目 录

1 AAA

1.1 AAA配置命令

1.1.1 access-limit enable

【命令】

access-limit enable *max-user-number*

undo access-limit enable

【视图】

ISP 域视图

【缺省级别】

2：系统级

【参数】

max-user-number：表示当前 ISP 域可容纳接入用户数的最大值，取值范围为 1～2147483646。

【描述】

access-limit enable 命令用来限制当前 ISP 域可容纳接入用户数。当接入此域的用户数超过当前 ISP 域可容纳的最大用户数后，新接入的用户将被拒绝。**undo access-limit enable** 命令用来恢复缺省情况。

缺省情况下，不限制当前 ISP 域可容纳的接入用户数。

需要注意的是，由于系统资源有限，如果当前 ISP 域下接入的用户过多，接入用户之间会发生资源的争用，因此适当地配置该值可以使属于当前 ISP 域的用户获得可靠的性能保障。

相关配置可参考命令 **display domain**。

【举例】

指定 ISP 域 test 最多可容纳 500 个接入用户。

```
<Sysname> system-view
[Sysname] domain test
[Sysname-isp-test] access-limit enable 500
```

1.1.2 accounting command

【命令】

accounting command hwtacacs-scheme *hwtacacs-scheme-name*

undo accounting command

【视图】

ISP 域视图

【缺省级别】

2：系统级

【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。

【描述】

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。

缺省情况下，命令行计费采用当前 ISP 域的缺省计费方法。

需要注意的是：

- 当前 ISP 域所引用的 HWTACACS 方案必须是已配置的。
- 命令行计费支持的远程 AAA 方案目前仅为 HWTACACS 方案。

相关配置可参考命令 **accounting default** 和 **hwtacacs scheme**。

【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
```

1.1.3 accounting default

【命令】

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

undo accounting default

【视图】

ISP 域视图

【缺省级别】

2：系统级

【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。

【描述】

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。

缺省情况下，当前 ISP 域的缺省计费方法为 **local**。

需要注意的是：

- 当前 ISP 域所引用的 RADIUS 或 HWTACACS 方案必须是已配置的。
- 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。

相关配置可参考命令 **local-user**、**hwtacacs scheme** 和 **radius scheme**。

【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** 作为备份计费方法。

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

1.1.4 accounting lan-access

【命令】

accounting lan-access { **local** | **none** | **radius-scheme** *radius-scheme-name* [**local** | **none**] }

undo accounting lan-access

【视图】

ISP 域视图

【缺省级别】

2：系统级

【参数】

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。

【描述】

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。

缺省情况下，lan-access 用户采用当前 ISP 域的缺省计费方法。

需要注意的是，当前 ISP 域所引用的 RADIUS 方案必须是已配置的。

相关配置可参考命令 **local-user**、**accounting default** 和 **radius scheme**。

【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** 作为备份计费方法。

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

1.1.5 accounting login

【命令】

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

undo accounting login

【视图】

ISP 域视图

【缺省级别】

2：系统级

【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。

【描述】

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。

缺省情况下，login 用户采用当前 ISP 域的缺省计费方法。

需要注意的是：

- 当前 ISP 域所引用的 RADIUS 或 HWTACACS 方案必须是已配置的。
- FTP 类型的 login 用户不支持计费流程。

相关配置可参考命令 **local-user**、**accounting default**、**hwtacacs scheme** 和 **radius scheme**。

【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** 作为备份计费方法。

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

1.1.6 accounting optional

【命令】

accounting optional

undo accounting optional

【视图】

ISP 域视图

【缺省级别】

2：系统级

【参数】

无

【描述】

accounting optional 命令用来打开计费可选开关。**undo accounting optional** 命令用来关闭计费可选开关。

缺省情况下，计费可选开关处于关闭状态。

需要注意的是：

- 对上线用户计费时，如果发现没有可用的计费服务器或与计费服务器通信失败时，若配置了本命令，则用户可以继续使用网络资源，且系统不再为其发送实时计费更新报文，否则用户连接将被切断。该命令适用于不是特别关心计费结果的情况下。
- 计费可选开关打开的情况下，本地用户视图下的 **access-limit** 命令配置的本地用户的连接数限制功能不生效。

【举例】

打开 ISP 域 test 的计费可选开关。

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

1.1.7 authentication default

【命令】

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

undo authentication default

【视图】

ISP 域视图

【缺省级别】

2：系统级

【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。

【描述】

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。

缺省情况下，当前 ISP 域的缺省认证方法为 **local**。

需要注意的是：

- 当前 ISP 域所引用的 RADIUS 或 HWTACACS 方案必须是已配置的。
- 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。

相关配置可参考命令 **local-user**、**hwtacacs scheme**、**radius scheme**。

【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** 作为备份认证方法。

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

1.1.8 authentication lan-access

【命令】

authentication lan-access { **local** | **none** | **radius-scheme** *radius-scheme-name* [**local** | **none**] }

undo authentication lan-access

【视图】

ISP 域视图

【缺省级别】

2：系统级

【参数】

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。

【描述】

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。

缺省情况下，lan-access 用户采用当前 ISP 域的缺省认证方法。

需要注意的是，当前 ISP 域所引用的 RADIUS 方案必须是已配置的。

相关配置可参考命令 **local-user**、**authentication default** 和 **radius scheme**。

【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 **local** 作为备份认证方法。

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

1.1.9 authentication login

【命令】

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

undo authentication login

【视图】

ISP 域视图

【缺省级别】

2：系统级

【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。

【描述】

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。

缺省情况下，login 用户采用当前 ISP 域的缺省认证方法。

需要注意的是，当前 ISP 域所引用的 RADIUS 或 HWTACACS 方案必须是已配置的。

相关配置可参考命令 **local-user**、**authentication default**、**hwtacacs scheme**、**radius scheme**。

【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** 作为备份认证方法。

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

1.1.10 authentication super

【命令】

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

undo authentication super

【视图】

ISP 域视图

【缺省级别】

2：系统级

【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。

【描述】

authentication super 命令用来配置级别切换认证方法。**undo authentication super** 命令用来恢复缺省情况。

缺省情况下，级别切换认证采用当前 ISP 域的缺省认证方法。

需要注意的是，当前 ISP 域所引用的 RADIUS 方案和 HWTACACS 方案必须是已配置的。

相关配置可参考命令 **hwtacacs scheme**、**radius scheme** 和“基础命令参考/CLI”中的命令 **super authentication-mode**。

【举例】

在 ISP 域 test 下，配置使用 HWTACACS 方案 tac 进行级别切换认证。

```
<Sysname> system-view
[Sysname] super authentication-mode scheme
```

```
[Sysname] domain test
[Sysname-domain-test] authentication super hwtacacs-scheme tac
```

1.1.11 authorization command

【命令】

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

undo authorization command

【视图】

ISP 域视图

【缺省级别】

2：系统级

【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，认证通过的用户只有系统所给予的 0 级别的命令行访问权限。

【描述】

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。

缺省情况下，命令行授权采用当前 ISP 域的缺省授权方法。

需要注意的是：

- 当前 ISP 域所引用的 HWTACACS 方案必须是已配置的。
- 对用户采用本地命令行授权时，成功登录设备的用户只能执行不大于本地用户级别的命令行。

相关配置可参考命令 **local-user**、**authorization default** 和 **hwtacacs scheme**。

【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** 作为备份授权方法。

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

1.1.12 authorization default

【命令】

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

undo authorization default

【视图】

ISP 域视图

【缺省级别】

2：系统级

【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 访问设备的用户）只有系统所给予的 0 级别的命令行访问权限，其中 FTP 用户可访问设备的根目录；认证通过的非 Login 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。

【描述】

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。

缺省情况下，当前 ISP 域的缺省授权方法为 **local**。

需要注意的是：

- 当前 ISP 域所引用的 RADIUS、HWTACACS 必须是已配置的。
- 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。

相关配置可参考命令 **local-user**、**hwtacacs scheme**、**radius scheme**。

【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** 作为备份授权方法。

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

1.1.13 authorization lan-access

【命令】

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

undo authorization lan-access

【视图】

ISP 域视图

【缺省级别】

2：系统级

【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。

【描述】

authorization lan-access 命令用来为 lan-access 用户配置授权方法。**undo authorization lan-access** 命令用来为恢复缺省情况。

缺省情况下，lan-access 用户采用当前 ISP 域的缺省授权方法。

需要注意的是：

- 当前 ISP 域所引用的 RADIUS 方案必须是已配置的。
- 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。

相关配置可参考命令 **local-user**、**authorization default** 和 **radius scheme**。

【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** 作为备份授权方法。

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

1.1.14 authorization login

【命令】

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

undo authorization login

【视图】

ISP 域视图

【缺省级别】

2：系统级

【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 访问设备的用户）只有系统所给予的 0 级别的命令行访问权限，其中 FTP 用户可访问设备的根目录。

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。

【描述】

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。

缺省情况下，login 用户采用当前 ISP 域的缺省授权方法。

需要注意的是：

- 当前 ISP 域所引用的 RADIUS 或 HWTACACS 方案必须是已配置的。
- 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。

相关配置可参考命令 **local-user**、**authorization default**、**hwtacacs scheme**、**radius scheme**。

【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** 作为备份授权方法。

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

1.1.15 cut connection

【命令】

cut connection { **access-type** { **dot1x** | **mac-authentication** } | **all** | **domain** *isp-name* | **interface** *interface-type interface-number* | **ip** *ip-address* | **mac** *mac-address* | **ucibindex** *ucib-index* | **user-name** *user-name* | **vlan** *vlan-id* } [**slot** *slot-number*]

【视图】

系统视图

【缺省级别】

2：系统级

【参数】

access-type：指定接入方式。

- **dot1x**：表示 802.1X 认证接入方式；
- **mac-authentication**：表示 MAC 地址认证接入方式；

all：指定所有用户连接。

domain *isp-name*：指定 ISP 域。其中，*isp-name* 为 ISP 域名，为 1～24 个字符的字符串。

interface *interface-type interface-number*：指定接口。其中，*interface-type interface-number* 为接口类型和接口编号。目前只支持二层以太网端口。

ip *ip-address*：指定 IP 地址。

mac *mac-address*：指定 MAC 地址。其中，*mac-address* 为 H-H-H 格式。

ucibindex *ucib-index*：指定连接索引号，取值范围为 0～4294967295。

user-name *user-name*：指定用户名。其中，*user-name* 表示用户名，为 1～80 个字符的字符串，区分大小写。若用户输入的用户名未携带域名，则系统默认其带缺省域名或强制认证域名。

vlan *vlan-id*：指定用户所在 VLAN。其中，*vlan-id* 的取值范围为 1～4094。

slot *slot-number*：指定设备在 IRF 中的成员编号。

【描述】

cut connection 命令用来强制切断指定 AAA 用户的连接。

此命令目前只对 lan-access 服务类型的用户有效。

需要注意的是：

- 如果客户端配置的用户名携带版本号或者用户名中存在空格，则无法通过用户名来检索和切断用户连接，但是通过其他方式（如 IP 地址、连接索引号等）仍然可以检索和切断用户的连接。
- 如果接入用户的接口上配置了指定接入类型的强制认证域（例如 802.1X 强制认证域），则通过该接口上线的指定接入类型的用户将使用强制认证域进行认证、授权和计费，因此若要通过 **cut connection domain** *isp-name* 命令切断该类用户连接，则必须指定用户使用的强制认证域名。

相关配置可参考命令 **display connection** 和 **service-type**。

【举例】

切断 ISP 域 test 下的所有用户连接。

```
<Sysname> system-view
[Sysname] cut connection domain test
```

1.1.16 display connection

【命令】

display connection [**access-type** { **dot1x** | **mac-authentication** } | **domain** *isp-name* | **interface** *interface-type interface-number* | **ip** *ip-address* | **mac** *mac-address* | **ucibindex** *ucib-index* | **user-name** *user-name* | **vlan** *vlan-id*] [**slot** *slot-number*] [**|** { **begin** | **exclude** | **include** } *regular-expression*]

【视图】

任意视图

【缺省级别】

1：监控级

【参数】

access-type：显示指定接入方式的用户连接。

- **dot1x**：表示 802.1X 认证接入方式；
- **mac-authentication**：表示 MAC 地址认证接入方式；

domain *isp-name*：显示指定 ISP 域中的用户连接。其中，*isp-name* 表示 ISP 域名，为 1～24 个字符的字符串，不区分大小写。

interface *interface-type interface-number*：显示指定接口的用户连接。其中，*interface-type interface-number* 为接口类型和接口编号。

ip *ip-address*：显示指定 IP 地址的用户连接。

mac *mac-address*：显示指定 MAC 地址的用户连接。其中，*mac-address* 为 H-H-H 格式。

ucibindex *ucib-index*：显示指定连接索引的用户连接。其中，*ucib-index* 表示连接索引号，取值范围为 0～4294967295。

user-name *user-name*：显示指定用户名的用户连接。其中，*user-name* 表示用户名，为 1～80 个字符的字符串，区分大小写。若用户输入的用户名未携带域名，则系统默认其带缺省域名或强制认证域名。

vlan *vlan-id*：显示指定 VLAN 的用户连接。其中，*vlan-id* 的取值范围为 1～4094。

slot *slot-number*：显示指定成员设备上用户的连接，*slot-number* 表示设备在 IRF 中的成员编号。

begin：从包含指定正则表达式的行开始显示。

exclude：只显示不包含指定正则表达式的行。

include：只显示包含指定正则表达式的行。

regular-expression：表示正则表达式，为 1～256 个字符的字符串，区分大小写。

【描述】

display connection 命令用来显示所有或指定的 AAA 用户连接的相关信息。

需要注意的是：

- 不指定任何参数的情况下，系统显示所有 AAA 用户连接的概要信息。
- 指定参数 **ucibindex** 的情况下，显示详细的用户连接信息，指定其它参数则显示概要信息。
- 对于 FTP 类型用户，无法显示 AAA 用户连接的相关信息。

- 如果接入用户的接口上配置了强制认证域（例如 802.1X 强制认证域），则通过该接口上线的用户将使用强制认证域进行认证、授权和计费。通过本命令查看到的用户名形式与用户输入的用户名是否携带域名有关，如果用户输入的用户名未携带域名分隔符，则设备默认以“*用户输入的用户名*@*强制认证域名*”的形式显示用户名，因此若要通过 **display connection domain** *isp-name* 命令显示该类用户信息，则必须指定用户使用的强制认证域名；如果用户输入的用户名中已经包含了域名分隔符，则系统仅显示用户输入的用户名，而不携带强制认证域名。例如，用户输入的用户名为 aaa@123，上线时使用的强制认证域为 dom，则设备上显示出的用户名为 aaa@123，而不是 aaa@123@dom。

相关配置可参考命令 **cut connection**。

【举例】

显示所有 AAA 用户连接的相关信息。

```
<Sysname> display connection
Slot:  1
Index=0   , Username=telnet@system
IP=10.0.0.1
IPv6=N/A

 Total 1 connection(s) matched on slot 1.
 Total 1 connection(s) matched.
```

显示连接索引为 0 的 AAA 用户连接的详细信息。

```
<Sysname> display connection ucibindex 0
Slot:  1
Index=0   , Username=telnet@system
IP=10.0.0.1
IPv6=N/A
Access=Admin   ,AuthMethod=PAP
Port Type=Virtual ,Port Name=N/A
Initial VLAN=999, Authorization VLAN=20
ACL Group=Disable
CAR=Disable
Priority=Disable
SessionTimeout=60(s), Terminate-Action=Radius-Request
Start=2011-01-16 10:53:03 ,Current=2011-01-16 10:57:06 ,Online=00h04m03s
 Total 1 connection matched.
Slot:  2
 Total 0 connection matched.
```

表1-1 display connection 命令显示信息描述表

字段	描述
Slot	用户连接所在的IRF成员设备编号
Index	用户连接的索引号
Username	当前连接的用户名，格式为*username@domain*
MAC	该用户的MAC地址

字段	描述
IP	该用户IPv4地址
IPv6	该用户IPv6地址
Access	用户接入类型
AuthMethod	认证方法
Port Type	用户接入的端口类型
Port Name	用户接入的端口名称
Initial VLAN	用户所在的初始VLAN
Authorization VLAN	授权untagged VLAN
Authorization Tagged VLAN list	授权tagged VLAN列表
ACL Group	授权ACL组
CAR(kbps)	授权CAR参数信息
UpPeakRate	上行峰值速率
DnPeakRate	下行峰值速率
UpAverageRate	上行平均速率
DnAverageRate	下行平均速率
Priority	用户报文的处理优先级
SessionTimeout	服务器下发的SessionTimeout属性值，单位为秒，其涵义由Termiante-Action类型决定： • Termiante-Action 类型为 Default 时，该值为用户剩余在线时间 • Termiante-Action 类型为 Radius-Request 时，该值为用户重认证周期
Terminate-Action	到达SessionTimeout指定的时间时设备采取的动作，包括以下两种类型： • Default：切断用户 • Radius-Request：向用户发起重认证
Start=xxx ,Current=xxx ,Online=xxx	用户上线的时间，当前的系统时间，用户在线时长
Total 1 connection(s) matched.	总计1个AAA用户连接

1.1.17 display domain

【命令】

display domain [*isp-name*] [**|** { **begin** | **exclude** | **include** } *regular-expression*]

【视图】

任意视图

【缺省级别】

1：监控级

【参数】

isp-name：指定 ISP 域名，为 1～24 个字符的字符串。

|：使用正则表达式对显示信息进行过滤。有关正则表达式的详细介绍，请参见“基础配置指导”中的“CLI”。

begin：从包含指定正则表达式的行开始显示。

exclude：只显示不包含指定正则表达式的行。

include：只显示包含指定正则表达式的行。

regular-expression：表示正则表达式，为 1～256 个字符的字符串，区分大小写。

【描述】

display domain 命令用来显示指定 ISP 域的配置信息。

如果不指定 ISP 域，则显示系统中所有 ISP 域的配置信息。

相关配置可参考命令 **access-limit enable**、**domain** 和 **state**。

【举例】

显示系统中所有 ISP 域的配置信息。

```
<Sysname> display domain
0  Domain : system
   State :  Active
   Access-limit :  Disabled
   Accounting method : Required
   Default authentication scheme      : local
   Default authorization scheme       : local
   Default accounting scheme          : local
   Domain User Template:
   Idle-cut : Disabled
   Self-service : Disabled
   Authorization attributes :

1  Domain : test
   State : Active
   Access-limit : Disabled
   Accounting method : Required
   Default authentication scheme      : local
   Default authorization scheme       : local
   Default accounting scheme          : local
   Lan-access authentication scheme   : radius:test, local
   Lan-access authorization scheme    : hwtacacs:hw, local
   Lan-access accounting scheme       : local
   Domain User Template:
   Idle-cut : Disabled
   Self-service : Disabled
   Authorization attributes :
```

```
Default Domain Name: system
Total 2 domain(s).
```

表1-2 display domain 命令显示信息描述表

字段	描述
Domain	ISP域名
State	ISP域的当前状态 • Active：激活状态，表示系统允许该域下的用户请求网络服务 • Block：阻塞状态，表示系统不允许该域下的用户请求网络服务
Access-limit	ISP所能容纳的最大接入用户数（若显示为Disabled，则表示不限制当前ISP域可容纳接入用户数）
Accounting method	计费方法是否可选 • Required：必选，表示如果发现没有可用的计费服务器或与计费服务器通信失败时，将切断用户连接 • Optional：可选，表示如果发现没有可用的计费服务器或与计费服务器通信失败时，用户可以继续使用网络资源
Default authentication scheme	缺省的认证方法
Default authorization scheme	缺省的授权方法
Default accounting scheme	缺省的计费方法
Lan-access authentication scheme	lan-access用户的认证方法
Lan-access authorization scheme	lan-access用户的授权方法
Lan-access accounting scheme	lan-access用户的计费方法
Domain User Template	ISP域的用户模板，定义了与域用户相关的一些功能
Idle-cut	ISP域的用户闲置切断功能 • Disabled：未使能，表示不对用户进行限制切断控制 • Enabled：使能，表示当域中的用户在指定的最大空闲时间内的产生的流量小于指定的最小数据流量时，会被强制下线
Self-service	自助服务定位功能 • Disabled：自助服务定位功能处于未使能状态 • Self-service URL：用户可以通过浏览器访问该 URL 指定的服务器页面，并进行相应的操作
Authorization attributes	ISP域的缺省授权属性
Default Domain Name	缺省ISP域名
Total 2 domain(s).	总计2个ISP域

1.1.18 domain

【命令】

domain *isp-name*

undo domain *isp-name*

【视图】

系统视图

【缺省级别】

3：管理级

【参数】

isp-name：ISP 域名，为 1～24 个字符的字符串，不区分大小写，不能包括“/”、“\”、“:”、“*”、“?”、“<”、“>”、“”” 、“|” 以及“@”字符。

【描述】

domain 命令用来创建 ISP 域并进入其视图。**undo domain** 命令用来删除指定的 ISP 域。

缺省情况下，系统存在一个名称为 system 的 ISP 域。

需要注意的是：

- 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。
- 不能删除系统缺省的 ISP 域，除非先恢复要删除的域为非缺省域，系统缺省的 ISP 域的配置请参考 **domain default enable** 命令。

相关配置可参考命令 **state** 和 **display domain**。

【举例】

创建一个新的 ISP 域 test，并进入其视图。

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

1.1.19 domain default enable

【命令】

domain default enable *isp-name*

undo domain default enable

【视图】

系统视图

【缺省级别】

3：管理级

【参数】

isp-name：ISP 域名，为 1～24 个字符的字符串，不区分大小写。

【描述】

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。

缺省情况下，系统缺省的 ISP 域为 system。

需要注意的是：

- 缺省的 ISP 域有且只有一个。
- 指定的缺省 ISP 域要必须存在，否则会导致用户名中未携带域名的用户无法进行认证。
- 配置为缺省的 ISP 域不能被删除，除非先恢复要删除的域为非缺省域。

相关配置可参考命令 **domain**、**state** 和 **display domain**。

【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
```

1.1.20 domain if-unknown

【命令】

domain if-unknown *isp-name*

undo domain if-unknown

【视图】

系统视图

【缺省级别】

3：管理级

【参数】

isp-name：ISP 域名，为 1～24 个字符的字符串，不区分大小写，不能包括“/”、“\”、“:”、“*”、“?”、“<”、“>”、“”” 以及“@”字符。

【描述】

domain if-unknown 命令用来为未知域名的用户指定 ISP 域。**undo if-unknown** 命令用来恢复缺省情况。

缺省情况下，没有为未知域名的用户指定 ISP 域。

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，例如 802.1X、MAC 地址认证。

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。

相关配置可参考命令 **domain default enable**。

【举例】

为未知域名的用户指定 ISP 域为 test。

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

1.1.21 idle-cut enable

【命令】

idle-cut enable *minute* [*flow*]

undo idle-cut enable

【视图】

ISP 域视图

【缺省级别】

2：系统级

【参数】

minute：指定闲置检测时间，取值范围为 1～600，单位为分钟。

flow：指定用户在闲置检测时间内产生的数据流量，取值范围为 1～10240000，单位为字节，缺省值为 10240。

【描述】

idle-cut enable 命令用来设置当前 ISP 域下的用户闲置切断功能。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。**undo idle-cut enable** 命令用来恢复缺省情况。

缺省情况下，用户闲置切断功能处于关闭状态。

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。

【举例】

允许 ISP 域 test 中的用户启用闲置切断功能，闲置检测时间为 50 分钟，允许用户闲置时的最小数据流量为 1024 个字节。

```
<Sysname> system-view
[Sysname] domain test
[Sysname-isp-test] idle-cut enable 50 1024
```

1.1.22 self-service-url enable

【命令】

self-service-url enable *url-string*

undo self-service-url enable

【视图】

ISP 域视图

【缺省级别】

2：系统级

【参数】

url-string：表示自助服务器的 URL，为 1～64 个字符的字符串。字符串必须以“http://”开始，字符串中不能包括“?”字符。该 URL 在安装 RADIUS 服务器时由服务器管理员指定。

【描述】

self-service-url enable 命令用来指定自助服务器的 URL。**undo self-service-url enable** 命令用来恢复缺省情况。

缺省情况下，自助服务器定位功能处于关闭状态。

自助服务即用户可以对自己的帐号和密码进行管理和控制。目前，仅 CAMS/iMC 类型的 RADIUS 服务器支持自助服务。

【举例】

在 ISP 域 test 下，配置自助服务器修改用户密码页面的 URL 为 http://10.153.89.94/selfservice。

```
<Sysname> system-view
[Sysname] domain test
[Sysname-isp-test] self-service-url enable http://10.153.89.94/selfservice
```

1.1.23 state（ISP domain view）

【命令】

state { **active** | **block** }

undo state

【视图】

ISP 域视图

【缺省级别】

2：系统级

【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。

【描述】

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。

缺省情况下，当一个 ISP 域被创建以后，其状态为 **active**（ISP 域视图）。

当指定某个 ISP 域处于 **block** 状态时，不允许该域下的用户请求网络服务，但是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，域下的接入用户不能再请求网络服务。

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

1.2 本地用户配置命令

1.2.1 access-limit

【命令】

access-limit *max-user-number*

undo access-limit

【视图】

本地用户视图

【缺省级别】

3：管理级

【参数】

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

【描述】

access-limit 命令用来设置当前用户名可容纳的最大接入用户数。**undo access-limit** 命令用来取消对当前用户名的接入用户数限制。

缺省情况下，不限制当前本地用户名可容纳的接入用户数。

需要注意的是：

- 本地用户的 **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 用户不支持计费，因此 FTP 用户不受此属性限制。

相关配置可参考命令 **display local-user**。

【举例】

允许同时以用户名 abc 在线的用户数为 5。

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

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

【命令】

authorization-attribute { **acl** *acl-number* | **idle-cut** *minute* | **level** *level* **user-role** { **guest** | **guest-manager** | **security-audit** } | **vlan** *vlan-id* | **work-directory** *directory-name* } *

undo authorization-attribute { **acl** | **idle-cut** | **level** | **user-role** | **vlan** | **work-directory** } *

【视图】

本地用户视图/用户组视图

【缺省级别】

3：管理级

【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 *minute*：设置本地用户的闲置切断时间。其中，*minute* 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。

level *level*：指定本地用户的级别，取值范围为 0～3。其中 0 为访问级、1 为监控级、2 为系统级、3 为管理级，数值越小，用户的级别越低。当登录设备用户界面的验证方式配置为 **scheme** 时，用户成功登录后所能访问的命令行的级别由本参数决定。缺省情况下，本地用户的级别为 0，即用户成功登录后缺省可以访问级别为 0 的命令行。

user-role：指定授权本地用户的角色，不同角色的用户具有不同的命令行使用权限。该属性仅在本地用户视图下支持。未被授权为某特殊角色的本地用户，其认证成功后具有的访问权限受其它本地用户授权属性限制。目前，设备支持的本地用户角色包括以下几种：

- **guest**：表示授权本地用户为来宾用户。通常，该角色的用户通过 Web 页面创建。
- **guest-manager**：表示授权本地用户为来宾管理员，该类型的本地用户通过认证后，仅能通过 Web 访问来宾用户相关的页面，比如创建、修改和删除来宾用户。
- **security-audit** 表示授权本地用户为安全日志管理员，该类型的本地用户通过认证后，仅能执行与安全日志文件操作相关的命令，比如保存安全日志文件等，可执行命令的具体情况请参见“网络管理和监控命令参考”中的“信息中心”。

vlan *vlan-id*：指定本地用户的授权 VLAN。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。其中，*vlan-id* 为 VLAN 编号，取值范围为 1～4094。

work-directory *directory-name*：授权 FTP/SFTP 用户可以访问的目录。其中，*directory-name* 表示 FTP/SFTP 用户可以访问的目录，为 1～135 个字符的字符串，不区分大小写，且该目录必须已经存在。缺省情况下，FTP/SFTP 用户可访问设备的根目录，可通过本参数来修改用户可以访问的目录。

【描述】

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** 命令用来删除配置的授权属性，恢复用户具有的缺省访问权限。

缺省情况下，未对本地用户或用户组设置任何授权属性。

需要注意的是：

- 可配置的授权属性都有其明确的使用环境和用途，请仅针对用户的服务类型配置对应的授权属性。
- 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。
- 避免主备切换后 FTP/SFTP 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。

- 系统中只剩一个角色为安全日志管理员的本地用户时，该本地用户就不能被删除，而且也不能修改或删除该本地用户的安全日志管理员角色，除非再指定一个新的用户为安全日志管理员。
- 一个本地用户只能被指定为一种角色，后设置的角色会覆盖前面设置的角色。

【举例】

配置本地用户 abc 的授权 VLAN 为 VLAN 2。

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

1.2.3 bind-attribute

【命令】

bind-attribute { **ip** *ip-address* | **location port** *slot-number subslot-number port-number* | **mac** *mac-address* | **vlan** *vlan-id* } *

undo bind-attribute { **ip** | **location** | **mac** | **vlan** } *

【视图】

本地用户视图

【缺省级别】

3：管理级

【参数】

ip *ip-address*：指定用户的 IP 地址。

location port *slot-number subslot-number port-number*：指定用户绑定的端口。其中 *slot-number* 为单板所在槽位号，取值范围为 0～255；*subslot-number* 为子槽位号，取值范围为 0～15；*port-number* 为端口号，取值范围 0～255。

mac *mac-address*：指定用户的 MAC 地址。其中，*mac-address* 为 H-H-H 格式。

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。

【描述】

bind-attribute 命令用来设置用户的绑定属性。**undo bind-attribute** 命令用来删除配置的用户绑定属性。

缺省情况下，未设置用户的任何绑定属性。

需要注意的是，当对本地用户进行认证时，如果配置了绑定属性，则会检查用户的实际属性与配置的绑定属性是否一致，如果不一致则认证失败。而且，由于认证检测时不区分用户的接入服务类型，即会对所有类型的用户都进行已配置绑定属性的认证检测，因此在配置绑定属性时要考虑某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。

【举例】

配置本地用户 abc 的绑定 IP 为 3.3.3.3。

```
<Sysname> system-view
[Sysname] local-user abc
[Sysname-luser-abc] bind-attribute ip 3.3.3.3
```

1.2.4 display local-user

【命令】

display local-user [**idle-cut** { **disable** | **enable** } | **service-type** { **ftp** | **lan-access** | **ssh** | **telnet** | **terminal** | **web** } | **state** { **active** | **block** } | **user-name** *user-name* | **vlan** *vlan-id*] [**slot** *slot-number*] [**|** { **begin** | **exclude** | **include** } *regular-expression*]

【视图】

任意视图

【缺省级别】

1：监控级

【参数】

idle-cut { **disable** | **enable** }：显示使能或未使能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。
- **lan-access**：lan-access 类型用户（主要指以太网接入用户，比如 802.1X 用户）。
- **ssh**：SSH 用户。
- **telnet**：Telnet 用户。
- **terminal**：从 CON 口登录的终端用户。
- **web**：Web 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** 表示用于处于阻塞状态，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。

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。

slot *slot-number*：显示指定成员设备的所有本地用户信息，*slot-number* 表示设备在 IRF 中的成员编号。

begin：从包含指定正则表达式的行开始显示。

exclude：只显示不包含指定正则表达式的行。

include：只显示包含指定正则表达式的行。

regular-expression：表示正则表达式，为 1～256 个字符的字符串，区分大小写。

【描述】

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。

需要注意的是：如果不指定任何参数，则显示所有本地用户信息。

相关配置可参考命令 **local-user**。

【举例】

显示所有本地用户的相关信息。

```
<Sysname> display local-user
The contents of local user abc:
 State:                    Active
 ServiceType:              lan-access
 Access-limit:             Enabled           Current AccessNum: 0
 Max AccessNum:            300
 User-group:               system
 Bind attributes:
  IP address:              1.2.3.4
  Bind location:           0/4/1 (SLOT/SUBSLOT/PORT)
  MAC address:             00-01-00-02-00-03
  Vlan ID:                 100
 Authorization attributes:
  Idle TimeOut:            10(min)
  Work Directory:          flash:/
  User Privilege:          3
  Acl ID:                  2000
  Vlan ID:                 100
  Expiration date:          12:12:12-2018/09/16
 Password aging:           Enabled (30 days)
 Password length:          Enabled (4 characters)
 Password composition:     Enabled (4 types,  2 characters per type)
Total 1 local user(s) matched.
```

表1-3 display local-user 命令显示信息描述表

字段	描述
State	本地用户的状态（Active：激活、Block：阻塞）
ServiceType	本地用户的服务类型（ftp、lan-access、ssh、telnet、terminal）
Access-limit	是否对使用该用户名的接入连接数进行限制（Enabled：使能连接限制功能、Disabled：未使能连接限制功能）
Current AccessNum	使用该用户名的当前接入用户数
Max AccessNum	最大接入用户数
User-group	本地用户所属用户组
Bind attributes	本地用户的绑定属性
IP address	本地用户绑定的IP地址

字段	描述
Bind location	本地用户绑定的端口
MAC address	本地用户绑定的MAC地址
VLAN ID	本地用户绑定的VLAN
Authorization attributes	本地用户的授权属性
Idle TimeOut	本地用户闲置切断时间（单位为分钟）
Work Directory	FTP/SFTP用户可以访问的目录
User Privilege	本地用户级别
VLAN ID	本地用户授权VLAN
Expiration date	本地用户的有效期
Password aging	本地用户密码的老化时间
Password length	本地用户密码的最小长度
Password composition	本地用户密码的组合策略
Total 1 local user(s) matched.	总计有1个本地用户匹配

1.2.5 display user-group

【命令】

display user-group [*group-name*] [**|** { **begin** | **exclude** | **include** } *regular-expression*]

【视图】

任意视图

【缺省级别】

2：系统级

【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。

|：使用正则表达式对显示信息进行过滤。有关正则表达式的详细介绍，请参见“基础配置指导”中的“CLI”。

begin：从包含指定正则表达式的行开始显示。

exclude：只显示不包含指定正则表达式的行。

include：只显示包含指定正则表达式的行。

regular-expression：表示正则表达式，为 1～256 个字符的字符串，区分大小写。

【描述】

display user-group 命令用来显示用户组的相关配置。不指定用户组名称，则显示所有用户组的相关配置。

相关配置请参考命令 **user-group**。

【举例】

显示用户组 abc 的相关配置。

```
<Sysname> display user-group abc
The contents of user group abc:
 Authorization attributes:
  Idle-cut:                120(min)
  Work Directory:          FLASH:
  Level:                   1
  Acl Number:              2000
  Vlan ID:                 1
  Password aging:           Enabled (1 days)
 Password length:          Enabled (4 characters)
 Password composition:     Enabled (1 types,  1 characters per type)
Total 1 user group(s) matched.
```

表1-4 display user-group 命令显示信息描述表

字段	描述
Idle-cut	闲置切断时间（单位：分钟）
Work Directory	FTP/SFTP用户可以访问的目录
Level	本地用户的级别
Acl Number	授权ACL号
Vlan ID	授权VIAN ID
Password aging	本地用户密码老化时间
Password length	本地用户密码最小长度
Password composition	本地用户密码组合策略
Total 1 user group(s) matched.	总计有1个用户组匹配

1.2.6 expiration-date（Local user view）

【命令】

expiration-date *time*

undo expiration-date

【视图】

本地用户视图

【缺省级别】

3：管理级

【参数】

time：本地用户的有效期，精确到秒，格式为 HH:MM:SS-MM/DD/YYYY（时:分:秒-月/日/年）、HH:MM:SS-YYYY/MM/DD（时:分:秒-年/月/日）、MM/DD/YYYY-HH:MM:SS（月/日/年-时:分:秒）

或 YYYY/MM/DD-HH:MM:SS（年/月/日-时:分:秒）。其中，HH:MM:SS 中的 HH 取值范围为 0～23，MM 和 SS 取值范围为 0～59；MM/DD/YYYY 或 YYYY/MM/DD 中的 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。除表示零点外，格式中的前导 0 可以省略不写，比如 2:2:0-2011/2/2 等效于 02:02:00-2011/02/02。

【描述】

expiration-date 命令用来设置本地用户的有效期。**undo expiration-date** 用来取消本地用户的有效期配置。

缺省情况下，未设置用户的有效期，设备不进行用户有效期的检查。

在有用户临时需要接入网络的情况下，设备管理员可以为用户建立临时使用的来宾帐户，并通过本命令与 **vaildity-date** 命令一起完成对用户有效起止时间的控制。当用户进行本地认证时，接入设备检查当前系统时间是否在该用户的生效时间与有效期之间，若在则允许用户登录，否则拒绝用户登录。

【举例】

配置用户 abc 的有效期为 2011/05/31 的 12:10:20。

```
<Sysname> system-view
[Sysname] local-user abc
[Sysname-luser-abc] expiration-date 12:10:20-2011/05/31
```

1.2.7 group

【命令】

group *group-name*

undo group

【视图】

本地用户视图

【缺省级别】

3：管理级

【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。

【描述】

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。

缺省情况下，用户属于系统默认创建的用户组 system。

【举例】

设置本地用户 111 所属的用户组为 abc。

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

1.2.8 group-attribute allow-guest

【命令】

group-attribute allow-guest

undo group-attribute allow-guest

【视图】

用户组视图

【缺省级别】

3：管理级

【参数】

无

【描述】

group-attribute allow-guest 命令用来设置用户组的来宾可选属性，即允许来宾用户管理员在 Web 页面上创建的来宾用户加入该用户组。**undo group-attribute allow-guest** 命令用来恢复缺省情况。

缺省情况下，用户组不具有来宾可选属性，来宾用户管理员在 Web 界面上创建的来宾用户不能加入该用户组。

需要注意的是，系统默认创建的用户组 system 缺省就具有来宾可选属性，并且该属性不能被删除。

【举例】

设置用户组 test 允许来宾用户加入。

```
<Sysname> system-view
[Sysname] user-group test
[Sysname-ugroup-test] group-attribute allow-guest
```

1.2.9 local-user

【命令】

local-user *user-name*

undo local-user { *user-name* | **all** [**service-type** { **ftp** | **lan-access** | **ssh** | **telnet** | **terminal** | **web** }] }

【视图】

系统视图

【缺省级别】

3：管理级

【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”。

all：所有的用户。

service-type：指定用户的类型。具体用户类型如下：

- **ftp**：表示 FTP 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）；
- **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。
- **web**：表示 Web 用户。

【描述】

local-user 命令用来添加本地用户并进入本地用户视图。**undo local-user** 命令用来删除指定的本地用户。

缺省情况下，无本地用户。

相关配置可参考命令 **display local-user** 和 **service-type**。

【举例】

添加名称为 user1 的本地用户。

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

1.2.10 password

【命令】

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

undo password

【视图】

本地用户视图

【缺省级别】

2：系统级

【参数】

hash: 以哈希加密算法方式保存密码并显示为密码的 hash 值。

cipher：表示以密文方式设置用户密码。

simple：表示以明文方式设置用户密码。

password：设置的明文密码或密文密码，区分大小写。

- 如果未指定哈希加密算法保存时，明文密码为 1～63 个字符的字符串；密文密码为 1～117 个字符的字符串；
- 如果指定哈希加密算法保存，明文密码为 1～63 个字符的字符串；密文密码为 1～110 个字符的字符串。

【描述】

password 命令用来设置本地用户的密码。**undo password** 命令用来取消本地用户的密码。

需要注意的是：

- 如果不指定任何参数，则表示以交互式方式设置本地用户密码，涵义与指定 **simple** 关键字相同。仅支持 Password Control 特性的设备上才支持本方式。相关命令的具体介绍请参见“安全命令参考”中的“Password Control”。
- 以明文或密文方式设置的用户密码，均以密文的方式保存在配置文件中。
- 使能 Password Control 特性的全局密码管理功能（通过命令 **password-control enable**）后，本地用户密码的设置将受到 Password Control 特性的约束，比如密码的长度、复杂度等将会受到限制，并且设备上将不显示配置的本地用户密码。另外，用户也不能再通过 **password hash cipher** *password* 命令配置用户密码。

相关配置可参考命令 **display local-user**。

【举例】

设置本地用户 user1 的密码为明文 123456。

```
<Sysname> system-view
[Sysname] local-user user1
[Sysname-luser-user1] password simple 123456
```

以交互式方式设置本地用户 user1 的密码为 123456。

```
<Sysname> system-view
[Sysname] local-user user1
[Sysname-luser-user1] password
Password:******
Confirm :******
```

1.2.11 service-type

【命令】

service-type { **ftp** | **lan-access** | { **ssh** | **telnet** | **terminal** } * | **web** }

undo service-type { **ftp** | **lan-access** | { **ssh** | **telnet** | **terminal** } * | **web**}

【视图】

本地用户视图

【缺省级别】

3：管理级

【参数】

ftp：指定用户可以使用 FTP 服务。若授权 FTP 服务，缺省授权 FTP 用户可访问设备的根目录。

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）。

web：指定用户可以使用 Web 服务。

【描述】

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。

缺省情况下，系统不对用户授权任何服务。

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】

指定用户可以使用 Telnet 服务。

```
<Sysname> system-view
[Sysname] local-user user1
[Sysname-luser-user1] service-type telnet
```

1.2.12 state（Local user view）

【命令】

state { **active** | **block** }

undo state

【视图】

本地用户视图

【缺省级别】

2：系统级

【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。

【描述】

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。

缺省情况下，当一个本地用户被创建以后，其状态为 **active**（本地用户视图）。

当指示某个用户处于 **block** 状态时，不允许当前本地用户请求网络服务，但是不影响其它用户。

相关配置可参考命令 **local-user**。

【举例】

设置本地用户 user1 处于“阻塞”状态。

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

1.2.13 user-group

【命令】

user-group *group-name*

undo user-group *group-name*

【视图】

系统视图

【缺省级别】

3：管理级

【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。

【描述】

user-group 命令用来创建用户组并进入其视图。**undo user-group** 命令用来删除指定的用户组。

用户组是一个本地用户策略及属性的集合，某些需要集中管理的策略或者属性可在在用户组中统一配置和管理。目前，用户组中可配置的内容包括本地用户密码的控制策略和用户的授权属性。

需要注意的是：

- 当用户组中有本地用户时，不允许使用 **undo user-group** 删除该用户组。
- 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。

相关配置可参考命令 **display user-group**。

【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]
```

1.2.14 validity-date（Local user view）

【命令】

validity-date *time*

undo validity-date

【视图】

本地用户视图

【缺省级别】

3：管理级

【参数】

time：本地用户的生效时间，精确到秒，格式为 HH:MM:SS-MM/DD/YYYY（时:分:秒-月/日/年）、MM/DD/YYYY-HH:MM:SS（月/日/年-时:分:秒）、YYYY/MM/DD-HH:MM:SS（年/月/日-时:分:秒）或 HH:MM:SS-YYYY/MM/DD（时:分:秒-年/月/日）。其中，HH:MM:SS 中的 HH 取值范围为 0～23，MM 和 SS 取值范围为 0～59；MM/DD/YYYY 中的 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。除表示零点外，格式中的前导 0 可以省略不写，比如 2:2:0-2011/2/2 等效于 02:02:00-2011/02/02。

【描述】

validity-date 命令用来设置本地用户的生效时间。**undo validity-date** 用来取消本地用户的生效时间配置。

缺省情况下，未设置用户的生效时间，设备不进行用户生效时间的检查。

在有用户临时需要接入网络的情况下，设备管理员可以为用户建立临时使用的来宾帐户，并通过本命令与 **expiration-date** 命令一起完成对用户有效起止时间的控制。当用户进行本地认证时，接入设备检查当前系统时间是否在该用户的生效时间与有效期之间，若在则允许用户登录，否则拒绝用户登录。

【举例】

配置用户 abc 的生效时间为 2011/04/30 的 12:10:20，有效期截至 2011/05/31 的 12:10:20。

```
<Sysname> system-view
[Sysname] local-user abc
[Sysname-luser-abc] validity-date 12:10:20-2011/04/30
[Sysname-luser-abc] expiration-date 12:10:20-2011/05/31
```

1.3 RADIUS配置命令

1.3.1 accounting-on enable

【命令】

accounting-on enable [**interval** *seconds* | **send** *send-times*] *

undo accounting-on enable

【视图】

RADIUS 方案视图

【缺省级别】

2：系统级

【参数】

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

【描述】

accounting-on enable 命令用来配置 accounting-on 功能。在 accounting-on 功能处于使能的情况下，若设备重启，则设备会在重启之后发送 accounting-on 报文通知该方案所使用的计费 RADIUS 服务器，要求 RADIUS 服务器停止计费且强制该设备的用户下线。**undo accounting-on enable** 命令用来恢复缺省情况。

缺省情况下，accounting-on 功能处于关闭状态。

需要注意的是：

- 执行完该命令后，请执行 **save** 操作，以保证设备重启后 accounting-on 功能生效。
- 在执行 accounting-on 功能的过程中，使用该命令重新设置的报文重发间隔时间以及报文最大发送次数会立即生效。

【举例】

使能 RADIUS 认证方案 radius1 的 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
```

1.3.2 attribute 25 car

【命令】

attribute 25 car

undo attribute 25 car

【视图】

RADIUS 方案视图

【缺省级别】

2：系统级

【参数】

无

【描述】

attribute 25 car 命令用来开启 RADIUS Attribute 25 的 CAR 参数解析功能。**undo attribute 25 car** 命令用来恢复缺省情况。

缺省情况下，RADIUS Attribute 25 的 CAR 参数解析功能处于关闭状态。

相关配置可参考命令 **display radius scheme** 和 **display connection**。

【举例】

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
```

1.3.3 data-flow-format (RADIUS scheme view)

【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** }

【视图】

RADIUS 方案视图

【缺省级别】

2：系统级

【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。

【描述】

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。

缺省情况下，数据流的单位为 **byte**，数据包的单位为 **one-packet**。

需要注意的是，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。

相关配置可参考命令 **display radius scheme**。

【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
```

1.3.4 display radius scheme

【命令】

display radius scheme [*radius-scheme-name*] [**slot** *slot-number*] [**|** { **begin** | **exclude** | **include** } *regular-expression*]

【视图】

任意视图

【缺省级别】

2：系统级

【参数】

radius-scheme-name：指定 RADIUS 方案名。

slot *slot-number*：显示指定成员设备上的 RADIUS 方案配置信息，*slot-number* 表示设备在 IRF 中的成员编号。

|：使用正则表达式对显示信息进行过滤。有关正则表达式的详细介绍，请参见“基础配置指导”中的“CLI”。

begin：从包含指定正则表达式的行开始显示。

exclude：只显示不包含指定正则表达式的行。

include：只显示包含指定正则表达式的行。

regular-expression：表示正则表达式，为 1～256 个字符的字符串，区分大小写。

【描述】

display radius scheme 命令用来显示所有或指定 RADIUS 方案的配置信息。

需要注意的是：如果不指定 RADIUS 方案名，则显示所有 RADIUS 方案的配置信息。

相关配置可参考命令 **radius scheme**。

【举例】

显示所有 RADIUS 方案的配置信息。

```
<Sysname> display radius scheme
------------------------------------------------------------------
SchemeName  : radius1
  Index : 0                          Type : extended
  Primary Auth Server:
    IP: 1.1.1.1                                 Port: 1812   State: active
    Encryption Key : ******
    VPN instance   : 1
  Primary Acct Server:
    IP: 1.1.1.1                                 Port: 1813   State: active
    Encryption Key : ******
    VPN instance   : 1
  Second Auth Server:
    IP: 1.1.2.1                                 Port: 1812   State: active
    Encryption Key : N/A
    VPN instance   : N/A
    IP: 1.1.3.1                                 Port: 1812   State: active
    Encryption Key : N/A
    VPN instance   : N/A
  Second Acct Server:
    IP: 1.1.2.1                                 Port: 1813   State: block
    Encryption Key : N/A
    VPN instance   : N/A
  Auth Server Encryption Key : ******
  Acct Server Encryption Key : N/A
  VPN instance               : 1
  Accounting-On packet disable, send times : 50 , interval : 3s
  Interval for timeout(second)                          : 3
  Retransmission times for timeout                      : 3
  Interval for realtime accounting(minute)              : 12
  Retransmission times of realtime-accounting packet    : 5
  Retransmission times of stop-accounting packet        : 500
  Quiet-interval(min)                                   : 5
```

```
  Username format                                    : without-domain
  Data flow unit                                     : Byte
  Packet unit                                        : one
  NAS-IP address                                     : 1.1.1.1
  Attribute 25                                       : car
----------------------------------------------------------------------
Total 1 RADIUS scheme(s).
```

表1-5 display radius scheme 命令显示信息描述表

字段	描述
SchemeName	RADIUS方案的名称
Index	RADIUS方案的索引号
Type	设备支持的RADIUS服务器的类型 • **extended** 类型：要求 RADIUS 客户端和 RADIUS 服务器按照私有 RADIUS 协议的规程和报文格式进行交互 • **standard** 类型：要求 RADIUS 客户端和 RADIUS 服务器按照标准 RADIUS 协议（RFC 2865/2866 或更新）的规程和报文格式进行交互
Primary Auth Server	主认证服务器相关信息
Primary Acct Server	主计费服务器相关信息
Second Auth Server	从认证服务器相关信息
Second Acct Server	从计费服务器相关信息
IP	认证/计费服务器的IP地址
Port	认证/计费服务器的接入端口号 未配置时，显示缺省值
State	认证/计费服务器的目前状态 • active：激活 • block：阻塞
Encryption Key	认证/计费报文的共享密钥（明文或密文） • 已配置时，显示为****** • 未配置时，显示为 N/A
VPN instance	服务器所属的MPLS L3VPN 未配置时，显示为N/A
Auth Server Encryption Key	认证报文的共享密钥 • 已配置时，显示为****** • 未配置时，显示为 N/A
Acct Server Encryption Key	计费报文的共享密钥 • 已配置时，显示为****** • 未配置时，显示为 N/A

字段	描述
VPN instance	RADIUS方案所属的MPLS L3VPN 未配置时，不显示
Accounting-On packet disable	accounting-on功能未使能
send times	accounting-on报文的重发次数
interval	accounting-on报文的重发间隔（秒）
Interval for timeout(second)	RADIUS服务器的响应超时时间（秒）
Retransmission times for timeout	发送RADIUS报文的最大尝试次数
Interval for realtime accounting(minute)	实时计费的时间间隔（分钟）
Retransmission times of realtime-accounting packet	允许实时计费请求无响应的最大次数
Retransmission times of stop-accounting packet	发起停止计费请求的最大尝试次数
Quiet-interval(min)	主服务器恢复激活状态的时间
Username format	发送给RADIUS服务器的用户名格式
Data flow unit	发送给RADIUS服务器的数据流的单位
Packet unit	发送给RADIUS服务器的数据包的单位
NAS-IP address	发送RADIUS报文的源IP地址
Attribute 25	将RADIUS Attribute 25解析为CAR参数
Total 1 RADIUS scheme(s).	共计1个RADIUS方案

1.3.5 display radius statistics

【命令】

display radius statistics [**slot** *slot-number*] [**|** { **begin** | **exclude** | **include** } *regular-expression*]

【视图】

任意视图

【缺省级别】

2：系统级

【参数】

slot *slot-number*：显示指定成员设备上 RADIUS 报文的统计信息，*slot-number* 表示设备在 IRF 中的成员编号。

|：使用正则表达式对显示信息进行过滤。有关正则表达式的详细介绍，请参见“基础配置指导”中的“CLI”。

begin：从包含指定正则表达式的行开始显示。

exclude：只显示不包含指定正则表达式的行。

include：只显示包含指定正则表达式的行。

regular-expression：表示正则表达式，为 1～256 个字符的字符串，区分大小写。

【描述】

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

相关配置可参考命令 **radius scheme**。

【举例】

显示 RADIUS 报文的统计信息。

```
<Sysname> display radius statistics
state statistic(total=4096):
     DEAD = 4096     AuthProc = 0        AuthSucc = 0
AcctStart = 0         RLTSend = 0         RLTWait = 0
 AcctStop = 0          OnLine = 0            Stop = 0

Received and Sent packets statistic:
Sent PKT total   = 1547     Received PKT total = 23
Resend Times     Resend total
1                508
2                508
Total            1016
RADIUS received packets statistic:
Code =  2   Num = 15       Err = 0
Code =  3   Num = 4        Err = 0
Code =  5   Num = 4        Err = 0
Code = 11   Num = 0        Err = 0

Running statistic:
RADIUS received messages statistic:
Normal auth request      Num = 24       Err = 0        Succ = 24
EAP auth request         Num = 0        Err = 0        Succ = 0
Account request          Num = 4        Err = 0        Succ = 4
Account off request      Num = 503      Err = 0        Succ = 503
PKT auth timeout         Num = 15       Err = 5        Succ = 10
PKT acct_timeout         Num = 1509     Err = 503      Succ = 1006
Realtime Account timer   Num = 0        Err = 0        Succ = 0
PKT response             Num = 23       Err = 0        Succ = 23
Session ctrl pkt         Num = 0        Err = 0        Succ = 0
Normal author request    Num = 0        Err = 0        Succ = 0
Set policy result        Num = 0        Err = 0        Succ = 0
Accounting on request    Num = 5        Err = 0        Succ = 5
Accounting on response   Num = 0        Err = 0        Succ = 0
Dynamic Author Ext request Num = 0        Err = 0        Succ = 0
RADIUS sent messages statistic:
Auth accept              Num = 10
Auth reject              Num = 14
EAP auth replying        Num = 0
Account success          Num = 4
Account failure          Num = 3
```

```
Server ctrl req          Num = 0
RecError_MSG_sum = 0
SndMSG_Fail_sum  = 0
Timer_Err        = 0
Alloc_Mem_Err    = 0
State Mismatch   = 0
Other_Error      = 0

No-response-acct-stop packet = 1
Discarded No-response-acct-stop packet for buffer overflow = 0
```

表1-6 display radius statistics 命令显示信息描述表

字段	描述
state statistic(total=4096)	各状态的用户数统计信息（用户总数为4096）
DEAD	处于空闲态的用户数
AuthProc	处于认证等待态的用户数
AuthSucc	处于认证成功态的用户数
AcctStart	处于计费开始态的用户数
RLTSend	处于实时计费发送态的用户数
RLTWait	处于实时计费等待态的用户数
AcctStop	处于计费等待停止态的用户数
OnLine	处于在线态的用户数
Stop	处于停止态的用户数
Received and Sent packets statistic	RADIUS模块收发报文的数目统计信息
Sent PKT total	发送报文总数
Received PKT total	接收报文总数
Resend Times	重传报文的次数
Resend total	单次重传报文数
Total	重传报文总数
RADIUS received packets statistic	RADIUS模块接收报文数目统计
Code	报文类型
Num	报文总数
Err	处理失败的报文数或消息数
Succ	成功处理的消息数
Running statistic	RADIUS模块收发报文的分类统计信息
RADIUS received messages statistic	RADIUS已接收消息数目统计
Normal auth request	普通认证请求报文数

字段	描述
EAP auth request	EAP认证请求报文数
Account request	计费请求报文数
Account off request	计费停止请求报文数
PKT auth timeout	认证超时报文数
PKT acct_timeout	计费超时报文数
Realtime Account timer	实时计费请求报文数
PKT response	服务器的响应报文数
Session ctrl pkt	会话控制报文数
Normal author request	普通授权请求报文数
Set policy result	Set policy结果报文数
Accounting on request	accounting on请求报文数
Accounting on response	accounting on响应报文数
Dynamic Author Ext request	动态授权扩展请求报文数
RADIUS sent messages statistic	RADIUS模块已发送消息数目统计
Auth accept	认证接收报文数
Auth reject	认证拒绝报文数
EAP auth replying	EAP认证回应报文数
Account success	计费成功报文数
Account failure	计费失败报文数
Server ctrl req	服务器控制请求报文数
RecError_MSG_sum	接收错误消息总数
SndMSG_Fail_sum	发送消息失败总数
Timer_Err	启动定时器失败报文数
Alloc_Mem_Err	申请内存失败报文数
State Mismatch	状态不匹配报文数
Other_Error	其它错误报文数
No-response-acct-stop packet	停止计费报文无响应数
Discarded No-response-acct-stop packet for buffer overflow	因缓存区满而丢弃的无响应停止计费报文总数

1.3.6 display stop-accounting-buffer (for RADIUS)

【命令】

display stop-accounting-buffer { **radius-scheme** *radius-scheme-name* | **session-id** *session-id* | **time-range** *start-time stop-time* | **user-name** *user-name* } [**slot** *slot-number*] [**|** { **begin** | **exclude** | **include** } *regular-expression*]

【视图】

任意视图

【缺省级别】

2：系统级

【参数】

radius-scheme *radius-scheme-name*：显示缓存的、向指定 RADIUS 方案中的计费服务器发送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。

session-id *session-id*：显示缓存的指定会话 ID 的停止计费请求报文。其中，*session-id* 为 1～50 个字符的字符串。

time-range *start-time stop-time*：显示缓存的指定时间段内的停止计费请求报文，即只要是在指定时间段内的发起且被暂存的停止计费请求报文都会被显示。其中，*start-time* 为请求时间段的起始时间；*stop-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*：显示缓存的指定用户名的停止计费请求报文。其中，*user-name* 表示用户名，为 1～80 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。

slot *slot-number*：显示指定成员设备上缓存的停止计费请求报文，*slot-number* 表示设备在 IRF 中的成员编号。

|：使用正则表达式对显示信息进行过滤。有关正则表达式的详细介绍，请参见“基础配置指导”中的“CLI”。

begin：从包含指定正则表达式的行开始显示。

exclude：只显示不包含指定正则表达式的行。

include：只显示包含指定正则表达式的行。

regular-expression：表示正则表达式，为 1～256 个字符的字符串，区分大小写。

【描述】

display stop-accounting-buffer 命令用来显示缓存的没有得到响应的停止计费请求报文的相关信息，主要包括该计费请求报文所属的会话 ID、用户名以及产生停止计费请求的时间。

在发送停止计费请求报文而 RADIUS 服务器没有响应时，设备会尝试重传该报文，如果发送该报文的最大尝试次数超过指定的值（由 **retry** 命令设置）后仍然没有得到响应，则设备会缓存该报文，然后再发起一次请求，若继续无响应，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。

相关配置可参考命令 **reset stop-accounting-buffer**、**stop-accounting-buffer enable**、**user-name-format**、**retry** 和 **retry stop-accounting**。

【举例】

显示系统缓存的用户名为 abc 的停止计费请求报文的相关信息。

```
<Sysname> display stop-accounting-buffer user-name abc
RDIdx Session-ID               user name                 Happened time
1     1000326232325010         abc                      23:27:16-08/31/2006
1     1000326232326010         abc                      23:33:01-08/31/2006
Total 2 record(s) Matched
```

1.3.7 key (RADIUS scheme view)

【命令】

key { **accounting** | **authentication** } [**cipher** | **simple**] *key*

undo key { **accounting** | **authentication** }

【视图】

RADIUS 方案视图

【缺省级别】

2：系统级

【参数】

accounting：指定 RADIUS 计费报文的共享密钥。

authentication：指定 RADIUS 认证/授权报文的共享密钥。

cipher：表示以密文方式设置共享密钥。

simple：表示以明文方式设置共享密钥。

key：设置的明文密钥或密文密钥，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。不指定 **simple** 和 **cipher** 时，表示以明文方式设置共享密钥。

【描述】

key 命令用来配置 RADIUS 认证/授权或计费报文的共享密钥。**undo key** 命令用来删除配置。

缺省情况下，无共享密钥。

需要注意的是：

- 以明文或密文方式设置的共享密钥，均以密文的方式保存在配置文件中。
- 设备优先采用配置 RADIUS 认证/授权/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/授权/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。

相关配置可参考命令 **display radius scheme**。

【举例】

将 RADIUS 方案 radius1 的计费报文的共享密钥设置为明文 ok。

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

将 RADIUS 方案 radius1 的计费报文的共享密钥设置为明文 ok。

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

```
[Sysname] radius scheme radius1
[Sysname-radius-radius1] key accounting ok
```

1.3.8 nas-ip (RADIUS scheme view)

【命令】

nas-ip { *ipv4-address* | **ipv6** *ipv6-address* }

undo nas-ip

【视图】

RADIUS 方案视图

【缺省级别】

2：系统级

【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。

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，不能为本地链路地址。

【描述】

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** 命令用来恢复缺省情况。

缺省情况下，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 IP 地址。

需要注意的是：

- 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，为保证认证和计费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。
- RADIUS 方案视图下的命令 **nas-ip** 只对本 RADIUS 方案有效，系统视图下的命令 **radius nas-ip** 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。
- 本命令配置的源 IP 地址与 RADIUS 方案中设置的服务器 IP 地址的协议版本必须保持一致，否则配置不生效。
- 如果重复执行此命令，新配置的源地址会覆盖原有的源地址。

相关配置可参考命令 **radius nas-ip**。

【举例】

配置设备发送 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
```

1.3.9 primary accounting (RADIUS scheme view)

【命令】

primary accounting { *ipv4-address* | **ipv6** *ipv6-address* } [*port-number* | **key** [**cipher** | **simple**] *key* | **vpn-instance** *vpn-instance-name*] *

undo primary accounting

【视图】

RADIUS 方案视图

【缺省级别】

2：系统级

【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。其中，*ipv6-address* 为合法的 IPv6 全球单播地址。

port-number：主 RADIUS 计费服务器的 UDP 端口号，缺省为 1813，取值范围为 1～65535。此端口号必须与服务器提供计费服务的端口号保持一致。

key [**cipher** | **simple**] *key*：与主 RADIUS 计费服务器交互的计费报文的共享密钥。此共享密钥必须与服务器上配置的共享密钥保持一致。

- **cipher** *key*：以密文方式设置共享密钥，*key* 为 1～117 个字符的字符串，区分大小写。
- **simple** *key*：以明文方式设置共享密钥，*key* 为 1～64 个字符的字符串，区分大小写。
- 不指定 **cipher** 和 **simple** 时，表示以明文方式设置共享密钥。

vpn-instance *vpn-instance-name*：主 RADIUS 计费服务器所属的 VPN。*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。

【描述】

primary accounting 命令用来配置主 RADIUS 计费服务器。**undo primary accounting** 命令用来删除设置的主 RADIUS 计费服务器。

缺省情况下，未配置主计费服务器。

需要注意的是：

- 主计费服务器和从计费服务器的 IP 地址不能相同，且 IP 地址协议版本必须一致。
- 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，则使用命令 **key accounting** [**cipher** | **simple**] *key* 命令设置的共享密钥。
- 若设备与 MPLS VPN 私网服务器通信，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 实例名称。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。
- 计费服务器与认证/授权服务器的 IP 地址协议版本必须一致。
- 如果在发送计费开始请求过程中修改了主计费服务器，则设备在与当前服务器通信超时后，将会重新从主服务器开始依次查找状态为 **active** 的服务器进行通信。

- 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。
- 以明文或密文方式设置的共享密钥，均以密文的方式保存在配置文件中。

相关配置可参考命令 **key** 和 **vpn-instance** (RADIUS scheme view)。

【举例】

设置 RADIUS 方案 radius1 的主计费服务器的 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 hello。

```
<Sysname> system-view
[Sysname] radius scheme radius1
[Sysname-radius-radius1] primary accounting 10.110.1.2 1813 key simple hello
```

1.3.10 primary authentication (RADIUS scheme view)

【命令】

primary authentication { *ipv4-address* | **ipv6** *ipv6-address* } [*port-number* | **key** [**cipher** | **simple**] *key* | **vpn-instance** *vpn-instance-name*] *

undo primary authentication

【视图】

RADIUS 方案视图

【缺省级别】

2：系统级

【参数】

ipv4-address：主 RADIUS 认证/授权服务器的 IPv4 地址。

ipv6 *ipv6-address*：主 RADIUS 认证/授权服务器的 IPv6 地址。其中，*ipv6-address* 为合法的 IPv6 全球单播地址。

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

key [**cipher** | **simple**] *key*：与主 RADIUS 认证/授权服务器交互的认证/授权报文的共享密钥。此共享密钥必须与服务器上配置的共享密钥保持一致。

- **cipher** *key*：以密文方式设置共享密钥。*key* 为 1～117 个字符的字符串，区分大小写。
- **simple** *key*：以明文方式设置共享密钥。*key* 为 1～64 个字符的字符串，区分大小写。
- 不指定 **cipher** 和 **simple** 时，表示以明文方式设置共享密钥。

vpn-instance *vpn-instance-name*：主 RADIUS 认证/授权服务器所属的 VPN。*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/授权服务器位于公网中。

【描述】

primary authentication 命令用来配置主 RADIUS 认证/授权服务器。**undo primary authentication** 命令用来删除设置的主 RADIUS 认证/授权服务器。

缺省情况下，未配置主认证/授权服务器。

需要注意的是：

- 设备与主认证/授权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，则使用命令 **key authenticaiton** [**cipher** | **simple**] *key* 命令设置的共享密钥。
- 若设备与 MPLS VPN 私网服务器通信，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 实例名称。本命令指定的服务器所属的 VPN 比 RADIUS 方案所属的 VPN 具优先级高。
- 主认证/授权服务器和从认证/授权服务器的 IP 地址不能相同，且 IP 地址协议版本必须一致。
- 认证/授权服务器与计费服务器的 IP 地址协议版本必须一致。
- 如果在认证过程中使用本命令删除了主认证服务器，则设备在与当前服务器通信超时后，将会重新从主服务器开始依次查找状态为 **active** 的服务器进行通信。
- 以明文或密文方式设置的共享密钥，均以密文的方式保存在配置文件中。

相关配置可参考命令 **key** 和 **vpn-instance** (RADIUS scheme view)。

【举例】

设置 RADIUS 方案 radius1 的主认证/授权服务器的 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/授权报文的共享密钥为明文 hello。

```
<Sysname> system-view
[Sysname] radius scheme radius1
[Sysname-radius-radius1] primary authentication 10.110.1.1 1812 key hello
```

1.3.11 radius client

【命令】

radius client enable

undo radius client

【视图】

系统视图

【缺省级别】

2：系统级

【参数】

无

【描述】

radius client enable 命令用来使能 RADIUS 客户端的监听端口，使能后的端口可以接收和发送 RADIUS 报文。**undo radius client** 命令用来关闭 RADIUS 客户端的监听端口。

缺省情况下，监听端口处于使能状态。

需要注意的是，关闭 RADIUS 客户端的监听端口后：

- 在线用户的计费结束报文无法发出，也不能被缓存下来尝试继续发送。RADIUS 服务器因为收不到在线用户的下线报文，会出现有一段时间用户已经下线，但 RADIUS 服务器上还有此用户的情况。另外，已缓存的计费报文会发送失败，如果发送失败的次数达到配置的最大次

数后，仍然没有收到响应，计费报文将从缓存中被删除。计费报文的发送失败，都会直接影响用户计费信息的准确性。

- 如果配置了本地认证/授权/计费作为备份方法，则 RADIUS 请求失败后会转由设备本地继续认证/授权/计费，其中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。

【举例】

使能 RADIUS 客户端的监听端口。

```
<Sysname> system-view
[Sysname] radius client enable
```

1.3.12 radius dscp

【命令】

radius dscp *dscp-value*

undo radius dscp

【视图】

系统视图

【缺省级别】

2：系统级

【参数】

dscp-value：报文的 DSCP 优先级，取值范围为 0～63。

【描述】

radius dscp 命令用来配置 IPv4 RADIUS 报文的 DSCP 优先级。**undo radius dscp** 命令用来恢复缺省情况。

缺省情况下，IPv4 RADIUS 报文的 DSCP 优先级为 0。

【举例】

配置 IPv4 RADIUS 报文的 DSCP 优先级为 6。

```
<Sysname> system-view
[Sysname] radius dscp 6
```

1.3.13 radius ipv6 dscp

【命令】

radius ipv6 dscp *dscp-value*

undo radius ipv6 dscp

【视图】

系统视图

【缺省级别】

2：系统级

【参数】

dscp-value：报文的 DSCP 优先级，取值范围为 0～63。

【描述】

radius ipv6 dscp 命令用来配置 IPv6 RADIUS 报文的 DSCP 优先级。**undo radius ipv6 dscp** 命令用来恢复缺省情况。

缺省情况下，IPv6 RADIUS 报文的 DSCP 优先级为 0。

【举例】

配置 IPv6 RADIUS 报文的 DSCP 优先级为 6。

```
<Sysname> system-view
[Sysname] radius ipv6 dscp 6
```

1.3.14 radius nas-ip

【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*]

【视图】

系统视图

【缺省级别】

2：系统级

【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。

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，不能为本地链路地址。

vpn-instance *vpn-instance-name*：指定私网源 IPv4 地址所属的 VPN。*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。

【描述】

radius nas-ip 命令用来指定设备发送 RADIUS 报文使用的源地址。**undo radius nas-ip** 命令用来删除指定的源地址。

缺省情况下，不指定源地址，即以发送报文的接口地址作为源地址。

需要注意的是：

- 系统最多允许指定 1 个公网源地址和 15 个私网源地址。新配置的公网源地址会覆盖原有的公网源地址。而且，每一个 VPN 只能指定一个私网源地址，新配置会覆盖原有配置。
- 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，为保证认证和计费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。

- RADIUS 方案视图下的命令 **nas-ip** 只对本 RADIUS 方案有效，系统视图下的命令 **radius nas-ip** 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。

相关配置可参考命令 **nas-ip**。

【举例】

配置设备发送 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
```

1.3.15 radius scheme

【命令】

radius scheme *radius-scheme-name*

undo radius scheme *radius-scheme-name*

【视图】

系统视图

【缺省级别】

3：管理级

【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。

【描述】

radius scheme 命令用来创建 RADIUS 方案并进入其视图。**undo radius scheme** 命令用来删除指定的 RADIUS 方案。

缺省情况下，未定义 RADIUS 方案。

需要注意的是：

- 一个 RADIUS 方案可以同时被多个 ISP 域引用。
- 不允许使用 **undo radius scheme** 命令删除被 ISP 域引用的 RADIUS 方案。

相关配置可参考命令 **display radius scheme**。

【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]
```

1.3.16 radius trap

【命令】

radius trap { accounting-server-down | authentication-error-threshold | authentication-server-down }

undo radius trap { accounting-server-down | authentication-error-threshold | authentication-server-down }

【视图】

系统视图

【缺省级别】

2：系统级

【参数】

accounting-server-down：表示 RADIUS 计费服务器可达状态改变时发送 Trap 信息。

authentication-error-threshold：表示认证失败次数超过阈值时发送 Trap 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改变时发送 Trap 信息。

【描述】

radius trap 命令用来使能 RADIUS Trap 功能。**undo radius trap** 命令用来关闭指定的 RADIUS Trap 功能。

缺省情况下，RADIUS Trap 功能处于关闭状态。

使能 RADIUS 服务器可达状态改变时的 Trap 功能后，Trap 信息的发送包括以下两种情况：

- 当 NAS 向 RADIUS 服务器发送计费或认证请求没有响应时，会重传请求，当重传次数达到最大传送次数时仍然没有响应时，NAS 认为该服务器不可达，并发送 Trap 信息。
- 当 NAS 收到处于不可达状态的 RADIUS 服务器发送的报文时，则认为该服务器可达，并发送一次 Trap 报文。

使能认证失败次数超过阈值时的 Trap 功能后，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，系统会发送一次 Trap 报文。

【举例】

使能 RADIUS 计费服务器可达状态改变时的 Trap 功能。

```
<Sysname> system-view
[Sysname] radius trap accounting-server-down
```

1.3.17 reset radius statistics

【命令】

reset radius statistics [**slot** *slot-number*]

【视图】

用户视图

【缺省级别】

2：系统级

【参数】

slot *slot-number*：清除指定成员设备上 RADIUS 协议的统计信息，*slot-number* 表示设备在 IRF 中的成员编号。

【描述】

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

相关配置请参考命令 **display radius statistics**。

【举例】

清除 RADIUS 协议的统计信息。

```
<Sysname> reset radius statistics
```

1.3.18 reset stop-accounting-buffer (for RADIUS)

【命令】

reset stop-accounting-buffer { **radius-scheme** *radius-scheme-name* | **session-id** *session-id* | **time-range** *start-time stop-time* | **user-name** *user-name* } [**slot** *slot-number*]

【视图】

用户视图

【缺省级别】

2：系统级

【参数】

radius-scheme *radius-scheme-name*：根据指定 RADIUS 方案清除缓存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。

session-id *session-id*：根据指定会话 ID 清除缓存的停止计费响应报文。其中，*session-id* 为会话 ID，为 1～50 个字符的字符串。

time-range *start-time stop-time*：根据指定停止计费请求时刻的起始和结束时间清除缓存的停止计费响应报文。其中，*start-time* 为请求时间段的起始时间；*stop-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*：根据指定用户名清除缓存的停止计费响应报文。其中，*user-name* 表示用户名，为 1～80 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。

slot *slot-number*：根据指定成员设备清除缓存的停止计费响应报文，*slot-number* 表示设备在 IRF 中的成员编号。

【描述】

reset stop-accounting-buffer 命令用来清除缓存中的没有得到响应的停止计费请求报文。

相关配置可参考命令 **stop-accounting-buffer enable** 和 **display stop-accounting-buffer**。

【举例】

清除用户 user0001@test 缓存在系统中的停止计费请求报文。

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

清除从 2011 年 8 月 31 日 0 点 0 分 0 秒到 2011 年 8 月 31 日 23 点 59 分 59 秒期间内系统缓存的停止计费请求报文。

```
<Sysname> reset stop-accounting-buffer time-range 0:0:0-08/31/2011 23:59:59-08/31/2011
```

1.3.19 retry

【命令】

retry *retry-times*

undo retry

【视图】

RADIUS 方案视图

【缺省级别】

2：系统级

【参数】

retry-times：发送 RAIUDS 报文的最大尝试次数，取值范围为 1～20。

【描述】

retry 命令用来设置发送 RADIUS 报文的最大尝试次数，即由于某 RADIUS 服务器未响应或未及时响应设备发送的 RAIUDS 报文，设备尝试向该服务器发送 RADIUS 报文的最大次数。**undo retry** 命令用来恢复缺省情况。

缺省情况下，发送 RADIUS 报文的最大尝试次数为 3 次。

需要注意的是：

- 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 RADIUS 服务器在应答超时定时器规定的时长内没有响应设备，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超过最大传送次数而 RADIUS 服务器仍旧没有响应，则设备将认为本次请求失败。
- 发送 RADIUS 报文的最大尝试次数与 RADIUS 服务器应答超时时间的乘积不能超过 75 秒。

相关配置可参考命令 **radius scheme** 和 **timer response-timeout**。

【举例】

设置在 RADIUS 方案 radius1 下，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
```

1.3.20 retry realtime-accounting

【命令】

retry realtime-accounting *retry-times*

undo retry realtime-accounting

【视图】

RADIUS 方案视图

【缺省级别】

2：系统级

【参数】

retry-times：允许实时计费请求无响应的最大次数，取值范围为 1～255。

【描述】

retry realtime-accounting 命令用来设置允许实时计费请求无响应的最大次数。**undo retry realtime-accounting** 命令用来恢复缺省情况。

缺省情况下，设备最多允许 5 次实时计费请求无响应，之后将切断用户连接。

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，保证在设备向 RADIUS 服务器发出的实时计费请求没有得到响应的次数超过所设定的限度时，设备才会切断用户连接。

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。

相关配置可参考命令 **retry**、**timer response-timeout** 和 **timer realtime-accounting**。

【举例】

设置 RADIUS 方案 radius1 最多允许 10 次实时计费请求无响应。

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

1.3.21 retry stop-accounting (RADIUS scheme view)

【命令】

retry stop-accounting *retry-times*

undo retry stop-accounting

【视图】

RADIUS 方案视图

【缺省级别】

2：系统级

【参数】

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

【描述】

retry stop-accounting 命令用来设置发起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。

缺省情况下，发起停止计费请求的最大尝试次数为 500。

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 5，设备允许的停止计费请求无响应的最大次数为 20 次（**retry stop-accounting** 命令设置），则其含义为：设备发起停止计费请求，如果 3 秒钟内得不到回应就重新发起一次请求，如果尝试 5 次都没有得到回应就认为该次停止计费请求失败，设备会将其缓存在本机上，然后再发起一次请求，重复上述过程，20 次尝试均失败以后，设备将其丢弃。

相关配置可参考命令 **retry**、**retry stop-accounting**、**timer response-timeout** 和 **display stop-accounting-buffer**。

【举例】

在 RADIUS 方案 radius1 中，设置设备最多可以尝试向该方案中的服务器发起 1000 次停止计费请求。

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

1.3.22 secondary accounting (RADIUS scheme view)

【命令】

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

undo secondary accounting [*ipv4-address* | **ipv6** *ipv6-address*]

【视图】

RADIUS 方案视图

【缺省级别】

2：系统级

【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。其中，*ipv6-address* 为合法的 IPv6 全球单播地址。

port-number：从 RADIUS 计费服务器的 UDP 端口号，缺省为 1813，取值范围为 1～65535。此端口号必须与服务器提供计费服务的端口号保持一致。

key [**cipher** | **simple**] *key*：与从 RADIUS 计费服务器交互的计费报文的共享密钥。此共享密钥必须与服务器上配置的共享密钥保持一致。

- **cipher** *key*：以密文方式设置共享密钥。*key* 为 1～117 个字符的字符串，区分大小写。
- **simple** *key*：以明文方式设置共享密钥。*key* 为 1～64 个字符的字符串，区分大小写。
- 不指定 **cipher** 和 **simple** 时，表示以明文方式设置共享密钥。

vpn-instance *vpn-instance-name*：从 RADIUS 计费服务器所属的 VPN。*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。

【描述】

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。

缺省情况下，未配置从计费服务器。

需要注意的是：

- 可通过多次执行本命令，配置多个从 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。每个 RADIUS 方案中最多支持配置 16 个从 RADIUS 计费服务器。
- 从 RADIUS 计费服务器的 IP 地址协议版本与主 RADIUS 计费服务器必须一致，并且各从 RADIUS 计费服务器的 IP 地址协议版本也必须一致。
- 主计费服务器和从计费服务器的 IP 地址不能相同，并且各从计费服务器的 IP 地址也不能相同。
- 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** [**cipher** | **simple**] *key* 命令设置的共享密钥。
- 若设备与 MPLS VPN 私网服务器通信，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 实例名称。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。
- 计费服务器与认证服务器的 IP 地址协议版本必须一致。
- 如果在发送计费开始请求过程中删除了从服务器，则设备在与当前服务器通信超时后，将会重新从主服务器开始依次查找状态为 **active** 的服务器进行通信。
- 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。
- 以明文或密文方式设置的共享密钥，均以密文的方式保存在配置文件中。

相关配置可参考命令 **key**、**state** 和 **vpn-instance** (RADIUS scheme view)。

【举例】

设置 RADIUS 方案 radius1 的从计费服务器：IP 地址分别为 10.110.1.1，10.110.1.2，均使用 UDP 端口 1813 提供 RADIUS 计费服务，计费报文的共享密钥为明文 hello。

```
<Sysname> system-view
[Sysname] radius scheme radius1
[Sysname-radius-radius1] secondary accounting 10.110.1.1 1813 key hello
[Sysname-radius-radius1] secondary accounting 10.110.1.2 1813 key hello
```

1.3.23 secondary authentication (RADIUS scheme view)

【命令】

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

undo secondary authentication [*ipv4-address* | **ipv6** *ipv6-address*]

【视图】

RADIUS 方案视图

【缺省级别】

2：系统级

【参数】

ipv4-address：从 RADIUS 认证/授权服务器的 IPv4 地址。

ipv6 *ipv6-address*：从 RADIUS 认证/授权服务器的 IPv6 地址。其中，*ipv6-address* 为合法的 IPv6 全球单播地址。

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

key [**cipher** | **simple**] *key*：从 RADIUS 认证/授权服务器的认证/授权报文的共享密钥。此共享密钥必须与服务器上配置的共享密钥保持一致。

- **cipher** *key*：以密文方式设置共享密钥。*key* 为 1～117 个字符的字符串，区分大小写。
- **simple** *key*：以明文方式设置共享密钥。*key* 为 1～64 个字符的字符串，区分大小写。
- 不指定 **cipher** 和 **simple** 时，表示以明文方式设置共享密钥。

vpn-instance *vpn-instance-name*：从 RADIUS 认证/授权服务器所属的 VPN。*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/授权服务器位于公网中。

【描述】

secondary authentication 命令用来配置从 RADIUS 认证/授权服务器。**undo secondary authentication** 命令用来删除指定的从 RADIUS 认证/授权服务器。

缺省情况下，未配置从认证/授权服务器。

需要注意的是：

- 可通过多次执行本命令，配置多个从 RADIUS 认证/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。每个 RADIUS 方案中最多支持配置 16 个从 RADIUS 计费服务器。
- 主认证/授权服务器和从认证/授权服务器的 IP 地址协议版本必须一致，并且各从 RADIUS 认证/授权服务器的 IP 地址协议版本也必须一致。
- 主认证/授权服务器和从认证/授权服务器的 IP 地址不能相同，并且各从认证服务器的 IP 地址不能相同。
- 认证/授权服务器与计费服务器的 IP 地址协议版本必须一致。
- 设备与从认证/授权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** [**cipher** | **simple**] *key* 命令设置的共享密钥。
- 若设备与 MPLS VPN 私网服务器通信，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 实例名称。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。
- 如果在认证过程中使用本命令删除了从认证服务器，则设备在与当前服务器通信超时后，将会重新从主服务器开始依次查找状态为 **active** 的服务器进行通信。
- 以明文或密文方式设置的共享密钥，均以密文的方式保存在配置文件中。

相关配置可参考命令 **key**、**state** 和 **vpn-instance** (RADIUS scheme view)。

【举例】

设置 RADIUS 方案 radius1 的从认证/授权服务器：IP 地址分别为 10.110.1.1，10.110.1.2，均使用 UDP 端口 1812 提供 RADIUS 认证/授权服务，认证/授权报文的共享密钥为明文 hello。

```
<Sysname> system-view
[Sysname] radius scheme radius1
[Sysname-radius-radius1] secondary authentication 10.110.1.1 1812 key simple hello
[Sysname-radius-radius1] secondary authentication 10.110.1.2 1812 key simple hello
```

1.3.24 security-policy-server

【命令】

security-policy-server *ip-address*

undo security-policy-server { *ip-address* | **all** }

【视图】

RADIUS 方案视图

【缺省级别】

2：系统级

【参数】

ip-address：安全策略服务器 IP 地址。

all：所有安全策略服务器。

【描述】

security-policy-server 命令用来指定安全策略服务器。**undo security-policy-server** 命令用来删除指定的安全策略服务器。

缺省情况下，未指定安全策略服务器。

需要注意的是：

- 一个 RADIUS 方案中最多可以指定 8 个安全策略服务器。
- 只有当该 RADIUS 方案没有被用户使用时，才能改变此配置。

【举例】

指定 RADIUS 方案 radius1 的安全策略服务器 IP 地址为 10.110.1.2。

```
<Sysname> system-view
[Sysname] radius scheme radius1
[Sysname-radius-radius1] security-policy-server 10.110.1.2
```

1.3.25 server-type

【命令】

server-type { **extended** | **standard** }

undo server-type

【视图】

RADIUS 方案视图

【缺省级别】

2：系统级

【参数】

extended：指定 **extended** 类型的 RADIUS 服务器（一般为 CAMS/iMC），即要求 RADIUS 客户端和 RADIUS 服务器按照私有 RADIUS 协议的规程和报文格式进行交互。

standard：指定 **standard** 类型的 RADIUS 服务器，即要求 RADIUS 客户端和 RADIUS 服务器按照标准 RADIUS 协议（RFC 2865/2866 或更新）的规程和报文格式进行交互。

【描述】

server-type 命令用来配置设备支持的 RADIUS 服务器类型。**undo server-type** 命令用来恢复缺省情况。

缺省情况下，设备支持的 RADIUS 服务器类型为 **standard**。

【举例】

将 RADIUS 方案 radius1 的 RADIUS 服务器类型设置为 **standard**。

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

1.3.26 state primary

【命令】

state primary { **accounting** | **authentication** } { **active** | **block** }

【视图】

RADIUS 方案视图

【缺省级别】

2：系统级

【参数】

accounting：设置主 RADIUS 计费服务器的状态。

authentication：设置主 RADIUS 认证/授权服务器的状态。

active：设置主 RADIUS 服务器的状态为 **active**，即处于正常工作状态。

block：设置主 RADIUS 服务器的状态为 **block**，即处于通信中断状态。

【描述】

state primary 命令用来设置主 RADIUS 服务器的状态。

缺省情况下，RADIUS 方案中配置了 IP 地址的主 RADIUS 服务器状态为 **active**。

需要注意的是：

- 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** 的从服务器进行通信。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**。

- 如果主服务器与所有从服务器状态都是 **block**，则默认使用主服务器进行认证或计费。

相关配置可参考命令 **display radius scheme** 和 **state secondary**。

【举例】

将 RADIUS 方案 radius1 的主认证服务器的状态设置为 **block**。

```
<Sysname> system-view
[Sysname] radius scheme radius1
[Sysname-radius-radius1] state primary authentication block
```

1.3.27 state secondary

【命令】

state secondary { **accounting** | **authentication** } [**ip** *ipv4-address* | **ipv6** *ipv6-address*] { **active** | **block** }

【视图】

RADIUS 方案视图

【缺省级别】

2：系统级

【参数】

accounting：设置从 RADIUS 计费服务器的状态。

authentication：设置从 RADIUS 认证/授权服务器的状态。

ip *ipv4-address*：指定从 RADIUS 服务器的 IPv4 地址。

ipv6 *ipv6-address*：指定从 RADIUS 服务器的 IPv6 地址。

active：设置从 RADIUS 服务器的状态为 **active**，即处于正常工作状态。

block：设置从 RADIUS 服务器的状态为 **block**，即处于通信中断状态。

【描述】

state secondary 命令用来设置从 RADIUS 服务器的状态。

缺省情况下，RADIUS 方案中配置了 IP 地址的各从 RADIUS 服务器状态为 **active**。

需要注意的是：

- 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/授权服务器或从计费服务器的状态。
- 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。

相关配置可参考命令 **display radius scheme** 和 **state primary**。

【举例】

将 RADIUS 方案 radius1 的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
```

1.3.28 stop-accounting-buffer enable (RADIUS scheme view)

【命令】

stop-accounting-buffer enable

undo stop-accounting-buffer enable

【视图】

RADIUS 方案视图

【缺省级别】

2：系统级

【参数】

无

【描述】

stop-accounting-buffer enable 命令用来允许在设备上缓存没有得到响应的停止计费请求报文。**undo stop-accounting-buffer enable** 命令用来禁止在设备上缓存没有得到响应的停止计费请求报文。

缺省情况下，允许设备缓存没有得到响应的停止计费请求报文。

由于停止计费请求报文涉及到话单结算、并最终影响收费多少，对用户和 ISP 都有比较重要的影响，因此设备应该尽最大努力把它发送给 RADIUS 计费服务器。所以，如果 RADIUS 计费服务器对设备发出的停止计费请求报文没有响应，设备应将其缓存在本机上，然后发送直到 RADIUS 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后将其丢弃。但在计费服务器已被删除的情况下，停止计费报文不会被缓存。

相关配置可参考命令 **reset stop-accounting-buffer** 和 **display stop-accounting-buffer**。

【举例】

指示设备能够缓存没有得到响应的停止计费请求报文。

```
<Sysname> system-view
[Sysname] radius scheme radius1
[Sysname-radius-radius1] stop-accounting-buffer enable
```

1.3.29 timer quiet (RADIUS scheme view)

【命令】

timer quiet *minutes*

undo timer quiet

【视图】

RADIUS 方案视图

【缺省级别】

2：系统级

【参数】

minutes：恢复激活状态的时间，取值范围为 0～255，单位为分钟。当该参数取值为 0 时，若当前用户使用的认证或计费服务器不可达，则设备并不会切换它的状态，而是保持其为 **active**，并且将使用该服务器的用户认证或计费的报文发送给下一个状态为 **active** 的服务器，而后续其它用户的认证请求报文仍然可以发送给该服务器进行处理。

【描述】

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。

缺省情况下，服务器恢复激活状态的时间为 5 分钟。

本命令除了可以调节服务器恢复激活状态的时间之外，还可以控制是否对不可达服务器进行状态切换。例如，若判断主服务器不可达是网络端口短暂中断或者服务器忙碌造成的，则可以结合网络的实际运行状况，将服务器的恢复激活时间置为 0，使得用户尽可能得集中在主服务器上进行认证和计费。

建议根据配置的从服务器数量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。

相关配置可参考命令 **display radius scheme**。

【举例】

设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
```

1.3.30 timer realtime-accounting (RADIUS scheme view)

【命令】

timer realtime-accounting *minutes*

undo timer realtime-accounting

【视图】

RADIUS 方案视图

【缺省级别】

2：系统级

【参数】

minutes：实时计费的时间间隔，取值范围为 0～60，非零取值必须为 3 的倍数，单位为分钟。0 表示设备不向 RADIUS 服务器发送在线用户的计费信息。

【描述】

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。

缺省情况下，实时计费的时间间隔为 12 分钟。

需要注意的是：

- 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 RADIUS 服务器发送一次在线用户的计费信息。
- 当实时计费间隔设置为 0 时，如果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对设备和 RADIUS 服务器的性能有一定的相关性要求，取值小，会增加网络中的数据流量，对设备和 RADIUS 服务器的性能要求就高；取值大，会影响计费的准确性。因此要结合网络的实际情况合理设置计费间隔的大小，一般情况下，建议当用户量比较大（*f*1000）时，尽量把该间隔的值设置得大一些。以下是实时计费间隔与用户量之间的推荐比例关系：

表1-7 实时计费间隔与用户量之间的推荐比例关系

用户数	实时计费间隔（分钟）
1～99	3
100～499	6
500～999	12
*f*1000	*f*15

相关配置可参考命令 **retry realtime-accounting** 。

【举例】

将 RADIUS 方案 radius1 的实时计费的时间间隔设置为 51 分钟。

```
<Sysname> system-view
[Sysname] radius scheme radius1
[Sysname-radius-radius1] timer realtime-accounting 51
```

1.3.31 timer response-timeout (RADIUS scheme view)

【命令】

timer response-timeout *seconds*

undo timer response-timeout

【视图】

RADIUS 方案视图

【缺省级别】

2：系统级

【参数】

seconds：RADIUS 服务器响应超时时间，取值范围为 1～10，单位为秒。

【描述】

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。

缺省情况下，RADIUS 服务器响应超时时间为 3 秒。

如果在 RADIUS 请求报文（认证/授权请求或计费请求）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 服务器响应超时时长，本命令用于调整这个时长。

需要注意的是，发送 RADIUS 报文的最大尝试次数与 RADIUS 服务器响应超时时间的乘积不能超过 75 秒。

相关配置可参考命令 **retry**。

【举例】

将 RADIUS 方案 radius1 的响应超时定时器设置为 5 秒。

```
<Sysname> system-view
[Sysname] radius scheme radius1
[Sysname-radius-radius1] timer response-timeout 5
```

1.3.32 user-name-format (RADIUS scheme view)

【命令】

user-name-format { **keep-original** | **with-domain** | **without-domain** }

【视图】

RADIUS 方案视图

【缺省级别】

2：系统级

【参数】

keep-original：发送给 RADIUS 服务器的用户名与用户输入的保持一致。

with-domain：发送给 RADIUS 服务器的用户名带 ISP 域名。

without-domain：发送给 RADIUS 服务器的用户名不带 ISP 域名。

【描述】

user-name-format 命令用来设置发送给 RADIUS 服务器的用户名格式。

缺省情况下，RADIUS 方案发送给 RADIUS 服务器的用户名携带有 ISP 域名。

需要注意的是：

- 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，那么请不要在两个乃至两个以上的 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 服务器的用户名不会有改动。

相关配置可参考命令 **radius scheme**。

【举例】

指定发送给 RADIUS 方案 radius1 中 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
```

1.3.33 vpn-instance (RADIUS scheme view)

【命令】

vpn-instance *vpn-instance-name*

undo vpn-instance

【视图】

RADIUS 方案视图

【缺省级别】

2：系统级

【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。

【描述】

vpn-instance 命令用来配置 RADIUS 方案所属的 VPN。**undo vpn-instance** 命令用来取消 RADIUS 方案所属的 VPN。

需要注意的是：

- 本命令配置的 VPN 对于该方案下的所有 IPv4 协议的 RADIUS 认证/授权/计费服务器生效，但设备优先使用配置 RADIUS 认证/授权/计费服务器时为各服务器单独指定的 VPN。
- 目前，本命令指定的 VPN 对于 IPv6 协议的 RADIUS 认证/授权/计费服务器不生效。

相关配置可参考命令 **display radius scheme**。

【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
```

1.4 HWTACACS配置命令

1.4.1 data-flow-format (HWTACACS scheme view)

【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** }

【视图】

HWTACACS 方案视图

【缺省级别】

2：系统级

【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。

【描述】

data-flow-format 命令用来配置发送到 HWTACACS 服务器的数据流的单位。**undo data-flow-format** 命令用来恢复缺省情况。

缺省情况下，数据的单位为 **byte**，数据包的单位为 **one-packet**。

需要注意的是，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。

相关配置可参考命令 **display hwtacacs**。

【举例】

在HWTACACS方案radius1中，设置发往HWTACACS服务器的数据流的数据单位为**kilo-byte**、数据包的单位为 **kilo-packet**。

```
<Sysname> system-view
[Sysname] hwtacacs scheme hwt1
[Sysname-hwtacacs-hwt1] data-flow-format data kilo-byte packet kilo-packet
```

1.4.2 display hwtacacs

【命令】

display hwtacacs [*hwtacacs-scheme-name* [**statistics**]] [**slot** *slot-number*] [**|** { **begin** | **exclude** | **include** } *regular-expression*]

【视图】

任意视图

【缺省级别】

1：监控级

【参数】

hwtacacs-scheme-name：指定 HWTACACS 方案名。

statistics：显示 HWTACACS 服务器的统计信息。不指定该参数，则显示 HWTACACS 方案的配置信息。

slot *slot-number*：显示指定成员设备上的 HWTACACS 方案的配置信息或统计信息，*slot-number* 表示设备在 IRF 中的成员编号。

|：使用正则表达式对显示信息进行过滤。有关正则表达式的详细介绍，请参见“基础配置指导”中的“CLI”。

begin：从包含指定正则表达式的行开始显示。

exclude：只显示不包含指定正则表达式的行。

include：只显示包含指定正则表达式的行。

regular-expression：表示正则表达式，为 1～256 个字符的字符串，区分大小写。

【描述】

display hwtacacs 命令用来查看 HWTACACS 方案的配置信息或 HWTACACS 服务器的统计信息。

需要注意的是：如果不指定 HWTACACS 方案名，则显示所有 HWTACACS 方案的配置信息。

相关配置请参考命令 **hwtacacs scheme**。

【举例】

查看 HWTACACS 方案 gy 的配置情况。

```
<Sysname> display hwtacacs gy
  -------------------------------------------------------------------
  HWTACACS-server template name     : gy
  Primary-authentication-server     : 172.31.1.11:49
  VPN instance                      : vpn1
  Primary-authorization-server      : 172.31.1.11:49
  VPN instance                      : vpn1
  Primary-accounting-server         : 172.31.1.11:49
  VPN instance                      : vpn1
  Secondary-authentication-server   : 0.0.0.0:0
  VPN instance                      : -
  Secondary-authorization-server    : 0.0.0.0:0
  VPN instance                      : -
  Secondary-accounting-server       : 0.0.0.0:0
```

```
VPN instance                      : -
Current-authentication-server     : 172.31.1.11:49
Current-authorization-server      : 172.31.1.11:49
Current-accounting-server         : 172.31.1.11:49
NAS-IP-address                    : 0.0.0.0
key authentication                : ******
key authorization                 : ******
key accounting                    : ******
VPN instance                      : -
Quiet-interval(min)               : 5
Realtime-accounting-interval(min) : 12
Response-timeout-interval(sec)    : 5
Acct-stop-PKT retransmit times    : 100
Username format                   : with-domain
Data traffic-unit                 : B
Packet traffic-unit               : one-packet
-----------------------------------------------------------------------
```

表1-8 display hwtacacs 命令显示信息描述表

字段	描述
HWTACACS-server template name	HWTACACS服务器方案名
Primary-authentication-server	主认证服务器IP地址/接入端口号 未配置主认证服务器时，IP地址/接入端口号显示为0.0.0.0:0。下面各服务器同理显示
Primary-authorization-server	主授权服务器IP地址/接入端口号
Primary-accounting-server	主计费服务器IP地址/接入端口号
Secondary-authentication-server	从认证服务器IP地址/接入端口号
Secondary-authorization-server	从授权服务器IP地址/接入端口号
Secondary-accounting-server	从计费服务器IP地址/接入端口号
Current-authentication-server	当前认证服务器IP地址/接入端口号
Current-authorization-server	当前授权服务器IP地址/接入端口号
Current-accounting-server	当前计费服务器IP地址/接入端口号
VPN instance	服务器所属的MPLS L3VPN
NAS-IP-address	NAS的IP地址 未指定NAS的IP地址时，此处显示为0.0.0.0
key authentication	认证密钥 • 已配置时，显示为****** • 未配置时，显示为-
key authorization	授权密钥 • 已配置时，显示为****** • 未配置时，显示为-

字段	描述
key accounting	计费密钥 • 已配置时，显示为****** • 未配置时，显示为-
Quiet-interval	主服务器恢复激活状态的时间
Realtime-accounting-interval	实时计费间隔
Response-timeout-interval	服务器响应超时间隔
Acct-stop-PKT retransmit times	停止计费报文的重传次数
Username format	发送给HWTACACS服务器的用户名格式
Data traffic-unit	数据流量单位
Packet traffic-unit	包流量单位

查看 HWTACACS 方案 gy 中各服务器的统计信息。

```
<Sysname> display hwtacacs gy statistics
---[HWTACACS template gy primary authentication]---
HWTACACS server open number: 10
HWTACACS server close number: 10
HWTACACS authen client access request packet number: 10
HWTACACS authen client access response packet number: 6
HWTACACS authen client unknown type number: 0
HWTACACS authen client timeout number: 4
HWTACACS authen client packet dropped number: 4
HWTACACS authen client access request change password number: 0
HWTACACS authen client access request login number: 5
HWTACACS authen client access request send authentication number: 0
HWTACACS authen client access request send password number: 0
HWTACACS authen client access connect abort number: 0
HWTACACS authen client access connect packet number: 5
HWTACACS authen client access response error number: 0
HWTACACS authen client access response failure number: 0
HWTACACS authen client access response follow number: 0
HWTACACS authen client access response getdata number: 0
HWTACACS authen client access response getpassword number: 5
HWTACACS authen client access response getuser number: 0
HWTACACS authen client access response pass number: 1
HWTACACS authen client access response restart number: 0
HWTACACS authen client malformed access response number: 0
HWTACACS authen client round trip time(s): 5
---[HWTACACS template gy primary authorization]---
HWTACACS server open number: 1
HWTACACS server close number: 1
HWTACACS author client request packet number: 1
HWTACACS author client response packet number: 1
```

```
HWTACACS author client timeout number: 0
HWTACACS author client packet dropped number: 0
HWTACACS author client unknown type number: 0
HWTACACS author client request EXEC number: 1
HWTACACS author client response error number: 0
HWTACACS author client response EXEC number: 1
HWTACACS author client round trip time(s): 3
---[HWTACACS template gy primary accounting]---
HWTACACS server open number: 0
HWTACACS server close number: 0
HWTACACS account client request packet number: 0
HWTACACS account client response packet number: 0
HWTACACS account client unknown type number: 0
HWTACACS account client timeout number: 0
HWTACACS account client packet dropped number: 0
HWTACACS account client request command level number: 0
HWTACACS account client request connection number: 0
HWTACACS account client request EXEC number: 0
HWTACACS account client request network number: 0
HWTACACS account client request system event number: 0
HWTACACS account client request update number: 0
HWTACACS account client response error number: 0
HWTACACS account client round trip time(s): 0
```

1.4.3 display stop-accounting-buffer (for HWTACACS)

【命令】

display stop-accounting-buffer hwtacacs-scheme *hwtacacs-scheme-name* [**slot** *slot-number*] [**|** { **begin** | **exclude** | **include** } *regular-expression*]

【视图】

任意视图

【缺省级别】

2：系统级

【参数】

hwtacacs-scheme *hwtacacs-scheme-name*：根据指定 HWTACACS 方案显示缓存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。

slot *slot-number*：显示指定成员设备上的缓存的停止计费请求报文，*slot-number* 表示设备在 IRF 中的成员编号。

|：使用正则表达式对显示信息进行过滤。有关正则表达式的详细介绍，请参见“基础配置指导”中的“CLI”。

begin：从包含指定正则表达式的行开始显示。

exclude：只显示不包含指定正则表达式的行。

include：只显示包含指定正则表达式的行。

regular-expression：表示正则表达式，为 1～256 个字符的字符串，区分大小写。

【描述】

display stop-accounting-buffer 命令用来显示缓存的没有得到响应的停止计费请求报文。

相关配置可参考命令 **reset stop-accounting-buffer**、**stop-accounting-buffer enable** 和 **retry stop-accounting**。

【举例】

显示 HWTACACS 方案 hwt1 缓存的停止计费请求报文。

```
<Sysname> display stop-accounting-buffer hwtacacs-scheme hwt1
  Slot  1:
Total 0 record(s) Matched
```

1.4.4 hwtacacs nas-ip

【命令】

hwtacacs nas-ip *ip-address* [**vpn-instance** *vpn-instance-name*]

undo hwtacacs nas-ip *ip-address* [**vpn-instance** *vpn-instance-name*]

【视图】

系统视图

【缺省级别】

2：系统级

【参数】

ip-address：指定的源 IP 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。

vpn-instance *vpn-instance-name*：指定私网源 IP 地址所属的 VPN。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。

【描述】

hwtacacs nas-ip 命令用来指定设备发送 HWTACACS 报文使用的源地址。**undo hwtacacs nas-ip** 命令用来删除指定的源地址。

缺省情况下，不指定源地址，即以发送报文的接口地址作为源地址。

需要注意的是：

- 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，为保证认证和计费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。
- 系统最多允许指定 1 个公网源地址和 15 个私网源地址。新配置的公网源地址会覆盖原有的公网源地址。而且，每一个 VPN 只能指定一个私网源地址，新配置会覆盖原有配置。
- HWTACACS 方案视图下的命令 **nas-ip** 只对本 HWTACACS 方案有效，系统视图下的命令 **hwtacacs nas-ip** 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。

相关配置可参考命令 **nas-ip**。

【举例】

配置设备发送 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
```

1.4.5 hwtacacs scheme

【命令】

hwtacacs scheme *hwtacacs-scheme-name*

undo hwtacacs scheme *hwtacacs-scheme-name*

【视图】

系统视图

【缺省级别】

3：管理级

【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。

【描述】

hwtacacs scheme 命令用来创建 HWTACACS 方案并进入其视图。**undo hwtacacs scheme** 命令用来删除指定的 HWTACACS 方案。

缺省情况下，没有定义 HWTACACS 方案。

需要注意的是：

- 一个 HWTACACS 方案可以同时被多个 ISP 域引用。
- 不允许使用 **undo hwtacacs scheme** 命令删除被 ISP 域引用的 HWTACACS 方案。

【举例】

创建名为 hwt1 的 HWTACACS 方案并进入相应的 HWTACACS 视图。

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

1.4.6 key (HWTACACS scheme view)

【命令】

key { **accounting** | **authentication** | **authorization** } [**cipher** | **simple**] *key*

undo key { **accounting** | **authentication** | **authorization** }

【视图】

HWTACACS 方案视图

【缺省级别】

2：系统级

【参数】

accounting：配置 HWTACACS 计费报文的共享密钥。

authentication：配置 HWTACACS 认证报文的共享密钥。

authorization：配置 HWTACACS 授权报文的共享密钥。

cipher：表示以密文方式设置共享密钥。

simple：表示以明文方式设置共享密钥。

key：设置的明文密钥或密文密钥，区分大小写。明文密钥为 1～255 个字符的字符串；密文密钥为 1～373 个字符的字符串。不指定 **simple** 和 **cipher** 时，表示以明文方式设置共享密钥。

【描述】

key 命令用来配置 HWTACACS 认证、授权、计费报文的共享密钥。**undo key** 命令用来删除配置。

缺省情况下，无共享密钥。

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。

以明文或密文方式设置的共享密钥，均以密文的方式保存在配置文件中。

相关配置可参考命令 **display hwtacacs**。

【举例】

配置 HWTACACS 计费报文共享密钥为明文 hello。

```
<Sysname> system-view
[Sysname] hwtacacs scheme hwt1
[Sysname-hwtacacs-hwt1] key accounting simple hello
```

配置 HWTACACS 计费报文共享密钥为明文 hello。

```
<Sysname> system-view
[Sysname] hwtacacs scheme hwt1
[Sysname-hwtacacs-hwt1] key accounting hello
```

1.4.7 nas-ip (HWTACACS scheme view)

【命令】

nas-ip *ip-address*

undo nas-ip

【视图】

HWTACACS 方案视图

【缺省级别】

2：系统级

【参数】

ip-address：指定的源 IP 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。

【描述】

nas-ip 命令用来指定设备发送 HWTACACS 报文使用的源地址。**undo nas-ip** 命令用来恢复缺省情况。

缺省情况下，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 IP 地址。

需要注意的是：

- 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，为保证认证和计费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。
- 如果重复执行此命令，新配置的源地址会覆盖原有的源地址。
- HWTACACS 方案视图下的命令 **nas-ip** 只对本 HWTACACS 方案有效，系统视图下的命令 **hwtacacs nas-ip** 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。

相关配置可参考命令 **hwtacacs nas-ip**。

【举例】

配置设备发送 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
```

1.4.8 primary accounting (HWTACACS scheme view)

【命令】

primary accounting *ip-address* [*port-number* | **vpn-instance** *vpn-instance-name*] *

undo primary accounting

【视图】

HWTACACS 方案视图

【缺省级别】

2：系统级

【参数】

ip-address：主 HWTACACS 计费服务器的 IP 地址。

port-number：主 HWTACACS 计费服务器的 TCP 端口号，缺省为 49，取值范围为 1～65535。此端口号必须与服务器提供计费服务的端口号保持一致。

vpn-instance *vpn-instance-name*：主 HWTACACS 计费服务器所属的 VPN。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。

【描述】

primary accounting 命令用来配置主 HWTACACS 计费服务器。**undo primary accounting** 命令用来删除配置的主 HWTACACS 计费服务器。

缺省情况下，未配置主计费服务器。

需要注意的是：

- 主计费服务器和从计费服务器的 IP 地址不能相同。
- 若设备与 MPLS VPN 私网服务器通信，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 实例名称。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。

相关配置可参考命令 **display hwtacacs** 和 **vpn-instance** (HWTACACS scheme view)。

【举例】

配置主 HWTACACS 计费服务器的 IP 地址为 10.163.155.12，使用 TCP 端口 49 提供 HWTACACS 计费服务。

```
<Sysname> system-view
[Sysname] hwtacacs scheme test1
[Sysname-hwtacacs-test1] primary accounting 10.163.155.12 49
```

1.4.9 primary authentication (HWTACACS scheme view)

【命令】

primary authentication *ip-address* [*port-number* | **vpn-instance** *vpn-instance-name*] *

undo primary authentication

【视图】

HWTACACS 方案视图

【缺省级别】

2：系统级

【参数】

ip-address：主 HWTACACS 认证服务器的 IP 地址。

port-number：主 HWTACACS 认证服务器的 TCP 端口号，缺省为 49，取值范围为 1～65535。此端口号必须与服务器提供认证服务的端口号保持一致。

vpn-instance *vpn-instance-name*：主 HWTACACS 认证服务器所属的 VPN。*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。

【描述】

primary authentication 命令用来配置主 HWTACACS 认证服务器。**undo primary authentication** 命令用来删除配置的主 HWTACACS 认证服务器。

缺省情况下，未配置主认证服务器。

需要注意的是：

- 主认证服务器和从认证服务器的 IP 地址不能相同。
- 若设备与 MPLS VPN 私网服务器通信，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 实例名称。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。

相关配置可参考命令 **display hwtacacs** 和 **vpn-instance** (HWTACACS scheme view)。

【举例】

配置主 HWTACACS 认证服务器的 IP 地址为 10.163.155.13，使用 TCP 端口 49 提供 HWTACACS 认证服务。

```
<Sysname> system-view
[Sysname] hwtacacs scheme hwt1
[Sysname-hwtacacs-hwt1] primary authentication 10.163.155.13 49
```

1.4.10 primary authorization

【命令】

primary authorization *ip-address* [*port-number* | **vpn-instance** *vpn-instance-name*] *

undo primary authorization

【视图】

HWTACACS 方案视图

【缺省级别】

2：系统级

【参数】

ip-address：主 HWTACACS 授权服务器的 IP 地址。

port-number：主 HWTACACS 授权服务器的 TCP 端口号，缺省为 49，取值范围为 1～65535。此端口号必须与服务器提供授权服务的端口号保持一致。

vpn-instance *vpn-instance-name*：主 HWTACACS 授权服务器所属的 VPN。*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。

【描述】

primary authorization 命令用来配置主 HWTACACS 授权服务器。**undo primary authorization** 命令用来删除配置的主 HWTACACS 授权服务器。

缺省情况下，未配置主授权服务器。

需要注意的是：

- 主授权服务器和从授权服务器的 IP 地址不能相同。
- 若设备与 MPLS VPN 私网服务器通信，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 实例名称。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。

相关配置可参考命令 **display hwtacacs** 和 **vpn-instance** (HWTACACS scheme view)。

【举例】

配置主 HWTACACS 授权服务器的 IP 地址为 10.163.155.13，使用 TCP 端口 49 提供 HWTACACS 授权服务。

```
<Sysname> system-view
[Sysname] hwtacacs scheme hwt1
[Sysname-hwtacacs-hwt1] primary authorization 10.163.155.13 49
```

1.4.11 reset hwtacacs statistics

【命令】

reset hwtacacs statistics { **accounting** | **all** | **authentication** | **authorization** } [**slot** *slot-number*]

【视图】

用户视图

【缺省级别】

1：监控级

【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。

slot *slot-number*：清除指定成员设备上的 HWTACACS 协议的统计信息，*slot-number* 表示设备在 IRF 中的成员编号。

【描述】

reset hwtacacs statistics 命令用来清除 HWTACACS 协议的统计信息。

相关配置请参考命令 **display hwtacacs**。

【举例】

清除 HWTACACS 协议的所有统计信息。

```
<Sysname> reset hwtacacs statistics all
```

1.4.12 reset stop-accounting-buffer (for HWTACACS)

【命令】

reset stop-accounting-buffer hwtacacs-scheme *hwtacacs-scheme-name* [**slot** *slot-number*]

【视图】

用户视图

【缺省级别】

2：系统级

【参数】

hwtacacs-scheme *hwtacacs-scheme-name*：根据指定 HWTACACS 方案清除缓存的停止计费请求报文。其中，*hwtacacs-server-name* 为 HWTACACS 方案名，为 1～32 个字符的字符串。

slot *slot-number*：清除指定成员设备上缓存的停止计费请求报文，*slot-number* 表示设备在 IRF 中的成员编号。

【描述】

reset stop-accounting-buffer 命令用来清除缓存中的没有得到响应的停止计费请求报文。

相关配置可参考命令 **stop-accounting-buffer enable** 和 **display stop-accounting-buffer**。

【举例】

清除 HWTACACS 方案 hwt1 缓存在系统中的停止计费请求报文。

```
<Sysname> reset stop-accounting-buffer hwtacacs-scheme hwt1
```

1.4.13 retry stop-accounting (HWTACACS scheme view)

【命令】

retry stop-accounting *retry-times*

undo retry stop-accounting

【视图】

HWTACACS 方案视图

【缺省级别】

2：系统级

【参数】

retry-times：停止计费请求报文的最大重试次数，取值范围为 1～300。

【描述】

retry stop-accounting 命令用来设置当出现没有得到响应的停止计费请求时，将该报文存入设备缓存后，发送停止计费请求报文的最大次数。**undo retry stop-accounting** 命令用来恢复缺省情况。

缺省情况下，停止计费请求报文的最大发送次数为 100。

相关配置可参考命令 **reset stop-accounting-buffer** 和 **display stop-accounting-buffer**。

【举例】

在 HWTACACS 方案 hwt1 中，设置设备最多可以尝试向该方案中的服务器发送 50 次停止计费请求报文。

```
<Sysname> system-view
[Sysname] hwtacacs scheme hwt1
[Sysname-hwtacacs-hwt1] retry stop-accounting 50
```

1.4.14 secondary accounting (HWTACACS scheme view)

【命令】

secondary accounting *ip-address* [*port-number* | **vpn-instance** *vpn-instance-name*] *

undo secondary accounting

【视图】

HWTACACS 方案视图

【缺省级别】

2：系统级

【参数】

ip-address：从 HWTACACS 计费服务器的 IP 地址。

port-number：从 HWTACACS 计费服务器的端口号，缺省为 49，取值范围为 1～65535。此端口号必须与服务器提供计费服务的端口号保持一致。

vpn-instance *vpn-instance-name*：从 HWTACACS 计费服务器所属的 VPN。*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。

【描述】

secondary accounting 命令用来配置从 HWTACACS 计费服务器。**undo secondary accounting** 命令用来删除配置的从 HWTACACS 计费服务器。

缺省情况下，未配置从计费服务器。

需要注意的是：

- 主计费服务器和从计费服务器的 IP 地址不能相同。
- 若设备与 MPLS VPN 私网服务器通信，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 实例名称。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。

相关配置可参考命令 **display hwtacacs** 和 **vpn-instance** (HWTACACS scheme view)。

【举例】

配置从 HWTACACS 计费服务器的 IP 地址为 10.163.155.12，使用 TCP 端口 49 提供 HWTACACS 计费服务。

```
<Sysname> system-view
[Sysname] hwtacacs scheme hwt1
[Sysname-hwtacacs-hwt1] secondary accounting 10.163.155.12 49
```

1.4.15 secondary authentication (HWTACACS scheme view)

【命令】

secondary authentication *ip-address* [*port-number* | **vpn-instance** *vpn-instance-name*] *

undo secondary authentication

【视图】

HWTACACS 方案视图

【缺省级别】

2：系统级

【参数】

ip-address：从 HWTACACS 认证服务器的 IP 地址。

port-number：从 HWTACACS 认证服务器的 TCP 端口号，缺省为 49，取值范围为 1～65535。此端口号必须与服务器提供认证服务的端口号保持一致。

vpn-instance *vpn-instance-name*：从 HWTACACS 认证服务器所属的 VPN。*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。

【描述】

secondary authentication 命令用来配置从 HWTACACS 认证服务器。**undo secondary authentication** 命令用来删除配置的从 HWTACACS 认证服务器。

缺省情况下，未配置从认证服务器。

需要注意的是：

- 主认证服务器和从认证服务器的 IP 地址不能相同。
- 若设备与 MPLS VPN 私网服务器通信，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 实例名称。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。

相关配置可参考命令 **display hwtacacs** 和 **vpn-instance** (HWTACACS scheme view)。

【举例】

配置从 HWTACACS 认证服务器的 IP 地址为 10.163.155.13，使用 TCP 端口 49 提供 HWTACACS 认证服务。

```
<Sysname> system-view
[Sysname] hwtacacs scheme hwt1
[Sysname-hwtacacs-hwt1] secondary authentication 10.163.155.13 49
```

1.4.16 secondary authorization

【命令】

secondary authorization *ip-address* [*port-number* | **vpn-instance** *vpn-instance-name*] *

undo secondary authorization

【视图】

HWTACACS 方案视图

【缺省级别】

2：系统级

【参数】

ip-address：从 HWTACACS 授权服务器的 IP 地址。

port-number：从 HWTACACS 授权服务器的 TCP 端口号，缺省为 49，取值范围为 1～65535。此端口号必须与服务器提供授权服务的端口号保持一致。

vpn-instance *vpn-instance-name*：从 HWTACACS 授权服务器所属的 VPN。*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。

【描述】

secondary authorization 命令用来配置从 HWTACACS 授权服务器。**undo secondary authorization** 命令用来删除配置的从 HWTACACS 授权服务器。

缺省情况下，未配置从授权服务器。

需要注意的是：

- 主授权服务器和从授权服务器的 IP 地址不能相同。
- 若设备与 MPLS VPN 私网服务器通信，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 实例名称。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。

相关配置可参考命令 **display hwtacacs** 和 **vpn-instance** (HWTACACS scheme view)。

【举例】

配置从 HWTACACS 授权服务器的 IP 地址为 10.163.155.13，使用 TCP 端口 49 提供 HWTACACS 授权服务。

```
<Sysname> system-view
[Sysname] hwtacacs scheme hwt1
[Sysname-hwtacacs-hwt1] secondary authorization 10.163.155.13 49
```

1.4.17 stop-accounting-buffer enable (HWTACACS scheme view)

【命令】

stop-accounting-buffer enable

undo stop-accounting-buffer enable

【视图】

HWTACACS 方案视图

【缺省级别】

2：系统级

【参数】

无

【描述】

stop-accounting-buffer enable 命令用来允许在设备上缓存没有得到响应的停止计费请求报文。**undo stop-accounting-buffer enable** 命令用来禁止在设备上缓存没有得到响应的停止计费请求报文。

缺省情况下，允许设备缓存没有得到响应的停止计费请求报文。

由于停止计费请求报文涉及到话单结算、并最终影响收费多少，对用户和ISP都有比较重要的影响，因此设备应该尽最大努力把它发送给HWTACACS计费服务器。所以，如果HWTACACS计费服务器对设备发出的停止计费请求报文没有响应，设备应将其缓存在本机上，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后将其丢弃。

相关配置可参考命令 **reset stop-accounting-buffer** 和 **display stop-accounting-buffer**。

【举例】

指示对于HWTACACS方案hwt1中的服务器，设备能够缓存没有得到响应的停止计费请求报文。

```
<Sysname> system-view
[Sysname] hwtacacs scheme hwt1
[Sysname-hwtacacs-hwt1] stop-accounting-buffer enable
```

1.4.18 timer quiet (HWTACACS scheme view)

【命令】

timer quiet *minutes*

undo timer quiet

【视图】

HWTACACS方案视图

【缺省级别】

2：系统级

【参数】

minutes：恢复激活状态的时间，取值范围为1～255，单位为分钟。

【描述】

timer quiet 命令用来设置主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。

缺省情况下，主服务器恢复激活状态的时间为5分钟。

相关配置可参考命令 **display hwtacacs**。

【举例】

设置主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
```

1.4.19 timer realtime-accounting (HWTACACS scheme view)

【命令】

timer realtime-accounting *minutes*

undo timer realtime-accounting

【视图】

HWTACACS方案视图

【缺省级别】

2：系统级

【参数】

minutes：实时计费的时间间隔，取值范围为 0～60，非零取值必须为 3 的倍数，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。

【描述】

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。

缺省情况下，实时计费的时间间隔为 12 分钟。

需要注意的是：

- 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对设备和 HWTACACS 服务器的性能有一定的相关性要求，取值越小，对设备和 HWTACACS 服务器的性能要求越高。建议当用户量比较大（*f*1000）时，尽量把该间隔的值设置得大一些。以下是实时计费间隔与用户量之间的推荐比例关系：

表1-9 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
*f*1000	*f*15

【举例】

将 HWTACACS 方案 hwt1 的实时计费的时间间隔设置为 51 分钟。

```
<Sysname> system-view
[Sysname] hwtacacs scheme hwt1
[Sysname-hwtacacs-hwt1] timer realtime-accounting 51
```

1.4.20 timer response-timeout (HWTACACS scheme view)

【命令】

timer response-timeout *seconds*

undo timer response-timeout

【视图】

HWTACACS 方案视图

【缺省级别】

2：系统级

【参数】

seconds：HWTACACS 服务器响应超时时间，取值范围为 1～300，单位为秒。

【描述】

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。

缺省情况下，HWTACACS 服务器响应超时时间为 5 秒。

需要注意的是，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。

相关配置可参考命令 **display hwtacacs**。

【举例】

配置 TACACS 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
```

1.4.21 user-name-format (HWTACACS scheme view)

【命令】

user-name-format { **keep-original** | **with-domain** | **without-domain** }

【视图】

HWTACACS 方案视图

【缺省级别】

2：系统级

【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 服务器的用户名带 ISP 域名。

without-domain：发送给 HWTACACS 服务器的用户名不带 ISP 域名。

【描述】

user-name-format 命令用来设置发送给 HWTACACS 服务器的用户名格式。

缺省情况下，HWTACACS 方案默认发送给 HWTACACS 服务器的用户名携带有 ISP 域名。

需要注意的是：

- 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 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】

指定发送给 HWTACACS 方案 hwt1 的用户不带 ISP 域名。

```
<Sysname> system-view
[Sysname] hwtacacs scheme hwt1
[Sysname-hwtacacs-hwt1] user-name-format without-domain
```

1.4.22 vpn-instance (HWTACACS scheme view)

【命令】

vpn-instance *vpn-instance-name*

undo vpn-instance

【视图】

HWTACACS 方案视图

【缺省级别】

2：系统级

【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。

【描述】

vpn-instance 命令用来配置 HWTACACS 方案所属的 VPN。**undo vpn-instance** 命令用来取消 HWTACACS 方案所属的 VPN。

需要注意的是，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。

相关配置可参考命令 **display hwtacacs**。

【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
```

1.5 RADIUS服务器配置命令

1.5.1 authorization-attribute（RADIUS-server user view）

【命令】

authorization-attribute { **acl** *acl-number* | **vlan** *vlan-id* } *

undo authorization-attribute { **acl** | **vlan** } *

【视图】

RADIUS 服务器用户视图

【缺省级别】

2：系统级

【参数】

acl *acl-number*：指定 RADIUS 用户的授权 ACL。其中，*acl-number* 为授权 ACL 的编号，取值范围为 2000～5999。

vlan *vlan-id*：指定 RADIUS 用户的授权 VLAN。其中，*vlan-id* 为 VLAN 编号，取值范围为 1～4094。

【描述】

authorization-attribute 命令用来设置 RADIUS 用户的授权属性，该属性在用户认证通过之后，由作为 RADIUS 服务器的设备在认证回应报文中告知 RADIUS 客户端，RADIUS 客户端将授权属性下发给用户，并对用户进行权限控制。**undo authorization-attribute** 命令用来删除配置的授权属性。

缺省情况下，未设置任何授权属性。

相关配置可参考命令 **radius-server user**。

【举例】

配置 RADIUS 用户 user1 的授权 VLAN 为 VLAN 3。

```
<Sysname> system-view
[Sysname] radius-server user user1
[Sysname-rdsuser-user1] authorization-attribute vlan 3
```

1.5.2 description (RADIUS-server user view)

【命令】

description *text*

undo description

【视图】

RADIUS 服务器用户视图

【缺省级别】

2：系统级

【参数】

text：RADIUS 用户的描述信息，为 1～255 个字符的字符串，区分大小写。

【描述】

description 命令用来配置 RADIUS 用户的描述信息。这些描述信息能够帮助管理员记忆并管理用户信息。**undo description** 命令用来取消 RADIUS 用户的描述信息。

缺省情况下，未设置 RADIUS 用户的描述信息。

相关配置可参考命令 **radius-server user**。

【举例】

配置 RADIUS 用户 user1 的描述信息为 VIP user。

```
<Sysname> system-view
[Sysname] radius-server user user1
```

```
[Sysname-rdsuser-user1] description VIP user
```

1.5.3 expiration-date (RADIUS-server user view)

【命令】

expiration-date *time*

undo expiration-date

【视图】

RADIUS 服务器用户视图

【缺省级别】

2：系统级

【参数】

time：RADIUS 用户的有效期，精确到秒，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）。其中，HH:MM:SS 中的 HH 取值范围为 0～23，MM 和 SS 取值范围为 0～59；MM/DD/YYYY 中的 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。除表示零点外，格式中的前导 0 可以省略不写，比如 2:2:0-2010/2/2 等效于 02:02:00-2010/02/02。

【描述】

expiration-date 命令用来配置 RADIUS 用户的有效期。**undo expiration-date** 用来取消 RADIUS 用户的有效期配置。

缺省情况下，未设置 RADIUS 用户的有效期，设备不进行用户有效期的检查。

在有用户需要临时接入网络的情况下，设备管理员可以为用户建立临时使用的来宾帐户，并通过该配置对来宾帐户进行有效期的控制。当该用户通过认证时，RADIUS 服务器设备检查当前系统时间是否在用户的有效期内，若在有效期内则允许用户登录，否则拒绝用户登录。

需要注意的是，如果设备管理员手工修改系统时间，或其它原因导致系统时间发生变化，则在用户认证时使用修改后的系统时间与配置的用户有效期进行比较。

相关配置可参考命令 **radius-server user**。

【举例】

配置 RADIUS 用户 user1 的有效期为 2012/05/31 的 12:10:20。

```
<Sysname> system-view
[Sysname] radius-server user user1
[Sysname-rdsuser-user1] expiration-date 12:10:20-2012/05/31
```

1.5.4 password (RADIUS-server user view)

【命令】

password [**cipher** | **simple**] *password*

undo password

【视图】

RADIUS 服务器用户视图

【缺省级别】

2：系统级

【参数】

cipher：表示以密文方式设置用户密码。

simple：表示以明文方式设置用户密码。

password：设置的明文密码或密文密码，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。不指定 **cipher** 或 **simple** 时，表示以明文方式设置用户密码。

【描述】

password 命令用来设置 RADIUS 用户的密码。**undo password** 命令用来取消 RADIUS 用户的密码。

缺省情况下，未设置 RADIUS 用户的密码。

以明文或密文方式设置的密码，均以密文的方式保存在配置文件中。

相关配置可参考命令 **radius-server user**。

【举例】

设置 RADIUS 用户 user1 的密码为明文 123456。

```
<Sysname> system-view
[Sysname] radius-server user1
[Sysname-rdsuser-user1] password simple 123456
```

1.5.5 radius-server client-ip

【命令】

radius-server client-ip *ip-address* [**key** [**cipher** | **simple**] *string*]

undo radius-server client-ip { *ip-address* | **all** }

【视图】

系统视图

【缺省级别】

2：系统级

【参数】

ip-address：RADIUS 客户端的 IPv4 地址。

key *string*：指定与 RADIUS 客户端通信的共享密钥。

cipher：表示以密文方式设置共享密钥。

simple：表示以明文方式设置共享密钥。

string：设置的明文密钥或密文密钥，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。不指定 **cipher** 或 **simple** 时，表示以明文方式设置共享密钥。

all：指定所有 RADIUS 客户端。

【描述】

radius-server client-ip 命令用来指定 RADIUS 客户端。**undo radius-server client-ip** 命令用来删除指定或所有的 RADIUS 客户端。

缺省情况下，未指定任何 RADIUS 客户端。

需要注意的是：

- 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。设备可支持的最大 RADIUS 客户端个数与设备的存储容量有关，请以设备的实际情况为准。
- 以明文或密文方式设置的密码，均以密文的方式保存在配置文件中。

【举例】

指定一个 RADIUS 客户端的 IP 地址为 10.1.1.1，共享密钥为明文 1234。

```
<Sysname> system-view
[Sysname] radius-server client-ip 10.1.1.1 key simple 1234
```

1.5.6 radius-server user

【命令】

radius-server user *user-name*

undo radius-server user { *user-name* | **all** }

【视图】

系统视图

【缺省级别】

2：系统级

【参数】

user-name：RADIUS 用户名，为 1～64 个字符的字符串，区分大小写。用户名可以携带域名，不能包括符号“?”、“<”、“>”、“\”、“"”、“%”、“'”、“&”、“#”以及空格，且不能为“a”、“al”或“all”。

all：指定所有的 RADIUS 用户。

【描述】

radius-server user 命令用来创建 RADIUS 用户并进入 RADIUS 服务器用户视图。**undo radius-server user** 命令用来删除指定或所有的 RADIUS 用户。

缺省情况下，不存在任何 RADIUS 用户。

需要注意的是：

- 设备可支持的最大 RADIUS 用户个数与设备的型号有关，请以设备的实际情况为准。
- RADIUS 服务器上添加的用户名是否携带域名要与接入设备上设置的发送给 RADIUS 服务器的用户名格式保持一致。例如，若接入设备上设置的发送给 RADIUS 服务器的用户名携带域

名（**user-name-format with-domain**），则 RADIUS 服务器上添加的 RADIUS 用户名也需要携带域名。

相关配置可参考命令 **user-name-format**（RADIUS scheme view）。

【举例】

创建名称为 user1 的 RADIUS 用户，并进入该用户视图。

```
<Sysname> system-view
[Sysname] radius-server user user1
[Sysname-rdsuser-user1]
```