

H3C 无线控制器

远程 IPv6 Portal 认证典型配置举例(V7)

资料版本：6W100-20191125

Copyright © 2019 新华三技术有限公司 版权所有，保留一切权利。

非经本公司书面许可，任何单位和个人不得擅自摘抄、复制本文档内容的部分或全部，并不得以任何形式传播。

除新华三技术有限公司的商标外，本手册中出现的其它公司的商标、产品标识及商品名称，由各自权利人拥有。

本文档中的信息可能变动，恕不另行通知。

目 录

1 简介.....	1
2 配置前提.....	1
3 配置举例.....	1
3.1 组网需求.....	1
3.2 配置思路.....	1
3.3 配置注意事项.....	2
3.4 配置步骤.....	2
3.4.1 配置 iMC.....	2
3.4.2 配置 AC.....	10
3.4.3 配置 Switch.....	14
3.5 验证配置.....	16
3.6 配置文件.....	17
4 相关资料.....	20

1 简介

本文档介绍 IPv6 远程 Portal 认证典型配置举例。

2 配置前提

本文档适用于使用 Comware V7 软件版本的无线控制器和接入点产品，不严格与具体软、硬件版本对应，如果使用过程中与产品实际情况有差异，请参考相关产品手册，或以设备实际情况为准。

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。

本文档假设您已了解 AAA、Portal 认证和 WLAN 特性。

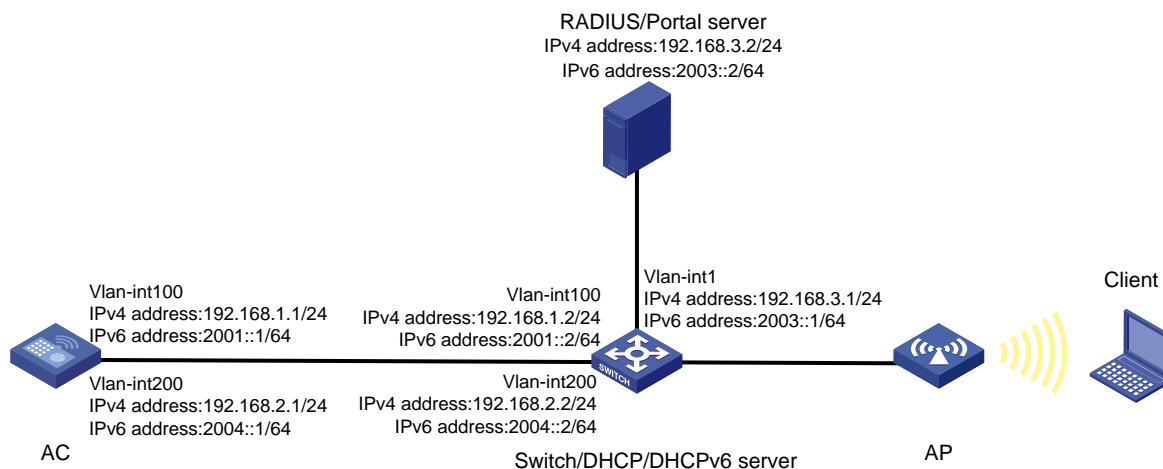
3 配置举例

3.1 组网需求

如图 1 所示，Switch 作为 DHCP 和 DHCPv6 server 为 AP 和 Client 分配 IPv4 和 IPv6 地址，要求：

- 对无线用户采用直接方式的 Portal 认证。
- 采用一台 iMC 承担 Portal 认证服务器和 Portal Web 服务器的职责。
- 采用 RADIUS 服务器作为认证/计费服务器。

图1 Portal 远程认证组网图



3.2 配置思路

- 为了使用户可以在 VLAN 内的任何二层端口上访问网络资源，且移动接入端口时无须重复认证，必须开启 Portal 用户漫游功能。

- 短时间内 Portal 客户端的频繁上下线可能会造成 Portal 认证失败,需要关闭 Portal 客户端 ARP 表项固化功能。
- 为了使服务器对用户授权信息进行动态修改或强制用户下线,必须开启 RADIUS session control 功能。
- 为了使用户通过一次 Portal 认证既能访问 IPv4 网络也能访问 IPv6 网络,需要开启 Portal 支持双协议栈功能。

3.3 配置注意事项

- 配置 AP 的序列号时请确保该序列号与 AP 唯一对应,AP 的序列号可以通过 AP 设备背面的标签获取。
- AC 上配置的 Portal 认证服务器、Portal Web 服务器的服务器类型必须与实际服务器一致。
- 设备重定向给用户的 Portal Web 服务器的 URL 默认是不携带参数,需要根据实际应用手动添加需要携带的参数信息

3.4 配置步骤

3.4.1 配置iMC



说明

下面以 iMC 为例(使用 iMC 版本为: iMC PLAT 7.1、iMC EIA 7.1、iMC EIP 7.1)说明 RADIUS server 和 Portal server 的基本配置。

(1) 配置 RADIUS server

增加接入设备

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,单击<增加>按钮,进入“增加接入设备”页面。

- 设置认证、计费共享密钥为 radius,该共享密钥与 AC 上配置 RADIUS 服务器时的密钥一致,其它保持缺省配置;
- 单击<手工增加>按钮,进入“手工增加接入设备”页面,填写起始 IP 地址为 192.168.1.1,单击<确定>按钮完成操作。
- 单击<增加 IPv6 设备>按钮,进入“手工增加接入设备”页面,添加 IPv6 地址为 2001::1 的接入设备。

图2 增加接入设备

用户 > 接入策略管理 > 接入设备管理 > 接入设备配置 > 增加接入设备 ? 帮助

接入配置

认证端口 *	1812	计费端口 *	1813
组网方式	不启用混合组网	业务类型	LAN接入业务
接入设备类型	H3C(General)	业务分组	未分组
共享密钥 *	●●●●	确认共享密钥 *	●●●●
接入设备分组	无		

设备列表

设备名称	设备IP地址	设备型号	备注	删除
未找到符合条件的记录。				

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，单击<增加>按钮，进入“增加接入策略”页面。

- 填写接入策略名；
- 选择业务分组；
- 其它参数可采用缺省配置。

图3 增加接入策略配置

用户 > 接入策略管理 > 接入策略管理 > 增加接入策略

基本信息

接入策略名 *	AccessPolicy
业务分组 *	未分组
描述	

授权信息

接入时段	无	分配IP地址 *	否
下行速率(Kbps)		上行速率(Kbps)	
优先级		<input type="checkbox"/> 启用RSA认证	
证书认证	<input checked="" type="radio"/> 不启用 <input type="radio"/> EAP证书认证 <input type="radio"/> WAPI证书认证		
认证证书类型	EAP-TLS认证		
下发VLAN		下发用户组	
<input type="checkbox"/> 下发User Profile			
<input type="checkbox"/> 下发ACL			

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，单击<增加>按钮，进入“增加接入服务”页面。

- 填写服务名；
- 缺省接入策略选择已配置好的接入策略；
- 其它参数可采用缺省配置。

图4 增加接入服务配置

用户 > 接入策略管理 > 接入服务管理 > 增加接入服务

基本信息

服务名 * RadiusServer 服务后缀

业务分组 * 未分组 缺省接入策略 * AccessPolicy

缺省安全策略 * 不使用 缺省内网外连策略 * 不使用

缺省私有属性下发策略 * 不使用 缺省单帐号最大绑定终端数 * 0 缺省单帐号在线数量限制 * 0

服务描述

可申请 Portal无感知认证

接入场景列表

增加

名称	接入策略	安全策略	私有属性下发策略	内网外连策略	优先级	修改	删除
未找到符合条件的记录。							

确定 取消

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，单击<增加>按钮，进入增加接入用户页面。在接入信息部分：

- 如果用户已存在，用户姓名选择可接入的用户，如果用户不存在，则需要单击<增加用户>按钮添加新用户；
- 填写账号名；
- 设置密码；
- 选中之前配置的服务；
- 其它参数可采用缺省配置。

图5 增加接入用户

The screenshot shows the 'Add Access User' configuration page. The 'Access Information' section includes fields for 'User Name' (Client1), 'Account Name' (Client), and 'Password'. There are several checkboxes for user types: 'Pre-open User', 'Default BYOD User', 'MAC Address Authentication User', 'Host Name User', and 'Fast Authentication User'. Other options include 'Allow User to Change Password', 'Enable User Password Control Strategy', and 'Require Password Change on Next Login'. Fields for 'Validity Period', 'Expiration Time', 'Maximum Idle Time (minutes)', and 'Online Quantity Limit' (set to 1) are also present. The 'Access Service' section shows a table with one entry: 'RadiusServer' with a status of 'Applicable' and an assigned IP address.

(2) 配置 Portal server

配置 Portal 认证服务。

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/Portal 服务管理/服务器配置]菜单项，进入服务器配置页面。

- 根据实际组网情况调整以下参数，本例中使用缺省配置。

图6 Portal 认证服务器配置页面

The screenshot shows the 'Portal Server Configuration' page. The 'Basic Information' section has a 'Log Level' dropdown set to 'Info'. The 'Portal Server' section includes 'Request Timeout (seconds)' (4), 'User Center Query Timeout (minutes)' (5), 'Request Timeout (seconds)' (20), and 'LB Device Address'. The 'Portal Web' section includes 'Request Timeout (seconds)' (15), 'Check User Request Text', 'HTTP Interface Display Method' (set to 'None'), 'Authentication Code', 'Use Cache' (set to 'Yes'), and 'HTTPS Interface Display Method' (set to 'None'). The 'Portal URL' field contains a list of URLs: http://192.168.3.2:8080/portal/, https://192.168.3.2:8443/portal/, http://[2003::2]:8080/portal/, and https://[2003::2]:8443/portal/. The 'Advanced Information' section shows a table for 'Service Instance List' with columns for 'Service Instance Name' and 'Service Type', and a 'Confirm' button at the bottom.

配置 IP 地址组。

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 Portal 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。

- 填写 IP 地址组名；
- IPv6 选择“是”（仅 IPv6，IPv4 地址选“否”）；
- 输入起始地址和终止地址，输入的地址范围中应包含用户主机的 IP 地址；
- 选择业务分组，本例中使用缺省的“未分组”；
- 选择 IP 地址组的类型为“普通”。（仅 IPv4 地址组配置本项）

图7 增加 IPv4 地址组配置页面

用户 > 接入策略管理 > Portal服务管理 > IP地址组配置 > 增加IP地址组

增加IP地址组

IP地址组名 *	Portal_user4
IPv6 *	否
起始地址 *	192.168.2.1
终止地址 *	192.168.2.255
业务分组	未分组
类型 *	普通

确定 取消

图8 增加 IPv6 地址组配置页面

用户 > 接入策略管理 > Portal服务管理 > IP地址组配置 > 增加IP地址组

增加IP地址组

IP地址组名 *	Portal_user6
IPv6 *	是
起始地址 *	2004::1
终止地址 *	2004::FFFF:FFFF:FFFF:FFFF
业务分组	未分组

确定 取消

增加 Portal 设备。

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 Portal 设备配置页面，在该页面中单击<增加>按钮，进入增加设备信息配置页面。

- 填写设备名；
- IPv4 用户版本选择“Portal 2.0”，IPv6 用户版本选择“Portal 3.0”；
- 指定 IP 地址为与接入用户相连的设备接口 IP；
- 选择是否支持逃生心跳功能和用户心跳功能，本例中选择否。
- 输入密钥，与 AC 上的配置保持一致；
- 选择组网方式为直连；
- 其它参数可采用缺省配置。

图9 增加 IPv4 设备信息配置页面

用户 > 接入策略管理 > Portal服务管理 > 设备配置 > 增加设备信息

增加设备信息

设备信息

设备名 *	NAS4	业务分组 *	未分组
版本 *	Portal 2.0	IP地址 *	192.168.2.1
监听端口 *	2000	本地Challenge *	否
认证重发次数 *	0	下线重发次数 *	1
支持逃生心跳 *	否	支持用户心跳 *	否
密钥 *	确认密钥 *
组网方式 *	直连		
设备描述			

确定 取消

图10 增加 IPv6 设备信息配置页面

用户 > 接入策略管理 > Portal服务管理 > 设备配置 > 增加设备信息

增加设备信息

设备信息

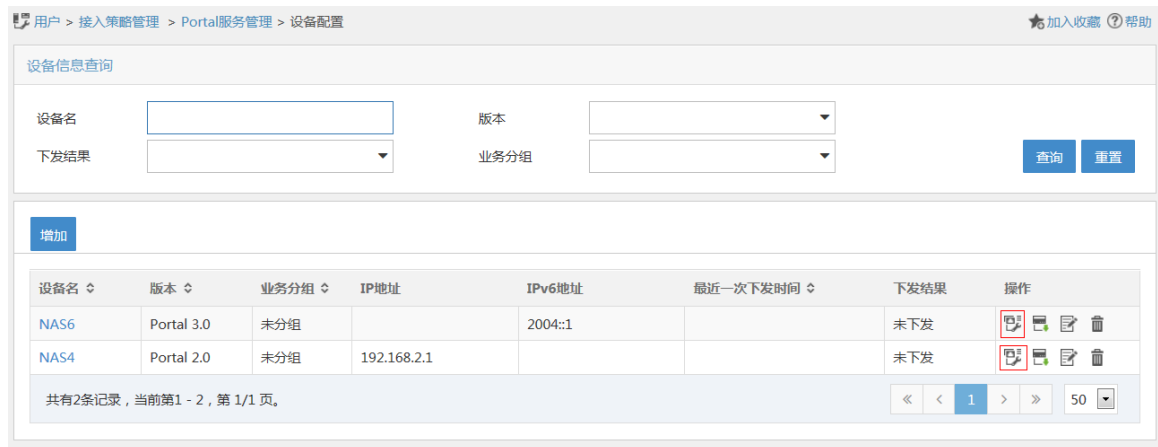
设备名 *	NAS6	业务分组 *	未分组
版本 *	Portal 3.0	IP地址 *	2004::1
监听端口 *	2000	本地Challenge *	否
认证重发次数 *	0	下线重发次数 *	1
支持逃生心跳 *	否	支持用户心跳 *	否
密钥 *	确认密钥 *
组网方式 *	直连		
设备描述			

确定 取消

Portal 设备关联 IP 地址组。

在 Portal 设备配置页面中的设备信息列表中,点击 NAS4 或者 NAS6 设备的<端口组信息管理>链接,进入端口组信息配置页面。

图11 IPv4 或 IPv6 设备信息列表



在端口组信息配置页面中点击<增加>按钮，进入增加端口组信息配置页面。

- 填写端口组名；
- 选择 IP 地址组，用户接入网络时使用的 IP 地址必须属于所选的 IP 地址组；
- 其它参数可采用缺省配置。

图12 增加 IPv4 端口组信息配置页面

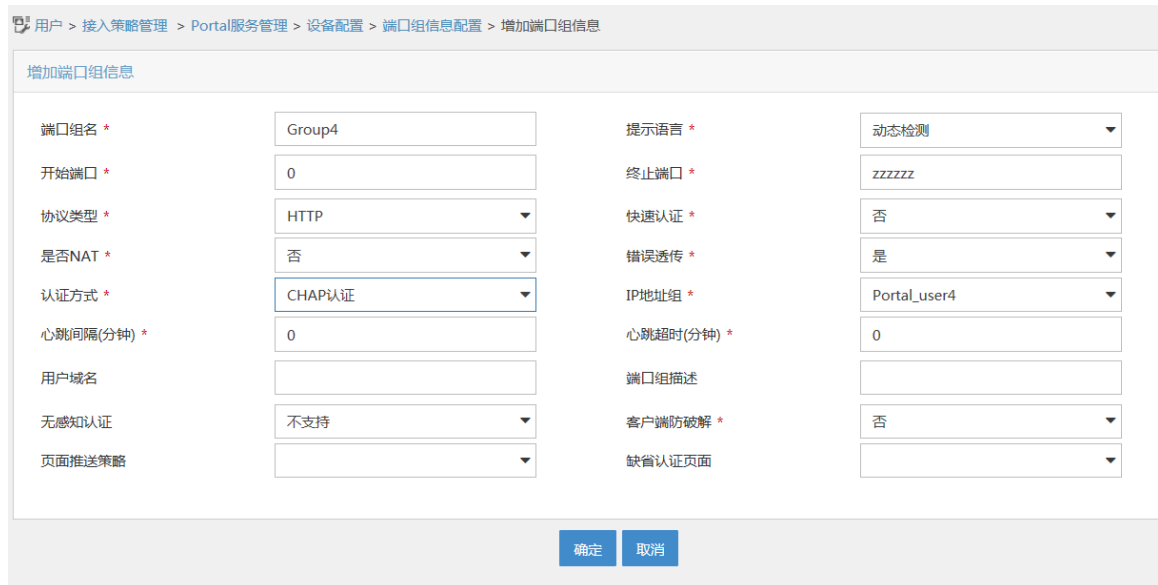


图13 增加 IPv6 端口组信息配置页面

用户 > 接入策略管理 > Portal服务管理 > 设备配置 > 端口组信息配置 > 增加端口组信息

增加端口组信息

端口组名 *	Group6	提示语言 *	动态检测
开始端口 *	0	终止端口 *	zzzzzz
协议类型 *	HTTP	快速认证 *	否
是否NAT *	否	错误透传 *	是
认证方式 *	CHAP认证	IP地址组 *	Portal_User6
心跳间隔(分钟) *	0	心跳超时(分钟) *	0
用户域名		端口组描述	
无感知认证	不支持	客户端防破解 *	否
页面推送策略		缺省认证页面	

确定 取消

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。

3.4.2 配置AC

(1) 配置 AC 的接口

创建 VLAN 100 以及对应的 VLAN 接口，并为该接口配置 IPv4 和 IPv6 地址。AP 将通过该 VLAN 与 AC 建立 CAPWAP 隧道。

```
<AC> system-view
[AC] vlan 100
[AC-vlan100] quit
[AC] interface vlan-interface 100
[AC-Vlan-interface100] ip address 192.168.1.1 24
[AC-Vlan-interface100] ipv6 address 2001::1 64
[AC-Vlan-interface100] quit
```

创建 VLAN 200 及其对应的 VLAN 接口，并为该接口配置 IPv4 和 IPv6 地址。Client 将使用该 VLAN 接入无线网络。

```
[AC] vlan 200
[AC-vlan200] quit
[AC] interface vlan-interface 200
[AC-Vlan-interface200] ip address 192.168.2.1 24
[AC-Vlan-interface200] ipv6 address 2004::1 64
[AC-Vlan-interface200] quit
```

配置 AC 与 Switch 相连的接口 GigabitEthernet1/0/1 的属性为 Trunk，允许 VLAN 1、VLAN 100 和 VLAN 200 通过。

```
[AC] interface gigabitethernet 1/0/1
[AC-GigabitEthernet1/0/1] port link-type trunk
[AC-GigabitEthernet1/0/1] port trunk permit vlan 1 100 200
```

```
[AC-GigabitEthernet1/0/1] quit
```

(2) 配置静态路由

配置到 iMC 的静态路由。

```
[AC] ip route-static 192.168.3.0 255.255.255.0 192.168.2.2
```

```
[AC] ipv6 route-static 2003:: 64 2004::2
```

(3) 配置无线服务

创建无线服务模板 st1，并进入无线服务模板视图。

```
[AC] wlan service-template st1
```

配置 SSID 为 service。

```
[AC-wlan-st-st1] ssid service
```

配置无线服务模板 VLAN 为 VLAN200。

```
[AC-wlan-st-st1] vlan 200
```

开启通过 ND 方式学习客户端 IPv6 地址功能。

```
[AC-wlan-st-st1] client ipv6-snooping nd-learning enable
```

开启通过 DHCPv6 方式学习客户端 IPv6 地址功能。

```
[AC-wlan-st-st1] client ipv6-snooping dhcpv6-learning enable
```

使能无线服务模板 st1。

```
[AC-wlan-st-st1] service-template enable
```

```
[AC-wlan-st-st1] quit
```

创建 AP，配置 AP 名称为 office，型号名称选择 WA4320i-ACN，并配置序列号 219801A0CNC138011454。

```
[AC] wlan ap office model WA4320i-ACN
```

```
[AC-wlan-ap-office] serial-id 219801A0CNC138011454
```

进入 Radio 2 视图。

```
[AC-wlan-ap-office] radio 2
```

将无线服务模板 st1 绑定到 radio 2，并开启射频。

```
[AC-wlan-ap-office-radio-2] service-template st1
```

```
[AC-wlan-ap-office-radio-2] radio enable
```

```
[AC-wlan-ap-office-radio-2] quit
```

```
[AC-wlan-ap-office] quit
```

(4) 配置 IPv4 RADIUS 方案

创建名称为 rs1 的 RADIUS 方案，并进入该方案视图。

```
[AC] 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。

```
[AC-radius-rs1] primary authentication 192.168.3.2
```

```
[AC-radius-rs1] primary accounting 192.168.3.2
```

```
[AC-radius-rs1] key authentication simple radius
```

```
[AC-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。

```
[AC-radius-rs1] user-name-format without-domain
```

设置设备发送 RADIUS 报文使用的源 IP 地址为 192.168.1.1。

```
[AC-radius-rs1] nas-ip 192.168.1.1
```

```
[AC-radius-rs1] quit
```

(5) 配置 IPv6 RADIUS 方案

创建名称为 rs2 的 RADIUS 方案，并进入该方案视图。

```
[AC] radius scheme rs2
```

配置 RADIUS 方案的主认证和主计费服务器及其通信密钥。

```
[AC-radius-rs2] primary authentication ipv6 2003::2
```

```
[AC-radius-rs2] primary accounting ipv6 2003::2
```

```
[AC-radius-rs2] key authentication simple radius
```

```
[AC-radius-rs2] key accounting simple radius
```

配置发送给 RADIUS 服务器的用户名不携带 ISP 域名。

```
[AC-radius-rs2] user-name-format without-domain
```

设置设备发送 RADIUS 报文使用的源 IPv6 地址为 2001::1。

```
[AC-radius-rs2] nas-ip ipv6 2001::1
```

```
[AC-radius-rs2] quit
```

使能 RADIUS session control 功能。

```
[AC] radius session-control enable
```

开启 RADIUS DAE 服务，并进入 RADIUS DAE 服务器视图。

```
[AC] radius dynamic-author server
```

设置 RADIUS DAE 客户端的 IPv4 地址为 192.168.3.2，与 RADIUS DAE 客户端交互 DAE 报文时使用的共享密钥为明文 radius。

```
[AC-radius-da-server] client ip 192.168.3.2 key simple radius
```

设置 RADIUS DAE 客户端的 IPv6 地址为 2003::2，与 RADIUS DAE 客户端交互 DAE 报文时使用的共享密钥为明文 radius。

```
[AC-radius-da-server] client ipv6 2003::2 key simple radius
```

```
[AC-radius-da-server] quit
```

(6) 配置 IPv4 用户认证域

创建名为 dm1 的 ISP 域并进入其视图。

```
[AC] domain dm1
```

为 Portal 用户配置 AAA 认证方法为 RADIUS。

```
[AC-isp-dm1] authentication portal radius-scheme rs1
```

为 Portal 用户配置 AAA 授权方法为 RADIUS。

```
[AC-isp-dm1] authorization portal radius-scheme rs1
```

为 Portal 用户配置 AAA 计费方法为 none，不计费。

```
[AC-isp-dm1] accounting portal none
```

指定 ISP 域 dm1 下的用户闲置切断时间为 15 分钟，闲置切断时间内产生的流量为 1024 字节。

```
[AC-isp-dm1] authorization-attribute idle-cut 15 1024
```

```
[AC-isp-dm1] quit
```

(7) 配置 IPv6 用户认证域

创建名称为 dm2 的 ISP 域并进入其视图。

```
[AC] domain dm2
```

为 Portal 用户配置 AAA 认证方法为 RADIUS。

```
[AC-isp-dm2] authentication portal radius-scheme rs2
```

为 Portal 用户配置 AAA 授权方法为 RADIUS。

```
[AC-isp-dm2] authorization portal radius-scheme rs2
```

```

# 为 Portal 用户配置 AAA 计费方法为 none，不计费。
[AC-isp-dm2] accounting portal none
# 指定 ISP 域 dm2 下的用户闲置切断时间为 15 分钟，闲置切断时间内产生的流量为 1024 字节。
[AC-isp-dm2] authorization-attribute idle-cut 15 1024
[AC-isp-dm2] quit
(8) 配置 Portal 认证
# 配置 IPv4 Portal 认证服务器，名称为 newptv4，IP 地址为 192.168.3.2。
[AC] portal server newptv4
[AC-portal-server-newptv4] ip 192.168.3.2 key simple 123456
[AC-portal-server-newptv4] quit
# 配置 IPv6 Portal 认证服务器，名称为 newptv6，IPv6 地址为 2003::2。
[AC] portal server newptv6
[AC-portal-server-newptv6] ipv6 2003::2 key simple 123456
[AC-portal-server-newptv6] quit
# 配置 IPv4 Portal Web 服务器的 URL 为 http://192.168.3.2:8080/portal。
[AC] portal web-server newptv4
[AC-portal-websvr-newptv4] url http://192.168.3.2:8080/portal
# 配置设备重定向给用户的 Portal Web 服务器的 URL 中携带参数 ssid、wlanuserip 和 wlanacname，
其值分别为 AP 的 SSID、用户的 IP 地址和 AC 名称（这三个参数与中国移动对接时必配）。
[AC-portal-websvr-newptv4] url-parameter ssid ssid
[AC-portal-websvr-newptv4] url-parameter wlanuserip source-address
[AC-portal-websvr-newptv4] url-parameter wlanacname value AC
[AC-portal-websvr-newptv4] quit
# 配置 IPv6 Portal Web 服务器的 URL 为 http://[2003::2]:8080/portal。
[AC] portal web-server newptv6
[AC-portal-websvr-newptv6] url http://[2003::2]:8080/portal
# 配置设备重定向给用户的 Portal Web 服务器的 URL 中携带参数 ssid、wlanuserip 和 wlanacname，
其值分别为 AP 的 SSID、用户的 IP 地址和 AC 名称（与中国移动对接时必配）。
[AC-portal-websvr-newptv6] url-parameter ssid ssid
[AC-portal-websvr-newptv6] url-parameter wlanuserip source-address
[AC-portal-websvr-newptv6] url-parameter wlanacname value AC
[AC-portal-websvr-newptv6] quit
# 开启无线 Portal 漫游功能。
[AC] portal roaming enable
# 关闭无线 Portal 客户端 ARP 表项固化功能。
[AC] undo portal refresh arp enable
# 开启无线 Portal 客户端合法性检查功能。
[AC] portal host-check enable
# 在无线服务模板 st1 上使能直接方式的 Portal 认证。
[AC] wlan service-template st1
[AC-wlan-st-st1] portal enable method direct
[AC-wlan-st-st1] portal ipv6 enable method direct
# 配置接入的 IPv4 Portal 用户使用认证域为 dm1。
[AC-wlan-st-st1] portal domain dm1

```

```

# 配置接入的 IPv6 Portal 用户使用认证域为 dm2。
[AC-wlan-st-st1] portal ipv6 domain dm2
# 在无线服务模板 st1 上引用 IPv4 Portal Web 服务器 newptv4。
[AC-wlan-st-st1] portal apply web-server newptv4
# 在无线服务模板 st1 上引用 IPv6 Portal Web 服务器 newptv6。
[AC-wlan-st-st1] portal ipv6 apply web-server newptv6
# 开启 Portal 支持双协议栈功能。
[AC-wlan-st-st1] portal dual-stack enable
# 设置发送给 Portal 认证服务器的 Portal 报文中的 BAS-IP 和 BAS-IPv6 属性。
[AC-wlan-st-st1] portal bas-ip 192.168.2.1
[AC-wlan-st-st1] portal bas-ipv6 2004::1
[AC-wlan-st-st1] quit
# 配置一条 Portal 免认证规则：编号为 3，源接口为聚合接口 1。该规则表示从 AC 聚合接口 1 上的
用户不需要经过 Portal 认证即可以访问网络资源。
[AC] portal free-rule 3 source interface Bridge-Aggregation1

```

3.4.3 配置Switch

(1) 配置 Switch 的接口

创建 VLAN 100，用于转发 AC 和 AP 间 CAPWAP 隧道内的流量。

```

<Switch> system-view
[Switch] vlan 100
[Switch-vlan100] quit

```

创建 VLAN 200，用于转发 Client 无线报文。

```

[Switch] vlan 200
[Switch-vlan200] quit

```

配置 Switch 与 AC 相连的 GigabitEthernet1/0/1 接口的属性为 Trunk，允许 VLAN 1、VLAN 100 和 VLAN 200 通过。

```

[Switch] interface gigabitethernet 1/0/1
[Switch-GigabitEthernet1/0/1] port link-type trunk
[Switch-GigabitEthernet1/0/1] port trunk permit vlan 1 100 200
[Switch-GigabitEthernet1/0/1] quit

```

配置 Switch 与 AP 相连的 GigabitEthernet1/0/2 接口属性为 Access，并允许 VLAN 100 通过。

```

[Switch] interface gigabitethernet 1/0/2
[Switch-GigabitEthernet1/0/2] port link-type access
[Switch-GigabitEthernet1/0/2] port access vlan 100

```

使能 PoE 功能。

```

[Switch-GigabitEthernet1/0/2] poe enable
[Switch-GigabitEthernet1/0/2] quit

```

配置 VLAN 1 接口的 IPv4 地址和 IPv6 地址。

```

[Switch] interface vlan-interface 1
[Switch-Vlan-interface1] ip address 192.168.3.1 255.255.255.0
[Switch-Vlan-interface1] ipv6 address 2003::1 64
[Switch-Vlan-interface1] quit

```

配置 VLAN 100 接口的 IPv4 地址和 IPv6 地址。


```
[Switch] interface vlan-interface 100
[Switch-Vlan-interface100] ip address 192.168.1.2 255.255.255.0
[Switch-Vlan-interface100] ipv6 address 2001::2 64
[Switch-Vlan-interface100] quit
```

配置 VLAN 200 接口的 IPv4 地址和 IPv6 地址。

```
[Switch] interface vlan-interface 200
[Switch-Vlan-interface200] ip address 192.168.2.2 255.255.255.0
[Switch-Vlan-interface200] ipv6 address 2004::2 64
[Switch-Vlan-interface200] quit
```

(2) 配置 DHCP server

开启 DHCP server 功能。

```
[Switch] dhcp enable
```

配置 DHCP 地址池 100 为 AP 分配地址范围为 192.168.1.0/24，网关地址为 192.168.1.1。

```
[Switch] dhcp server ip-pool 100
[Switch-dhcp-pool-100] network 192.168.1.0 mask 255.255.255.0
[Switch-dhcp-pool-100] gateway-list 192.168.1.1
```

配置 DHCP Option43 的内容为 AC 的十六进制 IP 地址。

```
[Switch-dhcp-pool-100] option 43 hex 8007000001c0a80101
[Switch-dhcp-pool-100] quit
```

配置 DHCP 地址池 200 为 Client 分配地址范围为 192.168.2.0/24，为 Client 分配的 DNS 服务器地址为网关地址（实际使用过程中请根据实际网络规划配置无线客户端的 DNS 服务器地址），网关地址为 192.168.2.2。

```
[Switch] dhcp server ip-pool 200
[Switch-dhcp-pool-200] network 192.168.2.0 mask 255.255.255.0
[Switch-dhcp-pool-200] gateway-list 192.168.2.2
[Switch-dhcp-pool-200] dns-list 192.168.2.2
[Switch-dhcp-pool-200] quit
```

(3) 配置 DHCPv6 server

配置 DHCPv6 地址池 1，用于为 AP 分配 IPv6 地址。

```
[Switch] ipv6 dhcp pool 1
[Switch-dhcp6-pool-1] network 2001::/64
```

配置 Option 选项，使 AP 获取 AC 的 IPv6 地址。

```
[Switch-dhcp6-pool-1] option 52 hex 20010000000000000000000000000001
[Switch-dhcp6-pool-1] quit
```

```
[Switch] ipv6 dhcp server forbidden-address 2001::1
```

配置在 VLAN 100 接口下引用地址池 1，并配置该接口工作在 DHCPv6 服务器模式。

```
[Switch] interface vlan-interface 100
[Switch-Vlan-interface100] ipv6 dhcp server apply pool 1
[Switch-Vlan-interface100] ipv6 dhcp select server
```

取消 VLAN 100 接口对 RA 消息发布的抑制。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。

```
[Switch-Vlan-interface100] ipv6 nd autoconfig managed-address-flag
[Switch-Vlan-interface100] ipv6 nd autoconfig other-flag
[Switch-Vlan-interface100] undo ipv6 nd ra halt
```

```

[Switch-Vlan-interface100] quit
# 配置 DHCPv6 地址池 2，用于为 Client 分配 IPv6 地址。
[Switch] ipv6 dhcp pool 2
[Switch-dhcp6-pool-2] network 2004::/64
[Switch-dhcp6-pool-2] quit
[Switch] ipv6 dhcp server forbidden-address 2004::1
# 配置在 VLAN 200 接口下引用地址池 2，并配置该接口工作在 DHCPv6 服务器模式。
[Switch] interface Vlan-interface 200
[Switch-Vlan-interface200] ipv6 dhcp server apply pool 2
[Switch-Vlan-interface200] ipv6 dhcp select server
# 取消 VLAN 200 接口下对 RA 消息发布的抑制。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。
[Switch-Vlan-interface200] ipv6 nd autoconfig managed-address-flag
[Switch-Vlan-interface200] ipv6 nd autoconfig other-flag
[Switch-Vlan-interface200] undo ipv6 nd ra halt
[Switch-Vlan-interface200] quit

```

3.5 验证配置

用户通过网页方式进行 Portal 认证。用户在通过 IPv4 认证前，发起的所有 Web 访问均被重定向到 Portal 认证页面 (<http://192.168.3.2:8080/portal>)，在通过认证后，可访问非受限的互联网资源。通过执行以下显示命令查看 AC 上生成的 Portal 在线用户信息。

```

[AC] display portal user all
Total portal users: 1
Username: client
  AP name: office
  Radio ID: 2
  SSID: service
  Portal server: newptv4
  State: Online
  VPN instance: N/A
  MAC          IP          VLAN   Interface
  -----
  3829-5a40-9589 192.168.2.3 200    WLAN-BSS1/0/2
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

```

用户通过网页方式进行 Portal 认证。用户在通过 IPv6 认证前，发起的所有 Web 访问均被重定向到 Portal 认证页面 ([http://\[2003::2\]:8080/portal](http://[2003::2]:8080/portal))，在通过认证后，可访问非受限的互联网资源。通过执行以下显示命令查看 AC 上生成的 Portal 在线用户信息。

```

[AC] display portal user all
Total portal users: 1

```

```

Username: Client
  AP name: office
  Radio ID: 2
  SSID: service
  Portal server: newptv6
  State: Online
  VPN instance: N/A
  MAC          IP          VLAN  Interface
  3829-5a40-9589  2004::4549:7C7F:392E: 200  WLAN-BSS1/0/2
                    EE57
  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

```

3.6 配置文件

- AC:


```

#
vlan 100
#
vlan 200
#
wlan service-template st1
  ssid service
  vlan 200
  client ipv6-snooping nd-learning enable
  client ipv6-snooping dhcpv6-learning enable
  portal enable method direct
  portal domain dm1
  portal bas-ip 192.168.2.1
  portal apply web-server newptv4
  portal ipv6 enable method direct
  portal ipv6 domain dm2
  portal bas-ipv6 2004::1
  portal ipv6 apply web-server newptv6
  portal dual-stack enable
  service-template enable
#
interface Vlan-interface100
  ip address 192.168.1.1 255.255.255.0
  ipv6 address 2001::1/64
#
interface Vlan-interface200
  ip address 192.168.2.1 255.255.255.0

```

```

ipv6 address 2004::1/64
#
interface GigabitEthernet1/0/1
port link-mode bridge
port link-type trunk
port trunk permit vlan 1 100 200
#
ip route-static 192.168.3.0 24 192.168.2.2
ipv6 route-static 2003:: 64 2004::2
#
radius session-control enable
#
radius scheme rs1
primary authentication 192.168.3.2
primary accounting 192.168.3.2
key authentication cipher $c$3$2m4BXR2X65vE59L0SyYHH0tRVpkKDgym9w==
key accounting cipher $c$3$4ieHsnXQVnQ7GwywFS+H0MoQdb6SEmJSRg==
user-name-format without-domain
nas-ip 192.168.1.1
#
radius scheme rs2
primary authentication ipv6 2003::2
primary accounting ipv6 2003::2
key authentication cipher $c$3$8bAMsBFXCglbmynti08YCxotgTXyWzES0w==
key accounting cipher $c$3$QeTcfxJGTnPJ98PsCSbLnaZP6KAG6q42aQ==
user-name-format without-domain
nas-ip ipv6 2001::1
#
radius dynamic-author server
client ip 192.168.3.2 key cipher $c$3$19xAYe5vBJQMT0v6quHJFXtZlti404CjBg==
client ipv6 2003::2 key cipher $c$3$ELOjffzKgJuoRbJ/wZX0E9eVdGBFeTQzmHA==
#
domain dml
authorization-attribute idle-cut 15 1024
authentication portal radius-scheme rs1
authorization portal radius-scheme rs1
accounting portal none
#
domain dm2
authorization-attribute idle-cut 15 1024
authentication portal radius-scheme rs2
authorization portal radius-scheme rs2
accounting portal none
#
portal host-check enable
#
portal web-server newptv4
url http://192.168.3.2:8080/portal

```

```

url-parameter ssid ssid
url-parameter wlanacname value AC
url-parameter wlanuserip source-address
#
portal web-server newptv6
url http://[2003::2]:8080/portal
url-parameter ssid ssid
url-parameter wlanacname value AC
url-parameter wlanuserip source-address
#
portal server newptv4
ip 192.168.3.2 key cipher $c$3$XkIMNqFj0It2yZOqdfPeOeasD0Jk4oJQFA==
#
portal server newptv6
ipv6 2003::2 key cipher $c$3$9MzqVffe//Ma5x4a4gJOSQKrnSBS5EslXg==
#
wlan ap office model WA4320i-ACN
serial-id 219801A0CNC138011454
radio 2
radio enable
service-template st1
#
return

```

- **Switch:**

```

#
ipv6 dhcp server forbidden-address 2001::1
ipv6 dhcp server forbidden-address 2004::1
#
vlan 1
#
vlan 100
#
vlan 200
#
dhcp server ip-pool 100
gateway-list 192.168.1.1
network 192.168.1.0 mask 255.255.255.0
option 43 hex 8007000001c0a80101
#
dhcp server ip-pool 200
gateway-list 192.168.2.2
network 192.168.2.0 mask 255.255.255.0
dns-list 192.168.2.2
#
ipv6 dhcp pool 1
network 2001::/64
option 52 hex 20010000000000000000000000000001
#

```

```

ipv6 dhcp pool 2
 network 2004::/64
#
interface Vlan-interface1
 ip address 192.168.3.1 255.255.255.0
 ipv6 address 2003::1/64
#
interface Vlan-interface100
 ip address 192.168.1.2 255.255.255.0
 ipv6 dhcp select server
 ipv6 dhcp server apply pool 1
 ipv6 address 2001::2/64
 ipv6 nd autoconfig managed-address-flag
 ipv6 nd autoconfig other-flag
 undo ipv6 nd ra halt
#
interface Vlan-interface200
 ip address 192.168.2.2 255.255.255.0
 ipv6 dhcp select server
 ipv6 dhcp server apply pool 2
 ipv6 address 2004::2/64
 ipv6 nd autoconfig managed-address-flag
 ipv6 nd autoconfig other-flag
 undo ipv6 nd ra halt
#
interface GigabitEthernet1/0/1
 port link-type trunk
 port trunk permit vlan 1 100 200
#
interface GigabitEthernet1/0/2
 port access vlan 100
 poe enable
#
return

```

4 相关资料

- 《H3C 无线控制器产品 配置指导》中的“用户接入与认证配置指导”。
- 《H3C 无线控制器产品 命令参考》中的“用户接入与认证命令参考”。
- 《H3C 无线控制器产品 配置指导》中的“WLAN 接入配置指导”。
- 《H3C 无线控制器产品 命令参考》中的“WLAN 接入命令参考”。
- 《H3C 无线控制器产品 配置指导》中的“AP 管理配置指导”。
- 《H3C 无线控制器产品 命令参考》中的“AP 管理命令参考”。