目 录

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

mdc-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。

【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

mdc-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

mdc-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

mdc-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 dual-stack

accounting dual-stack 命令用来配置双协议栈用户的计费方式。

undo accounting dual-stack 命令用来恢复缺省情况。

【命令】

accounting dual-stack { **merge** | **separate** }

undo accounting dual-stack

【缺省情况】

双协议栈用户的计费方式为统一计费。

【视图】

ISP 域视图

【缺省用户角色】

network-admin

mdc-admin

【参数】

merge：统一计费方式，表示将双协议栈用户的 IPv4 流量和 IPv6 流量统一汇总后上送给计费服务器。

separate：分别计费方式，表示将双协议栈用户的 IPv4 流量和 IPv6 流量分别上送给计费服务器。

【使用指导】

双协议栈用户的主机上同时支持 IPv4 和 IPv6 两种协议，可能产生两种协议类型的流量。分别计费模式通常应用于 IPv4 流量费率和 IPv6 流量费率不一样的情况；统一计费模式通常应用于不需要区分 IPv4 流量和 IPv6 流量的情况。

【举例】

在 ISP 域 test 下，配置双栈用户的计费方式为分别计费。

```
<Sysname> system-view
[Sysname] domain test
[Sysname-isp-test] accounting dual-stack separate
```

1.1.6 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**] [**none**] | **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

mdc-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**

1.1.7 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

mdc-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**

1.1.8 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

mdc-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**

1.1.9 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

mdc-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。

【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-domain-test] accounting quota-out online
```

1.1.10 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

mdc-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-domain-test] accounting start-fail online
```

1.1.11 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

mdc-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 isp1
[Sysname-isp-domain-isp1] accounting update-fail online
```

1.1.12 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

mdc-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**

1.1.13 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

mdc-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**

1.1.14 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

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

1.1.15 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

mdc-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 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**

1.1.16 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

mdc-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-domain-test] authentication super hwtacacs-scheme tac
```

【相关命令】

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

1.1.17 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

mdc-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行授权方法，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**

1.1.18 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

mdc-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）只有系统所给予的缺省用户角色，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。关于缺省用户角色的详细介绍请参见“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】

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

1.1.19 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

mdc-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**

1.1.20 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

mdc-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）只有系统所给予的缺省用户角色，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。关于缺省用户角色的详细介绍请参见“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**
- **hwtacacs scheme**
- **local-user**
- **radius scheme**

1.1.21 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

mdc-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**

1.1.22 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*] | **idle-cut** *minutes* [*flow*] [**traffic** { **both** | **inbound** | **outbound** }] | **igmp max-access-number** *max-access-number* | **ip-pool** *pool-name* | **ipv6-pool** *ipv6-pool-name* | **mld max-access-number** *max-access-number* | **url** *url-string* | **user-group** *user-group-name* }

undo authorization-attribute { **acl** | **car** | **idle-cut** | **igmp** | **ip-pool** | **ipv6-pool** | **mld** | **url** | **user-group** }

【缺省情况】

当前 ISP 域下的用户闲置切换功能处于关闭状态，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

mdc-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 2000～5999。用户认证成功后，将仅被授权访问符合指定 ACL 规则的网络资源。Portal 用户在认证前，若被授权认证域，则将被授权访问符合指定 ACL 规则网络资源。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。

idle-cut *minutes*：指定用户的闲置切断时间。其中，*minutes* 的取值范围为 1～600，单位为分钟。此属性只对 Portal 用户生效。

flow：用户在闲置切断时间内产生的数据流量，取值范围 1～10240000，单位为字节，缺省值为 10240。

traffic：指定闲置切断时间内用户数据流量的统计方向。若不指定该参数，则表示统计用户双向数据流量。

- **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。

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 *pool-name*：指定为用户分配 IPv4 地址的地址池。其中，*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*：指定用户的强制 URL，为 1～255 个字符的字符串，区分大小写。用户认证成功后，此 URL 将被推送至客户端。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。

【使用指导】

用户上线后，设备会周期性检测用户的流量，若域内某用户在指定的闲置检测时间内产生的流量小于本命令中指定的数据流量，则会被强制下线。需要注意的是，服务器上也可以配置最大空闲时间实现对用户的闲置切断功能，具体为当用户在指定的闲置检测时间内产生的流量小于 10240 个字节（服务器上该阈值为固定值，不可配置）时，会被强制下线。但是，只有在设备上的闲置切断功能处于关闭状态时，服务器才会根据自身的配置来控制用户的闲置切断。

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。

【举例】

指定 ISP 域 test 下的用户闲置切断时间为 30 分钟，闲置切断时间内产生的流量为 10240 字节。

```
<Sysname> system-view
[Sysname] domain test
[Sysname-isp-test] authorization-attribute idle-cut 30 10240
```

【相关命令】

- **display domain**

1.1.23 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

mdc-admin

mdc-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 : Enabled
      Idle timeout: 2 minutes
      Flow: 10240 bytes
      Traffic direction: Both
    IP pool: appy
    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://portal
    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
Domain	ISP域名
State	ISP域的状态

字段	描述
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： • 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： • 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： • 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
Service type	ISP域的业务类型，取值为HSI，STB和VoIP
Session time	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： • Include idle time：保留用户闲置切断时间（或 Portal

字段	描述
	用户在线探测间隔） • Exclude idle time：扣除用户闲置切断时间（或 Portal 用户在线探测间隔）
Dual-stack accounting method	双协议栈用户的计费方式，包括以下取值： • 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	用户闲置切断功能，包括以下取值： • 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	用户数据流量的统计方向，包括以下取值： • 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
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	授权强制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

1.1.24 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

mdc-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”、“defaul”、“default”、“i”、“if”、“if-”、“if-u”、“if-un”、“if-unk”、“if-unkn”、“if-unkno”、“if-unknow”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)

1.1.25 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

mdc-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**

1.1.26 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-domain-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

mdc-admin

【参数】

isp-domain-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”、“defaul”、“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**

1.1.27 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

mdc-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**

1.1.28 service-type (ISP domain view)

service-type 命令用来设置当前 ISP 域的业务类型。

undo service-type 命令用来恢复缺省情况。

【命令】

service-type { **hsi** | **stb** | **voip** }

undo service-type

【缺省情况】

当前 ISP 域的业务类型为 **hsi**。

【视图】

ISP 域视图

【缺省用户角色】

network-admin

mdc-admin

【参数】

hsi：表示 HSI（High Speed Internet，高速上网）业务，主要指使用 802.1X 方式接入网络的用户业务。

stb：表示 STB（Set Top Box，机顶盒）业务，专指使用数字机顶盒接入网络的用户业务。

voip：表示（Voice over IP，IP 电话）业务，指使用 IP 电话的用户业务。

【使用指导】

本命令用来配置当前认证域的用户使用的业务类型，用来决定接入模块是否开启组播功能。

用户使用 HSI 业务类型的 ISP 域接入时，接入模块不会开启组播功能，可节省系统资源。

用户使用 STB 业务类型的 ISP 域接入时，接入模块会开启组播功能，可提高系统处理组播业务的性能。

用户使用 VoIP 业务类型的 ISP 域接入时，QoS 功能会开启保证用户语音数据的低延迟传送。

对于 802.1X 用户，ISP 域中配置的业务类型无效，系统强制使用 HSI 业务类型。

一个 ISP 域中，仅能配置一种类型的业务类型。

【举例】

设置域 test 下用户业务类型为 STB 终端业务。

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

1.1.29 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

mdc-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**

1.1.30 user-address-type

user-address-type 命令用来设置当前 ISP 域的用户地址类型。

undo user-address-type 命令用来恢复缺省情况。

【命令】

user-address-type { **ds-lite** | **ipv6** | **nat64** | **private-ds** | **private-ipv4** | **public-ds** | **public-ipv4** }

undo user-address-type

【缺省情况】

未指定当前 ISP 域的用户地址类型。

【视图】

ISP 域视图

【缺省用户角色】

network-admin

mdc-admin

【参数】

ds-lite：表示当前用户的地址类型为轻量级双栈地址。

ipv6：表示当前用户的地址类型为 IPv6 地址。

nat64：表示当前用户的地址类型为 NAT64 地址。

private-ds：表示当前用户的地址类型为私网双栈地址。

private-ipv4：表示当前用户的地址类型为私网 IPv4 地址。

public-ds：表示当前用户的地址类型为公网双栈地址。

public-ipv4：表示当前用户的地址类型为公网 IPv4 地址。

【使用指导】

当更改当前 ISP 域的用户地址类型时，不影响已经在线的用户。

【举例】

设置当前 ISP 域用户地址类型为私网 IPv4 地址。

```
<Sysname> system-view
[Sysname] domain test
[Sysname-isp-test] user-address-type private-ipv4
```

【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

mdc-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。

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】

- **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*| **url** *url-string* | **user-role** *role-name* | **vlan** *vlan-id* | **work-directory** *directory-name* } *

undo authorization-attribute { **acl** | **idle-cut** | **ip-pool** | **ipv6-pool** | **session-timeout** | **url** | **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。

在缺省 MDC 中由用户角色为 network-admin 或者 level-15 的用户创建的本地用户被授权用户角色 network-operator；在非缺省 MDC 中由用户角色为 mdc-admin 或者 level-15 的用户创建的本地用户被授权用户角色 mdc-operator。

【视图】

本地用户视图

用户组视图

【缺省用户角色】

network-admin

mdc-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 2000～5999。本地用户认证成功后，将被授权仅可以访问符合指定 ACL 规则的网络资源。

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。

url *url-string*：指定本地用户的强制 URL，为 1～255 个字符的字符串，区分大小写。用户认证成功后，此 URL 将被推送至客户端。

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 **acl**、**idle-cut**、**ip-pool**、**ipv6-pool**、**session-timeout** 有效。
- 对于 Lan-access 用户，仅授权属性 **acl**、**session-timeout**、**vlan**、**url** 有效。
- 对于 Telnet、Terminal 用户，仅授权属性 **idle-cut**、**user-role**、**work-directory** 有效。
- 对于 http、https 用户，仅授权属性 **user-role** 有效。

- 对于 SSH、FTP 用户，仅授权属性 **idle-cut**、**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。

为了避免设备上进行主备倒换后 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槽位信息。

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

mdc-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。
- 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 IP 为 3.3.3.3。

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

```
[Sysname] local-user abc class network
[Sysname-luser-network-abc] bind-attribute ip 3.3.3.3
```

【相关命令】

- **display local-user**

1.2.4 company

company 命令用来配置本地来宾用户所属公司。

undo company 命令用来恢复缺省情况。

【命令】

company *company-name*

undo company

【缺省情况】

未配置本地来宾用户所属公司。

【视图】

本地来宾用户视图

【缺省用户角色】

network-admin

mdc-admin

【参数】

company-name：本地来宾用户所属公司名称，为 1～255 个字符的字符串，区分大小写。

【举例】

配置本地来宾用户 abc 所属的公司名称为 yyy。

```
<Sysname> system-view
[Sysname] local-user abc class network guest
[Sysname-luser-network(guest)-abc] company yyy
```

【相关命令】

- **display local-user**

1.2.5 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

mdc-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**

1.2.6 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** [**guest**] } | **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** [**guest**] } | **vlan** *vlan-id*]

【视图】

任意视图

【缺省用户角色】

network-admin

network-operator

mdc-admin

mdc-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。

guest：来宾用户。

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:           Ten-GigabitEthernet1/0/1
    MAC address:              0001-0001-0001
    VLAN ID:                  2
  Authorization attributes:
```

```
    Idle timeout:             33 minutes
    Work directory:           flash:
    ACL number:               2000
  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

 Network access guest user1:
  State:                      Active
  Service type:               LAN-access/Portal
  User group:                 guest1
  Full name:                  Jack
  Company:                    cc
  Email:                      Jack@cc.com
  Phone:                      131129237
  Sponsor full name:          Sam
  Sponsor department:         security
  Sponsor email:              Sam@aa.com
  Description:                A guest from company cc
  Validity period:
    Start date and time:      2016/04/01-08:00:00
    Expiration date and time: 2017/04/03-18:00:00

Total 3 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 • 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

字段	描述
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 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
URL	本地用户的授权强制URL
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
Full name	本地来宾用户的姓名
Company	本地来宾用户的公司
Email	本地来宾用户的Email地址
Phone	本地来宾用户的电话号码
Sponsor full name	本地来宾用户接待人的姓名
Sponsor department	本地来宾用户接待人所属部门
Sponsor email	本地来宾用户接待人的Email地址
Description	网络接入类本地用户的描述信息
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 3 local users matched.	总计有3个本地用户匹配

1.2.7 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

mdc-admin

mdc-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
  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

字段	描述
VLAN ID	授权VLAN ID
IP pool	授权IPv4地址池
IPv6 pool	授权IPv6地址池
URL	授权强制URL
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

1.2.8 email

email 命令用来配置本地来宾用户的 Email 地址。

undo email 命令用来恢复缺省情况。

【命令】

email *email-string*

undo email

【缺省情况】

未配置本地来宾用户的 Email 地址。

【视图】

本地来宾用户视图

【缺省用户角色】

network-admin

mdc-admin

【参数】

email-string：本地来宾用户的 Email 地址，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。

【使用指导】

设备可以通过本命令配置的 Email 地址给来宾用户发送通知邮件。

【举例】

配置本地来宾用户 abc 的 Email 地址为 abc@yyy.com。

```
<Sysname> system-view
[Sysname] local-user abc class network guest
[Sysname-luser-network(guest)-abc] email abc@yyy.com
```

【相关命令】

- **display local-user**

1.2.9 full-name

full-name 命令用来配置本地来宾用户的姓名。

undo full-name 命令用来恢复缺省情况。

【命令】

full-name *name-string*

undo full-name

【缺省情况】

未配置本地来宾用户的姓名。

【视图】

本地来宾用户视图

【缺省用户角色】

network-admin

mdc-admin

【参数】

name-string：本地来宾用户的姓名，为 1～255 个字符的字符串，区分大小写。

【举例】

配置本地来宾用户 abc 的姓名为 abc Snow。

```
<Sysname> system-view
[Sysname] local-user abc class network guest
[Sysname-luser-network(guest)-abc] full-name abc Snow
```

【相关命令】

- **display local-user**

1.2.10 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

mdc-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**

1.2.11 local-guest email format

local-guest email format 命令用来配置本地来宾用户通知邮件的主题和内容。

undo local-guest email format 命令用来删除指定的本地来宾用户通知邮件的主题和内容。

【命令】

local-guest email format to { **guest** | **sponsor** } { **body** *body-string* | **subject** *sub-string* }

undo local-guest email format to { **guest** | **sponsor** } { **body** | **subject** }

【缺省情况】

未配置本地来宾用户通知邮件的主题和内容。

【视图】

系统视图

【缺省用户角色】

network-admin

mdc-admin

【参数】

to：指定邮件的收件人。

- **guest**：表示来宾用户。

- **sponsor**：表示来宾接待人。

body *body-string*：邮件的内容。其中，*body-string* 为 1～255 个字符的字符串，区分大小写。

subject *sub-string*：邮件的主题。其中，*sub-string* 为 1～127 个字符的字符串，区分大小写。

【使用指导】

在本地来宾用户创建过程中，设备需要向不同角色的用户发送通知邮件，邮件的主题和内容通过本命令设置。

可对不同的收件人指定不同的邮件主题和内容。同一类收件人的邮件格式只能存在一种配置，新配置将覆盖已有配置。

必须同时配置收件人的邮件主题和内容，否则设备不会给该收件人发送邮件。

【举例】

配置本地来宾用户通知邮件的主题和内容。

```
<Sysname> system-view
[Sysname] local-guest email format to guest subject Guest account information
[Sysname] local-guest email format to guest body A guest account has been created for you.
The username, password, and validity period of the account are given below.
```

【相关命令】

- **local-guest email sender**
- **local-guest email smtp-server**
- **local-guest send-email**

1.2.12 local-guest email sender

local-guest email sender 命令用来配置本地来宾用户通知邮件的发件人地址。

undo local-guest email sender 命令用来恢复缺省情况。

【命令】

local-guest email sender *email-address*

undo local-guest email sender

【缺省情况】

未配置本地来宾用户通知邮件的发件人地址。

【视图】

系统视图

【缺省用户角色】

network-admin

mdc-admin

【参数】

email-address：邮件发件人地址，为 1～255 个字符的字符串，区分大小写。

【使用指导】

未配置发件人地址的情况下，设备无法向任何收件人发送关于本地来宾用户的通知邮件。

只能存在一个本地来宾用户的发件人地址。多次执行本命令，最后一次执行的命令生效。

【举例】

配置本地来宾用户通知邮件的发件人地址为 abc@yyy.com。

```
<Sysname> system-view
[Sysname] local-guest email sender abc@yyy.com
```

【相关命令】

- **local-guest email format**
- **local-guest email smtp-server**
- **local-guest send-email**

1.2.13 local-guest email smtp-server

local-guest email smtp-server 命令用来配置为本地来宾用户发送 Email 使用的 SMTP 服务器。

undo local-guest send-email smtp-server 命令用来恢复缺省情况。

【命令】

local-guest email smtp-server *url-string*

undo local-guest email smtp-server

【缺省情况】

未配置为本地来宾用户发送 Email 使用的 SMTP 服务器。

【视图】

系统视图

【缺省用户角色】

network-admin

mdc-admin

【参数】

url-string：STMP 服务器的 URL，为 1～255 个字符的字符串，区分大小写，符合标准 SMTP 协议规范，以 smtp://开头。

【使用指导】

只能存在一个为本地来宾用户发送 Email 使用的 SMTP 服务器。多次执行本命令，最后一次执行的命令生效。

【举例】

配置为本地来宾用户发送 Email 使用的 SMTP 服务器 URL 为 smtp://www.test.com/smtp。

```
<Sysname> system-view
[Sysname] local-guest email smtp-server smtp://www.test.com/smtp
```

【相关命令】

- **local-guest email format**

- **local-guest email sender**
- **local-guest send-email**

1.2.14 local-guest generate

local-guest generate 命令用来批量创建本地来宾用户。

【命令】

local-guest generate username-prefix *name-prefix* [**password-prefix** *password-prefix*] **suffix** *suffix-number* [**group** *group-name*] **count** *user-count* **validity-datetime** *start-date start-time* **to** *expiration-date expiration-time*

【视图】

系统视图

【缺省用户角色】

network-admin

mdc-admin

【参数】

username-prefix *name-prefix*：用户名前缀，*name-prefix* 为 1～45 个字符的字符串，区分大小写，不能含有字符\、|、/、:、*、?、<、>或@。

password-prefix *password-prefix*：明文密码前缀，*password-prefix* 为 1～53 个字符的字符串，区分大小写。若不指定该参数，则由系统为用户逐一生成随机密码

suffix *suffix-string*：用户名和密码的递增编号后缀，*suffix-string* 为 1～10 个数字的字符串。

group *group-name*：用户所属用户组名，*group-name* 为 1～32 个字符的字符串，区分大小写。若不指定该参数，则表示用户属于 system 组。

count *user-count*：批量创建用户的数量，*user-count* 的取值范围为 1～256。

validity-datetime：用户有效期。

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。

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】

批量创建的本地来宾用户名由指定的用户名前缀和编号后缀组合而成，且每创建一个用户，用户名编号后缀递增 1。例如，当用户名前缀为 abc，递增编号后缀为 1，生成用户数量为 3 时，生成的用户名分别为 abc1、abc2 和 abc3。如果指定了密码前缀，则批量创建的本地来宾用户密码由密码前缀和编号后缀组合而成，且逐用户递增。

如果申请创建的本地来宾用户数量过多，导致资源不足时，部分本地来宾用户的批量创建将会失败。

如果批量创建的本地来宾用户与设备上已有的本地来宾用户重名，则批量创建的用户会覆盖已有的同名用户。

【举例】

批量创建 20 个本地来宾用户，用户名从 abc01 递增到 abc20，属于用户组 visit，有效期为 2014/10/01 00:00:00 到 2015/10/02 12:00:00。

```
<Sysname> system-view
[Sysname] local-guest generate username-prefix abc suffix 01 group visit count 20
validity-datetime 2014/10/01 00:00:00 to 2015/10/02 12:00:00
```

【相关命令】

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

1.2.15 local-guest send-email

local-guest send-email 命令用来配置向本地来宾用户邮箱和来宾接待人邮箱发送邮件。

【命令】

local-guest send-email user-name *user-name* **to** { **guest** | **sponsor** }

【视图】

用户视图

【缺省用户角色】

network-admin

mdc-admin

【参数】

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

to：指定邮件的收件人。

- **guest**：本地来宾用户。
- **sponsor**：来宾接待人。

【使用指导】

当本地来宾用户创建之后，设备管理员可通过此命令将用户的密码及有效期信息发送到本地来宾用户或来宾接待人邮箱中。

【举例】

向本地来宾用户 abc 的邮箱发送有关该用户帐号信息的通知邮件。

```
<Sysname> local-guest send-email user-name abc to guest
```

【相关命令】

- **email**
- **sponsor-email**

1.2.16 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** [**guest**] }]

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

【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

mdc-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。

guest：来宾用户，仅能在帐户有效期内提供 **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]
```

添加名称为 user3 的网络接入类本地来宾用户。

```
<Sysname> system-view
[Sysname] local-user user3 class network guest
[Sysname-luser-network(guest)-user3]
```

【相关命令】

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

1.2.17 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

mdc-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**

1.2.18 local-user-export

local-user-export 命令用来从设备导出本地来宾用户信息到指定路径的 CSV 文件。

【命令】

local-user-export class network guest url *url-string*

【视图】

系统视图

【缺省用户角色】

network-admin

mdc-admin

【参数】

class：指定本地用户的类别。

network：网络接入类用户。

guest：本地来宾用户。

url *url-string*：保存本地用户信息文件的 URL，为 1～255 个字符的字符串，不区分大小写。

【使用指导】

导出的 CSV 文件可直接或在编辑之后通过 **local-user-import** 命令导入到本设备或其它支持该命令的设备上使用，但文件内容必须符合该命令的要求。

本命令支持 TFTP 和 FTP 两种文件上传方式，具体的 URL 格式要求如下：

- TFTP 协议 URL 格式：tftp://*server*/*path*/*filename*，*server* 为 TFTP 服务器 IP 地址或主机名，例如 tftp://1.1.1.1/user/user.csv。
- FTP 协议 URL 格式：
  - 携带用户名和密码的格式为 ftp://*username*:*password*@*server*/*path*/*filename*。其中，*username* 为 FTP 用户名，*password* 为 FTP 认证密码，*server* 为 FTP 服务器 IP 地址或主机名，例如 ftp://1:1@1.1.1.1/user/user.csv。如果 FTP 用户名中携带域名，则该域名会被设备忽略，例如 ftp://1@abc:1@1.1.1.1/user/user.csv 将被当作 ftp://1:1@1.1.1.1/user/user.csv 处理。
  - 不需要携带用户名和密码的格式为 ftp://*server*/*path*/*filename*，例如 ftp://1.1.1.1/user/user.csv。

【举例】

导出本地来宾用户信息到 ftp://1.1.1.1/user/路径的 guest.csv 文件中。

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

```
[Sysname] local-user-export class network guest url ftp://1.1.1.1/user/guest.csv
```

【相关命令】

- **local-user-import**

1.2.19 local-user-import

local-user-import 命令用来从指定路径的文件中导入用户信息并创建本地用户。

【命令】

local-user-import class network guest url *url-string* **validity-datetime** *start-date start-time* **to** *expiration-date expiration-time* [**auto-create-group** | **override** | **start-line** *line-number*] *

【视图】

系统视图

【缺省用户角色】

network-admin

mdc-admin

【参数】

class：指定本地用户的类别。

network：网络接入类用户。

guest：本地来宾用户。

url *url-string*：要导入用户信息文件的 URL。其中，*url-string* 为 1～255 个字符的字符串，不区分大小写。

validity-datetime：指定用户的有效期。

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。

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。

auto-create-group：表示当设备上不存在用户所属的用户组时，系统会自动创建用户组，并将用户加入该用户组。若不指定该参数，则表示当设备上不存在用户所属的用户组时，系统不会创建对应的用户组，而是将该用户加入缺省用户组 system。

override：表示当导入的用户名已经存在于设备上时，系统使用导入的用户信息覆盖掉已有的同名用户配置。若不指定该参数，则表示不导入文件中的同名用户信息，即保留设备上已有的同名用户配置。

start-line *line-number*：表示从文件的指定行开始导入用户信息。其中，*line-number* 为文件内容的行编号。若不指定该参数，则表示导入文件中的所有用户信息。

【使用指导】

用于导入的 CSV 文件中包含多个用户信息，每个用户的各项字段严格按照以下顺序出现：

- Username：用户名。该字段必须存在。
- Password：明文用户密码。若该字段为空，则导入时系统会生成一个密文随机密码。
- User group：所属用户组，用于本地授权。若该字段为空，则表示属于 system 组。
- Guest full name：来宾用户姓名。
- Guest company：来宾用户公司。
- Guest email：来宾用户 Email 地址。
- Guest phone：来宾用户电话号码。
- Guest description：来宾用户描述信息。
- Sponsor full name：接待人姓名。
- Sponsor department：接待人部门。
- Sponsor email：接待人 Email 地址。

以上所有字段的取值必须满足设备上本地用户相应属性的取值要求，否则当前用户的导入操作将会失败，且导入操作中止。之后，可以根据系统提示信息中的出错行编号选择下次从指定行开始导入剩余用户信息。

CSV 文件中的不同用户信息之间用回车换行分隔，且每项信息之间以逗号分隔。如果某项信息中包含逗号，则必须在该条信息两端加双引号。例如：Jack,abc,visit,Jack Chen,ETP,jack@etp.com,1399899,”The manager of ETP, come from TP.”,Sam Wang,Ministry of personnel,Sam@yy.com

本命令支持 TFTP 和 FTP 两种文件下载方式，具体的文件 URL 格式要求如下：

- TFTP 协议 URL 格式：tftp://server/path/filename，server 为 TFTP 服务器 IP 地址或主机名，例如 tftp://1.1.1.1/user/user.csv。
- FTP 协议 URL 格式：
  - 携带用户名和密码的格式为 ftp://username:password@server/path/filename。其中，username 为 FTP 用户名，password 为 FTP 认证密码，server 为 FTP 服务器 IP 地址或主机名，例如 ftp://1:1@1.1.1.1/user/user.csv。如果 FTP 用户名中携带域名，则该域名会被设备忽略，例如 ftp://1@abc:1@1.1.1.1/user/user.csv 将被当作 ftp://1:1@1.1.1.1/user/user.csv 处理。
  - 不需要携带用户名和密码的格式为 ftp://path/filename，例如 ftp://1.1.1.1/user/user.csv。

【举例】

从 ftp://1.1.1.1/user/guest.csv 路径中导入本地来宾用户信息，用户的有效期为 2014/10/01 00:00:00 到 2014/10/02 12:00:00。

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

```
[Sysname] local-user-import class network guest url ftp://1.1.1.1/user/guest.csv
validity-datetime 2014/10/01 00:00:00 to 2014/10/02 12:00:00
```

【相关命令】

- **local-user-export**
- **display local-user**

1.2.20 password

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】

对于网络接入类本地用户：

password { **cipher** | **simple** } *string*

undo password

对于设备管理类本地用户：

- 非 FIPS 模式下：

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

undo password

- FIPS 模式下：

password

【缺省情况】

对于网络接入类本地用户：

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。

对于设备管理类本地用户：

- 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】

本地用户视图/本地来宾用户视图

【缺省用户角色】

network-admin

mdc-admin

【参数】

cipher：表示以密文方式设置密码。

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；密文密码为 1～117 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。该方式仅设备管理类本地用户支持。

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，对于设备管理类本地用户，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 :
```

设置网络接入类本地用户 user2 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**

1.2.21 phone

phone 命令用来配置本地来宾用户的电话号码。

undo phone 命令用来恢复缺省情况。

【命令】

phone *phone-number*

undo phone

【缺省情况】

未配置本地来宾用户电话号码。

【视图】

本地来宾用户视图

【缺省用户角色】

network-admin

mdc-admin

【参数】

phone-number：本地来宾用户的电话号码，为 1～32 个字符的字符串，只能包含数字和-。

【举例】

配置本地来宾用户 abc 的电话号码为 138-137239201。

```
<Sysname> system-view
[Sysname] local-user abc class network guest
[Sysname-luser-network(guest)-abc] phone 138-137239201
```

【相关命令】

- **display local-user**

1.2.22 service-type (Local user view)

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

mdc-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**

1.2.23 sponsor-department

sponsor-department 命令用来配置本地来宾用户接待人所属部门。

undo sponsor-department 命令用来恢复缺省情况。

【命令】

sponsor-department *department-string*

undo sponsor-department

【缺省情况】

未配置本地来宾用户接待人所属部门。

【视图】

本地来宾用户视图

【缺省用户角色】

network-admin

mdc-admin

【参数】

department-string：本地来宾用户接待人所属部门名称，为 1～127 个字符的字符串，区分大小写。

【举例】

配置本地来宾用户 abc 的接待人所属部门为 test。

```
<Sysname> system-view
[Sysname] local-user abc class network guest
[Sysname-luser-network(guest)-abc] sponsor-department test
```

【相关命令】

- **display local-user**

1.2.24 sponsor-email

sponsor-email 命令用来配置本地来宾用户接待人的 Email 地址。

undo sponsor-email 命令用来恢复缺省情况。

【命令】

sponsor-email *email-string*

undo sponsor-email

【缺省情况】

未配置本地来宾用户接待人的 Email 地址。

【视图】

本地来宾用户视图

【缺省用户角色】

network-admin

mdc-admin

【参数】

email-string：本地来宾接待人的 Email 地址，为按照 RFC 822 定义的 1～255 个字符的字符串，区分大小写。

【举例】

配置本地来宾用户 abc 的接待人 Email 地址为 Sam@a.com。

```
<Sysname> system-view
[Sysname] local-user abc class network guest
[Sysname-luser-network(guest)-abc] sponsor-email Sam@a.com
```

【相关命令】

- **display local-user**

1.2.25 sponsor-full-name

sponsor-full-name 命令用来配置本地来宾用户的接待人姓名。

undo sponsor-full-name 命令用来恢复缺省情况。

【命令】

sponsor-full-name *name-string*

undo sponsor-full-name

【缺省情况】

未配置本地来宾用户的接待人姓名。

【视图】

本地来宾用户视图

【缺省用户角色】

network-admin

mdc-admin

【参数】

name-string：本地来宾用户接待人姓名，为 1～255 个字符的字符串，区分大小写。

【举例】

配置本地来宾用户 abc 的接待人姓名为 Sam Li。

```
<Sysname> system-view
[Sysname] local-user abc class network guest
[Sysname-luser-network(guest)-abc] sponsor-full-name Sam Li
```

【相关命令】

- **display local-user**

1.2.26 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/本地来宾用户视图

【缺省用户角色】

network-admin

mdc-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**

1.2.27 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

mdc-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**

1.2.28 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

mdc-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。

设备作为 RADIUS 服务器时使用 RADIUS 用户数据库对接入用户进行身份验证，RADIUS 用户数据由网络接入类本地用户配置直接生成，但设备仅关心 RADIUS 用户的有效期结束时间，不关心其有效期开始时间。

【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 debice-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

mdc-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

mdc-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

mdc-admin

mdc-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单板上。开启 accounting-on 扩展功能后，当用户接入的单板重启时（整机未重启），设备会向 RADIUS 服务器发送携带单板标识的 accounting-on 报文，用于通知 RADIUS 服务器对该单板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。开启 accounting-on 扩展功能后，请执行 **save** 命令保证 accounting-on 扩展功能在单板下次重启后生效。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

mdc-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

mdc-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

mdc-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

mdc-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

mdc-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**
- **display radius scheme**

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

mdc-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

mdc-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

mdc-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

mdc-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* | **vpn-instance** *vpn-instance-name*] *

undo client { **ip** *ipv4-address* | **ipv6** *ipv6-address* } [**vpn-instance** *vpn-instance-name*]

【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

mdc-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。

vpn-instance *vpn-instance-name*：RADIUS DAE 客户端所属的 VPN 实例。*vpn-instance-name* 表示 MPLS L3VPN 的 VPN 实例名称，为 1～31 个字符的字符串，区分大小写。如果未指定本参数，则表示 RADIUS DAE 客户端位于公网中。

【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

mdc-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 RADUIS 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

mdc-admin

mdc-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:
    IP   : 2.2.2.2                                  Port: 1812
    VPN  : vpn1
    State: Active
    Test profile: 132
      Probe username: test
```

```
    Probe interval: 60 minutes
  Weight: 40
 Primary accounting server:
  IP   : 1.1.1.1                                Port: 1813
  VPN  : Not configured
  State: Active
  Weight: 40
 Second authentication server:
  IP   : 3.3.3.3                                Port: 1812
  VPN  : Not configured
  State: Block
  Test profile: Not configured
  Weight: 40
 Second accounting server:
  IP   : 3.3.3.3                                Port: 1813
  VPN  : Not configured
  State: Block (Mandatory)
  Weight: 0
 Accounting-On function                    : Enabled
  extended function                        : Enabled
  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(minutes)     : 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
------------------------------------------------------------------------
```

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

字段	描述
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
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 • 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	RADIUS认证/计费服务器所在的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
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(minutes)	实时计费更新报文的发送间隔（单位为分钟）
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
VPN	RADIUS方案所属的VPN名称 未配置时，显示为Not configured
User Name Format	发送给RADIUS服务器的用户名格式 • with-domain：携带域名

字段	描述
	• 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： • 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： • 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 • 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

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

mdc-admin

mdc-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
Packet Without Response	无回应信息的报文数
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

mdc-admin

mdc-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
aaa        1000326232326010    abc         23:33:01-08/31/2015  20
```

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

mdc-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

mdc-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

mdc-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 { *ipv4-address* | **ipv6** *ipv6-address* } [*port-number* | **key** { **cipher** | **simple** } *string* | **vpn-instance** *vpn-instance-name* | **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

mdc-admin

【参数】

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。

vpn-instance *vpn-instance-name*：主 RADIUS 计费服务器所属的 VPN 实例。*vpn-instance-name* 表示 MPLS L3VPN 的 VPN 实例名称，为 1～31 个字符的字符串，区分大小写。如果未指定本参数，则表示主 RADIUS 计费服务器位于公网中。

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 IP 地址、端口号和 VPN 参数不能完全相同。

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。

若服务器位于 MPLS VPN 私网中，为保证 RADIUS 报文被发送到指定的私网服务器，必须指定服务器所属的 VPN 实例。本命令指定的服务器所属的 VPN 实例比 RADIUS 方案所属的 VPN 实例具有更高的优先级。

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**
- **vpn-instance** (RADIUS scheme view)

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 { *ipv4-address* | **ipv6** *ipv6-address* } [*port-number* | **key** { **cipher** | **simple** } *string* | **test-profile** *profile-name* | **vpn-instance** *vpn-instance-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

mdc-admin

【参数】

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。

vpn-instance *vpn-instance-name*：主 RADIUS 认证服务器所属的 VPN 实例。*vpn-instance-name* 表示 MPLS L3VPN 的 VPN 实例名称，为 1～31 个字符的字符串，区分大小写。如果未指定本参数，则表示主 RADIUS 认证服务器位于公网中。

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 IP 地址、端口号和 VPN 参数不能完全相同。

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 authenticaiton** 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。

若服务器位于 MPLS VPN 私网中，为保证 RADIUS 报文被发送到指定的私网服务器，必须指定服务器所属的 VPN 实例。本命令指定的服务器所属的 VPN 比 RADIUS 方案所属的 VPN 优先级高。

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**
- **vpn-instance** (RADIUS scheme view)

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

mdc-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**

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

mdc-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

mdc-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、或关闭/重启用户接入端口。

【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* } [**vpn-instance** *vpn-instance-name*]

undo radius nas-ip { *ipv4-address* | **ipv6** *ipv6-address* } [**vpn-instance** *vpn-instance-name*]

【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

mdc-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。

vpn-instance *vpn-instance-name*：指定私网源 IP 地址所属的 VPN 实例。*vpn-instance-name* 表示 MPLS L3VPN 的 VPN 实例名称，为 1～31 个字符的字符串，区分大小写。若不指定该参数，则表示配置的是公网源地址。

【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 16 个源地址。其中，最多包括一个 IPv4 公网源地址和一个 IPv6 公网源地址，其余为私网源地址。对于同一个 VPN，系统视图下最多允许指定一个 IPv4 私网源地址和一个 IPv6 私网源地址。

【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

mdc-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* | **vpn-instance** *vpn-instance-name*] *

undo radius session-control client { **all** | { **ip** *ipv4-address* | **ipv6** *ipv6-address* } [**vpn-instance** *vpn-instance-name*] }

【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

mdc-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。

vpn-instance *vpn-instance-name*：session control 客户端所属的 VPN 实例。*vpn-instance-name* 表示 MPLS L3VPN 的 VPN 实例名称，为 1～31 个字符的字符串，区分大小写。如果不指定本参数，则表示 session control 客户端属于公网。

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、VPN 属性与已有的 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

mdc-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* [**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

mdc-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。

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，探测报文的发送间隔为 10 分钟。

```
<Sysname> system-view
[Sysname] radius-server test-profile abc username admin 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

mdc-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

mdc-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 RAIUDS 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

mdc-admin

【参数】

retries：发送 RAIUDS 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 RAIUDS 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

mdc-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

mdc-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 { *ipv4-address* | **ipv6** *ipv6-address* } [*port-number* | **key** { **cipher** | **simple** } *string* | **vpn-instance** *vpn-instance-name* | **weight** *weight-value*] *

undo secondary accounting [{ *ipv4-address* | **ipv6** *ipv6-address* } [*port-number* | **vpn-instance** *vpn-instance-name*] *]

【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

mdc-admin

【参数】

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。

vpn-instance *vpn-instance-name*：从 RADIUS 计费服务器所属的 VPN 实例。*vpn-instance-name* 表示 MPLS L3VPN 的 VPN 实例名称，为 1～31 个字符的字符串，区分大小写。如果未指定本参数，则表示从 RADIUS 计费服务器位于公网中。

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 IP 地址、端口号和 VPN 参数不能完全相同，并且各从计费服务器的 IP 地址、端口号和 VPN 参数也不能完全相同。

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。

若服务器位于 MPLS VPN 私网中，为保证 RADIUS 报文被发送到指定的私网服务器，必须指定服务器所属的 VPN 实例。本命令指定的服务器所属的 VPN 比 RADIUS 方案所属的 VPN 优先级高。

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**
- **vpn-instance** (RADIUS scheme view)

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 { *ipv4-address* | **ipv6** *ipv6-address* } [*port-number* | **key** { **cipher** | **simple** } *string* | **test-profile** *profile-name* | **vpn-instance** *vpn-instance-name* | **weight** *weight-value*] *

undo secondary authentication [{ *ipv4-address* | **ipv6** *ipv6-address* } [*port-number* | **vpn-instance** *vpn-instance-name*] *]

【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

mdc-admin

【参数】

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。

vpn-instance *vpn-instance-name*：从 RADIUS 认证服务器所属的 VPN 实例。*vpn-instance-name* 表示 MPLS L3VPN 的 VPN 实例名称，为 1～31 个字符的字符串，区分大小写。如果未指定本参数，则表示从 RADIUS 认证服务器位于公网中。

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 IP 地址、端口号和 VPN 参数不能完全相同，并且各从认证服务器的 IP 地址、端口号和 VPN 参数也不能完全相同。

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。

若服务器位于 MPLS VPN 私网中，为保证 RADIUS 报文被发送到指定的私网服务器，必须指定服务器所属的 VPN 实例。本命令指定的服务器所属的 VPN 比 RADIUS 方案所属的 VPN 优先级高。

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**
- **vpn-instance** (RADIUS scheme view)

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

mdc-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

mdc-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

mdc-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** } [{ *ipv4-address* | **ipv6** *ipv6-address* } [*port-number* | **vpn-instance** *vpn-instance-name*] *] { **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

mdc-admin

【参数】

accounting：从 RADIUS 计费服务器。

authentication：从 RADIUS 认证服务器。

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。

vpn-instance *vpn-instance-name*：从 RADIUS 服务器所属的 VPN 实例。*vpn-instance-name* 表示 MPLS L3VPN 实例名称，为 1～31 个字符的字符串，区分大小写。

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

mdc-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 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

mdc-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**

1.3.44 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

mdc-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

用户数	实时计费间隔（分钟）
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**

1.3.45 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

mdc-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**

1.3.46 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

mdc-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**

1.3.47 vpn-instance (RADIUS scheme view)

vpn-instance 命令用来配置 RADIUS 方案所属的 VPN。

undo vpn-instance 命令用来恢复缺省情况。

【命令】

vpn-instance *vpn-instance-name*

undo vpn-instance

【缺省情况】

RADIUS 方案属于公网。

【视图】

RADIUS 方案视图

【缺省用户角色】

network-admin

mdc-admin

【参数】

vpn-instance-name：MPLS L3VPN 的 VPN 实例名称，为 1～31 个字符的字符串，区分大小写。

【使用指导】

本命令配置的 VPN 对于该方案下的所有 RADIUS 认证/计费服务器生效，但设备优先使用配置 RADIUS 认证/计费服务器时为各服务器单独指定的 VPN。

【举例】

配置 RADIUS 方案 radius1 所属的 VPN 为 test。

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

【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

mdc-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

mdc-admin

mdc-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:
    IP   : 2.2.2.2         Port: 49     State: Active
    VPN Instance: 2
    Single-connection: Enabled
  Primary Author Server:
    IP   : 2.2.2.2         Port: 49     State: Active
    VPN Instance: 2
    Single-connection: Disabled
  Primary Acct Server:
    IP   : Not Configured  Port: 49     State: Block
    VPN Instance: Not configured
    Single-connection: Disabled
```

```
  VPN Instance                          : 2
  NAS IP Address                        : 2.2.2.3
  Server Quiet Period(minutes)          : 5
  Realtime Accounting Interval(minutes) : 12
  Stop-accounting packets buffering     : Enabled
    Retransmittion 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 TACACS 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
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 • Active：激活状态 • Block：静默状态
VPN Instance	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 • 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

字段	描述
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 • 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

字段	描述
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
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

mdc-admin

mdc-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
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* } [**vpn-instance** *vpn-instance-name*]

undo hwtacacs nas-ip { *ipv4-address* | **ipv6** *ipv6-address* } [**vpn-instance** *vpn-instance-name*]

【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

mdc-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。

vpn-instance *vpn-instance-name*：指定私网源 IP 地址所属的 VPN 实例。*vpn-instance-name* 表示 MPLS L3VPN 的 VPN 实例名称，为 1～31 个字符的字符串，区分大小写。若不指定该参数，则表示配置的是公网源地址。

【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 16 个源地址。其中，最多包括一个 IPv4 公网源地址和一个 IPv6 公网源地址，其余为私网源地址。对于同一个 VPN，系统视图下最多允许指定一个 IPv4 私网源地址和一个 IPv6 私网源地址。

【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

mdc-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

mdc-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

mdc-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 { *ipv4-address* | **ipv6** *ipv6-address* } [*port-number* | **key** { **cipher** | **simple** } *string* | **single-connection** | **vpn-instance** *vpn-instance-name*] *

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

mdc-admin

【参数】

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。

vpn-instance *vpn-instance-name*：主 HWTACACS 计费服务器所属的 VPN 实例。*vpn-instance-name* 表示 MPLS L3VPN 的 VPN 实例名称，为 1～31 个字符的字符串，区分大小写。如果未指定本参数，则表示主 HWTACACS 计费服务器位于公网中。

【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 IP 地址、端口号和 VPN 参数不能完全相同。

若服务器位于 MPLS VPN 私网中，为保证 HWTACACS 报文被发送到指定的私网服务器，必须指定服务器所属的 VPN 实例。本命令指定的服务器所属的 VPN 比 HWTACACS 方案所属的 VPN 优先级高。

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 hw1
[Sysname-hwtacacs-hw1] primary accounting 10.163.155.12 49 key simple 123456TESTacct&!
```

【相关命令】

- **display hwtacacs scheme**
- **key** (HWTACACS scheme view)
- **secondary accounting**
- **vpn-instance** (HWTACACS scheme view)

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 { *ipv4-address* | **ipv6** *ipv6-address* } [*port-number* | **key** { **cipher** | **simple** } *string* | **single-connection** | **vpn-instance** *vpn-instance-name*] *

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

mdc-admin

【参数】

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。

vpn-instance *vpn-instance-name*：主 HWTACACS 认证服务器所属的 VPN 实例。*vpn-instance-name* 表示 MPLS L3VPN 的 VPN 实例名称，为 1～31 个字符的字符串，区分大小写。如果未指定本参数，则表示主 HWTACACS 认证服务器位于公网中。

【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 IP 地址、端口号和 VPN 参数不能完全相同。

若服务器位于 MPLS VPN 私网中，为保证 HWTACACS 报文被发送到指定的私网服务器，必须指定服务器所属的 VPN 实例。本命令指定的服务器所属的 VPN 比 HWTACACS 方案所属的 VPN 优先级高。

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**
- **vpn-instance** (HWTACACS scheme view)

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 { *ipv4-address* | **ipv6** *ipv6-address* } [*port-number* | **key** { **cipher** | **simple** } *string* | **single-connection** | **vpn-instance** *vpn-instance-name*] *

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

mdc-admin

【参数】

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。

vpn-instance *vpn-instance-name*：主 HWTACACS 授权服务器所属的 VPN 实例。*vpn-instance-name* 表示 MPLS L3VPN 的 VPN 实例名称，为 1～31 个字符的字符串，区分大小写。如果未指定本参数，则表示主 HWTACACS 授权服务器位于公网中。

【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 IP 地址、端口号和 VPN 参数不能完全相同。

若服务器位于 MPLS VPN 私网中，为保证 HWTACACS 报文被发送到指定的私网服务器，必须指定服务器所属的 VPN 实例。本命令指定的服务器所属的 VPN 比 HWTACACS 方案所属的 VPN 优先级高。

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**
- **vpn-instance** (HWTACACS scheme view)

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

mdc-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

mdc-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

mdc-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 { *ipv4-address* | **ipv6** *ipv6-address* } [*port-number* | **key** { **cipher** | **simple** } *string* | **single-connection** | **vpn-instance** *vpn-instance-name*] *

undo secondary accounting [{ *ipv4-address* | **ipv6** *ipv6-address* } [*port-number* | **vpn-instance** *vpn-instance-name*] *]

【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

mdc-admin

【参数】

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。

vpn-instance *vpn-instance-name*：从 HWTACACS 计费服务器所属的 VPN 实例。*vpn-instance-name* 表示 MPLS L3VPN 的 VPN 实例名称，为 1～31 个字符的字符串，区分大小写。如果未指定本参数，则表示从 HWTACACS 计费服务器位于公网中。

【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 IP 地址、端口号和 VPN 参数不能完全相同，并且各从计费服务器的 IP 地址、端口号和 VPN 参数也不能完全相同。

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。

若服务器位于 MPLS VPN 私网中，为保证 HWTACACS 报文被发送到指定的私网服务器，必须指定服务器所属的 VPN 实例。本命令指定的服务器所属的 VPN 比 HWTACACS 方案所属的 VPN 优先级高。

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)
- **vpn-instance** (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 { *ipv4-address* | **ipv6** *ipv6-address* } [*port-number*] **key** { **cipher** | **simple** } *string* | **single-connection** | **vpn-instance** *vpn-instance-name*] *

undo secondary authentication [{ *ipv4-address* | **ipv6** *ipv6-address* } [*port-number* | **vpn-instance** *vpn-instance-name*] *]

【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

mdc-admin

【参数】

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。

vpn-instance *vpn-instance-name*：从 HWTACACS 认证服务器所属的 VPN 实例。*vpn-instance-name* 表示 MPLS L3VPN 的 VPN 实例名称，为 1～31 个字符的字符串，区分大小写。如果未指定本参数，则表示从 HWTACACS 服务器位于公网中。

【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 IP 地址、端口号和 VPN 参数不能完全相同，并且各从认证服务器的 IP 地址、端口号和 VPN 参数也不能完全相同。

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。

若服务器位于 MPLS VPN 私网中，为保证 HWTACACS 报文被发送到指定的私网服务器，必须指定服务器所属的 VPN 实例。本命令指定的服务器所属的 VPN 比 HWTACACS 方案所属的 VPN 优先级高。

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)
- **vpn-instance** (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 { *ipv4-address* | **ipv6** *ipv6-address* } [*port-number* | **key** { **cipher** | **simple** } *string* | **single-connection** | **vpn-instance** *vpn-instance-name*] *

undo secondary authorization [{ *ipv4-address* | **ipv6** *ipv6-address* } [*port-number* | **vpn-instance** *vpn-instance-name*] *]

【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

mdc-admin

【参数】

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。

vpn-instance *vpn-instance-name*：从 HWTACACS 授权服务器所属的 VPN 实例。*vpn-instance-name* 表示 MPLS L3VPN 的 VPN 实例名称，为 1～31 个字符的字符串，区分大小写。如果未指定本参数，则表示从 HWTACACS 授权服务器位于公网中。

【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 IP 地址、端口号和 VPN 参数不能完全相同，并且各从授权服务器的 IP 地址、端口号和 VPN 参数也不能完全相同。

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。

若服务器位于 MPLS VPN 私网中，为保证 HWTACACS 报文被发送到指定的私网服务器，必须指定服务器所属的 VPN 实例。本命令指定的服务器所属的 VPN 比 HWTACACS 方案所属的 VPN 优先级高。

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)
- **vpn-instance** (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

mdc-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

mdc-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

mdc-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

mdc-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

mdc-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**

1.4.22 vpn-instance (HWTACACS scheme view)

vpn-instance 命令用来配置 HWTACACS 方案所属的 VPN。

undo vpn-instance 命令用来恢复缺省情况。

【命令】

vpn-instance *vpn-instance-name*

undo vpn-instance

【缺省情况】

HWTACACS 方案属于公网。

【视图】

HWTACACS 方案视图

【缺省用户角色】

network-admin

mdc-admin

【参数】

vpn-instance-name：MPLS L3VPN 的 VPN 实例名称，为 1～31 个字符的字符串，区分大小写。

【使用指导】

本命令配置的 VPN 对于该方案下的所有 HWTACACS 认证/授权/计费服务器生效，但设备优先使用配置认证/授权/计费服务器时指定的各服务器所属的 VPN。

【举例】

配置 HWTACACS 方案 hw1 所属的 VPN 为 test。

```
<Sysname> system-view
[Sysname] hwtacacs scheme hwt1
[Sysname-hwtacacs-hwt1] vpn-instance test
```

【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

mdc-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

mdc-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。该服务器必须已经存在。

【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

mdc-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，且必须已经存在。

【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

mdc-admin

mdc-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

字段	描述
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	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*] [**vpn-instance** *vpn-instance-name*]

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

mdc-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。

vpn-instance *vpn-instance-name*：LDAP 服务器所属的 VPN 实例。*vpn-instance-name* 表示 MPLS L3VPN 实例的名称，为 1～31 个字符的字符串，区分大小写。不指定该参数时，表示 LDAP 服务器属于公网。

【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*] [**vpn-instance** *vpn-instance-name*]

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

mdc-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。

vpn-instance *vpn-instance-name*：LDAP 服务器所属的 VPN 实例。*vpn-instance-name* 表示 MPLS L3VPN 实例的名称，为 1～31 个字符的字符串，区分大小写。不指定该参数时，表示 LDAP 服务器属于公网。

【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

mdc-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

mdc-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

mdc-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

mdc-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

mdc-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**

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

mdc-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。

【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**

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

mdc-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

mdc-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

mdc-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

mdc-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

mdc-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

mdc-admin

mdc-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

network-operator

mdc-admin

mdc-operator

【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 networkaccess 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 networkaccess 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
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

mdc-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

mdc-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**