目 录

1 User Profile

1.1 User Profile简介

User Profile（用户配置文件）提供一个配置模板，用于保存预设配置（一系列配置的集合）。用户可以根据不同的应用场景在这个配置模板中定义不同的内容，比如CAR（Committed Access Rate，承诺访问速率）策略、QoS（Quality of Service，服务质量）策略或连接数限制策略等。

用户访问设备时，需要先进行上线用户身份认证（例如802.1X接入认证方式）。用户通过身份认证后，认证服务器会将与用户帐户绑定的User Profile名称下发给设备，设备会根据指定User Profile里配置的内容对上线用户进行限制。

基于User Profile的用户身份认证需要与认证服务器配合使用：

- 若用户采用远程认证，则需要在远程认证服务器上指定与该用户帐户相关联的User Profile。
- 若用户采用本地认证，则需要在设备对应的本地用户视图中指定该用户的授权User Profile。关于本地用户的相关配置，请参见“安全配置指导”中的“AAA”。

当用户通过认证上线后，其访问行为将受到User Profile的限制。当用户下线时，系统会自动取消相应的限制。因此，User Profile适用于限制上线用户的访问行为，没有用户上线（例如没有用户接入、用户没有通过认证或者用户下线）时，对应的User Profile配置并不生效。

使用User Profile之后，可以：

- 更精确地利用系统资源。比如基于接口进行流量监管，此时限制的是一群用户（从指定接口接入的用户）。使用User Profile之后，可以基于用户进行流量监管，此时限制的是单个用户。
- 更灵活地限制用户访问系统资源。比如只对当前接口的所有流进行流量监管，当用户的物理位置移动时（比如从另一个接口接入），则需要先取消旧的接入接口下的流量监管功能，再在新的接入接口下配置流量监管功能。使用User Profile之后，可以基于用户进行流量监管，只要用户上线，认证服务器会自动下发相应的User Profile，当用户下线，对应的配置亦会失效，不需要再进行手工调整。

1.2 User Profile配置任务简介

表1-1 User Profile配置任务简介

配置任务	说明	详细配置
配置User Profile	必选	1.3

1.3 配置User Profile

User Profile是和认证配合使用的，用户需要保证相应的认证配置。同时，需要在本地或服务器上配置指定下发给用户的User Profile。

表1-2 配置 User Profile

操作	命令	说明
进入系统视图	**system-view**	-
创建User Profile并进入相应的User Profile视图	**user-profile** *profile-name*	缺省情况下，不存在User Profile。 如果指定的User Profile已经存在，则直接进入相应的User Profile视图，不需要再创建

User Profile 创建之后，需要在 User Profile 视图下配置具体的内容才能对上线用户进行限制。目前支持配置 QoS 策略，关于 QoS 策略的详细内容请参见“ACL 和 QoS 配置指导”中的“QoS”。

1.4 User Profile显示和维护

在任意视图下执行 **display** 命令可以显示 User Profile 的配置信息和在线用户信息，通过查看显示信息验证配置的效果。

表1-3 显示 User Profile

操作	命令
显示user profile的配置信息和在线用户信息	**display user-profile** [**name** *profile-name*] [**slot** *slot-number*]

1.5 User Profile典型配置举例

1.5.1 802.1X本地认证/授权用户应用QoS策略典型配置举例

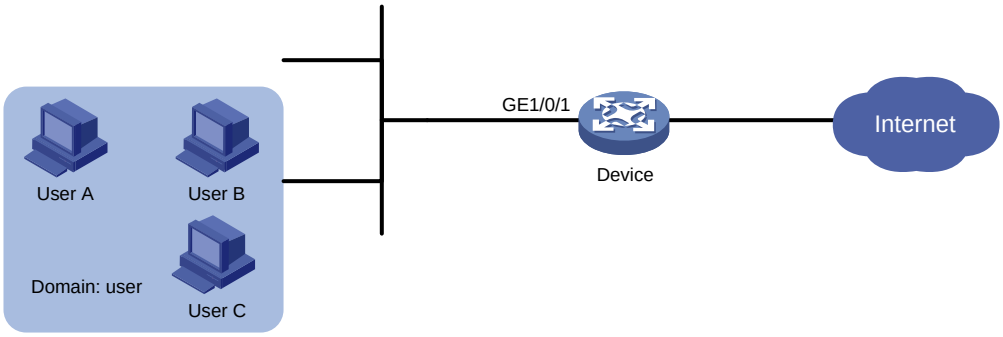
1. 组网需求

如 图 1-1 所示，接入设备Device上连接了三个 802.1X认证用户，这些用户属于同一个ISP域“user”，为了提高认证/授权的效率，该ISP域内用户采用Device本地认证方法。现要求对三个用户的流量进行如下控制：

- UserA 在每天上午 8:30 至 12:00 间即使通过认证也不不能访问网络。
- UserB 在通过认证后的上传速率限制为 2M。
- UserC 在通过认证后的下载速率限制为 4M。

2. 组网需求

图1-1 802.1X 本地认证/授权用户应用 Qos 策略组网示意图



3. 配置步骤

(1) 创建对 UserA 的接入时间进行控制的 QoS 策略

创建周期时间段 for_usera，时间范围为每天的 8:30～12:00。

```
[Device] time-range for_usera 8:30 to 12:00 daily
```

定义基本 IPv4 ACL 2000，匹配 for_usera 内的所有报文。

```
[Device] acl basic 2000
[Device-acl-basic-2000] rule permit time-range for_usera
[Device-acl-basic-2000] quit
```

创建流分类 for_usera，分类规则为匹配 ACL 2000。

```
[Device] traffic classifier for_usera
[Device-classifier-for_usera] if-match acl 2000
[Device-classifier-for_usera] quit
```

创建流行为 for_usera，动作为拒绝通过。

```
[Device] traffic behavior for_usera
[Device-behavior-for_usera] filter deny
[Device-behavior-for_usera] quit
```

创建 QoS 策略 for_usera，将流分类和流行为进行关联。

```
[Device] qos policy for_usera
[Device-qospolicy-for_usera] classifier for_usera behavior for_usera
[Device-qospolicy-for_usera] quit
```

(2) 为 UserA 创建 User Profile，并应用 QoS 策略

创建 User Profile，名称为 usera。

```
[Device] user-profile usera
```

由于是对 UserA 发送的报文进行过滤，因此在应用 QoS 策略时应该应用到设备的入方向。

```
[Device-user-profile-usera] qos apply policy for_usera inbound
[Device-user-profile-usera] quit
```

(3) 创建对 UserB 的速率进行限制的 QoS 策略

创建流分类 class，匹配所有报文。

```
[Device] traffic classifier class
[Device-classifier-class] if-match any
[Device-classifier-class] quit
```

创建流行为 for_userb，动作为流量监管，cir 为 2000kbps。

```
[Device] traffic behavior for_userb
[Device-behavior-for_userb] car cir 2000
[Device-behavior-for_userb] quit
```

创建 QoS 策略 for_userb，将流分类和流行为进行关联。

```
[Device] qos policy for_userb
[Device-qospolicy-for_userb] classifier class behavior for_userb
[Device-qospolicy-for_userb] quit
```

(4) 为 UserB 创建 User Profile，并应用 QoS 策略

创建 User Profile，名称为 userb。

```
[Device] user-profile userb
```

由于是对 UserB 发送的报文进行过滤，因此在应用 QoS 策略时应该应用到设备的入方向。

```
[Device-user-profile-userb] qos apply policy for_userb inbound
[Device-user-profile-userb] quit
```

(5) 创建对 UserC 的速率进行限制的 QoS 策略

创建流行为 for_userc，动作为流量监管，cir 为 4000kbps。

```
[Device] traffic behavior for_userc
[Device-behavior-for_userc] car cir 4000
[Device-behavior-for_userc] quit
```

创建 QoS 策略 for_userc，将流分类和流行为进行关联。

```
[Device] qos policy for_userc
[Device-qospolicy-for_userc] classifier class behavior for_userc
[Device-qospolicy-for_userc] quit
```

(6) 为 UserC 创建 User Profile，并应用 QoS 策略

创建 User Profile，名称为 userc。

```
[Device] user-profile userc
```

由于是对 UserC 接收的报文进行过滤，因此在应用 QoS 策略时应该应用到设备的出方向。

```
[Device-user-profile-userc] qos apply policy for_userc outbound
[Device-user-profile-userc] quit
```

(7) 创建本地用户

创建名称为 usera 的本地用户。

```
[Device] local-user usera class network
New local user added.
```

设置用户密码为“a12345”。

```
[Device-luser-network-usera] password simple a12345
```

设置用户接入类型为 lan-access。

```
[Device-luser-network-usera] service-type lan-access
```

设置用户的授权 User Profile 为 usera。

```
[Device-luser-network-usera] authorization-attribute user-profile usera
[Device-luser-network-usera] quit
```

创建名称为 userb 的本地用户。

```
[Device] local-user userb class network
New local user added.
```

设置用户密码为“b12345”。

```
[Device-luser-network-userb] password simple b12345
```
设置用户接入类型为 lan-access。
```
[Device-luser-network-userb] service-type lan-access
```
设置用户的授权 User Profile 为 userb。
```
[Device -luser-network-userb] authorization-attribute user-profile userb
[Device -luser-network-userb] quit
```
创建名称为 userc 的本地用户。
```
[Device] local-user userc class network
New local user added.
```
设置用户密码为“c12345”。
```
[Device-luser-network-userc] password simple c12345
```
设置用户接入类型为 lan-access。
```
[Device-luser-network-userc] service-type lan-access
```
设置用户的授权 User Profile 为 userc。
```
[Device-luser-network-userc] authorization-attribute user-profile userc
[Device-luser-network-userc] quit
```
(8) 配置本地用户的认证/授权/计费方法

配置 ISP 域“user”内的 802.1X 用户的 AAA 方案为本地认证/授权，不计费
```
[Device] domain user
[Device-isp-user] authentication lan-access local
[Device-isp-user] authorization lan-access local
[Device-isp-user] accounting login none
[Device-isp-user] quit
```
(9) 配置 802.1X 功能

开启指定端口 GigabitEthernet1/0/1 的 802.1X 特性。
```
[Device] interface gigabitethernet 1/0/1
[DeviceA-GigabitEthernet1/0/1] dot1x
```
配置基于 MAC 地址的接入控制方式（该配置可选，因为端口的接入控制在缺省情况下就是基于 MAC 地址的）。
```
[Device-GigabitEthernet1/0/1] dot1x port-method macbased
[Device-GigabitEthernet1/0/1] quit
```
开启全局 802.1X 特性。
```
[Device] dot1x
```
4. 验证配置

UserA、UserB、UserC 通过 802.1X 客户端连接网络，输入正确的用户名和密码后（注意用户名需要携带域名后缀，例如 UserA 应该输入用户名“usera@user”和密码“a12345”），认证成功并受到相应的 Qos 策略的限制。

使用 diplay user-profile 命令在 Device 上可以查看到如下配置信息和在线用户信息。
```
<Device> display user-profile
  User-Profile: usera
    Inbound:
      Policy: for_usera

    slot 1:
```

```
    User -:
      Authentication type: 802.1X
      Network attributes:
        Interface    : GigabitEthernet1/0/1
        MAC address  : 6805-ca06-557b
        Service VLAN : 1

User-Profile: userb
  Inbound:
    Policy: for_userb

  slot 1:
    User -:
      Authentication type: 802.1X
      Network attributes:
        Interface    : GigabitEthernet1/0/1
        MAC address  : 80c1-6ee0-2664
        Service VLAN : 1

User-Profile: userc
  Outbound:
    Policy: for_userc

  slot 1:
    User -:
      Authentication type: 802.1X
      Network attributes:
        Interface    : GigabitEthernet1/0/1
        MAC address  : 6805-ca05-3efa
        Service VLAN : 1
```