H3C BRAS 园区网应用配置举例

资料版本：6W102-20210223

产品版本：Release 7951P11

目 录

1 简介

本文介绍了 BRAS（Broadband Remote Access Server，宽带远程接入服务器）特性在校园网应用中的典型配置举例。

在校园网中，常见的需求如下：

(1) 用户数量较大，一般超过 2W 用户。

(2) 同时部署有线和无线业务，都需要认证，有线用户可以选择 PPPoE/IPoE/Portal/802.1X 认证，无线用户采用 IPoE Web/Portal 认证。

(3) 不同身份的用户有不同的网络访问权限，比如教师和学生的访问权限不同。

IPoE Web 认证与 Portal 认证在用户感知上是基本一致的，相比较 Portal 认证，IPoE Web 认证主要有以下优点：

(1) Portal 认证下 IPv4 和 IPv6 是彼此独立的，用户从 IPv4 认证上线后，要使用 IPv6 还需要再次认证；IPoE Web 认证可以做到 IPv4 和 IPv6 一次认证，双栈同时放行。

(2) Portal 认证只能支持用户在同一个接口的 VLAN 间漫游，IPoE Web 认证可以允许用户在所有开启 IPoE Web 的接口间漫游。

(3) Portal 认证只能支持 MAC Trigger 无感知认证，IPoE Web 不仅能支持 MAC Trigger 无感知认证，还可以支持 MAC 无感知认证。

2 配置前提

本文档中的配置均是在实验室环境下进行的配置和验证，配置前设备的所有参数均采用出厂时的缺省配置。如果您已经对设备进行了配置，为了保证配置效果，请确认现有配置和以下举例中的配置不冲突。

本文假设您已了解 PPPoE、IPoE、Portal、QoS、VLAN 终结和 QinQ 等特性。

3 使用限制

本文部分涉及特性仅在 standard 工作模式下支持。有关系统工作模式的介绍，请参见“基础配置指导”中的“设备管理”。

目前仅 SPEX 类单板/CSPEX 类单板（除 CSPEX-1104-E 之外）/CEPC 类单板支持支持配置 PPPoE、IPoE 和 Portal 功能。

仅 SPEX 类单板、CSPEX 类单板（CSPEX-1104-E 除外）、CEPC 类单板支持配置 ITA 功能，ITA 功能仅对 IPoE、Portal 和 PPPoE 用户生效。对于不同接入方式的用户，流量计费级别配置的数量各不相同，如表 3-1 所示。

表3-1 流量计费级别配置数量表

ITA 用户	流量计费级别配置的数量	
	SPEX-1204 单板	CSPEX 类单板（CSPEX-1104-E 除外）和 CEPC 类单板
通过VLAN接口接入的Portal用户	7个	7个
• 通过三层以太网接口/三层以太网子接口/三层聚合接口/三层聚合子接口接入的 Portal 用户 • IPoE 用户 • PPPoE 用户	1个（目前只支持level 1）	4个（目前只支持level 1～level 4）

4 IPv4 Portal 直接认证配置举例

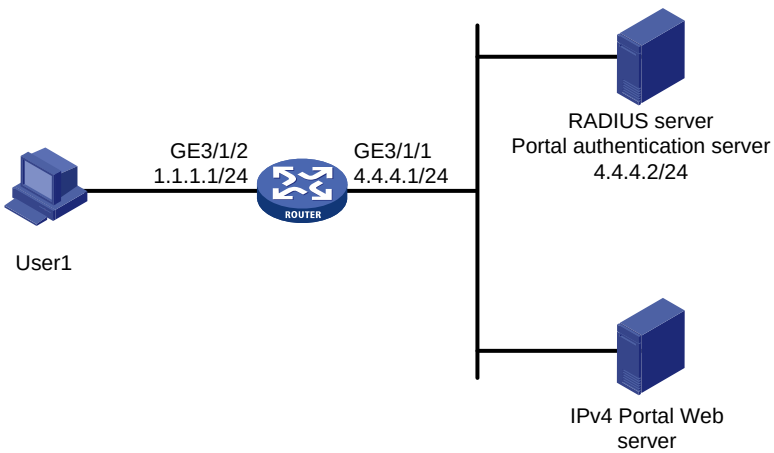
本举例是一个基本的认证举例，有线和无线用户都使用 IPv4 Portal 认证。

4.1 组网需求

如图 4-1 所示，用户主机与接入设备 Router 直接相连，接入设备 Router 与 IPv4 Portal 认证服务器、IPv4 Portal Web 服务器、RADIUS 服务器直接相连，采用直接方式的 Portal 认证。具体需求如下：

- 用户通过 DHCP 获取的公网 IPv4 地址进行认证，在通过 Portal 认证前，只能访问 IPv4 Portal Web 服务器；在通过 Portal 认证后，可以使用此 IPv4 地址访问非受限的互联网资源。
- 在服务器上部署深澜软件实现认证和计费管理。

图4-1 IPv4 Portal 直接认证配置举例



4.2 配置思路

- RADIUS 服务器上需要配置接入设备，并添加各用户名和密码。

- 为了在服务器上部署深澜软件实现认证和计费管理，需要在添加接入设备页面设置 Portal 协议和 Portal 密钥。
- 为了对用户主机访问进行 IPv4 Portal 认证，需要在 BRAS 上配置 Portal 服务器并且使能 Portal 认证。
- 为了实现通过 RADIUS 来对 Portal 用户进行认证/授权和计费，需要在 BRAS 上配置 RADIUS 方案并指定相应的认证/授权服务器和计费服务器，并将其应用于 Portal 用户所属的认证域。
- 为了在 BRAS 和 RADIUS 服务器之间安全地传输用户密码，并且能在 BRAS 上验证 RADIUS 服务器响应报文未被篡改，在 BRAS 和 RADIUS 服务器上都要设置交互报文时所使用的共享密钥（本例共享密钥为 123456）。

4.3 配置注意事项

- IPv4 Portal 应用场景中，如果采用深澜软件作为认证/计费服务器，需要注意的是，服务器上 Portal 协议建议选择 IPv4 和 IPv6 均支持的“H3C V3.0”。
- 为了避免端口号冲突导致服务不可用，需确保内部侦听端口号不是知名协议使用的端口号，且不能被其它基于 TCP 协议的服务占用。已被其他服务占用的 TCP 端口号可以通过 **display tcp** 命令查看。

4.4 配置步骤

4.4.1 配置 RADIUS 服务器和 Portal 服务器


说明

下面以深澜软件 4.10 版本服务器为例，说明 RADIUS 服务器和 Portal 服务器的基本配置。

(1) 在浏览器输入“http://4.4.4.2:8081”，登录服务器添加接入设备。

点击导航栏“设备管理”，选择“添加设备”页签，点击“添加”按钮。

- 设置设备名称为“BRAS”；
- 设置 NAS IP 为“4.4.4.1”；
- 设置我们的 IP 为“4.4.4.2”；
- 选择 NAS 类型为“华为、H3C、深澜网关”；
- 设置 DM 端口为“3799”；
- 设置 RADIUS 密钥为“123456”；
- 选择是否丢弃流量为“不丢弃”；
- 选择 Portal 协议为“H3C V3.0”；
- 设置 Portal 密钥为“123456”。

图4-2 添加接入设备配置页面

设置 RADIUS 信任。点击导航栏“Radius”， 选择“Radius 信任设置”链接进入 RADIUS 信任设置界面，持续点击右上角“生成”按钮直到生成成功。

选择“RADIUS 服务设置”页签选择用户名校验为“带域名”。

(2) 在浏览器输入“https://4.4.4.2:8080”，登录服务器添加用户。

选择“用户管理/添加用户”页签，点击“添加”按钮。添加用户 User1：帐号"User1"，密码“pass”。

4.4.2 配置 IPv4 地址及路由

按照图 4-1 配置各接口的 IPv4 地址，并确保 BRAS 设备和各服务器之间路由可达，具体配置过程略。

4.4.3 配置 BRAS

1. 配置 DHCPv4

配置 DHCPv4 地址池 1，为 1.1.1.0/24 网段的客户端分配 IPv4 地址等参数。

```
[Router]dhcp server ip-pool 1
[Router-dhcp-pool-1] gateway-list 1.1.1.1
[Router-dhcp-pool-1] network 1.1.1.0 mask 255.255.255.0
[Router-dhcp-pool-1] dns-list 8.8.8.8
[Router-dhcp-pool-1] quit
```

2. 配置 RADIUS 方案

创建名称为 rs1 的 RADIUS 方案并进入该方案视图。

```
<Router> system-view
[Router] radius scheme rs1
```

配置 RADIUS 方案的主认证和主计费服务器及其通信密钥。

```
[Router-radius-rs1] primary authentication 4.4.4.2
[Router-radius-rs1] primary accounting 4.4.4.2
[Router-radius-rs1] key authentication simple 123456
```

```
[Router-radius-rs1] key accounting simple 123456
```

配置发送给 RADIUS 服务器的用户名不携带 ISP 域名。

```
[Router-radius-rs1] user-name-format without-domain
[Router-radius-rs1] quit
```

3. 配置认证域

创建并进入名称为 dm1 的 ISP 域。

```
[Router] domain name dm1
```

配置 ISP 域使用的 RADIUS 方案 rs1。

```
[Router-isp-dm1] authentication portal radius-scheme rs1
[Router-isp-dm1] authorization portal radius-scheme rs1
[Router-isp-dm1] accounting portal radius-scheme rs1
[Router-isp-dm1] quit
```

配置系统缺省的 ISP 域 dm1，所有接入用户共用此缺省域的认证和计费方式。若用户登录时输入的用户名未携带 ISP 域名，则使用缺省域下的认证方案。

```
[Router] domain default enable dm1
```

4. 配置 Portal 认证

配置 Portal 认证服务器：名称为 newpt，IP 地址为 4.4.4.2，密钥为明文 portal，监听 Portal 报文的端口为 50100。

```
[Router] portal server newpt
[Router-portal-server-newpt] ip 4.4.4.2 key simple 123456
[Router-portal-server-newpt] port 50100
[Router-portal-server-newpt] quit
```

配置 Portal Web 服务器的 URL 为 http://2.2.2.2/index_9.html。（本处 URL 必须和服务器添加设备后设备表中对应的 Portal 重定向页面内容保持一致）

```
[Sysname] portal Web-server newpt
[Router-portal-Websvr-newpt] url http://2.2.2.2/index_9.html
[Router-portal-Websvr-newpt] quit
```

配置对 HTTPS 报文进行重定向的内部侦听端口号。

```
[Router] http-redirect https-port 8888
```

在接口 GigabitEthernet3/1/2 上开启直接方式的 Portal 认证。

```
[Router] interface GigabitEthernet3/1/2
[Router-GigabitEthernet3/1/2] portal enable method direct
```

在接口 GigabitEthernet3/1/2 上引用 Portal Web 服务器 newpt。

```
[Router-GigabitEthernet3/1/2] portal apply Web-server newpt
```

在接口 GigabitEthernet3/1/2 上设置发送给 Portal 认证服务器的 Portal 报文中的 BAS-IP 属性值为 4.4.4.1。

```
[Router-GigabitEthernet3/1/2] portal bas-ip 4.4.4.1
[Router-GigabitEthernet3/1/2] quit
```

4.5 验证配置

以上配置完成后，通过执行以下显示命令可查看接口 GigabitEthernet3/1/2 的 Portal 配置信息和 Portal 运行状态信息。

```
[Router] display portal interface GigabitEthernet3/1/2
```

```
 Portal information of GigabitEthernet3/1/2
     NAS-ID profile: Not configured
     Authorization : Strict checking
     ACL           : Disabled
     User profile  : Disabled
 IPv4:
     Portal status: Enabled
     Portal authentication method: Direct
     Portal Web server: newpt
     Portal mac-trigger-server: Not configured
     Authentication domain: Not configured
     Pre-auth policy: Not configured
     User-dhcp-only: Disabled
     Pre-auth IP pool: Not configured
     Max Portal users: Not configured
     Bas-ip: 4.4.4.1
     User detection:  Not configured
     Action for server detection:
         Server type    Server name                          Action
         --             --                                   --
     Layer3 source network:
         IP address              Mask

     Destination authenticate subnet:
         IP address              Mask
IPv6:
     Portal status: Disabled
     Portal authentication method: Disabled
     Portal Web server: Not configured
     Portal mac-trigger-server: Not configured
     Authentication domain: Not configured
     Pre-auth policy: Not configured
     User-dhcp-only: Disabled
     Pre-auth IP pool: Not configured
     Max Portal users: Not configured
     Bas-ipv6: Not configured
     User detection: Not configured
     Action for server detection:
         Server type    Server name                          Action
         --             --                                   --
     Layer3 source network:
         IP address                                          Prefix length

     Destination authenticate subnet:
         IP address                                          Prefix length
```

用户 User1 通过 Portal 认证之前，仅能访问 Portal Web 服务器的 Web 认证主页。

图4-3 IPv4 Portal Web 认证主页示意图

用户 User1 输入用户名 User1 和密码 pass，通过 IPv4 Portal 认证，登录成功，可以访问互联网资源。

图4-4 IPv4 Portal 用户登录成功示意图

Portal 用户认证通过后，可通过执行以下显示命令查看 Router 上生成的 Portal 在线用户信息。

```
[Router] display portal user interface GigabitEthernet3/1/2
Total portal users: 1
Username: User1
  Portal server: newpt
  State: Online
  VPN instance: N/A
  MAC                IP                 VLAN    Interface
  0015-e9a6-7cfe     1.1.1.3               --     GigabitEthernet3/1/2
  Authorization information:
    DHCP IP pool: N/A
    User profile: N/A
    Session group profile: N/A
```

```
    ACL number: N/A
    Inbound CAR: N/A
    Outbound CAR: N/A
    Inbound priority: N/A
    Outbound priority: N/A
```

4.6 配置文件

```
#
 dhcp enable
 dhcp server forbidden-ip 1.1.1.2
#
dhcp server ip-pool 1
 gateway-list 1.1.1.1
 network 1.1.1.0 mask 255.255.255.0
 dns-list 8.8.8.8
#
interface GigabitEthernet3/1/2
 port link-mode route
 ip address 1.1.1.1 255.255.255.0
 portal enable method direct
 portal apply Web-server newpt
 portal bas-ip 4.4.4.1
#
radius scheme rs1
 primary authentication 4.4.4.2
 primary accounting 4.4.4.2
 key authentication simple 123456
 key accounting simple 123456
 user-name-format without-domain
#
domain name dm1
 authentication portal radius-scheme rs1
 authorization portal radius-scheme rs1
 accounting portal radius-scheme rs1
#
 domain default enable dm1
#
portal server newpt
 ip 4.4.4.2 key simple 123456
 port 50100
#
portal Web-server newpt
 url http://2.2.2.2/index_9.html
#
```

5 IPv4 IPoE Web 认证配置举例

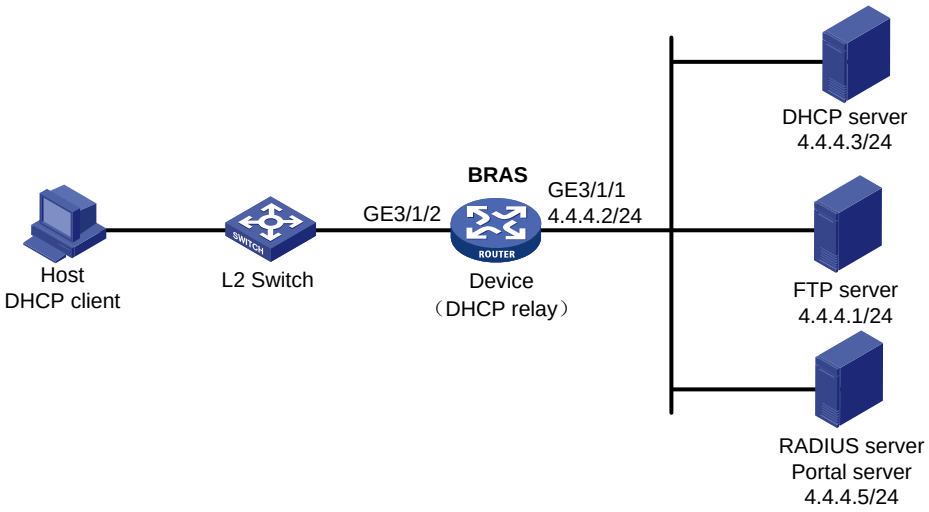
本举例是一个基本的认证举例，有线和无线用户都使用 IPv4 IPoE Web 认证。

5.1 组网需求

如图 5-1 所示：Device 为某学校的一台 BRAS 设备，为学校用户提供 IPoE 接入服务。要求：

- DHCP Client 经由二层网络以 IPoE 方式接入到 BRAS 接入设备。
- BRAS 接入设备作为 DHCP 中继向远端 DHCP 服务器申请 IP 地址。
- 由一台安装了 H3C iMC 的服务器同时承担 RADIUS 服务器、Portal 认证服务器和 Portal Web 服务器的职责。
- FTP server 是一台内网服务器，只有老师可以访问，学生无法访问。
- IPoE Web 认证通过后限速 5Mbps。

图5-1 IPoE 双栈用户普通 Web 认证配置组网图



5.2 配置思路

为了保证用户的带宽需求，本例通过授权 User Profile 进行速率控制。

IPoE Web 认证前域中的流量，区分 HTTP、HTTPS 和普通 IP 报文分别通过不同的队列上送。IPoE Web 认证中针对上送 CPU 的流量，配置如下三种类和流行为组来处理：

- 流分类匹配 HTTP 同时 User Group 为前域标记的，对应的流行为 **redirect http-to-cpu**。
- 流分类匹配 HTTPS 同时 User Group 为前域标记的，对应的流行为 **redirect https-to-cpu**。
- 流分类匹配 IP 同时 User Group 为前域标记的，对应的流行为 **deny**。

5.3 配置注意事项

本配置中 DHCP Server 是由设备进行模拟，实际应用建议使用专门的 DHCP 服务器。

缺省情况下，未配置对 HTTPS 报文进行重定向的内部侦听端口号。需要通过 **http-redirect https-port** 命令用来配置对 HTTPS 报文进行重定向的侦听端口号，并且配置的侦听端口不要跟已有端口冲突。

当 BRAS 接入用户下线时，DHCP 中继需要查询中继用户地址表项，若存在对应表项，则会向 DHCP 服务器发送 Release 报文，通知 DHCP 服务器释放该地址租约。这就需要在 DHCP 中继上使用 **dhcp relay client-information record** 命令开启 DHCP 中继用户地址表项记录功能。

本配置中使用到限速私有属性，有关私有属性的详细介绍，请参见 14 附录。

5.4 配置步骤

5.4.1 配置 IP 地址及路由

按照图 5-1配置各接口的 IP 地址，并确保 BRAS 设备和各服务器之间路由可达，具体配置过程略。

5.4.2 设置 DNS 服务器

请正确设置 DNS 服务器，以便服务器可以根据 IPoE 双栈用户先上线的协议栈类型，解析出 Web 认证页面 http://www.h3c.web.com 对应的 IPv4 URL 地址或 IPv6 URL 地址。DNS 服务器具体设置过程略。

5.4.3 配置 DHCP 服务器

1. 配置 DHCPv4 地址池

开启 DHCP 服务。

```
<DHCP> system-view
[DHCP] dhcp enable
```

创建名称为 pool1 的 DHCPv4 地址池并进入其视图。

```
[DHCP] dhcp server ip-pool pool1
```

配置地址池动态分配的 IP 地址网段 192.168.0.0/24。

```
[DHCP-dhcp-pool-pool1] network 192.168.0.0 24
```

配置为用户分配的网关地址为 192.168.0.1。

```
[DHCP-dhcp-pool-pool1] gateway-list 192.168.0.1
```

将 192.168.0.1 设置为禁止地址。

```
[DHCP-dhcp-pool-pool1] forbidden-ip 192.168.0.1
[DHCP-dhcp-pool-pool1] quit
```

通过配置静态路由，将目的地址为 192.168.0.0 网段的 DHCPv4 应答报文的下一跳指定为连接 DHCPv4 客户端网络的接口 IPv4 地址 4.4.4.2。

```
[DHCP] ip route-static 192.168.0.0 24 4.4.4.2
```

5.4.4 配置 RADIUS 服务器

说明

下面以 iMC（版本为 iMC PLAT 7.3 (E0705P02)）为例，说明 RADIUS 服务器的基本配置。不同 iMC 版本配置可能有所不同，具体配置请以实际版本及对应版本的 iMC 服务器手册为准，本节配置仅供参考。

(1) 配置接入设备

登录进入 iMC 管理平台，选择“用户”页签，单击导航树中的[接入策略管理/接入设备管理/接入设备配置]菜单项，进入接入设备配置页面，在该页面中单击<增加>按钮，进入如图 5-2 所示增加接入设备页面。

- 输入共享密钥为：radius。
- 其他采用缺省配置。

图5-2 增加接入设备

在该页面中设备列表下方单击<手工增加>，在如图 5-3 所示页面输入接入设备地址 4.4.4.2 并单击<确定>。

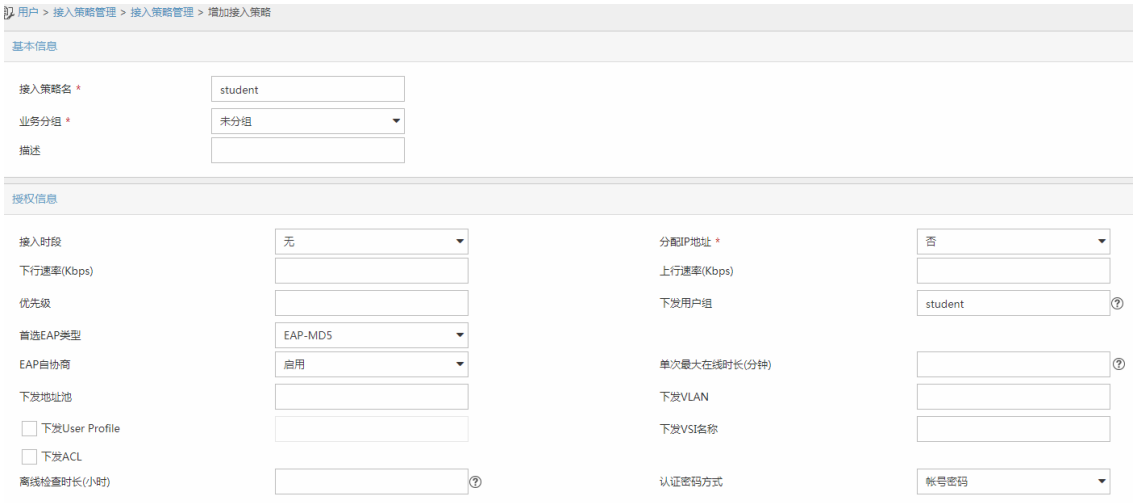
图5-3 手动增加接入设备

(2) 增加接入策略

单击导航树中的[接入策略管理/接入策略管理]菜单项，进入接入策略管理页面，在该页面中单击<增加>按钮，进入如图 5-4 所示增加接入策略页面。

- 输入接入策略名为：student。
- 其他采用缺省配置。

图5-4 增加接入策略



(3) 增加接入服务

单击导航树中的[接入策略管理/接入服务管理]菜单项，进入接入服务管理页面，在该页面中单击<增加>按钮，进入如图 5-5 所示增加接入服务页面。

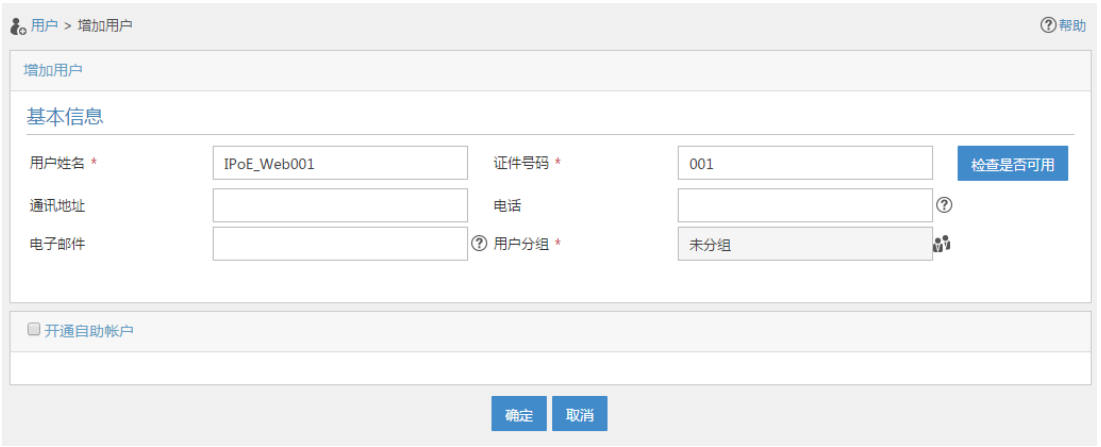
- 输入服务名为：IPoE_Server
- 缺省接入策略选择已创建的策略“AccessPolicy”。
- 其他采用缺省配置。

图5-5 增加接入服务

(4) 在 IMC 界面增加用户

单击导航树中的[用户管理/增加用户]菜单项，进入如图 5-6 所示增加用户页面，填写用户姓名和证件号码为：IPoE_Web001 和 001。

图5-6 增加用户



单击<确定>按钮后完成用户的添加。

(5) 增加接入用户

单击导航树中的[接入用户管理/接入用户]菜单项，进入接入用户页面，在该页面中单击<增加>按钮，进入如图 5-7 所示增加接入用户页面。

- 用户姓名选择：IPoE_Web001
- 账号名填写为：user1
- 密码为：pass1
- 接入服务选择之前已创建的 IPoE_Server

图5-7 增加接入用户

5.4.5 配置 Portal 服务器

说明

下面以 iMC（版本为 iMC PLAT 7.3 (E0705P02)）为例，说明 Portal 服务器的基本配置。不同 iMC 版本配置可能有所不同，具体配置请以实际版本及对应版本的 iMC 服务器手册为准，本节配置仅供参考。

(1) 配置 Portal 主页。

单击导航树中的[接入策略管理/Portal 服务管理/服务器配置]菜单项，进入服务器配置页面，配置 Portal 主页，采用缺省配置即可，并单击<确定>按钮完成操作，如图 5-8 所示。

图5-8 Portal 服务器配置页面

(2) 配置 Portal 认证的地址组范围

单击导航树中的[接入策略管理/Portal 服务管理/IP 地址组配置]菜单项，进入“IP 地址组配置”页面，在该页面中单击<增加>按钮，进入“增加 IP 地址组配置”页面添加 IPv4 地址组，如图 5-9 所示。

- 输入 IP 地址组名为“IPoE_Web_User”；
- 输入起始地址为“192.168.0.1”、终止地址为“192.168.0.255”。用户主机 IP 地址必须包含在该 IP 地址组范围内；
- 其他采用缺省配置；
- 单击<确定>按钮完成操作。

图5-9 增加 IP 地址组配置页面（IPv4）

(3) 增加 Portal 接入设备信息

单击导航树中的[接入策略管理/Portal 服务管理/设备配置]菜单项，进入“设备配置”页面，在该页面中单击<增加>按钮，进入“增加设备信息”页面，如图 5-10 所示。

- 输入设备名为“NAS”；

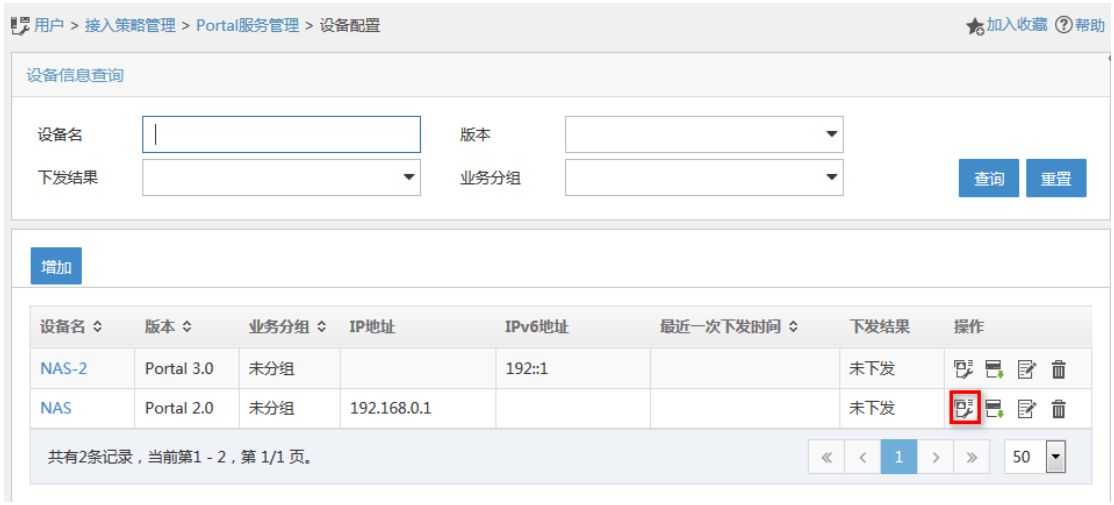
- 输入 IP 地址为“4.4.4.2”，该地址为 Portal 报文出接口 GigabitEthernet3/1/1 的 IP 地址；
- 输入密钥为“123456”；
- 选择组网方式为“直连”；
- 其它参数采用缺省值，并单击<确定>按钮完成操作。

图5-10 增加设备信息配置页面（IPv4）

(4) 配置端口组信息

如图 5-11 所示返回[接入策略管理/Portal 服务管理/设备配置]菜单项，单击<端口组信息管理>按钮，进入“端口组信息配置”页面。

图5-11 设备信息列表



在“端口组信息配置”页面中单击<增加>按钮，进入“增加端口组信息”页面，如图 8-14 所示。

- 输入端口组名为“group”；
- 选择 IP 地址组为“IPoE_Web_User”，用户接入网络时使用的 IP 地址必须属于所选的 IP 地址组；

- 其它参数采用缺省值，并单击<确定>按钮完成操作。

图5-12 增加端口组信息配置页面（IPv4）

5.4.6 配置 BRAS

1. 配置 DHCP 中继

全局开启 DHCP。

```
[BRAS] dhcp enable
```

启用 DHCP 中继的用户地址表项记录功能。

```
[BRAS] dhcp relay client-information record
```

关闭 DHCP 中继动态用户地址表项定时刷新功能。

```
[BRAS] undo dhcp relay client-information refresh enable
```

创建中继地址池 pool1，指定匹配该地址池的 DHCPv4 客户端所在的网段地址，并指定中继地址池对应的 DHCP 服务器地址。

```
[BRAS] dhcp server ip-pool pool1
[BRAS-dhcp-pool-pool1] gateway-list 192.168.0.1 export-route
[BRAS-dhcp-pool-pool1] remote-server 4.4.4.3
[BRAS-dhcp-pool-pool1] quit
```

配置接口工作在 DHCPv4 中继模式。

```
[BRAS] interface gigabitethernet 3/1/2
[BRAS-GigabitEthernet3/1/2] dhcp select relay proxy
```

配置防攻击功能。

```
[BRAS-GigabitEthernet3/1/2] dhcp flood-protection enable
```

2. 配置 Portal 认证服务器

配置 IPv4 Portal 认证服务器：名称为 newpt1，IP 地址为 4.4.4.5，密钥为明文 123456。

```
[BRAS] portal server newpt1
[BRAS-portal-server-newpt1] ip 4.4.4.5 key simple 123456
[BRAS-portal-server-newpt1] quit
```

3. 配置 HTTPS 的内部侦听端口

配置 HTTPS 的内部侦听端口，端口不要跟已有端口冲突即可。

```
[BRAS] http-redirect https-port 11111
```

4. 创建本地用户组

创建认证前域用户组，名称为 Web。

```
[BRAS] user-group Web
New user group added.
[BRAS-ugroup-Web] quit
```

创建学生用户组，名称为 student。

```
[BRAS] user-group student
New user group added.
[BRAS-ugroup-student] quit
```

5. 配置 QoS

(1) 配置用于认证前域用户的 ACL 规则

创建 IPv4 高级 ACL Web_permit 规则如下：匹配用户组 Web 中用户的目的地址为 Portal 服务器地址的报文。

```
[BRAS] acl advanced name Web_permit
[BRAS-acl-ipv4-adv-Web_permit] rule 0 permit ip destination 4.4.4.5 0 user-group Web
[BRAS-acl-ipv4-adv-Web_permit] quit
```

创建 IPv4 高级 ACL neiwang 规则如下：匹配用户组 student 中用户的目的地址为内网服务器地址的报文。

```
[BRAS] acl advanced name neiwang
[BRAS-acl-ipv4-adv-neiwang] rule 0 permit ip destination 4.4.4.1 0 user-group student
[BRAS-acl-ipv4-adv-neiwang] quit
```

创建 IPv4 高级 ACL Web_http 规则如下：匹配用户组 Web 中用户的目的端口为 80 的 TCP 报文(即 HTTP 报文)。

```
[BRAS] acl advanced name Web_http
[BRAS-acl-ipv4-adv-Web_http] rule 0 permit tcp destination-port eq www user-group Web
[BRAS-acl-ipv4-adv-Web_http] quit
```

创建 IPv4 高级 ACL Web_https 规则如下：匹配用户组 Web 中用户的目的端口为 443 的 TCP 报文(即 HTTPS 报文)。

```
[BRAS] acl advanced name Web_https
[BRAS-acl-ipv4-adv-Web_https] rule 0 permit tcp destination-port eq 443 user-group Web
[BRAS-acl-ipv4-adv-Web_https] quit
```

创建 IPv4 高级 ACL ip 规则如下：匹配用户组 Web 中用户的 IP 报文。

```
[BRAS] acl advanced name ip
[BRAS-acl-ipv4-adv-ip] rule 0 permit ip user-group Web
[BRAS-acl-ipv4-adv-ip] quit
```

创建 IPv4 高级 ACL neiwang_out 规则如下：匹配用户组 student 中源地址为内网服务器 IP 地址的报文。

```
[BRAS] acl advanced name neiwang_out
[BRAS-acl-ipv4-adv-neiwang_out] rule 0 permit ip source 4.4.4.1 0 user-group student
[BRAS-acl-ipv4-adv-neiwang_out] quit
```

创建 IPv4 高级 ACL Web_out 规则如下：匹配用户组 Web 中源地址为 Portal 服务器 IP 地址的报文。

```
[BRAS] acl advanced name Web_out
[BRAS-acl-ipv4-adv-Web_out] rule 0 permit ip source 4.4.4.5 0 user-group Web
[BRAS-acl-ipv4-adv-Web_out] quit
```

(2) 配置用于认证前域用户的类

配置类 Web_permit，匹配 ACL Web_permit。

```
[BRAS] traffic classifier Web_permit operator or
[BRAS-classifier-Web_permit] if-match acl name Web_permit
[BRAS-classifier-Web_permit] quit
```

配置类 neiwang，匹配 ACL neiwang。

```
[BRAS] traffic classifier neiwang operator or
[BRAS-classifier-neiwang] if-match acl name neiwang
[BRAS-classifier-neiwang] quit
```

配置类 Web_http，匹配 ACL Web_http。

```
[BRAS] traffic classifier Web_http operator or
[BRAS-classifier-Web_http] if-match acl name Web_http
[BRAS-classifier-Web_http] quit
```

配置类 Web_https，匹配 ACL Web_https。

```
[BRAS] traffic classifier Web_https operator or
[BRAS-classifier-Web_https] if-match acl name Web_https
[BRAS-classifier-Web_https] quit
```

配置类 Web_deny，匹配 ACL ip。

```
[BRAS] traffic classifier Web_deny operator or
[BRAS-classifier-Web_deny] if-match acl name ip
[BRAS-classifier-Web_deny] quit
```

配置类 neiwang_out，匹配 ACL neiwang_out。

```
[BRAS] traffic classifier neiwang_out operator or
[BRAS-classifier-neiwang_out] if-match acl name neiwang_out
[BRAS-classifier-neiwang_out] quit
```

配置类 Web_out，匹配 ACL Web_out。

```
[BRAS] traffic classifier Web_out operator or
[BRAS-classifier-Web_out] if-match acl name Web_out
[BRAS-classifier-Web_out] quit
```

(3) 配置流行为

配置流行为 Web_permit，允许用户组 Web 中用户的目的地址为 Portal 服务器 IP 地址的报文通过。

```
[BRAS] traffic behavior Web_permit
[BRAS-behavior-Web_permit] filter permit
[BRAS-behavior-Web_permit] free account
[BRAS-behavior-Web_permit] quit
```

配置流行为 neiwang，允许用户组 Web 中用户的目的地址为内网服务器 IP 地址的报文通过。

```
[BRAS] traffic behavior neiwang
[BRAS-behavior-neiwang] filter permit
[BRAS-behavior-neiwang] quit
```

配置流行为 Web_http，对用户组 Web 中用户的目的端口为 80 的 TCP 报文(即 HTTP 报文)重定向到 CPU。

```
[BRAS] traffic behavior Web_http
[BRAS-behavior-Web_http] redirect http-to-cpu
[BRAS-behavior-Web_http] quit
```

配置流行为 Web_https，对用户组 Web 中用户的目的端口为 443 的 TCP 报文(即 HTTPS 报文)重定向到 CPU。

```
[BRAS] traffic behavior Web_https
[BRAS-behavior-Web_https] redirect https-to-cpu
[BRAS-behavior-Web_https] quit
```

配置流行为 Web_deny，禁止用户组 Web 中用户的所有 IP 报文通过。

```
[BRAS] traffic behavior Web_deny
[BRAS-behavior-Web_deny] filter deny
[BRAS-behavior-Web_deny] free account
[BRAS-behavior-Web_deny] quit
```

配置流行为 neiwang_out，允许用户组 Web 中源地址为内网服务器 IP 地址的报文通过。

```
[BRAS] traffic behavior neiwang_out
[BRAS-behavior-neiwang_out] filter permit
[BRAS-behavior-neiwang_out] quit
```

配置流行为 Web_out，允许用户组 Web 中源地址为 Portal 服务器 IP 地址的报文通过。

```
[BRAS] traffic behavior Web_out
[BRAS-behavior-Web_out] filter permit
[BRAS-behavior-Web_out] free account
[BRAS-behavior-Web_out] quit
```

(4) 配置 QoS 策略

配置入方向 QoS 策略 Web

```
[BRAS] qos policy Web
```

为类指定对应的流行为，规则为对于用户组 Web 中的用户：

允许目的地址为 Portal 服务器和内网服务器 IP 地址的报文通过；

对于目的端口为 80（HTTP 报文）和 443（HTTPS 报文）的报文重定向到 CPU；

除上述报文外，其余报文均禁止通过。

```
[BRAS-qospolicy-Web] classifier Web_permit behavior Web_permit
[BRAS-qospolicy-Web] classifier neiwang behavior neiwang
[BRAS-qospolicy-Web] classifier Web_http behavior Web_http
[BRAS-qospolicy-Web] classifier Web_https behavior Web_https
[BRAS-qospolicy-Web] classifier Web_deny behavior Web_deny
[BRAS-qospolicy-Web] quit
```

配置出方向 QoS 策略 out

```
[BRAS] qos policy out
```

为类指定对应的流行为，规则为：允许用户组 Web 中源地址为 Portal 服务器和内网服务器 IP 地址的报文通过，其余报文均禁止通过。

```
[BRAS-qospolicy-out] classifier neiwang_out behavior neiwang_out
[BRAS-qospolicy-out] classifier Web_out behavior Web_out
[BRAS-qospolicy-out] classifier Web_deny behavior Web_deny
```

```
[BRAS-qospolicy-out] quit
```

(5) 配置应用策略

对接收的用户流量应用 QoS 策略，策略名为 Web。

```
[BRAS] qos apply policy Web global inbound
```

对发送的上线用户流量应用 QoS 策略，策略名为 out。

```
[BRAS] qos apply policy out global outbound
```

(6) 查看应用的策略是否生效

查看入方向 QoS 策略的配置信息和运行情况。

```
[BRAS] display qos policy global slot 3 inbound
  Direction: Inbound
  Policy: Web
   Classifier: Web_permit
     Operator: OR
     Rule(s) :
      If-match acl name Web_permit
     Behavior: Web_permit
      Filter enable: Permit
      Free account enable
   Classifier: neiwang
     Operator: OR
     Rule(s) :
      If-match acl name neiwang
     Behavior: neiwang
      Filter enable: permit
   Classifier: Web_http
     Operator: OR
     Rule(s) :
      If-match acl name Web_http
     Behavior: Web_http
      Redirecting:
        Redirect http to CPU
   Classifier: Web_https
     Operator: OR
     Rule(s) :
      If-match acl name Web_https
     Behavior: Web_https
      Redirecting:
        Redirect https to CPU
   Classifier: Web_deny
     Operator: OR
     Rule(s) :
      If-match acl name ip
     Behavior: Web_deny
      Filter enable: Deny
      Free account enable
```

查看出方向 QoS 策略的配置信息和运行情况。

```
[BRAS] display qos policy global slot 3 outbound
```

```
Direction: Outbound
Policy: out
 Classifier: neiwang_out
   Operator: OR
   Rule(s) :
    If-match acl name neiwang_out
   Behavior: neiwang_out
    Filter enable: permit
 Classifier: Web_out
   Operator: OR
   Rule(s) :
    If-match acl name Web_out
   Behavior: Web_out
    Filter enable: Permit
    Free account enable
 Classifier: Web_deny
   Operator: OR
   Rule(s) :
    If-match acl name ip
   Behavior: Web_deny
    Filter enable: Deny
    Free account enable
```

6. 配置 RADIUS 方案

创建名称为 rs1 的 RADIUS 方案并进入该方案视图。

```
[BRAS] radius scheme rs1
```

配置 RADIUS 方案的主认证和主计费服务器及其通信密钥。

```
[BRAS-radius-rs1] primary authentication 4.4.4.5
[BRAS-radius-rs1] primary accounting 4.4.4.5
[BRAS-radius-rs1] key authentication simple radius
[BRAS-radius-rs1] key accounting simple radius
```

配置发送给 RADIUS 服务器的用户名不携带 ISP 域名。

```
[BRAS-radius-rs1] user-name-format without-domain
[BRAS-radius-rs1] quit
```

设置 RADIUS DAE 客户端的 IP 地址为 4.4.4.5，与 RADIUS DAE 客户端交互 DAE 报文时使用的共享密钥为明文 radius，需要注意的是认证两端明文密钥需要一致。

```
[BRAS] radius session-control enable
[BRAS] radius dynamic-author server
[BRAS-radius-da-server] client ip 4.4.4.5 key simple radius
[BRAS-radius-da-server] quit
```

7. 配置 User Profile

配置名称为 car 的 User Profile 对上线用户发送和接收的报文进行流量监管。报文正常流速为 5210kbps，允许 325625byte 的突发流量通过，速率小于等于 5210kbps 时正常发送，大于 5210kbps 时，报文被丢弃。

```
[BRAS] user-profile car
[BRAS-user-profile-car] qos car inbound any cir 5210 cbs 325625
[BRAS-user-profile-car] qos car outbound any cir 5210 cbs 325625
```

```
[BRAS-user-profile-car] quit
```

8. 配置认证前域和 Web 认证域

配置 IPoE 用户认证前使用的认证域。

```
[BRAS] domain name dm1
[BRAS-isp-dm1] authentication ipoe none
[BRAS-isp-dm1] authorization ipoe none
[BRAS-isp-dm1] accounting ipoe none
```

配置前域授权用户组和地址池。

```
[BRAS-isp-dm1] authorization-attribute user-group Web
[BRAS-isp-dm1] authorization-attribute ip-pool pool1
```

配置 Web 认证页面 URL。

```
[BRAS-isp-dm1] Web-server url http://www.h3c.web.com
[BRAS-isp-dm1] quit
```

配置 IPoE 用户在 Web 认证阶段使用的认证域。

```
[BRAS] domain name dm2
[BRAS-isp-dm2] authentication ipoe radius-scheme rs1
[BRAS-isp-dm2] authorization ipoe radius-scheme rs1
[BRAS-isp-dm2] accounting ipoe radius-scheme rs1
[BRAS-isp-dm2] authorization-attribute user-profile car
[BRAS-isp-dm2] quit
```

9. 配置 IPoE

开启 IPoE 功能，并配置二层接入模式。

```
[BRAS] interface gigabitethernet 3/1/2
[BRAS-GigabitEthernet3/1/2] ip subscriber l2-connected enable
```

配置 IPoE 用户采用 Web 认证方式。

```
[BRAS-GigabitEthernet3/1/2] ip subscriber authentication-method Web
The operation may cut all users on this interface. Continue?[Y/N]:y
```

配置 Web 认证前域为 dm1，Web 认证域为 dm2。

```
[BRAS-GigabitEthernet3/1/2] ip subscriber pre-auth domain dm1
[BRAS-GigabitEthernet3/1/2] ip subscriber Web-auth domain dm2
[BRAS-GigabitEthernet3/1/2] quit
```

5.4.7 验证配置

用户认证前域认证通过之后，可以使用以下的显示命令查看 IPoE 用户在线信息，其中，用户获得的 IPv4 地址为 192.168.0.2。student 身份用户上线后，无法访问 4.4.4.1 的 FTP 服务器。

```
[BRAS] display ip subscriber session verbose
Basic:
  Description                 : -
  Username                    : 001b21a80949
  Domain                      : dm1
  VPN instance                : N/A
  IP address                  : 192.168.0.2
  User address type           : N/A
  MAC address                 : 001b-21a8-0949
```

```
  Service-VLAN/Customer-VLAN  : -/-
  Access interface            : GE3/1/2
  User ID                     : 0x30000004
  VPI/VCI(for ATM)            : -/-
  VSI Index                   : -
  VSI link ID                 : -
  VXLAN ID                    : -
  DNS servers                 : N/A
  IPv6 DNS servers            : N/A
  DHCP lease                  : 86400 sec
  DHCP remain lease           : 86383 sec
  DHCPv6 lease                : N/A
  DHCPv6 remain lease         : N/A
  Access time                 : May 27 00:48:51 2018
  Online time(hh:mm:ss)       : 00:00:19
  Service node                : Slot 3 CPU 0
  Authentication type         : Web pre-auth
  IPv4 access type            : DHCP
  IPv4 detect state           : Detecting
  State                       : Online

AAA:
  ITA policy name             : N/A
  IP pool                     : pool1
  IPv6 pool                   : N/A
  IPv6 nd preifx pool         : N/A
  Primary DNS server          : N/A
  Secondary DNS server        : N/A
  Primary IPv6 DNS server     : N/A
  Secondary IPv6 DNS server   : N/A
  Session idle cut            : N/A
  Session duration            : N/A, remaining: N/A
  Traffic quota               : N/A
  Traffic remained            : N/A
  Acct start-fail action      : Online
  Acct update-fail action     : Online
  Acct quota-out action       : Offline
  Dual-stack accounting mode  : Merge
  Max IPv4 multicast addresses: 4
  IPv4 multicast address list : N/A
  Max IPv6 multicast addresses: 4
  IPv6 multicast address list : N/A
  Accounting start time       : May 27 00:48:51 2018
  Redirect URL                : http://www.h3c.web.com
  Subscriber ID               : -

QoS:
  User profile                : N/A
```

```
  Session group profile       : N/A
  User group ACL              : Web (active)
  Inbound CAR                 : N/A
  Outbound CAR                : N/A
  Inbound user priority       : N/A
  Outbound user priority      : N/A

Flow statistic:
  Uplink   packets/bytes      : 0/0
  Downlink packets/bytes      : 0/0
  IPv6 uplink   packets/bytes : 0/0
  IPv6 downlink packets/bytes : 0/0
```

用户认证前域认证通过之后，登录 Web 页面，如图 8-16 所示。

图5-13 登录 Web 页面

在认证页面输入用户名和密码单击<上线>按钮进行 Web 认证，可以使用以下的显示命令查看 IPoE 用户在线信息。

```
[BRAS] display ip subscriber session verbose
Basic:
  Description                 : -
  Username                    : user1@dm2
  Domain                      : dm2
  VPN instance                : N/A
  IP address                  : 192.168.0.2
  User address type           : N/A
  MAC address                 : 001b-21a8-0949
  Service-VLAN/Customer-VLAN  : -/-
  Access interface            : GE3/1/2
  User ID                     : 0x30000004
```

```
  VPI/VCI(for ATM)            : -/-
  VSI Index                   : -
  VSI link ID                 : -
  VXLAN ID                    : -
  DNS servers                 : N/A
  IPv6 DNS servers            : N/A
  DHCP lease                  : 86400 sec
  DHCP remain lease           : 86356 sec
  DHCPv6 lease                : N/A
  DHCPv6 remain lease         : N/A
  Access time                 : May 27 00:48:51 2018
  Online time(hh:mm:ss)       : 00:00:04
  Service node                : Slot 3 CPU 0
  Authentication type         : Web
  IPv4 access type            : DHCP
  IPv4 detect state           : Detecting
  State                       : Online

AAA:
  ITA policy name             : N/A
  IP pool                     : pool1
  IPv6 pool                   : N/A
  IPv6 nd preifx pool         : N/A
  Primary DNS server          : N/A
  Secondary DNS server        : N/A
  Primary IPv6 DNS server     : N/A
  Secondary IPv6 DNS server   : N/A
  Session idle cut            : N/A
  Session duration            : 86400 sec, remaining: 86395 sec
  Traffic quota               : N/A
  Traffic remained            : N/A
  Acct start-fail action      : Online
  Acct update-fail action     : Online
  Acct quota-out action       : Offline
  Dual-stack accounting mode  : Merge
  Max IPv4 multicast addresses: 4
  IPv4 multicast address list : N/A
  Max IPv6 multicast addresses: 4
  IPv6 multicast address list : N/A
  Accounting start time       : May 27 00:49:32 2018
  Subscriber ID               : -

QoS:
  User profile                : car (active)
  Session group profile       : N/A
  User group ACL              : student (active)
  Inbound CAR                 : N/A
  Outbound CAR                : N/A
```

```
  Inbound user priority       : N/A
  Outbound user priority      : N/A

Flow statistic:
  Uplink   packets/bytes      : 0/0
  Downlink packets/bytes      : 0/0
  IPv6 uplink   packets/bytes : 0/0
  IPv6 downlink packets/bytes : 0/0
```

5.4.8 配置文件

- DHCP 服务器：

```
#
 dhcp enable
#
dhcp server ip-pool pool1
 gateway-list 192.168.0.1
 network 192.168.0.0 mask 255.255.255.0
 forbidden-ip 192.168.0.1
#
interface GigabitEthernet3/1/1
 port link-mode route
 ip address 4.4.4.3 255.255.255.0
#
 ip route-static 192.168.0.0 24 4.4.4.2
#
```

- Router A（BRAS）：

```
#
 dhcp enable
 dhcp relay client-information record
 undo dhcp relay client-information refresh enable
#
traffic classifier neiwang operator or
 if-match acl name neiwang
#
traffic classifier neiwang_out operator or
 if-match acl name neiwang_out
#
traffic classifier Web_deny operator or
 if-match acl name ip
#
traffic classifier Web_http operator or
 if-match acl name Web_http
#
traffic classifier Web_https operator or
 if-match acl name Web_https
#
traffic classifier Web_out operator or
```

```
 if-match acl name Web_out
#
traffic classifier Web_permit operator or
 if-match acl name Web_permit
#
traffic behavior neiwang
 filter permit
#
traffic behavior neiwang_out
 filter permit
#
traffic behavior Web_deny
 filter deny
 free account
#
traffic behavior Web_http
 redirect http-to-cpu
#
traffic behavior Web_https
 redirect https-to-cpu
#
traffic behavior Web_out
 filter permit
 free account
#
traffic behavior Web_permit
 filter permit
 free account
#
qos policy out
 classifier Web_out behavior Web_out
 classifier neiwang_out behavior neiwang_out
 classifier Web_deny behavior Web_deny
#
qos policy Web
 classifier Web_permit behavior Web_permit
 classifier neiwang behavior neiwang
 classifier Web_http behavior Web_http
 classifier Web_https behavior Web_https
 classifier Web_deny behavior Web_deny
#
interface GigabitEthernet3/1/1
 ip address 4.4.4.2 255.255.255.0
#
interface GigabitEthernet3/1/2
 port link-mode route
 dhcp select relay proxy
 dhcp flood-protection enable
```

```
 ip subscriber l2-connected enable
 ip subscriber authentication-method Web
 ip subscriber pre-auth domain dm1
 ip subscriber Web-auth domain dm2
#
 qos apply policy Web global inbound
 qos apply policy out global outbound
#
dhcp server ip-pool pool1
 gateway-list 192.168.0.1 export-route
 remote-server 4.4.4.3
#
acl advanced name ip
 rule 0 permit ip user-group Web
#
acl advanced name neiwang
 rule 0 permit ip destination 4.4.4.1 0 user-group student
#
acl advanced name neiwang_out
 rule 0 permit ip source 4.4.4.1 0 user-group student
#
acl advanced name Web_http
 rule 0 permit tcp destination-port eq www user-group Web
#
acl advanced name Web_https
 rule 0 permit tcp destination-port eq 443 user-group Web
#
acl advanced name Web_out
 rule 0 permit ip source 4.4.4.5 0 user-group Web
#
acl advanced name Web_permit
 rule 0 permit ip destination 4.4.4.5 0 user-group Web
#
user-profile car
 qos car inbound any cir 5210 cbs 325625 ebs 0
 qos car outbound any cir 5210 cbs 325625 ebs 0
#
radius scheme rs1
 primary authentication 4.4.4.5
 primary accounting 4.4.4.5
 key authentication cipher $c$3$FhQVcgn3kq1exL0CdTzatcgc9xF9vL3ZOw==
 key accounting cipher $c$3$ntIHBRM4ZkG+2JRZQTdKmNl0kYJmhZz5Zg==
 user-name-format without-domain
#
radius dynamic-author server
 client ip 4.4.4.5 key cipher $c$3$lYC2ERe8ts2gtE6M2xfoDDB8NmGw6J9v/Q==
#
domain name dm1
```

```
 authorization-attribute user-group Web
 authorization-attribute ip-pool pool1
 authentication ipoe none
 authorization ipoe none
 accounting ipoe none
 Web-server url http://www.h3c.web.com
#
domain name dm2
 authorization-attribute user-profile car
 authentication ipoe radius-scheme rs1
 authorization ipoe radius-scheme rs1
 accounting ipoe radius-scheme rs1
#
user-group Web
#
user-group student
#
portal server newpt1
 ip 4.4.4.5 key cipher $c$3$UnoFeLybwld9jDwLnHJQptDE7YZry2EVlw==
#
 http-redirect https-port 11111
```

6 IPoE Web 双栈用户 MAC 无感知认证配置举例(IPv6 不认证方式)

在网络向 IPv6 演进的过程中，由于一段时间内，各种网络资源还没有全面支持 IPv6，因此需要以 IPv4/IPv6 双协议栈运行。

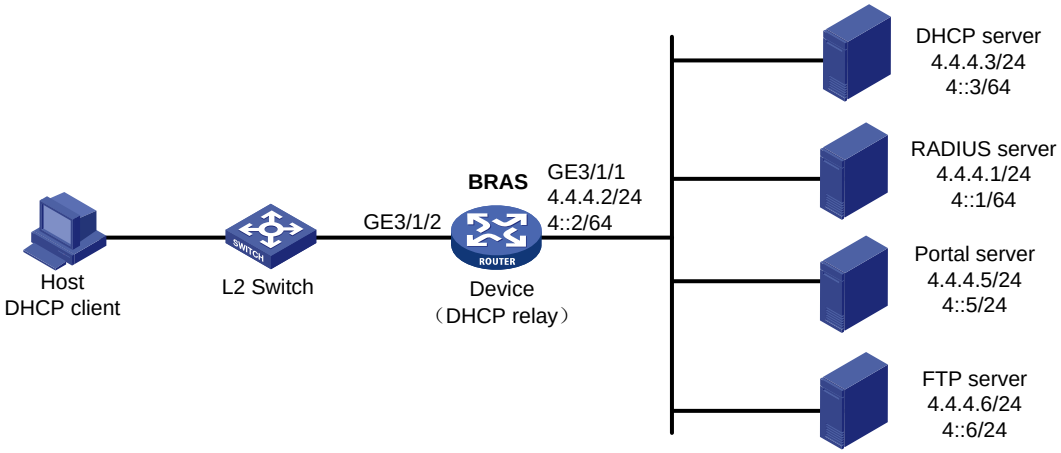
本举例描述一个对 IPv6 使用比较初级的场景，部署时只有 IPv4 使用认证，IPv6 不认证，直接使用网络资源。

6.1 组网需求

如图 6-1 所示：Device 为某学校的一台 BRAS 设备，为学校用户提供 IPoE 接入服务。要求：

- DHCP Client 经由二层网络以 IPoE 方式接入到 BRAS 接入设备。
- BRAS 接入设备作为 DHCP 中继向远端 DHCP 服务器申请 IP 地址。
- 由一台安装了 H3C iMC 的服务器同时承担 Portal 认证服务器和 Portal Web 服务器的职责。
- 由一台支持 MAC 绑定功能的 RADIUS 服务器同时承担认证、授权和计费服务器以及 MAC 绑定服务器的职责。
- FTP server 是一台内网服务器。
- IPoE Web 认证通过后限速 5Mbps。

图6-1 IPoE 双栈用户 MAC 无感知认证配置组网图



6.2 配置思路

为了保证用户的带宽需求，本例通过授权 User Profile 进行速率控制。

IPoE Web 认证前域中的流量，区分 HTTP、HTTPS 和普通 IP 报文分别通过不同的队列上送。IPoE Web 认证中针对上送 CPU 的流量，配置如下三种类和流行为组来处理：

- 流分类匹配 HTTP 同时 User Group 为前域标记的，对应的流行为 **redirect http-to-cpu**。
- 流分类匹配 HTTPS 同时 User Group 为前域标记的，对应的流行为 **redirect https-to-cpu**。
- 流分类匹配 IP 同时 User Group 为前域标记的，对应的流行为 **redirect cpu**。

当 BRAS 接入用户下线时，DHCP 中继需要查询中继用户地址表项，若存在对应表项，则会向 DHCP 服务器发送 Release 报文，通知 DHCP 服务器释放该地址租约。这就需要在 DHCP 中继上使用 **dhcp relay client-information record** 命令开启 DHCP 中继用户地址表项记录功能。

6.3 配置注意事项

本配置中 DHCP Server 是由设备进行模拟，实际应用建议使用专门的 DHCP 服务器。

缺省情况下，未配置对 HTTPS 报文进行重定向的内部侦听端口号。需要通过 **http-redirect https-port** 命令用来配置对 HTTPS 报文进行重定向的侦听端口号，并且配置的侦听端口不要跟已有端口冲突。

本配置使用 NDRA 方式为终端分配 IPv6 地址，但 IPv6 业务不做认证，直接访问网络。

本配置中使用到限速私有属性，有关私有属性的详细介绍，请参见 14 附录。

6.4 配置步骤

6.4.1 配置 IP 地址及路由

按照图 6-1配置各接口的 IP 地址，并确保 BRAS 设备和各服务器之间路由可达，具体配置过程略。

6.4.2 设置 DNS 服务器

请正确设置 DNS 服务器，以便服务器可以根据 IPoE 双栈用户先上线的协议栈类型，解析出 Web 认证页面 http://www.h3c.web.com 对应的 IPv4 URL 地址或 IPv6 URL 地址。DNS 服务器具体设置过程略。

6.4.3 配置 DHCP 服务器

1. 配置 DHCPv4 地址池

开启 DHCP 服务。

```
<DHCP> system-view
[DHCP] dhcp enable
```

创建名称为 pool1 的 DHCPv4 地址池并进入其视图。

```
[DHCP] dhcp server ip-pool pool1
```

配置地址池动态分配的 IP 地址网段 192.168.0.0/24。

```
[DHCP-dhcp-pool-pool1] network 192.168.0.0 24
```

配置为用户分配的网关地址为 192.168.0.1。

```
[DHCP-dhcp-pool-pool1] gateway-list 192.168.0.1
```

将 192.168.0.1 设置为禁止地址。

```
[DHCP-dhcp-pool-pool1] forbidden-ip 192.168.0.1
[DHCP-dhcp-pool-pool1] quit
```

通过配置静态路由，将目的地址为 192.168.0.0 网段的 DHCPv4 应答报文的下一跳指定为连接 DHCPv4 客户端网络的接口 IPv4 地址 4.4.4.2。

```
[DHCP] ip route-static 192.168.0.0 24 4.4.4.2
```

6.4.4 配置 RADIUS 服务器

对于 RADIUS 服务器上 AAA 和 MAC 绑定配置，具体需要参见 RADIUS server 的配置说明书。

6.4.5 配置 Portal 服务器

说明

下面以 iMC（版本为 iMC PLAT 7.3 (E0705P02)）为例，说明 Portal 服务器的基本配置。不同 iMC 版本配置可能有所不同，具体配置请以实际版本及对应版本的 iMC 服务器手册为准，本节配置仅供参考。

(1) 配置 Portal 主页。

单击导航树中的[接入策略管理/Portal 服务管理/服务器配置]菜单项，进入服务器配置页面，配置 Portal 主页，采用缺省配置即可，并单击<确定>按钮完成操作，如图 6-2 所示。

图6-2 Portal 服务器配置页面

(2) 配置 Portal 认证的地址组范围

单击导航树中的[接入策略管理/Portal 服务管理/IP 地址组配置]菜单项，进入“IP 地址组配置”页面，在该页面中单击<增加>按钮，进入“增加 IP 地址组配置”页面，如图 6-3 所示。

- 输入 IP 地址组名为“IPoE_Web_User”；
- 输入起始地址为“192.168.0.1”、终止地址为“192.168.0.255”。用户主机 IP 地址必须包含在该 IP 地址组范围内；
- 其他采用缺省配置；
- 单击<确定>按钮完成操作。

图6-3 增加 IP 地址组配置页面

(3) 增加 Portal 接入设备信息

单击导航树中的[接入策略管理/Portal 服务管理/设备配置]菜单项，进入“设备配置”页面，在该页面中单击<增加>按钮，进入“增加设备信息”页面，如图 6-4 所示。

- 输入设备名为“NAS”；

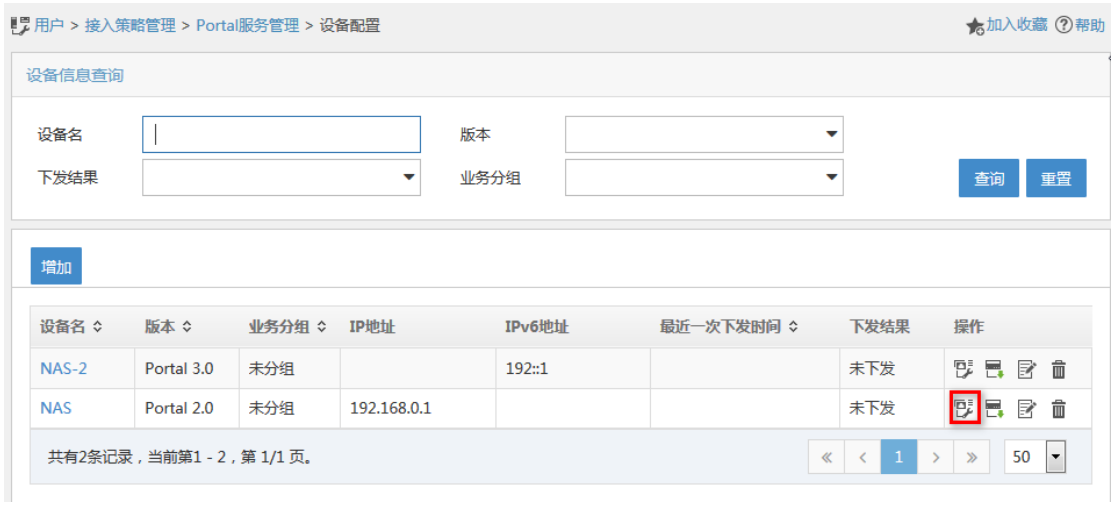
- 输入 IP 地址为“4.4.4.2”，该地址为 Portal 报文出接口 GigabitEthernet3/1/1 的 IP 地址；
- 输入密钥为“123456”；
- 选择组网方式为“直连”；
- 其它参数采用缺省值，并单击<确定>按钮完成操作。

图6-4 增加设备信息配置页面

(4) 配置端口组信息

如图 6-5 所示返回[接入策略管理/Portal 服务管理/设备配置]菜单项，单击<端口组信息管理>按钮，进入“端口组信息配置”页面。

图6-5 设备信息列表



在“端口组信息配置”页面中单击<增加>按钮，进入“增加端口组信息”页面，如图 6-6 所示。

- 输入端口组名为“group”；
- 选择 IP 地址组为“IPoE_Web_User”，用户接入网络时使用的 IP 地址必须属于所选的 IP 地址组；

- 其它参数采用缺省值，并单击<确定>按钮完成操作。

图6-6 增加端口组信息配置页面

最后单击导航树中的[接入策略管理/业务参数配置/系统配置手工生效]菜单项，使以上Portal 认证服务器配置生效。

6.4.6 配置 BRAS

1. 配置 DHCP 中继

全局开启 DHCP。

```
[BRAS] dhcp enable
```

启用 DHCP 中继的用户地址表项记录功能。

```
[BRAS] dhcp relay client-information record
```

关闭 DHCP 中继动态用户地址表项定时刷新功能。

```
[BRAS] undo dhcp relay client-information refresh enable
```

创建中继地址池 pool1，指定匹配该地址池的 DHCPv4 客户端所在的网段地址，并指定中继地址池对应的 DHCP 服务器地址。

```
[BRAS] dhcp server ip-pool pool1
[BRAS-dhcp-pool-pool1] gateway-list 192.168.0.1 export-route
[BRAS-dhcp-pool-pool1] remote-server 4.4.4.3
[BRAS-dhcp-pool-pool1] quit
```

配置接口工作在 DHCPv4 中继模式。

```
[BRAS] interface gigabitethernet 3/1/2
[BRAS-GigabitEthernet3/1/2] dhcp select relay proxy
[BRAS-GigabitEthernet3/1/2] dhcp flood-protection enable
```

配置漫游时重新分配地址功能。

```
[BRAS-GigabitEthernet3/1/2] dhcp session-mismatch action fast-renew
```

配置 IPv6 地址。

```
[BRAS-GigabitEthernet3/1/2] ipv6 address 192::1 64
```

取消设备发布 RA 消息的抑制。

```
[BRAS-GigabitEthernet3/1/2] undo ipv6 nd ra halt
```

2. 配置 Portal 认证服务器

配置 IPv4 Portal 认证服务器：名称为 newpt1，IP 地址为 4.4.4.5，密钥为明文 123456。

```
[BRAS] portal server newpt1
[BRAS-portal-server-newpt1] ip 4.4.4.5 key simple 123456
[BRAS-portal-server-newpt1] quit
```

3. 配置 HTTPS 的内部侦听端口

配置 HTTPS 的内部侦听端口，端口不要跟已有端口冲突即可。

```
[BRAS] http-redirect https-port 11111
```

4. 创建本地用户组

创建认证前域用户组，名称为 Web。

```
[BRAS] user-group Web
New user group added.
[BRAS-ugroup-Web] quit
```

5. 配置 QoS

(1)　配置用于认证前域用户的 ACL 规则

创建 IPv4 高级 ACL Web_permit 规则如下：匹配用户组 Web 中用户的目的地址为 Portal 服务器地址的报文。

```
[BRAS] acl advanced name Web_permit
[BRAS-acl-ipv4-adv-Web_permit] rule 0 permit ip destination 4.4.4.5 0 user-group Web
[BRAS-acl-ipv4-adv-Web_permit] quit
```

创建 IPv4 高级 ACL neiwang 规则如下：匹配用户组 Web 中用户的目的地址为内网服务器地址的报文。

```
[BRAS] acl advanced name neiwang
[BRAS-acl-ipv4-adv-neiwang] rule 0 permit ip destination 4.4.4.1 0 user-group Web
[BRAS-acl-ipv4-adv-neiwang] quit
```

创建 IPv4 高级 ACL Web_http 规则如下：匹配用户组 Web 中用户的目的端口为 80 的 TCP 报文(即 HTTP 报文)。

```
[BRAS] acl advanced name Web_http
[BRAS-acl-ipv4-adv-Web_http] rule 0 permit tcp destination-port eq www user-group Web
[BRAS-acl-ipv4-adv-Web_http] quit
```

创建 IPv4 高级 ACL Web_https 规则如下：匹配用户组 Web 中用户的目的端口为 443 的 TCP 报文(即 HTTPS 报文)。

```
[BRAS] acl advanced name Web_https
[BRAS-acl-ipv4-adv-Web_https] rule 0 permit tcp destination-port eq 443 user-group Web
[BRAS-acl-ipv4-adv-Web_https] quit
```

创建 IPv4 高级 ACL ip 规则如下：匹配用户组 Web 中用户的 IP 报文。

```
[BRAS] acl advanced name ip
[BRAS-acl-ipv4-adv-ip] rule 0 permit ip user-group Web
[BRAS-acl-ipv4-adv-ip] quit
```

创建 IPv4 高级 ACL neiwang_out 规则如下：匹配用户组 Web 中源地址为内网服务器 IP 地址的报文。

```
[BRAS] acl advanced name neiwang_out
[BRAS-acl-ipv4-adv-neiwang_out] rule 0 permit ip source 4.4.4.1 0 user-group Web
```

```
[BRAS-acl-ipv4-adv-neiwang_out] quit
```

创建 IPv4 高级 ACL Web_out 规则如下：匹配用户组 Web 中源地址为 Portal 服务器 IP 地址的报文。

```
[BRAS] acl advanced name Web_out
[BRAS-acl-ipv4-adv-Web_out] rule 0 permit ip source 4.4.4.5 0 user-group Web
[BRAS-acl-ipv4-adv-Web_out] quit
```

(2) 配置用于认证前域用户的类

配置类 Web_permit，匹配 ACL Web_permit。

```
[BRAS] traffic classifier Web_permit operator or
[BRAS-classifier-Web_permit] if-match acl name Web_permit
[BRAS-classifier-Web_permit] quit
```

配置类 neiwang，匹配 ACL neiwang。

```
[BRAS] traffic classifier neiwang operator or
[BRAS-classifier-neiwang] if-match acl name neiwang
[BRAS-classifier-neiwang] quit
```

配置类 Web_http，匹配 ACL Web_http。

```
[BRAS] traffic classifier Web_http operator or
[BRAS-classifier-Web_http] if-match acl name Web_http
[BRAS-classifier-Web_http] quit
```

配置类 Web_https，匹配 ACL Web_https。

```
[BRAS] traffic classifier Web_https operator or
[BRAS-classifier-Web_https] if-match acl name Web_https
[BRAS-classifier-Web_https] quit
```

配置类 ip_cpu，匹配 ACL ip。

```
[BRAS] traffic classifier ip_cpu operator or
[BRAS-classifier-ip_cpu] if-match acl name ip
[BRAS-classifier-ip_cpu] quit
```

配置类 Web_deny，匹配 ACL ip。

```
[BRAS] traffic classifier Web_deny operator or
[BRAS-classifier-Web_deny] if-match acl name ip
[BRAS-classifier-Web_deny] quit
```

配置类 neiwang_out，匹配 ACL neiwang_out。

```
[BRAS] traffic classifier neiwang_out operator or
[BRAS-classifier-neiwang_out] if-match acl name neiwang_out
[BRAS-classifier-neiwang_out] quit
```

配置类 Web_out，匹配 ACL Web_out。

```
[BRAS] traffic classifier Web_out operator or
[BRAS-classifier-Web_out] if-match acl name Web_out
[BRAS-classifier-Web_out] quit
```

(3) 配置流行为

配置流行为 Web_permit，允许用户组 Web 中用户的目的地址为 Portal 服务器 IP 地址的报文通过。

```
[BRAS] traffic behavior Web_permit
[BRAS-behavior-Web_permit] filter permit
[BRAS-behavior-Web_permit] free account
```

```
[BRAS-behavior-Web_permit] quit
```

配置流行为 neiwang，允许用户组 Web 中用户的目的地址为内网服务器 IP 地址的报文通过。

```
[BRAS] traffic behavior neiwang
[BRAS-behavior-neiwang] filter permit
[BRAS-behavior-neiwang] quit
```

配置流行为 Web_http，对用户组 Web 中用户的目的端口为 80 的 TCP 报文(即 HTTP 报文)重定向到 CPU。

```
[BRAS] traffic behavior Web_http
[BRAS-behavior-Web_http] redirect http-to-cpu
[BRAS-behavior-Web_http] quit
```

配置流行为 Web_https，对用户组 Web 中用户的目的端口为 443 的 TCP 报文(即 HTTPS 报文)重定向到 CPU。

```
[BRAS] traffic behavior Web_https
[BRAS-behavior-Web_https] redirect https-to-cpu
[BRAS-behavior-Web_https] quit
```

配置流行为 Web_cpu，对用户组 Web 中用户的所有 IP 报文都重定向到 CPU。

```
[BRAS] traffic behavior Web_cpu
[BRAS-behavior-Web_cpu] redirect cpu
[BRAS-behavior-Web_cpu] quit
```

配置流行为 Web_deny，禁止用户组 Web 中用户的所有 IP 报文通过。

```
[BRAS] traffic behavior Web_deny
[BRAS-behavior-Web_deny] filter deny
[BRAS-behavior-Web_deny] free account
[BRAS-behavior-Web_deny] quit
```

配置流行为 neiwang_out，允许用户组 Web 中源地址为内网服务器 IP 地址的报文通过。

```
[BRAS] traffic behavior neiwang_out
[BRAS-behavior-neiwang_out] filter permit
[BRAS-behavior-neiwang_out] quit
```

配置流行为 Web_out，允许用户组 Web 中源地址为 Portal 服务器 IP 地址的报文通过。

```
[BRAS] traffic behavior Web_out
[BRAS-behavior-Web_out] filter permit
[BRAS-behavior-Web_out] free account
[BRAS-behavior-Web_out] quit
```

(4) 配置 QoS 策略

配置入方向 QoS 策略 Web

```
[BRAS] qos policy Web
```

为类指定对应的流行为，规则为对于用户组 Web 中的用户：

允许目的地址为 Portal 服务器和内网服务器 IP 地址的报文通过；

对于目的端口为 80（HTTP 报文）和 443（HTTPS 报文）的报文重定向到 CPU，用户组为 Web 的 IP 报文重定向到 CPU；

除上述报文外，其余报文均禁止通过。

```
[BRAS-qospolicy-Web] classifier Web_permit behavior Web_permit
[BRAS-qospolicy-Web] classifier neiwang behavior neiwang
[BRAS-qospolicy-Web] classifier Web_http behavior Web_http
```

```
[BRAS-qospolicy-Web] classifier Web_https behavior Web_https
[BRAS-qospolicy-Web] classifier ip_cpu behavior Web_cpu
[BRAS-qospolicy-Web] classifier Web_deny behavior Web_deny
[BRAS-qospolicy-Web] quit
```

配置出方向 QoS 策略 out

```
[BRAS] qos policy out
```

为类指定对应的流行为，规则为：允许用户组 Web 中源地址为 Portal 服务器和内网服务器 IP 地址的报文通过，其余报文均禁止通过。

```
[BRAS-qospolicy-out] classifier Web_out behavior Web_out
[BRAS-qospolicy-out] classifier neiwang_out behavior neiwang_out
[BRAS-qospolicy-out] classifier Web_deny behavior Web_deny
[BRAS-qospolicy-out] quit
```

(5) 配置应用策略

对接收的用户流量应用 QoS 策略，策略名为 Web。

```
[BRAS] qos apply policy Web global inbound
```

对发送的上线用户流量应用 QoS 策略，策略名为 out。

```
[BRAS] qos apply policy out global outbound
```

(6) 查看应用的策略是否生效

查看入方向 QoS 策略的配置信息和运行情况。

```
[BRAS] display qos policy global slot 3 inbound
  Direction: Inbound
  Policy: Web
   Classifier: Web_permit
     Operator: OR
     Rule(s) :
      If-match acl name Web_permit
     Behavior: Web_permit
      Filter enable: Permit
      Free account enable
   Classifier: neiwang
     Operator: OR
     Rule(s) :
      If-match acl name neiwang
     Behavior: neiwang
      Filter enable: Permit
   Classifier: Web_http
     Operator: OR
     Rule(s) :
      If-match acl name Web_http
     Behavior: Web_http
      Redirecting:
        Redirect http to CPU
   Classifier: Web_https
     Operator: OR
     Rule(s) :
      If-match acl name Web_https
```

```
    Behavior: Web_https
     Redirecting:
       Redirect https to CPU
  Classifier: Web_cpu
    Operator: OR
    Rule(s) :
     If-match acl name ip
   Behavior: Web_cpu
     Redirecting:
       Redirect to the CPU
 Classifier: Web_deny
    Operator: OR
    Rule(s) :
     If-match acl name ip
    Behavior: Web_deny
     Filter enable: Deny
     Free account enable
```

查看出方向 QoS 策略的配置信息和运行情况。

```
[BRAS] display qos policy global slot 3 outbound
  Direction: Outbound
  Policy: out
   Classifier: neiwang_out
     Operator: OR
     Rule(s) :
      If-match acl name neiwang_out
     Behavior: neiwang_out
      Filter enable: Permit
   Classifier: Web_out
     Operator: OR
     Rule(s) :
      If-match acl name Web_out
     Behavior: Web_out
      Filter enable: Permit
      Free account enable
   Classifier: Web_deny
     Operator: OR
     Rule(s) :
      If-match acl name ip
     Behavior: Web_deny
      Filter enable: Deny
      Free account enable
```

6. 配置 RADIUS 方案

创建名称为 rs1 的 RADIUS 方案并进入该方案视图。

```
[BRAS] radius scheme rs1
```

配置 RADIUS 方案的主认证和主计费服务器及其通信密钥。

```
[BRAS-radius-rs1] primary authentication 4.4.4.1
[BRAS-radius-rs1] primary accounting 4.4.4.1
```

```
[BRAS-radius-rs1] key authentication simple radius
[BRAS-radius-rs1] key accounting simple radius
```

配置发送给 RADIUS 服务器的用户名不携带 ISP 域名。

```
[BRAS-radius-rs1] user-name-format without-domain
[BRAS-radius-rs1] quit
```

设置 RADIUS DAE 客户端的 IP 地址为 4.4.4.1，与 RADIUS DAE 客户端交互 DAE 报文时使用的共享密钥为明文 radius。

```
[BRAS] radius dynamic-author server
[BRAS-radius-da-server] client ip 4.4.4.1 key simple radius
[BRAS-radius-da-server] quit
```

7. 配置 User Profile

配置名称为 car 的 User Profile 对上线用户发送的报文进行流量监管。报文正常流速为 5210kbps，允许 325625byte 的突发流量通过，速率小于等于 5210kbps 时正常发送，大于 5210kbps 时，报文被丢弃。

```
[BRAS] user-profile car
[BRAS-user-profile-car] qos car inbound any cir 5210 cbs 325625
[BRAS-user-profile-car] quit
```

8. 配置认证前域和 Web 认证域

配置 IPoE 用户认证前使用的认证域。

```
[BRAS] domain name dm1
[BRAS-isp-dm1] authentication ipoe none
[BRAS-isp-dm1] authorization ipoe none
[BRAS-isp-dm1] accounting ipoe none
```

配置前域授权用户组和地址池。

```
[BRAS-isp-dm1] authorization-attribute user-group Web
[BRAS-isp-dm1] authorization-attribute ip-pool pool1
```

配置 Web 认证页面 URL。

```
[BRAS-isp-dm1] Web-server url http://www.h3c.web.com
[BRAS-isp-dm1] quit
```

配置 IPoE 用户在 Web 认证阶段使用的认证域。

```
[BRAS] domain name dm2
[BRAS-isp-dm2] authentication ipoe radius-scheme rs1
[BRAS-isp-dm2] authorization ipoe radius-scheme rs1
[BRAS-isp-dm2] accounting ipoe radius-scheme rs1
[BRAS-isp-dm2] authorization-attribute user-profile car
[BRAS-isp-dm2] quit
```

9. 配置 IPoE

开启 IPoE 功能，并配置二层接入模式。

```
[BRAS] interface gigabitethernet 3/1/2
[BRAS-GigabitEthernet3/1/2] ip subscriber l2-connected enable ipv4
```

配置 IPoE 用户采用 Web MAC 认证方式。

```
[BRAS-GigabitEthernet3/1/2] ip subscriber authentication-method Web mac-auth
The operation may cut all users on this interface. Continue?[Y/N]:y
```

开启 IPoE 漫游功能。

```
[BRAS-GigabitEthernet3/1/2] ip subscriber roaming enable
```

配置 Web 认证前域为 dm1，Web 认证域和 Web MAC 认证域均为 dm2。

```
[BRAS-GigabitEthernet3/1/2] ip subscriber pre-auth domain dm1
[BRAS-GigabitEthernet3/1/2] ip subscriber Web-auth domain dm2
[BRAS-GigabitEthernet3/1/2] ip subscriber mac-auth domain dm2
[BRAS-GigabitEthernet3/1/2] quit
```

6.4.7 验证配置

用户认证前域认证通过之后，可以使用以下的显示命令查看 IPoE 用户在线信息，其中，用户获得的 IPv4 地址为 192.168.0.2。

```
[BRAS] display ip subscriber session verbose
Basic:
  Description                 : -
  Username                    : 001b21a80949
  Domain                      : dm1
  VPN instance                : N/A
  IP address                  : 192.168.0.2
  User address type           : N/A
  MAC address                 : 001b-21a8-0949
  Service-VLAN/Customer-VLAN  : -/-
  Access interface            : GE3/1/2
  User ID                     : 0x30000004
  VPI/VCI(for ATM)            : -/-
  VSI Index                   : -
  VSI link ID                 : -
  VXLAN ID                    : -
  DNS servers                 : N/A
  IPv6 DNS servers            : N/A
  DHCP lease                  : 86400 sec
  DHCP remain lease           : 86383 sec
  Access time                 : May 27 00:48:51 2018
  Online time(hh:mm:ss)       : 00:00:19
  Service node                : Slot 3 CPU 0
  Authentication type         : Web pre-auth
  IPv4 access type            : DHCP
  IPv4 detect state           : Detecting
  State                       : Online

AAA:
  ITA policy name             : N/A
  IP pool                     : pool1
  IPv6 pool                   : N/A
  IPv6 nd preifx pool         : N/A
  Primary DNS server          : N/A
  Secondary DNS server        : N/A
  Primary IPv6 DNS server     : N/A
  Secondary IPv6 DNS server   : N/A
```

```
  Session idle cut             : N/A
  Session duration             : N/A, remaining: N/A
  Traffic quota                : N/A
  Traffic remained             : N/A
  Acct start-fail action       : Online
  Acct update-fail action      : Online
  Acct quota-out action        : Offline
  Dual-stack accounting mode   : Merge
  Max IPv4 multicast addresses: 4
  IPv4 multicast address list : N/A
  Max IPv6 multicast addresses: 4
  IPv6 multicast address list : N/A
  Accounting start time        : May 27 00:48:51 2018
  Redirect URL                 : http://www.h3c.web.com
  Subscriber ID                : -

QoS:
  User profile                 : N/A
  Session group profile        : N/A
  User group ACL               : Web (active)
  Inbound CAR                  : N/A
  Outbound CAR                 : N/A
  Inbound user priority        : N/A
  Outbound user priority       : N/A

Flow statistic:
  Uplink   packets/bytes       : 0/0
  Downlink packets/bytes       : 0/0
  IPv6 uplink   packets/bytes : 0/0
  IPv6 downlink packets/bytes : 0/0
```

用户认证前域认证通过之后，登录 Web 页面，如图 8-16 所示。

图6-7 登录 Web 页面

在认证页面输入用户名和密码单击<上线>按钮进行 Web 认证，可以使用以下的显示命令查看 IPoE 用户在线信息。

```
[BRAS] display ip subscriber session verbose
Basic:
  Description                 : -
  Username                    : user1@dm2
  Domain                      : dm2
  VPN instance                : N/A
  IP address                  : 192.168.0.2
  User address type           : N/A
  MAC address                 : 001b-21a8-0949
  Service-VLAN/Customer-VLAN  : -/-
  Access interface            : GE3/1/2
  User ID                     : 0x30000004
  VPI/VCI(for ATM)            : -/-
  VSI Index                   : -
  VSI link ID                 : -
  VXLAN ID                    : -
  DNS servers                 : N/A
  IPv6 DNS servers            : N/A
  DHCP lease                  : 86400 sec
  DHCP remain lease           : 86356 sec
  Access time                 : May 27 00:49:20 2018
  Online time(hh:mm:ss)       : 00:00:04
  Service node                : Slot 3 CPU 0
  Authentication type         : Web
  IPv4 access type            : DHCP
```

```
  IPv4 detect state           : Detecting
  State                       : Online

AAA:
  ITA policy name             : N/A
  IP pool                     : pool1
  IPv6 pool                   : N/A
  IPv6 nd preifx pool         : N/A
  Primary DNS server          : N/A
  Secondary DNS server        : N/A
  Primary IPv6 DNS server     : N/A
  Secondary IPv6 DNS server   : N/A
  Session idle cut            : N/A
  Session duration            : 86400 sec, remaining: 86395 sec
  Traffic quota               : N/A
  Traffic remained            : N/A
  Acct start-fail action      : Online
  Acct update-fail action     : Online
  Acct quota-out action       : Offline
  Dual-stack accounting mode  : Merge
  Max IPv4 multicast addresses: 4
  IPv4 multicast address list : N/A
  Max IPv6 multicast addresses: 4
  IPv6 multicast address list : N/A
  Accounting start time       : May 27 00:49:20 2018
  Subscriber ID               : -

QoS:
  User profile                : car (active)
  Session group profile       : N/A
  User group ACL              : N/A
  Inbound CAR                 : N/A
  Outbound CAR                : N/A
  Inbound user priority       : N/A
  Outbound user priority      : N/A

Flow statistic:
  Uplink   packets/bytes      : 0/0
  Downlink packets/bytes      : 0/0
  IPv6 uplink   packets/bytes : 0/0
  IPv6 downlink packets/bytes : 0/0
```

6.4.8 配置文件

- DHCP 服务器：

```
#
 dhcp enable
```

```
#
dhcp server ip-pool pool1
 gateway-list 192.168.0.1
 network 192.168.0.0 mask 255.255.255.0
 forbidden-ip 192.168.0.1
#
interface GigabitEthernet3/1/1
 port link-mode route
 ip address 4.4.4.3 255.255.255.0
#
 ip route-static 192.168.0.0 24 4.4.4.2
#
```

- Router A（BRAS）：

```
#
 dhcp enable
 dhcp relay client-information record
 undo dhcp relay client-information refresh enable
#
traffic classifier ip_cpu operator or
 if-match acl name ip
#
traffic classifier ip_deny operator or
 if-match acl name ip
#
traffic classifier neiwang operator or
 if-match acl name neiwang
#
traffic classifier neiwang_out operator or
 if-match acl name neiwang_out
#
traffic classifier Web_http operator or
 if-match acl name Web_http
#
traffic classifier Web_https operator or
 if-match acl name Web_https
#
traffic classifier Web_out operator or
 if-match acl name Web_out
#
traffic classifier Web_permit operator or
 if-match acl name Web_permit
#
traffic behavior neiwang
 filter permit
#
traffic behavior neiwang_out
 filter permit
#
```

```
traffic behavior Web_cpu
 redirect cpu
#
traffic behavior Web_deny
 filter deny
 free account
#
traffic behavior Web_http
 redirect http-to-cpu
#
traffic behavior Web_https
 redirect https-to-cpu
#
traffic behavior Web_out
 filter permit
 free account
#
traffic behavior Web_permit
 filter permit
 free account
#
qos policy out
 classifier Web_out behavior Web_out
 classifier neiwang_out behavior neiwang_out
 classifier ip_deny behavior Web_deny
#
qos policy Web
 classifier Web_permit behavior Web_permit
 classifier neiwang behavior neiwang
 classifier Web_http behavior Web_http
 classifier Web_https behavior Web_https
 classifier ip_cpu behavior Web_cpu
 classifier ip_deny behavior Web_deny
#
interface GigabitEthernet3/1/1
 ip address 4.4.4.2 255.255.255.0
 ipv6 address 4::2/64
#
interface GigabitEthernet3/1/2
 port link-mode route
 dhcp select relay proxy
 dhcp flood-protection enable
 dhcp session-mismatch action fast-renew
 ipv6 address 192::1/64
 undo ipv6 nd ra halt
 ip subscriber l2-connected enable ipv4
 ip subscriber authentication-method Web mac-auth
 ip subscriber roaming enable
```

```
 ip subscriber pre-auth domain dm1
 ip subscriber mac-auth domain dm2
 ip subscriber Web-auth domain dm2
#
 qos apply policy Web global inbound
 qos apply policy out global outbound
#
dhcp server ip-pool pool1
 gateway-list 192.168.0.1 export-route
 remote-server 4.4.4.3
#
acl advanced name ip
 rule 0 permit ip user-group Web
#
acl advanced name neiwang
 rule 0 permit ip destination 4.4.4.6 0 user-group Web
#
acl advanced name neiwang_out
 rule 0 permit ip source 4.4.4.6 0 user-group Web
#
acl advanced name Web_http
 rule 0 permit tcp destination-port eq www user-group Web
#
acl advanced name Web_https
 rule 0 permit tcp destination-port eq 443 user-group Web
#
acl advanced name Web_out
 rule 0 permit ip source 4.4.4.5 0 user-group Web
#
acl advanced name Web_permit
 rule 0 permit ip destination 4.4.4.5 0 user-group Web
#
user-profile car
 qos car inbound any cir 5210 cbs 325625 ebs 0
#
radius scheme rs1
 primary authentication 4.4.4.1
 primary accounting 4.4.4.1
 key authentication cipher $c$3$FhQVcgn3kq1exL0CdTzatcgc9xF9vL3ZOw==
 key accounting cipher $c$3$ntIHBRM4ZkG+2JRZQTdKmNl0kYJmhZz5Zg==
 user-name-format without-domain
#
radius dynamic-author server
 client ip 4.4.4.1 key cipher $c$3$lYC2ERe8ts2gtE6M2xfoDDB8NmGw6J9v/Q==
#
domain name dm1
 authorization-attribute user-group Web
 authorization-attribute ip-pool pool1
```

```
 authentication ipoe none
 authorization ipoe none
 accounting ipoe none
 Web-server url http://www.h3c.web.com
#
domain name dm2
 authorization-attribute user-profile car
 authentication ipoe radius-scheme rs1
 authorization ipoe radius-scheme rs1
 accounting ipoe radius-scheme rs1
#
user-group Web
#
portal server newpt1
 ip 4.4.4.5 key cipher $c$3$UnoFeLybwld9jDwLnHJQptDE7YZry2EVlw==
#
 http-redirect https-port 11111
#
```

7 IPoE Web 双栈用户 MAC 无感知认证配置举例(ND 前缀池方式)

在网络向 IPv6 演进的过程中，由于一段时间内，各种网络资源还没有全面支持 IPv6，因此需要以 IPv4/IPv6 双协议栈运行。

本举例描述一个对部署时对 IPv4 和 IPv6 都做认证的场景，而且实现任意一个协议栈认证通过，两个协议同时放行。

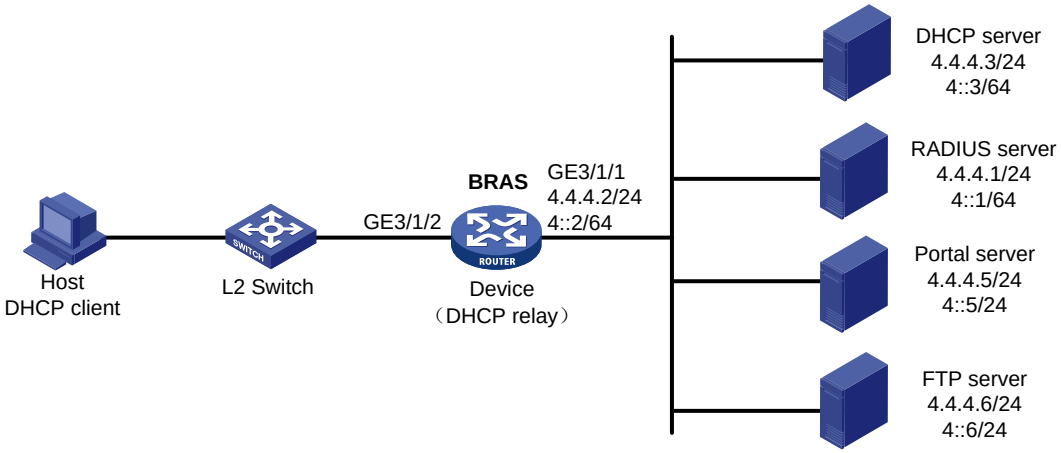
本举例使用 NDRA 来分配 IPv6 地址，这种方案既适合有线用户，也适合无线用户。但此方案需要的 IPv6 地址资源较多，可能不适合部分用户。

7.1 组网需求

如图 7-1 所示：Device 为某学校的一台 BRAS 设备，为学校用户提供 IPoE 接入服务。要求：

- DHCP Client 经由二层网络以 IPoE 方式接入到 BRAS 接入设备。
- BRAS 接入设备作为 DHCP 中继向远端 DHCP 服务器申请 IP 地址。
- 由一台安装了 H3C iMC 的服务器同时承担 Portal 认证服务器和 Portal Web 服务器的职责。
- 由一台支持 MAC 绑定功能的 RADIUS 服务器同时承担认证、授权和计费服务器以及 MAC 绑定服务器的职责。
- FTP server 是一台内网服务器。
- IPoE Web 认证通过后限速 5Mbps。

图7-1 IPoE 双栈用户 MAC 无感知认证配置组网图



7.2 配置思路

为了保证用户的带宽需求，本例通过授权 User Profile 进行速率控制。

IPoE Web 认证前域中的流量，区分 HTTP、HTTPS 和普通 IP 报文分别通过不同的队列上送。IPoE Web 认证中针对上送 CPU 的流量，配置如下三种类和流行为组来处理：

- 流分类匹配 HTTP 同时 User Group 为前域标记的，对应的流行为 **redirect http-to-cpu**。
- 流分类匹配 HTTPS 同时 User Group 为前域标记的，对应的流行为 **redirect https-to-cpu**。
- 流分类匹配 IP 同时 User Group 为前域标记的，对应的流行为 **redirect cpu**。

当 BRAS 接入用户下线时，DHCP 中继需要查询中继用户地址表项，若存在对应表项，则会向 DHCP 服务器发送 Release 报文，通知 DHCP 服务器释放该地址租约。这就需要在 DHCP 中继上使用 **dhcp relay client-information record** 命令开启 DHCP 中继用户地址表项记录功能。

7.3 配置注意事项

本例中 DHCP Server 是由设备进行模拟，实际应用建议使用专门的 DHCP 服务器。

缺省情况下，未配置对 HTTPS 报文进行重定向的内部侦听端口号。需要通过 **http-redirect https-port** 命令用来配置对 HTTPS 报文进行重定向的侦听端口号，并且配置的侦听端口不要跟已有端口冲突。

本配置可以实现对安卓手机、iPhone、PC 终端都分配 IPv4/IPv6 地址，并都做认证，但需要的 IPv6 地址资源较多，需要结合实际情况选择部署方式。

本配置中使用到限速私有属性，有关私有属性的详细介绍，请参见 14 附录。

7.4 配置步骤

7.4.1 配置 IP 地址及路由

按照图 7-1配置各接口的 IP 地址，并确保 BRAS 设备和各服务器之间路由可达，具体配置过程略。

7.4.2 设置 DNS 服务器

请正确设置 DNS 服务器，以便服务器可以根据 IPoE 双栈用户先上线的协议栈类型，解析出 Web 认证页面 http://www.h3c.web.com 对应的 IPv4 URL 地址或 IPv6 URL 地址。DNS 服务器具体设置过程略。

7.4.3 配置 DHCP 服务器

1. 配置 DHCPv4 地址池

开启 DHCP 服务。

```
<DHCP> system-view
[DHCP] dhcp enable
```

创建名称为 pool1 的 DHCPv4 地址池并进入其视图。

```
[DHCP] dhcp server ip-pool pool1
```

配置地址池动态分配的 IP 地址网段 192.168.0.0/24。

```
[DHCP-dhcp-pool-pool1] network 192.168.0.0 24
```

配置为用户分配的网关地址为 192.168.0.1。

```
[DHCP-dhcp-pool-pool1] gateway-list 192.168.0.1
```

将 192.168.0.1 设置为禁止地址。

```
[DHCP-dhcp-pool-pool1] forbidden-ip 192.168.0.1
[DHCP-dhcp-pool-pool1] quit
```

通过配置静态路由，将目的地址为 192.168.0.0 网段的 DHCPv4 应答报文的下一跳指定为连接 DHCPv4 客户端网络的接口 IPv4 地址 4.4.4.2。

```
[DHCP] ip route-static 192.168.0.0 24 4.4.4.2
```

7.4.4 配置 RADIUS 服务器

对于 RADIUS 服务器上 AAA 和 MAC 绑定配置，具体需要参见 RADIUS server 的配置说明书。

7.4.5 配置 Portal 服务器

说明

下面以 iMC（版本为 iMC PLAT 7.3 (E0705P02)）为例，说明 Portal 服务器的基本配置。不同 iMC 版本配置可能有所不同，具体配置请以实际版本及对应版本的 iMC 服务器手册为准，本节配置仅供参考。

(1) 配置 Portal 主页。

单击导航树中的[接入策略管理/Portal 服务管理/服务器配置]菜单项，进入服务器配置页面，配置 Portal 主页，采用缺省配置即可，并单击<确定>按钮完成操作，如图 7-2 所示。

图7-2 Portal 服务器配置页面

(2) 配置 Portal 认证的地址组范围

单击导航树中的[接入策略管理/Portal 服务管理/IP 地址组配置]菜单项，进入“IP 地址组配置”页面，在该页面中单击<增加>按钮，进入“增加 IP 地址组配置”页面，如图 7-3 所示。

- 输入 IP 地址组名为“IPoE_Web_User”；
- 输入起始地址为“192.168.0.1”、终止地址为“192.168.0.255”。用户主机 IP 地址必须包含在该 IP 地址组范围内；
- 其他采用缺省配置；
- 单击<确定>按钮完成操作。

图7-3 增加 IP 地址组配置页面（IPv4）

如图 7-4 所示，继续上述操作添加 IPv6 地址组。

- 输入 IP 地址组名为“IPoE_Web_User-2”；
- IPv6 选项框选择“是”；

- 输入起始地址为“192::1”、终止地址为“192::FFFF”。用户主机 IPv6 地址必须包含在该 IP 地址组范围内；
- 其他采用缺省配置；
- 单击<确定>按钮完成操作。

图7-4 增加 IP 地址组配置页面（IPv6）

(3) 增加 Portal 接入设备信息

单击导航树中的[接入策略管理/Portal 服务管理/设备配置]菜单项，进入“设备配置”页面，在该页面中单击<增加>按钮，进入“增加设备信息”页面，如图 7-5 所示。

- 输入设备名为“NAS”；
- 输入 IP 地址为“4.4.4.2”，该地址为 Portal 报文出接口 GigabitEthernet3/1/1 的 IP 地址；
- 输入密钥为“123456”；
- 选择组网方式为“直连”；
- 其它参数采用缺省值，并单击<确定>按钮完成操作。

图7-5 增加设备信息配置页面（IPv4）

如图 7-6 所示，继续上述操作添加设备的 IPv6 信息。

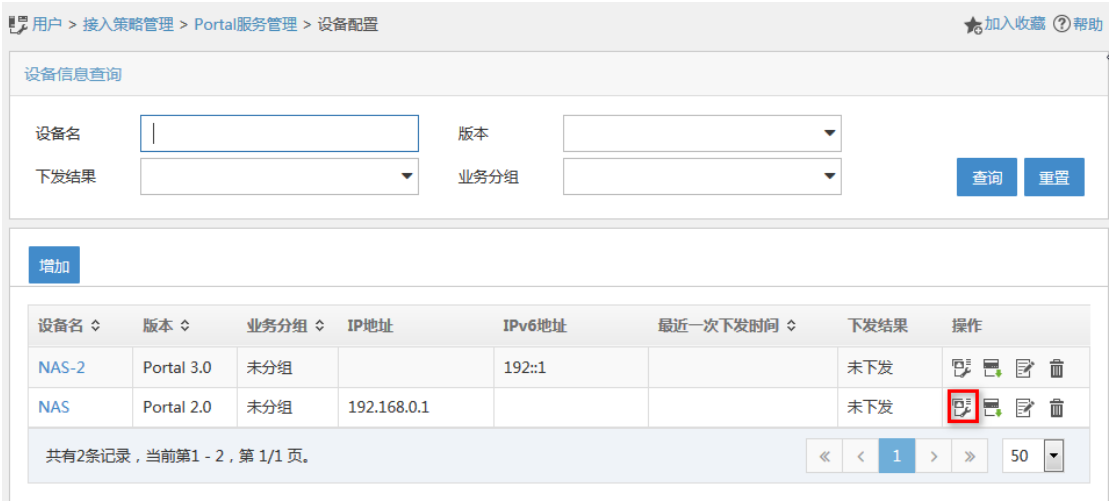
- 输入设备名为“NAS-2”；
- 版本选择“Portal 3.0”；
- 输入 IP 地址为“4::2”，该地址为 Portal 报文出接口 GigabitEthernet3/1/1 的 IP 地址；
- 输入密钥为“123456”；
- 选择组网方式为“直连”；
- 其它参数采用缺省值，并单击<确定>按钮完成操作。

图7-6 增加设备信息配置页面（IPv6）

(4) 配置端口组信息

如图 7-7 所示返回[接入策略管理/Portal 服务管理/设备配置]菜单项，单击<端口组信息管理>按钮，进入“端口组信息配置”页面。

图7-7 设备信息列表



在“端口组信息配置”页面中单击<增加>按钮，进入“增加端口组信息”页面，如图 7-8 所示。

- 输入端口组名为“group”；
- 选择 IP 地址组为“IPoE_Web_User”，用户接入网络时使用的 IP 地址必须属于所选的 IP 地址组；
- 其它参数采用缺省值，并单击<确定>按钮完成操作。

图7-8 增加端口组信息配置页面（IPv4）

如图 7-9 所示，继续上述操作添加端口组的 IPv6 信息。

- 输入端口组名为“group-2”；
- 选择 IP 地址组为“IPoE_Web_User-2”，用户接入网络时使用的 IPv6 地址必须属于所选的 IPv6 地址组；
- 其它参数采用缺省值，并单击<确定>按钮完成操作。

图7-9 增加端口组信息配置页面（IPv6）

最后单击导航树中的[接入策略管理/业务参数配置/系统配置手工生效]菜单项，使以上Portal 认证服务器配置生效。

7.4.6 配置 BRAS

1. 配置 DHCP 中继

全局开启 DHCP。

```
[BRAS] dhcp enable
```

启用 DHCP 中继的用户地址表项记录功能。

```
[BRAS] dhcp relay client-information record
```

关闭 DHCP 中继动态用户地址表项定时刷新功能。

```
[BRAS] undo dhcp relay client-information refresh enable
```

创建中继地址池 pool1，指定匹配该地址池的 DHCPv4 客户端所在的网段地址，并指定中继地址池对应的 DHCP 服务器地址。

```
[BRAS] dhcp server ip-pool pool1
[BRAS-dhcp-pool-pool1] gateway-list 192.168.0.1 export-route
[BRAS-dhcp-pool-pool1] remote-server 4.4.4.3
[BRAS-dhcp-pool-pool1] quit
```

创建前缀地址池 1，指定给用户分配的前缀。

```
[BRAS]ipv6 dhcp prefix-pool 1 prefix 192::/48 assign-len 64
```

创建名称为 pool2 的 DHCPv6 地址池并进入其视图。

```
[DHCP] ipv6 dhcp pool pool2
```

配置地址池关联的前缀地址池 1。

```
[DHCP-dhcp6-pool-pool2] prefix-pool 1 export-route
[DHCP-dhcp6-pool-pool2] quit
```

配置接口工作在 DHCPv4 中继模式。

```
[BRAS] interface gigabitethernet 3/1/2
[BRAS-GigabitEthernet3/1/2] dhcp select relay proxy
```

配置 DHCP 防攻击功能。

```
[BRAS-GigabitEthernet3/1/2] dhcp flood-protection enable
```

配置漫游时重新分配地址功能。

```
[BRAS-GigabitEthernet3/1/2] dhcp session-mismatch action fast-renew
[BRAS-GigabitEthernet3/1/2] ipv6 dhcp session-mismatch action fast-renew
```

配置自动生成 IPv6 链路本地地址，该 IPv6 链路本地地址作为用户的网关。

```
[BRAS-GigabitEthernet3/1/2] ipv6 address auto link-local
```

取消设备发布 RA 消息的抑制。

```
[BRAS-GigabitEthernet3/1/2] undo ipv6 nd ra halt
```

2. 配置 Portal 认证服务器

配置 IPv4 Portal 认证服务器：名称为 newpt1，IP 地址为 4.4.4.5，密钥为明文 123456。

```
[BRAS] portal server newpt1
[BRAS-portal-server-newpt1] ip 4.4.4.5 key simple 123456
[BRAS-portal-server-newpt1] quit
```

配置 IPv6 Portal 认证服务器：名称为 newpt2，IPv6 地址为 4::5，密钥为明文 123456。

```
[BRAS] portal server newpt2
[BRAS-portal-server-newpt2] ipv6 4::5 key simple 123456
[BRAS-portal-server-newpt2] quit
```

3. 配置 HTTPS 的内部侦听端口

配置 HTTPS 的内部侦听端口，端口不要跟已有端口冲突即可。

```
[BRAS] http-redirect https-port 11111
```

4. 创建本地用户组

创建认证前域用户组，名称为 Web。

```
[BRAS] user-group Web
New user group added.
[BRAS-ugroup-Web] quit
```

5. 配置 QoS

(1)　配置用于认证前域用户的 ACL 规则

分别为 IPv4 和 IPv6 高级 ACL Web_permit 创建规则如下：匹配用户组 Web 中用户的目的地址为 Portal 服务器地址的报文。

```
[BRAS] acl advanced name Web_permit
[BRAS-acl-ipv4-adv-Web_permit] rule 0 permit ip destination 4.4.4.5 0 user-group Web
[BRAS-acl-ipv4-adv-Web_permit] quit
[BRAS] acl ipv6 advanced name Web_permit
[BRAS-acl-ipv6-adv-Web_permit] rule 0 permit ipv6 destination 4::5 128 user-group Web
[BRAS-acl-ipv6-adv-Web_permit] quit
```

分别为 IPv4 和 IPv6 高级 ACL neiwang 创建规则如下：匹配用户组 Web 中用户的目的地址为内网服务器地址的报文。

```
[BRAS] acl advanced name neiwang
[BRAS-acl-ipv4-adv-neiwang] rule 0 permit ip destination 4.4.4.6 0 user-group Web
[BRAS-acl-ipv4-adv-neiwang] quit
[BRAS] acl ipv6 advanced name neiwang
[BRAS-acl-ipv6-adv-neiwang] rule 0 permit ipv6 destination 4::6 128 user-group Web
[BRAS-acl-ipv6-adv-neiwang] quit
```

分别为 IPv4 和 IPv6 高级 ACL Web_http 创建规则如下：匹配用户组 Web 中用户的目的端口为 80 的 TCP 报文(即 HTTP 报文)。

```
[BRAS] acl advanced name Web_http
[BRAS-acl-ipv4-adv-Web_http] rule 0 permit tcp destination-port eq www user-group Web
[BRAS-acl-ipv4-adv-Web_http] quit
[BRAS] acl ipv6 advanced name Web_http
[BRAS-acl-ipv6-adv-Web_http] rule 0 permit tcp destination-port eq www user-group Web
[BRAS-acl-ipv6-adv-Web_http] quit
```

分别为 IPv4 和 IPv6 高级 ACL Web_https 创建规则如下：匹配用户组 Web 中用户的目的端口为 443 的 TCP 报文(即 HTTPS 报文)。

```
[BRAS] acl advanced name Web_https
[BRAS-acl-ipv4-adv-Web_https] rule 0 permit tcp destination-port eq 443 user-group Web
[BRAS-acl-ipv4-adv-Web_https] quit
[BRAS] acl ipv6 advanced name Web_https
[BRAS-acl-ipv6-adv-Web_https] rule 0 permit tcp destination-port eq 443 user-group Web
[BRAS-acl-ipv6-adv-Web_https] quit
```

分别为 IPv4 和 IPv6 高级 ACL ip 创建规则如下：匹配用户组 Web 中用户的 IP 报文。

```
[BRAS] acl advanced name ip
[BRAS-acl-ipv4-adv-ip] rule 0 permit ip user-group Web
[BRAS-acl-ipv4-adv-ip] quit
[BRAS] acl ipv6 advanced name ip
[BRAS-acl-ipv6-adv-ip] rule 0 permit ipv6 user-group Web
[BRAS-acl-ipv6-adv-ip] quit
```

分别为 IPv4 和 IPv6 高级 ACL neiwang_out 创建规则如下：匹配用户组 Web 中源地址为内网服务器 IP 地址的报文。

```
[BRAS] acl advanced name neiwang_out
[BRAS-acl-ipv4-adv-neiwang_out] rule 0 permit ip source 4.4.4.6 0 user-group Web
[BRAS-acl-ipv4-adv-neiwang_out] quit
[BRAS] acl ipv6 advanced name neiwang_out
[BRAS-acl-ipv6-adv-neiwang_out] rule 0 permit ipv6 source 4::6 128 user-group Web
[BRAS-acl-ipv6-adv-neiwang_out] quit
```

分别为 IPv4 和 IPv6 高级 ACL Web_out 创建规则如下：匹配用户组 Web 中源地址为 Portal 服务器 IP 地址的报文。

```
[BRAS] acl advanced name Web_out
[BRAS-acl-ipv4-adv-Web_out] rule 0 permit ip source 4.4.4.5 0 user-group Web
[BRAS-acl-ipv4-adv-Web_out] quit
[BRAS] acl ipv6 advanced name Web_out
[BRAS-acl-ipv6-adv-Web_out] rule 0 permit ipv6 source 4::5 128 user-group Web
[BRAS-acl-ipv6-adv-Web_out] quit
```

(2) 配置用于认证前域用户的类

配置类 Web_permit，匹配 ACL Web_permit。

```
[BRAS] traffic classifier Web_permit operator or
[BRAS-classifier-Web_permit] if-match acl name Web_permit
[BRAS-classifier-Web_permit] if-match acl ipv6 name Web_permit
[BRAS-classifier-Web_permit] quit
```

配置类 neiwang，匹配 ACL neiwang。

```
[BRAS] traffic classifier neiwang operator or
[BRAS-classifier-neiwang] if-match acl name neiwang
[BRAS-classifier-neiwang] if-match acl ipv6 name neiwang
[BRAS-classifier-neiwang] quit
```

配置类 Web_http，匹配 ACL Web_http。

```
[BRAS] traffic classifier Web_http operator or
[BRAS-classifier-Web_http] if-match acl name Web_http
[BRAS-classifier-Web_http] if-match acl ipv6 name Web_http
[BRAS-classifier-Web_http] quit
```

配置类 Web_https，匹配 ACL Web_https。

```
[BRAS] traffic classifier Web_https operator or
[BRAS-classifier-Web_https] if-match acl name Web_https
[BRAS-classifier-Web_https] if-match acl ipv6 name Web_https
[BRAS-classifier-Web_https] quit
```

配置类 ip_cpu，匹配 ACL ip。

```
[BRAS] traffic classifier ip_cpu operator or
[BRAS-classifier-ip_cpu] if-match acl name ip
[BRAS-classifier-ip_cpu] if-match acl ipv6 name ip
[BRAS-classifier-ip_cpu] quit
```

配置类 ip_deny，匹配 ACL ip。

```
[BRAS] traffic classifier ip_deny operator or
[BRAS-classifier-ip_deny] if-match acl name ip
[BRAS-classifier-ip_deny] if-match acl ipv6 name ip
[BRAS-classifier-ip_deny] quit
```

配置类 neiwang_out，匹配 ACL neiwang_out。

```
[BRAS] traffic classifier neiwang_out operator or
[BRAS-classifier-neiwang_out] if-match acl name neiwang_out
[BRAS-classifier-neiwang_out] if-match acl ipv6 name neiwang_out
[BRAS-classifier-neiwang_out] quit
```

配置类 Web_out，匹配 ACL Web_out。

```
[BRAS] traffic classifier Web_out operator or
[BRAS-classifier-Web_out] if-match acl name Web_out
[BRAS-classifier-Web_out] if-match acl ipv6 name Web_out
[BRAS-classifier-Web_out] quit
```

(3) 配置流行为

配置流行为 Web_permit，允许用户组 Web 中用户的目的地址为 Portal 服务器 IP 地址的报文通过。

```
[BRAS] traffic behavior Web_permit
[BRAS-behavior-Web_permit] filter permit
[BRAS-behavior-Web_permit] free account
[BRAS-behavior-Web_permit] quit
```

配置流行为 neiwang，允许用户组 Web 中用户的目的地址为内网服务器 IP 地址的报文通过。

```
[BRAS] traffic behavior neiwang
[BRAS-behavior-neiwang] filter permit
[BRAS-behavior-neiwang] quit
```

配置流行为 Web_http，对用户组 Web 中用户的目的端口为 80 的 TCP 报文(即 HTTP 报文)重定向到 CPU。

```
[BRAS] traffic behavior Web_http
[BRAS-behavior-Web_http] redirect http-to-cpu
[BRAS-behavior-Web_http] quit
```

配置流行为 Web_https，对用户组 Web 中用户的目的端口为 443 的 TCP 报文(即 HTTPS 报文)重定向到 CPU。

```
[BRAS] traffic behavior Web_https
[BRAS-behavior-Web_https] redirect https-to-cpu
[BRAS-behavior-Web_https] quit
```

配置流行为 Web_cpu，对用户组 Web 中用户的所有 IP 报文都重定向到 CPU。

```
[BRAS] traffic behavior Web_cpu
[BRAS-behavior-Web_cpu] redirect cpu
[BRAS-behavior-Web_cpu] quit
```

配置流行为 Web_deny，禁止用户组 Web 中用户的所有 IP 报文通过。

```
[BRAS] traffic behavior Web_deny
[BRAS-behavior-Web_deny] filter deny
[BRAS-behavior-Web_deny] free account
[BRAS-behavior-Web_deny] quit
```

配置流行为 neiwang_out，允许用户组 Web 中源地址为内网服务器 IP 地址的报文通过。

```
[BRAS] traffic behavior neiwang_out
[BRAS-behavior-neiwang_out] filter permit
[BRAS-behavior-neiwang_out] quit
```

配置流行为 Web_out，允许用户组 Web 中源地址为 Portal 服务器 IP 地址的报文通过。

```
[BRAS] traffic behavior Web_out
[BRAS-behavior-Web_out] filter permit
[BRAS-behavior-Web_out] free account
[BRAS-behavior-Web_out] quit
```

(4) 配置 QoS 策略

配置入方向 QoS 策略 Web

```
[BRAS] qos policy Web
```

为类指定对应的流行为，规则为对于用户组 Web 中的用户：

允许目的地址为 Portal 服务器和内网服务器 IP 地址的报文通过；

对于目的端口为 80（HTTP 报文）和 443（HTTPS 报文）的报文重定向到 CPU；

除上述报文外，其余报文都重定向到 CPU，如果重定向无感知认证失败，则丢弃报文。

```
[BRAS-qospolicy-Web] classifier Web_permit behavior Web_permit
[BRAS-qospolicy-Web] classifier neiwang behavior neiwang
[BRAS-qospolicy-Web] classifier Web_http behavior Web_http
[BRAS-qospolicy-Web] classifier Web_https behavior Web_https
[BRAS-qospolicy-Web] classifier ip_cpu behavior Web_cpu
[BRAS-qospolicy-Web] classifier ip_deny behavior Web_deny
[BRAS-qospolicy-Web] quit
```

配置出方向 QoS 策略 out

```
[BRAS] qos policy out
```

为类指定对应的流行为，规则为：允许用户组 Web 中源地址为 Portal 服务器和内网服务器 IP 地址的报文通过，其余报文均禁止通过。

```
[BRAS-qospolicy-out] classifier Web_out behavior Web_out
[BRAS-qospolicy-out] classifier neiwang_out behavior neiwang_out
[BRAS-qospolicy-out] classifier ip_deny behavior Web_deny
[BRAS-qospolicy-out] quit
```

(5) 配置应用策略

对接收的用户流量应用 QoS 策略，策略名为 Web。

```
[BRAS] qos apply policy Web global inbound
```

对发送的上线用户流量应用 QoS 策略，策略名为 out。

```
[BRAS] qos apply policy out global outbound
```

(6) 查看应用的策略是否生效

查看入方向 QoS 策略的配置信息和运行情况。

```
[BRAS] display qos policy global slot 3 inbound
Direction: Inbound
  Policy: Web
   Classifier: Web_permit
     Operator: OR
     Rule(s) :
      If-match acl name Web_permit
      If-match acl ipv6 name Web_permit
     Behavior: Web_permit
      Filter enable: Permit
      Free account enable
   Classifier: neiwang
     Operator: OR
     Rule(s) :
      If-match acl name neiwang
      If-match acl ipv6 name neiwang
     Behavior: neiwang
      Filter enable: Permit
   Classifier: Web_http
     Operator: OR
     Rule(s) :
      If-match acl name Web_http
      If-match acl ipv6 name Web_http
     Behavior: Web_http
      Redirecting:
        Redirect http to CPU
   Classifier: Web_https
     Operator: OR
     Rule(s) :
      If-match acl name Web_https
      If-match acl ipv6 name Web_https
     Behavior: Web_https
      Redirecting:
        Redirect https to CPU
```

```
  Classifier: ip_cpu
    Operator: OR
    Rule(s) :
     If-match acl name ip
     If-match acl ipv6 name ip
    Behavior: Web_cpu
     Redirecting:
       Redirect to the CPU
  Classifier: ip_deny
    Operator: OR
    Rule(s) :
     If-match acl name ip
     If-match acl ipv6 name ip
    Behavior: Web_deny
     Filter enable: Deny
     Free account enable
```

查看出方向 QoS 策略的配置信息和运行情况。

```
[BRAS] display qos policy global slot 3 outbound
Direction: Outbound
  Policy: out
   Classifier: Web_out
     Operator: OR
     Rule(s) :
      If-match acl name Web_out
      If-match acl ipv6 name Web_out
     Behavior: Web_out
      Filter enable: Permit
      Free account enable
   Classifier: neiwang_out
     Operator: OR
     Rule(s) :
      If-match acl name neiwang_out
      If-match acl ipv6 name neiwang_out
     Behavior: neiwang_out
      Filter enable: Permit
   Classifier: ip_deny
     Operator: OR
     Rule(s) :
      If-match acl name ip
      If-match acl ipv6 name ip
     Behavior: Web_deny
      Filter enable: Deny
      Free account enable
```

6. 配置 RADIUS 方案

创建名称为 rs1 的 RADIUS 方案并进入该方案视图。

```
[BRAS] radius scheme rs1
```

配置 RADIUS 方案的主认证和主计费服务器及其通信密钥。

```
[BRAS-radius-rs1] primary authentication 4.4.4.1
[BRAS-radius-rs1] primary accounting 4.4.4.1
[BRAS-radius-rs1] key authentication simple radius
[BRAS-radius-rs1] key accounting simple radius
```

配置发送给 RADIUS 服务器的用户名不携带 ISP 域名。

```
[BRAS-radius-rs1] user-name-format without-domain
[BRAS-radius-rs1] quit
```

设置 RADIUS DAE 客户端的 IP 地址为 4.4.4.1，与 RADIUS DAE 客户端交互 DAE 报文时使用的共享密钥为明文 radius。

```
[BRAS] radius dynamic-author server
[BRAS-radius-da-server] client ip 4.4.4.1 key simple radius
[BRAS-radius-da-server] quit
```

7. 配置 User Profile

配置名称为 car 的 User Profile 对上线用户发送的报文进行流量监管。报文正常流速为 5210kbps，允许 325625byte 的突发流量通过，速率小于等于 5210kbps 时正常发送，大于 5210kbps 时，报文被丢弃。

```
[BRAS] user-profile car
[BRAS-user-profile-car] qos car inbound any cir 5210 cbs 325625
[BRAS-user-profile-car] quit
```

8. 配置认证前域和 Web 认证域

配置 IPoE 用户认证前使用的认证域。

```
[BRAS] domain name dm1
[BRAS-isp-dm1] authentication ipoe none
[BRAS-isp-dm1] authorization ipoe none
[BRAS-isp-dm1] accounting ipoe none
```

配置前域授权用户组和地址池。

```
[BRAS-isp-dm1] authorization-attribute user-group Web
[BRAS-isp-dm1] authorization-attribute ip-pool pool1
[BRAS-isp-dm1] authorization-attribute ipv6-nd-prefix-pool pool2
```

配置 Web 认证页面 URL。

```
[BRAS-isp-dm1] Web-server url http://www.h3c.web.com
[BRAS-isp-dm1] Web-server ipv6-url http://www.h3c.web.com
[BRAS-isp-dm1] quit
```

配置 IPoE 用户在 Web 认证阶段使用的认证域。

```
[BRAS] domain name dm2
[BRAS-isp-dm2] authentication ipoe radius-scheme rs1
[BRAS-isp-dm2] authorization ipoe radius-scheme rs1
[BRAS-isp-dm2] accounting ipoe radius-scheme rs1
[BRAS-isp-dm2] authorization-attribute user-profile car
[BRAS-isp-dm2] quit
```

9. 配置 IPoE

开启 IPoE 功能，并配置二层接入模式。

```
[BRAS] interface gigabitethernet 3/1/2
[BRAS-GigabitEthernet3/1/2] ip subscriber l2-connected enable
```

```
[BRAS-GigabitEthernet3/1/2] ip subscriber initiator ndrs enable
```

配置 IPoE 用户采用 Web MAC 认证方式。

```
[BRAS-GigabitEthernet3/1/2] ip subscriber authentication-method Web mac-auth
The operation may cut all users on this interface. Continue?[Y/N]:y
```

配置 IPoE 漫游功能。

```
[BRAS-GigabitEthernet3/1/2] ip subscriber roaming enable
```

配置 Web 认证前域为 dm1，Web 认证域和 Web MAC 认证域均为 dm2。

```
[BRAS-GigabitEthernet3/1/2] ip subscriber pre-auth domain dm1
[BRAS-GigabitEthernet3/1/2] ip subscriber Web-auth domain dm2
[BRAS-GigabitEthernet3/1/2] ip subscriber mac-auth domain dm2
[BRAS-GigabitEthernet3/1/2] quit
```

7.4.7 验证配置

用户认证前域认证通过之后，可以使用以下的显示命令查看 IPoE 用户在线信息，其中，用户获得的 IPv4 地址为 192.168.0.2，IPv6 地址为 192::2。

```
[BRAS] display ip subscriber session verbose
Basic:
  Description                 : -
  Username                    : 001b21a80949
  Authorization Domain        : dm1
  Authentication Domain       : dm1
  VPN instance                : N/A
  IP address                  : 192.168.0.2
  IPv6 ND Prefix              : 192::/64
  User address type           : N/A
  MAC address                 : 001b-21a8-0949
  Service-VLAN/Customer-VLAN  : -/-
  Access interface            : GE3/1/2
  User ID                     : 0x30000004
  VPI/VCI(for ATM)            : -/-
  VSI Index                   : -
  VSI link ID                 : -
  VXLAN ID                    : -
  DNS servers                 : N/A
  IPv6 DNS servers            : N/A
  DHCP lease                  : 86400 sec
  DHCP remain lease           : 86383 sec
  DHCPv6 lease                : N/A
  DHCPv6 remain lease         : N/A
  Access time                 : May 27 00:48:51 2018
  Online time(hh:mm:ss)       : 00:00:19
  Service node                : Slot 3 CPU 0
  Authentication type         : Web pre-auth
  IPv4 access type            : DHCP
  IPv6 access type            : NDRS
  IPv4 detect state           : Detecting
  IPv6 detect state           : Detecting
```

```
  State                          : Online

AAA:
  ITA policy name                : N/A
  IP pool                        : pool1
  IPv6 pool                      : N/A
  IPv6 nd preifx pool            : pool2
  Primary DNS server             : N/A
  Secondary DNS server           : N/A
  Primary IPv6 DNS server        : N/A
  Secondary IPv6 DNS server      : N/A
  Session idle cut               : N/A
  Session duration               : N/A, remaining: N/A
  Traffic quota                  : N/A
  Traffic remained               : N/A
  Acct start-fail action         : Online
  Acct update-fail action        : Online
  Acct quota-out action          : Offline
  Dual-stack accounting mode     : Merge
  Max IPv4 multicast addresses: 4
  IPv4 multicast address list : N/A
  Max IPv6 multicast addresses: 4
  IPv6 multicast address list : N/A
  Accounting start time          : May 27 00:48:51 2018
  Redirect URL                   : http://www.h3c.web.com
  Subscriber ID                  : -

QoS:
  User profile                   : N/A
  Session group profile          : N/A
  User group ACL                 : Web (active)
  Inbound CAR                    : N/A
  Outbound CAR                   : N/A
  Inbound user priority          : N/A
  Outbound user priority         : N/A

Flow statistic:
  Uplink   packets/bytes         : 0/0
  Downlink packets/bytes         : 0/0
  IPv6 uplink   packets/bytes : 0/0
  IPv6 downlink packets/bytes : 0/0
```

用户认证前域认证通过之后，登录 Web 页面，如图 8-16 所示。

图7-10 登录 Web 页面

在认证页面输入用户名和密码单击<上线>按钮进行 Web 认证，可以使用以下的显示命令查看 IPoE 用户在线信息。

```
[BRAS] display ip subscriber session verbose
Basic:
  Description                 : -
  Username                    : user1@dm2
  Authorization Domain        : dm1
  Authentication Domain       : dm1
  VPN instance                : N/A
  IP address                  : 192.168.0.2
  IPv6 ND Prefix              : 192::/64
  User address type           : N/A
  MAC address                 : 001b-21a8-0949
  Service-VLAN/Customer-VLAN  : -/-
  Access interface            : GE3/1/2
  User ID                     : 0x30000004
  VPI/VCI(for ATM)            : -/-
  VSI Index                   : -
  VSI link ID                 : -
  VXLAN ID                    : -
  DNS servers                 : N/A
  IPv6 DNS servers            : N/A
  DHCP lease                  : 86400 sec
  DHCP remain lease           : 86356 sec
  DHCPv6 lease                : N/A
  DHCPv6 remain lease         : N/A
  Access time                 : May 27 00:49:20 2018
```

```
  Online time(hh:mm:ss)       : 00:00:04
  Service node                : Slot 3 CPU 0
  Authentication type         : Web
  IPv4 access type            : DHCP
  IPv6 access type            : NDRS
  IPv4 detect state           : Detecting
  IPv6 detect state           : Detecting
  State                       : Online

AAA:
  ITA policy name             : N/A
  IP pool                     : pool1
  IPv6 pool                   : N/A
  IPv6 nd preifx pool         : pool2
  Primary DNS server          : N/A
  Secondary DNS server        : N/A
  Primary IPv6 DNS server     : N/A
  Secondary IPv6 DNS server   : N/A
  Session idle cut            : N/A
  Session duration            : 86400 sec, remaining: 86395 sec
  Traffic quota               : N/A
  Traffic remained            : N/A
  Acct start-fail action      : Online
  Acct update-fail action     : Online
  Acct quota-out action       : Offline
  Dual-stack accounting mode  : Merge
  Max IPv4 multicast addresses: 4
  IPv4 multicast address list : N/A
  Max IPv6 multicast addresses: 4
  IPv6 multicast address list : N/A
  Accounting start time       : May 27 00:49:20 2018
  Subscriber ID               : -

QoS:
  User profile                : car (active)
  Session group profile       : N/A
  User group ACL              : N/A
  Inbound CAR                 : N/A
  Outbound CAR                : N/A
  Inbound user priority       : N/A
  Outbound user priority      : N/A

Flow statistic:
  Uplink   packets/bytes      : 0/0
  Downlink packets/bytes      : 0/0
  IPv6 uplink   packets/bytes : 0/0
  IPv6 downlink packets/bytes : 0/0
```

7.4.8 配置文件

- DHCP 服务器：

```
#
 dhcp enable
#
 ipv6 dhcp server forbidden-address 192::1
#
dhcp server ip-pool pool1
 gateway-list 192.168.0.1
 network 192.168.0.0 mask 255.255.255.0
 forbidden-ip 192.168.0.1
#
interface GigabitEthernet3/1/1
 port link-mode route
 ip address 4.4.4.3 255.255.255.0
#
 ip route-static 192.168.0.0 24 4.4.4.2
#
```

- Router A（BRAS）：

```
#
 dhcp enable
 dhcp relay client-information record
 undo dhcp relay client-information refresh enable
#
 ipv6 dhcp prefix-pool 1 prefix 192::/48 assign-len 64
#
traffic classifier ip_cpu operator or
 if-match acl name ip
 if-match acl ipv6 name ip
#
traffic classifier ip_deny operator or
 if-match acl name ip
 if-match acl ipv6 name ip
#
traffic classifier neiwang operator or
 if-match acl name neiwang
 if-match acl ipv6 name neiwang
#
traffic classifier neiwang_out operator or
 if-match acl name neiwang_out
 if-match acl ipv6 name neiwang_out
#
traffic classifier Web_http operator or
 if-match acl name Web_http
 if-match acl ipv6 name Web_http
#
traffic classifier Web_https operator or
```

```
 if-match acl name Web_https
 if-match acl ipv6 name Web_https
#
traffic classifier Web_out operator or
 if-match acl name Web_out
 if-match acl ipv6 name Web_out
#
traffic classifier Web_permit operator or
 if-match acl name Web_permit
 if-match acl ipv6 name Web_permit
#
traffic behavior neiwang
 filter permit
#
traffic behavior neiwang_out
 filter permit
#
traffic behavior Web_cpu
 redirect cpu
#
traffic behavior Web_deny
 filter deny
 free account
#
traffic behavior Web_http
 redirect http-to-cpu
#
traffic behavior Web_https
 redirect https-to-cpu
#
traffic behavior Web_out
 filter permit
 free account
#
traffic behavior Web_permit
 filter permit
 free account
#
qos policy out
 classifier Web_out behavior Web_out
 classifier neiwang_out behavior neiwang_out
 classifier ip_deny behavior Web_deny
#
qos policy Web
 classifier Web_permit behavior Web_permit
 classifier neiwang behavior neiwang
 classifier Web_http behavior Web_http
 classifier Web_https behavior Web_https
```

```
 classifier ip_cpu behavior Web_cpu
 classifier ip_deny behavior Web_deny
#
interface GigabitEthernet3/1/1
 ip address 4.4.4.2 255.255.255.0
 ipv6 address 4::2/64
#
interface GigabitEthernet3/1/2
 port link-mode route
 dhcp select relay proxy
 dhcp flood-protection enable
 ipv6 dhcp flood-protection enable
 dhcp session-mismatch action fast-renew
 ipv6 dhcp session-mismatch action fast-renew
 ipv6 address auto link-local
 undo ipv6 nd ra halt
 ip subscriber l2-connected enable
 ip subscriber initiator ndrs enable
 ip subscriber authentication-method Web mac-auth
 ip subscriber roaming enable
 ip subscriber pre-auth domain dm1
 ip subscriber mac-auth domain dm2
 ip subscriber Web-auth domain dm2
#
 qos apply policy Web global inbound
 qos apply policy out global outbound
#
dhcp server ip-pool pool1
 gateway-list 192.168.0.1 export-route
 remote-server 4.4.4.3
#
ipv6 dhcp pool pool2
 prefix-pool 1 export-route
#
acl advanced name ip
 rule 0 permit ip user-group Web
#
acl advanced name neiwang
 rule 0 permit ip destination 4.4.4.6 0 user-group Web
#
acl advanced name neiwang_out
 rule 0 permit ip source 4.4.4.6 0 user-group Web
#
acl advanced name Web_http
 rule 0 permit tcp destination-port eq www user-group Web
#
acl advanced name Web_https
 rule 0 permit tcp destination-port eq 443 user-group Web
```

```
#
acl advanced name Web_out
 rule 0 permit ip source 4.4.4.5 0 user-group Web
#
acl advanced name Web_permit
 rule 0 permit ip destination 4.4.4.5 0 user-group Web
#
acl ipv6 advanced name ip
 rule 0 permit ipv6 user-group Web
#
acl ipv6 advanced name neiwang
 rule 0 permit ipv6 destination 4::6/128 user-group Web
#
acl ipv6 advanced name neiwang_out
 rule 0 permit ipv6 source 4::6/128 user-group Web
#
acl ipv6 advanced name Web_http
 rule 0 permit tcp destination-port eq www user-group Web
#
acl ipv6 advanced name Web_https
 rule 0 permit tcp destination-port eq 443 user-group Web
#
acl ipv6 advanced name Web_out
 rule 0 permit ipv6 source 4::5/128 user-group Web
#
acl ipv6 advanced name Web_permit
 rule 0 permit ipv6 destination 4::5/128 user-group Web
#
user-profile car
 qos car inbound any cir 5210 cbs 325625 ebs 0
#
radius scheme rs1
 primary authentication 4.4.4.1
 primary accounting 4.4.4.1
 key authentication cipher $c$3$FhQVcgn3kq1exL0CdTzatcgc9xF9vL3ZOw==
 key accounting cipher $c$3$ntIHBRM4ZkG+2JRZQTdKmNl0kYJmhZz5Zg==
 user-name-format without-domain
#
radius dynamic-author server
 client ip 4.4.4.1 key cipher $c$3$lYC2ERe8ts2gtE6M2xfoDDB8NmGw6J9v/Q==
#
domain name dm1
 authorization-attribute user-group Web
 authorization-attribute ip-pool pool1
 authorization-attribute ipv6-nd-prefix-pool pool2
 authentication ipoe none
 authorization ipoe none
 accounting ipoe none
```

```
 Web-server url http://www.h3c.web.com
 Web-server ipv6-url http://www.h3c.web.com
#
domain name dm2
 authorization-attribute user-profile car
 authentication ipoe radius-scheme rs1
 authorization ipoe radius-scheme rs1
 accounting ipoe radius-scheme rs1
#
user-group Web
#
portal server newpt1
 ip 4.4.4.5 key cipher $c$3$UnoFeLybwld9jDwLnHJQptDE7YZry2EVlw==
#
portal server newpt2
 ipv6 4::5 key cipher $c$3$HxisNWeML9fhYRS+7umwGbYwAkL+KGiCjw==
#
 http-redirect https-port 11111
#
```

8 IPoE 双栈用户普通 Web 认证配置举例(DHCPv6 方式)

在网络向 IPv6 演进的过程中，由于一段时间内，各种网络资源还没有全面支持 IPv6，因此需要以 IPv4、IPv6 双协议栈运行。本举例描述的是对 IPv4 和 IPv6 都做认证的部署场景，而且实现任意一个协议栈认证通过后，两个协议同时放行。

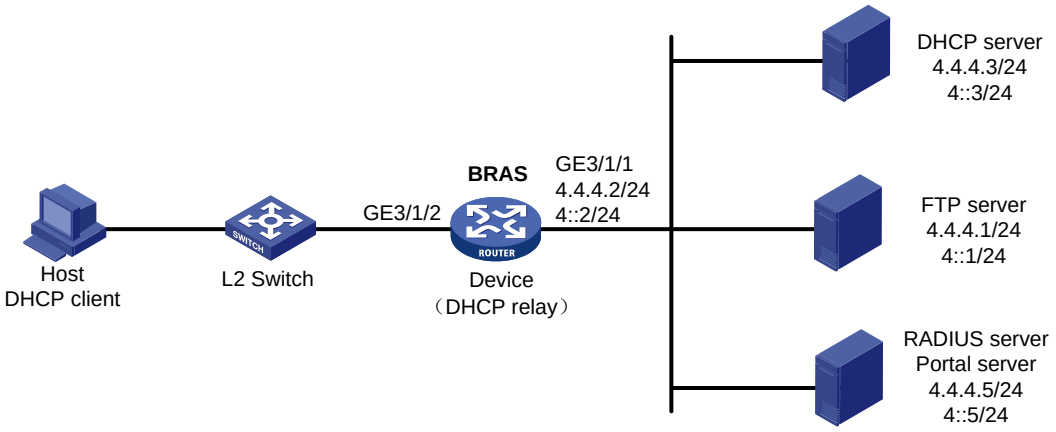
本举例使用 DHCPv6 来分配 IPv6 地址，这种方案更适合有线用户，因为安卓终端不支持 DHCPv6，也就不能获取 IPv6 地址访问 IPv6 网络资源。

8.1 组网需求

如图 8-1 所示：Device 为某学校的一台 BRAS 设备，为学校用户提供 IPoE 接入服务。要求：

- DHCP Client 经由二层网络以 IPoE 方式接入到 BRAS 接入设备。
- BRAS 接入设备作为 DHCP 中继向远端 DHCP 服务器申请 IP 地址。
- 由一台安装了 H3C iMC 的服务器同时承担 RADIUS 服务器、Portal 认证服务器和 Portal Web 服务器的职责。
- FTP server 是一台内网服务器。
- IPoE Web 认证通过后限速 5Mbps。

图8-1 IPoE 双栈用户普通 Web 认证配置组网图



8.2 配置思路

为了保证用户的带宽需求，本例通过授权 User Profile 进行速率控制。

IPoE Web 认证前域中的流量，区分 HTTP、HTTPS 和普通 IP 报文分别通过不同的队列上送。IPoE Web 认证中针对上送 CPU 的流量，配置如下三种类和流行为组来处理：

- 流分类匹配 HTTP 同时 User Group 为前域标记的，对应的流行为 **redirect http-to-cpu**。
- 流分类匹配 HTTPS 同时 User Group 为前域标记的，对应的流行为 **redirect https-to-cpu**。
- 流分类匹配 IP 同时 User Group 为前域标记的，对应的流行为 **deny**。

8.3 配置注意事项

本例中 DHCP Server 是由设备进行模拟，实际应用建议使用专门的 DHCP 服务器。

缺省情况下，未配置对 HTTPS 报文进行重定向的内部侦听端口号。需要通过 **http-redirect https-port** 命令用来配置对 HTTPS 报文进行重定向的侦听端口号，并且配置的侦听端口不要跟已有端口冲突。

本配置使用 DHCPv4 为终端分配 IPv4 地址，DHCPv6 为终端分配 IPv6 地址，并实现一次认证，双栈同时放行。但使用这种配置，安卓手机可能会无法获得 IPv6 地址。

当 BRAS 接入用户下线时，DHCP 中继需要查询中继用户地址表项，若存在对应表项，则会向 DHCP 服务器发送 Release 报文，通知 DHCP 服务器释放该地址租约。这就需要在 DHCP 中继上使用 **dhcp relay client-information record** 命令开启 DHCP 中继用户地址表项记录功能。

本配置中使用到限速私有属性，有关私有属性的详细介绍，请参见 14 附录。

8.4 配置步骤

8.4.1 配置 IP 地址及路由

按照图 8-1配置各接口的 IP 地址，并确保 BRAS 设备和各服务器之间路由可达，具体配置过程略。

8.4.2 设置 DNS 服务器

请正确设置 DNS 服务器，以便服务器可以根据 IPoE 双栈用户先上线的协议栈类型，解析出 Web 认证页面 http://www.h3c.web.com 对应的 IPv4 URL 地址或 IPv6 URL 地址。DNS 服务器具体设置过程略。

8.4.3 配置 DHCP 服务器

1. 配置 DHCPv4 地址池

开启 DHCP 服务。

```
<DHCP> system-view
[DHCP] dhcp enable
```

创建名称为 pool1 的 DHCPv4 地址池并进入其视图。

```
[DHCP] dhcp server ip-pool pool1
```

配置地址池动态分配的 IP 地址网段 192.168.0.0/24。

```
[DHCP-dhcp-pool-pool1] network 192.168.0.0 24
```

配置为用户分配的网关地址为 192.168.0.1。

```
[DHCP-dhcp-pool-pool1] gateway-list 192.168.0.1
```

将 192.168.0.1 设置为禁止地址。

```
[DHCP-dhcp-pool-pool1] forbidden-ip 192.168.0.1
[DHCP-dhcp-pool-pool1] quit
```

通过配置静态路由，将目的地址为 192.168.0.0 网段的 DHCPv4 应答报文的下一跳指定为连接 DHCPv4 客户端网络的接口 IPv4 地址 4.4.4.2。

```
[DHCP] ip route-static 192.168.0.0 24 4.4.4.2
```

2. 配置 DHCPv6 地址池

创建名称为 pool2 的 DHCPv6 地址池并进入其视图。

```
[DHCP] ipv6 dhcp pool pool2
```

配置地址池动态分配的 IPv6 地址网段 192::0/64。

```
[DHCP-dhcp6-pool-pool2] network 192::0/64
[DHCP-dhcp6-pool-pool2] quit
```

将 192::1 设置为禁止地址。

```
[DHCP] ipv6 dhcp server forbidden-address 192::1
```

配置接口 GigabitEthernet3/1/1 工作在 DHCPv6 服务器模式。

```
[DHCP] interface gigabitethernet 3/1/1
[DHCP-GigabitEthernet3/1/1] ipv6 dhcp select server
[DHCP-GigabitEthernet3/1/1] quit
```

通过配置静态路由，将目的地址为 192::0 网段的 DHCPv6 应答报文的下一跳指定为连接 DHCPv6 客户端网络的接口 IPv6 地址 4::2。

```
[DHCP] ipv6 route-static 192::0 64 4::2
```

8.4.4 配置 RADIUS 服务器

说明

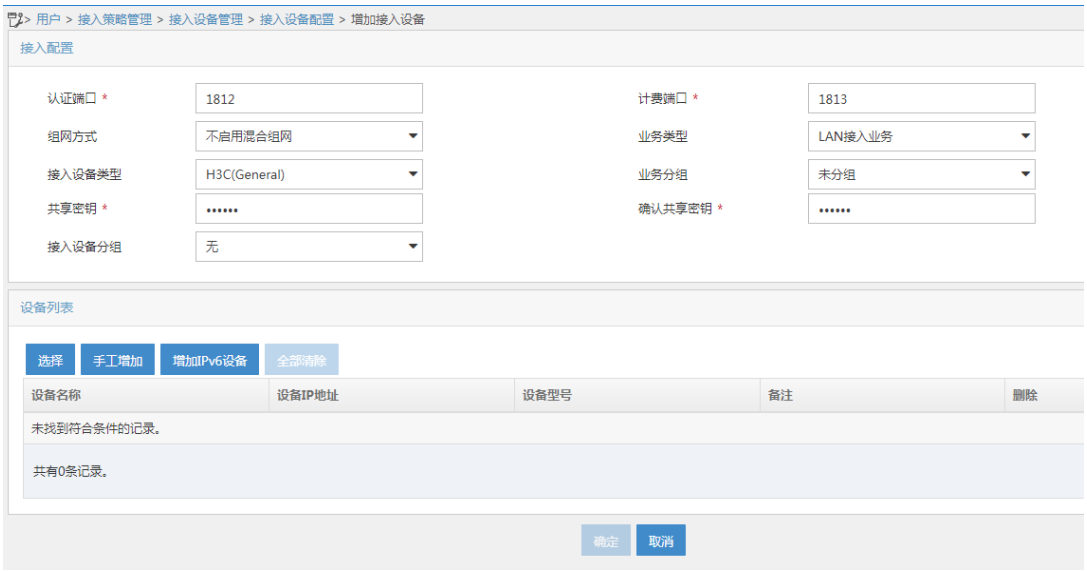
下面以 iMC（版本为 iMC PLAT 7.3 (E0705P02)）为例，说明 RADIUS 服务器的基本配置。不同 iMC 版本配置可能有所不同，具体配置请以实际版本及对应版本的 iMC 服务器手册为准，本节配置仅供参考。

(1) 配置接入设备

登录进入 iMC 管理平台，选择“用户”页签，单击导航树中的[接入策略管理/接入设备管理/接入设备配置]菜单项，进入接入设备配置页面，在该页面中单击<增加>按钮，进入如图 8-2 所示增加接入设备页面。

- 输入共享密钥为：radius。
- 其他采用缺省配置。

图8-2 增加接入设备



在该页面中设备列表下方单击<手工增加>，在如图 8-3 所示页面输入接入设备地址 4.4.4.2 并单击<确定>。

图8-3 手动增加接入设备

(2) 增加接入策略

单击导航树中的[接入策略管理/接入策略管理]菜单项，进入接入策略管理页面，在该页面中单击<增加>按钮，进入如图 8-4 所示增加接入策略页面。

- 输入接入策略名为：AccessPolicy。
- 其他采用缺省配置。

图8-4 增加接入策略

(3) 增加接入服务

单击导航树中的[接入策略管理/接入服务管理]菜单项，进入接入服务管理页面，在该页面中单击<增加>按钮，进入如图 8-5 所示增加接入服务页面。

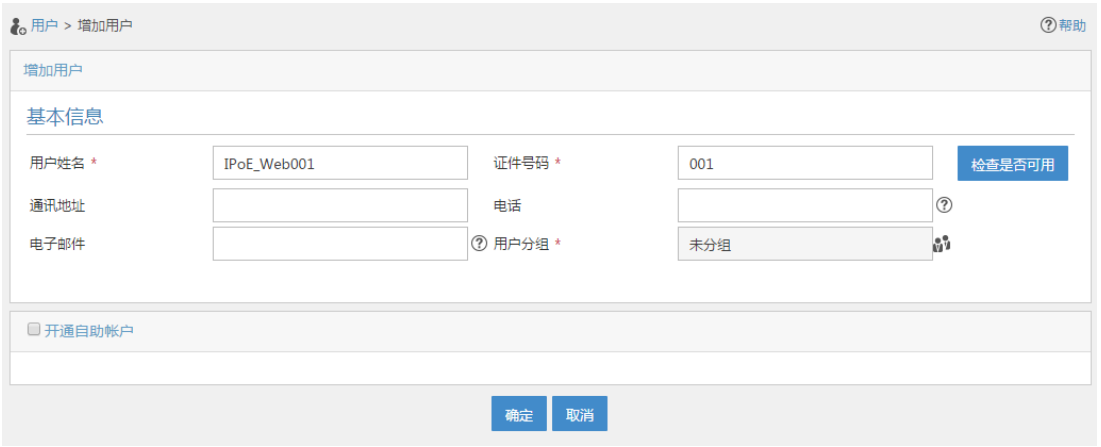
- 输入服务名为：IPoE_Server
- 缺省接入策略选择已创建的策略“AccessPolicy”。
- 其他采用缺省配置。

图8-5 增加接入服务

(4) 在 IMC 界面增加用户

单击导航树中的[用户管理/增加用户]菜单项，进入如图 8-6 所示增加用户页面，填写用户姓名和证件号码为：IPoE_Web001 和 001。

图8-6 增加用户



单击<确定>按钮后完成用户的添加。

(5) 增加接入用户

单击导航树中的[接入用户管理/接入用户]菜单项，进入接入用户页面，在该页面中单击<增加>按钮，进入如图 8-7 所示增加接入用户页面。

- 用户姓名选择：IPoE_Web001
- 账号名填写为：user1
- 密码为：pass1
- 接入服务选择之前已创建的 IPoE_Server

图8-7 增加接入用户

8.4.5 配置 Portal 服务器

说明

下面以 iMC（版本为 iMC PLAT 7.3 (E0705P02)）为例，说明 Portal 服务器的基本配置。不同 iMC 版本配置可能有所不同，具体配置请以实际版本及对应版本的 iMC 服务器手册为准，本节配置仅供参考。

(1) 配置 Portal 主页。

单击导航树中的[接入策略管理/Portal 服务管理/服务器配置]菜单项，进入服务器配置页面，配置 Portal 主页，采用缺省配置即可，并单击<确定>按钮完成操作，如图 8-8 所示。

图8-8 Portal 服务器配置页面

(2) 配置 Portal 认证的地址组范围

单击导航树中的[接入策略管理/Portal 服务管理/IP 地址组配置]菜单项，进入“IP 地址组配置”页面，在该页面中单击<增加>按钮，进入“增加 IP 地址组配置”页面，如图 8-9 所示。

- 输入 IP 地址组名为“IPoE_Web_User”；
- 输入起始地址为“192.168.0.1”、终止地址为“192.168.0.255”。用户主机 IP 地址必须包含在该 IP 地址组范围内；
- 其他采用缺省配置；
- 单击<确定>按钮完成操作。

图8-9 增加 IP 地址组配置页面（IPv4）

如图 8-10 所示，继续上述操作添加 IPv6 地址组。

- 输入 IP 地址组名为“IPoE_Web_User-2”；
- IPv6 选项框选择“是”；

- 输入起始地址为“192::1”、终止地址为“192::FFFF”。用户主机 IPv6 地址必须包含在该 IP 地址组范围内；
- 其他采用缺省配置；
- 单击<确定>按钮完成操作。

图8-10 增加 IP 地址组配置页面（IPv6）

(3) 增加 Portal 接入设备信息

单击导航树中的[接入策略管理/Portal 服务管理/设备配置]菜单项，进入“设备配置”页面，在该页面中单击<增加>按钮，进入“增加设备信息”页面，如图 8-11 所示。

- 输入设备名为“NAS”；
- 输入 IP 地址为“4.4.4.2”，该地址为 Portal 报文出接口 GigabitEthernet3/1/1 的 IP 地址；
- 输入密钥为“123456”；
- 选择组网方式为“直连”；
- 其它参数采用缺省值，并单击<确定>按钮完成操作。

图8-11 增加设备信息配置页面（IPv4）

如图 8-12 所示，继续上述操作添加设备的 IPv6 信息。

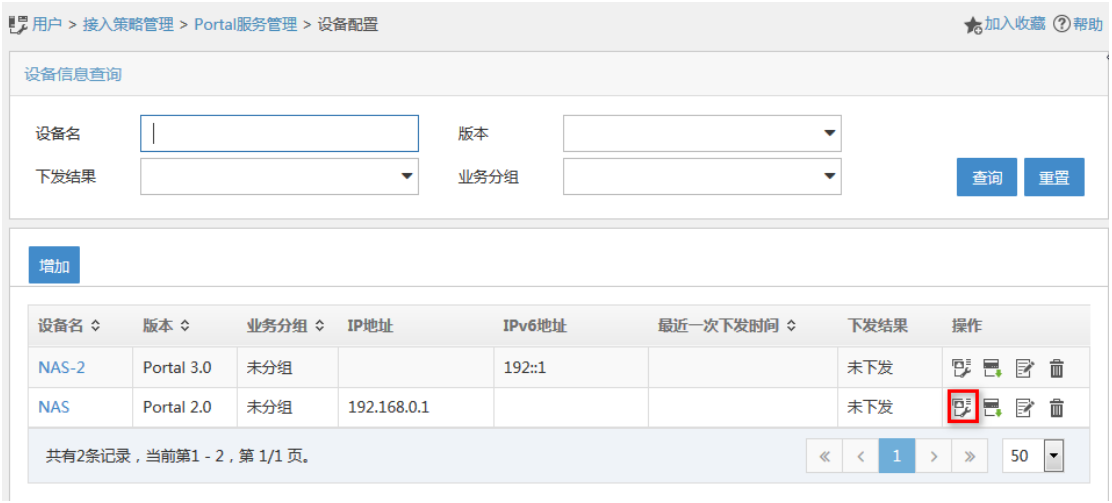
- 输入设备名为“NAS-2”；
- 版本选择“Portal 3.0”；
- 输入 IP 地址为“4::2”，该地址为 Portal 报文出接口 GigabitEthernet3/1/1 的 IP 地址；
- 输入密钥为“123456”；
- 选择组网方式为“直连”；
- 其它参数采用缺省值，并单击<确定>按钮完成操作。

图8-12 增加设备信息配置页面（IPv6）

(4) 配置端口组信息

如图 8-13 所示返回[接入策略管理/Portal 服务管理/设备配置]菜单项，单击<端口组信息管理>按钮，进入“端口组信息配置”页面。

图8-13 设备信息列表



在“端口组信息配置”页面中单击<增加>按钮，进入“增加端口组信息”页面，如图 8-14 所示。

- 输入端口组名为“group”；
- 选择 IP 地址组为“IPoE_Web_User”，用户接入网络时使用的 IP 地址必须属于所选的 IP 地址组；
- 其它参数采用缺省值，并单击<确定>按钮完成操作。

图8-14 增加端口组信息配置页面（IPv4）

如图 8-15 所示，继续上述操作添加端口组的 IPv6 信息。

- 输入端口组名为“group-2”；
- 选择 IP 地址组为“IPoE_Web_User-2”，用户接入网络时使用的 IPv6 地址必须属于所选的 IPv6 地址组；
- 其它参数采用缺省值，并单击<确定>按钮完成操作。

图8-15 增加端口组信息配置页面（IPv6）

8.4.6 配置 BRAS

1. 配置 DHCP 中继

全局开启 DHCP。

```
[BRAS] dhcp enable
```

启用 DHCP 中继的用户地址表项记录功能。

```
[BRAS] dhcp relay client-information record
```

关闭 DHCP 中继动态用户地址表项定时刷新功能。

```
[BRAS] undo dhcp relay client-information refresh enable
```

创建中继地址池 pool1，指定匹配该地址池的 DHCPv4 客户端所在的网段地址，并指定中继地址池对应的 DHCP 服务器地址。

```
[BRAS] dhcp server ip-pool pool1
[BRAS-dhcp-pool-pool1] gateway-list 192.168.0.1 export-route
[BRAS-dhcp-pool-pool1] remote-server 4.4.4.3
[BRAS-dhcp-pool-pool1] quit
```

创建中继地址池 pool2，指定匹配该地址池的 DHCPv6 客户端所在的网段地址，并指定中继地址池对应的 DHCP 服务器地址。

```
[BRAS] ipv6 dhcp pool pool2
[BRAS-dhcp6-pool-pool2] gateway-list 192::1
[BRAS-dhcp6-pool-pool2] remote-server 4::3
[BRAS-dhcp6-pool-pool2] quit
```

配置接口工作在 DHCPv4 中继模式。

```
[BRAS] interface gigabitethernet 3/1/2
[BRAS-GigabitEthernet3/1/2] dhcp select relay proxy
```

配置自动生成 IPv6 链路本地地址，该 IPv6 链路本地地址作为用户的网关。

```
[BRAS-GigabitEthernet3/1/2] ipv6 address auto link-local
```

配置接口工作在 DHCPv6 中继模式，开启 DHCPv6 中继用户表项记录功能。

```
[BRAS-GigabitEthernet3/1/2] ipv6 dhcp select relay
```

```
[BRAS-GigabitEthernet3/1/2] ipv6 dhcp relay client-information record
[BRAS-GigabitEthernet3/1/2] ipv6 dhcp relay release-agent
```

配置 DHCP 防攻击功能。

```
[BRAS-GigabitEthernet3/1/2] dhcp flood-protection enable
[BRAS-GigabitEthernet3/1/2] ipv6 dhcp flood-protection enable
```

配置清除用户表项时通知 DHCPv6 服务器释放租约。

```
[BRAS-GigabitEthernet3/1/2] ipv6 dhcp relay release-agent
```

取消设备发布 RA 消息的抑制。配置被管理地址的配置标志位为 1，即主机通过 DHCPv6 服务器获取 IPv6 地址。配置其他信息配置标志位为 1，即主机通过 DHCPv6 服务器获取除 IPv6 地址以外的其他信息

```
[BRAS-GigabitEthernet3/1/2] undo ipv6 nd ra halt
[BRAS-GigabitEthernet3/1/2] ipv6 nd autoconfig managed-address-flag
[BRAS-GigabitEthernet3/1/2] ipv6 nd autoconfig other-flag
```

配置漫游时重新分配地址功能。

```
[BRAS-GigabitEthernet3/1/2] dhcp session-mismatch action fast-renew
[BRAS-GigabitEthernet3/1/2] ipv6 dhcp session-mismatch action fast-renew
```

2. 配置 Portal 认证服务器

配置 IPv4 Portal 认证服务器：名称为 newpt1，IP 地址为 4.4.4.5，密钥为明文 123456。

```
[BRAS] portal server newpt1
[BRAS-portal-server-newpt1] ip 4.4.4.5 key simple 123456
[BRAS-portal-server-newpt1] quit
```

配置 IPv6 Portal 认证服务器：名称为 newpt2，IPv6 地址为 4::5，密钥为明文 123456。

```
[BRAS] portal server newpt2
[BRAS-portal-server-newpt2] ipv6 4::5 key simple 123456
[BRAS-portal-server-newpt2] quit
```

3. 配置 HTTPS 的内部侦听端口

配置 HTTPS 的内部侦听端口，端口不要跟已有端口冲突即可。

```
[BRAS] http-redirect https-port 11111
```

4. 创建本地用户组

创建认证前域用户组，名称为 Web。

```
[BRAS] user-group Web
New user group added.
[BRAS-ugroup-Web] quit
```

5. 配置 QoS

(1)　配置用于认证前域用户的 ACL 规则

分别为 IPv4 和 IPv6 高级 ACL Web_permit 创建规则如下：匹配用户组 Web 中用户的目的地址为 Portal 服务器地址的报文。

```
[BRAS] acl advanced name Web_permit
[BRAS-acl-ipv4-adv-Web_permit] rule 0 permit ip destination 4.4.4.5 0 user-group Web
[BRAS-acl-ipv4-adv-Web_permit] quit
[BRAS] acl ipv6 advanced name Web_permit
[BRAS-acl-ipv6-adv-Web_permit] rule 0 permit ipv6 destination 4::5 128 user-group Web
[BRAS-acl-ipv6-adv-Web_permit] quit
```

分别为 IPv4 和 IPv6 高级 ACL neiwang 创建规则如下：匹配用户组 Web 中用户的目的地址为内网服务器地址的报文。

```
[BRAS] acl advanced name neiwang
[BRAS-acl-ipv4-adv-neiwang] rule 0 permit ip destination 4.4.4.1 0 user-group Web
[BRAS-acl-ipv4-adv-neiwang] quit
[BRAS] acl ipv6 advanced name neiwang
[BRAS-acl-ipv6-adv-neiwang] rule 0 permit ipv6 destination 4::1 128 user-group Web
[BRAS-acl-ipv6-adv-neiwang] quit
```

分别为 IPv4 和 IPv6 高级 ACL Web_http 创建规则如下：匹配用户组 Web 中用户的目的端口为 80 的 TCP 报文(即 HTTP 报文)。

```
[BRAS] acl advanced name Web_http
[BRAS-acl-ipv4-adv-Web_http] rule 0 permit tcp destination-port eq www user-group Web
[BRAS-acl-ipv4-adv-Web_http] quit
[BRAS] acl ipv6 advanced name Web_http
[BRAS-acl-ipv6-adv-Web_http] rule 0 permit tcp destination-port eq www user-group Web
[BRAS-acl-ipv6-adv-Web_http] quit
```

分别为 IPv4 和 IPv6 高级 ACL Web_https 创建规则如下：匹配用户组 Web 中用户的目的端口为 443 的 TCP 报文(即 HTTPS 报文)。

```
[BRAS] acl advanced name Web_https
[BRAS-acl-ipv4-adv-Web_https] rule 0 permit tcp destination-port eq 443 user-group Web
[BRAS-acl-ipv4-adv-Web_https] quit
[BRAS] acl ipv6 advanced name Web_https
[BRAS-acl-ipv6-adv-Web_https] rule 0 permit tcp destination-port eq 443 user-group Web
[BRAS-acl-ipv6-adv-Web_https] quit
```

分别为 IPv4 和 IPv6 高级 ACL ip 创建规则如下：匹配用户组 Web 中用户的 IP 报文。

```
[BRAS] acl advanced name ip
[BRAS-acl-ipv4-adv-ip] rule 0 permit ip user-group Web
[BRAS-acl-ipv4-adv-ip] quit
[BRAS] acl ipv6 advanced name ip
[BRAS-acl-ipv6-adv-ip] rule 0 permit ipv6 user-group Web
[BRAS-acl-ipv6-adv-ip] quit
```

分别为 IPv4 和 IPv6 高级 ACL neiwang_out 创建规则如下：匹配用户组 Web 中源地址为内网服务器 IP 地址的报文。

```
[BRAS] acl advanced name neiwang_out
[BRAS-acl-ipv4-adv-neiwang_out] rule 0 permit ip source 4.4.4.1 0 user-group Web
[BRAS-acl-ipv4-adv-neiwang_out] quit
[BRAS] acl ipv6 advanced name neiwang_out
[BRAS-acl-ipv6-adv-neiwang_out] rule 0 permit ipv6 source 4::1 128 user-group Web
[BRAS-acl-ipv6-adv-neiwang_out] quit
```

分别为 IPv4 和 IPv6 高级 ACL Web_out 创建规则如下：匹配用户组 Web 中源地址为 Portal 服务器 IP 地址的报文。

```
[BRAS] acl advanced name Web_out
[BRAS-acl-ipv4-adv-Web_out] rule 0 permit ip source 4.4.4.5 0 user-group Web
[BRAS-acl-ipv4-adv-Web_out] quit
[BRAS] acl ipv6 advanced name Web_out
[BRAS-acl-ipv6-adv-Web_out] rule 0 permit ipv6 source 4::5 128 user-group Web
```

```
[BRAS-acl-ipv6-adv-Web_out] quit
```

(2) 配置用于认证前域用户的类

配置类 Web_permit，匹配 ACL Web_permit。

```
[BRAS] traffic classifier Web_permit operator or
[BRAS-classifier-Web_permit] if-match acl name Web_permit
[BRAS-classifier-Web_permit] if-match acl ipv6 name Web_permit
[BRAS-classifier-Web_permit] quit
```

配置类 neiwang，匹配 ACL neiwang。

```
[BRAS] traffic classifier neiwang operator or
[BRAS-classifier-neiwang] if-match acl name neiwang
[BRAS-classifier-neiwang] if-match acl ipv6 name neiwang
[BRAS-classifier-neiwang] quit
```

配置类 Web_http，匹配 ACL Web_http。

```
[BRAS] traffic classifier Web_http operator or
[BRAS-classifier-Web_http] if-match acl name Web_http
[BRAS-classifier-Web_http] if-match acl ipv6 name Web_http
[BRAS-classifier-Web_http] quit
```

配置类 Web_https，匹配 ACL Web_https。

```
[BRAS] traffic classifier Web_https operator or
[BRAS-classifier-Web_https] if-match acl name Web_https
[BRAS-classifier-Web_https] if-match acl ipv6 name Web_https
[BRAS-classifier-Web_https] quit
```

配置类 Web_deny，匹配 ACL ip。

```
[BRAS] traffic classifier Web_deny operator or
[BRAS-classifier-Web_deny] if-match acl name ip
[BRAS-classifier-Web_deny] if-match acl ipv6 name ip
[BRAS-classifier-Web_deny] quit
```

配置类 neiwang_out，匹配 ACL neiwang_out。

```
[BRAS] traffic classifier neiwang_out operator or
[BRAS-classifier-neiwang_out] if-match acl name neiwang_out
[BRAS-classifier-neiwang_out] if-match acl ipv6 name neiwang_out
[BRAS-classifier-neiwang_out] quit
```

配置类 Web_out，匹配 ACL Web_out。

```
[BRAS] traffic classifier Web_out operator or
[BRAS-classifier-Web_out] if-match acl name Web_out
[BRAS-classifier-Web_out] if-match acl ipv6 name Web_out
[BRAS-classifier-Web_out] quit
```

(3) 配置流行为

配置流行为 Web_permit，允许用户组 Web 中用户的目的地址为 Portal 服务器 IP 地址的报文通过。

```
[BRAS] traffic behavior Web_permit
[BRAS-behavior-Web_permit] filter permit
[BRAS-behavior-Web_permit] free account
[BRAS-behavior-Web_permit] quit
```

配置流行为 neiwang，允许用户组 Web 中用户的目的地址为内网服务器 IP 地址的报文通过。

```
[BRAS] traffic behavior neiwang
[BRAS-behavior-neiwang] filter permit
[BRAS-behavior-neiwang] quit
```

配置流行为 Web_http，对用户组 Web 中用户的目的端口为 80 的 TCP 报文(即 HTTP 报文)重定向到 CPU。

```
[BRAS] traffic behavior Web_http
[BRAS-behavior-Web_http] redirect http-to-cpu
[BRAS-behavior-Web_http] quit
```

配置流行为 Web_https，对用户组 Web 中用户的目的端口为 443 的 TCP 报文(即 HTTPS 报文)重定向到 CPU。

```
[BRAS] traffic behavior Web_https
[BRAS-behavior-Web_https] redirect https-to-cpu
[BRAS-behavior-Web_https] quit
```

配置流行为 Web_deny，禁止用户组 Web 中用户的所有 IP 报文通过。

```
[BRAS] traffic behavior Web_deny
[BRAS-behavior-Web_deny] filter deny
[BRAS-behavior-Web_deny] free account
[BRAS-behavior-Web_deny] quit
```

配置流行为 neiwang_out，允许用户组 Web 中源地址为内网服务器 IP 地址的报文通过。

```
[BRAS] traffic behavior neiwang_out
[BRAS-behavior-neiwang_out] filter permit
[BRAS-behavior-neiwang_out] quit
```

配置流行为 Web_out，允许用户组 Web 中源地址为 Portal 服务器 IP 地址的报文通过。

```
[BRAS] traffic behavior Web_out
[BRAS-behavior-Web_out] filter permit
[BRAS-behavior-Web_out] free account
[BRAS-behavior-Web_out] quit
```

(4) 配置 QoS 策略

配置入方向 QoS 策略 Web

```
[BRAS] qos policy Web
```

为类指定对应的流行为，规则为对于用户组 Web 中的用户：

允许目的地址为 Portal 服务器和内网服务器 IP 地址的报文通过；

对于目的端口为 80（HTTP 报文）和 443（HTTPS 报文）的报文重定向到 CPU；

除上述报文外，其余报文均禁止通过。

```
[BRAS-qospolicy-Web] classifier Web_permit behavior Web_permit
[BRAS-qospolicy-Web] classifier neiwang behavior neiwang
[BRAS-qospolicy-Web] classifier Web_http behavior Web_http
[BRAS-qospolicy-Web] classifier Web_https behavior Web_https
[BRAS-qospolicy-Web] classifier Web_deny behavior Web_deny
[BRAS-qospolicy-Web] quit
```

配置出方向 QoS 策略 out

```
[BRAS] qos policy out
```

为类指定对应的流行为，规则为：允许用户组 Web 中源地址为 Portal 服务器和内网服务器 IP 地址的报文通过，其余报文均禁止通过。

```
[BRAS-qospolicy-out] classifier neiwang_out behavior neiwang_out
[BRAS-qospolicy-out] classifier Web_out behavior Web_out
[BRAS-qospolicy-out] classifier Web_deny behavior Web_deny
[BRAS-qospolicy-out] quit
```

(5) 配置应用策略

对接收的用户流量应用 QoS 策略，策略名为 Web。

```
[BRAS] qos apply policy Web global inbound
```

对发送的上线用户流量应用 QoS 策略，策略名为 out。

```
[BRAS] qos apply policy out global outbound
```

(6) 查看应用的策略是否生效

查看入方向 QoS 策略的配置信息和运行情况。

```
[BRAS] display qos policy global slot 3 inbound
  Direction: Inbound
  Policy: Web
   Classifier: Web_permit
     Operator: OR
     Rule(s) :
      If-match acl name Web_permit
      If-match acl ipv6 name Web_permit
     Behavior: Web_permit
      Filter enable: Permit
      Free account enable
   Classifier: neiwang
     Operator: OR
     Rule(s) :
      If-match acl name neiwang
      If-match acl ipv6 name neiwang
     Behavior: neiwang
      Filter enable: Permit
   Classifier: Web_http
     Operator: OR
     Rule(s) :
      If-match acl name Web_http
      If-match acl ipv6 name Web_http
     Behavior: Web_http
      Redirecting:
        Redirect http to CPU
   Classifier: Web_https
     Operator: OR
     Rule(s) :
      If-match acl name Web_https
      If-match acl ipv6 name Web_https
     Behavior: Web_https
      Redirecting:
        Redirect https to CPU
   Classifier: Web_deny
     Operator: OR
```

```
    Rule(s) :
     If-match acl name ip
     If-match acl ipv6 name ip
    Behavior: Web_deny
     Filter enable: Deny
     Free account enable
```

查看出方向 QoS 策略的配置信息和运行情况。

```
[BRAS] display qos policy global slot 3 outbound
  Direction: Outbound
  Policy: out
   Classifier: neiwang_out
     Operator: OR
     Rule(s) :
      If-match acl name neiwang_out
      If-match acl ipv6 name neiwang_out
     Behavior: neiwang_out
      Filter enable: Permit
   Classifier: Web_out
     Operator: OR
     Rule(s) :
      If-match acl name Web_out
      If-match acl ipv6 name Web_out
     Behavior: Web_out
      Filter enable: Permit
      Free account enable
   Classifier: Web_deny
     Operator: OR
     Rule(s) :
      If-match acl name ip
      If-match acl ipv6 name ip
     Behavior: Web_deny
      Filter enable: Deny
      Free account enable
```

6. 配置 RADIUS 方案

创建名称为 rs1 的 RADIUS 方案并进入该方案视图。

```
[BRAS] radius scheme rs1
```

配置 RADIUS 方案的主认证和主计费服务器及其通信密钥。

```
[BRAS-radius-rs1] primary authentication 4.4.4.5
[BRAS-radius-rs1] primary accounting 4.4.4.5
[BRAS-radius-rs1] key authentication simple radius
[BRAS-radius-rs1] key accounting simple radius
```

配置发送给 RADIUS 服务器的用户名不携带 ISP 域名。

```
[BRAS-radius-rs1] user-name-format without-domain
[BRAS-radius-rs1] quit
```

设置 RADIUS DAE 客户端的 IP 地址为 4.4.4.5，与 RADIUS DAE 客户端交互 DAE 报文时使用的共享密钥为明文 radius，需要注意的是认证两端明文密钥需要一致。

```
[BRAS] radius dynamic-author server
[BRAS-radius-da-server] client ip 4.4.4.5 key simple radius
[BRAS-radius-da-server] quit
```

7. 配置 User Profile

配置名称为 car 的 User Profile 对上线用户发送的报文进行流量监管。报文正常流速为 5210kbps，允许 325625byte 的突发流量通过，速率小于等于 5210kbps 时正常发送，大于 5210kbps 时，报文被丢弃。

```
[BRAS] user-profile car
[BRAS-user-profile-car] qos car inbound any cir 5210 cbs 325625
[BRAS-user-profile-car] quit
```

8. 配置认证前域和 Web 认证域

配置 IPoE 用户认证前使用的认证域。

```
[BRAS] domain name dm1
[BRAS-isp-dm1] authentication ipoe none
[BRAS-isp-dm1] authorization ipoe none
[BRAS-isp-dm1] accounting ipoe none
```

配置前域授权用户组和地址池。

```
[BRAS-isp-dm1] authorization-attribute user-group Web
[BRAS-isp-dm1] authorization-attribute ip-pool pool1
[BRAS-isp-dm1] authorization-attribute ipv6-pool pool2
```

配置 Web 认证页面 URL。

```
[BRAS-isp-dm1] Web-server url http://www.h3c.web.com
[BRAS-isp-dm1] Web-server ipv6-url http://www.h3c.web.com
[BRAS-isp-dm1] quit
```

配置 IPoE 用户在 Web 认证阶段使用的认证域。

```
[BRAS] domain name dm2
[BRAS-isp-dm2] authentication ipoe radius-scheme rs1
[BRAS-isp-dm2] authorization ipoe radius-scheme rs1
[BRAS-isp-dm2] accounting ipoe radius-scheme rs1
[BRAS-isp-dm2] authorization-attribute user-profile car
[BRAS-isp-dm2] quit
```

9. 配置 IPoE

开启 IPoE 功能，并配置二层接入模式。

```
[BRAS] interface gigabitethernet 3/1/2
[BRAS-GigabitEthernet3/1/2] ip subscriber l2-connected enable
```

配置 IPoE 用户采用 Web 认证方式。

```
[BRAS-GigabitEthernet3/1/2] ip subscriber authentication-method Web
The operation may cut all users on this interface. Continue?[Y/N]:y
```

配置 Web 认证前域为 dm1，Web 认证域为 dm2。

```
[BRAS-GigabitEthernet3/1/2] ip subscriber pre-auth domain dm1
[BRAS-GigabitEthernet3/1/2] ip subscriber Web-auth domain dm2
[BRAS-GigabitEthernet3/1/2] quit
```

8.4.7 验证配置

用户认证前域认证通过之后，可以使用以下的显示命令查看 IPoE 用户在线信息，其中，用户获得的 IPv4 地址为 192.168.0.2，IPv6 地址为 192::2。

```
[BRAS] display ip subscriber session verbose
Basic:
  Description                 : -
  Username                    : 001b21a80949
  Domain                      : dm1
  VPN instance                : N/A
  IP address                  : 192.168.0.2
  IPv6 address                : 192::2
  User address type           : N/A
  MAC address                 : 001b-21a8-0949
  Service-VLAN/Customer-VLAN  : -/-
  Access interface            : GE3/1/2
  User ID                     : 0x30000004
  VPI/VCI(for ATM)            : -/-
  VSI Index                   : -
  VSI link ID                 : -
  VXLAN ID                    : -
  DNS servers                 : N/A
  IPv6 DNS servers            : N/A
  DHCP lease                  : 86400 sec
  DHCP remain lease           : 86383 sec
  DHCPv6 lease                : 2592000 sec
  DHCPv6 remain lease         : 2591981 sec
  Access time                 : May 27 00:48:51 2018
  Online time(hh:mm:ss)       : 00:00:19
  Service node                : Slot 3 CPU 0
  Authentication type         : Web pre-auth
  IPv4 access type            : DHCP
  IPv6 access type            : DHCP
  IPv4 detect state           : Detecting
  IPv6 detect state           : Detecting
  State                       : Online

AAA:
  ITA policy name             : N/A
  IP pool                     : pool1
  IPv6 pool                   : pool2
  IPv6 nd preifx pool         : N/A
  Primary DNS server          : N/A
  Secondary DNS server        : N/A
  Primary IPv6 DNS server     : N/A
  Secondary IPv6 DNS server   : N/A
  Session idle cut            : N/A
  Session duration            : N/A, remaining: N/A
```

```
  Traffic quota               : N/A
  Traffic remained            : N/A
  Acct start-fail action      : Online
  Acct update-fail action     : Online
  Acct quota-out action       : Offline
  Dual-stack accounting mode  : Merge
  Max IPv4 multicast addresses: 4
  IPv4 multicast address list : N/A
  Max IPv6 multicast addresses: 4
  IPv6 multicast address list : N/A
  Accounting start time       : May 27 00:48:51 2018
  Redirect URL                : http://www.h3c.web.com
  Subscriber ID               : -

QoS:
  User profile                : N/A
  Session group profile       : N/A
  User group ACL              : Web (active)
  Inbound CAR                 : N/A
  Outbound CAR                : N/A
  Inbound user priority       : N/A
  Outbound user priority      : N/A

Flow statistic:
  Uplink   packets/bytes      : 0/0
  Downlink packets/bytes      : 0/0
  IPv6 uplink   packets/bytes : 0/0
  IPv6 downlink packets/bytes : 0/0
```

用户认证前域认证通过之后，登录 Web 页面，如图 8-16 所示。

图8-16 登录 Web 页面

在认证页面输入用户名和密码单击<上线>按钮进行 Web 认证，可以使用以下的显示命令查看 IPoE 用户在线信息。

```
[BRAS] display ip subscriber session verbose
Basic:
  Description                 : -
  Username                    : user1@dm2
  Domain                      : dm2
  VPN instance                : N/A
  IP address                  : 192.168.0.2
  IPv6 address                : 192::2
  User address type           : N/A
  MAC address                 : 001b-21a8-0949
  Service-VLAN/Customer-VLAN  : -/-
  Access interface            : GE3/1/2
  User ID                     : 0x30000004
  VPI/VCI(for ATM)            : -/-
  VSI Index                   : -
  VSI link ID                 : -
  VXLAN ID                    : -
  DNS servers                 : N/A
  IPv6 DNS servers            : N/A
  DHCP lease                  : 86400 sec
  DHCP remain lease           : 86356 sec
  DHCPv6 lease                : 2592000 sec
  DHCPv6 remain lease         : 2591954 sec
  Access time                 : May 27 00:48:51 2018
  Online time(hh:mm:ss)       : 00:00:04
```

```
  Service node                : Slot 3 CPU 0
  Authentication type         : Web
  IPv4 access type            : DHCP
  IPv6 access type            : DHCP
  IPv4 detect state           : Detecting
  IPv6 detect state           : Detecting
  State                       : Online

AAA:
  ITA policy name             : N/A
  IP pool                     : pool1
  IPv6 pool                   : pool2
  IPv6 nd preifx pool         : N/A
  Primary DNS server          : N/A
  Secondary DNS server        : N/A
  Primary IPv6 DNS server     : N/A
  Secondary IPv6 DNS server   : N/A
  Session idle cut            : N/A
  Session duration            : 86400 sec, remaining: 86395 sec
  Traffic quota               : N/A
  Traffic remained            : N/A
  Acct start-fail action      : Online
  Acct update-fail action     : Online
  Acct quota-out action       : Offline
  Dual-stack accounting mode  : Merge
  Max IPv4 multicast addresses: 4
  IPv4 multicast address list : N/A
  Max IPv6 multicast addresses: 4
  IPv6 multicast address list : N/A
  Accounting start time       : May 27 00:49:32 2018
  Subscriber ID               : -

QoS:
  User profile                : car (active)
  Session group profile       : N/A
  User group ACL              : N/A
  Inbound CAR                 : N/A
  Outbound CAR                : N/A
  Inbound user priority       : N/A
  Outbound user priority      : N/A

Flow statistic:
  Uplink   packets/bytes      : 0/0
  Downlink packets/bytes      : 0/0
  IPv6 uplink   packets/bytes : 0/0
  IPv6 downlink packets/bytes : 0/0
```

8.4.8 配置文件

- DHCP 服务器：

```
#
 dhcp enable
#
 ipv6 dhcp server forbidden-address 192::1
#
dhcp server ip-pool pool1
 gateway-list 192.168.0.1
 network 192.168.0.0 mask 255.255.255.0
 forbidden-ip 192.168.0.1
#
ipv6 dhcp pool pool2
 network 192::/64
#
interface GigabitEthernet3/1/1
 port link-mode route
 ip address 4.4.4.3 255.255.255.0
 ipv6 dhcp select server
 ipv6 address 4::3/64
#
 ip route-static 192.168.0.0 24 4.4.4.2
 ipv6 route-static 192:: 64 4::2
#
```

- Router A（BRAS）：

```
#
 dhcp enable
 dhcp relay client-information record
 undo dhcp relay client-information refresh enable
#
traffic classifier neiwang operator or
 if-match acl name neiwang
 if-match acl ipv6 name neiwang
#
traffic classifier neiwang_out operator or
 if-match acl name neiwang_out
 if-match acl ipv6 name neiwang_out
#
traffic classifier Web_deny operator or
 if-match acl name ip
 if-match acl ipv6 name ip
#
traffic classifier Web_http operator or
 if-match acl name Web_http
 if-match acl ipv6 name Web_http
#
traffic classifier Web_https operator or
```

```
 if-match acl name Web_https
 if-match acl ipv6 name Web_https
#
traffic classifier Web_out operator or
 if-match acl name Web_out
 if-match acl ipv6 name Web_out
#
traffic classifier Web_permit operator or
 if-match acl name Web_permit
 if-match acl ipv6 name Web_permit
#
traffic behavior neiwang
 filter permit
#
traffic behavior neiwang_out
 filter permit
#
traffic behavior Web_deny
 filter deny
 free account
#
traffic behavior Web_http
 redirect http-to-cpu
#
traffic behavior Web_https
 redirect https-to-cpu
#
traffic behavior Web_out
 filter permit
 free account
#
traffic behavior Web_permit
 filter permit
 free account
#
qos policy out
 classifier Web_out behavior Web_out
 classifier neiwang_out behavior neiwang_out
 classifier Web_deny behavior Web_deny
#
qos policy Web
 classifier Web_permit behavior Web_permit
 classifier neiwang behavior neiwang
 classifier Web_http behavior Web_http
 classifier Web_https behavior Web_https
 classifier Web_deny behavior Web_deny
#
interface GigabitEthernet3/1/1
```

```
 ip address 4.4.4.2 255.255.255.0
 ipv6 address 4::2/64
#
interface GigabitEthernet3/1/2
  port link-mode route
 dhcp select relay proxy
 dhcp flood-protection enable
 ipv6 dhcp select relay
 ipv6 dhcp flood-protection enable
 ipv6 dhcp relay client-information record
 ipv6 dhcp relay release-agent
 ipv6 address auto link-local
 ipv6 nd autoconfig managed-address-flag
 ipv6 nd autoconfig other-flag
 undo ipv6 nd ra halt
 ip subscriber l2-connected enable
 ip subscriber authentication-method Web
 ip subscriber pre-auth domain dm1
 ip subscriber Web-auth domain dm2
#
 qos apply policy Web global inbound
 qos apply policy out global outbound
#
dhcp server ip-pool pool1
 gateway-list 192.168.0.1 export-route
 remote-server 4.4.4.3
#
ipv6 dhcp pool pool2
 gateway-list 192::1
 remote-server 4::3
#
acl advanced name ip
 rule 0 permit ip user-group Web
#
acl advanced name neiwang
 rule 0 permit ip destination 4.4.4.1 0 user-group Web
#
acl advanced name neiwang_out
 rule 0 permit ip source 4.4.4.1 0 user-group Web
#
acl advanced name Web_http
 rule 0 permit tcp destination-port eq www user-group Web
#
acl advanced name Web_https
 rule 0 permit tcp destination-port eq 443 user-group Web
#
acl advanced name Web_out
 rule 0 permit ip source 4.4.4.5 0 user-group Web
```

```
#
acl advanced name Web_permit
 rule 0 permit ip destination 4.4.4.5 0 user-group Web
#
acl ipv6 advanced name ip
 rule 0 permit ipv6 user-group Web
#
acl ipv6 advanced name neiwang
 rule 0 permit ipv6 destination 4::1/128 user-group Web
#
acl ipv6 advanced name neiwang_out
 rule 0 permit ipv6 source 4::1/128 user-group Web
#
acl ipv6 advanced name Web_http
 rule 0 permit tcp destination-port eq www user-group Web
#
acl ipv6 advanced name Web_https
 rule 0 permit tcp destination-port eq 443 user-group Web
#
acl ipv6 advanced name Web_out
 rule 0 permit ipv6 source 4::5/128 user-group Web
#
acl ipv6 advanced name Web_permit
 rule 0 permit ipv6 destination 4::5/128 user-group Web
#
user-profile car
 qos car inbound any cir 5210 cbs 325625 ebs 0
#
radius scheme rs1
 primary authentication 4.4.4.5
 primary accounting 4.4.4.5
 key authentication cipher $c$3$FhQVcgn3kq1exL0CdTzatcgc9xF9vL3ZOw==
 key accounting cipher $c$3$ntIHBRM4ZkG+2JRZQTdKmNl0kYJmhZz5Zg==
 user-name-format without-domain
#
radius dynamic-author server
 client ip 4.4.4.5 key cipher $c$3$lYC2ERe8ts2gtE6M2xfoDDB8NmGw6J9v/Q==
#
domain name dm1
 authorization-attribute user-group Web
 authorization-attribute ip-pool pool1
 authorization-attribute ipv6-pool pool2
 authentication ipoe none
 authorization ipoe none
 accounting ipoe none
 Web-server url http://www.h3c.web.com
 Web-server ipv6-url http://www.h3c.web.com
#
```

```
domain name dm2
 authorization-attribute user-profile car
 authentication ipoe radius-scheme rs1
 authorization ipoe radius-scheme rs1
 accounting ipoe radius-scheme rs1
#
user-group Web
#
portal server newpt1
 ip 4.4.4.5 key cipher $c$3$UnoFeLybwld9jDwLnHJQptDE7YZry2EVlw==
#
portal server newpt2
 ipv6 4::5 key cipher $c$3$HxisNWeML9fhYRS+7umwGbYwAkL+KGiCjw==
#
 http-redirect https-port 11111
#
```

9 IPoE 双栈用户普通 Web 认证配置举例(IPv4 静态，IPv6 动态)

在网络向 IPv6 演进的过程中，由于一段时间内，各种网络资源还没有全面支持 IPv6，因此需要以 IPv4/IPv6 双协议栈运行。

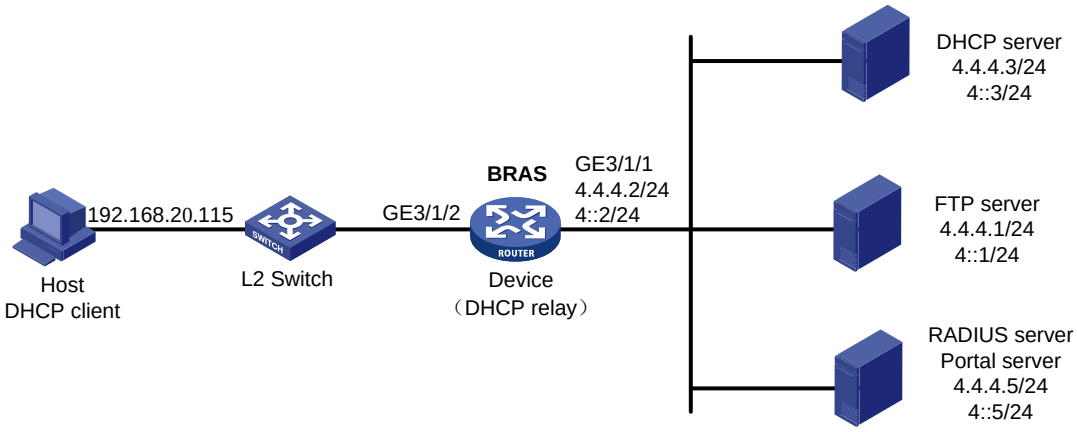
少数用户之前使用的是 IPv4 静态地址，希望继续保持；同时 IPv6 静态配置比较麻烦，希望使用动态分配方式，这里介绍一个 IPv4 使用静态地址，IPv6 使用 DHCPv6 分配地址的举例。

9.1 组网需求

如图 9-1 所示：Router A 为某学校的一台 BRAS 设备，为学校用户提供 IPoE 接入服务。要求：

- DHCP Client 经由二层网络以 IPoE 方式接入到 BRAS 接入设备。
- BRAS 接入设备作为 DHCPv6 服务器，为终端分配地址。
- 由一台安装了 H3C iMC 的服务器同时承担 RADIUS 服务器、Portal 认证服务器和 Portal Web 服务器的职责。
- FTP server 是一台内网服务器。
- IPoE Web 认证通过后限速 5Mbps。

图9-1 IPoE 双栈用户普通 Web 认证配置组网图



9.2 配置思路

为了保证用户的带宽需求，本例通过授权 User Profile 进行速率控制。

IPoE Web 认证前域中的流量，区分 HTTP、HTTPS 和普通 IP 报文分别通过不同的队列上送。IPoE Web 认证中针对上送 CPU 的流量，配置如下三种类和流行为组来处理：

- 流分类匹配 HTTP 同时 User Group 为前域标记的，对应的流行为 **redirect http-to-cpu**。
- 流分类匹配 HTTPS 同时 User Group 为前域标记的，对应的流行为 **redirect https-to-cpu**。
- 流分类匹配 IP 同时 User Group 为前域标记的，对应的流行为 **deny**。

9.3 配置注意事项

缺省情况下，未配置对 HTTPS 报文进行重定向的内部侦听端口号。需要通过 **http-redirect https-port** 命令用来配置对 HTTPS 报文进行重定向的侦听端口号，并且配置的侦听端口不要跟已有端口冲突。

本配置中使用到限速私有属性，有关私有属性的详细介绍，请参见 14 附录。

9.4 配置步骤

9.4.1 配置 IP 地址及路由

按照图 9-1 配置各接口的 IP 地址，并确保 BRAS 设备和各服务器之间路由可达，具体配置过程略。

9.4.2 设置 DNS 服务器

请正确设置 DNS 服务器，以便服务器可以根据 IPoE 双栈用户先上线的协议栈类型，解析出 Web 认证页面 http://www.h3c.web.com 对应的 IPv4 URL 地址或 IPv6 URL 地址。DNS 服务器具体设置过程略。

9.4.3 配置 DHCP 服务器

1. 配置 DHCPv6 地址池

全局开启 DHCP。

```
[BRAS] dhcp enable
```

创建名称为 v4 的 DHCPv4 地址池并进入其视图。

```
[BRAS] dhcp server ip-pool v4
```

配置地址池网关和分配的地址网段。

```
[BRAS-dhcp-pool-v4] gateway-list 192.168.20.1 export-route
[BRAS-dhcp-pool-v4] network 192.168.20.0 mask 255.255.255.0 export-route
[BRAS-dhcp-pool-v4] forbidden-ip 192.168.20.1
[BRAS-dhcp-pool-v4] forbidden-ip 192.168.20.115
[BRAS-dhcp-pool-v4] quit
```

创建名称为 v6 的 DHCPv6 地址池并进入其视图。

```
[BRAS] ipv6 dhcp pool v6
```

配置地址池动态分配的 IPv6 地址网段 192::0/64。

```
[BRAS-dhcp6-pool-v6] network 2408:8667:20::/64 export-route
[BRAS-dhcp6-pool-v6] dns-server 2409:8667::1
[BRAS-dhcp6-pool-v6] quit
```

配置接口 RAGG3 工作在 DHCPv6 服务器模式。

```
[BRAS] interface Route-Aggregation3
[BRAS-Route-Aggregation3] ipv6 dhcp select server
[BRAS-Route-Aggregation3] quit
```

9.4.4 配置 RADIUS 服务器

说明

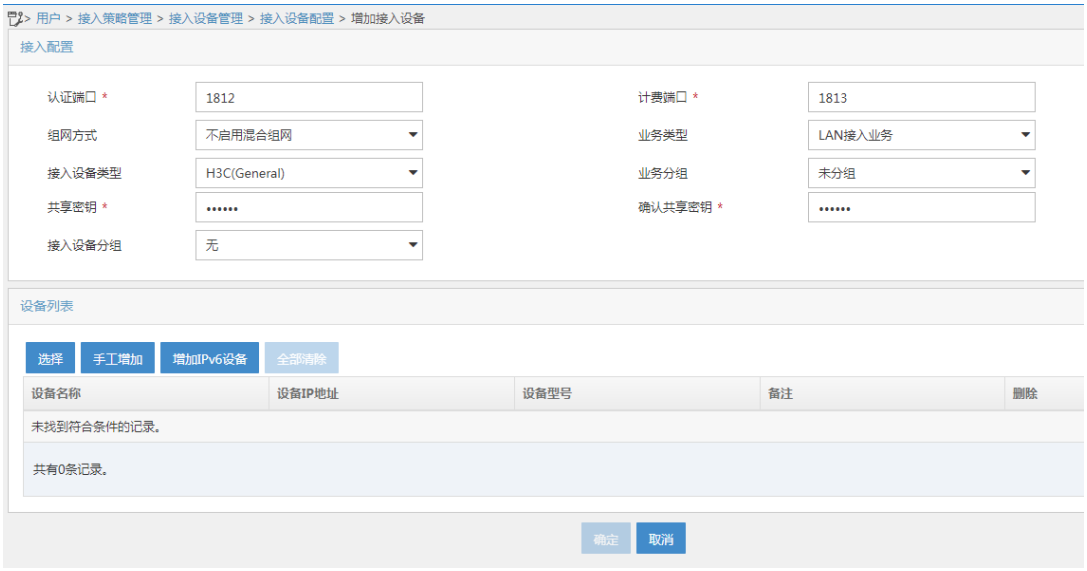
下面以 iMC（版本为 iMC PLAT 7.3 (E0705P02)）为例，说明 RADIUS 服务器的基本配置。不同 iMC 版本配置可能有所不同，具体配置请以实际版本及对应版本的 iMC 服务器手册为准，本节配置仅供参考。

(1) 配置接入设备

登录进入 iMC 管理平台，选择“用户”页签，单击导航树中的[接入策略管理/接入设备管理/接入设备配置]菜单项，进入接入设备配置页面，在该页面中单击<增加>按钮，进入如图 9-2 所示增加接入设备页面。

- 输入共享密钥为：radius。
- 其他采用缺省配置。

图9-2 增加接入设备



在该页面中设备列表下方单击<手工增加>，在如图 9-3 所示页面输入接入设备地址 4.4.4.2 并单击<确定>。

图9-3 手动增加接入设备

(2) 增加接入策略

单击导航树中的[接入策略管理/接入策略管理]菜单项，进入接入策略管理页面，在该页面中单击<增加>按钮，进入如图 9-4 所示增加接入策略页面。

- 输入接入策略名为：AccessPolicy。
- 其他采用缺省配置。

图9-4 增加接入策略

(3) 增加接入服务

单击导航树中的[接入策略管理/接入服务管理]菜单项，进入接入服务管理页面，在该页面中单击<增加>按钮，进入如图 9-5 所示增加接入服务页面。

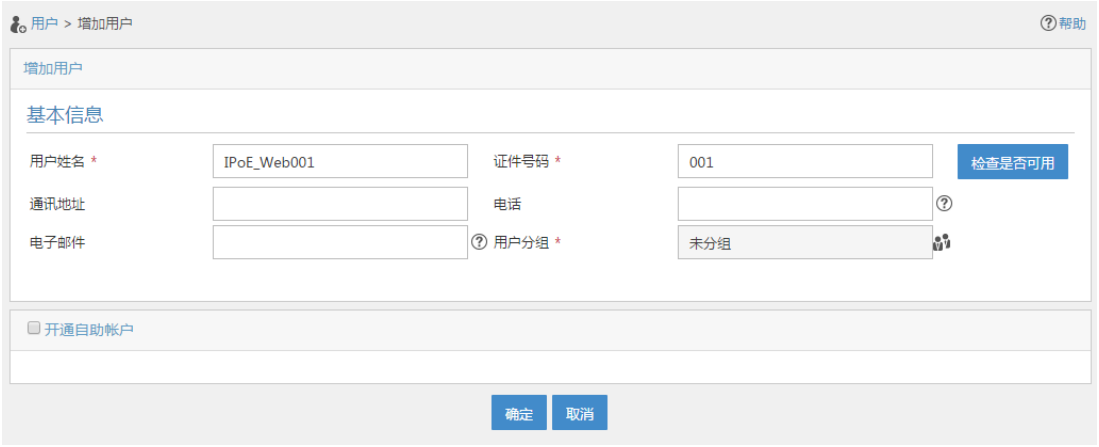
- 输入服务名为：IPoE_Server
- 缺省接入策略选择已创建的策略“AccessPolicy”。
- 其他采用缺省配置。

图9-5 增加接入服务

(4) 在 IMC 界面增加用户

单击导航树中的[用户管理/增加用户]菜单项，进入如图 9-6 所示增加用户页面，填写用户姓名和证件号码为：IPoE_Web001 和 001。

图9-6 增加用户



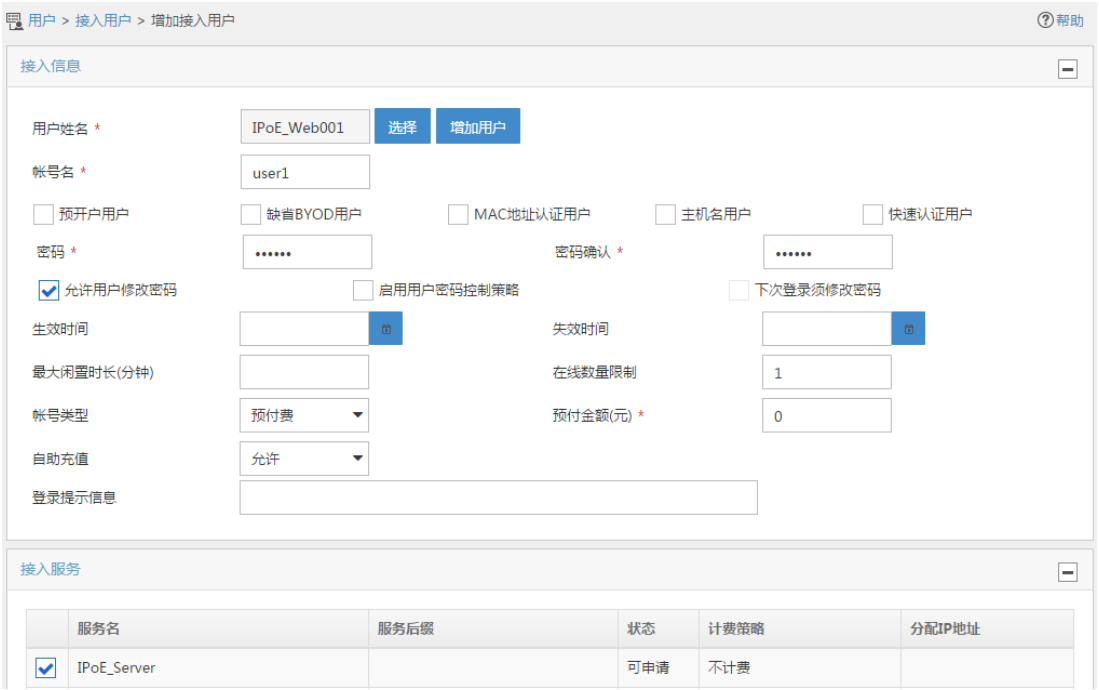
单击<确定>按钮后完成用户的添加。

(5) 增加接入用户

单击导航树中的[接入用户管理/接入用户]菜单项，进入接入用户页面，在该页面中单击<增加>按钮，进入如图 9-7所示增加接入用户页面。

- 用户姓名选择：IPoE_Web001
- 账号名填写为：user1
- 密码为：pass1
- 接入服务选择之前已创建的 IPoE_Server

图9-7 增加接入用户



9.4.5 配置 Portal 服务器

说明

下面以 iMC（版本为 iMC PLAT 7.3 (E0705P02)）为例，说明 Portal 服务器的基本配置。不同 iMC 版本配置可能有所不同，具体配置请以实际版本及对应版本的 iMC 服务器手册为准，本节配置仅供参考。

(1) 配置 Portal 主页。

单击导航树中的[接入策略管理/Portal 服务管理/服务器配置]菜单项，进入服务器配置页面，配置 Portal 主页，采用缺省配置即可，并单击<确定>按钮完成操作，如图 9-8 所示。

图9-8 Portal 服务器配置页面

(2) 配置 Portal 认证的地址组范围

单击导航树中的[接入策略管理/Portal 服务管理/IP 地址组配置]菜单项，进入“IP 地址组配置”页面，在该页面中单击<增加>按钮，进入“增加 IP 地址组配置”页面，如图 9-9 所示。

- 输入 IP 地址组名为“IPoE_Web_User”；
- 输入起始地址为“192.168.0.1”、终止地址为“192.168.0.255”。用户主机 IP 地址必须包含在该 IP 地址组范围内；
- 其他采用缺省配置；
- 单击<确定>按钮完成操作。

图9-9 增加 IP 地址组配置页面（IPv4）

如图 9-10 所示，继续上述操作添加 IPv6 地址组。

- 输入 IP 地址组名为“IPoE_Web_User-2”；
- IPv6 选项框选择“是”；
- 输入起始地址为“192::1”、终止地址为“192::FFFF”。用户主机 IPv6 地址必须包含在该 IP 地址组范围内；
- 其他采用缺省配置；
- 单击<确定>按钮完成操作。

图9-10 增加 IP 地址组配置页面（IPv6）

(3) 增加 Portal 接入设备信息

单击导航树中的[接入策略管理/Portal 服务管理/设备配置]菜单项，进入“设备配置”页面，在该页面中单击<增加>按钮，进入“增加设备信息”页面，如图 9-11 所示。

- 输入设备名为“NAS”；
- 输入 IP 地址为“4.4.4.2”，该地址为 Portal 报文出接口 GigabitEthernet3/1/1 的 IP 地址；
- 输入密钥为“123456”；
- 选择组网方式为“直连”；
- 其它参数采用缺省值，并单击<确定>按钮完成操作。

图9-11 增加设备信息配置页面（IPv4）

如图 9-12 所示，继续上述操作添加设备的 IPv6 信息。

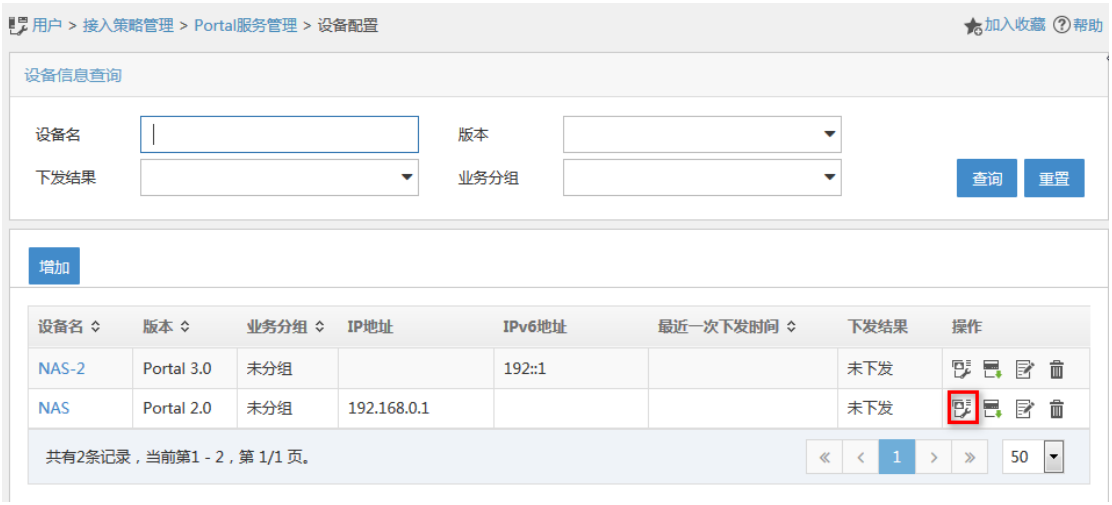
- 输入设备名为“NAS-2”；
- 版本选择“Portal 3.0”；
- 输入 IP 地址为“4::2”，该地址为 Portal 报文出接口 GigabitEthernet3/1/1 的 IP 地址；
- 输入密钥为“123456”；
- 选择组网方式为“直连”；
- 其它参数采用缺省值，并单击<确定>按钮完成操作。

图9-12 增加设备信息配置页面（IPv6）

(4) 配置端口组信息

如图 9-13 所示返回[接入策略管理/Portal 服务管理/设备配置]菜单项，单击<端口组信息管理>按钮，进入“端口组信息配置”页面。

图9-13 设备信息列表



在“端口组信息配置”页面中单击<增加>按钮，进入“增加端口组信息”页面，如图 9-14 所示。

- 输入端口组名为“group”；
- 选择 IP 地址组为“IPoE_Web_User”，用户接入网络时使用的 IP 地址必须属于所选的 IP 地址组；
- 其它参数采用缺省值，并单击<确定>按钮完成操作。

图9-14 增加端口组信息配置页面（IPv4）

如图 9-15 所示，继续上述操作添加端口组的 IPv6 信息。

- 输入端口组名为“group-2”；
- 选择 IP 地址组为“IPoE_Web_User-2”，用户接入网络时使用的 IPv6 地址必须属于所选的 IPv6 地址组；
- 其它参数采用缺省值，并单击<确定>按钮完成操作。

图9-15 增加端口组信息配置页面（IPv6）

9.4.6 配置 BRAS

1. 配置 IPv6 基础配置

配置自动生成 IPv6 链路本地地址，该 IPv6 链路本地地址作为用户的网关。

```
[BRAS-Route-Aggregation3] ipv6 address auto link-local
```

配置 DHCP 防攻击功能。

```
[BRAS-Route-Aggregation3] dhcp flood-protection enable
[BRAS-Route-Aggregation3] ipv6 dhcp flood-protection enable
```

取消设备发布 RA 消息的抑制。配置被管理地址的配置标志位为 1，即主机通过 DHCPv6 服务器获取 IPv6 地址。配置其他信息配置标志位为 1，即主机通过 DHCPv6 服务器获取除 IPv6 地址以外的其他信息。

```
[BRAS-Route-Aggregation3] undo ipv6 nd ra halt
[BRAS-Route-Aggregation3] ipv6 nd autoconfig managed-address-flag
[BRAS-Route-Aggregation3] ipv6 nd autoconfig other-flag
```

配置漫游时重新分配地址功能。

```
[BRAS-Route-Aggregation3] ipv6 dhcp session-mismatch action fast-renew
```

2. 配置 Portal 认证服务器

配置 IPv4 Portal 认证服务器：名称为 newpt1，IP 地址为 4.4.4.5，密钥为明文 123456。

```
[BRAS] portal server newpt1
[BRAS-portal-server-newpt1] ip 4.4.4.5 key simple 123456
[BRAS-portal-server-newpt1] quit
```

配置 IPv6 Portal 认证服务器：名称为 newpt2，IPv6 地址为 4::5，密钥为明文 123456。

```
[BRAS] portal server newpt2
[BRAS-portal-server-newpt2] ipv6 4::5 key simple 123456
[BRAS-portal-server-newpt2] quit
```

3. 配置 HTTPS 的内部侦听端口

配置 HTTPS 的内部侦听端口，端口不要跟已有端口冲突即可。

```
[BRAS] http-redirect https-port 11111
```

4. 创建本地用户组

创建认证前域用户组，名称为 Web。

```
[BRAS] user-group Web
New user group added.
[BRAS-ugroup-Web] quit
```

5. 配置 QoS

(1)　配置用于认证前域用户的 ACL 规则

分别为 IPv4 和 IPv6 高级 ACL Web_permit 创建规则如下：匹配用户组 Web 中用户的目的地址为 Portal 服务器地址的报文。

```
[BRAS] acl advanced name Web_permit
[BRAS-acl-ipv4-adv-Web_permit] rule 0 permit ip destination 4.4.4.5 0 user-group Web
[BRAS-acl-ipv4-adv-Web_permit] quit
[BRAS] acl ipv6 advanced name Web_permit
[BRAS-acl-ipv6-adv-Web_permit] rule 0 permit ipv6 destination 4::5 128 user-group Web
[BRAS-acl-ipv6-adv-Web_permit] quit
```

分别为 IPv4 和 IPv6 高级 ACL neiwang 创建规则如下：匹配用户组 Web 中用户的目的地址为内网服务器地址的报文。

```
[BRAS] acl advanced name neiwang
[BRAS-acl-ipv4-adv-neiwang] rule 0 permit ip destination 4.4.4.1 0 user-group Web
[BRAS-acl-ipv4-adv-neiwang] quit
[BRAS] acl ipv6 advanced name neiwang
[BRAS-acl-ipv6-adv-neiwang] rule 0 permit ipv6 destination 4::1 128 user-group Web
[BRAS-acl-ipv6-adv-neiwang] quit
```

分别为 IPv4 和 IPv6 高级 ACL Web_http 创建规则如下：匹配用户组 Web 中用户的目的端口为 80 和 8080 的 TCP 报文(即 HTTP 报文)。

```
[BRAS] acl advanced name Web_http
[BRAS-acl-ipv4-adv-Web_http] rule 0 permit tcp destination-port eq www user-group Web
[BRAS-acl-ipv4-adv-Web_http] rule 0 permit tcp destination-port eq 8080 user-group Web
[BRAS-acl-ipv4-adv-Web_http] quit
[BRAS] acl ipv6 advanced name Web_http
[BRAS-acl-ipv6-adv-Web_http] rule 0 permit tcp destination-port eq www user-group Web
[BRAS-acl-ipv6-adv-Web_http] rule 0 permit tcp destination-port 8080 www user-group Web
[BRAS-acl-ipv6-adv-Web_http] quit
```

分别为 IPv4 和 IPv6 高级 ACL Web_https 创建规则如下：匹配用户组 Web 中用户的目的端口为 443 的 TCP 报文(即 HTTPS 报文)。

```
[BRAS] acl advanced name Web_https
[BRAS-acl-ipv4-adv-Web_https] rule 0 permit tcp destination-port eq 443 user-group Web
[BRAS-acl-ipv4-adv-Web_https] quit
[BRAS] acl ipv6 advanced name Web_https
[BRAS-acl-ipv6-adv-Web_https] rule 0 permit tcp destination-port eq 443 user-group Web
[BRAS-acl-ipv6-adv-Web_https] quit
```

分别为 IPv4 和 IPv6 高级 ACL ip 创建规则如下：匹配用户组 Web 中用户的 IP 报文。

```
[BRAS] acl advanced name ip
[BRAS-acl-ipv4-adv-ip] rule 0 permit ip user-group Web
[BRAS-acl-ipv4-adv-ip] quit
[BRAS] acl ipv6 advanced name ip
[BRAS-acl-ipv6-adv-ip] rule 0 permit ipv6 user-group Web
[BRAS-acl-ipv6-adv-ip] quit
```

分别为 IPv4 和 IPv6 高级 ACL neiwang_out 创建规则如下：匹配用户组 Web 中源地址为内网服务器 IP 地址的报文。

```
[BRAS] acl advanced name neiwang_out
[BRAS-acl-ipv4-adv-neiwang_out] rule 0 permit ip source 4.4.4.1 0 user-group Web
[BRAS-acl-ipv4-adv-neiwang_out] quit
[BRAS] acl ipv6 advanced name neiwang_out
[BRAS-acl-ipv6-adv-neiwang_out] rule 0 permit ipv6 source 4::1 128 user-group Web
[BRAS-acl-ipv6-adv-neiwang_out] quit
```

分别为 IPv4 和 IPv6 高级 ACL Web_out 创建规则如下：匹配用户组 Web 中源地址为 Portal 服务器 IP 地址的报文。

```
[BRAS] acl advanced name Web_out
[BRAS-acl-ipv4-adv-Web_out] rule 0 permit ip source 4.4.4.5 0 user-group Web
[BRAS-acl-ipv4-adv-Web_out] quit
[BRAS] acl ipv6 advanced name Web_out
[BRAS-acl-ipv6-adv-Web_out] rule 0 permit ipv6 source 4::5 128 user-group Web
[BRAS-acl-ipv6-adv-Web_out] quit
```

(2) 配置用于认证前域用户的类

配置类 Web_permit，匹配 ACL Web_permit。

```
[BRAS] traffic classifier Web_permit operator or
[BRAS-classifier-Web_permit] if-match acl name Web_permit
[BRAS-classifier-Web_permit] if-match acl ipv6 name Web_permit
```

```
[BRAS-classifier-Web_permit] quit
```

配置类 neiwang，匹配 ACL neiwang。

```
[BRAS] traffic classifier neiwang operator or
[BRAS-classifier-neiwang] if-match acl name neiwang
[BRAS-classifier-neiwang] if-match acl ipv6 name neiwang
[BRAS-classifier-neiwang] quit
```

配置类 Web_http，匹配 ACL Web_http。

```
[BRAS] traffic classifier Web_http operator or
[BRAS-classifier-Web_http] if-match acl name Web_http
[BRAS-classifier-Web_http] if-match acl ipv6 name Web_http
[BRAS-classifier-Web_http] quit
```

配置类 Web_https，匹配 ACL Web_https。

```
[BRAS] traffic classifier Web_https operator or
[BRAS-classifier-Web_https] if-match acl name Web_https
[BRAS-classifier-Web_https] if-match acl ipv6 name Web_https
[BRAS-classifier-Web_https] quit
```

配置类 Web_deny，匹配 ACL ip。

```
[BRAS] traffic classifier Web_deny operator or
[BRAS-classifier-Web_deny] if-match acl name ip
[BRAS-classifier-Web_deny] if-match acl ipv6 name ip
[BRAS-classifier-Web_deny] quit
```

配置类 neiwang_out，匹配 ACL neiwang_out。

```
[BRAS] traffic classifier neiwang_out operator or
[BRAS-classifier-neiwang_out] if-match acl name neiwang_out
[BRAS-classifier-neiwang_out] if-match acl ipv6 name neiwang_out
[BRAS-classifier-neiwang_out] quit
```

配置类 Web_out，匹配 ACL Web_out。

```
[BRAS] traffic classifier Web_out operator or
[BRAS-classifier-Web_out] if-match acl name Web_out
[BRAS-classifier-Web_out] if-match acl ipv6 name Web_out
[BRAS-classifier-Web_out] quit
```

(3) 配置流行为

配置流行为 Web_permit，允许用户组 Web 中用户的目的地址为 Portal 服务器 IP 地址的报文通过。

```
[BRAS] traffic behavior Web_permit
[BRAS-behavior-Web_permit] filter permit
[BRAS-behavior-Web_permit] free account
[BRAS-behavior-Web_permit] quit
```

配置流行为 neiwang，允许用户组 Web 中用户的目的地址为内网服务器 IP 地址的报文通过。

```
[BRAS] traffic behavior neiwang
[BRAS-behavior-neiwang] filter permit
[BRAS-behavior-neiwang] quit
```

配置流行为 Web_http，对用户组 Web 中用户的目的端口为 80 的 TCP 报文(即 HTTP 报文)重定向到 CPU。

```
[BRAS] traffic behavior Web_http
```

```
[BRAS-behavior-Web_http] redirect http-to-cpu
[BRAS-behavior-Web_http] quit
```

配置流行为 Web_https，对用户组 Web 中用户的目的端口为 443 的 TCP 报文(即 HTTPS 报文)重定向到 CPU。

```
[BRAS] traffic behavior Web_https
[BRAS-behavior-Web_https] redirect https-to-cpu
[BRAS-behavior-Web_https] quit
```

配置流行为 Web_deny，禁止用户组 Web 中用户的所有 IP 报文通过。

```
[BRAS] traffic behavior Web_deny
[BRAS-behavior-Web_deny] filter deny
[BRAS-behavior-Web_permit] free account
[BRAS-behavior-Web_deny] quit
```

配置流行为 neiwang_out，允许用户组 Web 中源地址为内网服务器 IP 地址的报文通过。

```
[BRAS] traffic behavior neiwang_out
[BRAS-behavior-neiwang_out] filter permit
[BRAS-behavior-neiwang_out] quit
```

配置流行为 Web_out，允许用户组 Web 中源地址为 Portal 服务器 IP 地址的报文通过。

```
[BRAS] traffic behavior Web_out
[BRAS-behavior-Web_out] filter permit
[BRAS-behavior-Web_out] free account
[BRAS-behavior-Web_out] quit
```

(4) 配置 QoS 策略

配置入方向 QoS 策略 Web

```
[BRAS] qos policy Web
```

为类指定对应的流行为，规则为对于用户组 Web 中的用户：

允许目的地址为 Portal 服务器和内网服务器 IP 地址的报文通过；

对于目的端口为 80（HTTP 报文）和 443（HTTPS 报文）的报文重定向到 CPU；

除上述报文外，其余报文均禁止通过。

```
[BRAS-qospolicy-Web] classifier Web_permit behavior Web_permit
[BRAS-qospolicy-Web] classifier neiwang behavior neiwang
[BRAS-qospolicy-Web] classifier Web_http behavior Web_http
[BRAS-qospolicy-Web] classifier Web_https behavior Web_https
[BRAS-qospolicy-Web] classifier Web_deny behavior Web_deny
[BRAS-qospolicy-Web] quit
```

配置出方向 QoS 策略 out

```
[BRAS] qos policy out
```

为类指定对应的流行为，规则为：允许用户组 Web 中源地址为 Portal 服务器和内网服务器 IP 地址的报文通过，其余报文均禁止通过。

```
[BRAS-qospolicy-out] classifier neiwang_out behavior neiwang_out
[BRAS-qospolicy-out] classifier Web_out behavior Web_out
[BRAS-qospolicy-out] classifier Web_deny behavior Web_deny
[BRAS-qospolicy-out] quit
```

(5) 配置应用策略

对接收的用户流量应用 QoS 策略，策略名为 Web。

```
[BRAS] qos apply policy Web global inbound
```

对发送的上线用户流量应用 QoS 策略，策略名为 out。

```
[BRAS] qos apply policy out global outbound
```

(6) 查看应用的策略是否生效

查看入方向 QoS 策略的配置信息和运行情况。

```
[BRAS] display qos policy global slot 3 inbound
  Direction: Inbound
  Policy: Web
   Classifier: Web_permit
     Operator: OR
     Rule(s) :
      If-match acl name Web_permit
      If-match acl ipv6 name Web_permit
     Behavior: Web_permit
      Filter enable: Permit
      Free account enable
   Classifier: neiwang
     Operator: OR
     Rule(s) :
      If-match acl name neiwang
      If-match acl ipv6 name neiwang
     Behavior: neiwang
      Filter enable: Permit
   Classifier: Web_http
     Operator: OR
     Rule(s) :
      If-match acl name Web_http
      If-match acl ipv6 name Web_http
     Behavior: Web_http
      Redirecting:
        Redirect http to CPU
   Classifier: Web_https
     Operator: OR
     Rule(s) :
      If-match acl name Web_https
      If-match acl ipv6 name Web_https
     Behavior: Web_https
      Redirecting:
        Redirect https to CPU
   Classifier: Web_deny
     Operator: OR
     Rule(s) :
      If-match acl name ip
      If-match acl ipv6 name ip
     Behavior: Web_deny
      Filter enable: Deny
```

查看出方向 QoS 策略的配置信息和运行情况。

```
[BRAS] display qos policy global slot 3 outbound
  Direction: Outbound
  Policy: out
   Classifier: neiwang_out
     Operator: OR
     Rule(s) :
      If-match acl name neiwang_out
      If-match acl ipv6 name neiwang_out
     Behavior: neiwang_out
      Filter enable: Permit
   Classifier: Web_out
     Operator: OR
     Rule(s) :
      If-match acl name Web_out
      If-match acl ipv6 name Web_out
     Behavior: Web_out
      Filter enable: Permit
      Free account enable
   Classifier: Web_deny
     Operator: OR
     Rule(s) :
      If-match acl name ip
      If-match acl ipv6 name ip
     Behavior: Web_deny
      Filter enable: Deny
```

6. 配置 RADIUS 方案

创建名称为 rs1 的 RADIUS 方案并进入该方案视图。

```
[BRAS] radius scheme rs1
```

配置 RADIUS 方案的主认证和主计费服务器及其通信密钥。

```
[BRAS-radius-rs1] primary authentication 4.4.4.5
[BRAS-radius-rs1] primary accounting 4.4.4.5
[BRAS-radius-rs1] key authentication simple radius
[BRAS-radius-rs1] key accounting simple radius
```

配置发送给 RADIUS 服务器的用户名不携带 ISP 域名。

```
[BRAS-radius-rs1] user-name-format without-domain
[BRAS-radius-rs1] quit
```

设置 RADIUS DAE 客户端的 IP 地址为 4.4.4.5，与 RADIUS DAE 客户端交互 DAE 报文时使用的共享密钥为明文 radius，需要注意的是认证两端明文密钥需要一致。

```
[BRAS] radius dynamic-author server
[BRAS-radius-da-server] client ip 4.4.4.5 key simple radius
[BRAS-radius-da-server] quit
```

7. 配置 User Profile

配置名称为 car 的 User Profile 对上线用户发送的报文进行流量监管。报文正常流速为 5210kbps，允许 325625byte 的突发流量通过，速率小于等于 5210kbps 时正常发送，大于 5210kbps 时，报文被丢弃。

```
[BRAS] user-profile car
```

```
[BRAS-user-profile-car] qos car inbound any cir 5210 cbs 325625
[BRAS-user-profile-car] qos car outbound any cir 5210 cbs 325625
[BRAS-user-profile-car] quit
```

8. 配置认证前域和 Web 认证域

配置 IPoE 用户认证前使用的认证域。

```
[BRAS] domain name pre-Web
[BRAS-isp-pre-Web] authentication ipoe none
[BRAS-isp-pre-Web] authorization ipoe none
[BRAS-isp-pre-Web] accounting ipoe none
```

配置前域授权用户组和地址池。

```
[BRAS-isp-pre-Web] authorization-attribute user-group Web
[BRAS-isp-pre-Web] authorization-attribute ip-pool v4
[BRAS-isp-pre-Web] authorization-attribute ipv6-pool v6
```

配置 Web 认证页面 URL。

```
[BRAS-isp-dm1] Web-server url http://www.h3c.web.com
[BRAS-isp-dm1] Web-server ipv6-url http://www.h3c.web.com
[BRAS-isp-dm1] quit
```

配置 IPoE 用户在 Web 认证阶段使用的认证域。

```
[BRAS] domain name Web
[BRAS-isp-Web] authentication ipoe radius-scheme rs1
[BRAS-isp-Web] authorization ipoe radius-scheme rs1
[BRAS-isp-Web] accounting ipoe radius-scheme rs1
[BRAS-isp-Web] authorization-attribute user-profile car
[BRAS-isp-Web] quit
```

9. 配置 IPoE

开启 IPoE 功能，并配置二层接入模式。

```
[BRAS] interface Route-Aggregation3
[BRAS-Route-Aggregation3] ip subscriber l2-connected enable
```

使能未知源 IP 报文触发方式。

```
[BRAS-Route-Aggregation3] ip subscriber initiator unclassified-ip enable matching-user
[BRAS-Route-Aggregation3] ip subscriber initiator unclassified-ipv6 enable matching-user
```

配置 IPoE 用户采用 Web 认证方式。

```
[BRAS-Route-Aggregation3] ip subscriber authentication-method Web
The operation may cut all users on this interface. Continue?[Y/N]:y
```

配置 Web 认证前域为 pre-Web，Web 认证域为 Web。

```
[BRAS-Route-Aggregation3] ip subscriber pre-auth domain pre-Web
[BRAS-Route-Aggregation3] ip subscriber Web-auth domain Web
[BRAS-Route-Aggregation3] quit
```

配置用户静态配置的 IPv4 地址为 IPoE 静态用户。

```
[BRAS] ip subscriber session static ip 192.168.20.115 domain pre-Web interface
Route-Aggregation3 support-ds
```

9.4.7 验证配置

用户认证前域认证通过之后，可以使用以下的显示命令查看 IPoE 用户在线信息，其中，用户获得的 IPv4 地址为 192.168.20.115，IPv6 地址为 2408:8667:20::1。

```
[BRAS] display ip subscriber session verbose
Basic:
  Description                 : -
  Username                    : 80c16ee016ed
  Authorization domain        : pre-Web
  Authentication domain       : pre-Web
  VPN instance                : N/A
  IP address                  : 192.168.20.115
  IPv6 address                : 2408:8667:20::1
  User address type           : N/A
  MAC address                 : 80c1-6ee0-16ed
  IPv6 DUID                   : 80c1-6ee0-16ed
  Service-VLAN/Customer-VLAN  : -/-
  Access interface            : RAGG3
  User ID                     : 0x38200001
  VPI/VCI(for ATM)            : -/-
  VSI Index                   : -
  VSI link ID                 : -
  VXLAN ID                    : -
  DNS servers                 : N/A
  IPv6 DNS servers            : 2409:8667::1
  DHCP lease                  : N/A
  DHCP remain lease           : N/A
  DHCPv6 lease                : 2592000 sec
  DHCPv6 remain lease         : N/A
  DHCPv6 PD lease             : N/A
  DHCPv6 PD remain lease      : N/A
  Access time                 : Jul 31 09:33:09 2020
  Online time(hh:mm:ss)       : 01:39:05
  Service node                : Slot 2 CPU 0
  Authentication type         : Web pre-auth
  IPv4 access type            : Static
  IPv6 access type            : DHCP
  IPv4 detect state           : Detecting
  IPv6 detect state           : Detecting
  State                       : Online

AAA:
  ITA policy name             : N/A
  IP pool                     : v4
  IPv6 pool                   : v6
  IPv6 nd preifx pool         : N/A
  Primary DNS server          : N/A
  Secondary DNS server        : N/A
```

```
  Primary IPv6 DNS server     : N/A
  Secondary IPv6 DNS server   : N/A
  Session idle cut            : N/A
  Session duration            : N/A, remaining: N/A
  Traffic quota               : N/A
  Traffic remained            : N/A
  Acct start-fail action      : Online
  Acct update-fail action     : Online
  Acct quota-out action       : Offline
  Dual-stack accounting mode  : Merge
  Max IPv4 multicast addresses: 4
  IPv4 multicast address list : N/A
  Max IPv6 multicast addresses: 4
  IPv6 multicast address list : N/A
  Accounting start time       : Jul 31 09:33:09 2020
  Redirect URL                : http://www.h3c.web.com
  Redirect IPv6 URL           : http://www.h3c.web.com
  Subscriber ID               : -

QoS:
  User profile                : N/A
  Session group profile       : N/A
  User group ACL              : Web (active)
  Inbound CAR                 : N/A
  Outbound CAR                : N/A
  Inbound user priority       : N/A
  Outbound user priority      : N/A

Flow statistic:
  Uplink   packets/bytes      : 183/22084
  Downlink packets/bytes      : 0/0
  IPv6 uplink   packets/bytes : 0/0
  IPv6 downlink packets/bytes : 0/0
```

用户认证前域认证通过之后，登录 Web 页面，如图 8-16 所示。

图9-16 登录 Web 页面

在认证页面输入用户名和密码单击<上线>按钮进行 Web 认证，可以使用以下的显示命令查看 IPoE 用户在线信息。

```
[BRAS] display ip subscriber session verbose
Basic:
  Description                 : -
  Username                    : bj1
  Authorization domain        : Web
  Authentication domain       : Web
  VPN instance                : N/A
  IP address                  : 192.168.20.115
  IPv6 address                : 2408:8667:20::1
  User address type           : N/A
  MAC address                 : 80c1-6ee0-16ed
  IPv6 DUID                   : 80c1-6ee0-16ed
  Service-VLAN/Customer-VLAN  : -/-
  Access interface            : RAGG3
  User ID                     : 0x38200001
  VPI/VCI(for ATM)            : -/-
  VSI Index                   : -
  VSI link ID                 : -
  VXLAN ID                    : -
  DNS servers                 : N/A
  IPv6 DNS servers            : 2409:8667::1
  DHCP lease                  : N/A
  DHCP remain lease           : N/A
  DHCPv6 lease                : 2592000 sec
  DHCPv6 remain lease         : N/A
```

```
  DHCPv6 PD lease             : N/A
  DHCPv6 PD remain lease      : N/A
  Access time                 : Jul 31 09:33:09 2020
  Online time(hh:mm:ss)       : 00:00:17
  Service node                : Slot 2 CPU 0
  Authentication type         : Web
  IPv4 access type            : Static
  IPv6 access type            : DHCP
  IPv4 detect state           : Detecting
  IPv6 detect state           : Detecting
  State                       : Online

AAA:
  ITA policy name             : N/A
  IP pool                     : v4
  IPv6 pool                   : v6
  IPv6 nd preifx pool         : N/A
  Primary DNS server          : N/A
  Secondary DNS server        : N/A
  Primary IPv6 DNS server     : N/A
  Secondary IPv6 DNS server   : N/A
  Session idle cut            : N/A
  Session duration            : 86400 sec, remaining: N/A
  Traffic quota               : N/A
  Traffic remained            : N/A
  Acct start-fail action      : Online
  Acct update-fail action     : Online
  Acct quota-out action       : Offline
  Dual-stack accounting mode  : Merge
  Max IPv4 multicast addresses: 4
  IPv4 multicast address list : N/A
  Max IPv6 multicast addresses: 4
  IPv6 multicast address list : N/A
  Accounting start time       : Jul 31 11:27:11 2020
  Redirect URL                : N/A
  Redirect IPv6 URL           : -
  Subscriber ID               : -

QoS:
  User profile                : car (active)
  Session group profile       : N/A
  User group ACL              : N/A
  Inbound CAR                 : N/A
  Outbound CAR                : N/A
  Inbound user priority       : N/A
  Outbound user priority      : N/A

Flow statistic:
```

```
  Uplink   packets/bytes      : 67/11569
  Downlink packets/bytes      : 8/7519
  IPv6 uplink   packets/bytes : 0/0
  IPv6 downlink packets/bytes : 0/0
```

9.4.8 配置文件

- Router A（BRAS）：

```
#
 dhcp enable
#
 ip subscriber session static ip 192.168.20.115 domain pre-Web interface Route-Aggregation3
support-ds
#
traffic classifier ip_cpu operator or
 if-match acl name ip
 if-match acl ipv6 name ip
#
traffic classifier ip_deny operator or
 if-match acl name ip
 if-match acl ipv6 name ip
#
traffic classifier neiwang operator or
 if-match acl name neiwang
 if-match acl ipv6 name neiwang
#
traffic classifier neiwang_out operator or
 if-match acl name neiwang_out
 if-match acl ipv6 name neiwang_out
#
traffic classifier Web_http operator or
 if-match acl name Web_http
 if-match acl ipv6 name Web_http
#
traffic classifier Web_https operator or
 if-match acl name Web_https
 if-match acl ipv6 name Web_https
#
traffic classifier Web_out operator or
 if-match acl name Web_out
 if-match acl ipv6 name Web_out
#
traffic classifier Web_permit operator or
 if-match acl name Web-permit
 if-match acl ipv6 name Web-permit
#
traffic behavior ip_cpu
 redirect cpu
#
```

```
traffic behavior neiwang
 filter permit
#
traffic behavior neiwang_out
 filter permit
#
#
traffic behavior Web_cpu
 redirect cpu
#
traffic behavior Web_deny
 filter deny
 free account
#
traffic behavior Web_http
 redirect http-to-cpu
#
traffic behavior Web_https
 redirect https-to-cpu
#
traffic behavior Web_out
 free account
#
traffic behavior Web_permit
 free account
#
qos policy out
 classifier Web_out behavior Web_out
 classifier neiwang_out behavior neiwang_out
 classifier ip_deny behavior Web_deny
#
qos policy Web
 classifier Web_permit behavior Web_permit
 classifier neiwang behavior neiwang
 classifier Web_http behavior Web_http
 classifier Web_https behavior Web_https
 classifier ip_cpu behavior Web_cpu
 classifier ip_deny behavior Web_deny
#
user-profile car
 qos car inbound any cir 5210 cbs 325625
 qos car outbound any cir 5210 cbs 325625
#
dhcp server ip-pool v4
 gateway-list 192.168.20.1 export-route
 network 192.168.20.0 mask 255.255.255.0 export-route
 forbidden-ip 192.168.20.1
 forbidden-ip 192.168.20.115
```

```
#
ipv6 dhcp pool v6
 network 2408:8667:20::/64 export-route
 dns-server 2409:8667::1
#
interface Route-Aggregation3
 ipv6 dhcp select server
 ipv6 address auto link-local
 ipv6 nd autoconfig managed-address-flag
 ipv6 nd autoconfig other-flag
 undo ipv6 nd ra halt
 ip subscriber l2-connected enable
 ip subscriber initiator dhcpv6 enable
 ip subscriber initiator unclassified-ip enable matching-user
 ip subscriber initiator unclassified-ipv6 enable matching-user
 ip subscriber initiator arp enable
 ip subscriber authentication-method Web
 ip subscriber pre-auth domain pre-Web
 ip subscriber Web-auth domain Web
#
interface GigabitEthernet2/2/18
 port link-mode route
 port link-aggregation group 3
#
interface GigabitEthernet2/2/19
 port link-mode route
 ip address 192.168.2.24 255.255.255.0
#
 qos apply policy Web global inbound
 qos apply policy out global outbound
#
acl advanced name ip
 rule 5 permit ip user-group Web
#
acl advanced name neiwang
 rule 5 permit ip destination 4.4.4.1 0 user-group Web
#
acl advanced name neiwang_out
 rule 5 permit ip source 4.4.4.1 0 user-group Web
#
acl advanced name Web-permit
 rule 5 permit ip destination 4.4.4.5 0 user-group Web
#
acl advanced name Web_http
 rule 5 permit tcp destination-port eq www user-group Web
 rule 10 permit tcp destination-port eq 8080 user-group Web
#
acl advanced name Web_https
```

```
 rule 5 permit tcp destination-port eq 443 user-group Web
#
acl advanced name Web_out
 rule 5 permit ip source 4.4.4.5 0 user-group Web
#
acl ipv6 advanced name ip
 rule 5 permit ipv6 user-group Web
#
acl ipv6 advanced name neiwang
 rule 5 permit ipv6 destination 4::1/128 user-group Web
#
acl ipv6 advanced name neiwang_out
 rule 5 permit ipv6 source 4::1/128 user-group Web
#
acl ipv6 advanced name Web-permit
 rule 5 permit ipv6 destination 4::5/128 user-group Web
#
acl ipv6 advanced name Web_http
 rule 5 permit tcp destination-port eq www user-group Web
 rule 10 permit tcp destination-port eq 8080 user-group Web
#
acl ipv6 advanced name Web_https
 rule 5 permit tcp destination-port eq 443 user-group Web
#
acl ipv6 advanced name Web_out
 rule 5 permit ipv6 source 4::5/128 user-group Web
#
radius scheme rs1
 primary authentication 192.168.2.249
 primary accounting 192.168.2.249
 key authentication simple radius
 key accounting simple radius
 nas-ip 192.168.2.24
#
radius dynamic-author server
 client ip 4.4.4.5 key simple radius
#
domain name pre-Web
 authorization-attribute user-group Web
 authorization-attribute ip-pool v4
 authorization-attribute ipv6-pool v6
 authentication ipoe none
 authorization ipoe none
 accounting ipoe none
 Web-server url http://www.h3c.web.com
 Web-server ipv6-url http://www.h3c.web.com
#
domain name Web
```

```
 authentication ipoe radius-scheme imc
 authorization ipoe radius-scheme imc
 accounting ipoe radius-scheme imc
#
user-group Web
#
portal server newpt1
 ip 4.4.4.5 key simple radius
#
portal server newpt2
 ipv6 4::5 key simple radius
#
 http-redirect https-port 11111
#
```

10 哑终端配置举例

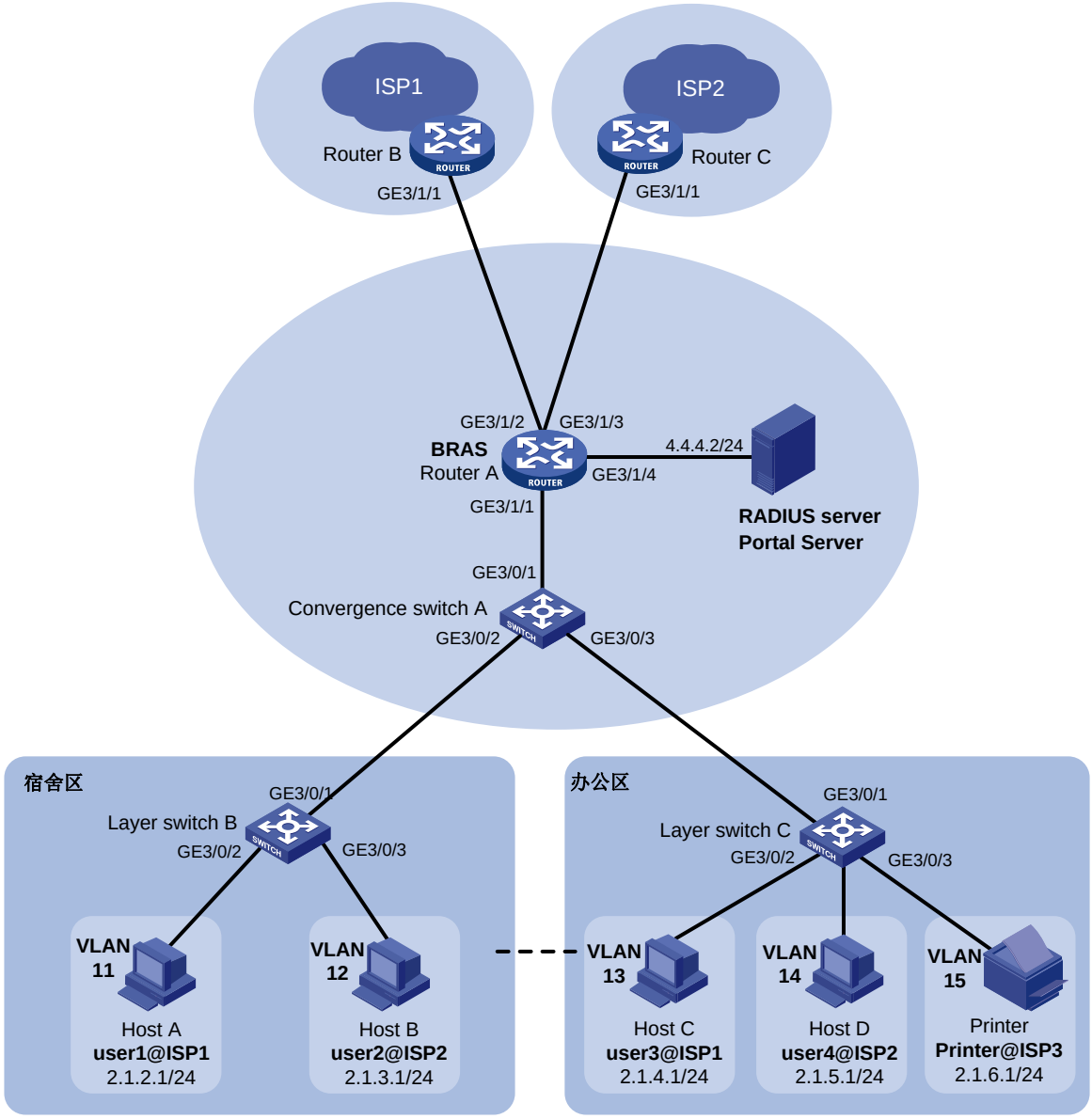
在校园网环境里，存在许多不需要访问外网的网络资源，如打印机、服务器等，这些资源只需要校内用户能够访问使用即可，没有更多的认证需求。这里介绍一个对这种业务的配置举例。这里的举例是基于 IPoE 的，与直接配置接口地址，做 IP 转发的方案相比，最大的优势是端口规划和地址规划简单，不需要接专线。

10.1 组网需求

如图 10-1 所示，某校园网的宿舍区和办公区直挂在 BRAS 下，且 BRAS 作为出口设备分别接不同的运营商 ISP1 和 ISP2，要求实现如下需求：

- 办公区打印机通过静态 IPoE 方式接入，不允许访问互联网资源。

图10-1 BRAS 校园网用户组多出口配置举例



设备	接口	IP地址	设备	接口	IP地址
RADIUS server	-	4.4.4.2/24	Router A（BRAS）	GE3/1/1	2.1.1.1/24
Portal server	-	4.4.4.2/24		GE3/1/2	3.3.3.1/24
Router B	GE3/1/1	3.3.3.2/24		GE3/1/3	5.5.5.1/24
Router C	GE3/1/1	5.5.5.2/24		GE3/1/4	4.4.4.1/24

10.2 配置思路

为了实现不允许办公区打印机访问互联网资源，需要对 BRAS 设备的接口 GE3/1/2 和 GE3/1/3 发送的报文进行过滤。

10.3 配置步骤

10.3.1 配置 IP 地址及路由

按照图 10-1 配置各接口的 IP 地址，并确保 BRAS 设备和各服务器之间路由可达，具体配置过程略。

10.3.2 配置 BRAS

1. 配置地址池

创建并进入名字为 pool1 的地址池。

```
[BRAS] dhcp enable
[BRAS] dhcp server ip-pool pool1
[BRAS-dhcp-pool-pool1] gateway-list 2.1.1.1 export-route
[BRAS-dhcp-pool-pool1] network 2.1.1.1 16 export-route
[BRAS-dhcp-pool-pool1] quit
[BRAS] dhcp server forbidden-ip 2.1.0.0 2.1.255.255
```

2. 配置认证域

创建并进入名字为 isp3 的 ISP 域。

```
[BRAS] domain name isp3
```

配置 ISP 域 isp3 使用不认证。

```
[BRAS-isp-isp3] authentication ipoe none
[BRAS-isp-isp3] authorization ipoe none
[BRAS-isp-isp3] accounting ipoe none
[BRAS-isp-isp3] authorization-attribute ip-pool pool1
[BRAS-isp-isp3] quit
```

3. 配置静态 IPoE 用户接入

配置 ACL 规则列表 3002，匹配打印机。

```
[BRAS] acl advanced 3002
[BRAS-acl-ipv4-adv-3002] rule 5 deny ip source 2.1.6.1 0
[BRAS-acl-ipv4-adv-3002] quit
```

使能 IPoE 功能，并指定二层接入模式。

```
[BRAS] interface gigabitEthernet 3/1/1
[BRAS-GigabitEthernet3/1/1] ip subscriber l2-connected enable
```

使能未知源 IP 报文触发方式。

```
[BRAS-GigabitEthernet3/1/1] ip subscriber initiator unclassified-ip enable matching-user
```

使能 ARP 报文触发方式。

```
[BRAS-GigabitEthernet3/1/1] ip subscriber initiator arp enable
```

为办公区打印机配置 IP 地址为 2.1.6.1，认证域为 isp3 的静态会话。

```
[BRAS-GigabitEthernet3/1/1] quit
[BRAS]ip subscriber session static ip 2.1.6.1 domain isp3 interface GigabitEthernet3/1/1
request-online gateway ip 2.1.1.1
```

应用 ACL3002 对接口 GigabitEthernet3/1/2 收到的报文进行过滤。

```
[BRAS] interface gigabitEthernet 3/1/2
[BRAS-GigabitEthernet3/1/2] packet-filter 3002 outbound
```

```
[BRAS-GigabitEthernet3/1/2] quit
```

应用 ACL3002 对接口 GigabitEthernet3/1/3 收到的报文进行过滤。

```
[BRAS] interface gigabitEthernet 3/1/3
[BRAS-GigabitEthernet3/1/3] packet-filter 3002 outbound
[BRAS-GigabitEthernet3/1/3] quit
```

10.4 验证配置

查看 IPoE 静态用户打印机的详细信息。

```
<BRAS> display ip subscriber session static verbose
Basic:
  Description                 : -
  Username                    : N/A
  Domain                      : isp3
  VPN instance                : N/A
  IP address                  : 2.1.6.1
  User address type           : N/A
  MAC address                 : 000c-29b6-c756
  Service-VLAN/Customer-VLAN  : -/-
  Access interface            : GE3/1/1
  User ID                     : 0x38080000
  VPI/VCI(for ATM)            : -/-
  VSI Index                   : -
  VSI link ID                 : -
  VXLAN ID                    : -
  DNS servers                 : N/A
  IPv6 DNS servers            : N/A
  DHCP lease                  : N/A
  DHCP remain lease           : N/A
  Access time                 : Mar 21 13:27:21 2016
  Online time(hh:mm:ss)       : 00:00:49
  Service node                : Chassis 1 Slot 3 CPU 0
  Authentication type         : Bind
  IPv4 access type            : Static
  IPv4 detect state           : Detecting
  State                       : Online

AAA:
  ITA policy name             : N/A
  IP pool                     : pool1
  IPv6 pool                   : N/A
  IPv6 nd preifx pool         : N/A
  Primary DNS server          : N/A
  Secondary DNS server        : N/A
  Primary IPv6 DNS server     : N/A
  Secondary IPv6 DNS server   : N/A
  Session idle cut            : 1800 sec, 10240 bytes, direction:Both
  Session duration            : N/A, remaining: N/A
```

```
  Traffic quota               : N/A
  Traffic remained            : N/A
  Acct start-fail action      : Online
  Acct update-fail action     : Online
  Acct quota-out action       : Offline
  Dual-stack accounting mode  : Merge
  Max IPv4 multicast addresses: 4
  IPv4 multicast address list : N/A
  Max IPv6 multicast addresses: 4
  IPv6 multicast address list : N/A
  Accounting start time       : Mar 21 13:27:21 2016
  Subscriber ID               : -

QoS:
  User profile                : N/A
  Session group profile       : N/A
  User group ACL              : N/A
  Inbound CAR                 : N/A
  Outbound CAR                : N/A
  Inbound user priority       : N/A
  Outbound user priority      : N/A

Flow statistic:
  Uplink   packets/bytes      : 43/5179
  Downlink packets/bytes      : 0/0
  IPv6 uplink   packets/bytes : 0/0
  IPv6 downlink packets/bytes : 0/0
```

10.5 配置文件

```
#
dhcp enable
dhcp server forbidden-ip 2.1.0.0 2.1.255.255
#
dhcp server ip-pool pool1
 gateway-list 2.1.1.1 export-route
 network 2.1.0.0 mask 255.255.0.0 export-route
#
ip subscriber session static ip 2.1.6.1 domain isp3 interface GigabitEthernet3/1/1
request-online gateway ip 2.1.1.1
#
interface GigabitEthernet3/1/1
 port link-mode route
 ip subscriber l2-connected enable
 ip subscriber initiator unclassified-ip enable matching-user
#
interface GigabitEthernet3/1/2
 port link-mode route
 ip address 3.3.3.1 255.255.255.0
```

```
 packet-filter 3002 outbound
#
interface GigabitEthernet3/1/3
 port link-mode route
 ip address 5.5.5.1 255.255.255.0
 packet-filter 3002 outbound
#
acl advanced 3002
 rule 5 deny ip source 2.1.6.1 0
#
domain name isp3
 authorization-attribute ip-pool pool1
 authentication ipoe none
 authorization ipoe none
 accounting ipoe none
#
```

11 IPoE Web 用户组多出口配置举例（Radius 授权方式）

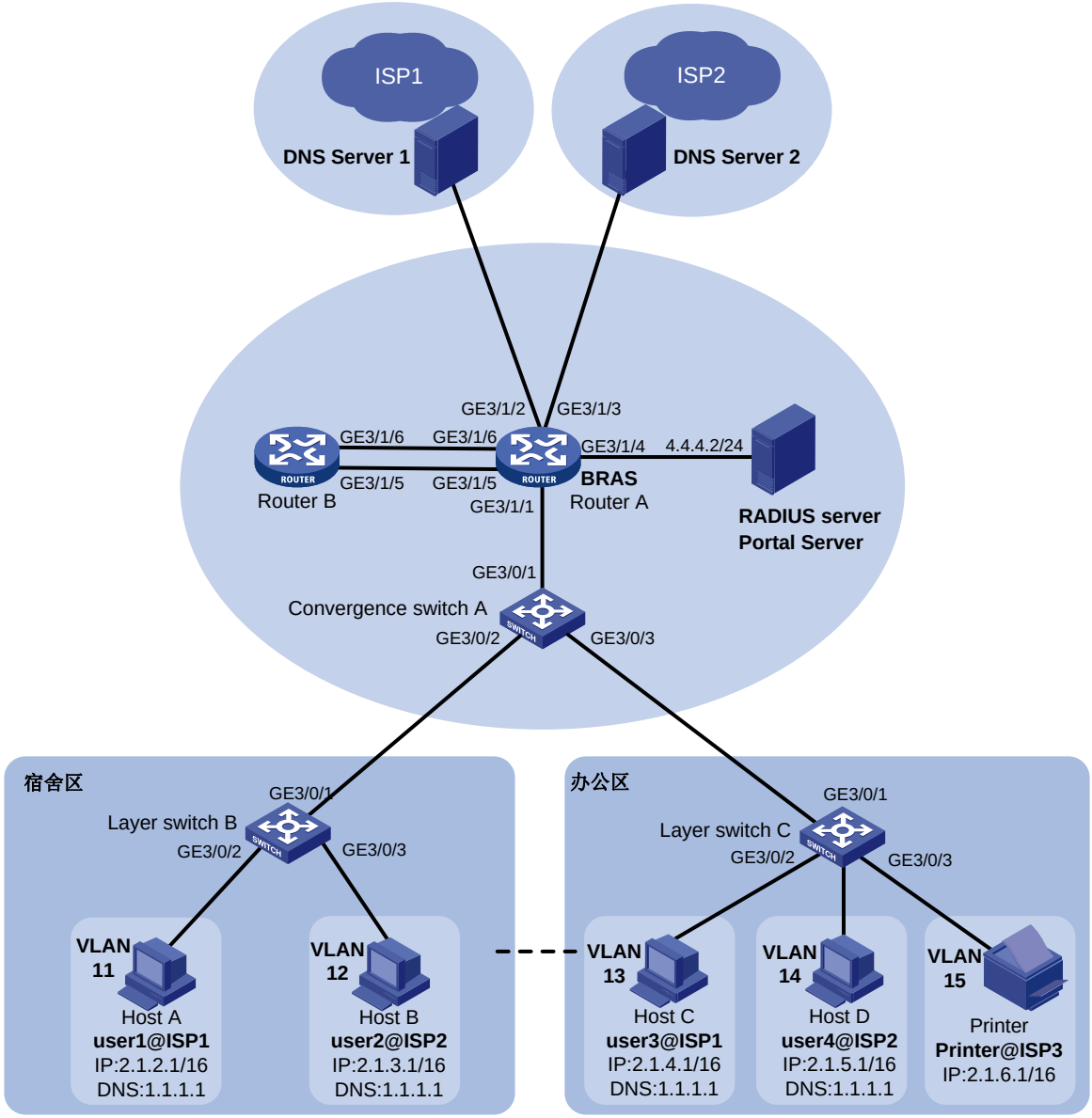
在校园网部署中，常常存在多个运营商出口，而且各出口带宽及资源各不相同。为尽量提高使用体验，下面介绍一个通过用户组来实现流量分担到多个出口的举例。

11.1 组网需求

如图 11-1 所示，某校园网的宿舍区和办公区直挂在 BRAS 下，且 BRAS 作为出口设备分别接不同的运营商 ISP1 和 ISP2，要求实现如下需求：

- 宿舍区和办公区用户通过 IPoE Web 方式接入，在通过认证前，只能访问 Web 服务器；在通过认证后，可以访问互联网资源。
- 办公区打印机通过静态 IPoE 方式接入，不允许访问互联网资源。
- 宿舍区和办公区用户通过在用户名后面增加@ISP1 和@ISP2 的方式携带域名上线，BRAS 则根据域用户对应的用户组来为用户指定固定的运营商出口。
- 用户通过域名方式访问网络资源时被分到的 IP 地址是最优 IP 地址，即用户使用自己所属运营商的 DNS 服务器为其提供域名查询服务。
- 通过远程 AAA 服务器授权用户组的方式实现用户组多出口功能。

图11-1 BRAS 校园网用户组多出口配置举例



设备	接口	IP地址	设备	接口	IP地址
RADIUS server	-	4.4.4.2/24	Router A（BRAS）	GE3/1/1	2.1.1.1/16
Portal server	-	4.4.4.2/24		GE3/1/2	3.3.3.1/24
DNS Server 1	-	3.3.3.2/24		GE3/1/3	5.5.5.1/24
DNS Server 2	-	5.5.5.2/24		GE3/1/4	4.4.4.1/24
Router B	GE3/1/5	-		GE3/1/5	-
	GE3/1/5.100	6.6.100.2/24		GE3/1/5.100	6.6.100.1/24
	GE3/1/5.200	6.6.200.2/24		GE3/1/5.200	6.6.200.1/24
	GE3/1/6	7.7.7.2/24		GE3/1/6	7.7.7.1/24

11.2 配置思路

- RADIUS 服务器上需要配置接入设备，并添加各用户名和密码。
- 为了使深澜软件充当 Portal 服务器的角色，需要在添加接入设备页面设置 Portal 协议和 Portal 密钥。
- 为了对校园网访问进行 IPoE 认证，需要在 BRAS 上配置 Portal 服务器并且使能 IPoE 认证。
- 为了实现通过 RADIUS 来对 IPoE 用户进行认证/授权和计费，需要在 BRAS 上配置 RADIUS 方案并指定相应的认证/授权服务器和计费服务器，并将其应用于 IPoE 用户所属的认证域。
- 为了在 BRAS 和 RADIUS 服务器之间安全地传输用户密码，并且能在 BRAS 上验证 RADIUS 服务器响应报文未被篡改，在 BRAS 和 RADIUS 服务器上都要设置交互报文时所使用的共享密钥（本例共享密钥为 123456）。
- 为了保证实现用户组多出口功能，需要先在 BRAS 上配置不同的用户组 group1 和 group2，分别对应 ISP1 和 ISP2 中的用户，再配置策略路由分别指定各用户组的流量转发出口。
- 为了实现不同的用户使用各自所属运营商的 DNS 服务器为其提供域名查询服务以获取最优的域名解析 IP 地址，可以通过对用户的 DNS 查询报文进行重定向，根据不同的运营商用户进行 NAT 转换，从而将 DNS 查询报文转到各自对应的 DNS 运营商处获取 IP 地址。本例中使用 SR6608 充当 Router B 作为 NAT 转换设备。
- 为通过远程 AAA 服务器授权用户组实现用户组多出口功能，需要在服务器上添加 RADIUS 属性“group1”和“group2”，并设置 RADIUS 属性、控制策略和产品策略。
- 为了实现不允许办公区打印机访问互联网资源，需要对 BRAS 设备的接口 GE3/1/2 和 GE3/1/3 发送的报文进行过滤。

11.3 配置注意事项

为了避免端口号冲突导致服务不可用，需确保内部侦听端口号不是知名协议使用的端口号，且不能被其它基于 TCP 协议的服务占用。已被其他服务占用的 TCP 端口号可以通过 **`display tcp`** 命令查看。

本配置中使用到 User-Group 私有属性，有关私有属性的详细介绍，请参见 14 附录。

11.4 配置步骤

11.4.1 配置 RADIUS 服务器和 Portal 服务器(仅适用于 AAA 远程认证方式)


说明

下面以深澜软件 4.0.9 版本服务器为例，说明 RADIUS 服务器和 Portal 服务器的基本配置。

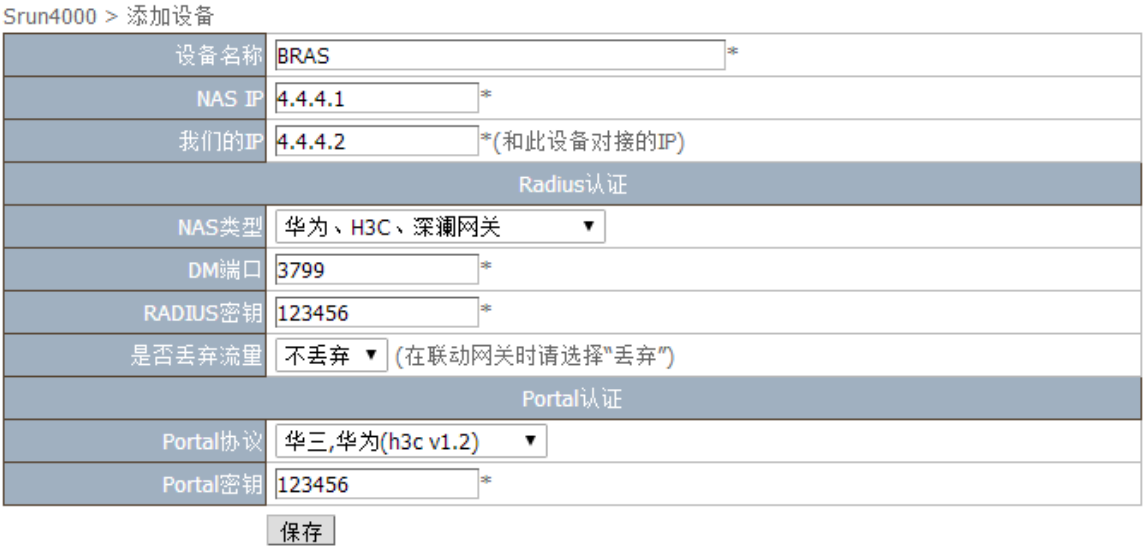
(1) 在浏览器输入“http://4.4.4.2:8081”，登录服务器添加接入设备和 RADIUS 属性。

点击导航栏“设备管理”，选择“添加设备”页签，点击“添加”按钮。

- 设置设备名称为“BRAS”；
- 设置 NAS IP 为“4.4.4.1”；

- 设置我们的 IP 为“4.4.4.2”；
- 选择 NAS 类型为“华为、H3C、深澜网关”；
- 设置 DM 端口为“3799”；
- 设置 RADIUS 密钥为“123456”；
- 选择是否丢弃流量为“不丢弃”；
- 选择 Portal 协议为“华三，华为（h3c v1.2）”；
- 设置 Portal 密钥为“123456”。

图11-2 添加接入设备配置页面



设置 RADIUS 信任。点击导航栏“Radius”， 选择“Radius 信任设置”链接进入 RADIUS 信任设置界面，持续点击右上角“生成”按钮直到生成成功。

选择“RADIUS 服务设置”页签选择用户名校验为“带域名”。

添加 RADIUS 属性“group1”和“group2”，以下以“group1”为例。

点击导航栏“Radius”，选择“添加 Radius 属性”页签，点击“添加”按钮。

- 设置名称为“gp1”（对于 RADIUS 属性“group2”，本处设置为“gp2”）；
- 设置属性名为“group1”（对于 RADIUS 属性“group2”，本处设置为“group2”）；
- 设置 Vendor ID 为“25506”；
- 设置 Vendor name 为“H3C”；
- 设置属性 ID 为“140”；
- 选择值类型为“字符串”；
- 设置字典文件为“dictionary.h3c”；
- 选择 Nas 类型为“华为、H3C、深澜网关”；
- 选择发送条件为“正常用户发送”；
- 设置格式为“%s”；
- 选择可变性为“无（使用固定值）”；

- 设置固定值为“group1”（对于 RADIUS 属性“group2”，本处设置为“group2”）。

图11-3 RADIUS 属性配置页面

(2) 在浏览器输入“https://4.4.4.2:8080”，登录服务器配置策略和用户。

配置控制策略“group1”和“group2”。

进入“策略管理/控制策略”，点击“添加”按钮，添加控制策略。

- 控制策略为“group1”（对于控制策略“group2”，本处设置为“group2”）；
- Radius 下发自定义属性选择“group1”（对于控制策略“group2”，本处设置为“group2”）。

配置产品策略“policy1”和“policy2”。

选择“策略管理/产品策略”页签，点击“添加”按钮，添加产品策略“policy1”和“policy2”，以下以添加“policy1”为例。

- 设置产品名称为“policy1”（对于产品策略“policy2”，本处设置为“policy2”）；
- 选择计费模式为“免费策略”；
- 选择控制策略为“group1”（对于产品策略“policy2”，本处设置为“group2”）；

添加组织结构

选择“系统设置/权限管理/组织结构”页签，点击 图标，分别新建“宿舍区”和“办公区”组织。

添加用户。

选择“用户管理/添加用户”页签，点击“添加”按钮。

- 添加用户 user1：帐号"user1@isp1"，密码“pass1”；选择组织结构为“宿舍区”；选择产品为“policy1”。
- 添加用户 user2：帐号"user2@isp2"，密码“pass2”；选择组织结构为“宿舍区”；选择产品为“policy2”。
- 添加用户 user3：帐号"user3@isp1"，密码“pass3”；选择组织结构为“办公区”；选择产品为“policy1”。

- 添加用户 user4：帐号"user4@isp2"，密码“pass4”；选择组织结构为“办公区”；选择产品为“policy2”。

11.4.2 配置 DNS 服务器

本例中以 Windows Server2003 搭建 DNS 服务器。

在 DNS Server1 中添加域名列表 www.test1.com------100.1.1.1，具体配置过程略。

在 DNS Server2 中添加域名列表 www.test2.com------200.1.1.1，具体配置过程略。

11.4.3 配置 IP 地址及路由

按照图 11-1 配置各接口的 IP 地址，确保 BRAS 设备和 Router B 以及各服务器之间路由可达，具体配置过程略。

11.4.4 配置 BRAS

1. 配置 DHCP 地址池

全局开启 DHCP。

```
[BRAS] dhcp enable
```

创建地址池 pool1，指定该地址池的 DHCPv4 网关和网段地址。

```
[BRAS] dhcp server ip-pool pool1
[BRAS-dhcp-pool-pool1] gateway-list 2.1.1.1 export-route
[BRAS-dhcp-pool-pool1] network 2.1.0.0 16 export-route
[BRAS-dhcp-pool-pool1] forbidden-ip 2.1.1.1
[BRAS-dhcp-pool-pool1] quit
```

配置对地址不一致的 request 报文发送 nak 报文的功能。

```
[BRAS] dhcp server request-ip-address check
```

创建名称为 pool2 的 DHCPv6 地址池并进入其视图。

```
[BRAS] ipv6 dhcp pool pool2
```

配置地址池动态分配的 IPv6 地址网段 192::0/64。

```
[BRAS-dhcp6-pool-pool2] network 192::0/64
[BRAS-dhcp6-pool-pool2] quit
```

将 192::1 设置为禁止地址。

```
[BRAS] ipv6 dhcp server forbidden-address 192::1
```

配置接口 GigabitEthernet3/1/1 工作在 DHCPv6 服务器模式。

```
[BRAS] interface gigabitethernet 3/1/1
[BRAS-GigabitEthernet3/1/1] ipv6 dhcp select server
[BRAS-GigabitEthernet3/1/1] quit
```

配置自动生成 IPv6 链路本地地址，该 IPv6 链路本地地址作为用户的网关。

```
[BRAS-GigabitEthernet3/1/1] ipv6 address 192::1 64
```

取消设备发布 RA 消息的抑制。

```
[BRAS-GigabitEthernet3/1/1] undo ipv6 nd ra halt
```

2. 配置 Portal 认证服务器

配置 IPv4 Portal 认证服务器：名称为 newpt1，IP 地址为 4.4.4.5，密钥为明文 123456。

```
[BRAS] portal server newpt1
[BRAS-portal-server-newpt1] ip 4.4.4.5 key simple 123456
[BRAS-portal-server-newpt1] quit
```

配置 IPv6 Portal 认证服务器：名称为 newpt2，IPv6 地址为 4::5，密钥为明文 123456。

```
[BRAS] portal server newpt2
[BRAS-portal-server-newpt2] ipv6 4::5 key simple 123456
[BRAS-portal-server-newpt2] quit
```

3. 配置 HTTPS 的内部侦听端口

配置 HTTPS 的内部侦听端口，端口不要跟已有端口冲突即可。

```
[BRAS] http-redirect https-port 11111
```

4. 创建本地用户组

创建认证前域用户组，名称为 Web。

```
[BRAS] user-group Web
New user group added.
[BRAS-ugroup-Web] quit
```

创建用户组 group1，名称为 group1。

```
[BRAS] user-group group1
New user group added.
[BRAS-ugroup-group1] quit
```

创建用户组 group2，名称为 group2。

```
[BRAS] user-group group2
New user group added.
[BRAS-ugroup-group2] quit
```

5. 配置 QoS

(1)　配置用于认证前域用户的 ACL 规则

分别为 IPv4 和 IPv6 高级 ACL Web_permit 创建规则如下：匹配用户组 Web 中用户的目的地址为 Portal 服务器地址的报文。

```
[BRAS] acl advanced name Web_permit
[BRAS-acl-ipv4-adv-Web_permit] rule 0 permit ip destination 4.4.4.5 0 user-group Web
[BRAS-acl-ipv4-adv-Web_permit] quit
[BRAS] acl ipv6 advanced name Web_permit
[BRAS-acl-ipv6-adv-Web_permit] rule 0 permit ipv6 destination 4::5 128 user-group Web
[BRAS-acl-ipv6-adv-Web_permit] quit
```

分别为 IPv4 和 IPv6 高级 ACL neiwang 创建规则如下：匹配用户组 Web 中用户的目的地址为内网服务器地址的报文。

```
[BRAS] acl advanced name neiwang
[BRAS-acl-ipv4-adv-neiwang] rule 0 permit ip destination 4.4.4.6 0 user-group Web
[BRAS-acl-ipv4-adv-neiwang] quit
[BRAS] acl ipv6 advanced name neiwang
[BRAS-acl-ipv6-adv-neiwang] rule 0 permit ipv6 destination 4::6 128 user-group Web
[BRAS-acl-ipv6-adv-neiwang] quit
```

分别为 IPv4 和 IPv6 高级 ACL Web_http 创建规则如下：匹配用户组 Web 中用户的目的端口为 80 的 TCP 报文(即 HTTP 报文)。

```
[BRAS] acl advanced name Web_http
```

```
[BRAS-acl-ipv4-adv-Web_http] rule 0 permit tcp destination-port eq www user-group Web
[BRAS-acl-ipv4-adv-Web_http] quit
[BRAS] acl ipv6 advanced name Web_http
[BRAS-acl-ipv6-adv-Web_http] rule 0 permit tcp destination-port eq www user-group Web
[BRAS-acl-ipv6-adv-Web_http] quit
```

分别为 IPv4 和 IPv6 高级 ACL Web_https 创建规则如下：匹配用户组 Web 中用户的目的端口为 443 的 TCP 报文(即 HTTPS 报文)。

```
[BRAS] acl advanced name Web_https
[BRAS-acl-ipv4-adv-Web_https] rule 0 permit tcp destination-port eq 443 user-group Web
[BRAS-acl-ipv4-adv-Web_https] quit
[BRAS] acl ipv6 advanced name Web_https
[BRAS-acl-ipv6-adv-Web_https] rule 0 permit tcp destination-port eq 443 user-group Web
[BRAS-acl-ipv6-adv-Web_https] quit
```

分别为 IPv4 和 IPv6 高级 ACL ip 创建规则如下：匹配用户组 Web 中用户的 IP 报文。

```
[BRAS] acl advanced name ip
[BRAS-acl-ipv4-adv-ip] rule 0 permit ip user-group Web
[BRAS-acl-ipv4-adv-ip] quit
[BRAS] acl ipv6 advanced name ip
[BRAS-acl-ipv6-adv-ip] rule 0 permit ipv6 user-group Web
[BRAS-acl-ipv6-adv-ip] quit
```

分别为 IPv4 和 IPv6 高级 ACL neiwang_out 创建规则如下：匹配用户组 Web 中源地址为内网服务器 IP 地址的报文。

```
[BRAS] acl advanced name neiwang_out
[BRAS-acl-ipv4-adv-neiwang_out] rule 0 permit ip source 4.4.4.6 0 user-group Web
[BRAS-acl-ipv4-adv-neiwang_out] quit
[BRAS] acl ipv6 advanced name neiwang_out
[BRAS-acl-ipv6-adv-neiwang_out] rule 0 permit ipv6 source 4::6 128 user-group Web
[BRAS-acl-ipv6-adv-neiwang_out] quit
```

分别为 IPv4 和 IPv6 高级 ACL Web_out 创建规则如下：匹配用户组 Web 中源地址为 Portal 服务器 IP 地址的报文。

```
[BRAS] acl advanced name Web_out
[BRAS-acl-ipv4-adv-Web_out] rule 0 permit ip source 4.4.4.5 0 user-group Web
[BRAS-acl-ipv4-adv-Web_out] quit
[BRAS] acl ipv6 advanced name Web_out
[BRAS-acl-ipv6-adv-Web_out] rule 0 permit ipv6 source 4::5 128 user-group Web
[BRAS-acl-ipv6-adv-Web_out] quit
```

分别为 IPv4 和 IPv6 高级 ACL redirect_group 创建规则如下：匹配用户组 group1、group2 用户的 IP 报文。

```
[BRAS] acl advanced name redirect_group1
[BRAS-acl-ipv4-adv-redirect_group1] rule 0 permit ip user-group group1
[BRAS-acl-ipv4-adv-redirect_group1] quit
[BRAS] acl ipv6 advanced name redirect_group1
[BRAS-acl-ipv6-adv-redirect_group1] rule 0 permit ipv6 user-group group1
[BRAS-acl-ipv6-adv-redirect_group1] quit
[BRAS] acl advanced name redirect_group2
[BRAS-acl-ipv4-adv-redirect_group2] rule 0 permit ip user-group group2
[BRAS-acl-ipv4-adv-redirect_group2] quit
```

```
[BRAS] acl ipv6 advanced name redirect_group2
[BRAS-acl-ipv6-adv-redirect_group2] rule 0 permit ipv6 user-group group2
[BRAS-acl-ipv6-adv-redirect_group2] quit
```

(2) 配置用于认证前域用户的类

配置类 Web_permit，匹配 ACL Web_permit。

```
[BRAS] traffic classifier Web_permit operator or
[BRAS-classifier-Web_permit] if-match acl name Web_permit
[BRAS-classifier-Web_permit] if-match acl ipv6 name Web_permit
[BRAS-classifier-Web_permit] quit
```

配置类 neiwang，匹配 ACL neiwang。

```
[BRAS] traffic classifier neiwang operator or
[BRAS-classifier-neiwang] if-match acl name neiwang
[BRAS-classifier-neiwang] if-match acl ipv6 name neiwang
[BRAS-classifier-neiwang] quit
```

配置类 Web_http，匹配 ACL Web_http。

```
[BRAS] traffic classifier Web_http operator or
[BRAS-classifier-Web_http] if-match acl name Web_http
[BRAS-classifier-Web_http] if-match acl ipv6 name Web_http
[BRAS-classifier-Web_http] quit
```

配置类 Web_https，匹配 ACL Web_https。

```
[BRAS] traffic classifier Web_https operator or
[BRAS-classifier-Web_https] if-match acl name Web_https
[BRAS-classifier-Web_https] if-match acl ipv6 name Web_https
[BRAS-classifier-Web_https] quit
```

配置类 ip_cpu，匹配 ACL ip。

```
[BRAS] traffic classifier ip_cpu operator or
[BRAS-classifier-ip_cpu] if-match acl name ip
[BRAS-classifier-ip_cpu] if-match acl ipv6 name ip
[BRAS-classifier-ip_cpu] quit
```

配置类 ip_deny，匹配 ACL ip。

```
[BRAS] traffic classifier ip_deny operator or
[BRAS-classifier-ip_deny] if-match acl name ip
[BRAS-classifier-ip_deny] if-match acl ipv6 name ip
[BRAS-classifier-ip_deny] quit
```

配置类 neiwang_out，匹配 ACL neiwang_out。

```
[BRAS] traffic classifier neiwang_out operator or
[BRAS-classifier-neiwang_out] if-match acl name neiwang_out
[BRAS-classifier-neiwang_out] if-match acl ipv6 name neiwang_out
[BRAS-classifier-neiwang_out] quit
```

配置类 Web_out，匹配 ACL Web_out。

```
[BRAS] traffic classifier Web_out operator or
[BRAS-classifier-Web_out] if-match acl name Web_out
[BRAS-classifier-Web_out] if-match acl ipv6 name Web_out
[BRAS-classifier-Web_out] quit
```

配置类 redirect_group1，匹配 ACL redirect_group1。

```
[BRAS] traffic classifier redirect_group1 operator or
[BRAS-classifier-redirect_group1] if-match acl name redirect_group1
[BRAS-classifier-redirect_group1] traffic classifier redirect_group1_v6 operator or
[BRAS-classifier-redirect_group1_v6] if-match acl ipv6 name redirect_group1
[BRAS-classifier-redirect_group1_v6] quit
```

配置类 redirect_group2，匹配 ACL redirect_group2。

```
[BRAS] traffic classifier redirect_group2 operator or
[BRAS-classifier-redirect_group2] if-match acl name redirect_group2
[BRAS-classifier-redirect_group2] traffic classifier redirect_group2_v6 operator or
[BRAS-classifier-redirect_group2_v6] if-match acl ipv6 name redirect_group2
[BRAS-classifier-redirect_group2_v6] quit
```

(3) 配置流行为

配置流行为 Web_permit，允许用户组 Web 中用户的目的地址为 Portal 服务器 IP 地址的报文通过。

```
[BRAS] traffic behavior Web_permit
[BRAS-behavior-Web_permit] filter permit
[BRAS-behavior-Web_permit] free account
[BRAS-behavior-Web_permit] quit
```

配置流行为 neiwang，允许用户组 Web 中用户的目的地址为内网服务器 IP 地址的报文通过。

```
[BRAS] traffic behavior neiwang
[BRAS-behavior-neiwang] filter permit
[BRAS-behavior-neiwang] quit
```

配置流行为 Web_http，对用户组 Web 中用户的目的端口为 80 的 TCP 报文(即 HTTP 报文)重定向到 CPU。

```
[BRAS] traffic behavior Web_http
[BRAS-behavior-Web_http] redirect http-to-cpu
[BRAS-behavior-Web_http] quit
```

配置流行为 Web_https，对用户组 Web 中用户的目的端口为 443 的 TCP 报文(即 HTTPS 报文)重定向到 CPU。

```
[BRAS] traffic behavior Web_https
[BRAS-behavior-Web_https] redirect https-to-cpu
[BRAS-behavior-Web_https] quit
```

配置流行为 Web_cpu，对用户组 Web 中用户的所有 IP 报文都重定向到 CPU。

```
[BRAS] traffic behavior Web_cpu
[BRAS-behavior-Web_cpu] redirect cpu
[BRAS-behavior-Web_cpu] quit
```

配置流行为 Web_deny，禁止用户组 Web 中用户的所有 IP 报文通过。

```
[BRAS] traffic behavior Web_deny
[BRAS-behavior-Web_deny] filter deny
[BRAS-behavior-Web_deny] free account
[BRAS-behavior-Web_deny] quit
```

配置流行为 neiwang_out，允许用户组 Web 中源地址为内网服务器 IP 地址的报文通过。

```
[BRAS] traffic behavior neiwang_out
[BRAS-behavior-neiwang_out] filter permit
[BRAS-behavior-neiwang_out] quit
```

配置流行为 Web_out，允许用户组 Web 中源地址为 Portal 服务器 IP 地址的报文通过。

```
[BRAS] traffic behavior Web_out
[BRAS-behavior-Web_out] filter permit
[BRAS-behavior-Web_out] free account
[BRAS-behavior-Web_out] quit
```

配置流行为 redirect，允许用户组 group1\group2 的 IP 报文重定向到指定下一跳。

```
[BRAS] traffic behavior redirect_group1
[BRAS-behavior-redirect_group1] redirect next-hop 6.6.100.2
[BRAS-behavior-redirect_group1] traffic behavior redirect_group1_v6
[BRAS-behavior-redirect_group1_v6] redirect next-hop 6:6:100::2
[BRAS-behavior-redirect_group1_v6] traffic behavior redirect_group2
[BRAS-behavior-redirect_group2] redirect next-hop 6.6.200.2
[BRAS-behavior-redirect_group2] traffic behavior redirect_group2_v6
[BRAS-behavior-redirect_group2_v6] redirect next-hop 6:6:200::2
[BRAS-behavior-redirect_group2_v6] quit
```

(4) 配置 QoS 策略

配置入方向 QoS 策略 Web

```
[BRAS] qos policy Web
```

为类指定对应的流行为，规则为对于用户组 Web 中的用户：

允许目的地址为 Portal 服务器和内网服务器 IP 地址的报文通过；

对于目的端口为 80（HTTP 报文）和 443（HTTPS 报文）的报文重定向到 CPU；

除上述报文外，其余报文都重定向到 CPU，如果重定向无感知认证失败，则丢弃报文。

```
[BRAS-qospolicy-Web] classifier Web_permit behavior Web_permit
[BRAS-qospolicy-Web] classifier neiwang behavior neiwang
[BRAS-qospolicy-Web] classifier Web_http behavior Web_http
[BRAS-qospolicy-Web] classifier Web_https behavior Web_https
[BRAS-qospolicy-Web] classifier ip_cpu behavior Web_cpu
[BRAS-qospolicy-Web] classifier ip_deny behavior Web_deny
[BRAS-qospolicy-Web] classifier redirect_group1 behavior redirect_group1
[BRAS-qospolicy-Web] classifier redirect_group1_v6 behavior redirect_group1_v6
[BRAS-qospolicy-Web] classifier redirect_group2 behavior redirect_group2
[BRAS-qospolicy-Web] classifier redirect_group2_v6 behavior redirect_group2_v6
[BRAS-qospolicy-Web] quit
```

配置出方向 QoS 策略 out

```
[BRAS] qos policy out
```

为类指定对应的流行为，规则为：允许用户组 Web 中源地址为 Portal 服务器和内网服务器 IP 地址的报文通过，其余报文均禁止通过。

```
[BRAS-qospolicy-out] classifier Web_out behavior Web_out
[BRAS-qospolicy-out] classifier neiwang_out behavior neiwang_out
[BRAS-qospolicy-out] classifier ip_deny behavior Web_deny
[BRAS-qospolicy-out] quit
```

(5) 配置应用策略

对接收的用户流量应用 QoS 策略，策略名为 Web。

```
[BRAS] qos apply policy Web global inbound
```

对发送的上线用户流量应用 QoS 策略，策略名为 out。

```
[BRAS] qos apply policy out global outbound
```

(6) 查看应用的策略是否生效

查看入方向 QoS 策略的配置信息和运行情况。

```
[BRAS] display qos policy global slot 3 inbound
Direction: Inbound
  Policy: Web
   Classifier: Web_permit
     Operator: OR
     Rule(s) :
      If-match acl name Web_permit
      If-match acl ipv6 name Web_permit
     Behavior: Web_permit
      Filter enable: Permit
      Free account enable
   Classifier: neiwang
     Operator: OR
     Rule(s) :
      If-match acl name neiwang
      If-match acl ipv6 name neiwang
     Behavior: neiwang
      Filter enable: Permit
   Classifier: Web_http
     Operator: OR
     Rule(s) :
      If-match acl name Web_http
      If-match acl ipv6 name Web_http
     Behavior: Web_http
      Redirecting:
        Redirect http to CPU
   Classifier: Web_https
     Operator: OR
     Rule(s) :
      If-match acl name Web_https
      If-match acl ipv6 name Web_https
     Behavior: Web_https
      Redirecting:
        Redirect https to CPU
   Classifier: ip_cpu
     Operator: OR
     Rule(s) :
      If-match acl name ip
      If-match acl ipv6 name ip
     Behavior: Web_cpu
      Redirecting:
        Redirect to the CPU
   Classifier: ip_deny
     Operator: OR
     Rule(s) :
```

```
      If-match acl name ip
      If-match acl ipv6 name ip
    Behavior: Web_deny
      Filter enable: Deny
      Free account enable
  Classifier: redirect_group1
    Operator: OR
    Rule(s) :
      If-match acl name redirect_group1
    Behavior: redirect_group1
      Redirecting:
        Redirect to next-hop 6.6.100.2
  Classifier: redirect_group1_v6
    Operator: OR
    Rule(s) :
      If-match acl ipv6 name redirect_group1_v6
    Behavior: redirect_group1_v6
      Redirecting:
        Redirect to next-hop 6:6:100:2
  Classifier: redirect_group2
    Operator: OR
    Rule(s) :
      If-match acl name redirect_group2
    Behavior: redirect_group2
      Redirecting:
        Redirect to next-hop 6.6.200.2
  Classifier: redirect_group2_v6
    Operator: OR
    Rule(s) :
      If-match acl ipv6 name redirect_group2_v6
    Behavior: redirect_group2_v6
      Redirecting:
        Redirect to next-hop 6:6:200:2
```

查看出方向 QoS 策略的配置信息和运行情况。

```
[BRAS] display qos policy global slot 3 outbound
Direction: Outbound
  Policy: out
   Classifier: Web_out
     Operator: OR
     Rule(s) :
       If-match acl name Web_out
       If-match acl ipv6 name Web_out
     Behavior: Web_out
       Filter enable: Permit
       Free account enable
   Classifier: neiwang_out
     Operator: OR
```

```
    Rule(s) :
     If-match acl name neiwang_out
     If-match acl ipv6 name neiwang_out
    Behavior: neiwang_out
     Filter enable: Permit
  Classifier: ip_deny
    Operator: OR
    Rule(s) :
     If-match acl name ip
     If-match acl ipv6 name ip
    Behavior: Web_deny
     Filter enable: Deny
     Free account enable
```

6. 配置 RADIUS 方案

创建名称为 rs1 的 RADIUS 方案并进入该方案视图。

```
[BRAS] radius scheme rs1
```

配置 RADIUS 方案的主认证和主计费服务器及其通信密钥。

```
[BRAS-radius-rs1] primary authentication 4.4.4.1
[BRAS-radius-rs1] primary accounting 4.4.4.1
[BRAS-radius-rs1] key authentication simple radius
[BRAS-radius-rs1] key accounting simple radius
```

配置发送给 RADIUS 服务器的用户名不携带 ISP 域名。

```
[BRAS-radius-rs1] user-name-format without-domain
[BRAS-radius-rs1] quit
```

设置 RADIUS DAE 客户端的 IP 地址为 4.4.4.1，与 RADIUS DAE 客户端交互 DAE 报文时使用的共享密钥为明文 radius。

```
[BRAS] radius dynamic-author server
[BRAS-radius-da-server] client ip 4.4.4.1 key simple radius
[BRAS-radius-da-server] quit
```

7. 配置 User Profile

配置名称为 car 的 User Profile 对上线用户发送的报文进行流量监管。报文正常流速为 5210kbps，允许 325625byte 的突发流量通过，速率小于等于 5210kbps 时正常发送，大于 5210kbps 时，报文被丢弃。

```
[BRAS] user-profile car
[BRAS-user-profile-car] qos car inbound any cir 5210 cbs 325625
[BRAS-user-profile-car] quit
```

8. 配置认证前域和 Web 认证域

配置 IPoE 用户认证前使用的认证域。

```
[BRAS] domain name dm1
[BRAS-isp-dm1] authentication ipoe none
[BRAS-isp-dm1] authorization ipoe none
[BRAS-isp-dm1] accounting ipoe none
```

配置前域授权用户组和地址池。

```
[BRAS-isp-dm1] authorization-attribute user-group Web
```

```
[BRAS-isp-dm1] authorization-attribute ip-pool pool1
[BRAS-isp-dm1] authorization-attribute ipv6-pool pool2
```

配置 Web 认证页面 URL。

```
[BRAS-isp-dm1] Web-server url http://www.h3c.web.com
[BRAS-isp-dm1] Web-server ipv6-url http://www.h3c.web.com
[BRAS-isp-dm1] quit
```

配置 IPoE 用户在 Web 认证阶段使用的认证域。

```
[BRAS] domain name dm2
[BRAS-isp-dm2] authentication ipoe radius-scheme rs1
[BRAS-isp-dm2] authorization ipoe radius-scheme rs1
[BRAS-isp-dm2] accounting ipoe radius-scheme rs1
[BRAS-isp-dm2] authorization-attribute user-profile car
[BRAS-isp-dm2] quit
```

9. 配置 IPoE

开启 IPoE 功能，并配置二层接入模式。

```
[BRAS] interface gigabitethernet 3/1/2
[BRAS-GigabitEthernet3/1/2] ip subscriber l2-connected enable
```

使能未知源 IP 报文触发方式。

```
[BRAS-Route-Aggregation3] ip subscriber initiator unclassified-ip enable matching-user
[BRAS-Route-Aggregation3] ip subscriber initiator unclassified-ipv6 enable matching-user
```

配置 IPoE 用户采用 Web MAC 认证方式。

```
[BRAS-GigabitEthernet3/1/2] ip subscriber authentication-method Web mac-auth
The operation may cut all users on this interface. Continue?[Y/N]:y
```

配置 Web 认证前域为 dm1，Web 认证域和 Web MAC 认证域均为 dm2。

```
[BRAS-GigabitEthernet3/1/2] ip subscriber pre-auth domain dm1
[BRAS-GigabitEthernet3/1/2] ip subscriber Web-auth domain dm2
[BRAS-GigabitEthernet3/1/2] ip subscriber mac-auth domain dm2
[BRAS-GigabitEthernet3/1/2] quit
```

11.4.5 配置 Router B（NAT 设备）

说明

- 此处以 SR6608 路由器作为 NAT 设备进行举例。当以 SR8800-X 路由器作为 NAT 设备时，除当前配置外还必须在配置了 NAT 业务的接口上通过 **nat service** 命令指定提供 NAT 处理的 slot；否则接口的 NAT 功能不生效。有关 **nat service** 命令的详细介绍，请参见对应产品命令手册。
- 为使 DNS 请求和回应报文能够被正确转发，必须确保 Router B 上到用户网段 2.1.0.0/16 的路由出接口仅为 Gigabitethernet3/1/5.100 和 Gigabitethernet3/1/5.200，到 DNS 服务器的路由出接口仅为 Gigabitethernet3/1/6。

1. 配置内部服务器 NAT 转换

在接口 GigabitEthernet3/1/5.100 上配置 NAT 内部服务器，对从该接口收到的 DNS 报文进行目的 IP 地址转换（1.1.1.1->3.3.3.2），对从该接口发送出去的 DNS 报文进行源 IP 地址转换（3.3.3.2->1.1.1.1）。

```
[RouterB] interface gigabitethernet 3/1/5.100
[RouterB-GigabitEthernet3/1/5.100] nat server protocol udp global 1.1.1.1 53 inside 3.3.3.2
53
```

配置接口 GigabitEthernet3/1/5.100 能够终结最外层 VLAN ID 为 100 的 VLAN 报文。

```
[RouterB-GigabitEthernet3/1/5.100] vlan-type dot1q vid 100
[RouterB-GigabitEthernet3/1/5.100] quit
```

在接口 GigabitEthernet3/1/5.200 上配置 NAT 内部服务器，对从该接口收到的 DNS 报文进行目的 IP 地址转换（1.1.1.1->5.5.5.2），对从该接口发送出去的 DNS 报文进行源 IP 地址转换（5.5.5.2->1.1.1.1）。

```
[RouterB] interface gigabitethernet 3/1/5.200
[RouterB-GigabitEthernet3/1/5.200] nat server protocol udp global 1.1.1.1 53 inside 5.5.5.2
53
```

配置接口 GigabitEthernet3/1/5.200 能够终结最外层 VLAN ID 为 200 的 VLAN 报文。

```
[RouterB-GigabitEthernet3/1/5.200] vlan-type dot1q vid 200
[RouterB-GigabitEthernet3/1/5.200] quit
```

2. 配置出方向动态 NAT 转换

配置 ACL 3000，匹配源 IP 地址是 2.1.0.0/16 网段的用户的 DNS 报文和源 IP 地址为 3.3.3.2 和 5.5.5.2 的 DNS Server 的 DNS 报文。

```
[RouterB] acl advanced 3000
[RouterB-acl-ipv4-adv-3000] rule 5 permit udp source 2.1.0.0 0.0.255.255 source-port eq dns
[RouterB-acl-ipv4-adv-3000] rule 10 permit udp source 3.3.3.2 0 source-port eq dns
[RouterB-acl-ipv4-adv-3000] rule 15 permit udp source 5.5.5.2 0 source-port eq dns
[RouterB-acl-ipv4-adv-3000] quit
```

创建一个地址组 1，并添加地址组成员：7.7.7.100～7.7.7.254。

```
[RouterB] nat address-group 1
[RouterB-address-group-1] address 7.7.7.100 7.7.7.254
[RouterB-address-group-1] quit
```

在接口 GigabitEthernet3/1/6 上配置出方向动态地址转换，允许对匹配 ACL 3000 的报文使用地址组 1 中的地址进行地址转换，且在转换的时候使用 UDP 的端口信息。

```
[RouterB] interface gigabitethernet 3/1/6
[RouterB-GigabitEthernet3/1/6] nat outbound 3000 address-group 1
[RouterB-GigabitEthernet3/1/6] quit
```

11.5 验证配置

通过 Portal 认证之前，用户仅能访问 Portal Web 服务器的 Web 认证主页。

图11-4 Portal Web 认证主页示意图

用户通过 Portal 认证之后，可以访问互联网资源。以 Host A 为例，输入用户名 user1@ isp1 和密码 pass1 后，登录成功。

图11-5 用户登录成功示意图

查看用户 user1@isp1 的详细信息。

```
[BRAS] display ip subscriber session verbose
Basic:
  Description                 : -
  Username                    : user1@isp1
  Authorization Domain        : dm2
  Authentication Domain       : dm2
  VPN instance                : N/A
  IP address                  : 2.1.2.1
  IPv6 address                : 192::2
  User address type           : N/A
  MAC address                 : 38ad-befc-1e47
  IPv4 DUID                   : 38ad-befc-1e47
```

```
  Service-VLAN/Customer-VLAN  : -/-
  Access interface            : GE3/1/2
  User ID                     : 0x3000abf2
  VPI/VCI(for ATM)            : -/-
  VSI Index                   : -
  VSI link ID                 : -
  VXLAN ID                    : -
  DNS servers                 : 211.138.24.66
                                211.138.30.66
  IPv6 DNS servers            : 4444::1
  DHCP lease                  : 86400 sec
  DHCP remain lease           : 86242 sec
  DHCPv6 lease                : N/A
  DHCPv6 remain lease         : N/A
  Access time                 : Apr  8 15:19:11 2020
  Online time(hh:mm:ss)       : 00:02:37
  Service node                : Slot 3 CPU 0
  Authentication type         : Web
  IPv4 access type            : DHCP
  IPv6 access type            : DHCP
  IPv4 detect state           : Detecting
  IPv6 detect state           : Detecting
  State                       : Online

AAA:
  ITA policy name             : N/A
  IP pool                     : pool1
  IPv6 pool                   : pool2
  IPv6 nd preifx pool         : N/A
  Primary DNS server          : N/A
  Secondary DNS server        : N/A
  Primary IPv6 DNS server     : 4444::1
  Secondary IPv6 DNS server   : N/A
  Session idle cut            : N/A
  Session duration            : N/A, remaining: N/A
  Traffic quota               : N/A
  Traffic remained            : N/A
  Acct start-fail action      : Online
  Acct update-fail action     : Online
  Acct quota-out action       : Offline
  Dual-stack accounting mode  : Merge
  Max IPv4 multicast addresses: 4
  IPv4 multicast address list : N/A
  Max IPv6 multicast addresses: 4
  IPv6 multicast address list : N/A
  Accounting start time       : Apr  8 15:19:11 2020
  Redirect URL                : N/A
  Redirect IPv6 URL           : N/A
```

```
  Subscriber ID               : -

QoS:
  User profile                : N/A
  Session group profile       : N/A
  User group ACL              : group1 (active)
  Inbound CAR                 : N/A
  Outbound CAR                : N/A
  Inbound user priority       : N/A
  Outbound user priority      : N/A

Flow statistic:
  Uplink   packets/bytes      : 26/1698
  Downlink packets/bytes      : 0/0
  IPv6 uplink   packets/bytes : 0/0
  IPv6 downlink packets/bytes : 0/0
```

打开 Router B 的 NAT 报文调试开关。

```
<RouterB> terminal monitor
<RouterB> terminal debugging
<RouterB> debugging nat packet
```

在 host A 上 ping www.test1.com。

```
C:\Users>ping www.test1.com
正在 Ping www.test1.com [100.1.1.1] 具有 32 字节的数据:
来自 100.1.1.1 的回复: 字节=32 时间=1ms TTL=127
来自 100.1.1.1 的回复: 字节=32 时间=1ms TTL=127
来自 100.1.1.1 的回复: 字节=32 时间=1ms TTL=127
来自 100.1.1.1 的回复: 字节=32 时间=1ms TTL=127
100.1.1.1 的 Ping 统计信息:
    数据包: 已发送 = 4，已接收 = 4，丢失 = 0 (0% 丢失)，
往返行程的估计时间(以毫秒为单位):
    最短 = 1ms，最长 = 1ms，平均 = 1ms
C:\Users>
```

在 Router B 上打印如下 NAT 调试信息。

```
<RouterB>*Apr 10 19:35:23:097 2017 H3C NAT/7/COMMON: -MDC=1-Slot=3;
 PACKET: (GigabitEthernet3/1/5.100-in-config) Protocol: UDP
         2.1.2.1:64192 -         1.1.1.1:   53(VPN:    0) ------>
         2.1.2.1:64192 -         3.3.3.2:   53(VPN:    0)
*Apr 10 19:35:23:097 2017 H3C NAT/7/COMMON: -MDC=1-Slot=3;
 PACKET: (GigabitEthernet3/1/6-out-config) Protocol: UDP
         2.1.2.1:64192 -         3.3.3.2:   53(VPN:    0) ------>
       7.7.7.116: 1754 -         3.3.3.2:   53(VPN:    0)
*Apr 10 19:35:23:098 2017 H3C NAT/7/COMMON: -MDC=1-Slot=3;
 PACKET: (GigabitEthernet3/1/6-in-session) Protocol: UDP
         3.3.3.2:   53 -       7.7.7.116: 1754(VPN:    0) ------>
         3.3.3.2:   53 -         2.1.2.1:64192(VPN:    0)
*Apr 10 19:35:23:098 2017 H3C NAT/7/COMMON: -MDC=1-Slot=3;
 PACKET: (GigabitEthernet3/1/5.100-out-session) Protocol: UDP
         3.3.3.2:   53 -         2.1.2.1:64192(VPN:    0) ------>
```

```
        1.1.1.1:    53 -          2.1.2.1:64192(VPN:     0)
```

以上信息表明，当 Host A 使用 user1@isp1 登录后访问域名 www.test1.com 时，用户发出的目的地址是 1.1.1.1 的 DNS 报文被重定向到 Router B，并由 Router B 经过一些列的 NAT 转换并最终将 DNS 请求报文发送到了 ISP1 的 DNS Server1，由其为 Host A 解析出最优的 IP 地址 100.1.1.1。

11.6 配置文件

- BRAS

```
#
 dhcp enable
 dhcp server request-ip-address check
#
 ipv6 dhcp server forbidden-address 192::1
#
traffic classifier ip_cpu operator or
 if-match acl name ip
 if-match acl ipv6 name ip
#
traffic classifier ip_deny operator or
 if-match acl name ip
 if-match acl ipv6 name ip
#
traffic classifier neiwang operator or
 if-match acl name neiwang
 if-match acl ipv6 name neiwang
#
traffic classifier neiwang_out operator or
 if-match acl name neiwang_out
 if-match acl ipv6 name neiwang_out
#
traffic classifier redirect_group1 operator or
 if-match acl name redirect_group1
#
traffic classifier redirect_group2 operator or
 if-match acl name redirect_group2
#
traffic classifier redirect_group1_v6 operator or
 if-match acl name redirect_group1_v6
#
traffic classifier redirect_group2_v6 operator or
 if-match acl name redirect_group2_v6
#
traffic classifier Web_http operator or
 if-match acl name Web_http
 if-match acl ipv6 name Web_http
#
traffic classifier Web_https operator or
 if-match acl name Web_https
```

```
 if-match acl ipv6 name Web_https
#
traffic classifier Web_out operator or
 if-match acl name Web_out
 if-match acl ipv6 name Web_out
#
traffic classifier Web_permit operator or
 if-match acl name Web_permit
 if-match acl ipv6 name Web_permit
#
traffic behavior http_redirect
 redirect http-to-cpu
#
traffic behavior https_redirect
 redirect https-to-cpu
#
traffic behavior neiwang
 filter permit
#
traffic behavior neiwang_out
 filter permit
#
traffic behavior redirect_group1
 redirect next-hop 6.6.100.2
#
traffic behavior redirect_group2
 redirect next-hop 6.6.200.2
#
traffic behavior redirect_group1_v6
 redirect next-hop 6:6:100::2
#
traffic behavior redirect_group2_v6
 redirect next-hop 6:6:200::2
#
qos policy out
 classifier Web_out behavior Web_out
 classifier neiwang_out behavior neiwang_out
 classifier ip_deny behavior Web_deny
#
qos policy Web
 classifier Web_permit behavior Web_permit
 classifier neiwang behavior neiwang
 classifier Web_http behavior Web_http
 classifier Web_https behavior Web_https
 classifier ip_cpu behavior Web_cpu
 classifier ip_deny behavior Web_deny
 classifier redirect_group1 behavior redirect_group1
 classifier redirect_group1_v6 behavior redirect_group1_v6
```

```
 classifier redirect_group2 behavior redirect_group2
 classifier redirect_group2_v6 behavior redirect_group2_v6
#
user-profile car
 qos car inbound any cir 5120 cbs 365625 ebs 0
#
dhcp server ip-pool pool1
 gateway-list 2.1.1.1 export-route
 network 2.1.0.0 mask 255.255.0.0 export-route
 dns-list 211.138.24.66 211.138.30.66
 forbidden-ip 2.1.1.1
#
ipv6 dhcp pool pool2
 network 192::/64 export-route
 dns-server 4444::1
#
interface GigabitEthernet3/1/2
 port link-mode route
 ipv6 dhcp select server
 ipv6 address 192::1/64
 ipv6 nd autoconfig managed-address-flag
 ipv6 nd autoconfig other-flag
 undo ipv6 nd ra halt
 ip subscriber l2-connected enable
 ip subscriber initiator unclassified-ip enable matching-user
 ip subscriber initiator unclassified-ipv6 enable matching-user
 ip subscriber authentication-method Web mac-auth
 ip subscriber pre-auth domain dm1
 ip subscriber Web-auth domain dm2
 ip subscriber mac-auth domain dm2
#
 qos apply policy Web global inbound
 qos apply policy out global inbound
#
acl advanced name ip
 rule 0 permit ip user-group Web
#
acl advanced name neiwang
 rule 0 permit ip destination 4.4.4.6 0 user-group Web
#
acl advanced name neiwang_out
 rule 0 permit ip source 4.4.4.6 0 user-group Web
#
acl advanced name redirect_group1
 rule 0 permit ip user-group group1
#
acl advanced name redirect_group2
 rule 0 permit ip user-group group2
```

```
#
acl advanced name Web_http
 rule 0 permit tcp destination-port eq www user-group Web
#
acl advanced name Web_https
 rule 0 permit tcp destination-port eq 443 user-group Web
#
acl advanced name Web_out
 rule 0 permit ip source 4.4.4.5 0 user-group Web
#
acl advanced name Web_permit
 rule 0 permit ip destination 4.4.4.5 0 user-group Web
#
acl ipv6 advanced name ip
 rule 0 permit ipv6 user-group Web
#
acl ipv6 advanced name neiwang
 rule 0 permit ipv6 destination 4::6/128 user-group Web
#
acl ipv6 advanced name neiwang_out
 rule 0 permit ipv6 source 4::6/128 user-group Web
#
acl ipv6 advanced name redirect_group1_v6
 rule 0 permit ipv6 user-group group1
#
acl ipv6 advanced name redirect_group2_v6
 rule 0 permit ipv6 user-group group2
#
acl ipv6 advanced name Web_http
 rule 0 permit tcp destination-port eq www user-group Web
#
acl ipv6 advanced name Web_https
 rule 0 permit tcp destination-port eq 443 user-group Web
#
acl ipv6 advanced name Web_out
 rule 0 permit ipv6 source 4::5/128 user-group Web
#
acl ipv6 advanced name Web_permit
 rule 0 permit ipv6 destination 4::5/128 user-group Web
#
radius scheme rs1
 primary authentication 4.4.4.1
 primary accounting 4.4.4.1
 key authentication simple radius
 key accounting simple radius
 user-name-format without-domain
#
radius dynamic-author server
```

```
 client ip 4.4.4.1 key simple radius
#
domain name dm1
 authorization-attribute user-group Web
 authorization-attribute ip-pool pool1
 authorization-attribute ipv6-pool pool2
 authentication ipoe none
 authorization ipoe none
 accounting ipoe none
 Web-server url http://www.h3c.web.com
#
domain name dm2
 authorization-attribute user-profile car
 authentication ipoe radius-scheme rs1
 authorization ipoe radius-scheme rs1
 accounting ipoe radius-scheme rs1
#
user-group group1
#
user-group group2
#
user-group Web
#
portal server newpt1
 ip 4.4.4.5 simple 123456
#
portal server newpt2
 ipv6 4::5 simple 123456
#
 http-redirect https-port 11111
#
```

- Router B（NAT 设备）

```
#
nat address-group 1
 address 7.7.7.100 7.7.7.254
#
interface GigabitEthernet3/1/5
 port link-mode route
#
interface GigabitEthernet3/1/5.100
 ip address 6.6.100.2 255.255.255.0
 nat server protocol udp global 1.1.1.1 53 inside 3.3.3.2 53
 vlan-type dot1q vid 100
#
interface GigabitEthernet3/1/5.200
 ip address 6.6.200.2 255.255.255.0
 nat server protocol udp global 1.1.1.1 53 inside 5.5.5.2 53
 vlan-type dot1q vid 200
```

```
#
interface GigabitEthernet3/1/6
 port link-mode route
 ip address 7.7.7.2 255.255.255.0
 nat outbound 3000 address-group 1
#
acl advanced 3000
 rule 5 permit udp source 2.1.0.0 0.0.255.255 source-port eq dns
 rule 10 permit udp source 3.3.3.2 0 source-port eq dns
 rule 15 permit udp source 5.5.5.2 0 source-port eq dns
#
```

12 ITA 应用配置举例

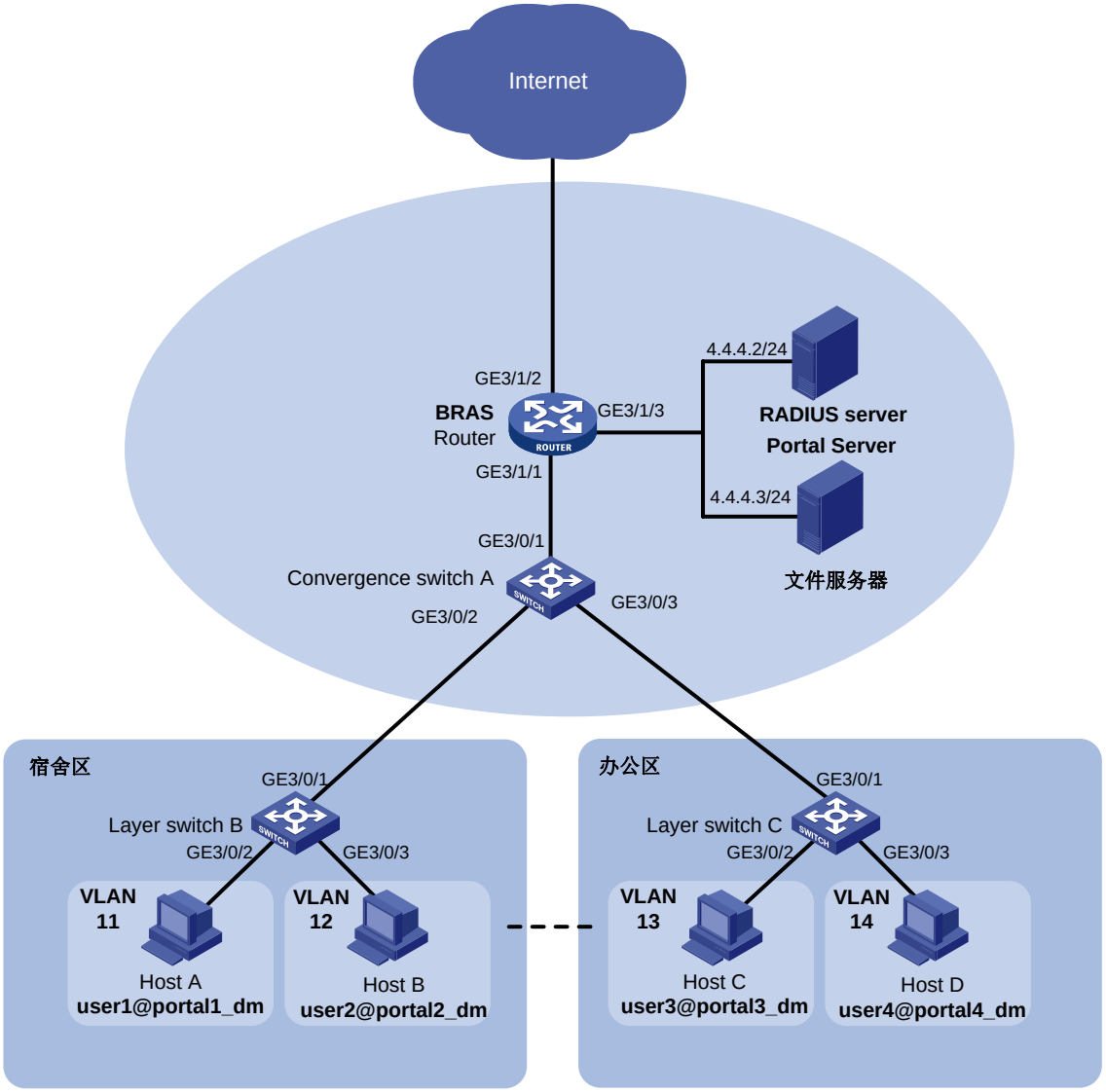
在校园网中，由于出口带宽往往比较有限，而校园内流量又往往比较大，普通的基于账号的带宽限制难以满足要求，因此需要区分不同业务，做出精准控制。如下介绍一个使用 ITA 实现访问内外网分别限速的案例。

12.1 组网需求

如图 12-1 所示，某校园网的宿舍区和办公区部署在 BRAS 下，且校园网中存在大量内部服务器，具体需求如下：

- 宿舍区和办公区用户均通过 Portal 认证接入，未通过身份验证时，仅可以访问 Portal Web 服务器的 Web 认证主页，通过 Portal 认证后，可以访问互联网资源。
- 宿舍区的用户 A 通过 Portal 认证后，访问内网时非 ITA 计费、固定限速 5M，访问外网时非 ITA 计费、AAA 动态授权限速 10M；
- 宿舍区的用户 B 通过 Portal 认证后，访问内网时 ITA 计费、固定限速 5M，访问外网时 ITA 计费、AAA 动态授权限速 10M；
- 办公区的用户 C 通过 Portal 认证后，访问内网时不计费、固定限速 5M，访问外网时非 ITA 计费、AAA 动态授权限速 10M；
- 办公区的用户 D 通过 Portal 认证后，访问内网时 ITA 计费、AAA 动态授权限速 5M，访问外网时 ITA 计费、AAA 动态授权限速 10M；
- 用户 A、B、C 访问外网欠费后仍能访问内网。
- 使用不同的方法实现下发 ITA 策略：对于用户 A、B 和 C，在用户域里下发 ITA 策略；对于用户 D，通过 AAA 服务器下发 ITA 策略。

图12-1 BRAS 校园网 ITA 应用配置举例



设备	接口	IP地址	设备	接口	IP地址
RADIUS server	-	4.4.4.2/24	Router（BRAS）	GE3/1/1	2.1.1.1/24
Portal server	-	4.4.4.2/24		GE3/1/2	3.3.3.1/24
文件服务器	-	4.4.4.3/24		GE3/1/3	4.4.4.1/24

12.2 配置思路

- RADIUS 服务器上需要配置接入设备、RADIUS 属性、计费策略、控制策略（例如配置 AAA 动态授权限速 10M）、产品策略，并添加各用户名和密码。
- 为了使 RADIUS 服务器同时充当 Portal 服务器的角色，需要在添加接入设备页面设置 Portal 协议和 Portal 密钥。
- 为了对校园网访问进行 Portal 认证，需要在 BRAS 上配置 Portal 服务器并且使能 Portal 认证。

- 为了实现通过 RADIUS 来对 Portal 用户进行认证/授权和计费，需要在 BRAS 上配置 RADIUS 方案并指定相应的认证/授权服务器和计费服务器，并将其应用于 Portal 用户所属的认证域。
- 为了在 BRAS 和 RADIUS 服务器之间安全地传输用户密码，并且能在 BRAS 上验证 RADIUS 服务器响应报文未被篡改，在 BRAS 和 RADIUS 服务器上都要设置交互报文时所使用的共享密钥（本例共享密钥为 123456）。
- 由于要对用户访问内网和外网的流量分别进行计费和限速，需要在 BRAS 上配置 ACL、QoS 策略和 ITA 策略。将内网网段流量标记计费级别为 2，设备自动将除内网之外的流量标识为 1。
- 为了实现用户 A 通过 Portal 认证后，访问内网时非 ITA 计费、固定限速 5M，访问外网时非 ITA 计费、AAA 动态授权限速 10M。设备上配置用户 A 的 ITA 策略时：
  - 对内网流量（流量计费级别为 2 的流量）不指定计费类型（不配置 **ipv4** 关键字），即不进行 ITA 计费，并配置其流量监管承诺信息速率为 5000kbps；
  - 不在设备上对外网流量做计费类型和限速配置。
- 为了实现用户 B 通过 Portal 认证后，访问内网时 ITA 计费、固定限速 5M，访问外网时 ITA 计费、AAA 动态授权限速 10M。设备上配置用户 B 的 ITA 策略时：
  - 指定内网流量（流量计费级别为 2 的流量）计费类型为 IPv4（配置 **ipv4** 关键字）进行 ITA 计费，并配置流量监管承诺信息速率为 5000kbps；
  - 指定外网流量计费类型为 IPv4（配置 **ipv4** 关键字），不在设备上配置流量监管承诺信息速率；
  - 开启 ITA 业务流量与用户总计费流量分离功能。
- 为了实现用户 C 通过 Portal 认证后，访问内网时不计费、固定限速 5M，访问外网时非 ITA 计费、AAA 动态授权限速 10M。设备上配置用户 C 的 ITA 策略时：
  - 对内网流量（流量计费级别为 2 的流量）不指定计费类型（不配置 **ipv4** 关键字），即不进行 ITA 计费，并配置其流量监管承诺信息速率为 5000kbps；
  - 不在设备上对外网流量做计费类型和限速配置；
  - 开启 ITA 业务流量与用户总计费流量分离功能。
- 为了实现用户 D 通过 Portal 认证后，访问内网时 ITA 计费、AAA 动态授权限速 5M，访问外网时 ITA 计费、AAA 动态授权限速 10M。配置用户 D 的 ITA 策略时：
  - AAA 服务器上下发 ITA 策略。
  - 设备上指定内网流量（流量计费级别为 2 的流量）计费类型为 IPv4（配置 **ipv4** 关键字）进行 ITA 计费，并配置流量监管承诺信息速率为 5000kbps；
  - 设备上指定外网流量计费类型为 IPv4（配置 **ipv4** 关键字），配置流量监管承诺信息速率为 10000kbps。
- 为了实现用户 A、B、C 访问外网欠费了仍可以访问内网，在 RADIUS 服务器配置访问外网的控制策略 con_pl1 时，设置使用条件为当前访问外网流量不超过 42949672960Byte（40GB），表示当前访问外网流量不超过 42949672960Byte（40GB）时，使用本控制策略，超过就会使用访问内网的控制策略 con_pl2，可继续访问内网。

12.3 配置注意事项

为了避免端口号冲突导致服务不可用，需确保内部侦听端口号不是知名协议使用的端口号，且不能被其它基于 TCP 协议的服务占用。已被其他服务占用的 TCP 端口号可以通过 **display tcp** 命令查看。

本配置中使用到 Accounting-Level、ITA-Policy-Name 私有属性，有关私有属性的详细介绍，请参见 14 附录。

12.4 配置步骤

12.4.1 配置 RADIUS 服务器和 Portal 服务器

说明

下面以深澜软件 4.0.9 版本服务器为例，说明 RADIUS 服务器和 Portal 服务器的基本配置。

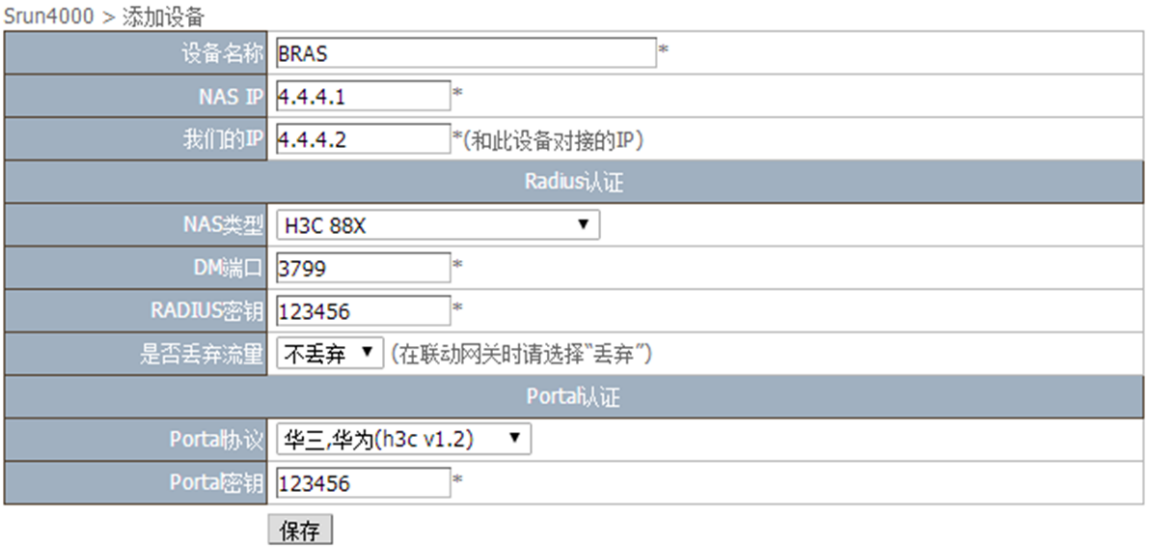
(1) 在浏览器输入“http://4.4.4.2:8081”，登录服务器添加接入设备和 RADIUS 属性。

添加接入设备。

点击导航栏“设备管理”，选择“添加设备”页签，点击“添加”按钮。

- 设置设备名称为“BRAS”；
- 设置 NAS IP 为“4.4.4.1”；
- 设置我们的 IP 为“4.4.4.2”；
- 选择 NAS 类型为“H3C 88X”；
- 设置 DM 端口为“3799”；
- 设置 RADIUS 密钥为“123456”；
- 选择是否丢弃流量为“不丢弃”；
- 选择 Portal 协议为“华三，华为（h3c v1.2）”；
- 设置 Portal 密钥为“123456”。

图12-2 添加接入设备配置页面



设置 RADIUS 信任。点击导航栏“Radius”， 选择“Radius 信任设置”链接进入 RADIUS 信任设置界面，持续点击右上角“生成”按钮直到生成成功。

添加 RADIUS 属性“RADIUS 属性 1”和“RADIUS 属性 2”，以下以“RADIUS 属性 1”为例。

点击导航栏“Radius”，选择“添加 Radius 属性”页签，点击“添加”按钮。

- 设置名称为“RADIUS 属性 1”（对于 RADIUS 属性“RADIUS 属性 2”，本处设置为“RADIUS 属性 2”）；
- 设置属性名为“H3C-Accounting-Level”；
- 设置 Vendor ID 为“25506”；
- 设置 Vendor name 为“H3C”；
- 设置属性 ID 为“215”；
- 选择值类型为“整数”；
- 设置字典文件为“dictionary.h3c”；
- 选择 Nas 类型为“H3C 88X”；
- 选择发送条件为“无条件发送”；
- 设置格式为“%d”；
- 选择可变性为“无（使用固定值）”；
- 设置固定值为“1”（对于 RADIUS 属性“RADIUS 属性 2”属性固定值设置为“2”）。

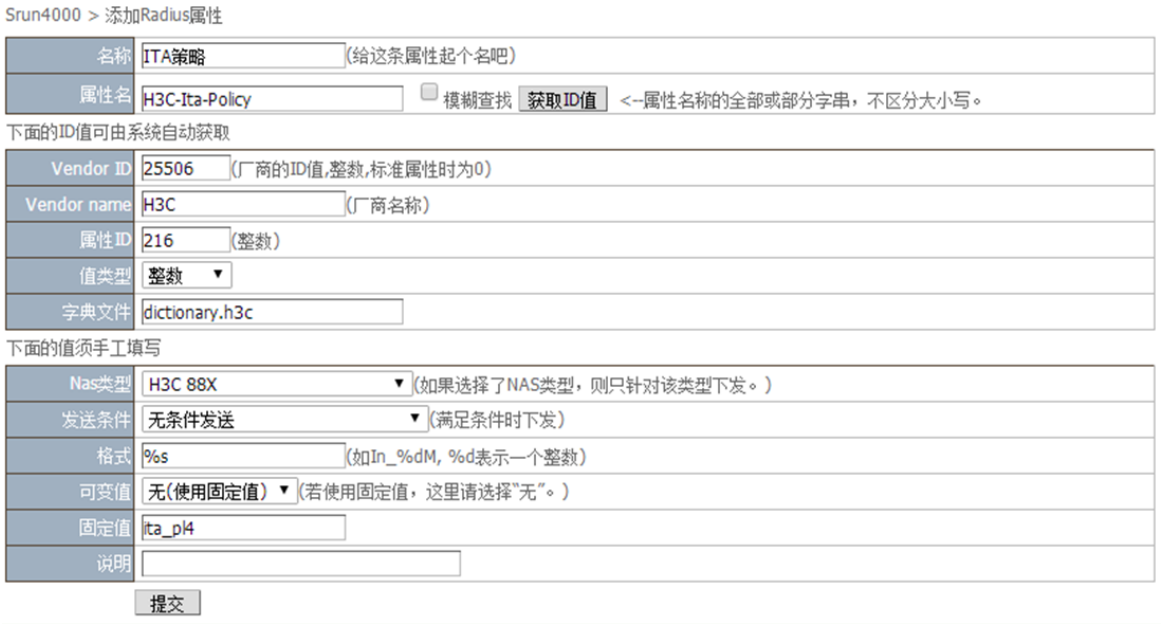
图12-3 RADIUS 属性“RADIUS 属性 1”配置页面

添加 RADIUS 属性“ITA 策略”。

选择“添加 Radius 属性”页签，点击“添加”按钮。

- 设置名称为“ITA 策略”；
- 设置属性名为“H3C-ita-Policy”；
- 设置 Vendor ID 为“25506”；
- 设置 Vendor name 为“H3C”；
- 设置属性 ID 为“216”；
- 选择值类型为“字符串”；
- 设置字典文件为“dictionary.h3c”；
- 选择 Nas 类型为“H3C 88X”；
- 选择发送条件为“无条件发送”；
- 设置格式为“%s”；
- 选择可变性为“无（使用固定值）”；
- 设置固定值为“portal4_dm”。

图12-4 RADIUS 属性“ITA 策略”配置页面



选择“RADIUS 服务设置”页签选择用户名校验为“带域名”。

(2) 在浏览器输入“https://4.4.4.2:8080”，登录服务器配置策略和用户

配置计费策略。

选择“计费策略”页签，点击“添加”按钮。

- 设置计费模式，例如 1GB 收费 5 元。
- 设置消费封顶，例如 100 元。

图12-5 计费策略配置页面

配置对用户 A、B、C 访问外网的控制策略“con_pl1”。

选择“策略管理/控制策略”页签，点击“添加”按钮。

- 设置控制策略为“con_pl1”。
- 选择下行速率为“10Mbps”；
- 选择上行速率为“10Mbps”；

- 选择策略变更模式为“在线变更，下发内置 COA 变更带宽”；
- 选择是否下发内置属性为“是”；
- 选择 COA 下发内置属性为“是”。
- 选择 Radius 下发自定义属性为“RADIUS 属性 1”。
- 设置使用条件为“sum_bytes<=42949672960”，表示当前访问外网流量不超过 42949672960Byte 时，使用本控制策略。

配置对用户 A、B、C 访问内网的控制策略“con_pl2”。

选择“策略管理/控制策略”页签，点击“添加”按钮。

- 设置控制策略为“con_pl2”。
- 选择策略变更模式为“在线变更，下发内置 COA 变更带宽”；
- 选择是否下发内置属性为“是”；
- 选择 COA 下发内置属性为“是”。
- 选择 Radius 下发自定义属性为“RADIUS 属性 2”。

配置对用户 D 的控制策略“con_pl3”。

选择“策略管理/控制策略”页签，点击“添加”按钮，添加控制策略“con_pl3”。

- 设置控制策略为“con_pl3”；
- 选择下行速率为“不限制”；
- 选择上行速率为“不限制”；
- 选择 Radius 下发自定义属性为“ITA 策略”。

配置对用户 A、B、C 的产品策略“policy1”和“policy2”。

选择“策略管理/产品策略”页签，点击“添加”按钮，添加产品策略“policy1”和“policy2”，以下以添加“policy1”为例。

- 设置产品名称为“policy1”（对于产品策略“policy2”，本处设置为“policy2”）；
- 选择计费模式为“流量计费”；
- 选择控制策略为“con_pl1”（对于产品策略“policy2”，本处设置为“con_pl2”）；

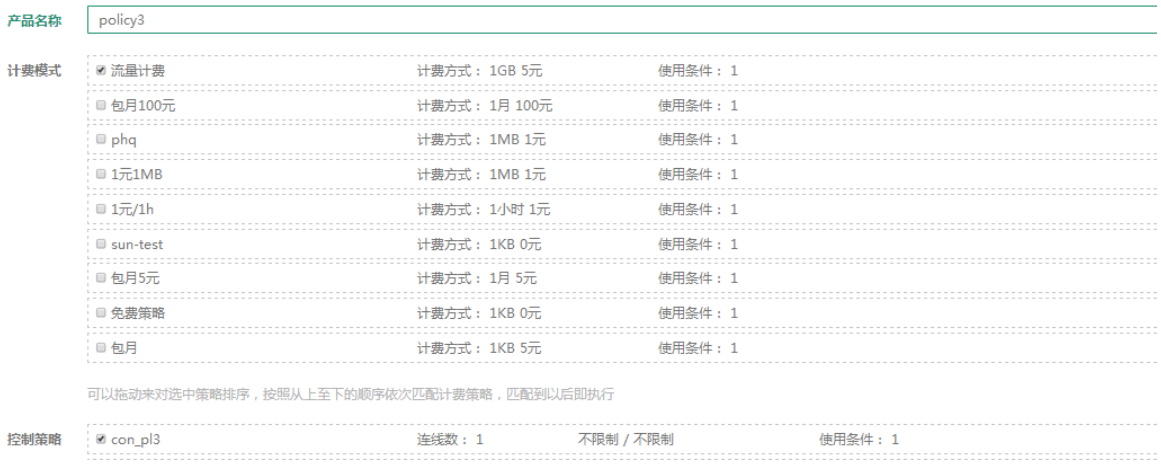
图12-6 产品策略“policy1”配置页面

配置对用户 D 的产品策略“policy3”。

选择“策略管理/产品策略”页签，点击“添加”按钮，添加产品策略“policy3”。

- 设置产品名称为“policy3”；
- 选择计费模式为“流量计费”；
- 选择控制策略为“con_pl3”；

图12-7 产品策略“policy3”配置页面



添加组织结构

选择“系统设置/权限管理/组织结构”页签，点击 图标，分别新建“宿舍区”和“办公区”组织。

添加用户。

选择“用户管理/添加用户”页签，点击“添加”按钮。

- 添加用户 user1：帐号"user1@portal1_dm"，密码“pass1”；选择组织结构为“宿舍区”；选择产品为“policy1”和“policy2”。
- 添加用户 user2：帐号"user2@portal2_dm"，密码“pass2”；选择组织结构为“宿舍区”；选择产品为“policy1”和“policy2”。
- 添加用户 user3：帐号"user3@portal3_dm"，密码“pass3”；选择组织结构为“办公区”；选择产品为“policy1”和“policy2”。
- 添加用户 user4：帐号"user4@portal4_dm"，密码“pass4”；选择组织结构为“办公区”；选择产品为“policy3”。

12.4.2 配置 IP 地址及路由

按照图 12-1 配置各接口的 IP 地址，并确保 BRAS 设备和各服务器之间路由可达，具体配置过程略。

12.4.3 配置 BRAS

1. 配置 DHCP

使能 DHCP 功能。

```
[BRAS] dhcp enable
```

创建 DHCP 地址池 pool1。

```
[BRAS] dhcp server ip-pool pool1
```

配置地址池动态分配的IP地址网段2.1.0.0/16，分配的网关地址2.1.1.1及DNS服务器地址8.8.8.8。

```
[BRAS-dhcp-pool-pool1] network 2.1.0.0 16
[BRAS-dhcp-pool-pool1] gateway-list 2.1.1.1
[BRAS-dhcp-pool-pool1] dns-list 8.8.8.8
```

将 2.1.1.1 设置为禁止分配地址。

```
[BRAS-dhcp-pool-pool1] forbidden-ip 2.1.1.1
[BRAS-dhcp-pool-pool1] quit
```

2. 配置 ACL 和 QoS 策略

配置 ACL 规则列表 3000

```
[BRAS] acl advanced 3000
```

配置匹配用户（用户网段为 2.1.0.0/16）和服务器（服务器网段为 4.4.4.0/24）间互访的报文。

```
[BRAS-acl-ipv4-adv-3000] rule 10 permit ip source 2.1.0.0 0.0.255.255 destination 4.4.4.0
0.0.0.255
[BRAS-acl-ipv4-adv-3000] rule 20 permit ip source 4.4.4.0 0.0.0.255 destination 2.1.0.0
0.0.255.255
```

配置匹配用户（用户网段为 2.1.6.0/16）间互访的报文。

```
[BRAS-acl-ipv4-adv-3000] rule 30 permit ip source 2.1.0.0 0.0.255.255 destination 2.1.0.0
0.0.255.255
[BRAS-acl-ipv4-adv-3000] quit
```

配置流分类器 cl_usern，并设置流匹配规则为用户 ACL 3000 的用户报文。

```
[BRAS] traffic classifier cl_usern
[BRAS-classifier-cl_usern] if-match acl 3000
[BRAS-classifier-cl_usern] quit
```

定义流行为 be_usern，标记计费级别为 2。

```
[BRAS] traffic behavior be_usern
[BRAS-behavior-be_usern] remark account-level 2
[BRAS-behavior-be_usern] quit
```

定义策略 policy_share 并绑定流分类及行为。

```
[BRAS] qos policy policy_share
[BRAS-qospolicy-policy_share] classifier cl_usern behavior be_usern
[BRAS-qospolicy-policy_share] quit
```

在接口上对接收到的上线用户流量应用 QoS 策略。

```
[BRAS] interface gigabitethernet 3/1/1
[BRAS-GigabitEthernet3/1/1] qos apply policy policy_share inbound
[BRAS-GigabitEthernet3/1/1] qos apply policy policy_share outbound
[BRAS-GigabitEthernet3/1/1] quit
```

3. 配置 Radius 方案

创建名字为 rs1 的 Radius 方案并进入该方案视图，指定认证、授权和计费服务器。

```
[BRAS] radius scheme rs1
```

配置 Radius 方案的主认证和主计费服务器及其通信密钥。

```
[BRAS-radius-rs1] primary authentication 4.4.4.2
```

```
[BRAS-radius-rs1] primary accounting 4.4.4.2
[BRAS-radius-rs1] key authentication simple 123456
[BRAS-radius-rs1] key accounting simple 123456
```

设置设备发送 RADIUS 报文使用的源地址。

```
[BRAS-radius-rs1] nas-ip 4.4.4.1
[BRAS-radius-rs1] quit
```

设置 RADIUS DAE 客户端的 IP 地址为 4.4.4.2，与 RADIUS DAE 客户端交互 DAE 报文时使用的共享密钥为明文 123456。

```
[BRAS] radius dynamic-author server
[BRAS-radius-da-server] client ip 4.4.4.2 key simple 123456
[BRAS-radius-da-server] quit
```

4. 配置 ITA 策略

- 配置用户 A 的 ITA 策略

配置 ITA 策略 ita_pl1。

```
[BRAS] ita policy ita_pl1
[BRAS-ita-policy-ita_pl1] accounting-method radius-scheme rs1
```

配置计费级别。

```
[BRAS-ita-policy-ita_pl1] accounting-level 2 car inbound cir 5000 outbound cir 5000
[BRAS-ita-policy-ita_pl1] quit
```

- 配置用户 B 的 ITA 策略

配置 ITA 策略 ita_pl2。

```
[BRAS] ita policy ita_pl2
[BRAS-ita-policy-ita_pl2] accounting-method radius-scheme rs1
```

配置计费级别。

```
[BRAS-ita-policy-ita_pl2] accounting-level 1 ipv4
[BRAS-ita-policy-ita_pl2] accounting-level 2 ipv4 car inbound cir 5000 outbound cir 5000
```

开启 ITA 业务流量与用户总计费流量分离功能。

```
[BRAS-ita-policy-ita_pl2] traffic-separate enable
[BRAS-ita-policy-ita_pl2] quit
```

- 配置用户 C 的 ITA 策略

配置 ITA 策略 ita_pl3。

```
[BRAS] ita policy ita_pl3
[BRAS-ita-policy-ita_pl3] accounting-method radius-scheme rs1
```

配置计费级别。

```
[BRAS-ita-policy-ita_pl3] accounting-level 2 car inbound cir 5000 outbound cir 5000
```

开启 ITA 业务流量与用户总计费流量分离功能。

```
[BRAS-ita-policy-ita_pl3] traffic-separate enable
[BRAS-ita-policy-ita_pl3] quit
```

- 配置用户 D 的 ITA 策略

配置 ITA 策略 ita_pl4。

```
[BRAS] ita policy ita_pl4
[BRAS-ita-policy-ita_pl4] accounting-method radius-scheme rs1
```

配置计费级别。

```
[BRAS-ita-policy-ita_pl4] accounting-level 1 ipv4 car inbound cir 10000 outbound cir 10000
[BRAS-ita-policy-ita_pl4] accounting-level 2 ipv4 car inbound cir 5000 outbound cir 5000
[BRAS-ita-policy-ita_pl4] quit
```

5. 配置认证域

创建并进入名字为 portal1_dm 的 ISP 域。

```
[BRAS] domain name portal1_dm
```

配置 ISP 域使用的 Radius 方案 rs1。

```
[BRAS-isp-portal1_dm] authentication portal radius-scheme rs1
[BRAS-isp-portal1_dm] authorization portal radius-scheme rs1
[BRAS-isp-portal1_dm] accounting portal radius-scheme rs1
```

配置当前 portal1_dm 域使用的 ITA 策略 ita_pl1。

```
[BRAS-isp-portal1_dm] ita-policy ita_pl1
```

创建并进入名字为 portal2_dm 的 ISP 域。

```
[BRAS] domain name portal2_dm
```

配置 ISP 域使用的 Radius 方案 rs1。

```
[BRAS-isp-portal2_dm] authentication portal radius-scheme rs1
[BRAS-isp-portal2_dm] authorization portal radius-scheme rs1
[BRAS-isp-portal2_dm] accounting portal none
```

配置当前 portal2_dm 域使用的 ITA 策略 ita_pl2。

```
[BRAS-isp-portal2_dm] ita-policy ita_pl2
```

创建并进入名字为 portal3_dm 的 ISP 域。

```
[BRAS] domain name portal3_dm
```

配置 ISP 域使用的 Radius 方案 rs1。

```
[BRAS-isp-portal3_dm] authentication portal radius-scheme rs1
[BRAS-isp-portal3_dm] authorization portal radius-scheme rs1
[BRAS-isp-portal3_dm] accounting portal radius-scheme rs1
```

配置当前 portal3_dm 域使用的 ITA 策略 ita_pl3。

```
[BRAS-isp-portal3_dm] ita-policy ita_pl3
```

创建并进入名字为 portal4_dm 的 ISP 域。

```
[BRAS] domain name portal4_dm
```

配置 ISP 域使用的 Radius 方案 rs1。

```
[BRAS-isp-portal4_dm] authentication portal radius-scheme rs1
[BRAS-isp-portal4_dm] authorization portal radius-scheme rs1
[BRAS-isp-portal4_dm] accounting portal radius-scheme rs1
```

6. 配置 Portal 认证

配置 Portal 认证服务器：名称为 newpt，IP 地址为 4.4.4.2，密钥为明文 123456，监听 Portal 报文的端口为 50100。

```
[BRAS] portal server newpt
[BRAS-portal-server-newpt] ip 4.4.4.2 key simple 123456
[BRAS-portal-server-newpt] port 50100
[BRAS-portal-server-newpt] quit
```

配置 Portal Web 服务器的 URL 为 http://4.4.4.2/index_9.html（本处 URL 必须和服务器添加设备后设备表中对应的 Portal 重定向页面内容保持一致）。

```
[BRAS] portal Web-server newpt
[BRAS-portal-Websvr-newpt] url http://4.4.4.2/index_9.html
[BRAS-portal-Websvr-newpt] quit
```

配置对 HTTPS 报文进行重定向的内部侦听端口号。

```
[BRAS] http-redirect https-port 8888
```

在接口 GigabitEthernet3/1/1 上使能直接方式的 Portal 认证。

```
[BRAS] interface gigabitethernet 3/1/1
[BRAS-GigabitEthernet3/1/1] portal enable method direct
```

在接口 GigabitEthernet3/1/1 上引用 Portal Web 服务器 newpt。

```
[BRAS-GigabitEthernet3/1/1] portal apply Web-server newpt
```

在接口 GigabitEthernet3/1/1 上设置发送给 Portal 认证服务器的 Portal 报文中的 BAS-IP 属性值为 2.1.1.1。

```
[BRAS-GigabitEthernet3/1/1] portal bas-ip 2.1.1.1
[BRAS-GigabitEthernet3/1/1] quit
```

12.5 验证配置

用户通过 Portal 认证之前，仅能访问 Portal Web 服务器的 Web 认证主页。

图12-8 Portal Web 认证主页示意图

用户通过 Portal 认证之后，可以访问互联网资源。以用户 A 为例，输入用户名 user1@portal1_dm 和密码 pass1 后，登录成功。

图12-9 用户登录成功示意图

显示用户 A 的详细信息。

```
[BRAS] display portal user ip 2.1.0.1 verbose
Basic:
  Current IP address: 2.1.0.1
  Original IP address: 2.1.0.1
  Username: user1@portal1_dm
  User ID: 0x10000024
  Session-ID: 67890012345679012345678890123453457890126678900123456789O
  Access interface: GigabitEthernet3/1/1
  Service-VLAN/Customer-VLAN: -/-
  MAC address: 001b-21c6-95c1
  Domain name: portal1_dm
  VPN instance: N/A
  Status: Online
  Portal server: sl
  Portal authentication method: Direct
AAA:
  Realtime accounting interval: 720s, retry times: 5
  Idle cut: N/A
  Session duration: 0 sec, remaining: 0 sec
  Remaining traffic: N/A
  Login time: 2016-03-25 15:44:09 UTC
  Online time: 3:4:10
  ITA policy name: ita_pl1
  DHCP IP pool: N/A
ACL&QoS&Multicast:
  Inbound CAR: CIR 10485760 bps PIR 10485760 bps CBS N/A (active)
  Outbound CAR: CIR 10485760 bps PIR 10485760 bps CBS N/A (active)
  Level-2 Inbound CAR: CIR 5120000 bps PIR 5120000 bps
          Outbound CAR: CIR 5120000 bps PIR 5120000 bps
  Inbound priority: N/A
  Outbound priority: N/A
```

```
  ACL number: N/A
  User profile: N/A
  Session group profile: N/A
  Max multicast addresses: 4
  Multicast address list: N/A
  User group: N/A
Flow statistic:
  Uplink   packets/bytes: 1069/132646
  Downlink packets/bytes: 630/120000
  Level-2 uplink   packets/bytes: 500/64000
          downlink packets/bytes: 365/34200
ITA:
  level-2 uplink   packets/bytes: 4/32
          downlink packets/bytes: 2/12
```

通过以上显示信息，可以看出用户 A 访问外网的流量 AAA 动态授权限速 10M，访问内网的流量固定限速 5M，非 ITA 计费。

显示用户 B 的详细信息。

```
[BRAS] display portal user ip 2.1.0.10 verbose
Basic:
  Current IP address: 2.1.0.10
  Original IP address: 2.1.0.10
  Username: user2@portal2_dm
  User ID: 0x10000023
  Session-ID: 67890012345679012345678890123453457890126678900123456789O
  Access interface: GigabitEthernet3/1/1
  Service-VLAN/Customer-VLAN: -/-
  MAC address: 002c-22c7-99d3
  Domain name: portal2_dm
  VPN instance: N/A
  Status: Online
  Portal server: sl
  Portal authentication method: Direct
AAA:
  Realtime accounting interval: 720s, retry times: 5
  Idle cut: N/A
  Session duration: 0 sec, remaining: 0 sec
  Remaining traffic: N/A
  Login time: 2016-03-25 14:53:33 UTC
  Online time: 3:4:10
  ITA policy name: ita_pl2
  DHCP IP pool: N/A
ACL&QoS&Multicast:
  Inbound CAR: CIR 10485760 bps PIR 10485760 bps CBS N/A (active)
  Outbound CAR: CIR 10485760 bps PIR 10485760 bps CBS N/A (active)
  Level-2 Inbound CAR: CIR 5120000 bps PIR 5120000 bps
          Outbound CAR: CIR 5120000 bps PIR 5120000 bps
  Inbound priority: N/A
  Outbound priority: N/A
```

```
  ACL number: N/A
  User profile: N/A
  Session group profile: N/A
  Max multicast addresses: 4
  Multicast address list: N/A
  User group: N/A
Flow statistic:
  Uplink   packets/bytes: 3782/223924
  Downlink packets/bytes: 2629/154291
  Level-1 uplink   packets/bytes: 3074/211168
          downlink packets/bytes: 2060/143268
  Level-2 uplink   packets/bytes: 698/12756
          downlink packets/bytes: 569/11023
ITA:
  level-1 uplink   packets/bytes: 0/0
          downlink packets/bytes: 0/0
  level-2 uplink   packets/bytes: 4/32
          downlink packets/bytes: 2/12
```

通过以上显示信息，可以看出用户 B 访问外网的流量 AAA 动态授权限速 10M，访问内网的流量固定限速 5M，ITA 计费。

显示用户 C 的详细信息。

```
[BRAS] display portal user ip 2.1.0.20 verbose
Basic:
  Current IP address: 2.1.0.20
  Original IP address: 2.1.0.20
  Username: user3@portal3_dm
  User ID: 0x1000002b
  Session-ID: 67890012345679012345678890123453457890126678900123456789O
  Access interface: GigabitEthernet3/1/1
  Service-VLAN/Customer-VLAN: -/-
  MAC address: 005d-23e5-95f5
  Domain name: portal3_dm
  VPN instance: N/A
  Status: Online
  Portal server: sl
  Portal authentication method: Direct
AAA:
  Realtime accounting interval: 720s, retry times: 5
  Idle cut: N/A
  Session duration: 0 sec, remaining: 0 sec
  Remaining traffic: N/A
  Login time: 2016-03-25 17:15:47 UTC
  ITA policy name: ita_pl3
  Online time: 3:4:10
  DHCP IP pool: N/A
ACL&QoS&Multicast:
  Inbound CAR: CIR 10485760 bps PIR 10485760 bps CBS N/A (active)
  Outbound CAR: CIR 10485760 bps PIR 10485760 bps CBS N/A (active)
```

```
  Level-2 Inbound CAR: CIR 5120000 bps PIR 5120000 bps
          Outbound CAR: CIR 5120000 bps PIR 5120000 bps
  Inbound priority: N/A
  Outbound priority: N/A
  ACL number: N/A
  User profile: N/A
  Session group profile: N/A
  Max multicast addresses: 4
  Multicast address list: N/A
  User group: N/A
Flow statistic:
  Uplink   packets/bytes: 15500/50142
  Downlink packets/bytes: 139/6763
  Level-2 uplink   packets/bytes: 1623/3450
          downlink packets/bytes: 65/153
ITA:
  level-2 uplink   packets/bytes: 4/32
          downlink packets/bytes: 2/12
```

通过以上显示信息，可以看出用户 C 访问外网的流量 AAA 动态授权限速 10M，访问内网的流量固定限速 5M，非 ITA 计费。

显示用户 D 的详细信息。外网 AAA 动态授权限速 10M，内网 AAA 动态授权限速 5M。

```
[BRAS] display portal user ip 2.1.0.30 verbose
Basic:
  Current IP address: 2.1.0.30
  Original IP address: 2.1.0.30
  Username: user4@portal4_dm
  User ID: 0x1000002e
  Session-ID: 67890012345679012345678890123453457890126678900123456789O
  Access interface: GigabitEthernet3/1/1
  Service-VLAN/Customer-VLAN: -/-
  MAC address: 008f-65f8-97d6
  Domain name: portal4_dm
  VPN instance: N/A
  Status: Online
  Portal server: sl
  Portal authentication method: Direct
AAA:
  Realtime accounting interval: 720s, retry times: 5
  Idle cut: N/A
  Session duration: 0 sec, remaining: 0 sec
  Remaining traffic: N/A
  Login time: 2016-03-25 17:48:30 UTC
  Online time: 3:4:10
  ITA policy name: ita_pl4
  DHCP IP pool: N/A
ACL&QoS&Multicast:
  Inbound CAR: N/A
  Outbound CAR: N/A
```

```
  Level-1 Inbound CAR: CIR 10240000 bps PIR 10240000 bps
          Outbound CAR: CIR 10240000 bps PIR 10240000 bps
  Level-2 Inbound CAR: CIR 5120000 bps PIR 5120000 bps
          Outbound CAR: CIR 5120000 bps PIR 5120000 bps
  Inbound priority: N/A
  Outbound priority: N/A
  ACL number: N/A
  User profile: N/A
  Session group profile: N/A
  Max multicast addresses: 4
  Multicast address list: N/A
  User group: N/A
Flow statistic:
  Uplink   packets/bytes: 1746/56780
  Downlink packets/bytes: 2218/39684
  Level-1 uplink   packets/bytes: 256/16780
          downlink packets/bytes: 250/26340
  Level-2 uplink   packets/bytes: 120/12300
          downlink packets/bytes: 210/15027
ITA:
  level-1 uplink   packets/bytes: 0/0
          downlink packets/bytes: 0/0
  level-2 uplink   packets/bytes: 4/32
          downlink packets/bytes: 2/12
```

通过以上显示信息，可以看出用户 D 访问外网的流量 AAA 动态授权限速 10M，访问内网的流量固定限速 5M，ITA 计费。

12.6 配置文件

```
#
 dhcp enable
#
traffic classifier cl_usern operator and
 if-match acl 3000
#
traffic behavior be_usern
 remark account-level 2
#
qos policy policy_share
 classifier cl_usern behavior be_usern
#
dhcp server ip-pool pool1
 gateway-list 2.1.1.1
 network 2.1.0.0 mask 255.255.0.0
 dns-list 8.8.8.8
 forbidden-ip 2.1.1.1
#
interface GigabitEthernet3/1/1
 port link-mode route
```

```
 ip address 2.1.1.1 255.255.0.0
 qos apply policy policy_share inbound
 qos apply policy policy_share outbound
 portal enable method direct
 portal bas-ip 2.1.1.1
 portal apply Web-server newpt
#

#
acl advanced 3000
 rule 10 permit ip source 2.1.0.0 0.0.255.255 destination 4.4.4.0 0.0.0.255
 rule 20 permit ip source 4.4.4.0 0.0.0.255 destination 2.1.0.0 0.0.255.255
 rule 30 permit ip source 2.1.0.0 0.0.255.255 destination 2.1.0.0 0.0.255.255
#
radius scheme rs1
 primary authentication 4.4.4.2
 primary accounting 4.4.4.2
 key authentication cipher $c$3$pu+zPzqQg+Eh9/KZTPXoXufp7EEMmCMpSw==
 key accounting cipher $c$3$CKtV37dXqv5zE+EJZbjz2c1xsrQaXYXTog==
 nas-ip 4.4.4.1
#
radius dynamic-author server
 client ip 4.4.4.2 key cipher $c$3$8HFjFX3mSr3v8uEXPro6G3ArmE0L6dGJFQ==
#
ita policy ita_pl1
 accounting-method radius-scheme rs1
 accounting-level 2 car inbound cir 5000 outbound cir 5000
#
ita policy ita_pl2
 accounting-method radius-scheme rs1
 accounting-level 1 ipv4
 accounting-level 2 ipv4 car inbound cir 5000 outbound cir 5000
 traffic-separate enable
#
ita policy ita_pl3
 accounting-method radius-scheme rs1
 accounting-level 2 car inbound cir 5000 outbound cir 5000
 traffic-separate enable
#
ita policy ita_pl4
 accounting-method radius-scheme rs1
 accounting-level 1 ipv4 car inbound cir 10000 outbound cir 10000
 accounting-level 2 ipv4 car inbound cir 5000 outbound cir 5000
#
domain name portal1_dm
 ita-policy ita_pl1
 authentication portal radius-scheme rs1
 authorization portal radius-scheme rs1
```

```
 accounting portal radius-scheme rs1
#
domain name portal2_dm
 ita-policy ita_pl2
 authentication portal radius-scheme rs1
 authorization portal radius-scheme rs1
 accounting portal none
#
domain name portal3_dm
 ita-policy ita_pl3
 authentication portal radius-scheme rs1
 authorization portal radius-scheme rs1
 accounting portal radius-scheme rs1
#
domain name portal4_dm
 authentication portal radius-scheme rs1
 authorization portal radius-scheme rs1
 accounting portal radius-scheme rs1
#
domain name system
#
portal Web-server newpt
 url http://4.4.4.2/index_9.html
#
portal server newpt
 ip 4.4.4.2 key cipher $c$3$Xf8y+egjtWzvz6vWp3DHn79F2+i3vQOEZQ==
#
```

13 相关资料

- H3C SR8800-X 路由器 BRAS 业务配置指导-R7951P11
- H3C SR8800-X 路由器 BRAS 业务命令参考-R7951P11

14 附录

本文档中使用到如下 H3C RADIUS 私有属性，在与其他 RADISU 服务器对接时请确认私有属性匹配。

表14-1 H3C RADIUS 属性支持列表

属性名	属性编号	功能描述
Input-Peak-Rate	1	用户接入到 NAS 的上行峰值速率，以 bps 为单位。
Input-Average-Rate	2	用户接入到 NAS 的上行平均速率，以 bps 为单位。
Output-Peak-Rate	4	从 NAS 到用户的下行峰值速率，以 bps 为单位。

Output-Average-Rate	5	从 NAS 到用户的下行平均速率，以 bps 为单位。
User-Group	140	用户认证成功后下发的用户组，一个用户可以属于多个用户组，多个用户组之间用分号格开
Accounting-Level	215	计费流量的类别，ITA 功能用于表示计费级别，取值范围 1~8
ITA-Policy-Name	216	ITA（Intelligent Target Accounting）策略名称