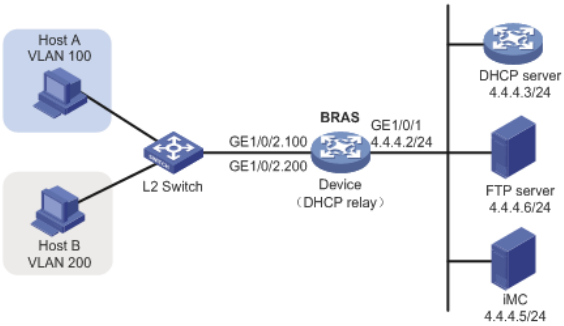
多网段接入IPOE DHCP方式普通WEB认证配置案例

ipoe DHCP 张腾 2019-09-24 发表

组网及说明



1、Host A属于VLAN 100，网段为192.168.100.0/24，并通过BRAS上的GigabitEthernet1/0/2.100接口上线

2、Host B属于VLAN 200，网段为192.168.200.0/24，并通过BRAS上的GigabitEthernet1/0/2.200接口上线

3、Host A和Host B均作为DHCP client经由二层网络以IPoE方式接入到BRAS接入设备

4、BRAS接入设备作为DHCP中继向远端DHCP服务器申请IP地址

5、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

6、FTP server是一台内网服务器

配置步骤

(1) 配置DHCP服务器(即4.4.4.3这台DHCP server，此处由H3C设备充当DHCP server)

全局开启DHCP。

system-view

[DHCP-server] dhcp enable

创建名称为pool1地址池并进入其视图。

[DHCP-server]dhcp server ip-pool pool1

配置地址池动态分配的IP地址网段192.168.100.0/24，分配的网关地址192.168.100.1和DNS服务器地址8.8.8.8。

[DHCP-server-ip-pool-pool1] network 192.168.100.0 24

[DHCP-server-ip-pool-pool1] gateway-list 192.168.100.1

[DHCP-server-ip-pool-pool1] dns-list 8.8.8.8

将192.168.100.1设置为禁止地址。

[DHCP-server-ip-pool-pool1] forbidden-ip 192.168.100.1

[DHCP-server-ip-pool-pool1] quit

创建名称为pool2地址池并进入其视图。

[DHCP-server]dhcp server ip-pool pool2

配置地址池动态分配的IP地址网段192.168.200.0/24，分配的网关地址192.168.200.1和DNS服务器地址8.8.8.8。

[DHCP-server-ip-pool-pool2] network 192.168.200.0 24

[DHCP-server-ip-pool-pool2] gateway-list 192.168.200.1

[DHCP-server-ip-pool-pool2] dns-list 8.8.8.8

将192.168.200.1设置为禁止地址。

[DHCP-server-ip-pool-pool2] forbidden-ip 192.168.200.1

[DHCP-server-ip-pool-pool2] quit

通过配置静态路由，将目的地址为192.168.100.0网段和192.168.200.0网段的DHCP应答报文的下一跳指定为连接DHCP客户端网络的接口IP地址4.4.4.2。

[DHCP-server] ip route-static 192.168.100.0 24 4.4.4.2

[DHCP-server] ip route-static 192.168.200.0 24 4.4.4.2

(2) 配置Device(即BRAS设备)

如果BRAS作为DHCP中继设备的话,配置如下:

a. 配置DHCP relay

全局开启DHCP。

system-view

[Device] dhcp enable

启用DHCP中继的用户地址表项记录功能。

[Device] dhcp relay client-information record

关闭DHCP中继动态用户地址表项定时刷新功能。
[Device] undo dhcp relay client-information refresh enable
创建远端BAS IP地址池pool1，指定匹配该地址池的DHCPv4客户端所在的网段地址，将192.168.100.1设置为禁止地址，并指定远端BAS IP地址池对应的DHCP服务器地址。
[Device]dhcp server ip-pool pool1
[Device-ip-pool-pool1] gateway 192.168.100.1 export-route
[Device-ip-pool-pool1] forbidden-ip 192.168.100.1
[Device-ip-pool-pool1] remote-server 4.4.4.3
[Device-ip-pool-pool1] quit
创建普通IP地址池pool2，配置地址池动态分配的IP地址网段192.168.200.0/24，指定匹配该地址池的DHCPv4客户端所在的网段地址，将192.168.200.1设置为禁止地址，并指定远端BAS IP地址池对应的DHCP服务器地址。
[Device]dhcp server ip-pool pool2
[Device-ip-pool-pool2] gateway-list 192.168.200.1 export-route
[Device-ip-pool-pool2] forbidden-ip 192.168.200.1
[Device-ip-pool-pool2] remote-server 4.4.4.3
[Device-ip-pool-pool2] quit
配置接口GigabitEthernet1/0/2.100的IP地址为192.168.100.1，配置接口工作在DHCP中继模式，并指定DHCP服务器地址为4.4.4.3。
[Device] interface gigabitethernet 1/0/2.100
[Device–GigabitEthernet1/0/2.100] ip address 192.168.100.1 24
[Device–GigabitEthernet1/0/2.100] dhcp select relay
[Device–GigabitEthernet1/0/2.100] **dhcp relay server-address 4.4.4.3**
[Device–GigabitEthernet1/0/2.100] quit
配置接口GigabitEthernet1/0/2.200的IP地址为192.168.100.1，配置接口工作在DHCP中继模式，并指定DHCP服务器地址为4.4.4.3。
[Device] interface gigabitethernet 1/0/2.200
[Device–GigabitEthernet1/0/2.200] ip address 192.168.200.1 24
[Device–GigabitEthernet1/0/2.200] dhcp select relay
[Device–GigabitEthernet1/0/2.200] **dhcp relay server-address 4.4.4.3**
[Device–GigabitEthernet1/0/2.200] quit
如果BRAS作为DHCP server的话，这章节配置改为：
 # 全局开启DHCP。
system-view
[Device] dhcp enable
 # 创建IP地址池pool1，指定网关IP地址为192.168.100.1，掩码长度24，将192.168.100.1设置为禁止地址，并指定DNS服务器地址8.8.8.8。
[Device]dhcp server ip-pool pool1
[Device-ip-pool-pool1] gateway 192.168.100.1
[Device-ip-pool-pool1] forbidden-ip 192.168.100.1
[Device-ip-pool-pool1] dns-list 8.8.8.8
[Device-ip-pool-pool1] network 192.168.100.0 24
 # 创建IP地址池pool2，指定网关IP地址为192.168.200.1，掩码长度24，将192.168.200.1设置为禁止地址，并指定DNS服务器地址8.8.8.8。
[Device]dhcp server ip-pool pool2
[Device-ip-pool-pool2] gateway 192.168.200.1 24
[Device-ip-pool-pool2] forbidden-ip 192.168.200.1
[Device-ip-pool-pool2] dns-list 8.8.8.8
[Device-ip-pool-pool2] network 192.168.200.0 24
 # 配置接口GigabitEthernet1/0/2.100的IP地址为192.168.100.1，并引用IP地址池pool1。
[Device] interface gigabitethernet 1/0/2.100
[Device–GigabitEthernet1/0/2.100] ip address 192.168.100.1 24
[Device–GigabitEthernet1/0/2.100] dhcp server apply ip-pool pool1
 # 配置接口GigabitEthernet1/0/2.200的IP地址为192.168.100.1，并引用IP地址池pool2。
[Device] interface gigabitethernet 1/0/2.200
[Device–GigabitEthernet1/0/2.200] ip address 192.168.200.1 24
[Device–GigabitEthernet1/0/2.200] dhcp server apply ip-pool pool2
b. 配置VLAN终结
配置子接口GigabitEthernet1/0/2.100能够终结最外层VLAN ID为100的VLAN报文。
[Device] interface gigabitethernet 1/0/2.100
[Device–GigabitEthernet1/0/2.100] vlan-type dot1q vid 100
[Device–GigabitEthernet1/0/2.100] quit
配置子接口GigabitEthernet1/0/2.200能够终结最外层VLAN ID为200的VLAN报文。
[Device] interface gigabitethernet 1/0/2.200

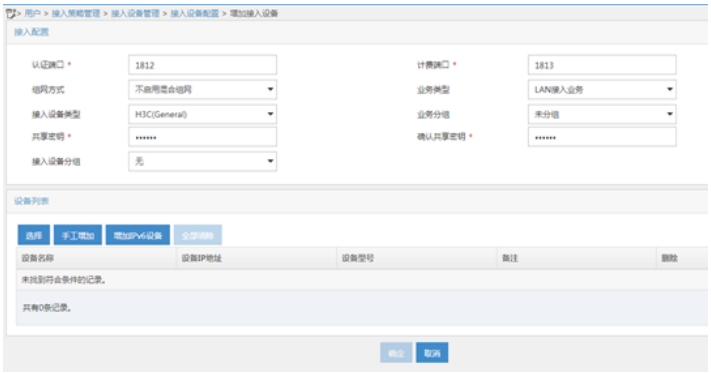
[Device–GigabitEthernet1/0/2.200] vlan-type dot1q vid 200
[Device–GigabitEthernet1/0/2.200] quit
c. 配置Portal认证服务器
配置Portal认证服务器：名称为newpt，IP地址为4.4.4.5，密钥为明文123456。
[Device] portal server newpt
[Device-portal-server-newpt] ip 4.4.4.5 key simple 123456
[Device-portal-server-newpt] quit
d. 配置对HTTPS报文进行重定向的内部侦听端口号
配置对HTTPS报文进行重定向的内部侦听端口号为11111。
[Device] http-redirect https-port 11111
e. 创建本地用户组
创建认证前域用户组，名称为web。
[Device] user-group web
New user group added.
[Device-ugroup-web] quit
f. 配置用于认证前域用户的ACL规则
为IPv4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。
[Device] acl advanced name web_permit
[Device-acl-ipv4-adv-web_permit] rule 0 permit ip destination 4.4.4.5 0 user-group web
[Device-acl-ipv4-adv-web_permit] quit
为IPv4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。
[Device] acl advanced name neiwang
[Device-acl-ipv4-adv-neiwang] rule 0 permit ip destination 4.4.4.6 0 user-group web
[Device-acl-ipv4-adv-neiwang] quit
为IPv4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)。
[Device] acl advanced name web_http
[Device-acl-ipv4-adv-web_http] rule 0 permit tcp destination-port eq www user-group web
[Device-acl-ipv4-adv-web_http] quit
为IPv4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)。
[Device] acl advanced name web_https
[Device-acl-ipv4-adv-web_https] rule 0 permit tcp destination-port eq 443 user-group web
[Device-acl-ipv4-adv-web_https] quit
为IPv4高级ACL ip创建规则如下：匹配用户组web中用户的IP报文。
[Device] acl advanced name ip
[Device-acl-ipv4-adv-ip] rule 0 permit ip user-group web
[Device-acl-ipv4-adv-ip] quit
为IPv4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。
[Device] acl advanced name neiwang_out
[Device-acl-ipv4-adv-neiwang_out] rule 0 permit ip source 4.4.4.6 0 user-group web
[Device-acl-ipv4-adv-neiwang_out] quit
为IPv4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。
[Device] acl advanced name web_out
[Device-acl-ipv4-adv-web_out] rule 0 permit ip source 4.4.4.5 0 user-group web
[Device-acl-ipv4-adv-web_out] quit
g. 配置用于认证前域用户的类
配置类web_permit，匹配ACL web_permit。
[Device] traffic classifier web_permit operator and
[Device-classifier-web_permit] if-match acl name web_permit
[Device-classifier-web_permit] quit
配置类neiwang，匹配ACL neiwang。
[Device] traffic classifier neiwang operator and
[Device-classifier-neiwang] if-match acl name neiwang
[Device-classifier-neiwang] quit
配置类web_http，匹配ACL web_http。
[Device] traffic classifier web_http operator and
[Device-classifier-web_http] if-match acl name web_http
[Device-classifier-web_http] quit
配置类web_https，匹配ACL web_https。
[Device] traffic classifier web_https operator and
[Device-classifier-web_https] if-match acl name web_https

[Device-classifier-web_https] quit
配置类web_deny，匹配ACL ip。
[Device] traffic classifier web_deny operator and
[Device-classifier-web_deny] if-match acl name ip
[Device-classifier-web_deny] quit
配置类neiwang_out，匹配ACL neiwang_out。
[Device] traffic classifier neiwang_out operator and
[Device-classifier-neiwang_out] if-match acl name neiwang_out
[Device-classifier-neiwang_out] quit
配置类web_out，匹配ACL web_out。
[Device] traffic classifier web_out operator and
[Device-classifier-web_out] if-match acl name web_out
[Device-classifier-web_out] quit
h. 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。
[Device] traffic behavior web_permit
[Device-behavior-web_permit] filter permit
[Device-behavior-web_permit] free account
[Device-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。
[Device] traffic behavior neiwang
[Device-behavior-neiwang] filter permit
[Device-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
。
[Device] traffic behavior web_http
[Device-behavior-web_http] redirect http-to-cpu
[Device-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C
PU。
[Device] traffic behavior web_https
[Device-behavior-web_https] redirect https-to-cpu
[Device-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。
[Device] traffic behavior web_deny
[Device-behavior-web_deny] filter deny
[Device-behavior-web_deny] free account
[Device-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。
[Device] traffic behavior neiwang_out
[Device-behavior-neiwang_out] filter permit
[Device-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。
[Device] traffic behavior web_out
[Device-behavior-web_out] filter permit
[Device-behavior-web_out] free account
[Device-behavior-web_out] quit
i. 配置QoS策略
配置入方向QoS策略web
[Device] 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。
[Device-qospolicy-web] classifier web_permit behavior web_permit
[Device-qospolicy-web] classifier neiwang behavior neiwang
[Device-qospolicy-web] classifier web_http behavior web_http
[Device-qospolicy-web] classifier web_https behavior web_https
[Device-qospolicy-web] classifier web_deny behavior web_deny
[Device-qospolicy-web] quit
配置出方向QoS策略out
[Device] 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。

[Device-qospolicy-out] classifier web_out behavior web_out
[Device-qospolicy-out] classifier neiwang_out behavior neiwang_out
[Device-qospolicy-out] classifier web_deny behavior web_deny
[Device-qospolicy-out] quit
j. 配置应用策略
对接收的用户流量应用QoS策略，策略名为web。
[Device] 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。
[Device] qos apply policy out global outbound
k. 配置RADIUS方案
创建名称为rs1的RADIUS方案并进入该方案视图。
[Device] 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。
[Device-radius-rs1] primary authentication 4.4.4.5
[Device-radius-rs1] primary accounting 4.4.4.5
[Device-radius-rs1] key authentication simple radius
[Device-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。
[Device-radius-rs1] user-name-format without-domain
[Device-radius-rs1] quit
（可选）开启RADIUS session control功能（使用iMC作为RADIUS服务器时建议配置该功能）。
[Device] radius session-control enable
l. **配置认证前域和Web认证域（注意认证前域不需要授权地址池）**
配置IPoE用户认证前使用的认证域。
[Device] domain name dm1
[Device-isp-dm1] authentication ipoe none
[Device-isp-dm1] authorization ipoe none
[Device-isp-dm1] accounting ipoe none
配置认证前域授权用户组。
[Device-isp-dm1] authorization-attribute user-group web
配置Web认证页面URL和Web认证服务器IP地址。
[Device-isp-dm1] web-server url http://4.4.4.5:8080/portal/
[Device-isp-dm1] web-server ip 4.4.4.5
[Device-isp-dm1] quit
配置IPoE用户在Web认证阶段使用的认证域。
[Device] domain name dm2
[Device-isp-dm2] authentication ipoe radius-scheme rs1
[Device-isp-dm2] authorization ipoe radius-scheme rs1
[Device-isp-dm2] accounting ipoe radius-scheme rs1
[Device-isp-dm2] quit
m. 配置IPoE
在子接口GigabitEthernet1/0/2.100和子接口GigabitEthernet1/0/2.200上开启IPoE功能，并配置二层接入模式。
[Device] interface range gigabitethernet 1/0/2.100 gigabitethernet 1/0/2.200
[Device–if-range] ip subscriber l2-connected enable
配置IPoE用户采用Web认证方式。
[Device–if-range] 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。
[Device–if-range] ip subscriber pre-auth domain dm1
[Device–if-range] ip subscriber web-auth domain dm2
[Device–if-range] quit

---

(3) 配置RADIUS服务器
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1-1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1-1 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1-2所示页面输入接入设备地址4.4.4.2并单击<确定>。

图1-2 手动增加接入设备

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1-3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1-3 增加接入策略

增加接入服务

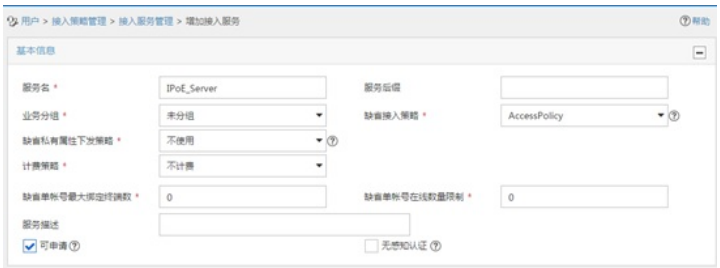
单击导航树中的[接入策略管理/接入服务管理]菜单项，进入接入服务管理页面，在该页面中单击<增加>按钮，进入如图1-4所示增加接入服务页面。

¡ 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。

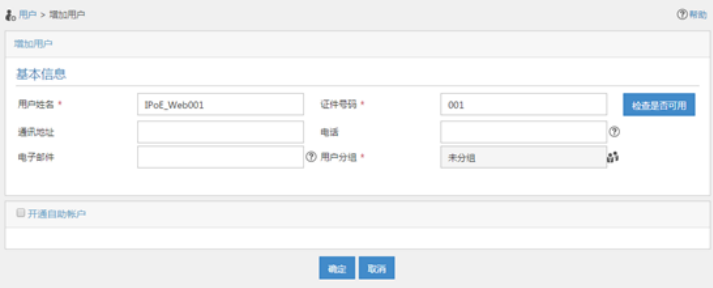
图1-4 增加接入服务



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1-5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1-5 增加用户



单击<确定>按钮后完成用户的添加。

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1-6所示增加接入用户页面。

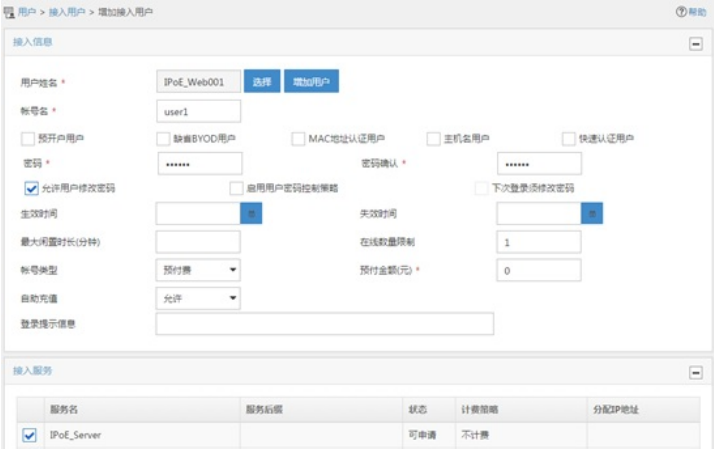
¡ 用户姓名选择：IPoE_Web001

¡ 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1-6 增加接入用户



(4) 配置Portal服务器

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1-7所示。

图1-7 Portal服务器配置页面

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1-8所示。

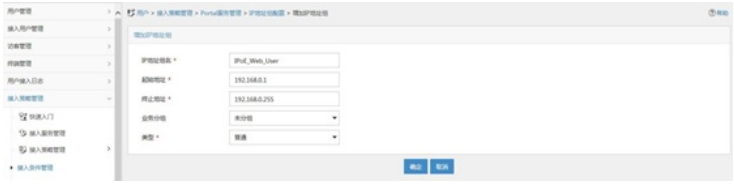
¡ 输入IP地址组名为“IPoE_Web_User”。

¡ 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1-8 增加IP地址组配置页面



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1-9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GigabitEthernet1/0/1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1-9 增加设备信息配置页面

配置端口组信息

如图1-10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1-10 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1-11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1-11 增加端口组信息配置页面

配置关键点

1、多网段接入组网，只需要一个认证前域，认证前域不需要授权地址池，而是在对应的子接口调用所属网段的地址池；

2、 接口上开启了IPoE功能后，**缺省情况下丢弃接收到的用户报文，需要配置IPoE用户触发方式**：

ip subscriber initiator dhcp enable 开启DHCP报文触发方式

ip subscriber initiator arp enable 开启ARP报文触发用户上线功能

ip subscriber initiator unclassified-ip enable matching-user 开启未知源IP报文触发方式

三种触发方式是选配的，例如DHCP给终端下发地址的场景，需开启 ip subscriber initiator dhcp

enable，否则设备收到终端的discover报文也会丢弃；
3、典型配置里没有配置 ip subscriber initiator dhcp enable 是因为
B75主线版本DHCP触发命令没有了，IPoE Web开启后即认为是DHCP触发，至于ARP触发、未知源IP触发看场景的，这里是非必配。
如果参考以上配置终端无法获取地址，说明版本不是B75主线版本，则需要在对应子接口下开启DHCP报文触发方式：
[Device] interface range gigabitethernet 1/0/2.100 gigabitethernet 1/0/2.200
[Device–if-range] ip subscriber initiator dhcp enable