目 录

1 AAA配置命令

1.1 AAA配置命令

1.1.1 aaa nas-id profile

【命令】

aaa nas-id profile *profile-name*

undo aaa nas-id profile *profile-name*

【视图】

系统视图

【缺省级别】

2：系统级

【参数】

profile-name：保存 NAS-ID 与 VLAN 绑定关系的 Profile 名称，为 1～16 个字符的字符串，不区分大小写。

【描述】

aaa nas-id profile 命令用来创建一个 NAS-ID Profile 或者进入一个已创建的 NAS-ID-Profile 视图。

undo aaa nas-id profile 命令用来删除一个指定的 NAS-ID Profile。

相关配置可参考命令 **nas-id bind vlan**。

【举例】

创建一个名字为 aaa 的 NAS-ID Profile。

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

1.1.2 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。**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。对当前 ISP 域下所能接入的用户数进行限制后，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。

【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
```

1.1.3 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。

【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，命令行计费采用缺省的计费方法。

需要注意的是：

- 当前 ISP 域所引用的 HWTACACS 方案必须是已配置的。
- 目前只有 HWTACACS 方案支持命令行计费。

相关配置可参考命令 **accounting default**、**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
```

1.1.4 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。

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。

【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。
- 本命令所配置的计费方法不区分用户类型，即对所有类型的用户都起作用。此配置的优先级低于具体接入方式的配置。
- 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 **hwtacacs scheme** 和 **radius scheme**。

【举例】

在系统缺省的 ISP 域 system 下，配置缺省计费方法为 **local**。

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

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
```

1.1.5 accounting dvpn

【命令】

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

undo accounting dvpn

【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 dvpn 命令用来为 DVPN 用户配置计费方法。**undo accounting dvpn** 命令用来恢复缺省情况。

缺省情况下，DVPN 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 DVPN 用户配置计费方法为 **local**。

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

在 ISP 域 test 下，配置 DVPN 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 dvpn radius-scheme rd local
```

1.1.6 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。

【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 用户采用命令 **accounting default** 配置的缺省计费方法。

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 **accounting default** 和 **radius scheme**。

说明

本命令仅在配置了 SAP 高密以太网板的设备上支持。

【举例】

在系统缺省的 ISP 域 system 下，为 lan-access 用户配置计费方法为 **local**。

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

1.1.7 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。

local：本地计费。实现了本地用户连接数的统计和限制，并没有实际的费用统计功能。

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。

【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 用户采用缺省的计费方法。

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。
- login 接入方式中的 FTP 服务不支持计费流程。

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

【举例】

在系统缺省的 ISP 域 system 下，为 login 用户配置计费方法为 **local**。

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

1.1.8 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。该命令适用于只认证但不关心计费的情况。
- 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
```

1.1.9 accounting portal

【命令】

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

undo accounting portal

【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。

【描述】

accounting portal 命令用来为 Portal 用户配置计费方法。**undo accounting portal** 命令用来恢复缺省情况。

缺省情况下，Portal 用户采用缺省的计费方法。

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 **accounting default** 和 **radius scheme**。

【举例】

在系统缺省的 ISP 域 system 下，为 Portal 用户配置计费方法为 **local**。

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

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

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

```
[Sysname-isp-test] accounting portal radius-scheme rd local
```

1.1.10 accounting ppp

【命令】

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

undo accounting ppp

【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。

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。

【描述】

accounting ppp 命令用来为 PPP 用户配置计费方法。**undo accounting ppp** 命令用来恢复缺省情况。

缺省情况下，PPP 用户采用缺省的计费方法。

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。

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

【举例】

在系统缺省的 ISP 域 system 下，为 PPP 用户配置计费方法为 **local**。

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

在 ISP 域 test 下，配置 PPP 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 ppp radius-scheme rd local
```

1.1.11 accounting ssl-vpn

【命令】

accounting ssl-vpn radius-scheme *radius-scheme-name*

undo accounting ssl-vpn

【视图】

ISP 域视图

【缺省级别】

2：系统级

【参数】

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 ssl-vpn 命令用来为 SSL VPN 用户配置计费方法。**undo accounting ssl-vpn** 命令用来恢复缺省情况。

缺省情况下，SSL VPN 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 **accounting default** 和 **radius scheme**。

【举例】

在 ISP 域 test 下，配置 SSL VPN 用户使用 RADIUS 方案 rd 进行计费。

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

1.1.12 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。

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。

【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。
- 本命令配置的认证方法不区分用户类型，即对所有类型的用户都起作用。此配置的优先级低于具体接入方式的配置。

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

【举例】

在系统缺省的 ISP 域 system 下，配置缺省认证方法为 **local**。

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

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
```

1.1.13 authentication dvpn

【命令】

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

undo authentication dvpn

【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 dvpn 命令用来为 DVPN 用户配置认证方案。**undo authentication dvpn** 命令用来恢复缺省情况。

缺省情况下，DVPN 用户采用当前 ISP 域的缺省认证方案。

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 DVPN 用户配置认证方法为 **local**。

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

在 ISP 域 test 下，配置 DVPN 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 dvpn radius-scheme rd local
```

1.1.14 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。

【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 用户采用缺省的认证方案。

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 **authentication default** 和 **radius scheme**。

说明

本命令仅在配置了 SAP 高密以太网板的设备上支持。

【举例】

在系统缺省的 ISP 域 system 下，为 lan-access 用户配置认证方法为 **local**。

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

1.1.15 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。

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。

【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 用户采用缺省的认证方法。

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 **authentication default**、**hwtacacs scheme** 和 **radius scheme** 。

【举例】

在系统缺省的 ISP 域 system 下，为 login 用户配置认证方法为 **local**。

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

1.1.16 authentication portal

【命令】

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

undo authentication portal

【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。

【描述】

authentication portal 命令用来为 Portal 用户配置认证方法。**undo authentication portal** 命令用来恢复缺省情况。

缺省情况下，Portal 用户采用缺省的认证方法。

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 **authentication default** 和 **radius scheme**。

【举例】

在系统缺省的 ISP 域 system 下，为 Portal 用户配置认证方法为 **local**。

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

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

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

1.1.17 authentication ppp

【命令】

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

undo authentication ppp

【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。

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。

【描述】

authentication ppp 命令用来为 PPP 用户配置认证方法。**undo authentication ppp** 命令用来恢复缺省情况。

缺省情况下，PPP 用户采用缺省的认证方法。

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 **authentication default**、**hwtacacs scheme** 和 **radius scheme**。

【举例】

在系统缺省的 ISP 域 system 下，为 PPP 用户配置认证方法为 **local**。

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

在 ISP 域 test 下，配置 PPP 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 ppp radius-scheme rd local
```

1.1.18 authentication ssl-vpn

【命令】

authentication ssl-vpn radius-scheme *radius-scheme-name*

undo authentication ssl-vpn

【视图】

ISP 域视图

【缺省级别】

2：系统级

【参数】

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 ssl-vpn 命令用来为 SSL VPN 用户配置认证方法。**undo authentication ssl-vpn** 命令用来恢复缺省情况。

缺省情况下，SSL VPN 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 **authentication default** 和 **radius scheme**。

【举例】

在 ISP 域 test 下，配置 SSL VPN 用户使用 RADIUS 方案 rd 进行认证。

```
<Sysname> system-view
[Sysname] domain system
[Sysname-isp-system] authentication ssl-vpn radius-scheme rd
```

1.1.19 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，级别切换认证采用缺省的认证方法。

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“基础配置指导/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
```

1.1.20 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。

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，命令行授权采用缺省的授权方法。

需要注意的是：

- 当前 ISP 域所引用的 HWTACACS 方案必须是已配置的。
- 对于本地授权，本地用户必须存在，而且当前要授权的命令行的级别不能大于本地用户的级别，否则本地授权失败。

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

【举例】

在系统缺省的 ISP 域 system 下，配置命令行授权方法为 **local**。

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

1.1.21 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。

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/aux/异步串口或者 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。

【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 或 HWTACACS 方案必须是已配置的。
- **authorization default** 命令配置的授权方法不区分用户类型，即对所有类型的用户都起作用。此配置的优先级低于具体接入方式的配置。
- RADIUS 授权是特殊的流程，只是在认证和授权方法中引用的 RADIUS 方案相同的条件下，RADIUS 授权起作用，否则授权失败。

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

【举例】

在系统缺省的 ISP 域 system 下，配置缺省授权方法为 **local**。

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

在 ISP 域 test 下，配置缺省计费方法为使用 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
```

1.1.22 authorization dvpn

【命令】

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

undo authorization dvpn

【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 DVPN 用户可直接接入到 VPN 域。

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 dvpn 命令用来为 DVPN 用户配置授权方法。**undo authorization dvpn** 命令用来恢复缺省情况。

缺省情况下，DVPN 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 DVPN 用户配置授权方法为 **local**。

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

在 ISP 域 test 下，配置 DVPN 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 dvpn radius-scheme rd local
```

1.1.23 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。

【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 用户采用缺省的授权方法。

需要注意的是：

- 当前 ISP 域所引用的 RADIUS 方案必须是已配置的。
- RADIUS 授权是特殊的流程，只是在认证和授权方法中引用的 RADIUS 方案相同的条件下，RADIUS 授权起作用，否则授权失败。

相关配置可参考命令 **authorization default** 和 **radius scheme**。

说明

本命令仅在配置了 SAP 高密以太网板的设备上支持。

【举例】

在系统缺省的 ISP 域 system 下，为 lan-access 用户配置授权方法为 **local**。

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

1.1.24 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。

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/aux/异步串口或者 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。

【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 用户采用缺省的授权方法。

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。
- RADIUS 授权是特殊的流程，只是在认证和授权方法中引用的 RADIUS 方案相同的条件下，RADIUS 授权起作用，否则授权失败。

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

【举例】

在系统缺省的 ISP 域 system 下，为 login 用户配置授权方法为 **local**。

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

1.1.25 authorization portal

【命令】

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

undo authorization portal

【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 Portal 用户可直接访问网络。

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

【描述】

authorization portal 命令用来为 Portal 用户配置授权方法。**undo authorization portal** 命令用来恢复缺省情况。

缺省情况下，Portal 用户采用缺省的授权方法。

需要注意的是：

- 当前 ISP 域所引用的 RADIUS 方案必须是已配置的。
- RADIUS 授权是特殊的流程，只是在认证和授权方法中引用的 RADIUS 方案相同的条件下，RADIUS 授权起作用，否则授权失败。

相关配置可参考命令 **authorization default** 和 **radius scheme**。

【举例】

在系统缺省的 ISP 域 system 下，为 Portal 用户配置授权方法为 **local**。

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

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

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

1.1.26 authorization ppp

【命令】

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

undo authorization ppp

【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。

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 PPP 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。

【描述】

authorization ppp 命令用来为 PPP 用户配置授权方法。**undo authorization ppp** 命令用来恢复缺省情况。

缺省情况下，PPP 用户采用缺省的授权方法。

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。
- RADIUS 授权是特殊的流程，只是在认证和授权方法中引用的 RADIUS 方案相同的条件下，RADIUS 授权起作用，否则授权失败。

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

【举例】

在系统缺省的 ISP 域 system 下，为 PPP 用户配置授权证方法为 **local**。

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

在 ISP 域 test 下，配置 PPP 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 ppp radius-scheme rd local
```

1.1.27 authorization ssl-vpn

【命令】

authorization ssl-vpn radius-scheme *radius-scheme-name*

undo authorization ssl-vpn

【视图】

ISP 域视图

【缺省级别】

2：系统级

【参数】

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 ssl-vpn 命令用来为 SSL VPN 用户配置授权方法。**undo authentication ssl-vpn** 命令用来恢复缺省情况。

缺省情况下，SSL VPN 用户采用当前 ISP 域的缺省授权方法。

- 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 **authorization default** 和 **radius scheme**。

【举例】

在 ISP 域 test 下，配置 SSL VPN 用户使用 RADIUS 方案 rd 进行授权。

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

1.1.28 authorization-attribute user-profile

【命令】

authorization-attribute user-profile *profile-name*

undo authorization-attribute user-profile

【视图】

ISP 域视图

【缺省级别】

3：管理级

【参数】

profile-name：指定的 User Profile 名称，为 1～31 个字符的字符串，区分大小写。User Profile 的相关配置请参考“安全配置指导”中的“User Profile”。

【描述】

authorization-attribute user-profile 命令用于配置当前 ISP 域的缺省授权 User Porfile。**undo authorization-attribute user-profile** 命令用于恢复缺省情况。

缺省情况下，当前 ISP 域无缺省授权 User Porfile。

如果当前 ISP 域的用户认证成功，但认证服务器（包括本地认证下的接入设备）未对该 ISP 域下发授权 User Porfile，则系统使用本配置指定的 User Porfile 作为当前 ISP 域的授权 User Porfile。

需要注意的是，重复配置本命令，会覆盖原有的配置。

【举例】

配置 test 域下的缺省授权 User Profile 为 profile1。

```
<Sysname> system-view
[Sysname] domain test
[Sysname-isp-test] authorization-attribute user-profile profile1
```

1.1.29 cut connection

【命令】

集中式设备：

cut connection { **access-type portal** | **all** | **domain** *isp-name* | **interface** *interface-type interface-number* | **ip** *ip-address* | **mac** *mac-address* | **ucibindex** *ucib-index* | **user-name** *user-name* }

分布式设备：

cut connection { **access-type** { **dot1x** | **mac-authentication** | **portal** } | **all** | **domain** *isp-name* | **interface** *interface-type interface-number* | **ip** *ip-address* | **mac** *mac-address* | **ucibindex** *ucib-index* | **user-name** *user-name* } [**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。各类型接入方式的为：

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

all：切断所有用户连接。

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接口。

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。输入的用户名必须带域名，否则系统默认其带缺省域名。

slot *slot-number*：指定单板所在槽位号。（分布式设备）

【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、Portal 和 PPP 服务类型的用户有效。

需要注意的是，如果 802.1X 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。

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
```

1.1.30 display connection

【命令】

集中式设备：

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

分布式设备：

display connection [**access-type** { **dot1x** | **mac-authentication** | **portal** } | **domain** *isp-name* | **interface** *interface-type interface-number* | **ip** *ip-address* | **mac** *mac-address* | **ucibindex** *ucib-index* | **user-name** *user-name*] [**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：指定接入方式。各类型接入方式为：

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

domain *isp-name*：显示指定 ISP 域下的全部用户连接。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*：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接口。

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*：显示指定连接索引的所有用户连接。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。输入的用户名必须带域名，否则系统默认其带缺省域名。

slot *slot-number*：显示指定单板上所有用户的连接，*slot-number* 表示单板所在的槽位号。（分布式设备）

|：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 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。

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。（集中式设备）

```
<Sysname> display connection

Index=1   ,Username=telnet@system
IP=10.0.0.1
IPv6=N/A
 Total 1 connection(s) matched.
```

显示所有 AAA 用户连接的相关信息。（分布式设备）

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

 Total 1 connection(s) matched on slot 0.
 Total 1 connection(s) matched.
```

显示连接索引为 0 的 AAA 用户连接的详细信息。（集中式设备）

```
<Sysname> display connection ucibindex 0
Index=0   , Username=telnet@system
IP=10.0.0.1
IPv6=N/A
Access=Admin   ,AuthMethod=PAP
Port Type=Virtual ,Port Name=N/A
ACL Group=Disable
User Profile=N/A
CAR=Disable
Priority=Disable
Start=2009-07-16 10:53:03 ,Current=2009-07-16 10:57:06 ,Online=00h04m03s
 Total 1 connection matched.
```

显示连接索引为 0 的 AAA 用户连接的详细信息。（分布式设备）

```
<Sysname> display connection ucibindex 0
Slot:  0
Index=0   , Username=telnet@system
IP=10.0.0.1
```

```
IPv6=N/A
Access=Admin    ,AuthMethod=PAP
Port Type=Virtual ,Port Name=N/A
ACL Group=Disable
User Profile=N/A
CAR=Disable
Priority=Disable
Start=2009-07-16 10:53:03 ,Current=2009-07-16 10:57:06 ,Online=00h04m03s
 Total 1 connection matched.
Slot:  1
 Total 0 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	槽位号
Index	索引号
Username	当前连接的用户名，格式为 *username@domain*
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
ACL Group	授权 ACL 组
User Profile	授权 User Profile
CAR(kbps)	授权 CAR 参数信息
Priority	用户报文的处理优先级
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

1.1.31 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 :
```

```
    User-profile : profile1

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	域名
State	状态（Active：激活、Block：阻塞）
Access-limit	接入限制数（Disabled：未使能）
Accounting method	计费方法（Required：必选、Optional：可选）
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	域用户模板
Idle-cut	闲置切断功能（Disabled：未使能、Enabled：使能）
Self-service	自助服务功能（Disabled：未使能）
Authorization attributes	授权属性
User-profile	缺省授权 User Profile 名称
Default Domain Name	缺省 ISP 域名
Total 2 domain(s).	总计 2 个 ISP 域

1.1.32 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“@”等字符。

【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：

- 使用此命令时，如果指定的 ISP 域不存在，系统将会创建一个新的 ISP 域，所有的 ISP 域在创建后即处于 **active** 状态。
- 系统中缺省存在的 ISP 域 system，不能被删除，只能修改。

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]
```

1.1.33 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：缺省的 ISP 域名，为 1～24 个字符的字符串。

【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。
- 缺省 ISP 域要生效，必须保证该域存在，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 **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
```

1.1.34 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：表示允许用户在线后连续的最大空闲时间，取值范围为 1～120，单位为分钟。

flow：表示允许用户闲置时的最小数据流量，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，当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。**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最大空闲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。

相关配置可参考命令 **domain**。

【举例】

允许 ISP 域 test 中的用户启用闲置切断功能，用户的最大空闲时间为 50 分钟，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
```

1.1.35 ip pool

【命令】

ip pool *pool-number low-ip-address* [*high-ip-address*]

undo ip pool *pool-number*

【视图】

系统视图/ISP 域视图

【缺省级别】

2：系统级

【参数】

pool-number：地址池编号，取值范围为 0～99。

low-ip-address 和 *high-ip-address*：分别为地址池的起始和结束 IP 地址。一个地址池中起始 IP 和结束 IP 地址之间的地址数不能超过 1024。如果在定义 IP 地址池时不指定结束 IP 地址，则该地址池中只有一个 IP 地址，即起始 IP 地址。

【描述】

ip pool 命令用来定义为 PPP 用户分配 IP 地址的地址池。**undo ip pool** 命令用来删除指定的 IP 地址池。

缺省情况下，没有定义为 PPP 用户分配 IP 地址的地址池。

需要注意的是：

- 在系统视图下，配置 IP 地址池。通过在接口视图下使用命令 **remote address** 为 PPP 用户分配 IP 地址。
- 在 ISP 域视图下，配置的 IP 地址池用于为相应的 ISP 域的 PPP 用户分配 IP 地址。这主要用于通过某接口接入的 PPP 用户较多，而接口所能分配的地址不够用的情况。例如，运行 PPPoE 协议的 GE 接口，最多可以接入 4096 个用户，但在该 GE 接口的 Virtual Template 上，只能配置一个地址池，而一个地址池最多只有 1024 个地址，这显然不能满足要求。通过配置 ISP 域的地址池，可以为 ISP 的 PPP 用户分配地址，从而解决接口地址池中地址不够的问题。

相关配置请参考“二层技术-广域网接入命令参考/PPP 和 MP”中的命令 **remote address**。

【举例】

配置 IP 地址池 0，地址范围为 129.102.0.1 到 129.102.0.10。

```
<Sysname> system-view
[Sysname] domain test
[Sysname-isp-test] ip pool 0 129.102.0.1 129.102.0.10
```

1.1.36 nas-id bind vlan

【命令】

nas-id *nas-identifier* **bind vlan** *vlan-id*

undo nas-id *nas-identifier* **bind vlan** *vlan-id*

【视图】

NAS-ID Profile 视图

【缺省级别】

2：系统级

【参数】

nas-identifier：NAS-ID 名称，为 1～20 个字符的字符串，区分大小写。

vlan-id：与 NAS-ID 绑定的 VLAN ID，取值范围为 1～4094。

【描述】

nas-id bind vlan 命令用来设置 NAS-ID 与 VLAN 的绑定关系，即把一个 NAS-ID 指定给一个 VLAN。**undo nas-id bind vlan** 命令用来删除一个指定的 NAS-ID 和 VLAN 的绑定关系。

缺省情况下，未设置任何绑定关系。

需要注意的是：

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

相关配置可参考命令 **aaa nas-id profile**。

【举例】

把 NAS-ID 222 指定给 VLAN 2。

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

1.1.37 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：表示自助服务器修改用户密码页面的 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。

【描述】

self-service-url enable 命令用来设置自助服务器定位功能。**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。

需要注意的是：

- 此命令需要与支持自助服务的 RADIUS 服务器配合使用，如 CAMS/iMC。自助服务即用户可以对自己的帐号或卡号进行管理和控制。安装自助服务软件的服务器即自助服务器。
- 如果在设备上配置了此命令，用户可以通过如下操作定位到自助服务器：用户在 802.1X 客户端软件上选择“更改用户密码”；客户端软件打开用户缺省的浏览器（IE 或者 NetScape 等），定位到指定的自助服务器更改用户密码的 URL 页面；用户可以在该页面上修改自己的密码。
- 只有用户通过认证后才能进行在客户端软件上选择“更改用户密码”选项，否则该选项为灰色，不可用。

【举例】

在系统缺省的 ISP 域 system 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/modPasswd1x.jsp|userName。

```
<Sysname> system-view
[Sysname] domain system
[Sysname-isp-system]                    self-service-url                    enable
http://10.153.89.94/selfservice/modPasswd1x.jsp|userName
```

1.1.38 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）。

当指示某个 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。

相关配置可参考命令 **domain**。

【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** 命令只在配置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* | **callback-number** *callback-number* | **idle-cut** *minute* | **level** *level* | **user-profile** *profile-name* | **user-role security-audit** | **vlan** *vlan-id* | **work-directory** *directory-name* } *

undo authorization-attribute { **acl** | **callback-number** | **idle-cut** | **level** | **user-profile** | **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。

callback-number *callback-number*：指定本地用户的授权 PPP 回呼号码。其中，*callback-number* 为 1～64 个字符的字符串，区分大小写。

idle-cut *minute*：启用本地用户的闲置切断功能。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。缺省值为 0。

user-profile *profile-name*：指定本地用户的授权 User Profile。其中，*profile-name* 表示用户配置文件的名称，为 1～32 个字符的字符串，只能包含英文字母、数字、下划线，且必须以英文字母开始，区分大小写。当用户通过认证上线后，其访问行为将受到 User Profile 中预设配置的限制。关于 User Profile 的详细介绍请参见“安全配置指导”中的“User Profile”。

user-role security-audit：授权本地用户的角色，对不同角色的用户下发不同的命令行使用权限。其中，**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”。该属性仅在本地用户视图下支持。

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

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。

【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。

缺省情况下，未设置任何授权属性。

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，而且本地用户授权属性的下发并不区分用户的服务类型，即会对所有类型的接入用户都下发已配置的授权属性，因此配置下发的授权属性时要考虑该类型的用户是否需要某些属性。例如，PPP 接入用户不需要下发授权目录，因此就不要设置 PPP 用户的 **work-directory** 属性。
- 用户组的授权属性对于组内的所有本地用户生效。
- 若本地用户与所属的用户组都配置了授权属性，则本地用户的配置生效。
- 如果配置登录用户界面的验证方式（**authentication-mode**）为不认证（none）或采用密码认证（password），则用户登录到系统后所能访问的命令级别由用户界面的级别确定。关于配置登录用户界面的验证方式的具体内容请参见“基础命令参考/登录设备”中的命令 **authentication-mode**；如果配置的认证方式需要用户名和口令，则用户登录系统后所能访问的命令级别由用户的级别确定。对于 SSH 用户，使用 RSA 公钥认证时，其所能使用的命令以用户界面上设置的级别为准。
- 如果通过文件系统命令删除指定的 FTP/SFTP 用户可以访问的目录，则 FTP/SFTP 用户将不能访问此目录；
- 如果在当前指定的 FTP/SFTP 用户可以访问的目录中携带备板槽位信息，则主备切换后 FTP/SFTP 用户将不能正常登录，建议用户在指定工作目录时不要携带槽位信息。
- 在系统中只有一个安全日志管理员的情况下，这个角色为安全日志管理员的本地用户就不能被删除，而且也不能去授权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。

【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 { **call-number** *call-number* [**:** *subcall-number*] | **ip** *ip-address* | **location port** *slot-number subslot-number port-number* | **mac** *mac-address* | **vlan** *vlan-id* } *

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

【视图】

本地用户视图

【缺省级别】

3：管理级

【参数】

call-number *call-number*：指定 ISDN 用户认证的主叫号码。其中 *call-number* 为 1～64 个字符的字符串。该绑定属性仅适用于 PPP 用户。

subcall-number：指定子主叫号码。如果配置了子主叫号码，则主叫号码与子主叫号码的总长度不能大于 62 个字符。

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

location 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。绑定的端口只针对端口号，不区分端口类型。该绑定属性仅适用于 lan-access 类型的用户。

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

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

【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，配置的绑定属性是本地用户进行认证时需要检测的项目，如果用户的实际属性与配置的绑定属性不符，则检测不通过，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，本地用户的 **bind-attribute ip** 命令只适用于支持 IP 地址上传功能的 802.1X 认证；对于不支持 IP 地址上传功能的 MAC 地址认证，如果配置了该命令，会导致本地认证失败。

【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】

集中式设备：

display local-user [**service-type** { **dvpn** | **ftp** | **portal** | **ppp** | **ssh** | **telnet** | **terminal** | **web** } | **state** { **active** | **block** } | **user-name** *user-name*] [**|** { **begin** | **exclude** | **include** } *regular-expression*]

分布式设备：

display local-user [**idle-cut** { **disable** | **enable** } | **service-type** { **dvpn** | **ftp** | **lan-access** | **portal** | **ppp** | **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** }：显示指定闲置切断功能的所有本地用户信息。其中，**disable** 表示禁止用户启用闲置切断功能；**enable** 表示允许用户启用闲置切断功能。

service-type：显示指定用户类型的所有本地用户信息。

- **dvpn**：DVPN 隧道用户。
- **ftp** 指定用户为 FTP 类型。
- **lan-access** 指定用户为 lan-access 类型（主要指以太网接入用户，比如 802.1X 用户）；该参数仅在配置了 SAP 高密以太网板的设备上支持。
- **portal** 为 Portal 用户。
- **ppp** 为 PPP 用户。
- **ssh** 为 SSH 用户。
- **telnet** 为 Telnet 用户；
- **terminal** 为从 CON 口、AUX 口、Asyn 口登录的终端用户；
- **web** 为 Web 用户。

state { **active** | **block** }：显示指定状态下的所有本地用户信息。其中，**active** 表示系统允许用户请求网络服务；**block** 表示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*：显示指定单板的所有本地用户信息，*slot-number* 表示单板所在的槽位号。（分布式设备）

|：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 local-user 命令用来显示所有或指定的本地用户的相关信息。

相关配置可参考命令 **local-user**。

【举例】

- 集中式设备

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:                    ppp
 Access-limit:                   Enable            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:                   0001-0002-0003
  Vlan ID:                       100
 Authorization attributes:
  Idle TimeOut:                  10(min)
  Work Directory:                cfa0:/
  User Privilege:                3
  Acl ID:                        2000
  Vlan ID:                       100
  User Profile:                  prof1
 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	本地用户状态（Active：激活、Block：阻塞）
ServiceType	本地用户使用的服务类型（ftp、lan-access、portal、ppp、ssh、telnet、terminal、web）

字段	描述
Access-limit	当前用户名的连接数限制
Current AccessNum	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	本地用户的 IP 地址
Bind location	本地用户绑定的端口
MAC address	本地用户的 MAC 地址
VLAN ID	本地用户绑定的 VLAN
Calling Number	ISDN 用户的主叫号码
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）
Callback-number	本地用户的授权 PPP 回呼号码
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
User Profile	本地用户授权 User Profile
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

- 分布式设备

显示槽位号为 0 的接口板上的本地用户 bbb 的相关信息。

```
<Sysname> display local-user user-name bbb slot 0
Slot:  0
The contents of local user bbb:
 State:                          Active
 ServiceType:                    ftp
 Access-limit:                   Enable            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:                 0001-0002-0003
  Vlan ID:                     100
 Authorization attributes:
  Idle TimeOut:                10(min)
  Work Directory:              cfa0:/
  User Privilege:              3
  Acl ID:                      2000
  Vlan ID:                     100
  User Profile:                prof1
 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1-4 display local-user 命令显示信息描述表

字段	描述
Slot	接口板所在槽位号
State	本地用户状态（Active：激活、Block：阻塞）
ServiceType	本地用户使用的服务类型（ftp、lan-access、portal、ppp、ssh、telnet、terminal）
Access-limit	当前用户名的连接数限制
Current AccessNum	当前接入用户数 ● 若不指定接口板，则显示所有接口板上该用户的接入数总和 ● 若指定接口板，则显示指定接口板上用户的接入数
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	本地用户的 IP 地址
Bind location	本地用户绑定的端口
MAC address	本地用户的 MAC 地址
VLAN ID	本地用户绑定的 VLAN
Calling Number	ISDN 用户的主叫号码
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）
Callback-number	本地用户的授权 PPP 回呼号码
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
User Profile	本地用户授权 User Profile

字段	描述
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。

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:           cfa0:
  Level:                    1
  Acl Number:               2000
  Vlan ID:                  1
  User-Profile:             1
  Callback-number:          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1-5 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 VlAN ID
User-Profile	授权 User Profile 名称
Callback-number	PPP 回呼号码
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）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 2:2:0-2008/2/2 等效于 02:02:00-2008/02/02。

【描述】

expiration-date 命令用来配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，并通过该配置对来宾帐户进行有效期的控制。当该用户进行本地认证时，接入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。

【举例】

配置用户 abc 的有效期为 2008/05/31 的 12:10:20。

```
<Sysname> system-view
[Sysname] local-user abc
[Sysname-luser-abc] expiration-date 12:10:20-2008/05/31
```

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 local-user

【命令】

local-user *user-name*

undo local-user { *user-name* | **all** [**service-type** { **ftp** | **lan-access** | **portal** | **ppp** | **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），该参数仅在配置了 SAP 高密以太网板的设备上支持；
- **portal**：表示 Portal 用户；
- **ppp**：表示 PPP 用户；
- **ssh**：表示 SSH 用户；
- **telnet**：表示 Telnet 用户；
- **terminal**：表示从 Console 口、AUX 口、Asyn 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]
```

1.2.9 local-user password-display-mode

【命令】

local-user password-display-mode { **auto** | **cipher-force** }

undo local-user password-display-mode

【视图】

系统视图

【缺省级别】

2：系统级

【参数】

auto：自动方式，即接入用户的密码显示方式与该用户通过 **password** 命令设置的密码显示方式一致。

cipher-force：强制密文方式，即所有接入用户的密码显示方式必须采用密文方式。

【描述】

local-user password-display-mode 命令用来设置所有本地用户密码的显示方式。**undo local-user password-display-mode** 命令用来恢复缺省情况。

缺省情况下，所有接入用户的密码显示方式为自动方式。

当采用 **cipher-force** 方式后：

- 即使通过 **password** 命令指定密码显示方式为明文显示（即 **simple** 方式），密码仍然会显示为密文。
- 使用 **save** 命令保存当前配置，重启设备后，即使恢复为 **auto** 方式，原来配置为明文显示的密码仍然显示为密文。

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

【举例】

设置所有本地用户采用密文方式显示密码。

```
<Sysname> system-view
[Sysname] local-user password-display-mode cipher-force
```

1.2.10 password

【命令】

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

undo password

【视图】

本地用户视图

【缺省级别】

2：系统级

【参数】

cipher：表示密码为密文显示。

simple：表示密码为明文显示。

password：表示设置的密码。明文密码可以是长度小于等于 63 的连续字符串，如：aabbcc。密文密码的长度取值为 24 或 88，如_(TT8F]Y\5SQ=^Q`MAF4<1!!。

- 对于 **simple** 方式，*password* 必须是明文密码。
- 对于 **cipher** 方式，*password* 可以是密文密码也可以是明文密码。

【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：

- 当采用 **local-user password-display-mode cipher-force** 命令后，即使用户通过 **password** 命令指定密码显示方式为明文显示（即 **simple** 方式）后，密码也会显示为密文。
- 在 **cipher** 方式下，长度小于等于 16 的明文密码会被加密为长度是 24 的密文，长度大于 16 且小于等于 63 的明文密码会被加密为长度是 88 的密文。当用户输入长度为 24 的密码时，如果密码能够被系统解密，则按密文密码处理；若不能被解密，则按明文密码处理。

相关配置可参考命令 **display local-user**。

【举例】

设置名称为 user1 的密码为明文显示，密码为 123456。

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

1.2.11 service-type

【命令】

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

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

【视图】

本地用户视图

【缺省级别】

3：管理级

【参数】

dvpn：指定用户可以使用 DVPN 服务。

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

lan-access：指定用户可以使用 lan-access 服务。主要指以太网接入用户，比如 802.1X 用户。该参数仅在配置了 SAP 高密以太网板的设备上支持。

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、AUX 口、Asyn 口登录）。

portal：指定用户可以使用 Portal 服务。

ppp：指定用户可以使用 PPP 服务。

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。

【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]
```

1.3 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，包括使能 accounting-on 功能、配置 accounting-on 报文重发时间间隔和 accounting-on 报文的最大发送次数。在 accounting-on 功能处于使能的情况下，设备重启后，会发送 accounting-on 报文通知 RADIUS 服务器该设备已经重启，要求 RADIUS 服务器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：

- 设备启动后，如果当前系统中没有使能 accounting-on 功能的 RADIUS 方案，则执行完该命令后，必须执行 **save** 操作，这样设备重启后 accounting-on 功能才能生效。
- 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。

相关配置可参考命令 **radius scheme**。

【举例】

使能 RADIUS 认证方案 rd 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 rd
[Sysname-radius-rd] 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：设置数据的单位。

byte：数据单位为字节。

giga-byte：数据单位千兆字节。

kilo-byte：数据单位为千字节。

mega-byte：数据单位为兆字节。

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 RADIUS 服务器的数据流单位应与 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】

设置发往 RADIUS 服务器的数据流的数据单位为千字节、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】

集中式设备：

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

分布式设备：

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*：显示指定单板上的 RADIUS 方案配置信息，*slot-number* 表示单板所在的槽位号。（分布式设备）

|：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。
- 如果不指定单板所在槽位号，则仅显示主控板上 RADIUS 方案的配置信息。
- 如果不指定成员设备编号，则显示所有成员设备上 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 : 345
    VPN instance   : 1
  Primary Acct Server:
    IP: 1.1.1.1                                 Port: 1813   State: active
    Encryption Key : 345
    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 : 123
  Acct Server Encryption Key : N/A
  VPN instance               : N/A
  Accounting-On packet disable, send times : 5 , 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1-6 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	RADIUS 服务器的类型
Primary Auth Server	主认证服务器
Primary Acct Server	主计费服务器
Second Auth Server	从认证服务器
Second Acct Server	从计费服务器
Encryption Key	认证/计费服务器的共享密钥
IP	主认证/计费服务器 IP 地址 未配置时，显示为 N/A
Port	主认证/计费服务器接入端口号 未配置时，显示缺省值
State	主认证/计费服务器目前状态 ● active：激活 ● block：阻塞
VPN instance	服务器所属的 MPLS L3VPN
Auth Server Encryption Key	认证服务器的共享密钥
Acct Server Encryption Key	计费服务器的共享密钥
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)	超时时间(秒)

字段	描述
Retransmission times for timeout	超时重发次数
Interval for realtime accounting(minute)	实时计费间隔(分钟)
Retransmission times of realtime-accounting packet	实时计费报文重发次数
Retransmission times of stop-accounting packet	无响应停止计费报文重发次数
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	流量数据的单位
Packet unit	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】

集中式设备：

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

分布式设备：

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*：显示指定接口板上 RADIUS 报文的统计信息，*slot-number* 表示单板所在的槽位号。（分布式设备）

|：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】

- 集中式设备

显示 RADIUS 报文的统计信息。

```
<Sysname> display radius statistics
state statistic(total=18000):
     DEAD = 18000     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:
Auth request             Num = 24       Err = 0        Succ = 24
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 = 0        Err = 0        Succ = 0
Accounting on response   Num = 1        Err = 0        Succ = 0
Distribute request       Num = 0        Err = 0        Succ = 0
RADIUS sent messages statistic:
Auth accept              Num = 10
Auth reject              Num = 14
Auth continue            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1-7 display radius statistics 命令显示信息描述表

字段	描述
state statistic(total=18000)	状态统计（总数=18000）
DEAD	空闲态用户数
AuthProc	认证等待态用户数
AuthSucc	认证成功态用户数
AcctStart	计费开始态用户数
RLTSend	实时计费发送态用户数
RLTWait	实时计费等待态用户数
AcctStop	计费等待停止态用户数
OnLine	在线态用户数
Stop	停止态用户数
Received and Sent packets statistic	收发报文数目统计
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	错误报文数
Running statistic	运行间报文数目统计
RADIUS received messages statistic	RADIUS 已接收消息数目统计
Auth request	普通认证请求报文数
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

字段	描述
PKT response	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
Succ	成功报文数
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
Distribute request	分发请求报文数
RADIUS sent messages statistic	RADIUS 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
Auth continue	继续进行认证过程的报文数
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

- 分布式设备

显示槽位号为 0 的单板上的 RADIUS 报文统计信息。

```
<Sysname> display radius statistics slot 0
 Slot  0:state statistic(total=8000):
     DEAD = 8000     AuthProc = 0        AuthSucc = 0
AcctStart = 0         RLTSend = 0         RLTWait = 0
 AcctStop = 0          OnLine = 0            Stop = 0
 StateErr = 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:
Auth request             Num = 24       Err = 0        Succ = 24
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 = 0        Err = 0        Succ = 0
Accounting on response   Num = 0        Err = 0        Succ = 0
Distribute request       Num = 0        Err = 0        Succ = 0
RADIUS sent messages statistic:
Auth accept              Num = 10
Auth reject              Num = 14
Auth continue            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1-8 display radius statistics 命令显示信息描述表

字段	描述
slot	接口板所在槽位号
state statistic(total=18000)	状态统计（总数=18000）

字段	描述
DEAD	空闲态用户数
AuthProc	认证等待态用户数
AuthSucc	认证成功态用户数
AcctStart	计费开始态用户数
RLTSend	实时计费发送态用户数
RLTWait	实时计费等待态用户数
AcctStop	计费等待停止态用户数
OnLine	在线态用户数
Stop	停止态用户数
StateErr	未知错误态用户数
Received and Sent packets statistic	收发报文数目统计
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	错误报文数
Running statistic	运行间报文数目统计
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
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	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
Succ	成功报文数

字段	描述
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
Distribute request	分发请求报文数
RADIUS sent messages statistic	RAIUDS 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
Auth continue	继续进行认证过程的报文数
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

【命令】

集中式设备：

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

分布式设备：

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*：根据指定 RADIUS 方案显示缓存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*：根据指定会话 ID 显示缓存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*：根据停止计费请求时刻的起始和停止时间显示缓存的停止计费请求报文。其中，*start-time* 为请求时间段的起始时间；*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）。如果使用本参数，则停止计费请求时刻在 *start-time* 到 *stop-time* 范围内的、暂存的停止计费请求报文都会被显示。

user-name *user-name*：根据指定用户名显示缓存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*：显示指定接口板上缓存的停止计费请求报文，*slot-number* 表示单板所在的槽位号。（分布式设备）

|：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。

需要注意的是：

- 可以选择显示发往某个 RADIUS 方案的报文；也可以根据用户会话的 *session-id* 或用户名来显示报文；还可以指定一个时间段，显示那些发起停止计费请求的时刻处于指定时间段内的报文。根据显示的报文信息，可以帮助诊断与排除 RADIUS 相关故障。
- 在发送停止计费请求报文而 RADIUS 服务器没有响应时，设备系统会缓存该报文，然后以一定的次数发送，具体发送的次数由 **retry stop-accounting** 命令设置。

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

【举例】

- 集中式设备

显示从 2006 年 8 月 31 日 0 点 0 分 0 秒到 2006 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> display stop-accounting-buffer time-range 0:0:0-08/31/2006 23:59:59-08/31/2006
Total find    0 record（0）
```

- 分布式设备

在槽位号为 0 的单板上，显示从 2006 年 8 月 31 日 0 点 0 分 0 秒到 2006 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> display stop-accounting-buffer time-range 0:0:0-08/31/2006 23:59:59-08/31/2006
slot 0
 Slot  0:
Total 0 record(s) Matched
```

1.3.7 key (RADIUS scheme view)

【命令】

key { **accounting** | **authentication** } *string*

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。

string：密钥，为 1～64 个字符的字符串，区分大小写。

【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：

- 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 的认证/授权报文的共享密钥设置为 hello。

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

将 RADIUS 方案 radius1 的计费报文的共享密钥设置为 ok。

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

1.3.8 nas device-id

【命令】

nas device-id *device-id*

undo nas device-id

【视图】

系统视图

【缺省级别】

2：系统级

【参数】

device-id：表示设备 ID，取值为 1 或 2。

【描述】

nas device-id 命令用于配置双机热备模式下的设备 ID。双机热备组网环境下的两台设备的设备 ID 分别为 1 和 2。**undo nas device-id** 命令用于恢复缺省情况。

缺省情况下，设备工作在单机模式，无设备 ID。

需要注意的是：

- 改变设备 ID 后，设备上所有在线用户均会被强制下线。
- 为保证双机模式下两台设备之间的业务备份正常工作，需要保证两台设备的设备 ID 分别为 1 和 2。
- 由于设备 ID 是设备运行在双机模式下的标志，因此单机运行的环境下，不建议配置此命令。

说明

本命令仅集中式设备支持。

【举例】

在双机热备的组网环境中，配置本端设备运行在双机热备模式，设备 ID 为 1。

```
<Sysname> system-view
[Sysname] nas device-id 1
Warning: This command will cut all user connections on this device. Continue? [Y
/N]
```

在对端设备上，应该配置设备的设备 ID 为 2。

1.3.9 nas-backup-ip

【命令】

nas-backup-ip *ip-address*

undo nas-backup-ip

【视图】

RADIUS 方案视图

【缺省级别】

2：系统级

【参数】

ip-address：指定的备份源 IP 地址，禁止配置全 0 地址、全 1 地址、D 类地址、E 类地址和环回地址。在双机热备运行的环境下，此地址必须指定为对端设备上发送 RADIUS 报文的源 IP 地址。

【描述】

nas-backup-ip 命令用来设置设备发送 RADIUS 报文使用的备份源 IP 地址。**undo nas-backup-ip** 命令用来恢复缺省情况。

缺省情况下，未指定设备发送 RADIUS 报文使用的备份源 IP 地址。

需要注意的是：

- 指定发送 RADIUS 报文使用的备份源 IP 地址，可以保证双机热备环境中主设备发生故障时，服务器发送的报文可以被备份设备收到并进行处理。
- RADIUS 方案视图下的命令 **nas-backup-ip** 只对本 RADIUS 方案有效，系统视图下的命令 **radius nas-backup-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。
- 本命令只能指定一个备份源 IP 地址，新配置的备份源 IP 地址会覆盖原有的备份源 IP 地址。

相关配置可参考命令 **nas-ip** 或 **radius nas-ip**。

说明

本命令仅集中式设备支持。

【举例】

在双机热备的组网环境中，设置本端设备发送 RADIUS 报文使用的源 IP 地址为 2.2.2.2，备份源 IP 为 3.3.3.3。

```
<Sysname> system-view
[Sysname] radius scheme aaa
[Sysname-radius-aaa] nas-ip 2.2.2.2
[Sysname-radius-aaa] nas-backup-ip 3.3.3.3
```

在对端设备上，应该设置设备发送 RADIUS 报文使用的源 IP 地址为 3.3.3.3，备份源 IP 为 2.2.2.2。

1.3.10 nas-ip (RADIUS scheme view)

【命令】

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

undo nas-ip

【视图】

RADIUS 方案视图

【缺省级别】

2：系统级

【参数】

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

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

【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。

需要注意的是：

- 指定发送 RADIUS 报文使用的源地址，可以避免物理接口故障时从服务器返回的报文不可达。一般推荐使用 Loopback 接口地址。
- 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，否则配置能成功但不能生效。

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 test1
[Sysname-radius-test1] nas-ip 10.1.1.1
```

1.3.11 primary accounting (RADIUS scheme view)

【命令】

primary accounting { *ip-address* | **ipv6** *ipv6-address* } [*port-number* | **key** *string* | **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】

ip-address：主 RADIUS 计费服务器的 IPv4 地址。

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

port-number：UDP 端口号，缺省为 1813，取值范围为 1～65535。

key *string*：主 RADIUS 计费服务器的计费报文的共享密钥，为 1～64 个字符的字符串，区分大小写。

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，否则将提示配置不成功。
- 需保证设备上的 RADIUS 服务端口与 RADIUS 服务器上的端口设置一致。
- 需保证设备上设置的计费报文的共享密钥与 RADIUS 服务器上的完全一致。
- 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** *string* 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，需保证本命令中指定的 VPN 实例和服务器实际所在的 VPN 实例一致。
- 主计费服务器和从计费服务器的 IP 地址协议版本必须一致，否则提示错误。
- 计费服务器与认证服务器的 IP 地址协议版本必须一致，否则提示错误。
- 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。
- 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。

相关配置可参考命令 **key**、**radius scheme**、**state** 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。

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

1.3.12 primary authentication (RADIUS scheme view)

【命令】

primary authentication { *ip-address* | **ipv6** *ipv6-address* } [*port-number* | **key** *string* | **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】

ip-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。

port-number：UDP 端口号，缺省为 1812，取值范围为 1～65535。

key *string*：主 RADIUS 认证/授权服务器的认证/授权报文的共享密钥，为 1～64 个字符的字符串，区分大小写。

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：

- 当创建一个新的 RADIUS 方案之后，需要对属于此方案的 RADIUS 服务器的 IP 地址和 UDP 端口号进行设置。这些服务器包括认证/授权和计费服务器，而每种服务器又有主服务器和从服务器的区别。在实际组网环境中，上述参数的设置需要根据具体需求来决定。但是必须至少设置一个认证/授权服务器和一个计费服务器。同时在配置过程中，请保证设备上的 RADIUS 服务端口设置与 RADIUS 服务器上的端口设置保持一致。
- 需保证设备上设置的认证/授权报文的共享密钥与 RADIUS 服务器上的完全一致。
- 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** *string* 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，需保证本命令中指定的 VPN 和服务器实际所在的 VPN 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，否则将提示配置不成功。
- 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，否则提示错误。
- 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，否则提示错误。
- 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。
- 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。

相关配置可参考命令 **key**、**radius scheme**、**state** 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。

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

1.3.13 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，RADIUS 可以接受认证/授权/计费请求，也可以处理 RADIUS 的定时器消息，但报文发送会失败，同时不能接收来自 RADIUS 服务器的报文。
- 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，且不能被缓存。同时，RADIUS 服务器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。
- 关闭 RADIUS 客户端的监听端口后，如果配置了 RADIUS 方案和本地认证/授权/计费方法，则 RADIUS 请求失败后会转由本地方法继续认证/授权/计费。
- 关闭 RADIUS 客户端的监听端口后，缓存的计费报文的发送会失败，失败次数达到配置的最大次数后，计费报文将从缓存中被删除。

【举例】

使能 RADIUS 客户端的监听端口。

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

1.3.14 radius nas-backup-ip

【命令】

radius nas-backup-ip *ip-address* [**vpn-instance** *vpn-instance-name*]

undo radius nas-backup-ip

【视图】

系统视图

【缺省级别】

2：系统级

【参数】

ip-address：指定的备份源 IP 地址，禁止配置全 0 地址、全 1 地址、D 类地址、E 类地址和环回地址。在双机热备运行的环境下，此地址必须指定为对端设备上发送 RADIUS 报文的源 IP 地址。**vpn-instance** *vpn-instance-name*：备份源 IP 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。若指定该参数，则表示配置的是私网备份源地址；若不指定该参数，则表示配置的是公网备份源地址。

【描述】

radius nas-backup-ip 命令用来设置设备发送 RADIUS 报文使用的备份源 IP 地址。**undo radius nas-backup-ip** 命令用来恢复缺省情况。

缺省情况下，未指定设备发送 RADIUS 报文使用的备份源 IP 地址。

需要注意的是：

- 设置发送 RADIUS 报文使用的备份源 IP 地址，可以保证双机热备环境中主设备发生故障时，服务器发送的报文可以被备份设备收到并进行处理。
- 包括公网备份源地址和私网备份源地址在内，系统最多允许指定 16 个备份源地址。其中，最多只能指定一个公网备份源地址，新配置的公网备份源地址会覆盖原有的公网备份源地址。而且，每一个 VPN 只能指定一个私网备份源地址，新配置会覆盖原有配置。
- RADIUS 方案视图下的命令 **nas-backup-ip** 只对本 RADIUS 方案有效，系统视图下的命令 **radius nas-backup-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-backup-ip**。

说明

本命令仅集中式设备支持。

【举例】

在双机热备的组网环境中，设置本端设备发送 RADIUS 报文使用的源 IP 地址为 2.2.2.2，备份源 IP 为 3.3.3.3。

```
<Sysname> system-view
[Sysname] radius nas-ip 2.2.2.2
[Sysname] radius nas-backup-ip 3.3.3.3
```

在对端设备上，应该设置设备发送 RADIUS 报文使用的源 IP 地址为 3.3.3.3，备份源 IP 为 2.2.2.2。

1.3.15 radius nas-ip

【命令】

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

undo radius nas-ip { *ip-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】

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

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

vpn-instance *vpn-instance-name*：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。若指定该参数，则表示配置的是私网源地址；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：

- 包括公网源地址和私网源地址在内，系统最多允许指定 16 个源地址。其中，最多只能指定一个公网源地址，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 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 地址与使用该源地址的 RADIUS 方案中设置的服务器 IP 地址的协议版本必须保持一致，否则配置能成功但不能生效。

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
```

1.3.16 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：

- RADIUS 协议的配置是以 RADIUS 方案为单位进行的。每个 RADIUS 方案至少须指明 RADIUS 认证/授权/计费服务器的 IP 地址、UDP 端口号以及 RADIUS 客户端与之交互所需的一些参数。
- 一个 RADIUS 方案可以同时被多个 ISP 域引用。
- 当有使用 RADIUS 方案的用户在线时，不允许使用 **undo radius scheme** 命令删除该方案。

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]
```

1.3.17 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与认证请求总数的百分比，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，NAS 认为服务器不可达，并发送 Trap 信息。具体为，当 NAS 向服务器发送的报文累计次数达到最大传送次数时，系统发送一次 Trap 报文。
- 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
```

1.3.18 reset radius statistics

【命令】

集中式设备：

reset radius statistics

分布式设备：

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*：清除指定单板上 RADIUS 协议的统计信息，*slot-number* 表示单板所在的槽位号。（分布式设备）

【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 scheme**。

【举例】

清除 RADIUS 协议的统计信息。

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

1.3.19 reset stop-accounting-buffer

【命令】

集中式设备：

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

分布式设备：

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*：根据指定单板清除缓存的停止计费响应报文，*slot-number* 表示单板所在的槽位号。（分布式设备）。

【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**、**retry stop-accounting**、**user-name-format** 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 2006 年 8 月 31 日 0 点 0 分 0 秒到 2006 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 0:0:0-08/31/2006 23:59:59-08/31/2006
```

1.3.20 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，则设备将认为本次认证失败。
- 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
```

1.3.21 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，最多允许 5 次实时计费请求无响应。

需要注意的是：

- 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 服务器长时间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，在设备端尽量与 RADIUS 服

务器同步切断用户连接。设备提供对连续实时计费请求无响应次数限制的设置——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，设备将切断用户连接。

- 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，设备允许实时计费失败的最大次数为 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 **radius scheme** 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
```

1.3.22 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，允许停止计费请求无响应的最大次数。**undo retry stop-accounting** 命令用来恢复缺省情况。

缺省情况下，缓存的停止计费请求报文的最大发送次数为 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，如果重传 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 **radius scheme** 和 **display stop-accounting-buffer**。

【举例】

设置对于 RADIUS 方案 radius1 中的服务器，设备最多可以将缓存的停止计费请求报文发送 1000 次。

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

1.3.23 secondary accounting (RADIUS scheme view)

【命令】

secondary accounting { *ipv4-address* | **ipv6** *ipv6-address* } [*port-number* | **key** *string* | **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。

port-number：UDP 端口号，缺省为 1813，取值范围为 1～65535。

key *string*：从 RADIUS 计费服务器的计费报文的共享密钥，为 1～64 个字符的字符串，区分大小写。

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，否则提示错误。
- 主计费服务器和从计费服务器的 IP 地址不能相同，并且各个从计费服务器的 IP 地址也不能相同，否则将提示配置不成功。
- 需保证设备上的 RADIUS 服务端口与 RADIUS 服务器上的端口设置一致。
- 需保证设备上设置的计费报文的共享密钥与 RADIUS 服务器上的完全一致。

- 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** *string* 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，需保证本命令中指定的 VPN 和服务器实际所在的 VPN 一致。
- 计费服务器与认证服务器的 IP 地址协议版本必须一致，否则提示错误。
- 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。

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

【举例】

设置 RADIUS 方案 radius1 的从计费服务器的 IP 地址为 10.110.1.1，使用 UDP 端口 1813 提供 RADIUS 计费服务。

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

设置 RADIUS 方案 radius2 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。

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

1.3.24 secondary authentication (RADIUS scheme view)

【命令】

secondary authentication { *ipv4-address* | **ipv6** *ipv6-address* } [*port-number* | **key** *string* | **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。

port-number：UDP 端口号，缺省为 1812，取值范围为 1～65535。

key *string*：从 RADIUS 认证/授权服务器的认证/授权报文的共享密钥，为 1～64 个字符的字符串，区分大小写。

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，否则提示错误。
- 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，否则将提示配置不成功。
- 需保证设备上的 RADIUS 服务端口与 RADIUS 服务器上的端口设置一致。
- 需保证设备上设置的认证/授权报文的共享密钥与 RADIUS 服务器上的完全一致。
- 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** *string* 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，需保证本命令中指定的 VPN 和服务器实际所在的 VPN 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，否则提示错误。
- 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。

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

【举例】

设置 RADIUS 方案 radius1 的从认证/授权服务器的 IP 地址为 10.110.1.2，使用 UDP 端口 1812 提供 RADIUS 认证/授权服务。

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

设置 RADIUS 方案 radius2 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。

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

1.3.25 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 IP 地址。

【描述】

security-policy-server 命令用来设置安全策略服务器。**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 方案中可以配置多个安全策略服务器 IP 地址，最多不能超过 8 个。
- 只有当该 RADIUS 方案没有被用户使用时，才能改变此配置。

相关配置可参考命令 **radius nas-ip**。

【举例】

设置 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
```

1.3.26 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**。

相关配置可参考命令 **radius scheme**。

【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
```

1.3.27 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 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
```

1.3.28 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 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/授权服务器或从服务器计费的状态。
- 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** 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
```

1.3.29 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**、**radius scheme** 和 **display stop-accounting-buffer**。

【举例】

指示对于 RADIUS 方案 radius1 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] radius scheme radius1
[Sysname-radius-radius1] stop-accounting-buffer enable
```

1.3.30 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 test1
[Sysname-radius-test1] timer quiet 10
```

1.3.31 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，单位为分钟，非零取值必须为 3 的倍数。

【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1-9 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

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

【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
```

1.3.32 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 服务器应答超时时间，取值范围为 1～10，单位为秒。

【描述】

timer response-timeout 命令用来设置 RADIUS 服务器应答超时时间。**undo timer response-timeout** 命令用来恢复缺省情况。

缺省情况下，RADIUS 服务器应答超时时间为 3 秒。

需要注意的是：

- 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，以保证用户确实能够得到 RADIUS 服务，这段时间被称为 RADIUS 服务器响应超时时长。设备系统中用于控制这个时长的定时器就被称为 RADIUS 服务器响应超时定时器，命令 **timer response-timeout** 就是用来设置这个定时器时长的。
- 根据网络状况，合理地设置这个定时器的时长，有利于提高系统性能。
- 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 **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
```

1.3.33 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。

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
```

1.3.34 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 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 **radius scheme** 和 **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：设置数据的单位。

byte：数据单位为字节。

giga-byte：数据单位千兆字节。

kilo-byte：数据单位为千字节。

mega-byte：数据单位为兆字节。

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**。

相关配置可参考命令 **display hwtacacs**。

【举例】

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】

集中式设备：

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

分布式设备：

display hwtacacs [*hwtacacs-scheme-name* [**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】

hwtacacs-scheme-name：指定 HWTACACS 方案名。

statistics：显示 HWTACACS 服务器的详细统计信息。

slot *slot-number*：显示指定单板上的 HWTACACS 方案的配置信息或统计信息，*slot-number* 表示单板所在的槽位号。（分布式设备）

|：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。
- 如果不指定单板所在槽位号，则显示主控板上 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
  VPN instance                      : -
  Current-authorization-server      : 172.31.1.11:49
  VPN instance                      : -
  Current-accounting-server         : 172.31.1.11:49
  VPN instance                      : -
  NAS-IP-address                    : 0.0.0.0
  key authentication                : 790131
  key authorization                 : 790131
```

```
key accounting                    : 790131
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1-10 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	备认证服务器 IP 地址/接入端口号
Secondary-authorization-server	备授权服务器 IP 地址/接入端口号
Secondary-accounting-server	备计费服务器 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 ● 未指定时，IP 地址显示为 0.0.0.0
key authentication	认证密钥
key authorization	授权密钥
key accounting	计费密钥
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

1.4.3 display stop-accounting-buffer

【命令】

集中式设备：

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

分布式设备：

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*：显示指定单板上的缓存的停止计费请求报文，*slot-number* 表示单板的槽位号。（分布式设备）

|：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】

- 集中式设备

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
Total 0 record(s) Matched
```

- 分布式设备

在槽位号为 0 的接口板上，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 0
  Slot  0:
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 类地址和环回地址。

vpn-instance *vpn-instance-name*：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。若指定该参数，则表示配置的是私网源地址；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：

- 指定发送 HWTACACS 报文使用的源地址，可以避免物理接口故障时从服务器返回的报文不可达。
- 包括公网源地址和私网源地址在内，系统最多允许指定 16 个源地址。其中，最多只能指定一个公网源地址，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，当有使用 HWTACACS 方案的用户在线时，不允许使用 **undo hwtacacs scheme** 命令删除该方案。

【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** } *string*

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

【视图】

HWTACACS 方案视图

【缺省级别】

2：系统级

【参数】

accounting：指示 HWTACACS 计费报文的共享密钥。

authentication：指示 HWTACACS 认证报文的共享密钥。

authorization：指示 HWTACACS 授权报文的共享密钥。

string：密钥，为 1～64 个字符的字符串，区分大小写。

【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。

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 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 类地址和环回地址。

【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，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：

- 指定发送 HWTACACS 报文使用的源地址，可以避免物理接口故障时从服务器返回的报文不可达。
- 本命令只能指定一个源地址，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，必须是合法的单播地址。

port-number：主 HWTACACS 计费服务器的端口号，缺省为 49，取值范围为 1～65535。

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，否则将提示配置不成功。
- 需保证设备上的 HWTACACS 服务端口与 HWTACACS 服务器上的端口设置一致。
- 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，需保证本命令中指定的 VPN 实例和服务器实际所在的 VPN 实例一致。
- 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。
- 如果重复执行此命令，新的配置将覆盖原来的配置。
- 只有当没有活跃、用于发送计费报文的 TCP 连接使用该计费服务器时，才允许删除该服务器。删除服务器只对之后的报文有效。

相关配置可参考命令 **display hwtacacs**、**hwtacacs scheme** 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，必须是合法的单播地址。

port-number：主 HWTACACS 认证服务器的端口号，缺省为 49，取值范围为 1～65535。

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，否则将提示配置不成功。
- 需保证设备上的 HWTACACS 服务端口与 HWTACACS 服务器上的端口设置一致。
- 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，需保证本命令中指定的 VPN 和服务器实际所在的 VPN 一致。
- 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。
- 如果重复执行此命令，新的配置将覆盖原来的配置。
- 只有当没有活跃的、用于发送认证报文的 TCP 连接使用该认证服务器时，才允许删除该服务器。删除服务器只对之后的报文有效。

相关配置可参考命令 **display hwtacacs**、**hwtacacs scheme** 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，必须是合法的单播地址。

port-number：主 HWTACACS 授权服务器的端口号，缺省为 49，取值范围为 1～65535。

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，否则将提示配置不成功。
- 需保证设备上的 HWTACACS 服务端口与 HWTACACS 服务器上的端口设置一致。
- 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，需保证本命令中指定的 VPN 和服务器实际所在的 VPN 一致。
- 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。
- 如果重复执行此命令，新的配置将覆盖原来的配置。
- 只有当没有活跃的、用于发送授权报文的 TCP 连接使用该授权服务器，才允许删除该服务器。删除服务器只对之后的报文有效。

相关配置可参考命令 **display hwtacacs**、**hwtacacs scheme** 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】

集中式设备：

reset hwtacacs statistics { **accounting** | **all** | **authentication** | **authorization** }

分布式设备：

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*：清除指定单板板上的 HWTACACS 协议的统计信息，*slot-number* 表示单板所在的槽位号。（分布式设备）

【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

【命令】

集中式设备：

reset stop-accounting-buffer hwtacacs-scheme *hwtacacs-scheme-name*

分布式设备：

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*：清除指定单板板上缓存的停止计费请求报文，*slot-number* 表示单板所在的槽位号。（分布式设备）

【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**、**retry stop-accounting** 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，停止计费请求报文的最大重试次数。**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**、**hwtacacs scheme** 和 **display stop-accounting-buffer**。

【举例】

设置对于 HWTACACS 方案 hwt1 中的服务器，设备系统最多可以将缓存的停止计费请求报文发送 50 次。

```
<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，必须是合法的单播地址。

port-number：从 HWTACACS 计费服务器的端口号，缺省为 49，取值范围为 1～65535。

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，否则将提示配置不成功。
- 需保证设备上的 HWTACACS 服务端口与 HWTACACS 服务器上的端口设置一致。
- 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，需保证本命令中指定的 VPN 和服务器实际所在的 VPN 一致。
- 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。
- 如果重复执行此命令，新的配置将覆盖原来的配置。
- 只有当没有活跃的、用于发送计费报文的 TCP 连接使用该计费服务器时，才允许删除该服务器。

相关配置可参考命令 **display hwtacacs**、**hwtacacs scheme** 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 服务器的 IP 地址，必须是合法的单播地址。

port-number：从 HWTACACS 服务器的端口号，缺省为 49，取值范围为 1～65535。

vpn-instance *vpn-instance-name*：从 HWTACACS 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，否则将提示配置不成功。
- 需保证设备上的 HWTACACS 服务端口与 HWTACACS 服务器上的端口设置一致。

- 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，需保证本命令中指定的 VPN 和服务器实际所在的 VPN 一致。
- 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。
- 如果重复执行此命令，新的配置将覆盖原来的配置。
- 只有当没有活跃的、用于发送认证报文的 TCP 连接使用该认证服务器时，才允许删除该服务器。

相关配置可参考命令 **display hwtacacs**、**hwtacacs scheme** 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，必须是合法的单播地址。

port-number：从 HWTACACS 授权服务器的端口号，缺省为 49，取值范围为 1～65535。

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，否则将提示配置不成功。
- 需保证设备上的 HWTACACS 服务端口与 HWTACACS 服务器上的端口设置一致。
- 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，需保证本命令中指定的 VPN 和服务器实际所在的 VPN 一致。
- 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。

- 如果重复执行此命令，新的配置将覆盖原来的配置。
- 只有当没有活跃的、用于发送授权报文的 TCP 连接使用该授权服务器，才允许删除该服务器。

相关配置可参考命令 **display hwtacacs**、**hwtacacs scheme** 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**、**hwtacacs scheme** 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，单位为分钟，非零取值必须为 3 的倍数。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1-11 实时计费间隔与用户量之间的推荐比例关系

用户数	实时计费间隔（分钟）
1～99	3
100～499	6
500～999	12
*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：服务器应答超时时间，取值范围为 1～300，单位为秒。

【描述】

timer response-timeout 命令用来设置 HWTACACS 服务器应答超时时间。**undo timer response-timeout** 命令用来恢复缺省情况。

缺省情况下，HWTACACS 服务器应答超时时间为 5 秒。

需要注意的是，由于 HWTACACS 是基于 TCP 实现的，因此，服务器应答超时或 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 服务器应答超时时间为 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。
- 无线用户漫游时，建议配置参数 **keep-original**，否则可能引起认证失败。

相关配置可参考命令 **hwtacacs scheme**。

【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 **hwtacacs scheme** 和 **display hwtacacs scheme**。

【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
```