目 录

第1章 802.1x 配置命令

1.1 802.1x 配置命令

1.1.1 display dot1x

【命令】

display dot1x [**sessions** | **statistics**] [**interface** *interface-list*]

【视图】

任意视图

【参数】

sessions：显示 802.1x 的会话连接信息。

statistics：显示 802.1x 的相关统计信息。

interface：显示指定端口的 802.1x 相关信息。

interface-list：以太网端口列表，表示多个以太网端口，表示方式为 *interface-list* = { *interface-num* [**to** *interface-num*] } & < 1-10 >。其中，*interface-num* 为单个以太网端口，可表示为 *interface-num* = { *interface-type interface-num* | *interface-name* }，*interface-type* 为端口类型，*interface-num* 为端口号，*interface-name* 为端口名，它们各自的含义和取值范围请参见本书“端口配置”部分的命令参数。

【描述】

display dot1x 命令用来显示 802.1x 的相关信息，包括配置信息、运行情况（会话连接信息）以及相关统计信息等。

如果在执行本命令的时候不指定端口，系统将显示交换机所有 802.1x 相关信息。根据该命令的输出信息，可以帮助用户确认当前的 802.1x 配置是否正确，并进一步有助于 802.1x 故障的诊断与排除。

相关配置可参考命令 **reset dot1x statistics, dot1x, dot1x retry, dot1x max-user, dot1x port-control, dot1x port-method, dot1x timer**。

【举例】

显示 802.1x 的配置信息（以 S3026E 为例）。

```
<Quidway> display dot1x
Equipment 802.1X protocol is enabled
 CHAP authentication is enabled
```

```
DHCP-launch is disabled
Dynamic-binding-user is disabled
Proxy trap checker is disabled
Proxy logoff checker is disabled

Configure: Transmit Period 30     s,  Commit Period   15     s
           ReAuth Period   3600   s
           Quiet Period    60     s,  Value of Quiet Period Timer is disabled
           Supp Timeout    30     s,  Value of Server Timeout  000100 s
           The maximal retransmitting times     3
           Handshake period                     15     s

Total maximum on-line user number is 512
Total current on-line user number is 0

Ethernet0/1  is link-up
  802.1X protocol is disabled
  Proxy trap checker is disabled
  Proxy logoff checker is disabled
  Version-Check is disabled
  The port is a(n) authenticator
  Authenticate Mode is auto
  Port Control Type is Mac-based
  ReAuthenticate is disabled
  Max on-line user number is 64
```

……（以下略）

表1-1 802.1x 配置信息描述表

域名	描述
Equipment 802.1X protocol is enabled	交换机 802.1X 特性已经开启
CHAP authentication is enabled	使能 CHAP 认证
DHCP-launch is disabled	在 DHCP 环境中，如果用户私自配置静态 IP，交换机触发对该用户的身份认证
Dynamic-binding-user is disabled	是否开启动态用户绑定功能：enable 表示开启；disable 表示关闭
Proxy trap checker is disabled	是否检测通过代理登录用户的接入：disable 表示不检测；enable 表示检测用户使用代理后，发送 Trap 报文
Proxy logoff checker is disabled	是否检测通过代理登录用户的接入：disable 表示不检测；enable 表示检测用户使用代理后，切断用户连接
Transmit Period	发送间隔定时器

域名	描述
Handshake Period	802.1x 的握手报文的发送时间间隔
ReAuth Period	802.1x 重认证定时器
Quiet Period	静默定时器设置的静默时长
Quiet Period Timer is disabled	静默定时器状态：disable 表示处于关闭状态；enable 表示处于开启状态
Supp Timeout	Supplicant 认证超时定时器
Server Timeout	Authentication Server 超时定时器
The maximal retransmitting times	交换机可重复向接入用户发送认证请求帧的次数
Total maximum on-line user number	最多可接入用户数
Total current on-line user number	当前在线接入用户数
Ethernet0/1 is link-up	端口 Ethernet 0/1 的状态为 Up
802.1X protocol is disabled	该端口未使能 802.1X 协议
Proxy trap checker is disabled	该端口是否检测通过代理登录用户的接入：disable 表示不检测；enable 表示检测用户使用代理后，发送 Trap 报文
Proxy logoff checker is disabled	该端口是否检测通过代理登录用户的接入：disable 表示不检测；enable 表示检测用户使用代理后，切断用户连接
Version-Check is disabled	端口是否开启客户端版本检测功能：disable 表示关闭；enable 表示开启
The port is a(n) authenticator	该端口担当 Authenticator 作用
Authenticate Mode is auto	端口接入控制的模式为 auto
Port Control Type is Mac-based	端口接入控制方式为 Mac-based，即基于 MAC 地址对接入用户进行认证
ReAuthenticate is disabled	端口是否开启 802.1x 重认证功能：disable 表示关闭；enable 表示开启
Max on-line user number	本端口最多可容纳的接入用户数
…	略

1.1.2 dot1x

【命令】

dot1x [**interface** *interface-list*]

undo dot1x [**interface** *interface-list*]

【视图】

系统视图/以太网端口视图

【参数】

interface *interface-list*：以太网端口列表，表示多个以太网端口，表示方式为 *interface-list* = { *interface-num* [**to** *interface-num*] } & < 1-10 >。其中，*interface-num* 为单个以太网端口，可表示为 *interface-num* = { *interface-type interface-num* | *interface-name* }，*interface-type* 为端口类型，*interface-num* 为端口号，*interface-name* 为端口名，它们各自的含义和取值范围请参见本书“端口配置”部分的命令参数。

【描述】

dot1x 命令用来开启指定端口上或全局（即当前设备）的 802.1x 特性，**undo dot1x** 命令用来关闭指定端口上或全局的 802.1x 特性。

缺省情况下，所有端口及全局的 802.1x 特性都处于关闭状态。

在系统视图下使用该命令时，如果不输入 *interface-list* 参数，则表示开启全局的 802.1x 特性；如果指定了 *interface-list*，则表示开启指定端口的 802.1x 特性。在以太网端口视图下使用该命令时，不能输入 *interface-list* 参数，仅打开当前端口的 802.1x 特性。

802.1x 特性启动前后，均可以使用配置命令来配置全局或端口的 802.1x 特性参数。如果在开启全局 802.1x 特性前没有配置全局或端口的其它 802.1x 特性参数，则这些参数在运行时均为缺省值。

全局 802.1x 特性开启后，必须再开启端口的 802.1x 特性，802.1x 的配置才能在端口上生效。

如果端口启动了 802.1x，则不能配置该端口的最大 MAC 地址学习个数（通过命令 **mac-address max-mac-count** 配置），反之，如果端口配置了最大 MAC 地址学习个数，则禁止在该端口上启动 802.1x。

相关配置可参考命令 **display dot1x**。

【举例】

开启以太网端口 Ethernet 0/1 上的 802.1x 特性。

```
[Quidway] dot1x interface Ethernet 0/1
```

开启全局的 802.1x 特性。

```
[Quidway] dot1x
```

1.1.3 dot1x authentication-method

【命令】

S3026E、S3026E FM、S3026E FS 和 S3050C 交换机使用下列命令：

dot1x authentication-method { **chap** | **pap** | **eap** }

undo dot1x authentication-method

S3026、S3026FM、S3026FS 交换机使用下列命令：

dot1x authentication-method { **chap** | **pap** | **eap md5-challenge** }

undo dot1x authentication-method

【视图】

系统视图

【参数】

chap：采用 CHAP 认证方式。

pap：采用 PAP 认证方式。

eap：采用 EAP 认证方式。

【描述】

dot1x authentication-method 命令用来设置 802.1x 用户的认证方法，**undo dot1x authentication-method** 命令用来恢复 802.1x 用户的缺省认证方法。

缺省情况下，802.1x 用户认证方法为 CHAP 认证。

PAP（Password Authentication Protocol）是一种两次握手认证协议，它采用明文方式传送口令;

CHAP（Challenge Handshake Authentication Protocol）是一种三次握手认证协议，它只在网络上传输用户名，而并不传输口令。相比之下，CHAP 认证保密性较好，更为安全可靠。

EAP 认证功能，意味着交换机直接把 802.1x 用户的认证信息以 EAP 报文发送给 RADIUS 服务器完成认证，而无须将 EAP 报文转换成标准的 RADIUS 报文后再发给 RADIUS 服务器来完成认证。

📖 说明：

对于 EAP 认证方式:

- S3026E、S3026E FM、S3026E FS 和 S3050C 交换机支持 PEAP、EAP-TLS 和 EAP-MD5 三种认证方式，如果要采用 PEAP、EAP-TLS 或者 EAP-MD5 这三种认证方法之一，只需启动 EAP 认证即可;
- S3026、S3026 FM 和 S3026 FS 交换机仅支持 EAP-MD5 认证方式。

相关配置可参考命令 **display dot1x**。

【举例】

设置交换机采用 PAP 认证。

```
[Quidway] dot1x authentication-method pap
```

1.1.4 dot1x dhcp-launch

【命令】

dot1x dhcp-launch

undo dot1x dhcp-launch

【视图】

系统视图

【参数】

无

【描述】

dot1x dhcp-launch 命令用来在 DHCP 环境中，如果用户私自配置静态 IP，设置 802.1x 不允许以太网交换机触发对该用户的身份认证，**undo dot1x dhcp-launch** 命令用来设置允许交换机触发对该用户的身份认证。

缺省情况下，用户私自配置静态 IP，交换机可以触发对其的身份认证。

相关配置可参考命令 **display dot1x**。

【举例】

设置在 DHCP 环境中，用户私自配置静态 IP 的情况下，交换机不触发对其的身份认证。

```
[Quidway] dot1x dhcp-launch
```

1.1.5 dot1x dynamic-binding-user enable

【命令】

dot1x dynamic-binding-user enable

undo dot1x dynamic-binding-user enable

【视图】

系统视图

【参数】

无

【描述】

dot1x dynamic-binding-user enable 用来开启 802.1x 动态用户绑定功能，**undo dot1x dynamic-binding-user enable** 用来关闭 802.1x 动态用户绑定功能。

缺省情况下，802.1x 动态用户绑定功能处于关闭状态。

802.1x 动态用户绑定功能是指：当 802.1x 用户通过认证后，交换机对该用户的 IP 地址、MAC 地址、接入端口，以及接入端口所属的 VLAN 进行动态绑定。此后，交换机只允许与这四项都匹配的报文通过。如果在用户上网过程中，交换机发现用户的报文有任何一项发生了变化，都会强制该用户下线。

配置时请注意：

(1) 如果用户采用动态获取 IP 地址的方式，动态用户绑定功能需要与 DHCP Snooping 特性配合：

- 在交换机上全局开启 DHCP Snooping；
- 在交换机与 DHCP 服务器相连的端口上配置信任端口。

(2) 如果用户采用静态 IP 地址方式，需要使用华为公司的 802.1x 客户端，并在[802.1x 创建连接-设置特殊属性]窗口中的“用户选项”处，选中“上传 IP 地址”复选框。。

S3000 系列交换机中，S3026E、S3026E FM、S3026E FS 和 S3050C 支持此命令；S3026、S3026 FM 和 S3026 FS 不支持此命令。

相关配置可参考命令 **dot1x**。

【举例】

开启交换机动态用户绑定功能。

```
<Quidway> system-view
System View: return to User View with Ctrl+Z.
[Quidway] dot1x dynamic-binding-user enable
```

1.1.6 dot1x guest-vlan

【命令】

dot1x guest-vlan *vlan-id* [**interface** *interface-list*]

undo dot1x guest-vlan *vlan-id* [**interface** *interface-list*]

【视图】

系统视图/以太网端口视图

【参数】

vlan-id：Guest VLAN 的 VLAN ID，取值范围为 1～4094。

interface_list：使能 Guest VLAN 的端口列表。*interface_list* = { *interface_type interface_num* | *interface_name* } [**to** { *interface_type interface_num* | *interface_name* }] *&<1-10>*。其中 *interface_type* 为端口类型，*interface_num* 为端口号，*interface_name* 为端口名，它们各自的含义和取值范围请参见本书“端口”部分的命令参数，此处不再赘述。关键字 **to** 之后的端口号要大于或等于 **to** 之前的端口号。命令中&<1-10>表示前面的参数最多可以重复输入 10 次。

【描述】

dot1x guest-vlan 命令用来开启指定端口的 Guest VLAN 功能。**undo dot1x guest-vlan** 命令用来关闭 Guest VLAN 功能。

在系统视图下使用该命令时，如果不输入 *interface-list* 参数，则表示开启所有端口的 Guest VLAN 功能；如果指定了 *interface-list*，则表示开启指定端口的 Guest VLAN 功能。

在以太网端口视图下使用该命令时，不能输入 *interface-list* 参数，仅打开当前端口的 Guest VLAN 功能。

S3000 系列交换机中，S3026E、S3026E FM、S3026E FS 和 S3050C 支持此命令；S3026、S3026 FM 和 S3026 FS 不支持此命令。

相关配置可参考命令 **name**, **vlan-assignment-mode**。

【举例】

设置认证方式为基于端口的方式。

```
[Quidway] dot1x port-method portbased
```

开启所有端口的 Guest VLAN 功能。

```
[Quidway] dot1x guest-vlan 1
```

1.1.7 dot1x max-user

【命令】

dot1x max-user *user-number* [**interface** *interface-list*]

undo dot1x max-user [**interface** *interface-list*]

【视图】

系统视图/以太网端口视图

【参数】

user-number：端口可容纳接入用户数量的最大值，对于 S3026、S3026E、S3026E FM、S3026E FS 和 S3050C 交换机，取值范围为 1～64；对于 S3026 FM 和 S3026 FS 交换机，取值范围为 1～256。

缺省情况下，对于 S3026、S3026E、S3026E FM、S3026E FS 和 S3050C 交换机，端口上可容纳接入用户数量的最大值为 64；对于 S3026 FM 和 S3026 FS 交换机，端口上可容纳接入用户数量的最大值为 256。

interface *interface-list*：以太网端口列表，表示多个以太网端口，表示方式为 *interface-list* = { *interface-num* [**to** *interface-num*] } & < 1-10 >。其中，*interface-num* 为单个以太网端口，可表示为 *interface-num* = { *interface-type interface-num* | *interface-name* }，*interface-type* 为端口类型，*interface-num* 为端口号，*interface-name* 为端口名，它们各自的含义和取值范围请参见本书“端口配置”部分的命令参数。

【描述】

dot1x max-user 命令用来设置 802.1x 在指定端口上可容纳接入用户数量的最大值，**undo dot1x max-user** 命令用来恢复该值的缺省值。

在系统视图下执行该命令可以作用于 *interface-list* 参数所指定的某个端口，如果不指定任何端口则将作用于所有端口。在以太网端口视图下执行该命令时，不能输入 *interface-list* 参数，只能作用于当前端口。

相关配置可参考命令 **display dot1x**。

【举例】

设置端口 Ethernet 0/1 最多可容纳 32 个接入用户。

```
[Quidway] dot1x max-user 32 interface Ethernet 0/1
```

1.1.8 dot1x port-control

【命令】

dot1x port-control { **auto** | **authorized-force** | **unauthorized-force** } [**interface** *interface-list*]

undo dot1x port-control [**interface** *interface-list*]

【视图】

系统视图/以太网端口视图

【参数】

auto：自动识别模式；指示端口初始状态为非授权状态，仅允许 EAPoL 报文收发，不允许用户访问网络资源；如果认证流程通过，则端口切换到授权状态，允许用户访问网络资源。这也是最常见的情况。

authorized-force：强制授权模式；指示端口始终处于授权状态，允许用户不经认证授权即可访问网络资源。

unauthorized-force：强制非授权模式；指示端口始终处于非授权状态，不允许用户访问网络资源。

interface *interface-list*：以太网端口列表，表示多个以太网端口，表示方式为 *interface-list* = { *interface-num* [**to** *interface-num*] } & < 1-10 >。其中，*interface-num* 为单个以太网端口，可表示为 *interface-num* = { *interface-type interface-num* | *interface-name* }，*interface-type* 为端口类型，*interface-num* 为端口号，*interface-name* 为端口名，它们各自的含义和取值范围请参见本书“端口配置”部分的命令参数。

【描述】

dot1x port-control 命令用来设置 802.1x 在指定端口上进行接入控制的模式，**undo dot1x port-control** 命令用来恢复缺省的接入控制模式。

缺省情况下，接入控制模式为 **auto**。

dot1x port-control 命令用来设置 802.1x 在指定端口上进行接入控制的模式，即端口处于什么状态。在系统视图下执行该命令可以作用于 *interface-list* 参数所指定的某个端口，如果不指定任何端口则将作用于所有端口。在以太网端口视图下执行该命令时，不能输入 *interface-list* 参数，只能作用于当前端口。

相关配置可参考命令 **display dot1x**。

【举例】

指定端口 Ethernet 0/1 处于强制非受控状态。

```
[Quidway] dot1x port-control unauthorized-force interface Ethernet 0/1
```

1.1.9 dot1x port-method

【命令】

dot1x port-method { **macbased** | **portbased** } [**interface** *interface-list*]

undo dot1x port-method [**interface** *interface-list*]

【视图】

系统视图/以太网端口视图

【参数】

macbased：指示 802.1x 认证系统基于 MAC 地址对接入用户进行认证。

portbased：指示 802.1x 认证系统基于端口号对接入用户进行认证。

interface *interface-list*：以太网端口列表，表示多个以太网端口，表示方式为 *interface-list* = { *interface-num* [**to** *interface-num*] } & < 1-10 >。其中，*interface-num* 为单个以太网端口，可表示为 *interface-num* = { *interface-type*

interface-num | *interface-name* }，*interface-type* 为端口类型，*interface-num* 为端口号，*interface-name* 为端口名，它们各自的含义和取值范围请参见本书“端口配置”部分的命令参数。

缺省情况下，接入控制方式为 **macbased**。

【描述】

dot1x port-method 命令用来设置 802.1x 在指定端口上进行接入控制的方式，**undo dot1x port-method** 命令用来恢复缺省的接入控制方式。

此命令用来设置 802.1x 在指定端口上进行接入控制的方式，即基于什么来对用户进行认证。当采用 **macbased** 方式时，该端口下的所有接入用户均需要单独认证，当某个用户下线时，也只有该用户无法使用网络；当采用 **portbased** 方式时，只要该端口下的第一个用户认证成功后，其他接入用户无须认证就可使用网络资源，但是当第一个用户下线后，其他用户也会被拒绝使用网络。

在系统视图下执行该命令可以作用于 *interface-list* 参数所指定的某个端口，如果不指定任何端口则将作用于所有端口。在以太网端口视图下执行该命令时，不能输入 *interface-list* 参数，只能作用于当前端口。

相关配置可参考命令 **display dot1x**。

【举例】

指定端口 Ethernet 0/1 基于端口号对接入用户进行认证。

```
[Quidway] dot1x port-method portbased interface Ethernet 0/1
```

1.1.10 dot1x quiet-period

【命令】

dot1x quiet-period

undo dot1x quiet-period

【视图】

系统视图

【参数】

无

【描述】

dot1x quiet-period 命令用来开启 quiet-period 定时器功能，**undo dot1x quiet-period** 命令用来关闭该定时器功能。

当 802.1x 用户认证失败以后，Authenticator 设备（如 Quidway 系列以太网交换机）需要静默一段时间（该时间由静默定时器设置）后再重新发起认证，在静默期间，Authenticator 设备不进行 802.1x 认证的相关处理。

缺省情况下，关闭 quiet-period 定时器功能。

相关配置可参考命令 **display dot1x**，**dot1x timer**。

【举例】

打开 quiet-period 定时器。

```
[Quidway] dot1x quiet-period
```

1.1.11 dot1x re-authenticate

【命令】

dot1x re-authenticate [**interface** *interface-list*]

undo dot1x re-authenticate [**interface** *interface-list*]

【视图】

系统视图/以太网端口视图

【参数】

interface *interface-list*：以太网端口列表，表示多个以太网端口，表示方式为 *interface-list* = { *interface-num* [**to** *interface-num*] } & < 1-10 >。其中，*interface-num* 为单个以太网端口，可表示为 *interface-num* = { *interface-type interface-num* | *interface-name* }，其中 *interface-type* 为端口类型，*interface-num* 为端口号，*interface-name* 为端口名。

【描述】

dot1x re-authenticate 用来开启特定端口或设备所有 Authenticator 端口的 802.1X 重认证特性，**undo dot1x re-authenticate** 用来关闭特定端口或设备所有 Authenticator 端口的 802.1X 重认证特性。

缺省情况下，所有端口的 802.1X 重认证特性都处于关闭状态。

在系统视图下使用该命令时，如果不输入 *interface-list* 参数，则表示开启所有端口的 802.1X 重认证特性；如果指定了 *interface-list* 参数，则表示开启指定端口的 802.1X 重认证特性。以太网端口视图下使用该命令时，不能输入 *interface-list* 参数，仅打开当前端口的 802.1X 重认证特性。

在配置端口 802.1X 重认证特性之前，必须开启全局 802.1X 特性和该端口的 802.1x 特性。

S3000 系列交换机中，S3026E、S3026E FM、S3026E FS 和 S3050C 支持此命令；S3026、S3026 FM 和 S3026 FS 不支持此命令。

【举例】

在端口 Ethernet 0/1 上启动 802.1X 重认证功能。

```
[Quidway-Ethernet0/1] dot1x re-authenticate
 Re-authentication is enabled on port Ethernet0/1
```

1.1.12 dot1x retry

【命令】

dot1x retry *max-retry-value*

undo dot1x retry

【视图】

系统视图

【参数】

max-retry-value：可重复向接入用户发送认证请求帧的最大次数，取值范围为 1～10。缺省情况下，可重复向接入用户发送认证请求帧的最大次数为 3 次。

【描述】

dot1x retry 命令用来设置以太网交换机可重复向接入用户发送认证请求帧的最大次数，**undo dot1x retry** 命令用来将该最大发送次数恢复为缺省值。

如果交换机初次向用户发送认证请求帧后，在规定的时间里没有收到用户的响应，则交换机将再次向用户发送该认证请求。此命令就是用来设置以太网交换机可重复向接入用户发送认证请求帧的次数。取值为 1 时表示只允许向用户发送一次认证请求帧，即如果没有收到响应，不再重复发送；取值为 2 时表示在首次向用户发送请求又没有收到响应后将重复发送 1 次；……依次类推。本命令设置后将作用于所有端口。

相关配置可参考命令 **display dot1x**。

【举例】

指示本机最多向接入用户发送 9 次认证请求帧。

```
[Quidway] dot1x retry 9
```

1.1.13 dot1x retry-version-max

【命令】

dot1x retry-version-max *max-retry-version-value*

undo dot1x retry-version-max

【视图】

系统视图

【参数】

max-retry-version-value：重复向接入用户发送版本请求帧的最大次数，取值范围为 1～10。缺省为 3 次。

【描述】

dot1x retry-version-max 命令用来设置以太网交换机可重复向接入用户发送版本请求帧的最大次数，**undo dot1x retry-version-max** 命令用来将该最大发送次数恢复为缺省值。

当交换机初次向用户发送客户端版本请求帧后，如果在一定时间（由版本验证的超时定时器指定）内没有收到客户端的响应，交换机会再次向客户端发送版本请求，当发送次数达到由本配置任务配置的最大次数后仍没有收到响应，交换机不再对客户端的版本进行验证，而继续进行后续的认证过程。本命令设置后将作用于所有启动版本验证功能的端口。

S3000 系列交换机中，S3026E、S3026E FM、S3026E FS 和 S3050C 支持此命令；S3026、S3026 FM 和 S3026 FS 不支持此命令。

相关配置可参考命令 **display dot1x**，**dot1x timer**。

【举例】

配置交换机最多向接入用户发送 6 次版本请求帧。

```
[Quidway] dot1x retry-version-max 6
```

1.1.14 dot1x supp-proxy-check

【命令】

dot1x supp-proxy-check { **logoff** | **trap** } [**interface** *interface-list*]

undo dot1x supp-proxy-check { **logoff** | **trap** } [**interface** *interface-list*]

【视图】

系统视图/以太网端口视图

【参数】

logoff：检测用户使用代理后，切断用户连接。

trap：检测用户使用代理后，发送 Trap 报文。

interface *interface-list*：以太网端口列表，表示多个以太网端口，表示方式为 *interface-list* = { *interface-num* [**to** *interface-num*] } & < 1-10 >。其中，*interface-num* 为单个以太网端口，可表示为 *interface-num* = { *interface-type interface-num* | *interface-name* }，*interface-type* 为端口类型，*interface-num* 为端口号，*interface-name* 为端口名，它们各自的含义和取值范围请参见本书“端口配置”部分的命令参数。

【描述】

dot1x supp-proxy-check 命令用来设置交换机对通过代理登录的用户的检测及接入控制，**undo dot1x supp-proxy-check** 命令用来取消交换机对通过代理登录的用户的检测及相关控制的设置。

需要注意的是，该功能的实现需要华为 802.1X 客户端程序的配合，即需要通过代理登录的用户需要运行华为 802.1X 客户端程序（该客户端程序要求版本为 V1.29 或以上）。

此命令如果在系统视图下执行，可以作用于 *interface-list* 参数所指定的某个端口；如果在以太网端口视图下执行，不能输入 *interface-list* 参数，只能作用于当前端口。在系统视图下开启全局的代理用户检测与控制后，必须再开启指定端口的代理用户检测与控制特性，此特性的配置才能在该端口上生效。

相关配置可参考命令 **display dot1x**。

【举例】

设置端口 Ethernet0/1～Ethernet0/8 检测到用户使用代理后，切断该用户的连接。

```
[Quidway] dot1x supp-proxy-check logoff
[Quidway] dot1x supp-proxy-check logoff interface Ethernet 0/1 to Ethernet 0/8
```

设置端口 Ethernet 0/9 检测到登录的用户使用代理后，交换机发送 Trap 报文。

```
[Quidway] dot1x supp-proxy-check trap
[Quidway] dot1x supp-proxy-check trap interface Ethernet 0/9
```

或

```
[Quidway] dot1x supp-proxy-check trap
[Quidway] interface Ethernet 0/9
[Quidway-Ethernet0/9] dot1x supp-proxy-check trap
```

1.1.15 dot1x timer

【命令】

dot1x timer { **handshake-period** *handshake-period-value* | **reauth-period** *reauth-period-value* | **quiet-period** *quiet-period-value* | **tx-period** *tx-period-value* | **supp-timeout** *supp-timeout-value* | **server-timeout** *server-timeout-value* | **ver-period** *ver-period-value* }

undo dot1x timer { handshake-period | reauth-period | quiet-period | tx-period | supp-timeout | server-timeout | ver-period }

【视图】

系统视图

【参数】

tx-period：传送超时定时器。当 Authenticator 设备向 Supplicant 设备发送 Request/Identity 请求报文（该报文用于请求用户的用户名，或者用户名和密码）后，Authenticator 设备启动定时器 **tx-period**，若在该定时器设置的时长内，Supplicant 设备未成功发送认证应答报文，则 Authenticator 设备将重发认证请求报文。

tx-period-value：传送超时定时器设置的时长，取值范围为 10～120，单位为秒。缺省情况下，*tx-period-value* 为 30 秒。

supp-timeout：Supplicant 认证超时定时器。当 Authenticator 设备向 Supplicant 设备发送了 Request/Challenge 请求报文（该报文用于请求 Supplicant 设备的 MD5 加密密文）后，Authenticator 设备启动 **supp-timeout** 定时器，若在该定时器设置的时长内，Supplicant 设备未成功响应，Authenticator 设备将重发该报文。

supp-timeout-value：Supplicant 认证超时定时器设置的时长，取值范围为 10～120，单位为秒。缺省情况下，*supp-timeout-value* 为 30 秒。

server-timeout：Authentication Server 超时定时器。若在该定时器设置的时长内，Authentication Server 未成功响应，Authenticator 设备将重发认证请求报文。

server-timeout-value：RADIUS 服务器超时定时器设置的时长，取值范围为 100～300，单位为秒。缺省情况下，*server-timeout-value* 为 100 秒。

handshake-period：此定时器是在用户认证成功后启动的，系统以此间隔为周期发送握手请求报文。如果 **dot1x retry** 命令配置重试次数为 N，则系统连续 N 次没有收到客户端的响应报文，就认为用户已经下线，将用户置为下线状态。

handshake-period-value：握手时间间隔，取值范围为 1～1024，单位为秒。缺省情况下，握手报文的发送时间间隔为 15 秒。

reauth-period：重认证超时定时器。在该定时器设置的时长内，Supplicant 设备会发起 802.1X 重认证。

reauth-period-value：重认证超时定时器设置的时长，取值范围为 1～86400，单位为秒。缺省值为 3600 秒。

quiet-period：静默定时器。对用户认证失败以后，Authenticator 设备需要静默一段时间（该时间由静默定时器设置）后再重新发起认证，在静默期间，Authenticator 设备不处理认证功能。

quiet-period-value：静默定时器设置的静默时长，取值范围 10～120，单位为秒。缺省情况下，*quiet-period-value* 为 60 秒。

ver-period：客户端版本请求超时定时器。若在该定时器设置的时长内，Supplicant 设备未成功发送版本应答报文，则 Authenticator 设备将重发版本请求报文。

ver-period-value：版本请求超时定时器设置的时长，取值范围为 1～30，单位为秒。缺省值为 1 秒。

【描述】

dot1x timer 命令用来配置 802.1x 的各项定时器参数，**undo dot1x timer** 命令用来将指定的定时器恢复为缺省值。

802.1x 在运行时会启动很多定时器以控制接入用户（Supplicant）、接入认证设备（Authenticator）以及认证服务器（Authenticator Server）之间进行合理、有序的交互。使用此命令可以改变部分定时器值（另外部分定时器是不可调节的），以调节交互进程。这在较为特殊或比较恶劣的网络环境下可能是必需的措施。不过，一般情况下，请保持这些定时器的缺省值。

相关配置可参考命令 **display dot1x**。

【举例】

#设置 Authentication Server 超时定时器时长为 150 秒。

```
[Quidway] dot1x timer server-timeout 150
```

1.1.16 dot1x version-check

【命令】

dot1x version-check [**interface** *interface-list*]

undo dot1x version-check [**interface** *interface-list*]

【视图】

系统视图/以太网端口视图

【参数】

interface *interface-list*：以太网端口列表，表示多个以太网端口，表示方式为 *interface-list* = { *interface-num* [**to** *interface-num*] } & < 1-10 >。其中，*interface-num* 为单个以太网端口，可表示为 *interface-num* = { *interface-type interface-num* | *interface-name* }，其中 *interface-type* 为端口类型，*interface-num* 为端口号，*interface-name* 为端口名。

【描述】

dot1x version-check 用来开启指定端口上的 802.1X 客户端版本检测特性，**undo dot1x version-check** 用来关闭指定端口上对 802.1X 客户端的版本检测特性。

缺省情况下，所有端口的 802.1X 客户端版本检测特性都处于关闭状态。

在系统视图下使用该命令时，如果不输入 *interface-list* 参数，则表示开启所有端口的 802.1X 客户端版本检测特性；如果指定了 *interface-list* 参数，则表示开启指定端口的 802.1X 客户端版本检测特性。以太网端口视图下使用该命令时，不能输入 *interface-list* 参数，仅打开当前端口的 802.1X 版本检测特性。

S3000 系列交换机中，S3026E、S3026E FM、S3026E FS 和 S3050C 支持此命令；S3026、S3026 FM 和 S3026 FS 不支持此命令。

【举例】

配置端口 Ethernet0/1 在接收到认证报文时检测 802.1X 客户端的版本。

```
[Quidway-Ethernet0/1] dot1x version-check
```

1.1.17 reset dot1x statistics

【命令】

reset dot1x statistics [**interface** *interface-list*]

【视图】

用户视图

【参数】

interface *interface-list*：以太网端口列表，表示多个以太网端口，表示方式为 *interface-list* = { *interface-num* [**to** *interface-num*] } & < 1-10 >。其中，*interface-num* 为单个以太网端口，可表示为 *interface-num* = { *interface-type interface-num* | *interface-name* }，*interface-type* 为端口类型，*interface-num* 为端口号，*interface-name* 为端口名，它们各自的含义和取值范围请参见本书“端口配置”部分的命令参数。

【描述】

reset dot1x statistics 命令用来清除 802.1x 的统计信息。

当用户想删除 802.1x 原有统计信息，重新进行相关信息统计时，可以使用该命令。

在清除原有的统计信息时，如果不指定端口类型和端口号，则清除交换机上的全局及所有端口的 802.1x 统计信息；如果指定端口类型和端口号，则清除指定端口上的 802.1x 统计信息。

相关配置可参考命令 **display dot1x**。

【举例】

清除以太网端口 Ethernet 0/1 上的 802.1x 统计信息。

```
<Quidway> reset dot1x statistics interface Ethernet 0/1
```

第2章 AAA 和 RADIUS 协议配置命令

2.1 AAA 配置命令

2.1.1 access-limit

【命令】

access-limit { **disable** | **enable** *max-user-number* }

undo access-limit

【视图】

ISP 域视图

【参数】

disable：表示不对当前 ISP 域可容纳的接入用户数作限制。

enable *max-user-number*：指示当前 ISP 域可容纳接入用户数的最大值，对于 S3026、S3026E、S3026E FM、S3026E FS 和 S3050C 交换机，取值范围为 1～512；对于 S3026 FM 和 S3026 FS 交换机，取值范围为 1～1024。

【描述】

access-limit 命令用来指定当前 ISP 域可容纳接入用户数的最大值。**undo access-limit** 命令用来恢复缺省设置。

缺省情况下，不对当前 ISP 域可容纳的接入用户数作限制。

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。

【举例】

指定 ISP 域“huawei163.net”最多可容纳 500 个接入用户。

```
[Quidway-isp-huawei163.net] access-limit enable 500
```

2.1.2 attribute

【命令】

attribute { **ip** *ip-address* | **mac** *mac-address* | **idle-cut** *second* | **access-limit** *max-user-number* | **vlan** *vlanid* | **location** { **nas-ip** *ip-address* **port** *portnum* | **port** *portnum* } }*

undo attribute { **ip** | **mac** | **idle-cut** | **access-limit** | **vlan** | **location** }*

【视图】

本地用户视图

【参数】

ip：指定用户的 IP 地址。

mac：指定用户的 MAC 地址。其中，*mac-address* 为点分十六进制格式（即形如 *X-X-X* 的样式）。

idle-cut *second*：允许/禁止本地用户启用闲置切断功能（闲置切断的具体数据则取决于用户所在 ISP 域下的配置）。*second* 为设定的闲置切断时间，取值范围 60~7200，单位为秒。

access-limit *max-user-number*：指定可以用当前用户名接入设备的最大用户数。对于 S3026、S3026E、S3026E FM、S3026E FS 和 S3050C 交换机，取值范围为 1～512；对于 S3026 FM 和 S3026 FS 交换机，取值范围为 1～1024。

vlan *vlanid*：设置用户的 VLAN 属性，即设置用户所属于的 VLAN，*vlanid* 为整数，取值范围 1~4094。

location：设置用户的端口绑定属性。

nas-ip *ip-address*：用户远端端口绑定时接入服务器的 IP 地址，*ip-address* 为 IP 地址，为点分十进制格式。缺省为 127.0.0.1，表示为本机。

port *portnum*：设置用户绑定的端口，*portnum* 输入为“槽号 子卡号 端口号”样式，如绑定的端口没有子卡号，对应项输入 0 即可。

【描述】

attribute 命令用来设置本地用户的一些属性值；**undo attribute** 命令用来取消对本地用户属性值的设置。

需要说明的是：当指定用户绑定的是远程端口，则该用户必需指定 **nas-ip** 参数，若用户绑定的是本地端口，则不需要指定 **nas-ip** 参数。

相关配置可参考命令 **display local-user**。

【举例】

设置用户 huawei1 的 IP 地址为 10.110.50.1。

```
[Quidway-luser-huawei1] attribute ip 10.110.50.1
```

2.1.3 cut connection

【命令】

cut connection { **all** | **access-type dot1x** | **domain** *domain-name* | **interface** *interface-type interface-number* | **ip** *ip-address* | **mac** *mac-address* |

radius-scheme *radius-scheme-name* | **vlan** *vlanid* | **ucibindex** *ucib-index* | **user-name** *user-name* }

【视图】

系统视图

【参数】

all：切断所有用户连接。

access-type：根据接入方式切断用户连接。其中，**dot1x** 指定切断所有 802.1x 用户连接。

domain *isp-name*：切断某个 ISP 域下的全部用户连接。其中，*isp-name* 为 ISP 域名，为不超过 24 个字符的字符串。指定的 ISP 域必须已经存在。

interface *interface-type interface-number*：切断某个端口的所有用户连接。

ip *ip-address*：切断 IP 地址为 *ip-address* 的所有用户连接。

mac *mac-address*：切断 MAC 地址为 *mac-address* 的用户连接。其中，*mac-address* 为点分十六进制格式（即形如 *X-X-X* 的样式）。

radius-scheme *radius-scheme-name*：切断名称为 *radius-scheme-name* 的 RADIUS 服务器的所有用户连接。*radius-scheme-name* 为不超过 32 个字符的字符串。

vlan *vlanid*：切断 ID 为 *vlanid* 的所有用户连接。其中，*vlanid* 的取值范围为 1～4094。

ucibindex *ucib-index*：切断连接索引号为 *ucib-index* 的用户连接。其中，*ucib-index* 的取值范围为 0～4119。

user-name *user-name*：切断用户名为 *user-name* 的用户连接。其中，*user-name* 为用户名，为字符串形式，字符串中不能包括“/”、“:”、“*”、“?”、“<”以及“>”等字符，并且“@”出现的次数不能多于 1 次。对于 S3026E、S3026E FM、S3026E FS 和 S3050C 交换机，用户名取值不超过 80 个字符；纯用户名（“@”以前部分，即用户标识）不能超过 55 个字符；对于 S3026、S3026 FM 和 S3026 FS 交换机，用户名取值不超过 32 个字符；纯用户名（“@”以前部分，即用户标识）不能超过 24 个字符。

【描述】

cut connection 命令用来强制切断某个或某类用户的连接。

相关配置可参考命令 **display connection**。

【举例】

切断域名为“huawei163.net”的 ISP 域下的所有连接。

```
[Quidway] cut connection domain huawei163.net
```

2.1.4 display connection

【命令】

display connection [**access-type dot1x** | **domain** *isp-name* | **interface** *interface-type interface-number* | **ip** *ip-address* | **mac** *mac-address* | **radius-scheme** *radius-scheme-name* | **vlan** *vlanid* | **ucibindex** *ucib-index* | **user-name** *user-name*]

【视图】

任意视图

【参数】

access-type：显示某种接入方式下的用户连接。其中，**dot1x** 表示显示所有 802.1x 用户连接。

domain *isp-name*：显示某个 ISP 域下的全部用户连接。其中，*isp-name* 为 ISP 域名，为不超过 24 个字符的字符串。指定的 ISP 域必须已经存在。

interface *interface-type interface-number*：显示某个接口的所有用户连接。

ip *ip-address*：显示某个 IP 地址为 *ip-address* 的所有用户连接。

mac *mac-address*：显示某个 MAC 地址为 *mac-address* 的用户连接。其中，*mac-address* 为点分十六进制格式（即形如 X-X-X 的样式）。

radius-scheme *radius-scheme-name*：显示名称为 *radius-scheme-name* 的 RADIUS 服务器的所有用户连接。*radius-scheme-name* 为不超过 32 个字符的字符串。

vlan *vlanid*：显示 ID 为 *vlanid* 的所有用户连接。其中，*vlanid* 的取值范围为 1～4094。

ucibindex *ucib-index*：显示某个连接索引号为 *ucib-index* 的用户连接。其中，*ucib-index* 的取值范围为 0～535。

user-name *user-name*：显示某个用户名为 *user-name* 的用户连接。其中，*user-name* 为用户名，为字符串形式，字符串中不能包括“/”、“:”、“*”、“?”、“<”以及“>”等字符，并且“@”出现的次数不能多于 1 次。对于 S3026E、S3026E FM、S3026E FS 和 S3050C 交换机，用户名取值不超过 80 个字符；纯用户名（“@”以前部分，即用户标识）不能超过 55 个字符；对于 S3026、S3026 FM 和 S3026 FS 交换机，用户名取值不超过 32 个字符；纯用户名（“@”以前部分，即用户标识）不能超过 24 个字符。

【描述】

display connection 命令用来显示所有或指定的用户连接的相关信息。根据输出的信息，可以帮助诊断与排除用户连接方面的故障。

不指定任何参数时，显示所有用户连接的相关信息。

相关配置可参考命令 **cut connection**。

【举例】

显示所有用户连接的相关信息。

```
<Quidway> display connection
Total 0 connections matched ,0 listed.
```

2.1.5 display domain

【命令】

display domain [*isp-name*]

【视图】

任意视图

【参数】

isp-name：ISP 域名。为不超过 24 个字符的字符串。所指定的 ISP 域必须已经存在。

【描述】

display domain 命令用来显示指定 ISP 域的配置信息或所有 ISP 域的概要信息。

缺省情况下，显示系统中所有 ISP 域的概要信息。

根据输出的信息，可以帮助诊断与排除与 ISP 域有关的故障。

相关配置可参考命令 **access-limit**，**domain**，**radius-scheme**，**user-template**，**state**，**display domain**。

【举例】

显示系统中所有 ISP 域的概要信息（以 S3026E 为例）。

```
<Quidway> display domain
0  Domain = system
   State = Active     Access-limit = Disable
   Vlan-assignment-mode = Integer
   Domain User Template:
   Idle-cut = Disable
   Self-service = Disable
   Messenger Time = Disable

Default Domain Name: system
Total 1 domain(s).1 listed.
```

对上述显示信息的各项解释如下表所示。

表2-1 display domain 显示信息描述表

域名	解释
0 Domain	ISP 域索引号 域名
State	状态
AccessLimit	接入用户连接数限制
Vlan-assignment-mode	动态 VLAN 下发模式，有整型（Integer）和字符串（String）两种模式
Default Domain Name	缺省的 ISP 域

2.1.6 display local-user

【命令】

display local-user [**domain** *isp-name* | **idle-cut** { **enable** | **disable** } | **service-type** { **telnet** | **ftp** | **lan-access** | **ssh** } | **state** { **active** | **block** } | **user-name** *user-name* | **vlan** *vlanid*]

【视图】

任意视图

【参数】

domain *isp-name*：显示属于某个 ISP 域的全部本地用户。其中，*isp-name* 为 ISP 域名，为不超过 24 个字符的字符串。指定的 ISP 域必须已经存在。

idle-cut：根据是否启用闲置切断功能显示本地用户。其中，**disable** 表示用户没有启用闲置切断功能；**enable** 表示用户启用了闲置切断功能。此参数仅对配置了 lan-access 业务的用户有效，对于其他业务类型的用户，命令 **display local-user idle-cut enable** 和 **display local-user idle-cut disable** 不会显示任何用户信息。

service-type：根据用户类型显示本地用户。其中，**telnet** 指定显示 telnet 类型的用户；**ftp** 指定显示 ftp 类型的用户；**lan-access** 指定显示 lan-access 类型的用户（主要指以太网接入用户，比如 802.1x 用户）；**ssh** 指定显示 SSH 类型的用户（S3026、S3026 FM 和 S3026 FS 不支持）。

state { active | block }：显示处于某种状态的本地用户。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*：显示用户名为 *user-name* 的本地用户。其中，*user-name* 为用户名，为字符串形式，字符串中不能包括“/”、“:”、“*”、“?”、“<”以及“>”等字符，并且“@”出现的次数不能多于 1 次。对于 S3026E、S3026E FM、S3026E FS 和 S3050C 交换机，用户名取值不超过 80 个字符；纯用户名（“@”以前部分，即用户标识）不能超过 55 个字符；对于 S3026、S3026 FM 和 S3026 FS

交换机，用户名取值不超过 32 个字符；纯用户名（“@”以前部分，即用户标识）不能超过 24 个字符。

vlan-id *vlanid*：显示 VLAN ID 为 *vlanid* 的本地用户。其中，*vlanid* 为整数，取值范围 1~4094。

【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。根据输出的信息，可以帮助诊断与排除与本地用户有关的故障。

缺省情况下，显示所有本地用户的相关信息。

相关配置可参考命令 **local-user**。

【举例】

显示所有本地用户的相关信息。

```
<Quidway> display local-user
The contents of local user user1:
 State:          Active            ServiceType Mask: T
 Idle-cut:       Disable
 Access-limit:   Disable           Current AccessNum: 0
 Bind location:  Disable
 Vlan ID:        Disable
 IP address:     Disable
 MAC address:    Disable
 User Privilege: 1

Total 1 local user(s) Matched, 1 listed.
```

对上述显示信息的各项解释如下表所示。

表2-2 display local-user 显示信息描述表

域名	解释
State	状态
Idle Cut	闲置切断开关
AccessLimit	接入用户连接数限制
Bind location	是否与端口捆绑
VLAN ID	用户所属的 VLAN
IP address	用户的 IP 地址
MAC address	用户的 MAC 地址
User Privilege	用户权限

2.1.7 domain

【命令】

domain { *isp-name* | **default** { **disable** | **enable** *isp-name* } }

undo domain *isp-name*

【视图】

系统视图

【参数】

isp-name：ISP 域名。为不超过 24 个字符的字符串，且不能包括“/”、“:”、“*”、“?”、“<”以及“>”等字符。

default enable *isp-name*：指定缺省 ISP 域为 *isp-name*。

disable：不允许配置缺省 ISP，此时恢复为系统缺省的 ISP 域 system。

【描述】

domain 命令用来创建一个 ISP 域，或者进入已创建 ISP 域的视图，**undo domain** 命令用来删除指定的 ISP 域。

缺省情况下，系统中已创建了一个名为“system”的 ISP 域，其各项属性均为缺省值。

ISP 域即 ISP 用户群，一个 ISP 域即是由同属于一个 ISP 的用户构成的用户群。一般说来，在“userid@isp-name”形式（例如 gw20010608@huawei163.net）的用户名中，“@”后的“isp-name”（如例中的“huawei163.net”）即为 ISP 域的域名。在 Quidway 系列交换机对用户进行接入控制时，对于用户名为“userid@isp-name”形式的 ISP 用户，系统就将把“userid”作为用于身份认证的用户名，把“isp-name”作为域名。

引入 ISP 域的设置是为了支持多 ISP 的应用环境：在这种环境中，同一个接入设备接入的有可能是不同 ISP 的用户。由于各 ISP 用户的用户属性（例如用户名及密码构成、服务类型/权限等）有可能各不相同，因此有必要通过设置 ISP 域的方法把它们区别开。在 ISP 域视图下，可以为每个 ISP 域配置包括 AAA 方案（使用的 RADIUS 方案等）在内的一整套单独的 ISP 域属性。

对于交换机来说，每个接入用户都属于一个 ISP 域。系统中最多可以配置 16 个 ISP 域。

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。

相关配置可参考命令 **access-limit**，**radius-scheme**，**state**，**display domain**。

【举例】

创建一个新的 ISP 域“huawei163.net”，并进入其视图。

```
[Quidway] domain huawei163.net
New Domain added.
[Quidway-isp-huawei163.net]
```

2.1.8 idle-cut

【命令】

idle-cut { **disable** | **enable** *minute flow* }

【视图】

ISP 域视图

【参数】

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。

minute：允许的最大空闲时间，单位为分钟，取值范围为 1～120。

flow：设置的最小数据流量，单位为字节，取值范围为 1～10,240,000（即 10M）。

【描述】

idle-cut 命令用来设置当前 ISP 域下的用户模板。

缺省情况下，当一个 ISP 域被创建以后，其用户模板属性处于 **disable**，即用户闲置切断开关处于关闭状态。

所谓用户模板，是指一组缺省用户属性的集合。当某个请求网络服务的用户不具有某项必须具备的属性时，则指定用户模板中的属性作为其缺省属性。目前，用户模板仅能设置用户闲置切断开关：如果在对某个用户进行认证后，用户及 RADIUS 服务器均没有明确指出其 idle-cut 是否开启，则指定用户模板中的 idle-cut 开关状态作为该用户 idle-cut 开关的状态。

由于用户模板的作用范围局限于一个 ISP 域，因此对于不同 ISP 域的用户，需要分别配置用户模板属性。

相关配置可参考命令 **domain**。

【举例】

允许当前 ISP 域“huawei163.net”下的用户启用用户模板中的闲置切断属性（即允许用户使用闲置切断功能），最大空闲时间为 50 分，设置的最小数据流为 500 字节。

```
[Quidway-isp-huawei163.net] idle-cut enable 50 500
```

2.1.9 local-user

【命令】

local-user *user-name*

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

【视图】

系统视图

【参数】

user-name：本地用户名，为字符串形式，字符串中不能包括“/”、“:”、“*”、“?”、“<”以及“>”等字符，并且“@”出现的次数不能多于 1 次。对于 S3026E、S3026E FM、S3026E FS 和 S3050C 交换机，用户名取值不超过 80 个字符；纯用户名（“@”以前部分，即用户标识）不能超过 55 个字符；对于 S3026、S3026 FM 和 S3026 FS 交换机，用户名取值不超过 32 个字符；纯用户名（“@”以前部分，即用户标识）不能超过 24 个字符。

service-type：指定用户的类型。其中，**telnet** 指定用户为 telnet 类型；**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）；**ssh** 指定用户为 SSH 类型（S3026、S3026 FM 和 S3026 FS 不支持）。

all：所有的用户。

【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, service-type**。

【举例】

添加名称为 huawei1 的本地用户

```
[Quidway] local-user huawei1
[Quidway-luser-huawei1]
```

2.1.10 local-user password-display-mode

【命令】

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

undo local-user password-display-mode

【视图】

系统视图

【参数】

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

auto：自动方式，即接入用户的密码显示方式可以由用户自己通过 **password** 命令来设置。

【描述】

local-user password-display-mode 命令用来设置所有接入用户的密码显示方式，**undo local-user password-display-mode** 命令用来取消设置的所有用户的密码显示方式。

当采用 **cipher-force** 方式后，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，也不起作用。

缺省情况下，所有接入用户的密码显示方式为 **auto**。

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

【举例】

强制所有接入用户采用密码密文方式显示。

```
[Quidway] local-user password-display-mode cipher-force
```

2.1.11 messenger

【命令】

messenger time { **enable** *limit interval* | **disable** }

undo messenger time

【视图】

ISP 域视图

【参数】

limit：设置交换机在用户剩余多长上网时间时，开始向客户端发送提醒消息。单位为分钟，取值范围为 1～60。

interval：发送提醒消息的间隔。单位为分钟，取值范围为 5～60，必须为 5 的倍数。

【描述】

messenger time enable 命令用来开启信使提醒功能并配置其相关参数；**messenger time disable** 命令用来关闭信使提醒功能；**undo messenger time** 命令用来恢复信使提醒功能为缺省情况。

缺省情况下，交换机关闭信使提醒功能。

信使提醒功能指在用户使用网络的过程中，客户端以信息提醒对话框形式，提醒用户剩余的上网时间，使用户可以提前安排自己的工作。

信使提醒功能的实现如下：

- 在交换机上用如下命令配置上网剩余时间（*limit*）及发送提醒消息的间隔（*interval*）；
- 每隔这个时间间隔，交换机将用户上网剩余时间通知到客户端；
- 客户端即以对话框的形式，提醒用户上网时间。

【举例】

设置当用户剩余 30 分钟上网时间的时候开始发送提醒消息，每隔 5 分钟发送一次。

```
[Quidway-isp-system] messenger time enable 30 5
```

2.1.12 name

【命令】

name *string*

undo name

【视图】

VLAN 视图

【参数】

string：为下发的 VLAN 指定名称，为不超过 32 个字符的字符串。

【描述】

name 用来配置下发 VLAN 的名称，**undo name** 用来删除该下发 VLAN 的名称。

缺省情况下，下发 VLAN 无名称。

此命令用来配合动态 VLAN 下发功能使用。动态 VLAN 下发的相关介绍请参见命令 **vlan-assignment-mode**。

S3000 系列交换机中，S3026E、S3026E FM、S3026E FS 和 S3050C 支持此命令；S3026、S3026 FM 和 S3026 FS 不支持此命令。

相关配置可参考命令 **dot1x guest-vlan**，**vlan-assignment-mode**。

【举例】

为 VLAN 100 设置名称为 test。

```
[Quidway] vlan 100
[Quidway-vlan100] name test
```

2.1.13 password

【命令】

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

undo password

【视图】

本地用户视图

【参数】

simple：表示密码为明文。

cipher：表示密码为密文。

password：表示设置的密码，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，结果视输入而定。明文密码可以是长度小于等于 16 的连续字符串，如：huawei918。密文口令的长度必须是 24 位，如_(TT8F]Y\5SQ=^Q`MAF4<1!!。

【描述】

password 命令用来设置本地用户的密码显示方式，**undo password** 命令用来取消指定的密码显示方式。

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，也不起作用。

相关配置可参考命令 **display local-user**。

【举例】

设置名称为 huawei1 的用户采用明文加密方式，密码为 20030422。

```
[Quidway-luser-huawei1] password simple 20030422
```

2.1.14 radius-scheme

【命令】

radius-scheme *radius-scheme-name*

undo radius-scheme

【视图】

ISP 域视图

【参数】

radius-scheme-name：RADIUS 方案名，为不超过 32 个字符的字符串。

【描述】

radius-scheme 命令用来指定当前 ISP 域引用的 RADIUS 方案。**undo radius-scheme** 命令用来恢复域引用缺省的 RADIUS 方案。

缺省情况下，当一个 ISP 域被创建以后，其引用的 RADIUS 方案为系统缺省的 RADIUS 方案（名为“system”，相关参数的配置请参见本章的“RADIUS 配置”一节）。

radius-scheme 命令为当前 ISP 域指定引用的 RADIUS 方案。所指定引用的 RADIUS 方案必须是已经设置好的。

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

【举例】

指定当前 ISP 域“huawei163.net”引用的 RADIUS 方案为“huawei”。

```
[Quidway-isp-huawei163.net] radius-scheme Huawei
```

2.1.15 self-service-url

【命令】

self-service-url enable *url-string*

self-service-url disable

【视图】

ISP 域视图

【参数】

url-string：自助服务器修改用户密码页面的 URL，为字符串形式，长度为 1~64 个字符。字符串中不能包括 “?”字符，如自助服务器的 URL 中包括“?”，则在命令行输入该 URL 时，需要将“?”转换为“|”。

【描述】

self-service-url enable 命令用来启动自助服务器定位功能，**self-service-url disable** 命令用来关闭自助服务器定位功能。

缺省情况下，交换机关闭自助服务器定位功能。

此命令需要与支持自助服务的 RADIUS 服务器配合使用，如 CAMS。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。

如果在交换机上配置了此命令，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 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。

```
[Quidway-isp-system] self-service-url enable
http://10.153.89.94/selfservice/modPasswd1x.jsp|userName
```

2.1.16 service-type

【命令】

S3026E、S3026E FM、S3026E FS 和 S3050C 交换机使用下列命令：

service-type { **ftp** [**ftp-directory** *directory*] | **lan-access** | { **ssh** | **telnet** }* [**level** *level*] }

undo service-type { **ftp** [**ftp-directory**] | **lan-access** | { **ssh** | **telnet** }* [**level** *level*] }

S3026、S3026 FM 和 S3026 FS 交换机使用下列命令：

service-type { **ftp** [**ftp-directory** *directory*] | **lan-access** | **telnet** [**level** *level*] }

undo service-type { **ftp** [**ftp-directory**] | **lan-access** | **telnet** [**level** *level*] }

【视图】

本地用户视图

【参数】

ftp：指定用户为 ftp 类型。

ftp-directory *directory*：指定 ftp 用户的路径。*directory* 为不超过 64 字符的字符串。

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）。

ssh: 指定用户为 SSH 类型。（S3026、S3026 FM 和 S3026 FS 不支持）

telnet：指定用户为 telnet 类型。

level *level*：指定 Telnet 用户或者 SSH 用户的级别。*level* 为整数，取值范围 0~3。缺省为 1。

【描述】

service-type 命令用来设置指定用户的服务类型，**undo service-type** 命令用来取消用户指定的服务类型。

【举例】

设置用户 huawei1 为 lan-access 用户。

```
[Quidway-luser-huawei1] service-type lan-access
```

2.1.17 state

【命令】

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

【视图】

ISP 域视图/本地用户视图

【参数】

active：指定当前 ISP 域（ISP 域视图）/当前用户（本地用户视图）处于活动状态，即系统允许该域下的用户（ISP 域视图）/当前用户（本地用户视图）请求网络服务。

block：指定当前 ISP 域（ISP 域视图）/当前用户（本地用户视图）处于“挂起”状态，即系统不允许该域下的用户（ISP 域视图）/当前用户（本地用户视图）请求网络服务。

【描述】

state 命令用来设置当前 ISP 域/当前用户的状态。

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

当一个本地用户被创建以后，其状态为 **active**（本地用户视图）。

在 ISP 域视图下，每个 ISP 域有两个状态：active 或 block。当指示某个 ISP 域处于 active 状态时，允许该域下的用户请求网络服务；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“huawei163.net”处于“挂起”状态，其下的接入用户不能再请求网络服务。

```
[Quidway-isp-huawei163.net] state block
```

设置用户 huawei1 处于“挂起”状态

```
[Quidway-luser-huawei1] state block
```

2.1.18 vlan-assignment-mode

【命令】

vlan-assignment-mode { **integer** | **string** }

【视图】

ISP 域视图

【参数】

integer：配置 VLAN 下发模式为整型。

string：配置 VLAN 下发模式为字符串型。

【描述】

vlan-assignment-mode 命令用来配置 VLAN 下发模式（整型或者字符串型）。

缺省情况下，VLAN 下发模式为 **integer**，即交换机支持 RADIUS 认证服务器下发整型的 VLAN ID。

动态 VLAN 下发是指以太网交换机根据 RADIUS 服务器下发的属性值，将已经通过身份认证的用户所在端口加入到不同的 VLAN 中，从而对用户所能访问的网络资源进行控制。在实际应用中，为了与 Guest VLAN 配合使用，一般将端口设置为基于端口的方式；如果将端口设置为基于 MAC 地址的方式，则每个端口下面只能连接一个用户。

目前交换机支持 RADIUS 认证服务器下发整型和字符串型的 VLAN ID：

- 整型：交换机根据 RADIUS 认证服务器下发的整型 ID 将端口加入相应 VLAN 中，如果该 VLAN 不存在，则首先创建 VLAN，而后将端口加入到新创建的 VLAN 中。
- 字符串型：交换机根据 RADIUS 认证服务器下发的字符串型 ID，与交换机上已存在 VLAN 的名称进行比对，如果找到匹配项，则将该端口加入相应 VLAN 中，否则 VLAN 下发失败，用户无法通过认证。

📖 **说明：**

对于字符串型 VLAN 下发模式，交换机在处理过程中遵循整型优先的原则：如果 RADIUS 服务器下发的 VLAN 名称是全数字的字符串，如字符串“1024”，并且转换成整型的数值在合法的 VLAN 范围之内，则交换机会将全数字型的字符串转换为整型处理，将认证端口加入转换后的整型数值 VLAN 中，即该端口会被加入到 VLAN 1024 内。

S3000 系列交换机中，S3026E、S3026E FM、S3026E FS 和 S3050C 支持此命令；S3026、S3026 FM 和 S3026 FS 不支持此命令。

相关配置可参考命令 **name**，**dot1x guest-vlan**。

【举例】

配置 VLAN 下发模式为字符串型。

```
[Quidway-isp-huawei163.net] vlan-assignment-mode string
```

2.2 RADIUS 协议配置命令

2.2.1 accounting-on enable

【命令】

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

undo accounting-on { **enable** | **send** | **interval** }

【视图】

RADIUS 方案视图

【参数】

times：设定发送 Accounting-On 报文的最大次数，取值范围 1～256 次，缺省值为 15 次。

interval：发送 Accounting-On 报文的时间间隔，取值范围 1～30 秒，缺省值为 3 秒。

【描述】

accounting-on enable 命令用来启动设备重启用户再认证功能，**undo accounting-on enable** 命令用来关闭该功能，并恢复发送 Accounting-On 报文的时间间隔和最大次数为缺省值。

undo accounting-on send 命令用来恢复发送 Accounting-On 报文的最大次数为缺省值。

undo accounting-on interval 命令用来恢复发送 Accounting-On 报文的时间间隔为缺省值。

缺省情况下，设备重启用户再认证功能处于关闭状态。

设备重启用户再认证功能能够解决交换机重启后，在线用户无法再次登录的问题。启动设备重启用户再认证功能后，交换机每次发生重启时：

- 交换机生成 Accounting-On 报文，该报文主要包括 NAS-ID、NAS-IP（源 IP）和会话 ID 信息；
- 交换机每隔设定的时间间隔向 CAMS 发送 Accounting-On 报文；
- CAMS 收到 Accounting-On 报文后，立即向交换机发送一个响应报文，并根据 Accounting-On 报文中的 NAS-ID、NAS-IP 和会话 ID，找到并删除通过交换机接入的原用户在线信息，并按照最后一次计费更新报文结束计费。
- 当交换机收到 CAMS 的响应报文后，即停止发送 Accounting-On 报文。
- 如果交换机发送 Accounting-On 报文的次数已达到设定的最大发送次数，但是仍没有收到 CAMS 的响应报文，则交换机停止发送 Accounting-On 报文。

📖 **说明：**

Accounting-On 报文中的主要属性：NAS-ID、NAS-IP 和会话 ID 由交换机自动生成，其中 NAS-IP 还可以通过命令（**nas-ip**）手工配置，如果手工配置，请注意配置正确、合法的 IP 地址；如果不配置，交换机会自动选择 VLAN 虚接口的 IP 地址作为 NAS-IP 地址。

S3000 系列交换机中，S3026E、S3026E FM、S3026E FS 和 S3050C 支持此命令；S3026、S3026 FM 和 S3026 FS 不支持此命令。

相关配置可参考命令 **nas-ip**。

【举例】

启动名为 CAMS 的 RADIUS 方案的设备重启用户再认证功能。

```
<Quidway> system-view
[Quidway] radius scheme CAMS
[Quidway-radius-CAMS] accounting-on enable
```

2.2.2 accounting optional

【命令】

accounting optional

undo accounting optional

【视图】

RADIUS 方案视图

【参数】

无

【描述】

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

系统缺省为关闭 RADIUS 计费可选开关。

在对用户上线计费时如果发现没有可用的RADIUS计费服务器或与RADIUS计费服务器通信失败时，若配置了 **accounting optional** 命令，则用户可以继续使用网络资源。否则用户将被切断。

配置了 **accounting optional** 命令的 RADIUS 方案内的所有用户，不再发送实时计费更新报文和停止计费报文。

RADIUS 方案视图下的计费可选开关配置对使用此 RADIUS 方案的计费有效。

【举例】

打开名为 CAMS 的 RADIUS 方案计费可选开关。

```
[Quidway-radius-cams] accounting optional
```

2.2.3 data-flow-format

【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

【视图】

RADIUS 方案视图

【参数】

data：设置数据的单位。

byte：数据单位为比特。

giga-byte：数据单位吉比特。

kilo-byte：数据单位为千比特。

mega-byte：数据单位为兆比特。

packet：设置数据包的单位。

giga-packet：数据包的单位为“giga-packet”。

kilo-packet：数据包的单位为“kilo-packet”。

mega-packet：数据包的单位为“mega-packet”。

one-packet：数据包的单位为“one-packet”。

【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** 命令用来恢复发送到 RADIUS 服务器的数据流的单位为缺省设置。

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 radius**。

【举例】

设置发往服务器 huawei 的数据流的单位为千比特，数据包的单位为 kilo-packet

```
[Quidway-radius-huawei] data-flow-format data kilo-byte packet kilo-packet
```

2.2.4 display local-server statistics

【命令】

display local-server statistics

【视图】

任意视图

【参数】

无

【描述】

display local-server statistics 命令用来显示本地 RADIUS 认证服务器的统计信息。

相关配置可参考命令 **local-server**。

【举例】

显示本地 RADIUS 认证服务器的统计信息。

```
<Quidway> display local-server statistics
The localserver packet statistics:
Receive:                  0          Send:                     0
Discard:                  0          Receive Packet Error:  0
Auth Reveive:           0          Auth Send:             0
```

```
        Acct Receive:           0          Acct Send:              0
```

2.2.5 display radius

【命令】

display radius [*radius-scheme-name*]

【视图】

任意视图

【参数】

radius-scheme-name：RADIUS 方案名，为不超过 32 个字符的字符串。此项如果为空，则显示所有 RADIUS 方案的配置信息。

【描述】

display radius 命令用来显示所有或指定 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（以 S3026E 交换机为例）。

```
<Quidway> display radius
------------------------------------------------------------------
SchemeName  =system                          Index=0    Type=huawei
Primary Auth IP  =127.0.0.1        Port=1645   State=active
Primary Acct IP  =127.0.0.1        Port=1646   State=active
Second  Auth IP  =0.0.0.0          Port=1812   State=block
Second  Acct IP  =0.0.0.0          Port=1813   State=block
Auth Server Encryption Key= huawei
Acct Server Encryption Key= huawei
Accounting method = required
Accounting method = required
TimeOutValue(in second)=3 RetryTimes=3 RealtimeACCT(in minute)=12
Permitted send realtime PKT failed counts       =5
Quiet-interval(min)                             =5
Retry sending times of noresponse acct-stop-PKT =500
Username format                                 =without-domain
Data flow unit                                  =Byte
Packet unit                                     =1
------------------------------------------------------------------
Total 1 RADIUS scheme(s). 1 listed
```

表2-3 Radius 服务器配置信息描述表

域名	描述
SchemeName	RADIUS 服务器的名称
Index	RADIUS 服务器的索引号
Type	RADIUS 服务器的类型
Primary Auth IP/ Port/ State	主认证服务器 IP 地址/接入端口号/该服务器目前状态
Primary Acct IP/ Port/ State	主计费服务器 IP 地址/接入端口号/该服务器目前状态
Second Auth IP/ Port/ State	备份认证服务器 IP 地址/接入端口号/该服务器目前状态
Second Acct IP/ Port/ State	备份计费服务器 IP 地址/接入端口号/该服务器目前状态
Auth Server Encryption Key	认证服务器的登录密码
Acct Server Encryption Key	计费服务器的登录密码
TimeOutValue (seconds)	RADIUS 服务器响应超时定时器时长
Retry Times	RAIUDS 请求报文的最大传送次数
Permitted send realtime PKT failed counts	允许发送的实时计费请求无响应报文的最大次数
Quiet-interval(min)	静默时间间隔
Retry sending times of noresponse acct-stop-PKT	缓存的停止计费请求报文的最大重发次数
Username format	用户名的格式
Data flow unit	数据流的单位
Packet unit	报文包的单位

2.2.6 display radius statistics

【命令】

display radius statistics

【视图】

任意视图

【参数】

无

【描述】

display radius statistics 命令用来显示 RADIUS 报文的统计信息。根据显示的信息，可以帮助诊断与排除 RADIUS 相关故障。

相关配置可参考命令 **radius scheme**。

【举例】

显示 RADIUS 报文的统计信息（以 S3026E 交换机为例）。

```
<Quidway> display radius statistics
state statistic(total=776):
     DEAD=776      AuthProc=0        AuthSucc=0
AcctStart=0         RLTSend=0         RLTWait=0
 AcctStop=0          OnLine=0            Stop=0
 StateErr=0

Receive and Send packets statistic:
Send PKT total  :0        Receive PKT total:0
RADIUS received packets statistic:
Code= 2,Num=0       ,Err=0
Code= 3,Num=0       ,Err=0
Code= 5,Num=0       ,Err=0
Code=11,Num=0       ,Err=0
Code=22,Num=0       ,Err=0

Running statistic:
RADIUS received messages statistic:
Normal auth request             ,Num=0       ,Err=0       ,Succ=0
EAP auth request                ,Num=0       ,Err=0       ,Succ=0
Account request                 ,Num=0       ,Err=0       ,Succ=0
Account off request             ,Num=0       ,Err=0       ,Succ=0
Leaving request                 ,Num=0       ,Err=0       ,Succ=0
<以下略>
```

2.2.7 display stop-accounting-buffer

【命令】

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

【视图】

任意视图

【参数】

radius-scheme *radius-scheme-name*：根据 RADIUS 服务器名显示暂存的停止计费请求报文。其中，*radius-scheme-name* 为 RADIUS 方案名，为不超过 32 个字符的字符串。

session-id *session-id*：根据会话 ID 显示暂存的停止计费请求报文。其中，*session-id* 为会话 ID，为不超过 50 个字符的字符串。

time-range *start-time stop-time*：根据停止计费请求时刻显示暂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-yyyy/mm/dd。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*：根据用户名显示暂存的停止计费请求报文。

【描述】

display stop-accounting-buffer 命令用来显示缓存在交换机系统中的停止计费请求报文。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，交换机系统会缓存该报文，然后以一定的次数重新发送，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, retry stop-accounting**。

【举例】

显示从 2002 年 8 月 31 日 0 点 0 分 0 秒到 2002 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。

```
<Quidway> display stop-accounting-buffer time-range 0:0:0-2002/08/31
23:59:59-2002/08/31
Total find    0 record
```

2.2.8 key

【命令】

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

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

【视图】

RADIUS 方案视图

【参数】

accounting：指示设置/删除 RADIUS 计费报文的加密密钥。

authentication：指示设置/删除 RADIUS 认证/授权报文的加密密钥。

string：密钥。为不超过 16 个字符的字符串。缺省情况下，密钥为“huawei”。

【描述】

key 命令用来设置 RADIUS 认证/授权或计费报文的加密密钥，**undo key** 命令用来恢复相应的加密密钥为缺省设置。

RADIUS 客户端（即交换机系统）与 RADIUS 服务器使用 MD5 算法来加密交互的 RADIUS 报文，双方通过设置加密密钥来验证报文的合法性。只有在密钥一致的情况下，双方才能彼此接收对方发来的报文并作出响应。因此，必须保证交换机系统上设置的加密密钥与 RADIUS 服务器上的完全一样。在认证/授权服务器与计费服务器不相同且这两台服务器中的加密密钥也不同时，必须分别设置认证/授权报文和计费报文的加密密钥。

相关配置可参考命令 primary accounting, primary authentication, radius scheme。

【举例】

例 1：

将 RADIUS 方案“huawei”的认证/授权报文的加密密钥设置为“hello”。

```
[Quidway-radius-huawei] key authentication hello
```

例 2：

将 RADIUS 方案“huawei”的计费报文的加密密钥设置为“ok”。

```
[Quidway-radius-huawei] key accounting ok
```

2.2.9 local-server

【命令】

local-server nas-ip *ip-address* **key** *password*

undo local-server nas-ip *ip-address*

【视图】

系统视图

【参数】

nas-ip *ip-address*：设置接入服务器的 NAS-IP 地址，地址采用点分十进制格式。缺省存在一个 NAS-IP 为 127.0.0.1 的本地服务器。

key *password*：设置认证报文的加密密钥，为不超过 16 个字符的字符串，缺省为 huawei。

【描述】

local-server 命令用来设置本地 RADIUS 认证服务器的相关参数，**undo local-server** 命令用来删除某个设置的本地 RADIUS 认证服务器。

Quidway 系列交换机除了支持传统的作为 RADIUS 客户端的服务——即分别采用认证/授权服务器、计费服务器的方式进行用户的认证管理外，还提供了本机的简单 RADIUS 服务器端功能（包括认证和授权），称之为本地 RADIUS 认证服务器功能。

注意：

- 采用华为公司的本地 RADIUS 服务器功能时，其认证/授权服务的 UDP 端口号必须为 1645，计费服务的 UDP 端口号为 1646。
- 用此命令配置的报文加密密钥（key *password*）必须和在 RADIUS 方案视图下用命令 **key authentication** 配置的认证/授权报文加密密钥一致。

Quidway 系列交换机最多支持 16 个本地 RADIUS 服务器。

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

【举例】

设置本地 RADIUS 方案的 IP 地址为 10.110.1.2、登录密码为 huawei。

```
[Quidway] local-server nas-ip 10.110.1.2 key huawei
```

2.2.10 nas-ip

【命令】

nas-ip *ip-address*

undo nas-ip

【视图】

RADIUS 方案视图

【参数】

ip-address：源 IP 地址，点分十进制形式。

【描述】

nas-ip 命令用来设置 NAS（交换机）发送 RADIUS 报文使用的源 IP 地址，这样发送到 RADIUS 服务器的所有报文携带相同的源 IP 地址。**undo nas-ip** 命令用来删除配置。

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。

缺省情况下，报文的源 IP 地址是发送接口的 IP 地址。

相关配置可参考命令 **display radius**。

【举例】

配置 NAS（交换机）发送 RADIUS 报文使用的源 IP 地址为 10.1.1.1。

```
[Quidway] radius scheme test1
[Quidway-radius-test1] nas-ip 10.1.1.1
```

2.2.11 primary accounting

【命令】

primary accounting *ip-address* [*port-number*]

undo primary accounting

【视图】

RADIUS 方案视图

【参数】

ip-address：IP 地址，为点分十进制格式。

port-number：UDP 端口号。取值范围为 1～65535。

【描述】

primary accounting 命令用来设置主 RADIUS 计费服务器的 IP 地址和端口号，**undo primary accounting** 命令用来将主 RADIUS 计费服务器的 IP 地址和端口号恢复为缺省值。

缺省情况下，对于系统创建的 RADIUS 方案“system”，其主计费服务器的 IP 地址为 127.0.0.1，UDP 端口号为 1646；对于新创建的 RADIUS 方案，其主计费服务器的 IP 地址为 0.0.0.0，UDP 端口号为 1813。

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备份服务器的区别。 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，请保证交换机上的 RADIUS 服务端口设置与 RADIUS 服务器上的端口设置保持一致。

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

【举例】

设置 RADIUS 方案“huawei”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。

```
[Quidway-radius-huawei] primary accounting 10.110.1.2 1813
```

2.2.12 primary authentication

【命令】

primary authentication *ip-address* [*port-number*]

undo primary authentication

【视图】

RADIUS 方案视图

【参数】

ip-address：IP 地址，为点分十进制格式。

port-number：UDP 端口号。取值范围为 1～65535。

【描述】

primary authentication 命令用来设置主 RADIUS 认证/授权的 IP 地址和端口号，**undo primary authentication** 命令用来将主 RADIUS 认证/授权的 IP 地址和端口号恢复为缺省值。

缺省情况下，对于系统创建的 RADIUS 方案“system”，其主认证服务器的 IP 地址为 127.0.0.1，UDP 端口号为 1645，备份认证服务器的 IP 地址为 0.0.0.0，UDP 端口号为 1812；对于新创建的 RADIUS 方案，其主、备份认证服务器的 IP 地址为 0.0.0.0，UDP 端口号为 1812。

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备份服务器的区别。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，请保证交换机上的 RADIUS 服务端口设置与 RADIUS 服务器上的端口设置保持一致。

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

【举例】

设置 RADIUS 方案“huawei”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。

```
[Quidway-radius-huawei] primary authentication 10.110.1.1 1812
```

2.2.13 radius nas-ip

【命令】

radius nas-ip *ip-address*

undo radius nas-ip

【视图】

系统视图

【参数】

ip-address：指定的源 IP 地址，点分十进制形式。

【描述】

radius nas-ip 命令用来指定 NAS 发送 RADIUS 报文使用的源地址。**undo radius nas-ip** 命令用来恢复缺省状态。

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。

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。

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。

相关配置可参考命令 **nas-ip**。

【举例】

配置交换机发送 radius 报文使用的源地址为 129.10.10.1。

```
[Quidway] radius nas-ip 129.10.10.1
```

2.2.14 radius scheme

【命令】

radius scheme *radius-scheme-name*

undo radius scheme *radius-scheme-name*

【视图】

系统视图

【参数】

radius-scheme-name：RADIUS 方案名，为不超过 32 个字符的字符串。

【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，系统中已创建了一个名为“system”的 RADIUS 方案，其各项属性均为缺省值。

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（交

换机系统）与之交互所需的一些参数。因此，在进行其它 RADIUS 协议配置之前，必须先创建 RADIUS 方案并进入其视图。

一个 RADIUS 方案可以同时被多个 ISP 域引用。包括系统缺省创建的“system”方案在内，用户最多能够配置 16 个 RADIUS 方案。

undo radius scheme 命令虽然可以用来删除指定的 RADIUS 方案，但是不能删除缺省的 RADIUS 方案。注意：当有使用该方案的用户在线时不允许删除。

相关配置可参考命令 **key**，**retry realtime-accounting**， **radius-scheme**，**timer realtime-accounting**，**stop-accounting-buffer enable, retry stop-accounting**，**server-type**，**state**，**user-name-format**，**retry**，**display radius**，**display radius statistics**。

【举例】

创建名为“huawei”的 RADIUS 方案并进入其视图。

```
[Quidway] radius scheme huawei
[Quidway-radius-huawei]
```

2.2.15 reset radius statistics

【命令】

reset radius statistics

【视图】

用户视图

【参数】

无

【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**。

【举例】

清除 RADIUS 协议的统计信息。

```
<Quidway> reset radius statistics
```

2.2.16 reset stop-accounting-buffer

【命令】

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

【视图】

用户视图

【参数】

radius-scheme *radius-scheme-name*：根据 RADIUS 服务器名删除暂存的停止计费请求报文。其中，*radius-scheme-name* 为 RADIUS 方案名，为不超过 32 个字符的字符串。

session-id *session-id*：根据会话 ID 删除暂存的停止计费请求报文。其中，*session-id* 为会话 ID，为不超过 50 个字符的字符串。

time-range *start-time stop-time*：根据停止计费请求时刻删除暂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-yyyy/mm/dd。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删除。

user-name *user-name*：根据用户名删除暂存的停止计费请求报文。

【描述】

reset stop-accounting-buffer 命令用来删除那些缓存的、没有得到响应的停止计费请求报文。

在发送停止计费请求报文而 RADIUS 服务器没有响应时，交换机系统会缓存该报文，然后以一定的次数重新发送，具体发送的次数由 **retry stop-accounting** 命令设置。

reset stop-accounting-buffer 命令用来删除缓存在交换机系统中的停止计费请求报文。可以选择删除发往某个 RADIUS 方案的报文；也可以根据用户会话的 session-id 或用户名来删除报文；还可以指定一个时间段，删除那些发起停止计费请求的时刻处于指定时间段内的报文。

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

【举例】

删除用户“user0001@huawei163.net”缓存在系统中的停止计费请求报文。

```
<Quidway> reset stop-accounting-buffer user-name user0001@huawei163.net
```

删除从 2002 年 8 月 31 日 0 点 0 分 0 秒到 2002 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。

```
<Quidway> reset stop-accounting-buffer time-range 0:0:0-2002/08/31
23:59:59-2002/08/31
```

2.2.17 retry

【命令】

retry *retry-times*

undo retry

【视图】

RADIUS 方案视图

【参数】

retry-times：最大传送次数，取值范围为 1～20。缺省情况下，RAIUDS 请求报文的最大传送次数为 3 次。

【描述】

retry 命令用来设置 RAIUDS 请求报文的最大传送次数，**undo retry** 命令用来将 RAIUDS 请求报文的最大传送次数恢复为缺省值。

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 服务器在响应超时定时器规定的时长内没有响应 NAS，则 NAS 有必要向 RADIUS 服务器重传 RADIUS 请求报文。

假设最大重传次数为 N，则如果累计的传送次数超过（N-[N/2]）次而主 RADIUS 服务器仍旧没有响应，则交换机将认为其与当前 RADIUS 服务器的通信已经中断，并将转而向其它的 RADIUS 服务器发送请求报文。

根据网络状况合理的设置重发次数可以提高系统的响应速度。

相关配置可参考命令 **radius scheme**。

【举例】

设置在 RADIUS 方案“huawei”下，RAIUDS 请求报文的最大传送次数为 5 次。

```
[Quidway-radius-huawei] retry 5
```

2.2.18 retry realtime-accounting

【命令】

retry realtime-accounting *retry-times*

undo retry realtime-accounting

【视图】

RADIUS 方案视图

【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。缺省情况下，最多允许 5 次实时计费请求无响应。

【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** 命令用来恢复允许实时计费请求无响应的最大次数为缺省值。

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 NAS 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 NAS 端尽量与 RADIUS 服务器同步切断用户连接。Quidway 系列交换机提供对连续实时计费请求无响应次数限制的设置，在交换机向 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，交换机将切断用户连接。

相关配置可参考命令 **radius scheme**，**timer realtime-accounting**。

【举例】

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

```
[Quidway-radius-huawei] retry realtime-accounting 10
```

2.2.19 retry stop-accounting

【命令】

retry stop-accounting *retry-times*

undo retry stop-accounting

【视图】

RADIUS 方案视图

【参数】

retry-times：缓存的停止计费请求报文的最大重发次数，取值范围为 10～65535。缺省情况下，取值为 500。

【描述】

retry stop-accounting 命令用来指示当出现没有得到响应的停止计费请求时，将该报文存入交换机缓存后，停止计费请求报文的最大重发次数。**undo retry stop-accounting** 命令用来恢复停止计费请求报文的最大重发次数为缺省值。

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 NAS 应该尽最大努力把它发送给 RADIUS 计费服务器。所以，如果 RADIUS 计费服务器对交换机发出的停止计费请求报文没有响应，交换机

应将其缓存在本机上，然后重新发送直到 RADIUS 计费服务器产生响应，或者在重新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**，**radius scheme** ，**display stop-accounting-buffer**。

【举例】

指示对于 RADIUS 方案“huawei”中的服务器，交换机系统最多可以将缓存的停止计费请求报文重发 1000 次。

```
[Quidway-radius-huawei] retry stop-accounting 1000
```

2.2.20 secondary accounting

【命令】

secondary accounting *ip-address* [*port-number*]

undo secondary accounting

【视图】

RADIUS 方案视图

【参数】

ip-address：IP 地址，为点分十进制格式。缺省情况下，备份计费服务器的 IP 地址均为 0.0.0.0。

port-number：UDP 端口号。取值范围为 1～65535。缺省情况下，计费服务的 UDP 端口号为 1813。

【描述】

secondary accounting 命令用来设置备份 RADIUS 计费服务器的 IP 地址和端口号，**undo secondary accounting** 命令用来将备份 RADIUS 计费服务器的 IP 地址和端口号恢复为缺省值。

具体的描述请参见 **primary accounting** 命令的描述部分。

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

【举例】

设置 RADIUS 方案“huawei”的备份计费服务器的 IP 地址为 10.110.1.1、使用 UDP 端口 1813 提供 RADIUS 计费服务。

```
[Quidway-radius-huawei] secondary accounting 10.110.1.1 1813
```

2.2.21 secondary authentication

【命令】

secondary authentication *ip-address* [*port-number*]

undo secondary authentication

【视图】

RADIUS 方案视图

【参数】

ip-address：IP 地址，为点分十进制格式。缺省情况下，备份认证/授权的 IP 地址均为 0.0.0.0。

port-number：UDP 端口号。取值范围为 1～65535。缺省情况下，认证/授权服务的 UDP 端口号为 1812。

【描述】

secondary authentication 命令用来设置备份 RADIUS 认证/授权服务器的 IP 地址和端口号，**undo secondary authentication** 命令用来将备份 RADIUS 认证/授权服务器的 IP 地址和端口号恢复为缺省值。

具体的描述请参见 **primary authentication** 命令的描述部分。

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

【举例】

设置 RADIUS 方案“huawei”的备份认证/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。

```
[Quidway-radius-huawei] secondary authentication 10.110.1.2 1812
```

2.2.22 server-type

【命令】

server-type { **huawei** | **iphotel** | **portal** | **standard** }

undo server-type

【视图】

RADIUS 方案视图

【参数】

huawei：指示交换机系统支持 Huawei 类型的 RADIUS 服务器，即要求 RADIUS 客户端（交换机系统）和 RADIUS 服务器按照华为公司私有 RADIUS 协议的规程和报文格式进行交互。

iphotel：指示交换机系统支持 IP Hotel 类型的 RADIUS 服务器，即要求 RADIUS 客户端（交换机系统）和 RADIUS 服务器按照 IP Hotel（RADIUS 协议的一种扩展）的规程和报文格式进行交互。

portal：指示交换机系统支持 Portal 类型的 RADIUS 服务器，即要求 RADIUS 客户端（交换机系统）和 RADIUS 服务器按照 Portal（RADIUS 协议的一种扩展）的规程和报文格式进行交互。

standard：指示交换机系统支持 Standard 类型的 RADIUS 服务器，即要求 RADIUS 客户端（交换机系统）和 RADIUS 服务器按照标准 RADIUS 协议（RFC 2138/2139 或更新）的规程和报文格式进行交互。

【描述】

server-type 命令用来指定交换机系统支持的 RADIUS 服务器类型。**undo server-type** 命令用来恢复交换机系统支持的 RADIUS 服务器类型为缺省设置。

缺省情况下，对于新创建的 RADIUS 方案，其支持的 RADIUS 服务器类型为 **standard**；对于系统缺省创建的 RADIUS 方案“system”，其缺省支持的 RADIUS 服务器类型为 **huawei**。

Quidway 系列交换机同时支持标准的 RADIUS 协议和华为公司的 IP Hotel、201+、Portal 等扩展 RADIUS 业务平台。可以通过 **server-type** 命令来选择支持何种 RADIUS 服务器类型。

相关配置可参考命令 **radius scheme**。

【举例】

将 RADIUS 方案“huawei”的 RADIUS 服务器类型设置为 IP Hotel。

```
[Quidway-radius-huawei] server-type iphotel
```

2.2.23 state

【命令】

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

【视图】

RADIUS 方案视图

【参数】

primary：指示设置主 RADIUS 服务器的状态。

secondary：指示设置备份 RADIUS 服务器的状态。

accounting：指示设置 RADIUS 计费服务器的状态。

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

block：指示 RADIUS 服务器的状态为 **block**，即处于宕机状态。

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

【描述】

state 命令用来设置 RADIUS 服务器的状态。

缺省情况下，所有 RADIUS 方案中各 RADIUS 服务器的状态均为 **block**。

对于某个 RADIUS 方案中的主、备服务器（无论是认证/授权服务器还是计费服务器），当主服务器因故障而导致其与 NAS 的通信中断时，NAS 会主动地转而与备份服务器交互报文。当主服务器恢复正常后，NAS 却不会立即恢复与其通信，而是继续与备份服务器通信；直到备份服务器也出现故障后，NAS 才能再转而恢复与主服务器交互报文。为了使 NAS 在主服务器故障排除后迅速恢复与其通信，需要通过 **state** 命令手工将主服务器的状态设为 **active**。

当主服务器与备份服务器的状态都为 **active** 或都为 **block** 时，NAS 将只把报文发送到主服务器上。

相关配置可参考命令 **radius scheme**, **primary authentication**, **secondary authentication**, **primary accounting**, **secondary accounting**。

【举例】

将 RADIUS 方案“huawei”的备份认证服务器的状态设置为 active。

```
[Quidway-radius-huawei] state secondary authenticaiton active
```

2.2.24 stop-accounting-buffer enable

【命令】

stop-accounting-buffer enable

undo stop-accounting-buffer enable

【视图】

RADIUS 方案视图

【参数】

无

【描述】

stop-accounting-buffer enable 命令用来允许在交换机系统上缓存没有得到响应的停止计费请求报文。**undo stop-accounting-buffer enable** 命令用来禁止在交换机系统上缓存没有得到响应的停止计费请求报文。

缺省情况下，允许交换机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 NAS 应该尽最大努力把它发送给 RADIUS 计费服务器。所以，如果 RADIUS 计费服务器对交换机发出的停止计费请求报文没有响应，交换机应将其缓存在本机上，然后重新发送直到 RADIUS 计费服务器产生响应，或者在重新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**，**radius scheme** ，**display stop-accounting-buffer**。

【举例】

指示对于 RADIUS 方案“huawei”中的服务器，交换机系统能够缓存没有得到响应的停止计费请求报文。

```
[Quidway-radius-huawei] stop-accounting-buffer enable
```

2.2.25 timer

【命令】

timer *seconds*

undo timer

【视图】

RADIUS 方案视图

【参数】

seconds：RADIUS 服务器响应超时定时器，单位为秒，取值范围为 1～10。缺省情况下，RADIUS 服务器响应超时定时器为 3 秒。

【描述】

timer 命令用来设置 RADIUS 服务器响应超时定时器，**undo timer** 命令用来将 RADIUS 服务器响应超时定时器恢复为缺省值。

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，NAS 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，交换机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，**timer** 命令就是用来设置这个定时器长度的。

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。

相关配置可参考命令 **radius scheme**, **retry**。

【举例】

将 RADIUS 方案“huawei”的响应超时定时器设置为 5 秒。

```
[Quidway-radius-huawei] timer 5
```

2.2.26 timer quiet

【命令】

timer quiet *minutes*

undo timer quiet

【视图】

RADIUS 方案视图

【参数】

minutes：静默时间间隔，单位为分钟，取值范围为 1～255，缺省值为 5 分钟。

【描述】

timer quiet 命令用来配置静默时间间隔，即主、备份 RADIUS 服务器切换的时间间隔，**undo timer quiet** 命令用来恢复静默时间间隔为缺省值。

静默时间作用如下：

- 交换机首先向主 RADIUS 服务器发送 RADIUS 报文；
- 在确定主服务器没有响应后，交换机就会向备份 RADIUS 服务器发送 RADIUS 报文；
- 每隔静默时间间隔，交换机就会将主 RADIUS 服务器状态置为 active，下次 RADIUS 报文将发送至主服务器。

S3000 系列交换机中，S3026E、S3026E FM、S3026E FS 和 S3050C 支持此命令；S3026、S3026 FM 和 S3026 FS 不支持此命令。

【举例】

设置 RADIUS 方案“huawei”的静默时间间隔为 3 分钟。

```
[Quidway] radius scheme huawei
[Quidway-radius-huawei] timer quiet 3
```

2.2.27 timer realtime-accounting

【命令】

timer realtime-accounting *minutes*

undo timer realtime-accounting

【视图】

RADIUS 方案视图

【参数】

minutes：实时计费的时间间隔，单位为分钟，取值范围为 3～60，必须为 3 的倍数。缺省情况下，实时计费的时间间隔为 12 分钟。

【描述】

timer realtime-accounting 命令用来设置实时计费的时间间隔，**undo timer realtime-accounting** 命令用来将实时计费的时间间隔恢复为缺省值。

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，NAS 会向 RADIUS 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 NAS 和 RADIUS 服务器的性能有一定的相关性要求——取值越小，对 NAS 和 RADIUS 服务器的性能要求越高。建议当用户量比较大（≥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2-4 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
≥1000	≥15

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

【举例】

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

```
[Quidway-radius-huawei ] timer realtime-accounting 51
```

2.2.28 user-name-format

【命令】

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

【视图】

RADIUS 方案视图

【参数】

with-domain：指定发送给 RADIUS 服务器的用户名带域名。

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

【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，发送给 RADIUS 服务器的用户名携带有 ISP 域名。

接入用户通常以“userid@isp-name”的格式命名，“@”后面的部分为 ISP 域名，交换机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，交换机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。

🕮 **说明：**

- 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;
- IEEE 802.1X 规定，EAP 认证方式不应改动报文内容，因此当配置交换机采用 EAP 认证方式时，**user-name-format** 命令无效。

相关配置可参考命令 **radius scheme**。

【举例】

指定发送给 RADIUS 方案“huawei”中 RADIUS 服务器的用户名不得携带域名。

```
[Quidway-radius-huawei] user-name-format without-domain
```

第3章 EAD 配置命令

📖 说明：

Quidway S3000 系列以太网交换机中，S3026E、S3026E FM、S3026E FS 和 S3050C 支持 EAD 特性；S3026、S3026 FM 和 S3026 FS 不支持 EAD 特性。

3.1 EAD 配置命令

3.1.1 session-control-server

【命令】

session-control-server *ip-address*

undo session-control-server [*ip-address* | **all**]

【视图】

RADIUS 方案视图

【参数】

ip-address：安全策略服务器的 IP 地址。

all：所有安全策略服务器的 IP 地址。

【描述】

session-control-server 命令用来配置安全策略服务器的 IP 地址。**undo session-control-server** 命令用来取消安全策略服务器的 IP 地址的配置。

每个 RADIUS 方案中最多允许配置 8 个不同 IP 的安全策略服务器地址。在用户上网过程中，交换机只会响应从认证服务器以及安全策略服务器发来的会话控制报文。

【举例】

配置安全策略服务器的 IP 地址为 192.168.0.1。

```
<Quidway>system-view
System View: return to User View with Ctrl+Z.
[Quidway] radius scheme Quidway
[Quidway-radius-Quidway] session-control-server 192.168.0.1
```

第4章 HABP 配置命令

4.1 HABP 命令

4.1.1 display debugging habp

【命令】

display debugging habp

【视图】

任意视图

【参数】

无

【描述】

display debugging habp 命令用来显示 HABP 的调试开关状态。

【举例】

显示 HABP 的调试状态。

```
<Quidway> display debugging habp
HABP Debugging switch is on
```

以上信息表示交换机的 HABP 调试处于开启状态。

4.1.2 display habp

【命令】

display habp

【视图】

任意视图

【参数】

无

【描述】

display habp 命令用来显示 HABP 特性的配置信息和状态。

【举例】

显示 HABP 特性的配置信息和状态。

```
[Quidway] display habp
Global HABP information:
        HABP Mode: Server
        Sending HABP request packets every 20 seconds
        Bypass VLAN: 2
```

表4-1 显示信息描述表

域名	解释
HABP Mode	当前交换机的 HABP 特性的工作模式，可以为 server 或者 client
Sending HABP request packets every 20 seconds	HABP 请求报文的发送时间间隔
Bypass VLAN	在指定的 VLAN 内发送 HABP 报文

4.1.3 display habp table

【命令】

display habp table

【视图】

任意视图

【参数】

无

【描述】

display habp table 命令用来显示 HABP 的 MAC 地址表的信息。

【举例】

显示 HABP 的 MAC 地址表的信息。

```
[Quidway] display habp table
MAC             Holdtime  Receive Port
001f-3c00-0030  53        Ethernet0/1
```

表4-2 显示信息描述表

域名	解释
MAC	HABP 的 MAC 地址表项中的 MAC 地址
Holdtime	MAC 地址表项的保持时间，在此时间内如果该表项没有被刷新过，该表项将被老化
Receive Port	学习到该 MAC 地址表项的端口

4.1.4 display habp traffic

【命令】

display habp traffic

【视图】

任意视图

【参数】

无

【描述】

display habp traffic 命令用来显示 HABP 报文的统计信息。

【举例】

显示 HABP 报文的统计信息。

```
[Quidway] display habp traffic
HABP counters :
        Packets output: 0, Input: 0
        ID error: 0, Type error: 0, Version error: 0
        Sent failed: 0
```

表4-3 显示信息描述表

域名	解释
Packets output	发送的 HABP 报文数
Input	接收的 HABP 报文数
ID error	ID 错误的报文数
Type error	类型错误的报文数
Version error	版本错误的报文数
Sent failed	发送失败的报文数

4.1.5 habp enable

【命令】

habp enable

undo habp enable

【视图】

系统视图

【参数】

无

【描述】

habp enable 命令用来启动交换机的 HABP 特性，**undo hapb enable** 命令用来。

缺省情况下，交换机上不启动 HABP 特性。

如果交换机上启动了 802.1x 特性，如果不启动交换机的 HABP 特性，作为管理设备的交换机将不能管理下挂的交换机。因此在启动了 802.1x 特性的网络中，需要启动相应交换机的 HABP 特性。

【举例】

启动交换机的 HABP 特性。

```
[Quidway] habp enable
```

4.1.6 habp server vlan

【命令】

habp server vlan *vlan-id*

undo habp server

【视图】

系统视图

【参数】

vlan-id：VLAN 的 ID，取值范围 1～4094。

【描述】

habp server vlan 命令用来在交换机上设置 HABP 特性的模式为 server 模式，同时指定 HABP 报文在指定的 VLAN 内传播，**undo hapb server vlan** 命令用来恢复交换机 HABP 特性为缺省模式。

缺省情况下，交换机的 HABP 特性工作在 client 模式下。

用户必须首先使用 **habp enable** 命令在交换机上启动 HABP 特性，然后才能指定 HABP 特性工作在 server 模式下。

【举例】

在交换机上设置 HABP 特性的模式为 server 模式，同时指定 HABP 报文在指定的 VLAN 2 内传播。

```
[Quidway] habp server vlan 2
```

4.1.7 habp timer

【命令】

habp timer *interval*

undo habp timer

【视图】

系统视图

【参数】

interval：发送 HABP 请求报文的时间间隔，取值范围为 5～600，单位为秒。缺省情况下，交换机发送 HABP 请求报文的时间间隔为 20 秒。

【描述】

habp timer 命令用来设置交换机发送 HABP 请求报文的时间间隔，**undo habp timer** 命令用来将发送 HABP 请求报文的时间间隔恢复为缺省值。

本配置只需要在 HABP 特性工作模式为 server 的交换机上进行配置。

【举例】

设置发送 HABP 请求报文的时间间隔为 50 秒。

```
[Quidway] habp timer 50
```