C773218C737EC8EE993B4F2DED30F48EDACE915F0281810082269009E1
    4EC474BAF2932E69D3B1F18517AD9594184CCDFCEAE96EC4D5EF93133E84B47093C52B20CD
    35D02492B3959EC6499625BC4FA5082E22C5B374E16DD00132CE71B020217091AC717B6123
    91C76C1FB2E88317C1BD8171D41ECB83E210C03CC9B32E810561C21621C73D6DAAC028F4B1
    585DA7F42519718CC9B09EEF0381850002818100A1E456C8DA2AD1BB83B1BDF2A1A6B5A6E8
    3642B460402445DA7E4036715F468F76655E114D460B7112F57143EE020AEF4A5BFAD07B74
    0FBCB1C64DA8A2BCE619283421445EEC77D3CF0D11866E9656AD6511F4926F8376967B0AB7
    15F9FB7B514BC1174155DD6E073B1FCB3A2749E6C5FEA81003E16729497D0EAD9105E3E76A

```

显示所有本地 ECDSA 密钥对中的公钥信息。

```
<Sysname> display public-key local ecdsa public
```

```

=====
Key name: ecdsakey (default)
Key type: ECDSA
Time when key pair created: 15:42:04 2011/05/12
Key code:
    3049301306072A8648CE3D020106082A8648CE3D03010103320004C10CF7CE42193F7FC2AF
    68F5DC877835A43009DB6135558A7FB8316C361B0690B4FD84A14C0779C76DD6145BF9362B
    1D

```

```

=====
Key name: ecdsal
Key type: ECDSA
Time when key pair created: 15:43:33 2011/05/12
Key code:
    3049301306072A8648CE3D020106082A8648CE3D03010103320004A1FB84D92315B8DB72D1
    AE672C7CFA5135D5F5B02377F2F092F182EC83B5819795BC94CCBD3EBA7D4F0F2B2EB20C58
    4D

```

显示名称为 rsa1 的本地 RSA 密钥对中的公钥信息。

```
<Sysname> display public-key local rsa public name rsa1
```

```

=====
Key name: rsal
Key type: RSA
Time when key pair created: 15:42:26 2011/05/12
Key code:
    30819F300D06092A864886F70D010101050003818D0030818902818100DEBC46F217DDF11D
    426E7095AA45CD6BF1F87343D952569AC223A01365E0D8C91D49D347C143C5D8FAADA896AA
    1A827E580F2502F1926F52197230E1DE391A64015C43DD79DC4E9E171BAEA1DEB4C71DAED7
    9A6EDFD460D8945D27D39B7C9822D56AEA5B7C2CCFF1B6BC524AD498C3B87D4BD6EB36AF03

```

```
92D8C6D940890BF4290203010001
# 显示名称为 dsa1 的本地 DSA 密钥对中的公钥信息。
<Sysname> display public-key local dsa public name dsa1

=====
Key name: dsa1
Key type: DSA
Time when key pair created: 15:35:42 2011/05/12
Key code:
    308201B83082012C06072A8648CE3804013082011F02818100D757262C4584C44C211F18BD
    96E5F061C4F0A423F7FE6B6B85B34CEF72CE14A0D3A5222FE08CECE65BE6C265854889DC1E
    DBD13EC8B274DA9F75BA26CCB987723602787E922BA84421F22C3C89CB9B06FD60FE01941D
    DD77FE6B12893DA76EEBC1D128D97F0678D7722B5341C8506F358214B16A2FAC4B36895038
    7811C7DA33021500C773218C737EC8EE993B4F2DED30F48EDACE915F0281810082269009E1
    4EC474BAF2932E69D3B1F18517AD9594184CCDFCEAE96EC4D5EF93133E84B47093C52B20CD
    35D02492B3959EC6499625BC4FA5082E22C5B374E16DD00132CE71B020217091AC717B6123
    91C76C1FB2E88317C1BD8171D41ECB83E210C03CC9B32E810561C21621C73D6DAAC028F4B1
    585DA7F42519718CC9B09EEF0381850002818100A1E456C8DA2AD1BB83B1BDF2A1A6B5A6E8
    3642B460402445DA7E4036715F468F76655E114D460B7112F57143EE020AEF4A5BFAD07B74
    0FBCB1C64DA8A2BCE619283421445EEC77D3CF0D11866E9656AD6511F4926F8376967B0AB7
    15F9FB7B514BC1174155DD6E073B1FCB3A2749E6C5FEA81003E16729497D0EAD9105E3E76A
```

```
# 显示名称为 ecdsa1 的本地 ECDSA 密钥对中的公钥信息。
<Sysname> display public-key local ecdsa public name ecdsa1

=====
Key name: ecdsa1
Key type: ECDSA
Time when key pair created: 15:43:33 2011/05/12
Key code:
    3049301306072A8648CE3D020106082A8648CE3D03010103320004A1FB84D92315B8DB72D1
    AE672C7CFA5135D5F5B02377F2F092F182EC83B5819795BC94CCBD3EBA7D4F0F2B2EB20C58
    4D
```

表1-1 display public-key local public 命令显示信息描述表

字段	描述
Key name	本地非对称密钥对的名称 default表示该名称为密钥对的默认名称，即执行 public-key local create 命令没有指定密钥名称时，生成的密钥对的名称 <ul style="list-style-type: none">hostkey: RSA 主机密钥对的默认名称serverkey: RSA 服务器密钥对的默认名称。只有密钥类型为 RSA 时，才会存在服务器密钥对dsakey: DSA 主机密钥对的默认名称ecdsakey: ECDSA 主机密钥对的默认名称

字段	描述
Key type	密钥类型，取值包括： <ul style="list-style-type: none"> • RSA：密钥类型为 RSA • DSA：密钥类型为 DSA • ECDSA：密钥类型为 ECDSA
Time when key pair created	本地非对称密钥对产生的时间
Key code	本地非对称密钥对的公钥数据

【相关命令】

- `public-key local create`

1.1.2 display public-key peer

`display public-key peer` 命令用来显示保存在本地的远端主机的公钥信息。

【命令】

`display public-key peer [brief | name publickey-name]`

【视图】

任意视图

【缺省用户角色】

network-admin
network-operator

【参数】

brief：显示保存在本地的所有远端主机公钥的简要信息。

name publickey-name：显示保存在本地的指定远端主机公钥的详细信息，*publickey-name* 为远端主机公钥的名称，为 1~64 个字符的字符串，区分大小写。

【使用指导】

如果没有指定任何参数，则显示所有保存在本地的远端主机公钥的详细信息。

可以通过 `public-key peer` 命令或 `public-key peer import sshkey` 命令将远端主机的公钥配置到本地。

【举例】

显示保存在本地的公钥名称为 `idrsa` 的远端主机公钥的详细信息。

```
<Sysname> display public-key peer name idrsa
```

```
=====
```

```
Key name: idrsa
```

```
Key type: RSA
```

```
Key modulus: 1024
```

```
Key code:
```

```
30819F300D06092A864886F70D010101050003818D0030818902818100C5971581A78B5388
```

```
B3C9063EC6B53D395A6704D9752B6F9B7B1F734EEB5DD509F0B050662C46FFB8D27F797E37
918F6270C5793F1FC63638970A0E4D51A3CEF7CFF6E92BFAFD73F530E0BDE27056E81F2525
6D0883836FD8E68031B2C272FE2EA75C87734A7B8F85B8EBEB3BD51CC26916AF3B3FDC32C3
42C142D41BB4884FEB0203010001
```

表1-2 display public-key peer name 命令显示信息描述表

字段	描述
Key name	远端主机公钥的名称
Key type	密钥类型，取值包括RSA、DSA和ECDSA
Key modulus	密钥模数的长度，单位为比特
Key code	公钥数据

显示保存在本地的所有远端主机公钥的简要信息。

```
<Sysname> display public-key peer brief
Type  Modulus  Name
-----
RSA   1024      idrsa
DSA   1024      10.1.1.1
```

表1-3 display public-key peer brief 命令显示信息描述表

字段	描述
Type	密钥类型，取值包括RSA、DSA和ECDSA
Modulus	密钥模数的长度，单位为比特
Name	远端主机公钥的名称

【相关命令】

- public-key peer
- public-key peer import sshkey

1.1.3 peer-public-key end

peer-public-key end 命令用来从公钥视图退回到系统视图，并保存用户输入的公钥。

【命令】

```
peer-public-key end
```

【视图】

公钥视图

【缺省用户角色】

network-admin

【使用指导】

本命令用于通过手工配置方式将远端主机的公钥保存到本地设备上。手工配置方式是指：

- (1) 执行 **public-key peer** 命令进入公钥视图。
- (2) 在公钥视图手工输入远端主机的公钥。
- (3) 执行 **peer-public-key end** 命令退出公钥视图，并保存输入的公钥。

输入的公钥数据必须满足一定的格式要求。在保存公钥之前，设备会进行公钥合法性的检测：

- 如果用户配置的公钥字符串不满足格式要求，那么将会显示相关提示信息，用户配置的公钥将被丢弃，本次配置失败；
- 如果用户配置的公钥字符串合法，例如输入的公钥数据为通过 **display public-key local public** 命令显示的公钥，则保存该公钥。

【举例】

退出公钥视图，并保存用户输入的公钥。

```
<Sysname> system-view
[Sysname] public-key peer key1
Enter public key view. Return to system view with "peer-public-key end" command.
[Sysname-pkey-public-key-key1]30819F300D06092A864886F70D010101050003818D0030818902818100
C0EC8014F82515F6335A0A
[Sysname-pkey-public-key-key1]EF8F999C01EC94E5760A079BD73E4F4D97F3500EDB308C29481B77E719
D1643135877E13B1C531B4
[Sysname-pkey-public-key-key1]FF1877A5E2E7B1FA4710DB0744F66F6600EEFE166F1B854E2371D5B952
ADF6B80EB5F52698FCF3D6
[Sysname-pkey-public-key-key1]1F0C2EAAD9813ECB16C5C7DC09812D4EE3E9A0B074276FFD4AF2050BD4
A9B1DDE675AC30CB020301
[Sysname-pkey-public-key-key1]0001
[Sysname-pkey-public-key-key1] peer-public-key end
[Sysname]
```

【相关命令】

- **display public-key local public**
- **display public-key peer**
- **public-key peer**

1.1.4 public-key local create

public-key local create 命令用来生成本地非对称密钥对。

【命令】

非 FIPS 模式下：

```
public-key local create { dsa | ecdsa [ secp192r1 | secp256r1 | secp384r1 |  
secp521r1 ] | rsa } [ name key-name ]
```

FIPS 模式下：

```
public-key local create { dsa | ecdsa [ secp256r1 | secp384r1 | secp521r1 ]  
| rsa } [ name key-name ]
```

【缺省情况】

不存在本地非对称密钥对。

【视图】

系统视图

【缺省用户角色】

network-admin

【参数】

dsa: 本地密钥对类型为 DSA。

ecdsa: 本地密钥对类型为 ECDSA。

- **secp192r1**: 采用名称为 secp192r1 的椭圆曲线生成本地 ECDSA 密钥对，密钥长度为 192 比特。
- **secp256r1**: 采用名称为 secp256r1 的椭圆曲线生成本地 ECDSA 密钥对，密钥长度为 256 比特。
- **secp384r1**: 采用名称为 secp384r1 的椭圆曲线生成本地 ECDSA 密钥对，密钥长度为 384 比特。
- **secp521r1**: 采用名称为 secp521r1 的椭圆曲线生成本地 ECDSA 密钥对，密钥长度为 521 比特。

如果不指定以上任一种密钥对算法参数，非 FIPS 模式下，则采用名称为 secp192r1 的椭圆曲线生成本地 ECDSA 密钥对，密钥长度为 192 比特；FIPS 模式下，采用名称为 secp256r1 的椭圆曲线生成本地 ECDSA 密钥对，密钥长度为 256 比特。

rsa: 本地密钥对类型为 RSA。

name key-name: 生成指定名称的本地非对称密钥对。*key-name* 为本地非对称密钥对的名称，为 1~64 个字符的字符串，不区分大小写，字符串中只能包含字母、数字及“-”。如果不指定本参数，则生成的 RSA 主机密钥对的默认名称为 **hostkey**，RSA 服务器密钥对的默认名称为 **serverkey**，DSA 密钥对的默认名称为 **dsakey**，ECDSA 密钥对的默认名称为 **ecdsakey**。

【使用指导】

创建密钥对时，设备会提示用户输入密钥模数的长度。密钥模数越长，安全性越好，但是生成密钥的时间越长。关于密钥模数长度的配置限制和注意事项请参见 [表 1-4](#)。


生成密钥对时，如果不指定密钥对名称，系统会以缺省名称命名密钥对，并把该密钥对标记为默认（default）。

用户可以使用缺省的密钥对名称创建其他密钥对，但系统不会把该密钥对标记为默认（default）。

非默认名称密钥对的密钥类型和名称不能完全相同，否则需要用户确认是否覆盖原有的密钥对。不同类型的密钥对，名称可以相同。

执行此命令后，生成的密钥对将保存在设备中，设备重启后密钥不会丢失。

表1-4 不同类型密钥对对比

密钥对类型	生成的密钥对	密钥模数长度
RSA	<ul style="list-style-type: none"> 非 FIPS 模式下： <ul style="list-style-type: none"> 不指定密钥对名称时，将同时生成两个密钥对服务器密钥对和主机密钥对 指定密钥对名称时，只生成一个主机密钥对 FIPS 模式下：只生成一个主机密钥对，包括一个公钥和一个私钥 <p> 说明 目前，只有 SSH1.5 中应用了 RSA 服务器密钥对</p>	<ul style="list-style-type: none"> 非 FIPS 模式下：长度取值范围为 512~2048 比特，缺省值为 1024 比特，建议密钥模数的长度大于或等于 768 比特 FIPS 模式下：长度取值为 2048 比特
DSA	只生成一个主机密钥对	<ul style="list-style-type: none"> 非 FIPS 模式下：长度取值范围为 512~2048 比特，缺省值为 1024 比特，建议密钥模数的长度大于或等于 768 比特 FIPS 模式下：长度取值为 2048 比特
ECDSA	只生成一个主机密钥对	<ul style="list-style-type: none"> 非 FIPS 模式下：长度取值为 192、256、384 或 521 比特 FIPS 模式下：长度取值为 256、384 或 521 比特

【举例】

生成默认名称的本地 RSA 非对称密钥对。

```
<Sysname> system-view
[Sysname] public-key local create rsa
The range of public key modulus is (512 ~ 2048).
If the key modulus is greater than 512, it will take a few minutes.
Press CTRL+C to abort.
Input the modulus length [default = 1024]:
Generating Keys...
.....
.+++++
..+++++++
.....
Create the key pair successfully.
```

生成默认名称的本地 DSA 非对称密钥对。

```
<Sysname> system-view
[Sysname] public-key local create dsa
The range of public key modulus is (512 ~ 2048).
If the key modulus is greater than 512, it will take a few minutes.
Press CTRL+C to abort.
Input the modulus length [default = 1024]:
```

```

Generating Keys...
.+++++*
.....+.+.
.....+.+.
...+.+.+.+.+.+.+.+.+.+.+.
.....+.+.+.+.+.+.+.+.+.+.
.....+.+.+.+.+.+.+.+.+.+.
....+++++*
Create the key pair successfully.
# 生成默认名称的本地 ECDSA 非对称密钥对。
<Sysname> system-view
[Sysname] public-key local create ecdsa
Generating Keys...
Create the key pair successfully.
# 生成名称为 rsa1 的本地 RSA 非对称密钥对。
<Sysname> system-view
[Sysname] public-key local create rsa name rsa1
The range of public key modulus is (512 ~ 2048).
If the key modulus is greater than 512, it will take a few minutes.
Press CTRL+C to abort.
Input the modulus length [default = 1024]:
Generating Keys...
...+++++
.....+++++
Create the key pair successfully.
# 生成名称为 dsa1 的本地 DSA 非对称密钥对。
<Sysname> system-view
[Sysname] public-key local create dsa name dsa1
The range of public key modulus is (512 ~ 2048).
If the key modulus is greater than 512, it will take a few minutes.
Press CTRL+C to abort.
Input the modulus length [default = 1024]:
Generating Keys...
.+++++*
.....+.+.
.....+.+.
...+.+.+.+.+.+.+.+.+.+.+.
.....+.+.+.+.+.+.+.+.+.+.
.....+.+.+.+.+.+.+.+.+.+.
....+++++*
Create the key pair successfully.
# 生成名称为 ecdsa1 的本地 ECDSA 非对称密钥对。
<Sysname> system-view
[Sysname] public-key local create ecdsa name ecdsa1
Generating Keys...
Create the key pair successfully.
# 在 FIPS 模式下生成默认名称的本地 RSA 非对称密钥对。

```


name key-name: 销毁指定名称的本地非对称密钥对。*key-name* 为本地非对称密钥对名称，为1~64个字符的字符串，不区分大小写，字符串中可以包含字母、数字及“-”。如果不指定本参数，则销毁指定类型默认名称的本地非对称密钥对。

【使用指导】

在如下几种情况下，建议用户销毁旧的非对称密钥对，并生成新的密钥对：

- 本地设备的私钥泄露。这种情况下，非法用户可能会冒充本地设备访问网络。
- 保存密钥对的存储设备出现故障，导致设备上没有公钥对应的私钥，无法再利用旧的非对称密钥对进行加解密和数字签名。
- 本地证书到达有效期，需要删除对应的本地密钥对。本地证书的详细介绍，请参见“安全配置指导”中的“PKI”。

【举例】

销毁默认名称的本地 RSA 非对称密钥对。

```
<Sysname> system-view
[Sysname] public-key local destroy rsa
Confirm to destroy the key pair? [Y/N]:y
```

销毁默认名称的本地 DSA 非对称密钥对。

```
<Sysname> system-view
[Sysname] public-key local destroy dsa
Confirm to destroy the key pair? [Y/N] :y
```

销毁默认名称的本地 ECDSA 非对称密钥对。

```
<Sysname> system-view
[Sysname] public-key local destroy ecdsa
Confirm to destroy the key pair? [Y/N]:y
```

销毁名称为 **rsa1** 的本地 RSA 非对称密钥对。

```
<Sysname> system-view
[Sysname] public-key local destroy rsa name rsa1
Confirm to destroy the key pair? [Y/N]:y
```

销毁名称为 **dsa1** 的本地 DSA 非对称密钥对。

```
<Sysname> system-view
[Sysname] public-key local destroy dsa name dsa1
Confirm to destroy the key pair? [Y/N] :y
```

销毁名称为 **ecdsa1** 的本地 ECDSA 非对称密钥对。

```
<Sysname> system-view
[Sysname] public-key local destroy ecdsa name ecdsa1
Confirm to destroy the key pair? [Y/N]:y
```

【相关命令】

- **public-key local create**

1.1.6 public-key local export dsa

public-key local export dsa 命令用来根据指定格式显示本地 DSA 主机公钥或将其导出到指定文件。

【命令】

```
public-key local export dsa [ name key-name ] { openssh | ssh2 } [ filename ]
```

【视图】

系统视图

【缺省用户角色】

network-admin

【参数】

name *key-name*: 显示或导出指定本地 DSA 密钥对的主机公钥。*key-name* 为本地密钥对的名称，为 1~64 个字符的字符串，不区分大小写，字符串中可以包含字母、数字及“-”。如果不指定本参数，则显示或导出默认名称的本地 DSA 密钥对的主机公钥。

openssh: 主机公钥格式为 OpenSSH。

ssh2: 主机公钥格式为 SSH2.0。

filename: 指定存储导出公钥的文件名称，不区分大小写，取值不能为“hostkey”、“serverkey”、“dsakey”和“ecdsakey”，不能全部为“.”，并且第一个字符不能为“/”，不能包含字符“/”和“..”。文件名为取值 1~128 个字符的字符串。文件名的详细介绍，请参见“基础配置指导”中的“文件系统管理”。如果不指定本参数，则按照指定格式显示本地 DSA 主机公钥。

【使用指导】

本命令用于采用从公钥文件中导入的方式将本地的主机公钥保存到远端设备上：

(1) 使用下列任一方法把导出的公钥保存到文件中：

- 在本地设备上执行 **public-key local export** 命令按照指定格式显示本地主机公钥（执行命令时不指定 *filename* 参数），再通过粘贴复制方式将显示的主机公钥保存到文件中。
- 在本地设备上执行 **public-key local export** 命令按照指定格式将本地主机公钥导出到指定文件（执行命令时指定 *filename* 参数）。需要注意的是，不能将主机公钥导出到工作路径 **pkey** 目录以及 **pkey** 的子目录中。

(2) 将所获得的证书文件通过 FTP 的二进制模式或 TFTP 上传到远端主机。有关 FTP 和 TFTP 的详细使用请参见“基础配置指导”中的“FTP 和 TFTP”。

(3) 在远端主机上，执行 **public-key peer import sshkey** 命令将本地的主机公钥保存到远端设备上。

SSH2.0 和 OpenSSH 是两种不同类型的公钥格式，用户需要根据服务器端支持的对端公钥格式，来选择导出的主机公钥格式。

【举例】

以 OpenSSH 格式导出默认名称的本地 DSA 密钥对的主机公钥，文件名为 key.pub。

```
<Sysname> system-view
```

```
[Sysname] public-key local export dsa openssh key.pub
```

以 SSH2.0 格式显示默认名称的本地 DSA 密钥对的主机公钥。

```
<Sysname> system-view
```

```
[Sysname] public-key local export dsa ssh2
```

```
---- BEGIN SSH2 PUBLIC KEY ----
```

```
Comment: "dsa-key-2011/05/12"
```

```

AAAAB3NzaC1kc3MAAACBANdXJixFhMRMIR8YvZbl8GHE8KQj9/5ra4WzTO9yzhSg06UiL+CM7OZb5sJlhUiJ3B7b
0T7IsnTan3W6Jsy5h3I2Anh+kiuoRCHyLDyJy5sG/WD+AZQd3Xf+axKJPadu68HRKNl/BnjXcittQchQbzWCFLFq
L6xLNolQOHgRx9ozAAAAFQDHcyGmc37I7pk7Ty3tMPSO2s6RXwAAAIEAgiaQCeFOxHS68pMuadOx8YUXrZWUGEzN
/OrpbsTV75MTPoS0cJPFKyDNNdAkkroVnsZJliW8T6UiliLFs3ThbdABMs5xsCAhcJGscXthI5HHbB+y6IMXwb2B
cdQey4PiEMA8ybMugQVhwhYhxz1tqsAo9LFYXaf0JRlXjMmwnu8AAACAQZEs400SvNIVfnqxwvA7PvOVEA89tKni
/f6GDBvWY9Z2Q499pAqUBtYcqQea8T4zBINxx2eF3lLaZJrIvAS205zXxSzQoU9190kakdMdasIjQLWYGyepFc3s
TwmIf1QeweUwLVAPaOesKaCERjxg+e4maYwLAvySGT4c9NJlxLo=

```

```
---- END SSH2 PUBLIC KEY ----
```

以 OpenSSH 格式显示默认名称的本地 DSA 密钥对的主机公钥。

```
<Sysname> system-view
```

```
[Sysname] public-key local export dsa openssh
```

```
ssh-dss
```

```

AAAAB3NzaC1kc3MAAACBANdXJixFhMRMIR8YvZbl8GHE8KQj9/5ra4WzTO9yzhSg06UiL+CM7OZb5sJlhUiJ3B7b
0T7IsnTan3W6Jsy5h3I2Anh+kiuoRCHyLDyJy5sG/WD+AZQd3Xf+axKJPadu68HRKNl/BnjXcittQchQbzWCFLFq
L6xLNolQOHgRx9ozAAAAFQDHcyGmc37I7pk7Ty3tMPSO2s6RXwAAAIEAgiaQCeFOxHS68pMuadOx8YUXrZWUGEzN
/OrpbsTV75MTPoS0cJPFKyDNNdAkkroVnsZJliW8T6UiliLFs3ThbdABMs5xsCAhcJGscXthI5HHbB+y6IMXwb2B
cdQey4PiEMA8ybMugQVhwhYhxz1tqsAo9LFYXaf0JRlXjMmwnu8AAACAQZEs400SvNIVfnqxwvA7PvOVEA89tKni
/f6GDBvWY9Z2Q499pAqUBtYcqQea8T4zBINxx2eF3lLaZJrIvAS205zXxSzQoU9190kakdMdasIjQLWYGyepFc3s
TwmIf1QeweUwLVAPaOesKaCERjxg+e4maYwLAvySGT4c9NJlxLo= dsa-key

```

以 OpenSSH 格式导出名称为 dsa1 的本地 DSA 密钥对的主机公钥，文件名为 dsa1.pub。

```
<Sysname> system-view
```

```
[Sysname] public-key local export dsa name dsal openssh dsal.pub
```

以 SSH2.0 格式显示名称为 dsa1 的本地 DSA 密钥对的主机公钥。

```
<Sysname> system-view
```

```
[Sysname] public-key local export dsa name dsal ssh2
```

```
---- BEGIN SSH2 PUBLIC KEY ----
```

```
Comment: "dsa-key-2011/05/12"
```

```

AAAAB3NzaC1kc3MAAACBANdXJixFhMRMIR8YvZbl8GHE8KQj9/5ra4WzTO9yzhSg06UiL+CM7OZb5sJlhUiJ3B7b
0T7IsnTan3W6Jsy5h3I2Anh+kiuoRCHyLDyJy5sG/WD+AZQd3Xf+axKJPadu68HRKNl/BnjXcittQchQbzWCFLFq
L6xLNolQOHgRx9ozAAAAFQDHcyGmc37I7pk7Ty3tMPSO2s6RXwAAAIEAgiaQCeFOxHS68pMuadOx8YUXrZWUGEzN
/OrpbsTV75MTPoS0cJPFKyDNNdAkkroVnsZJliW8T6UiliLFs3ThbdABMs5xsCAhcJGscXthI5HHbB+y6IMXwb2B
cdQey4PiEMA8ybMugQVhwhYhxz1tqsAo9LFYXaf0JRlXjMmwnu8AAACBAKHkVsjaKtG7g7G98qGmtaboNkK0YEAK
Rdp+QDZxX0aPdmVeEU1GC3ES9XFD7gIK70pb+tB7dA+8scZNqKK85hkoNCFEXux3088NEYZullatZRH0km+DdpZ7
CrcV+ft7UUVBF0FV3W4HOx/LoidJ5sX+qBAD4WcpSX0OrZEF4+dq

```

```
---- END SSH2 PUBLIC KEY ----
```

以 OpenSSH 格式显示名称为 dsa1 的本地 DSA 密钥对的主机公钥。

```
<Sysname> system-view
```

```
[Sysname] public-key local export dsa name dsal openssh
```

```
ssh-dss
```

```

AAAAB3NzaC1kc3MAAACBANdXJixFhMRMIR8YvZbl8GHE8KQj9/5ra4WzTO9yzhSg06UiL+CM7OZb5sJlhUiJ3B7b
0T7IsnTan3W6Jsy5h3I2Anh+kiuoRCHyLDyJy5sG/WD+AZQd3Xf+axKJPadu68HRKNl/BnjXcittQchQbzWCFLFq
L6xLNolQOHgRx9ozAAAAFQDHcyGmc37I7pk7Ty3tMPSO2s6RXwAAAIEAgiaQCeFOxHS68pMuadOx8YUXrZWUGEzN
/OrpbsTV75MTPoS0cJPFKyDNNdAkkroVnsZJliW8T6UiliLFs3ThbdABMs5xsCAhcJGscXthI5HHbB+y6IMXwb2B
cdQey4PiEMA8ybMugQVhwhYhxz1tqsAo9LFYXaf0JRlXjMmwnu8AAACBAKHkVsjaKtG7g7G98qGmtaboNkK0YEAK
Rdp+QDZxX0aPdmVeEU1GC3ES9XFD7gIK70pb+tB7dA+8scZNqKK85hkoNCFEXux3088NEYZullatZRH0km+DdpZ7
CrcV+ft7UUVBF0FV3W4HOx/LoidJ5sX+qBAD4WcpSX0OrZEF4+dq dsa-key

```

【相关命令】

- **public-key local create**
- **public-key peer import sshkey**

1.1.7 public-key local export ecdsa

public-key local export ecdsa 命令用来根据指定格式显示本地 ECDSA 主机公钥或将其导出到指定文件。

【命令】

```
public-key local export ecdsa [ name key-keyname ] { openssh | ssh2 }  
[ filename ]
```

【视图】

系统视图

【缺省用户角色】

network-admin

【参数】

name key-name: 显示或导出指定本地 ECDSA 密钥对的主机公钥。*key-name* 为本地密钥对的名称，为 1~64 个字符的字符串，不区分大小写，字符串中可以包含字母、数字及“-”。如果不指定本参数，则显示或导出默认名称的本地 ECDSA 密钥对的主机公钥。

openssh: 主机公钥格式为 OpenSSH。

ssh2: 主机公钥格式为 SSH2.0。

filename: 指定存储导出公钥的文件的名称，不区分大小写，取值不能为“hostkey”、“serverkey”、“dsa-key”和“ecdsa-key”，不能全部为“.”，并且第一个字符不能为“/”，不能包含字符“./”和“../”。文件名为取值 1~128 个字符的字符串。文件名的详细介绍，请参见“基础配置指导”中的“文件系统管理”。如果不指定本参数，则按照指定格式显示本地 ECDSA 主机公钥。

【使用指导】

本命令用于采用从公钥文件中导入的方式将本地的主机公钥保存到远端设备上：

(1) 使用下列任一方法把导出的公钥保存到文件中：

- 在本地设备上执行 **public-key local export** 命令按照指定格式显示本地主机公钥（执行命令时不指定 *filename* 参数），再通过粘贴复制方式将显示的主机公钥保存到文件中。
- 在本地设备上执行 **public-key local export** 命令按照指定格式将本地主机公钥导出到指定文件（执行命令时指定 *filename* 参数）。需要注意的是，不能将主机公钥导出到工作路径 **pkey** 目录以及 **pkey** 的子目录中。

(2) 将所获得的证书文件通过 FTP 的二进制模式或 TFTP 上传到远端主机。有关 FTP 和 TFTP 的详细使用请参见“基础配置指导”中的“FTP 和 TFTP”。

(3) 在远端主机上，执行 **public-key peer import sshkey** 命令将本地的主机公钥保存到远端设备上。

SSH2.0 和 OpenSSH 是两种不同类型的公钥格式，用户需要根据服务器端支持的对端公钥格式，来选择导出的主机公钥格式。

目前，只支持导出椭圆曲线为 **secp256r1** 的 ECDSA 主机公钥。

【举例】

以 OpenSSH 格式导出本地 ECDSA 主机公钥，文件名为 key.pub。

```
<Sysname> system-view
```

```
[Sysname] public-key local export ecdsa openssh key.pub
# 以 SSH2.0 格式显示本地 ECDSA 主机公钥。

<Sysname> system-view
[Sysname] public-key local export ecdsa ssh2
---- BEGIN SSH2 PUBLIC KEY ----
Comment: "ecdsa-sha2-nistp256-2014/07/06"
AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBREw5tkARpbV+sYArt/xcW+UJEAevx7OckT
tTLPBiLP5bWkSdKbvo+3oHRuIyZqmNTicxuBjuBap+pHc9l9C58=
---- END SSH2 PUBLIC KEY ----

# 以 OpenSSH 格式显示本地 ECDSA 主机公钥。

<Sysname> system-view
[Sysname] public-key local export ecdsa openssh
ecdsa-sha2-nistp256
AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBREw5tkARpbV+sYArt/xcW+UJEAevx7OckT
tTLPBiLP5bWkSdKbvo+3oHRuIyZqmNTicxuBjuBap+pHc9l9C58=
ecdsa-key
```

【相关命令】

```
public-key local create
public-key peer import sshkey
```

1.1.8 public-key local export rsa

public-key local export rsa 命令用来根据指定格式显示本地 RSA 主机公钥或将其导出到指定文件。

【命令】

非 FIPS 模式下：

```
public-key local export rsa [ name key-name ] { openssh | ssh1 | ssh2 }
[ filename ]
```

FIPS 模式下：

```
public-key local export rsa [ name key-name ] { openssh | ssh2 } [ filename ]
```

【视图】

系统视图

【缺省用户角色】

network-admin

【参数】

name key-name：显示或导出指定本地 RSA 密钥对的主机公钥。*key-name* 为本地密钥对的名称，为 1~64 个字符的字符串，不区分大小写，字符串中可以包含字母、数字及“-”。如果不指定本参数，则显示或导出默认名称的本地 RSA 密钥对的主机公钥。

openssh：主机公钥格式为 OpenSSH。

ssh1：主机公钥格式为 SSH1.5。

ssh2：主机公钥格式为 SSH2.0。

filename: 指定存储导出公钥的文件的名称, 不区分大小写, 取值不能为“hostkey”、“serverkey”、“dsakey”和“ecdsakey”, 不能全部为“.”, 并且第一个字符不能为“/”, 不能包含字符“/”和“..”。文件名为取值 1~128 个字符的字符串。文件名的详细介绍, 请参见“基础配置指导”中的“文件系统管理”。如果不指定本参数, 则按照指定格式显示本地 RSA 主机公钥。

【使用指导】

本命令用于采用从公钥文件中导入的方式将本地的主机公钥保存到远端设备上:

(1) 使用下列任一方法把导出的公钥保存到文件中:

- 在本地设备上执行 **public-key local export** 命令按照指定格式显示本地主机公钥 (执行命令时不指定 *filename* 参数), 再通过粘贴复制方式将显示的主机公钥保存到文件中。
- 在本地设备上执行 **public-key local export** 命令按照指定格式将本地主机公钥导出到指定文件 (执行命令时指定 *filename* 参数)。需要注意的是, 不能将主机公钥导出到工作路径 **pkey** 目录以及 **pkey** 的子目录中。

(2) 将所获得的证书文件通过 FTP 的二进制模式或 TFTP 上传到远端主机。有关 FTP 和 TFTP 的详细使用请参见“基础配置指导”中的“FTP 和 TFTP”。

(3) 在远端主机上, 执行 **public-key peer import sshkey** 命令将本地的主机公钥保存到远端设备上。

SSH1.5、SSH2.0 和 OpenSSH 是三种不同类型的公钥格式, 用户需要根据服务器端支持的对端公钥格式, 来选择导出的主机公钥格式。FIPS 模式下只支持 SSH2.0 和 OpenSSH。

【举例】

以 OpenSSH 格式导出默认名称的本地 RSA 密钥对的主机公钥, 文件名为 key.pub。

```
<Sysname> system-view
```

```
[Sysname] public-key local export rsa openssh key.pub
```

以 SSH2.0 格式显示默认名称的本地 RSA 密钥对的主机公钥。

```
<Sysname> system-view
```

```
[Sysname] public-key local export rsa ssh2
```

```
---- BEGIN SSH2 PUBLIC KEY ----
```

```
Comment: "rsa-key-2011/05/12"
```

```
AAAAB3NzaC1yc2EAAAADAQABAAQDAPKr+/gTCyWZyabuCJuJjMeMPQaj/kixzOCCAl+hDMmEGMrSfddq/bYcb  
gM7BuitlAgB3x0dFyTPi85DcCznTW4goPXAKFjuzCbGfj4chakSr+/ajlk3rM+XOvyvPJilneKJqhPT0xdv4tlas  
+mLNloY0dImbws2kwE7lrgglCQ==
```

```
---- END SSH2 PUBLIC KEY ----
```

以 OpenSSH 格式显示默认名称的本地 RSA 密钥对的主机公钥。

```
<Sysname> system-view
```

```
[Sysname] public-key local export rsa openssh
```

```
ssh-rsa
```

```
AAAAB3NzaC1yc2EAAAADAQABAAQDAPKr+/gTCyWZyabuCJuJjMeMPQaj/kixzOCCAl+hDMmEGMrSfddq/bYcb  
gM7BuitlAgB3x0dFyTPi85DcCznTW4goPXAKFjuzCbGfj4chakSr+/ajlk3rM+XOvyvPJilneKJqhPT0xdv4tlas  
+mLNloY0dImbws2kwE7lrgglCQ== rsa-key
```

以 OpenSSH 格式导出名称为 rsa1 的本地 RSA 密钥对的主机公钥, 文件名为 rsa1.pub。

```
<Sysname> system-view
```

```
[Sysname] public-key local export rsa name rsa1 openssh rsa1.pub
```

以 SSH2.0 格式显示名称为 rsa1 的本地 RSA 密钥对的主机公钥。

```
<Sysname> system-view
```

```
[Sysname] public-key local export rsa name rsa1 ssh2
---- BEGIN SSH2 PUBLIC KEY ----
Comment: "rsa-key-2011/05/12"
AAAAB3NzaC1yc2EAAAADAQABAAQDevEbyF93xHUUJucJWqRclr8fhzQ9lSVprCI6ATZeDYr1J00fBQ8XY+q2o
lqoagn5YDyUC8ZJvUhlyMOHeORpkAVxD3XncTp4XG66h3rTHHa7Xmm7f1GDYlF0n05t8mCLVaupbfCzP8ba8UkrU
mMO4fUvW6zavA5LYxtlAiQv0KQ==
---- END SSH2 PUBLIC KEY ----

# 以 OpenSSH 格式显示名称为 rsa1 的本地 RSA 密钥对的主机公钥。

<Sysname> system-view
[Sysname] public-key local export rsa name rsa1 openssh
ssh-rsa
AAAAB3NzaC1yc2EAAAADAQABAAQDevEbyF93xHUUJucJWqRclr8fhzQ9lSVprCI6ATZeDYr1J00fBQ8XY+q2o
lqoagn5YDyUC8ZJvUhlyMOHeORpkAVxD3XncTp4XG66h3rTHHa7Xmm7f1GDYlF0n05t8mCLVaupbfCzP8ba8UkrU
mMO4fUvW6zavA5LYxtlAiQv0KQ== rsa-key
```

【相关命令】

- **public-key local create**
- **public-key peer import sshkey**

1.1.9 public-key peer

public-key peer 命令用来指定远端主机公钥的名称，并进入公钥视图。如果指定的远端主机公钥名称已经存在，则直接接进入该公钥视图。

undo public-key peer 命令用来删除指定的远端主机公钥。

【命令】

```
public-key peer keyname
undo public-key peer keyname
```

【缺省情况】

不存在远端主机公钥。

【视图】

系统视图

【缺省用户角色】

network-admin

【参数】

keyname：远端主机公钥的名称，为 1~64 个字符的字符串，区分大小写。

【使用指导】

进入公钥视图后，可以开始输入公钥数据。在输入公钥数据时，字符之间可以有空格，也可以按回车键继续输入数据。保存公钥数据时，将删除空格和回车符。

通过手工配置方式创建远端主机公钥时，用户需要事先获取并记录远端主机十六进制形式的公钥，并在本地设备上执行以下操作：

- (1) 执行本命令进入公钥视图。
- (2) 在公钥视图，手工输入远端主机的公钥。

(3) 执行 **peer-public-key end** 命令，保存输入的远端主机公钥，并从公钥视图退回到系统视图。

输入的公钥数据必须满足一定的格式要求。通过 **display public-key local public** 命令显示的公钥可以作为输入的公钥数据。

【举例】

指定远端主机公钥名称为 **key1**，并进入公钥视图。

```
<Sysname> system-view
[Sysname] public-key peer key1
Enter public key view. Return to system view with "peer-public-key end" command.
[Sysname-pkey-public-key-key1]
```

【相关命令】

- **display public-key local public**
- **display public-key peer**
- **peer-public-key end**

1.1.10 public-key peer import sshkey

public-key peer import sshkey 命令用来配置从公钥文件中导入远端主机的公钥。

undo public-key peer 命令用来删除指定的远端主机公钥。

【命令】

```
public-key peer keyname import sshkey filename
undo public-key peer keyname
```

【缺省情况】

不存在远端主机公钥。

【视图】

系统视图

【缺省用户角色】

network-admin

【参数】

keyname：远端主机公钥的名称，为 1~64 个字符的字符串，区分大小写。

filename：指定导入公钥数据的文件名，不区分大小写，取值不能为“hostkey”、“serverkey”、“dsa-key”和“ecdsa-key”，不能全部为“.”，并且第一个字符不能为“/”，不能包含字符“/”和“../”。文件名为取值 1~128 个字符的字符串。文件名的详细介绍，请参见“基础配置指导”中的“文件系统管理”。

【使用指导】

执行本命令后，系统会对指定公钥文件中的公钥进行格式转换，将其转换为 PKCS 标准编码格式，并将该远端主机的公钥保存到本地设备。

从公钥文件中导入远端主机的公钥前，需要远端主机将其公钥保存到公钥文件中，并将该公钥文件上传到本地设备。例如，在远端主机上执行 **public-key local export** 命令将其公钥导出到公钥文件中，并通过 **FTP** 或 **TFTP**，以二进制方式将该公钥文件保存到本地设备。

目前，非 **FIPS** 模式下，设备支持的公钥格式为 **SSH1.5**、**SSH2.0** 和 **OpenSSH**；**FIPS** 模式下，设备支持的格式为 **SSH2.0** 和 **OpenSSH**。

【举例】

配置从公钥文件 **key.pub** 中导入远端主机的公钥，公钥名称为 **key2**。

```
<Sysname> system-view
```

```
[Sysname] public-key peer key2 import sshkey key.pub
```

【相关命令】

- **display public-key peer**
- **public-key local export dsa**
- **public-key local export ecdsa**
- **public-key local export rsa**

目 录

1 PKI	1-1
1.1 PKI配置命令.....	1-1
1.1.1 attribute.....	1-1
1.1.2 ca identifier	1-2
1.1.3 certificate request entity	1-3
1.1.4 certificate request from	1-4
1.1.5 certificate request mode	1-5
1.1.6 certificate request polling.....	1-6
1.1.7 certificate request url	1-6
1.1.8 common-name.....	1-7
1.1.9 country	1-8
1.1.10 crl check enable.....	1-8
1.1.11 crl url.....	1-9
1.1.12 display pki certificate access-control-policy	1-10
1.1.13 display pki certificate attribute-group	1-11
1.1.14 display pki certificate domain	1-13
1.1.15 display pki certificate request-status	1-17
1.1.16 display pki crl domain.....	1-19
1.1.17 fqdn	1-20
1.1.18 ip.....	1-21
1.1.19 ldap-server	1-22
1.1.20 locality	1-23
1.1.21 organization.....	1-23
1.1.22 organization-unit	1-24
1.1.23 pki abort-certificate-request	1-24
1.1.24 pki certificate access-control-policy	1-25
1.1.25 pki certificate attribute-group	1-26
1.1.26 pki delete-certificate.....	1-27
1.1.27 pki domain.....	1-28
1.1.28 pki entity	1-28
1.1.29 pki export	1-29
1.1.30 pki import	1-36
1.1.31 pki request-certificate.....	1-40

1.1.32 pki retrieve-certificate	1-41
1.1.33 pki retrieve-crl	1-42
1.1.34 pki storage	1-43
1.1.35 pki validate-certificate	1-44
1.1.36 public-key dsa	1-46
1.1.37 public-key ecdsa	1-47
1.1.38 public-key rsa	1-48
1.1.39 root-certificate fingerprint	1-50
1.1.40 rule	1-51
1.1.41 source	1-52
1.1.42 state	1-53
1.1.43 usage	1-53

1 PKI



说明

设备运行于 FIPS 模式时，本特性部分配置相对于非 FIPS 模式有所变化，具体差异请见本文相关描述。有关 FIPS 模式的详细介绍请参见“安全配置指导”中的“FIPS”。

1.1 PKI配置命令

1.1.1 attribute

attribute 命令用来配置属性规则，用于根据证书的颁发者名、主题名以及备用主题名来过滤证书。

undo attribute 命令用来删除证书属性规则。

【命令】

```
attribute id { alt-subject-name { fqdn | ip } | { issuer-name | subject-name }  
             { dn | fqdn | ip } } { ctn | equ | nctn | nequ } attribute-value  
undo attribute id
```

【缺省情况】

不存在属性规则，即对证书的颁发者名、主题名以及备用主题名没有限制。

【视图】

证书属性组视图

【缺省用户角色】

network-admin

【参数】

id: 证书属性规则序号，取值范围为 1~16。

alt-subject-name: 表示证书备用主题名（Subject Alternative Name）。

fqdn: 指定实体的 FQDN。

ip: 指定实体的 IP 地址。

dn: 指定实体的 DN。

issuer-name: 表示证书颁发者名（Issuer Name）。

subject-name: 表示证书主题名（Subject Name）。

ctn: 表示包含操作。

equ: 表示相等操作。

nctn: 表示不包含操作。

nequ: 表示不等操作。

attribute-value: 指定证书属性值，为 1~255 个字符的字符串，不区分大小写。

【使用指导】

各证书属性中可包含的属性域个数有所不同：

- 主题名和颁发者名中均只能包含一个 DN，但是均可以同时包含多个 FQDN 和 IP；
- 备用主题名中不能包含 DN，但是可以同时包含多个 FQDN 和 IP。

不同类型的证书属性域与操作关键字的组合代表了不同的匹配条件，具体如下表所示：

表1-1 对证书属性域的操作涵义

操作	DN	FQDN/IP
ctn	DN中包含指定的属性值	任意一个FQDN/IP中包含了指定的属性值
nctn	DN中不包含指定的属性值	所有FQDN/IP中均不包含指定的属性值
equ	DN等于指定的属性值	任意一个FQDN/IP等于指定的属性值
nequ	DN不等于指定的属性值	所有FQDN/IP均不等于指定的属性值

如果证书的相应属性中包含了属性规则里指定的属性域，且满足属性规则中定义的匹配条件，则认为该属性与属性规则相匹配。例如：属性规则 2 中定义，证书的主题名 DN 中包含字符串 **abc**。如果某证书的主题名的 DN 中确实包含了字符串 **abc**，则认为该证书的主题名与属性规则 2 匹配。

只有证书中的相应属性与某属性组中的所有属性规则都匹配上，才认为该证书与此属性组匹配。如果证书中的某属性中没有包含属性规则中指定的属性域，或者不满足属性规则中的匹配条件，则认为该证书与此属性组不匹配。

【举例】

创建一个名为 **mygroup** 的证书属性组，并进入证书属性组视图。

```
<Sysname> system-view
```

```
[Sysname] pki certificate attribute-group mygroup
```

创建证书属性规则 1，定义证书主题名中的 DN 包含字符串 **abc**。

```
[Sysname-pki-cert-attribute-group-mygroup] attribute 1 subject-name dn ctn abc
```

创建证书属性规则 2，定义证书颁发者名中的 FQDN 不等于字符串 **abc**。

```
[Sysname-pki-cert-attribute-group-mygroup] attribute 2 issuer-name fqdn nequ abc
```

创建证书属性规则 3，定义证书主题备用名中的 IP 地址不等于 **10.0.0.1**。

```
[Sysname-pki-cert-attribute-group-mygroup] attribute 3 alt-subject-name ip nequ 10.0.0.1
```

【相关命令】

- **display pki certificate attribute-group**
- **rule**

1.1.2 ca identifier

ca identifier 命令用来指定设备信任的 CA 名称。

undo ca identifier 命令用来恢复缺省情况。

【命令】

```
ca identifier name
```

undo ca identifier

【缺省情况】

未指定设备信任的 CA。

【视图】

PKI 域视图

【缺省用户角色】

network-admin

【参数】

name: 设备信任的 CA 名称，为 1~63 个字符的字符串，区分大小写。

【使用指导】

获取 CA 证书时，必须指定信任的 CA 名称，这个名称会被作为 SCEP 消息的一部分发送给 CA 服务器。但是一般情况下，CA 服务器会忽略收到的 SCEP 消息中的 CA 名称的具体内容。但是如果同一台服务器上配置了两个 CA，且它们的 URL 是相同的，则服务器将根据 SCEP 消息中的 CA 名称选择对应的 CA。因此，使用此命令指定的 CA 名称必须与希望获取的 CA 证书对应的 CA 名称一致。

【举例】

```
# 指定设备信任的 CA 名称为 new-ca。
<Sysname> system-view
[Sysname] pki domain aaa
[Sysname-pki-domain-aaa] ca identifier new-ca
```

1.1.3 certificate request entity

certificate request entity 命令用来指定用于申请证书的 PKI 实体名称。

undo certificate request entity 命令用来恢复缺省情况。

【命令】

```
certificate request entity entity-name
undo certificate request entity
```

【缺省情况】

未指定设备申请证书所使用的 PKI 实体名称。

【视图】

PKI 域视图

【缺省用户角色】

network-admin

【参数】

entity-name: 用于申请证书的 PKI 实体名称，为 1~31 个字符的字符串，不区分大小写。

【使用指导】

本命令用于在 PKI 域中指定申请证书的 PKI 实体。PKI 实体描述了申请证书的实体的各种属性（通用名、组织部门、组织、地理区域、省、国家、FQDN、IP），这些属性用于描述 PKI 实体的身份信息。

一个 PKI 域中只能指定一个 PKI 实体名称，多次执行本命令，最后一次执行的命令生效。

【举例】

指定申请证书的 PKI 实体名称为 en1。

```
<Sysname> system-view
[Sysname] pki domain aaa
[Sysname-pki-domain-aaa] certificate request entity en1
```

【相关命令】

- `pki entity`

1.1.4 certificate request from

`certificate request from` 命令用来配置证书申请的注册受理机构。

`undo certificate request from` 命令用来恢复缺省情况。

【命令】

```
certificate request from { ca | ra }
undo certificate request from
```

【缺省情况】

未指定证书申请的注册受理机构。

【视图】

PKI 域视图

【缺省用户角色】

network-admin

【参数】

ca: 表示实体从 CA 申请证书。

ra: 表示实体从 RA 申请证书。

【使用指导】

选择从 CA 还是 RA 申请证书，由 CA 服务器决定，需要了解 CA 服务器上由什么机构来受理证书申请。

推荐使用独立运行的 RA 作为注册受理机构。

【举例】

指定实体从 RA 申请证书。

```
<Sysname> system-view
[Sysname] pki domain aaa
[Sysname-pki-domain-aaa] certificate request from ra
```

1.1.5 certificate request mode

certificate request mode 命令用来配置证书申请方式。

undo certificate request mode 命令用来恢复缺省情况。

【命令】

```
certificate request mode { auto [ password { cipher | simple } string ] |  
manual }  
undo certificate request mode
```

【缺省情况】

证书申请方式为手工方式。

【视图】

PKI 域视图

【缺省用户角色】

network-admin

【参数】

auto: 表示用自动方式申请证书。

password: 指定吊销证书时使用的密码。

cipher: 以密文方式设置密码。

simple: 以明文方式设置密码，该密码将以密文形式存储。

string: 密码字符串，区分大小写。明文密码为 1~31 个字符的字符串，密文密码为 1~73 个字符的字符串。

manual: 表示用手工方式申请证书。

【使用指导】

两种申请方式都属于在线申请，具体情况如下：

- 如果是自动方式，则设备会在与 PKI 域关联的应用（例如 IKE）需要做身份认证时，自动向证书注册机构发起获取 CA 证书和申请本地证书的操作。自动方式下，可以指定吊销证书时使用的密码，是否需要指定密码是由 CA 服务器的策略决定的。
- 如果为手工方式，则需要手工完成获取 CA 证书、申请本地证书的操作。

【举例】

指定证书申请方式为自动方式。

```
<Sysname> system-view  
[Sysname] pki domain aaa  
[Sysname-pki-domain-aaa] certificate request mode auto
```

指定证书申请方式为自动方式，并设置吊销证书时使用的密码为明文 123456。

```
<Sysname> system-view  
[Sysname] pki domain aaa  
[Sysname-pki-domain-aaa] certificate request mode auto password simple 123456
```

【相关命令】

- `pki request-certificate`

1.1.6 certificate request polling

`certificate request polling` 命令用来配置证书申请状态的查询周期和最大次数。

`undo certificate request polling` 命令用来恢复缺省情况。

【命令】

```
certificate request polling { count count | interval interval }  
undo certificate request polling { count | interval }
```

【缺省情况】

证书申请状态的查询周期为 20 分钟，最多查询 50 次。

【视图】

PKI 域视图

【缺省用户角色】

network-admin

【参数】

count count: 表示证书申请状态的查询次数，取值范围为 1~100。

interval interval: 表示证书申请状态的查询周期，取值范围为 5~168，单位为分钟。

【使用指导】

设备发送证书申请后,如果 CA 服务器采用手工方式来签发证书申请,则不会立刻响应设备的申请。这种情况下,设备通过定期向 CA 服务器发送状态查询消息,能够及时获取到被 CA 签发的证书。CA 签发证书后,设备将通过发送状态查询得到证书,之后停止发送状态查询消息。如果达到最大查询次数时,CA 服务器仍未签发证书,则设备停止发送状态查询消息,本次证书申请失败。如果 CA 服务器采用自动签发证书的方式,则设备可以立刻得到证书,这种情况下设备不会向 CA 服务器发送状态查询消息。

【举例】

指定证书申请状态的查询周期为 15 分钟，最多查询 40 次。

```
<Sysname> system-view  
[Sysname] pki domain aaa  
[Sysname-pki-domain-aaa] certificate request polling interval 15  
[Sysname-pki-domain-aaa] certificate request polling count 40
```

【相关命令】

- `display pki certificate request-status`

1.1.7 certificate request url

`certificate request url` 命令用来配置实体通过 SCEP 进行证书申请的注册受理机构服务器的 URL。

undo certificate request url 命令用来恢复缺省情况。

【命令】

```
certificate request url url-string
undo certificate request url
```

【缺省情况】

未指定注册受理机构服务器的 URL。

【视图】

PKI 域视图

【缺省用户角色】

network-admin

【参数】

url-string: 表示证书申请的注册受理机构服务器的 URL，为 1~511 个字符的字符串，区分大小写。实际可输入的 URL 长度受命令行允许输入的最大字符数限制。

【使用指导】

本命令配置的 URL 内容包括注册受理机构服务器的位置及 CGI 命令接口脚本位置，格式为 *http://server_location/cgi_script_location*。

【举例】

```
# 指定实体进行证书申请的注册受理机构服务器的 URL 为
http://169.254.0.1/certsrv/mscep/mscep.dll。

<Sysname> system-view
[Sysname] pki domain a
[Sysname-pki-domain-a] certificate request url http://169.254.0.1/certsrv/mscep/mscep.dll
```

1.1.8 common-name

common-name 命令用来配置 PKI 实体的通用名，比如用户名称。

undo common-name 命令用来恢复缺省情况。

【命令】

```
common-name common-name-string
undo common-name
```

【缺省情况】

未配置 PKI 实体的通用名。

【视图】

PKI 实体视图

【缺省用户角色】

network-admin

【参数】

common-name-string: PKI 实体的通用名, 为 1~63 个字符的字符串, 区分大小写, 不能包含逗号。

【举例】

配置 PKI 实体 en 的通用名为 test。

```
<Sysname> system-view
[Sysname] pki entity en
[Sysname-pki-entity-en] common-name test
```

1.1.9 country

country 命令用来配置 PKI 实体所属的国家代码。

undo country 命令用来恢复缺省情况。

【命令】

```
country country-code-string
undo country
```

【缺省情况】

未配置 PKI 实体所属的国家代码。

【视图】

PKI 实体视图

【缺省用户角色】

network-admin

【参数】

country-code-string: PKI 实体所属的国家代码, 为标准的两字符代码, 区分大小写, 例如中国为 CN。

【举例】

配置 PKI 实体 en 所属的国家代码为 CN。

```
<Sysname> system-view
[Sysname] pki entity en
[Sysname-pki-entity-en] country CN
```

1.1.10 crl check enable

crl check enable 命令用来开启 CRL 检查。

undo crl check enable 命令用来关闭 CRL 检查。

【命令】

```
crl check enable
undo crl check enable
```


【缺省情况】

CRL 检查处于开启状态。

【视图】

PKI 域视图

【缺省用户角色】

network-admin

【使用指导】

CRL（Certificate Revocation List，证书废除列表）是一个由 CA 签发的文件，该文件中包含被该 CA 吊销的所有证书的列表。一个证书有可能在有效期达到之前被 CA 吊销。使能 CRL 检查的目的是查看设备上的实体证书或者即将要导入、获取到设备上的实体证书是否已经被 CA 吊销，若检查结果表明实体证书已被吊销，那么该证书就不被设备信任。

【举例】

禁止 CRL 检查。

```
<Sysname> system-view
[Sysname] pki domain aaa
[Sysname-pki-domain-aaa] undo crl check enable
```

【相关命令】

- **pki import**
- **pki retrieve-certificate**
- **pki validate-certificate**

1.1.11 crl url

crl url 命令用来设置 CRL 发布点的 URL。

undo crl url 命令用来恢复缺省情况。

【命令】

```
crl url url-string
undo crl url
```

【缺省情况】

未设置 CRL 发布点的 URL。

【视图】

PKI 域视图

【缺省用户角色】

network-admin

【参数】

url-string：表示 CRL 发布点的 URL，为 1~511 个字符的字符串，区分大小写。格式为 **ldap://server_location** 或 **http://server_location**。实际可输入的 URL 长度受命令行允许输入的最大字符数限制。

【使用指导】

如果 CRL 检查处于使能状态，则进行 CRL 检查之前，需要首先从 PKI 域指定的 CRL 发布点获取 CRL。若 PKI 域中未配置 CRL 发布点的 URL 时，从该待验证的证书中获取发布点信息：优先获取待验证的证书中记录的发布点，如果待验证的证书中没有记录发布点，则获取 CA 证书中记录的发布点（若待验证的证书为 CA 证书，则获取上一级 CA 证书中记录的发布点）。如果无法通过任何途径得到发布点，则通过 SCEP 协议获取 CRL。

若配置了 LDAP 格式的 CRL 发布点 URL，则表示要通过 LDAP 协议获取 CRL。若该 URL 中未携带主机名，则需要根据 PKI 域中配置的 LDAP 服务器地址信息来得到完整的 LDAP 发布点 URL。

【举例】

```
# 指定 CRL 发布点的 URL 为 http://169.254.0.30。
<Sysname> system-view
[Sysname] pki domain aaa
[Sysname-pki-domain-aaa] crl url http://169.254.0.30
```

【相关命令】

- **ldap-server**
- **pki retrieve-crl**

1.1.12 display pki certificate access-control-policy

display pki certificate access-control-policy 命令用来显示证书访问控制策略的配置信息。

【命令】

```
display pki certificate access-control-policy [policy-name ]
```

【视图】

任意视图

【缺省用户角色】

network-admin
network-operator

【参数】

policy-name：指定证书访问控制策略名称，为 1~31 个字符的字符串，不区分大小写。

【使用指导】

若不指定证书访问控制策略的名称，则显示所有证书访问控制策略的配置信息。

【举例】

```
# 显示证书访问控制策略 mypolicy 的配置信息。
<Sysname> display pki certificate access-control-policy mypolicy
Access control policy name: mypolicy
    Rule 1 deny    mygroup1
    Rule 2 permit  mygroup2
# 显示所有证书属性访问控制策略的配置信息。
```

```

<Sysname> display pki certificate access-control-policy
Total PKI certificate access control policies: 2
Access control policy name: mypolicy1
    Rule 1  deny    mygroup1
    Rule 2  permit  mygroup2
Access control policy name: mypolicy2
    Rule 1  deny    mygroup3
    Rule 2  permit  mygroup4

```

表1-2 display pki certificate access-control-policy 命令显示信息描述表

字段	描述
Total PKI certificate access control policies	PKI证书访问控制策略的总数
Access control policy name	证书访问控制策略名
Rule <i>number</i>	访问控制规则编号
permit	当证书的属性与属性组里定义的属性匹配时，认为该证书有效，通过了访问控制策略的检测
deny	当证书的属性与属性组里定义的属性匹配时，认为该证书无效，未通过访问控制策略的检测

【相关命令】

- **pki certificate access-control-policy**
- **rule**

1.1.13 display pki certificate attribute-group

display pki certificate attribute-group 命令用来显示证书属性组的配置信息。

【命令】

```
display pki certificate attribute-group [ group-name ]
```

【视图】

任意视图

【缺省用户角色】

```
network-admin
network-operator
```

【参数】

group-name：指定证书属性组名，为 1~31 个字符的字符串，不区分大小写。

【使用指导】

若不指定证书属性组的名称，则显示所有证书属性组的配置信息。

【举例】

显示证书属性组 mygroup 的信息。

```
<Sysname> display pki certificate attribute-group mygroup
```

```

Attribute group name: mygroup
    Attribute 1 subject-name      dn      ctn      abc
    Attribute 2 issuer-name      fqdn    nctn    app
# 显示所有证书属性组的信息。
<Sysname> display pki certificate attribute-group
Total PKI certificate attribute groups: 2.
Attribute group name: mygroup1
    Attribute 1 subject-name      dn      ctn      abc
    Attribute 2 issuer-name      fqdn    nctn    app
Attribute group name: mygroup2
    Attribute 1 subject-name      dn      ctn      def
    Attribute 2 issuer-name      fqdn    nctn    fqdn

```

表1-3 display pki certificate attribute-group 命令显示信息描述表

字段	描述
Total PKI certificate attribute groups	PKI证书属性组的总数
Attribute group name	证书属性组名称
Attribute <i>number</i>	属性规则编号
subject-name	证书主题名
alt-subject-name	证书备用主题名
issuer-name	证书颁发者名
dn	实体的DN
fqdn	实体的FQDN
ip	实体的IP地址
ctn	表示包含操作
nctn	表示不包含操作
equ	表示等于操作
nequ	表示不等操作
Attribute 1 subject-name dn ctn abc	属性规则内容，包括以下参数： <ul style="list-style-type: none"> alt-subject-name: 表示证书备用主题名 issuer-name: 表示证书颁发者名 subject-name: 表示证书主题名 fqdn: 表示实体的 FQDN ip: 表示实体的 IP 地址 dn: 表示实体的 DN ctn: 表示包含操作 equ: 表示相等操作 nctn: 表示不包含操作 nequ: 表示不等操作

【相关命令】

- `attribute`
- `pki certificate attribute-group`

1.1.14 display pki certificate domain

`display pki certificate domain` 命令用来显示证书的内容。

【命令】

```
display pki certificate domain domain-name { ca | local | peer [ serial  
serial-num ] }
```

【视图】

任意视图

【缺省用户角色】

network-admin
network-operator

【参数】

domain-name: 显示指定证书所在的 PKI 域的名称，为 1~31 个字符的字符串，不区分大小写，不能包括“~”、“*”、“\”、“|”、“:”、“.”、“<”、“>”、“”和“'”。

ca: 显示 CA 证书。

local: 显示本地证书。

peer: 显示对端证书。

serial serial-num: 指定要显示的对端证书的序列号。

【使用指导】

显示 CA 证书时，会显示此 PKI 域中所有 CA 证书的详细信息，若 PKI 域中存在 RA 证书，则同时显示 RA 证书的详细信息。

显示本地证书时，会显示此 PKI 域中所有本地证书的详细信息。

显示对端证书时，如果不指定序列号，将显示所有对端证书的简要信息；如果指定序列号，将显示该序号对应的指定对端证书的详细信息。

【举例】

显示 PKI 域 aaa 中的 CA 证书。

```
<Sysname> display pki certificate domain aaa ca  
Certificate:  
  Data:  
    Version: 1 (0x0)  
    Serial Number:  
      5c:72:dc:c4:a5:43:cd:f9:32:b9:c1:90:8f:dd:50:f6  
    Signature Algorithm: sha1WithRSAEncryption  
    Issuer: C=cn, O=docm, OU=rnd, CN=rootca  
    Validity  
      Not Before: Jan  6 02:51:41 2011 GMT
```

```

    Not After : Dec  7 03:12:05 2013 GMT
Subject: C=cn, O=ccc, OU=ppp, CN=rootca
Subject Public Key Info:
    Public Key Algorithm: rsaEncryption
        Public-Key: (1024 bit)
        Modulus:
            00:c4:fd:97:2c:51:36:df:4c:ea:e8:c8:70:66:f0:
            28:98:ec:5a:ee:d7:35:af:86:c4:49:76:6e:dd:40:
            4a:9e:8d:c0:cb:d9:10:9b:61:eb:0c:e0:22:ce:f6:
            57:7c:bb:bb:1b:1d:b6:81:ad:90:77:3d:25:21:e6:
            7e:11:0a:d8:1d:3c:8e:a4:17:1e:8c:38:da:97:f6:
            6d:be:09:e3:5f:21:c5:a0:6f:27:4b:e3:fb:9f:cd:
            c1:91:18:ff:16:ee:d8:cf:8c:e3:4c:a3:1b:08:5d:
            84:7e:11:32:5f:1a:f8:35:25:c0:7e:10:bd:aa:0f:
            52:db:7b:cd:5d:2b:66:5a:fb
        Exponent: 65537 (0x10001)
Signature Algorithm: sha1WithRSAEncryption
    6d:b1:4e:d7:ef:bb:1d:67:53:67:d0:8f:7c:96:1d:2a:03:98:
    3b:48:41:08:a4:8f:a9:c1:98:e3:ac:7d:05:54:7c:34:d5:ee:
    09:5a:11:e3:c8:7a:ab:3b:27:d7:62:a7:bb:bc:7e:12:5e:9e:
    4c:1c:4a:9f:d7:89:ca:20:46:de:c5:b3:ce:36:ca:5e:6e:dc:
    e7:c6:fe:3f:c5:38:dd:d5:a3:36:ad:f4:3d:e6:32:7f:48:df:
    07:f0:a2:32:89:86:72:22:cd:ed:e5:0f:95:df:9c:75:71:e7:
    fe:34:c5:a0:64:1c:f0:5c:e4:8f:d3:00:bd:fa:90:b6:64:d8:
    88:a6

```

显示 PKI 域 aaa 中的本地证书。

```

<Sysname> display pki certificate domain aaa local
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number:
            bc:05:70:1f:0e:da:0d:10:16:1e
        Signature Algorithm: sha256WithRSAEncryption
        Issuer: C=CN, O=sec, OU=software, CN=abdfdc
        Validity
            Not Before: Jan  7 20:05:44 2011 GMT
            Not After : Jan  7 20:05:44 2012 GMT
        Subject: O=OpenCA Labs, OU=Users, CN=fips fips-sec
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
                Public-Key: (1024 bit)
                Modulus:
                    00:b2:38:ad:8c:7d:78:38:37:88:ce:cc:97:17:39:
                    52:e1:99:b3:de:73:8b:ad:a8:04:f9:a1:f9:0d:67:
                    d8:95:e2:26:a4:0b:c2:8c:63:32:5d:38:3e:fd:b7:
                    4a:83:69:0e:3e:24:e4:ab:91:6c:56:51:88:93:9e:
                    12:a4:30:ad:ae:72:57:a7:ba:fb:bc:ac:20:8a:21:
                    46:ea:e8:93:55:f3:41:49:e9:9d:cc:ec:76:13:fd:

```

```

a5:8d:cb:5b:45:08:b7:d1:c5:b5:58:89:47:ce:12:
bd:5c:ce:b6:17:2f:e0:fc:c0:3e:b7:c4:99:31:5b:
8a:f0:ea:02:fd:2d:44:7a:67
Exponent: 65537 (0x10001)
X509v3 extensions:
  X509v3 Basic Constraints:
    CA:FALSE
  Netscape Cert Type:
    SSL Client, S/MIME
  X509v3 Key Usage:
    Digital Signature, Non Repudiation, Key Encipherment
  X509v3 Extended Key Usage:
    TLS Web Client Authentication, E-mail Protection, Microsoft Smartcardlogin
  Netscape Comment:
    User Certificate of OpenCA Labs
  X509v3 Subject Key Identifier:
    91:95:51:DD:BF:4F:55:FA:E4:C4:D0:10:C2:A1:C2:99:AF:A5:CB:30
  X509v3 Authority Key Identifier:
    keyid:DF:D2:C9:1A:06:1F:BC:61:54:39:FE:12:C4:22:64:EB:57:3B:11:9F

  X509v3 Subject Alternative Name:
    email:fips@ccc.com
  X509v3 Issuer Alternative Name:
    email:pki@openca.org
  Authority Information Access:
    CA Issuers - URI:http://titan/pki/pub/cacert/cacert.crt
    OCSP - URI:http://titan:2560/
    1.3.6.1.5.5.7.48.12 - URI:http://titan:830/

  X509v3 CRL Distribution Points:

    Full Name:
      URI:http://titan/pki/pub/crl/cacrl.crl

Signature Algorithm: sha256WithRSAEncryption
94:ef:56:70:48:66:be:8f:9d:bb:77:0f:c9:f4:65:77:e3:bd:
ea:9a:b8:24:ae:a1:38:2d:f4:ab:e8:0e:93:c2:30:33:c8:ef:
f5:e9:eb:9d:37:04:6f:99:bd:b2:c0:e9:eb:b1:19:7e:e3:cb:
95:cd:6c:b8:47:e2:cf:18:8d:99:f4:11:74:b1:1b:86:92:98:
af:a2:34:f7:1b:15:ee:ea:91:ed:51:17:d0:76:ec:22:4c:56:
da:d6:d1:3c:f2:43:31:4f:1d:20:c8:c2:c3:4d:e5:92:29:ee:
43:c6:d7:72:92:e8:13:87:38:9a:9c:cd:54:38:b2:ad:ba:aa:
f9:a4:68:b5:2a:df:9a:31:2f:42:80:0c:0c:d9:6d:b3:ab:0f:
dd:a0:2c:c0:aa:16:81:aa:d9:33:ca:01:75:94:92:44:05:1a:
65:41:fa:1e:41:b5:8a:cc:2b:09:6e:67:70:c4:ed:b4:bc:28:
04:50:a6:33:65:6d:49:3c:fc:a8:93:88:53:94:4c:af:23:64:
cb:af:e3:02:d1:b6:59:5f:95:52:6d:00:00:a0:cb:75:cf:b4:
50:c5:50:00:65:f4:7d:69:cc:2d:68:a4:13:5c:ef:75:aa:8f:

```

```
3f:ca:fa:eb:4d:d5:5d:27:db:46:c7:f4:7d:3a:b2:fb:a7:c9:
de:18:9d:c1
```

显示 PKI 域 aaa 中的所有对端证书的简要信息。

```
<Sysname> display pki certificate domain aaa peer
Total peer certificates: 1
```

```
Serial Number: 9a0337eb2156balf5476e4d754a5a9f7
Subject Name: CN=sldsslserver
```

显示 PKI 域 aaa 中的一个特定序号的对端证书的详细信息。

```
<Sysname> display pki certificate domain aaa peer serial 9a0337eb2156balf5476e4d754a5a9f7
```

Certificate:

Data:

Version: 3 (0x2)

Serial Number:

9a:03:37:eb:21:56:ba:1f:54:76:e4:d7:54:a5:a9:f7

Signature Algorithm: sha1WithRSAEncryption

Issuer: C=cn, O=ccc, OU=sec, CN=ssl

Validity

Not Before: Oct 15 01:23:06 2010 GMT

Not After : Jul 26 06:30:54 2012 GMT

Subject: CN=sldsslserver

Subject Public Key Info:

Public Key Algorithm: rsaEncryption

Public-Key: (1024 bit)

Modulus:

```
00:c2:cf:37:76:93:29:5e:cd:0e:77:48:3a:4d:0f:
a6:28:a4:60:f8:31:56:28:7f:81:e3:17:47:78:98:
68:03:5b:72:f4:57:d3:bf:c5:30:32:0d:58:72:67:
04:06:61:08:3b:e9:ac:53:b9:e7:69:68:1a:23:f2:
97:4c:26:14:c2:b5:d9:34:8b:ee:c1:ef:af:1a:f4:
39:da:c5:ae:ab:56:95:b5:be:0e:c3:46:35:c1:52:
29:9c:b7:46:f2:27:80:2d:a4:65:9a:81:78:53:d4:
ca:d3:f5:f3:92:54:85:b3:ab:55:a5:03:96:2b:19:
8b:a3:4d:b2:17:08:8d:dd:81
```

Exponent: 65537 (0x10001)

X509v3 extensions:

X509v3 Authority Key Identifier:

keyid:9A:83:29:13:29:D9:62:83:CB:41:D4:75:2E:52:A1:66:38:3C:90:11

X509v3 Key Usage: critical

Digital Signature, Non Repudiation, Key Encipherment, Data Encipherment, Key

Agreement

Netscape Cert Type:

SSL Server

X509v3 Subject Alternative Name:

DNS:docm.com

X509v3 Subject Key Identifier:


```
3C:76:95:9B:DD:C2:7F:5F:98:83:B7:C7:A0:F8:99:1E:4B:D7:2F:26
X509v3 CRL Distribution Points:
```

```
Full Name:
URI:http://s03130.ccc.sec.com:447/ssl.crl
```

```
Signature Algorithm: sha1WithRSAEncryption
61:2d:79:c7:49:16:e3:be:25:bb:8b:70:37:31:32:e5:d3:e3:
31:2c:2d:c1:f9:bf:50:ad:35:4b:c1:90:8c:65:79:b6:5f:59:
36:24:c7:14:63:44:17:1e:e4:cf:10:69:fc:93:e9:70:53:3c:
85:aa:40:7e:b5:47:75:0f:f0:b2:da:b4:a5:50:dd:06:4a:d5:
17:a5:ca:20:19:2c:e9:78:02:bd:19:77:da:07:1a:42:df:72:
ad:07:7d:e5:16:d6:75:eb:6e:06:58:ee:76:31:63:db:96:a2:
ad:83:b6:bb:ba:4b:79:59:9d:59:6c:77:59:5b:d9:07:33:a8:
f0:a5
```

表1-4 display pki certificate 命令显示信息描述表

字段	描述
Version	证书版本号
Serial Number	证书序列号
Signature Algorithm	签名算法
Issuer	证书颁发者
Validity	证书有效期
Subject	证书所属的实体信息
Subject Public Key Info	证书所属的实体的公钥信息
X509v3 extensions	X.509版本3格式的证书扩展属性

【相关命令】

- `pki domain`
- `pki retrieve-certificate`

1.1.15 display pki certificate request-status

`display pki certificate request-status` 命令用来显示证书的申请状态。

【命令】

```
display pki certificate request-status [ domain domain-name ]
```

【视图】

任意视图

【缺省用户角色】

```
network-admin
network-operator
```

【参数】

domain *domain-name*: 指定证书所在的 PKI 域的名称，为 1~31 个字符的字符串，不区分大小写，不能包括 “~”、“*”、“\”、“|”、“:”、“.”、“<”、“>”、“” 和 “'”。

【使用指导】

若不指定 PKI 域的名称，则显示所有 PKI 域的证书申请状态。

【举例】

```
# 显示 PKI 域 aaa 的证书申请状态。
<Sysname> display pki certificate request-status domain aaa
Certificate Request Transaction 1
    Domain name: aaa
    Status: Pending
    Key usage: General
    Remain polling attempts: 10
    Next polling attempt after : 1191 seconds
```

```
# 显示所有 PKI 域的证书申请状态。
<Sysname> display pki certificate request-status
Certificate Request Transaction 1
    Domain name: domain1
    Status: Pending
    Key usage: General
    Remain polling attempts: 10
    Next polling attempt after : 1191 seconds
Certificate Request Transaction 2
    Domain name: domain2
    Status: Pending
    Key usage: Signature
    Remain polling attempts: 10
    Next polling attempt after : 188 seconds
```

表1-5 display pki certificate request 命令显示信息描述表

字段	描述
Certificate Request Transaction <i>number</i>	证书申请任务的编号，从1开始顺序编号
Domain name	PKI域名
Status	证书申请状态。目前，仅有一种取值Pending，表示等待
Key usage	证书用途，包括以下取值： <ul style="list-style-type: none">• General: 表示通用，既可以用于加密也可以用于签名• Signature: 表示用于签名• Encryption: 表示用于加密
Remain polling attempts	剩余的证书申请状态的查询次数
Next polling attempt after	当前到下次查询证书申请状态的时间间隔，单位为秒

【相关命令】

- `certificate request polling`
- `pki domain`
- `pki retrieve-certificate`

1.1.16 `display pki crl domain`

`display pki crl domain` 命令用来显示存储在本地的 CRL。

【命令】

`display pki crl domain domain-name`

【视图】

任意视图

【缺省用户角色】

`network-admin`
`network-operator`

【参数】

domain *domain-name*: 指定 CRL 所在的 PKI 域的名称，为 1~31 个字符的字符串，不区分大小写，不能包括“~”、“*”、“\”、“|”、“:”、“.”、“<”、“>”、“”和“'”。

【使用指导】

用户可以通过该命令查看证书吊销列表，看所需的证书是否已经被吊销。

【举例】

显示 PKI 域 `aaa` 存储在本地的 CRL。

```
<Sysname> display pki crl domain aaa
```

```
Certificate Revocation List (CRL):
```

```
Version 2 (0x1)
```

```
Signature Algorithm: sha1WithRSAEncryption
```

```
Issuer: /C=cn/O=docm/OU=sec/CN=therootca
```

```
Last Update: Apr 28 01:42:13 2011 GMT
```

```
Next Update: NONE
```

```
CRL extensions:
```

```
    X509v3 CRL Number:
```

```
        6
```

```
    X509v3 Authority Key Identifier:
```

```
        keyid:49:25:DB:07:3A:C4:8A:C2:B5:A0:64:A5:F1:54:93:69:14:51:11:EF
```

```
Revoked Certificates:
```

```
    Serial Number: CDE626BF7A44A727B25F9CD81475C004
```

```
    Revocation Date: Apr 28 01:37:52 2011 GMT
```

```
    CRL entry extensions:
```

```
        Invalidity Date:
```

```
            Apr 28 01:37:49 2011 GMT
```

```
    Serial Number: FCADFA81E1F56F43D3F2D3EF7EB56DE5
```

```

Revocation Date: Apr 28 01:33:28 2011 GMT
CRL entry extensions:
    Invalidity Date:
        Apr 28 01:33:09 2011 GMT
Signature Algorithm: sha1WithRSAEncryption
57:ac:00:3e:1e:e2:5f:59:62:04:05:9b:c7:61:58:2a:df:a4:
5c:e5:c0:14:af:c8:e7:de:cf:2a:0a:31:7d:32:da:be:cd:6a:
36:b5:83:e8:95:06:bd:b4:c0:36:fe:91:7c:77:d9:00:0f:9e:
99:03:65:9e:0c:9c:16:22:ef:4a:40:ec:59:40:60:53:4a:fc:
8e:47:57:23:e0:75:0a:a4:1c:0e:2f:3d:e0:b2:87:4d:61:8a:
4a:cb:cb:37:af:51:bd:53:78:76:a1:16:3d:0b:89:01:91:61:
52:d0:6f:5c:09:59:15:be:b8:68:65:0c:5d:1b:a1:f8:42:04:
ba:aa

```

表1-6 display pki crl domain 显示信息描述表

字段	描述
Version	CRL版本号
Signature Algorithm	CA签名该CRL采用的签名算法
Issuer	颁发该CRL的CA证书名称
Last Update	上次更新CRL的时间
Next Update	下次更新CRL的时间
CRL extensions	CRL扩展属性
X509v3 CRL Number	X509版本3格式的CRL序号
X509v3 Authority Key Identifier	X509版本3格式的签发该CRL的CA的标识符
keyid	公钥标识符 一个CA可能有多个密钥对，该字段用于标识CA用哪个密钥对对该CRL进行签名
Revoked Certificates	撤销的证书信息
Serial Number	被吊销证书的序列号
Revocation Date	证书被吊销的日期
CRL entry extensions:	CRL项目扩展属性
Signature Algorithm:	签名算法以及签名数据

【相关命令】

- **pki retrieve-crl**

1.1.17 fqdn

fqdn 命令用来配置 PKI 实体的 FQDN。

undo fqdn 命令用来恢复缺省情况。

【命令】

```
fqdn fqdn-name-string  
undo fqdn
```

【缺省情况】

未配置 PKI 实体的 FQDN。

【视图】

PKI 实体视图

【缺省用户角色】

network-admin

【参数】

fqdn-name-string: PKI 实体的 FQDN，为 1~255 个字符的字符串，区分大小写。形式为 *hostname@domainname*

【使用指导】

FQDN 是实体在网络中的唯一标识，由一个主机名和一个域名组成。

【举例】

```
# 配置 PKI 实体 en 的 FQDN 为 abc@pki.domain.com。  
<Sysname> system-view  
[Sysname] pki entity en  
[Sysname-pki-entity-en] fqdn abc@pki.domain.com
```

1.1.18 ip

ip 命令用来配置 PKI 实体的 IP 地址。

undo ip 命令用来恢复缺省情况。

【命令】

```
ip { ip-address | interface interface-type interface-number }  
undo ip
```

【缺省情况】

未配置 PKI 实体的 IP 地址。

【视图】

PKI 实体视图

【缺省用户角色】

network-admin

【参数】

ip-address: 指定 PKI 实体的 IP 地址。

interface *interface-type interface-numbe*: 指定接口的主 IP 地址作为 PKI 实体的 IP 地址。*interface-type interface-number* 表示接口类型及接口编号。

【使用指导】

通过本命令，可以直接指定 PKI 实体的 IP 地址，也可以指定设备上某接口的主 IP 地址作为 PKI 实体的 IP 地址。如果指定使用某接口的 IP 地址，则不要求本配置执行时该接口上已经配置了 IP 地址，只要设备申请证书时，该接口上配置了 IP 地址，就可以直接使用该地址作为 PKI 实体身份的一部分。

【举例】

配置 PKI 实体 en 的 IP 地址为 192.168.0.2。

```
<Sysname> system-view
[Sysname] pki entity en
[Sysname-pki-entity-en] ip 192.168.0.2
```

1.1.19 ldap-server

ldap-server 命令用来指定 LDAP 服务器。

undo ldap-server 命令用来恢复缺省情况。

【命令】

```
ldap-server host hostname [ port port-number ]
undo ldap-server
```

【缺省情况】

未指定 LDAP 服务器。

【视图】

PKI 域视图

【缺省用户角色】

network-admin

【参数】

host *hostname*: LDAP 服务器的主机名，为 1~255 个字符的字符串，区分大小写，支持 IPv4 与 IPv6 地址的表示方法以及 DNS 域名的表示方法。

port *port-number*: LDAP 服务器的端口号，取值范围为 1~65535，缺省值为 389。

【使用指导】

以下两种情况下，需要配置 LDAP 服务器：

- 通过 LDAP 协议获取本地证书或对端证书时，需要指定 LDAP 服务器。
- 通过 LDAP 协议获取 CRL 时，若 PKI 域中配置的 LDAP 格式的 CRL 发布点 URL 中未携带主机名或 IP 地址，则需要根据此处配置的 LDAP 服务器地址来得到完整的 LDAP 发布点 URL。

在一个 PKI 域中，只能指定一个 LDAP 服务器，多次执行本命令，最后一次执行的命令生效。

【举例】

指定 LDAP 服务器的 IP 地址为 10.0.0.1。

```
<Sysname> system-view
[Sysname] pki domain aaa
[Sysname-pki-domain-aaa] ldap-server host 10.0.0.1
```

【相关命令】

- `pki retrieve-certificate`
- `pki retrieve-crl`

1.1.20 locality

locality 命令用来配置 PKI 实体所在的地理区域名称，比如城市名称。

undo locality 命令用来恢复缺省情况。

【命令】

```
locality locality-name
```

```
undo locality
```

【缺省情况】

未配置 PKI 实体所在的地理区域名称。

【视图】

PKI 实体视图

【缺省用户角色】

network-admin

【参数】

locality-name: PKI 实体所在的地理区域的名称，为 1~63 个字符的字符串，区分大小写，不能包含逗号。

【举例】

配置 PKI 实体 en 所在地理区域的名称为 pukras。

```
<Sysname> system-view  
[Sysname] pki entity en  
[Sysname-pki-entity-en] locality pukras
```

1.1.21 organization

organization 命令用来配置 PKI 实体所属组织的名称。

undo organization 命令用来恢复缺省情况。

【命令】

```
organization org-name
```

```
undo organization
```

【缺省情况】

未配置 PKI 实体所属组织名称。

【视图】

PKI 实体视图

【缺省用户角色】

network-admin

【参数】

org-name: PKI 实体所属的组织名称，为 1~63 个字符的字符串，区分大小写，不能包含逗号。

【举例】

配置 PKI 实体 en 所属的组织名称为 abc。

```
<Sysname> system-view
[Sysname] pki entity en
[Sysname-pki-entity-en] organization abc
```

1.1.22 organization-unit

organization-unit 命令用来指定实体所属的组织部门的名称。

undo organization-unit 命令用来恢复缺省情况。

【命令】

```
organization-unit org-unit-name
undo organization-unit
```

【缺省情况】

未配置 PKI 实体所属组织部门的名称。

【视图】

PKI 实体视图

【缺省用户角色】

network-admin

【参数】

org-unit-name: PKI 实体所属组织部门的名称，为 1~63 个字符的字符串，区分大小写，不能包含逗号。使用该参数可在同一个组织内区分不同部门的 PKI 实体。

【举例】

配置 PKI 实体 en 所属组织部门的名称为 rdtest。

```
<Sysname> system-view
[Sysname] pki entity en
[Sysname-pki-entity-en] organization-unit rdtest
```

1.1.23 pki abort-certificate-request

pki abort-certificate-request 命令用来停止证书申请过程。

【命令】

```
pki abort-certificate-request domain domain-name
```

【视图】

系统视图

【缺省用户角色】

network-admin

【参数】

domain *domain-name*: 指定证书所在的 PKI 域的名称，为 1~31 个字符的字符串，不区分大小写，不能包括 “~”、“*”、“\”、“|”、“:”、“.”、“<”、“>”、“” 和 “'”。

【使用指导】

用户在证书申请时，可能由于某种原因需要改变证书申请的一些参数，比如通用名、国家代码、FQDN 等，而此时证书申请正在运行，为了新的申请不与之前的申请发生冲突，建议先停止之前的申请程序，再进行新的申请。

【举例】

```
# 停止证书申请过程。
<Sysname> system-view
[Sysname] pki abort-certificate-request domain 1
The certificate request is in process.
Confirm to abort it? [Y/N]:y
```

【相关命令】

- **display pki certificate request-status**
- **pki request-certificate domain**

1.1.24 pki certificate access-control-policy

pki certificate access-control-policy 命令用来创建证书访问控制策略，并进入证书访问控制策略视图。如果指定的证书访问控制策略已存在，则直接进入其视图。

undo pki certificate access-control-policy 命令用来删除指定的证书访问控制策略。

【命令】

```
pki certificate access-control-policy policy-name
undo pki certificate access-control-policy policy-name
```

【缺省情况】

不存在证书访问控制策略。

【视图】

系统视图

【缺省用户角色】

network-admin

【参数】

policy-name: 表示证书访问控制策略名称，为 1~31 个字符的字符串，不区分大小写。

【使用指导】

一个证书访问控制策略中可以定义多个证书属性的访问控制规则。

【举例】

配置一个名称为 **mypolicy** 的证书访问控制策略，并进入证书访问控制策略视图。

```
<Sysname> system-view
[Sysname] pki certificate access-control-policy mypolicy
[Sysname-pki-cert-acp-mypolicy]
```

【相关命令】

- **display pki certificate access-control-policy**
- **rule**

1.1.25 pki certificate attribute-group

pki certificate attribute-group 命令用来创建证书属性组并进入证书属性组视图。如果指定的证书属性组已存在，则直接进入其视图。

undo pki certificate attribute-group 命令用来删除指定的证书属性组。

【命令】

```
pki certificate attribute-group group-name
undo pki certificate attribute-group group-name
```

【缺省情况】

不存在证书属性组。

【视图】

系统视图

【缺省用户角色】

network-admin

【参数】

group-name：证书属性组名称，为 1~31 个字符的字符串，不区分大小写。

【使用指导】

一个证书属性组就是一系列证书属性规则（通过 **attribute** 命令配置）的集合，这些属性规则定义了对证书的颁发者名、主题名以及备用主题名进行过滤的匹配条件。当证书属性组下没有任何属性规则时，则认为对证书的属性没有任何限制。

【举例】

创建一个名为 **mygroup** 的证书属性组，并进入证书属性组视图。

```
<Sysname> system-view
[Sysname] pki certificate attribute-group mygroup
[Sysname-pki-cert-attribute-group-mygroup]
```

【相关命令】

- **attribute**
- **display pki certificate attribute-group**
- **rule**

1.1.26 pki delete-certificate

pki delete-certificate 命令用来删除 PKI 域中的证书。

【命令】

```
pki delete-certificate domain domain-name { ca | local | peer [ serial  
serial-num ] }
```

【视图】

系统视图

【缺省用户角色】

network-admin

【参数】

domain domain-name: 证书所在的 PKI 域的名称，为 1~31 个字符的字符串，不区分大小写，不能包括“~”、“*”、“\”、“|”、“:”、“.”、“<”、“>”、“”和“'”。

ca: 表示删除 CA 证书。

local: 表示删除本地证书。

peer: 表示删除对端证书。

serial serial-num: 表示通过指定序列号删除一个指定的对端证书。*serial-num* 为对端证书的序列号，为 1~127 个字符的字符串，不区分大小写。在每个 CA 签发的证书范围内，序列号可以唯一标识一个证书。如果不指定本参数，则表示删除本 PKI 域中的所有对端证书。

【使用指导】

删除 CA 证书时将同时删除所在 PKI 域中的本地证书和所有对端证书，以及 CRL。

如果需要删除指定的对端证书，则需要首先通过 **display pki certificate** 命令查看本域中已有的对端证书的序列号，然后再通过指定序列号的方式删除该对端证书。

【举例】

删除 PKI 域 aaa 中的 CA 证书。

```
<Sysname> system-view  
[Sysname] pki delete-certificate domain aaa ca  
Local certificates, peer certificates and CRL will also be deleted while deleting the CA  
certificate.  
Confirm to delete the CA certificate? [Y/N]:y  
[Sysname]
```

删除 PKI 域 aaa 中的本地证书。

```
<Sysname> system-view  
[Sysname] pki delete-certificate domain aaa local  
[Sysname]
```

删除 PKI 域 aaa 中的所有对端证书。

```
<Sysname> system-view  
[Sysname] pki delete-certificate domain aaa peer  
[Sysname]
```

首先查看 PKI 域 aaa 中的对端证书，然后通过指定序列号的方式删除对端证书。

```
<Sysname> system-view
```

```
[Sysname] display pki certificate domain aaa peer
Total peer certificates: 1
```

```
Serial Number: 9a0337eb2156balf5476e4d754a5a9f7
```

```
Subject Name: CN=abc
```

```
[Sysname] pki delete-certificate domain aaa peer serial 9a0337eb2156balf5476e4d754a5a9f7
```

【相关命令】

- **display pki certificate**

1.1.27 pki domain

pki domain 命令用来创建 PKI 域，并进入 PKI 域视图。如果指定的 PKI 域已存在，则直接进入 PKI 域视图。

undo pki domain 命令用来删除指定的 PKI 域。

【命令】

```
pki domain domain-name
```

```
undo pki domain domain-name
```

【缺省情况】

不存在 PKI 域。

【视图】

系统视图

【缺省用户角色】

network-admin

【参数】

domain-name: PKI 域名，为 1~31 个字符的字符串，不区分大小写，不能包括“~”、“*”、“\”、“|”、“:”、“.”、“<”、“>”、“”和“'”。

【使用指导】

删除 PKI 域的同时，会将该域相关的证书和 CRL 都删除掉，因此请慎重操作。

【举例】

创建 PKI 域 aaa 并进入 PKI 域视图。

```
<Sysname> system-view
[Sysname] pki domain aaa
[Sysname-pki-domain-aaa]
```

1.1.28 pki entity

pki entity 命令用来创建 PKI 实体，并进入 PKI 实体视图。如果指定的 PKI 实体已存在，则直接进入 PKI 实体视图。

undo pki entity 命令用来删除指定的 PKI 实体。

【命令】

```
pki entity entity-name
undo pki entity entity-name
```

【缺省情况】

不存在 PKI 实体。

【视图】

系统视图

【缺省用户角色】

network-admin

【参数】

entity-name: PKI 实体的名称，为 1~31 个字符的字符串，不区分大小写。

【使用指导】

在 PKI 实体视图下可配置 PKI 实体的各种属性（通用名、组织部门、组织、地理区域、省、国家、FQDN、IP），这些属性用于描述 PKI 实体的身份信息。当申请证书时，PKI 实体的信息将作为证书中主题（Subject）部分的内容。

【举例】

创建名称为 en 的 PKI 实体，并进入该实体视图。

```
<Sysname> system-view
[Sysname] pki entity en
[Sysname-pki-entity-en]
```

【相关命令】

- **pki domain**

1.1.29 pki export

pki export 命令用来将 PKI 域中的 CA 证书、本地证书导出到文件中或终端上。

【命令】

```
pki export domain domain-name der { all | ca | local } filename filename
pki export domain domain-name p12 { all | local } passphrase p12-key filename
filename
pki export domain domain-name pem { { all | local } [ { 3des-cbc | aes-128-cbc
| aes-192-cbc | aes-256-cbc | des-cbc } pem-key ] | ca } [ filename filename ]
```

【视图】

系统视图

【缺省用户角色】

network-admin

【参数】

domain *domain-name*: 证书所在的 PKI 域的名称, 为 1~31 个字符的字符串, 不区分大小写, 不能包括 “~”、“*”、“\”、“|”、“:”、“.”、“<”、“>”、“” 和 “'”。

der: 指定证书文件格式为 DER 编码 (包括 PKCS#7 格式的证书)。

p12: 指定证书文件格式为 PKCS#12 编码。

pem: 指定证书文件格式为 PEM 编码。

all: 表示导出所有证书, 包括 PKI 域中所有的 CA 证书和本地证书, 但不包括 RA 证书。

ca: 表示导出 CA 证书。

local: 表示导出本地证书或者本地证书和其对应私钥。

passphrase *p12-key*: 指定对 PKCS12 编码格式的本地证书对应的私钥进行加密所采用的口令。

3des-cbc: 对本地证书对应的私钥数据采用 3DES_CBC 算法进行加密。

aes-128-cbc: 对本地证书对应的私钥数据采用 128 位 AES_CBC 算法进行加密。

aes-192-cbc: 对本地证书对应的私钥数据采用 192 位 AES_CBC 算法进行加密。

aes-256-cbc: 对本地证书对应的私钥数据采用 256 位 AES_CBC 算法进行加密。

des-cbc: 对本地证书对应的私钥数据采用 DES_CBC 算法进行加密。

pem-key: 指定对 PEM 编码格式的本地证书对应的私钥进行加密所采用的口令。

filename *filename*: 指定保存证书的文件名, 不区分大小写。如果不指定本参数, 则表示要将证书直接导出到终端上显示, 这种方式仅 PEM 编码格式的证书才支持。

【使用指导】

导出 CA 证书时, 如果 PKI 域中只有一个 CA 证书则导出单个 CA 证书到用户指定的一个文件或终端, 如果是一个 CA 证书链则导出整个 CA 证书链到用户指定的一个文件或终端。

导出本地证书时, 设备上实际保存证书的证书文件名称并不一定是用户指定的名称, 它与本地证书的密钥对用途相关, 具体的命名规则如下 (假设用户指定的文件名为 *certificate*):

- 如果本地证书的密钥对用途为签名, 则证书文件名称为 *certificate-signature*;
- 如果本地证书的密钥对用途为加密, 则证书文件名称为 *certificate-encryption*;
- 如果本地证书的密钥对用途为通用 (RSA/ECDSA/DSA), 则证书文件名称为用户输入的 *certificate*。

导出本地证书时, 如果 PKI 域中有两个本地证书, 则导出结果如下:

- 若指定文件名, 则将每个本地证书分别导出到一个单独的文件中;
- 若不指定文件名, 则将所有本地证书一次性全部导出到终端上, 并由不同的提示信息进行分割显示。

导出所有证书时, 如果 PKI 域中只有本地证书或者只有 CA 证书, 则导出结果与单独导出相同。如果 PKI 域中存在本地证书和 CA 证书, 则具体导出结果如下:

- 若指定文件名, 则将每个本地证书分别导出到一个单独的文件, 该本地证书对应的完整 CA 证书链也会同时导出到该文件中。
- 若不指定文件名, 则将所有的本地证书及域中的 CA 证书或者 CA 证书链一次性全部导出到终端上, 并由不同的提示信息进行分割显示。

以 PKCS12 格式导出所有证书时, PKI 域中必须有本地证书, 否则会导出失败。

以 PEM 格式导出本地证书或者所有证书时，若不指定私钥的加密算法和私钥加密口令，则不会导出本地证书对应的私钥信息。

以 PEM 格式导出本地证书或者所有证书时，若指定私钥加密算法和私钥加密口令，且此时本地证书有匹配的私钥，则同时导出本地证书的私钥信息；如果此时本地证书没有匹配的私钥，则导出该本地证书失败。

导出本地证书时，若当前 PKI 域中的密钥对配置已被修改，导致本地证书的公钥与该密钥对的公钥部分不匹配，则导出该本地证书失败。

导出本地证书或者所有证书时，如果 PKI 域中有两个本地证书，则导出某种密钥用途的本地证书失败并不会影响导出另外一个本地证书。

指定的文件名中可以带完整路径，当系统中不存在用户所指定路径时，则会导出失败。

【举例】

导出 PKI 域中的 CA 证书到 DER 编码的文件，文件名称为 cert-ca.der。

```
<Sysname> system-view
```

```
[Sysname] pki export domain domain1 der ca filename cert-ca.der
```

导出 PKI 域中的本地证书到 DER 编码的文件，文件名称为 cert-lo.der。

```
<Sysname> system-view
```

```
[Sysname] pki export domain domain1 der local filename cert-lo.der
```

导出 PKI 域中的所有证书到 DER 编码的文件，文件名称为 cert-all.p7b。

```
<Sysname> system-view
```

```
[Sysname] pki export domain domain1 der all filename cert-all.p7b
```

导出 PKI 域中的 CA 证书到 PEM 编码的文件，文件名称为 cacert。

```
<Sysname> system-view
```

```
[Sysname] pki export domain domain1 pem ca filename cacert
```

导出 PKI 域中的本地证书及其对应的私钥到 PEM 编码的文件，指定保护私钥信息的加密算法为 DES_CBC、加密口令为 111，文件名称为 local.pem。

```
<Sysname> system-view
```

```
[Sysname] pki export domain domain1 pem local des-cbc 111 filename local.pem
```

导出 PKI 域中所有证书到 PEM 编码的文件，不指定加密算法和加密口令，不导出本地证书对应的私钥信息，文件名称为 all.pem。

```
<Sysname> system-view
```

```
[Sysname] pki export domain domain1 pem all filename all.pem
```

以 PEM 格式导出 PKI 域中本地证书及其对应的私钥到终端，指定保护私钥信息的加密算法为 DES_CBC、加密口令为 111。

```
<Sysname> system-view
```

```
[Sysname] pki export domain domain1 pem local des-cbc 111
```

```
%The signature usage local certificate:
```

```
Bag Attributes
```

```
    friendlyName:
```

```
        localKeyID: 99 0B C2 3B 8B D1 E4 33 42 2B 31 C3 37 C0 1D DF 0D 79 09 1D
```

```
subject=/C=CN/O=OpenCA Labs/OU=Users/CN=chktest chktest
```

```
issuer=/C=CN/O=OpenCA Labs/OU=software/CN=abcd
```

```
-----BEGIN CERTIFICATE-----
```

```
MIIEqjCCA5KgAwIBAgILAOHID4rI04kBfYgwdQYJKoZIhvcNAQELBQAwRTELMAkG
```

```
A1UEBhMCQ04xFDASBgNVBAoMCO9wZW5DQSBMYWJzMREwDwYDVQQLDhzb2Z0d2Fy
ZTENMASGA1UEAwWEYWJjZDAeFw0xMTA0MjYxMzMxMjlaFw0xMjA0MjUxMzMxMjla
ME0xCzAJBgNVBAYTAkNOMRQwEgYDVQQKDATPcGVuQ0EgTGFIczEOMAwGA1UECwwF
VXNlcnMxGDAWBgNVBAMMD2Noa3Rlc3QgY2hrdGVzdDCBnzANBgkqhkiG9w0BAQEF
AAOBjQAwgYkCgYEA54rUZ0Ux2kApceE4ATpQ437CU6ovuHS5eJKZyky8fhMoTHhE
jE2KfBQIzOZSgo2mdgpkccjr9Ek6IUC03ed1lPn0IG/YaAl4Tjgkiv+w1Nr1SvAy
cnPaSUko2Qb09sg3ycyelzqpbqj775ulGpcXyXYD9OY63/Cp5+DRQ92zGsCAwEA
AaOAhUwggIRMAkGA1UdEwQCMAAUAYDVR0gBEkwRzAGBgQqAwMEMAYGBCoDAwUw
NQYEkGMDBJAtMCsGCCsGAQUFBwIBFh9odHRwczoVL3RpdGFuL3BraS9wdWiwY3Bz
L2Jhc2ljbMEGECWCSAGG+EIBAQQEAWIFoDALBgNVHQ8EBAMCBsAwKQYDVR0lBCIw
IAYIKwYBBQUHAWIGCCsGAQUFBwMEBgorBgEEAYI3FAICMC4GCWCSAGG+EIBDQqh
Fh9Vc2VyIENlcnRpZmljYXRlIG9mIE9wZW5DQSBMYWJzMBOGA1UdDgQWBBTPw8FY
ut7Xr2Ct/23zU/ybgU9dQjAfBgNVHSMEGDAWgBQzEQ58yIC54wxodp6JzZvn/gx0
CDAaBgNVHREEEZARgQ9jaGt0ZXN0QGgzYy5jb20wGQYDVR0SBBIwEIEOcGtpQG9w
ZW5jYS5vcmcwgYEGCCsGAQUFBwEBBHUwczAyBggrBgEFBQcwAoYmaHR0cDovL3Rp
dGFuL3BraS9wdWiwY2FjZlZlL2NhY2VydC5jcnQwHgYIKwYBBQUHMAGGEmh0dHA6
Ly90aXRhbjoyNTYwLzAdBggrBgEFBQcwDIYRaHR0cDovL3RpdGFuOjgzMC8wPAYD
VR0fBDUwMzAxoC+gLYYraHR0cDovLzE5Mi4xNjgUNDAUMTI4L3BraS9wdWiwY3Js
L2NhY3JzLmNybdANBgkqhkiG9w0BAQsFAAOCAQEAGcMeSpBjiuRmsJW0iZK5nygB
tgD8c0b+n4v/F36sJjY1fRFSr4gPLixZhPWhTrgsCd+QMELRCDNHDxvt3/1NEG12
X6BVjLcKXKH/EQe0fnwK+7PegAJ15P56xDeACHz2oysvNQ0Ot6hGylMqaZ8pKUKv
UDS8c+HgIBrhmxvXztI08NlimYHq27Wyr9j6NpSS60mFmI5whzCWfTSHzq1T2DNd
no0id18S2idApfCZL8zoMWEFI163JZSarv+H5Kbb063dxXfbsqX9Noxggh0gD8dK
7X7/rTJuuhTWVof5gxSUJp+aCCdvSKg0lvJY+tJeXoaznrINVw3SuXJ+Ax8GEw==
-----END CERTIFICATE-----
```

Bag Attributes

friendlyName:

localKeyID: 99 0B C2 3B 8B D1 E4 33 42 2B 31 C3 37 C0 1D DF 0D 79 09 1D

Key Attributes: <No Attributes>

-----BEGIN ENCRYPTED PRIVATE KEY-----

```
MIICwzA9BgkqhkiG9w0BBQowMDAbBgkqhkiG9w0BBQwwDgQIAbfceE+KoYYoCAggA
MBEGBSSoAwIHBAjB+UsJM07JRQSCAoABqtASbjGTQbdxL3n4wNHmyWLxbvL9v27C
Uu6MjYJDCipVzxHU0rExgn+6cQsK5uK99FPBmy4q9/nnyrooTX8BVlXAjenvgyii
WQLwnIglIuM8j2aPkQ3wbael+0RACjSLy1u/PCl5sp6CDxI0b9xz6cxIGxKvUOCc
/gxdgk97XZSW/0qnOSZkhgeqBZuxq6Va8iRyho7RCStVxQaeiAZpq/WoZbcS5CKI
/WXEBQd4AX2UxN0Ld/On7Wc6KFToixROTxWtft8SEsKGPdfrEKq3fSTWlxokB8nM
bkRtU+fUiY27V/mr1RHO6+yEr+/wGGClBy5YDoD4I9xPkGUkmqx+kfYbMo4yxkSi
JdL+X3uEjHnQ/rvnPSKBEU/URwXHxMX9CdCTSqH/SajnrGuB/E4JhOEnS/H9dIM+
DN6iz1IwPFklbcK9KMgWVlbosymXmuEbYCYmSmhZb5FnR/RIyE804Jz9ifin3g0Q
ZrykfG7LHL7Ga4nh0hpEeDiHGEMcQU+g0EtfpOLTI8cMJf7kdNWDnI0AYCvBAAM
3CY3BE1DVjJq3ioyHSJca8C+3lzcueuAF+107Y4Zluq3dqWuUjE+/1BZJbMmaQA
X6NmXKNzmtTPcMtojf+n3+uju0le0d0QYXQz/wPsV+9IYRYasjzoXE5dhZ5sIPOd
u9x9hhp5Ns23bwyNP135qTNjx9i/CZMKvLKym3Yg+Bg8Df4bBrFrsh1U0ifmmp
ir2+Ouh1C+GbHOxWNEBCa8iAq91k6FGFJ00LA2oIvChnh45tM7BjjKTHk+RZdMiA
0TKSWuOyihrwxdUEWh999GKUpkwDHLZJFd21z/kWspqThodEx8ea
```

-----END ENCRYPTED PRIVATE KEY-----

以 PEM 格式导出 PKI 域中所有证书到终端,指定保护本地证书对应私钥的加密算法为 DES_CBC、加密口令为 111。


```

<Sysname> system-view
[Sysname] pki export domain domain1 pem all des-cbc 111

%The signature usage local certificate:
Bag Attributes
    friendlyName:
        localKeyID: 99 0B C2 3B 8B D1 E4 33 42 2B 31 C3 37 C0 1D DF 0D 79 09 1D
subject=/C=CN/O=OpenCA Labs/OU=Users/CN=chktest chktest
issuer=/C=CN/O=OpenCA Labs/OU=software/CN=abcd
-----BEGIN CERTIFICATE-----
MIIEBqjCCA5KgAwIBAgILAOHID4rI04kBFYgwdQYJKoZIhvcNAQELBQAwRTElMAkG
A1UEBhMCQ04xZDASBgNVBAoMC09wZW5DQSBMYWJzMREwDwYDVQQwLDAhzb2Z0d2Fy
ZTENMA5GA1UEAwEYEWJjZDAeFw0xMTA0MjYxMzMzMjlaFw0xMjA0MjYxMzMzMjla
ME0xCzAJBgNVBAYTAkNOMRQwEgYDVQQKDATPcGVuQ0EgTGFIczEOMAwGA1UECwwF
VXNlcnMxGDAWBgNVBAMMD2Noa3Rlc3QgY2hrdGVzdDCBnzANBgkqhkiG9w0BAQEF
AAOBjQAwGykCgYEA54rUZ0Ux2kApceE4ATpQ437CU6ovuHS5eJKZyky8fhMoTHHe
jE2KfBQIzOZSgo2mdgpkccjr9Ek6IUC03ed1lPn0IG/YaA14Tjgkiv+w1NrlSvAy
cnPaSuko2Qb09sg3ycyelzqpbqqj775ulGpcXyXYD9OY63/Cp5+DRQ92zGsCAwEA
AaOCAhUwggIRMAkGA1UdEwQCMAAwUAYDVR0gBEKwRzAGBgQqAwMEMAYGBCoDAwUw
NQYEkGMDBJatMCsGCCSGAQUFBwIBFh9odHRwczoV3RpdGFuL3BraS9wdWlvY3Bz
L2Jhc2ljbEBEGCWCsSAGG+EIBAQQEAWIFoDALBgNVHQ8EBAMCBsAwKQYDVR0lBCIw
IAYIKwYBBQUHAWIGCCSGAQUFBwMEBgorBgEEAYI3FAICMC4GCWCGSAGG+EIBDQqh
Fh9Vc2VyIENlcnRpZmljYXRlIG9mIE9wZW5DQSBMYWJzMBOGA1UdDgQWBWBTpW8FY
ut7Xr2Ct/23zU/ybgU9dQjAfBgNVHSMEGDAWgBQzEQ58yIC54wxodp6JzZvn/gx0
CDAaBgNVHREEEzARgQ9jaGt0ZXN0QGgzYy5jb20wGQYDVR0SBBIwEIEOcGtpQG9w
ZW5jYS5vcmcwgYEGCCSGAQUFBwEBBHUwcZAYBggrBgEFBQcwAoYmaHR0cDovL3Rp
dGFuL3BraS9wdWlvY2FjZjZlZjZlZjZlZjZlZjZlZjZlZjZlZjZlZjZlZjZlZjZl
Ly90aXRhbjoyNTYwLzAdBggrBgEFBQcwDIYRaHR0cDovL3RpdGFuOjgzMC8wPAYD
VR0fBDUwMzAxoC+gLYYraHR0cDovLzE5Mi4xNjgUNDAUMTI4L3BraS9wdWlvY3Js
L2NhY3JsLmNybdANBgkqhkiG9w0BAQsFAAOCAQEAGcMeSpBJiurmsJW0iZK5nygB
tgD8c0b+n4v/F36sJjY1fRFSr4gPLIxZhPWhTrqsCd+QMELRCDNHDxvt3/1NEG12
X6BVjLcKXKH/EQe0fnwK+7PegAJ15P56xDeACHz2oysvNQ00t6hGylMqaz8pKUKv
UDS8c+HgIBrhmxvXztI08N1imYHq27Wy9j6NpSS60mMFmI5whzCWfTSHzqlT2DNd
no0id18SZidApfCZL8zoMWEFI163JZSarv+H5Kbb063dxXfbsqX9Noxggh0gD8dK
7X7/rTJuuhTWVof5gxSUJp+aCCdvSKg0lvJY+tJeXoaznrINVw3SuXJ+Ax8GEw==
-----END CERTIFICATE-----
Bag Attributes: <No Attributes>
subject=/C=CN/O=OpenCA Labs/OU=software/CN=abcd
issuer=/C=CN/O=OpenCA Labs/OU=software/CN=abcd
-----BEGIN CERTIFICATE-----
MIIEYTCCA0mgAwIBAgIBFzANBgkqhkiG9w0BAQsFADBFMQswCQYDVQQGEwJDTjEU
MBIGA1UECgwLT3BlbkNBIEExhYnMxETAPBgNVBAsMCHNvZnR3YXJlMQ0wCwYDVQQD
DARhYmNkMB4XDTEyMDQxODExNDQ0N1oXDTEyMDQxNzExNDQ0N1owRTElMAkGA1UE
BhMCQ04xZDASBgNVBAoMC09wZW5DQSBMYWJzMREwDwYDVQQwLDAhzb2Z0d2FyZTEN
MASGA1UEAwEYEWJjZDCCASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBAM1g
vomMF8S4u6q51bOwjKFUBWxyvOy4D897LmOSedaCyDt6Lvp+PBEHfWBYBpsHhk7
kmnSNhX5dZ6NxunHaARZ2VlccTsYKyvAQapuaThy1tuOcpHAB+jQQL9dPoqdk0xp
jvmPdLW+k832Konn9U4dIivS0n+/KMgh0g5UyzHGqUUOo7s9qFuQf5EjQon40TZg

```

```
BwUnFYRlvGe7bSQpXjwi8LTyxHPy+dDVjO5CP+rXx5IiToFy1YGWewkyn/WeswDf
Yx7ZludNus5vKWTihgx2Qa1gb+sqUMwI/WUET7gh02dRxPUdUbgIYF0saTndKPYd
4oBg16M0SMsHhe9nF5UCAwEAAaOCAVowggFWMA8GA1UdEwEB/wQFMAMBAf8wCwYD
VR0PBAQDAgEGMB0GA1UdDgQWBQzEQ58yIC54wxodp6JzZvn/gx0CDAfBgNVHSME
GDAWgBQzEQ58yIC54wxodp6JzZvn/gx0CDAZBgNVHREEEjAQgQ5wa2lAb3BlbmNh
Lm9yZzAZBgNVHRIEEjAQgQ5wa2lAb3BlbmNhLm9yZzCBgQYIKwYBBQUHAQEEdTBz
MDIGCCsGAQUFBzAChiZodHRwOi8mdcGl0YW4vcGtpL3B1Yi9jYWN1cnQvY2FjZXJ0
LmNydDAeBggrBgEFBQcwAYYSaHR0cDovL3RpdGFuOjI1NjAvMB0GCCsGAQUFBzAM
hhFodHRwOi8mdcGl0YW46ODMwLzA8BgNVHR8ENTAzMDGgL6AthitodHRwOi8vMTky
LjE2OC40MC4xMjgvcGtpL3B1Yi9jcmwvY2FjcmwvY3JsMA0GCSqGSIb3DQEBCwUA
A4IBAQC0qOSSmVQNfa5ELtRKYF62C/Y8QTLbk6lZDTZuIzN15SGKQcbNM970ffCD
LklzosityEVE7PLnii3bZ5khcGO3byyXfluAqRyOGVJcudaw7uIQqgv0AJQ+zaQSHi
d4kQf5QWgYkQ55/C5puOmcMRgCbMpr2lYkqXLDjTIAZiHRZ/sTp6c+ie2bFxi/YT
3xYbO0wDMuGOKJjpsyKTKcbG9NdfbDyFgzEYAobyYqAUB3C0/bMfBduwhQWKSoyE
6vZsPGAeisCmAl3dIp49jPgVkiXoShraYf1jLsWzJG1zem8QvWYzOqKEDwq3SV0Z
cXK8gzDBcsobcUMkwIYPAmDlkAPX
```

-----END CERTIFICATE-----

Bag Attributes

friendlyName:

localKeyID: 99 0B C2 3B 8B D1 E4 33 42 2B 31 C3 37 C0 1D DF 0D 79 09 1D

Key Attributes: <No Attributes>

-----BEGIN ENCRYPTED PRIVATE KEY-----

```
MIICwzA9BgkqhkiG9w0BBQ0wMDABBgkqhkiG9w0BBQwwDgQICUSKSW9GVmICAggA
MBEGBSsOAwIHBAi5QZM+1SYWPASCAoBKDYule5f2BXL9ZhI9zWAJpx2cShz/9PsW
5Qm106D+xSjleAzKx/m4Xb4xRU8oOAuzulDlWfSHKXoaa0OoRSiOEXleg0eo/2vv
CHCvKHfTjr4gVSSa7i4I+aQ6AitrI6q99Wlkn/e/IE5U1UE4ZhcsIiFJG+IvG7S8
f9liWQ2CImy/hjgFCD9nqSLN8wUzP7O2SdLVlUb5z4FR6VISZdgTFE8j7ko2HtUs
HVSg0nml14EwPtPMMbHefcuQ6b82y1M+dWfVxBN9K031N4tZNfPWwLSRRPvjUzBG
dKtj3/IFdV7/tUMy9JJSp4iFtlh7SZPcOoGp1ZW+YUR30I7YnFE+9Yp/46KWT8
bk7j0STRnZX/xMy/9E52uHkLdW1ET3TXralMYt/4jg4M0jUvoi3GS2Kbo+czsUn
gKqgwYnxVfRSvt8d6GBYrpf2tMFS9LEyngPKXExd+m4mAryuT5PhdFTkb1B190Lp
UIBjk3IXnr7AdrhvYlKh0UuQE95emXBD/K0H1D73cMrtmogL8F4yS5B2hpIr/v5/
eW35+1QMnJ9FtHFVnLx9w19lX8iNfsoBhg6FQ/hNSioN7rNBe7wwIRzxPVfEhO8
5ajQxWlidRn5RkzfUo6HuAcq02QTpSXI6wf2bzsVmr5sk+fRaELD/cwL6VjtXO6x
ZBLJcUyAwvScrOtTEK7Q5n0I34gQd4qcF0D1x9yQ4sqvTeU/7Jkm6XCPV05/5uiF
RLCfFAwaJMBdIQ6jDQHnpWT67uNDWdEzaPmuTVMme5Woc5zsQE5DY3hWu4oqFdDz
kPLnbX74IZ0gOLki9eIJkVswNF5HkBCKS50ejlW6TgbMNZ+JPk2w
```

-----END ENCRYPTED PRIVATE KEY-----

以 PEM 格式导出 PKI 域中 CA 证书到终端。

```
<Sysname> system-view
```

```
[Sysname] pki export domain domain1 pem ca
```

-----BEGIN CERTIFICATE-----

```
MIIB+TCCAWICEQDMbgjRKYgg3vpGFVY6pa3ZMA0GCSqGSIb3DQEBBQUAMD0xCzAJ
BgNVBAYTAmNuMQwwCgYDVQQKEwNoM2MxETAPBgNVBAsTCGgzYy10ZXN0MQ0wCwYD
VQQDEwQ4MDQzMB4XDTEyMDMyMjA0NDQyNFoXDTEyMDMyMzA0MzUyNFowPTELMAkG
A1UEBhMCY24xDDAKBgNVBAoTA2gzYzERMA8GA1UECzMIA2NjLXRlc3QxDTALBgNV
BAMTBDBgNDMwZ8wDQYJKoZIhvcNAQEBBQADgY0AMIGJAoGBAOvDAYQhyc++G7h5
eNDzJs22OQjCn/4JqnNKIdKz1BbaJT8/+IueSn9JISg64Ex2WBeCd/tcmnSW57ag
```

```
dCvNIUYXXVOGca2iaSOElqCF4CQfV9zLrBtA7giHD49T+JbxLrrJLmdIQMJ+vYdC
sCxIp3YMAiuCahVLZeXklooqwqIXAgMBAAEwDQYJKoZIhvcNAQEFBQADgYEAElm7
W2Lp9Xk4nZVIpVV76CkNe8/C+Id00GCRUUVQFSMvo7PdEd76bmYX2KzJSz+DlMqy
TdVrgG9Fp6XTFO80aKJGe6NapsfhJHKS+Q7mL0XpXeMONgK+e3dX7rsDxsY7hF+j
0gwsHrjV7kWvwJvDlhzGW6xbpr4DRmdcao19Cr6o=
```

-----END CERTIFICATE-----

导出 PKI 域中 CA 证书到 PEM 编码的文件，指定文件名称为 cacert。

```
<Sysname> system-view
```

```
[Sysname] pki export domain domain1 pem ca filename cacert
```

导出 PKI 域中 CA 证书（证书链）到终端。

```
<Sysname> system-view
```

```
[Sysname] pki export domain domain1 pem ca
```

-----BEGIN CERTIFICATE-----

```
MIIB7jCCAVcCEQCDsVShJFEMifVG8zRRoSsWMA0GCSqGSIb3DQEBBQUAMDCxCzAJ
BgNVBAYTAmNuMQwwCgYDVQQKEwNoM2MxDDAKBgNVBAStA2gzYzEMMAoGA1UEAxMD
YWNhMB4XDTEwMDEwNjAyNTc0NFoXDTEwMTAzMTMyMFowODEMAkGA1UEBhMC
Y24xDDAKBgNVBAoTA2gzYzEMMAoGA1UECjMDaDNjMQ0wCwYDVQQDEwRhYWNhMIGf
MA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQDcuJsWhAJXEDmowGb5z7VDVms54TKi
xnanJJCWvBORU64ftvpVB7xQekbkjgAS9FjDyXlLQ8IyIsYIp5ebJr8P+n9i9Pl7j
lBx5mi4XeIldyv20jfN5oSQ+gWY9/m1R8uv13RS05r3rxPg+7EvKBjmiy0Giddw
vu3Y3WrjBPP6GQIDAQABMA0GCSqGSIb3DQEBBQUAA4GBAJrQddzVQEiy4AcgtzUL
ltkmlmWoz87+jUsgFB+H+xeYiZE4sancf2UwH8kXWqZ5AuReFCCBC2fkvvQvUGnV
cso7JXAhfw8sUFok9eHz2R+GSoEk5BZFzZ8eCmNyGq9ln6mJs0lhAqMpsCW6G2zh
5mus7FTHhywXpJ22/fnHg6lm
```

-----END CERTIFICATE-----

-----BEGIN CERTIFICATE-----

```
MIIB8DCCAVKCEQD2PBUX/rvslNw9uTrZB3DlMA0GCSqGSIb3DQEBBQUAMDOxCzAJ
BgNVBAYTAmNuMQwwCgYDVQQKEwNoM2MxDDAKBgNVBAStA2gzYzEPMA0GA1UEAxMG
cm9mdcGNhMB4XDTEwMDEwNjAyNTY1OFoXDTEwNDZzMtMxMFowNzELMAkGA1UE
BhMCY24xDDAKBgNVBAoTA2gzYzEMMAoGA1UECjMDaDNjMQwwCgYDVQQDEwNhY2Ew
gZ8wDQYJKoZIhvcNAQEFBQADgY0AMIGJAoGBAOek1R7DpeEV72N1OLz+dydIDT0
zVZDdPxfLgQYWSfIBwWFKJEyQ/4y8VIfDI0EGTM4dsOX/QFwudhl/Czkio3dWLh
Q1y5XCJy68vQKR82WZ2mah5Nuekus3LSZZBoZKTAOY5MCCMFcULM858dtSq15Sh
xF7tKSeAT7ARlJxTAgMBAAEwDQYJKoZIhvcNAQEFBQADgYEADJQCo6m0RNup0ewa
ItX4XK/tYcJXAQWMA0IuwaWpr+ofqVVgYBPwVpYglhJDOuIZxKdR2pfQOA4f35wM
Vz6kAuJLATsEA1GW9ACUWa5PHwVgJk9BDEXhKSJ2e7odmrg/iROhJjc1NMV3pvIs
CuFiCLxRQcMGhCNH1On4wuydssc=
```

-----END CERTIFICATE-----

-----BEGIN CERTIFICATE-----

```
MIIB8jCCAVsCEfxy3MSlQ835MrnBkI/dUPYwDQYJKoZIhvcNAQEFBQAwojELMAK
GA1UEBhMCY24xDDAKBgNVBAoTA2gzYzEMMAoGA1UECjMDaDNjMQ8wDQYDVQQDEwZy
b290Y2EwHhcNMTEwMTAzMTQxMjMxMjMxMjMxMjMxMjMxMjMxMjMxMjMxMjMxMjMx
EwJjbjEMMAoGA1UEChMDaDNjMQwwCgYDVQQLEwNoM2MxMjMxMjMxMjMxMjMxMjMx
YTCBnzANBgkqhkiG9w0BAQEFAAOBjQAwGyKCGYEAxP2XLF230zq6MhwZvAomOxa
7tc1r4bESXZu3UBKno3Ay9kQm2HrDOAiZvZXfLu7Gx22ga2Qdz01IeZ+EQrYHTyO
pBcejDjal/ZtvgnjXyHfOG8nS+P7n83BkRj/Fu7Yz4zjTKMbCF2EfheYXxr4NSXA
fhC9qg9S23vNXStmWvcsAwEAATANBgkqhkiG9w0BAQUFAAOBQBtsU7X77sdZ1Nn
0I981h0qA5g7SEEIpi+pwZjJrH0FVHw01e4JWhHjyHqrOyfyXyqe7vH4SXp5MHEqf
```

```
14nKIEbexbPONspebtznxv4/xTjdlaM2rfQ95jJ/SN8H8KIyiYZyIs3t5Q+V35x1
cef+NMWgZBzwXOSP0wC9+pC2ZNiIpg==
-----END CERTIFICATE-----
```

导出 PKI 域中的本地证书及其对应的私钥到 PKCS12 编码的文件，指定保护私钥信息的加密口令为 123，文件名称为 **cert-lo.der**。

```
<Sysname> system-view
[Sysname] pki export domain domain1 p12 local passphrase 123 filename cert-lo.der
# 导出 PKI 域中的所有证书到 PKCS12 编码的文件，指定文件名称为 cert-all.p7b。
<Sysname> system-view
[Sysname] pki export domain domain1 p12 all passphrase 123 filename cert-all.p7b
```

【相关命令】

- **pki domain**

1.1.30 pki import

pki import 命令用来将 CA 证书、本地证书或对端证书导入到指定的 PKI 域中保存。

【命令】

```
pki import domain domain-name { der { ca | local | peer } filename filename
| p12 local filename filename | pem { ca | local | peer } [ filename filename ] }
```

【视图】

系统视图

【缺省用户角色】

network-admin

【参数】

domain *domain-name*: 保存证书的 PKI 域的名称，为 1~31 个字符的字符串，不区分大小写，不能包括“~”、“*”、“\”、“|”、“:”、“.”、“<”、“>”、“”和“'”。

der: 指定证书文件格式为 DER 编码（包括 PKCS#7 格式的证书）。

p12: 指定证书文件格式为 PKCS#12 编码。

pem: 指定证书文件格式为 PEM 编码。

ca: 表示 CA 证书。

local: 表示本地证书。

peer: 表示对端证书。

filename *filename*: 要导入的证书所在的文件名，不区分大小写。如果不指定本参数，则表示要通过直接在终端上粘贴证书内容的方式导入证书，这种方式仅 PEM 编码格式的证书才支持。

【使用指导】

如果设备所处的环境中，没有证书的发布点，或者 CA 服务器不支持通过 SCEP 协议与设备交互，则可通过此命令将证书导入到设备。另外，当证书对应的密钥对由 CA 服务器生成时，CA 服务器会将证书和对应的密钥对打包成一个文件，使用这样的证书前也需要通过此命令将其导入到设备。只有 PKCS#12 格式或 PEM 格式的证书文件中可能包含密钥对。

证书导入之前：

- 需要通过 **FTP**、**TFTP** 等协议将证书文件传送到设备的存储介质中。如果设备所处的环境不允许使用 **FTP**、**TFTP** 等协议，则可以直接在终端上粘贴证书的内容，但是粘贴的证书必须是 **PEM** 格式的，因为只有 **PEM** 编码的证书内容为可打印字符。
- 必须存在签发本地证书（或对端证书）的 **CA** 证书链才能成功导入本地证书（或对端证书），这里的 **CA** 证书链可以是保存在设备上的 **PKI** 域中的，也可以是本地证书（或对端证书）中携带的。因此，若设备和本地证书（或对端证书）中都没有 **CA** 证书链，则需要首先执行导入 **CA** 证书的命令。

导入本地证书或对端证书时：

- 如果用户要导入的本地证书（或对端证书）中含有 **CA** 证书链，则可以通过导入本地证书（或对端证书）的命令一次性将 **CA** 证书和本地证书（或对端证书）均导入到设备。导入的过程中，如果发现签发此本地证书（或对端证书）的 **CA** 证书已经存在于设备上的任一 **PKI** 域中，则系统会提示用户是否将其进行覆盖。
- 如果要导入的本地证书（或对端证书）中不含有 **CA** 证书链，但签发此本地证书（或对端证书）的 **CA** 证书已经存在于设备上的任一 **PKI** 域中，则可以直接导入本地证书（或对端证书）。

导入 **CA** 证书时：

- 若要导入的 **CA** 证书为根 **CA** 或者包含了完整的证书链（即含有根证书），则可以导入到设备。
- 若要导入的 **CA** 证书没有包含完整的证书链（即不含有根证书），但能够与设备上已有的 **CA** 证书拼接成完整的证书链，则也可以导入到设备；如果不能与设备上已有的 **CA** 证书拼接成完成的证书链，则不能导入到设备。

一些情况下，在证书导入的过程中，需要用户确认或输入相关信息：

- 若要导入的证书文件中包含了根证书，且设备上目前还没有任何 **PKI** 域中有此根证书，且要导入的 **PKI** 域中没有配置 **root-certificate fingerprint**，则在导入过程中还需要确认该根证书的指纹信息是否与用户的预期一致。用户需要通过联系 **CA** 服务器管理员来获取预期的根证书指纹信息。
- 当导入含有密钥对的本地证书时，需要输入口令。用户需要联系 **CA** 服务器管理员取得口令的内容。

导入含有密钥对的本地证书时，系统首先会根据查找到的 **PKI** 域中已有的密钥对配置来保存该密钥对。若 **PKI** 域中已保存了对应的密钥对，则设备会提示用户选择是否覆盖已有的密钥对。若 **PKI** 域中没有任何密钥对的配置，则根据密钥对的算法及证书的密钥用途，生成相应的密钥对配置。密钥对的具体保存规则如下：

- 如果本地证书携带的密钥对的用途为通用，则依次查找指定 **PKI** 域中通用用途、签名用途、加密用途的密钥对配置，并以找到配置中的密钥对名称保存该密钥对；若以上用途的密钥对配置均不存在，则提示用户输入密钥对名称（缺省的密钥对名称为 **PKI** 域的名称），并生成相应的密钥对配置。
- 如果本地证书携带的密钥对的用途为签名，则依次查找指定 **PKI** 域中通用用途、签名用途的密钥对配置，并以找到配置中的密钥对名称保存该密钥对；若以上两种用途的密钥对配置均不存在，则提示用户输入密钥对名称（缺省的密钥对名称为 **PKI** 域的名称），并生成相应的密钥对配置。
- 如果本地证书携带的密钥对的用途为加密，则查找指定 **PKI** 域中加密用途的密钥对配置，并以该配置中的密钥对名称保存密钥对；若加密用途密钥对的配置不存在，则提示用户输入密钥对名称（缺省的密钥对名称为 **PKI** 域的名称），并生成相应的密钥对配置。

由于以上过程中系统会自动更新或生成密钥对配置，因此建议用户在进行此类导入操作后，保存配置文件。

【举例】

向 PKI 域 aaa 中导入 CA 证书，证书文件格式为 PEM 编码，证书文件名称为 rootca_pem.cer，证书文件中包含根证书。

```
<Sysname> system-view
[Sysname] pki import domain aaa pem ca filename rootca_pem.cer
The trusted CA's finger print is:
    MD5  fingerprint:FFFF 3EFF FFFF 37FF FFFF 137B FFFF 7535
    SHA1 fingerprint:FFFF FF7F FF2B FFFF 7618 FF4C FFFF 0A7D FFFF FF69
Is the finger print correct?(Y/N):y
[Sysname]
```

向 PKI 域 bbb 中导入 CA 证书，证书文件格式为 PEM 编码，证书文件名称为 aca_pem.cer，证书文件中不包含根证书。

```
<Sysname> system-view
[Sysname] pki import domain bbb pem ca filename aca_pem.cer
[Sysname]
```

向 PKI 域 bbb 中导入本地证书，证书文件格式为 PKCS#12 编码，证书文件名称为 local-ca.p12，证书文件中包含了密钥对。

```
<Sysname> system-view
[Sysname] pki import domain bbb p12 local filename local-ca.p12
Please input challenge password:
*****
[Sysname]
```

向 PKI 域 bbb 中通过粘贴证书内容的方式导入 PEM 编码的本地证书。证书中含有密钥对和 CA 证书链。

```
<Sysname> system-view
[Sysname] pki import domain bbb pem local
Enter PEM-formatted certificate.
End with a Ctrl+c on a line by itself.
Bag Attributes
localKeyID: 01 00 00 00
friendlyName: {F7619D96-3AC2-40D4-B6F3-4EAB73DEED73}
Microsoft CSP Name: Microsoft Enhanced Cryptographic Provider v1.0
Key Attributes
X509v3 Key Usage: 10
-----BEGIN RSA PRIVATE KEY-----
Proc-Type: 4, ENCRYPTED
DEK-Info: DES-EDE3-CBC, 8DCE37F0A61A4B8C

k9C3KHY5S3EtnF5iQymvHYrVFy5ZdjSasU5y4XFubjdcvmpFHQteMjD0GKX6+xO
kuKbvpyCnWsPVg56sL/PDRyrRmqLmtUV3bpyQsFXgnc7p+Snj3CG2Ciw9XApYbW
Ec1TDCD75yuQckpVQdhguTvoPQXf9zHmiGu5jLkySp2k7ec/Mc97Ef+qqpfnHpQp
GDmMqnFpp59ZzB21OGlbGz1PcsjoT+EGpZg6B1KrPiCyFim95L9dWVwX9sk+U1s2
+8wqac8jETwWM0UZ1NGJ50JJz1QYIzMbcrw+S5WlPxACTIz1cldlB1b1kpc+7mcX
4W+MxFzsL88IJ99T72eu4iUNsy26g0BZMAcc1sJA3A4w9RNhfs9hSG43S3hAh51i
```

```
JPp720LfYBlkQHn/MgMCZASWDJ5G0eSXQt9QymHath4BiT9v7zetnQqf4q8plfd/
Xqd9zEF1BPpoJFtJqXwxHUCKgw6kJeC4CxHvi9ZCJU/upg9IpigufPoaDOPIa+Pm
GbRqSyy55c1Vde5G0ccGN1DZ94DW7AypazgLPBbrkIYAdjFPRmq+zMOdyqsGMTNj
jnheI5l784pNOAKuGi0i/uXmRRcfoMh6qAnK6YZGS7rOLC9CfPmy8fgY+/Sl9d9x
Q00ru0lpsxzh9c2YfuaiXFIx0auKl6o5+ZZYn7Rg/xy2Y0awVP+d0925GoAcHO40
cCl6jA/HsGAU9HkpwKHL35lmBDRLEzQeBFcaGwSmlJvRfE4tkJM7+Uz2QHJOFP10
0VLqMgxMlpk3TvBWgzHGJDe7TdZFCDPMPPhod8pi4P8gGXmQd01PhyQ==
```

```
-----END RSA PRIVATE KEY-----
```

Bag Attributes

localKeyID: 01 00 00 00

subject=/CN=sldsslserver

issuer=/C=cn/O=ccc/OU=sec/CN=ssl

```
-----BEGIN CERTIFICATE-----
```

```
MIICjzCCAfIgAwIBAgIRAJODN+shVrofVHbk1lSlqfcwDQYJKoZIhvcNAQEFBQAw
NzELMAkGA1UEBhMCY24xDDAKBgNVBAoTA2gzYzEMMAoGA1UECzMdc2VjMQwwCgYD
VQQDEwNzc2wwHhcNMTAxMDEyMzA2WhcNMTIwNzI2MDYzMDU0WjAXMRUwEwYD
VQQDEwxxzGRzc2xzZXJ2ZXIwZDQYJKoZIhvcNAQEBBQADgY0AMIGJAoGBAMLP
N3aTKV7NDndIOk0PpiikYPgxVih/geMXR3iYaANbcvRX07/FMDINWHJnBAZhCDvp
rFO552loGiPyl0wmFMK12TSL7sHvrxr0OdrFrqtWlbW+DsNGNcFSKZy3RvIngC2k
ZZqBeFPuytP185JUhbOrVaUDlisZi6NNshcIjd2BAGMBAAGjgbowgbcwHwYDVR0j
BBgwFoAUomoPeynZYoPLQdRlLlKhZjg8kBEwDgYDVR0PAQH/BAQDAGP4MBEGCWCG
SAGG+EIBAQQEAWIGQDASBgNVHREECzAJggdoM2MuY29tMB0GA1UdDgQWBQB8dpWb
3cJ/X5iDt8eg+JkeS9cvJjA+BgNVHR8ENzAlMD0gMaAvhilodHRwOi8vczAzMTMw
LmgzYy5odWF3ZWktM2NvbS5jb206NDQ3L3NzbC5jcmwwDQYJKoZIhvcNAQEFBQAD
gYEAAYS15x0kW474lu4twnZey5dPjMSwtwfm/UK01S8GQjGV5tl9ZNiTHFGNEFx7k
zxBp/JPpcFM8hapAfrVHDQ/wstq0pVDdBkrVF6XKIBks6XgCvRl32gcaQt9yrQd9
5RbWdetuBljudjFj25airYO2u7pLeVmdWWx3WVvZBZo8KU=
```

```
-----END CERTIFICATE-----
```

Bag Attributes: <Empty Attributes>

subject=/C=cn/O=ccc/OU=sec/CN=ssl

issuer=/C=cn/O=ccc/OU=sec/CN=ssl

```
-----BEGIN CERTIFICATE-----
```

```
MIIB7DCCAUVCEG+jJTPxxiE67pl2ff0SnOMwDQYJKoZIhvcNAQEFBQAwNzELMAkG
A1UEBhMCY24xDDAKBgNVBAoTA2gzYzEMMAoGA1UECzMdc2VjMQwwCgYDVQQDEwNzc
2wwHhcNMDkwnZMxMDY0ODQ2WhcNMTIwNzI2MDYyODU4WjA3MQswCQYDVQQGEwJj
bjEMMAoGA1UEChMDaDnJmQwwCgYDVQQLEwNzc2VWxwDQYJKoZIhvcNAQEBBQAD
BgkqhkiG9w0BAQEFAAOBjQAwGykCgYEA8QSMetQ70GONiFh7iJkvGQ8nC15zCF1
cqC/RcJhE/88LkKyQcu9j+Tz8Bk9Qj2UPaZdrk8fOrgtBsa7lZ+UO3j3l30q84l+
HjWq8yxVLRQahU3gqJze6pGR2l0s76u6GRyCX/zizGrHKqYlNnxK44NyRZx2klQ2
tKQAFpXCPikCAWEAATANBgkqhkiG9w0BAQUFAAOBgQBWsaMgRbBMTYNrrYCMjY6g
c7PBjvajVOKNUMxaDalePmXfKCx19l+PKM7+i8I/zLcoQ0+sHbva26a2/C4sNvoJ
2QZs6GtAOahP6CDqXC5VuNBu6eTKNKjL+mf6uuDeMxrlDNha0iymdrXXVIp5cuIu
fl7xgArs8Ks6aXDXM1o4DQ==
```

```
-----END CERTIFICATE-----
```

Please input the password:*****

Local certificate already exist, confirm to overwrite it? [Y/N]:y

The PKI domain already has a CA certificate. If it is overwritten, local certificates, peer certificates and CRL of this domain will also be deleted.

Overwrite it? [Y/N]:y

The system is going to save the key pair. You must specify a key pair name, which is a case-insensitive string of 1 to 64 characters. Valid characters include a to z, A to Z, 0 to 9, and hyphens (-).

Please enter the key pair name [default name: bbb]:

The key pair already exists.

Please enter the key pair name:

import-key

【相关命令】

- `display pki certificate`
- `public-key dsa`
- `public-key ecdsa`
- `public-key rsa`

1.1.31 pki request-certificate

`pki request-certificate` 命令用来手工申请本地证书或生成 PKCS#10 证书申请。

【命令】

```
pki request-certificate domain domain-name [ password password ] [ pkcs10  
[ filename filename ] ]
```

【视图】

系统视图

【缺省用户角色】

network-admin

【参数】

domain *domain-name*: 指定证书申请所属的 PKI 域名，为 1~31 个字符的字符串，不区分大小写，不能包括 “~”、“*”、“\”、“|”、“:”、“.”、“<”、“>”、“” 和 “'”。

password *password*: 在证书撤销时需要提供的口令，为 1~31 个字符的字符串，区分大小写。该口令包含在提交给 CA 的证书申请中，在吊销该证书时，需要提供该口令。

pkcs10: 在终端上显示出 BASE64 格式的 PKCS#10 证书申请信息，该信息可用于带外方式（如电话、磁盘、电子邮件等）的证书请求。

filename *filename*: 将 PKCS#10 格式的证书申请信息保存到本地的文件中。其中，*filename* 表示保存证书申请信息的文件名，不区分大小写。

【使用指导】

当 SCEP 协议不能正常通信时，可以通过执行指定参数 **pkcs10** 的本命令打印出本地的证书申请信息（BASE64 格式），或者通过执行指定 **pkcs10 filename filename** 参数的本命令将证书申请信息直接保存到本地的指定文件中，然后通过带外方式将这些本地证书申请信息发送给 CA 进行证书申请。指定的文件名中可以带完整路径，当系统中不存在用户所指定路径时，则会保存失败。

此命令不会被保存在配置文件中。

【举例】

在终端上显示 PKCS#10 格式的证书申请信息。

```
<Sysname> system-view
[Sysname] pki request-certificate domain aaa pkcs10

*** Request for general certificate ***
-----BEGIN NEW CERTIFICATE REQUEST-----
MIIBTDCBtgIBADANMQswCQYDVQQDEwJqajCBnzANBgkqhkiG9w0BAQEFAAOBjQAw
gYkCgYEAw5Drj8ofs9THA4ezkDcQPBy8pvHlkumampPsJmx8sGG52NftbrDTnTT5
ALx3LJijB3d/ndKpcHT/DfbJVDCn5gdw32tBZyCkEwMHZN3ol2z7Nmdu5TED6iN8
4m+hfp1QWoV6lty3o9pxAXuQl8peUDcfN6WV3LBXYy1lWCtkLkECAwEAAaAAMA0G
CSqGSIB3DQEBBAUAA4GBAA8E7BaIdmT6NVCZgv/I/ltqZH3TS4e4H9Qo5NiCKiEw
R8owVmAOXvtGMbyqBNcDTG0f5NbHrXZQT5+MbFJOnm5K/mnlro5TJKMTKV46PlCZ
JUjsugaY02GBY0BVcylpC9iIXLuXNIqjh1MBIqVsallQOHS7YMvnop6hXAQlkM4c
-----END NEW CERTIFICATE REQUEST-----

# 手工申请本地证书。

[Sysname] pki request-certificate domain openca
Start to request general certificate ...

.....

Certificate requested successfully.
```

【相关命令】

- **display pki certificate**

1.1.32 pki retrieve-certificate

pki retrieve-certificate 命令用来从证书发布服务器上在线获取证书并下载至本地。

【命令】

```
pki retrieve-certificate domain domain-name { ca | local | peer entity-name }
```

【视图】

系统视图

【缺省用户角色】

network-admin

【参数】

domain *domain-name*: 指定证书所在的 PKI 域的名称，为 1~31 个字符的字符串，不区分大小写，不能包括“~”、“*”、“\”、“|”、“.”、“.”、“<”、“>”、“”和“'”。

ca: 表示获取 CA 证书。

local: 表示获取本地证书。

peer *entity-name*: 表示获取对端的证书。其中 *entity-name* 为对端的实体名，为 1~31 个字符的字符串，不区分大小写。

【使用指导】

获取 CA 证书是通过 SCEP 协议进行的。获取 CA 证书时，如果本地已有 CA 证书存在，则该操作将不被允许。这种情况下，若要重新获取 CA 证书，请先使用 **pki delete-certificate** 命令删除已有的 CA 证书与对应的本地证书后，再执行此命令。

获取本地证书和对端证书是通过 LDAP 协议进行的。获取本地证书或对端证书时，如果本地已有本地证书或对端证书，则该操作是被允许进行的。最终，属于一个 PKI 实体的同一种公钥算法的本地证书只能存在一个，后者直接覆盖已有的，但对于 RSA 算法的证书而言，可以存在一个签名用途的证书和一个加密用途的证书。

所有获取到的 CA 证书、本地证书或对端证书只有通过验证之后才会被保存到本地证书库中。

此命令不会被保存在配置文件中。

【举例】

从证书发布服务器上获取 CA 证书。（需要用户确认 CA 根证书的指纹）

```
<Sysname> system-view
[Sysname] pki retrieve-certificate domain aaa ca
The trusted CA's finger print is:
    MD5  fingerprint:5C41 E657 A0D6 ECB4 6BD6 1823 7473 AABC
    SHA1 fingerprint:1616 E7A5 D89A 2A99 9419 1C12 D696 8228 87BC C266
Is the finger print correct?(Y/N):y
Retrieved the certificates successfully.
```

从证书发布服务器上获取本地证书。

```
<Sysname> system-view
[Sysname] pki retrieve-certificate domain aaa local
Retrieved the certificates successfully.
```

从证书发布服务器上获取对端证书。

```
<Sysname> system-view
[Sysname] pki retrieve-certificate domain aaa peer en1
Retrieved the certificates successfully.
```

【相关命令】

- **display pki certificate**
- **pki delete-certificate**

1.1.33 pki retrieve-crl

pki retrieve-crl 命令用来获取 CRL 并下载至本地。

【命令】

pki retrieve-crl domain *domain-name*

【视图】

系统视图

【缺省用户角色】

network-admin

【参数】

domain-name: 指定 CRL 所属的 PKI 域的名称, 为 1~31 个字符的字符串, 不区分大小写, 不能包括 “~”、“*”、“\”、“|”、“:”、“.”、“<”、“>”、“” 和 “'”。

【使用指导】

获取 CRL 的目的是为了验证 PKI 域中的本地证书和对端证书的合法性。若要成功获取 CRL, PKI 域中必须存在 CA 证书。

设备支持通过 HTTP、LDAP 或 SCEP 协议从 CRL 发布点上获取 CRL, 具体采用那种协议, 由 PKI 域中 CRL 发布点的配置决定:

- 若配置的 CRL 发布点 URL 格式为 HTTP 格式, 则通过 HTTP 协议获取 CRL。
- 若配置的 CRL 发布点 URL 格式为 LDAP 格式, 则通过 LDAP 协议获取 CRL。若配置的 CRL 发布点 URL(通过命令 **cr1 url**)中缺少主机名, 例如 `ldap:///CN=8088,OU=test,U=rd,C=cn`, 则还需要在 PKI 域中配置 LDAP 服务器的 URL(通过命令 **ldap server**)。此时, 设备会将配置的 LDAP 服务器 URL 和配置的 CRL 发布点 URL 中的不完整的 LDAP 发布点拼装成完整的 LDAP 发布点, 再通过 LDAP 协议获取 CRL。
- 若 PKI 域中没有配置 CRL 发布点, 则设备会依次从本地证书、CA 证书中查找 CRL 的发布点, 如果从中查找到了 CRL 发布点, 则通过该发布点获取 CRL; 否则, 通过 SCEP 协议获取 CRL。

【举例】

从 CRL 发布点上获取 CRL。

```
<Sysname> system-view
[Sysname] pki retrieve-crl domain aaa
Retrieve CRL of the domain aaa successfully.
```

【相关命令】

- **cr1 url**
- **ldap server**

1.1.34 pki storage

pki storage 命令用来配置证书和 CRL 的存储路径。

undo pki storage 命令用来恢复缺省情况。

【命令】

```
pki storage { certificates | crls } dir-path
undo pki storage { certificates | crls }
```

【缺省情况】

证书和 CRL 的存储路径为设备存储介质上的 PKI 目录。

【视图】

系统视图

【缺省用户角色】

network-admin

【参数】

certificates: 指定证书的存储目录。

crls: 指定 CRL 的存储目录。

dir-path: 存储目录的路径名称，区分大小写，不能以 ‘/’ 开头，不能包含 “./”。*dir-path* 可以是绝对路径也可以是相对路径，但必须已经存在。

【使用指导】

dir-path 只能是当前主用设备上的路径，不能是其它从设备上的路径。

设备缺省的 PKI 目录在设备首次成功申请、获取或导入证书时自动创建。

如果需要指定的目录还不存在，需要先使用 **mkdir** 命令创建这个目录，再使用此命令配置存储路径。

若修改了证书或 CRL 的存储目录，则原存储路径下的证书文件（以 .cer 和 .p12 为后缀的文件）和 CRL 文件（以 .crl 为后缀的文件）将被移动到该路径下保存，且原存储路径下的其它文件不受影响。

【举例】

设置证书的存储路径为 flash:/pki-new。

```
<Sysname> system-view
```

```
[Sysname] pki storage certificates flash:/pki-new
```

设置 CRL 存储路径为 pki-new。

```
<Sysname> system-view
```

```
[Sysname] pki storage crls pki-new
```

1.1.35 pki validate-certificate

pki validate-certificate 命令用来验证证书的有效性。

【命令】

```
pki validate-certificate domain domain-name { ca | local }
```

【视图】

系统视图

【缺省用户角色】

network-admin

【参数】

domain *domain-name*: 指定证书所在的 PKI 域的名称，为 1~31 个字符的字符串，不区分大小写，不能包括 “~”、“*”、“\”、“|”、“:”、“.”、“<”、“>”、“” 和 “'”。

ca: 表示验证 CA 证书。

local: 表示验证本地证书。

【使用指导】

证书验证的内容包括：证书是否由用户信任的 CA 签发；证书是否仍在有效期内；如果使能了 CRL 检查功能，还会验证证书是否被吊销。如果验证证书的时候，PKI 域中没有 CRL，则会先从本地证书库中查找是否存在 CRL，如果找到 CRL，则把证书库中保存的 CRL 加载到该 PKI 域中，否则，就从 CA 服务器上获取并保存到本地。

导入证书、申请证书、获取证书以及应用程序使用 **PKI** 功能时，都会自动对证书进行验证，因此一般不需要使用此命令进行额外的验证。如果用户希望在没有任何前述操作的情况下单独执行证书的验证，可以使用此命令。

验证 **CA** 证书时，会对从当前 **CA** 到根 **CA** 的整条 **CA** 证书链进行 **CRL** 检查。

【举例】

验证 **PKI** 域 **aaa** 中的 **CA** 证书的有效性。

```
<Sysname> system-view
[Sysname] pki validate-certificate domain aaa ca
Verifying certificate.....
    Serial Number:
        f6:3c:15:31:fe:bb:ec:94:dc:3d:b9:3a:d9:07:70:e5
    Issuer:
        C=cn
        O=ccc
        OU=ppp
        CN=rootca
    Subject:
        C=cn
        O=abc
        OU=test
        CN=aca
```

```
Verify result: OK
Verifying certificate.....
    Serial Number:
        5c:72:dc:c4:a5:43:cd:f9:32:b9:c1:90:8f:dd:50:f6
    Issuer:
        C=cn
        O=ccc
        OU=ppp
        CN=rootca
    Subject:
        C=cn
        O=ccc
        OU=ppp
        CN=rootca
```

Verify result: OK

验证 **PKI** 域 **aaa** 中的本地证书的有效性。

```
<Sysname> system-view
[Sysname] pki validate-certificate domain aaa local
Verifying certificate.....
    Serial Number:
        bc:05:70:1f:0e:da:0d:10:16:1e
    Issuer:
        C=CN
        O=sec
```

```
OU=software
CN=bca
Subject:
O=OpenCA Labs
OU=Users
CN=fips fips-sec
```

Verify result: OK

【相关命令】

- **cr1 check**
- **pki domain**

1.1.36 public-key dsa

public-key dsa 命令用来指定证书申请使用的 DSA 密钥对。

undo public-key 命令用来恢复缺省情况。

【命令】

```
public-key dsa name key-name [ length key-length ]
undo public-key
```

【缺省情况】

未指定证书申请使用的密钥对。

【视图】

PKI 域视图

【缺省用户角色】

network-admin

【参数】

name *key-name*: 密钥对的名称，为 1~64 个字符的字符串，不区分大小写，只能包含字母、数字和连字符“-”。

length *key-length*: 密钥的长度。非 FIPS 模式下，*key-length* 的取值范围为 512~2048，单位为比特，缺省值为 1024；FIPS 模式下，*key-length* 的取值为 2048，单位为比特，缺省值为 2048。密钥越长，密钥安全性越高，但相关的公钥运算越耗时。

【使用指导】

本命令中引用的密钥对并不要求已经存在，可以通过以下任意一种途径获得：

- 通过执行 **public-key local create** 命令生成。
- 通过应用程序认证过程触发生成。例如 IKE 协商过程中，如果使用数字签名认证方式，则可能会触发生成密钥对。
- 通过导入证书（使用 **pki import** 命令）的方式从外界获得。

一个 PKI 域中只能同时存在一种算法（RSA、DSA 或 ECDSA）的密钥对。在同一个 PKI 域中多次执行 **public-key dsa** 命令，最后一次执行的命令生效。

本命令中指定的密钥长度仅对将要由设备生成的密钥对有效。如果执行本命令时，设备上已经存在指定名称的密钥对，则后续通过此命令指定的该密钥对的密钥长度没有意义。如果指定名称的密钥对是通过导入证书的方式获得，则通过本命令指定的密钥长度也没有意义。

【举例】

指定证书申请所使用的 DSA 密钥对为 abc，密钥的长度为 2048 比特。

```
<Sysname> system-view
[Sysname] pki domain aaa
[Sysname-pki-domain-aaa] public-key dsa name abc length 2048
```

【相关命令】

- **pki import**
- **public-key local create**（安全命令参考/公钥管理）

1.1.37 public-key ecdsa

public-key ecdsa 命令用来指定证书申请使用的 ECDSA 密钥对。

undo public-key 命令用来恢复缺省情况。

【命令】

非 FIPS 模式下：

```
public-key ecdsa name key-name [ secp192r1 | secp256r1 | secp384r1 | secp521r1 ]
undo public-key
```

FIPS 模式下：

```
public-key ecdsa name key-name [ secp256r1 | secp384r1 | secp521r1 ]
undo public-key
```

【缺省情况】

未指定证书申请使用的密钥对。

【视图】

PKI 域视图

【缺省用户角色】

network-admin

【参数】

name *key-name*：密钥对的名称，为 1~64 个字符的字符串，不区分大小写，只能包含字母、数字和连字符“-”。

secp192r1：密钥对使用的椭圆曲线算法的名称为 secp192r1，密钥长度为 192 比特。

secp256r1：密钥对使用的椭圆曲线算法的名称为 secp256r1，密钥长度为 256 比特。

secp384r1：密钥对使用的椭圆曲线算法的名称为 secp384r1，密钥长度为 384 比特。

secp521r1：密钥对使用的椭圆曲线算法的名称为 secp521r1，密钥长度为 521 比特。

【使用指导】

本命令中引用的密钥对并不要求已经存在，可以通过以下任意一种途径获得：

- 通过执行 **public-key local create** 命令生成。
- 通过应用程序认证过程触发生成。例如 IKE 协商过程中，如果使用数字签名认证方式，则可能会触发生成密钥对。
- 通过导入证书（使用 **pki import** 命令）的方式从外界获得。

若未指定任何参数，则在非 FIPS 模式下缺省使用密钥对 **secp192r1**；在 FIPS 模式下缺省使用密钥对 **secp256r1**。

一个 PKI 域中只能同时存在一种算法（RSA、DSA 或 ECDSA）的密钥对。在同一个 PKI 域中多次执行 **public-key ecdsa** 命令，最后一次执行的命令生效。

本命令中指定的密钥长度仅对将要由设备生成的密钥对有效。如果执行本命令时，设备上已经存在指定名称的密钥对，则后续通过此命令指定的该密钥对的密钥长度没有意义。如果指定名称的密钥对是通过导入证书的方式获得，则通过本命令指定的密钥长度也没有意义。

【举例】

指定证书申请所使用的 ECDSA 密钥对为 abc，椭圆曲线算法的名称为 secp384r1。

```
<Sysname> system-view
[Sysname] pki domain aaa
[Sysname-pki-domain-aaa] public-key ecdsa name abc secp384r1
```

【相关命令】

- **pki import**
- **public-key local create**（安全命令参考/公钥管理）

1.1.38 public-key rsa

public-key rsa 命令用来指定证书申请使用的 RSA 密钥对。

undo public-key 命令用来恢复缺省情况。

【命令】

```
public-key rsa { { encryption name encryption-key-name [ length key-length ]
| signature name signature-key-name [ length key-length ] } * | general name
key-name [ length key-length ] }
undo public-key
```

【缺省情况】

未指定证书申请使用的密钥对。

【视图】

PKI 域视图

【缺省用户角色】

network-admin

【参数】

encryption：指定密钥对的用途为加密。

name encryption-key-name: 加密密钥对的名称，为 1~64 个字符的字符串，不区分大小写，只能包含字母、数字和连字符“-”。

signature: 指定密钥对的用途为签名。

name signature-key-name: 签名密钥对的名称，为 1~64 个字符的字符串，不区分大小写，只能包含字母、数字和连字符“-”。

general: 指定密钥对的用途为通用，既可以用于签名也可以用于加密。

name key-name: 通用密钥对的名称，为 1~64 个字符的字符串，不区分大小写，只能包含字母、数字和连字符“-”。

length key-length: 密钥的长度。非 FIPS 模式下，*key-length* 的取值范围为 512~2048，单位为比特，缺省为 1024；FIPS 模式下，*key-length* 的取值为 2048，单位为比特，缺省为 2048。密钥越长，密钥安全性越高，但相关的公钥运算越耗时。

【使用指导】

本命令中引用的密钥对并不要求已经存在，可以通过以下任意一种途径获得：

- 通过执行 **public-key local create** 命令生成。
- 通过应用程序认证过程触发生成。例如 IKE 协商过程中，如果使用数字签名认证方式，则可能会触发生成密钥对。
- 通过导入证书（使用 **pki import** 命令）的方式从外界获得。

一个 PKI 域中只能同时存在一种算法（RSA、DSA 或 ECDSA）的密钥对。对于 RSA 密钥对来说，一个 PKI 域中只允许单独存在一种用途的 RSA 密钥对，或同时存在一个用于签名的和一个用于加密的 RSA 密钥对。因此，在一个 PKI 域中，RSA 签名密钥对和 RSA 加密密钥对的配置不会互相覆盖。

分别指定 RSA 签名密钥对和 RSA 加密密钥对时，它们的密钥长度可以不相同。

本命令中指定的密钥长度仅对将要由设备生成的密钥对有效。如果执行本命令时，设备上已经存在指定名称的密钥对，则后续通过此命令指定的该密钥对的密钥长度没有意义。如果指定名称的密钥对是通过导入证书的方式获得，则通过本命令指定的密钥长度也没有意义。

【举例】

指定证书申请所使用的 RSA 密钥对为 abc，密钥用途为通用，密钥的长度为 2048 比特。

```
<Sysname> system-view
[Sysname] pki domain aaa
[Sysname-pki-domain-aaa] public-key rsa general name abc length 2048
```

指定证书申请所使用的加密 RSA 密钥对为 rsa1（密钥的长度为 2048 比特），签名 RSA 密钥对为 sig1（密钥的长度为 2048 比特）。

```
<Sysname> system-view
[Sysname] pki domain aaa
[Sysname-pki-domain-aaa] public-key rsa encryption name rsa1 length 2048
[Sysname-pki-domain-aaa] public-key rsa signature name sig1 length 2048
```

【相关命令】

- **pki import**
- **public-key local create**（安全命令参考/公钥管理）

1.1.39 root-certificate fingerprint

root-certificate fingerprint 命令用来配置验证 CA 根证书时所使用的指纹。

undo root-certificate fingerprint 命令用来恢复缺省情况。

【命令】

非 FIPS 模式下：

```
root-certificate fingerprint { md5 | sha1 } string
undo root-certificate fingerprint
```

FIPS 模式下：

```
root-certificate fingerprint sha1 string
undo root-certificate fingerprint
```

【缺省情况】

未指定验证 CA 根证书时使用的指纹。

【视图】

PKI 域视图

【缺省用户角色】

network-admin

【参数】

md5：使用 MD5 指纹。

sha1：使用 SHA1 指纹。

string：指定所使用的指纹信息。当选择 MD5 指纹时，*string* 必须为 32 个字符的字符串，并且以 16 进制的形式输入；当选择 SHA1 指纹时，*string* 必须为 40 个字符的字符串，并且以 16 进制的形式输入。

【使用指导】

当本地证书申请模式为自动方式且 PKI 域中没有 CA 证书时，必须通过本命令配置验证 CA 证书时所使用的指纹。当 IKE 协商等应用触发设备进行本地证书申请时，设备会自动从 CA 服务器上获取 CA 证书，如果获取的 CA 证书中包含了本地不存在的 CA 根证书，则设备会验证该 CA 根证书的指纹。此时，如果设备上没有配置 CA 根证书指纹或者配置了错误的 CA 根证书指纹，则本地证书申请失败。

通过 **pki import** 命令导入 CA 证书或者通过 **pki retrieve-certificate** 命令获取 CA 证书时，可以选择是否配置验证 CA 根证书使用的指纹：如果 PKI 域中配置了验证 CA 根证书使用的指纹，则当导入的 CA 证书文件或者获取的 CA 证书中包含本地不存在的 CA 根证书时，直接使用配置的 CA 根证书指纹进行验证。如果配置了错误的 CA 根证书指纹，则 CA 证书导入和 CA 证书获取均会失败；否则，需要用户来确认该 CA 证书的 CA 根证书指纹是否可信。

【举例】

配置验证 CA 根证书时使用的 MD5 指纹。（仅非 FIPS 模式下支持）

```
<Sysname> system-view
[Sysname] pki domain aaa
[Sysname-pki-domain-aaa] root-certificate fingerprint md5 12EF53FA355CD23E12EF53FA355CD23E
```

配置验证 CA 根证书时使用的 SHA1 指纹。

```
<Sysname> system-view
[Sysname] pki domain aaa
[Sysname-pki-domain-aaa] root-certificate fingerprint sha1
D1526110AAD7527FB093ED7FC037B0B3CDDAD93
```

【相关命令】

- **certificate request mode**
- **pki import**
- **pki retrieve-certificate**

1.1.40 rule

rule 命令用来配置证书属性的访问控制规则。

undo rule 命令用来删除指定的证书属性访问控制规则。

【命令】

```
rule [ id ] { deny | permit } group-name
undo rule id
```

【缺省情况】

不存在证书属性的访问控制规则。

【视图】

证书访问控制策略视图

【缺省用户角色】

network-admin

【参数】

id: 证书属性访问控制规则编号，取值范围为 1~16，缺省值为当前还未被使用的且合法的最小编号，取值越小优先级越高。

deny: 当证书的属性与所关联的属性组匹配时，认为该证书无效，未通过访问控制策略的检测。

permit: 当证书的属性与所关联的属性组匹配时，认为该证书有效，通过了访问控制策略的检测。

group-name: 规则所关联的证书属性组名称，为 1~31 个字符的字符串，不区分大小写。

【使用指导】

配置证书属性访问控制规则时，可以关联一个当前并不存在的证书属性组，后续可以通过命令 **pki certificate attribute-group** 完成相应的配置。

若规则所关联的证书属性组中没有定义任何属性规则（通过命令 **attribute** 配置），或关联的证书属性组不存在，则认为被检测的证书属性与该属性组匹配。

如果一个访问控制策略中有多个规则，则按照规则编号从小到大的顺序遍历所有规则，一旦证书与某一个规则匹配，则立即结束检测，不再继续匹配其它规则；若遍历完所有规则后，证书没有与任何规则匹配，则认为该证书不能通过访问控制策略的检测。

【举例】

配置一个访问控制规则，要求当证书与证书属性组 **mygroup** 匹配时，认为该证书有效，通过了访问控制策略的检测。

```
<Sysname> system-view
[Sysname] pki certificate access-control-policy mypolicy
[Sysname-pki-cert-acp-mypolicy] rule 1 permit mygroup
```

【相关命令】

- **attribute**
- **display pki certificate access-control-policy**
- **pki certificate attribute-group**

1.1.41 source

source 命令用来指定 PKI 操作产生的协议报文使用的源 IP 地址。

undo source 命令用来恢复缺省情况。

【命令】

```
source { ip | ipv6 } { ip-address | interface interface-type
interface-number }
undo source
```

【缺省情况】

PKI 操作产生的协议报文的源 IP 地址为系统根据路由表项查找到的出接口的地址。

【视图】

PKI 域视图

【缺省用户角色】

network-admin

【参数】

ip *ip-address*: 指定源 IPv4 地址。

ipv6 *ip-address*: 指定源 IPv6 地址。

interface *interface-type interface-number*: 指定该接口的主 IPv4 地址或接口上最小的 IPv6 地址为源 IP 地址。*interface-type interface-number* 表示接口类型和接口编号。

【使用指导】

如果希望 PKI 操作产生的协议报文的源 IP 地址是一个特定的地址，则需要配置此命令，例如 CA 服务器上的策略要求仅接受来自指定地址或网段的证书申请。如果该 IP 地址是动态获取的，则可以指定一个接口，使用该接口上的 IP 地址作为源地址。

此处指定的源 IP 地址，必须与 CA 服务器之间路由可达。

一个 PKI 域中只能存在一个源 IP 地址，后配置的生效。

【举例】

指定 PKI 操作产生的协议报文的源 IP 地址为 111.1.1.8。

```

<Sysname> system-view
[Sysname] pki domain aaa
[Sysname-pki-domain-aaa] source ip 111.1.1.8
# 指定 PKI 操作产生的协议报文的源 IPv6 地址为 1::8。

<Sysname> system-view
[Sysname] pki domain 1
[Sysname-pki-domain-1] source ipv6 1::8
# 指定 PKI 操作产生的协议报文的源 IP 地址为接口 Vlan-interface1 的 IP 地址。

<Sysname> system-view
[Sysname] pki domain aaa
[Sysname-pki-domain-aaa] source ip interface vlan-interface 1
# 指定 PKI 操作产生的协议报文的源 IPv6 地址为接口 Vlan-interface1 的 IPv6 地址。

<Sysname> system-view
[Sysname] pki domain 1
[Sysname-pki-domain-1] source ipv6 interface vlan-interface 1

```

1.1.42 state

state 命令用来配置 PKI 实体所属的州或省的名称。

undo state 命令用来恢复缺省情况。

【命令】

```

state state-name
undo state

```

【缺省情况】

未配置 PKI 实体所属的州或省的名称。

【视图】

PKI 实体视图

【缺省用户角色】

network-admin

【参数】

state-name: PKI 实体所属的州或省的名称，为 1~63 个字符的字符串，区分大小写，不能包含逗号。

【举例】

配置 PKI 实体 en 所在省为 countryA。

```

<Sysname> system-view
[Sysname] pki entity en
[Sysname-pki-entity-en] state countryA

```

1.1.43 usage

usage 命令用来指定证书的扩展用途。

undo usage 命令用来删除指定证书的扩展用途。

【命令】

```
usage { ike | ssl-client | ssl-server } *  
undo usage [ ike | ssl-client | ssl-server ] *
```

【缺省情况】

未指定证书的扩展用途，表示可用于 IKE、SSL 客户端和 SSL 服务器端用途。

【视图】

PKI 域视图

【缺省用户角色】

network-admin

【参数】

ike: 指定证书扩展用途为 IKE，即 IKE 对等体使用的证书。

ssl-client: 指定证书扩展用途为 SSL 客户端，即 SSL 客户端使用的证书。

ssl-server: 指定证书扩展用途为 SSL 服务器端，即 SSL 服务器端使用的证书。

【使用指导】

若不指定任何参数，则 **undo usage** 命令表示删除所有指定的证书扩展用途，证书的用途由证书的使用者决定，PKI 不做任何限定。

证书中携带的扩展用途与 CA 服务器的策略相关，申请到的证书中的扩展用途可能与此处指定的不完全一致，最终请以 CA 服务器的实际情况为准。

【举例】

指定证书扩展用途为 IKE。

```
<Sysname> system-view  
[Sysname] pki domain aaa  
[Sysname-pki-domain-aaa] usage ike
```

目 录

1 IPsec	1-1
1.1 IPsec配置命令	1-1
1.1.1 ah authentication-algorithm	1-1
1.1.2 description	1-2
1.1.3 display ipsec { ipv6-policy policy }	1-3
1.1.4 display ipsec { ipv6-policy-template policy-template }	1-8
1.1.5 display ipsec profile	1-10
1.1.6 display ipsec sa	1-11
1.1.7 display ipsec statistics	1-16
1.1.8 display ipsec transform-set	1-18
1.1.9 display ipsec tunnel	1-19
1.1.10 encapsulation-mode	1-22
1.1.11 esn enable	1-23
1.1.12 esp authentication-algorithm	1-24
1.1.13 esp encryption-algorithm	1-25
1.1.14 ike-profile	1-26
1.1.15 ikev2-profile	1-27
1.1.16 ipsec { ipv6-policy policy }	1-28
1.1.17 ipsec { ipv6-policy policy } isakmp template	1-29
1.1.18 ipsec { ipv6-policy policy } local-address	1-30
1.1.19 ipsec { ipv6-policy-template policy-template }	1-31
1.1.20 ipsec anti-replay check	1-32
1.1.21 ipsec anti-replay window	1-33
1.1.22 ipsec apply	1-34
1.1.23 ipsec decrypt-check enable	1-35
1.1.24 ipsec df-bit	1-35
1.1.25 ipsec fragmentation	1-36
1.1.26 ipsec global-df-bit	1-37
1.1.27 ipsec limit max-tunnel	1-38
1.1.28 ipsec logging packet enable	1-38
1.1.29 ipsec profile	1-39
1.1.30 ipsec redundancy enable	1-40
1.1.31 ipsec sa global-duration	1-41

1.1.32 ipsec sa idle-time	1-42
1.1.33 ipsec transform-set.....	1-42
1.1.34 local-address	1-43
1.1.35 pfs	1-44
1.1.36 protocol	1-45
1.1.37 qos pre-classify	1-46
1.1.38 redundancy replay-interval	1-46
1.1.39 remote-address	1-47
1.1.40 reset ipsec sa.....	1-48
1.1.41 reset ipsec statistics	1-50
1.1.42 reverse-route dynamic	1-50
1.1.43 reverse-route preference	1-52
1.1.44 reverse-route tag	1-52
1.1.45 sa duration	1-53
1.1.46 sa hex-key authentication	1-54
1.1.47 sa hex-key encryption	1-55
1.1.48 sa idle-time.....	1-57
1.1.49 sa spi	1-58
1.1.50 sa string-key	1-59
1.1.51 security acl	1-60
1.1.52 snmp-agent trap enable ipsec.....	1-62
1.1.53 tfc enable	1-63
1.1.54 transform-set.....	1-64

2 IKE 2-1

2.1 IKE配置命令.....	2-1
2.1.1 authentication-algorithm	2-1
2.1.2 authentication-method	2-2
2.1.3 certificate domain	2-3
2.1.4 description	2-4
2.1.5 dh	2-4
2.1.6 display ike proposal.....	2-5
2.1.7 display ike sa.....	2-7
2.1.8 display ike statistics.....	2-10
2.1.9 dpd.....	2-12
2.1.10 encryption-algorithm	2-13
2.1.11 exchange-mode.....	2-15

2.1.12 ike dpd	2-15
2.1.13 ike identity	2-16
2.1.14 ike invalid-spi-recovery enable	2-18
2.1.15 ike keepalive interval	2-19
2.1.16 ike keepalive timeout	2-19
2.1.17 ike keychain.....	2-20
2.1.18 ike limit	2-21
2.1.19 ike nat-keepalive.....	2-22
2.1.20 ike profile	2-22
2.1.21 ike proposal.....	2-23
2.1.22 ike signature-identity from-certificate	2-24
2.1.23 keychain	2-25
2.1.24 local-identity.....	2-25
2.1.25 match local address (IKE keychain view).....	2-27
2.1.26 match local address (IKE profile view)	2-28
2.1.27 match remote.....	2-29
2.1.28 pre-shared-key	2-30
2.1.29 priority (IKE keychain view)	2-32
2.1.30 priority (IKE profile view).....	2-32
2.1.31 proposal.....	2-33
2.1.32 reset ike sa.....	2-34
2.1.33 reset ike statistics.....	2-34
2.1.34 sa duration	2-35
2.1.35 snmp-agent trap enable ike	2-36

3 IKEv2..... 3-1

3.1 IKEv2 配置命令	3-1
3.1.1 address	3-1
3.1.2 authentication-method	3-2
3.1.3 certificate domain	3-3
3.1.4 config-exchange.....	3-4
3.1.5 dh	3-5
3.1.6 display ikev2 policy	3-6
3.1.7 display ikev2 profile.....	3-7
3.1.8 display ikev2 proposal	3-9
3.1.9 display ikev2 sa.....	3-10
3.1.10 display ikev2 statistics.....	3-14

3.1.11 dpd	3-16
3.1.12 encryption	3-17
3.1.13 hostname	3-18
3.1.14 identity	3-19
3.1.15 identity local	3-20
3.1.16 ikev2 cookie-challenge	3-21
3.1.17 ikev2 dpd	3-21
3.1.18 ikev2 keychain	3-23
3.1.19 ikev2 nat-keepalive	3-23
3.1.20 ikev2 policy	3-24
3.1.21 ikev2 profile	3-25
3.1.22 ikev2 proposal	3-26
3.1.23 integrity	3-27
3.1.24 keychain	3-28
3.1.25 match local (IKEv2 profile view)	3-29
3.1.26 match local address (IKEv2 policy view)	3-30
3.1.27 match remote	3-30
3.1.28 nat-keepalive	3-32
3.1.29 peer	3-33
3.1.30 pre-shared-key	3-34
3.1.31 prf	3-35
3.1.32 priority (IKEv2 policy view)	3-36
3.1.33 priority (IKEv2 profile view)	3-37
3.1.34 proposal	3-37
3.1.35 reset ikev2 sa	3-38
3.1.36 reset ikev2 statistics	3-39
3.1.37 sa duration	3-40

1 IPsec



说明

设备运行于 FIPS 模式时，本特性部分配置相对于非 FIPS 模式有所变化，具体差异请见本文相关描述。有关 FIPS 模式的详细介绍请参见“安全配置指导”中的“FIPS”。

1.1 IPsec配置命令

1.1.1 ah authentication-algorithm

ah authentication-algorithm 命令用来配置 AH 协议采用的认证算法。

undo ah authentication-algorithm 命令用来恢复缺省情况。

【命令】

非 FIPS 模式下：

```
ah authentication-algorithm { aes-xcbc-mac | md5 | sha1 | sha256 | sha384 | sha512 } *
```

```
undo ah authentication-algorithm
```

FIPS 模式下：

```
ah authentication-algorithm { sha1 | sha256 | sha384 | sha512 } *
```

```
undo ah authentication-algorithm
```

【缺省情况】

AH 协议未采用任何认证算法。

【视图】

IPsec 安全提议视图

【缺省用户角色】

network-admin

【参数】

aes-xcbc-mac：采用 HMAC-AES-XCBC-96 认证算法，密钥长度 128 比特。本参数仅适用于 IKEv2 协商。

md5：采用 HMAC-MD5 认证算法，密钥长度 128 比特。

sha1：采用 HMAC-SHA1 认证算法，密钥长度 160 比特。

sha256：采用 HMAC-SHA-256 认证算法，密钥长度 256 比特。

sha384：采用 HMAC-SHA-384 认证算法，密钥长度 384 比特。

sha512：采用 HMAC-SHA-512 认证算法，密钥长度 512 比特。

【使用指导】

非 FIPS 模式下，每个 IPsec 安全提议中均可以配置多个 AH 认证算法，其优先级为配置顺序。

对于手工方式以及 IKEv1（第 1 版本的 IKE 协议）协商方式的 IPsec 安全策略，IPsec 安全提议中配置顺序首位的 AH 认证算法生效。为保证成功建立 IPsec 隧道，隧道两端指定的 IPsec 安全提议中配置的首个 AH 认证算法需要一致。

【举例】

配置 IPsec 安全提议采用的 AH 认证算法为 HMAC-SHA1 算法，密钥长度为 160 比特。

```
<Sysname> system-view
[Sysname] ipsec transform-set tran1
[Sysname-ipsec-transform-set-tran1] ah authentication-algorithm sha1
```

1.1.2 description

description 命令用来配置 IPsec 安全策略/IPsec 安全策略模板/IPsec 安全框架的描述信息。

undo description 命令用来恢复缺省情况。

【命令】

```
description text
undo description
```

【缺省情况】

无描述信息。

【视图】

IPsec 安全策略视图
IPsec 安全策略模板视图
IPsec 安全框架视图

【缺省用户角色】

network-admin

【参数】

text: IPsec 安全策略/IPsec 安全策略模板/IPsec 安全框架的描述信息，为 1~80 个字符的字符串，区分大小写。

【使用指导】

当系统中存在多个 IPsec 安全策略/IPsec 安全策略模板/IPsec 安全框架时，可通过配置相应的描述信息来有效区分不同的安全策略。

【举例】

配置序号为 1 的 IPsec 安全策略 policy1 的描述信息为 CenterToA。

```
<Sysname> system-view
[Sysname] ipsec policy policy1 1 isakmp
[Sysname-ipsec-policy-isakmp-policy1-1] description CenterToA
```

1.1.3 display ipsec { ipv6-policy | policy }

display ipsec { ipv6-policy | policy } 命令用来显示 IPsec 安全策略的信息。

【命令】

display ipsec { ipv6-policy | policy } [policy-name [seq-number]]

【视图】

任意视图

【缺省用户角色】

network-admin
network-operator

【参数】

ipv6-policy: 显示 IPv6 IPsec 安全策略的信息。

policy: 显示 IPv4 IPsec 安全策略的信息。

policy-name: IPsec 安全策略的名称，为 1~63 个字符的字符串，不区分大小写。

seq-number: IPsec 安全策略表项的序号，取值范围为 1~65535。

【使用指导】

如果不指定任何参数，则显示所有 IPsec 安全策略的信息。

如果指定了 *policy-name* 和 *seq-number*，则显示指定的 IPsec 安全策略表项的信息；如果指定了 *policy-name* 而没有指定 *seq-number*，则显示所有名称相同的 IPsec 安全策略表项的信息。

【举例】

显示所有 IPv4 IPsec 安全策略的信息。

```
<Sysname> display ipsec policy
-----
IPsec Policy: mypolicy
-----

-----
Sequence number: 1
Mode: Manual
-----

The policy configuration is incomplete:
    ACL not specified
    Incomplete transform-set configuration
Description: This is my first IPv4 manual policy
Security data flow:
Remote address: 2.5.2.1
Transform set: transform

Inbound AH setting:
    AH SPI: 1200 (0x000004b0)
    AH string-key: *****
    AH authentication hex key:
```

Inbound ESP setting:
ESP SPI: 1400 (0x00000578)
ESP string-key:
ESP encryption hex key:
ESP authentication hex key:

Outbound AH setting:
AH SPI: 1300 (0x00000514)
AH string-key: *****
AH authentication hex key:

Outbound ESP setting:
ESP SPI: 1500 (0x000005dc)
ESP string-key: *****
ESP encryption hex key:
ESP authentication hex key:

Sequence number: 2
Mode: ISAKMP

The policy configuration is incomplete:
Remote-address not set
ACL not specified
Transform-set not set
Description: This is my first IPv4 Isakmp policy
Traffic Flow Confidentiality: Enabled
Security data flow:
Selector mode: standard
Local address:
Remote address:
Transform set:
IKE profile:
IKEv2 profile:
SA duration(time based): 3600 seconds
SA duration(traffic based): 1843200 kilobytes
SA idle time:

IPsec Policy: mycompletepolicy
Interface: LoopBack2

Sequence number: 1
Mode: Manual

Description: This is my complete policy

```

Security data flow: 3100
Remote address: 2.2.2.2
Transform set: completetetransform

Inbound AH setting:
  AH SPI: 5000 (0x00001388)
  AH string-key: *****
  AH authentication hex key:

Inbound ESP setting:
  ESP SPI: 7000 (0x00001b58)
  ESP string-key: *****
  ESP encryption hex key:
  ESP authentication hex key:

Outbound AH setting:
  AH SPI: 6000 (0x00001770)
  AH string-key: *****
  AH authentication hex key:

Outbound ESP setting:
  ESP SPI: 8000 (0x00001f40)
  ESP string-key: *****
  ESP encryption hex key:
  ESP authentication hex key:

-----
Sequence number: 2
Mode: ISAKMP
-----
Description: This is my complete policy
Traffic Flow Confidentiality: Enabled
Security data flow: 3200
Selector mode: standard
Local address:
Remote address: 5.3.6.9
Transform set: completetetransform
IKE profile:
IKEv2 profile:
SA duration(time based): 3600 seconds
SA duration(traffic based): 1843200 kilobytes
SA idle time:
# 显示所有 IPv6 IPsec 安全策略的详细信息。
<Sysname> display ipsec ipv6-policy
-----
IPsec Policy: mypolicy
-----

```

```

-----
Sequence number: 1
Mode: Manual
-----

Description: This is my first IPv6 policy
Security data flow: 3600
Remote address: 1000::2
Transform set: mytransform

Inbound AH setting:
  AH SPI: 1235 (0x000004d3)
  AH string-key: *****
  AH authentication hex key:

Inbound ESP setting:
  ESP SPI: 1236 (0x000004d4)
  ESP string-key: *****
  ESP encryption hex key:
  ESP authentication hex key:

Outbound AH setting:
  AH SPI: 1237 (0x000004d5)
  AH string-key: *****
  AH authentication hex key:

Outbound ESP setting:
  ESP SPI: 1238 (0x000004d6)
  ESP string-key: *****
  ESP encryption hex key:
  ESP authentication hex key:

```

表1-1 display ipsec { ipv6-policy | policy } 命令显示信息描述表

字段	描述
IPsec Policy	IPsec安全策略的名称
Interface	应用了IPsec安全策略的接口名称
Sequence number	IPsec安全策略表项的顺序号
Mode	IPsec安全策略采用的协商方式 <ul style="list-style-type: none"> • Mannul: 手工方式 • ISAKMP: IKE 协商方式 • Template: 策略模板方式

字段	描述
The policy configuration is incomplete	<p>IPsec安全策略配置不完整，可能的原因包括：</p> <ul style="list-style-type: none"> • ACL 未配置 • IPsec 安全提议未配置 • ACL 中没有 permit 规则 • IPsec 安全提议配置不完整 • IPsec 隧道对端 IP 地址未指定 • IPsec SA 的 SPI 和密钥与 IPsec 安全策略的 SPI 和密钥不匹配
Description	IPsec安全策略的描述信息
Traffic Flow Confidentiality	TFC（Traffic Flow Confidentiality）填充功能的开启状态
Security data flow	IPsec安全策略引用的ACL
Selector mode	<p>IPsec安全策略的数据流保护方式</p> <ul style="list-style-type: none"> • standard: 标准方式 • aggregation: 聚合方式 • per-host: 主机方式
Local address	IPsec隧道的本端IP地址（仅IKE协商方式的IPsec安全策略下存在）
Remote address	IPsec隧道的对端IP地址或主机名
Transform set	IPsec安全策略引用的IPsec安全提议的名称
IKE profile	IPsec安全策略引用的IKE Profile的名称
IKEv2 profile	IPsec安全策略引用的IKEv2 Profile的名称
SA duration(time based)	基于时间的IPsec SA生命周期，单位为秒
SA duration(traffic based)	基于流量的IPsec SA生命周期，单位为千字节
SA idle time	IPsec SA的空闲超时时间，单位为秒
Inbound AH setting	入方向采用的AH协议的相关设置
Outbound AH setting	出方向采用的AH协议的相关设置
AH SPI	AH协议的SPI
AH string-key	AH协议的字符类型的密钥，若配置，则显示为*****，否则显示为空
AH authentication hex key	AH协议的十六进制密钥，若配置，则显示为*****，否则显示为空
Inbound ESP setting	入方向采用的ESP协议的相关设置
Outbound ESP setting	出方向采用的ESP协议的相关设置
ESP SPI	ESP协议的SPI
ESP string-key	ESP协议的字符类型的密钥，若配置，则显示为*****，否则显示为空
ESP encryption hex key	ESP协议的十六进制加密密钥，若配置，则显示为*****，否则显示为空

字段	描述
ESP authentication hex key	ESP协议的十六进制认证密钥，若配置，则显示为*****，否则显示为空

【相关命令】

- `ipsec { ipv6-policy | policy }`

1.1.4 `display ipsec { ipv6-policy-template | policy-template }`

`display ipsec { ipv6-policy-template | policy-template }` 命令用来显示 IPsec 安全策略模板的信息。

【命令】

```
display ipsec { ipv6-policy-template | policy-template } [ template-name
[ seq-number ] ]
```

【视图】

任意视图

【缺省用户角色】

network-admin
network-operator

【参数】

ipv6-policy-template: 显示 IPv6 IPsec 安全策略模板的信息。

policy-template: 显示 IPv4 IPsec 安全策略模板的信息。

template-name: 指定 IPsec 安全策略模板的名称，为 1~63 个字符的字符串，不区分大小写。

seq-number: 指定 IPsec 安全策略模板表项的序号，取值范围为 1~65535。

【使用指导】

如果不指定任何参数，则显示所有 IPsec 安全策略模板的信息。

如果指定了 *template-name* 和 *seq-number*，则显示指定的 IPsec 安全策略模板表项的信息；
如果指定了 *template-name* 而没有指定 *seq-number*，则显示所有名称相同的 IPsec 安全策略模板表项的信息。

【举例】

显示所有 IPv4 IPsec 安全策略模板的信息。

```
<Sysname> display ipsec policy-template
```

```
-----
IPsec Policy Template: template
-----
```

```
-----
Sequence number: 1
-----
```

```
Description: This is policy template
```

```
Traffic Flow Confidentiality: Disabled
Security data flow :
Selector mode: standard
Local address:
IKE profile:
IKEv2 profile:
Remote address: 162.105.10.2
Transform set: testprop
IPsec SA local duration(time based): 3600 seconds
IPsec SA local duration(traffic based): 1843200 kilobytes
SA idle time:
```

显示所有 IPv6 IPsec 安全策略模板的信息。

```
<Sysname> display ipsec ipv6-policy-template
```

```
-----
IPsec Policy Template: template6
-----
```

```
-----
Sequence number: 1
-----
Description: This is policy template
Traffic Flow Confidentiality: Disabled
Security data flow :
Selector mode: standard
Local address:
IKE profile:
IKEv2 profile:
Remote address: 200::1
Transform set: testprop
IPsec SA local duration(time based): 3600 seconds
IPsec SA local duration(traffic based): 1843200 kilobytes
SA idle time:
```

表1-2 display ipsec { ipv6-policy-template | policy-template } 命令显示信息描述表

字段	描述
IPsec Policy Template	IPsec安全策略模板名称
Sequence number	IPsec安全策略模板表项的序号
Description	IPsec安全策略模板的描述信息
Traffic Flow Confidentiality	TFC（Traffic Flow Confidentiality）填充功能的开启状态
Security data flow	IPsec安全策略模板引用的ACL
Selector mode	IPsec安全策略模板的数据流保护方式 <ul style="list-style-type: none">standard: 标准方式aggregation: 聚合方式per-host: 主机方式

字段	描述
Local address	IPsec隧道的本端IP地址
IKE profile	IPsec安全策略模板引用的IKE Profile名称
IKEv2 profile	IPsec安全策略引用的IKEv2 Profile的名称
Remote address	IPsec隧道的对端IP地址
Transform set	IPsec安全策略模板引用的安全提议的名称
IPsec SA local duration(time based)	基于时间的IPsec SA生命周期，单位为秒
IPsec SA local duration(traffic based)	基于流量的IPsec SA生命周期，单位为千字节
SA idle time	IPsec SA的空闲超时时间，单位为秒

【相关命令】

- `ipsec { ipv6-policy | policy } isakmp template`

1.1.5 display ipsec profile

`display ipsec profile` 命令用来显示 IPsec 安全框架的信息。

【命令】

`display ipsec profile [profile-name]`

【视图】

任意视图

【缺省用户角色】

network-admin
network-operator

【参数】

profile-name: 指定 IPsec 安全框架的名称，为 1～63 个字符的字符串，不区分大小写。

【使用指导】

如果没有指定任何参数，则显示所有 IPsec 安全框架的配置信息。

【举例】

显示所有 IPsec 安全框架的配置信息。

```
<Sysname> display ipsec profile
```

```
-----
IPsec profile: profile
Mode: manual
```

```
-----
Transform set: prop1
```

```
Inbound AH setting:
AH SPI: 12345 (0x00003039)
```

```

AH string-key:
AH authentication hex key: *****
Inbound ESP setting:
ESP SPI: 23456 (0x00005ba0)
ESP string-key:
ESP encryption hex-key: *****
ESP authentication hex-key: *****
Outbound AH setting:
AH SPI: 12345 (0x00003039)
AH string-key:
AH authentication hex key: *****
Outbound ESP setting:
ESP SPI: 23456 (0x00005ba0)
ESP string-key:
ESP encryption hex key: *****
ESP authentication hex key: *****

```

表1-3 display ipsec profile 命令显示信息描述表

字段	描述
IPsec profile	IPsec安全框架的名称
Mode	IPsec安全框架采用的协商方式
Description	IPsec安全框架的描述信息
Transform set	IPsec安全策略引用的IPsec安全提议的名称
Inbound AH setting	入方向采用的AH协议的相关设置
Outbound AH setting	出方向采用的AH协议的相关设置
AH SPI	AH协议的SPI
AH string-key	AH协议的字符类型的密钥
AH authentication hex key	AH协议的十六进制密钥
Inbound ESP setting	入方向采用的ESP协议的相关设置
Outbound ESP setting	出方向采用的ESP协议的相关设置
ESP SPI	ESP协议的SPI
ESP string-key	ESP协议的字符类型的密钥
ESP encryption hex key	ESP协议的十六进制加密密钥
ESP authentication hex key	ESP协议的十六进制认证密钥

【相关命令】

- **ipsec profile**

1.1.6 display ipsec sa

display ipsec sa 命令用来显示 IPsec SA 的相关信息。

【命令】

```
display ipsec sa [ brief | count | interface interface-type interface-number
| { ipv6-policy | policy } policy-name [ seq-number ] | profile profile-name
| remote [ ipv6 ] ip-address ]
```

【视图】

任意视图

【缺省用户角色】

network-admin
network-operator

【参数】

brief: 显示所有的 IPsec SA 的简要信息。

count: 显示 IPsec SA 的个数。

interface interface-type interface-number: 显示指定接口下的 IPsec SA 的详细信息。
interface-type interface-number 表示接口类型和接口编号。

ipv6-policy: 显示由指定 IPv6 IPsec 安全策略创建的 IPsec SA 的详细信息。

policy: 显示由指定 IPv4 IPsec 安全策略创建的 IPsec SA 的详细信息。

policy-name: IPsec 安全策略的名称，为 1~63 个字符的字符串，不区分大小写。

seq-number: IPsec 安全策略的顺序号，取值范围为 1~65535。

profile: 显示由指定 IPsec 安全框架创建的 IPsec SA 的详细信息。

profile-name: IPsec 安全框架的名称，为 1~63 个字符的字符串，不区分大小写。

remote ip-address: 显示指定对端 IP 地址的 IPsec SA 的详细信息。

ipv6: 显示指定 IPv6 对端地址的 IPsec SA 的详细信息。若不指定本参数，则表示显示指定 IPv4 对端地址的 IPsec SA 的详细信息。

【使用指导】

如果不指定任何参数，则显示所有 IPsec SA 的详细信息。

【举例】

显示 IPsec SA 的简要信息。

```
<Sysname> display ipsec sa brief
```

Interface/Global	Dst Address	SPI	Protocol	Status
Vlan100	10.1.1.1	400	ESP	Active
Vlan100	255.255.255.255	4294967295	ESP	Active
Vlan100	100::1/64	500	AH	Active
Global	--	600	ESP	Active

表1-4 display ipsec sa brief 命令显示信息描述表

字段	描述
Interface/Global	IPsec SA属于的接口或是全局（全局IPsec SA由IPsec安全框架生成）

字段	描述
Dst Address	IPsec隧道对端的IP地址 IPsec安全框架生成的SA中，该值无意义，显示为“--”
SPI	IPsec SA的SPI
Protocol	IPsec采用的安全协议
Status	IPsec SA的状态，取值只能为Active，表示SA处于可用状态

显示 IPsec SA 的个数。

```
<Sysname> display ipsec sa count
Total IPsec SAs count: 4
```

显示所有 IPsec SA 的详细信息。

```
<Sysname> display ipsec sa
-----

Interface: Vlan-interface100
-----

-----
IPsec policy: r2
Sequence number: 1
Mode: ISAKMP
-----

Tunnel id: 3
Encapsulation mode: tunnel
Perfect Forward Secrecy:
Inside VRF: vp1
Extended Sequence Numbers enable: Y
Traffic Flow Confidentiality enable: N
Path MTU: 1443
Tunnel:
    local  address: 2.2.2.2
    remote address: 1.1.1.2
Flow:
    sour addr: 192.168.2.0/255.255.255.0  port: 0  protocol: ip
    dest addr: 192.168.1.0/255.255.255.0  port: 0  protocol: ip

[Inbound ESP SAs]
SPI: 3564837569 (0xd47blac1)
Connection ID: 90194313219
Transform set: ESP-ENCRYPT-AES-CBC-128 ESP-AUTH-SHA1
SA duration (kilobytes/sec): 4294967295/604800
SA remaining duration (kilobytes/sec): 1843200/2686
Max received sequence-number: 5
Anti-replay check enable: Y
Anti-replay window size: 32
UDP encapsulation used for NAT traversal: N
```

```

Status: Active

[Outbound ESP SAs]
SPI: 801701189 (0x2fc8fd45)
Connection ID: 64424509441
Transform set: ESP-ENCRYPT-AES-CBC-128 ESP-AUTH-SHA1
SA duration (kilobytes/sec): 4294967295/604800
SA remaining duration (kilobytes/sec): 1843200/2686
Max sent sequence-number: 6
UDP encapsulation used for NAT traversal: N
Status: Active

-----

Global IPsec SA

-----

-----

IPsec profile: profile
Mode: Manual

-----

Encapsulation mode: transport
[Inbound AH SA]
SPI: 1234563 (0x0012d683)
Connection ID: 64426789452
Transform set: AH-SHA1
No duration limit for this SA
[Outbound AH SA]
SPI: 1234563 (0x002d683)
Connection ID: 64428999468
Transform set: AH-SHA1
No duration limit for this SA

```

表1-5 display ipsec sa 命令显示信息描述表

字段	描述
Interface	IPsec SA所在的接口
Global IPsec SA	全局IPsec SA
IPsec policy	采用的IPsec安全策略名
IPsec profile	采用的IPsec安全框架名
Sequence number	IPsec安全策略表项序号
Mode	IPsec安全策略采用的协商方式 <ul style="list-style-type: none"> • Manual: 手工方式 • ISAKMP: IKE 协商方式 • Template: IKE 模板方式
Tunnel id	IPsec隧道的ID号

字段	描述
Encapsulation mode	采用的报文封装模式，有两种：传输（transport）和隧道（tunnel）模式
Perfect Forward Secrecy	<p>此IPsec安全策略发起协商时使用完善的前向安全（PFS）特性，取值包括：</p> <ul style="list-style-type: none"> • 768-bit Diffie-Hellman 组（dh-group1） • 1024-bit Diffie-Hellman 组（dh-group2） • 1536-bit Diffie-Hellman 组（dh-group5） • 2048-bit Diffie-Hellman 组（dh-group14） • 2048-bit 和 256_bit 子群 Diffie-Hellman 组（dh-group24） • 256-bit ECP 模式 Diffie-Hellman 组（dh-group19） • 384-bit ECP 模式 Diffie-Hellman 组（dh-group20）
Extended Sequence Numbers enable	ESN（Extended Sequence Number，扩展序列号）功能是否开启
Traffic Flow Confidentiality enable	TFC（Traffic Flow Confidentiality）填充功能是否开启
Inside VRF	（暂不支持）被保护数据所属的VRF实例名称
Path MTU	IPsec SA的路径MTU值
Tunnel	IPsec隧道的端点地址信息
local address	IPsec隧道的本端IP地址
remote address	IPsec隧道的对端IP地址
Flow	受保护的数据流信息
sour addr	数据流的源IP地址
dest addr	数据流的目的IP地址
port	端口号
protocol	<p>协议类型，取值包括：</p> <ul style="list-style-type: none"> • ip: IPv4 协议 • ipv6: IPv6 协议
Inbound ESP SAs	入方向的ESP协议的IPsec SA信息
Outbound ESP SAs	出方向的ESP协议的IPsec SA信息
Inbound AH SAs	入方向的AH协议的IPsec SA信息
Outbound AH SAs	出方向的AH协议的IPsec SA信息
SPI	IPsec SA的SPI
Connection ID	IPsec SA标识
Transform set	IPsec安全提议所采用的安全协议及算法
SA duration (kilobytes/sec)	IPsec SA生存时间，单位为千字节或者秒
SA remaining duration (kilobytes/sec)	剩余的IPsec SA生存时间，单位为千字节或者秒
Max received sequence-number	入方向接收到的报文最大序列号

字段	描述
Max sent sequence-number	出方向发送的报文最大序列号
Anti-replay check enable	抗重放检测功能是否开启
Anti-replay window size	抗重放窗口宽度
Status	IPsec SA的状态，取值仅为Active，表示SA处于可用状态
No duration limit for this SA	手工方式创建的IPsec SA无生命周期

【相关命令】

- `ipsec sa global-duration`
- `reset ipsec sa`

1.1.7 display ipsec statistics

`display ipsec statistics` 命令用来显示 IPsec 处理的报文的统计信息。

【命令】

`display ipsec statistics [tunnel-id tunnel-id]`

【视图】

任意视图

【缺省用户角色】

network-admin
network-operator

【参数】

tunnel-id tunnel-id: 显示指定 IPsec 隧道处理的报文统计信息。其中，*tunnel-id* 为隧道的 ID 号，取值范围为 0~4294967295。通过 `display ipsec tunnel brief` 可以查看到已建立的 IPsec 隧道的 ID 号。

【使用指导】

如果不指定任何参数，则显示 IPsec 处理的所有报文的统计信息。

【举例】

显示所有 IPsec 处理的报文统计信息。

```
<Sysname> display ipsec statistics
IPsec packet statistics:
  Received/sent packets: 47/64
  Received/sent bytes: 3948/5208
  Dropped packets (received/sent): 0/45

Dropped packets statistics
  No available SA: 0
  Wrong SA: 0
  Invalid length: 0
```

```

Authentication failure: 0
Encapsulation failure: 0
Decapsulation failure: 0
Replayed packets: 0
ACL check failure: 45
MTU check failure: 0
Loopback limit exceeded: 0
Crypto speed limit exceeded: 0

```

显示 ID 为 1 的 IPsec 隧道处理的报文统计信息。

```
<Sysname> display ipsec statistics tunnel-id 1
```

```

IPsec packet statistics:
Received/sent packets: 5124/8231
Received/sent bytes: 52348/64356
Dropped packets (received/sent): 0/0

```

```

Dropped packets statistics
No available SA: 0
Wrong SA: 0
Invalid length: 0
Authentication failure: 0
Encapsulation failure: 0
Decapsulation failure: 0
Replayed packets: 0
ACL check failure: 0
MTU check failure: 0
Loopback limit exceeded: 0
Crypto speed limit exceeded: 0

```

表1-6 display ipsec statistics 命令显示信息描述表

字段	描述
IPsec packet statistics	IPsec处理的报文统计信息
Received/sent packets	接收/发送的受安全保护的数据包的数目
Received/sent bytes	接收/发送的受安全保护的字节数目
Dropped packets (received/sent)	被设备丢弃了的受安全保护的数据包的数目（接收/发送）
Dropped packets statistics	被丢弃的数据包的详细信息
No available SA	因为找不到IPsec SA而被丢弃的数据包的数目
Wrong SA	因为IPsec SA错误而被丢弃的数据包的数目
Invalid length	因为数据包长度不正确而被丢弃的数据包的数目
Authentication failure	因为认证失败而被丢弃的数据包的数目
Encapsulation failure	因为加封装失败而被丢弃的数据包的数目
Decapsulation failure	因为解封装失败而被丢弃的数据包的数目
Replayed packets	被丢弃的重放的数据包的数目

字段	描述
ACL check failure	因为ACL检测失败而被丢弃的数据包的数目
MTU check failure	因为MTU检测失败而被丢弃的数据包的数目
Loopback limit exceeded	因为本机处理的次数超过限制而被丢弃的数据包的数目
Crypto speed limit exceeded	因为加密速度的限制而被丢弃的数据包的数目

【相关命令】

- `reset ipsec statistics`

1.1.8 display ipsec transform-set

`display ipsec transform-set` 命令用来显示 IPsec 安全提议的信息。

【命令】

`display ipsec transform-set [transform-set-name]`

【视图】

任意视图

【缺省用户角色】

network-admin
network-operator

【参数】

transform-set-name: 指定 IPsec 安全提议的名称, 为 1~63 个字符的字符串, 不区分大小写。

【使用指导】

如果没有指定 IPsec 安全提议的名称, 则显示所有 IPsec 安全提议的信息。

【举例】

显示所有 IPsec 安全提议的信息。

```
<Sysname> display ipsec transform-set
IPsec transform set: mytransform
  State: incomplete
  Encapsulation mode: tunnel
  ESN: Enabled
  PFS:
  Transform: ESP

IPsec transform set: completeTransform
  State: complete
  Encapsulation mode: transport
  ESN: Enabled
  PFS:
  Transform: AH-ESP
  AH protocol:
```

```

    Integrity: SHA1
ESP protocol:
    Integrity: SHA1
    Encryption: AES-CBC-128

```

表1-7 display ipsec transform-set 命令显示信息描述表

字段	描述
IPsec transform set	IPsec安全提议的名称
State	IPsec安全提议是否完整
Encapsulation mode	IPsec安全提议采用的封装模式，包括两种：传输（transport）和隧道（tunnel）模式
ESN	ESN（Extended Sequence Number，扩展序列号）功能的开启状态
PFS	<p>PFS（Perfect Forward Secrecy，完善的前向安全性）特性的配置，取值包括：</p> <ul style="list-style-type: none"> • 768-bit Diffie-Hellman 组（dh-group1） • 1024-bit Diffie-Hellman 组（dh-group2） • 1536-bit Diffie-Hellman 组（dh-group5） • 2048-bit Diffie-Hellman 组（dh-group14） • 2048-bit 和 256_bit 子群 Diffie-Hellman 组（dh-group24） • 256-bit ECP 模式 Diffie-Hellman 组（dh-group19） • 384-bit ECP 模式 Diffie-Hellman 组（dh-group20）
Transform	IPsec安全提议采用的安全协议，包括三种：AH协议、ESP协议、AH-ESP（先采用ESP协议，再采用AH协议）
AH protocol	AH协议相关配置
ESP protocol	ESP协议相关配置
Integrity	安全协议采用的认证算法
Encryption	安全协议采用的加密算法

【相关命令】

- **ipsec transform-set**

1.1.9 display ipsec tunnel

display ipsec tunnel 命令用来显示 IPsec 隧道的信息。

【命令】

```
display ipsec tunnel { brief | count | tunnel-id tunnel-id }
```

【视图】

任意视图

【缺省用户角色】

```

network-admin
network-operator

```

【参数】

brief: 显示 IPsec 隧道的简要信息。

count: 显示 IPsec 隧道的个数。

tunnel-id tunnel-id: 显示指定的 IPsec 隧道的详细信息。其中，*tunnel-id* 为隧道的 ID 号，取值范围为 0~4294967295。

【使用指导】

IPsec 通过在特定通信方之间（例如两个安全网关之间）建立“通道”，来保护通信方之间传输的用户数据，该通道通常称为 IPsec 隧道。

【举例】

显示所有 IPsec 隧道的简要信息。

```
<Sysname> display ipsec tunnel brief
```

Tunn-id	Src Address	Dst Address	Inbound SPI	Outbound SPI	Status
0	--	--	1000 3000	2000 4000	Active
1	1.2.3.1	2.2.2.2	5000 7000	6000 8000	Active

表1-8 display ipsec tunnel brief 命令显示信息描述表

字段	描述
Tunn-id	IPsec隧道的ID号
Src Address	IPsec隧道的源地址 在IPsec Profile生成的SA中，该值无意义，显示为“--”
Dst Address	IPsec隧道的目的地址 在IPsec Profile生成的SA中，该值无意义，显示为“--”
Inbound SPI	IPsec隧道中生效的入方向SPI 如果该隧道使用了两种安全协议，则会分为两行分别显示两个入方向的SPI
Outbound SPI	IPsec隧道中生效的出方向SPI 如果该隧道使用了两种安全协议，则会分为两行分别显示两个出方向的SPI
Status	IPsec SA的状态，取值仅为Active，表示SA处于可用状态

显示 IPsec 隧道的数目。

```
<Sysname> display ipsec tunnel count
```

```
Total IPsec Tunnel Count: 2
```

显示所有 IPsec 隧道的详细信息。

```
<Sysname> display ipsec tunnel
```

```
Tunnel ID: 0
```

```
Status: Active
```

```
Perfect forward secrecy:
```

```
Inside vpn-instance:
```

```
SA's SPI:
    outbound: 2000      (0x000007d0)  [AH]
    inbound:  1000      (0x000003e8)  [AH]
    outbound: 4000      (0x00000fa0)  [ESP]
    inbound:  3000      (0x00000bb8)  [ESP]
```

```
Tunnel:
    local  address:
    remote address:
```

```
Flow:
```

```
Tunnel ID: 1
Status: Active
Perfect forward secrecy:
Inside vpn-instance:
```

```
SA's SPI:
    outbound: 6000      (0x00001770)  [AH]
    inbound:  5000      (0x00001388)  [AH]
    outbound: 8000      (0x00001f40)  [ESP]
    inbound:  7000      (0x00001b58)  [ESP]
```

```
Tunnel:
    local  address: 1.2.3.1
    remote address: 2.2.2.2
```

```
Flow:
    as defined in ACL 3100
```

显示 ID 号为 1 的 IPsec 隧道的详细信息。

```
<Sysname> display ipsec tunnel tunnel-id 1
```

```
Tunnel ID: 1
Status: Active
Perfect forward secrecy:
Inside vpn-instance:
SA's SPI:
    outbound: 6000      (0x00001770)  [AH]
    inbound:  5000      (0x00001388)  [AH]
    outbound: 8000      (0x00001f40)  [ESP]
    inbound:  7000      (0x00001b58)  [ESP]
```

```
Tunnel:
    local  address: 1.2.3.1
    remote address: 2.2.2.2
```

```
Flow:
    as defined in ACL 3100
```

表1-9 display ipsec tunnel 命令显示信息描述表

字段	描述
Tunnel ID	IPsec隧道的ID，用来唯一地标识一个IPsec隧道
Status	IPsec隧道的状态，取值仅为Active，表示隧道处于可用状态

字段	描述
Perfect forward secrecy	<p>此IPsec安全策略发起协商时使用完善的前向安全（PFS）特性，取值包括：</p> <ul style="list-style-type: none"> • 768-bit Diffie-Hellman 组（dh-group1） • 1024-bit Diffie-Hellman 组（dh-group2） • 1536-bit Diffie-Hellman 组（dh-group5） • 2048-bit Diffie-Hellman 组（dh-group14） • 2048-bit 和 256_bit 子群 Diffie-Hellman 组（dh-group24） • 256-bit ECP 模式 Diffie-Hellman 组（dh-group19） • 384-bit ECP 模式 Diffie-Hellman 组（dh-group20）
Inside vpn-instance	（暂不支持）被保护数据所属的VPN实例名
SA's SPI	出方向和入方向的IPsec SA的SPI
Tunnel	IPsec隧道的端点地址信息
local address	IPsec隧道的本端IP地址
remote address	IPsec隧道的对端IP地址
Flow	IPsec隧道保护的数据流，包括源地址、目的地址、源端口、目的端口、协议
as defined in ACL 3001	手工方式建立的IPsec隧道所保护的数据流的范围，例如IPsec隧道保护ACL 3001中定义的所有数据流

1.1.10 encapsulation-mode

encapsulation-mode 命令用来配置安全协议对报文的封装模式。

undo encapsulation-mode 命令用来恢复缺省情况。

【命令】

```
encapsulation-mode { transport | tunnel }
undo encapsulation-mode
```

【缺省情况】

使用隧道模式对 IP 报文进行封装。

【视图】

IPsec 安全提议视图

【缺省用户角色】

network-admin

【参数】

transport：采用传输模式。

tunnel：采用隧道模式。

【使用指导】

传输模式下的安全协议主要用于保护上层协议报文，仅传输层数据被用来计算安全协议头，生成的安全协议头以及加密的用户数据（仅针对 ESP 封装）被放置在原 IP 头后面。若要求端到端的安全保障，即数据包进行安全传输的起点和终点为数据包的实际起点和终点时，才能使用传输模式。

隧道模式下的安全协议用于保护整个 IP 数据包，用户的整个 IP 数据包都被用来计算安全协议头，生成的安全协议头以及加密的用户数据（仅针对 ESP 封装）被封装在一个新的 IP 数据包中。这种模式下，封装后的 IP 数据包有内外两个 IP 头，其中的内部 IP 头为原有的 IP 头，外部 IP 头由提供安全服务的设备添加。在安全保护由设备提供的情况下，数据包进行安全传输的起点或终点不为数据包的实际起点和终点时（例如安全网关后的主机），则必须使用隧道模式。隧道模式用于保护两个安全网关之间的数据传输。

在 IPsec 隧道的两端，IPsec 安全提议所采用的封装模式要一致。

【举例】

指定 IPsec 安全提议 tran1 采用传输模式对 IP 报文进行封装。

```
<Sysname> system-view
[Sysname] ipsec transform-set tran1
[Sysname-ipsec-transform-set-tran1] encapsulation-mode transport
```

【相关命令】

- **ipsec transform-set**

1.1.11 esn enable

esn enable 命令用来开启 ESN（Extended Sequence Number，扩展序列号）功能。

undo esn enable 命令用来关闭 ESN 功能。

【命令】

```
esn enable [ both ]
undo esn enable
```

【缺省情况】

ESN 功能处于关闭状态。

【视图】

IPsec 安全提议视图

【缺省用户角色】

network-admin

【参数】

both: 既支持扩展序列号，又支持非扩展序列号。若不指定该参数，则表示仅支持扩展序列号。

【使用指导】

ESN 功能用于扩展防重放序列号的范围，可将抗重放序列号长度由传统的 32 比特扩大到 64 比特。在有大量数据流需要使用 IPsec SA 保护进行高速传输的情况下，该功能可避免防重放序列号被过快消耗而引发频繁地重协商。

只有发起方和响应方都开启了 ESN 功能，ESN 功能才能生效。

【举例】

在 IPsec 安全提议中开启 ESN 功能。

```
<Sysname> system-view
[Sysname] ipsec transform-set tran1
[Sysname-ipsec-transform-set-tran1] esn enable
```

【相关命令】

- **display ipsec transform-set**

1.1.12 esp authentication-algorithm

esp authentication-algorithm 命令用来配置 ESP 协议采用的认证算法。

undo esp authentication-algorithm 命令用来恢复缺省情况。

【命令】

非 FIPS 模式下：

```
esp authentication-algorithm { aes-xcbc-mac | md5 | sha1 | sha256 | sha384 |
sha512 } *
undo esp authentication-algorithm
```

FIPS 模式下：

```
esp authentication-algorithm { sha1 | sha256 | sha384 | sha512 } *
undo esp authentication-algorithm
```

【缺省情况】

ESP 协议未采用任何认证算法。

【视图】

IPsec 安全提议视图

【缺省用户角色】

network-admin

【参数】

aes-xcbc-mac：采用 HMAC-AES-XCBC-96 认证算法，密钥长度为 128 比特。本参数仅适用于 IKEv2 协商。

md5：采用 HMAC-MD5 认证算法，密钥长度 128 比特。

sha1：采用 HMAC-SHA1 认证算法，密钥长度 160 比特。

sha256：采用 HMAC-SHA-256 认证算法，密钥长度 256 比特。

sha384：采用 HMAC-SHA-384 认证算法，密钥长度 384 比特。

sha512：采用 HMAC-SHA-512 认证算法，密钥长度 512 比特。

【使用指导】

非 FIPS 模式下，每个 IPsec 安全提议中均可以配置多个 ESP 认证算法，其优先级为配置顺序。

对于手工方式以及 IKEv1（第 1 版本的 IKE 协议）协商方式的 IPsec 安全策略，IPsec 安全提议中配置顺序首位的 ESP 认证算法生效。为保证成功建立 IPsec 隧道，隧道两端指定的 IPsec 安全提议中配置的首个 ESP 认证算法需要一致。

【举例】

在 IPsec 安全提议中配置 ESP 认证算法为 HMAC-SHA1 算法。

```
<Sysname> system-view
[Sysname] ipsec transform-set tran1
[Sysname-ipsec-transform-set-tran1] esp authentication-algorithm sha1
```

【相关命令】

- **ipsec transform-set**

1.1.13 esp encryption-algorithm

esp encryption-algorithm 命令用来配置 ESP 协议采用的加密算法。

undo esp encryption-algorithm 命令用来恢复缺省情况。

【命令】

非 FIPS 模式下：

```
esp encryption-algorithm { 3des-cbc | aes-cbc-128 | aes-cbc-192 |
aes-cbc-256 | aes-ctr-128 | aes-ctr-192 | aes-ctr-256 | camellia-cbc-128 |
camellia-cbc-192 | camellia-cbc-256 | des-cbc | gmac-128 | gmac-192 |
gmac-256 | gcm-128 | gcm-192 | gcm-256 | null } *
undo esp encryption-algorithm.
```

FIPS 模式下：

```
esp encryption-algorithm { aes-cbc-128 | aes-cbc-192 | aes-cbc-256 |
aes-ctr-128 | aes-ctr-192 | aes-ctr-256 | gmac-128 | gmac-192 | gmac-256 |
gcm-128 | gcm-192 | gcm-256 } *
undo esp encryption-algorithm
```

【缺省情况】

ESP 协议未采用任何加密算法。

【视图】

IPsec 安全提议视图

【缺省用户角色】

network-admin

【参数】

3des-cbc：采用 CBC 模式的 3DES 算法，密钥长度为 168 比特。

aes-cbc-128：采用 CBC 模式的 AES 算法，密钥长度为 128 比特。

aes-cbc-192：采用 CBC 模式的 AES 算法，密钥长度为 192 比特。

aes-cbc-256：采用 CBC 模式的 AES 算法，密钥长度为 256 比特。

aes-ctr-128：采用 CTR 模式的 AES 算法，密钥长度为 128 比特。本参数仅适用于 IKEv2 协商。

aes-ctr-192: 采用 CTR 模式的 AES 算法, 密钥长度为 192 比特。本参数仅适用于 IKEv2 协商。

aes-ctr-256: 采用 CTR 模式的 AES 算法, 密钥长度为 256 比特。本参数仅适用于 IKEv2 协商。

camellia-cbc-128: 采用 CBC 模式的 Camellia 算法, 密钥长度为 128 比特。本参数仅适用于 IKEv2 协商。

camellia-cbc-192: 采用 CBC 模式的 Camellia 算法, 密钥长度为 192 比特。本参数仅适用于 IKEv2 协商。

camellia-cbc-256: 采用 CBC 模式的 Camellia 算法, 密钥长度为 256 比特。本参数仅适用于 IKEv2 协商。

des-cbc: 采用 CBC 模式的 DES 算法, 密钥长度为 64 比特。

gmac-128: 采用 GMAC 算法, 密钥长度为 128 比特。本参数仅适用于 IKEv2 协商。

gmac-192: 采用 GMAC 算法, 密钥长度为 192 比特。本参数仅适用于 IKEv2 协商。

gmac-256: 采用 GMAC 算法, 密钥长度为 256 比特。本参数仅适用于 IKEv2 协商。

gcm-128: 采用 GCM 算法, 密钥长度为 128 比特。本参数仅适用于 IKEv2 协商。

gcm-192: 采用 GCM 算法, 密钥长度为 192 比特。本参数仅适用于 IKEv2 协商。

gcm-256: 采用 GCM 算法, 密钥长度为 256 比特。本参数仅适用于 IKEv2 协商。

null: 采用 NULL 加密算法, 表示不进行加密。

【使用指导】

每个 IPsec 安全提议中均可以配置多个 ESP 加密算法, 其优先级为配置顺序。

对于手工方式以及 IKEv1 (第 1 版本的 IKE 协议) 协商方式的 IPsec 安全策略, IPsec 安全提议中配置顺序首位的 ESP 加密算法生效。为保证成功建立 IPsec 隧道, 隧道两端指定的 IPsec 安全提议中配置的首个 ESP 加密算法需要一致。

GCM、GMAC 属于组合模式算法 (Combined mode algorithm)。其中, GCM 算法能同时为 ESP 协议提供加密与认证服务, GMAC 只能提供认证服务。组合模式算法只能用于仅采用 ESP 协议的配置环境, 不能用于同时采用 AH 协议和 ESP 协议的配置环境, 且不能与普通的 ESP 认证算法同时使用。

【举例】

在 IPsec 安全提议中配置 ESP 加密算法为 CBC 模式的 AES 算法, 密钥长度为 128 比特。

```
<Sysname> system-view
[Sysname] ipsec transform-set tran1
[Sysname-ipsec-transform-set-tran1] esp encryption-algorithm aes-cbc-128
```

【相关命令】

- **ipsec transform-set**

1.1.14 ike-profile

ike-profile 命令用来指定 IPsec 安全策略/IPsec 安全策略模板/IPsec 安全框架引用的 IKE profile。

undo ike-profile 命令用来恢复缺省情况。

【命令】

ike-profile *profile-name*

undo ike-profile

【缺省情况】

IPsec 安全策略/IPsec 安全策略模板/IPsec 安全框架中未引用 IKE profile。

【视图】

IPsec 安全策略视图

IPsec 安全策略模板视图

IPsec 安全框架视图

【缺省用户角色】

network-admin

【参数】

profile-name: IKE profile 的名称，为 1~63 个字符的字符串，不区分大小写。

【使用指导】

IPsec 安全策略、IPsec 安全策略模板、IPsec 安全框架中若不引用 IKE profile，则使用系统视图下配置的 IKE profile 进行协商，若系统视图下没有任何 IKE profile，则使用全局的 IKE 参数进行协商。

IPsec 安全策略、IPsec 安全策略模板、IPsec 安全框架引用的 IKE profile 中定义了用于 IKE 协商的相关参数。

IPsec 安全策略/IPsec 安全策略模板/IPsec 安全框架下只能引用一个 IKE profile。

【举例】

指定 IPsec 安全策略 policy1 中引用的 IKE profile 为 profile1。

```
<Sysname> system-view
```

```
[Sysname] ipsec policy policy1 10 isakmp
```

```
[Sysname-ipsec-policy-isakmp-policy1-10] ike-profile profile1
```

【相关命令】

- **ike profile**（安全命令参考/IKE）

1.1.15 ikev2-profile

ikev2-profile 命令用来指定 IPsec 安全策略视图/IPsec 安全策略模板视图引用的 IKEv2 profile。

undo ikev2-profile 命令用来恢复缺省情况。

【命令】

ikev2-profile *profile-name*

undo ikev2-profile

【缺省情况】

未引用 IKEv2 profile。

【视图】

IPsec 安全策略视图

IPsec 安全策略模板视图

【缺省用户角色】

network-admin

【参数】

profile-name: IKEv2 profile 的名称，为 1~63 个字符的字符串，不区分大小写。

【使用指导】

IPsec 安全策略/IPsec 安全策略模板引用的 IKEv2 profile 中定义了用于 IKEv2 协商的相关参数。

一个 IPsec 安全策略视图/一个 IPsec 安全策略模板视图下只能引用一个 IKEv2 profile。发起方必须引用 IKEv2 profile，响应方引用 IKEv2 profile 表示此 IPsec 策略只允许用此 IKEv2 profile 协商，否则表示此 IPsec 策略允许用任何 IKEv2 profile 协商。

【举例】

指定 IPsec 安全策略 policy1 中引用的 IKEv2 profile 为 profile1。

```
<Sysname> system-view
[Sysname] ipsec policy policy1 10 isakmp
[Sysname-ipsec-policy-isakmp-policy1-10] ikev2-profile profile1
```

【相关命令】

- **display ipsec ipv6-policy**
- **display ipsec policy**
- **ikev2 profile**

1.1.16 ipsec { ipv6-policy | policy }

ipsec { ipv6-policy | policy } 命令用来创建一条 IPsec 安全策略，并进入 IPsec 安全策略视图。如果指定的 IPsec 安全策略已经存在，则直接进入 IPsec 安全策略视图。

undo ipsec { ipv6-policy | policy } 命令用来删除 IPsec 安全策略。

【命令】

```
ipsec { ipv6-policy | policy } policy-name seq-number [ isakmp | manual ]
undo ipsec { ipv6-policy | policy } policy-name [ seq-number ]
```

【缺省情况】

不存在 IPsec 安全策略。

【视图】

系统视图

【缺省用户角色】

network-admin

【参数】

ipv6-policy: 指定 IPv6 IPsec 安全策略。

policy: 指定 IPv4 IPsec 安全策略。

policy-name: IPsec 安全策略的名称，为 1~63 个字符的字符串，不区分大小写。

seq-number: IPsec 安全策略的序号，取值范围为 1~65535。

isakmp: 指定通过 IKE 协商建立 IPsec SA。

manual: 指定用手工方式建立 IPsec SA。

【使用指导】

创建 IPsec 安全策略时，必须指定协商方式（**isakmp** 或 **manual**）。进入已创建的 IPsec 安全策略时，可以不指定协商方式。

不能修改已创建的 IPsec 安全策略的协商方式。

一个 IPsec 安全策略是若干具有相同名称、不同顺序号的 IPsec 安全策略表项的集合。在同一个 IPsec 安全策略中，顺序号越小的 IPsec 安全策略表项优先级越高。

对于 **undo** 命令，携带 *seq-number* 参数时表示删除一个 IPsec 安全策略表项，不携带该参数时表示删除一个指定的 IPsec 安全策略。

IPv4 IPsec 安全策略和 IPv6 IPsec 安全策略名称可以相同。

【举例】

创建一个名称为 **policy1**、顺序号为 100、采用 IKE 方式协商 IPsec SA 的 IPsec 安全策略，并进入 IPsec 安全策略视图。

```
<Sysname> system-view
[Sysname] ipsec policy policy1 100 isakmp
[Sysname-ipsec-policy-isakmp-policy1-100]
```

创建一个名称为 **policy1**、顺序号为 101、采用手工方式建立 IPsec SA 的 IPsec 安全策略，并进入 IPsec 安全策略视图。

```
<Sysname> system-view
[Sysname] ipsec policy policy1 101 manual
[Sysname-ipsec-policy-manual-policy1-101]
```

【相关命令】

- **display ipsec { ipv6-policy | policy }**
- **ipsec apply**

1.1.17 ipsec { ipv6-policy | policy } isakmp template

ipsec { ipv6-policy | policy } isakmp template 命令用来引用 IPsec 安全策略模板创建一条 IKE 协商方式的 IPsec 安全策略。

undo ipsec { ipv6-policy | policy } 命令用来删除 IPsec 安全策略。

【命令】

```
ipsec { ipv6-policy | policy } policy-name seq-number isakmp template
template-name
undo ipsec { ipv6-policy | policy } policy-name [ seq-number ]
```

【缺省情况】

不存在 IPsec 安全策略。

【视图】

系统视图

【缺省用户角色】

network-admin

【参数】

ipv6-policy: 指定 IPv6 IPsec 安全策略。

policy: 指定 IPv4 IPsec 安全策略。

policy-name: IPsec 安全策略的名称，为 1~63 个字符的字符串，不区分大小写。

seq-number: IPsec 安全策略的序号，取值范围为 1~65535，值越小优先级越高。

isakmp template template-name: 指定被引用的 IPsec 安全策略模板。**template-name** 表示 IPsec 安全策略模板的名称，为 1~63 个字符的字符串，不区分大小写。

【使用指导】

对于 **undo** 命令，携带 **seq-number** 参数时表示删除一个 IPsec 安全策略表项，不携带该参数时表示删除一个指定的 IPsec 安全策略。

应用了该类 IPsec 安全策略的接口不能发起协商，仅可以响应远端设备的协商请求。由于 IPsec 安全策略模板中未定义的可选参数由发起方来决定，而响应方会接受发起方的建议，因此这种方式创建的 IPsec 安全策略适用于通信对端（例如对端的 IP 地址）未知的情况下，允许这些对端设备向本端设备主动发起协商。

【举例】

引用 IPsec 策略模板 temp1，创建名称为 policy2、序号为 200 的 IPsec 安全策略。

```
<Sysname> system-view
```

```
[Sysname] ipsec policy policy2 200 isakmp template temp1
```

【相关命令】

- **display ipsec { ipv6-policy | policy }**
- **ipsec { ipv6-policy-template | policy-template }**

1.1.18 ipsec { ipv6-policy | policy } local-address

ipsec { ipv6-policy | policy } local-address 命令用来配置 IPsec 安全策略为共享源接口 IPsec 安全策略，即将指定的 IPsec 安全策略与一个源接口进行绑定。

undo ipsec { ipv6-policy | policy } local-address 命令用来取消 IPsec 安全策略为共享源接口 IPsec 安全策略。

【命令】

```
ipsec { ipv6-policy | policy } policy-name local-address interface-type  
interface-number
```

```
undo ipsec { ipv6-policy | policy } policy-name local-address
```

【缺省情况】

IPsec 安全策略不是共享源接口 IPsec 安全策略。

【视图】

系统视图

【缺省用户角色】

network-admin

【参数】

ipv6-policy: 指定 IPv6 IPsec 安全策略。

policy: 指定 IPv4 IPsec 安全策略。

policy-name: 共享该接口 IP 地址的 IPsec 安全策略的名称，为 1~63 个字符的字符串，不区分大小写。

local-address interface-type interface-number: 指定的共享源接口的名称。
interface-type interface-number 为接口类型和接口编号。

【使用指导】

在不同的接口上应用安全策略时，各个接口将分别协商生成 IPsec SA。如果两个互为备份的接口上都引用了 IPsec 安全策略，并采用相同的安全策略，则在主备链路切换时，接口状态的变化会触发重新进行 IKE 协商，从而导致 IPsec 业务流的暂时中断。通过将一个 IPsec 安全策略与一个源接口绑定，使之成为共享源接口 IPsec 安全策略，可以实现多个应用该共享源接口 IPsec 安全策略的出接口共享同一个指定的源接口（称为共享源接口）协商出的 IPsec SA。只要该源接口的状态不变化，各接口上 IPsec 业务就不会中断。

当非共享源接口 IPsec 安全策略应用于业务接口，并已经生成 IPsec SA 时，如果将该安全策略配置为共享源接口安全策略，则已经生成的 IPsec SA 将被删除。

只有 IKE 协商方式的 IPsec 安全策略才能配置为 IPsec 共享源接口安全策略，手工方式的 IPsec 安全策略不能配置为共享源接口 IPsec 安全策略。

一个 IPsec 安全策略只能与一个源接口绑定，多次执行本命令，最后一次执行的命令生效。

一个源接口可以同时与多个 IPsec 安全策略绑定。

推荐使用状态较为稳定的接口作为共享源接口，例如 Loopback 接口。

【举例】

配置 IPsec 安全策略 map 为共享源接口安全策略，共享源接口为 Loopback11。

```
<Sysname> system-view
[Sysname] ipsec policy map local-address loopback 11
```

【相关命令】

- **ipsec { ipv6-policy | policy }**

1.1.19 ipsec { ipv6-policy-template | policy-template }

ipsec { ipv6-policy-template | policy-template } 命令用来创建一个 IPsec 安全策略模板，并进入 IPsec 安全策略模板视图。如果指定的 IPsec 安全策略模板已经存在，则直接进入 IPsec 安全策略模板视图。

undo ipsec { ipv6-policy-template | policy-template } 命令用来删除 IPsec 安全策略模板。

【命令】

ipsec { ipv6-policy-template | policy-template } template-name seq-number

```
undo ipsec { ipv6-policy-template | policy-template } template-name  
[ seq-number ]
```

【缺省情况】

不存在 IPsec 安全策略模板。

【视图】

系统视图

【缺省用户角色】

network-admin

【参数】

ipv6-policy-template: 指定 IPv6 IPsec 安全策略模板。

policy-template: 指定 IPv4 IPsec 安全策略模板。

template-name: IPsec 安全策略模板的名称，为 1~63 个字符的字符串，不区分大小写。

seq-number: IPsec 安全策略模板表项的顺序号，取值范围为 1~65535，值越小优先级越高。

【使用指导】

IPsec 安全策略模板与直接配置的 IKE 协商方式的 IPsec 安全策略中可配置的参数类似，但是配置较为简单，除了 IPsec 安全提议和 IKE 对等体之外的其它参数均为可选。

- 携带 *seq-number* 参数的 **undo** 命令用来删除一个 IPsec 安全策略模板表项。
- 一个 IPsec 安全策略模板是若干具有相同名称、不同顺序号的 IPsec 安全策略模板表项的集合。
- IPv4 IPsec 安全策略模板和 IPv6 IPsec 安全策略模板名称可以相同。

【举例】

创建一个名称为 *template1*、顺序号为 100 的 IPsec 安全策略模板，并进入 IPsec 安全策略模板视图。

```
<Sysname> system-view  
[Sysname] ipsec policy-template template1 100  
[Sysname-ipsec-policy-template-template1-100]
```

【相关命令】

- **display ipsec { ipv6-policy-template | policy-template }**
- **ipsec { ipv6-policy | policy }**
- **ipsec { ipv6-policy | policy } isakmp template**

1.1.20 ipsec anti-replay check

ipsec anti-replay check 命令用来开启 IPsec 抗重放检测功能。

undo ipsec anti-replay check 用来关闭 IPsec 抗重放检测功能。

【命令】

```
ipsec anti-replay check  
undo ipsec anti-replay check
```

【缺省情况】

IPsec 抗重放检测功能处于开启状态。

【视图】

系统视图

【缺省用户角色】

network-admin

【使用指导】

对重放报文的解封装无意义，并且解封装过程涉及密码学运算，会消耗设备大量的资源，导致业务可用性下降，造成了拒绝服务攻击。通过开启 IPsec 抗重放检测功能，将检测到的重放报文在解封装处理之前丢弃，可以降低设备资源的消耗。

在某些特定环境下，业务数据报文的接收顺序可能与正常的顺序差别较大，虽然并非有意的重放攻击，但会被抗重放检测认为是重放报文，导致业务数据报文被丢弃，影响业务的正常运行。因此，这种情况下就可以通过关闭 IPsec 抗重放检测功能来避免业务数据报文的错误丢弃，也可以通过适当地增大抗重放窗口的宽度，来适应业务正常运行的需要。

只有 IKE 协商的 IPsec SA 才能够支持抗重放检测，手工方式生成的 IPsec SA 不支持抗重放检测。因此该功能开启与否对手工方式生成的 IPsec SA 没有影响。

【举例】

开启 IPsec 抗重放检测功能。

```
<Sysname> system-view
[Sysname] ipsec anti-replay check
```

【相关命令】

- **ipsec anti-replay window**

1.1.21 ipsec anti-replay window

ipsec anti-replay window 命令用来配置 IPsec 抗重放窗口的宽度。

undo ipsec anti-replay window 命令用来恢复缺省情况。

【命令】

```
ipsec anti-replay window width
undo ipsec anti-replay window
```

【缺省情况】

IPsec 抗重放窗口的宽度为 64。

【视图】

系统视图

【缺省用户角色】

network-admin

【参数】

width: IPsec 抗重放窗口的宽度，取值可以为 64、128、256、512、1024，单位为报文个数。

【使用指导】

在某些特定环境下，业务数据报文的接收顺序可能与正常的顺序差别较大，虽然并非有意的重放攻击，但会被抗重放检测认为是重放报文，导致业务数据报文被丢弃，影响业务的正常运行。因此，这种情况下就可以通过关闭 IPsec 抗重放检测功能来避免业务数据报文的错误丢弃，也可以通过适当地增大抗重放窗口的宽度，来适应业务正常运行的需要。

修改后的抗重放窗口宽度仅对新协商成功的 IPsec SA 生效。

【举例】

```
# 配置 IPsec 抗重放窗口的宽度为 128。
<Sysname> system-view
[Sysname] ipsec anti-replay window 128
```

【相关命令】

- **ipsec anti-replay check**

1.1.22 ipsec apply

ipsec apply 命令用来在接口上应用 IPsec 安全策略。

undo ipsec apply 命令用来从接口上取消应用的 IPsec 安全策略。

【命令】

```
ipsec apply { ipv6-policy | policy } policy-name
undo ipsec apply { ipv6-policy | policy }
```

【缺省情况】

接口上未应用 IPsec 安全策略。

【视图】

接口视图

【缺省用户角色】

network-admin

【参数】

ipv6-policy: 指定 IPv6 IPsec 安全策略。

policy: 指定 IPv4 IPsec 安全策略。

policy-name: IPsec 安全策略的名称，为 1~63 个字符的字符串，不区分大小写。

【使用指导】

一个接口下最多只能应用一个 IPv4/IPv6 类型的 IPsec 安全策略，但可以同时应用一个 IPv4 类型的 IPsec 安全策略和一个 IPv6 类型的 IPsec 安全策略。

IKE 方式的 IPsec 安全策略可以应用到多个接口上，但建议只应用到一个接口上；手工方式的 IPsec 安全策略只能应用到一个接口上。

【举例】

```
# 在接口 Vlan-interface100 上应用名为 policy1 的 IPsec 安全策略。
<Sysname> system-view
```

```
[Sysname] interface vlan-interface 100
[Sysname-Vlan-interface100] ipsec apply policy policy1
```

【相关命令】

- **display ipsec { ipv6-policy | policy }**
- **ipsec { ipv6-policy | policy }**

1.1.23 ipsec decrypt-check enable

ipsec decrypt-check enable 命令用来开启解封装后 IPsec 报文的 ACL 检查功能。

undo ipsec decrypt-check 命令用来关闭解封装后 IPsec 报文的 ACL 检查功能。

【命令】

```
ipsec decrypt-check enable
undo ipsec decrypt-check enable
```

【缺省情况】

解封装后 IPsec 报文的 ACL 检查功能处于开启状态。

【视图】

系统视图

【缺省用户角色】

network-admin

【使用指导】

在隧道模式下，接口入方向上解封装的 IPsec 报文的内部 IP 头有可能不在当前 IPsec 安全策略引用的 ACL 的保护范围内，如网络中一些恶意伪造的攻击报文就可能有此问题，所以设备需要重新检查解封装后的报文的 IP 头是否在 ACL 保护范围内。开启该功能后可以保证 ACL 检查不通过的报文被丢弃，从而提高网络安全性。

【举例】

开启解封装后 IPsec 报文的 ACL 检查功能。

```
<Sysname> system-view
[Sysname] ipsec decrypt-check enable
```

1.1.24 ipsec df-bit

ipsec df-bit 命令用来为当前接口设置 IPsec 封装后外层 IP 头的 DF 位。

undo ipsec df-bit 命令用来恢复缺省情况。

【命令】

```
ipsec df-bit { clear | copy | set }
undo ipsec df-bit
```

【缺省情况】

接口下未设置 IPsec 封装后外层 IP 头的 DF 位，采用全局设置的 DF 位。

【视图】

接口视图

【缺省用户角色】

network-admin

【参数】

clear: 表示清除外层 IP 头的 DF 位，IPsec 封装后的报文可被分片。

copy: 表示外层 IP 头的 DF 位从原始报文 IP 头中拷贝。

set: 表示设置外层 IP 头的 DF 位，IPsec 封装后的报文不能分片。

【使用指导】

该功能仅在 IPsec 的封装模式为隧道模式时有效（因为传输模式不会增加新的 IP 头，因此对于传输模式无影响）。

该功能用于设置 IPsec 隧道模式封装后的外层 IP 头的 DF 位，原始报文 IP 头的 DF 位不会被修改。

如果有多个接口应用了共享源接口安全策略，则这些接口上必须使用相同的 DF 位设置。

转发报文时对报文进行分片、重组，可能会导致报文的转发延时较大。若设置了封装后 IPsec 报文的 DF 位，则不允许对 IPsec 报文进行分片，可以避免引入分片延时。这种情况下，要求 IPsec 报文转发路径上各个接口的 MTU 大于 IPsec 报文长度，否则，会导致 IPsec 报文被丢弃。如果无法保证转发路径上各个接口的 MTU 大于 IPsec 报文长度，则建议清除 DF 位。

【举例】

在接口 Vlan-interface100 上设置 IPsec 封装后外层 IP 头的 DF 位。

```
<Sysname> system-view
[Sysname] interface vlan-interface 100
[Sysname-Vlan-interface100] ipsec df-bit set
```

【相关命令】

- **ipsec global-df-bit**

1.1.25 ipsec fragmentation

ipsec fragmentation 命令用来配置 IPsec 分片功能。

undo ipsec fragmentation 命令用来恢复缺省情况。

【命令】

```
ipsec fragmentation { after-encryption | before-encryption }
undo ipsec fragmentation
```

【缺省情况】

IPsec 分片功能为封装前分片。

【视图】

系统视图

【缺省用户角色】

network-admin

【参数】

after-encryption: 表示开启 IPsec 封装后分片功能。

before-encryption: 表示开启 IPsec 封装前分片功能。

【使用指导】

IPsec 封装前分片功能处于开启状态时，设备会先判断报文在经过 IPsec 封装之后大小是否会超过发送接口的 MTU 值，如果封装后的大小超过发送接口的 MTU 值，且报文的 DF 位未置位那么会先对其分片再封装；如果待报文的 DF 位被置位，那么设备会丢弃该报文，并发送 ICMP 差错控制报文。

IPsec 封装后分片功能处于开启状态时，无论报文封装后大小是否超过发送接口的 MTU 值，设备会直接对其先进行 IPsec 封装处理，再由后续业务对其进行分片。

【举例】

开启 IPsec 封装后分片功能。

```
<Sysname>system-view
```

```
[Sysname] ipsec fragmentation after-encryption
```

1.1.26 ipsec global-df-bit

ipsec global-df-bit 命令用来为所有接口设置 IPsec 封装后外层 IP 头的 DF 位。

undo ipsec global-df-bit 命令用来恢复缺省情况。

【命令】

```
ipsec global-df-bit { clear | copy | set }
```

```
undo ipsec global-df-bit
```

【缺省情况】

IPsec 封装后外层 IP 头的 DF 位从原始报文 IP 头中拷贝。

【视图】

系统视图

【缺省用户角色】

network-admin

【参数】

clear: 表示清除外层 IP 头的 DF 位，IPsec 封装后的报文可被分片。

copy: 表示外层 IP 头的 DF 位从原始报文 IP 头中拷贝。

set: 表示设置外层 IP 头的 DF 位，IPsec 封装后的报文不能分片。

【使用指导】

该功能仅在 IPsec 的封装模式为隧道模式时有效（因为传输模式不会增加新的 IP 头，因此对于传输模式无影响）。

该功能用于设置 IPsec 隧道模式封装后的外层 IP 头的 DF 位，原始报文 IP 头的 DF 位不会被修改。转发报文时对报文进行分片、重组，可能会导致报文的转发延时较大。若设置了封装后 IPsec 报文的 DF 位，则不允许对 IPsec 报文进行分片，可以避免引入分片延时。这种情况下，要求 IPsec 报

文转发路径上各个接口的 MTU 大于 IPsec 报文长度，否则，会导致 IPsec 报文被丢弃。如果无法保证转发路径上各个接口的 MTU 大于 IPsec 报文长度，则建议清除 DF 位。

【举例】

为所有接口设置 IPsec 封装后外层 IP 头的 DF 位。

```
<Sysname> system-view
[Sysname] ipsec global-df-bit set
```

【相关命令】

- **ipsec df-bit**

1.1.27 ipsec limit max-tunnel

ipsec limit max-tunnel 命令用来配置本端允许建立 IPsec 隧道的最大数。

undo ipsec limit max-tunnel 命令用来恢复缺省情况。

【命令】

```
ipsec limit max-tunnel tunnel-limit
undo ipsec limit max-tunnel
```

【缺省情况】

不限制本端允许建立 IPsec 隧道的最大数。

【视图】

系统视图

【缺省用户角色】

network-admin

【参数】

tunnel-limit：指定允许本端建立 IPsec 隧道的最大数，取值范围为 1～4294967295。

【使用指导】

本端允许建立 IPsec 隧道的最大数与内存资源有关。内存充足时可以设置较大的数值，提高 IPsec 的并发性能；内存不足时可以设置较小的数值，降低 IPsec 占用内存的资源。

【举例】

配置本端允许建立 IPsec 隧道的最大数为 5000。

```
<Sysname> system-view
[Sysname] ipsec limit max-tunnel 5000
```

【相关命令】

- **ike limit**

1.1.28 ipsec logging packet enable

ipsec logging packet enable 命令用来开启 IPsec 报文日志记录功能。

undo ipsec logging packet enable 命令用来关闭 IPsec 报文日志记录功能。

【命令】

```
ipsec logging packet enable
undo ipsec logging packet enable
```

【缺省情况】

IPsec 报文日志记录功能处于关闭状态。

【视图】

系统视图

【缺省用户角色】

network-admin

【使用指导】

开启 IPsec 报文日志记录功能后，设备会在丢弃 IPsec 报文的情况下，例如入方向找不到对应的 IPsec SA，AH/ESP 认证失败或 ESP 加密失败等时，输出相应的日志信息，该日志信息内容主要包括报文的源和目的 IP 地址、报文的 SPI 值、报文的序列号信息，以及设备丢包的原因。

【举例】

```
# 开启 IPsec 报文日志记录功能。
<Sysname> system-view
[Sysname] ipsec logging packet enable
```

1.1.29 ipsec profile

ipsec profile 命令用来创建一个 IPsec 安全框架，并进入 IPsec 安全框架视图。如果指定的 IPsec 安全框架已经存在，则直接进入 IPsec 安全框架视图。

undo ipsec profile 命令用来删除 IPsec 安全框架。

【命令】

```
ipsec profile profile-name [ manual | isakmp ]
undo ipsec profile profile-name
```

【缺省情况】

不存在 IPsec 安全框架。

【视图】

系统视图

【缺省用户角色】

network-admin

【参数】

profile-name: IPsec 安全框架的名称，为 1～63 个字符的字符串，不区分大小写。

manual: 手工方式的 IPsec 安全框架。

【使用指导】

创建 IPsec 安全框架时，必须指定协商方式（**manual** 或 **isakmp**）；进入已创建的 IPsec 安全框架时，可以不指定协商方式。

手工方式 IPsec profile 专门用于为应用协议配置 IPsec 安全策略，它相当于一个手工方式创建的 IPsec 安全策略，其中的应用协议可包括但不限于 OSPFv3、RIPng。

IKE 协商方式 IPsec profile 用于为应用协议模块自动协商生成安全联盟，不限制对端的地址，不需要进行 ACL 匹配，且适用于 IPv4 和 IPv6 应用协议，其中的应用协议模块包括但是不限于 ADVPN 等。

【举例】

配置名称为 profile1 的 IPsec 安全框架，通过手工配置建立安全联盟。

```
<Sysname> system-view
[Sysname] ipsec profile profile1 manual
[Sysname-ipsec-profile-manual-profile1]
```

配置名称为 profile1 的 IPsec 安全框架，通过 IKE 协商建立安全联盟。

```
<Sysname> system-view
[Sysname] ipsec profile profile1 isakmp
[Sysname-ipsec-profile-isakmp-profile1]
```

【相关命令】

- **display ipsec profile**

1.1.30 ipsec redundancy enable

ipsec redundancy enable 命令用来开启 IPsec 冗余备份功能。

undo ipsec redundancy enable 命令用来关闭 IPsec 冗余备份功能。

【命令】

```
ipsec redundancy enable
undo ipsec redundancy enable
```

【缺省情况】

IPsec 冗余备份功能处于关闭状态。

【视图】

系统视图

【缺省用户角色】

network-admin

【使用指导】

开启冗余备份功能后，系统会根据命令 **redundancy replay-interval** 指定的备份间隔将接口上 IPsec 入方向抗重放窗口的左侧值和出方向 IPsec 报文的抗重放序号进行备份，当发生主备切换时，可以保证主备 IPsec 流量不中断和抗重放保护不间断。

【举例】

开启 IPsec 冗余备份功能。

```
<Sysname> system-view
[Sysname] ipsec redundancy enable
```

【相关命令】

- **redundancy replay-interval**

1.1.31 ipsec sa global-duration

ipsec sa global-duration 命令用来配置全局的 IPsec SA 生存时间。

undo ipsec sa global-duration 命令用来恢复缺省情况。

【命令】

```
ipsec sa global-duration { time-based seconds | traffic-based kilobytes }
undo ipsec sa global-duration { time-based | traffic-based }
```

【缺省情况】

IPsec SA 基于时间的生存时间为 3600 秒，基于流量的生存时间为 1843200 千字节。

【视图】

系统视图

【缺省用户角色】

network-admin

【参数】

time-based seconds: 指定基于时间的全局生存时间，取值范围为 180~604800，单位为秒。

traffic-based kilobytes: 指定基于流量的全局生存时间，取值范围为 2560~4294967295，单位为千字节。如果流量达到此值，则生存时间到期。

【使用指导】

IPsec 安全策略/IPsec 安全策略模板视图下也可配置 IPsec SA 的生存时间，若 IPsec 安全策略/IPsec 安全策略模板视图和全局都配置了 IPsec SA 的生存时间，则优先采用 IPsec 安全策略/IPsec 安全策略模板视图下的配置值与对端协商。

IKE 为 IPsec 协商建立 IPsec SA 时，采用本地配置的生存时间和对端提议的 IPsec SA 生存时间中较小的一个。

可同时存在基于时间和基于流量两种方式的 IPsec SA 生存时间，只要 IPsec SA 的生存时间到达指定的时间或流量时，该 IPsec SA 就会失效。IPsec SA 失效前，IKE 将为 IPsec 对等体协商建立新的 IPsec SA，这样，在旧的 IPsec SA 失效前新的 IPsec SA 就已经准备好。在新的 IPsec SA 开始协商而没有协商好之前，继续使用旧的 IPsec SA 保护通信。在新的 IPsec SA 协商好之后，则立即采用新的 IPsec SA 保护通信。

【举例】

配置全局的 IPsec SA 生存时间为两个小时，即 7200 秒。

```
<Sysname> system-view
[Sysname] ipsec sa global-duration time-based 7200
```

配置全局的 IPsec SA 生存时间为 10M 字节，即传输 10240 千字节的流量后，当前的 IPsec SA 过期。

```
[Sysname] ipsec sa global-duration traffic-based 10240
```

【相关命令】

- **display ipsec sa**
- **sa duration**

1.1.32 ipsec sa idle-time

ipsec sa idle-time 命令用来开启全局的 IPsec SA 空闲超时功能，并配置全局 IPsec SA 空闲超时时间。在指定超时时间内没有流量匹配的 IPsec SA 即被删除。

undo ipsec sa idle-time 命令用来关闭全局的 IPsec SA 空闲超时功能。

【命令】

```
ipsec sa idle-time seconds
undo ipsec sa idle-time
```

【缺省情况】

全局的 IPsec SA 空闲超时功能处于关闭状态。

【视图】

系统视图

【缺省用户角色】

network-admin

【参数】

seconds: IPsec SA 的空闲超时时间，取值范围为 60～86400，单位为秒。

【使用指导】

此功能只适用于 IKE 协商出的 IPsec SA。

IPsec 安全策略/IPsec 安全策略模板/IPsec 安全框架视图下也可配置 IPsec SA 的空闲超时时间，若 IPsec 安全策略/IPsec 安全策略模板/IPsec 安全框架视图和全局都配置了 IPsec SA 的空闲超时时间，则优先采用 IPsec 安全策略/IPsec 安全策略模板/IPsec 安全框架视图下的配置值。

【举例】

开启全局的 IPsec SA 空闲超时功能，并配置全局 IPsec SA 的空闲超时时间为 600 秒。

```
<Sysname> system-view
[Sysname] ipsec sa idle-time 600
```

【相关命令】

- **display ipsec sa**
- **sa idle-time**

1.1.33 ipsec transform-set

ipsec transform-set 命令用来创建 IPsec 安全提议，并进入 IPsec 安全提议视图。如果指定的 IPsec 安全提议已经存在，则直接进入 IPsec 安全提议视图。

undo ipsec transform-set 命令用来删除指定的 IPsec 安全提议。

【命令】

```
ipsec transform-set transform-set-name  
undo ipsec transform-set transform-set-name
```

【缺省情况】

不存在 IPsec 安全提议。

【视图】

系统视图

【缺省用户角色】

network-admin

【参数】

transform-set-name: IPsec 安全提议的名称，为 1~63 个字符的字符串，不区分大小写。

【使用指导】

IPsec 安全提议是 IPsec 安全策略的一个组成部分，它用于保存 IPsec 需要使用的安全协议、加密/认证算法以及封装模式，为 IPsec 协商 SA 提供各种安全参数。

【举例】

创建名为 tran1 的 IPsec 安全提议，并进入 IPsec 安全提议视图。

```
<Sysname> system-view  
[Sysname] ipsec transform-set tran1  
[Sysname-transform-set-tran1]
```

【相关命令】

- **display ipsec transform-set**

1.1.34 local-address

local-address 命令用来配置 IPsec 隧道的本端 IP 地址。

undo local-address 命令用来恢复缺省情况。

【命令】

```
local-address { ipv4-address | ipv6 ipv6-address }  
undo local-address
```

【缺省情况】

IPsec 隧道的本端 IPv4 地址为应用 IPsec 安全策略的接口的主 IPv4 地址，本端 IPv6 地址为应用 IPsec 安全策略的接口的第一个 IPv6 地址。

【视图】

IPsec 安全策略视图

IPsec 安全策略模板视图

【缺省用户角色】

network-admin

【参数】

ipv4-address: IPsec 隧道的本端 IPv4 地址。

ipv6 ipv6-address: IPsec 隧道的本端 IPv6 地址。

【使用指导】

采用 IKE 协商方式的 IPsec 安全策略上，发起方的 IPsec 隧道的对端 IP 地址必须与响应方的 IPsec 隧道本端 IP 地址一致。

【举例】

配置 IPsec 隧道的本端 IP 地址为 1.1.1.1。

```
<Sysname> system-view
[Sysname] ipsec policy map 1 isakmp
[Sysname-ipsec-policy-isakmp-map-1] local-address 1.1.1.1
```

【相关命令】

- **remote-address**

1.1.35 pfs

pfs 命令用来配置在使用此安全提议发起 IKE 协商时使用 PFS（Perfect Forward Secrecy，完善的前向安全）特性。

undo pfs 命令用来恢复缺省情况。

【命令】

非 FIPS 模式下：

```
pfs { dh-group1 | dh-group2 | dh-group5 | dh-group14 | dh-group24 |
dh-group19 | dh-group20 }
```

```
undo pfs
```

FIPS 模式下：

```
pfs { dh-group14 | dh-group19 | dh-group20 }
```

```
undo pfs
```

【缺省情况】

使用 IPsec 安全策略发起 IKE 协商时不使用 PFS 特性。

【视图】

IPsec 安全提议视图

【缺省用户角色】

network-admin

【参数】

dh-group1: 采用 768-bit Diffie-Hellman 组。

dh-group2: 采用 1024-bit Diffie-Hellman 组。

dh-group5: 采用 1536-bit Diffie-Hellman 组。

dh-group14: 采用 2048-bit Diffie-Hellman 组。

dh-group24: 采用 2048-bit 和 256-bit 子群 Diffie-Hellman 组。

dh-group19: 采用 256-bit ECP 模式 Diffie-Hellman 组。本参数仅适用于 IKEv2 协商。

dh-group20: 采用 384-bit ECP 模式 Diffie-Hellman 组。本参数仅适用于 IKEv2 协商。

【使用指导】

384-bit ECP 模式 Diffie-Hellman 组 (**dh-group20**)、256-bit ECP 模式 Diffie-Hellman 组 (**dh-group19**)、2048-bit 和 256-bit 子群 Diffie-Hellman 组 (**dh-group24**)、2048-bit Diffie-Hellman 组 (**dh-group14**)、1536-bit Diffie-Hellman 组 (**dh-group5**)、1024-bit Diffie-Hellman 组 (**dh-group2**)、768-bit Diffie-Hellman 组 (**dh-group1**) 算法的强度, 即安全性和需要计算的时间依次递减。

IKEv1 协商时发起方的 PFS 强度必须大于或等于响应方的 PFS 强度, 否则 IKE 协商会失败。IKEv2 不受该限制。

不配置 PFS 特性的一端, 按照对端的 PFS 特性要求进行 IKE 协商。

【举例】

配置 IPsec 安全提议使用 PFS 特性, 并采用 2048-bit Diffie-Hellman 组。

```
<Sysname> system-view
[Sysname] ipsec transform-set tran1
[Sysname-ipsec-transform-set-tran1] pfs dh-group14
```

1.1.36 protocol

protocol 命令用来配置 IPsec 安全提议采用的安全协议。

undo protocol 命令用来恢复缺省情况。

【命令】

```
protocol { ah | ah-esp | esp }
undo protocol
```

【缺省情况】

使用 ESP 安全协议。

【视图】

IPsec 安全提议视图

【缺省用户角色】

network-admin

【参数】

ah: 采用 AH 协议对报文进行保护。

ah-esp: 先用 ESP 协议对报文进行保护, 再用 AH 协议对报文进行保护。

esp: 采用 ESP 协议对报文进行保护。

【使用指导】

在 IPsec 隧道的两端, IPsec 安全提议所采用的安全协议必须一致。

【举例】

```
# 配置 IPsec 安全提议采用 AH 协议。
<Sysname> system-view
[Sysname] ipsec transform-set tran1
[Sysname-ipsec-transform-set-tran1] protocol ah
```

1.1.37 qos pre-classify

qos pre-classify 命令用来开启 QoS 预分类功能。

undo qos pre-classify 命令用来关闭 QoS 预分类功能。

【命令】

```
qos pre-classify
undo qos pre-classify
```

【缺省情况】

QoS 预分类功能处于关闭状态,即 QoS 使用 IPsec 封装后报文的外层 IP 头信息来对报文进行分类。

【视图】

IPsec 安全策略视图

IPsec 安全策略模板视图

【缺省用户角色】

network-admin

【使用指导】

QoS 预分类功能是指, QoS 基于被封装报文的原始 IP 头信息对报文进行分类。

【举例】

```
# 在 IPsec 安全策略中开启 QoS 预分类功能。
<Sysname> system-view
[Sysname] ipsec policy policy1 100 manual
[Sysname-ipsec-policy-manual-policy1-100] qos pre-classify
```

1.1.38 redundancy replay-interval

redundancy replay-interval 命令用来配置抗重放窗口和序号的同步间隔。

undo redundancy replay-interval 命令用来恢复缺省情况。

【命令】

```
redundancy    replay-interval    inbound    inbound-interval    outbound
outbound-interval
undo redundancy replay-interval
```

【缺省情况】

同步入方向抗重放窗口的报文间隔为 1000,同步出方向 IPsec SA 抗重放序号的报文间隔为 100000。

【视图】

IPsec 安全策略视图

IPsec 安全策略模板视图

【缺省用户角色】

network-admin

【参数】

inbound inbound-interval: 同步入方向 IPsec SA 抗重放窗口左侧值的报文间隔，取值范围为 0~1000，单位为报文个数，取值为 0，表示不同步防重放窗口。

outbound outbound-interval: 同步出方向 IPsec SA 抗重放序号的报文间隔，取值范围为 1000~100000，单位为报文个数。

【使用指导】

IPsec 冗余备份功能处于开启状态时，抗重放序号同步间隔的配置才会生效。

调小同步的报文间隔，可以增加主备间保持抗重放窗口和序号一致的精度，但同时转发性能会有一定影响。

【举例】

配置同步入方向抗重放窗口的报文间隔为 800，同步出方向抗重放序号的报文间隔为 50000。

```
<Sysname> system-view
[Sysname] ipsec policy test 1 manual
[sysname-ipsec-policy-manual-test-1] redundancy replay-interval inbound 800 outbound 50000
```

【相关命令】

- **ipsec anti-replay check**
- **ipsec anti-replay window**
- **ipsec redundancy enable**

1.1.39 remote-address

remote-address 命令用来指定 IPsec 隧道的对端 IP 地址。

undo remote-address 命令用来恢复缺省情况。

【命令】

```
remote-address { [ ipv6 ] host-name | ipv4-address | ipv6 ipv6-address }
undo remote-address { [ ipv6 ] host-name | ipv4-address | ipv6 ipv6-address }
```

【缺省情况】

未指定 IPsec 隧道的对端 IP 地址。

【视图】

IPsec 安全策略视图

IPsec 安全策略模板视图

【缺省用户角色】

network-admin

【参数】

ipv6: 指定 IPv6 IPsec 隧道的对端地址或主机名称。如果不指定该参数，则表示指定 IPv4 IPsec 隧道的对端地址或主机名称。

hostname: IPsec 隧道的对端主机名，为 1~253 个字符的字符串，不区分大小写。该主机名可被 DNS 服务器解析为 IP 地址。

ipv4-address: IPsec 隧道的对端 IPv4 地址。

ipv6-address: IPsec 隧道的对端 IPv6 地址。

【使用指导】

IKE 协商发起方必须配置 IPsec 隧道的对端 IP 地址，对于使用 IPsec 安全策略模板的响应方可选配。

手工方式的 IPsec 安全策略不支持域名解析，因此只能指定 IP 地址类型的对端 IP 地址。

对于主机名方式的对端地址，地址更新的查询过程有所不同。

- 若此处指定对端主机名由 DNS 服务器来解析，则本端按照 DNS 服务器通知的域名解析有效期，在该有效期超时之后向 DNS 服务器查询主机名对应的最新的 IP 地址。
- 若此处指定对端主机名由本地配置的静态域名解析（通过 **ip host** 命令配置）来解析，则更改此主机名对应的 IP 地址之后，需要在 IPsec 安全策略或 IPsec 安全策略模板中重新配置 **remote-address**，才能使得本端解析到更新后的对端 IP 地址。

例如，本端已经存在一条静态域名解析配置，它指定了主机名 **test** 对应的 IP 地址为 1.1.1.1。若先后执行以下配置：

在 IPsec 安全策略 **policy1** 中指定 IPsec 隧道的对端主机名为 **test**。

```
[Sysname] ipsec policy policy1 1 isakmp
[Sysname-ipsec-policy-isakmp-policy1-1] remote-address test
```

更改主机名 **test** 对应的 IP 地址为 2.2.2.2。

```
[Sysname] ip host test 2.2.2.2
```

则，需要在 IPsec 安全策略 **policy1** 中重新指定对端主机名，使得本端可以根据更新后的本地域名解析配置得到最新的对端 IP 地址 2.2.2.2，否则仍会解析为原来的 IP 地址 1.1.1.1。

重新指定 IPsec 隧道的对端主机名为 **test**。

```
[Sysname] ipsec policy policy1 1 isakmp
[Sysname-ipsec-policy-isakmp-policy1-1] remote-address test
```

【举例】

指定 IPsec 隧道的对端 IPv4 地址为 10.1.1.2。

```
<Sysname> system-view
[Sysname] ipsec policy policy1 10 manual
[Sysname-ipsec-policy-manual-policy1-10] remote-address 10.1.1.2
```

【相关命令】

- **ip host**（三层技术-IP 业务/域名解析）
- **local-address**

1.1.40 reset ipsec sa

reset ipsec sa 命令用来清除已经建立的 IPsec SA。

【命令】

```
reset ipsec sa [ { ipv6-policy | policy } policy-name [ seq-number ] | profile  
policy-name | remote { ipv4-address | ipv6 ipv6-address } | spi { ipv4-address  
| ipv6 ipv6-address } { ah | esp } spi-num ]
```

【视图】

用户视图

【缺省用户角色】

network-admin

【参数】

{ ipv6-policy | policy } policy-name [seq-number]: 表示根据 IPsec 安全策略名称清除 IPsec SA。

- **ipv6-policy**: IPv6 IPsec 安全策略。
- **policy**: IPv4 IPsec 安全策略。
- **policy-name**: IPsec 安全策略的名称，为 1~63 个字符的字符串，不区分大小写。
- **seq-number**: IPsec 安全策略表项的序号，取值范围为 1~65535。如果不指定该参数，则表示指定名称为 *policy-name* 的安全策略中所有安全策略表项。

profile profile-name: 表示根据 IPsec 安全框架名称清除 IPsec SA。 *profile-name* 表示 IPsec 安全框架的名称，为 1~63 个字符的字符串，不区分大小写。

remote: 表示根据对端 IP 地址清除 IPsec SA。

- **ipv4-address**: 对端的 IPv4 地址。
- **ipv6 ipv6-address**: 对端的 IPv6 地址。

spi { ipv4-address | ipv6 ipv6-address } { ah | esp } spi-num: 表示根据 SA 的三元组信息（对端 IP 地址、安全协议、安全参数索引）清除 IPsec SA。

- **ipv4-address**: 对端的 IPv4 地址。
- **ipv6 ipv6-address**: 对端的 IPv6 地址。
- **ah**: AH 协议。
- **esp**: ESP 协议。
- **spi-num**: 安全参数索引，取值范围为 256~4294967295。

【使用指导】

如果不指定任何参数，则清除所有的 IPsec SA。

如果指定了一个 IPsec SA 的三元组信息，则将清除符合该三元组的某一个方向的 IPsec SA 以及对应的另外一个方向的 IPsec SA。若是同时采用了两种安全协议，则还会清除另外一个协议的出方向和入方向的 IPsec SA。

对于出方向 IPsec SA，三元组是它的唯一标识；对于入方向 IPsec SA，SPI 是它的唯一标识。因此，若是希望通过指定出方向的三元组信息来清除 IPsec SA，则需要准确指定三元组信息（其中，IPsec 安全框架生成的 SA 由于没有地址信息，所以地址信息可以任意）；若是希望通过指定入方向的三元组信息来清除 IPsec SA，则只需要准确指定 SPI 值即可，另外两个信息可以任意。

通过手工建立的 IPsec SA 被清除后，系统会立即根据对应的手工 IPsec 安全策略建立新的 IPsec SA。

通过 IKE 协商建立的 IPsec SA 被清除后，系统会在有报文需要进行 IPsec 保护时触发协商新的 IPsec SA。

【举例】

```
# 清除所有 IPsec SA。
<Sysname> reset ipsec sa
# 清除 SPI 为 256、对端地址为 10.1.1.2、安全协议为 AH 的出方向和入方向的 IPsec SA。
<Sysname> reset ipsec sa spi 10.1.1.2 ah 256
# 清除 IPsec 对端地址为 10.1.1.2 的所有 IPsec SA。
<Sysname> reset ipsec sa remote 10.1.1.2
# 清除 IPsec 安全策略名称为 policy1、顺序号为 10 的所有 IPsec SA。
<Sysname> reset ipsec sa policy policy1 10
# 清除 IPsec 安全策略 policy1 中的所有 IPsec SA。
<Sysname> reset ipsec sa policy policy1
```

【相关命令】

- **display ipsec sa**

1.1.41 reset ipsec statistics

reset ipsec statistics 命令用来清除 IPsec 的报文统计信息。

【命令】

```
reset ipsec statistics [ tunnel-id tunnel-id ]
```

【视图】

用户视图

【缺省用户角色】

network-admin

【参数】

tunnel-id tunnel-id: 清除指定 IPsec 隧道的报文统计信息。其中，*tunnel-id* 为隧道的 ID 号，取值范围为 0~4294967295。如果未指定本参数，则清除 IPsec 的所有报文统计信息。

【举例】

```
# 清除 IPsec 的所有报文统计信息。
<Sysname> reset ipsec statistics
```

【相关命令】

- **display ipsec statistics**

1.1.42 reverse-route dynamic

reverse-route dynamic 命令用来开启 IPsec 反向路由注入功能。

undo reverse-route dynamic 命令用来关闭 IPsec 反向路由注入功能。

【命令】

```
reverse-route dynamic
undo reverse-route dynamic
```

【缺省情况】

IPsec 反向路由注入功能处于关闭状态。

【视图】

IPsec 安全策略视图
IPsec 安全策略模板视图

【缺省用户角色】

network-admin

【使用指导】

在企业中心侧网关设备上的某安全策略视图/安全策略模板视图下开启 IPsec 反向路由注入功能后，设备会根据协商的 IPsec SA 自动生成一条静态路由，该路由的目的地址为受保护的对端私网，下一跳地址为 IPsec 隧道的对端地址。

开启反向路由注入功能时，会删除本策略协商出的所有 IPsec SA。当有新的流量触发生成 IPsec SA 时，根据新协商的 IPsec 生成路由信息。

关闭反向路由注入功能时，会删除本策略协商出的所有 IPsec SA。

生成的静态路由随 IPsec SA 的创建而创建，随 IPsec SA 的删除而删除。

需要查看生成的路由信息时，可以通过 **display ip routing-table** 命令查看。

【举例】

开启 IPsec 反向路由注入功能，根据协商成功的 IPsec SA 动态生成静态路由，目的地址为受保护的对端私网网段 3.0.0.0/24，下一跳地址为对端隧道地址 1.1.1.2。

```
<Sysname> system-view
[Sysname] ipsec policy 1 1 isakmp
[Sysname-ipsec-policy-isakmp-1-1] reverse-route dynamic
[Sysname-ipsec-policy-isakmp-1-1] quit
```

隧道两端的 IPsec SA 协商成功后，可查看到生成如下静态路由（其它显示信息略）。

```
[Sysname] display ip routing-table
```

```
Destinations : 1          Routes : 1
```

Destination/Mask	Proto	Pre	Cost	NextHop	Interface
3.0.0.0/24	Static	60	0	1.1.1.2	Vlan100

【相关命令】

- **display ip routing-table**（三层技术-IP 路由命令参考/IP 路由基础）
- **ipsec policy**
- **ipsec policy-template**

1.1.43 reverse-route preference

reverse-route preference 命令用来设置 IPsec 反向路由注入功能生成的静态路由的优先级。

undo reverse-route preference 命令用来恢复缺省情况。

【命令】

```
reverse-route preference number  
undo reverse-route preference
```

【缺省情况】

IPsec 反向路由注入功能生成的静态路由的优先级为 60。

【视图】

IPsec 安全策略视图

IPsec 安全策略模板视图

【缺省用户角色】

network-admin

【参数】

number: 静态路由的优先级，取值范围为 1~255。该值越小，优先级越高。

【使用指导】

若对静态路由优先级进行修改，会删除本策略协商生成的所有 IPsec SA 和根据这些 IPsec SA 生成的静态路由。

【举例】

配置 IPsec 反向路由注入功能生成的静态路由的优先级为 100。

```
<Sysname> system-view  
[Sysname] ipsec policy 1 1 isakmp  
[Sysname-ipsec-policy-isakmp-1-1] reverse-route preference 100
```

【相关命令】

- **ipsec policy**
- **ipsec policy-template**

1.1.44 reverse-route tag

reverse-route tag 命令用来设置 IPsec 反向路由注入功能生成的静态路由的 Tag 值。

undo reverse-route tag 命令用来恢复缺省情况。

【命令】

```
reverse-route tag tag-value  
undo reverse-route tag
```

【缺省情况】

IPsec 反向路由注入功能生成的静态路由的 Tag 值为 0。

【视图】

IPsec 安全策略视图

IPsec 安全策略模板视图

【缺省用户角色】

network-admin

【参数】

tag-value: 静态路由的 Tag 值，取值范围为 1~4294967295。

【使用指导】

本 Tag 值用于标识静态路由，以便在路由策略中根据 Tag 值对路由进行灵活的控制，若对静态路由 Tag 值进行修改，则会删除本策略协商生成的所有 IPsec SA 和根据这些 IPsec SA 生成的静态路由。

【举例】

配置 IPsec 反向路由注入功能生成的静态路由的 Tag 值为 50。

```
<Sysname>system-view
[Sysname] ipsec policy 1 1 isakmp
[Sysname-ipsec-policy-isakmp-1-1] reverse-route tag 50
```

【相关命令】

- **ipsec policy**
- **ipsec policy-template**

1.1.45 sa duration

sa duration 命令用来配置 IPsec SA 的生存时间。

undo sa duration 命令用来删除 IPsec SA 生存时间。

【命令】

```
sa duration { time-based seconds | traffic-based kilobytes }
undo sa duration { time-based | traffic-based }
```

【缺省情况】

IPsec 安全策略/IPsec 安全策略模板/IPsec 安全框架的 IPsec SA 生存时间为当前全局的 IPsec SA 生存时间。

【视图】

IPsec 安全策略视图

IPsec 安全策略模板视图

IPsec 安全框架视图

【缺省用户角色】

network-admin

【参数】

time-based *seconds*: 指定基于时间的生存时间，取值范围为 180~604800，单位为秒。

traffic-based kilobytes: 指定基于流量的生存时间，取值范围为 2560～4294967295，单位为千字节。

【使用指导】

当 IKE 协商 IPsec SA 时，如果采用的 IPsec 安全策略/IPsec 安全策略模板/IPsec 安全框架下未配置 IPsec SA 的生存时间，将采用全局的 IPsec SA 生存时间（通过命令 **ipsec sa global-duration** 设置）与对端协商。如果 IPsec 安全策略/IPsec 安全策略模板/IPsec 安全框架下配置了 IPsec SA 的生存时间，则优先使用 IPsec 安全策略/IPsec 安全策略模板/IPsec 安全框架下的配置值与对端协商。

IKE 为 IPsec 协商建立 IPsec SA 时，采用本地配置的生存时间和对端提议的 IPsec SA 生存时间中较小的一个。

【举例】

配置 IPsec 安全策略 policy1 的 IPsec SA 生存时间为两个小时，即 7200 秒。

```
<Sysname> system-view
[Sysname] ipsec policy policy1 100 isakmp
[Sysname-ipsec-policy-isakmp-policy1-100] sa duration time-based 7200
```

配置 IPsec 安全策略 policy1 的 IPsec SA 生存时间为 20M 字节，即传输 20480 千字节的流量后，当前的 IPsec SA 就过期。

```
<Sysname> system-view
[Sysname] ipsec policy policy1 100 isakmp
[Sysname-ipsec-policy-isakmp-policy1-100] sa duration traffic-based 20480
```

【相关命令】

- **display ipsec sa**
- **ipsec sa global-duration**

1.1.46 sa hex-key authentication

sa hex-key authentication 命令用来为手工创建的 IPsec SA 配置认证密钥。

undo sa hex-key authentication 命令用来删除指定的 IPsec SA 的认证密钥。

【命令】

```
sa hex-key authentication { inbound | outbound } { ah | esp } { cipher | simple }
string
undo sa hex-key authentication { inbound | outbound } { ah | esp }
```

【缺省情况】

未配置 IPsec SA 使用的认证密钥。

【视图】

IPsec 安全策略视图

IPsec 安全框架视图

【缺省用户角色】

network-admin

【参数】

inbound: 指定入方向 IPsec SA 使用的认证密钥。

outbound: 指定出方向 IPsec SA 使用的认证密钥。

ah: 指定 AH 协议。

esp: 指定 ESP 协议。

cipher: 以密文形式设置密钥。

simple: 以明文形式设置密钥，该密钥将以密文形式存储。

string: 明文密钥为十六进制格式的字符串，不区分大小写。对于不同的算法，密钥长度不同：HMAC-MD5 算法，密钥长度为 16 个字节；HMAC-SHA1 算法，密钥长度为 20 个字节。密文密钥为 1~85 个字符的字符串，区分大小写。

【使用指导】

此命令仅用于手工方式的 IPsec 安全策略及 IPsec 安全框架。

必须分别配置 **inbound** 和 **outbound** 两个方向的 IPsec SA 参数。

在 IPsec 隧道的两端设置的 IPsec SA 参数必须是完全匹配的。本端的入方向 IPsec SA 的认证密钥必须和对端的出方向 IPsec SA 的认证密钥一致；本端的出方向 IPsec SA 的认证密钥必须和对端的入方向 IPsec SA 的认证密钥一致。

对于要应用于 IPv6 路由协议的 IPsec 安全框架，还必须保证本端出方向 SA 的密钥和本端入方向 SA 的密钥一致。

在 IPsec 隧道的两端，应当以相同的方式输入密钥。如果一端以字符串方式输入密钥，另一端以十六进制方式输入密钥，则不能建立 IPsec 隧道。

在相同方向和协议的情况下，多次执行本命令，最后一次执行的命令生效。

【举例】

配置采用 AH 协议的入方向 IPsec SA 的认证密钥为明文 0x112233445566778899aabbccddeeff00；出方向 IPsec SA 的认证密钥为明文 0xaabbccddeeff001100aabbccddeeff00。

```
<Sysname> system-view
[Sysname] ipsec policy policy1 100 manual
[Sysname-ipsec-policy-manual-policy1-100] sa hex-key authentication inbound ah simple
112233445566778899aabbccddeeff00
[Sysname-ipsec-policy-manual-policy1-100] sa hex-key authentication outbound ah simple
aabbccddeeff001100aabbccddeeff00
```

【相关命令】

- **display ipsec sa**
- **sa string-key**

1.1.47 sa hex-key encryption

sa hex-key encryption 命令用来为手工创建的 IPsec SA 配置加密密钥。

undo sa hex-key encryption 命令用来删除指定的 IPsec SA 的加密密钥。

【命令】

sa hex-key encryption { inbound | outbound } esp { cipher | simple } string

```
undo sa hex-key encryption { inbound | outbound } esp
```

【缺省情况】

未配置 IPsec SA 使用的加密密钥。

【视图】

IPsec 安全策略视图

IPsec 安全框架视图

【缺省用户角色】

network-admin

【参数】

inbound: 指定入方向 IPsec SA 使用的加密密钥。

outbound: 指定出方向 IPsec SA 使用的加密密钥。

esp: 指定 ESP 协议。

cipher: 以密文形式设置密钥。

simple: 以明文形式设置密钥，该密钥将以密文形式存储。

string: 明文密钥为 16 进制格式的字符串，不区分大小写。对于不同的算法，密钥长度不同，详见 [表 1-10](#)。密文密钥为 1~117 个字符的字符串，区分大小写。

表1-10 算法与密钥长度对照表

算法	密钥长度（字节）
DES-CBC	8
3DES-CBC	24
AES128-CBC	16
AES192-CBC	24
AES256-CBC	32

【使用指导】

此命令仅用于手工方式的 IPsec 安全策略及 IPsec 安全框架。

必须分别配置 **inbound** 和 **outbound** 两个方向的 IPsec SA 参数。

在 IPsec 隧道的两端设置的 IPsec SA 参数必须是完全匹配的。本端的入方向 IPsec SA 的加密密钥必须和对端的出方向 IPsec SA 的加密密钥一致；本端的出方向 IPsec SA 的加密密钥必须和对端的入方向 IPsec SA 的加密密钥一致。

对于要应用于 IPv6 路由协议的 IPsec 安全框架，还必须保证本端出方向 SA 的密钥和本端入方向 SA 的密钥一致。

在 IPsec 隧道的两端，应当以相同的方式输入密钥。如果一端以字符串方式输入密钥，另一端以十六进制方式输入密钥，则不能建立 IPsec 隧道。

相同方向的情况下，多次执行本命令，最后一次执行的命令生效。

【举例】

配置采用 ESP 协议的入方向 IPsec SA 的加密算法的密钥为明文 0x1234567890abcdef；出方向 IPsec SA 的加密算法的密钥为明文 0xabcdefabcdef1234。

```
<Sysname> system-view
[Sysname] ipsec policy policy1 100 manual
[Sysname-ipsec-policy-manual-policy1-100] sa hex-key encryption inbound esp simple
1234567890abcdef
[Sysname-ipsec-policy-manual-policy1-100] sa hex-key encryption outbound esp simple
abcdefabcdef1234
```

【相关命令】

- **display ipsec sa**
- **sa string-key**

1.1.48 sa idle-time

sa idle-time 命令用来配置 IPsec SA 的空闲超时时间。在指定的超时时间内，没有流量使用的 IPsec SA 将被删除。

undo sa idle-time 命令用来恢复缺省情况。

【命令】

```
sa idle-time seconds
undo sa idle-time
```

【缺省情况】

IPsec 安全策略/IPsec 安全策略模板/IPsec 安全框架下的 IPsec SA 空闲超时时间为当前全局的 IPsec SA 空闲超时时间。

【视图】

IPsec 安全策略视图
IPsec 安全策略模板视图
IPsec 安全框架视图

【缺省用户角色】

network-admin

【参数】

seconds：IPsec SA 的空闲超时时间，取值范围为 60～86400，单位为秒。

【使用指导】

此功能只适用于 IKE 协商出的 IPsec SA，且只有通过 **ipsec sa idle-time** 命令开启空闲超时功能后，本功能才会生效。

如果 IPsec 安全策略/IPsec 安全策略模板/IPsec 安全框架视图下没有配置 IPsec SA 空闲超时时间，将采用全局的 IPsec SA 空闲超时时间（通过命令 **ipsec sa idle-time** 设置）决定 IPsec SA 是否空闲并进行删除。如果 IPsec 安全策略/IPsec 安全策略模板/IPsec 安全框架视图下配置了 IPsec SA 空闲超时时间，则优先使用 IPsec 安全策略/IPsec 安全策略模板/IPsec 安全框架视图下的配置值。

【举例】

```
# 配置 IPsec 安全策略的 IPsec SA 的空闲超时时间为 600 秒。  
<Sysname> system-view  
[Sysname] ipsec policy map 100 isakmp  
[Sysname-ipsec-policy-isakmp-map-100] sa idle-time 600
```

【相关命令】

- **display ipsec sa**
- **ipsec sa idle-time**

1.1.49 sa spi

sa spi 命令用来配置 IPsec SA 的 SPI。

undo sa spi 命令用来删除指定的 IPsec SA 的 SPI。

【命令】

```
sa spi { inbound | outbound } { ah | esp } spi-number  
undo sa spi { inbound | outbound } { ah | esp }
```

【缺省情况】

不存在 IPsec SA 的 SPI。

【视图】

IPsec 安全策略视图

IPsec 安全框架视图

【缺省用户角色】

network-admin

【参数】

inbound: 指定入方向 IPsec SA 的 SPI。

outbound: 指定出方向 IPsec SA 的 SPI。

ah: 指定 AH 协议。

esp: 指定 ESP 协议。

spi-number: IPsec SA 的安全参数索引，取值范围为 256～4294967295。

【使用指导】

此命令仅用于手工方式的 IPsec 安全策略以及 IPsec 安全框架。对于 IKE 协商方式的 IPsec 安全策略，IKE 将自动协商 IPsec SA 的参数并创建 IPsec SA，不需要手工设置 IPsec SA 的参数。

必须分别配置 **inbound** 和 **outbound** 两个方向 IPsec SA 的参数，且保证每一个方向上的 IPsec SA 的唯一性：对于出方向 IPsec SA，必须保证三元组（对端 IP 地址、安全协议、SPI）唯一；对于入方向 IPsec SA，必须保证 SPI 唯一。

在 IPsec 隧道的两端设置的 IPsec SA 参数必须是完全匹配的。本端的入方向 IPsec SA 的 SPI 必须和对端的出方向 IPsec SA 的 SPI 一样；本端的出方向 IPsec SA 的 SPI 必须和对端的入方向 IPsec SA 的 SPI 一样。

在配置应用于 IPv6 路由协议的 IPsec 安全框架时，还需要注意的是：

- 本端出方向 IPsec SA 的 SPI 必须和本端入方向 IPsec SA 的 SPI 保持一致；
- 同一个范围内的、所有设备上的 IPsec SA 的 SPI 均要保持一致。该范围与协议相关：对于 OSPFv3，是 OSPFv3 邻居之间或邻居所在的区域；对于 RIPng，是 RIPng 直连邻居之间或邻居所在的进程。

【举例】

配置入方向 IPsec SA 的 SPI 为 10000，出方向 IPsec SA 的 SPI 为 20000。

```
<Sysname> system-view
[Sysname] ipsec policy policy1 100 manual
[Sysname-ipsec-policy-manual-policy1-100] sa spi inbound ah 10000
[Sysname-ipsec-policy-manual-policy1-100] sa spi outbound ah 20000
```

【相关命令】

- **display ipsec sa**

1.1.50 sa string-key

sa string-key 命令用来为手工创建的 IPsec SA 配置字符串形式的密钥。

undo sa string-key 命令用来删除指定的 IPsec SA 的字符串形式的密钥。

【命令】

```
sa string-key { inbound | outbound } { ah | esp } { cipher | simple } string
undo sa string-key { inbound | outbound } { ah | esp }
```

【缺省情况】

未配置 IPsec SA 使用的密钥。

【视图】

IPsec 安全策略视图

IPsec 安全框架视图

【缺省用户角色】

network-admin

【参数】

inbound：指定入方向 IPsec SA 的密钥。

outbound：指定出方向 IPsec SA 的密钥。

ah：指定 AH 协议。

esp：指定 ESP 协议。

cipher：以密文形式设置密钥。

simple：以明文形式设置密钥，该密钥将以密文形式存储。

string：密钥字符串，区分大小写。明文密钥为 1~255 个字符的字符串，密文密钥为 1~373 个字符的字符串。对于不同的算法，系统会根据输入的字符串自动生成符合算法要求的密钥。对于 ESP 协议，系统会自动地同时生成认证算法的密钥和加密算法的密钥。

【使用指导】

此命令仅用于手工方式的 IPsec 安全策略及 IPsec 安全框架。

必须分别配置 **inbound** 和 **outbound** 两个方向 IPsec SA 的参数。

在 IPsec 隧道的两端设置的 IPsec SA 参数必须是完全匹配的。本端入方向 IPsec SA 的密钥必须和对端出方向 IPsec SA 的密钥一样；本端出方向 IPsec SA 的密钥必须和对端入方向 IPsec SA 的密钥一样。

在 IPsec 隧道的两端，应当以相同的方式输入密钥。如果一端以字符串方式输入密钥，另一端以十六进制方式输入密钥，则不能正确地建立 IPsec 隧道。

在配置应用于 IPv6 路由协议的 IPsec 安全框架时，还需要注意的是：

- 本端出方向 IPsec SA 的密钥必须和本端入方向 IPsec SA 的密钥保持一致；
- 同一个范围内的，所有设备上的 IPsec SA 的密钥均要保持一致。该范围内容与协议相关：对于 OSPFv3，是 OSPFv3 邻居之间或邻居所在的区域；对于 RIPng，是 RIPng 直连邻居之间或邻居所在的进程。

多次执行本命令，最后一次执行的命令生效。

【举例】

配置采用 AH 协议的入方向 IPsec SA 的密钥为明文字符串 **abcdef**；出方向 IPsec SA 的密钥为明文字符串 **efcdab**。

```
<Sysname> system-view
[Sysname] ipsec policy policy1 100 manual
[Sysname-ipsec-policy-manual-policy1-100] sa string-key inbound ah simple abcdef
[Sysname-ipsec-policy-manual-policy1-100] sa string-key outbound ah simple efcdab
```

在要应用于 IPv6 路由协议的安全策略中，配置采用 AH 协议的入方向 IPsec SA 的密钥为明文字符串 **abcdef**；出方向 IPsec SA 的密钥为明文字符串 **abcdef**。

```
<Sysname> system-view
[Sysname] ipsec policy policy1 100 manual
[Sysname-ipsec-policy-manual-policy1-100] sa string-key inbound ah simple abcdef
[Sysname-ipsec-policy-manual-policy1-100] sa string-key outbound ah simple abcdef
```

【相关命令】

- **display ipsec sa**
- **sa hex-key**

1.1.51 security acl

security acl 命令用来指定 IPsec 安全策略/IPsec 安全策略模板引用的 ACL。

undo security acl 命令用来恢复缺省情况。

【命令】

```
security acl [ ipv6 ] { acl-number | name acl-name } [ aggregation | per-host ]
undo security acl
```

【缺省情况】

IPsec 安全策略/IPsec 安全策略模板未引用 ACL。

【视图】

IPsec 安全策略视图

IPsec 安全策略模板视图

【缺省用户角色】

network-admin

【参数】

ipv6: 指定 IPv6 ACL。

acl-number: ACL 编号，取值范围为 3000~3999。

name acl-name: ACL 名称，为 1~63 个字符的字符串，不区分大小写。

aggregation: 指定 IPsec 安全策略的数据流保护方式为聚合方式。不支持对 IPv6 数据流采用该保护方式。

per-host: 指定 IPsec 安全策略的数据流保护方式为主机方式。

【使用指导】

对于 IKE 协商方式的 IPsec 安全策略，数据流的保护方式包括以下几种：

- **标准方式**：一条隧道保护一条数据流。ACL 中的每一个规则对应的数据流都会由一条单独创建的隧道来保护。不指定 **aggregation** 和 **per-host** 参数的情况下，缺省采用此方式。
- **聚合方式**：一条隧道保护 ACL 中定义的所有数据流。ACL 中的所有规则对应的数据流只会由一条创建的隧道来保护。对于聚合方式和标准方式都支持的设备，聚合方式仅用于和老版本的设备互通。
- **主机方式**：一条隧道保护一条主机到主机的数据流。ACL 中的每一个规则对应的不同主机之间的数据流，都会由一条单独创建的隧道来保护。这种方式下，受保护的网段之间存在多条数据流的情况下，将会消耗更多的系统资源。

手工方式的 IPsec 安全策略缺省使用聚合方式，且仅支持聚合方式；IKE 协商方式的 IPsec 安全策略中可以通过配置来选择不同的保护方式。

【举例】

配置 IPsec 安全策略引用 IPv4 高级 ACL 3001。

```
<Sysname> system-view
[Sysname] acl advanced 3001
[Sysname-acl-ipv4-adv-3001] rule permit tcp source 10.1.1.0 0.0.0.255 destination 10.1.2.0 0.0.0.255
[Sysname-acl-ipv4-adv-3001] quit
[Sysname] ipsec policy policy1 100 manual
[Sysname-ipsec-policy-manual-policy1-100] security acl 3001
```

配置 IPsec 安全策略引用 IPv4 高级 ACL 3002，并设置数据流保护方式为聚合方式。

```
<Sysname> system-view
[Sysname] acl advanced 3002
[Sysname-acl-ipv4-adv-3002] rule 0 permit ip source 10.1.2.1 0.0.0.255 destination 10.1.2.2 0.0.0.255
[Sysname-acl-ipv4-adv-3002] rule 1 permit ip source 10.1.3.1 0.0.0.255 destination 10.1.3.2 0.0.0.255
[Sysname-acl-ipv4-adv-3002] quit
```

```
[Sysname] ipsec policy policy2 1 isakmp
[Sysname-ipsec-policy-isakmp-policy2-1] security acl 3002 aggregation
```

【相关命令】

- `display ipsec sa`
- `display ipsec tunnel`

1.1.52 snmp-agent trap enable ipsec

`snmp-agent trap enable ipsec` 命令用来开启 IPsec 告警功能。

`undo snmp-agent trap enable ipsec` 命令用来关闭指定的 IPsec 告警功能。

【命令】

```
snmp-agent trap enable ipsec [ auth-failure | decrypt-failure |
encrypt-failure | global | invalid-sa-failure | no-sa-failure | policy-add |
policy-attach | policy-delete | policy-detach | tunnel-start | tunnel-stop]
*

undo snmp-agent trap enable ipsec [ auth-failure | decrypt-failure |
encrypt-failure | global | invalid-sa-failure | no-sa-failure | policy-add |
policy-attach | policy-delete | policy-detach | tunnel-start | tunnel-stop]
*
```

【缺省情况】

IPsec 的所有告警功能均处于关闭状态。

【视图】

系统视图

【缺省用户角色】

network-admin

【参数】

auth-failure: 表示认证失败时的告警功能。

decrypt-failure: 表示解密失败时的告警功能。

encrypt-failure: 表示加密失败时的告警功能。

global: 表示全局告警功能。

invalid-sa-failure: 表示无效 SA 的告警功能。

no-sa-failure: 表示无法查找到 SA 时的告警功能。

policy-add: 表示添加 IPsec 安全策略时的告警功能。

policy-attach: 表示将 IPsec 安全策略应用到接口时的告警功能。

policy-delete: 表示删除 IPsec 安全策略时的告警功能。

policy-detach: 表示将 IPsec 安全策略从接口下删除时的告警功能。

tunnel-start: 表示创建 IPsec 隧道时的告警功能。

tunnel-stop: 表示删除 IPsec 隧道时的告警功能。

【使用指导】

如果不指定任何参数，则表示开启或关闭所有类型的 IPsec 告警功能。

如果希望生成并输出某种类型的 IPsec 告警信息，则需要保证 IPsec 的全局告警功能以及相应类型的告警功能均处于开启状态。

【举例】

开启全局 IPsec Trap 告警。

```
<Sysname> system-view  
[Sysname] snmp-agent trap enable ipsec global
```

开启创建 IPsec 隧道时的告警功能。

```
[Sysname] snmp-agent trap enable ipsec tunnel-start
```

1.1.53 tfc enable

tfc enable 命令用来开启 TFC（Traffic Flow Confidentiality）填充功能。

undo tfc enable 命令用来关闭 TFC 填充功能。

【命令】

tfc enable

undo tfc enable

【缺省情况】

TFC 填充功能处于关闭状态。

【视图】

IPsec 安全策略视图

IPsec 安全策略模板视图

【缺省用户角色】

network-admin

【使用指导】

TFC 填充功能可隐藏原始报文的长度，但可能对报文的加封装及解封装处理性能稍有影响，且仅对于使用 ESP 协议以传输模式封装的 UDP 报文以及使用 ESP 协议以隧道模式封装的原始 IP 报文生效。

【举例】

指定 IPsec 安全策略 policy1 中开启 TFC 填充功能。

```
<Sysname> system-view  
[Sysname] ipsec policy policy1 10 isakmp  
[Sysname-ipsec-policy-isakmp-policy1-10] tfc enable
```

【相关命令】

- **display ipsec ipv6-policy**
- **display ipsec policy**

1.1.54 transform-set

transform-set 命令用来指定 IPsec 安全策略/IPsec 安全策略模板/IPsec 安全框架所引用的 IPsec 安全提议。

undo transform-set 命令用来取消 IPsec 安全策略/IPsec 安全策略模板/IPsec 安全框架引用的 IPsec 安全提议。

【命令】

```
transform-set transform-set-name<1-6>  
undo transform-set [ transform-set-name ]
```

【缺省情况】

IPsec 安全策略/IPsec 安全策略模板/IPsec 安全框架未引用 IPsec 安全提议。

【视图】

IPsec 安全策略视图
IPsec 安全策略模板视图
IPsec 安全框架视图

【缺省用户角色】

network-admin

【参数】

transform-set-name<1-6>: IPsec 安全提议的名称，为 1~63 个字符的字符串，不区分大小写。<1-6>表示前面的参数最多可以输入 6 次。

【使用指导】

对于手工方式的 IPsec 安全策略，只能引用一个 IPsec 安全提议。多次执行本命令，最后一次执行的命令生效。

对于 IKE 协商方式的 IPsec 安全策略，一条 IPsec 安全策略最多可以引用六个 IPsec 安全提议。IKE 协商过程中，IKE 将会在隧道两端配置的 IPsec 安全策略中查找能够完全匹配的 IPsec 安全提议。如果 IKE 在两端找不到完全匹配的 IPsec 安全提议，则 SA 不能协商成功，需要被保护的报文将被丢弃。

若不指定任何参数，则 **undo transform-set** 命令表示删除所有引用的 IPsec 安全提议。

【举例】

```
# 配置 IPsec 安全策略引用名称为 prop1 的 IPsec 安全提议。  
<Sysname> system-view  
[Sysname] ipsec transform-set prop1  
[Sysname-ipsec-transform-set-prop1] quit  
[Sysname] ipsec policy policy1 100 manual  
[Sysname-ipsec-policy-manual-policy1-100] transform-set prop1
```

【相关命令】

- **ipsec { ipv6-policy | policy }**
- **ipsec profile**
- **ipsec transform-set**

2 IKE



说明

设备运行于 FIPS 模式时，本特性部分配置相对于非 FIPS 模式有所变化，具体差异请见本文相关描述。有关 FIPS 模式的详细介绍请参见“安全配置指导”中的“FIPS”。

2.1 IKE配置命令

2.1.1 authentication-algorithm

authentication-algorithm 命令用来指定 IKE 提议使用的认证算法。

undo authentication-algorithm 命令用来恢复缺省情况。

【命令】

非 FIPS 模式下：

```
authentication-algorithm { md5 | sha | sha256 | sha384 | sha512 }
```

```
undo authentication-algorithm
```

FIPS 模式下：

```
authentication-algorithm { sha | sha256 | sha384 | sha512 }
```

```
undo authentication-algorithm
```

【缺省情况】

非 FIPS 模式下：

IKE 提议使用的认证算法为 HMAC-SHA1

FIPS 模式下：

IKE 提议使用的认证算法为 HMAC-SHA256。

【视图】

IKE 提议视图

【缺省用户角色】

network-admin

【参数】

md5：指定认证算法为 HMAC-MD5。

sha：指定认证算法为 HMAC-SHA1。

sha256：指定认证算法为 HMAC-SHA256。

sha384：指定认证算法为 HMAC-SHA384。

sha512：指定认证算法为 HMAC-SHA512。

【举例】

指定 IKE 提议 1 的认证算法为 HMAC-SHA1。

```
<Sysname> system-view
[Sysname] ike proposal 1
[Sysname-ike-proposal-1] authentication-algorithm sha
```

【相关命令】

- **display ike proposal**

2.1.2 authentication-method

authentication-method 命令用来指定 IKE 提议使用的认证方法。

undo authentication-method 命令用来恢复缺省情况。

【命令】

```
authentication-method { dsa-signature | pre-share | rsa-signature }
undo authentication-method
```

【缺省情况】

IKE 提议使用预共享密钥的认证方法。

【视图】

IKE 提议视图

【缺省用户角色】

network-admin

【参数】

dsa-signature: 指定认证方法为 DSA 数字签名方法。

pre-share: 指定认证方法为预共享密钥方法。

rsa-signature: 指定认证方法为 RSA 数字签名方法。

【使用指导】

预共享密钥认证机制简单、不需要证书，常在小型组网环境中使用；数字签名认证安全性更高，常在“中心—分支”模式的组网环境中使用。例如，在“中心—分支”组网中使用预共享密钥认证进行 IKE 协商时，中心侧可能需要为每个分支配置一个预共享密钥，当分支很多时，配置会很复杂，而使用数字签名认证时中心只需配置一个 PKI 域。

协商双方必须有匹配的认证方法。

如果指定认证方法为 RSA 数字签名方法或者 DSA 数字签名方法，则还必须保证对端从 CA（证书认证机构）获得数字证书。

如果指定认证方法为预共享密钥方法，必须使用 **pre-shared-key** 命令在两端配置相同的预共享密钥。

【举例】

指定 IKE 提议 1 的认证方法为预共享密钥。

```
<Sysname> system-view
[Sysname] ike proposal 1
```

```
[Sysname-ike-proposal-1] authentication-method pre-share
```

【相关命令】

- **display ike proposal**
- **ike keychain**
- **pre-shared-key**

2.1.3 certificate domain

certificate domain 命令用来指定 IKE 协商采用数字签名认证时使用的 PKI 域。

undo certificate domain 命令用来取消指定 IKE 协商时使用的 PKI 域。

【命令】

```
certificate domain domain-name  
undo certificate domain domain-name
```

【缺省情况】

未指定用于 IKE 协商的 PKI 域。

【视图】

IKE profile 视图

【缺省用户角色】

network-admin

【参数】

domain-name: PKI 域的名称，为 1~31 个字符的字符串，不区分大小写。

【使用指导】

可通过多次执行本命令指定多个 PKI 域，一个 IKE profile 中最多可以引用六个 PKI 域。如果在 IKE profile 中指定了 PKI 域，则使用指定的 PKI 域发送本端证书请求、验证对端证书请求、发送本端证书、验证对端证书、进行数字签名。如果 IKE profile 中没有指定 PKI 域，则使用设备上配置的 PKI 域进行以上证书相关的操作。

IKE 可以通过 PKI 自动获取 CA 证书、自动申请证书，对这种情况，有几点需要说明：

- 对于发起方：若在 IKE profile 中指定了 PKI 域，且 PKI 域中的证书申请为自动申请方式，则发起方会自动获取 CA 证书；若在 IKE profile 中没有指定 PKI 域，则发起方不会自动获取 CA 证书，需要手动获取 CA 证书。
- 对于响应方：第一阶段采用主模式的 IKE 协商时，响应方不会自动获取 CA 证书，需要手动获取 CA 证书；第一阶段采用野蛮模式的 IKE 协商时，若响应方找到了匹配的 IKE profile 并且 IKE profile 下指定了 PKI 域，且 PKI 域中的证书申请为自动申请方式，则会自动获取 CA 证书；否则，响应方不会自动获取 CA 证书，需要手动获取 CA 证书。
- 在 IKE 协商过程中先自动获取 CA 证书，再自动申请证书。若 CA 证书存在，则不获取 CA 证书，直接自动申请证书。

【举例】

在 IKE profile 1 中指定 IKE 协商时使用的 PKI 域。

```
<Sysname> system-view
```

```
[Sysname] ike profile 1
[Sysname-ike-profile-1] certificate domain abc
```

【相关命令】

- **authentication-method**
- **pki domain**（安全命令参考/PKI）

2.1.4 description

description 命令用来配置 IKE 提议的描述信息。

undo description 命令用来恢复缺省情况。

【命令】

```
description text
undo description
```

【缺省情况】

不存在 IKE 提议的描述信息。

【视图】

IKE 提议视图

【缺省用户角色】

network-admin

【参数】

text: IKE 提议的描述信息，为 1~80 个字符的字符串，区分大小写。

【使用指导】

当系统中存在多个 IKE 提议时，可通过配置相应的描述信息来有效区分不同的 IKE 提议。

【举例】

配置序号为 1 的 IKE 提议的描述信息为 test。

```
<Sysname> system-view
[Sysname] ike proposal 1
[Sysname-ike-proposal-1] description test
```

2.1.5 dh

dh 命令用来配置 IKE 阶段 1 密钥协商时所使用的 DH 密钥交换参数。

undo dh 命令用来恢复缺省情况。

【命令】

非 FIPS 模式下：

```
dh { group1 | group14 | group2 | group24 | group5 }
undo dh
```

FIPS 模式下：

```
dh group14
```

undo dh

【缺省情况】

非 FIPS 模式下：

IKE 提议使用的 DH 密钥交换参数为 **group1**，即 768-bit 的 Diffie-Hellman group。

FIPS 模式下：

IKE 提议使用的 DH 密钥交换参数为 **group14**，即 2048-bit 的 Diffie-Hellman group。

【视图】

IKE 提议视图

【缺省用户角色】

network-admin

【参数】

group1：指定阶段 1 密钥协商时采用 768-bit 的 Diffie-Hellman group。

group14：指定阶段 1 密钥协商时采用 2048-bit 的 Diffie-Hellman group。

group2：指定阶段 1 密钥协商时采用 1024-bit 的 Diffie-Hellman group。

group24：指定阶段 1 密钥协商时采用含 256-bit 的 sub-group 的 2048-bit Diffie-Hellman group。

group5：指定阶段 1 密钥协商时采用 1536-bit 的 Diffie-Hellman group。

【使用指导】

group1 提供了最低的安全性，但是处理速度最快。**group24** 提供了最高的安全性，但是处理速度最慢。其它的 Diffie-Hellman group 随着其位数的增加提供更高的安全性，但是处理速度会相应减慢。请根据实际组网环境中对安全性和性能的要求选择合适的 Diffie-Hellman group。

【举例】

指定 IKE 提议 1 使用 2048-bit 的 Diffie-Hellman group。

```
<Sysname> system-view
[Sysname] ike proposal 1
[Sysname-ike-proposal-1] dh group14
```

【相关命令】

- **display ike proposal**

2.1.6 display ike proposal

display ike proposal 命令用来显示所有 IKE 提议的配置信息。

【命令】

display ike proposal

【视图】

任意视图

【缺省用户角色】

network-admin

network-operator

【使用指导】

IKE 提议按照优先级的先后顺序显示。如果没有配置任何 IKE 提议，则只显示缺省的 IKE 提议。

【举例】

显示 IKE 提议的配置信息。

```
<Sysname> display ike proposal
Priority Authentication Authentication Encryption Diffie-Hellman Duration
          method      algorithm      algorithm      group      (seconds)
-----
1         RSA-SIG      MD5          DES-CBC      Group 1      5000
11        PRE-SHARED-KEY MD5          DES-CBC      Group 1      50000
default   PRE-SHARED-KEY   SHA1         DES-CBC      Group 1      86400
```

表2-1 display ike proposal 命令显示信息描述表

字段	描述
Priority	IKE提议的优先级
Authentication method	IKE提议使用的认证方法，包括： <ul style="list-style-type: none">• PRE-SHARED-KEY：预共享密钥• RSA-SIG：RSA 签名• DSA-SIG：DSA 签名
Authentication algorithm	IKE提议使用的认证算法，包括： <ul style="list-style-type: none">• MD5：HMAC-MD5 算法• SHA1：HMAC-SHA1 算法• SHA256：HMAC-SHA256 算法• SHA384：HMAC-SHA384 算法• SHA512：HMAC-SHA512 算法
Encryption algorithm	IKE提议使用的加密算法，包括： <ul style="list-style-type: none">• 3DES-CBC：168 位 CBC 模式的 3DES 算法• AES-CBC-128：128 位 CBC 模式的 AES 算法• AES-CBC-192：192 位 CBC 模式的 AES 算法• AES-CBC-256：256 位 CBC 模式的 AES 算法• DES-CBC：56 位 CBC 模式的 DES 算法
Diffie-Hellman group	IKE阶段1密钥协商时所使用的DH密钥交换参数，包括： <ul style="list-style-type: none">• Group 1：DH group1• Group 2：DH group2• Group 5：DH group5• Group 14：DH group14• Group 24：DH group24
Duration (seconds)	IKE提议中指定的IKE SA存活时间，单位为秒

【相关命令】

- `ike proposal`

2.1.7 `display ike sa`

`display ike sa` 命令用来显示 IKE SA 的信息。

【命令】

```
display ike sa [ verbose [ connection-id connection-id | remote-address
[ ipv6 ] remote-address ] ]
```

【视图】

任意视图

【缺省用户角色】

network-admin
network-operator

【参数】

verbose: 显示 IKE SA 的详细信息。
connection-id connection-id: 按照连接标识符显示 IKE SA 的详细信息，取值范围为 1~2000000000。
remote-address: 显示指定对端 IP 地址的 IKE SA 的详细信息。
ipv6: 指定 IPv6 地址。
remote-address: 对端的 IP 地址。

【使用指导】

若不指定任何参数，则显示所有 IKE SA 的摘要信息。

【举例】

```
# 显示所有 IKE SA 的摘要信息。
<Sysname> display ike sa
  Connection-ID  Remote          Flag      DOI
-----
      1          202.38.0.2      RD        IPsec
Flags:
RD--READY RL--REPLACED FD-FADING RK-REKEY
```

表2-2 `display ike sa` 命令显示信息描述表

字段	描述
Connection-ID	IKE SA 的标识符
Remote	此IKE SA的对端的IP地址

字段	描述
Flags	IKE SA的状态，包括： <ul style="list-style-type: none"> RD--READY: 表示此 IKE SA 已建立成功 RL--REPLACED: 表示此 IKE SA 已经被新的 IKE SA 代替，一段时间后将被删除 FD-FADING: 表示此 IKE SA 正在接近超时时间，目前还在使用，但即将被删除 RK-REKEY: 表示此 IKE SA 是 Rekey SA Unknown: 表示 IKE 协商的状态未知
DOI	IKE SA所属解释域，包括： <ul style="list-style-type: none"> IPSEC: 表示此 IKE SA 使用的 DOI 为 IPSEC DOI

显示当前 IKE SA 的详细信息。

```
<Sysname> display ike sa verbose
-----
Connection ID: 2
Outside VPN:
Inside VPN:
Profile: prof1
Transmitting entity: Initiator
-----
Local IP: 4.4.4.4
Local ID type: IPV4_ADDR
Local ID: 4.4.4.4

Remote IP: 4.4.4.5
Remote ID type: IPV4_ADDR
Remote ID: 4.4.4.5

Authentication-method: PRE-SHARED-KEY
Authentication-algorithm: SHA1
Encryption-algorithm: AES-CBC-128

Life duration(sec): 86400
Remaining key duration(sec): 86379
Exchange-mode: Main
Diffie-Hellman group: Group 1
NAT traversal: Not detected

Extend authentication: Enabled
Assigned IP address: 192.168.2.1
```

显示目的地址为 4.4.4.5 的 IKE SA 的详细信息。

```
<Sysname> display ike sa verbose remote-address 4.4.4.5
-----
Connection ID: 2
Outside VPN:
Inside VPN:
```

```

Profile: prof1
Transmitting entity: Initiator
-----
Local IP: 4.4.4.4
Local ID type: IPV4_ADDR
Local ID: 4.4.4.4

Remote IP: 4.4.4.5
Remote ID type: IPV4_ADDR
Remote ID: 4.4.4.5

Authentication-method: PRE-SHARED-KEY
Authentication-algorithm: SHA1
Encryption-algorithm: AES-CBC-128

Life duration(sec): 86400
Remaining key duration(sec): 86379
Exchange-mode: Main
Diffie-Hellman group: Group 1
NAT traversal: Not detected

Extend authentication: Enabled
Assigned IP address: 192.168.2.1

```

表2-3 display ike sa verbose 命令显示信息描述表

字段	描述
Connection ID	IKE SA的标识符
Outside VPN	（暂不支持）接收报文的接口所属的MPLS L3VPN的VPN实例名称
Inside VPN	（暂不支持）被保护数据所属的MPLS L3VPN的VPN实例名称
Profile	IKE SA协商过程中匹配到的IKE profile的名称，如果协商过程中没有匹配到任何profile，则该字段不会显示任何KE profile名称
Transmitting entity	IKE协商中的实体角色，包括： <ul style="list-style-type: none"> Initiator：发起方 Responder：响应方
Local IP	本端安全网关的IP地址
Local ID type	本端安全网关的身份信息类型
Local ID	本端安全网关的身份信息
Remote IP	对端安全网关的IP地址
Remote ID type	对端安全网关的身份信息类型
Remote ID	对端安全网关的身份信息

字段	描述
Authentication-method	IKE提议使用的认证方法，包括： <ul style="list-style-type: none"> • PRE-SHARED-KEY: 预共享密钥 • RSA-SIG: RSA 签名 • DSA-SIG: DSA 签名
Authentication-algorithm	IKE提议使用的认证算法，包括： <ul style="list-style-type: none"> • MD5: HMAC-MD5 算法 • SHA1: HMAC-SHA1 算法 • SHA256: HMAC-SHA256 算法 • SHA384: HMAC-SHA384 算法 • SHA512: HMAC-SHA512 算法
Encryption-algorithm	IKE提议使用的加密算法，包括： <ul style="list-style-type: none"> • 3DES-CBC: 168 位 CBC 模式的 3DES 算法 • AES-CBC-128: 128 位 CBC 模式的 AES 算法 • AES-CBC-192: 192 位 CBC 模式的 AES 算法 • AES-CBC-256: 256 位 CBC 模式的 AES 算法 • DES-CBC: 56 位 CBC 模式的 DES 算法 •
Life duration(sec)	IKE SA的存活时间，单位为秒
Remaining key duration(sec)	IKE SA的剩余存活时间，单位为秒
Exchange-mode	IKE第一阶段的协商模式，包括： <ul style="list-style-type: none"> • Main: 主模式 • Aggressive: 野蛮模式
Diffie-Hellman group	IKE第一阶段密钥协商时所使用的DH密钥交换参数，包括： <ul style="list-style-type: none"> • Group 1: DH group1 • Group 2: DH group2 • Group 5: DH group5 • Group 14: DH group14 • Group 24: DH group24
NAT traversal	是否检测到协商双方之间存在NAT网关设备
Extend authentication	是否开启扩展认证： <ul style="list-style-type: none"> • Enabled: 开启 • Disabled: 关闭
Assigned IP address	本端分配给对端的IP地址，如果没有分配则不显示

2.1.8 display ike statistics

display ike statistics 命令用来显示 IKE 的统计信息。

【命令】

display ike statistics

【视图】

任意视图

【缺省用户角色】

network-admin
network-operator

【举例】

```
# 显示 IKE 的统计信息。
<Sysname> display ike statistics
IKE statistics:
  No matching proposal: 0
  Invalid ID information: 0
  Unavailable certificate: 0
  Unsupported DOI: 0
  Unsupported situation: 0
  Invalid proposal syntax: 0
  Invalid SPI: 0
  Invalid protocol ID: 0
  Invalid certificate: 0
  Authentication failure: 0
  Invalid flags: 0
  Invalid message id: 0
  Invalid cookie: 0
  Invalid transform ID: 0
  Malformed payload: 0
  Invalid key information: 0
  Invalid hash information: 0
  Unsupported attribute: 0
  Unsupported certificate type: 0
  Invalid certificate authority: 0
  Invalid signature: 0
  Unsupported exchange type: 0
  No available SA: 1
  Retransmit timeout: 0
  Not enough memory: 0
  Enqueue fails: 0
```

表2-4 display ike statistics 命令显示信息描述表

字段	描述
No matching proposal	提议不匹配
Invalid ID information	无效的ID信息
Unavailable certificate	本地未发现此证书

字段	描述
Unsupported DOI	不支持的DOI
Unsupported situation	不支持的形式
Invalid proposal syntax	无效的提议语法
Invalid SPI	无效的SPI
Invalid protocol ID	无效的协议ID
Invalid certificate	无效的证书
Authentication failure	认证失败
Invalid flags	无效的标记
Invalid message id	无效的消息ID
Invalid cookie	无效的cookie
Invalid transform ID	无效的transform ID
Malformed payload	畸形载荷
Invalid key information	无效的密钥信息
Invalid hash information	无效的hash信息
Unsupported attribute	不支持的属性
Unsupported certificate type	不支持的证书类型
Invalid certificate authority	无效的证书授权
Invalid signature	无效的签名
Unsupported exchange type	不支持的交换类型
No available SA	没有可用的SA
Retransmit timeout	重传超时
Not enough memory	内存不足
Enqueue fails	入队列失败

【相关命令】

- `reset ike statistics`

2.1.9 dpd

`dpd` 命令用来配置 IKE DPD 功能。

`undo dpd` 命令用来关闭 IKE DPD 功能。

【命令】

```
dpd interval interval [ retry seconds ] { on-demand | periodic }
```

```
undo dpd interval
```

【缺省情况】

IKE DPD 功能处于关闭状态。

【视图】

IKE profile 视图

【缺省用户角色】

network-admin

【参数】

interval interval: 指定触发 IKE DPD 探测的时间间隔，取值范围为 1~300，单位为秒。对于按需探测模式，指定经过多长时间没有从对端收到 IPsec 报文，则触发一次 DPD 探测；对于定时探测模式，指触发一次 DPD 探测的时间间隔。

retry seconds: 指定 DPD 报文的重传时间间隔，取值范围为 1~60，单位为秒。缺省情况下，DPD 报文的重传时间间隔为 5 秒。

on-demand: 指定按需探测模式，根据流量来探测对端是否存活，在本端发送用户报文时，如果发现当前距离最后一次收到对端报文的时间超过指定的触发 IKE DPD 探测的时间间隔，则触发 DPD 探测。

periodic: 指定定时探测模式，按照触发 IKE DPD 探测的时间间隔定时探测对端是否存活。

【使用指导】

IKE DPD 有两种模式：按需探测模式和定时探测模式。一般若无特别要求，建议使用按需探测模式，在此模式下，仅在本端需要发送报文时，才会触发探测；如果需要尽快地检测出对端的状态，则可以使用定时探测模式。在定时探测模式下工作，会消耗更多的带宽和计算资源，因此当设备与大量的 IKE 对端通信时，应优先考虑使用按需探测模式。

如果 IKE profile 视图下和系统视图下都配置了 IKE DPD 功能，则 IKE profile 视图下的 DPD 配置生效，如果 IKE profile 视图下没有配置 IKE DPD 功能，则采用系统视图下的 DPD 配置。

建议配置的 **interval** 时间大于 **retry** 时间，使得直到当前 DPD 探测结束才可以触发下一次 DPD 探测，在重传 DPD 报文过程中不会触发新的 DPD 探测。

【举例】

为 IKE profile 1 配置 IKE DPD 功能，指定若 10 秒内没有从对端收到 IPsec 报文，则触发 IKE DPD 探测，DPD 请求报文的重传时间间隔为 5 秒，探测模式为按需探测。

```
<Sysname> system-view
[Sysname] ike profile 1
[Sysname-ike-profile-1] dpd interval 10 retry 5 on-demand
```

【相关命令】

- **ike dpd**

2.1.10 encryption-algorithm

encryption-algorithm 命令用来指定 IKE 提议使用的加密算法。

undo encryption-algorithm 命令用来恢复缺省情况。

【命令】

非 FIPS 模式下：

```
encryption-algorithm { 3des-cbc | aes-cbc-128 | aes-cbc-192 | aes-cbc-256 |  
des-cbc }
```

```
undo encryption-algorithm
```

FIPS 模式下：

```
encryption-algorithm { aes-cbc-128 | aes-cbc-192 | aes-cbc-256 }
```

```
undo encryption-algorithm
```

【缺省情况】

非 FIPS 模式下：

IKE 提议使用的加密算法为 **des-cbc**，即 CBC 模式的 56-bit DES 加密算法。

FIPS 模式下：

IKE 提议使用的加密算法为 **aes-cbc-128**，即 CBC 模式的 AES 算法，AES 算法采用 128 比特的密钥进行加密。

【视图】

IKE 提议视图

【缺省用户角色】

network-admin

【参数】

3des-cbc：指定 IKE 安全提议采用的加密算法为 CBC 模式的 3DES 算法，3DES 算法采用 168 比特的密钥进行加密。

aes-cbc-128：指定 IKE 安全提议采用的加密算法为 CBC 模式的 AES 算法，AES 算法采用 128 比特的密钥进行加密。

aes-cbc-192：指定 IKE 安全提议采用的加密算法为 CBC 模式的 AES 算法，AES 算法采用 192 比特的密钥进行加密。

aes-cbc-256：指定 IKE 安全提议采用的加密算法为 CBC 模式的 AES 算法，AES 算法采用 256 比特的密钥进行加密。

des-cbc：指定 IKE 安全提议采用的加密算法为 CBC 模式的 DES 算法，DES 算法采用 56 比特的密钥进行加密。

【举例】

指定 IKE 提议 1 的加密算法为 128 比特的 CBC 模式的 AES。

```
<Sysname> system-view
```

```
[Sysname] ike proposal 1
```

```
[Sysname-ike-proposal-1] encryption-algorithm aes-cbc-128
```

【相关命令】

- **display ike proposal**

2.1.11 exchange-mode

exchange-mode 命令用来选择 IKE 第一阶段的协商模式。

undo exchange-mode 命令用来恢复缺省情况。

【命令】

非 FIPS 模式下：

```
exchange-mode { aggressive | main }
```

```
undo exchange-mode
```

FIPS 模式下：

```
exchange-mode main
```

```
undo exchange-mode
```

【缺省情况】

IKE 第一阶段的协商模式为主模式。

【视图】

IKE profile 视图

【缺省用户角色】

network-admin

【参数】

aggressive：野蛮模式。

main：主模式。

【使用指导】

当本端的 IP 地址为自动获取（如本端用户为拨号方式，IP 地址为动态分配），且采用预共享密钥认证方式时，建议将本端的协商模式配置为野蛮模式。

【举例】

配置 IKE 第一阶段协商使用主模式。

```
<Sysname> system-view
```

```
[Sysname] ike profile 1
```

```
[Sysname-ike-profile-1] exchange-mode main
```

【相关命令】

- **display ike proposal**

2.1.12 ike dpd

ike dpd 命令用来配置全局 IKE DPD 功能。

undo ike dpd 命令用来关闭全局 IKE DPD 功能。

【命令】

```
ike dpd interval interval [ retry seconds ] { on-demand | periodic }
```

```
undo ike dpd interval
```

【缺省情况】

全局 IKE DPD 功能处于关闭状态。

【视图】

系统视图

【缺省用户角色】

network-admin

【参数】

interval interval: 指定触发 IKE DPD 探测的时间间隔，取值范围为 1~300，单位为秒。对于按需探测模式，指定经过多长时间没有从对端收到 IPsec 报文，则触发一次 DPD 探测；对于定时探测模式，指触发一次 DPD 探测的时间间隔。

retry seconds: 指定 DPD 报文的重传时间间隔，取值范围为 1~60，单位为秒，缺省值为 5 秒。

on-demand: 指定按需探测模式，根据流量来探测对端是否存活，在本端发送 IPsec 报文时，如果发现当前距离最后一次收到对端报文的时间超过指定的触发 IKE DPD 探测的时间间隔（即通过 *interval* 指定的时间），则触发 DPD 探测。

periodic: 指定定时探测模式，按照触发 IKE DPD 探测的时间间隔（即通过 *interval* 指定的时间）定时探测对端是否存活。

【使用指导】

IKE DPD 有两种模式：按需探测模式和定时探测模式。一般若无特别要求，建议使用按需探测模式，在此模式下，仅在本端需要发送报文时，才会触发探测；如果需要尽快地检测出对端的状态，则可以使用定时探测模式。在定时探测模式下工作，会消耗更多的带宽和计算资源，因此当设备与大量的 IKE 对端通信时，应优先考虑使用按需探测模式。

如果 IKE profile 视图下和系统视图下都配置了 DPD 探测功能，则 IKE profile 视图下的 DPD 配置生效，如果 IKE profile 视图下没有配置 DPD 探测功能，则采用系统视图下的 DPD 配置。

建议配置的 **interval** 大于 **retry**，使得直到当前 DPD 探测结束才可以触发下一次 DPD 探测，在重传 DPD 报文的过程中不触发新的 DPD 探测。

【举例】

配置流量触发 IKE DPD 探测间隔时间为 10 秒，重传时间间隔为 5 秒，探测模式为按需探测。

```
<Sysname> system-view
[Sysname] ike dpd interval 10 retry 5 on-demand
```

【相关命令】

- **dpd**

2.1.13 ike identity

ike identity 命令用来配置本端身份信息，用于在 IKE 认证协商阶段向对端标识自己的身份。

undo ike identity 命令用来恢复缺省情况。

【命令】

```
ike identity { address { ipv4-address | ipv6 ipv6-address } | dn | fqdn  
[ fqdn-name ] | user-fqdn [ user-fqdn-name ] }  
undo ike identity
```

【缺省情况】

使用 IP 地址标识本端的身份，该 IP 地址为 IPsec 安全策略应用的接口 IP 地址。

【视图】

系统视图

【缺省用户角色】

network-admin

【参数】

address { *ipv4-address* | **ipv6** *ipv6-address* }：指定标识本端身份的 IP 地址，其中 *ipv4-address* 为标识本端身份的 IPv4 地址，*ipv6-address* 为标识本端身份的 IPv6 地址。

dn：使用从数字证书中获得的 DN 名作为本端身份。

fqdn *fqdn-name*：指定标识本端身份的 FQDN 名称，*fqdn-name* 表示 FQDN 名称，为 1~255 个字符的字符串，区分大小写，例如 **www.test.com**。不指定 *fqdn-name* 时，则设备将使用 **sysname** 命令配置的设备的名称作为本端 FQDN 类型的身份。

user-fqdn *user-fqdn-name*：指定标识本端身份的 User FQDN 名称，*user-fqdn-name* 表示 User FQDN 名称，为 1~255 个字符的字符串，区分大小写，例如 **adc@test.com**。不指定 *user-fqdn-name* 时，则设备将使用 **sysname** 命令配置的设备的名称作为本端 user FQDN 类型的身份。

【使用指导】

本命令用于全局配置 IKE 对等体的本端身份，适用于所有 IKE SA 的协商，而 IKE profile 下的 **local-identity** 为局部配置身份，仅适用于使用本 IKE profile 的 IKE SA 的协商。

如果本端的认证方式为数字签名方式，则本端可以配置任何类型的身份信息；如果本端的认证方式为预共享密钥方式，则只能配置除 DN 之外的其它类型的身份信息。

如果希望在采用数字签名认证时，总是从证书中的主题字段取得本端身份，则可以通过 **ike signature-identity from-certificate** 命令实现。如果没有配置 **ike signature-identity from-certificate**，并且 IPsec 安全策略或 IPsec 安全策略模板下指定的 IKE profile 中配置了本端身份（由 **local-identity** 命令指定），则使用 IKE profile 中配置的本端身份；若 IPsec 安全策略或 IPsec 安全策略模板下未指定 IKE profile 或 IKE profile 下没有配置本端身份，则使用全局配置的本端身份（由 **ike identity** 命令指定）。

【举例】

指定使用 IP 地址 2.2.2.2 标识本端身份。

```
<sysname> system-view  
[sysname] ike identity address 2.2.2.2
```

【相关命令】

- **local-identity**

- `ike signature-identity from-certificate`

2.1.14 ike invalid-spi-recovery enable

`ike invalid-spi-recovery enable` 命令用来开启针对无效 IPsec SPI 的 IKE SA 恢复功能。

`undo ike invalid-spi-recovery enable` 命令用来关闭针对无效 IPsec SPI 的 IKE SA 恢复功能。

【命令】

```
ike invalid-spi-recovery enable
undo ike invalid-spi-recovery enable
```

【缺省情况】

针对无效 IPsec SPI 的 IKE SA 恢复功能处于关闭状态。

【视图】

系统视图

【缺省用户角色】

network-admin

【使用指导】

当 IPsec 隧道一端的安全网关出现问题（例如安全网关重启）导致本端 IPsec SA 丢失时，会造成 IPsec 流量黑洞现象：一端（接收端）的 IPsec SA 已经完全丢失，而另一端（发送端）还持有对应的 IPsec SA 且不断地向对端发送报文，当接收端收到发送端使用此 IPsec SA 封装的 IPsec 报文时，就会因为找不到对应的 SA 而持续丢弃报文，形成流量黑洞。该现象造成 IPsec 通信链路长时间得不到恢复（只有等到发送端旧的 IPsec SA 生命周期超时，并重建 IPsec SA 后，两端的 IPsec 流量才能得以恢复），因此需要采取有效的 IPsec SA 恢复手段来快速恢复中断的 IPsec 通信链路。

SA 由 SPI 唯一标识，接收方根据 IPsec 报文中的 SPI 在 SA 数据库中查找对应的 IPsec SA，若接收方找不到处理该报文的 IPsec SA，则认为此报文的 SPI 无效。如果接收端当前存在 IKE SA，则会向对端发送删除对应 IPsec SA 的通知消息，发送端 IKE 接收到此通知消息后，就会立即删除此无效 SPI 对应的 IPsec SA。之后，当发送端需要继续向接收端发送报文时，就会触发两端重建 IPsec SA，使得中断的 IPsec 通信链路得以恢复；如果接收端当前不存在 IKE SA，就不会触发本端向对端发送删除 IPsec SA 的通知消息，接收端将默认丢弃无效 SPI 的 IPsec 报文，使得链路无法恢复。后一种情况下，如果开启了 IPsec 无效 SPI 恢复 IKE SA 功能，就会触发本端与对端协商新的 IKE SA 并发送删除消息给对端，从而使链路恢复正常。

由于开启此功能后，若攻击者伪造大量源 IP 地址不同但目的 IP 地址相同的无效 SPI 报文发给设备，会导致设备因忙于与无效对端协商建立 IKE SA 而面临受到 DoS（Denial of Service）攻击的风险，通常情况下，建议关闭针对无效 IPsec SPI 的 IKE SA 恢复功能。

【举例】

开启 IPsec 无效 SPI 恢复 IKE SA 功能。

```
<Sysname> system-view
[Sysname] ike invalid-spi-recovery enable
```

2.1.15 ike keepalive interval

ike keepalive interval 命令用来配置通过 IKE SA 向对端发送 IKE Keepalive 报文的时间间隔。

undo ike keepalive interval 命令用来恢复缺省情况。

【命令】

```
ike keepalive interval interval  
undo ike keepalive interval
```

【缺省情况】

不向对端发送 IKE Keepalive 报文。

【视图】

系统视图

【缺省用户角色】

network-admin

【参数】

interval: 指定向对端发送 IKE SA 的 Keepalive 报文的时间间隔，取值范围为 20~28800，单位为秒。

【使用指导】

当有检测对方 IKE SA 和 IPsec SA 是否存活的需求时，通常建议配置 IKE DPD，不建议配置 IKE Keepalive 功能。仅当对方不支持 IKE DPD 特性，但支持 IKE Keepalive 功能时，才考虑配置 IKE Keepalive 功能。

本端配置的 IKE Keepalive 报文的等待超时时间要大于对端发送的时间间隔。由于网络中一般不会出现超过三次的报文丢失，所以，本端的超时时间可以配置为对端配置的发送 IKE Keepalive 报文的时间间隔的三倍。

【举例】

配置本端向对端发送 Keepalive 报文的时间间隔为 200 秒。

```
<Sysname> system-view  
[Sysname] ike keepalive interval 200
```

【相关命令】

- **ike keepalive timeout**

2.1.16 ike keepalive timeout

ike keepalive timeout 命令用来配置本端等待对端发送 IKE Keepalive 报文的超时时间。

undo ike keepalive timeout 命令用来恢复缺省情况。

【命令】

```
ike keepalive timeout seconds  
undo ike keepalive timeout
```

【缺省情况】

未配置本端等待对端发送 IKE Keepalive 报文的超时时间。

【视图】

系统视图

【缺省用户角色】

network-admin

【参数】

seconds: 指定本端等待对端发送 IKE Keepalive 报文的超时时间，取值范围为 20~28800，单位为秒。

【使用指导】

当本端 IKE SA 在配置的超时时间内未收到 IKE Keepalive 报文时，则删除该 IKE SA 以及由其协商的 IPsec SA

本端配置的等待对端发送 IKE Keepalive 报文的超时时间要大于对端发送 IKE Keepalive 报文的时间间隔。由于网络中一般不会出现超过三次的报文丢失，所以，本端的超时时间可以配置为对端配置的发送 IKE Keepalive 报文的时间间隔的三倍。

【举例】

配置本端等待对端发送 IKE Keepalive 报文的超时时间为 20 秒。

```
<Sysname> system-view
[Sysname] ike keepalive timeout 20
```

【相关命令】

- **ike keepalive interval**

2.1.17 ike keychain

ike keychain 命令用来创建 IKE keychain，并进入 IKE keychain 视图。如果指定的 IKE keychain 已经存在，则直接进入 IKE keychain 视图。

undo ike keychain 命令用来删除指定的 IKE keychain。

【命令】

```
ike keychain keychain-name
undo ike keychain keychain-name
```

【缺省情况】

不存在 IKE keychain。

【视图】

系统视图

【缺省用户角色】

network-admin

【参数】

keychain-name: IKE keychain 的名称，为 1~63 个字符的字符串，不区分大小写。

【使用指导】

在 IKE 需要通过预共享密钥方式进行认证时，需要创建并指定 IKE keychain。

【举例】

创建 IKE keychain key1 并进入 IKE keychain 视图。

```
<Sysname> system-view
[Sysname] ike keychain key1
[Sysname-ike-keychain-key1]
```

【相关命令】

- **authentication-method**
- **pre-shared-key**

2.1.18 ike limit

ike limit 命令用来配置对本端 IKE SA 数目的限制。

undo ike limit 命令用来恢复缺省情况。

【命令】

```
ike limit { max-negotiating-sa negotiation-limit | max-sa sa-limit }
undo ike limit { max-negotiating-sa | max-sa }
```

【缺省情况】

不限制 IKE SA 数目。

【视图】

系统视图

【缺省用户角色】

network-admin

【参数】

max-negotiating-sa *negotiation-limit*: 指定允许同时处于协商状态的 IKE SA 和 IPsec SA 的最大总和数，取值范围为 1~99999。

max-sa *sa-limit*: 指定允许建立的 IKE SA 的最大数，取值范围为 1~99999。

【使用指导】

可以通过 **max-negotiating-sa** 参数设置允许同时协商更多的 IKE SA，以充分利用设备处理能力，以便在设备有较强处理能力的情况下得到更高的新建性能；可以通过该参数设置允许同时协商更少的 IKE SA，以避免产生大量不能完成协商的 IKE SA，以便在设备处理能力较弱时保证一定的新建性能。

可以通过 **max-sa** 参数设置允许建立更多的 IKE SA，以便在设备有充足内存的情况下得到更高的并发性能；可以通过该参数设置允许建立更少的 IKE SA，以便在设备没有充足的内存的情况下，使 IKE 不过多占用系统内存。

【举例】

配置本端允许同时处于协商状态的 IKE SA 和 IPsec SA 的最大总和数为 200。

```
<Sysname> system-view  
[Sysname] ike limit max-negotiating-sa 200
```

配置本端允许成功建立的 IKE SA 的最大数为 5000。

```
<Sysname> system-view  
[Sysname] ike limit max-sa 5000
```

2.1.19 ike nat-keepalive

ike nat-keepalive 命令用来配置向对端发送 NAT Keepalive 报文的时间间隔。

undo ike nat-keepalive 命令用来恢复缺省情况。

【命令】

```
ike nat-keepalive seconds  
undo ike nat-keepalive
```

【缺省情况】

向对端发送 NAT Keepalive 报文的时间间隔为 20 秒。

【视图】

系统视图

【缺省用户角色】

network-admin

【参数】

seconds：指定向对端发送 NAT Keepalive 报文的时间间隔，取值范围为 5～300，单位为秒。

【使用指导】

该命令仅对位于 NAT 之后的设备（即该设备位于 NAT 设备连接的私网侧）有意义。NAT 之后的 IKE 网关设备需要定时向 NAT 之外的 IKE 网关设备发送 NAT Keepalive 报文，以便维持 NAT 设备上对应的 IPsec 流量的会话存活，从而让 NAT 之外的设备可以访问 NAT 之后的设备。

因此，需要确保该命令配置的时间小于 NAT 设备上会话表项的存活时间。

【举例】

配置向对端发送 NAT Keepalive 报文的时间间隔为 5 秒。

```
<Sysname> system-view  
[Sysname] ike nat-keepalive 5
```

2.1.20 ike profile

ike profile 命令用来创建一个 IKE profile，并进入 IKE profile 视图。如果指定的 IKE profile 已经存在，则直接进入 IKE profile 视图。

undo ike profile 命令用来删除指定的 IKE profile。

【命令】

```
ike profile profile-name
```


undo ike profile *profile-name*

【缺省情况】

不存在 IKE profile。

【视图】

系统视图

【缺省用户角色】

network-admin

【参数】

profile-name: IKE profile 名称，为 1~63 个字符的字符串，不区分大小写。

【举例】

创建 IKE profile 1，并进入其视图。

```
<Sysname> system-view
[Sysname] ike profile 1
[Sysname-ike-profile-1]
```

2.1.21 ike proposal

ike proposal 命令用来创建 IKE 提议，并进入 IKE 提议视图。如果指定的 IKE 提议已经存在，则直接进入 IKE 提议视图。

undo ike proposal 命令用来删除指定 IKE 提议。

【命令】

ike proposal *proposal-number*
undo ike proposal *proposal-number*

【缺省情况】

系统提供一条缺省的 IKE 提议，此缺省的 IKE 提议具有最低的优先级。缺省的提议的参数不可修改，其参数包括：

- 加密算法：非 FIPS 模式下使用 DES-CBC，FIPS 模式下使用 AES-CBC-128
- 认证算法：HMAC-SHA1
- 认证方法：预共享密钥
- DH 密钥交换参数：非 FIPS 模式使用 group1，FIPS 模式下使用 group14
- IKE SA 存活时间：86400 秒

【视图】

系统视图

【缺省用户角色】

network-admin

【参数】

proposal-number: IKE 提议序号，取值范围为 1~65535。该序号同时表示优先级，数值越小，优先级越高。

【使用指导】

在进行 IKE 协商的时候，协商发起方会将自己的 IKE 提议发送给对端，由对端进行匹配。若发起方使用的 IPsec 安全策略中没有引用 IKE profile，则会将当前系统中所有的 IKE 提议发送给对端；否则，发起方会将引用的 IKE profile 中的所有 IKE 提议发送给对端。

响应方则以对端发送的 IKE 提议优先级从高到低的顺序与本端所有的 IKE 提议进行匹配，一旦找到匹配项则停止匹配并使用匹配的提议，否则继续查找其它的 IKE 提议。如果本端配置中没有和对端匹配的 IKE 提议，则使用系统缺省的 IKE 提议进行匹配。

【举例】

创建 IKE 提议 1，并进入 IKE 提议视图。

```
<Sysname> system-view
[Sysname] ike proposal 1
[Sysname-ike-proposal-1]
```

【相关命令】

- **display ike proposal**

2.1.22 ike signature-identity from-certificate

ike signature-identity from-certificate 命令用来配置设备使用由本端证书中获得的身份信息参与数字签名认证。

undo ike signature-identity from-certificate 命令用来恢复缺省情况。

【命令】

```
ike signature-identity from-certificate
undo ike signature-identity from-certificate
```

【缺省情况】

当使用数字签名认证方式时，本端身份信息由 **local-identity** 或 **ike identity** 命令指定。

【视图】

系统视图

【缺省用户角色】

network-admin

【使用指导】

当使用数字签名认证方式时，本端的身份总是从本端证书的主题字段中获得，不论 **local-identity** 或 **ike identity** 如何配置。

在采用 IPsec 野蛮协商模式以及数字签名认证方式的情况下，与仅支持使用 DN 类型身份进行数字签名认证的 ComwareV5 设备互通时需要配置本命令。

如果没有配置 **ike signature-identity from-certificate**，并且 IPsec 安全策略或 IPsec 安全策略模板下指定的 IKE profile 中配置了本端身份（由 **local-identity** 命令指定），则使用 IKE profile 中配置的本端身份；若 IPsec 安全策略或 IPsec 安全策略模板下未指定 IKE profile 或 IKE profile 下没有配置本端身份，则使用全局配置的本端身份（由 **ike identity** 命令指定）。

【举例】

在采用数字签名认证时，指定总从本端证书中的主题字段取得本端身份。

```
<Sysname> system-view
[sysname] ike signature-identity from-certificate
```

【相关命令】

- **local-identity**
- **ike identity**

2.1.23 keychain

keychain 命令用来指定采用预共享密钥认证时使用的 IKE keychain。

undo keychain 命令用取消指定的 IKE keychain。

【命令】

```
keychain keychain-name
undo keychain keychain-name
```

【缺省情况】

未指定采用预共享密钥认证时使用的 IKE keychain。

【视图】

IKE profile 视图

【缺省用户角色】

network-admin

【参数】

keychain-name: IKE keychain 名称，为 1~63 个字符的字符串，不区分大小写。

【使用指导】

一个 IKE profile 中最多可以指定六个 IKE keychain，先配置的 IKE keychain 优先级高。

【举例】

在 IKE profile 1 中指定名称为 abc 的配置的 IKE keychain。

```
<Sysname> system-view
[Sysname] ike profile 1
[Sysname-ike-profile-1] keychain abc
```

【相关命令】

- **ike keychain**

2.1.24 local-identity

local-identity 命令用来配置本端身份信息，用于在 IKE 认证协商阶段向对端标识自己的身份。

undo local-identity 命令用来恢复缺省情况。

【命令】

```
local-identity { address { ipv4-address | ipv6 ipv6-address } | dn | fqdn  
[ fqdn-name ] | user-fqdn [ user-fqdn-name ] }  
undo local-identity
```

【缺省情况】

未配置本端身份信息。此时使用系统视图下通过 **ike identity** 命令配置的身份信息作为本端身份信息。若两者都没有配置，则使用 IP 地址标识本端的身份，该 IP 地址为 IPsec 安全策略应用的接口的 IP 地址。

【视图】

IKE profile 视图

【缺省用户角色】

network-admin

【参数】

address { *ipv4-address* | **ipv6** *ipv6-address* }：指定标识本端身份的 IP 地址，其中 *ipv4-address* 为标识本端身份的 IPv4 地址，*ipv6-address* 为标识本端身份的 IPv6 地址。

dn：使用从本端数字证书中获得的 DN 名作为本端身份。

fqdn *fqdn-name*：指定标识本端身份的 FQDN 名称，*fqdn-name* 为 1~255 个字符的字符串，区分大小写，例如 **www.test.com**。不指定 *fqdn-name* 时，则设备将使用 **sysname** 命令配置的设备名称作为本端 FQDN 类型的身份。

user-fqdn *user-fqdn-name*：指定标识本端身份的 user FQDN 名称，*user-fqdn-name* 为 1~255 个字符的字符串，区分大小写，例如 **adc@test.com**。不指定 *user-fqdn-name* 时，则设备将使用 **sysname** 命令配置的设备名称作为本端 user FQDN 类型的身份。

【使用指导】

如果本端的认证方式为数字签名方式，则本端可以配置任何类型的身份信息；如果本端的认证方式为预共享密钥方式，则只能配置除 DN 之外的其它类型的身份信息。

如果本端的认证方式为数字签名方式，且配置的本端身份为 IP 地址，但这个 IP 地址与本端证书中的 IP 地址不同，则设备将使用 FQDN 类型的本端身份标识，该标识为使用 **sysname** 命令配置的设备名称。

响应方使用发起方的身份信息查找本地的 IKE profile，通过与 **match remote** 命令中指定的发起方身份信息进行匹配，可查找到本端要采用的 IKE profile。

一个 IKE profile 中只能配置一条本端身份信息。

IKE profile 下的本端身份信息优先级高于系统视图下通过 **ike identity** 命令配置的本端身份信息。如果 IKE profile 下未配置本端身份信息，则使用系统视图下配置的本端身份信息。

【举例】

指定使用 IP 地址 2.2.2.2 标识本端身份。

```
<Sysname> system-view  
[Sysname] ike profile prof1  
[Sysname-ike-profile-prof1] local-identity address 2.2.2.2
```

【相关命令】

- `match remote`
- `ike identity`

2.1.25 match local address (IKE keychain view)

`match local address` 命令用来限制 IKE keychain 的使用范围，即 IKE keychain 只能用于指定地址或指定接口的地址上的 IKE 协商。

`undo match local address` 命令用来恢复缺省情况。

【命令】

```
match local address { interface-type interface-number | { ipv4-address | ipv6  
ipv6-address } }  
undo match local address
```

【缺省情况】

未限制 IKE keychain 的使用范围。

【视图】

IKE keychain 视图

【缺省用户角色】

network-admin

【参数】

`interface-type interface-number`: 本端接口名称。可以是任意的三层接口。

`ipv4-address`: 本端接口的 IPv4 地址。

`ipv6 ipv6-address`: 本端接口的 IPv6 地址。

【使用指导】

此命令用于限制 IKE keychain 只能用于指定地址或指定接口的地址上的协商，这里的地址指的是 IPsec 安全策略/IPsec 安全策略模板下配置的本端地址（通过命令 `local-address` 配置），若本端地址没有配置，则为引用 IPsec 安全策略的接口的 IP 地址。

一个 IKE profile 中最多可以指定六个 IKE keychain，先配置的 IKE keychain 优先级高。若希望本端在匹配某些 IKE keychain 的时候，不按照配置的优先级来查找，则可以通过本命令来指定这类 IKE keychain 的使用范围。例如，IKE keychain A 中的预共享密钥的匹配地址范围大（2.2.0.0/16），IKE keychain B 中的预共享密钥的匹配地址范围小（2.2.2.0/24），IKE keychain A 先于 IKE keychain B 配置。假设对端 IP 地址为 2.2.2.6，那么依据配置顺序本端总是选择 keychain A 与对端协商。若希望本端接口（假设接口地址为 3.3.3.3）使用 keychain B 与对端协商，可以配置 keychain B 在指定地址 3.3.3.3 的接口上使用。

【举例】

创建 IKE keychain，名称为 key1。

```
<Sysname> system-view
```

```
[Sysname] ike keychain key1
```

限制 IKE keychain key1 只能在 2.2.2.1 的 IP 地址上使用。

```
[sysname-ike-keychain-key1] match local address 2.2.2.1
```

2.1.26 match local address (IKE profile view)

match local address 命令用来限制 IKE profile 的使用范围，即 IKE profile 只能用于指定地址或指定接口的地址上的 IKE 协商。

undo match local address 命令用来恢复缺省情况。

【命令】

```
match local address { interface-type interface-number | { ipv4-address |  
ipv6 ipv6-address } }  
undo match local address
```

【缺省情况】

未限制 IKE profile 的使用范围。

【视图】

IKE profile 视图

【缺省用户角色】

network-admin

【参数】

interface-type interface-number: 本端接口名称。可以是任意三层接口。

ipv4-address: 本端接口 IPv4 地址。

ipv6 ipv6-address: 本端接口 IPv6 地址。

【使用指导】

此命令用于限制 IKE profile 只能用于指定地址或指定接口的地址上的协商，这里的地址指的是 IPsec 安全策略/IPsec 安全策略模板下配置的本端地址（通过命令 **local-address** 配置），若本端地址没有配置，则为引用 IPsec 安全策略的接口的 IP 地址。

先配置的 IKE profile 优先级高，若希望本端在匹配某些 IKE profile 的时候，不按照配置的优先级来查找，则可以通过本命令来指定这类 IKE profile 的使用范围。例如，IKE profile A 中的 **match remote** 地址范围大（**match remote identity address range 2.2.2.1 2.2.2.100**），IKE profile B 中的 **match remote** 地址范围小（**match remote identity address range 2.2.2.1 2.2.2.10**），IKE profile A 先于 IKE profile B 配置。假设对端 IP 地址为 2.2.2.6，那么依据配置顺序本端总是选择 profile A 与对端协商。若希望本端接口（假设接口地址为 3.3.3.3）使用 profile B 与对端协商，可以配置 profile B 在指定地址 3.3.3.3 的接口上使用。

【举例】

创建 IKE profile，名称为 prof1。

```
<Sysname> system-view
```

```
[Sysname] ike profile prof1
```

限制 IKE profile prof1 只能在 2.2.2.1 的 IP 地址上使用。

```
[sysname-ike-profile-prof1] match local address 2.2.2.1
```

2.1.27 match remote

match remote 命令用来配置一条用于匹配对端身份的规则。

undo match remote 命令用来删除一条用于匹配对端身份的规则。

【命令】

```
match remote { certificate policy-name | identity { address { { ipv4-address  
[ mask | mask-length ] | range low-ipv4-address high-ipv4-address } | ipv6  
{ ipv6-address [ prefix-length ] | range low-ipv6-address  
high-ipv6-address } } | fqdn fqdn-name | user-fqdn user-fqdn-name } }  
undo match remote { certificate policy-name | identity { address  
{ { ipv4-address [ mask | mask-length ] | range low-ipv4-address  
high-ipv4-address } | ipv6 { ipv6-address [ prefix-length ] | range  
low-ipv6-address high-ipv6-address } } | fqdn fqdn-name | user-fqdn  
user-fqdn-name } }
```

【缺省情况】

未配置用于匹配对端身份的规则。

【视图】

IKE profile 视图

【缺省用户角色】

network-admin

【参数】

certificate policy-name: 基于对端数字证书中的信息匹配 IKE profile。其中, *policy-name* 是证书访问控制策略的名称, 为 1~31 个字符的字符串。本参数用于响应方根据收到的发起方证书中的 DN 字段来过滤使用的 IKE profile。

identity: 基于指定的对端身份信息匹配 IKE profile。本参数用于响应方根据发起方通过 **local-identity** 命令配置的身份信息来选择使用的 IKE profile。

address ipv4-address [mask | mask-length]: 对端 IPv4 地址或 IPv4 网段。其中, *ipv4-address* 为 IPv4 地址, *mask* 为子网掩码, *mask-length* 为子网掩码长度, 取值范围为 0~32。

address range low-ipv4-address high-ipv4-address: 对端 IPv4 地址范围。其中 *low-ipv4-address* 为起始 IPv4 地址, *high-ipv4-address* 为结束 IPv4 地址。结束地址必须大于起始地址。

address ipv6 ipv6-address [prefix-length]: 对端 IPv6 地址或 IPv6 网段。其中, *ipv6-address* 为 IPv6 地址, *prefix-length* 为 IPv6 前缀, 取值范围为 0~128。

address ipv6 range low-ipv6-address high-ipv6-address: 对端 IPv6 地址范围。其中 *low-ipv6-address* 为起始 IPv6 地址, *high-ipv6-address* 为结束 IPv6 地址。结束地址必须大于起始地址。

fqdn fqdn-name: 对端 FQDN 名称, 为 1~255 个字符的字符串, 区分大小写, 例如 *www.test.com*。

user-fqdn user-fqdn-name: 对端 User FQDN 名称，为 1~255 个字符的字符串，区分大小写，例如 abc@test.com。

【使用指导】

响应方根据发起方的身份信息通过本配置查找 IKE profile 并验证对端身份，发起方根据响应方的身份信息通过本配置验证对端身份。

协商双方都必须配置至少一个 **match remote** 规则，当对端的身份与 IKE profile 中配置的 **match remote** 规则匹配时，则使用此 IKE profile 中的信息与对端完成认证。为了使得每个对端能够匹配到唯一的 IKE profile，不建议在两个或两个以上 IKE profile 中配置相同的 **match remote** 规则，否则能够匹配到哪个 IKE profile 是不可预知的。

match remote 规则可以配置多个，并同时都有效，其匹配优先级为配置顺序。

【举例】

创建 IKE profile，名称为 prof1。

```
<Sysname> system-view
```

```
[Sysname] ike profile prof1
```

指定需要匹配对端身份类型为 FQDN，取值为 www.test.com。

```
[Sysname-ike-profile-prof1] match remote identity fqdn www.test.com
```

指定需要匹配对端身份类型为 IP 地址，取值为 10.1.1.1。

```
[Sysname-ike-profile-prof1] match remote identity address 10.1.1.1
```

【相关命令】

- **local-identity**

2.1.28 pre-shared-key

pre-shared-key 命令用来配置预共享密钥。

undo pre-shared-key 命令用来取消指定的预共享密钥。

【命令】

非 FIPS 模式下：

```
pre-shared-key { address { ipv4-address [ mask | mask-length ] | ipv6 ipv6-address [ prefix-length ] } | hostname host-name } key { cipher | simple } string
```

```
undo pre-shared-key { address { ipv4-address [ mask | mask-length ] | ipv6 ipv6-address [ prefix-length ] } | hostname host-name }
```

FIPS 模式下：

```
pre-shared-key { address { ipv4-address [ mask | mask-length ] | ipv6 ipv6-address [ prefix-length ] } | hostname host-name } key [ cipher string ]
```

```
undo pre-shared-key { address { ipv4-address [ mask | mask-length ] | ipv6 ipv6-address [ prefix-length ] } | hostname host-name }
```

【缺省情况】

未配置预共享密钥。

【视图】

IKE keychain 视图

【缺省用户角色】

network-admin

【参数】

address: 对端的地址。

ipv4-address: 对端的 IPv4 地址。

mask: 对端的 IPv4 地址掩码，缺省值为 255.255.255.255。

mask-length: 对端的 IPv4 地址掩码长度，取值范围为 0~32，缺省值为 32。

ipv6: 指定对端的 IPv6 地址。

ipv6-address: 对端的 IPv6 地址。

prefix-length: 对端的 IPv6 地址前缀长度，取值范围为 0~128，缺省值为 128。

hostname host-name: 对端主机名。取值范围为 1~255，区分大小写。

key: 设置的预共享密钥。

cipher: 以密文方式设置密钥。

simple: 以明文方式设置密钥，该密钥将以密文形式存储。

string: 密钥字符串，区分大小写。非 FIPS 模式下，明文密钥为 1~128 个字符的字符串；密文密钥为 1~201 个字符的字符串。FIPS 模式下，明文密钥为 1~128 个字符的字符串；密文密钥为 15~201 个字符的字符串。

【使用指导】

配置预共享密钥的同时，还通过参数 **address** 和 **hostname** 指定了使用该预共享密钥的匹配条件，即与哪些 IP 地址或哪些主机名的对端协商时，才可以使用该预共享密钥。

IKE 协商双方必须配置了相同的预共享密钥，预共享密钥类型的身份认证才会成功。

在 FIPS 模式下，支持以交互式方式设置预共享密钥，且为 15~128 个字符的字符串，区分大小写，密码元素的最少组合类型为 4（必须包括数字、大写字母、小写字母以及特殊字符），但不能包含问号字符“?”；非 FIPS 模式下，不支持交互式设置预共享密钥。

【举例】

创建 IKE keychain key1 并进入 IKE keychain 视图。

```
<Sysname> system-view
```

```
[Sysname] ike keychain key1
```

配置与地址为 1.1.1.2 的对端使用的预共享密钥为明文的 123456TESTplat&!

```
[Sysname-ike-keychain-key1] pre-shared-key address 1.1.1.2 255.255.255.255 key simple  
123456TESTplat&!
```

【相关命令】

- **authentication-method**
- **keychain**

2.1.29 priority (IKE keychain view)

priority 命令用来指定 IKE keychain 的优先级。

undo priority 命令用来恢复缺省情况。

【命令】

```
priority priority  
undo priority
```

【缺省情况】

IKE keychain 的优先级为 100。

【视图】

IKE keychain 视图

【缺省用户角色】

network-admin

【参数】

priority *priority*: IKE keychain 优先级，取值范围为 1～65535。该数值越小，优先级越高。

【使用指导】

配置了 **match local address** 的 IKE keychain，优先级高于所有未配置 **match local address** 的 IKE keychain。即 IKE keychain 的使用优先级首先决定于其中是否配置了 **match local address**，其次取决于它的优先级。

【举例】

指定 IKE keychain key1 的优先级为 10。

```
<Sysname> system-view  
[Sysname] ike keychain key1  
[Sysname-ike-keychain-key1] priority 10
```

2.1.30 priority (IKE profile view)

priority 命令用来指定 IKE profile 的优先级。

undo priority 命令用来恢复缺省情况。

【命令】

```
priority priority  
undo priority
```

【缺省情况】

IKE profile 的优先级为 100。

【视图】

IKE-Profile 视图

【缺省用户角色】

network-admin

【参数】

priority *priority*: IKE profile 优先级号, 取值范围为 1~65535。该数值越小, 优先级越高。

【使用指导】

配置了 **match local address** 的 IKE profile, 优先级高于所有未配置 **match local address** 的 IKE profile。即 IKE profile 的匹配优先级首先决定于其中是否配置了 **match local address**, 其次决定于它的优先级。

【举例】

```
# 指定在 IKE profile prof1 的优先级为 10。  
<Sysname> system-view  
[Sysname] ike profile prof1  
[Sysname-ike-profile-prof1] priority 10
```

2.1.31 proposal

proposal 命令用来配置 IKE profile 引用的 IKE 提议。

undo proposal 命令用来恢复缺省情况。

【命令】

```
proposal proposal-number&<1-6>  
undo proposal
```

【缺省情况】

IKE profile 未引用 IKE 提议, 使用系统视图下配置的 IKE 提议进行 IKE 协商。

【视图】

IKE profile 视图

【缺省用户角色】

network-admin

【参数】

proposal-number&<1-6>: IKE 提议序号, 取值范围为 1~65535。该序号在 IKE profile 中与优先级无关, 先配置的 IKE 提议优先级高。&<1-6>表示前面的参数最多可以输入 6 次。

【使用指导】

IKE 协商过程中, 对于发起方, 如果使用的 IPsec 安全策略下指定了 IKE profile, 则使用 IKE profile 中引用的 IKE 提议进行协商; 对于响应方, 则使用系统视图下配置的 IKE 提议与对端发送的 IKE 提议进行匹配。

【举例】

```
# 设置 IKE profile prof1 引用序号为 10 的 IKE 安全提议。  
<Sysname> system-view  
[Sysname] ike profile prof1  
[Sysname-ike-profile-prof1] proposal 10
```

【相关命令】

- `ike proposal`

2.1.32 reset ike sa

`reset ike sa` 命令用来清除 IKE SA。

【命令】

`reset ike sa [connection-id connection-id]`

【视图】

用户视图

【缺省用户角色】

network-admin

【参数】

connection-id connection-id: 清除指定连接 ID 的 IKE SA，取值范围为 1~2000000000。

【使用指导】

删除 IKE SA 时，会向对端发送删除通知消息。

【举例】

查看当前的 IKE SA。

```
<Sysname> display ike sa
Total IKE SAs: 2
Connection-ID Remote      Flag      DOI
-----
1             202.38.0.2   RD        IPsec
2             202.38.0.3   RD        IPsec
```

Flags:

RD--READY RL--REPLACED FD-FADING RK-REKEY

清除连接 ID 号为 2 的 IKE SA。

```
<Sysname> reset ike sa connection-id 2
```

查看当前的 IKE SA。

```
<Sysname> display ike sa

Total IKE SAs: 1
Connection-ID Remote      Flag      DOI
-----
1             202.38.0.2   RD        IPsec
```

Flags:

RD--READY RL--REPLACED FD-FADING RK-REKEY

2.1.33 reset ike statistics

`reset ike statistics` 命令用于清除 IKE 的 MIB 统计信息。

【命令】

```
reset ike statistics
```

【视图】

用户视图

【缺省用户角色】

network-admin

【举例】

清除 IKE 的 MIB 统计信息。

```
<Sysname> reset ike statistics
```

【相关命令】

- `snmp-agent trap enable ike`

2.1.34 sa duration

`sa duration` 命令用来指定一个 IKE 提议的 IKE SA 存活时间。

`undo sa duration` 命令用来恢复缺省情况。

【命令】

```
sa duration seconds
```

```
undo sa duration
```

【缺省情况】

IKE 提议的 IKE SA 存活时间为 86400 秒。

【视图】

IKE 提议视图

【缺省用户角色】

network-admin

【参数】

seconds: 指定 IKE SA 存活时间，取值范围为 60~604800，单位为秒。

【使用指导】

在指定的 IKE SA 存活时间超时前，设备会提前协商另一个 IKE SA 来替换旧的 IKE SA。在新的 IKE SA 还没有协商完之前，依然使用旧的 IKE SA；在新的 IKE SA 建立后，将立即使用新的 IKE SA，而旧的 IKE SA 在存活时间超时后，将被自动清除。

如果协商双方配置了不同的 IKE SA 存活时间，则时间较短的存活时间生效。

【举例】

指定 IKE 提议 1 的 IKE SA 存活时间 600 秒（10 分钟）。

```
<Sysname> system-view
```

```
[Sysname] ike proposal 1
```

```
[Sysname-ike-proposal-1] sa duration 600
```

【相关命令】

- `display ike proposal`

2.1.35 snmp-agent trap enable ike

`snmp-agent trap enable ike` 命令用来开启 IKE 的告警功能。

`undo snmp-agent trap enable ike` 命令用来关闭指定的 IKE 告警功能。

【命令】

```
snmp-agent trap enable ike [ attr-not-support | auth-failure |  
cert-type-unsupport | cert-unavailable | decrypt-failure | encrypt-failure  
| global | invalid-cert-auth | invalid-cookie | invalid-id |  
invalid-proposal | invalid-protocol | invalid-sign | no-sa-failure |  
proposal-add | proposal-delete | tunnel-start | tunnel-stop |  
unsupport-exch-type ] *  
  
undo snmp-agent trap enable ike [ attr-not-support | auth-failure |  
cert-type-unsupport | cert-unavailable | decrypt-failure | encrypt-failure  
| global | invalid-cert-auth | invalid-cookie | invalid-id |  
invalid-proposal | invalid-protocol | invalid-sign | no-sa-failure |  
proposal-add | proposal-delete | tunnel-start | tunnel-stop |  
unsupport-exch-type ] *
```

【缺省情况】

IKE 的所有告警功能均处于关闭状态。

【视图】

系统视图

【缺省用户角色】

network-admin

【参数】

attr-not-support: 表示属性参数不支持时的告警功能。

auth-failure: 表示认证失败时的告警功能。

cert-type-unsupport: 表示证书类型不支持时的告警功能。

cert-unavailable: 表示无法获取证书时的告警功能。

decrypt-failure: 表示解密失败时的告警功能。

encrypt-failure: 表示加密失败时的告警功能。

global: 表示全局告警功能。

invalid-cert-auth: 表示证书认证无效时的告警功能。

invalid-cookie: 表示 cookie 无效时的告警功能。

invalid-id: 表示身份信息无效时的告警功能。

invalid-proposal: 表示 IKE 提议无效时的告警功能。

invalid-protocol: 表示安全协议无效时的告警功能。

invalid-sign: 表示证书签名无效时的告警功能。
no-sa-failure: 表示无法查到 SA 时的告警功能。
proposal-add: 表示添加 IKE 提议时的告警功能。
proposal-delete: 表示删除 IKE 提议时的告警功能。
tunnel-start: 表示创建 IKE 隧道时的告警功能。
tunnel-stop: 表示删除 IKE 隧道时的告警功能。
unsupport-exch-type: 表示协商类型不支持时的告警功能。

【使用指导】

如果不指定任何参数，则表示开启或关闭所有类型的 IKE 告警功能。

如果希望生成并输出某种类型的 IKE 告警信息，则需要保证 IKE 的全局告警功能以及相应类型的告警功能均处于开启状态。

【举例】

```
# 开启全局 IKE 告警功能。
<Sysname> system-view
[Sysname] snmp-agent trap enable ike global
# 开启创建 IKE 隧道时的告警功能。
[Sysname] snmp-agent trap enable ike tunnel-start
```

3 IKEv2

3.1 IKEv2配置命令

3.1.1 address

address 命令用来指定 IKEv2 peer 的主机地址。

undo address 命令用来恢复缺省情况。

【命令】

```
address { ipv4-address [ mask | mask-length ] | ipv6 ipv6-address
[ prefix-length ] }
undo address
```

【缺省情况】

未指定 IKEv2 peer 的主机地址。

【视图】

IKEv2 peer 视图

【缺省用户角色】

network-admin

【参数】

ipv4-address: IKEv2 peer 的 IPv4 主机地址。

Mask: IPv4 地址子网掩码。

mask-length: IPv4 地址的掩码长度，取值范围为 0~32。

ipv6 *ipv6-address*: IKEv2 peer 的 IPv6 主机地址。

prefix-length: IPv6 地址的前缀长度，取值范围为 0~128。

【使用指导】

使用主机地址查询 IKEv2 peer 对于 IKEv2 协商中的发起方和响应方均适用。

同一 keychain 视图下的不同 IKEv2 peer 不能配置相同的地址。

【举例】

创建一个 IKEv2 keychain，名称为 key1。

```
<Sysname> system-view
```

```
[Sysname] ikev2 keychain key1
```

创建一个 IKEv2 peer，名称为 peer1。

```
[Sysname-ikev2-keychain-key1] peer peer1
```

指定 IKEv2 peer 的 IP 地址为 3.3.3.3，掩码为 255.255.255.0。

```
[Sysname-ikev2-keychain-key1-peer-peer1] address 3.3.3.3 255.255.255.0
```


【相关命令】

- `ikev2 keychain`
- `peer`

3.1.2 authentication-method

`authentication-method` 命令用来指定 IKEv2 本端和对端的身份认证方式。

`undo authentication-method` 命令用来删除 IKEv2 本端或对端身份认证方式。

【命令】

```
authentication-method { local | remote } { dsa-signature | ecdsa-signature  
| pre-share | rsa-signature }  
undo authentication-method local  
undo authentication-method remote { dsa-signature | ecdsa-signature |  
pre-share | rsa-signature }
```

【缺省情况】

未配置本端和对端的认证方式。

【视图】

IKEv2 profile 视图

【缺省用户角色】

network-admin

【参数】

local: 指定本端的身份认证方式。

remote: 指定对端的身份认证方式。

dsa-signature: 表示身份认证方式为 DSA 数字签名方式。

ecdsa-signature: 表示身份认证方式为 ECDSA 数字签名方式。

pre-share: 表示身份认证方式为预共享密钥方式。

rsa-signature: 表示身份认证方式为 RSA 数字签名方式。

【使用指导】

一个 IKEv2 profile 中，必须配置 IKEv2 本端和对端的身份认证方式。本端和对端可以采用不同的身份认证方式。

只能指定一个本端身份认证方式，可以指定多个对端身份认证方式。在有多对端且对端身份认证方式未知的情况下，可以通过多次执行本命令指定多个对端的身份认证方式。

如果本端或对端的身份认证方式为 RSA、DSA 或 ECDSA 数字签名方式（**rsa-signature**、**dsa-signature** 或 **ecdsa-signature**），则还必须通过命令 **certificate domain** 指定 PKI 域来获取用于签名和验证的数字证书。若没有指定 PKI 域，则使用系统视图下通过命令 **pki domain** 配置的 PKI 域。

如果本端或对端的认证方式为预共享密钥方式（**pre-share**），则还必须在本 IKEv2 profile 引用的 keychain 中指定对等体的预共享密钥。

【举例】

```
# 创建 IKEv2 profile profile1。
<Sysname> system-view
[Sysname] ikev2 profile profile1
# 指定本端的认证方式为预共享密钥方式，对端的认证方式为 RSA 数字签名方式。
[Sysname-ikev2-profile-profile1] authentication local pre-share
[Sysname-ikev2-profile-profile1] authentication remote rsa-signature
# 指定对端用于签名和验证的 certificate 域为 gen1。
[Sysname-ikev2-profile-profile1] certificate domain gen1
# 指定 IKEv2 profile 引用的 keychain 为 keychain1。
[Sysname-ikev2-profile-profile1] keychain keychain1
```

【相关命令】

- **display ikev2 profile**
- **certificate domain** (ikev2 profile view)
- **keychain** (ikev2 profile view)

3.1.3 certificate domain

certificate domain 命令用来指定 IKEv2 协商采用数字签名认证时使用的 PKI 域。

undo certificate domain 命令用来取消配置 IKEv2 协商时使用的 PKI 域。

【命令】

```
certificate domain domain-name [ sign | verify ]
undo certificate domain domain-name
```

【缺省情况】

使用系统视图下配置的 PKI 域来验证证书。

【视图】

IKEv2 profile 视图

【缺省用户角色】

network-admin

【参数】

domain-name: PKI 域的名称，为 1~31 个字符的字符串，不区分大小写。

sign: 指定本端使用该 PKI 域中的本地证书生成数字签名。

verify: 指定本端使用该 PKI 域中的 CA 证书来验证对端证书。

【使用指导】

如果没有指定 **sign** 和 **verify**，则表示指定的 PKI 域既用于签名也用于验证。一个 PKI 域用于签名还是验证取决于最后一次的配置，例如，先配了 **certificate domain abc sign**，然后再配 **certificate domain abc verify**，那么最终 PKI 域 abc 只用于验证功能。

可通过多次执行本命令分别指定用于数字签名的 PKI 域和用于验证的 PKI 域。

如果本端的认证方式配置为 RSA、DSA 或 ECDSA 数字签名方式，则必须通过本命令指定 PKI 域来获取用于签名的本地证书；如果对端的认证方式配置为 RSA、DSA 或 ECDSA 数字签名方式，则使用本命令指定 PKI 域来获取用于验证的 CA 证书，若未指定 PKI 域，则使用系统视图下的所有 PKI 域来验证。

【举例】

```
# 创建 IKEv2 profile，名称为 profile1。
<Sysname> system-view
[Sysname] ikev2 profile profile1
# 配置 IKEv2 profile 引用的 PKI 域 abc 用于签名，PKI 域 def 用于验证。
[Sysname-ikev2-profile-profile1] certificate domain abc sign
[Sysname-ikev2-profile-profile1] certificate domain def verify
```

【相关命令】

- **authentication-method**
- **pki domain**（安全命令参考/PKI）

3.1.4 config-exchange

config-exchange 命令用来开启配置交换功能。

undo config-exchange 命令用来关闭指定的配置交换功能。

【命令】

```
config-exchange { request | set { accept | send } }
undo config-exchange { request | set { accept | send } }
```

【缺省情况】

所有的配置交换功能均处于关闭状态。

【视图】

IKEv2 profile 视图

【缺省用户角色】

network-admin

【参数】

request: 表示本端在 Auth 交换请求报文中携带配置交换请求载荷。

set: 表示本端在 Info 报文中携带配置交换设置载荷。

accept: 表示本端可接受配置交换设置载荷。

send: 表示本端可发送配置交换设置载荷。

【使用指导】

配置交换包括请求数据、回应数据、主动推数据和回应推数据，请求和推送的数据可以为网关地址，内部地址，路由信息等，目前仅支持中心侧内部地址分配。分支侧可以申请地址，但申请到的地址暂无用。

本端可以同时配置 **request** 和 **set** 参数。

如果本端配置了 **request** 参数，则只要对端能获取到对应的请求数据，就会对本端的请求进行响应。

如果本端配置了 **set send** 参数，则对端必须配置 **set accept** 参数来配合使用。

如果本端配置了 **set send** 参数，且没有收到配置请求时，IKEv2 SA 协商成功后才会推送地址给对端。

【举例】

```
# 创建 IKEv2 profile，名称为 profile1。
<Sysname> system-view
[Sysname] ikev2 profile profile1
# 配置本端在 Auth 交换请求报文中携带配置交换请求载荷。
[Sysname-ikev2-profile-profile1] config-exchange request
```

【相关命令】

- **display ikev2 profile**

3.1.5 dh

dh 命令用来配置 IKEv2 密钥协商时所使用的 DH 密钥交换参数。

undo dh 命令用来恢复缺省情况。

【命令】

非 FIPS 模式下：

```
dh { group1 | group14 | group2 | group24 | group5 | group19 | group20 } *
undo dh
```

FIPS 模式下：

```
dh { group14 | group19 | group20 } *
undo dh
```

【缺省情况】

IKEv2 安全提议未定义 DH 组。

【视图】

IKEv2 安全提议视图

【缺省用户角色】

network-admin

【参数】

group1：指定密钥协商时采用 768-bit 的 Diffie-Hellman group。

group2：指定密钥协商时采用 1024-bit 的 Diffie-Hellman group。

group5：指定密钥协商时采用 1536-bit 的 Diffie-Hellman group。

group14：指定密钥协商时采用 2048-bit 的 Diffie-Hellman group。

group24：指定密钥协商时采用含 256-bit 的 sub-group 的 2048-bit Diffie-Hellman group。

group19：指定密钥协商时采用 ECP 模式含 256-bit 的 Diffie-Hellman group。

group20: 指定密钥协商时采用 ECP 模式含 384-bit 的 Diffie-Hellman group。

【使用指导】

group1 提供了最低的安全性，但是处理速度最快。**group24** 提供了最高的安全性，但是处理速度最慢。其他的 **group** 随着位数的增加，提供了更高的安全性，但是处理速度会相应减慢。请根据实际组网环境中对安全性和性能的要求选择合适的 Diffie-Hellman group。

一个 IKEv2 安全提议中至少需要配置一个 DH 组，否则该安全提议不完整。

一个 IKEv2 安全提议中可以配置多个 DH 组，其使用优先级按照配置顺序依次降低。

【举例】

指定 IKEv2 提议 1 使用 768-bit 的 Diffie-Hellman group。

```
<Sysname> system-view
[Sysname] ikev2 proposal 1
[Sysname-ikev2-proposal-1] dh group1
```

【相关命令】

- **ikev2 proposal**

3.1.6 display ikev2 policy

display ikev2 policy 命令用来显示 IKEv2 安全策略的配置信息。

【命令】

```
display ikev2 policy [ policy-name | default ]
```

【视图】

任意视图

【缺省用户角色】

network-admin
network-operator

【参数】

policy-name: IKEv2 安全策略的名称，为 1~63 个字符的字符串，不区分大小写。

default: 缺省的 IKEv2 安全策略。

【使用指导】

如果未指定任何参数，则表示显示所有 IKEv2 安全策略的配置信息。

【举例】

显示所有 IKEv2 安全策略的配置信息。

```
<Sysname> display ikev2 policy
IKEv2 policy: 1
  Priority: 100
  Match local address: 1.1.1.1
  Match local address ipv6: 1::1:1:1
  Match VRF:
  Proposal: 1
```

```

Proposal: 2
IKEv2 policy: default
Match VRF:
Proposal: default
display ikev2 policy 命令显示信息描述表

```

字段	描述
IKEv2 policy	IKEv2安全策略的名称
Priority	IKEv2安全策略优先级
Match local address	匹配IKEv2安全策略的本端IPv4地址
Match local address ipv6	匹配IKEv2安全策略的本端IPv6地址
Match VRF	（暂不支持）匹配IKEv2安全策略的VRF
Proposal	IKEv2安全策略引用的IKEv2安全提议名称

【相关命令】

- **ikev2 policy**

3.1.7 display ikev2 profile

display ikev2 profile 命令用来显示 IKEv2 profile 的配置信息。

【命令】

```
display ikev2 profile [ profile-name ]
```

【视图】

任意视图

【缺省用户角色】

```

network-admin
network-operator

```

【参数】

profile-name: IKEv2 profile 的名称，为 1~63 个字符的字符串，不区分大小写。如果不指定本参数，则表示显示所有 IKEv2 profile 的配置信息。

【举例】

显示所有 IKEv2 profile 的配置信息。

```

<Sysname> display ikev2 profile
IKEv2 profile: 1
Priority: 100
Match criteria:
  Local address 1.1.1.1
  Local address Vlan-interface100
  Local address 1::1:1
  Remote identity ipv4 address 3.3.3.3/32

```

```

VRF vrf1
Inside-vrf:
Local identity: address 1.1.1.1
Local authentication method: pre-share
Remote authentication methods: pre-share
Keychain: Keychain1
Sign certificate domain:
    Domain1
    abc
Verify certificate domain:
    Domain2
    YY
SA duration: 500
DPD: Interval 32, retry 23, periodic
Config exchange: Request, Set send, Set accept
NAT keepalive: 10
AAA authorization: Domain domain1, username ikev2

```

表3-1 display ikev2 profile 命令显示信息描述表

字段	描述
IKEv2 profile	IKEv2 profile的名称
Priority	IKEv2 profile的优先级
Match criteria	查找IKEv2 profile的匹配条件
Inside-vrf	（暂不支持）内网VRF名称
Local identity	本端身份信息
Local authentication method	本端认证方法
Remote authentication methods	对端认证方法
Keychain	IKEv2 profile引用的keychain
Sign certificate domain	用于签名的PKI域
Verify certificate domain	用于验证的PKI域
SA duration	IKEv2 SA生命周期
DPD	DPD功能参数：探测的间隔时间（单位为秒）、重传时间间隔（单位为秒）、探测模式（按需探测或周期探测） 若未开启DPD功能，则显示为Disabled
Config exchange	配置交换功能： <ul style="list-style-type: none"> Request: 表示本端将在 Auth 交换请求报文中携带配置交换请求载荷 Set accept: 表示本端可接受配置交换设置载荷 Set send: 表示本端可发送配置交换设置载荷
NAT keepalive	发送NAT保活报文的时间间隔（单位为秒）

【相关命令】

- ikev2 profile

3.1.8 display ikev2 proposal

display ikev2 proposal 命令用来显示 IKEv2 安全提议的配置信息。

【命令】

```
display ikev2 proposal [ name | default ]
```

【视图】

任意视图

【缺省用户角色】

- network-admin
- network-operator

【参数】

name: IKEv2 安全提议的名称，为 1~63 个字符的字符串，不区分大小写。
default: 缺省的 IKEv2 安全提议。

【使用指导】

IKEv2 安全提议按照优先级从高到低的顺序显示。若不指定任何参数，则显示所有 IKEv2 提议的配置信息。

【举例】

```
# 显示所有 IKEv2 安全提议的配置信息。
<Sysname> display ikev2 proposal
IKEv2 proposal : 1
  Encryption: 3DES-CBC AES-CBC-128 AES-CTR-192 CAMELLIA-CBC-128
  Integrity: MD5 SHA256 AES-XCBC-MAC
  PRF: MD5 SHA256 AES-XCBC-MAC
  DH Group: MODP1024/Group2 MODP1536/Group5

IKEv2 proposal : default
  Encryption: AES-CBC-128 3DES-CBC
  Integrity: SHA1 MD5
  PRF: SHA1 MD5
  DH Group: MODP1536/Group5 MODP1024/Group2
```

表3-2 display ikev2 proposal 命令显示信息描述表

字段	描述
IKEv2 proposal	IKEv2安全提议的名称
Encryption	IKEv2安全提议采用的加密算法
Integrity	IKEv2安全提议采用的完整性校验算法
PRF	IKEv2安全提议采用的PRF算法

字段	描述
DH Group	IKEv2安全提议采用的DH组

【相关命令】

- **ikev2 proposal**

3.1.9 display ikev2 sa

display ikev2 sa 命令用来显示 IKEv2 SA 的信息。

【命令】

```
display ikev2 sa [ count | [ { local | remote } { ipv4-address | ipv6
ipv6-address } ] [ verbose [ tunnel tunnel-id ] ] ]
```

【视图】

任意视图

【缺省用户角色】

network-admin
network-operator

【参数】

count: 显示 IKEv2 SA 的数量。

local: 显示指定本端地址的 IKEv2 SA 信息。

remote: 显示指定对端地址的 IKEv2 SA 信息。

ipv4-address: 本端或对端的 IPv4 地址。

ipv6 ipv6-address: 本端或对端的 IPv6 地址。

verbose: 显示 IKEv2 SA 的详细信息。如果不指定该参数，则表示显示 IKEv2 SA 的摘要信息。

tunnel tunnel-id: 显示指定 IPsec 隧道的 IKEv2 SA 详细信息。*tunnel-id* 为 IPsec 隧道标识符，取值范围为 1~2000000000。

【使用指导】

若不指定任何参数，则显示所有 IKEv2 SA 的摘要信息。

【举例】

显示所有 IKEv2 SA 的摘要信息。

```
<Sysname> display ikev2 sa
```

Tunnel ID	Local	Remote	Status
1	1.1.1.1/500	1.1.1.2/500	EST
2	2.2.2.1/500	2.2.2.2/500	EST

Status:

IN-NEGO: Negotiating, EST: Established, DEL: Deleting

显示对端地址为 1.1.1.2 的 IKEv2 SA 的摘要信息。

```
<Sysname> display ikev2 sa remote 1.1.1.2
```

Tunnel ID	Local	Remote	Status
1	1.1.1.1/500	1.1.1.2/500	EST

Status:

IN-NEGO: Negotiating, EST: Established, DEL: Deleting

表3-3 display ikev2 sa 命令显示信息描述表

字段	描述
Tunnel ID	IKEv2 SA的隧道标识符
Local	IKEv2 SA的本端IP地址
Remote	IKEv2 SA的对端IP地址
Status	IKEv2 SA的状态： <ul style="list-style-type: none"> IN-NEGO (Negotiating)：表示此 IKE SA 正在协商 EST (Established)：表示此 IKE SA 已建立成功 DEL (Deleting)：表示此 IKE SA 将被删除

显示所有 IKEv2 SA 的详细信息。

```
<Sysname> display ikev2 sa verbose
Tunnel ID: 1
Local IP/Port: 1.1.1.1/500
Remote IP/Port: 1.1.1.2/500
Outside VRF: -
Inside VRF: -
Local SPI: 8f8af3dbf5023a00
Remote SPI: 0131565b9b3155fa

Local ID type: FQDN
Local ID: device_a
Remote ID type: FQDN
Remote ID: device_b

Auth sign method: Pre-shared key
Auth verify method: Pre-shared key
Integrity algorithm: HMAC_MD5
PRF algorithm: HMAC_MD5
Encryption algorithm: AES-CBC-192

Life duration: 86400 secs
Remaining key duration: 85604 secs
Diffie-Hellman group: MODP1024/Group2
NAT traversal: Not detected
DPD: Interval 20 secs, retry interval 2 secs
Transmitting entity: Initiator

Local window: 1
Remote window: 1
```

Local request message ID: 2
Remote request message ID: 2
Local next message ID: 0
Remote next message ID: 0

Pushed IP address: 192.168.1.5
Assigned IP address: 192.168.2.24

显示对端地址为 1.1.1.2 的 IKEv2 SA 的详细信息。

<Sysname> display ikev2 sa remote 1.1.1.2 verbose

Tunnel ID: 1
Local IP/Port: 1.1.1.1/500
Remote IP/Port: 1.1.1.2/500
Outside VRF: -
Inside VRF: -
Local SPI: 8f8af3dbf5023a00
Remote SPI: 0131565b9b3155fa

Local ID type: FQDN
Local ID: device_a
Remote ID type: FQDN
Remote ID: device_b

Auth sign method: Pre-shared key
Auth verify method: Pre-shared key
Integrity algorithm: HMAC_MD5
PRF algorithm: HMAC_MD5
Encryption algorithm: AES-CBC-192

Life duration: 86400 secs
Remaining key duration: 85604 secs
Diffie-Hellman group: MODP1024/Group2
NAT traversal: Not detected
DPD: Interval 30 secs, retry interval 10 secs
Transmitting entity: Initiator

Local window: 1
Remote window: 1
Local request message ID: 2
Remote request message ID: 2
Local next message ID: 0
Remote next message ID: 0

Pushed IP address: 192.168.1.5
Assigned IP address: 192.168.2.24

表3-4 display ikev2 sa verbose 命令显示信息描述表

字段	描述
Tunnel ID	IKEv2 SA的隧道标识符
Local IP/Port	本端安全网关的IP地址/端口号
Remote IP/Port	对端安全网关的IP地址/端口号
Outside VRF	（暂不支持）出方向被保护数据所属的VRF名称，-表示属于公网
Inside VRF	（暂不支持）入方向被保护数据所属的VRF名称，-表示属于公网
Local SPI	本端安全参数索引
Remote SPI	对端安全参数索引
Local ID type	本端安全网关的身份信息类型
Local ID	本端安全网关的身份信息
Remote ID type	对端安全网关的身份信息类型
Remote ID	对端安全网关的身份信息
Auth sign method	IKEv2安全提议中认证使用的签名方法
Auth verify method	IKEv2安全提议中认证使用的验证方法
Integrity algorithm	IKEv2安全提议中使用的完整性算法
PRF algorithm	IKEv2安全提议中使用的PRF算法
Encryption algorithm	IKEv2安全提议中使用的加密算法
Life duration	IKEv2 SA的生命周期（单位为秒）
Remaining key duration	IKEv2 SA的剩余生命周期（单位为秒）
Diffie-Hellman group	IKEv2密钥协商时所使用的DH密钥交换参数
NAT traversal	是否检测到协商双方之间存在NAT网关设备
DPD	DPD探测的时间间隔和重传时间（单位为秒），若未开启DPD探测功能，则显示为Disabled
Transmitting entity	IKEv2协商中的实体角色：发起方、响应方
Local window	本端IKEv2协商的窗口大小
Remote window	对端IKEv2协商的窗口大小
Local request message ID	本端下一次要发送的请求消息的序号
Remote request message ID	对端下一次要发送的请求消息的序号
Local next message ID	本端期望下一个接收消息的序号
Remote next message ID	对端期望下一个接收消息的序号
Pushed IP address	对端推送给本端的IP地址
Assigned IP address	本端分配给对端的IP地址

```
# 显示所有 IKEv2 SA 的个数。  
[Sysname-probe] display ikev2 sa count  
IKEv2 SAs count: 0
```

表3-5 display ikev2 sa count 命令显示信息描述表

字段	描述
IKEv2 SAs count	IKEv2 SA的总数

3.1.10 display ikev2 statistics

display ikev2 statistics 命令用来显示 IKEv2 统计信息。

【命令】

```
display ikev2 statistics
```

【视图】

任意视图

【缺省用户角色】

```
network-admin  
network-operator
```

【举例】

```
# 显示 IKEv2 的统计信息。  
<Sysname> display ikev2 statistics  
IKEv2 statistics:  
  Unsupported critical payload: 0  
  Invalid IKE SPI: 0  
  Invalid major version: 0  
  Invalid syntax: 0  
  Invalid message ID: 0  
  Invalid SPI: 0  
  No proposal chosen: 0  
  Invalid KE payload: 0  
  Authentication failed: 0  
  Single pair required: 0  
  TS unacceptable: 0  
  Invalid selectors: 0  
  Temporary failure: 0  
  No child SA: 0  
  Unknown other notify: 0  
  No enough resource: 0  
  Enqueue error: 0  
  No IKEv2 SA: 0  
  Packet error: 0  
  Other error: 0  
  Retransmit timeout: 0
```

```

DPD detect error: 0
Del child for IPsec message: 1
Del child for deleting IKEv2 SA: 1
Del child for receiving delete message: 0

```

表3-6 display ikev2 statistics 命令显示信息描述表

字段	描述
IKEv2 statistics	IKEv2统计信息
Unsupported critical payload	不支持的重要载荷
Invalid IKE SPI	无效的IKE SPI信息
Invalid major version	无效的主版本号
Invalid syntax	无效的语法
Invalid message ID	无效的Message ID
Invalid SPI	无效的SPI
No proposal chosen	提议不匹配
Invalid IKE payload	无效的IKE载荷
Authentication failed	认证失败
Single pair required	需要特定的地址对
TS unacceptable	不可接受的Traffic Selectors
Invalid selectors	无效的Selector
Temporary failure	临时错误
No child SA	找不到Child SA
Unknown other notify	未定义的其它通知类型
No enough resource	资源不够
Enqueue error	入队列错误
No IKEv2 SA	没有IKEv2 SA
Packet error	报文错误
Other error	其它错误
Retransmit timeout	重传超时
Dpd detect error	DPD探测失败
Del child for IPsec message	由于收到IPsec消息删除Child SA
Del child for deleting IKEv2 SA	由于删除IKEv2 SA删除Child SA
Del child for receiving delete message	由于收到删除消息删除Child SA

【相关命令】

- `reset ikev2 statistics`

3.1.11 dpd

`dpd` 用来配置 IKEv2 DPD 探测功能。

`undo dpd` 命令用来关闭 IKEv2 DPD 探测功能。

【命令】

```
dpd interval interval [ retry seconds ] { on-demand | periodic }  
undo dpd interval
```

【缺省情况】

IKEv2 profile 视图下的 DPD 探测功能处于关闭状态，使用全局的 DPD 配置。

【视图】

IKEv2 profile 视图

【缺省用户角色】

network-admin

【参数】

interval interval: 指定 IKEv2 DPD 探测的间隔时间，取值范围为 10~3600，单位为秒。对于按需探测模式，指定经过多长时间没有从对端收到 IPsec 报文，则本端发送 IPsec 报文时触发 DPD 探测；对于定时探测模式，指触发一次 DPD 探测的时间间隔。

retry seconds: 指定 DPD 报文的重传时间间隔，取值范围为 2~60，单位为秒。缺省值为 5 秒。

on-demand: 指定按需探测模式，即根据流量来探测对端是否存活，在本端发送用户报文时，如果发现当前距离最后一次收到对端报文的时间超过指定的触发 IKEv2 DPD 探测的时间间隔，则触发 DPD 探测。

periodic: 指定定时探测模式，即按照触发 IKEv2 DPD 探测的时间间隔定时探测对端是否存活。

【使用指导】

IKEv2 DPD 有两种模式：按需探测模式和定时探测模式。一般若无特别要求，建议使用按需探测模式，在此模式下，仅在本端需要发送报文时，才会触发探测；如果需要尽快地检测出对端的状态，则可以使用定时探测模式。在定时探测模式下工作，会消耗更多的带宽和计算资源，因此当设备与大量的 IKEv2 对端通信时，应优先考虑使用按需探测模式。

配置的 **interval** 一定要大于 **retry**，保证在重传 DPD 报文的过程中不触发新的 DPD 探测。

【举例】

为 IKEv2 profile1 配置 IKEv2 DPD 功能，指定若 10 秒内没有从对端收到 IPsec 报文，则触发 IKEv2 DPD 探测，DPD 请求报文的重传时间间隔为 5 秒，探测模式为按需探测。

```
<Sysname> system-view  
[Sysname] ikev2 profile profile1  
[Sysname-ikev2-profile-profile1] dpd interval 10 retry 5 on-demand
```

【相关命令】

- `ikev2 dpd`

3.1.12 encryption

`encryption` 命令用来指定 IKEv2 安全提议使用的加密算法。

`undo encryption` 命令用来恢复缺省情况。

【命令】

非 FIPS 模式下:

```
encryption { 3des-cbc | aes-cbc-128 | aes-cbc-192 | aes-cbc-256 | aes-ctr-128  
| aes-ctr-192 | aes-ctr-256 | camellia-cbc-128 | camellia-cbc-192 |  
camellia-cbc-256 | des-cbc } *
```

```
undo encryption
```

FIPS 模式下:

```
encryption { aes-cbc-128 | aes-cbc-192 | aes-cbc-256 | aes-ctr-128 |  
aes-ctr-192 | aes-ctr-256 } *
```

```
undo encryption
```

【缺省情况】

IKEv2 安全提议未定义加密算法。

【视图】

IKEv2 安全提议视图

【缺省用户角色】

network-admin

【参数】

3des-cbc: 指定 IKEv2 安全提议采用的加密算法为 CBC 模式的 3DES 算法, 3DES 算法采用 168 比特的密钥进行加密。

aes-cbc-128: 指定 IKEv2 安全提议采用的加密算法为 CBC 模式的 AES 算法, AES 算法采用 128 比特的密钥进行加密。

aes-cbc-192: 指定 IKEv2 安全提议采用的加密算法为 CBC 模式的 AES 算法, AES 算法采用 192 比特的密钥进行加密。

aes-cbc-256: 指定 IKEv2 安全提议采用的加密算法为 CBC 模式的 AES 算法, AES 算法采用 256 比特的密钥进行加密。

aes-ctr-128: 指定 IKEv2 安全提议采用的加密算法为 CTR 模式的 AES 算法, 密钥长度为 128 比特。

aes-ctr-192: 指定 IKEv2 安全提议采用的加密算法为 CTR 模式的 AES 算法, 密钥长度为 192 比特。

aes-ctr-256: 指定 IKEv2 安全提议采用的加密算法为 CTR 模式的 AES 算法, 密钥长度为 256 比特。

camellia-cbc-128: 指定 IKEv2 安全提议采用的加密算法为 CBC 模式的 camellia 算法，密钥长度为 128 比特。

camellia-cbc-192: 指定 IKEv2 安全提议采用的加密算法为 CBC 模式的 camellia 算法，密钥长度为 192 比特。

camellia-cbc-256: 指定 IKEv2 安全提议采用的加密算法为 CBC 模式的 camellia 算法，密钥长度为 256 比特。

des-cbc: 指定 IKEv2 安全提议采用的加密算法为 CBC 模式的 DES 算法，DES 算法采用 56 比特的密钥进行加密。

【使用指导】

IKEv2 安全提议中至少需要配置一个加密算法，否则该安全提议不完整，也不可用。一个 IKEv2 安全提议中可以配置多个加密算法，其使用优先级按照配置顺序依次降低。

【举例】

指定 IKEv2 安全提议 1 的加密算法为 CBC 模式的 168-bit 3DES。

```
<Sysname> system-view
[Sysname] ikev2 proposal prop1
[Sysname-ikev2-proposal-prop1] encryption 3des-cbc
```

【相关命令】

- **ikev2 proposal**

3.1.13 hostname

hostname 命令用来指定 IKEv2 peer 的主机名称。

undo hostname 命令用来恢复缺省情况。

【命令】

```
hostname name
undo hostname
```

【缺省情况】

未配置 IKEv2 peer 的主机名称。

【视图】

IKEv2 peer 视图

【缺省用户角色】

network-admin

【参数】

name: IKEv2 peer 主机名称，为 1~253 个字符的字符串，不区分大小写。

【使用指导】

主机名仅适用于在基于 IPsec 安全策略的 IKEv2 协商中发起方查询 IKEv2 peer，不适用于基于 IPsec 虚拟隧道接口的 IKEv2 协商。

【举例】

```
# 创建 IKEv2 keychain, 名称为 key1。
<Sysname> system-view
[Sysname] ikev2 keychain key1
# 创建一个 IKEv2 peer, 名称为 peer1。
[Sysname-ikev2-keychain-key1] peer peer1
# 指定 IKEv2 peer 的主机名为 test。
[Sysname-ikev2-keychain-key1-peer-peer1] hostname test
```

【相关命令】

- **ikev2 keychain**
- **peer**

3.1.14 identity

identity 命令用来指定 IKEv2 peer 的身份信息。

undo identity 命令用来恢复缺省情况。

【命令】

```
identity { address { ipv4-address | ipv6 { ipv6-address } } | fqdn fqdn-name |  
email email-string | key-id key-id-string }  
undo identity
```

【缺省情况】

未指定 IKEv2 peer 的身份信息。

【视图】

IKEv2 peer 视图

【缺省用户角色】

network-admin

【参数】

ipv4-address: 对端 IPv4 地址。

ipv6 *ipv6-address*: 对端 IPv6 地址。

fqdn *fqdn-name*: 对端 FQDN 名称, 为 1~255 个字符的字符串, 区分大小写, 例如 **www.test.com**。

email *email-string*: 指定标识对端身份的 E-mail 地址。 *email-string* 为按照 RFC 822 定义的 1~255 个字符的字符串, 区分大小写, 例如 **esec@test.com**。

key-id *key-id-string*: 指定标识对端身份的 Key-ID 名称。 *key-id-string* 为 1~255 个字符的字符串, 区分大小写, 通常为具体厂商的某种私有标识字符串。

【使用指导】

对等体身份信息仅用于 IKEv2 协商的响应方查询 IKEv2 peer, 因为发起方在发起 IKEv2 协商时并不知道对端的身份信息。

【举例】

```
# 创建一个 IKEv2 keychain, 名称为 key1。
<Sysname> system-view
[Sysname] ikev2 keychain key1
# 创建一个 IKEv2 peer, 名称为 peer1。
[Sysname-ikev2-keychain-key1] peer peer1
# 指定 IKEv2 peer 的身份信息为地址 1.1.1.2。
[Sysname-ikev2-keychain-key1-peer-peer1] identity address 1.1.1.2
```

【相关命令】

- **ikev2 keychain**
- **peer**

3.1.15 identity local

identity local 命令用来配置本端身份信息，用于在 IKEv2 认证协商阶段向对端标识自己的身份。

undo identity local 命令用来恢复缺省情况。

【命令】

```
identity local { address { ipv4-address | ipv6 ipv6-address } | dn | email email-string | fqdn fqdn-name | key-id key-id-string }
undo identity local
```

【缺省情况】

未指定 IKEv2 本端身份信息，使用应用 IPsec 安全策略的接口的 IP 地址作为本端身份。

【视图】

IKEv2 profile 视图

【缺省用户角色】

network-admin

【参数】

address { *ipv4-address* | **ipv6** *ipv6-address* }：指定标识本端身份的 IP 地址，其中 *ipv4-address* 为标识本端身份的 IPv4 地址，*ipv6-address* 为标识本端身份的 IPv6 地址。

dn：使用从本端数字证书中获得的 DN 名作为本端身份。

email *email-string*：指定标识本端身份的 E-mail 地址。*email-string* 为按照 RFC 822 定义的 1~255 个字符的字符串，区分大小写，例如 **sec@abc.com**。

fqdn *fqdn-name*：指定标识本端身份的 FQDN 名称。*fqdn-name* 为 1~255 个字符的字符串，区分大小写，例如 **www.test.com**。

key-id *key-id-string*：指定标识本端身份的 Key-ID 名称。*key-id-string* 为 1~255 个字符的字符串，区分大小写，通常为具体厂商的某种私有标识字符串。

【使用指导】

交换的身份信息用于协商双方在协商时识别对端身份。

【举例】

```
#创建 IKEv2 profile, 名称为 profile1。
<Sysname> system-view
[Sysname] ikev2 profile profile1
# 指定使用 IP 地址 2.2.2.2 标识本端身份。
[Sysname-ikev2-profile-profile1] identity local address 2.2.2.2
```

【相关命令】

- `peer`

3.1.16 ikev2 cookie-challenge

ikev2 cookie-challenge 命令用来开启 cookie-challenge 功能。
undo ikev2 cookie-challenge 命令用来关闭 cookie-challenge 功能。

【命令】

```
ikev2 cookie-challenge number
undo ikev2 cookie-challenge
```

【缺省情况】

IKEv2 cookie-challenge 功能处于关闭状态。

【视图】

系统视图

【缺省用户角色】

network-admin

【参数】

number: 指定触发响应方启用 cookie-challenge 功能的阈值，取值范围为 0~1000。

【使用指导】

若响应方配置了 cookie-challenge 功能，当响应方发现存在的半开 IKE SA 超过指定的数目时，就启用 cookie-challenge 机制。响应方收到 IKE_SA_INIT 请求后，构造一个 Cookie 通知载荷并响应发起方，若发起方能够正确携带收到的 Cookie 通知载荷向响应方重新发起 IKE_SA_INIT 请求，则可以继续后续的协商过程，防止由于源 IP 仿冒而耗费大量响应方的系统资源，造成对响应方的 DoS 攻击。

【举例】

```
# 开启 cookie-challenge 功能，并配置启用 cookie-challenge 功能的阈值为 450。
<Sysname> system-view
[Sysname] ikev2 cookie-challenge 450
```

3.1.17 ikev2 dpd

ikev2 dpd 命令用来配置全局 IKEv2 DPD 功能。
undo ikev2 dpd 命令用来关闭全局 IKEv2 DPD 功能。

【命令】

```
ikev2 dpd interval interval [ retry seconds ] { on-demand | periodic }  
undo ikev2 dpd interval
```

【缺省情况】

IKEv2 DPD 探测功能处于关闭状态。

【视图】

系统视图

【缺省用户角色】

network-admin

【参数】

interval interval: 指定触发 IKEv2 DPD 探测的时间间隔，取值范围为 10~3600，单位为秒。
对于按需探测模式，指定经过多长时间没有从对端收到 IPsec 报文，则发送报文前触发一次 DPD 探测；对于定时探测模式，指触发一次 DPD 探测的时间间隔。

retry seconds: 指定 DPD 报文的重传时间间隔，取值范围为 2~60，单位为秒，缺省值为 5 秒。

on-demand: 指定按需探测模式，即根据流量来探测对端是否存活，在本端发送 IPsec 报文时，如果发现当前距离最后一次收到对端报文的时间超过指定的触发 IKEv2 DPD 探测的时间间隔（即通过 *interval* 指定的时间），则触发 DPD 探测。

periodic: 指定定时探测模式，即按照触发 IKEv2 DPD 探测的时间间隔（即通过 *interval* 指定的时间）定时探测对端是否存活。

【使用指导】

IKEv2 DPD 有两种模式：按需探测模式和定时探测模式。一般若无特别要求，建议使用按需探测模式，在此模式下，仅在本端需要发送报文时，才会触发探测；如果需要尽快地检测出对端的状态，则可以使用定时探测模式。在定时探测模式下工作，会消耗更多的带宽和计算资源，因此当设备与大量的 IKEv2 对端通信时，应优先考虑使用按需探测模式。

如果 IKEv2 profile 视图下和系统视图下都配置了 DPD 探测功能，则 IKEv2 profile 视图下的 DPD 配置生效，如果 IKEv2 profile 视图下没有配置 DPD 探测功能，则采用系统视图下的 DPD 配置。

配置的 **interval** 一定要大于 **retry**，保证在重传 DPD 报文的过程中不触发新的 DPD 探测。

【举例】

配置根据流量来触发 IKEv2 DPD 探测的时间间隔为 15 秒。

```
<Sysname> system-view
```

```
[Sysname] ikev2 dpd interval 15 on-demand
```

配置定时触发 IKEv2 DPD 探测的时间间隔为 15 秒。

```
<Sysname> system-view
```

```
[Sysname] ikev2 dpd interval 15 periodic
```

【相关命令】

- **dpd** (IKEv2 profile view)

3.1.18 ikev2 keychain

ikev2 keychain 命令用来创建 IKEv2 keychain，并进入 IKEv2 keychain 视图。如果指定的 IKEv2 keychain 已经存在，则直接进入 IKEv2 keychain 视图。

undo ikev2 keychain 命令用来删除指定的 IKEv2 keychain。

【命令】

```
ikev2 keychain keychain-name
undo ikev2 keychain keychain-name
```

【缺省情况】

不存在 IKEv2 keychain。

【视图】

系统视图

【缺省用户角色】

network-admin

【参数】

keychain-name: IKEv2 keychain 的名称，为 1~63 个字符的字符串，不区分大小写，且不能包括字符“-”。

【使用指导】

任何一端采用了预共享密钥认证方式时，IKEv2 profile 下必须引用 keychain，且只能引用一个。配置的预共享密钥的值需要与对端 IKEv2 网关上配置的预共享密钥的值相同。

一个 IKEv2 keychain 下可以配置多个 IKEv2 peer。

【举例】

创建 IKEv2 keychain key1 并进入 IKEv2 keychain 视图。

```
<Sysname> system-view
[Sysname] ikev2 keychain key1
[Sysname-ikev2-keychain-key1]
```

3.1.19 ikev2 nat-keepalive

ikev2 nat-keepalive 命令用来配置向对端发送 NAT Keepalive 报文的时间间隔。

undo ikev2 nat-keepalive 命令用来恢复缺省情况。

【命令】

```
ikev2 nat-keepalive seconds
undo ikev2 nat-keepalive
```

【缺省情况】

探测到 NAT 后发送 NAT Keepalive 报文的时间间隔为 10 秒。

【视图】

系统视图

【缺省用户角色】

network-admin

【参数】

seconds: 向对端发送 NAT Keepalive 报文的时间间隔，取值范围为 5～3600，单位为秒。

【使用指导】

该命令仅对位于 NAT 之后的设备(即该设备位于 NAT 设备连接的私网侧)有意义。NAT 之后的 IKEv2 网关设备需要定时向 NAT 之外的 IKEv2 网关设备发送 NAT Keepalive 报文，以确保 NAT 设备上相应于该流量的会话存活，从而让 NAT 之外的设备可以访问 NAT 之后的设备。因此，配置的发送 NAT Keepalive 报文的时间间隔需要小于 NAT 设备上会话表项的存活时间。

【举例】

配置向 NAT 发送 NAT Keepalive 报文的时间间隔为 5 秒。

```
<Sysname> system-view  
[Sysname] ikev2 nat-keepalive 5
```

3.1.20 ikev2 policy

ikev2 policy 命令用来创建 IKEv2 安全策略，并进入 IKEv2 安全策略视图。如果指定的 IKEv2 安全策略已经存在，则直接进入 IKEv2 安全策略视图。

undo ikev2 policy 命令用来删除指定的 IKEv2 安全策略。

【命令】

```
ikev2 policy policy-name  
undo ikev2 policy policy-name
```

【缺省情况】

系统中存在一个名称为 **default** 的缺省 IKEv2 安全策略，该缺省的策略中包含一个缺省的 IKEv2 安全提议 **default**，且可与所有的本端地址相匹配。

【视图】

系统视图

【缺省用户角色】

network-admin

【参数】

policy-name: IKEv2 安全策略的名称，为 1～63 个字符的字符串，不区分大小写。

【使用指导】

IKE_SA_INIT 协商时，发起方根据应用 IPsec 安全策略的接口地址来选择要使用的 IKEv2 安全策略；响应方根据收到 IKEv2 报文的接口地址来选择要使用的 IKEv2 安全策略。选定 IKEv2 安全策略后，设备将根据安全策略中的安全提议进行加密算法、完整性校验算法、PRF 算法和 DH 组的协商。可以配置多个 IKEv2 安全策略。一个 IKEv2 安全策略中必须至少包含一个 IKEv2 安全提议，否则该策略不完整。

若发起方使用共享源接口方式 IPsec 策略，则 IKE_SA_INIT 协商时，使用共享源接口地址来选择要使用的 IKEv2 安全策略。

相同匹配条件下，配置的优先级可用于调整匹配 IKEv2 安全策略的顺序。

如果没有配置 IKEv2 安全策略，则使用默认的 IKEv2 安全策略 default。用户不能进入并配置默认的 IKEv2 安全策略 default。

【举例】

创建 IKEv2 安全策略 policy1，并进入 IKEv2 安全策略视图。

```
<Sysname> system-view
[Sysname] ikev2 policy policy1
[Sysname-ikev2-policy-policy1]
```

【相关命令】

- **display ikev2 policy**

3.1.21 ikev2 profile

ikev2 profile 命令用来创建 IKEv2 profile，并进入 IKEv2 profile 视图。如果指定的 IKEv2 profile 已经存在，则直接进入 IKEv2 profile 视图。

undo ikev2 profile 命令用来删除指定的 IKEv2 profile。

【命令】

```
ikev2 profile profile-name
undo ikev2 profile profile-name
```

【缺省情况】

不存在 IKEv2 profile。

【视图】

系统视图

【缺省用户角色】

network-admin

【参数】

profile-name：IKEv2 profile 的名称，为 1~63 个字符的字符串，不区分大小写。

【使用指导】

IKEv2 profile 用于保存非协商的 IKEv2 SA 的参数，如本端和对端的身份、本端和对端的认证方式、用于查找 IKEv2 profile 的匹配条件等。

【举例】

创建 IKEv2 profile，名称为 profile1，并进入 IKEv2 profile 视图。

```
<Sysname> system-view
[Sysname] ikev2 profile profile1
[Sysname-ikev2-profile-profile1]
```


【相关命令】

- `display ikev2 profile`

3.1.22 ikev2 proposal

`ikev2 proposal` 命令用来创建 IKEv2 安全提议，并进入 IKEv2 安全提议视图。如果指定的 IKEv2 安全提议已经存在，则直接进入 IKEv2 安全提议视图。

`undo ikev2 proposal` 命令用来删除指定的 IKEv2 安全提议。

【命令】

`ikev2 proposal proposal-name`

`undo ikev2 proposal proposal-name`

【缺省情况】

系统中存在一个名称为 `default` 的缺省 IKEv2 安全提议。

非 FIPS 模式下，缺省提议使用的算法：

- 加密算法：AES-CBC-128 和 3DES
- 完整性校验算法：HMAC-SHA1 和 HMAC-MD5
- PRF 算法：HMAC-SHA1 和 HMAC-MD5
- DH：group5 和 group2

FIPS 模式下，缺省提议使用的算法：

- 加密算法：AES-CBC-128 和 AES-CTR-128
- 完整性校验算法：HMAC-SHA1 和 HMAC-SHA256
- PRF 算法：HMAC-SHA1 和 HMAC-SHA256
- DH：group14 和 group19

【视图】

系统视图

【缺省用户角色】

network-admin

【参数】

proposal-name：指定 IKEv2 安全提议的名称，为 1～63 个字符的字符串，不区分大小写，且不能为 `default`。

【使用指导】

IKEv2 安全提议用于保存 IKE_SA_INIT 交换中所使用的安全参数，包括加密算法、完整性验证算法、PRF（pseudo-random function）算法和 DH 组。

在一个 IKEv2 安全提议中，至少需要配置一组安全参数，即一个加密算法、一个完整性验证算法、一个 PRF 算法和一个 DH 组。

在一个 IKEv2 安全提议中，可以配置多组安全参数，即多个加密算法、多个完整性验证算法、多个 PRF 算法和多个 DH 组，这些安全参数在实际协商过程中，将会形成多种安全参数的组合与对端进

行匹配。若实际协商过程中仅希望使用一组安全参数，请保证在 IKEv2 安全提议中仅配置了一套安全参数。

【举例】

创建 IKEv2 安全提议 prop1，并配置加密算法为 aes-cbc-128，完整性校验算法为 sha1，PRF 算法为 sha1，DH 组为 group2。

```
<Sysname> system-view
[Sysname] ikev2 proposal prop1
[Sysname-ikev2-proposal-prop1] encryption-algorithm aes-cbc-128
[Sysname-ikev2-proposal-prop1] authentication-algorithm sha1
[Sysname-ikev2-proposal-prop1] prf sha1
[Sysname-ikev2-proposal-prop1] dh group2
```

【相关命令】

- **encryption-algorithm**
- **integrity**
- **prf**
- **dh**

3.1.23 integrity

integrity 命令用来指定 IKEv2 安全提议使用的完整性校验算法。

undo integrity 命令用来恢复缺省情况。

【命令】

非 FIPS 模式下：

```
integrity { aes-xcbc-mac | md5 | sha1 | sha256 | sha384 | sha512 } *
undo integrity
```

FIPS 模式下：

```
integrity { sha1 | sha256 | sha384 | sha512 } *
undo integrity
```

【缺省情况】

未指定 IKEv2 安全提议使用的完整性校验算法。

【视图】

IKEv2 安全提议视图

【缺省用户角色】

network-admin

【参数】

aes-xcbc-mac：指定 IKEv2 安全提议采用的完整性校验算法为 HMAC-AES-XCBC-MAC。

md5：指定 IKEv2 安全提议采用的完整性校验算法为 HMAC-MD5。

sha1：指定 IKEv2 安全提议采用的完整性校验算法为 HMAC-SHA-1。

sha256：指定 IKEv2 安全提议采用的完整性校验算法为 HMAC-SHA-256。

sha384: 指定 IKEv2 安全提议采用的完整性校验算法为 HMAC-SHA-384。

sha512: 指定 IKEv2 安全提议采用的完整性校验算法为 HMAC-SHA-512。

【使用指导】

一个 IKEv2 安全提议中至少需要配置一个完整性校验算法，否则该安全提议不完整。一个 IKEv2 安全提议中可以配置多个完整性校验算法，其使用优先级按照配置顺序依次降低。

【举例】

```
# 创建 IKEv2 安全提议 prop1。
<Sysname> system-view
[Sysname] ikev2 proposal prop1
# 指定该安全提议使用的完整性校验算法为 MD5 和 SHA1，且优先选择 SHA1。
[Sysname-ikev2-proposal-prop1] integrity sha1 md5
```

【相关命令】

- **ikev2 proposal**

3.1.24 keychain

keychain 命令用来配置采用预共享密钥认证时使用的 Keychain。

undo keychain 命令用来恢复缺省情况。

【命令】

```
keychain keychain-name
undo keychain
```

【缺省情况】

IKEv2 profile 中未引用 Keychain。

【视图】

IKEv2 profile 视图

【缺省用户角色】

network-admin

【参数】

keychain-name: IKEv2 keychain 名称，为 1~63 个字符的字符串，不区分大小写，且不能包括字符-。

【使用指导】

任何一端采用了预共享密钥认证方式时，IKEv2 profile 下必须引用 keychain，且只能引用一个。不同的 IKEv2 profile 可以共享同一个 IKEv2 keychain。

【举例】

```
# 创建 IKEv2 profile，名称为 profile1。
<Sysname> system-view
[Sysname] ikev2 profile profile1
# 指定 IKEv2 profile 引用的 keychain，keychain 的名称为 keychain1。
```

```
[Sysname-ikev2-profile-profile1] keychain keychain1
```

【相关命令】

- **display ikev2 profile**
- **ikev2 keychain**

3.1.25 match local (IKEv2 profile view)

match local 命令用来限制 IKEv2 profile 的使用范围。

undo match local 命令用来取消对 IKEv2 profile 使用范围的限制。

【命令】

```
match local address { interface-type interface-number | ipv4-address | ipv6  
ipv6-address }  
undo match local address { interface-type interface-number | ipv4-address  
| ipv6 ipv6-address }
```

【缺省情况】

未限制 IKEv2 profile 的使用范围。

【视图】

IKEv2 profile 视图

【缺省用户角色】

network-admin

【参数】

address: 指定 IKEv2 profile 只能用于指定地址或指定接口的地址上的 IKEv2 协商。

interface-type interface-number: 本端接口编号和接口名称，可以是任意三层接口。

ipv4-address: 本端接口 IPv4 地址。

ipv6 *ipv6-address*: 本端接口 IPv6 地址。

【使用指导】

此命令用于限制 IKEv2 profile 只能用于指定地址或指定接口上的地址协商，这里的地址指的是本端收到 IKEv2 报文的接口 IP 地址，即只有 IKEv2 协商报文从该地址接收时，才会采用该 IKEv2 profile。IKEv2 profile 优先级可以手工配置，先配置的优先级高。若希望本端在匹配某些 IKEv2 profile 的时候，不按照手工配置的顺序来查找，则可以通过本命令来指定这类 IKEv2 profile 的使用范围。例如，IKEv2 profile A 中的 **match remote** 地址范围大（**match remote identity address range 2.2.2.1 2.2.2.100**），IKEv2 profile B 中的 **match remote** 地址范围小（**match remote identity address range 2.2.2.1 2.2.2.10**），IKEv2 profile A 先于 IKEv2 profile B 配置。假设对端 IP 地址为 2.2.2.6，那么依据配置顺序本端总是选择 profile A 与对端协商。若希望本端接口（假设接口地址为 3.3.3.3）使用 profile B 与对端协商，可以配置 profile B 在指定地址 3.3.3.3 的接口上使用。

通过该命令可以指定多个本端匹配条件。

【举例】

```
# 创建 IKEv2 profile，名称为 profile1。
```

```
<Sysname> system-view
[Sysname] ikev2 profile profile1
# 限制 IKEv2 profile profile1 只能在 IP 地址为 2.2.2.2 的接口上使用。
[Sysname-ikev2-profile-profile1] match local address 2.2.2.2
```

【相关命令】

- **match remote**

3.1.26 match local address (IKEv2 policy view)

match local address 命令用来指定匹配 IKEv2 安全策略的本端地址。

undo match local address 命令用来删除指定的用于匹配 IKEv2 安全策略的本端地址。

【命令】

```
match local address { interface-type interface-number | ipv4-address | ipv6
ipv6-address }
undo match local address { interface-type interface-number | ipv4-address |
ipv6 ipv6-address }
```

【缺省情况】

未指定用于匹配 IKEv2 安全策略的本端地址，表示本策略可匹配所有本端地址。

【视图】

IKEv2 安全策略视图

【缺省用户角色】

network-admin

【参数】

interface-type interface-number: 本端接口编号和接口名称，可以是任意三层接口。

ipv4-address: 本端接口 IPv4 地址。

ipv6 *ipv6-address*: 本端接口 IPv6 地址。

【使用指导】

根据本端地址匹配 IKEv2 安全策略时，优先匹配指定了本端地址匹配条件的策略，其次匹配未指定本端地址匹配条件的策略。

【举例】

指定用于匹配 IKEv2 安全策略 policy1 的本端地址为 3.3.3.3。

```
<Sysname> system-view
[Sysname] ikev2 policy policy1
[Sysname-ikev2-policy-policy1] match local address 3.3.3.3
```

【相关命令】

- **display ikev2 policy**

3.1.27 match remote

match remote 命令用来配置匹配对端身份的规则。

undo match remote 命令用来删除一条用于匹配对端身份的规则。

【命令】

```
match remote { certificate policy-name | identity { address { { ipv4-address  
[ mask | mask-length ] | range low-ipv4-address high-ipv4-address } | ipv6  
{ ipv6-address [ prefix-length ] | range low-ipv6-address  
high-ipv6-address } } | fqdn fqdn-name | email email-string | key-id  
key-id-string } }  
  
undo match remote { certificate policy-name | identity { address  
{ { ipv4-address [ mask | mask-length ] | range low-ipv4-address  
high-ipv4-address } | ipv6 { ipv6-address [ prefix-length ] | range  
low-ipv6-address high-ipv6-address } } | fqdn fqdn-name | email email-string  
| key-id key-id-string } }
```

【缺省情况】

未配置用于匹配对端身份的规则。

【视图】

IKEv2 profile 视图

【缺省用户角色】

network-admin

【参数】

certificate policy-name: 基于对端数字证书中的信息匹配 IKEv2 profile。其中，*policy-name* 是证书访问控制策略的名称，为 1~31 个字符的字符串，不区分大小写。本参数用于基于对端数字证书中的信息匹配 IKEv2 profile。

identity: 基于指定的对端身份信息匹配 IKEv2 profile。本参数用于响应方根据发起方通过 **identity local** 命令配置的身份信息来选择使用的 IKEv2 profile。

address ipv4-address [mask | mask-length]: 对端 IPv4 地址或 IPv4 网段。其中，*ipv4-address* 为 IPv4 地址，*mask* 为子网掩码，*mask-length* 为子网掩码长度，取值范围为 0~32。

address range low-ipv4-address high-ipv4-address: 对端 IPv4 地址范围。其中 *low-ipv4-address* 为起始 IPv4 地址，*high-ipv4-address* 为结束 IPv4 地址。结束地址必须大于起始地址。

address ipv6 ipv6-address [prefix-length]: 对端 IPv6 地址或 IPv6 网段。其中，*ipv6-address* 为 IPv6 地址，*prefix-length* 为 IPv6 前缀长度，取值范围为 0~128。

address ipv6 range low-ipv6-address high-ipv6-address: 对端 IPv6 地址范围。其中 *low-ipv6-address* 为起始 IPv6 地址，*high-ipv6-address* 为结束 IPv6 地址。结束地址必须大于起始地址。

fqdn fqdn-name: 对端 FQDN 名称，为 1~255 个字符的字符串，区分大小写，例如 *www.test.com*。

email email-string: 指定标识对等体身份的 E-mail 地址。*email-string* 为按照 RFC 822 定义的 1~255 个字符的字符串，区分大小写，例如 *sec@abc.com*。

key-id *key-id-string*: 指定标识对等体身份的 Key-ID 名称。*key-id-string* 为 1~255 个字符的字符串，区分大小写，通常为具体厂商的某种私有标识字符串。

【使用指导】

查找对端匹配的 IKEv2 profile 时，对端需要同时满足以下条件：

- 将对端的身份信息与本命令配置的匹配规则进行比较，二者必须相同。
- 查找 IKEv2 profile 和验证对端身份时，需要使用 **match remote**、**match local address** 一起匹配，若有其中一项不符合，则表示该 IKEv2 profile 不匹配。

查找到匹配的 IKEv2 profile 后，本端设备将用该 IKEv2 profile 中的信息与对端完成认证。

为了使得每个对端能够匹配到唯一的 IKEv2 profile，不建议在两个或两个以上 IKEv2 profile 中配置相同的 **match remote** 规则，否则能够匹配到哪个 IKEv2 profile 是不可预知的。**match remote** 规则可以配置多个，并同时都有效，其匹配优先级为配置顺序。

【举例】

创建 IKEv2 profile，名称为 profile1。

```
<Sysname> system-view
```

```
[Sysname] ikev2 profile profile1
```

指定匹配采用 FQDN 作为身份标识、且取值为 www.test.com 的对端。

```
[Sysname-ikev2-profile-profile1] match remote identity fqdn www.test.com
```

指定匹配采用 IP 地址作为身份标识、且取值为 10.1.1.1。

```
[Sysname-ikev2-profile-profile1] match remote identity address 10.1.1.1
```

【相关命令】

- **identity local**
- **match local address**

3.1.28 nat-keepalive

nat-keepalive 命令用来配置发送 NAT keepalive 的时间间隔。

undo nat-keepalive 命令用来恢复缺省情况。

【命令】

```
nat-keepalive seconds
```

```
undo nat-keepalive
```

【缺省情况】

使用全局的 IKEv2 NAT keepalive 配置。

【视图】

IKEv2 profile 视图

【缺省用户角色】

network-admin

【参数】

seconds: 发送 NAT keepalive 报文的时间间隔，取值范围为 5~3600，单位为秒。

【使用指导】

该命令仅对位于 NAT 之后的设备(即该设备位于 NAT 设备连接的私网侧)有意义。NAT 之后的 IKEv2 网关设备需要定时向 NAT 之外的 IKEv2 网关设备发送 NAT Keepalive 报文，以确保 NAT 设备上相应于该流量的会话存活，从而让 NAT 之外的设备可以访问 NAT 之后的设备。因此，配置的发送 NAT Keepalive 报文的时间间隔需要小于 NAT 设备上会话表项的存活时间。

【举例】

```
# 创建 IKEv2 profile，名称为 profile1。
<Sysname> system-view
[Sysname] ikev2 profile profile1
# 配置发送 NAT keepalive 报文的时间间隔为 1200 秒。
[Sysname-ikev2-profile-profile1] nat-keepalive 1200
```

【相关命令】

- **display ikev2 profile**
- **ikev2 nat-keepalive**

3.1.29 peer

peer 命令用来创建 IKEv2 peer，并进入 IKEv2 peer 视图。如果指定的 IKEv2 peer 已经存在，则直接进入 IKEv2 peer 视图。

undo peer 命令用来删除指定的 IKEv2 peer。

【命令】

```
peer name
undo peer name
```

【缺省情况】

不存在 IKEv2 peer。

【视图】

IKEv2 keychain 视图

【缺省用户角色】

network-admin

【参数】

name: IKEv2 peer 名称，为 1~63 个字符的字符串，不区分大小写。

【使用指导】

一个 IKEv2 peer 中包含了一个预共享密钥以及用于查找该 peer 的匹配条件，包括对端的主机名称（由命令 **hostname** 配置）、对端的 IP 地址（由命令 **address** 配置）和对端的身份（由命令 **identity** 配置）。其中，IKEv2 协商的发起方使用对端的主机名称或 IP 地址查找 peer，响应方使用对端的身份或 IP 地址查找 peer。

【举例】

```
# 创建 IKEv2 keychain key1 并进入 IKEv2 keychain 视图。
```



```
<Sysname> system-view
[Sysname] ikev2 keychain key1
# 创建一个 IKEv2 peer，名称为 peer1。
[Sysname-ikev2-keychain-key1] peer peer1
```

【相关命令】

- **ikev2 keychain**

3.1.30 pre-shared-key

pre-shared-key 命令用来配置 IKEv2 peer 的预共享密钥。

undo pre-shared-key 命令用来删除 IKEv2 peer 的预共享密钥。

【命令】

```
pre-shared-key [ local | remote ] { ciphertext | plaintext } string
undo pre-shared-key [ local | remote ]
```

【缺省情况】

未配置 IKEv2 peer 的预共享密钥。

【视图】

IKEv2 peer 视图

【缺省用户角色】

network-admin

【参数】

local：表示签名密钥。

remote：表示验证密钥。

ciphertext：以密文方式设置密钥。

plaintext：以明文方式设置密钥，该密钥将以密文形式存储。

string：密钥字符串，区分大小写。非 FIPS 模式下，明文密钥为 1~128 个字符的字符串；密文密钥为 1~201 个字符的字符串。FIPS 模式下，明文密钥为 15~128 个字符的字符串；密文密钥为 15~201 个字符的字符串。

【使用指导】

如果指定了参数 **local** 或 **remote**，则表示指定的是非对称密钥；若参数 **local** 和 **remote** 均不指定，则表示指定的是对称密钥。

执行 **undo** 命令时，指定要删除的密钥类型必须和已配置的密钥类型完全一致，该 **undo** 命令才会执行成功。例如，IKEv2 peer 视图下仅有 **pre-shared-key local** 的配置，则执行 **undo pre-shared-key** 和 **undo pre-shared-key remote** 命令均无效。

多次执行本命令，最后一次执行的命令生效。

【举例】

- 发起方示例

创建一个 IKEv2 keychain，名称为 key1。

```
<Sysname> system-view
```

```
[Sysname] ikev2 keychain key1
# 创建一个 IKEv2 peer，名称为 peer1。
[Sysname-ikev2-keychain-key1] peer peer1
# 配置 peer1 的对称预共享密钥为明文 111-key。
[Sysname-ikev2-keychain-key1-peer-peer1] pre-shared-key plaintext 111-key
[Sysname-ikev2-keychain-key1-peer-peer1] quit
# 创建一个 IKEv2 peer，名称为 peer2。
[Sysname-ikev2-keychain-key1] peer peer2
# 配置 peer2 的非对称预共享密钥，签名密钥为明文 111-key-a，验证密钥为明文 111-key-b。
[Sysname-ikev2-keychain-key1-peer-peer2] pre-shared-key local plaintext 111-key-a
[Sysname-ikev2-keychain-key1-peer-peer2] pre-shared-key remote plaintext 111-key-b
• 响应方示例
# 创建一个 IKEv2 keychain，名称为 telecom。
<Sysname> system-view
[Sysname] ikev2 keychain telecom
# 创建一个 IKEv2 peer，名称为 peer1。
[Sysname-ikev2-keychain-telecom] peer peer1
# 配置 peer1 的对称预共享密钥为明文 111-key。
[Sysname-ikev2-keychain-telecom-peer-peer1] pre-shared-key plaintext 111-key
[Sysname-ikev2-keychain-telecom-peer-peer1] quit
# 创建一个 IKEv2 peer，名称为 peer2。
[Sysname-ikev2-keychain-telecom] peer peer2
# 配置 IKEv2 peer 的非对称预共享密钥，签名密钥为明文 111-key-b，验证密钥为明文 111-key-a。
[Sysname-ikev2-keychain-telecom-peer-peer2] pre-shared-key local plaintext 111-key-b
[Sysname-ikev2-keychain-telecom-peer-peer2] pre-shared-key remote plaintext 111-key-a
```

【相关命令】

- **ikev2 keychain**
- **peer**

3.1.31 prf

prf 命令用来指定 IKEv2 安全提议使用的 PRF 算法。

undo prf 命令用来恢复缺省情况。

【命令】

非 FIPS 模式下：

```
prf { aes-xcbc-mac | md5 | sha1 | sha256 | sha384 | sha512 } *
undo prf
```

FIPS 模式下：

```
prf { sha1 | sha256 | sha384 | sha512 } *
undo prf
```

【缺省情况】

IKEv2 安全提议使用配置的完整性校验算法作为 PRF 算法。

【视图】

IKEv2 安全提议视图

【缺省用户角色】

network-admin

【参数】

aes-xcbc-mac: 指定 IKEv2 安全提议采用的 PRF 算法为 HMAC-AES-XCBC-MAC。

md5: 指定 IKEv2 安全提议采用的 PRF 算法为 HMAC-MD5。

sha1: 指定 IKEv2 安全提议采用的 PRF 算法为 HMAC-SHA-1。

sha256: 指定 IKEv2 安全提议采用的 PRF 算法为 HMAC-SHA-256。

sha384: 指定 IKEv2 安全提议采用的 PRF 算法为 HMAC-SHA-384。

sha512: 指定 IKEv2 安全提议采用的 PRF 算法为 HMAC-SHA-512。

【使用指导】

一个 IKEv2 安全提议中可以配置多个 PRF 算法，其使用优先级按照配置顺序依次降低。

【举例】

```
# 创建 IKEv2 安全提议 prop1。
<Sysname> system-view
[Sysname] ikev2 proposal prop1
# 指定该安全提议使用的 PRF 算法为 MD5 和 SHA1，且优先选择 SHA1。
[Sysname-ikev2-proposal-prop1] prf sha1 md5
```

【相关命令】

- **ikev2 proposal**
- **integrity**

3.1.32 priority (IKEv2 policy view)

priority 命令用来指定 IKEv2 安全策略的优先级。

undo priority 命令用来恢复缺省情况。

【命令】

```
priority priority
undo priority
```

【缺省情况】

IKEv2 安全策略的优先级为 100。

【视图】

IKEv2 安全策略视图

【缺省用户角色】

network-admin

【参数】

priority: IKEv2 安全策略优先级，取值范围为 1~65535。该数值越小，优先级越高。

【使用指导】

本命令配置的优先级仅用于响应方在查找 IKEv2 安全策略时调整 IKEv2 安全策略的匹配顺序。

【举例】

指定 IKEv2 安全策略 policy1 的优先级为 10。

```
<Sysname> system-view
[Sysname] ikev2 policy policy1
[Sysname-ikev2-policy-policy1] priority 10
```

【相关命令】

- **display ikev2 policy**

3.1.33 priority (IKEv2 profile view)

priority 命令用来配置 IKEv2 profile 的优先级。

undo priority 命令用来恢复缺省情况。

【命令】

```
priority priority
undo priority
```

【缺省情况】

IKEv2 profile 的优先级为 100。

【视图】

IKEv2 profile 视图

【缺省用户角色】

network-admin

【参数】

priority: IKEv2 profile 优先级，取值范围为 1~65535。该数值越小，优先级越高。

【使用指导】

本命令配置的优先级仅用于响应方在查找 IKEv2 Profile 时调整 IKEv2 Profile 的匹配顺序。

【举例】

指定 IKEv2 profile profile1 的优先级为 10。

```
<Sysname> system-view
[Sysname] ikev2 profile profile1
[Sysname-ikev2-profile-profile1] priority 10
```

3.1.34 proposal

proposal 命令用来指定 IKEv2 安全策略引用的 IKEv2 安全提议。

undo proposal 命令用来取消 IKEv2 安全策略引用的 IKEv2 安全提议。

【命令】

```
proposal proposal-name  
undo proposal proposal-name
```

【缺省情况】

IKEv2 安全策略未引用 IKEv2 安全提议。

【视图】

IKEv2 安全策略视图

【缺省用户角色】

network-admin

【参数】

proposal-name: 被引用的 IKEv2 安全提议的名称，为 1~63 个字符的字符串，不区分大小写。

【使用指导】

若同时指定了多个 IKEv2 安全提议，则它们的优先级按照配置顺序依次降低。

【举例】

配置 IKEv2 安全策略 policy1 引用 IKEv2 安全提议 proposal1。

```
<Sysname> system-view  
[Sysname] ikev2 policy policy1  
[Sysname-ikev2-policy-policy1] proposal proposal1
```

【相关命令】

- **display ikev2 policy**
- **ikev2 proposal**

3.1.35 reset ikev2 sa

reset ikev2 sa 命令用来清除 IKEv2 SA。

【命令】

```
reset ikev2 sa [ [ { local | remote } { ipv4-address | ipv6 ipv6-address } ]  
| tunnel tunnel-id ] [ fast ]
```

【视图】

用户视图

【缺省用户角色】

network-admin

【参数】

local: 清除指定本端地址的 IKEv2 SA 信息。

remote: 清除指定对端地址的 IKEv2 SA 信息。

ipv4-address: 本端或对端的 IPv4 地址。

ipv6 *ipv6-address*: 本端或对端的 IPv6 地址。

tunnel *tunnel-id*: 清除指定 IPsec 隧道的 IKEv2 SA 信息, *tunnel-id* 为 IPsec 隧道标识符, 取值范围为 1~2000000000。

fast: 不等待对端的回应, 直接删除本端的 IKEv2 SA。若不指定本参数, 则表示需要在收到对端的删除通知响应之后, 再删除本端的 IKEv2 SA。

【使用指导】

清除 IKEv2 SA 时, 会向对端发送删除通知消息, 同时删除子 SA。

如果不指定任何参数, 则删除所有 IKEv2 SA 及其协商生成的子 SA。

【举例】

删除对端地址为 1.1.1.2 的 IKEv2 SA。

```
<Sysname> display ikev2 sa
```

Tunnel ID	Local	Remote	Status
1	1.1.1.1/500	1.1.1.2/500	EST
2	2.2.2.1/500	2.2.2.2/500	EST

```
Status:
IN-NEGO: Negotiating, EST: Established, DEL: Deleting
<Sysname> reset ikev2 sa remote 1.1.1.2
<Sysname> display ikev2 sa
```

Tunnel ID	Local	Remote	Status
2	2.2.2.1/500	2.2.2.2/500	EST

```
Status:
IN-NEGO: Negotiating, EST: Established, DEL: Deleting
```

【相关命令】

- **display ikev2 sa**

3.1.36 reset ikev2 statistics

reset ikev2 statistics 命令用来清除 IKEv2 统计信息。

【命令】

reset ikev2 statistics

【视图】

用户视图

【缺省用户角色】

network-admin

【举例】

清除 IKEv2 的统计信息。

```
<Sysname> reset ikev2 statistics
```

【相关命令】

- **display ikev2 statistics**

3.1.37 sa duration

sa duration 命令用来配置 IKEv2 SA 的生命周期。

undo sa duration 命令用来恢复缺省情况。

【命令】

sa duration *seconds*

undo sa duration

【缺省情况】

IKEv2 SA 的生命周期为 86400 秒。

【视图】

IKEv2 profile 视图

【缺省用户角色】

network-admin

【参数】

seconds: IKEv2 SA 的生命周期，取值范围为 120～86400，单位为秒。

【使用指导】

在一个 IKEv2 SA 的生命周期到达之前，可以用该 IKEv2 SA 进行其它 IKEv2 协商。因此一个生命周期较长的 IKEv2 SA 可以节省很多用于重新协商的时间。但是，IKEv2 SA 的生命周期越长，攻击者越容易收集到更多的报文信息来对它实施攻击。

本端和对端的 IKEv2 SA 生命周期可以不一致，也不需要进行协商，由生命周期较短的一方在本端 IKEv2 SA 生命周期到达之后发起重协商。

【举例】

创建 IKEv2 profile，名称为 profile1。

```
<Sysname> system-view
```

```
[Sysname] ikev2 profile profile1
```

配置 IKEv2 SA 的生命周期为 1200 秒。

```
[Sysname-ikev2-profile-profile1] sa duration 1200
```

【相关命令】

- **display ikev2 profile**

目 录

1 SSH.....	1-1
1.1 SSH服务器端配置命令	1-1
1.1.1 display ssh server.....	1-1
1.1.2 display ssh user-information.....	1-3
1.1.3 free ssh	1-4
1.1.4 scp server enable	1-4
1.1.5 sftp server enable	1-5
1.1.6 sftp server idle-timeout.....	1-6
1.1.7 ssh server acl	1-6
1.1.8 ssh server acl-deny-log enable	1-7
1.1.9 ssh server authentication-retries	1-8
1.1.10 ssh server authentication-timeout	1-9
1.1.11 ssh server compatible-ssh1x enable.....	1-9
1.1.12 ssh server dscp	1-10
1.1.13 ssh server enable.....	1-11
1.1.14 ssh server ipv6 acl	1-11
1.1.15 ssh server ipv6 dscp.....	1-12
1.1.16 ssh server key-re-exchange enable.....	1-13
1.1.17 ssh server pki-domain	1-14
1.1.18 ssh server port	1-14
1.1.19 ssh server rekey-interval.....	1-15
1.1.20 ssh user.....	1-16
1.2 SSH客户端配置命令	1-18
1.2.1 bye.....	1-18
1.2.2 cd.....	1-19
1.2.3 cdup	1-19
1.2.4 delete.....	1-20
1.2.5 delete ssh client server-public-key	1-20
1.2.6 dir	1-21
1.2.7 display scp client source	1-22
1.2.8 display sftp client source	1-22
1.2.9 display ssh client server-public-key.....	1-23
1.2.10 display ssh client source.....	1-24

1.2.11 exit	1-25
1.2.12 get	1-25
1.2.13 help	1-25
1.2.14 ls	1-26
1.2.15 mkdir	1-27
1.2.16 put	1-28
1.2.17 pwd	1-28
1.2.18 quit	1-29
1.2.19 remove	1-29
1.2.20 rename	1-29
1.2.21 rmdir	1-30
1.2.22 scp	1-30
1.2.23 scp client ipv6 source	1-34
1.2.24 scp client source	1-34
1.2.25 scp ipv6	1-35
1.2.26 scp ipv6 suite-b	1-39
1.2.27 scp suite-b	1-41
1.2.28 sftp	1-43
1.2.29 sftp client ipv6 source	1-46
1.2.30 sftp client source	1-47
1.2.31 sftp ipv6	1-47
1.2.32 sftp ipv6 suite-b	1-50
1.2.33 sftp suite-b	1-52
1.2.34 ssh client ipv6 source	1-54
1.2.35 ssh client source	1-55
1.2.36 ssh2	1-56
1.2.37 ssh2 ipv6	1-59
1.2.38 ssh2 ipv6 suite-b	1-62
1.2.39 ssh2 suite-b	1-64
1.3 SSH2 协议配置命令	1-66
1.3.1 display ssh2 algorithm	1-66
1.3.2 ssh2 algorithm cipher	1-67
1.3.3 ssh2 algorithm key-exchange	1-68
1.3.4 ssh2 algorithm mac	1-70
1.3.5 ssh2 algorithm public-key	1-71

1 SSH



说明

设备运行于 FIPS 模式时，本特性部分配置相对于非 FIPS 模式有所变化，具体差异请见本文相关描述。有关 FIPS 模式的详细介绍请参见“安全配置指导”中的“FIPS”。

1.1 SSH服务器端配置命令

1.1.1 display ssh server

display ssh server 命令用来在 SSH 服务器端显示该服务器的状态信息或会话信息。

【命令】

```
display ssh server { session | status }
```

【视图】

任意视图

【缺省用户角色】

network-admin
network-operator

【参数】

session: 显示 SSH 服务器的会话信息。

status: 显示 SSH 服务器的状态信息。

【举例】

在 SSH 服务器端显示该服务器的状态信息。

```
<Sysname> display ssh server status
Stelnet server: Disable
SSH version : 2.0
SSH authentication-timeout : 60 second(s)
SSH server key generating interval : 0 hour(s)
SSH authentication retries : 3 time(s)
SFTP server: Disable
SFTP server Idle-Timeout: 10 minute(s)
NETCONF server: Disable
SCP server: Disable
SSH Server PKI domain name: aaa
```

表1-1 display ssh server status 命令显示信息描述表

字段	描述
Stelnet server	Stelnet服务器功能的状态
SSH version	SSH协议版本 SSH服务器兼容SSH1时，协议版本为1.99；SSH服务器不兼容SSH1时，协议版本为2.0
SSH authentication-timeout	认证超时时间
SSH server key generating interval	RSA服务器密钥对的最小更新间隔时间
SSH authentication retries	SSH用户认证尝试的最大次数
SFTP server	SFTP服务器功能的状态
SFTP server Idle-Timeout	SFTP用户连接的空闲超时时间
NETCONF server	NETCONF over SSH服务器功能的状态
SCP server	SCP服务器功能的状态
SSH Server PKI domain name	SSH服务器PKI域配置

在 SSH 服务器端显示该服务器的会话信息。

```
<Sysname> display ssh server session
UserPid  SessID Ver  Encrypt  State          Retries  Serv  Username
184      0      2.0    aes128-cbc Established    1      Stelnet  abc@123
```

表1-2 display ssh server session 显示信息描述表

字段	描述
UserPid	用户进程PID
SessID	会话ID
Ver	SSH服务器的协议版本
Encrypt	SSH服务器本端使用的加密算法
State	会话状态，包括： <ul style="list-style-type: none">• Init: 初始化状态• Ver-exchange: 版本协商• Keys-exchange: 密钥交换• Auth-request: 用户认证• Serv-request: 服务请求• Established: 会话已经建立• Disconnected: 断开会话
Retries	认证失败的次数
Serv	服务类型，包括SCP、SFTP、Stelnet和NETCONF
Username	客户端登录服务器时采用的用户名

1.1.2 display ssh user-information

`display ssh user-information` 命令用来在 SSH 服务器端显示 SSH 用户的信息。

【命令】

`display ssh user-information [username]`

【视图】

任意视图

【缺省用户角色】

network-admin
network-operator

【参数】

username: SSH 用户名，为 1~80 个字符的字符串，区分大小写。如果没有指定本参数，则显示所有 SSH 用户的信息。

【使用指导】

本命令仅用来显示 SSH 服务器端通过 `ssh user` 命令配置的 SSH 用户信息。

【举例】

显示所有 SSH 用户的信息。

```
<Sysname> display ssh user-information
Total ssh users:2
Username           Authentication-type  User-public-key-name  Service-type
yemx                password              Stelnet|SFTP
test                publickey             pubkey                 SFTP
```

表1-3 display ssh user-information 显示信息描述表

字段	描述
Total ssh users	SSH用户的总数
Username	用户名
Authentication-type	认证类型，取值包括password、publickey、password-publickey和any
User-public-key-name	用户公钥名称 如果认证类型为password，则该字段显示为空
Service-type	服务类型，取值包括SCP、SFTP、Stelnet和NETCONF 如果设备同时显示多个SSH服务类型时用 隔开

【相关命令】

- ssh user

1.1.3 free ssh

free ssh 命令用来强制释放已建立的 SSH 连接。

【命令】

```
free ssh { user-ip { ip-address | ipv6 ipv6-address } [ port port-number ] |  
user-pid pid-number | username username }
```

【视图】

用户视图

【缺省用户角色】

network-admin

【参数】

user-ip: 根据 IP 地址强制释放已建立的 SSH 连接。

ip-address: 待释放的 SSH 连接的源 IPv4 地址。

ipv6 *ipv6-address*: 待释放的 SSH 连接的源 IPv6 地址。

port *port-number*: 待释放的 SSH 连接的源端口。*port-number* 为源端口号, 取值范围为 1~65535。未指定本参数时, 表示强制释放对应 IP 地址建立的所有 SSH 连接。

user-pid *pid-number*: 根据进程号强制释放已建立的 SSH 连接。*pid-number* 为待释放的 SSH 连接进程号, 取值范围为 1~2147483647。可以通过 **display ssh server session** 查看当前 SSH 连接的进程号。

username *username*: 根据用户名强制释放已建立的 SSH 连接, 可以通过 **display ssh server session** 查看当前 SSH 连接的用户名。

【举例】

强制释放通过 IPv4 地址 192.168.15.45 建立的 SSH 连接。

```
<Sysname> free ssh user-ip 192.168.15.45  
Releasing SSH connection. Continue? [Y/N]:y
```

强制释放通过 IPv6 地址 2000::11 建立的 SSH 连接。

```
<Sysname> free ssh user-ip ipv6 2000::11  
Releasing SSH connection. Continue? [Y/N]:y
```

强制释放进程号为 417 的 SSH 连接。

```
<Sysname> free ssh user-pid 417  
Releasing SSH connection. Continue? [Y/N]:y
```

强制释放通过用户名 sshuser 建立的 SSH 连接。

```
<Sysname> free ssh username sshuser  
Releasing SSH connection. Continue? [Y/N]:y
```

【相关命令】

- **display ssh server session**

1.1.4 scp server enable

scp server enable 命令用来开启 SCP 服务器功能。

undo scp server enable 命令用来关闭 SCP 服务器功能。

【命令】

```
scp server enable
undo scp server enable
```

【缺省情况】

SCP 服务器功能处于关闭状态。

【视图】

系统视图

【缺省用户角色】

network-admin

【举例】

```
# 开启 SCP 服务器功能。
<Sysname> system-view
[Sysname] scp server enable
```

【相关命令】

- **display ssh server**

1.1.5 sftp server enable

sftp server enable 命令用来开启 SFTP 服务器功能。

undo sftp server enable 命令用来关闭 SFTP 服务器功能。

【命令】

```
sftp server enable
undo sftp server enable
```

【缺省情况】

SFTP 服务器功能处于关闭状态。

【视图】

系统视图

【缺省用户角色】

network-admin

【举例】

```
# 开启 SFTP 服务器功能。
<Sysname> system-view
[Sysname] sftp server enable
```

【相关命令】

- **display ssh server**

1.1.6 sftp server idle-timeout

sftp server idle-timeout 命令用来在 SFTP 服务器端设置 SFTP 用户连接的空闲超时时间。

undo sftp server idle-timeout 命令用来恢复缺省情况。

【命令】

```
sftp server idle-timeout time-out-value
undo sftp server idle-timeout
```

【缺省情况】

SFTP 用户连接的空闲超时时间为 10 分钟。

【视图】

系统视图

【缺省用户角色】

network-admin

【参数】

time-out-value: 超时时间，取值范围为 1~35791，单位为分钟。

【使用指导】

当 SFTP 用户连接的空闲时间超过设定的阈值后，系统会自动断开此用户的连接，从而有效避免用户长期占用连接而不进行任何操作。若同一时间内并发的 SFTP 连接数较多，可适当减小该值，及时释放系统资源给新用户接入。

【举例】

设置 SFTP 用户连接的空闲超时时间为 500 分钟。

```
<Sysname> system-view
[Sysname] sftp server idle-timeout 500
```

【相关命令】

- **display ssh server**

1.1.7 ssh server acl

ssh server acl 命令用来设置对 IPv4 SSH 客户端的访问控制。

undo ssh server acl 命令用来恢复缺省情况。

【命令】

```
ssh server acl { advanced-acl-number | basic-acl-number | mac
mac-acl-number }
undo ssh server acl
```

【缺省情况】

允许所有 IPv4 SSH 客户端向设备发起 SSH 访问。

【视图】

系统视图

【缺省用户角色】

network-admin

【参数】

advanced-acl-number: 指定 IPv4 高级 ACL，取值范围为 3000～3999。

basic-acl-number: 指定 IPv4 基本 ACL，取值范围为 2000～2999。

mac *acl-number*: 指定二层 ACL。*acl-number* 是二层 ACL 的编号，取值范围为 4000～4999。

【使用指导】

对 IPv4 SSH 客户端的访问控制通过引用 ACL 来实现，具体情况如下：

- 当引用的 ACL 不存在或者引用的 ACL 为空时，允许所有 IPv4 SSH 客户端访问设备。
- 当引用的 ACL 非空时，则只有匹配 ACL 中 **permit** 规则的 IPv4 SSH 客户端可以访问设备，其他客户端不可以访问设备。

该配置生效后，只会过滤新建立的 SSH 连接，不会影响已建立的 SSH 连接。

多次执行本命令，最后一次执行的命令生效。

【举例】

只允许 IPv4 地址为 1.1.1.1 的 SSH 客户端向设备发起 SSH 访问。

```
<Sysname> system-view
[Sysname] acl basic 2001
[Sysname-acl-ipv4-basic-2001] rule permit source 1.1.1.1 0
[Sysname-acl-ipv4-basic-2001] quit
[Sysname] ssh server acl 2001
```

【相关命令】

- **display ssh server**

1.1.8 ssh server acl-deny-log enable

ssh server acl-deny-log enable 命令用来开启匹配 ACL deny 规则后打印日志信息功能。

undo ssh server acl-deny-log enable 命令用来关闭匹配 ACL deny 规则后打印日志信息功能。

【命令】

```
ssh server acl-deny-log enable
undo ssh server acl-deny-log enable
```

【缺省情况】

匹配 ACL deny 规则后打印日志信息功能处于关闭状态。

【视图】

系统视图

【缺省用户角色】

network-admin

【使用指导】

通过配置 **ssh server acl** 和 **ssh server ipv6 acl** 命令，可限制 SSH 客户端对设备的访问。此时，通过配置 **ssh server acl-deny-log enable** 命令，设备可以记录匹配 **deny** 规则的 IP 用户的登录日志，用户可以查看非法登录的地址信息。

执行本配置后，SSH 客户端匹配 ACL deny 规则时，将产生日志信息。生成的日志信息将被发送到设备的信息中心，通过设置信息中心的参数，决定日志信息的输出规则（即是否允许输出以及输出方向）。

【举例】

开启匹配 ACL deny 规则后打印日志信息功能。

```
<Sysname> system-view
[Sysname] ssh server acl-deny-log enable
```

【相关命令】

- **ssh server acl**
- **ssh server ipv6 acl**

1.1.9 ssh server authentication-retries

ssh server authentication-retries 命令用来设置允许 SSH 用户认证尝试的最大次数。

undo ssh server authentication-retries 命令用来恢复缺省情况。

【命令】

```
ssh server authentication-retries retries
undo ssh server authentication-retries
```

【缺省情况】

允许 SSH 用户认证尝试的最大次数为 3 次。

【视图】

系统视图

【缺省用户角色】

network-admin

【参数】

retries: 指定每个 SSH 用户认证尝试的最大次数，取值范围为 1~5。

【使用指导】

通过本命令可以限制用户尝试登录的次数，防止非法用户对用户名和密码进行恶意地猜测和破解。如果用户的认证次数超过了最大认证次数，还未认证成功，则不再允许认证。不同认证方式的认证次数统计方式有所不同，具体统计方式请参考如下：

- 在 any 认证方式下，认证次数是指 SSH 客户端通过 **publickey** 和 **password** 两种方式进行认证尝试的总数
- 对于 **password-publickey** 认证方式，设备首先对 SSH 用户进行 **publickey** 认证，然后进行 **password** 认证，这个过程为一次认证尝试，而不是两次认证尝试。

该配置不会影响已经登录的 SSH 用户，仅对新登录的 SSH 用户生效。

【举例】

```
# 指定允许 SSH 用户认证尝试的最大次数为 4。
<Sysname> system-view
[Sysname] ssh server authentication-retries 4
```

【相关命令】

- **display ssh server**

1.1.10 ssh server authentication-timeout

ssh server authentication-timeout 命令用来在 SSH 服务器端设置 SSH 用户的认证超时时间。

undo ssh server authentication-timeout 命令用来恢复缺省情况。

【命令】

```
ssh server authentication-timeout time-out-value
undo ssh server authentication-timeout
```

【缺省情况】

SSH 用户的认证超时时间为 60 秒。

【视图】

系统视图

【缺省用户角色】

network-admin

【参数】

time-out-value: 认证超时时间，取值范围为 1~120，单位为秒。

【使用指导】

如果 SSH 用户在设置的认证超时时间内没有完成认证，SSH 服务器就拒绝该用户的连接。

为了防止不法用户建立起 TCP 连接后，不进行接下来的认证，而占用系统资源，妨碍其它合法用户的正常登录，可以适当调小 SSH 用户认证超时时间。

【举例】

```
# 设置 SSH 用户认证超时时间为 10 秒。
<Sysname> system-view
[Sysname] ssh server authentication-timeout 10
```

【相关命令】

- **display ssh server**

1.1.11 ssh server compatible-ssh1x enable

ssh server compatible-ssh1x enable 命令用来设置 SSH 服务器兼容 SSH1 版本的客户端。

undo ssh server compatible-ssh1x [enable] 命令用来恢复缺省情况。

【命令】

```
ssh server compatible-ssh1x enable
undo ssh server compatible-ssh1x [ enable ]
```

【缺省情况】

SSH 服务器不兼容 SSH1 版本的客户端。

【视图】

系统视图

【缺省用户角色】

```
network-admin
network-operator
```

【使用指导】

FIPS 模式下，不支持本命令。

该配置不会影响已经登录的 SSH 用户，仅对新登录的 SSH 用户生效。

执行 **undo** 命令时，指定 **enable** 和不指定 **enable** 均表示恢复缺省情况。

【举例】

```
# 配置服务器兼容 SSH1 版本的客户端。
<Sysname> system-view
[Sysname] ssh server compatible-ssh1x enable
```

【相关命令】

- **display ssh server**

1.1.12 ssh server dscp

ssh server dscp 命令用来设置 IPv4 SSH 服务器向 SSH 客户端发送的报文的 DSCP 优先级。

undo ssh server dscp 命令用来恢复缺省情况。

【命令】

```
ssh server dscp dscp-value
undo ssh server dscp
```

【缺省情况】

IPv4 SSH 报文的 DSCP 优先级为 48。

【视图】

系统视图

【缺省用户角色】

```
network-admin
```

【参数】

dscp-value: IPv4 SSH 报文的 DSCP 优先级，取值范围为 0~63。取值越大，优先级越高。

【使用指导】

DSCP 携带在 IP 报文中的 ToS 字段，用来体现报文自身的优先等级，决定报文传输的优先程度。

【举例】

配置 IPv4 SSH 服务器向 SSH 客户端发送的报文的 DSCP 优先级为 30。

```
<Sysname> system-view
[Sysname] ssh server dscp 30
```

1.1.13 ssh server enable

ssh server enable 命令用来开启 Stelnet 服务器功能。

undo ssh server enable 命令用来关闭 Stelnet 服务器功能。

【命令】

```
ssh server enable
undo ssh server enable
```

【缺省情况】

Stelnet 服务器功能处于关闭状态。

【视图】

系统视图

【缺省用户角色】

network-admin

【举例】

开启 Stelnet 服务器功能。

```
<Sysname> system-view
[Sysname] ssh server enable
```

【相关命令】

- **display ssh server**

1.1.14 ssh server ipv6 acl

ssh server ipv6 acl 命令用来设置对 IPv6 SSH 客户端的访问控制。

undo ssh server ipv6 acl 命令用来恢复缺省情况。

【命令】

```
ssh server ipv6 acl { ipv6 { advanced-acl-number | basic-acl-number } | mac
mac-acl-number }
undo ssh server ipv6 acl
```

【缺省情况】

允许所有 IPv6 SSH 客户端向设备发起 SSH 访问。

【视图】

系统视图

【缺省用户角色】

network-admin

【参数】

ipv6: 指定 IPv6 ACL。

advanced-acl-number: 指定 IPv6 高级 ACL，取值范围为 3000～3999。

basic-acl-number: 指定 IPv6 基本 ACL，取值范围为 2000～2999。

mac acl-number: 指定二层 ACL。**acl-number** 是二层 ACL 的编号，取值范围为 4000～4999。

【使用指导】

对 IPv6 SSH 客户端的访问控制通过引用 ACL 来实现，具体情况如下：

- 当引用的 ACL 不存在、或者引用的 ACL 为空时，允许所有 IPv6 SSH 客户端访问设备。
- 当引用的 ACL 非空时，则只有匹配 ACL 中 **permit** 规则的 IPv6 SSH 客户端可以访问设备，其他客户端不可以访问设备。

该配置生效后，只会过滤新建立的 SSH 连接，不会影响已建立的 SSH 连接。

多次执行本命令，最后一次执行的命令生效。

【举例】

只允许 1::1/64 网段内的 SSH 客户端向设备发起 SSH 访问。

```
<Sysname> system-view
[Sysname] acl ipv6 basic 2001
[Sysname-acl-ipv6-basic-2001] rule permit source 1::1 64
[Sysname-acl-ipv6-basic-2001] quit
[Sysname] ssh server ipv6 acl ipv6 2001
```

【相关命令】

- **display ssh server**

1.1.15 ssh server ipv6 dscp

ssh server ipv6 dscp 命令用来设置 IPv6 SSH 服务器向 SSH 客户端发送的报文的 DSCP 优先级。

undo ssh server ipv6 dscp 命令用来恢复缺省情况。

【命令】

```
ssh server ipv6 dscp dscp-value
undo ssh server ipv6 dscp
```

【缺省情况】

IPv6 SSH 报文的 DSCP 优先级为 48。

【视图】

系统视图

【缺省用户角色】

network-admin

【参数】

dscp-value: IPv6 SSH 报文的 DSCP 优先级, 取值范围为 0~63。取值越大, 优先级越高。

【使用指导】

DSCP 携带在 IPv6 报文中的 Traffic class 字段, 用来体现报文自身的优先等级, 决定报文传输的优先程度。

【举例】

配置 IPv6 SSH 服务器向 SSH 客户端发送的报文的 DSCP 优先级为 30。

```
<Sysname> system-view
[Sysname] ssh server ipv6 dscp 30
```

1.1.16 ssh server key-re-exchange enable

ssh server key-re-exchange enable 命令用来开启 SSH 算法重协商和密钥重交换功能。

undo ssh server key-re-exchange enable 命令用来关闭 SSH 算法重协商和密钥重交换功能。

【命令】

```
ssh server key-re-exchange enable [ interval interval ]
undo ssh server key-re-exchange enable
```

【视图】

系统视图

【缺省情况】

SSH 算法重协商和密钥重交换功能处于关闭状态。

【缺省用户角色】

network-admin

【参数】

interval interval: 配置 SSH 算法重协商和密钥重交换间隔时间。*interval* 取值范围为 1~24, 单位为小时, 缺省值为 1。

【使用指导】

FIPS 模式下不支持此功能。

配置该命令后, 服务器将在客户端和服务端第一次算法协商开始后根据用户设置的时间间隔定时向客户端发起算法协商请求, 进行算法协商和密钥交换操作。

本功能的开启和间隔时间变化不影响已存在的 SSH 连接。

【举例】

开启 SSH 算法重协商和密钥重交换功能。

```
<Sysname> sysname
[Sysname] ssh server key-re-exchange enable
```

1.1.17 ssh server pki-domain

ssh server pki-domain 命令用来配置服务器所属的 PKI 域。

undo ssh server pki-domain 命令用来恢复缺省情况。

【命令】

```
ssh server pki-domain domain-name
```

```
undo ssh server pki-domain
```

【缺省情况】

未配置服务器所属的 PKI 域。

【视图】

系统视图

【缺省用户角色】

network-admin

【参数】

domain-name: 验证服务端的 PKI 域名称，为 1~31 个字符的字符串，不区分大小写，不能包括“~”、“*”、“\”、“|”、“:”、“.”、“<”、“>”、“”和“'”。

【举例】

```
# 配置 SSH 服务器所属的 PKI 域为 serverpkidomain。
```

```
<Sysname> system-view
```

```
[Sysname] ssh server pki-domain serverpkidomain
```

1.1.18 ssh server port

ssh server port 命令用来配置 SSH 服务的端口号。

undo ssh server port 命令用来恢复缺省情况。

【命令】

```
ssh server port port-number
```

```
undo ssh server port
```

【缺省情况】

SSH 服务的端口号为 22。

【视图】

系统视图

【缺省用户角色】

network-admin

【参数】

port-number: SSH 服务的端口号，取值范围为 1~65535。

【使用指导】

如果修改端口号前 SSH 服务是开启的，则修改端口号后系统会自动重启 SSH 服务，正在访问的用户将被断开，用户需要重新建立 SSH 连接后才可以继续访问。

如果使用 1~1024 之间的知名端口号，有可能会对其他服务启动失败。

【举例】

配置 SSH 服务的端口号为 1025。

```
<Sysname> system-view
[Sysname] ssh server port 1025
```

1.1.19 ssh server rekey-interval

ssh server rekey-interval 命令用来设置 RSA 服务器密钥对的最小更新间隔时间。

undo ssh server rekey-interval 命令用来恢复缺省情况。

【命令】

```
ssh server rekey-interval interval
undo ssh server rekey-interval
```

【缺省情况】

RSA 服务器密钥对的最小更新间隔时间为 0，表示系统不更新 RSA 服务器密钥对。

【视图】

系统视图

【缺省用户角色】

network-admin

【参数】

interval：服务器密钥对的最小更新间隔时间，取值范围为 1~24，单位为小时。

【使用指导】

FIPS 模式下，不支持本命令。

通过定时更新服务器密钥对，可以防止对密钥对的恶意猜测和破解，从而提高了 SSH 连接的安全性。

配置该命令后，从首个 SSH1 用户登录开始，SSH 服务器需要等待后续有新的 SSH1 用户登录，才会更新当前的 RSA 服务器密钥对，然后使用新的 RSA 服务器密钥对与新登录的这个 SSH1 用户进行密钥对的协商，其中等待的最小时长就为此处配置的最小更新间隔时间。之后，重复此过程，直到下一个新的 SSH1 用户登录才会再次触发 RSA 服务器密钥的更新。

本配置仅对 SSH 客户端版本为 SSH1 的用户有效。

【举例】

设置 RSA 服务器密钥对的最小更新间隔时间为 3 小时。

```
<Sysname> system-view
[Sysname] ssh server rekey-interval 3
```


【相关命令】

- `display ssh server`

1.1.20 ssh user

`ssh user` 命令用来创建 SSH 用户，并指定 SSH 用户的服务类型和认证方式。

`undo ssh user` 命令用来删除 SSH 用户。

【命令】

非 FIPS 模式下：

```
ssh user username service-type { all | netconf | scp | sftp | stelnet }
authentication-type { password | { any | password-publickey | publickey }
[ assign { pki-domain domain-name | publickey keyname&<1-6> } ] }
```

```
undo ssh user username
```

FIPS 模式下：

```
ssh user username service-type { all | netconf | scp | sftp | stelnet }
authentication-type { password | password-publickey [ assign { pki-domain
domain-name | publickey keyname&<1-6> } ] }
```

```
undo ssh user username
```

【缺省情况】

不存在 SSH 用户。

【视图】

系统视图

【缺省用户角色】

network-admin

【参数】

username: SSH 用户名，为 1~80 个字符的字符串，区分大小写。用户名不能包括符号“\”、“|”、“/”、“.”、“*”、“?”、“<”、“>”和“@”，且不能为“a”、“al”、“all”。其中，“@”、“\”和“/”仅用于作为用户名的 ISP 域名分隔符，具体使用形式为：*pureusername@domain*、*pureusername/domain*、*domain\pureusername*。当创建 SCP 服务类型的用户时，用户名中请不要包含短横杠-，否则使用此用户名进行 SCP 登录会失败。

service-type: SSH 用户的服务类型。包括：

- **all:** 包括 **scp**、**sftp**、**stelnet** 和 **netconf** 四种服务类型。
- **scp:** 服务类型为 SCP（Secure Copy 的简称）。
- **sftp:** 服务类型为 SFTP（Secure FTP 的简称）。
- **stelnet:** 服务类型为 Stelnet（Secure Telnet 的简称）。
- **netconf:** 服务类型为 NETCONF。

authentication-type: SSH 用户的认证方式。包括：

- **password:** 强制指定该用户的认证方式为 **password**。该认证方式的加密机制简单，加密速度快，可结合 AAA（Authentication, Authorization, Accounting，认证、授权、计费）实现对用户认证、授权和计费，但容易受到攻击。
- **any:** 不指定用户的认证方式，用户既可以采用 **password** 认证，也可以采用 **publickey** 认证。
- **password-publickey:** 指定客户端版本为 **SSH2** 的用户认证方式为必须同时进行 **password** 和 **publickey** 两种认证，安全性更高；客户端版本为 **SSH1** 的用户认证方式为只要进行其中一种认证即可。
- **publickey:** 强制指定该用户的认证方式为 **publickey**。该认证方式的加密速度相对较慢，但认证强度高，不易受到暴力猜测密码等攻击方式的影响，而且具有较高的易用性。一次配置成功后，后续认证过程自动完成，不需要用户记忆和输入密码。

assign: 指定用于验证客户端的参数。

- **pki-domain domain-name:** 指定验证客户端证书的 **PKI** 域。*domain-name* 表示 **PKI** 域的名称，为 1~31 个字符的字符串，不区分大小写，不能包括“~”、“*”、“\”、“|”、“.”、“.”、“<”、“>”、“”和“'”。服务器端使用保存在该 **PKI** 域中的 **CA** 证书对客户端证书进行合法性检查，无需提前保存客户端的公钥，能够灵活满足大数量客户端的认证需求。
- **publickey keyname<1-6>:** 指定 **SSH** 客户端的公钥，可以指定多个 **SSH** 客户端的公钥。*keyname* 表示已经配置的客户端公钥名称，为 1~64 个字符的字符串，区分大小写。*<1-6>* 表示前面的参数最多可以输入 6 次。服务器端使用提前保存在本地的用户公钥对用户进行合法性检查，如果客户端密钥文件改变，服务器端需要及时更新本地配置。如果指定了多个用户公钥，则在验证 **SSH** 用户身份时，按照配置顺序使用指定的公钥依次对其进行验证，只要用户通过任意一个公钥验证即可。

【使用指导】

SSH 用户的配置与服务器端采用的认证方式有关，具体如下：

- 如果服务器采用了 **publickey** 认证，则必须在设备上创建相应的 **SSH** 用户，以及同名的本地用户（用于下发授权属性：工作目录、用户角色）。
- 如果服务器采用了 **password** 认证，则必须在设备上创建相应的本地用户（适用于本地认证），或在远程服务器（如 **RADIUS** 服务器，适用于远程认证）上创建相应的 **SSH** 用户。这种情况下，并不需要通过本配置创建相应的 **SSH** 用户，如果创建了 **SSH** 用户，则必须保证指定了正确的服务类型以及认证方式。
- 如果服务器采用了 **password-publickey** 或 **any** 认证，则必须在设备上创建相应的 **SSH** 用户，以及在设备上创建同名的本地用户（适用于本地认证）或者在远程认证服务器上创建同名的 **SSH** 用户（如 **RADIUS** 服务器，适用于远程认证）。

SCP 或 **SFTP** 用户登录时使用的工作目录与用户使用的认证方式有关：

- 采用 **publickey** 或 **password-publickey** 认证方式的用户，使用的工作目录为对应的本地用户视图下通过 **authorization-attribute** 命令设置的工作目录。
- 只采用 **password** 认证方式的用户，使用的工作目录为通过 **AAA** 授权的工作目录。

SSH 用户登录时拥有的用户角色与用户使用的认证方式有关：

- 采用 **publickey** 或 **password-publickey** 认证方式的用户，用户角色为对应的本地用户视图下通过 **authorization-attribute** 命令设置的用户角色。
- 采用 **password** 认证方式的用户，用户角色为通过 AAA 授权的用户角色。

使用该命令为用户指定公钥或 PKI 域时，以最后一次指定的公钥或 PKI 域为准。若不指定 **pki-domain** 和 **publickey**，则表示该用户采用证书认证方式登录，服务器使用其所属的 PKI 域来验证客户端的证书。

对 SSH 用户配置的修改，不会影响已经登录的 SSH 用户，仅对新登录的用户生效。

【举例】

创建 SSH 用户 **user1**，配置 **user1** 的服务类型为 **SFTP**，认证方式为 **password-publickey**，并指定客户端公钥为 **key1**。

```
<Sysname> system-view
[Sysname] ssh user user1 service-type sftp authentication-type password-publickey assign
publickey key1
```

创建设备管理类本地用户 **user1**，配置用户密码为明文 **123456TESTplat&!**，服务类型为 **SSH**，授权工作目录为 **flash:**，授权用户角色为 **network-admin**。

```
[Sysname] local-user user1 class manage
[Sysname-luser-manage-user1] password simple 123456TESTplat&!
[Sysname-luser-manage-user1] service-type ssh
[Sysname-luser-manage-user1] authorization-attribute work-directory flash: user-role
network-admin
```

【相关命令】

- **authorization-attribute**（安全命令参考/AAA）
- **display ssh user-information**
- **local-user**（安全命令参考/AAA）
- **pki domain**（安全命令参考/PKI）

1.2 SSH客户端配置命令

1.2.1 bye

bye 命令用来终止与远程 SFTP 服务器的连接，并退回到用户视图。

【命令】

bye

【视图】

SFTP 客户端视图

【缺省用户角色】

network-admin
network-operator

【使用指导】

该命令功能与 **exit**、**quit** 相同。

【举例】

```
# 终止与远程 SFTP 服务器的连接。  
sftp> bye  
<Sysname>
```

1.2.2 cd

cd 命令用来改变远程 SFTP 服务器上的工作路径。

【命令】

```
cd [ remote-path ]
```

【视图】

SFTP 客户端视图

【缺省用户角色】

network-admin

【参数】

remote-path: 目的工作路径的名称。

【使用指导】

命令“**cd ..**”用来返回到上一级目录。

命令“**cd /**”用来返回到系统的根目录。

【举例】

```
# 改变工作路径到 new1。  
sftp> cd new1  
Current Directory is: /new1  
sftp> pwd  
Remote working directory: /new1  
sftp>
```

1.2.3 cdup

cdup 命令用来返回到上一级目录。

【命令】

```
cdup
```

【视图】

SFTP 客户端视图

【缺省用户角色】

network-admin

【举例】

```
# 从当前工作目录/test1 返回到上一级目录。  
sftp> cd test1
```

```
Current Directory is:/test1
sftp> pwd
Remote working directory: /test1
sftp> cdup
Current Directory is:/
sftp> pwd
Remote working directory: /
sftp>
```

1.2.4 delete

delete 命令用来删除 SFTP 服务器上指定的文件。

【命令】

```
delete remote-file
```

【视图】

SFTP 客户端视图

【缺省用户角色】

network-admin

【参数】

remote-file: 要删除的文件的名称。

【使用指导】

该命令和 **remove** 功能相同。

【举例】

删除服务器上的文件 temp.c。

```
sftp> delete temp.c
Removing /temp.c
```

1.2.5 delete ssh client server-public-key

delete ssh client server-public-key 命令用来删除 SSH 客户端公钥文件中的服务器公钥信息。

【命令】

```
delete ssh client server-public-key [ server-ip ip-address ]
```

【视图】

系统视图

【缺省用户角色】

network-admin

【参数】

server-ip *ip-address*: 删除指定 IP 地址的服务器的公钥信息。不指定本参数时，删除公钥文件中所有服务器公钥信息。

【举例】

删除所有 SSH 客户端保存在公钥文件的服务器公钥。

```
<Sysname> system-view
[Sysname] delete ssh client server-public-key
Public keys of all SSH servers will be deleted. Continue? [Y/N]:y
```

删除 SSH 客户端保存的服务器 2.2.2.1 的公钥。

```
<Sysname> system-view
[Sysname] delete ssh client server-public-key server-ip 2.2.2.1
```

1.2.6 dir

dir 命令用来显示指定目录下文件及文件夹的信息。

【命令】

```
dir [ -a | -l ] [ remote-path ]
```

【视图】

SFTP 客户端视图

【缺省用户角色】

network-admin

【参数】

-a: 以列表的形式显示指定目录下文件及文件夹的详细信息，其中包括以“.”开头的文件及文件夹的详细信息。

-l: 以列表的形式显示指定目录下文件及文件夹的详细信息，但不包括以“.”开头的文件及文件夹的详细信息。

remote-path: 查询的目录名。如果没有指定 *remote-path*，则显示当前工作目录下文件及文件夹的信息。

【使用指导】

如果没有指定 **-a** 和 **-l** 参数，则显示指定目录下文件及文件夹的名称。

该命令功能与 **ls** 相同。

【举例】

以列表的形式显示当前工作目录下文件及文件夹的详细信息，其中包括以“.”开头的文件及文件夹的详细信息。

```
sftp> dir -a
drwxrwxrwx    2 1      1          512 Dec 18 14:12 .
drwxrwxrwx    2 1      1          512 Dec 18 14:12 ..
-rwxrwxrwx    1 1      1          301 Dec 18 14:11 010.pub
-rwxrwxrwx    1 1      1          301 Dec 18 14:12 011.pub
-rwxrwxrwx    1 1      1          301 Dec 18 14:12 012.pub
```

以列表的形式显示当前工作目录下文件及文件夹的详细信息，但不包括以“.”开头的文件及文件夹的详细信息。

```
sftp> dir -l
-rwxrwxrwx    1 1      1          301 Dec 18 14:11 010.pub
```

```

-rwxrwxrwx      1 1      1      301 Dec 18 14:12 011.pub
-rwxrwxrwx      1 1      1      301 Dec 18 14:12 012.pub

```

1.2.7 display scp client source

display scp client source 命令用来显示 SCP 客户端的源 IP 地址配置。

【命令】

```
display scp client source
```

【视图】

任意视图

【缺省用户角色】

```

network-admin
network-operator

```

【举例】

显示 SCP 客户端的源 IP 地址配置。

```

<Sysname> display scp client source
The source IP address of the SCP client is 192.168.0.1.
The source IPv6 address of the SCP client is 2:2::2:2.

```

【相关命令】

- **scp client ipv6 source**
- **scp client source**

1.2.8 display sftp client source

display sftp client source 命令用来显示 SFTP 客户端的源 IP 地址配置。

【命令】

```
display sftp client source
```

【视图】

任意视图

【缺省用户角色】

```

network-admin
network-operator

```

【举例】

显示 SFTP 客户端的源 IP 地址配置。

```

<Sysname> display sftp client source
The source IP address of the SFTP client is 192.168.0.1.
The source IPv6 address of the SFTP client is 2:2::2:2.

```

【相关命令】

- **sftp client ipv6 source**

- **sftp client source**

1.2.9 display ssh client server-public-key

display ssh client server-public-key 命令用来显示 SSH 客户端公钥文件中的服务器公钥信息。

【命令】

display ssh client server-public-key [**server-ip** *ip-address*]

【视图】

任意视图

【缺省用户角色】

network-admin
network-operator

【参数】

server-ip *ip-address*: 显示指定 IP 地址的服务器的公钥信息。不指定本参数时，显示公钥文件中所有服务器公钥信息。

【使用指导】

设备作为 SSH 客户端时使用本命令可以显示保存在公钥文件中的服务器公钥。该部分公钥信息在配置文件中不可见，用户登录未认证过的服务器并选择保存公钥时，对应公钥信息被写入公钥文件。

【举例】

显示 SSH 客户端保存在公钥文件中所有服务器公钥。

```
<Sysname> display ssh client server-public-key
Server address: 10.153.124.209
Key type: ecdsa-sha2-nistp256
Key length: 256
Key code:
AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBAOGpJfwJExK
eYb53KKqmrZ0V/XnYZKZEchyN9ax1IBt+toIXHeW5NfBE5ymeklPSNgQNhcndkU/
422fT15UmgM=

Server address: 2.2.2.1
Key type: rsa
Key length: 1024
Key code:
AAAAB3NzaC1yc2EAAAADAQABAAQGDIIUrHbeLx/W7xE1B1Ny3zeA8/uV9K6sjlp
dSlhx5XcOatdNM0D/sioYgSsy9IxKZPqBs+vadx/wCCB5+T2GLLu2qgaT0P9J+v
RR/9Y8fI2b4tS7PoNf/QKDVD7XnoiZ+dqd0tnnRf6GV+74cp8ZEUQdAoTeDzzaAh
7t6FbxrNrQ==
```

显示 SSH 客户端保存在公钥文件中的服务器 2.2.2.1 的公钥。

```
<Sysname> display ssh client server-public-key server-ip 2.2.2.1
Server address: 2.2.2.1
Key type: rsa
```



```

Key length: 1024
Key code:
AAAAB3NzaC1yc2EAAAADAQABAAQgQDIUrHbeLx/W7xE1B1Ny3zeA8/uV9K6sjlp
dSlhx5XcOatdNM0D/sioYgSsy9IxKZPqBs+vadqx/wCCB5+T2GLLu2qgaT0P9J+v
RR/9Y8fI2b4tS7PoNf/QKDVD7XnoiZ+dqd0tnnRf6GV+74cp8ZEUQdAoTeDzzaAh
7t6FbxxrNrQ==

```

表1-4 display ssh client server-public-key 命令显示信息描述表

字段	描述
Server address	服务器IP地址
Key type	公钥类型： <ul style="list-style-type: none"> dsa: 公钥算法为 DSA ecdsa-sha2-nistp256: 名称为 secp256r1 的椭圆曲线生成的 ECDSA 密钥，密钥长度为 256 比特 ecdsa-sha2-nistp384: 名称为 secp384r1 的椭圆曲线生成的 ECDSA 密钥，密钥长度为 384 比特 rsa: 公钥算法为 RSA
Key length	公钥长度，单位为比特
Key code	公钥内容

1.2.10 display ssh client source

display ssh client source 命令用来显示 STelnet 客户端的源 IP 地址配置。

【命令】

```
display ssh client source
```

【视图】

任意视图

【缺省用户角色】

```

network-admin
network-operator

```

【举例】

显示 STelnet 客户端的源 IP 地址配置。

```

<Sysname> display ssh client source
The source IP address of the SSH client is 192.168.0.1.
The source IPv6 address of the SSH client is 2::2:2:2.

```

【相关命令】

- ssh client ipv6 source
- ssh client source

1.2.11 exit

exit 命令用来终止与远程 SFTP 服务器的连接，并退回到用户视图。

【命令】

exit

【视图】

SFTP 客户端视图

【缺省用户角色】

network-admin
network-operator

【使用指导】

该命令功能与 **bye**、**quit** 相同。

【举例】

```
# 终止与远程 SFTP 服务器的连接。  
sftp> exit  
<Sysname>
```

1.2.12 get

get 命令用来从远程 SFTP 服务器上下载文件并存储在本地。

【命令】

get *remote-file* [*local-file*]

【视图】

SFTP 客户端视图

【缺省用户角色】

network-admin

【参数】

remote-file: 远程 SFTP 服务器上的文件名。

local-file: 本地文件名。如果没有指定本地文件名，则认为本地保存文件的文件名与服务器上的文件名相同。

【举例】

下载远程服务器上的 **temp1.c** 文件，并以文件名 **temp.c** 在本地保存。

```
sftp> get temp1.c temp.c  
Fetching /temp1.c to temp.c  
/temp.c                                100% 1424      1.4KB/s    00:00
```

1.2.13 help

help 命令用来显示 SFTP 客户端命令的帮助信息。

【命令】

help

【视图】

SFTP 客户端视图

【缺省用户角色】

network-admin
network-operator

【使用指导】

键入 **?** 和执行 **help** 命令的功能相同。

【举例】

查看帮助信息。

```
sftp> help
Available commands:

bye                               Quit sftp
cd [path]                        Change remote directory to 'path'
cdup                             Change remote directory to the parent directory
delete path                      Delete remote file
dir [-a|-l][path]               Display remote directory listing
    -a                           List all filenames
    -l                           List filename including the specific
                                information of the file

exit                             Quit sftp
get remote-path [local-path]    Download file
help                             Display this help text
ls [-a|-l][path]                Display remote directory
    -a                           List all filenames
    -l                           List filename including the specific
                                information of the file

mkdir path                       Create remote directory
put local-path [remote-path]    Upload file
pwd                              Display remote working directory
quit                             Quit sftp
rename oldpath newpath          Rename remote file
remove path                     Delete remote file
rmdir path                      Delete remote empty directory
?                               Synonym for help
```

1.2.14 ls

ls 命令用来显示指定目录下文件及文件夹的信息。

【命令】

ls [-a | -l] [remote-path]

【视图】

SFTP 客户端视图

【缺省用户角色】

network-admin

【参数】

-a: 以列表的形式显示指定目录下文件及文件夹的详细信息，其中包括以“.”开头的文件及文件夹的详细信息。

-l: 以列表的形式显示指定目录下文件及文件夹的详细信息，但不包括以“.”开头的文件及文件夹的详细信息。

remote-path: 查询的目录名。如果没有指定 **remote-path**，则显示当前工作目录下文件及文件夹的信息。

【使用指导】

如果没有指定 **-a** 和 **-l** 参数，则显示指定目录下文件及文件夹的名称。

该命令功能与 **dir** 相同。

【举例】

以列表的形式显示当前工作目录下文件及文件夹的详细信息，其中包括以“.”开头的文件及文件夹的详细信息。

```
sftp> ls -a
drwxrwxrwx    2 1      1          512 Dec 18 14:12 .
drwxrwxrwx    2 1      1          512 Dec 18 14:12 ..
-rwxrwxrwx    1 1      1          301 Dec 18 14:11 010.pub
-rwxrwxrwx    1 1      1          301 Dec 18 14:12 011.pub
-rwxrwxrwx    1 1      1          301 Dec 18 14:12 012.pub
```

以列表的形式显示当前工作目录下文件及文件夹的详细信息，但不包括以“.”开头的文件及文件夹的详细信息。

```
sftp> ls -l
-rwxrwxrwx    1 1      1          301 Dec 18 14:11 010.pub
-rwxrwxrwx    1 1      1          301 Dec 18 14:12 011.pub
-rwxrwxrwx    1 1      1          301 Dec 18 14:12 012.pub
```

1.2.15 mkdir

mkdir 命令用来在远程 SFTP 服务器上创建新的目录。

【命令】

mkdir remote-path

【视图】

SFTP 客户端视图

【缺省用户角色】

network-admin

【参数】

remote-path: 远程 SFTP 服务器上的目录名。

【举例】

在远程 SFTP 服务器上建立目录 test。

```
sftp> mkdir test
```

1.2.16 put

put 命令用来将本地的文件上传到远程 SFTP 服务器。

【命令】

```
put local-file [ remote-file ]
```

【视图】

SFTP 客户端视图

【缺省用户角色】

network-admin

【参数】

local-file: 本地的文件名。

remote-file: 远程 SFTP 服务器上的文件名。如果没有指定远程服务器上的文件名，则认为服务器上保存文件的文件名与本地的文件名相同。

【举例】

将本地 startup.bak 文件上传到远程 SFTP 服务器，并以 startup01.bak 文件名保存。

```
sftp> put startup.bak startup01.bak
```

```
Uploading startup.bak to /startup01.bak
```

```
startup01.bak                               100% 1424      1.4KB/s   00:00
```

1.2.17 pwd

pwd 命令用来显示远程 SFTP 服务器上的当前工作目录。

【命令】

```
pwd
```

【视图】

SFTP 客户端视图

【缺省用户角色】

network-admin

【举例】

显示远程 SFTP 服务器上的当前工作目录。

```
sftp> pwd
```

```
Remote working directory: /
```

以上显示信息表示当前的工作目录为根目录。

1.2.18 quit

quit 命令用来终止与远程 SFTP 服务器的连接，并退回到用户视图。

【命令】

quit

【视图】

SFTP 客户端视图

【缺省用户角色】

network-admin
network-operator

【使用指导】

该命令功能与 **bye**、**exit** 相同。

【举例】

```
# 终止与远程 SFTP 服务器的连接。  
sftp> quit  
<Sysname>
```

1.2.19 remove

remove 命令用来删除远程 SFTP 服务器上指定的文件。

【命令】

remove *remote-file*

【视图】

SFTP 客户端视图

【缺省用户角色】

network-admin

【参数】

remote-file: 要删除的文件的名称。

【使用指导】

该命令和 **delete** 命令相同。

【举例】

```
# 删除远程 SFTP 服务器上的文件 temp.c。  
sftp> remove temp.c  
Removing /temp.c
```

1.2.20 rename

rename 命令用来改变远程 SFTP 服务器上指定的文件或者文件夹的名字。

【命令】

rename *old-name new-name*

【视图】

SFTP 客户端视图

【缺省用户角色】

network-admin

【参数】

old-name: 原文件名或者文件夹名。

new-name: 新文件名或者文件夹名。

【举例】

将远程 SFTP 服务器上的文件 **temp1.c** 改名为 **temp2.c**。

```
sftp> dir
aa.pub  temp1.c
sftp> rename temp1.c temp2.c
sftp> dir
aa.pub  temp2.c
```

1.2.21 rmdir

rmdir 命令用来删除远程 SFTP 服务器上指定的目录。

【命令】

rmdir *remote-path*

【视图】

SFTP 客户端视图

【缺省用户角色】

network-admin

【参数】

remote-path: 远程 SFTP 服务器上的目录名。

【举例】

删除 SFTP 服务器上当前工作目录下的 **temp1** 目录。

```
sftp> rmdir temp1
```

1.2.22 scp

scp 命令用来与远程的 SCP 服务器建立连接，并进行文件传输。

【命令】

非 FIPS 模式下:

```
scp server [ port-number ] { put | get } source-file-name
[ destination-file-name ] [ identity-key { dsa | ecdsa-sha2-nistp256 |
```

```
ecdsa-sha2-nistp384 | rsa | { x509v3-ecdsa-sha2-nistp256 |
x509v3-ecdsa-sha2-nistp384 } pki-domain domain-name } | prefer-compress
zlib | prefer-ctos-cipher { 3des-cbc | aes128-cbc | aes128-ctr | aes128-gcm |
aes192-ctr | aes256-cbc | aes256-ctr | aes256-gcm | des-cbc } |
prefer-ctos-hmac { md5 | md5-96 | sha1 | sha1-96 | sha2-256 | sha2-512 } |
prefer-kex { dh-group-exchange-sha1 | dh-group1-sha1 | dh-group14-sha1 |
ecdh-sha2-nistp256 | ecdh-sha2-nistp384 } | prefer-stoc-cipher { 3des-cbc |
aes128-cbc | aes128-ctr | aes128-gcm | aes192-ctr | aes256-cbc | aes256-ctr |
aes256-gcm | des-cbc } | prefer-stoc-hmac { md5 | md5-96 | sha1 | sha1-96 |
sha2-256 | sha2-512 } ] * [ { public-key keyname | server-pki-domain
domain-name } | source { interface interface-type interface-number | ip
ip-address } ] * [ user username [ password password ] ]
```

FIPS 模式下:

```
scp server [ port-number ] { put | get } source-file-name
[ destination-file-name ] [ identity-key { ecdsa-sha2-nistp256 |
ecdsa-sha2-nistp384 | rsa | { x509v3-ecdsa-sha2-nistp256 |
x509v3-ecdsa-sha2-nistp384 } pki-domain domain-name } | prefer-compress
zlib | prefer-ctos-cipher { aes128-cbc | aes128-ctr | aes128-gcm | aes192-ctr
| aes256-cbc | aes256-ctr | aes256-gcm } | prefer-ctos-hmac { sha1 | sha1-96 |
sha2-256 | sha2-512 } | prefer-kex { dh-group14-sha1 | ecdh-sha2-nistp256 |
ecdh-sha2-nistp384 } | prefer-stoc-cipher { aes128-cbc | aes128-ctr |
aes128-gcm | aes192-ctr | aes256-cbc | aes256-ctr | aes256-gcm } |
prefer-stoc-hmac { sha1 | sha1-96 | sha2-256 | sha2-512 } ] * [ { public-key
keyname | server-pki-domain domain-name } | source { interface
interface-type interface-number | ip ip-address } ] * [ user username
[ password password ] ]
```

【视图】

用户视图

【缺省用户角色】

network-admin

【参数】

server: 服务器的 IPv4 地址或主机名称，为 1~253 个字符的字符串，不区分大小写。

port-number: 服务器端口号，取值范围为 1~65535，缺省值为 22。

get: 指定下载文件操作。

put: 指定上传文件操作。

source-file-name: 源文件名称，为 1~255 个字符的字符串，区分大小写。

destination-file-name: 目的文件名称，为 1~255 个字符的字符串，区分大小写。若未指定该参数，则表示使用源文件的名称作为目的文件名称。

identity-key: 客户端 **publickey** 认证时采用的公钥算法，非 FIPS 模式下，缺省算法为 **dsa**；FIPS 模式下，缺省算法为 **rsa**。如果服务器采用 **publickey** 认证，必须指定该参数。客户端使用指定算法的本地私钥生成数字签名或证书。

- **dsa:** 公钥算法为 DSA。
- **ecdsa-sha2-nistp256:** 指定公钥长度为 256 的 ECDSA 算法。
- **ecdsa-sha2-nistp384:** 指定公钥长度为 384 的 ECDSA 算法。
- **rsa:** 公钥算法为 RSA。
- **x509v3-ecdsa-sha2-nistp256:** x509v3-ecdsa-sha2-nistp256 公钥算法。
- **x509v3-ecdsa-sha2-nistp384:** x509v3-ecdsa-sha2-nistp384 公钥算法。
- **pki-domain domain-name:** 指定客户端证书的 PKI 域，为 1~31 个字符的字符串，不区分大小写，公钥算法为 x509v3 时，指定客户端证书所在 PKI 域名称，才能得到正确的本地证书。

prefer-compress: 服务器与客户端之间的首选压缩算法，缺省不支持压缩。

zlib: 压缩算法 ZLIB。

prefer-ctos-cipher: 客户端到服务器端的首选加密算法，缺省算法为 **aes128-ctr.des-cbc**、**3des-cbc**、**aes128-cbc**、**aes128-ctr**、**aes128-gcm**、**aes192-ctr**、**aes256-cbc**、**aes256-ctr**、**aes256-gcm** 算法的安全强度和运算花费时间依次递增。

- **3des-cbc:** 3DES-CBC 加密算法。
- **aes128-cbc:** 128 位的 AES-CBC 加密算法。
- **aes128-ctr:** 128 位 AES-CTR 加密算法。
- **aes128-gcm:** 128 位 AES-GCM 加密算法。
- **aes192-ctr:** 192 位 AES-CTR 加密算法。
- **aes256-cbc:** 256 位的 AES-CBC 加密算法。
- **aes256-ctr:** 256 位 AES-CTR 加密算法。
- **aes256-gcm:** 256 位 AES-GCM 加密算法。
- **des-cbc:** DES-CBC 加密算法。

prefer-ctos-hmac: 客户端到服务器端的首选 HMAC 算法，缺省算法为 **sha2-256**。**md5**、**md5-96**、**sha1**、**sha1-96**、**sha2-256**、**sha2-512** 算法的安全强度和运算花费时间依次递增。

- **md5:** HMAC 算法 HMAC-MD5。
- **md5-96:** HMAC 算法 HMAC-MD5-96。
- **sha1:** HMAC 算法 HMAC-SHA1。
- **sha1-96:** HMAC 算法 HMAC-SHA1-96。
- **sha2-256:** HMAC 算法 HMAC-SHA2-256。
- **sha2-512:** HMAC 算法 HMAC-SHA2-512。

prefer-kex: 密钥交换首选算法，缺省算法为 **ecdh-sha2-nistp256**。**dh-group-exchange-sha1**、**dh-group1-sha1**、**dh-group14-sha1**、**ecdh-sha2-nistp256**、**ecdh-sha2-nistp384** 算法的安全强度和运算花费时间依次递增。

- **dh-group-exchange-sha1:** 密钥交换算法 diffie-hellman-group-exchange-sha1。
- **dh-group1-sha1:** 密钥交换算法 diffie-hellman-group1-sha1。

- **dh-group14-sha1**: 密钥交换算法 diffie-hellman-group14-sha1。
- **ecdh-sha2-nistp256**: 密钥交换算法 ecdh-sha2-nistp256。
- **ecdh-sha2-nistp384**: 密钥交换算法 ecdh-sha2-nistp384。

prefer-stoc-cipher: 服务器端到客户端的首选加密算法, 缺省算法为 **aes128-ctr**。支持的加密算法与客户端到服务器端的加密算法相同。

prefer-stoc-hmac: 服务器端到客户端的首选 HMAC 算法, 缺省算法为 **sha2-256**。支持的加密算法与客户端到服务器端的 HMAC 算法相同。

public-key keyname: 指定服务器端的主机公钥, 用于验证服务器端的身份。其中, *keyname* 表示已经配置的主机公钥名称, 为 1~64 个字符的字符串, 不区分大小写。

server-pki-domain domain-name: 指定验证服务端证书的 PKI 域。其中, *domain-name* 表示验证服务端证书的 PKI 域名称, 为 1~31 个字符的字符串, 不区分大小写, 不能包括 “~”、“*”、“\”、“|”、“:”、“.”、“<”、“>”、“” 和 “'”。

source: 指定与服务器通信的源 IPv4 地址或者源接口。缺省情况下, 报文源 IPv4 地址为根据路由表项查找的发送此报文的出接口的主 IPv4 地址。为保证客户端与服务器之间的通信不会因为所指定的接口发生故障而中断, 通常建议指定 Loopback 接口作为源接口, 或者接口的 IPv4 地址作为源 IPv4 地址。

interface interface-type interface-number: 指定源接口。 *interface-type* *interface-number* 为接口类型和接口编号。系统将使用该接口的 IPv4 地址作为发送报文的源 IP 地址。

ip ip-address: 指定源 IPv4 地址。

user username: 指定 SCP 用户名, 为 1~80 个字符的字符串, 区分大小写。若用户登录时用户名中携带 ISP 域名, 则其形式为 *pureusername@domain*、*pureusername/domain*、*domain\pureusername*。

password password: 指定明文密码, 为 1~63 个字符的字符串, 区分大小写。

【使用指导】

当客户端主机公钥算法协商成功为证书时, 需要校验服务端证书是否正确, 这样需要通过 **server-pki-domain** 指定服务端证书所在的 PKI 域名称, 这样才能获取正确验证服务器证书。客户端使用保存在该 PKI 域中的 CA 证书对服务器证书进行合法性检查, 无需提前保存服务器的公钥。如果客户端没有指定验证服务端证书所在的 PKI 域, 则缺省使用客户端证书所在的 PKI 域进行验证。

如果不指定用户名和密码, 则表示以交互方式输入用户名和密码。

如果 SCP 服务器对客户端的认证方式为 **publickey** 认证, 则本命令指定的密码将被忽略。

【举例】

SCP 客户端采用 **publickey** 认证方式, 登录地址为 200.1.1.1 的远程 SCP 服务器, 下载名为 **abc.txt** 的文件, 采用如下连接策略, 并指定服务器端的公钥名称为 **svkey**:

- 首选密钥交换算法为 **dh-group14-sha1**;
- 服务器到客户端的首选加密算法为 **aes128-cbc**;
- 客户端到服务器的首选 HMAC 算法为 **sha1**;
- 服务器到客户端的 HMAC 算法为 **sha1-96**;

- 服务器与客户端之间的首选压缩算法为 **zlib**。

```
<Sysname> scp 200.1.1.1 get abc.txt prefer-kex dh-group14-sha1 prefer-stoc-cipher aes128-cbc  
prefer-ctos-hmac sha1 prefer-stoc-hmac sha1-96 prefer-compress zlib public-key svkey
```

1.2.23 scp client ipv6 source

scp client ipv6 source 命令用来配置 SCP 客户端发送 SCP 报文使用的源 IPv6 地址。

undo scp client ipv6 source 命令用来恢复缺省情况。

【命令】

```
scp client ipv6 source { interface interface-type interface-number | ipv6  
ipv6-address }  
undo scp client ipv6 source
```

【缺省情况】

未配置 SCP 客户端使用的源 IPv6 地址，设备自动选择 IPv6 SCP 报文的源 IPv6 地址，具体选择原则请参见 RFC 3484。

【视图】

系统视图

【缺省用户角色】

network-admin

【参数】

interface interface-type interface-number: 指定接口下与报文目的地址最匹配的 IPv6 地址作为源地址。*interface-type interface-number* 表示源接口类型与源接口编号。

ipv6 ipv6-address: 指定源 IPv6 地址。

【使用指导】

scp client ipv6 source 命令指定的源地址对所有的 IPv6 SCP 连接有效，**scp ipv6** 命令指定的源地址只对当前的 SCP 连接有效，后者优先级高。

多次执行本命令，最后一次执行的命令生效。

【举例】

指定 SCP 客户端发送 SCP 报文使用的源 IPv6 地址为 2:2::2:2。

```
<Sysname> system-view  
[Sysname] scp client ipv6 source ipv6 2:2::2:2
```

【相关命令】

- **display scp client source**

1.2.24 scp client source

scp client source 命令用来配置 SCP 客户端发送 SCP 报文使用的源 IPv4 地址。

undo scp client source 命令用来恢复缺省情况。

【命令】

```
scp client source { interface interface-type interface-number | ip
ip-address }
undo scp client source
```

【缺省情况】

未配置 SCP 客户端使用的源 IPv4 地址, SCP 客户端发送 SCP 报文使用的源 IPv4 地址为设备路由指定的 SCP 报文出接口的主 IP 地址。

【视图】

系统视图

【缺省用户角色】

network-admin

【参数】

interface interface-type interface-number: 指定接口的主 IP 地址作为源地址。
interface-type interface-number 表示源接口类型与源接口编号。
ip ip-address: 指定源 IP 地址。

【使用指导】

scp client source 命令指定的源地址对所有的 SCP 连接有效, **scp** 命令指定的源地址只对当前的 SCP 连接有效, 后者优先级高。

多次执行本命令, 最后一次执行的命令生效。

【举例】

指定 SCP 客户端发送 SCP 报文使用的源 IP 地址为 192.168.0.1。

```
<Sysname> system-view
[Sysname] scp client source ip 192.168.0.1
```

【相关命令】

- **display scp client source**

1.2.25 scp ipv6

scp ipv6 命令用来与远程的 IPv6 SCP 服务器建立连接, 并进行文件传输。

【命令】

非 FIPS 模式下:

```
scp ipv6 server [ port-number ] [ -i interface-type interface-number ] { put |
get } source-file-name [ destination-file-name ] [ identity-key { dsa |
ecdsa-sha2-nistp256 | ecdsa-sha2-nistp384 | rsa |
{ x509v3-ecdsa-sha2-nistp256 | x509v3-ecdsa-sha2-nistp384 } pki-domain
domain-name } | prefer-compress zlib | prefer-ctos-cipher { 3des-cbc |
aes128-cbc | aes128-ctr | aes128-gcm | aes192-ctr | aes256-cbc | aes256-ctr
| aes256-gcm | des-cbc } | prefer-ctos-hmac { md5 | md5-96 | sha1 | sha1-96 |
sha2-256 | sha2-512 } | prefer-kex { dh-group-exchange-sha1 | dh-group1-sha1
```

```
| dh-group14-sha1 | ecdh-sha2-nistp256 | ecdh-sha2-nistp384 } |
prefer-stoc-cipher { 3des-cbc | aes128-cbc | aes128-ctr | aes128-gcm |
aes192-ctr | aes256-cbc | aes256-ctr | aes256-gcm | des-cbc } |
prefer-stoc-hmac { md5 | md5-96 | sha1 | sha1-96 | sha2-256 | sha2-512 } ] *
[ { public-key keyname | server-pki-domain domain-name } | source { interface
interface-type interface-number | ipv6 ipv6-address } ] * [ user username
[ password password ] ]
```

FIPS 模式下：

```
scp ipv6 server [ port-number ] [ -i interface-type interface-number ] { put
| get } source-file-name [ destination-file-name ] [ identity-key
{ ecdsa-sha2-nistp256 | ecdsa-sha2-nistp384 | rsa |
{ x509v3-ecdsa-sha2-nistp256 | x509v3-ecdsa-sha2-nistp384 } pki-domain
domain-name } | prefer-compress zlib | prefer-ctos-cipher { aes128-cbc |
aes128-ctr | aes128-gcm | aes192-ctr | aes256-cbc | aes256-ctr | aes256-gcm }
| prefer-ctos-hmac { sha1 | sha1-96 | sha2-256 | sha2-512 } | prefer-kex
{ dh-group14-sha1 | ecdh-sha2-nistp256 | ecdh-sha2-nistp384 } |
prefer-stoc-cipher { aes128-cbc | aes128-ctr | aes128-gcm | aes192-ctr |
aes256-cbc | aes256-ctr | aes256-gcm } | prefer-stoc-hmac { sha1 | sha1-96 |
sha2-256 | sha2-512 } ] * [ { public-key keyname | server-pki-domain
domain-name } | source { interface interface-type interface-number | ipv6
ipv6-address } ] * [ user username [ password password ] ]
```

【视图】

用户视图

【缺省用户角色】

network-admin

【参数】

server：服务器的 IPv6 地址或主机名称，为 1~253 个字符的字符串，不区分大小写。

port-number：服务器端口号，取值范围为 1~65535，缺省值为 22。

-i interface-type interface-number：当前 SCP 客户端连接所使用的出接口的接口类型和接口编号。此参数用于 SCP 服务器的地址是链路本地地址的情况，而且指定的出接口必需具有链路本地地址。

get：指定下载文件操作。

put：指定上传文件操作。

source-file-name：源文件名称，为 1~255 个字符的字符串，区分大小写。

destination-file-name：目的文件名称，为 1~255 个字符的字符串，区分大小写。不指定该参数时，表示使用源文件的名称作为目的文件名称。

identity-key：客户端 publickey 认证时采用的公钥算法，非 FIPS 模式下，缺省算法为 **dsa**；FIPS 模式下，缺省算法为 **rsa**。如果服务器采用 publickey 认证，必须指定该参数。客户端使用指定算法的本地私钥生成数字签名或证书。

- **dsa**：公钥算法为 DSA。

- **ecdsa-sha2-nistp256**: 指定公钥长度为 256 的 ECDSA 算法。
- **ecdsa-sha2-nistp384**: 指定公钥长度为 384 的 ECDSA 算法。
- **rsa**: 公钥算法为 RSA。
- **x509v3-ecdsa-sha2-nistp256**: x509v3-ecdsa-sha2-nistp256 公钥算法。
- **x509v3-ecdsa-sha2-nistp384**: x509v3-ecdsa-sha2-nistp384 公钥算法。
- **pki-domain domain-name**: 指定客户端证书的 PKI 域, 为 1~31 个字符的字符串, 不区分大小写, 公钥算法为 x509v3 时, 指定客户端证书所在 PKI 域名称, 才能得到正确的本地证书。

prefer-compress: 服务器与客户端之间的首选压缩算法, 缺省不支持压缩。

zlib: 压缩算法 ZLIB。

prefer-ctos-cipher: 客户端到服务器端的首选加密算法, 缺省算法为 **aes128-ctr**、**des-cbc**、**3des-cbc**、**aes128-cbc**、**aes128-ctr**、**aes128-gcm**、**aes192-ctr**、**aes256-cbc**、**aes256-ctr**、**aes256-gcm** 算法的安全强度和运算花费时间依次递增。

- **3des-cbc**: 3DES-CBC 加密算法。
- **aes128-cbc**: 128 位的 AES-CBC 加密算法。
- **aes128-ctr**: 128 位 AES-CTR 加密算法。
- **aes128-gcm**: 128 位 AES-GCM 加密算法。
- **aes192-ctr**: 192 位 AES-CTR 加密算法。
- **aes256-cbc**: 256 位的 AES-CBC 加密算法。
- **aes256-ctr**: 256 位 AES-CTR 加密算法。
- **aes256-gcm**: 256 位 AES-GCM 加密算法。
- **des-cbc**: DES-CBC 加密算法。

prefer-ctos-hmac: 客户端到服务器端的首选 HMAC 算法, 缺省算法为 **sha2-256**、**md5**、**md5-96**、**sha1**、**sha1-96**、**sha2-256**、**sha2-512** 算法的安全强度和运算花费时间依次递增。

- **md5**: HMAC 算法 HMAC-MD5。
- **md5-96**: HMAC 算法 HMAC-MD5-96。
- **sha1**: HMAC 算法 HMAC-SHA1。
- **sha1-96**: HMAC 算法 HMAC-SHA1-96。
- **sha2-256**: HMAC 算法 HMAC-SHA2-256。
- **sha2-512**: HMAC 算法 HMAC-SHA2-512。

prefer-kex: 密钥交换首选算法, 缺省算法为 **ecdh-sha2-nistp256**。

dh-group-exchange-sha1、**dh-group1-sha1**、**dh-group14-sha1**、**ecdh-sha2-nistp256**、**ecdh-sha2-nistp384** 算法的安全强度和运算花费时间依次递增。

- **dh-group-exchange-sha1**: 密钥交换算法 diffie-hellman-group-exchange-sha1。
- **dh-group1-sha1**: 密钥交换算法 diffie-hellman-group1-sha1。
- **dh-group14-sha1**: 密钥交换算法 diffie-hellman-group14-sha1。
- **ecdh-sha2-nistp256**: 密钥交换算法 ecdh-sha2-nistp256。
- **ecdh-sha2-nistp384**: 密钥交换算法 ecdh-sha2-nistp384。

prefer-stoc-cipher: 服务器端到客户端的首选加密算法，缺省算法为 **aes128-ctr**。支持的加密算法与客户端到服务器端的加密算法相同。

prefer-stoc-hmac: 服务器端到客户端的首选 HMAC 算法，缺省算法为 **sha2-256**。支持的加密算法与客户端到服务器端的 HMAC 算法相同。

public-key keyname: 指定服务器端的主机公钥，用于验证服务器端的身份。其中，*keyname* 表示已经配置的主机公钥名称，为 1~64 个字符的字符串，不区分大小写。

server-pki-domain domain-name: 指定验证服务端证书的 PKI 域。其中，*domain-name* 表示验证服务端证书的 PKI 域名称，为 1~31 个字符的字符串，不区分大小写，不能包括 “~”、“*”、“\”、“|”、“:”、“.”、“<”、“>”、“” 和 “'”。

source: 指定与服务器通信的源 IPv6 地址或者源接口。缺省情况下，设备根据 RFC 3484 的规则自动选择一个源 IPv6 地址。为保证客户端与服务器之间的通信不会因为所指定的接口发生故障而中断，通常建议指定 Loopback 接口作为源接口，或者接口的 IPv6 地址作为源地址。

interface interface-type interface-number: 指定源接口。*interface-type interface-number* 为接口类型和接口编号。系统将使用该接口的 IPv6 地址作为发送报文的源 IP 地址。

ipv6 ipv6-address: 指定源 IPv6 地址。

user username: 指定 SCP 用户名，为 1~80 个字符的字符串，区分大小写。若用户登录时用户名中携带 ISP 域名，则其形式为 *pureusername@domain*、*pureusername/domain*、*domain\pureusername*。

password password: 指定明文密码，为 1~63 个字符的字符串，区分大小写。

【使用指导】

当客户端主机公钥算法协商成功为证书时，需要校验服务端证书是否正确，这样需要通过 **server-pki-domain** 指定服务端证书所在的 PKI 域名称，这样才能获取正确验证服务器证书。客户端使用保存在该 PKI 域中的 CA 证书对服务器证书进行合法性检查，无需提前保存服务器的公钥。如果客户端没有指定验证服务端证书所在的 PKI 域，则缺省使用客户端证书所在的 PKI 域进行验证。

如果不指定用户名和密码，则表示以交互方式输入用户名和密码。

如果 SCP 服务器对客户端的认证方式为 **publickey** 认证，则本命令指定的密码将被忽略。

【举例】

SCP 客户端采用 **publickey** 认证方式，登录地址为 2000::1 的远程 SCP 服务器，下载名为 abc.txt 的文件，采用如下连接策略，并指定服务器端的公钥名称为 **svkey**：

- 首选密钥交换算法为 **dh-group14-sha1**；
- 服务器到客户端的首选加密算法为 **aes128-cbc**；
- 客户端到服务器的首选 HMAC 算法为 **sha1**；
- 服务器到客户端的 HMAC 算法为 **sha1-96**；
- 服务器与客户端之间的首选压缩算法为 **zlib**。

```
<Sysname> scp ipv6 2000::1 get abc.txt prefer-kex dh-group14-sha1 prefer-stoc-cipher  
aes128-cbc prefer-ctos-hmac sha1 prefer-stoc-hmac sha1-96 prefer-compress zlib public-key  
svkey
```


1.2.26 scp ipv6 suite-b

scp ipv6 suite-b 命令用来与远程的 ipv6 SCP 服务器建立基于 Suite B 算法集的连接，并进行文件传输。

【命令】

```
scp ipv6 server [ port-number ] [ -i interface-type interface-number ] { put | get } source-file-name [ destination-file-name ] suite-b [ 128-bit | 192-bit ] pki-domain domain-name [ server-pki-domain domain-name ] [ prefer-compress zlib ] [ source { interface interface-type interface-number | ipv6 ipv6-address } ] * [ user username [ password password ] ]
```

【视图】

用户视图

【缺省用户角色】

network-admin

【参数】

server: 服务器的 IPv6 地址或主机名称，为 1~253 个字符的字符串，不区分大小写。

port-number: 服务器端口号，取值范围为 1~65535，缺省值为 22。

-i interface-type interface-number: 当前 SCP 客户端连接所使用的出接口的接口类型和接口编号。本参数用于 SCP 服务器的地址是链路本地地址的情况，而且指定的出接口必须具有链路本地地址。

get: 指定下载文件操作。

put: 指定上传文件操作。

source-file-name: 源文件名称，为 1~255 个字符的字符串，区分大小写。

destination-file-name: 目的文件名称，为 1~255 个字符的字符串，区分大小写。若未指定本参数，则表示使用源文件名称作为目的文件名称。

suite-b: 指定采用 Suite B 算法集。若未指定 128-bit 和 192-bit 参数，则表示同时采用 128-bit 和 192-bit 的算法集。

128-bit: 指定客户端采用安全级别为 128-bit 的 Suite B 算法集。

192-bit: 指定客户端采用安全级别为 192-bit 的 Suite B 算法集。

pki-domain domain-name: 配置客户端证书的 PKI 域。*domain-name* 为客户端证书的 PKI 域名称，为 1~31 个字符的字符串，不区分大小写，不能包括“~”、“*”、“\”、“|”、“:”、“.”、“<”、“>”、“”和“'”。

server-pki-domain domain-name: 配置验证服务端证书的 PKI 域。*domain-name* 为验证服务端证书的 PKI 域名称，为 1~31 个字符的字符串，不区分大小写，不能包括“~”、“*”、“\”、“|”、“:”、“.”、“<”、“>”、“”和“'”。如果客户端没有指定验证服务端证书所在的 PKI 域，则缺省使用客户端证书所在的 PKI 域进行验证。

prefer-compress: 服务器与客户端之间的首选压缩算法，缺省情况下，不支持压缩。

zlib: 压缩算法 ZLIB。

source: 指定与服务器通信的源 IPv6 地址或者源接口。缺省情况下，设备根据 RFC 3484 的规则自动选择一个源 IPv6 地址。为保证客户端与服务器之间的通信不会因为所指定的接口发生故障而中断，通常建议指定 Loopback 接口作为源接口，或者接口的 IPv6 地址作为源地址。

interface interface-type interface-number: 指定源接口。*interface-type interface-number* 为接口类型和接口编号。系统将使用该接口的 IPv6 地址作为发送报文的源 IPv6 地址。

ipv6 ipv6-address: 指定源 IPv6 地址。

user username: 指定 SCP 用户名，为 1~80 个字符的字符串，区分大小写。若用户登录时用户名中携带 ISP 域名，则其形式为 *pureusername@domain*、*pureusername/domain*、*domain\pureusername*。

password password: 指定明文密码，为 1~63 个字符的字符串，区分大小写。

【使用指导】

当客户端采用安全级别为 128-bit 的 Suite B 算法集与远程的 SCP 服务器建立连接时，客户端算法要求：

- 密钥交换算法为 **ecdh-sha2-nistp256**;
- 服务器到客户端的加密算法为 **aes128-gcm**;
- 客户端到服务器的加密算法为 **aes128-gcm**;
- 服务器到客户端的 HMAC 算法为 **aes128-gcm**;
- 客户端到服务器的 HMAC 算法为 **aes128-gcm**;
- 主机公钥算法为 **x509v3-ecdsa-sha2-nistp256**、**x509v3-ecdsa-sha2-nistp384**。

当客户端采用安全级别为 192-bit 的 Suite B 算法集与远程的 SCP 服务器建立连接时，客户端算法要求：

- 密钥交换算法为 **ecdh-sha2-nistp384**;
- 服务器到客户端的加密算法为 **aes256-gcm**;
- 客户端到服务器的加密算法为 **aes256-gcm**;
- 服务器到客户端的 HMAC 算法为 **aes256-gcm**;
- 客户端到服务器的 HMAC 算法为 **aes256-gcm**;
- 主机公钥算法为 **x509v3-ecdsa-sha2-nistp384**。

当客户端未采用安全级别为 128-bit 和 192-bit 的 Suite B 算法集与远程的 SCP 服务器建立连接时，客户端算法要求：

- 密钥交换算法为 **ecdh-sha2-nistp256**、**ecdh-sha2-nistp384**;
- 服务器到客户端的加密算法为 **aes128-gcm**、**aes256-gcm**;
- 客户端到服务器的加密算法为 **aes128-gcm**、**aes256-gcm**;
- 服务器到客户端的 HMAC 算法为 **aes128-gcm**、**aes256-gcm**;
- 客户端到服务器的 HMAC 算法为 **aes128-gcm**、**aes256-gcm**;
- 主机公钥算法为 **x509v3-ecdsa-sha2-nistp256**、**x509v3-ecdsa-sha2-nistp384**。

如果不指定用户名和密码，则表示以交互方式输入用户名和密码。

如果 SCP 服务器对客户端的认证方式为 **publickey** 认证，则本命令指定的密码将被忽略。

【举例】

SCP 客户端采用安全级别为 192-bit 的 Suite B 算法集，与登录地址为 2000::1 的远程 SCP 服务器建立连接，下载名为 abc.txt 的文件，采用如下连接策略：指定客户端证书的 PKI 域名称为 clientpkidomain，指定验证服务端证书的 PKI 域名称为 serverpkidomain。

```
<Sysname> scp ipv6 2000::1 get abc.txt suite-b 192-bit pki-domain clientpkidomain  
server-pki-domain serverpkidomain  
Username:
```

1.2.27 scp suite-b

scp suite-b 命令用来与远程的 SCP 服务器建立基于 Suite B 算法集的连接，并进行文件传输。

【命令】

```
scp server [ port-number ] { put | get } source-file-name  
[ destination-file-name ] suite-b [ 128-bit | 192-bit ] pki-domain  
domain-name [ server-pki-domain domain-name ] [ prefer-compress zlib ]  
[ source { interface interface-type interface-number | ip ip-address } ] *  
[ user username [ password password ] ]
```

【视图】

用户视图

【缺省用户角色】

network-admin

【参数】

server：服务器的 IPv4 地址或主机名称，为 1~253 个字符的字符串，不区分大小写。

port-number：服务器端口号，取值范围为 1~65535，缺省值为 22。

get：指定下载文件操作。

put：指定上传文件操作。

source-file-name：源文件名称，为 1~255 个字符的字符串，区分大小写。

destination-file-name：目的文件名称，为 1~255 个字符的字符串，区分大小写。若未指定本参数，则表示使用源文件名称作为目的文件名称。

suite-b：指定采用 Suite B 算法集。若未指定 128-bit 和 192-bit 参数，则表示同时采用 128-bit 和 192-bit 的算法集。

128-bit：指定客户端采用安全级别为 128-bit 的 Suite B 算法集。

192-bit：指定客户端采用安全级别为 192-bit 的 Suite B 算法集。

pki-domain domain-name：配置客户端证书的 PKI 域。**domain-name** 为客户端证书的 PKI 域名称，为 1~31 个字符的字符串，不区分大小写，不能包括“~”、“*”、“\”、“|”、“:”、“.”、“<”、“>”、“”和“'”。

server-pki-domain domain-name：配置验证服务端证书的 PKI 域。**domain-name** 为验证服务端证书的 PKI 域名称，为 1~31 个字符的字符串，不区分大小写，不能包括“~”、“*”、“\”、“|”、“:”、“.”、“<”、“>”、“”和“'”。如果客户端没有指定验证服务端证书所在的 PKI 域，则缺省使用客户端证书所在的 PKI 域进行验证。

prefer-compress: 服务器与客户端之间的首选压缩算法，缺省情况下，不支持压缩。

zlib: 压缩算法 ZLIB。

source: 指定与服务器通信的源 IP 地址或者源接口。缺省情况下，设备根据路由表项自动选择一个源 IPv4 地址。为保证客户端与服务器之间的通信不会因为所指定的接口发生故障而中断，通常建议指定 Loopback 接口作为源接口，或者接口的 IP 地址作为源地址。

interface interface-type interface-number: 指定源接口。*interface-type* *interface-number* 为接口类型和接口编号。系统将使用该接口的 IPv4 地址作为发送报文的源 IP 地址。

ip ip-address: 指定源 IPv4 地址。

user username: 指定 SCP 用户名，为 1~80 个字符的字符串，区分大小写。若用户登录时用户名中携带 ISP 域名，则其形式为 *pureusername@domain*、*pureusername/domain*、*domain\pureusername*。

password password: 指定明文密码，为 1~63 个字符的字符串，区分大小写。

【使用指导】

当客户端采用安全级别为 128-bit 的 Suite B 算法集与远程的 SCP 服务器建立连接时，客户端算法要求：

- 密钥交换算法为 **ecdh-sha2-nistp256**;
- 服务器到客户端的加密算法为 **aes128-gcm**;
- 客户端到服务器的加密算法为 **aes128-gcm**;
- 服务器到客户端的 HMAC 算法为 **aes128-gcm**;
- 客户端到服务器的 HMAC 算法为 **aes128-gcm**;
- 主机公钥算法为 **x509v3-ecdsa-sha2-nistp256**、**x509v3-ecdsa-sha2-nistp384**。

当客户端采用安全级别为 192-bit 的 Suite B 算法集与远程的 SCP 服务器建立连接时，客户端算法要求：

- 密钥交换算法为 **ecdh-sha2-nistp384**;
- 服务器到客户端的加密算法为 **aes256-gcm**;
- 客户端到服务器的加密算法为 **aes256-gcm**;
- 服务器到客户端的 HMAC 算法为 **aes256-gcm**;
- 客户端到服务器的 HMAC 算法为 **aes256-gcm**;
- 主机公钥算法为 **x509v3-ecdsa-sha2-nistp384**。

当客户端未采用安全级别为 128-bit 和 192-bit 的 Suite B 算法集与远程的 SCP 服务器建立连接时，客户端算法要求：

- 密钥交换算法为 **ecdh-sha2-nistp256**、**ecdh-sha2-nistp384**;
- 服务器到客户端的加密算法为 **aes128-gcm**、**aes256-gcm**;
- 客户端到服务器的加密算法为 **aes128-gcm**、**aes256-gcm**;
- 服务器到客户端的 HMAC 算法为 **aes128-gcm**、**aes256-gcm**;
- 客户端到服务器的 HMAC 算法为 **aes128-gcm**、**aes256-gcm**;
- 主机公钥算法为 **x509v3-ecdsa-sha2-nistp256**、**x509v3-ecdsa-sha2-nistp384**。

如果不指定用户名和密码，则表示以交互方式输入用户名和密码。

如果 SCP 服务器对客户端的认证方式为 publickey 认证，则本命令指定的密码将被忽略。

【举例】

SCP 客户端采用安全级别为 128-bit 的 Suite B 算法集，与登录地址为 200.1.1.1 的远程 SCP 服务器建立连接，下载名为 abc.txt 的文件，采用如下连接策略：指定客户端证书的 PKI 域名称为 clientpkidomain，指定验证服务端证书的 PKI 域名称为 serverpkidomain。

```
<Sysname> scp 200.1.1.1 get abc.txt suite-b 128-bit pki-domain clientpkidomain
server-pki-domain serverpkidomain
Username:
```

1.2.28 sftp

sftp 命令用来与远程 IPv4 SFTP 服务器建立连接，并进入 SFTP 客户端视图。

【命令】

非 FIPS 模式下：

```
sftp server [ port-number ] [ identity-key { dsa | ecdsa-sha2-nistp256 |
ecdsa-sha2-nistp384 | rsa | { x509v3-ecdsa-sha2-nistp256 |
x509v3-ecdsa-sha2-nistp384 } pki-domain domain-name } | prefer-compress
zlib | prefer-ctos-cipher { 3des-cbc | aes128-cbc | aes128-ctr | aes128-gcm |
aes192-ctr | aes256-cbc | aes256-ctr | aes256-gcm | des-cbc } |
prefer-ctos-hmac { md5 | md5-96 | sha1 | sha1-96 | sha2-256 | sha2-512 } |
prefer-kex { dh-group-exchange-sha1 | dh-group1-sha1 | dh-group14-sha1 |
ecdh-sha2-nistp256 | ecdh-sha2-nistp384 } | prefer-stoc-cipher { 3des-cbc |
aes128-cbc | aes128-ctr | aes128-gcm | aes192-ctr | aes256-cbc | aes256-ctr |
aes256-gcm | des-cbc } | prefer-stoc-hmac { md5 | md5-96 | sha1 | sha1-96 |
sha2-256 | sha2-512 } ] * [ dscp dscp-value | { public-key keyname |
server-pki-domain domain-name } | source { interface interface-type
interface-number | ip ip-address } ] *
```

FIPS 模式下：

```
sftp server [ port-number ] [ identity-key { ecdsa-sha2-nistp256 |
ecdsa-sha2-nistp384 | rsa | { x509v3-ecdsa-sha2-nistp256 |
x509v3-ecdsa-sha2-nistp384 } pki-domain domain-name } | prefer-compress
zlib | prefer-ctos-cipher { aes128-cbc | aes128-ctr | aes128-gcm | aes192-ctr
| aes256-cbc | aes256-ctr | aes256-gcm } | prefer-ctos-hmac { sha1 | sha1-96 |
sha2-256 | sha2-512 } | prefer-kex { dh-group14-sha1 | ecdh-sha2-nistp256 |
ecdh-sha2-nistp384 } | prefer-stoc-cipher { aes128-cbc | aes128-ctr |
aes128-gcm | aes192-ctr | aes256-cbc | aes256-ctr | aes256-gcm } |
prefer-stoc-hmac { sha1 | sha1-96 | sha2-256 | sha2-512 } ] * [ { public-key
keyname | server-pki-domain domain-name } | source { interface
interface-type interface-number | ip ip-address } ] *
```

【视图】

用户视图

【缺省用户角色】

network-admin

【参数】

server: 服务器 IPv4 地址或主机名称，为 1~253 个字符的字符串，不区分大小写。

port-number: 服务器端口号，取值范围为 1~65535，缺省值为 22。

identity-key: 客户端 **publickey** 认证时采用的公钥算法，非 FIPS 模式下，缺省算法为 **dsa**；FIPS 模式下，缺省算法为 **rsa**。如果服务器采用 **publickey** 认证，必须指定该参数。客户端使用指定算法的本地私钥生成数字签名或证书。

- **dsa:** 公钥算法为 DSA。
- **ecdsa-sha2-nistp256:** 指定公钥长度为 256 的 ECDSA 算法。
- **ecdsa-sha2-nistp384:** 指定公钥长度为 384 的 ECDSA 算法。
- **rsa:** 公钥算法为 RSA。
- **x509v3-ecdsa-sha2-nistp256:** x509v3-ecdsa-sha2-nistp256 公钥算法。
- **x509v3-ecdsa-sha2-nistp384:** x509v3-ecdsa-sha2-nistp384 公钥算法。
- **pki-domain domain-name:** 指定客户端证书的 PKI 域，为 1~31 个字符的字符串，不区分大小写，公钥算法为 x509v3 时，指定客户端证书所在 PKI 域名称，才能得到正确的本地证书。

prefer-compress: 服务器与客户端之间的首选压缩算法，缺省不支持压缩。

zlib: 压缩算法 ZLIB。

prefer-ctos-cipher: 客户端到服务器端的首选加密算法，缺省算法为 **aes128-ctr.des-cbc**、**3des-cbc**、**aes128-cbc**、**aes128-ctr**、**aes128-gcm**、**aes192-ctr**、**aes256-cbc**、**aes256-ctr**、**aes256-gcm** 算法的安全强度和运算花费时间依次递增。

- **3des-cbc:** 3DES-CBC 加密算法。
- **aes128-cbc:** 128 位的 AES-CBC 加密算法。
- **aes128-ctr:** 128 位 AES-CTR 加密算法。
- **aes128-gcm:** 128 位 AES-GCM 加密算法。
- **aes192-ctr:** 192 位 AES-CTR 加密算法。
- **aes256-cbc:** 256 位的 AES-CBC 加密算法。
- **aes256-ctr:** 256 位 AES-CTR 加密算法。
- **aes256-gcm:** 256 位 AES-GCM 加密算法。
- **des-cbc:** DES-CBC 加密算法。

prefer-ctos-hmac: 客户端到服务器端的首选 HMAC 算法，缺省算法为 **sha2-256**。**md5**、**md5-96**、**sha1**、**sha1-96**、**sha2-256**、**sha2-512** 算法的安全强度和运算花费时间依次递增。

- **md5:** HMAC 算法 HMAC-MD5。
- **md5-96:** HMAC 算法 HMAC-MD5-96。
- **sha1:** HMAC 算法 HMAC-SHA1。
- **sha1-96:** HMAC 算法 HMAC-SHA1-96。
- **sha2-256:** HMAC 算法 HMAC-SHA2-256。

- **sha2-512**: HMAC 算法 HMAC-SHA2-512。

prefer-kex : 密钥交换首选算法，缺省算法为 **ecdh-sha2-nistp256**。
dh-group-exchange-sha1、**dh-group1-sha1**、**dh-group14-sha1**、**ecdh-sha2-nistp256**、**ecdh-sha2-nistp384** 算法的安全强度和运算花费时间依次递增。

- **dh-group-exchange-sha1**: 密钥交换算法 diffie-hellman-group-exchange-sha1。
- **dh-group1-sha1**: 密钥交换算法 diffie-hellman-group1-sha1。
- **dh-group14-sha1**: 密钥交换算法 diffie-hellman-group14-sha1。
- **ecdh-sha2-nistp256**: 密钥交换算法 ecdh-sha2-nistp256。
- **ecdh-sha2-nistp384**: 密钥交换算法 ecdh-sha2-nistp384。

prefer-stoc-cipher: 服务器端到客户端的首选加密算法，缺省算法为 **aes128-ctr**。支持的加密算法与客户端到服务器端的加密算法相同。

prefer-stoc-hmac: 服务器端到客户端的首选 HMAC 算法，缺省算法为 **sha2-256**。支持的加密算法与客户端到服务器端的 HMAC 算法相同。

dscp dscp-value: 指定客户端发送的 SFTP 报文中携带的 DSCP 优先级，取值范围为 0~63，缺省值为 48。DSCP 携带在 IP 报文中的 ToS 字段，用来体现报文自身的优先等级，决定报文传输的优先程度。

public-key keyname: 指定服务器端的主机公钥，用于验证服务器端的身份。其中，*keyname* 表示已经配置的主机公钥名称，为 1~64 个字符的字符串，不区分大小写。

server-pki-domain domain-name: 指定验证服务端证书的 PKI 域。其中，*domain-name* 表示验证服务端证书的 PKI 域名称，为 1~31 个字符的字符串，不区分大小写，不能包括“~”、“*”、“\”、“|”、“:”、“.”、“<”、“>”、“”和“'”。

source: 指定与服务器通信的源 IPv4 地址或者源接口。缺省情况下，报文源 IPv4 地址为根据路由表项查找的发送此报文的出接口的主 IPv4 地址。为保证客户端与服务器之间的通信不会因为所指定的接口发生故障而中断，通常建议指定 Loopback 接口作为源接口，或者接口的 IPv4 地址作为源 IPv4 地址。

interface interface-type interface-number: 指定源接口。*interface-type* *interface-number* 为接口类型和接口编号。系统将采用该接口的主 IPv4 地址作为发送报文的源 IP 地址。

ip ip-address: 指定源 IPv4 地址。

【使用指导】

当客户端主机公钥算法协商成功为证书时，需要校验服务端证书是否正确，这样需要通过 **server-pki-domain** 指定服务端证书所在的 PKI 域名称，这样才能获取正确验证服务器证书。客户端使用保存在该 PKI 域中的 CA 证书对服务器证书进行合法性检查，无需提前保存服务器的公钥。如果客户端没有指定验证服务端证书所在的 PKI 域，则缺省使用客户端证书所在的 PKI 域进行验证。

【举例】

SFTP 客户端采用 publickey 认证方式，连接 IP 地址为 10.1.1.2 的 SFTP 服务器，采用如下连接策略，并指定服务器端的公钥名称为 svkey:

- 首选密钥交换算法为 **dh-group14-sha1**;
- 服务器到客户端的首选加密算法为 **aes128-cbc**;

- 客户端到服务器的首选 HMAC 算法为 **sha1**;
- 服务器到客户端的 HMAC 算法为 **sha1-96**;
- 服务器与客户端之间的首选压缩算法为 **zlib**。

```
<Sysname> sftp 10.1.1.2 prefer-kex dh-group14-sha1 prefer-stoc-cipher aes128-cbc
prefer-ctos-hmac sha1 prefer-stoc-hmac sha1-96 prefer-compress zlib public-key svkey
```

1.2.29 sftp client ipv6 source

sftp client ipv6 source 命令用来配置 SFTP 客户端发送 SFTP 报文使用的源 IPv6 地址。

undo sftp client ipv6 source 命令用来恢复缺省情况。

【命令】

```
sftp client ipv6 source { interface interface-type interface-number | ipv6
ipv6-address }
undo sftp client ipv6 source
```

【缺省情况】

未配置 SFTP 客户端使用的源 IPv6 地址，设备自动选择 IPv6 SFTP 报文的源 IPv6 地址，具体选择原则请参见 RFC 3484。

【视图】

系统视图

【缺省用户角色】

network-admin

【参数】

interface interface-type interface-number: 指定接口下与报文目的地址最匹配的 IPv6 地址作为源地址。*interface-type interface-number* 表示源接口类型与源接口编号。

ipv6 ipv6-address: 指定源 IPv6 地址。

【使用指导】

sftp client ipv6 source 命令指定的源地址对所有的 SFTP 连接有效，**sftp ipv6** 命令指定的源地址只对当前的 SFTP 连接有效。

使用该命令指定了源地址后，若 SFTP 用户使用 **sftp ipv6** 命令登录时又指定了源地址，则采用 **sftp ipv6** 命令中指定的源地址。

多次执行本命令，最后一次执行的命令生效。

【举例】

指定 SFTP 客户端发送 SFTP 报文使用的源 IPv6 地址为 2:2::2:2。

```
<Sysname> system-view
[Sysname] sftp client ipv6 source ipv6 2:2::2:2
```

【相关命令】

- **display sftp client source**

1.2.30 sftp client source

sftp client source 命令用来配置 SFTP 客户端发送 SFTP 报文使用的源 IPv4 地址。

undo sftp client source 命令用来恢复缺省情况。

【命令】

```
sftp client source { interface interface-type interface-number | ip
ip-address }
undo sftp client source
```

【缺省情况】

未配置 SFTP 客户端使用的源 IPv4 地址，SFTP 客户端发送 SFTP 报文使用的源 IPv4 地址为根据路由表项查找的发送此报文的出接口的主 IP 地址。

【视图】

系统视图

【缺省用户角色】

network-admin

【参数】

interface interface-type interface-number: 指定接口的主 IP 地址作为源地址。

interface-type interface-number 表示源接口类型与源接口编号。

ip ip-address: 指定源 IP 地址。

【使用指导】

sftp client source 命令指定的源地址对所有的 SFTP 连接有效，**sftp** 命令指定的源地址只对当前的 SFTP 连接有效。

使用该命令指定了源地址后，若 SFTP 用户使用 **sftp** 命令登录时又指定了源地址，则采用 **sftp** 命令中指定的源地址。

多次执行本命令，最后一次执行的命令生效。

【举例】

指定 SFTP 客户端发送 SFTP 报文使用的源 IP 地址为 192.168.0.1。

```
<Sysname> system-view
```

```
[Sysname] sftp client source ip 192.168.0.1
```

【相关命令】

- **display sftp client source**

1.2.31 sftp ipv6

sftp ipv6 命令用来建立 SFTP 客户端和与远程 IPv6 SFTP 服务器建立连接，并进入 SFTP 客户端视图。

【命令】

非 FIPS 模式下：


```
sftp ipv6 server [ port-number ] [ -i interface-type interface-number ]
[ identity-key { dsa | ecdsa-sha2-nistp256 | ecdsa-sha2-nistp384 | rsa |
{ x509v3-ecdsa-sha2-nistp256 | x509v3-ecdsa-sha2-nistp384 } pki-domain
domain-name } | prefer-compress zlib | prefer-ctos-cipher { 3des-cbc |
aes128-cbc | aes128-ctr | aes128-gcm | aes192-ctr | aes256-cbc | aes256-ctr |
aes256-gcm | des-cbc } | prefer-ctos-hmac { md5 | md5-96 | sha1 | sha1-96 |
sha2-256 | sha2-512 } | prefer-kex { dh-group-exchange-sha1 | dh-group1-sha1
| dh-group14-sha1 | ecdh-sha2-nistp256 | ecdh-sha2-nistp384 } |
prefer-stoc-cipher { 3des-cbc | aes128-cbc | aes128-ctr | aes128-gcm |
aes192-ctr | aes256-cbc | aes256-ctr | aes256-gcm | des-cbc } |
prefer-stoc-hmac { md5 | md5-96 | sha1 | sha1-96 | sha2-256 | sha2-512 } ] *
[ dscp dscp-value | { public-key keyname | server-pki-domain domain-name } |
source { interface interface-type interface-number | ipv6 ipv6-address } ] *
FIPS 模式下:
```

```
sftp ipv6 server [ port-number ] [ -i interface-type interface-number ]
[ identity-key { ecdsa-sha2-nistp256 | ecdsa-sha2-nistp384 | rsa |
{ x509v3-ecdsa-sha2-nistp256 | x509v3-ecdsa-sha2-nistp384 } pki-domain
domain-name } | prefer-compress zlib | prefer-ctos-cipher { aes128-cbc |
aes128-ctr | aes128-gcm | aes192-ctr | aes256-cbc | aes256-ctr | aes256-gcm }
| prefer-ctos-hmac { sha1 | sha1-96 | sha2-256 | sha2-512 } | prefer-kex
{ dh-group14-sha1 | ecdh-sha2-nistp256 | ecdh-sha2-nistp384 } |
prefer-stoc-cipher { aes128-cbc | aes128-ctr | aes128-gcm | aes192-ctr |
aes256-cbc | aes256-ctr | aes256-gcm } | prefer-stoc-hmac { sha1 | sha1-96 |
sha2-256 | sha2-512 } ] * [ { public-key keyname | server-pki-domain
domain-name } | source { interface interface-type interface-number | ipv6
ipv6-address } ] *
```

【视图】

用户视图

【缺省用户角色】

network-admin

【参数】

server: 服务器的 IPv6 地址或主机名称，为 1~253 个字符的字符串，不区分大小写。

port-number: 服务器端口号，取值范围为 1~65535，缺省值为 22。

-i interface-type interface-number: 客户端连接服务器时使用的出接口。其中，*interface-type interface-number* 表示接口类型和接口编号。本参数仅在客户端所连接的服务器的地址是链路本地地址时使用。指定的出接口必须具有链路本地地址。

identity-key: 客户端 **publickey** 认证时采用的公钥算法，非 FIPS 模式下，缺省算法为 **dsa**；FIPS 模式下，缺省算法为 **rsa**。如果服务器采用 **publickey** 认证，必须指定该参数。客户端使用指定算法的本地私钥生成数字签名或证书。

- **dsa:** 公钥算法为 DSA。

- **ecdsa-sha2-nistp256**: 指定公钥长度为 256 的 ECDSA 算法。
- **ecdsa-sha2-nistp384**: 指定公钥长度为 384 的 ECDSA 算法。
- **rsa**: 公钥算法为 RSA。
- **x509v3-ecdsa-sha2-nistp256**: x509v3-ecdsa-sha2-nistp256 公钥算法。
- **x509v3-ecdsa-sha2-nistp384**: x509v3-ecdsa-sha2-nistp384 公钥算法。
- **pki-domain domain-name**: 指定客户端证书的 PKI 域, 为 1~31 个字符的字符串, 不区分大小写, 公钥算法为 x509v3 时, 指定客户端证书所在 PKI 域名称, 才能得到正确的本地证书。

prefer-compress: 服务器与客户端之间的首选压缩算法, 缺省不支持压缩。

zlib: 压缩算法 ZLIB。

prefer-ctos-cipher: 客户端到服务器端的首选加密算法, 缺省算法为 **aes128-ctr**、**des-cbc**、**3des-cbc**、**aes128-cbc**、**aes128-ctr**、**aes128-gcm**、**aes192-ctr**、**aes256-cbc**、**aes256-ctr**、**aes256-gcm** 算法的安全强度和运算花费时间依次递增。

- **3des-cbc**: 3DES-CBC 加密算法。
- **aes128-cbc**: 128 位的 AES-CBC 加密算法。
- **aes128-ctr**: 128 位 AES-CTR 加密算法。
- **aes128-gcm**: 128 位 AES-GCM 加密算法。
- **aes192-ctr**: 192 位 AES-CTR 加密算法。
- **aes256-cbc**: 256 位的 AES-CBC 加密算法。
- **aes256-ctr**: 256 位 AES-CTR 加密算法。
- **aes256-gcm**: 256 位 AES-GCM 加密算法。
- **des-cbc**: DES-CBC 加密算法。

prefer-ctos-hmac: 客户端到服务器端的首选 HMAC 算法, 缺省算法为 **sha2-256**、**md5**、**md5-96**、**sha1**、**sha1-96**、**sha2-256**、**sha2-512** 算法的安全强度和运算花费时间依次递增。

- **md5**: HMAC 算法 HMAC-MD5。
- **md5-96**: HMAC 算法 HMAC-MD5-96。
- **sha1**: HMAC 算法 HMAC-SHA1。
- **sha1-96**: HMAC 算法 HMAC-SHA1-96。
- **sha2-256**: HMAC 算法 HMAC-SHA2-256。
- **sha2-512**: HMAC 算法 HMAC-SHA2-512。

prefer-kex: 密钥交换首选算法, 缺省算法为 **ecdh-sha2-nistp256**。
dh-group-exchange-sha1、**dh-group1-sha1**、**dh-group14-sha1**、**ecdh-sha2-nistp256**、**ecdh-sha2-nistp384** 算法的安全强度和运算花费时间依次递增。

- **dh-group-exchange-sha1**: 密钥交换算法 diffie-hellman-group-exchange-sha1。
- **dh-group1-sha1**: 密钥交换算法 diffie-hellman-group1-sha1。
- **dh-group14-sha1**: 密钥交换算法 diffie-hellman-group14-sha1。
- **ecdh-sha2-nistp256**: 密钥交换算法 ecdh-sha2-nistp256。
- **ecdh-sha2-nistp384**: 密钥交换算法 ecdh-sha2-nistp384。

prefer-stoc-cipher: 服务器端到客户端的首选加密算法，缺省算法为 **aes128-ctr**。支持的加密算法与客户端到服务器端的加密算法相同。

prefer-stoc-hmac: 服务器端到客户端的首选 HMAC 算法，缺省算法为 **sha2-256**。支持的加密算法与客户端到服务器端的 HMAC 算法相同。

dscp dscp-value: 指定客户端发送的 IPv6 SFTP 报文中携带的 DSCP 优先级，取值范围为 0~63，缺省值为 48。DSCP 携带在 IPv6 报文中的 Traffic class 字段，用来体现报文自身的优先等级，决定报文传输的优先程度。

public-key keyname: 指定服务器端的主机公钥，用于验证服务器端的身份。其中，*keyname* 表示已经配置的主机公钥名称，为 1~64 个字符的字符串，不区分大小写。

server-pki-domain domain-name: 指定验证服务端证书的 PKI 域。其中，*domain-name* 表示验证服务端证书的 PKI 域名称，为 1~31 个字符的字符串，不区分大小写，不能包括“~”、“*”、“\”、“|”、“:”、“.”、“<”、“>”、“”和“'”。

source: 指定与服务器通信的源 IPv6 地址或者源接口。缺省情况下，设备根据 RFC 3484 的规则自动选择一个源 IPv6 地址。为保证客户端与服务器之间的通信不会因为所指定的接口发生故障而中断，通常建议指定 Loopback 接口作为源接口，或者接口的 IPv6 地址作为源地址。

interface interface-type interface-number: 指定源接口。*interface-type* *interface-number* 为接口类型和接口编号。系统将使用该接口的 IPv6 地址作为发送报文的源 IP 地址。

ipv6 ipv6-address: 指定源 IPv6 地址。

【使用指导】

当客户端主机公钥算法协商成功为证书时，需要校验服务端证书是否正确，这样需要通过 **server-pki-domain** 指定服务端证书所在的 PKI 域名称，这样才能获取正确验证服务器证书。客户端使用保存在该 PKI 域中的 CA 证书对服务器证书进行合法性检查，无需提前保存服务器的公钥。如果客户端没有指定验证服务端证书所在的 PKI 域，则缺省使用客户端证书所在的 PKI 域进行验证。

【举例】

SFTP 客户端采用 **publickey** 认证方式，连接 IPv6 地址为 2000::1 的 SFTP 服务器，采用如下连接策略，并指定服务器端的公钥名称为 **svkey**：

- 首选密钥交换算法为 **dh-group14-sha1**；
- 服务器到客户端的首选加密算法为 **aes128-cbc**；
- 客户端到服务器的首选 HMAC 算法为 **sha1**；
- 服务器到客户端的 HMAC 算法为 **sha1-96**；
- 服务器与客户端之间的首选压缩算法为 **zlib**。

```
<Sysname> sftp ipv6 2000::1 prefer-kex dh-group14-sha1 prefer-stoc-cipher aes128-cbc
prefer-ctos-hmac sha1 prefer-stoc-hmac sha1-96 prefer-compress zlib public-key svkey
Username:
```

1.2.32 sftp ipv6 suite-b

sftp ipv6 suite-b 命令用来与远程的 ipv6 SFTP 服务器建立基于 Suite B 算法集的连接，并进入 SFTP 客户端视图。

【命令】

```
sftp ipv6 server [ port-number ] [ -i interface-type interface-number ]  
suite-b [ 128-bit | 192-bit ] pki-domain domain-name [ server-pki-domain  
domain-name ] [ prefer-compress zlib ] [ dscp dscp-value | source { interface  
interface-type interface-number | ipv6 ipv6-address } ] *
```

【视图】

用户视图

【缺省用户角色】

network-admin

【参数】

server: 服务器的 IPv6 地址或主机名称，为 1~253 个字符的字符串，不区分大小写。

port-number: 服务器端口号，取值范围为 1~65535，缺省值为 22。

-i interface-type interface-number: 客户端连接服务器时使用的出接口。其中，*interface-type interface-number* 表示接口类型和接口编号。本参数仅在客户端所连接的服务器的地址是链路本地地址时使用。指定的出接口必须具有链路本地地址。

suite-b: 指定采用 Suite B 算法集。若未指定 128-bit 和 192-bit 参数，则表示同时采用 128-bit 和 192-bit 的算法集。

128-bit: 指定客户端采用安全级别为 128-bit 的 Suite B 算法集。

192-bit: 指定客户端采用安全级别为 192-bit 的 Suite B 算法集。

pki-domain domain-name: 配置客户端证书的 PKI 域。*domain-name* 为客户端证书的 PKI 域名称，为 1~31 个字符的字符串，不区分大小写，不能包括“~”、“*”、“\”、“|”、“:”、“.”、“<”、“>”、“”和“'”。

server-pki-domain domain-name: 配置验证服务端证书的 PKI 域。*domain-name* 为验证服务端证书的 PKI 域名称，为 1~31 个字符的字符串，不区分大小写，不能包括“~”、“*”、“\”、“|”、“:”、“.”、“<”、“>”、“”和“'”。如果客户端没有指定验证服务端证书所在的 PKI 域，则缺省使用客户端证书所在的 PKI 域进行验证。

prefer-compress: 服务器与客户端之间的首选压缩算法，缺省情况下，不支持压缩。

zlib: 压缩算法 ZLIB。

dscp dscp-value: 指定客户端发送的 IPv6 SFTP 报文中携带的 DSCP 优先级，取值范围为 0~63，缺省值为 48。DSCP 携带在 IPv6 报文中的 Traffic class 字段，用来体现报文自身的优先等级，决定报文传输的优先程度。

source: 指定与服务器通信的源 IPv6 地址或者源接口。缺省情况下，设备根据 RFC 3484 的规则自动选择一个源 IPv6 地址。为保证客户端与服务器之间的通信不会因为所指定的接口发生故障而中断，通常建议指定 Loopback 接口作为源接口，或者接口的 IPv6 地址作为源地址。

interface interface-type interface-number: 指定源接口。*interface-type interface-number* 为接口类型和接口编号。系统将使用该接口的 IPv6 地址作为发送报文的源 IPv6 地址。

ipv6 ipv6-address: 指定源 IPv6 地址。

【使用指导】

当客户端采用安全级别为 128-bit 的 Suite B 算法集与远程的 SFTP 服务器建立连接时，客户端算法要求：

- 密钥交换算法为 **ecdh-sha2-nistp256**;
- 服务器到客户端的加密算法为 **aes128-gcm**;
- 客户端到服务器的加密算法为 **aes128-gcm**;
- 服务器到客户端的 HMAC 算法为 **aes128-gcm**;
- 客户端到服务器的 HMAC 算法为 **aes128-gcm**;
- 主机公钥算法为 **x509v3-ecdsa-sha2-nistp256**、**x509v3-ecdsa-sha2-nistp384**。

当客户端采用安全级别为 192-bit 的 Suite B 算法集与远程的 SFTP 服务器建立连接时，客户端算法要求：

- 密钥交换算法为 **ecdh-sha2-nistp384**;
- 服务器到客户端的加密算法为 **aes256-gcm**;
- 客户端到服务器的加密算法为 **aes256-gcm**;
- 服务器到客户端的 HMAC 算法为 **aes256-gcm**;
- 客户端到服务器的 HMAC 算法为 **aes256-gcm**;
- 主机公钥算法为 **x509v3-ecdsa-sha2-nistp384**。

当客户端未采用安全级别为 128-bit 和 192-bit 的 Suite B 算法集与远程的 SFTP 服务器建立连接时，客户端算法要求：

- 密钥交换算法为 **ecdh-sha2-nistp256**、**ecdh-sha2-nistp384**;
- 服务器到客户端的加密算法为 **aes128-gcm**、**aes256-gcm**;
- 客户端到服务器的加密算法为 **aes128-gcm**、**aes256-gcm**;
- 服务器到客户端的 HMAC 算法为 **aes128-gcm**、**aes256-gcm**;
- 客户端到服务器的 HMAC 算法为 **aes128-gcm**、**aes256-gcm**;
- 主机公钥算法为 **x509v3-ecdsa-sha2-nistp256**、**x509v3-ecdsa-sha2-nistp384**。

【举例】

SFTP 客户端采用安全级别为 192-bit 的 Suite B 算法集，与登录地址为 2000::1 的远程 SFTP 服务器建立连接，采用如下连接策略：指定客户端证书的 PKI 域名称为 **clientpkidomain**，指定验证服务端证书的 PKI 域名称为 **serverpkidomain**。

```
<Sysname> sftp ipv6 2000::1 suite-b 192-bit pki-domain clientpkidomain server-pki-domain
serverpkidomain
Username:
```

1.2.33 sftp suite-b

sftp suite-b 命令用来与远程的 IPv4 SFTP 服务器建立基于 Suite B 算法集的连接，并进入 SFTP 客户端视图。

【命令】

```
sftp server [ port-number ] suite-b [ 128-bit | 192-bit ] pki-domain
domain-name [ server-pki-domain domain-name ] [ prefer-compress zlib ] [ dscp
```

```
dscp-value | source { interface interface-type interface-number | ip  
ip-address } ] *
```

【视图】

用户视图

【缺省用户角色】

network-admin

【参数】

server: 服务器的 IPv4 地址或主机名称, 为 1~253 个字符的字符串, 不区分大小写。

port-number: 服务器端口号, 取值范围为 1~65535, 缺省值为 22。

suite-b: 指定采用 Suite B 算法集。若未指定 128-bit 和 192-bit 参数, 则表示同时采用 128-bit 和 192-bit 的算法集。

128-bit: 指定客户端采用安全级别为 128-bit 的 Suite B 算法集。

192-bit: 指定客户端采用安全级别为 192-bit 的 Suite B 算法集。

pki-domain domain-name: 配置客户端证书的 PKI 域。*domain-name* 为客户端证书的 PKI 域名称, 为 1~31 个字符的字符串, 不区分大小写, 不能包括 “~”、“*”、“\”、“|”、“:”、“.”、“<”、“>”、“” 和 “'”。

server-pki-domain domain-name: 配置验证服务端证书的 PKI 域。*domain-name* 为验证服务端证书的 PKI 域名称, 为 1~31 个字符的字符串, 不区分大小写, 不能包括 “~”、“*”、“\”、“|”、“:”、“.”、“<”、“>”、“” 和 “'”。如果客户端没有指定验证服务端证书所在的 PKI 域, 则缺省使用客户端证书所在的 PKI 域进行验证。

prefer-compress: 服务器与客户端之间的首选压缩算法, 缺省情况下, 不支持压缩。

zlib: 压缩算法 ZLIB。

dscp dscp-value: 指定客户端发送的 SFTP 报文中携带的 DSCP 优先级, 取值范围为 0~63, 缺省值为 48。DSCP 携带在 IP 报文中的 ToS 字段, 用来体现报文自身的优先等级, 决定报文传输的优先程度。

source: 指定与服务器通信的源 IP 地址或者源接口。缺省情况下, 设备根据路由表项自动选择一个源 IPv4 地址。为保证客户端与服务器之间的通信不会因为所指定的接口发生故障而中断, 通常建议指定 Loopback 接口作为源接口, 或者接口的 IP 地址作为源地址。

interface interface-type interface-number: 指定源接口。*interface-type interface-number* 为接口类型和接口编号。系统将使用该接口的 IPv4 地址作为发送报文的源 IP 地址。

ip ip-address: 指定源 IPv4 地址。

【使用指导】

当客户端采用安全级别为 128-bit 的 Suite B 算法集与远程的 SFTP 服务器建立连接时, 客户端算法要求:

- 密钥交换算法为 **ecdh-sha2-nistp256**;
- 服务器到客户端的加密算法为 **aes128-gcm**;
- 客户端到服务器的加密算法为 **aes128-gcm**;
- 服务器到客户端的 HMAC 算法为 **aes128-gcm**;

- 客户端到服务器的 HMAC 算法为 **aes128-gcm**;
 - 主机公钥算法为 **x509v3-ecdsa-sha2-nistp256**、**x509v3-ecdsa-sha2-nistp384**。
- 当客户端采用安全级别为 192-bit 的 Suite B 算法集与远程的 SFTP 服务器建立连接时，客户端算法要求：

- 密钥交换算法为 **ecdh-sha2-nistp384**;
- 服务器到客户端的加密算法为 **aes256-gcm**;
- 客户端到服务器的加密算法为 **aes256-gcm**;
- 服务器到客户端的 HMAC 算法为 **aes256-gcm**;
- 客户端到服务器的 HMAC 算法为 **aes256-gcm**;
- 主机公钥算法为 **x509v3-ecdsa-sha2-nistp384**。

当客户端未采用安全级别为 128-bit 和 192-bit 的 Suite B 算法集与远程的 SFTP 服务器建立连接时，客户端算法要求：

- 密钥交换算法为 **ecdh-sha2-nistp256**、**ecdh-sha2-nistp384**;
- 服务器到客户端的加密算法为 **aes128-gcm**、**aes256-gcm**;
- 客户端到服务器的加密算法为 **aes128-gcm**、**aes256-gcm**;
- 服务器到客户端的 HMAC 算法为 **aes128-gcm**、**aes256-gcm**;
- 客户端到服务器的 HMAC 算法为 **aes128-gcm**、**aes256-gcm**;
- 主机公钥算法为 **x509v3-ecdsa-sha2-nistp256**、**x509v3-ecdsa-sha2-nistp384**。

【举例】

SFTP 客户端采用安全级别为 128-bit 的 Suite B 算法集，与登录地址为 10.1.1.2 的远程 SFTP 服务器建立连接，采用如下连接策略：指定客户端证书的 PKI 域名称为 **clientpkidomain**，指定验证服务端证书的 PKI 域名称为 **serverpkidomain**。

```
<Sysname> sftp 10.1.1.2 suite-b 128-bit pki-domain clientpkidomain server-pki-domain
serverpkidomain
Username:
```

1.2.34 ssh client ipv6 source

ssh client ipv6 source 命令用来为配置 Stelnet 客户端发送 SSH 报文使用的源 IPv6 地址。

undo ssh client ipv6 source 命令用来恢复缺省情况。

【命令】

```
ssh client ipv6 source { interface interface-type interface-number | ipv6
ipv6-address }
undo ssh client ipv6 source
```

【缺省情况】

未配置 Stelnet 客户端使用的源 IPv6 地址，设备自动选择 IPv6 SSH 报文的源 IPv6 地址，具体选择原则请参见 RFC 3484。

【视图】

系统视图

【缺省用户角色】

network-admin

【参数】

interface *interface-type interface-number*: 指定接口下与报文目的地址最匹配的 IPv6 地址作为源地址。*interface-type interface-number* 表示源接口类型与源接口编号。

ipv6 *ipv6-address*: 指定源 IPv6 地址。

【使用指导】

ssh client ipv6 source 命令指定的源地址对所有的 IPv6 Stelnet 连接有效, **ssh2 ipv6** 命令指定的源地址只对当前的 Stelnet 连接有效。

使用该命令指定了源地址后, 若 SSH 用户使用 **ssh2 ipv6** 命令登录时又指定了源地址, 则采用 **ssh2 ipv6** 命令中指定的源地址。

多次执行本命令, 最后一次执行的命令生效。

【举例】

指定 Stelnet 客户端发送 SSH 报文使用的源 IPv6 地址为 2:2::2:2。

```
<Sysname> system-view
[Sysname] ssh client ipv6 source ipv6 2:2::2:2
```

【相关命令】

- **display ssh client source**

1.2.35 ssh client source

ssh client source 命令用来配置 Stelnet 客户端发送 SSH 报文使用的源 IPv4 地址。

undo ssh client source 命令用来恢复缺省情况。

【命令】

```
ssh client source { interface interface-type interface-number | ip
ip-address }
undo ssh client source
```

【缺省情况】

未配置 Stelnet 客户端使用的源 IPv4 地址, Stelnet 客户端发送 SSH 报文使用的源 IPv4 地址为设备路由指定的 SSH 报文出接口的主 IP 地址。

【视图】

系统视图

【缺省用户角色】

network-admin

【参数】

interface *interface-type interface-number*: 指定接口的主 IP 地址作为源地址。*interface-type interface-number* 表示源接口类型与源接口编号。

ip *ip-address*: 指定源 IPv4 地址。

【使用指导】

ssh client source 命令指定的源地址对所有的 Stelnet 连接有效，**ssh2** 命令指定的源地址只对当前的 Stelnet 连接有效。

使用该命令指定了源地址后，若 SSH 用户使用 **ssh2** 命令登录时又指定了源地址，则采用 **ssh2** 命令中指定的源地址。

多次执行本命令，最后一次执行的命令生效。

【举例】

指定 Stelnet 客户端发送 SSH 报文使用的源 IPv4 地址为 192.168.0.1。

```
<Sysname> system-view
```

```
[Sysname] ssh client source ip 192.168.0.1
```

【相关命令】

- **display ssh client source**

1.2.36 ssh2

ssh2 命令用来建立 Stelnet 客户端和 IPv4 Stelnet 服务器端的连接。

【命令】

非 FIPS 模式下：

```
ssh2 server [ port-number ] [ identity-key { dsa | ecdsa-sha2-nistp256 |  
ecdsa-sha2-nistp384 | rsa | { x509v3-ecdsa-sha2-nistp256 |  
x509v3-ecdsa-sha2-nistp384 } pki-domain domain-name } | prefer-compress  
zlib | prefer-ctos-cipher { 3des-cbc | aes128-cbc | aes128-ctr | aes128-gcm |  
aes192-ctr | aes256-cbc | aes256-ctr | aes256-gcm | des-cbc } |  
prefer-ctos-hmac { md5 | md5-96 | sha1 | sha1-96 | sha2-256 | sha2-512 } |  
prefer-kex { dh-group-exchange-sha1 | dh-group1-sha1 | dh-group14-sha1 |  
ecdh-sha2-nistp256 | ecdh-sha2-nistp384 } | prefer-stoc-cipher { 3des-cbc |  
aes128-cbc | aes128-ctr | aes128-gcm | aes192-ctr | aes256-cbc | aes256-ctr  
| aes256-gcm | des-cbc } | prefer-stoc-hmac { md5 | md5-96 | sha1 | sha1-96 |  
sha2-256 | sha2-512 } ] * [ dscp dscp-value | escape character | { public-key  
keyname | server-pki-domain domain-name } | source { interface  
interface-type interface-number | ip ip-address } ] *
```

FIPS 模式下：

```
ssh2 server [ port-number ] [ identity-key { ecdsa-sha2-nistp256 |  
ecdsa-sha2-nistp384 | rsa | { x509v3-ecdsa-sha2-nistp256 |  
x509v3-ecdsa-sha2-nistp384 } pki-domain domain-name } | prefer-compress  
zlib | prefer-ctos-cipher { aes128-cbc | aes128-ctr | aes128-gcm | aes192-ctr  
| aes256-cbc | aes256-ctr | aes256-gcm } | prefer-ctos-hmac { sha1 | sha1-96 |  
sha2-256 | sha2-512 } | prefer-kex { dh-group14-sha1 | ecdh-sha2-nistp256 |  
ecdh-sha2-nistp384 } | prefer-stoc-cipher { aes128-cbc | aes128-ctr |  
aes128-gcm | aes192-ctr | aes256-cbc | aes256-ctr | aes256-gcm } |  
prefer-stoc-hmac { sha1 | sha1-96 | sha2-256 | sha2-512 } ] * [ escape character
```

```
| { public-key keyname | server-pki-domain domain-name } | source { interface  
interface-type interface-number | ip ip-address } ] *
```

【视图】

用户视图

【缺省用户角色】

network-admin

【参数】

server: 服务器 IPv4 地址或主机名称，为 1~253 个字符的字符串，不区分大小写。

port-number: 服务器端口号，取值范围为 1~65535，缺省值为 22。

identity-key: 客户端 **publickey** 认证时采用的公钥算法，非 FIPS 模式下，缺省算法为 **dsa**；FIPS 模式下，缺省算法为 **rsa**。如果服务器采用 **publickey** 认证，必须指定该参数。客户端使用指定算法的本地私钥生成数字签名或证书。

- **dsa**: 公钥算法为 DSA。
- **ecdsa-sha2-nistp256**: 指定公钥长度为 256 的 ECDSA 算法。
- **ecdsa-sha2-nistp384**: 指定公钥长度为 384 的 ECDSA 算法。
- **rsa**: 公钥算法为 RSA。
- **x509v3-ecdsa-sha2-nistp256**: x509v3-ecdsa-sha2-nistp256 公钥算法。
- **x509v3-ecdsa-sha2-nistp384**: x509v3-ecdsa-sha2-nistp384 公钥算法。
- **pki-domain domain-name**: 指定客户端证书的 PKI 域，为 1~31 个字符的字符串，不区分大小写，公钥算法为 x509v3 时，指定客户端证书所在 PKI 域名称，才能得到正确的本地证书。

prefer-compress: 服务器与客户端之间的首选压缩算法，缺省不支持压缩。

zlib: 压缩算法 ZLIB。

prefer-ctos-cipher: 客户端到服务器端的首选加密算法，缺省算法为 **aes128-ctr.des-cbc**、**3des-cbc**、**aes128-cbc**、**aes128-ctr**、**aes128-gcm**、**aes192-ctr**、**aes256-cbc**、**aes256-ctr**、**aes256-gcm** 算法的安全强度和运算花费时间依次递增。

- **3des-cbc**: 3DES-CBC 加密算法。
- **aes128-cbc**: 128 位的 AES-CBC 加密算法。
- **aes128-ctr**: 128 位 AES-CTR 加密算法。
- **aes128-gcm**: 128 位 AES-GCM 加密算法。
- **aes192-ctr**: 192 位 AES-CTR 加密算法。
- **aes256-cbc**: 256 位的 AES-CBC 加密算法。
- **aes256-ctr**: 256 位 AES-CTR 加密算法。
- **aes256-gcm**: 256 位 AES-GCM 加密算法。
- **des-cbc**: DES-CBC 加密算法。

prefer-ctos-hmac: 客户端到服务器端的首选 HMAC 算法，缺省算法为 **sha2-256**、**md5**、**md5-96**、**sha1**、**sha1-96**、**sha2-256**、**sha2-512** 算法的安全强度和运算花费时间依次递增。

- **md5**: HMAC 算法 HMAC-MD5。

- **md5-96**: HMAC 算法 HMAC-MD5-96。
- **sha1**: HMAC 算法 HMAC-SHA1。
- **sha1-96**: HMAC 算法 HMAC-SHA1-96。
- **sha2-256**: HMAC 算法 HMAC-SHA2-256。
- **sha2-512**: HMAC 算法 HMAC-SHA2-512。

prefer-kex : 密钥交换首选算法，缺省算法为 **ecdh-sha2-nistp256**。
dh-group-exchange-sha1、**dh-group14-sha1**、**ecdh-sha2-nistp256**、**ecdh-sha2-nistp384** 算法的安全强度和运算花费时间依次递增。

- **dh-group-exchange-sha1**: 密钥交换算法 diffie-hellman-group-exchange-sha1。
- **dh-group1-sha1**: 密钥交换算法 diffie-hellman-group1-sha1。
- **dh-group14-sha1**: 密钥交换算法 diffie-hellman-group14-sha1。
- **ecdh-sha2-nistp256**: 密钥交换算法 ecdh-sha2-nistp256。
- **ecdh-sha2-nistp384**: 密钥交换算法 ecdh-sha2-nistp384。

prefer-stoc-cipher: 服务器端到客户端的首选加密算法，缺省算法为 **aes128-ctr**。支持的加密算法与客户端到服务器端的加密算法相同。

prefer-stoc-hmac: 服务器端到客户端的首选 HMAC 算法，缺省算法为 **sha2-256**。支持的加密算法与客户端到服务器端的 HMAC 算法相同。

dscp dscp-value: 指定客户端发送的 SFTP 报文中携带的 DSCP 优先级，取值范围为 0~63，缺省值为 48。DSCP 携带在 IP 报文中的 ToS 字段，用来体现报文自身的优先等级，决定报文传输的优先程度。

escape character: 指定退出字符。*character* 为一个字符，区分大小写，缺省为 ~，即输入 ~. 可以强制断开与服务端的连接。

public-key keyname: 指定服务器端的主机公钥，用于验证服务器端的身份。其中，*keyname* 表示已经配置的主机公钥名称，为 1~64 个字符的字符串，不区分大小写。

server-pki-domain domain-name: 指定验证服务端证书的 PKI 域。其中，*domain-name* 表示验证服务端证书的 PKI 域名称，为 1~31 个字符的字符串，不区分大小写，不能包括 “~”、“*”、“\”、“|”、“:”、“.”、“<”、“>”、“” 和 “'”。

source: 指定与服务器通信的源 IPv4 地址或者源接口。缺省情况下，报文源 IPv4 地址为根据路由表项查找的发送此报文的出接口的主 IPv4 地址。为保证客户端与服务器之间的通信不会因为所指定的接口发生故障而中断，通常建议指定 Loopback 接口作为源接口，或者接口的 IPv4 地址作为源地址。

interface interface-type interface-number: 指定源接口。*interface-type* *interface-number* 为接口类型和接口编号。系统将采用该接口的主 IPv4 地址作为发送报文的源 IP 地址。

ip ip-address: 指定源 IPv4 地址。

【使用指导】

当客户端主机公钥算法协商成功为证书时，需要校验服务端证书是否正确，这样需要通过 **server-pki-domain** 指定服务端证书所在的 PKI 域名称，这样才能获取正确验证服务器证书。客户端使用保存在该 PKI 域中的 CA 证书对服务器证书进行合法性检查，无需提前保存服务器的公

钥。如果客户端没有指定验证服务端证书所在的 PKI 域，则缺省使用客户端证书所在的 PKI 域进行验证。

关于退出字符的使用，需要注意的是：

- 退出字符与字符.配合使用可以强制断开客户端与服务器连接（该方式通常用于服务器端重启或发生异常的情况下，客户端快速中断当前连接）。
- 必须在一行中首先输入退出字符和.，该操作才能生效，若该行中曾经输入过其它字符或执行了其它操作（比如退格），则需要重新换行输入才能生效。
- 一般情况下，建议使用缺省退出字符，避免退出字符和.的组合与登录用户名相同。

【举例】

Stelnet 客户端采用 **publickey** 认证方式，登录地址为 3.3.3.3 的远程 Stelnet 服务器，采用如下连接策略，并指定服务器端的公钥名称为 **svkey**：

- 首选密钥交换算法为 **dh-group14-sha1**；
- 服务器到客户端的首选加密算法为 **aes128-cbc**；
- 客户端到服务器的首选 HMAC 算法为 **sha1**；
- 服务器到客户端的 HMAC 算法为 **sha1-96**；
- 服务器与客户端之间的首选压缩算法为 **zlib**；
- 输入\$.时强制断开客户端和服务端的连接。

```
<Sysname> ssh2 3.3.3.3 prefer-kex dh-group14-sha1 prefer-stoc-cipher aes128-cbc
prefer-ctos-hmac sha1 prefer-stoc-hmac sha1-96 prefer-compress zlib public-key svkey escape
$
```

1.2.37 ssh2 ipv6

ssh2 ipv6 命令用来建立 Stelnet 客户端和 IPv6 Stelnet 服务器端的连接。

【命令】

非 FIPS 模式下：

```
ssh2 ipv6 server [ port-number ] [ -i interface-type interface-number ]
[ identity-key { dsa | ecdsa-sha2-nistp256 | ecdsa-sha2-nistp384 | rsa |
{ x509v3-ecdsa-sha2-nistp256 | x509v3-ecdsa-sha2-nistp384 } pki-domain
domain-name } | prefer-compress zlib | prefer-ctos-cipher { 3des-cbc |
aes128-cbc | aes128-ctr | aes128-gcm | aes192-ctr | aes256-cbc | aes256-ctr |
aes256-gcm | des-cbc } | prefer-ctos-hmac { md5 | md5-96 | sha1 | sha1-96 |
sha2-256 | sha2-512 } | prefer-kex { dh-group-exchange-sha1 | dh-group1-sha1
| dh-group14-sha1 | ecdh-sha2-nistp256 | ecdh-sha2-nistp384 } |
prefer-stoc-cipher { 3des-cbc | aes128-cbc | aes128-ctr | aes128-gcm |
aes192-ctr | aes256-cbc | aes256-ctr | aes256-gcm | des-cbc } |
prefer-stoc-hmac { md5 | md5-96 | sha1 | sha1-96 | sha2-256 | sha2-512 } ] *
[ dscp dscp-value | escape character | { public-key keyname |
server-pki-domain domain-name } | source { interface interface-type
interface-number | ipv6 ipv6-address } ] *
```

FIPS 模式下：

```
ssh2 ipv6 server [ port-number ] [ -i interface-type interface-number ]
[ identity-key { ecdsa-sha2-nistp256 | ecdsa-sha2-nistp384 | rsa |
{ x509v3-ecdsa-sha2-nistp256 | x509v3-ecdsa-sha2-nistp384 } pki-domain
domain-name } | prefer-compress zlib | prefer-ctos-cipher { aes128-cbc |
aes128-ctr | aes128-gcm | aes192-ctr | aes256-cbc | aes256-ctr | aes256-gcm }
| prefer-ctos-hmac { sha1 | sha1-96 | sha2-256 | sha2-512 } | prefer-kex
{ dh-group14-sha1 | ecdh-sha2-nistp256 | ecdh-sha2-nistp384 } |
prefer-stoc-cipher { aes128-cbc | aes128-ctr | aes128-gcm | aes192-ctr |
aes256-cbc | aes256-ctr | aes256-gcm } | prefer-stoc-hmac { sha1 | sha1-96 |
sha2-256 | sha2-512 } ] * [ escape character | { public-key keyname |
server-pki-domain domain-name } | source { interface interface-type
interface-number | ipv6 ipv6-address } ] *
```

【视图】

用户视图

【缺省用户角色】

network-admin

【参数】

server: 服务器的 IPv6 地址或主机名称，为 1~253 个字符的字符串，不区分大小写。

port-number: 服务器端口号，取值范围为 1~65535，缺省值为 22。

-i interface-type interface-number: 客户端连接服务器时使用的出接口。其中，*interface-type interface-number* 表示接口类型和接口编号。本参数仅在客户端所连接的服务器的地址是链路本地地址时使用。指定的出接口必须具有链路本地地址。

identity-key: 客户端 **publickey** 认证时采用的公钥算法，非 FIPS 模式下，缺省算法为 **dsa**；FIPS 模式下，缺省算法为 **rsa**。如果服务器采用 **publickey** 认证，必须指定该参数。客户端使用指定算法的本地私钥生成数字签名或证书。

- **dsa**: 公钥算法为 DSA。
- **ecdsa-sha2-nistp256**: 指定公钥长度为 256 的 ECDSA 算法。
- **ecdsa-sha2-nistp384**: 指定公钥长度为 384 的 ECDSA 算法。
- **rsa**: 公钥算法为 RSA。
- **x509v3-ecdsa-sha2-nistp256**: x509v3-ecdsa-sha2-nistp256 公钥算法。
- **x509v3-ecdsa-sha2-nistp384**: x509v3-ecdsa-sha2-nistp384 公钥算法。
- **pki-domain domain-name**: 指定客户端证书的 PKI 域，为 1~31 个字符的字符串，不区分大小写，公钥算法为 x509v3 时，指定客户端证书所在 PKI 域名称，才能得到正确的本地证书。

prefer-compress: 服务器与客户端之间的首选压缩算法，缺省不支持压缩。

zlib: 压缩算法 ZLIB。

prefer-ctos-cipher: 客户端到服务器端的首选加密算法，缺省算法为 **aes128-ctr**。**des-cbc**、**3des-cbc**、**aes128-cbc**、**aes128-ctr**、**aes128-gcm**、**aes192-ctr**、**aes256-cbc**、**aes256-ctr**、**aes256-gcm** 算法的安全强度和运算花费时间依次递增。

- **3des-cbc**: 3DES-CBC 加密算法。
- **aes128-cbc**: 128 位的 AES-CBC 加密算法。
- **aes128-ctr**: 128 位 AES-CTR 加密算法。
- **aes128-gcm**: 128 位 AES-GCM 加密算法。
- **aes192-ctr**: 192 位 AES-CTR 加密算法。
- **aes256-cbc**: 256 位的 AES-CBC 加密算法。
- **aes256-ctr**: 256 位 AES-CTR 加密算法。
- **aes256-gcm**: 256 位 AES-GCM 加密算法。
- **des-cbc**: DES-CBC 加密算法。

prefer-ctos-hmac: 客户端到服务器端的首选 HMAC 算法，缺省算法为 **sha2-256**。**md5**、**md5-96**、**sha1**、**sha1-96**、**sha2-256**、**sha2-512** 算法的安全强度和运算花费时间依次递增。

- **md5**: HMAC 算法 HMAC-MD5。
- **md5-96**: HMAC 算法 HMAC-MD5-96。
- **sha1**: HMAC 算法 HMAC-SHA1。
- **sha1-96**: HMAC 算法 HMAC-SHA1-96。
- **sha2-256**: HMAC 算法 HMAC-SHA2-256。
- **sha2-512**: HMAC 算法 HMAC-SHA2-512。

prefer-kex: 密钥交换首选算法，缺省算法为 **ecdh-sha2-nistp256**。**dh-group-exchange-sha1**、**dh-group1-sha1**、**dh-group14-sha1**、**ecdh-sha2-nistp256**、**ecdh-sha2-nistp384** 算法的安全强度和运算花费时间依次递增。

- **dh-group-exchange-sha1**: 密钥交换算法 diffie-hellman-group-exchange-sha1。
- **dh-group1-sha1**: 密钥交换算法 diffie-hellman-group1-sha1。
- **dh-group14-sha1**: 密钥交换算法 diffie-hellman-group14-sha1。
- **ecdh-sha2-nistp256**: 密钥交换算法 ecdh-sha2-nistp256。
- **ecdh-sha2-nistp384**: 密钥交换算法 ecdh-sha2-nistp384。

prefer-stoc-cipher: 服务器端到客户端的首选加密算法，缺省算法为 **aes128-ctr**。支持的加密算法与客户端到服务器端的加密算法相同。

prefer-stoc-hmac: 服务器端到客户端的首选 HMAC 算法，缺省算法为 **sha2-256**。支持的加密算法与客户端到服务器端的 HMAC 算法相同。

dscp dscp-value: 指定客户端发送的 IPv6 SSH 报文中携带的 DSCP 优先级，取值范围为 0~63，缺省值为 48。DSCP 携带在 IPv6 报文中的 Traffic class 字段，用来体现报文自身的优先等级，决定报文传输的优先程度。

escape character: 指定退出字符。*character* 为一个字符，区分大小写，缺省为 ~，即输入 ~. 可以强制断开与服务端的连接。

public-key keyname: 指定服务器端的主机公钥，用于验证服务器端的身份。其中，*keyname* 表示已经配置的主机公钥名称，为 1~64 个字符的字符串，不区分大小写。

server-pki-domain domain-name: 指定验证服务端证书的 PKI 域。其中，*domain-name* 表示验证服务端证书的 PKI 域名称，为 1~31 个字符的字符串，不区分大小写，不能包括 “~”、“*”、“\”、“|”、“:”、“.”、“<”、“>”、“” 和 “'”。

source: 指定与服务器通信的源 IPv6 地址或者源接口。缺省情况下,设备根据 RFC 3484 的规则自动选择一个源 IPv6 地址。为保证客户端与服务器之间的通信不会因为所指定的接口发生故障而中断,通常建议指定 Loopback 接口作为源接口,或者接口的 IPv6 地址作为源地址。

interface interface-type interface-number: 指定源接口。*interface-type interface-number* 为接口类型和接口编号。系统将使用该接口的 IPv6 地址作为发送报文的源 IP 地址。

ipv6 ipv6-address: 指定源 IPv6 地址。

【使用指导】

当客户端主机公钥算法协商成功为证书时,需要校验服务端证书是否正确,这样需要通过 **server-pki-domain** 指定服务端证书所在的 PKI 域名称,这样才能获取正确验证服务器证书。客户端使用保存在该 PKI 域中的 CA 证书对服务器证书进行合法性检查,无需提前保存服务器的公钥。如果客户端没有指定验证服务端证书所在的 PKI 域,则缺省使用客户端证书所在的 PKI 域进行验证。

关于退出字符的使用,需要注意的是:

- 退出字符与字符.配合使用可以强制断开客户端与服务器连接(该方式通常用于服务器端重启或发生异常的情况下,客户端快速中断当前连接)。
- 必须在一行中首先输入退出字符和.,该操作才能生效,若该行中曾经输入过其它字符或执行了其它操作(比如退格),则需要重新换行输入才能生效。
- 一般情况下,建议使用缺省退出字符,避免退出字符和.的组合与登录用户名相同。

【举例】

SSH 客户端采用 **publickey** 认证方式,登录地址为 2000::1 的远程 Stelnet 服务器,采用如下连接策略,并指定服务器端的公钥名称为 **svkey**:

- 首选密钥交换算法为 **dh-group14-sha1**;
- 服务器到客户端的首选加密算法为 **aes128-cbc**;
- 客户端到服务器的首选 HMAC 算法为 **sha1**;
- 服务器到客户端的 HMAC 算法为 **sha1-96**;
- 服务器与客户端之间的首选压缩算法为 **zlib**;
- 输入\$.时强制断开客户端和服务端的连接。

```
<Sysname> ssh2 ipv6 2000::1 prefer-kex dh-group14-sha1 prefer-stoc-cipher aes128-cbc  
prefer-ctos-hmac sha1 prefer-stoc-hmac sha1-96 prefer-compress zlib public-key svkey $
```

1.2.38 ssh2 ipv6 suite-b

ssh2 ipv6 suite-b 命令用来与远程的 ipv6 Stelnet 服务器建立基于 Suite B 算法集的连接。

【命令】

```
ssh2 ipv6 server [ port-number ] [ -i interface-type interface-number ]  
suite-b [ 128-bit | 192-bit ] pki-domain domain-name [ server-pki-domain  
domain-name ] [ prefer-compress zlib ] [ dscp dscp-value | escape character |  
source { interface interface-type interface-number | ipv6 ipv6-address } ] *
```

【视图】

用户视图

【缺省用户角色】

network-admin

【参数】

server: 服务器的 IPv6 地址或主机名称, 为 1~253 个字符的字符串, 不区分大小写。

port-number: 服务器端口号, 取值范围为 1~65535, 缺省值为 22。

-i interface-type interface-number: 客户端连接服务器时使用的出接口。其中, *interface-type interface-number* 表示接口类型和接口编号。本参数仅在客户端所连接的服务器的地址是链路本地地址时使用。指定的出接口必须具有链路本地地址。

suite-b: 指定采用 Suite B 算法集。若未指定 128-bit 和 192-bit 参数, 则表示同时采用 128-bit 和 192-bit 的算法集。

128-bit: 指定客户端采用安全级别为 128-bit 的 Suite B 算法集。

192-bit: 指定客户端采用安全级别为 192-bit 的 Suite B 算法集。

pki-domain domain-name: 配置客户端证书的 PKI 域。*domain-name* 为客户端证书的 PKI 域名称, 为 1~31 个字符的字符串, 不区分大小写, 不能包括 “~”、“*”、“\”、“|”、“:”、“.”、“<”、“>”、“” 和 “'”。

server-pki-domain domain-name: 配置验证服务端证书的 PKI 域。*domain-name* 为验证服务端证书的 PKI 域名称, 为 1~31 个字符的字符串, 不区分大小写, 不能包括 “~”、“*”、“\”、“|”、“:”、“.”、“<”、“>”、“” 和 “'”。如果客户端没有指定验证服务端证书所在的 PKI 域, 则缺省使用客户端证书所在的 PKI 域进行验证。

prefer-compress: 服务器与客户端之间的首选压缩算法, 缺省情况下, 不支持压缩。

zlib: 压缩算法 ZLIB。

dscp dscp-value: 指定客户端发送的 IPv6 SSH 报文中携带的 DSCP 优先级, 取值范围为 0~63, 缺省值为 48。DSCP 携带在 IPv6 报文中的 Traffic class 字段, 用来体现报文自身的优先等级, 决定报文传输的优先程度。

escape character: 指定退出字符, 该退出字符与字符.配合使用可以强制断开客户端与服务器连接(该方式通常用于服务器端重启或发生异常的情况下, 客户端快速中断当前连接)。*character* 为一个字符, 区分大小写, 缺省为~, 即输入~.可以强制断开与服务端的连接。

source: 指定与服务器通信的源 IPv6 地址或者源接口。缺省情况下, 设备根据 RFC 3484 的规则自动选择一个源 IPv6 地址。为保证客户端与服务器之间的通信不会因为所指定的接口发生故障而中断, 通常建议指定 Loopback 接口作为源接口, 或者接口的 IPv6 地址作为源地址。

interface interface-type interface-number: 指定源接口。*interface-type interface-number* 为接口类型和接口编号。系统将使用该接口的 IPv6 地址作为发送报文的源 IPv6 地址。

ipv6 ipv6-address: 指定源 IPv6 地址。

关于退出字符的使用, 需要注意的是:

- 必须在一行中首先输入退出字符和., 该操作才能生效, 若该行中曾经输入过其它字符或执行了其它操作(比如退格), 则需要重新换行输入才能生效。

- 一般情况下，建议使用缺省退出字符，避免退出字符和.的组合与登录用户名相同。

【使用指导】

当客户端采用安全级别为 128-bit 的 Suite B 算法集与远程的 Stelnet 服务器建立连接时，客户端算法要求：

- 密钥交换算法为 **ecdh-sha2-nistp256**;
- 服务器到客户端的加密算法为 **aes128-gcm**;
- 客户端到服务器的加密算法为 **aes128-gcm**;
- 服务器到客户端的 HMAC 算法为 **aes128-gcm**;
- 客户端到服务器的 HMAC 算法为 **aes128-gcm**;
- 主机公钥算法为 **x509v3-ecdsa-sha2-nistp256**、**x509v3-ecdsa-sha2-nistp384**。

当客户端采用安全级别为 192-bit 的 Suite B 算法集与远程的 Stelnet 服务器建立连接时，客户端算法要求：

- 密钥交换算法为 **ecdh-sha2-nistp384**;
- 服务器到客户端的加密算法为 **aes256-gcm**;
- 客户端到服务器的加密算法为 **aes256-gcm**;
- 服务器到客户端的 HMAC 算法为 **aes256-gcm**;
- 客户端到服务器的 HMAC 算法为 **aes256-gcm**;
- 主机公钥算法为 **x509v3-ecdsa-sha2-nistp384**。

当客户端未采用安全级别为 128-bit 和 192-bit 的 Suite B 算法集与远程的 Stelnet 服务器建立连接时，客户端算法要求：

- 密钥交换算法为 **ecdh-sha2-nistp256**、**ecdh-sha2-nistp384**;
- 服务器到客户端的加密算法为 **aes128-gcm**、**aes256-gcm**;
- 客户端到服务器的加密算法为 **aes128-gcm**、**aes256-gcm**;
- 服务器到客户端的 HMAC 算法为 **aes128-gcm**、**aes256-gcm**;
- 客户端到服务器的 HMAC 算法为 **aes128-gcm**、**aes256-gcm**;
- 主机公钥算法为 **x509v3-ecdsa-sha2-nistp256**、**x509v3-ecdsa-sha2-nistp384**。

【举例】

SSH 客户端采用安全级别为 192-bit 的 Suite B 算法集，与登录地址为 2000::1 的远程 Stelnet 服务器建立连接，采用如下连接策略：指定客户端证书的 PKI 域名称为 **clientpkidomain**，指定验证服务端证书的 PKI 域名称为 **serverpkidomain**。

```
<Sysname> ssh2 ipv6 2000::1 suite-b 192-bit pki-domain clientpkidomain server-pki-domain
serverpkidomain
Username:
```

1.2.39 ssh2 suite-b

ssh2 suite-b 命令用来与远程的 IPv4 Stelnet 服务器建立基于 Suite B 算法集的连接。

【命令】

```
ssh2 server [ port-number ] suite-b [ 128-bit | 192-bit ] pki-domain
domain-name [ server-pki-domain domain-name ] [ prefer-compress zlib ] [ dscp
```

```
dscp-value | escape character | source { interface interface-type  
interface-number | ip ip-address } ] *
```

【视图】

用户视图

【缺省用户角色】

network-admin

【参数】

server: 服务器的 IPv4 地址或主机名称, 为 1~253 个字符的字符串, 不区分大小写。

port-number: 服务器端口号, 取值范围为 1~65535, 缺省值为 22。

suite-b: 指定采用 Suite B 算法集。若未指定 128-bit 和 192-bit 参数, 则表示同时采用 128-bit 和 192-bit 的算法集。

128-bit: 指定客户端采用安全级别为 128-bit 的 Suite B 算法集。

192-bit: 指定客户端采用安全级别为 192-bit 的 Suite B 算法集。

pki-domain domain-name: 配置客户端证书的 PKI 域。*domain-name* 为客户端证书的 PKI 域名称, 为 1~31 个字符的字符串, 不区分大小写, 不能包括 “~”、“*”、“\”、“|”、“:”、“.”、“<”、“>”、“” 和 “'”。

server-pki-domain domain-name: 配置验证服务端证书的 PKI 域。*domain-name* 为验证服务端证书的 PKI 域名称, 为 1~31 个字符的字符串, 不区分大小写, 不能包括 “~”、“*”、“\”、“|”、“:”、“.”、“<”、“>”、“” 和 “'”。如果客户端没有指定验证服务端证书所在的 PKI 域, 则缺省使用客户端证书所在的 PKI 域进行验证。

prefer-compress: 服务器与客户端之间的首选压缩算法, 缺省情况下, 不支持压缩。

zlib: 压缩算法 ZLIB。

dscp dscp-value: 指定客户端发送的 SFTP 报文中携带的 DSCP 优先级, 取值范围为 0~63, 缺省值为 48。DSCP 携带在 IP 报文中的 ToS 字段, 用来体现报文自身的优先等级, 决定报文传输的优先程度。

escape character: 指定退出字符, 该退出字符与字符.配合使用可以强制断开客户端与服务器连接(该方式通常用于服务器端重启或发生异常的情况下, 客户端快速中断当前连接)。*character* 为一个字符, 区分大小写, 缺省为~, 即输入~.可以强制断开与服务端的连接。

source: 指定与服务器通信的源 IP 地址或者源接口。缺省情况下, 设备根据路由表项自动选择一个源 IPv4 地址。为保证客户端与服务器之间的通信不会因为所指定的接口发生故障而中断, 通常建议指定 Loopback 接口作为源接口, 或者接口的 IP 地址作为源地址。

interface interface-type interface-number: 指定源接口。*interface-type interface-number* 为接口类型和接口编号。系统将使用该接口的 IPv4 地址作为发送报文的源 IP 地址。

ip ip-address: 指定源 IPv4 地址。

【使用指导】

当客户端采用安全级别为 128-bit 的 Suite B 算法集与远程的 Stelnet 服务器建立连接时, 客户端算法要求:

- 密钥交换算法为 **ecdh-sha2-nistp256**;

- 服务器到客户端的加密算法为 **aes128-gcm**;
- 客户端到服务器的加密算法为 **aes128-gcm**;
- 服务器到客户端的 HMAC 算法为 **aes128-gcm**;
- 客户端到服务器的 HMAC 算法为 **aes128-gcm**;
- 主机公钥算法为 **x509v3-ecdsa-sha2-nistp256**、**x509v3-ecdsa-sha2-nistp384**。

当客户端采用安全级别为 192-bit 的 Suite B 算法集与远程的 Stelnet 服务器建立连接时，客户端算法要求：

- 密钥交换算法为 **ecdh-sha2-nistp384**;
- 服务器到客户端的加密算法为 **aes256-gcm**;
- 客户端到服务器的加密算法为 **aes256-gcm**;
- 服务器到客户端的 HMAC 算法为 **aes256-gcm**;
- 客户端到服务器的 HMAC 算法为 **aes256-gcm**;
- 主机公钥算法为 **x509v3-ecdsa-sha2-nistp384**。

当客户端未采用安全级别为 128-bit 和 192-bit 的 Suite B 算法集与远程的 Stelnet 服务器建立连接时，客户端算法要求：

- 密钥交换算法为 **ecdh-sha2-nistp256**、**ecdh-sha2-nistp384**;
- 服务器到客户端的加密算法为 **aes128-gcm**、**aes256-gcm**;
- 客户端到服务器的加密算法为 **aes128-gcm**、**aes256-gcm**;
- 服务器到客户端的 HMAC 算法为 **aes128-gcm**、**aes256-gcm**;
- 客户端到服务器的 HMAC 算法为 **aes128-gcm**、**aes256-gcm**;
- 主机公钥算法为 **x509v3-ecdsa-sha2-nistp256**、**x509v3-ecdsa-sha2-nistp384**。

关于退出字符的使用，需要注意的是：

- 必须在一行中首先输入退出字符和.，该操作才能生效，若该行中曾经输入过其它字符或执行了其它操作（比如退格），则需要重新换行输入才能生效。
- 一般情况下，建议使用缺省退出字符，避免退出字符和.的组合与登录用户名相同。

【举例】

Stelnet 客户端采用 128-bit 的 Suite B 算法集，与登录地址为 3.3.3.3 的远程 Stelnet 服务器建立连接，采用如下连接策略：指定客户端证书的 PKI 域名称为 **clientpkidomain**，指定验证服务端证书的 PKI 域名称为 **serverpkidomain**。

```
<Sysname> ssh2 3.3.3.3 suite-b 128-bit pki-domain clientpkidomain server-pki-domain
serverpkidomain
Username:
```

1.3 SSH2协议配置命令

1.3.1 display ssh2 algorithm

display ssh2 algorithm 命令用来显示设备上配置的 SSH2 协议使用的算法优先列表。

【命令】

```
display ssh2 algorithm
```

【视图】

任意视图

【缺省用户角色】

network-admin
network-operator

【举例】

显示设备上配置的 SSH2 协议使用的算法优先列表。

```
<Sysname> display ssh2 algorithm
Key exchange algorithms : ecdh-sha2-nistp256 ecdh-sha2-nistp384 dh-group-exchange-sha1
dh-group14-sha1 dh-group1-sha1
Public key algorithms : x509v3-ecdsa-sha2-nistp256 x509v3-ecdsa-sha2-nistp384
ecdsa-sha2-nistp256 ecdsa-sha2-nistp384 rsa dsa
Encryption algorithms : aes128-ctr aes192-ctr aes256-ctr aes128-gcm aes256-gcm aes128-cbc
3des-cbc aes256-cbc des-cbc
MAC algorithms : sha2-256 sha2-512 sha1 md5 sha1-96 md5-96
```

表1-5 display ssh2 algorithm 命令显示信息描述表

字段	描述
Key exchange algorithms	按优先级前后顺序显示当前使用的密钥交换算法列表
Public key algorithms	按优先级前后顺序显示当前使用的主机算法列表
Encryption algorithms	按优先级前后顺序显示当前使用的加密算法列表
MAC algorithms	按优先级前后顺序显示当前使用的HMAC算法列表

【相关命令】

- **ssh2 algorithm key-exchange**
- **ssh2 algorithm public-key**
- **ssh2 algorithm cipher**
- **ssh2 algorithm mac**

1.3.2 ssh2 algorithm cipher

ssh2 algorithm cipher 命令用来配置 SSH2 协议使用的加密算法列表。

undo ssh2 algorithm cipher 命令用来恢复缺省情况。

【命令】

非 FIPS 模式下:

```
ssh2 algorithm cipher { 3des-cbc | aes128-cbc | aes128-ctr | aes128-gcm |
aes192-ctr | aes256-cbc | aes256-ctr | aes256-gcm | des-cbc } *
undo ssh2 algorithm cipher
```

FIPS 模式下:

```
ssh2 algorithm cipher { aes128-cbc | aes128-ctr | aes128-gcm | aes192-ctr |  
aes256-cbc | aes256-ctr | aes256-gcm } *  
undo ssh2 algorithm cipher
```

【缺省情况】

SSH2 协议采用的缺省加密算法从高到底的优先级列表为 **aes128-ctr**、**aes192-ctr**、**aes256-ctr**、**aes128-gcm**、**aes256-gcm**、**aes128-cbc**、**3des-cbc**、**aes256-cbc** 和 **des-cbc**。

【视图】

系统视图

【缺省用户角色】

network-admin

【参数】

3des-cbc: 3DES-CBC 加密算法。
aes128-cbc: 128 位 AES-CBC 加密算法。
aes128-ctr: 128 位 AES-CTR 加密算法。
aes128-gcm: 128 位 AES-GCM 加密算法。
aes192-ctr: 192 位 AES-CTR 加密算法。
aes256-cbc: 256 位 AES-CBC 加密算法。
aes256-ctr: 256 位 AES-CTR 加密算法。
aes256-gcm: 256 位 AES-GCM 加密算法。
des-cbc: DES-CBC 加密算法。

【使用指导】

当设备运行环境要求 SSH2 只能采用特定加密算法的情况下，可采用本命令将设备上的 SSH2 客户端、SSH2 服务器所能使用的加密算法限定在配置的范围。算法的配置顺序即为算法的优先级顺序。

【举例】

```
# 配置 SSH2 协议所使用的加密算法为 aes256-cbc。  
<Sysname> system-view  
[Sysname] ssh2 algorithm cipher aes256-cbc
```

【相关命令】

- **display ssh2 algorithm**
- **ssh2 algorithm key-exchange**
- **ssh2 algorithm mac**
- **ssh2 algorithm public-key**

1.3.3 ssh2 algorithm key-exchange

ssh2 algorithm key-exchange 命令用来配置 SSH2 协议使用的密钥交换算法列表。

undo ssh2 algorithm key-exchange 命令用来恢复缺省情况。

【命令】

非 FIPS 模式下：

```
ssh2 algorithm key-exchange { dh-group-exchange-sha1 | dh-group1-sha1 |  
dh-group14-sha1 | ecdh-sha2-nistp256 | ecdh-sha2-nistp384 } *  
undo ssh2 algorithm key-exchange
```

FIPS 模式下：

```
ssh2 algorithm key-exchange { dh-group14-sha1 | ecdh-sha2-nistp256 |  
ecdh-sha2-nistp384 } *  
undo ssh2 algorithm key-exchange
```

【缺省情况】

SSH2 协议采用的缺省密钥交换算法从高到底的优先级列表为 **ecdh-sha2-nistp256**、**ecdh-sha2-nistp384**、**dh-group-exchange-sha1**、**dh-group14-sha1** 和 **dh-group1-sha1**。

【视图】

系统视图

【缺省用户角色】

network-admin

【参数】

dh-group-exchange-sha1：密钥交换算法 diffie-hellman-group-exchange-sha1。

dh-group1-sha1：密钥交换算法 diffie-hellman-group1-sha1。

dh-group14-sha1：密钥交换算法 diffie-hellman-group14-sha1。

ecdh-sha2-nistp256：密钥交换算法 ecdh-sha2-nistp256。

ecdh-sha2-nistp384：密钥交换算法 ecdh-sha2-nistp384。

【使用指导】

当设备运行环境要求 SSH2 只能采用特定密钥交换算法的情况下，可采用本命令将设备上的 SSH2 客户端、SSH2 服务器所能使用的密钥交换算法限定在配置的范围内。算法的配置顺序即为算法的优先级顺序。

【举例】

配置 SSH2 协议所使用的密钥交换算法为 dh-group1-sha1。

```
<Sysname> system-view
```

```
[Sysname] ssh2 algorithm key-exchange dh-group1-sha1
```

【相关命令】

- **display ssh2 algorithm**
- **ssh2 algorithm cipher**
- **ssh2 algorithm mac**
- **ssh2 algorithm public-key**

1.3.4 ssh2 algorithm mac

ssh2 algorithm mac 命令用来配置 SSH2 协议使用的 HMAC 算法列表。

undo ssh2 algorithm mac 命令用来恢复缺省情况。

【命令】

非 FIPS 模式下：

```
ssh2 algorithm mac { md5 | md5-96 | sha1 | sha1-96 | sha2-256 | sha2-512 } *  
undo ssh2 algorithm mac
```

FIPS 模式下：

```
ssh2 algorithm mac { sha1 | sha1-96 | sha2-256 | sha2-512 } *  
undo ssh2 algorithm mac
```

【缺省情况】

SSH2 协议使用的缺省 HMAC 算法从高到底的优先级列表为 **sha2-256**、**sha2-512**、**sha1**、**md5**、**sha1-96** 和 **md5-96**。

【视图】

系统视图

【缺省用户角色】

network-admin

【参数】

md5：HMAC 算法 HMAC-MD5。

md5-96：HMAC 算法 HMAC-MD5-96。

sha1：HMAC 算法 HMAC-SHA1。

sha1-96：HMAC 算法 HMAC-SHA1-96。

sha2-256：HMAC 算法 HMAC-SHA2-256。

sha2-512：HMAC 算法 HMAC-SHA2-512。

【使用指导】

当设备运行环境要求 SSH2 只能采用特定 HMAC 算法的情况下，可采用本命令将设备上的 SSH2 客户端、SSH2 服务器所能使用的 HMAC 算法限定在配置的范围。算法的配置顺序即为算法的优先级顺序。

【举例】

配置 SSH2 协议所使用的 HMAC 算法为 md5。

```
<Sysname> system-view
```

```
[Sysname] ssh2 algorithm mac md5
```

【相关命令】

- **display ssh2 algorithm**
- **ssh2 algorithm cipher**
- **ssh2 algorithm key-exchange**

- `ssh2 algorithm public-key`

1.3.5 ssh2 algorithm public-key

`ssh2 algorithm public-key` 命令用来配置 SSH2 协议使用的主机签名算法列表。

`undo ssh2 algorithm public-key` 命令用来恢复缺省情况。

【命令】

非 FIPS 模式下：

```
ssh2 algorithm public-key { dsa | ecdsa-sha2-nistp256 | ecdsa-sha2-nistp384  
| rsa | x509v3-ecdsa-sha2-nistp256 | x509v3-ecdsa-sha2-nistp384 } *  
undo ssh2 algorithm public-key
```

FIPS 模式下：

```
ssh2 algorithm public-key { ecdsa-sha2-nistp256 | ecdsa-sha2-nistp384 | rsa  
| x509v3-ecdsa-sha2-nistp256 | x509v3-ecdsa-sha2-nistp384 } *  
undo ssh2 algorithm public-key
```

【缺省情况】

SSH2 协议使用的缺省主机签名算法从高到底的优先级列表为 `x509v3-ecdsa-sha2-nistp256`、`x509v3-ecdsa-sha2-nistp384`、`ecdsa-sha2-nistp256`、`ecdsa-sha2-nistp384`、`rsa` 和 `dsa`。

【视图】

系统视图

【缺省用户角色】

network-admin

【参数】

dsa：公钥算法为 DSA。

ecdsa-sha2-nistp256：指定公钥长度为 256 的 ECDSA 算法。

ecdsa-sha2-nistp384：指定公钥长度为 384 的 ECDSA 算法。

rsa：公钥算法为 RSA。

x509v3-ecdsa-sha2-nistp256：x509v3-ecdsa-sha2-nistp256 公钥算法。

x509v3-ecdsa-sha2-nistp384：x509v3-ecdsa-sha2-nistp384 公钥算法。

【使用指导】

当设备运行环境要求 SSH2 只能采用特定主机签名算法的情况下，可采用本命令将设备上的 SSH2 客户端、SSH2 服务器所能使用的主机签名算法限定在配置的范围内。算法的配置顺序即为算法的优先级顺序。

【举例】

配置 SSH2 协议所使用的主机签名算法为 **dsa**。

```
<Sysname> system-view
```

```
[Sysname] ssh2 algorithm public-key dsa
```


【相关命令】

- `display ssh2 algorithm`
- `ssh2 algorithm cipher`
- `ssh2 algorithm key-exchange`
- `ssh2 algorithm mac`

目 录

1 SSL	1-1
1.1 SSL配置命令	1-1
1.1.1 ciphersuite	1-1
1.1.2 client-verify.....	1-3
1.1.3 display ssl client-policy.....	1-5
1.1.4 display ssl server-policy	1-6
1.1.5 pki-domain (SSL client policy view).....	1-7
1.1.6 pki-domain (SSL server policy view)	1-7
1.1.7 prefer-cipher.....	1-8
1.1.8 server-verify enable.....	1-11
1.1.9 session.....	1-11
1.1.10 ssl client-policy	1-12
1.1.11 ssl renegotiation disable	1-13
1.1.12 ssl server-policy	1-14
1.1.13 ssl version disable.....	1-14
1.1.14 version	1-15

1 SSL



说明

设备运行于 FIPS 模式时，本特性部分配置相对于非 FIPS 模式有所变化，具体差异请见本文相关描述。有关 FIPS 模式的详细介绍请参见“安全配置指导”中的“FIPS”。

1.1 SSL配置命令

1.1.1 ciphersuite

ciphersuite 命令用来配置 SSL 服务器端策略支持的加密套件。

undo ciphersuite 命令用来恢复缺省情况。

【命令】

非 FIPS 模式下：

```
ciphersuite {  dhe_rsa_aes_128_cbc_sha |  dhe_rsa_aes_128_cbc_sha256 |
dhe_rsa_aes_256_cbc_sha          |          dhe_rsa_aes_256_cbc_sha256          |
ecdhe_ecdsa_aes_128_cbc_sha256   |   ecdhe_ecdsa_aes_128_gcm_sha256   |
ecdhe_ecdsa_aes_256_cbc_sha384   |   ecdhe_ecdsa_aes_256_gcm_sha384   |
ecdhe_rsa_aes_128_cbc_sha256     |   ecdhe_rsa_aes_128_gcm_sha256     |
ecdhe_rsa_aes_256_cbc_sha384     |   ecdhe_rsa_aes_256_gcm_sha384     |
exp_rsa_des_cbc_sha             |   exp_rsa_rc2_md5             |   exp_rsa_rc4_md5             |
rsa_3des_edc_cbc_sha            |  rsa_aes_128_cbc_sha            |  rsa_aes_128_cbc_sha256            |
rsa_aes_256_cbc_sha             |  rsa_aes_256_cbc_sha256             |  rsa_des_cbc_sha             |
rsa_rc4_128_md5 | rsa_rc4_128_sha } *
undo ciphersuite
```

FIPS 模式下：

```
ciphersuite {          ecdhe_ecdsa_aes_128_cbc_sha256          |
ecdhe_ecdsa_aes_256_cbc_sha384   |   ecdhe_ecdsa_aes_128_gcm_sha256   |
ecdhe_ecdsa_aes_256_gcm_sha384   |   ecdhe_rsa_aes_128_cbc_sha256   |
ecdhe_rsa_aes_128_gcm_sha256     |   ecdhe_rsa_aes_256_cbc_sha384     |
ecdhe_rsa_aes_256_gcm_sha384     |          rsa_aes_128_cbc_sha          |
rsa_aes_128_cbc_sha256 | rsa_aes_256_cbc_sha | rsa_aes_256_cbc_sha256 } *
undo ciphersuite
```

【缺省情况】

SSL 服务器端策略支持所有的加密套件。

【视图】

SSL 服务器端策略视图

【缺省用户角色】

network-admin

【参数】

dhe_rsa_aes_128_cbc_sha: 密钥交换算法采用 DHE RSA、数据加密算法采用 128 位的 AES、MAC 算法采用 SHA。

dhe_rsa_aes_128_cbc_sha256: 密钥交换算法采用 DHE RSA、数据加密算法采用 128 位的 AES_CBC、MAC 算法采用 SHA256。

dhe_rsa_aes_256_cbc_sha: 密钥交换算法采用 DHE RSA、数据加密算法采用 256 位的 AES、MAC 算法采用 SHA。

dhe_rsa_aes_256_cbc_sha256: 密钥交换算法采用 DHE RSA、数据加密算法采用 256 位的 AES_CBC、MAC 算法采用 SHA256。

ecdhe_ecdsa_aes_128_cbc_sha256: 密钥交换算法采用 ECDHE ECDSA、数据加密算法采用 128 位的 AES_CBC、MAC 算法采用 SHA256。

ecdhe_ecdsa_aes_128_gcm_sha256: 密钥交换算法采用 ECDHE ECDSA、数据加密算法采用 128 位的 AES_GCM、MAC 算法采用 SHA256。

ecdhe_ecdsa_aes_256_cbc_sha384: 密钥交换算法采用 ECDHE ECDSA、数据加密算法采用 256 位的 AES_CBC、MAC 算法采用 SHA384。

ecdhe_ecdsa_aes_256_gcm_sha384: 密钥交换算法采用 ECDHE ECDSA、数据加密算法采用 256 位的 AES_GCM、MAC 算法采用 SHA384。

ecdhe_rsa_aes_128_cbc_sha256: 密钥交换算法采用 ECDHE RSA、数据加密算法采用 128 位的 AES_CBC、MAC 算法采用 SHA256。

ecdhe_rsa_aes_128_gcm_sha256: 密钥交换算法采用 ECDHE RSA、数据加密算法采用 128 位的 AES_GCM、MAC 算法采用 SHA256。

ecdhe_rsa_aes_256_cbc_sha384: 密钥交换算法采用 ECDHE RSA、数据加密算法采用 256 位的 AES_CBC、MAC 算法采用 SHA384。

ecdhe_rsa_aes_256_gcm_sha384: 密钥交换算法采用 ECDHE RSA、数据加密算法采用 256 位的 AES_GCM、MAC 算法采用 SHA384。

exp_rsa_des_cbc_sha: 满足出口限制的算法套件。密钥交换算法采用 RSA、数据加密算法采用 DES_CBC、MAC 算法采用 SHA。

exp_rsa_rc2_md5: 满足出口限制的算法套件。密钥交换算法采用 RSA、数据加密算法采用 RC2、MAC 算法采用 MD5。

exp_rsa_rc4_md5: 满足出口限制的算法套件。密钥交换算法采用 RSA、数据加密算法采用 RC4、MAC 算法采用 MD5。

rsa_3des_ede_cbc_sha: 密钥交换算法采用 RSA、数据加密算法采用 3DES_EDE_CBC、MAC 算法采用 SHA。

rsa_aes_128_cbc_sha: 密钥交换算法采用 RSA、数据加密算法采用 128 位 AES_CBC、MAC 算法采用 SHA。

rsa_aes_128_cbc_sha256: 密钥交换算法采用 RSA、数据加密算法采用 128 位的 AES_CBC、MAC 算法采用 SHA256。

rsa_aes_256_cbc_sha: 密钥交换算法采用 RSA、数据加密算法采用 256 位 AES_CBC、MAC 算法采用 SHA。

rsa_aes_256_cbc_sha256: 密钥交换算法采用 RSA、数据加密算法采用 256 位的 AES_CBC、MAC 算法采用 SHA256。

rsa_des_cbc_sha: 密钥交换算法采用 RSA、数据加密算法采用 DES_CBC、MAC 算法采用 SHA。

rsa_rc4_128_md5: 密钥交换算法采用 RSA、数据加密算法采用 128 位的 RC4、MAC 算法采用 MD5。

rsa_rc4_128_sha: 密钥交换算法采用 RSA、数据加密算法采用 128 位的 RC4、MAC 算法采用 SHA。

【使用指导】

为了提高安全性，SSL 协议采用了如下算法：

- **数据加密算法：**用来对传输的数据进行加密，以保证数据传输的私密性。常用的数据加密算法通常为对称密钥算法，如 DES_CBC、3DES_EDE_CBC、AES_CBC、RC4 等。使用对称密钥算法时，要求 SSL 服务器端和 SSL 客户端具有相同的密钥。
- **MAC（Message Authentication Code，消息验证码）算法：**用来计算数据的 MAC 值，以防止发送的数据被篡改。常用的 MAC 算法有 MD5、SHA 等。使用 MAC 算法时，要求 SSL 服务器端和 SSL 客户端具有相同的密钥。
- **密钥交换算法：**用来实现密钥交换，以保证对称密钥算法、MAC 算法中使用的密钥在 SSL 服务器端和 SSL 客户端之间安全地传递。常用的密钥交换算法通常为非对称密钥算法，如 RSA。

通过本命令可以配置 SSL 服务器端策略支持的各种算法组合。例如，**rsa_des_cbc_sha** 表示 SSL 服务器端策略支持的密钥交换算法为 RSA、数据加密算法为 DES_CBC、MAC 算法为 SHA。

SSL 服务器接收到 SSL 客户端发送的客户端加密套件后，将服务器支持的加密套件与 SSL 客户端支持的加密套件比较。如果 SSL 服务器支持的加密套件中存在 SSL 客户端支持的加密套件，则加密套件协商成功；否则，加密套件协商失败。

多次执行本命令，最后一次执行的命令生效。

【举例】

指定 SSL 服务器端策略支持如下加密套件：

- 密钥交换算法为 DHE RSA、数据加密算法为 128 位的 AES、MAC 算法为 SHA
- 密钥交换算法为 RSA、数据加密算法为 128 位的 AES、MAC 算法为 SHA

```
<Sysname> system-view
[Sysname] ssl server-policy policy1
[Sysname-ssl-server-policy-policy1] ciphersuite dhe_rsa_aes_128_cbc_sha
rsa_aes_128_cbc_sha
```

【相关命令】

- **display ssl server-policy**
- **prefer-cipher**

1.1.2 client-verify

client-verify 命令用来配置 SSL 服务器端对 SSL 客户端的身份验证方案。

undo client-verify 命令用来恢复缺省情况。

【命令】

```
client-verify { enable | optional }  
undo client-verify [ enable ]
```

【缺省情况】

SSL 服务器端不对 SSL 客户端进行基于数字证书的身份验证。

【视图】

SSL 服务器端策略视图

【缺省用户角色】

network-admin

【参数】

enable: 表示 SSL 服务器端要求对 SSL 客户端进行基于数字证书的身份验证。

optional: 表示 SSL 服务器端不强制要求对 SSL 客户端进行基于数字证书的身份验证，即身份验证可选。

【使用指导】

SSL 通过数字证书实现对对端的身份进行验证。数字证书的详细介绍，请参见“安全配置指导”中的“PKI”。

设备作为 SSL 服务器端，支持灵活的 SSL 客户端认证方案，具体如下：

- 执行了 **client-verify enable** 命令的情况下，则 SSL 客户端必须将自己的数字证书提供给服务器，以便服务器对客户端进行基于数字证书的身份验证。只有身份验证通过后，SSL 客户端才能访问 SSL 服务器。
- 执行了 **client-verify optional** 命令的情况下，若 SSL 客户端未提供数字证书给服务器，SSL 客户端也能访问 SSL 服务器；若 SSL 客户端提供数字证书给服务器，只有身份验证通过后，SSL 客户端才能访问 SSL 服务器。
- 执行了 **undo client-verify [enable]** 命令的情况下，SSL 服务器端不要求 SSL 客户端提供数字证书，也不会对其进行基于数字证书的身份验证，SSL 客户端可以直接访问 SSL 服务器。

SSL 服务器端在基于数字证书对 SSL 客户端进行身份验证时，除了对 SSL 客户端发送的证书链进行验证，还要检查证书链中的除根 CA 证书外的每个证书是否均未被吊销。

【举例】

配置 SSL 服务器端要求对 SSL 客户端进行基于数字证书的身份验证。

```
<Sysname> system-view  
[Sysname] ssl server-policy policy1  
[Sysname-ssl-server-policy-policy1] client-verify enable
```

配置 SSL 服务器端对 SSL 客户端进行基于数字证书的身份验证是可选的。

```
<Sysname> system-view  
[Sysname] ssl server-policy policy1  
[Sysname-ssl-server-policy-policy1] client-verify optional
```

配置 SSL 服务器端不要求对 SSL 客户端进行基于数字证书的身份验证。

```
<Sysname> system-view
```

```
[Sysname] ssl server-policy policy1
[Sysname-ssl-server-policy-policy1] undo client-verify
```

【相关命令】

- **display ssl server-policy**

1.1.3 display ssl client-policy

display ssl client-policy 命令用来显示 SSL 客户端策略的信息。

【命令】

```
display ssl client-policy [ policy-name ]
```

【视图】

任意视图

【缺省用户角色】

network-admin
network-operator

【参数】

policy-name: 显示指定的 SSL 客户端策略的信息，为 1~31 个字符的字符串，不区分大小写。
如果不指定本参数，则显示所有 SSL 客户端策略的信息。

【举例】

显示名为 policy1 的 SSL 客户端策略的信息。

```
<Sysname> display ssl client-policy policy1
SSL client policy: policy1
  SSL version: SSL 3.0
  PKI domain: client-domain
  Preferred ciphersuite:
    RSA_AES_128_CBC_SHA
  Server-verify: enabled
```

表1-1 display ssl client-policy 命令显示信息描述表

字段	描述
SSL client policy	SSL客户端策略名
SSL version	SSL客户端策略使用的SSL协议版本
PKI domain	SSL客户端策略使用的PKI域
Preferred ciphersuite	SSL客户端策略支持的加密套件
Server-verify	SSL客户端策略的服务器端验证模式，取值包括： <ul style="list-style-type: none">• disabled: 不要求对 SSL 服务器进行基于数字证书的身份验证• enabled: 要求对 SSL 服务器进行基于数字证书的身份验证

1.1.4 display ssl server-policy

display ssl server-policy 命令用来显示 SSL 服务器端策略的信息。

【命令】

display ssl server-policy [*policy-name*]

【视图】

任意视图

【缺省用户角色】

network-admin
network-operator

【参数】

policy-name: 显示指定的 SSL 服务器端策略的信息, 为 1~31 个字符的字符串, 不区分大小写。
如果不指定本参数, 则显示所有 SSL 服务器端策略的信息。

【举例】

显示名为 policy1 的 SSL 服务器端策略的信息。

```
<Sysname> display ssl server-policy policy1
SSL server policy: policy1
  PKI domain: server-domain
  Ciphersuites:
    DHE_RSA_AES_128_CBC_SHA
    RSA_AES_128_CBC_SHA
  Session cache size: 600
  Caching timeout: 3600 seconds
  Client-verify: Enabled
```

表1-2 display ssl server-policy 命令显示信息描述表

字段	描述
SSL server policy	SSL服务器端策略名
PKI domain	SSL服务器端策略使用的PKI域
Ciphersuites	SSL服务器端策略支持的加密套件
Session cache size	SSL服务器端可以缓存的最大会话数目
Caching timeout	SSL服务器端会话缓存超时时间（单位为秒）
Client-verify	SSL服务器端策略的客户端验证模式，取值包括： <ul style="list-style-type: none">Disabled: 不要求对客户端进行基于数字证书的身份验证Enabled: 要求对客户端进行基于数字证书的身份验证Optional: SSL 服务器端对 SSL 客户端进行基于数字证书的身份验证是可选的

1.1.5 pki-domain (SSL client policy view)

pki-domain 命令用来配置 SSL 客户端策略所使用的 PKI 域。

undo pki-domain 命令用来恢复缺省情况。

【命令】

pki-domain *domain-name*

undo pki-domain

【缺省情况】

未指定 SSL 客户端策略所使用的 PKI 域。

【视图】

SSL 客户端策略视图

【缺省用户角色】

network-admin

【参数】

domain-name: PKI 域的域名，为 1~31 个字符的字符串，不区分大小写。

【使用指导】

如果通过本命令指定了 SSL 客户端策略使用的 PKI 域，则引用该客户端策略的 SSL 客户端将通过该 PKI 域获取客户端的数字证书。

【举例】

配置 SSL 客户端策略所使用的 PKI 域为 client-domain。

```
<Sysname> system-view
```

```
[Sysname] ssl client-policy policy1
```

```
[Sysname-ssl-client-policy-policy1] pki-domain client-domain
```

【相关命令】

- **display ssl client-policy**
- **pki domain**（安全命令参考/PKI）

1.1.6 pki-domain (SSL server policy view)

pki-domain 命令用来配置 SSL 服务器端策略所使用的 PKI 域。

undo pki-domain 命令用来恢复缺省情况。

【命令】

pki-domain *domain-name*

undo pki-domain

【缺省情况】

未指定 SSL 服务器端策略所使用的 PKI 域。

【视图】

SSL 服务器端策略视图

【缺省用户角色】

network-admin

【参数】

domain-name: PKI 域的域名，为 1~31 个字符的字符串，不区分大小写。

【使用指导】

如果通过本命令指定了 SSL 服务器端策略使用的 PKI 域，则引用该服务器端策略的 SSL 服务器将通过该 PKI 域获取服务器端的数字证书。

【举例】

配置 SSL 服务器端策略所使用的 PKI 域为 server-domain。

```
<Sysname> system-view
[Sysname] ssl server-policy policy1
[Sysname-ssl-server-policy-policy1] pki-domain server-domain
```

【相关命令】

- **display ssl server-policy**
- **pki domain**（安全命令参考/PKI）

1.1.7 prefer-cipher

prefer-cipher 命令用来配置 SSL 客户端策略支持的加密套件。

undo prefer-cipher 命令用来恢复缺省情况。

【命令】

非 FIPS 模式下：

```
prefer-cipher { dhe_rsa_aes_128_cbc_sha | dhe_rsa_aes_128_cbc_sha256 |
dhe_rsa_aes_256_cbc_sha | dhe_rsa_aes_256_cbc_sha256 |
ecdhe_ecdsa_aes_128_cbc_sha256 | ecdhe_ecdsa_aes_128_gcm_sha256 |
ecdhe_ecdsa_aes_256_cbc_sha384 | ecdhe_ecdsa_aes_256_gcm_sha384 |
ecdhe_rsa_aes_128_cbc_sha256 | ecdhe_rsa_aes_128_gcm_sha256 |
ecdhe_rsa_aes_256_cbc_sha384 | ecdhe_rsa_aes_256_gcm_sha384 |
exp_rsa_des_cbc_sha | exp_rsa_rc2_md5 | exp_rsa_rc4_md5 |
rsa_3des_edc_cbc_sha | rsa_aes_128_cbc_sha | rsa_aes_128_cbc_sha256 |
rsa_aes_256_cbc_sha | rsa_aes_256_cbc_sha256 | rsa_des_cbc_sha |
rsa_rc4_128_md5 | rsa_rc4_128_sha }
undo prefer-cipher
```

FIPS 模式下：

```
prefer-cipher { ecdhe_ecdsa_aes_128_cbc_sha256 |
ecdhe_ecdsa_aes_128_gcm_sha256 | ecdhe_ecdsa_aes_256_cbc_sha384 |
ecdhe_ecdsa_aes_256_gcm_sha384 | ecdhe_rsa_aes_128_cbc_sha256 |
ecdhe_rsa_aes_128_gcm_sha256 | ecdhe_rsa_aes_256_cbc_sha384 |
ecdhe_rsa_aes_256_gcm_sha384 | rsa_aes_128_cbc_sha |
rsa_aes_128_cbc_sha256 | rsa_aes_256_cbc_sha | rsa_aes_256_cbc_sha256 }
```

`undo prefer-cipher`

【缺省情况】

非 FIPS 模式下：

SSL 客户端策略支持的加密套件为 `rsa_rc4_128_md5`。

FIPS 模式下：

SSL 客户端策略支持的加密套件为 `rsa_aes_128_cbc_sha`。

【视图】

SSL 客户端策略视图

【缺省用户角色】

`network-admin`

【参数】

dhe_rsa_aes_128_cbc_sha: 密钥交换算法采用 DHE RSA、数据加密算法采用 128 位的 AES、MAC 算法采用 SHA。

dhe_rsa_aes_128_cbc_sha256: 密钥交换算法采用 DHE RSA、数据加密算法采用 128 位的 AES_CBC、MAC 算法采用 SHA256。

dhe_rsa_aes_256_cbc_sha: 密钥交换算法采用 DHE RSA、数据加密算法采用 256 位的 AES、MAC 算法采用 SHA。

dhe_rsa_aes_256_cbc_sha256: 密钥交换算法采用 DHE RSA、数据加密算法采用 256 位的 AES_CBC、MAC 算法采用 SHA256。

ecdhe_ecdsa_aes_128_cbc_sha256: 密钥交换算法采用 ECDHE ECDSA、数据加密算法采用 128 位的 AES_CBC、MAC 算法采用 SHA256。

ecdhe_ecdsa_aes_128_gcm_sha256: 密钥交换算法采用 ECDHE ECDSA、数据加密算法采用 128 位的 AES_GCM、MAC 算法采用 SHA256。

ecdhe_ecdsa_aes_256_cbc_sha384: 密钥交换算法采用 ECDHE ECDSA、数据加密算法采用 256 位的 AES_CBC、MAC 算法采用 SHA384。

ecdhe_ecdsa_aes_256_gcm_sha384: 密钥交换算法采用 ECDHE ECDSA、数据加密算法采用 256 位的 AES_GCM、MAC 算法采用 SHA384。

ecdhe_rsa_aes_128_cbc_sha256: 密钥交换算法采用 ECDHE RSA、数据加密算法采用 128 位的 AES_CBC、MAC 算法采用 SHA256。

ecdhe_rsa_aes_128_gcm_sha256: 密钥交换算法采用 ECDHE RSA、数据加密算法采用 128 位的 AES_GCM、MAC 算法采用 SHA256。

ecdhe_rsa_aes_256_cbc_sha384: 密钥交换算法采用 ECDHE RSA、数据加密算法采用 256 位的 AES_CBC、MAC 算法采用 SHA384。

ecdhe_rsa_aes_256_gcm_sha384: 密钥交换算法采用 ECDHE RSA、数据加密算法采用 256 位的 AES_GCM、MAC 算法采用 SHA384。

exp_rsa_des_cbc_sha: 满足出口限制的算法套件。密钥交换算法采用 RSA、数据加密算法采用 DES_CBC、MAC 算法采用 SHA。

exp_rsa_rc2_md5: 满足出口限制的算法套件。密钥交换算法采用 RSA、数据加密算法采用 RC2、MAC 算法采用 MD5。

exp_rsa_rc4_md5: 满足出口限制的算法套件。密钥交换算法采用 RSA、数据加密算法采用 RC4、MAC 算法采用 MD5。

rsa_3des_ede_cbc_sha: 密钥交换算法采用 RSA、数据加密算法采用 3DES_EDE_CBC、MAC 算法采用 SHA。

rsa_aes_128_cbc_sha: 密钥交换算法采用 RSA、数据加密算法采用 128 位 AES_CBC、MAC 算法采用 SHA。

rsa_aes_128_cbc_sha256: 密钥交换算法采用 RSA、数据加密算法采用 128 位的 AES_CBC、MAC 算法采用 SHA256。

rsa_aes_256_cbc_sha: 密钥交换算法采用 RSA、数据加密算法采用 256 位 AES_CBC、MAC 算法采用 SHA。

rsa_aes_256_cbc_sha256: 密钥交换算法采用 RSA、数据加密算法采用 256 位的 AES_CBC、MAC 算法采用 SHA256。

rsa_des_cbc_sha: 密钥交换算法采用 RSA、数据加密算法采用 DES_CBC、MAC 算法采用 SHA。

rsa_rc4_128_md5: 密钥交换算法采用 RSA、数据加密算法采用 128 位的 RC4、MAC 算法采用 MD5。

rsa_rc4_128_sha: 密钥交换算法采用 RSA、数据加密算法采用 128 位的 RC4、MAC 算法采用 SHA。

【使用指导】

为了提高安全性，SSL 协议采用了如下算法：

- 数据加密算法：用来对传输的数据进行加密，以保证数据传输的私密性。常用的数据加密算法通常为对称密钥算法。使用对称密钥算法时，要求 SSL 服务器端和 SSL 客户端具有相同的密钥。
- MAC（Message Authentication Code，消息验证码）算法：用来计算数据的 MAC 值，以防止发送的数据被篡改。常用的 MAC 算法有 MD5、SHA 等。使用 MAC 算法时，要求 SSL 服务器端和 SSL 客户端具有相同的密钥。
- 密钥交换算法：用来实现密钥交换，以保证对称密钥算法、MAC 算法中使用的密钥在 SSL 服务器端和 SSL 客户端之间安全地传递。常用的密钥交换算法通常为非对称密钥算法，如 RSA。

通过本命令可以配置 SSL 客户端策略支持的算法组合。例如，**rsa_des_cbc_sha** 表示 SSL 客户端支持的密钥交换算法为 RSA、数据加密算法为 DES_CBC、MAC 算法为 SHA。

SSL 客户端将本端支持的加密套件发送给 SSL 服务器，SSL 服务器将自己支持的加密套件与 SSL 客户端支持的加密套件比较。如果 SSL 服务器支持的加密套件中存在 SSL 客户端支持的加密套件，则加密套件协商成功；否则，加密套件协商失败。

多次执行本命令，最后一次执行的命令生效。

【举例】

配置 SSL 客户端策略支持的加密套件为：密钥交换算法采用 RSA、数据加密算法采用 128 位 AES_CBC、MAC 算法采用 SHA。

```
<Sysname> system-view
[Sysname] ssl client-policy policy1
[Sysname-ssl-client-policy-policy1] prefer-cipher rsa_aes_128_cbc_sha
```

【相关命令】

- `ciphersuite`
- `display ssl client-policy`

1.1.8 server-verify enable

server-verify enable 命令用来配置对服务器端进行基于数字证书的身份验证。

undo server-verify enable 命令用来取消对服务器端进行基于数字证书的身份验证，默认 SSL 服务器身份合法。

【命令】

```
server-verify enable
undo server-verify enable
```

【缺省情况】

SSL 客户端需要对 SSL 服务器端进行基于数字证书的身份验证。

【视图】

SSL 客户端策略视图

【缺省用户角色】

network-admin

【使用指导】

SSL 通过数字证书实现对对端的身份进行验证。数字证书的详细介绍，请参见“安全配置指导”中的“PKI”。

如果执行了 **server-verify enable** 命令，则 SSL 服务器端需要将自己的数字证书提供给客户端，以便客户端对服务器端进行基于数字证书的身份验证。只有身份验证通过后，SSL 客户端才会访问该 SSL 服务器。

【举例】

配置 SSL 客户端需要对 SSL 服务器端进行基于数字证书的身份验证。

```
<Sysname> system-view
[Sysname] ssl client-policy policy1
[Sysname-ssl-client-policy-policy1] server-verify enable
```

【相关命令】

- `display ssl client-policy`

1.1.9 session

session 命令用来配置 SSL 服务器上缓存的最大会话数目和 SSL 会话缓存的超时时间。

undo session 命令用来恢复缺省情况。

【命令】

```
session { cachesize size | timeout time } *
undo session { cachesize | timeout } *
```

【缺省情况】

SSL 服务器上缓存的最大会话数目为 500 个，SSL 会话缓存的超时时间为 3600 秒。

【视图】

SSL 服务器端策略视图

【缺省用户角色】

network-admin

【参数】

cache size *size*: 指定 SSL 服务器上缓存的最大会话数目。*size* 为缓存的最大会话数目，取值范围为 100~20480。

timeout *time*: 指定 SSL 会话缓存的超时时间。*time* 为会话缓存超时时间，取值范围为 1~4294967295，单位为秒。

【使用指导】

通过 SSL 握手协议协商会话参数并建立会话的过程比较复杂。为了简化 SSL 握手过程，SSL 允许重用已经协商出的会话参数建立会话。为此，SSL 服务器上需要保存已有的会话信息。保存的会话信息的数目和保存时间具有一定的限制：

- 如果缓存的会话数目达到最大值，SSL 将拒绝缓存新协商出的会话。
- 会话保存的时间超过设定的时间后，SSL 将删除该会话的信息。

【举例】

配置 SSL 服务器上缓存的最大会话数目为 600 个，SSL 会话缓存超时时间为 1800 秒。

```
<Sysname> system-view
[Sysname] ssl server-policy policy1
[Sysname-ssl-server-policy-policy1] session cache size 600 timeout 1800
```

【相关命令】

- **display ssl server-policy**

1.1.10 ssl client-policy

ssl client-policy 命令用来创建 SSL 客户端策略，并进入 SSL 客户端策略视图。如果指定的 SSL 客户端策略已经存在，则直接进入 SSL 客户端策略视图。

undo ssl client-policy 命令用来删除指定的 SSL 客户端策略。

【命令】

```
ssl client-policy policy-name
undo ssl client-policy policy-name
```

【缺省情况】

不存在 SSL 客户端策略。

【视图】

系统视图

【缺省用户角色】

network-admin

【参数】

policy-name: SSL 客户端策略名，为 1~31 个字符的字符串，不区分大小写。

【使用指导】

SSL 客户端策略视图下可以配置 SSL 客户端启动时使用的 SSL 参数，如使用的 PKI 域、支持的加密套件等。只有与应用层协议，如 DDNS（Dynamic Domain Name System，动态域名系统），关联后，SSL 客户端策略才能生效。

【举例】

创建 SSL 客户端策略 policy1，并进入 SSL 客户端策略视图。

```
<Sysname> system-view
[Sysname] ssl client-policy policy1
[Sysname-ssl-client-policy-policy1]
```

【相关命令】

- **display ssl client-policy**

1.1.11 ssl renegotiation disable

ssl renegotiation disable 命令用来关闭 SSL 重协商。

undo ssl renegotiation disable 命令用来恢复缺省情况。

【命令】

```
ssl renegotiation disable
undo ssl renegotiation disable
```

【缺省情况】

允许 SSL 重协商。

【视图】

系统视图

【缺省用户角色】

network-admin

【使用指导】

关闭 SSL 重协商是指，不允许复用已有的 SSL 会话进行 SSL 快速协商，每次 SSL 协商必须进行完整的 SSL 握手过程。关闭 SSL 重协商会导致系统付出更多的计算开销，但可以避免潜在的风险，安全性更高。

通常情况下，不建议关闭 SSL 重协商。本命令仅用于用户明确要求关闭重协商的场景。

【举例】

关闭 SSL 重协商。

```
<Sysname> system-view
[Sysname] ssl renegotiation disable
```

1.1.12 ssl server-policy

ssl server-policy 命令用来创建 SSL 服务器端策略，并进入 SSL 服务器端策略视图。如果指定的 SSL 服务器端策略已经存在，则直接进入 SSL 服务器端策略视图。

undo ssl server-policy 命令用来删除指定的 SSL 服务器端策略。

【命令】

```
ssl server-policy policy-name  
undo ssl server-policy policy-name
```

【缺省情况】

不存在 SSL 服务器端策略。

【视图】

系统视图

【缺省用户角色】

network-admin

【参数】

policy-name: SSL 服务器端策略名，为 1~31 个字符的字符串，不区分大小写。

【使用指导】

SSL 服务器端策略视图下可以配置 SSL 服务器启动时使用的 SSL 参数，如使用的 PKI 域、支持的加密套件等。只有与 HTTPS 等应用关联后，SSL 服务器端策略才能生效。

【举例】

创建 SSL 服务器端策略 policy1，并进入 SSL 服务器端策略视图。

```
<Sysname> system-view  
[Sysname] ssl server-policy policy1  
[Sysname-ssl-server-policy-policy1]
```

【相关命令】

- **display ssl server-policy**

1.1.13 ssl version disable

ssl version disable 命令用来禁止 SSL 服务器使用指定的 SSL 版本进行 SSL 协商。

undo ssl version disable 命令用来恢复缺省情况。

【命令】

非 FIPS 模式下：

```
ssl version { ssl3.0 | tls1.0 | tls1.1 } * disable  
undo ssl version { ssl3.0 | tls1.0 | tls1.1 } * disable
```

FIPS 模式下：

```
ssl version { tls1.0 | tls1.1 } * disable  
undo ssl version { tls1.0 | tls1.1 } * disable
```


【缺省情况】

非 FIPS 模式下：

SSL 服务器允许使用 SSL3.0、TLS1.0、TLS1.1 和 TLS1.2 版本进行协商。

FIPS 模式下：

SSL 服务器允许使用 TLS1.0、TLS1.1 和 TLS1.2 版本进行协商。

【视图】

系统视图

【缺省用户角色】

network-admin

【参数】

ssl3.0：SSL 协商的版本为 SSL3.0。

tls1.0：SSL 协商的版本为 TLS1.0。

tls1.1：SSL 协商的版本为 TLS1.1。

【使用指导】

当对系统安全性有较高要求时可以禁止 SSL 服务器使用 SSL3.0、TLS1.0 和 TLS1.1 版本进行协商。

需要注意的是，如果通过本命令关闭了指定版本的 SSL 协商功能，并不会同时关闭比其更低版本的 SSL 协商功能，例如，**ssl version tls1.1 disable** 命令仅表示关闭了 TLS1.1 版本的 SSL 协商功能，不会同时关闭 TLS1.0 版本。

【举例】

关闭 SSL 3.0。

```
<Sysname> system-view
[Sysname] ssl version ssl3.0 disable
```

1.1.14 version

version 命令用来配置 SSL 客户端策略使用的 SSL 协议版本。

undo version 命令恢复缺省情况。

【命令】

非 FIPS 模式下：

```
version { ssl3.0 | tls1.0 | tls1.1 | tls1.2 }
undo version
```

FIPS 模式下：

```
version { tls1.0 | tls1.1 | tls1.2 }
undo version
```

【缺省情况】

SSL 客户端策略使用的 SSL 协议版本为 TLS 1.0。

【视图】

SSL 客户端策略视图

【缺省用户角色】

network-admin

【参数】

ssl3.0: SSL 客户端策略使用的 SSL 协议版本为 SSL 3.0。

tls1.0: SSL 客户端策略使用的 SSL 协议版本为 TLS 1.0。

tls1.1: SSL 客户端策略使用的 SSL 协议版本为 TLS1.1。

tls1.2: SSL 客户端策略使用的 SSL 协议版本为 TLS1.2。

【使用指导】

对安全性要求较高的环境下，建议为不要为 SSL 客户端指定 SSL3.0 版本。

多次执行本命令，最后一次执行的命令生效。

【举例】

配置 SSL 客户端策略使用的 SSL 协议版本为 TLS 1.0。

```
<Sysname> system-view
```

```
[Sysname] ssl client-policy policy1
```

```
[Sysname-ssl-client-policy-policy1] version tls1.0
```

【相关命令】

- **display ssl client-policy**

目 录

1 攻击检测与防范.....	1-1
1.1 攻击检测与防范配置命令.....	1-1
1.1.1 attack-defense login reauthentication-delay.....	1-1
1.1.2 attack-defense tcp fragment enable	1-1

1 攻击检测与防范

1.1 攻击检测与防范配置命令

1.1.1 attack-defense login reauthentication-delay

attack-defense login reauthentication-delay 命令用来配置 Login 用户登录失败后重新进行认证的等待时长。

undo attack-defense login reauthentication-delay 命令用来恢复缺省情况。

【命令】

```
attack-defense login reauthentication-delay seconds
undo attack-defense login reauthentication-delay
```

【缺省情况】

Login 用户登录失败后重新进行认证不需要等待。

【视图】

系统视图

【缺省用户角色】

network-admin

【参数】

seconds: 设备管理用户登录失败后重新进行认证的等待时长，取值范围为 4~60，单位为秒。

【使用指导】

Login 用户登录失败后，若设备上配置了重新进行认证的等待时长，则系统将会延迟一定的时长之后再允许用户进行认证，可以避免设备受到字典式攻击。

Login 用户延迟认证功能与 Login 用户攻击防范功能无关，只要配置了延迟认证等待时间，即可生效。

【举例】

配置 Login 用户登录失败后重新进行认证的等待时长为 5 秒钟。

```
<Sysname> system-view
[Sysname] attack-defense login reauthentication-delay 5
```

1.1.2 attack-defense tcp fragment enable

attack-defense tcp fragment enable 命令用来开启 TCP 分片攻击防范功能。

undo attack-defense tcp fragment enable 命令用来关闭 TCP 分片攻击防范功能。

【命令】

```
attack-defense tcp fragment enable
```

```
undo attack-defense tcp fragment enable
```

【缺省情况】

TCP 分片攻击防范功能处于开启状态。

【视图】

系统视图

【缺省用户角色】

network-admin

【使用指导】

设备的包过滤功能一般是通过判断 TCP 首个分片中的五元组（源 IP 地址、源端口号、目的 IP 地址、目的端口号、传输层协议号）信息来决定后续 TCP 分片是否允许通过。RFC 1858 对 TCP 分片报文进行了规定，认为 TCP 分片报文中，首片报文中 TCP 报文长度小于 20 字节，或后续分片报文中分片偏移量等于 8 字节的报文为 TCP 分片攻击报文。这类报文可以成功绕过上述包过滤功能，对设备造成攻击。为防止这类攻击，可以在设备上开启 TCP 分片攻击防范功能，对 TCP 分片攻击报文进行丢弃。

如果设备上开启了 TCP 分片攻击防范功能，并应用了单包攻击防范策略，则 TCP 分片攻击防范功能会先于单包攻击防范策略检测并处理入方向的 TCP 报文。

【举例】

开启 TCP 分片攻击防范功能。

```
<Sysname> system-view
```

```
[Sysname] attack-defense tcp fragment enable
```

目 录

1 TCP攻击防御.....	1-1
1.1 TCP攻击防御配置命令.....	1-1
1.1.1 tcp anti-naptha enable	1-1
1.1.2 tcp check-state interval	1-1
1.1.3 tcp state	1-2

1 TCP攻击防御

1.1 TCP攻击防御配置命令

1.1.1 tcp anti-naptha enable

tcp anti-naptha enable 命令用来开启防止 Naptha 攻击功能。

undo tcp anti-naptha enable 命令用来关闭防止 Naptha 攻击功能。

【命令】

```
tcp anti-naptha enable
undo tcp anti-naptha enable
```

【缺省情况】

防止 Naptha 攻击功能处于关闭状态。

【视图】

系统视图

【缺省用户角色】

network-admin

【使用指导】

开启防止 Naptha 攻击功能后，设备周期性地对各状态的 TCP 连接数进行检测（检测周期由 **tcp check-state interval** 命令配置），当某状态的最大 TCP 连接数超过指定的最大连接数后（最大连接数由 **tcp state** 命令配置），将加速该状态下 TCP 连接的老化。

【举例】

```
# 开启防止 Naptha 攻击功能。
<Sysname> system-view
[Sysname] tcp anti-naptha enable
```

【相关命令】

- **tcp state**
- **tcp check-state interval**

1.1.2 tcp check-state interval

tcp check-state interval 命令用来配置 TCP 连接状态的检测周期。

undo tcp check-state interval 命令用来恢复缺省情况。

【命令】

```
tcp check-state interval interval
undo tcp check-state interval
```

【缺省情况】

TCP 连接状态的检测周期为 30 秒。

【视图】

系统视图

【缺省用户角色】

network-admin

【参数】

interval: TCP 连接状态的检测周期，取值范围为 1~60，单位为秒。

【使用指导】

设备周期性地检测处于 CLOSING、ESTABLISHED、FIN_WAIT_1、FIN_WAIT_2 和 LAST_ACK 五种状态的 TCP 连接数，如果检测到某个状态的 TCP 连接数目超过设定的最大连接数时，将加速该状态下 TCP 连接的老化。

开启防止 Naptha 攻击功能后，设备才会周期性地对各状态的 TCP 连接数进行检测。

【举例】

配置 TCP 连接状态的检测周期为 40 秒。

```
<Sysname> system-view
[Sysname] tcp check-state interval 40
```

【相关命令】

- **tcp anti-naptha enable**
- **tcp state**

1.1.3 tcp state

tcp state 命令用来配置 TCP 连接的某一状态下的最大 TCP 连接数。

undo tcp state 命令用来恢复为缺省情况。

【命令】

```
tcp state { closing | established | fin-wait-1 | fin-wait-2 | last-ack }
connection-limit number
undo tcp state { closing | established | fin-wait-1 | fin-wait-2 | last-ack }
connection-limit
```

【缺省情况】

CLOSING、ESTABLISHED、FIN_WAIT_1、FIN_WAIT_2 和 LAST_ACK 五种状态最大 TCP 连接数均为 50。

【视图】

系统视图

【缺省用户角色】

network-admin

【参数】

closing: TCP 连接的 CLOSING 状态。

established: TCP 连接的 ESTABLISHED 状态。

fin-wait-1: TCP 连接的 FIN_WAIT_1 状态。

fin-wait-2: TCP 连接的 FIN_WAIT_2 状态。

last-ack: TCP 连接的 LAST_ACK 状态。

connection-limit number: 最大 TCP 连接数，取值范围为 0~500，取值为 0 时，表示不会加速该状态下 TCP 连接的老化。

【使用指导】

开启防止 Naptha 攻击功能后，各状态的最大 TCP 连接数限制才能生效，连接数目超过最大连接数后，将加速该状态下 TCP 连接的老化。

【举例】

配置 ESTABLISHED 状态下的最大 TCP 连接数为 100。

```
<Sysname> system-view
```

```
[Sysname] tcp state established connection-limit 100
```

【相关命令】

- **tcp anti-naptha enable**
- **tcp check-state interval**

目 录

1 IP Source Guard	1-1
1.1 IP Source Guard配置命令	1-1
1.1.1 display ip source binding	1-1
1.1.2 display ip verify source excluded	1-2
1.1.3 display ipv6 source binding	1-3
1.1.4 display ipv6 source binding pd	1-5
1.1.5 ip source binding (interface view)	1-6
1.1.6 ip source binding (system view)	1-7
1.1.7 ip verify source	1-8
1.1.8 ip verify source exclude	1-9
1.1.9 ipv6 source binding (interface view)	1-10
1.1.10 ipv6 source binding (system view)	1-11
1.1.11 ipv6 verify source	1-12

1 IP Source Guard

1.1 IP Source Guard配置命令

1.1.1 display ip source binding

display ip source binding 命令用来显示 IPv4 绑定表项信息。

【命令】

```
display ip source binding [ static | [ arp-snooping | dhcp-relay | dhcp-server  
| dhcp-snooping | dot1x ] ] [ ip-address ip-address ] [ mac-address  
mac-address ] [ vlan vlan-id ] [ interface interface-type interface-number ]  
[ slot slot-number ]
```

【视图】

任意视图

【缺省用户角色】

network-admin
network-operator

【参数】

static: 显示配置的静态绑定表项。

arp-snooping: 显示 ARP Snooping 模块生成的动态绑定表项。

dhcp-relay: 显示 DHCP 中继模块生成的动态绑定表项。

dhcp-server: 显示 DHCP 服务器模块生成的动态绑定表项。

dhcp-snooping: 显示 DHCP Snooping 模块生成的动态绑定表项。

dot1x: 显示 802.1X 模块生成的动态绑定表项。指定该参数时，必须同时指定 802.1X 用户接入的 slot 信息，才能显示相应表项。

ip-address *ip-address*: 显示指定 IPv4 地址的绑定表项，*ip-address* 表示绑定的 IPv4 地址。

mac-address *mac-address*: 显示指定 MAC 地址的绑定表项，*mac-address* 表示绑定的 MAC 地址，格式为 H-H-H。

vlan *vlan-id*: 显示指定 VLAN 的绑定表项，*vlan-id* 表示绑定的 VLAN ID，取值范围为 1～4094。

interface *interface-type interface-number*: 显示指定接口的绑定表项，*interface-type interface-number* 表示绑定的接口类型和接口编号。

slot *slot-number*: 显示指定成员设备上的绑定表项，*slot-number* 表示设备在 IRF 中的成员编号。如果未指定本参数，则显示主设备上的绑定表项。

【举例】

显示公网所有接口的 IPv4 绑定表项和全局的 IPv4 静态绑定表项。

```
<Sysname> display ip source binding
Total entries found: 5
IP Address      MAC Address      Interface      VLAN Type
10.1.0.5        040a-0000-4000  GE1/0/1        1    DHCP snooping
10.1.0.6        040a-0000-3000  GE1/0/1        1    DHCP snooping
10.1.0.7        040a-0000-2000  GE1/0/1        1    DHCP snooping
10.1.0.8        040a-0000-1000  GE1/0/2        N/A  DHCP relay
10.1.0.9        040a-0000-2000  GE1/0/2        N/A  Static
```

表1-1 display ip source-binding 命令显示信息描述表

字段	描述
Total entries found	查询到的绑定表项总数
IP Address	绑定表项的IPv4地址（N/A表示该表项不绑定IP地址）
MAC Address	绑定表项的MAC地址（N/A表示该表项不绑定MAC地址）
Interface	绑定表项所属的接口（N/A表示该表项为全局绑定）
VLAN	绑定表项所属的VLAN（N/A表示该表项中没有VLAN信息）
Type	绑定表项类型： <ul style="list-style-type: none"> Static 表示配置的静态绑定表项，IP Source Guard 模块用该表项过滤报文，并且配合其它模块提供相应的安全服务 ARP snooping 表示 ARP Snooping 模块生成的动态绑定表项，IP Source Guard 模块用该表项过滤报文 802.1X 表示来源于 802.1X 模块的动态绑定表项，IP Source Guard 模块用该表项过滤报文 DHCP relay 表示 DHCP 中继模块生成的动态绑定表项，IP Source Guard 模块用该表项过滤报文 DHCP server 表示 DHCP 服务器模块生成的动态绑定表项，用于配合其它模块提供相应的安全服务 DHCP snooping 表示 DHCP Snooping 模块生成的动态绑定表项，IP Source Guard 模块用该表项过滤报文

【相关命令】

- ip source binding
- ip verify source

1.1.2 display ip verify source excluded

display ip verify source excluded 命令用来显示 IP Source Guard 免过滤条件生效情况。

【命令】

```
display ip verify source excluded [ vlan start-vlan-id [ to end-vlan-id ] ]
[ slot slot-number ]
```

【视图】

任意视图

【缺省用户角色】

network-admin
network-operator

【参数】

vlan *start-vlan-id* [**to** *end-vlan-id*]: 显示指定 VLAN 内的信息，*start-vlan-id* 表示起始 VLAN ID，*end-vlan-id* 表示结束 VLAN ID，取值范围均为 1~4094，*end-vlan-id* 的值要大于或等于 *start-vlan-id* 的值。

slot *slot-number*: 显示指定成员设备上的信息，*slot-number* 表示设备在 IRF 中的成员编号。如果未指定本参数，则显示所有设备上的信息。

【举例】

显示设备上所有的 IP Source Guard 免过滤条件生效情况。

```
<Sysname> display ip verify source excluded
Slot:
  Start VLAN ID      End VLAN ID      Status
  1                  20               Active
  24                  50               Active
  200                 300              Inactive
```

显示 IP Source Guard 免过滤 VLAN（VLAN3、VLAN5~VLAN10）生效情况。

```
<Sysname> display ip verify source excluded vlan 3
Slot:
  VLAN ID: 3
  Status: Active

<Sysname> display ip verify source excluded vlan 5 to 10
Slot:
  Start VLAN ID      End VLAN ID      Status
  5                  10               Active
```

表1-2 display ip verify source excluded 命令显示信息描述表格

字段	描述
Start VLAN ID	免过滤VLAN的起始VLAN ID
End VLAN ID	免过滤VLAN的结束VLAN ID
Status	免过滤条件生效状态，取值为： <ul style="list-style-type: none">Active: 已生效Inactive: 未生效

【相关命令】

- ip verify source exclude

1.1.3 display ipv6 source binding

display ipv6 source binding 命令用来显示 IPv6 地址绑定表项信息。

【命令】

```
display ipv6 source binding [ static | [ dhcpv6-snooping | dot1x ] ]
[ ip-address ipv6-address ] [ mac-address mac-address ] [ vlan vlan-id ]
[ interface interface-type interface-number ] [ slot slot-number ]
```

【视图】

任意视图

【缺省用户角色】

network-admin
network-operator

【参数】

static: 显示配置的静态地址绑定表项。

dhcpv6-snooping: 显示 DHCPv6 Snooping 模块生成的动态地址绑定表项。

dot1x: 显示 802.1X 模块生成的动态地址绑定表项。指定该参数时，必须同时指定 802.1X 用户接入的 slot 信息，才能显示相应表项。

ip-address ipv6-address: 显示指定 IPv6 地址的地址绑定表项，*ipv6-address* 表示绑定的 IPv6 地址。

mac-address mac-address: 显示指定 MAC 地址的地址绑定表项，*mac-address* 表示绑定的 MAC 地址，格式为 H-H-H。

vlan vlan-id: 显示指定 VLAN 的地址绑定表项，*vlan-id* 表示绑定的 VLAN ID，取值范围为 1～4094。

interface interface-type interface-number: 显示指定接口的地址绑定表项，*interface-type interface-number* 表示绑定的接口类型和接口编号。

slot slot-number: 显示指定成员设备上的地址绑定表项，*slot-number* 表示设备在 IRF 中的成员编号。如果未指定本参数，则显示主设备上的地址绑定表项。

【举例】

```
# 显示公网所有接口的 IPv6 地址绑定表项和全局的 IPv6 静态地址绑定表项。
<Sysname> display ipv6 source binding
Total entries found: 2
IPv6 Address      MAC Address      Interface      VLAN Type
2012:1222:2012:1222: 000f-2202-0435 GE1/0/1      1      DHCPv6 snooping
2012:1222:2012:1222
2012:1222:2012:1222: 000f-2202-0436 GE1/0/1      N/A      Static
2012:1222:2012:1223
```

表1-3 display ipv6 source-binding 命令显示信息描述表

字段	描述
Total entries found	查询到的地址绑定表项总数
IPv6 Address	地址绑定表项的IPv6地址（N/A表示该表项不绑定IPv6地址）
MAC Address	地址绑定表项的MAC地址（N/A表示该表项不绑定MAC地址）

字段	描述
Interface	地址绑定表项所属的接口（N/A表示该表项为全局绑定）
VLAN	地址绑定表项所属的VLAN（N/A表示该表项没有VLAN信息）
Interface	地址绑定表项所属的接口
Type	地址绑定表项类型： <ul style="list-style-type: none"> Static 表示配置的 IPv6 静态地址绑定表项，该表项被 IP Source Guard 模块用于过滤报文，并且配合其它模块提供相应的安全服务 DHCPv6 snooping 表示 DHCPv6 Snooping 模块生成的动态地址绑定表项，IP Source Guard 模块用该表项过滤报文 802.1X 表示来源于 802.1X 模块的动态地址绑定表项，IP Source Guard 模块用该表项过滤报文

【相关命令】

- `ipv6 source binding`
- `ipv6 verify source`

1.1.4 display ipv6 source binding pd

`display ipv6 source binding pd` 命令用来显示 IPv6 前缀绑定表项信息。

【命令】

```
display ipv6 source binding pd [ prefix prefix/prefix-length ] [ mac-address
mac-address ] [ vlan vlan-id ] [ interface interface-type interface-number ]
[ slot slot-number ]
```

【视图】

任意视图

【缺省用户角色】

network-admin
network-operator

【参数】

prefix *prefix/prefix-length*: 显示指定 IPv6 前缀/前缀长度对应的 IPv6 前缀绑定表项信息，其中，*prefix-length* 取值范围为 1~128。如果未指定本参数，则显示所有 IPv6 前缀/前缀长度对应的 IPv6 前缀绑定表项信息。

mac-address *mac-address*: 显示指定 MAC 地址的 IPv6 前缀绑定表项信息，*mac-address* 表示绑定的 MAC 地址，格式为 H-H-H。如果未指定本参数，则显示所有 MAC 地址对应的 IPv6 前缀绑定表项信息。

vlan *vlan-id*: 显示指定 VLAN 内的 IPv6 前缀绑定表项信息，*vlan-id* 表示绑定的 VLAN ID，取值范围为 1~4094。如果未指定本参数，则显示所有 VLAN 内的 IPv6 前缀绑定表项信息。

interface interface-type interface-number:显示指定接口的 IPv6 前缀绑定表项信息，*interface-type interface-number* 表示绑定的接口类型和接口编号。如果未指定本参数，则显示所有 MAC 地址对应的 IPv6 前缀绑定表项信息。

slot slot-number: 显示指定成员设备上的前缀绑定表项，*slot-number* 表示设备在 IRF 中的成员编号。如果未指定本参数，则显示主设备上的前缀绑定表项。

【使用指导】

IPv6 前缀绑定表项是通过动态获取方式生成的，目前只支持从 DHCPv6 Snooping 获取该表项信息。

【举例】

```
# 显示所有的 IPv6 前缀绑定表项。
<Sysname> display ipv6 source binding pd
Total entries found: 2
IPv6 prefix      MAC address      Interface      VLAN
2012:1111::/64    000f-2202-0435   GE1/0/1        1
2012:2222::/64    000f-2202-0436   GE2/0/1        2
```

表1-4 display ipv6 source binding pd 命令显示信息描述表

字段	描述
Total entries found	查询到的前缀绑定表项总数
IPv6 prefix	前缀绑定表项的IPv6前缀/前缀长度
MAC address	前缀绑定表项的MAC地址（N/A表示该表项不绑定MAC地址）
Interface	前缀绑定表项所属的接口（N/A表示该表项为全局绑定）
VLAN	前缀绑定表项所属的VLAN（N/A表示该表项中没有VLAN信息）

【相关命令】

- **ipv6 source binding**
- **ipv6 verify source**

1.1.5 ip source binding (interface view)

ip source binding 命令用来配置接口的 IPv4 静态绑定表项。

undo ip source binding 命令用来删除接口的 IPv4 静态绑定表项。

【命令】

```
ip source binding { ip-address ip-address | ip-address ip-address
mac-address mac-address | mac-address mac-address } [ vlan vlan-id ]
undo ip source binding { all | ip-address ip-address | ip-address ip-address
mac-address mac-address | mac-address mac-address } [ vlan vlan-id ]
```

【缺省情况】

接口上未配置 IPv4 静态绑定表项。

【视图】

二层以太网端口
VLAN 接口

【缺省用户角色】

network-admin

【参数】

all: 当前接口所有的 IPv4 静态绑定表项，本参数只在 **undo ip source binding** 命令中生效。

ip-address ip-address: 指定接口的 IPv4 静态绑定表项的 IPv4 地址。其中 *ip-address* 表示绑定的 IPv4 地址，必须为 A、B、C 三类地址之一，不能为 127.x.x.x 和 0.0.0.0。

mac-address mac-address: 指定接口的 IPv4 静态绑定表项的 MAC 地址。其中 *mac-address* 表示绑定的 MAC 地址，格式为 H-H-H，取值不能为全 0、全 F（广播 MAC）和组播 MAC。

vlan vlan-id: 指定接口的 IPv4 静态绑定表项的 VLAN。其中 *vlan-id* 表示绑定的 VLAN ID，取值范围为 1~4094。本参数仅在二层以太网接口视图下支持。

【使用指导】

接口的 IPv4 静态绑定表项用于过滤接口收到的 IPv4 报文，或者与 ARP Detection 功能配合使用检查接入用户的合法性。

【举例】

在接口 GigabitEthernet1/0/1 上配置一条 IPv4 静态绑定表项，仅允许源 IP 地址为 192.168.0.1 且源 MAC 地址为 0001-0001-0001 的报文通过。

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] ip source binding ip-address 192.168.0.1 mac-address
0001-0001-0001
```

【相关命令】

- **display ip source binding**
- **ip source binding (system view)**

1.1.6 ip source binding (system view)

ip source binding 命令用来配置全局的 IPv4 静态绑定表项。

undo ip source binding 命令用来删除已配置的全局 IPv4 静态绑定表项。

【命令】

```
ip source binding ip-address ip-address mac-address mac-address
undo ip source binding { all | ip-address ip-address mac-address
mac-address }
```

【缺省情况】

未配置全局 IPv4 静态绑定表项。

【视图】

系统视图

【缺省用户角色】

network-admin

【参数】

ip-address *ip-address*: 指定全局的 IPv4 静态绑定表项的 IPv4 地址。其中 *ip-address* 表示绑定的 IPv4 地址，必须为 A、B、C 三类地址之一，不能为 127.x.x.x 和 0.0.0.0。

mac-address *mac-address*: 指定全局的 IPv4 静态绑定表项的 MAC 地址。其中 *mac-address* 表示绑定的 MAC 地址，格式为 H-H-H，取值不能为全 0、全 F（广播 MAC）和组播 MAC。

all: 设备上所有全局的 IPv4 静态绑定表项，本参数只在 **undo ip source binding** 命令中生效。

【使用指导】

全局的 IPv4 静态绑定表项对设备的所有接口都生效。

【举例】

在设备上配置一条全局的 IPv4 静态绑定表项，允许源 IP 地址为 192.168.0.1 且源 MAC 地址为 0001-0001-0001 的报文通过。

```
<Sysname> system-view
```

```
[Sysname] ip source binding ip-address 192.168.0.1 mac-address 0001-0001-0001
```

【相关命令】

- **display ip source binding**
- **ip source binding** (interface view)

1.1.7 ip verify source

ip verify source 命令用来开启 IPv4 接口绑定功能。

undo ip verify source 命令用来关闭 IPv4 接口绑定功能。

【命令】

```
ip verify source { ip-address | ip-address mac-address | mac-address }  
undo ip verify source
```

【缺省情况】

接口的 IPv4 接口绑定功能处于关闭状态。

【视图】

二层以太网端口

VLAN 接口

【缺省用户角色】

network-admin

【参数】

ip-address: 表示绑定源 IPv4 地址，即根据接口收到的报文的源 IPv4 地址对报文进行过滤。

ip-address mac-address: 表示绑定源 IP 地址和 MAC 地址，即接口上收到的报文的源 IPv4 地址和源 MAC 地址都与某动态绑定表项匹配，该报文才能被正常转发，否则将被丢弃。

mac-address: 表示绑定源 MAC 地址，即根据接口收到的报文的源 MAC 地址对报文进行过滤。

【使用指导】

配置该功能后，IP Source Guard 模块会通过静态或动态绑定表项过滤接口收到的用户 IP 报文，符合绑定表项的用户报文被正常转发，不符合绑定表项的用户报文将被丢弃。

本命令中指定的绑定参数，仅对动态生成的绑定表项有效，是接口使用动态绑定表项过滤报文时关心的报文特征项。如果仅使用静态绑定表项来过滤接口的报文，则本命令仅用于控制是否开启接口的报文过滤功能，接口依据配置的静态绑定表项参数来过滤报文，而不关心本命令中指定的参数。管理员执行本命令修改绑定规则后，只对新接入的用户生效，不会影响已接入用户。当已接入用户下线再重新上线后，才会按照新的绑定规则进行检查。

【举例】

在二层以太网接口 GigabitEthernet1/0/1 上配置 IPv4 接口绑定功能，根据报文的源 IP 地址和源 MAC 地址对接口收到的报文进行过滤。

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] ip verify source ip-address mac-address
```

在 Vlan-interface100 上配置对报文的源 IP 和 MAC 地址的 IPv4 接口绑定功能，根据报文的源 IP 地址和源 MAC 地址对接口收到的报文进行过滤。

```
<Sysname> system-view
[Sysname] interface vlan-interface 100
[Sysname-Vlan-interface100] ip verify source ip-address mac-address
```

【相关命令】

- **display ip source binding**

1.1.8 ip verify source exclude

ip verify source exclude 命令用来配置 IP Source Guard 免过滤条件。

undo ip verify source exclude 命令用来删除 IP Source Guard 免过滤条件。

【命令】

```
ip verify source exclude vlan start-vlan-id [to end-vlan-id ]
undo ip verify source exclude vlan start-vlan-id [to end-vlan-id ]
```

【缺省情况】

未配置 IP Source Guard 免过滤条件。

【视图】

系统视图

【缺省用户角色】

network-admin

【参数】

vlan start-vlan-id [to end-vlan-id]: 指定 IP Source Guard 免过滤的 VLAN 范围。
start-vlan-id 表示过滤 VLAN 的起始 VLAN ID，*end-vlan-id* 表示免过滤的终止 VLAN ID，取值范围均为 1~4094，*end-vlan-id* 的值要大于或等于 *start-vlan-id* 的值。如果不指定

end-vlan-id 或指定的 *end-vlan-id* 和 *start-vlan-id* 相同时，则表示只有一个 VLAN，即 *start-vlan-id*。

【使用指导】

配置 IP Source Guard 免过滤条件后，对收到匹配上免过滤条件的 IPv4 报文，设备不做 IP Source Guard 检查，直接放行。

可以通过多次执行本命令，配置多个 IP Source Guard 免过滤 VLAN，但不同命令中的 VLAN 范围不能重叠。

执行 **undo** 命令删除已有的指定 VLAN 范围的 IP Source Guard 免过滤条件时，该 VLAN 范围必须和创建免过滤条件时指定的 VLAN 范围一致，否则删除操作无法成功。

【举例】

配置 IP Source Guard 免过滤的 VLAN 范围为 VLAN3、VLAN5~VLAN10。

```
<Sysname> system-view
[Sysname] ip verify source exclude vlan 3
[Sysname] ip verify source exclude vlan 5 to 10
```

【相关命令】

- **display ip verify source excluded**

1.1.9 ipv6 source binding (interface view)

ipv6 source binding 命令用来配置接口的 IPv6 静态绑定表项。

undo ipv6 source binding 命令用来删除接口配置的 IPv6 静态绑定表项。

【命令】

```
ipv6 source binding { ip-address ipv6-address | ip-address ipv6-address
mac-address mac-address | mac-address mac-address } [ vlan vlan-id ]
undo ipv6 source binding { all | ip-address ipv6-address | ip-address
ipv6-address mac-address mac-address | mac-address mac-address } [ vlan
vlan-id ]
```

【缺省情况】

接口上未配置 IPv6 静态绑定表项。

【视图】

二层以太网端口

VLAN 接口

【缺省用户角色】

network-admin

【参数】

all: 当前接口所有的 IPv6 静态绑定表项，本参数只在 **undo ipv6 source binding** 命令中生效。

ip-address *ipv6-address*: 指定接口的 IPv6 静态绑定表项的 IPv6 地址。其中 *ipv6-address* 表示绑定的 IPv6 地址，不能为全 0 地址、组播地址、环回地址。

mac-address *mac-address*: 指定接口的 IPv6 静态绑定表项的 MAC 地址。其中 *mac-address* 表示绑定的 MAC 地址，格式为 H-H-H，取值不能为全 0、全 F（广播 MAC）和组播 MAC。

vlan *vlan-id*: 指定接口的 IPv6 静态绑定表项的 VLAN。其中 *vlan-id* 表示绑定的 VLAN ID，取值范围为 1~4094。本参数仅在二层以太网接口视图下支持。

【使用指导】

接口的 IPv6 静态绑定表项用于过滤接口收到的 IPv6 报文。

【举例】

在接口 GigabitEthernet1/0/1 上配置一条 IPv6 静态绑定表项，仅允许源 IPv6 地址为 2001::1 且源 MAC 地址为 0002-0002-0002 的报文通过。

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] ipv6 source binding ip-address 2001::1 mac-address
0002-0002-0002
```

【相关命令】

- **display ipv6 source binding**
- **display ipv6 source binding pd**
- **ipv6 source binding** (system view)

1.1.10 ipv6 source binding (system view)

ipv6 source binding 命令用来配置全局的 IPv6 静态绑定表项。

undo ipv6 source binding 命令用来删除已配置的全局 IPv6 静态绑定表项。

【命令】

```
ipv6 source binding ip-address ipv6-address mac-address mac-address
undo ipv6 source binding { all | ip-address ipv6-address mac-address
mac-address }
```

【缺省情况】

未配置全局 IPv6 静态绑定表项。

【视图】

系统视图

【缺省用户角色】

network-admin

【参数】

ip-address *ipv6-address*: 指定全局的 IPv6 静态绑定表项的 IPv6 地址。其中 *ipv6-address* 表示绑定的 IPv6 地址，不能为全 0 地址、组播地址、环回地址。

mac-address *mac-address*: 指定全局的 IPv6 静态绑定表项的 MAC 地址。其中 *mac-address* 表示绑定的 MAC 地址，格式为 H-H-H，取值不能为全 0、全 F（广播 MAC）和组播 MAC。

all: 设备上所有全局的 IPv6 静态绑定表项，本参数只在 **undo ipv6 source binding** 命令中生效。

【使用指导】

全局的 IPv6 静态绑定表项对设备的所有接口都生效。

【举例】

在设备上配置一条全局的 IPv6 静态绑定表项，允许源 IPv6 地址为 2001::1 且源 MAC 地址为 0002-0002-0002 的报文通过。

```
<Sysname> system-view
[Sysname] ipv6 source binding ip-address 2001::1 mac-address 0002-0002-0002
```

【相关命令】

- **display ipv6 source binding**
- **display ipv6 source binding pd**
- **ipv6 source binding** (interface view)

1.1.11 ipv6 verify source

ipv6 verify source 命令用来开启 IPv6 接口绑定功能。

undo ipv6 verify source 命令用来关闭 IPv6 接口绑定功能。

【命令】

```
ipv6 verify source { ip-address | ip-address mac-address | mac-address }
undo ipv6 verify source
```

【缺省情况】

接口的 IPv6 接口绑定功能处于关闭状态。

【视图】

二层以太网端口

VLAN 接口

【缺省用户角色】

network-admin

【参数】

ip-address: 表示绑定源 IPv6 地址，即根据接口收到的报文的源 IPv6 地址对报文进行过滤。

ip-address mac-address: 表示绑定源 IPv6 地址和 MAC 地址，即接口上收到的报文的源 IPv6 地址和源 MAC 地址都与某动态绑定表项匹配，该报文才能被正常转发，否则将被丢弃。

mac-address: 表示绑定源 MAC 地址，即根据接口收到的报文的源 MAC 地址对报文进行过滤。

【使用指导】

配置该功能后，IP Source Guard 模块会通过静态或动态绑定表项过滤接口收到的用户 IPv6 报文，符合绑定表项的用户报文被正常转发，不符合绑定表项的用户报文将被丢弃。

本命令中指定的绑定参数，仅对动态生成的绑定表项有效，是接口使用动态绑定表项过滤报文时关心的报文特征项。如果仅使用静态绑定表项来过滤接口的报文，则本命令仅用于控制是否开启接口的报文过滤功能，接口依据配置的静态绑定表项参数来过滤报文，而不关心本命令中指定的参数。

管理员执行本命令修改绑定规则后，只对新接入的用户生效，不会影响已接入的用户。当已接入用户下线再重新上线后，才会按照新的绑定规则进行检查。

【举例】

在二层以太网接口 **GigabitEthernet1/0/1** 上配置 IPv6 接口绑定功能，根据报文的源 IPv6 地址和源 MAC 地址对接口收到的报文进行过滤。

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] ipv6 verify source ip-address mac-address
```

【相关命令】

- **display ipv6 source binding**
- **display ipv6 source binding pd**

目 录

1 ARP攻击防御.....	1-1
1.1 ARP防止IP报文攻击配置命令.....	1-1
1.1.1 arp resolving-route enable	1-1
1.1.2 arp resolving-route probe-count	1-1
1.1.3 arp resolving-route probe-interval.....	1-2
1.1.4 arp source-suppression enable.....	1-3
1.1.5 arp source-suppression limit	1-3
1.1.6 display arp source-suppression.....	1-4
1.2 ARP报文限速配置命令	1-5
1.2.1 arp rate-limit	1-5
1.2.2 arp rate-limit log enable.....	1-5
1.2.3 arp rate-limit log interval	1-6
1.2.4 snmp-agent trap enable arp	1-7
1.3 源MAC地址固定的ARP攻击检测配置命令	1-7
1.3.1 arp source-mac	1-7
1.3.2 arp source-mac aging-time	1-8
1.3.3 arp source-mac exclude-mac	1-9
1.3.4 arp source-mac threshold.....	1-9
1.3.5 display arp source-mac.....	1-10
1.4 ARP报文源MAC地址一致性检查配置命令	1-11
1.4.1 arp valid-check enable	1-11
1.5 ARP主动确认配置命令	1-11
1.5.1 arp active-ack enable	1-11
1.6 授权ARP配置命令	1-12
1.6.1 arp authorized enable.....	1-12
1.7 ARP Detection配置命令	1-13
1.7.1 arp detection enable.....	1-13
1.7.2 arp detection log enable	1-13
1.7.3 arp detection port-match-ignore	1-14
1.7.4 arp detection rule.....	1-15
1.7.5 arp detection trust.....	1-16
1.7.6 arp detection validate	1-16
1.7.7 arp restricted-forwarding enable.....	1-17

1.7.8 display arp detection	1-18
1.7.9 display arp detection statistics attack-source	1-18
1.7.10 display arp detection statistics packet-drop	1-19
1.7.11 reset arp detection statistics attack-source	1-20
1.7.12 reset arp detection statistics packet-drop	1-21
1.8 ARP自动扫描、固化配置命令	1-21
1.8.1 arp fixup	1-21
1.8.2 arp scan	1-22
1.9 ARP网关保护配置命令	1-23
1.9.1 arp filter source	1-23
1.10 ARP过滤保护配置命令	1-24
1.10.1 arp filter binding	1-24
1.11 配置ARP报文源IP地址检查功能配置命令	1-25
1.11.1 arp sender-ip-range	1-25

1 ARP攻击防御

1.1 ARP防止IP报文攻击配置命令

1.1.1 arp resolving-route enable

arp resolving-route enable 命令用来开启 ARP 黑洞路由功能。

undo arp resolving-route enable 命令用来关闭 ARP 黑洞路由功能。

【命令】

```
arp resolving-route enable
undo arp resolving-route enable
```

【缺省情况】

ARP 黑洞路由功能处于开启状态。

【视图】

系统视图

【缺省用户角色】

network-admin

【使用指导】

建议在网关设备上开启本功能。

【举例】

```
# 开启 ARP 黑洞路由功能。
<Sysname> system-view
[Sysname] arp resolving-route enable
```

【相关命令】

- **arp resolving-route probe-count**
- **arp resolving-route probe-interval**

1.1.2 arp resolving-route probe-count

arp resolving-route probe-count 命令用来配置发送 ARP 请求报文的次数。

undo arp resolving-route probe-count 命令用来恢复缺省情况。

【命令】

```
arp resolving-route probe-count count
undo arp resolving-route probe-count
```

【缺省情况】

发送 ARP 请求报文的次数为 3 次。

【视图】

系统视图

【缺省用户角色】

network-admin

【参数】

count: 发送 ARP 请求报文的次数，取值范围为 1~25。

【举例】

配置发送 ARP 请求报文的次数为 5 次。

```
<Sysname> system-view
[Sysname] arp resolving-route probe-count 5
```

【相关命令】

- **arp resolving-route enable**
- **arp resolving-route probe-interval**

1.1.3 arp resolving-route probe-interval

arp resolving-route probe-interval 命令用来配置发送 ARP 请求报文的时间间隔。

undo arp resolving-route probe-interval 命令用来恢复缺省情况。

【命令】

```
arp resolving-route probe-interval interval
undo arp resolving-route probe-interval
```

【缺省情况】

发送 ARP 请求报文的时间间隔是 1 秒。

【视图】

系统视图

【缺省用户角色】

network-admin

【参数】

interval: 发送 ARP 请求报文的时间间隔，取值范围为 1~5，单位为秒。

【举例】

配置发送 ARP 请求报文的时间间隔为 3 秒。

```
<Sysname> system-view
[Sysname] arp resolving-route probe-interval 3
```

【相关命令】

- **arp resolving-route enable**
- **arp resolving-route probe-count**

1.1.4 arp source-suppression enable

arp source-suppression enable 命令用来开启 ARP 源地址抑制功能。

undo arp source-suppression enable 命令用来关闭 ARP 源地址抑制功能。

【命令】

```
arp source-suppression enable
undo arp source-suppression enable
```

【缺省情况】

ARP 源地址抑制功能处于关闭状态。

【视图】

系统视图

【缺省用户角色】

network-admin

【使用指导】

建议在网关设备上开启本功能。

【举例】

```
# 开启 ARP 源地址抑制功能。
<Sysname> system-view
[Sysname] arp source-suppression enable
```

【相关命令】

- **display arp source-suppression**

1.1.5 arp source-suppression limit

arp source-suppression limit 命令用来配置 ARP 源抑制的阈值。

undo arp source-suppression limit 命令用来恢复缺省情况。

【命令】

```
arp source-suppression limit limit-value
undo arp source-suppression limit
```

【缺省情况】

ARP 源抑制的阈值为 10。

【视图】

系统视图

【缺省用户角色】

network-admin

【参数】

limit-value: ARP 源抑制的阈值，即设备在 5 秒间隔内可以处理的源 IP 相同，但目的 IP 地址不能解析的 IP 报文的最大数目，取值范围为 2~1024。

【使用指导】

如果网络中每 5 秒内从某 IP 地址向设备某接口发送目的 IP 地址不能解析的 IP 报文超过了设置的阈值，则设备将不再处理由此 IP 地址发出的 IP 报文直至该 5 秒结束，从而避免了恶意攻击所造成的危害。

【举例】

```
# 配置 ARP 源抑制的阈值为 100。
<Sysname> system-view
[Sysname] arp source-suppression limit 100
```

【相关命令】

- **display arp source-suppression**

1.1.6 display arp source-suppression

display arp source-suppression 命令用来显示当前 ARP 源抑制的配置信息。

【命令】

```
display arp source-suppression
```

【视图】

任意视图

【缺省用户角色】

network-admin
network-operator

【举例】

```
# 显示当前 ARP 源抑制的配置信息。
<Sysname> display arp source-suppression
  ARP source suppression is enabled
  Current suppression limit: 100
```

表1-1 display arp source-suppression 显示信息描述表

字段	描述
ARP source suppression is enabled	ARP源抑制功能处于开启状态
Current suppression limit	设备在5秒时间间隔内可以接收到的源IP相同，但目的IP地址不能解析的IP报文的最大数目

1.2 ARP报文限速配置命令

1.2.1 arp rate-limit

arp rate-limit 命令用来开启 ARP 报文限速功能，并设置 ARP 报文限速速率。

undo arp rate-limit 命令用来关闭 ARP 报文限速功能。

【命令】

```
arp rate-limit [ pps ]  
undo arp rate-limit
```

【缺省情况】

ARP 报文限速功能处于开启状态。

【视图】

二层以太网接口视图
二层聚合接口视图

【缺省用户角色】

network-admin

【参数】

pps: ARP 限速速率，单位为包每秒（pps），取值范围为 5~200。如果未指定本参数，则用来恢复设备缺省 ARP 限速速率。

【使用指导】

不指定限速速率时，设备使用缺省限速速率，超过限速部分的报文会被丢弃。

【举例】

在二层以太网接口 GigabitEthernet1/0/1 上开启 ARP 报文限速功能，并设置 ARP 报文限速速率为 50pps。

```
<Sysname> system-view  
[Sysname] interface gigabitethernet 1/0/1  
[Sysname-GigabitEthernet1/0/1] arp rate-limit 50
```

1.2.2 arp rate-limit log enable

arp rate-limit log enable 命令用来开启 ARP 报文限速日志功能。

undo arp rate-limit log enable 命令用来关闭 ARP 报文限速日志功能。

【命令】

```
arp rate-limit log enable  
undo arp rate-limit log enable
```

【缺省情况】

设备的 ARP 报文限速日志功能处于关闭状态。

【视图】

系统视图

【缺省用户角色】

network-admin

【使用指导】

当开启了 ARP 限速日志功能后，设备将这个时间间隔内的超速峰值作为日志的速率值发送到设备的信息中心，通过设置信息中心的参数，最终决定日志报文的输出规则（即是否允许输出以及输出方向）。有关信息中心参数的设置请参见“网络管理和监控配置指导”中的“信息中心”。

【举例】

开启 ARP 报文限速日志功能。

```
<Sysname> system-view
[Sysname] arp rate-limit log enable
```

1.2.3 arp rate-limit log interval

arp rate-limit log interval 命令用来配置当设备收到的 ARP 报文速率超过用户设定的限速值时，设备发送告警和日志的时间间隔。

undo arp rate-limit log interval 命令用来恢复缺省情况。

【命令】

```
arp rate-limit log interval interval
undo arp rate-limit log interval
```

【缺省情况】

当设备收到的 ARP 报文速率超过用户设定的限速值时，设备发送告警和日志的时间间隔为 60 秒。

【视图】

系统视图

【缺省用户角色】

network-admin

【参数】

interval: 当端口上的 ARP 报文速率超过用户设定的限速值时，设备发送告警和日志的时间间隔。取值范围为 1~86400，单位为秒。

【使用指导】

用户需要先开启发送告警或日志功能，然后配置此命令指定设备发送告警和日志的时间间隔，同时本命令必须和端口下的 **arp rate-limit** 命令配合使用，单独配置本命令无效。

【举例】

当设备收到的 ARP 报文速率超过用户设定的限速值时，配置设备发送告警和日志的时间间隔为 120 秒。

```
<Sysname> system-view
[Sysname] arp rate-limit log interval 120
```

【相关命令】

- `arp rate-limit`
- `arp rate-limit log enable`
- `snmp-agent trap enable arp`

1.2.4 snmp-agent trap enable arp

`snmp-agent trap enable arp` 命令用来开启 ARP 模块的告警功能。

`undo snmp-agent trap enable arp` 命令用来关闭 ARP 模块的告警功能。

【命令】

```
snmp-agent trap enable arp [ rate-limit ]
undo snmp-agent trap enable arp [ rate-limit ]
```

【缺省情况】

ARP 模块的告警功能处于关闭状态。

【视图】

系统视图

【缺省用户角色】

network-admin

【参数】

rate-limit: 开启 ARP 报文限速的告警功能。

【使用指导】

当开启了 ARP 模块的告警功能后，设备将这个时间间隔内的超速峰值作为告警信息发送出去，生成的告警信息将发送到设备的 SNMP 模块，通过设置 SNMP 中告警信息的发送参数，来决定告警信息输出的相关特性。

有关告警信息的详细描述，请参见“网络管理和监控配置指导”中的“SNMP”。

【举例】

```
# 开启 ARP 报文限速的告警功能。
<Sysname> system-view
[Sysname] snmp-agent trap enable arp rate-limit
```

1.3 源MAC地址固定的ARP攻击检测配置命令

1.3.1 arp source-mac

`arp source-mac` 命令用来开启源 MAC 地址固定的 ARP 攻击检测功能，并选择检查模式。

`undo arp source-mac` 命令用来关闭源 MAC 地址固定的 ARP 攻击检测功能。

【命令】

```
arp source-mac { filter | monitor }
undo arp source-mac [ filter | monitor ]
```


【缺省情况】

源 MAC 地址固定的 ARP 攻击检测功能处于关闭状态。

【视图】

系统视图

【缺省用户角色】

network-admin

【参数】

filter: 配置检查方式为过滤模式。

monitor: 配置检查方式为监控模式。

【使用指导】

建议在网关设备上开启本功能。

本特性根据 ARP 报文的源 MAC 地址对上送 CPU 的 ARP 报文进行统计，在 5 秒内，如果收到同一源 MAC 地址（源 MAC 地址固定）的 ARP 报文超过一定的阈值，则认为存在攻击，系统会将此 MAC 地址添加到攻击检测表项中。当开启了 ARP 日志信息功能（配置 **arp check log enable** 命令），且在该攻击检测表项老化之前，如果设置的检查模式为过滤模式，则会打印日志信息并且将该源 MAC 地址发送的 ARP 报文过滤掉；如果设置的检查模式为监控模式，则只打印日志信息，不会将该源 MAC 地址发送的 ARP 报文过滤掉。关于 ARP 日志信息功能的详细描述，请参见“三层技术-IP 业务配置指导”中的“ARP”。

如果 **undo arp source-mac** 命令中未指定检查模式，则关闭任意检查模式的源 MAC 地址固定的 ARP 攻击检测功能。

【举例】

开启源 MAC 地址固定的 ARP 攻击检测功能，并选择 **filter** 检查模式。

```
<Sysname> system-view
[Sysname] arp source-mac filter
```

1.3.2 arp source-mac aging-time

arp source-mac aging-time 命令用来配置源 MAC 地址固定的 ARP 攻击检测表项的老化时间。

undo arp source-mac aging-time 命令用来恢复缺省情况。

【命令】

```
arp source-mac aging-time time
undo arp source-mac aging-time
```

【缺省情况】

源 MAC 地址固定的 ARP 攻击检测表项的老化时间为 300 秒。

【视图】

系统视图

【缺省用户角色】

network-admin

【参数】

time: 源 MAC 地址固定的 ARP 攻击检测表项的老化时间，取值范围为 60～6000，单位为秒。

【举例】

配置源 MAC 地址固定的 ARP 攻击检测表项的老化时间为 60 秒。

```
<Sysname> system-view
[Sysname] arp source-mac aging-time 60
```

1.3.3 arp source-mac exclude-mac

arp source-mac exclude-mac 命令用来配置保护 MAC 地址。当配置了保护 MAC 地址之后，即使该 ARP 报文中的 MAC 地址存在攻击也不会被检测过滤。

undo arp source-mac exclude-mac 命令用来取消配置的保护 MAC 地址。

【命令】

```
arp source-mac exclude-mac mac-address&<1-10>
undo arp source-mac exclude-mac [ mac-address&<1-10> ]
```

【缺省情况】

未配置任何保护 MAC 地址。

【视图】

系统视图

【缺省用户角色】

network-admin

【参数】

mac-address&<1-10>: MAC 地址列表。其中，*mac-address* 表示配置的保护 MAC 地址，格式为 H-H-H。&<1-10>表示每次最多可以配置的保护 MAC 地址个数。

【使用指导】

如果 **undo** 命令中未指定 MAC 地址，则取消所有已配置的保护 MAC 地址。

【举例】

配置源 MAC 地址固定的 ARP 攻击检查的保护 MAC 地址为 001e-1200-0213。

```
<Sysname> system-view
[Sysname] arp source-mac exclude-mac 001e-1200-0213
```

1.3.4 arp source-mac threshold

arp source-mac threshold 命令用来配置源 MAC 地址固定的 ARP 报文攻击检测阈值，当在固定的时间（5 秒）内收到源 MAC 地址固定的 ARP 报文超过该阈值则认为存在 ARP 报文攻击。

undo arp source-mac threshold 命令用来恢复缺省情况。

【命令】

```
arp source-mac threshold threshold-value
undo arp source-mac threshold
```

【缺省情况】

源 MAC 地址固定的 ARP 报文攻击检测的阈值为 30。

【视图】

系统视图

【缺省用户角色】

network-admin

【参数】

threshold-value: 固定时间内源 MAC 地址固定的 ARP 报文攻击检测的阈值, 单位为报文个数, 取值范围为 1~5000。

【举例】

配置源 MAC 地址固定的 ARP 报文攻击检测阈值为 30 个。

```
<Sysname> system-view
[Sysname] arp source-mac threshold 30
```

1.3.5 display arp source-mac

display arp source-mac 命令用来显示检测到的源 MAC 地址固定的 ARP 攻击检测表项。

【命令】

```
display arp source-mac { interface interface-type interface-number | slot
slot-number }
```

【视图】

任意视图

【缺省用户角色】

network-admin
network-operator

【参数】

interface interface-type interface-number: 显示指定接口检测到的源 MAC 地址固定的 ARP 攻击检测表项, *interface-type interface-number* 表示指定接口的类型和编号。

slot slot-number: 显示指定成员设备检测到的源 MAC 地址固定的 ARP 攻击检测表项。
slot-number 表示设备在 IRF 中的成员编号。如果未指定本参数, 则显示主设备上检测到的源 MAC 地址固定的 ARP 攻击检测表项。

【举例】

显示接口 GigabitEthernet1/0/1 检测到的源 MAC 地址固定的 ARP 攻击检测表项。

```
<Sysname> display arp source-mac interface gigabitethernet 1/0/1
Source-MAC          VLAN ID  Interface          Aging-time
```

表1-2 display arp source-mac 命令显示信息描述表

字段	描述
Source-MAC	检测到攻击的源MAC地址
VLAN ID	检测到攻击的VLAN ID
Interface	攻击来源的接口
Aging-time	ARP防攻击策略表项老化剩余时间，单位为秒

1.4 ARP报文源MAC地址一致性检查配置命令

1.4.1 arp valid-check enable

arp valid-check enable 命令用来开启 ARP 报文源 MAC 地址一致性检查功能。

undo arp valid-check enable 命令用来关闭 ARP 报文源 MAC 地址一致性检查功能。

【命令】

```
arp valid-check enable
undo arp valid-check enable
```

【缺省情况】

ARP 报文源 MAC 地址一致性检查功能处于关闭状态。

【视图】

系统视图

【缺省用户角色】

network-admin

【使用指导】

ARP 报文源 MAC 地址一致性检查功能主要应用于网关设备。

开启 ARP 报文源 MAC 地址一致性检查功能后，设备会对接收的 ARP 报文进行检查，如果以太网数据帧首部中的源 MAC 地址和 ARP 报文中的源 MAC 地址不同，则丢弃该报文。

【举例】

开启 ARP 报文源 MAC 地址一致性检查功能。

```
<Sysname> system-view
[Sysname] arp valid-check enable
```

1.5 ARP主动确认配置命令

1.5.1 arp active-ack enable

arp active-ack enable 命令用来开启 ARP 主动确认功能。

undo arp active-ack enable 命令用来关闭 ARP 主动确认功能。

【命令】

```
arp active-ack [ strict ] enable
undo arp active-ack [ strict ] enable
```

【缺省情况】

ARP 主动确认功能处于关闭状态。

【视图】

系统视图

【缺省用户角色】

network-admin

【参数】

strict: ARP 主动确认功能的严格模式。

【使用指导】

ARP 的主动确认功能主要应用于网关设备，防止攻击者仿冒用户欺骗网关设备。通过 **strict** 参数开启或关闭主动确认的严格模式。开启严格模式后，ARP 主动确认功能执行更严格的检查，新建 ARP 表项前，需要本设备先对其 IP 地址发起 ARP 解析，解析成功后才能触发正常的主动确认流程，在主动确认流程成功后，才允许设备学习该表项。

【举例】

```
# 开启 ARP 主动确认功能。
<Sysname> system-view
[Sysname] arp active-ack enable
```

1.6 授权ARP配置命令

1.6.1 arp authorized enable

arp authorized enable 命令用来开启接口下的授权 ARP 功能。
undo arp authorized enable 命令用来关闭接口下的授权 ARP 功能。

【命令】

```
arp authorized enable
undo arp authorized enable
```

【缺省情况】

接口下的授权 ARP 功能处于关闭状态。

【视图】

VLAN 接口视图

【缺省用户角色】

network-admin

【举例】

开启 Vlan-interface200 接口下授权 ARP 功能。

```
<Sysname> system-view
[Sysname] interface vlan-interface 200
[Sysname-Vlan-interface200] arp authorized enable
```

1.7 ARP Detection配置命令

1.7.1 arp detection enable

arp detection enable 命令用来开启 ARP Detection 功能，即对 ARP 报文进行用户合法性检查。

undo arp detection enable 命令用来关闭 ARP Detection 功能。

【命令】

```
arp detection enable
undo arp detection enable
```

【缺省情况】

ARP Detection 功能处于关闭状态，即不进行用户合法性检查。

【视图】

VLAN 视图

【缺省用户角色】

network-admin

【举例】

在 VLAN 2 下开启 ARP Detection 功能。

```
<Sysname> system-view
[Sysname] vlan 2
[Sysname-vlan2] arp detection enable
```

【相关命令】

- **arp detection rule**
- **display arp detection**
- **display arp detection statistics attack-source**
- **reset arp detection statistics attack-source**

1.7.2 arp detection log enable

arp detection log enable 命令用来开启 ARP Detection 日志功能。

undo arp detection log enable 命令用来关闭 ARP Detection 日志功能。

【命令】

```
arp detection log enable [ interval interval ]
undo arp detection log enable
```

【缺省情况】

ARP Detection 日志功能处于关闭状态。

【视图】

系统视图

【缺省用户角色】

network-admin

【参数】

interval interval: ARP Detection 日志信息输出周期, *interval* 的取值范围为 0、10~3600, 单位为秒, 缺省值为 60。当 *interval* 取值为 0 时, 表示立即输出日志信息。

【使用指导】

ARP Detection 日志可以方便管理员定位问题和解决问题。设备生成的 ARP Detection 日志信息会交给信息中心模块处理, 信息中心模块的配置将决定日志信息的发送规则和发送方向。关于信息中心的详细描述请参见“网络管理和监控配置指导”中的“信息中心”。

当设备输出大量 ARP Detection 日志信息时, 会降低设备性能。这时用户可以关闭 ARP Detection 日志功能, 使设备不再输出 ARP Detection 日志信息。

对于单个成员设备, 设备最多同时输出 128 条 ARP Detection 日志信息。

【举例】

```
# 开启 ARP Detection 日志功能。
<Sysname> system-view
[Sysname] arp detection log enable
```

1.7.3 arp detection port-match-ignore

arp detection port-match-ignore 命令用来开启 ARP Detection 忽略端口匹配检查功能。

undo arp detection port-match-ignore 命令用来关闭 ARP Detection 忽略端口匹配检查功能。

【命令】

```
arp detection port-match-ignore
undo arp detection port-match-ignore
```

【缺省情况】

ARP Detection 忽略端口匹配检查功能处于关闭状态。

【视图】

系统视图

【缺省用户角色】

network-admin

【使用指导】

开启 ARP Detection 忽略端口匹配检查功能后, ARP Detection 在进行各类安全表项检查时, 忽略 ARP 报文入端口和表项中的端口是否匹配的检查。

【举例】

```
# 开启 ARP Detection 忽略端口匹配检查功能。  
<Sysname> system-view  
[Sysname] arp detection port-match-ignore
```

【相关命令】

- **arp detection enable**

1.7.4 arp detection rule

arp detection rule 命令用来配置用户合法性检查规则。

undo arp detection rule 命令用来删除用户合法性检查规则。

【命令】

```
arp detection rule rule-id { deny | permit } ip { ip-address [ mask ] | any } mac  
 { mac-address [ mask ] | any } [ vlan vlan-id ]  
undo arp detection rule [ rule-id ]
```

【缺省情况】

未配置用户合法性检查规则。

【视图】

系统视图

【缺省用户角色】

network-admin

【参数】

rule-id: 用户合法性规则编号，取值范围为 0~511，数值越小表示该用户合法性规则优先级越高。

deny: 丢弃指定范围内的 ARP 报文。

permit: 转发指定范围内的 ARP 报文。

ip { ip-address [mask] | **any** }: 指定报文的源 IP 地址范围。

- **ip-address**: 表示报文的源 IP 地址，为点分十进制形式。
- **mask**: 表示源 IP 地址的掩码，为点分十进制形式。如果未指定该参数，则 **ip-address** 表示主机地址。
- **any**: 表示任意源 IP 地址。

mac { mac-address [mask] | **any** }: 指定报文的源 MAC 地址范围。

- **mac-address**: 表示报文的源 MAC 地址，格式为 H-H-H。
- **mask**: 表示源 MAC 地址的掩码，格式为 H-H-H。如果未指定该参数，则 **mac-address** 表示主机 MAC 地址。
- **any**: 表示任意源 MAC 地址。

vlan **vlan-id**: 指定规则中匹配的 VLAN，**vlan-id** 的取值范围为 1~4094。如果未指定该参数，则不对报文中的 VLAN 进行匹配检查。

【使用指导】

只有配置了 **arp detection enable** 命令后，通过命令 **arp detection rule** 配置的规则才生效。

使用 **undo arp detection rule** 命令时，如果未指定 *rule-id*，则会删除设备上所有已配置的用户合法性规则。

【举例】

配置用户合法性规则，规则编号为 0，规则内容为转发源地址为 10.1.1.1，掩码为 255.255.0.0，源 MAC 地址为 0001-0203-0405，掩码为 ffff-ffff-0000 的 ARP 报文。并在 VLAN2 中开启用户合法性检查功能。

```
<Sysname> system-view
[Sysname] arp detection rule 0 permit ip 10.1.1.1 255.255.0.0 mac 0001-0203-0405
ffff-ffff-0000
[Sysname] vlan 2
[Sysname-vlan2] arp detection enable
```

【相关命令】

- **arp detection enable**

1.7.5 arp detection trust

arp detection trust 命令用来配置接口为 ARP 信任接口。

undo arp detection trust 命令用来恢复缺省情况。

【命令】

```
arp detection trust
undo arp detection trust
```

【缺省情况】

接口为 ARP 非信任接口。

【视图】

二层以太网接口视图
二层聚合接口视图

【缺省用户角色】

network-admin

【举例】

配置二层以太网接口 GigabitEthernet1/0/1 为 ARP 信任接口。

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] arp detection trust
```

1.7.6 arp detection validate

arp detection validate 命令用来开启对 ARP 报文的目的 MAC 地址或源 MAC 地址、IP 地址的有效性检查。

undo arp detection validate 命令用来关闭对 ARP 报文的有效性检查。

【命令】

```
arp detection validate { dst-mac | ip | src-mac } *  
undo arp detection validate [ dst-mac | ip | src-mac ] *
```

【缺省情况】

ARP 报文有效性检查功能处于关闭状态。

【视图】

系统视图

【缺省用户角色】

network-admin

【参数】

dst-mac: 检查 ARP 应答报文中的目的 MAC 地址，是否为全 0 或者全 1，是否和以太网报文头中的目的 MAC 地址一致。全 0、全 1、不一致的报文都是无效的，无效的报文需要被丢弃。

ip: 检查 ARP 报文源 IP 和目的 IP 地址，全 1 或者组播 IP 地址都是不合法的，需要丢弃。对于 ARP 应答报文，源 IP 和目的 IP 地址都进行检查；对于 ARP 请求报文，只检查源 IP 地址。

src-mac: 检查 ARP 报文中的源 MAC 地址和以太网报文头中的源 MAC 地址是否一致，一致认为有效，否则丢弃。

【使用指导】

开启有效性检查时可以指定某一种检查方式也可以配置成多种检查方式的组合。

关闭时可以指定关闭某一种或多种检查，在不指定检查方式时，表示关闭所有有效性检查。

【举例】

开启对 ARP 报文的 MAC 地址和 IP 地址的有效性检查。

```
<Sysname> system-view  
[Sysname] arp detection validate dst-mac ip src-mac
```

1.7.7 arp restricted-forwarding enable

arp restricted-forwarding enable 命令用来开启 ARP 报文强制转发功能。

undo arp restricted-forwarding enable 命令用来关闭 ARP 报文强制转发功能。

【命令】

```
arp restricted-forwarding enable  
undo arp restricted-forwarding enable
```

【缺省情况】

ARP 报文强制转发功能处于关闭状态。

【视图】

VLAN 视图

【缺省用户角色】

network-admin

【举例】

```
# 开启 VLAN 2 的 ARP 报文强制转发功能。
<Sysname> system-view
[Sysname] vlan 2
[Sysname-vlan2] arp restricted-forwarding enable
```

1.7.8 display arp detection

display arp detection 命令用来显示配置了 ARP Detection 功能的 VLAN。

【命令】

display arp detection

【视图】

任意视图

【缺省用户角色】

network-admin
network-operator

【举例】

```
# 显示所有配置了 ARP Detection 功能的 VLAN。
<Sysname> display arp detection
ARP detection is enabled in the following VLANs:
1-2, 4-5
```

表1-3 display arp detection 命令显示信息描述表

字段	描述
ARP detection is enabled in the following VLANs	配置了ARP Detection功能的VLAN信息，如果不存在配置了ARP Detection功能的VLAN，则显示“ARP detection is not enabled in any VLANs.”

【相关命令】

- **arp detection enable**

1.7.9 display arp detection statistics attack-source

display arp detection statistics attack-source 命令用来显示 ARP Detection 攻击源统计信息。

【命令】

display arp detection statistics attack-source slot slot-number

【视图】

任意视图

【缺省用户角色】

network-admin
network-operator

【参数】

slot slot-number: 显示指定成员设备的 ARP Detection 攻击源统计信息。*slot-number* 表示设备在 IRF 中的成员编号。

【举例】

显示 Slot1 所有的 ARP Detection 攻击源统计信息。

```
<Sysname> display arp detection statistics attack-source slot 1
Interface          VLAN  MAC address      IP address      Number      Time
GE1/0/1            1     0005-0001-0001  10.1.1.14      24          17:09:56
03-27-2017
```

表1-4 display arp detection attack statistics attack-source 命令显示信息描述表

字段	描述
Interface	ARP Detection攻击报文的入接口
VLAN	ARP Detection攻击报文所属VLAN
MAC address	ARP Detection攻击报文中的源MAC地址
IP address	ARP Detection攻击报文中的源IP地址
Number	ARP Detection攻击报文被拦截的次数
Time	最近一次拦截该ARP Detection攻击报文的时间

【相关命令】

- **arp detection enable**

1.7.10 display arp detection statistics packet-drop

display arp detection statistics packet-drop 命令用来显示 ARP Detection 丢弃报文的统计信息。

【命令】

```
display arp detection statistics packet-drop [ interface interface-type
interface-number ]
```

【视图】

任意视图

【缺省用户角色】

network-admin
network-operator

【参数】

interface interface-type interface-number: 显示指定接口的 ARP Detection 丢弃报文的统计信息。*interface-type interface-number* 用来指定接口类型和编号。如果未指定本参数，则显示所有接口的 ARP Detection 丢弃报文的统计信息。

【使用指导】

按接口显示用户合法性检查和报文有效性检查的统计情况，只显示 ARP Detection 功能报文的丢弃情况。

【举例】

```
# 显示 ARP Detection 丢弃报文的统计信息。
<Sysname> display arp detection statistics packet-drop
State: U-Untrusted T-Trusted
ARP packets dropped by ARP inspect checking:
Interface(State)      IP      Src-MAC  Dst-MAC  Inspect
GE1/0/1(U)            40      0        0        78
GE1/0/2(U)            0       0        0        0
GE1/0/3(T)            0       0        0        0
GE1/0/4(U)            0       0        30       0
```

表1-5 display arp detection statistics packet-drop 命令显示信息描述表

字段	描述
State	接口状态： <ul style="list-style-type: none">U: ARP 非信任接口T: ARP 信任接口
Interface(State)	ARP报文入接口，State表示该接口的信任状态
IP	ARP报文源和目的IP地址检查不通过丢弃的报文计数
Src-MAC	ARP报文源MAC地址检查不通过丢弃的报文计数
Dst-MAC	ARP报文目的MAC地址检查不通过丢弃的报文计数
Inspect	ARP报文结合用户合法性检查不通过丢弃的报文计数

【相关命令】

- reset arp detection statistics packet-drop**

1.7.11 reset arp detection statistics attack-source

reset arp detection statistics attack-source 命令用来清除 ARP Detection 攻击源统计信息。

【命令】

```
reset arp detection statistics attack-source [ slot slot-number ]
```

【视图】

用户视图

【缺省用户角色】

network-admin

【参数】

slot *slot-number*: 清除指定成员设备的 ARP Detection 攻击源统计信息。*slot-number* 表示设备在 IRF 中的成员编号。如果未指定本参数，则清除所有成员设备上的 ARP Detection 攻击源统计信息。

【举例】

清除所有的 ARP Detection 攻击源统计信息。

```
<Sysname> reset arp detection statistics attack-source
```

【相关命令】

- **arp detection enable**
- **display arp detection statistics attack-source**

1.7.12 reset arp detection statistics packet-drop

reset arp detection statistics packet-drop 命令用来清除 ARP Detection 的报文丢弃统计信息。

【命令】

```
reset arp detection statistics packet-drop [ interface interface-type  
interface-number ]
```

【视图】

用户视图

【缺省用户角色】

network-admin

【参数】

interface *interface-type interface-number*: 表示清除指定接口下的 ARP Detection 的报文丢弃统计信息。*interface-type interface-number* 用来指定接口类型和编号。如果未指定本参数，则清除所有接口下的 ARP Detection 报文丢弃统计信息。

【举例】

清除所有的 ARP Detection 的报文丢弃统计信息。

```
<Sysname> reset arp detection statistics packet-drop
```

【相关命令】

- **display arp detection statistics packet-drop**

1.8 ARP自动扫描、固化配置命令

1.8.1 arp fixup

arp fixup 命令用来将设备上的动态 ARP 表项转化成静态 ARP 表项。

undo arp fixup 命令用来将设备上有效静态 ARP 表项转化为动态 ARP 表项，将无效静态 ARP 表项删除。

【命令】

```
arp fixup
undo arp fixup
```

【视图】

系统视图

【缺省用户角色】

network-admin

【使用指导】

本命令将当前的动态 ARP 表项转换为静态 ARP 表项，后续学习到的动态 ARP 表项可以通过再次执行 **arp fixup** 命令进行固化。

固化后的静态 ARP 表项与配置产生的静态 ARP 表项相同。

固化生成的静态 ARP 表项数量同样受到设备可以支持的静态 ARP 表项数目的限制，由于静态 ARP 表项数量的限制可能导致只有部分动态 ARP 表项被固化。

如果用户执行固化前有 D 个动态 ARP 表项，S 个静态 ARP 表项，由于固化过程中存在动态 ARP 表项的老化或者新建动态 ARP 表项的情况，所以固化后的静态 ARP 表项可能为 $(D+S+M-N)$ 个。其中，M 为固化过程中新建的动态 ARP 表项个数，N 为固化过程中老化的动态 ARP 表项个数。

通过固化生成的静态 ARP 表项，可以通过命令行 **undo arp ip-address** 逐条删除，也可以通过命令行 **reset arp all** 或 **reset arp static** 全部删除。

【举例】

将设备上的动态 ARP 表项转化成静态 ARP 表项。

```
<Sysname> system-view
[Sysname] arp fixup
```

1.8.2 arp scan

arp scan 命令用来开启 ARP 自动扫描功能，并设置接口发送 ARP 报文的速率。

【命令】

```
arp scan [ start-ip-address to end-ip-address ] [ send-rate pps ]
```

【视图】

VLAN 接口视图

L3VE 接口视图

【缺省用户角色】

network-admin

【参数】

start-ip-address: ARP 扫描区间的起始 IP 地址。起始 IP 地址必须小于等于终止 IP 地址。

end-ip-address: ARP 扫描区间的终止 IP 地址。

send-rate pps: 接口发送 ARP 报文的速率, 单位为包每秒。pps 的取值范围为 10~1000, 且需要设置为 10 的整数倍, 否则设备会提示配置错误。如果未设置本参数, 则接口会向扫描区间的所有 IP 地址同时发送 ARP 请求报文。

【使用指导】

ARP 自动扫描功能可以对接口下指定地址范围内的邻居进行扫描, 对于已存在 ARP 表项的 IP 地址不进行扫描。

如果用户知道局域网内邻居分配的 IP 地址范围, 指定了 ARP 扫描区间, 则对该范围内的邻居进行扫描, 减少扫描等待的时间。如果指定的扫描区间同时在接口下多个 IP 地址的网段内, 则发送的 ARP 请求报文的源 IP 地址选择网段范围较小的接口 IP 地址。

如果用户不指定 ARP 扫描区间的起始 IP 地址和终止 IP 地址, 则仅对接口下的主 IP 地址网段内的邻居进行扫描。其中, 发送的 ARP 请求报文的源 IP 地址就是接口的主 IP 地址。

ARP 扫描区间的起始 IP 地址和终止 IP 地址必须与接口的 IP 地址(主 IP 地址或手工配置的从 IP 地址)在同一网段。

扫描操作可能比较耗时, 用户可以通过<Ctrl_C>来终止扫描(在终止扫描时, 对于已经收到的邻居应答, 会建立该邻居的动态 ARP 表项)。

接口上开启了 ARP 自动扫描功能后, 会向扫描区间的所有 IP 地址同时发送 ARP 请求报文, 这会造成设备瞬间 CPU 利用率过高、网络负载过大的问题。用户可以通过设置接口发送 ARP 报文的速率解决此问题。

当发送 ARP 报文的速率配置为较大值时, 为避免影响设备性能, 设备实际发送 ARP 报文的速率可能会小于该配置值。

【举例】

对接口 Vlan-interface2 下的主 IP 地址网段内的邻居进行扫描。

```
<Sysname> system-view
[Sysname] interface vlan-interface 2
[Sysname-Vlan-interface2] arp scan
```

对接口 Vlan-interface2 下指定地址范围内的邻居进行扫描。

```
<Sysname> system-view
[Sysname] interface vlan-interface 2
[Sysname-Vlan-interface2] arp scan 1.1.1.1 to 1.1.1.20
```

对 VLAN 接口 2 下指定地址范围内的邻居进行扫描, 并设置接口发送 ARP 报文的速率为 10pps。

```
<Sysname> system-view
[Sysname] interface vlan-interface 2
[Sysname-Vlan-interface2] arp scan 1.1.1.1 to 1.1.1.20 send-rate 10
```

1.9 ARP网关保护配置命令

1.9.1 arp filter source

arp filter source 命令用来开启 ARP 网关保护功能, 配置受保护的网关 IP 地址。

undo arp filter source 命令用来关闭 ARP 网关保护功能, 并删除已配置的受保护网关 IP 地址。

【命令】

```
arp filter source ip-address  
undo arp filter source ip-address
```

【缺省情况】

ARP 网关保护功能处于关闭状态。

【视图】

二层以太网接口视图
二层聚合接口视图

【缺省用户角色】

network-admin

【参数】

ip-address: 受保护的网关 IP 地址。

【使用指导】

每个接口最多支持配置 8 个受保护的网关 IP 地址。

不能在同一接口下同时配置命令 **arp filter source** 和 **arp filter binding**。

【举例】

在 GigabitEthernet1/0/1 下开启 ARP 网关保护功能，受保护的网关 IP 地址为 1.1.1.1。

```
<Sysname> system-view  
[Sysname] interface gigabitethernet 1/0/1  
[Sysname-GigabitEthernet1/0/1] arp filter source 1.1.1.1
```

1.10 ARP过滤保护配置命令

1.10.1 arp filter binding

arp filter binding 命令用来开启 ARP 过滤保护功能并配置 ARP 过滤保护表项。

undo arp filter binding 命令用来删除 ARP 过滤保护表项。

【命令】

```
arp filter binding ip-address mac-address  
undo arp filter binding ip-address
```

【缺省情况】

ARP 过滤保护功能处于关闭状态。

【视图】

二层以太网接口视图
二层聚合接口视图

【缺省用户角色】

network-admin

【参数】

ip-address: 允许通过的 ARP 报文的源 IP 地址。

mac-address: 允许通过的 ARP 报文的源 MAC 地址。

【使用指导】

ARP 过滤保护表项可以限制只有特定源 IP 地址和源 MAC 地址的 ARP 报文才允许通过。

每个接口最多支持配置 8 组允许通过的 ARP 报文的源 IP 地址和源 MAC 地址。

不能在同一接口下同时配置命令 **arp filter source** 和 **arp filter binding**。

【举例】

在 GigabitEthernet1/0/1 下开启 ARP 过滤保护功能，允许源 IP 地址为 1.1.1.1、源 MAC 地址为 0e10-0213-1023 的 ARP 报文通过。

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] arp filter binding 1.1.1.1 0e10-0213-1023
```

1.11 配置ARP报文源IP地址检查功能配置命令

1.11.1 arp sender-ip-range

arp sender-ip-range 命令用来配置可接受的 ARP 报文中 sender IP 的地址范围。

undo arp sender-ip-range 命令用来恢复缺省情况。

【命令】

```
arp sender-ip-range start-ip-address end-ip-address
undo arp sender-ip-range
```

【缺省情况】

未限制 ARP 报文中 sender IP 的地址范围。

【视图】

VLAN 视图

【缺省用户角色】

network-admin

【参数】

start-ip-address: 起始 IP 地址。

end-ip-address: 终止 IP 地址，必须大于等于起始 IP 地址。

【使用指导】

如果设备收到的 VLAN 内 ARP 报文的 sender IP 不在指定地址范围内，则将该 ARP 报文丢弃。

多次执行本命令，最后一次执行的命令生效。

【举例】

在 VLAN 2 内配置可接受的 ARP 报文中 sender IP 的地址范围为 1.1.1.1~1.1.1.20。

```
<Sysname> system-view
```

```
[Sysname] vlan 2
```

```
[Sysname-vlan2] arp sender-ip-range 1.1.1.1 1.1.1.20
```

目 录

1 ND攻击防御	1-1
1.1 ND协议报文源MAC地址一致性检查命令	1-1
1.1.1 ipv6 nd check log enable	1-1
1.1.2 ipv6 nd mac-check enable	1-1
1.2 ND Detection配置命令	1-2
1.2.1 display ipv6 nd detection statistics	1-2
1.2.2 ipv6 nd detection enable	1-3
1.2.3 ipv6 nd detection trust	1-3
1.2.4 reset ipv6 nd detection statistics	1-4
1.3 RA Guard配置命令	1-4
1.3.1 display ipv6 nd raguard policy	1-4
1.3.2 display ipv6 nd raguard statistics	1-6
1.3.3 if-match acl	1-7
1.3.4 if-match autoconfig managed-address-flag	1-7
1.3.5 if-match autoconfig other-flag	1-8
1.3.6 if-match hop-limit	1-9
1.3.7 if-match prefix	1-9
1.3.8 if-match router-preference	1-10
1.3.9 ipv6 nd raguard apply policy	1-11
1.3.10 ipv6 nd raguard log enable	1-12
1.3.11 ipv6 nd raguard policy	1-13
1.3.12 ipv6 nd raguard role	1-13
1.3.13 reset ipv6 nd raguard statistics	1-14

1 ND攻击防御

1.1 ND协议报文源MAC地址一致性检查命令

1.1.1 ipv6 nd check log enable

ipv6 nd check log enable 命令用来开启 ND 日志信息功能。

undo ipv6 nd check log enable 命令用来关闭 ND 日志信息功能。

【命令】

```
ipv6 nd check log enable
undo ipv6 nd check log enable
```

【缺省情况】

ND 日志信息功能处于关闭状态。

【视图】

系统视图

【缺省用户角色】

network-admin

【使用指导】

设备生成的 ND 日志信息会交给信息中心模块处理，信息中心模块的配置将决定日志信息的发送规则和发送方向。关于信息中心的详细描述请参见“网络管理和监控配置指导”中的“信息中心”。

为了防止设备输出过多的 ND 日志信息，一般情况下建议不要开启此功能。

【举例】

```
# 开启 ND 日志信息功能。
<Sysname> system-view
[Sysname] ipv6 nd check log enable
```

1.1.2 ipv6 nd mac-check enable

ipv6 nd mac-check enable 命令用来开启 ND 协议报文源 MAC 地址一致性检查功能。

undo ipv6 nd mac-check enable 命令用来关闭 ND 协议报文源 MAC 地址一致性检查功能。

【命令】

```
ipv6 nd mac-check enable
undo ipv6 nd mac-check enable
```

【缺省情况】

ND 协议报文源 MAC 地址一致性检查功能处于关闭状态。

【视图】

系统视图

【缺省用户角色】

network-admin

【使用指导】

网关设备开启该功能后，会对接收到的 ND 协议报文进行检查，如果 ND 报文中的源 MAC 地址和以太网数据帧首部的源 MAC 地址不一致，则丢弃该报文。

【举例】

开启 ND 协议报文源 MAC 地址一致性检查功能。

```
<Sysname> system-view
[Sysname] ipv6 nd mac-check enable
```

1.2 ND Detection配置命令

1.2.1 display ipv6 nd detection statistics

display ipv6 nd detection statistics 命令用来显示 ND Detection 丢弃 ND 报文的统计信息。

【命令】

```
display ipv6 nd detection statistics [ interface interface-type
interface-number ]
```

【视图】

任意视图

【缺省用户角色】

network-admin
network-operator

【参数】

interface interface-type interface-number: 显示指定接口 ND Detection 丢弃 ND 报文的统计信息。*interface-type interface-number* 表示接口类型和接口编号。如果未指定本参数，则显示所有接口的 ND Detection 功能丢弃 ND 报文的统计信息。

【举例】

显示 ND Detection 丢弃报文的统计信息。

```
<Sysname> display ipv6 nd detection statistics
ND packets dropped by ND detection:
Interface          Packets dropped
GE1/0/1            78
GE1/0/2            0
GE1/0/3            0
GE1/0/4            0
```

表1-1 display ipv6 nd detection statistics 命令显示信息描述表

字段	描述
ND packets dropped by ND detection:	根据ND Detection丢弃的ND报文
Interface	ND报文入接口
Packets dropped	丢弃的报文数目

1.2.2 ipv6 nd detection enable

ipv6 nd detection enable 命令用来开启 ND Detection 功能，即对 ND 报文进行合法性检查。

undo ipv6 nd detection enable 命令用来关闭 ND Detection 功能。

【命令】

```
ipv6 nd detection enable
undo ipv6 nd detection enable
```

【缺省情况】

ND Detection 功能处于关闭状态。

【视图】

VLAN 视图

【缺省用户角色】

network-admin

【举例】

```
# 在 VLAN 10 内开启 ND Detection 功能。
<Sysname> system-view
[Sysname] vlan 10
[Sysname-vlan10] ipv6 nd detection enable
```

1.2.3 ipv6 nd detection trust

ipv6 nd detection trust 命令用来配置接口为 ND 信任接口。

undo ipv6 nd detection trust 命令用来恢复缺省情况。

【命令】

```
ipv6 nd detection trust
undo ipv6 nd detection trust
```

【缺省情况】

接口为 ND 非信任接口。

【视图】

二层以太网接口视图

二层聚合接口视图

【缺省用户角色】

network-admin

【举例】

配置二层以太网接口 GigabitEthernet1/0/1 为 ND 信任接口。

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] ipv6 nd detection trust
```

配置二层聚合接口 Bridge-Aggregation1 为 ND 信任接口。

```
<Sysname> system-view
[Sysname] interface bridge-aggregation 1
[Sysname-Bridge-Aggregation1] ipv6 nd detection trust
```

1.2.4 reset ipv6 nd detection statistics

reset ipv6 nd detection statistics 命令用来清除 ND Detection 的统计信息。

【命令】

```
reset ipv6 nd detection statistics [ interface interface-type
interface-number ]
```

【视图】

用户视图

【缺省用户角色】

network-admin

【参数】

interface interface-type interface-number: 表示清除指定接口的 ND Detection 的统计信息。*interface-type interface-number* 表示接口类型和接口编号。如果未指定本参数，则清除所有接口 ND Detection 的统计信息。

【举例】

清除所有的 ND Detection 统计信息。

```
<Sysname> reset ipv6 nd detection statistics
```

1.3 RA Guard配置命令

1.3.1 display ipv6 nd raguard policy

display ipv6 nd raguard policy 命令用来显示 RA Guard 策略信息。

【命令】

```
display ipv6 nd raguard policy [ policy-name ]
```

【视图】

任意视图

【缺省用户角色】

network-admin
network-operator

【参数】

policy-name: RA Guard 策略名称, 为 1~31 个字符的字符串, 区分大小写。如果未指定本参数, 则显示所有 RA Guard 策略信息。

【举例】

```
# 显示 RA Guard 策略信息。
<Sysname> display ipv6 nd raguard policy
Total number of policies: 2
RA Guard policy: policy1
    if-match ACL 2001
    if-match autoconfig managed-address-flag on
    if-match autoconfig other-flag off
    if-match hop-limit maximum 128
    if-match hop-limit minimum 100
    if-match prefix ACL name aa
    if-match router-preference medium
    applied to VLAN 1-3 7
RA Guard policy: policy2
    if-match ACL name zdd
    if-match prefix ACL 2200
```

表1-2 display ipv6 nd raguard policy 命令显示信息描述表

字段	描述
Total number of policies	策略总数
RA Guard policy:	RA Guard策略名称
if-match ACL	匹配的ACL编号
if-match ACL name	匹配的ACL名称
if-match autoconfig managed-address-flag	匹配的被管理地址标记位。其取值： <ul style="list-style-type: none">on: 表示匹配被管理地址标志位置为 1off: 表示匹配被管理地址标志位置为 0
if-match autoconfig other-flag	匹配的其他信息配置标记位。其取值： <ul style="list-style-type: none">on: 表示匹配的其他信息配置标志位置为 1off: 表示匹配的其他信息配置标志位置为 0
if-match hop-limit maximum	匹配的最大跳数值
if-match hop-limit minimum	匹配的最小跳数值

字段	描述
if-match prefix ACL	匹配的前缀ACL名称
if-match prefix ACL name	匹配的前缀ACL名称
applied to VLAN	策略应用的VLAN

【相关命令】

- `ipv6 nd raguard policy`

1.3.2 display ipv6 nd raguard statistics

`display ipv6 nd raguard statistics` 命令用来显示 RA Guard 的报文统计信息。

【命令】

```
display ipv6 nd raguard statistics [ interface interface-type
interface-number ]
```

【视图】

任意视图

【缺省用户角色】

network-admin
network-operator

【参数】

interface interface-type interface-number: 显示指定接口的 RA Guard 的报文统计信息。*interface-type interface-number* 表示接口类型和接口编号。如果未指定本参数，则显示所有接口的 RA Guard 的报文统计信息。

【举例】

显示 RA Guard 的报文统计信息。

```
<Sysname> display ipv6 nd raguard statistics
RA messages dropped by RA guard:
Interface      Dropped
GE1/0/1        78
GE1/0/2         0
GE1/0/3        32
GE1/0/4         0
```

表1-3 display ipv6 nd raguard statistics 命令显示信息描述表

字段	描述
Interface	RA报文的入接口
Dropped	丢弃的RA报文的数目

【相关命令】

- `ipv6 nd raguard log enable`
- `reset ipv6 nd raguard statistics`

1.3.3 if-match acl

`if-match acl` 命令用来配置 ACL 匹配规则。

`undo if-match acl` 命令用来删除 ACL 匹配规则。

【命令】

```
if-match acl { ipv6-acl-number | name ipv6-acl-name }  
undo if-match acl
```

【缺省情况】

未配置 ACL 匹配规则。

【视图】

RA Guard 策略视图

【缺省用户角色】

network-admin

【参数】

`ipv6-acl-number`: IPv6 基本 ACL 的编号，取值范围为 2000~2999。

`name ipv6-acl-name`: IPv6 基本 ACL 的名称，为 1~63 个字符的字符串，不区分大小写，必须以英文字母 a~z 或 A~Z 开头。为避免混淆，ACL 的名称不允许使用 all。

【使用指导】

RA Guard 策略将 ACL 匹配规则与 RA 报文中的发送方 IP 地址进行匹配。如果匹配成功，则说明 RA 报文通过了 ACL 匹配规则的检查。

若 RA Guard 策略中引用的 ACL 不存在或 ACL 中未定义规则的情况下，则 ACL 规则匹配检查不生效。

【举例】

在 RA Guard 策略 policy1 中，配置 ACL 匹配规则，引用的规则编号为 2001。

```
<Sysname> system-view  
[Sysname] ipv6 nd raguard policy policy1  
[Sysname-raguard-policy-policy1] if-match acl 2001
```

1.3.4 if-match autoconfig managed-address-flag

`if-match autoconfig managed-address-flag` 命令用来配置被管理地址标志位匹配规则。

`undo if-match autoconfig managed-address-flag` 命令用来删除被管理地址标志位匹配规则。

【命令】

```
if-match autoconfig managed-address-flag { off | on }
```

```
undo if-match autoconfig managed-address-flag
```

【缺省情况】

未配置被管理地址标志位匹配规则。

【视图】

RA Guard 策略视图

【缺省用户角色】

network-admin

【参数】

off: 匹配被管理地址标志位置为 0。

on: 匹配被管理地址标志位置为 1。

【使用指导】

RA 报文中的被管理地址标志位用于确定用户是否采用有状态自动配置获取 IPv6 地址。如果该标志位置为 1，则用户将通过有状态自动配置（例如 DHCPv6 服务器）来获取 IPv6 地址；否则，将通过无状态自动配置获取 IPv6 地址，即根据路由器发布的前缀信息和自己的链路层地址生成 IPv6 地址。

【举例】

在 RA Guard 策略 policy1 中，配置被管理地址标志位匹配规则，设置被管理地址标志位为 1。

```
<Sysname> system-view
[Sysname] ipv6 nd rguard policy policy1
[Sysname-rguard-policy-policy1] if-match autoconfig managed-address-flag on
```

1.3.5 if-match autoconfig other-flag

if-match autoconfig other-flag 命令用来配置其他信息配置标志位匹配规则。

undo if-match autoconfig other-flag 命令用来删除其他信息配置标志位匹配规则。

【命令】

```
if-match autoconfig other-flag { off | on }
undo if-match autoconfig other-flag
```

【缺省情况】

未配置其他信息配置标志位匹配规则。

【视图】

RA Guard 策略视图

【缺省用户角色】

network-admin

【参数】

off: 匹配的其他信息标志位置为 0。

on: 匹配的其他信息标志位置为 1。

【使用指导】

RA 报文中的其他信息标志位用于确定主机是否采用有状态自动配置获取除 IPv6 地址外的其他信息。如果该标志位置为 1，主机将通过有状态自动配置（例如 DHCPv6 服务器）来获取除 IPv6 地址外的其他信息；否则，将通过无状态自动配置获取其他信息。

【举例】

在 RA Guard 策略 policy1 中，配置其他信息标志位匹配规则，设置其他信息标志位为 1。

```
<Sysname> system-view
[Sysname] ipv6 nd rguard policy policy1
[Sysname-rguard-policy-policy1] if-match autoconfig other-flag on
```

1.3.6 if-match hop-limit

if-match hop-limit 命令用来配置 RA 报文跳数最大值或最小值匹配规则。

undo if-match hop-limit 命令用来删除 RA 报文跳数最大值或最小值匹配规则。

【命令】

```
if-match hop-limit { maximum | minimum } limit
undo if-match hop-limit { maximum | minimum }
```

【缺省情况】

不存在 RA 报文跳数最大值或最小值匹配规则。

【视图】

RA Guard 策略视图

【缺省用户角色】

network-admin

【参数】

maximum: RA 报文跳数最大值。

minimum: RA 报文跳数最小值。

limit: RA 报文的跳数取值，取值范围为 1~255。

【使用指导】

如果 RA 报文里 **current hop limit** 位为 0（代表未指定 RA 报文跳数值），但该报文匹配的策略中配置了 RA 报文跳数最大值或最小值匹配规则，则系统会丢弃该报文。

【举例】

在 RA Guard 策略 policy1 中，配置 RA 报文内跳数匹配规则，设置 RA 报文跳数最大值为 128。

```
<Sysname> system-view
[Sysname] ipv6 nd rguard policy policy1
[Sysname-rguard-policy-policy1] if-match hop-limit maximum 128
```

1.3.7 if-match prefix

if-match prefix 命令用来配置前缀匹配规则。

undo if-match prefix 命令用来删除前缀匹配规则。

【命令】

```
if-match prefix acl { ipv6-acl-number | name ipv6-acl-name }  
undo if-match prefix acl
```

【缺省情况】

未配置前缀匹配规则。

【视图】

RA Guard 策略视图

【缺省用户角色】

network-admin

【参数】

ipv6-acl-number: IPv6 基本 ACL 的编号，取值范围为 2000~2999。

name *ipv6-acl-name*: IPv6 基本 ACL 的名称，为 1~63 个字符的字符串，不区分大小写，必须以英文字母 a~z 或 A~Z 开头。为避免混淆，ACL 的名称不允许使用 all。

【使用指导】

如果 RA 报文中携带的前缀与前缀 ACL 匹配，则该 RA 报文通过前缀匹配规则检查。

若 RA Guard 策略中引用的前缀 ACL 不存在或前缀 ACL 中未定义规则，则前缀匹配规则检查不生效。

【举例】

在 RA Guard 策略 policy1 中，配置前缀匹配规则，引用 ACL 规则编号为 2000。在编号为 2000 的 IPv6 基本 ACL 中，仅允许 1001::/64 或 3124:1123::/64 网段的报文通过，而拒绝来自所有其它网段的报文通过。

```
<Sysname> system-view  
[Sysname] acl ipv6 basic 2000  
[Sysname-acl-ipv6-basic-2000] rule permit source 1001:: 64  
[Sysname-acl-ipv6-basic-2000] rule permit source 3124:1123:: 64  
[Sysname-acl-ipv6-basic-2000] rule deny source any  
[Sysname-acl-ipv6-basic-2000] quit  
[Sysname] ipv6 nd raguard policy policy1  
[Sysname-raguard-policy-policy1] if-match prefix acl 2000
```

1.3.8 if-match router-preference

if-match router-preference maximum 命令用来配置路由最高优先级匹配规则。

undo if-match router-preference maximum 命令用来删除路由最高优先级匹配规则。

【命令】

```
if-match router-preference maximum { high | low | medium }  
undo if-match router-preference maximum
```

【缺省情况】

未配置路由最高优先级匹配规则。

【视图】

RA Guard 策略视图

【缺省用户角色】

network-admin

【参数】

high: 策略中匹配的路由器最高优先级为高级。

low: 策略中匹配的路由器最高优先级为低级。

medium: 策略中匹配的路由器最高优先级为中级。

【使用指导】

主机根据接收到的 RA 消息中的路由器优先级，可以选择优先级最高的路由器作为默认网关。

在路由器的优先级相同的情况下，遵循“先来先用”的原则，优先选择先接收到的 RA 消息对应的发送路由器作为默认网关。

如果接收 RA 报文的接口未配置接口角色，且 RA 报文中未定义路由优先级，但该报文匹配的策略中定义了路由最高优先级匹配规则，则系统会丢弃该报文。

【举例】

在 RA Guard 策略 policy1 中，配置匹配的 router 最高优先级为中级。

```
<Sysname> system-view
[Sysname] ipv6 nd raguard policy policy1
[Sysname-raguard-policy-policy1] if-match router-preference maximum medium
```

1.3.9 ipv6 nd raguard apply policy

ipv6 nd raguard apply policy 命令用来应用 RA Guard 策略。

undo ipv6 nd raguard apply policy 命令用来取消对 RA Guard 策略的应用。

【命令】

```
ipv6 nd raguard apply policy [ policy-name ]
undo ipv6 nd raguard apply policy
```

【缺省情况】

未应用 RA Guard 策略。

【视图】

VLAN 视图

【缺省用户角色】

network-admin

【参数】

policy-name: 指定的 RA Guard 策略名称，为 1~31 个字符的字符串，区分大小写。如果未指定本参数，配置该策略的 VLAN 中除了配置为路由器角色的接口外，其他接口都会直接丢弃 RA 报文。

【使用指导】

当一个接口收到的 RA 报文存在多层 VLAN 标签时，只会根据最外层 VLAN 标签对应的 VLAN 下的策略对 RA 报文进行匹配检查。

如果指定的策略名称 *policy-name* 的策略不存在，则该配置无效。

【举例】

在 VLAN 100 下应用 RA Guard 策略 policy1。

```
<Sysname> system-view
[Sysname] vlan 100
[Sysname-vlan100] ipv6 nd raguard apply policy policy1
```

【相关命令】

- **ipv6 nd raguard policy**

1.3.10 ipv6 nd raguard log enable

ipv6 nd raguard log enable 命令用来开启 RA Guard 日志功能。

undo ipv6 nd raguard log enable 命令用来关闭 RA Guard 日志功能。

【命令】

```
ipv6 nd raguard log enable
undo ipv6 nd raguard log enable
```

【缺省情况】

RA Guard 日志功能处于关闭状态。

【视图】

系统视图

【缺省用户角色】

network-admin

【使用指导】

RA Guard 日志可以方便管理员定位问题和解决问题，对处理 RA 报文的信息进行的记录。开启 RA Guard 日志功能后，设备在检测到非法 RA 报文时将生成检测日志，日志内容包括：受到攻击的接口名称、RA 报文的源 IP 地址和丢弃的 RA 报文总数。

设备生成的 RA Guard 日志会交给信息中心模块处理，信息中心模块的配置将决定日志信息的发送规则和发送方向。关于信息中心的详细描述请参见“网络管理和监控配置指导”中的“信息中心”。

【举例】

开启 RA Guard 日志功能。

```
<Sysname> system-view
[Sysname] ipv6 nd raguard log enable
```

【相关命令】

- **display ipv6 nd raguard statistics**
- **reset ipv6 nd raguard statistics**

1.3.11 ipv6 nd rguard policy

ipv6 nd rguard policy 命令用来创建 RA Guard 策略，并进入 RA Guard 策略视图。如果指定的 RA Guard 策略已经存在，则直接进入 RA Guard 策略视图。

undo ipv6 nd rguard policy 命令用来删除已创建的 RA Guard 策略。

【命令】

```
ipv6 nd rguard policy policy-name  
undo ipv6 nd rguard policy policy-name
```

【缺省情况】

不存在任何 RA Guard 策略。

【视图】

系统视图

【缺省用户角色】

network-admin

【参数】

policy-name: RA Guard 策略名称，用来唯一标识一个 RA Guard 策略，为 1~31 个字符的字符串，区分大小写。

【举例】

创建 RA Guard 策略 policy1，并进入 RA Guard 策略视图。

```
<Sysname> system-view  
[Sysname] ipv6 nd rguard policy policy1  
[Sysname-rguard-policy-policy1]
```

【相关命令】

- **display ipv6 nd rguard policy**
- **ipv6 nd rguard apply policy**

1.3.12 ipv6 nd rguard role

ipv6 nd rguard role 用来配置接口角色。

undo ipv6 nd rguard role 用来删除接口角色。

【命令】

```
ipv6 nd rguard role { host | router }  
undo ipv6 nd rguard role
```

【缺省情况】

未配置接口角色。

【视图】

二层以太网接口视图
二层聚合接口视图

【缺省用户角色】

network-admin

【参数】

host: 指定接口角色为用户，该角色的接口直接丢弃收到的 RA 报文。

router: 指定接口角色为路由器，该角色的接口直接转发收到的 RA 报文。

【使用指导】

用户可根据接口在组网中的位置来配置接口的角色。如果确认接口连得是用户主机，可以配置成用户角色，如果确定接口连得是路由器，可配置成路由器角色。

【举例】

配置接口 GigabitEthernet1/0/1 的接口角色为用户。

```
<Sysname> system-view
```

```
[Sysname] interface gigabitethernet 1/0/1
```

```
[Sysname-GigabitEthernet1/0/1] ipv6 nd raguard role host
```

1.3.13 reset ipv6 nd raguard statistics

reset ipv6 nd raguard statistics 命令用来清除 RA Guard 的报文统计信息。

【命令】

```
reset ipv6 nd raguard statistics [ interface interface-type  
interface-number ]
```

【视图】

用户视图

【缺省用户角色】

network-admin

【参数】

interface interface-type interface-number: 清除指定接口的 RA Guard 的统计信息。
interface-type interface-number 表示接口类型和接口编号。若未指定本参数，则清除所有接口的 RA Guard 的统计信息。

【举例】

清除所有接口的 RA Guard 的报文统计信息。

```
<Sysname> reset ipv6 nd raguard statistics
```

【相关命令】

- **display ipv6 nd raguard statistics**

目 录

1 SAVI	1-1
1.1 SAVI配置命令	1-1
1.1.1 ipv6 savi down-delay	1-1
1.1.2 ipv6 savi strict	1-1

1 SAVI

1.1 SAVI配置命令

1.1.1 ipv6 savi down-delay

ipv6 savi down-delay 命令用来配置动态绑定表项的延迟删除时间。

undo ipv6 savi down-delay 命令用来恢复缺省情况。

【命令】

```
ipv6 savi down-delay delay-time
undo ipv6 savi down-delay
```

【缺省情况】

动态绑定表项的延迟删除时间为 30 秒。

【视图】

系统视图

【缺省用户角色】

network-admin

【参数】

delay-time: 动态绑定表项的延迟删除时间，取值范围为 0~21474836，单位为秒。

【使用指导】

开启 SAVI 功能后，如果端口在 down 状态的持续时间超过所配置的延迟删除时间，系统将会删除该端口上相关的 DHCPv6 Snooping 表项和 ND Snooping 表项。

【举例】

```
# 配置端口状态为 down 后动态绑定表项的延迟删除时间为 100 秒。
<Sysname> system-view
[Sysname] ipv6 savi down-delay 100
```

1.1.2 ipv6 savi strict

ipv6 savi strict 命令用来开启 SAVI 功能。

undo ipv6 savi strict 命令用来关闭 SAVI 功能。

【命令】

```
ipv6 savi strict
undo ipv6 savi strict
```

【缺省情况】

SAVI 功能处于关闭状态。

【视图】

系统视图

【缺省用户角色】

network-admin

【举例】

开启 SAVI 功能。

```
<Sysname> system-view
```

```
[Sysname] ipv6 savi strict
```

【相关命令】

- **ipv6 verify source**（安全命令参考/IP Source Guard）

目 录

1 MFF.....	1-1
1.1 MFF配置命令	1-1
1.1.1 display mac-forced-forwarding interface.....	1-1
1.1.2 display mac-forced-forwarding vlan.....	1-1
1.1.3 mac-forced-forwarding	1-2
1.1.4 mac-forced-forwarding gateway probe.....	1-3
1.1.5 mac-forced-forwarding network-port.....	1-4
1.1.6 mac-forced-forwarding server.....	1-4

1 MFF

1.1 MFF配置命令

1.1.1 display mac-forced-forwarding interface

display mac-forced-forwarding interface 命令用来显示 MFF 端口配置信息。

【命令】

display mac-forced-forwarding interface

【视图】

任意视图

【缺省用户角色】

network-admin
network-operator

【举例】

显示 MFF 端口配置信息。

```
<Sysname> display mac-forced-forwarding interface
Network Port:
GE1/0/1          GE1/0/2
User Port:
GE1/0/3          GE1/0/4          GE1/0/5
...
```

表1-1 display mac-forced-forwarding interface 命令显示信息描述表

字段	描述
Network Port	配置为网络端口的端口列表
User Port	配置为用户端口的端口列表

【相关命令】

- **mac-forced-forwarding network-port**

1.1.2 display mac-forced-forwarding vlan

display mac-forced-forwarding vlan 命令用来显示指定 VLAN 的 MFF 信息。

【命令】

display mac-forced-forwarding vlan *vlan-id*

【视图】

任意视图

【缺省用户角色】

network-admin
network-operator

【参数】

vlan-id: 显示指定 VLAN 的 MFF 信息。

【举例】

```
# 显示 VLAN 2 的 MFF 信息。
<Sysname> display mac-forced-forwarding vlan 2
VLAN 2
Gateway:
-----
192.168.1.42          000f-e200-8046
Server:
-----
192.168.1.48          192.168.1.49
```

表1-2 display mac-forced-forwarding vlan 命令显示信息描述表

字段	描述
VLAN 2	网关IP所对应的VLAN ID
Gateway	网关IP地址和网关MAC地址，未学习到则显示“N/A”
Server	服务器的IP地址

【相关命令】

- **mac-forced-forwarding**
- **mac-forced-forwarding server**

1.1.3 mac-forced-forwarding

mac-forced-forwarding 命令用来开启 MFF 功能，并指定缺省网关。

undo mac-forced-forwarding 命令用来关闭 MFF 功能。

【命令】

```
mac-forced-forwarding default-gateway gateway-ip  
undo mac-forced-forwarding
```

【缺省情况】

MFF 功能处于关闭状态。

【视图】

VLAN 视图

【缺省用户角色】

network-admin

【参数】

default-gateway gateway-ip: MFF 的缺省网关 IP 地址。

【使用指导】

在开启 MFF 的 VLAN 中需要同时开启 ARP Snooping 功能，以便 MFF 根据 ARP Snooping 表项应答终端用户的 ARP 请求。

对于用户手动配置 IP 地址的网络（或者 VLAN），网关的 IP 地址必须是手工配置，MFF 只检查手工配置的网关是否是全 0 或全 1 的 IP 地址，全 0 或全 1 的 IP 地址不能作为网关地址进行配置。多次执行本命令，最后一次执行的命令生效。

【举例】

开启 VLAN 2 下的 MFF 功能。

```
<Sysname> system-view
[Sysname] vlan 2
[Sysname-vlan2] mac-forced-forwarding default-gateway 1.1.1.1
```

【相关命令】

- **mac-forced-forwarding server**

1.1.4 mac-forced-forwarding gateway probe

mac-forced-forwarding gateway probe 命令用来开启网关定时探测功能。

undo mac-forced-forwarding gateway probe 命令用来关闭网关定时探测功能。

【命令】

```
mac-forced-forwarding gateway probe
undo mac-forced-forwarding gateway probe
```

【缺省情况】

网关定时探测功能处于关闭状态。

【视图】

VLAN 视图

【缺省用户角色】

network-admin

【使用指导】

在配置 **mac-forced-forwarding gateway probe** 命令之前需要开启 **mac-forced-forwarding** 功能。对网关进行定时探测的时间间隔为 30 秒。

【举例】

开启网关定时探测功能。

```
<Sysname> system-view
[Sysname] vlan 2
[Sysname-vlan2] mac-forced-forwarding gateway probe
```

【相关命令】

- **mac-forced-forwarding**

1.1.5 mac-forced-forwarding network-port

mac-forced-forwarding network-port 命令用来配置端口为网络端口。

undo mac-forced-forwarding network-port 命令用来恢复缺省情况。

【命令】

mac-forced-forwarding network-port

undo mac-forced-forwarding network-port

【缺省情况】

端口为用户端口。

【视图】

二层以太网接口视图

二层聚合接口视图

【缺省用户角色】

network-admin

【使用指导】

上行连接网关的端口，级联组网（多个 MFF 设备连接在一起的组网）时连接其他 MFF 设备的端口，或者环型组网时设备之间的端口，都应该配置为网络端口。可以设置多个端口为网络端口。

不论端口所属 VLAN 是否开启了 MFF 功能，都可以配置端口的 MFF 角色。不过只有开启了 MFF 功能后，配置的 MFF 端口角色才真正生效。

网络端口支持链路聚合，用户端口不支持链路聚合。当网络端口加入了链路聚合组，且所属 VLAN 开启了 MFF 功能时，如果用户想取消网络端口的配置，则需要先将网络端口从链路聚合组中退出，然后再取消网络端口的配置。关于链路聚合的介绍，请参见“二层技术-以太网交换”中的“以太网链路聚合配置”。

【举例】

配置 GigabitEthernet1/0/1 端口为网络端口。

```
<Sysname> system-view
```

```
[Sysname] interface gigabitethernet 1/0/1
```

```
[Sysname-GigabitEthernet1/0/1] mac-forced-forwarding network-port
```

【相关命令】

- **mac-forced-forwarding**

1.1.6 mac-forced-forwarding server

mac-forced-forwarding server 命令用来配置网络中部署的服务器的 IP 地址。

undo mac-forced-forwarding server 命令用来删除服务器的 IP 地址。

【命令】

```
mac-forced-forwarding server server-ip&<1-10>  
undo mac-forced-forwarding server server-ip&<1-10>
```

【缺省情况】

未配置网络中部署的服务器的 IP 地址。

【视图】

VLAN 视图

【缺省用户角色】

network-admin

【参数】

server-ip&<1-10>: 网络中部署的服务器的 IP 地址，&<1-10>表示前面的参数最多可以输入 10 次。

【使用指导】

如果网络中部署了服务器,就需要在开启 MFF 功能的设备的服务器列表中添加此服务器的 IP 地址,否则,客户端与服务器之间不能进行通信。

服务器 IP 地址可以是相关业务的服务器的 IP 地址 (如 RADIUS 服务器)。

如果 MFF 设备的网络端口收到了源 IP 地址为服务器 IP 地址的 ARP 请求,则查询本设备记录的用户信息,利用查询到的用户信息代替客户端应答给服务器。即客户端发送给服务器的报文,都会通过网关进行转发,而服务器发送给客户端的报文,则不需经过网关转发。

MFF 不检查服务器的 IP 地址和网关 IP 地址是否在同一个网段,只检查是否是全 0 或全 1 的 IP 地址,全 0 或全 1 的 IP 地址不能作为服务器 IP 地址进行配置。

在配置 **mac-forced-forwarding server** 命令之前需要开启 MFF 功能。

【举例】

```
# 配置网络中部署的服务器的 IP 地址为 192.168.1.100。  
<Sysname> system-view  
[Sysname] vlan 2  
[Sysname-vlan2] mac-forced-forwarding server 192.168.1.100
```

【相关命令】

- **mac-forced-forwarding**

目 录

1 加密引擎.....	1-1
1.1 加密引擎配置命令.....	1-1
1.1.1 display crypto-engine.....	1-1
1.1.2 display crypto-engine statistics	1-2
1.1.3 reset crypto-engine statistics	1-3

1 加密引擎

1.1 加密引擎配置命令

1.1.1 display crypto-engine

display crypto-engine 命令用来显示加密引擎的基本信息。

【命令】

display crypto-engine

【视图】

任意视图

【缺省用户角色】

network-admin
network-operator

【举例】

```
# 显示加密引擎的基本信息。
<Sysname> display crypto-engine
  Crypto engine name: Software crypto engine
  Crypto engine state: Enabled
  Crypto engine type: Software
  Slot ID: 1
  CPU ID: 0
  Crypto engine ID: 0
  Symmetric algorithms: des-cbc des-ecb 3des-cbc aes-cbc aes-ecb aes-ctr camellia_cbc md5
sha1 sha2-256 sha2-384 sha2-512 md5-hmac sha1-hmac sha2-256-hmac sha2-384-hmac sha2-512-hmac
aes-xcbc aes-xcbc-hmac
  Asymmetric algorithms:
  Random number generation function: Supported
```

表1-1 display crypto-engine 命令显示信息描述表

字段	描述
Crypto engine name	加密引擎名称
Crypto engine state	加密引擎的状态 对于软件加密引擎，只包含以下一种： <ul style="list-style-type: none">Enabled: 已开启
Crypto engine type	加密引擎的类型，Software为软件加密
CPU ID	设备上的CPU编号
Crypto engine ID	加密引擎ID号
Symmetric algorithms	支持的对称加密算法

字段	描述
Asymmetric algorithms	支持的非对称加密算法
Random number generation function	是否支持获取随机数的功能 <ul style="list-style-type: none"> Supported: 支持 Not supported: 不支持

1.1.2 display crypto-engine statistics

display crypto-engine statistics 命令用来显示加密引擎的统计信息。

【命令】

display crypto-engine statistics [**engine-id** *engine-id* **slot** *slot-number*]

【视图】

任意视图

【缺省用户角色】

network-admin
network-operator

【参数】

engine-id *engine-id*: 显示指定加密引擎的统计信息, *engine-id* 为加密引擎 ID 编号, 当前设备仅支持软件加密引擎, 取值只能为 0。

slot *slot-number*: 显示指定成员设备上的加密引擎统计信息, *slot-number* 表示设备在 IRF 中的成员编号。

【使用指导】

若不指定任何参数, 则显示所有成员设备上的加密引擎统计信息。

【举例】

显示所有加密引擎统计信息。

```
<Sysname> display crypto-engine statistics
Slot ID: 1
CPU ID: 0
Crypto engine ID: 0
Submitted sessions: 0
Failed sessions: 0
Symmetric operations: 0
Symmetric errors: 0
Asymmetric operations: 0
Asymmetric errors: 0
Get-random operations: 0
Get-random errors: 0
```

表1-2 display crypto-engine statistics 命令显示信息描述表

字段	描述
Crypto engine ID	加密引擎ID
Submitted sessions	已创建的会话数目
Failed sessions	创建失败的会话数目
Symmetric operations	加密引擎使用对称算法的操作次数
Symmetric errors	加密引擎使用对称算法操作失败的次数
Asymmetric operations	加密引擎使用非对称算法操作的次数
Asymmetric errors	加密引擎使用非对称算法操作失败的次数
Get-random operations	加密引擎获取随机数操作的次数
Get-random errors	加密引擎获取随机数操作失败的次数

【相关命令】

- `reset crypto-engine statistics`

1.1.3 reset crypto-engine statistics

`reset crypto-engine statistics` 命令用来清除加密引擎的统计信息。

【命令】

`reset crypto-engine statistics [engine-id engine-id slot slot-number]`

【视图】

用户视图

【缺省用户角色】

network-admin

【参数】

engine-id engine-id: 清除指定加密引擎的统计信息, *engine-id* 为加密引擎 ID 编号, 当前设备仅支持软件加密引擎, 取值只能为 0。

slot slot-number: 清除指定成员设备上的加密引擎统计信息, *slot-number* 表示设备在 IRF 中的成员编号。

【使用指导】

若不指定任何参数, 清除所有成员设备上的加密引擎统计信息。

【举例】

清除加密引擎的统计信息。

```
<Sysname> reset crypto-engine statistics
```

【相关命令】

- `display crypto-engine statistics`

目 录

1 FIPS	1-1
1.1 FIPS配置命令	1-1
1.1.1 display crypto version	1-1
1.1.2 display fips status	1-1
1.1.3 fips mode enable	1-2
1.1.4 fips self-test	1-4

1 FIPS

1.1 FIPS配置命令

1.1.1 display crypto version

display crypto version 命令用来显示算法库的版本号。

【命令】

display crypto version

【视图】

任意视图

【缺省用户角色】

network-admin
network-operator

【使用指导】

相同的算法库版本号表示了一套相同的密码学算法。

【举例】

显示当前设备算法库的版本号。

```
<Sysname> display crypto version  
7.1.1.1.1.72
```

表1-1 display crypto version 命令显示信息描述表

字段	描述
7.1.1.1.1.72	版本号信息，格式为7.1.X，其中7.1表示Comware V700R001，X表示算法库的版本号

1.1.2 display fips status

display fips status 命令用来显示 FIPS 模式状态。

【命令】

display fips status

【视图】

任意视图

【缺省用户角色】

network-admin
network-operator

【举例】

```
# 显示 FIPS 模式状态。  
<Sysname> display fips status  
FIPS mode is enabled.
```

【相关命令】

- **fips mode enable**

1.1.3 fips mode enable

fips mode enable 命令用来开启 FIPS 模式。
undo fips mode enable 命令用来关闭 FIPS 模式。

【命令】

```
fips mode enable  
undo fips mode enable
```

【缺省情况】

FIPS 模式处于关闭状态。

【视图】

系统视图

【缺省用户角色】

network-admin

【使用指导】

开启 FIPS 模式并重启设备之后，设备会运行于支持 FIPS 140-2 标准的工作模式下。在该工作模式下，系统将具有更为严格的安全性要求，并会对密码模块进行相应的自检处理，以确认其处于正常运行状态。

用户执行了 **fips mode enable** 命令后，系统提供以下两种启动方式来进入 FIPS 模式：

- 自动重启方式：
该方式下，系统自动创建一个 FIPS 缺省配置文件（名称为 **fips-startup.cfg**），同时将其指定为下次启动配置文件，并且要求用户手工配置设备重启后登录设备的用户名和密码。如果用户在输入过程中想退出配置流程，可以使用 **<Ctrl+C>** 组合键中断配置流程，配置流程中断后，当前的 **fips mode enable** 命令设置也相应失败。
用户成功设置安全管理员用户名和登录密码之后，系统将自动使用指定的启动配置文件重启。
- 手动重启方式：
该方式下，系统不自动创建进入 FIPS 模式的下次启动配置文件。需要用户手工完成进入 FIPS 模式所需的所有必要配置，主要包括：
 - 开启全局 Password Control 功能。
 - 设置全局 Password Control 密码组合类型的个数为 4，每种类型至少 1 个字符。
 - 设置全局 Password Control 的密码最小长度为 15。

- 添加设备管理类本地用户，设置密码、用户角色和服务类型。本地用户的密码需要符合以上 Password Control 配置的限制，用户角色必须是 **network-admin**，服务类型为 **terminal**。
- 删除不符合 FIPS 标准的本地用户服务类型（Telnet、HTTP 和 FTP）。

然后手工保存当前配置文件为下次启动配置文件，并将二进制类型的下次启动配置文件删除后重启设备。

执行 **fips mode enable** 命令之后，系统会提示用户选择启动方式，若用户未在 30 秒内作出选择，则系统默认用户采用了手动启动方式。

用户执行了 **undo fips mode enable** 命令后，系统提供以下两种启动选择来退出 FIPS 模式：

- 自动重启方式：系统自动创建一个非 FIPS 缺省配置文件（名称为 **non-fips-startup.cfg**），同时将其指定为下次启动配置文件，之后自动使用非 FIPS 缺省配置文件重启。重启之后，当前登录用户不需要输入任何信息即可直接登录到非 FIPS 模式的系统。
- 手动重启方式：系统不自动创建进入非 FIPS 模式的下次启动配置文件，需要用户手工完成进入非 FIPS 模式所需的所有必要配置之后，手工重启设备。重启之后，当前登录用户需要根据配置的登录认证方式输入相应的用户信息登录到非 FIPS 模式的系统。

【举例】

开启 FIPS 模式，并选择自动重启方式进入 FIPS 模式。

```
<Sysname> system-view
[Sysname] fips mode enable
FIPS mode change requires a device reboot. Continue? [Y/N]:y
Reboot the device automatically? [Y/N]:y
The system will create a new startup configuration file for FIPS mode. After you set the login
username and password for FIPS mode, the device will reboot automatically.
Enter username(1-55 characters): root
Enter password(15-63 characters):
Confirm password:
Waiting for reboot... After reboot, the device will enter FIPS mode.
```

开启 FIPS 模式，并选择手动重启方式进入 FIPS 模式。

```
<Sysname> system-view
[Sysname] fips mode enable
FIPS mode change requires a device reboot. Continue? [Y/N]:y
Reboot the device automatically? [Y/N]:n
Change the configuration to meet FIPS mode requirements, save the configuration to the
next-startup configuration file, and then reboot to enter FIPS mode.
```

关闭 FIPS 模式，并选择自动重启方式进入非 FIPS 模式。

```
[Sysname] undo fips mode enable
FIPS mode change requires a device reboot. Continue? [Y/N]:y
The system will create a new startup configuration file for non-FIPS mode and then reboot
automatically. Continue? [Y/N]:y
Waiting for reboot... After reboot, the device will enter non-FIPS mode.
```

关闭 FIPS 模式，并选择手动重启方式进入非 FIPS 模式。

```
[Sysname] undo fips mode enable
FIPS mode change requires a device reboot. Continue? [Y/N]:y
```

The system will create a new startup configuration file for non-FIPS mode, and then reboot automatically. Continue? [Y/N]:n

Change the configuration to meet non-FIPS mode requirements, save the configuration to the next-startup configuration file, and then reboot to enter non-FIPS mode.

【相关命令】

- **display fips status**

1.1.4 fips self-test

fips self-test 命令用来手工触发密码算法自检。

【命令】

fips self-test

【视图】

系统视图

【缺省用户角色】

network-admin

【使用指导】

此命令仅在 **FIPS** 模式下支持。当管理员需要确认当前处于 **FIPS** 模式的系统中的密码算法模块是否正常工作时，可以执行本命令触发密码算法自检。手工触发的密码算法自检内容与设备启动时自动进行的启动自检内容相同。

只有所有密码算法自检都通过了，整个密码算法自检才算成功。密码算法自检失败后，设备会自动重启。

【举例】

手工触发密码算法自检。

```
<Sysname> system-view
[Sysname] fips self-test
Cryptographic Algorithms Known-Answer Tests are running ...
Slot 1:
Starting Known-Answer tests in the user space.
Known-answer test for 3DES passed.
Known-answer test for SHA1 passed.
Known-answer test for SHA224 passed.
Known-answer test for SHA256 passed.
Known-answer test for SHA384 passed.
Known-answer test for SHA512 passed.
Known-answer test for HMAC-SHA1 passed.
Known-answer test for HMAC-SHA224 passed.
Known-answer test for HMAC-SHA256 passed.
Known-answer test for HMAC-SHA384 passed.
Known-answer test for HMAC-SHA512 passed.
Known-answer test for AES passed.
Known-answer test for RSA(signature/verification) passed.
Pairwise conditional test for RSA(signature/verification) passed.
```

Pairwise conditional test for RSA(encrypt/decrypt) passed.
Pairwise conditional test for DSA(signature/verification) passed.
Pairwise conditional test for ECDSA(signature/verification) passed.
Known-answer test for ECDH passed.
Known-answer test for random number generator(x931) passed.
Known-answer test for DRBG passed.
Known-Answer tests in the user space passed.
Starting Known-Answer tests in the kernel.
Known-answer test for 3DES passed.
Known-answer test for AES passed.
Known-answer test for HMAC-SHA1 passed.
Known-answer test for HMAC-SHA256 passed.
Known-answer test for HMAC-SHA384 passed.
Known-answer test for HMAC-SHA512 passed.
Known-answer test for SHA1 passed.
Known-answer test for SHA256 passed.
Known-answer test for SHA384 passed.
Known-answer test for SHA512 passed.
Known-answer test for GCM passed.
Known-answer test for GMAC passed.
Known-Answer tests in the kernel passed.
Cryptographic Algorithms Known-Answer Tests passed.

目 录

1 802.1X Client.....	1-1
1.1 802.1X Client功能配置命令.....	1-1
1.1.1 display dot1x supplicant	1-1
1.1.2 dot1x supplicant anonymous identify.....	1-2
1.1.3 dot1x supplicant eap-method.....	1-3
1.1.4 dot1x supplicant enable	1-4
1.1.5 dot1x supplicant mac-address	1-4
1.1.6 dot1x supplicant password.....	1-5
1.1.7 dot1x supplicant ssl-client-policy	1-6
1.1.8 dot1x supplicant transmit-mode	1-7
1.1.9 dot1x supplicant username	1-7

1 802.1X Client

1.1 802.1X Client功能配置命令

1.1.1 display dot1x supplicant

display dot1x supplicant 命令用来显示 802.1X Client 认证信息。

【命令】

display dot1x supplicant [**interface** *interface-type interface-number*]

【视图】

任意视图

【缺省用户角色】

network-admin
network-operator

【参数】

interface interface-type interface-number: 表示显示指定接口上的 802.1X Client 认证信息。*interface-type interface-number* 为接口类型和接口编号。如果不指定本参数，则表示显示所有接口上的 802.1X Client 认证信息。

【举例】

显示接口 GigabitEthernet1/0/1 下 802.1X Client 认证信息。
<Sysname> display dot1x supplicant interface gigabitethernet 1/0/1
GigabitEthernet1/0/1
 Username : aaa
 EAP method : PEAP-MSCHAPv2
 Dot1x supplicant : Enabled
 Anonymous identifier : bbb
 SSL client policy : policy_1
 FSM state : Init
 EAPOL-Start packets : 0

表1-1 display dot1x supplicant interface 命令显示信息描述表

字段	描述
Username	用户名
EAP method	认证类型，包括以下取值： <ul style="list-style-type: none">• MD5• PEAP-GTC• PEAP-MSCHAPv2• TTLS-GTC• TTLS-MSCHAPv2

字段	描述
Dot1x supplicant	802.1X Client功能所处状态： <ul style="list-style-type: none"> • Enabled: 开启状态 • Disabled: 关闭状态
Anonymous identifier	匿名认证用户名
SSL client policy	802.1X Client引用的SSL客户端策略
FSM state	802.1X Client认证状态，包括以下取值： <ul style="list-style-type: none"> • Init: 初始状态 • Connecting: 正在连接状态 • Authenticating: 正在认证状态 • Authenticated: 认证成功状态 • Held: 静默状态
EAPOL-Start packets	发送的EAPOL-Start报文个数

1.1.2 dot1x supplicant anonymous identify

dot1x supplicant anonymous identify 命令用来配置 802.1X Client 匿名认证用户名。

undo dot1x supplicant anonymous identify 命令用来恢复缺省情况。

【命令】

```
dot1x supplicant anonymous identify identifier
undo dot1x supplicant anonymous identify
```

【缺省情况】

不存在 802.1X Client 匿名认证用户名。

【视图】

以太网接口视图

【缺省用户角色】

network-admin

【参数】

identifier: 表示 802.1X Client 匿名认证用户名，为 1~253 个字符的字符串，区分大小写。

【使用指导】

仅在采用 PEAP-MSCHAPv2、PEAP-GTC、TTLS-MSCHAPv2 和 TTLS-GTC 认证方法时，才需要配置匿名认证用户名。802.1X Client 在第一阶段的认证过程中，优先发送匿名认证用户名，而在第二阶段将在被加密的报文中发送配置的认证用户名。配置了 802.1X Client 匿名认证用户名可有效保护认证用户名不在第一阶段的认证过程中被泄露。如果设备上没有配置匿名认证用户名，则两个认证阶段均使用配置的认证用户名进行认证。

当 802.1X Client 采用的认证方法为 MD5-Challenge 时，配置的 802.1X Client 匿名认证用户名无效，设备仍将使用配置的认证用户名进行认证。

如果认证服务器厂商不支持匿名认证用户名，则不要配置匿名认证用户名。

【举例】

配置 802.1X Client 匿名认证用户名为 bbb。

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] dot1x supplicant anonymous identify bbb
```

【相关命令】

- **display dot1x supplicant**
- **dot1x supplicant enable**
- **dot1x supplicant username**

1.1.3 dot1x supplicant eap-method

dot1x supplicant eap-method 命令用来配置 802.1X Client 采用的 EAP 认证方法。

undo dot1x supplicant eap-method 命令用来恢复缺省情况。

【命令】

```
dot1x supplicant eap-method { md5 | peap-gtc | peap-mschapv2 | ttls-gtc |
ttls-mschapv2 }
undo dot1x supplicant eap-method
```

【缺省情况】

802.1X Client 采用的 EAP 认证方法为 MD5-Challenge。

【视图】

以太网接口视图

【缺省用户角色】

network-admin

【参数】

md5：表示采用的认证方法为 MD5-Challenge。

peap-gtc：表示采用的认证方法为 PEAP-GTC。

peap-mschapv2：表示采用的认证方法为 PEAP-MSCHAPv2。

ttls-gtc：表示采用的认证方法为 TTLS-GTC。

ttls-mschapv2：表示采用的认证方法为 TTLS-MSCHAPv2。

【使用指导】

配置的 802.1X Client 认证方法必须和认证服务器端支持的 EAP 认证方法保持一致。

【举例】

配置 802.1X Client 采用的认证方法为 PEAP-GTC。

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] dot1x supplicant eap-method peap-gtc
```

【相关命令】

- `display dot1x supplicant`
- `dot1x supplicant enable`

1.1.4 dot1x supplicant enable

`dot1x supplicant enable` 命令用来开启 802.1X Client 功能。

`undo dot1x supplicant enable` 命令用来关闭 802.1X Client 功能。

【命令】

```
dot1x supplicant enable
undo dot1x supplicant enable
```

【缺省情况】

802.1X Client 功能处于关闭状态。

【视图】

以太网接口视图

【缺省用户角色】

network-admin

【使用指导】

开启 802.1X Client 功能前，请确保设备（Authenticator）上关于 802.1X 认证的配置已完成。

【举例】

```
# 开启 802.1X Client 功能。
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] dot1x supplicant enable
```

【相关命令】

- `display dot1x supplicant`

1.1.5 dot1x supplicant mac-address

`dot1x supplicant mac-address` 命令用来配置 802.1X Client 认证使用的 MAC 地址。

`undo dot1x supplicant mac-address` 命令用来恢复缺省情况。

【命令】

```
dot1x supplicant mac-address mac-address
undo dot1x supplicant mac-address
```

【缺省情况】

802.1X Client 认证使用接口的 MAC 地址，若获取不到接口 MAC 地址则使用设备的 MAC 地址。

【视图】

以太网接口视图

【缺省用户角色】

network-admin

【参数】

mac-address: MAC 地址，格式为 H-H-H，不支持组播 MAC 地址、全 0 的 MAC 地址和全 F 的 MAC 地址。输入本参数时，可以省去 MAC 地址中每段开头的“0”，例如输入“f-e2-1”即表示输入“000f-00e2-0001”。

【使用指导】

设备作为 802.1X Client 时，为了保证各接口能够顺利通过 802.1X 认证，需要为各接口上配置不同的 MAC 地址。可通过以太网接口视图下的 **mac-address** 命令为接口配置不同的 MAC 地址，或通过本命令为以太网接口配置不同的 802.1X Client 认证使用的 MAC 地址。

【举例】

配置 802.1X Client 认证使用的 MAC 地址为 0001-0001-0001。

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] dot1x supplicant mac-address 1-1-1
```

1.1.6 dot1x supplicant password

dot1x supplicant password 命令用来配置 802.1X Client 认证密码。

undo dot1x supplicant password 命令用来恢复缺省情况。

【命令】

```
dot1x supplicant password { cipher | simple } string
undo dot1x supplicant password
```

【缺省情况】

不存在 802.1X Client 认证密码。

【视图】

以太网接口视图

【缺省用户角色】

network-admin

【参数】

cipher: 以密文方式设置密码。

simple: 以明文方式设置密码，该密码将以密文形式存储。

string: 密码字符串，区分大小写。明文密码为 1~127 个字符的字符串，密文密码为 1~201 个字符的字符串。

【举例】

配置 802.1X Client 的明文认证密码为 123456。

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] dot1x supplicant password simple 123456
```

【相关命令】

- `display dot1x supplicant`
- `dot1x supplicant enable`

1.1.7 dot1x supplicant ssl-client-policy

`dot1x supplicant ssl-client-policy` 命令用来指定 802.1X Client 引用的 SSL 客户端策略。

`undo dot1x supplicant ssl-client-policy` 命令用来恢复缺省情况。

【命令】

```
dot1x supplicant ssl-client-policy policy-name  
undo dot1x supplicant ssl-client-policy policy-name
```

【缺省情况】

802.1X Client 引用系统缺省的 SSL 客户端策略。

【视图】

以太网接口视图

【缺省用户角色】

network-admin

【参数】

policy-name: SSL 客户端策略名，为 1~31 个字符的字符串，不区分大小写，且引用的 SSL 客户端策略必须已存在。

【使用指导】

当 802.1X Client 认证采用 PEAP-MSCHAPv2、PEAP-GTC、TTLS-MSCHAPv2 或 TTLS-GTC 时，被认证设备作为 SSL 客户端会在 802.1X Client 第一阶段认证过程中，与对端 SSL 服务器进行 SSL 协商。在第二阶段被认证设备使用 SSL 协商出来的结果对交互的认证报文进行加密传输。

在 SSL 协商过程中，802.1X Client 作为 SSL 客户端连接 SSL 服务器时，需要使用本命令来引用 SSL 客户端策略。SSL 客户端策略中配置了 SSL 客户端启动时使用的 SSL 参数，包括使用的 PKI 域、支持的加密套件和使用的 SSL 协议版本。有关 SSL 客户端策略的详细配置请参见“安全配置指导”中的“SSL”。

当 802.1X Client 认证采用 MD5-Challenge 认证方法时，认证过程不会引用 SSL 客户端策略。

【举例】

在接口 GigabitEthernet1/0/1 下指定 802.1X Client 引用的 SSL 客户端策略为 policy_1。

```
<Sysname> system-view  
[Sysname] interface gigabitethernet 1/0/1  
[Sysname-GigabitEthernet1/0/1] dot1x supplicant ssl-client-policy policy_1
```

【相关命令】

- `display dot1x supplicant`
- `dot1x supplicant enable`

- **ssl client-policy** (安全命令参考/SSL)

1.1.8 dot1x supplicant transmit-mode

dot1x supplicant transmit-mode 命令用来配置 802.1X Client 认证使用的报文发送方式。

undo dot1x supplicant transmit-mode 命令用来恢复缺省情况。

【命令】

```
dot1x supplicant transmit-mode { multicast | unicast }  
undo dot1x supplicant transmit-mode
```

【缺省情况】

802.1X Client 认证使用单播方式发送 EAP-Response 和 EAPOL-Logoff 报文。

【视图】

以太网接口视图

【缺省用户角色】

network-admin

【参数】

multicast: 使用组播方式发送 EAP-Response 和 EAPOL-Logoff 报文，该报文目的地址为组播 MAC 地址 01-80-C2-00-00-03。

unicast: 使用单播方式发送 EAP-Response 和 EAPOL-Logoff 报文。

【使用指导】

设备作为 802.1X Client 进行 802.1X 认证时，如果网络中的 NAS 设备不支持接收单播 EAP-Response 或 EAPOL-Logoff 报文，会导致 802.1X 认证失败，此时建议开启组播发送方式。

【举例】

```
# 配置端口 GigabitEthernet1/0/1 上 802.1X Client 认证使用的报文类型为组播。  
<Sysname> system-view  
[Sysname] interface gigabitethernet 1/0/1  
[Sysname-GigabitEthernet1/0/1] dot1x supplicant transmit-mode multicast
```

1.1.9 dot1x supplicant username

dot1x supplicant username 命令用来配置 802.1X Client 认证用户名。

undo dot1x supplicant username 命令用来恢复缺省情况。

【命令】

```
dot1x supplicant username username  
undo dot1x supplicant username
```

【缺省情况】

不存在 802.1X Client 认证用户名。

【视图】

以太网接口视图

【缺省用户角色】

network-admin

【参数】

username: 表示 802.1X Client 认证用户名，为 1~253 个字符的字符串，区分大小写。

【使用指导】

802.1X Client 认证用户名可以携带域名，域名中可用的分隔符包括@、\、/和.，对应的用户名格式分别为 *username@domain-name*、*domain-name\username*、*username/domain-name* 和 *username.domain-name*，其中 *username* 为纯用户名、*domain-name* 为域名。如果用户名中包含有多个域名分隔符字符，则设备仅将最后一个出现的域名分隔符识别为实际使用的域名分隔符。若要指定域名分隔符\，则必须在输入时使用转义操作符\\，即输入\\。域名分隔符的使用方法同命令 **dot1x domain-delimiter**，有关此命令的详细介绍请参见“安全命令参考”中的“802.1X”。

【举例】

配置 802.1X Client 认证用户名为 aaa。

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] dot1x supplicant username aaa
```

【相关命令】

- **display dot1x supplicant**
- **dot1x domain-delimiter**（安全命令参考/802.1X）
- **dot1x supplicant enable**