H3C 无线控制器

802.1X 认证通过 iMC 服务器下发 ACL 典型配置举例 (V7)

资料版本：6W100-20191125

目 录

1 简介

本文档介绍无线用户 802.1X 认证通过 iMC 服务器下发 ACL 的典型配置案例。

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 WLAN 用户接入认证相关特性。

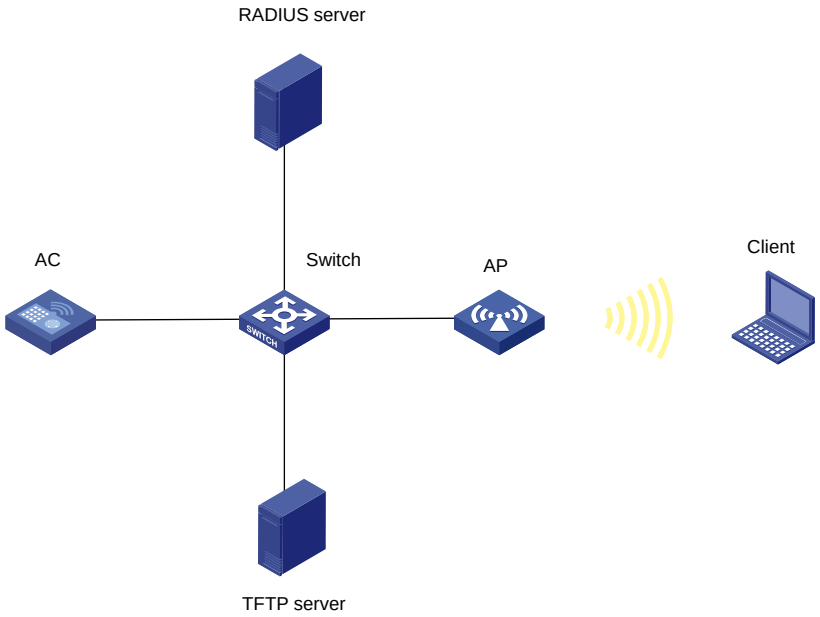
3 配置举例

3.1 组网需求

如图 1 所示，AP 通过交换机与 AC 相连，无线 802.1X 用户通过 AP 接入无线网络。具体要求如下：

- Client 通过 802.1X 认证接入无线网络。
- 通过 RADIUS 服务器下发授权 ACL，使 Client 不能访问 TFTP 服务器。

图1 802.1X 用户接入组网图



设备	接口	IP地址	设备	接口	IP地址
AC	Vlan-int100	138.100.1.101/16	Switch	Vlan-int100	138.100.1.100/16
	Vlan-int200	138.200.1.101/16		Vlan-int200	138.200.1.100/16
RADIUS server		8.1.1.50/16		Vlan-int8	8.1.1.100/16
TFTP server		8.1.1.5/16			

3.2 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。

3.3 配置步骤

3.3.1 配置AC

(1) 配置 AC 的接口

创建 VLAN 100 及其对应的 VLAN 接口，并为该接口配置 IP 地址。AC 将使用该接口的 IP 地址与 AP 建立 CAPWAP 隧道。

```
<AC> system-view
[AC] vlan 100
[AC-vlan100] quit
[AC] interface vlan-interface 100
[AC-Vlan-interface100] ip address 138.100.1.101 16
[AC-Vlan-interface100] quit
```

创建 VLAN 200 作为 Client 接入的业务 VLAN，并配置 VLAN 200 的接口 IP 地址，Client 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 138.200.1.101 16
[AC-Vlan-interface200] quit
```

配置 AC 和 Switch 相连的接口 GigabitEthernet1/0/1 为 Trunk 类型，禁止 VLAN 1 报文通过，允许 VLAN 100 和 VLAN 200 通过，当前 Trunk 口的 PVID 为 100。

```
[AC] interface gigabitethernet1/0/1
[AC-GigabitEthernet1/0/1] port link-type trunk
[AC-GigabitEthernet1/0/1] undo port trunk permit vlan 1
[AC-GigabitEthernet1/0/1] port trunk permit vlan 100 200
[AC-GigabitEthernet1/0/1] port trunk pvid vlan 100
[AC-GigabitEthernet1/0/1] quit
```

(2) 配置 802.1X 认证

全局使能端口安全。

```
[AC] port-security enable
```

选择 802.1X 认证方式为 EAP。

```
[AC] dot1x authentication-method eap
```

创建 RADIUS 方案并进入 RADIUS 方案视图。

```
[AC] radius scheme office
```

设置主认证 RADIUS 服务器的 IP 地址 8.1.1.50。

```
[AC-radius-office] primary authentication 8.1.1.50
```

设置主计费 RADIUS 服务器的 IP 地址 8.1.1.50。

```
[AC-radius-office] primary accounting 8.1.1.50
```

设置系统与认证 RADIUS 服务器交互报文时的共享密钥为 12345678。

```
[AC-radius-office] key authentication 12345678
```
设置系统与计费 RADIUS 服务器交互报文时的共享密钥为 12345678。
```
[AC-radius-office] key accounting 12345678
```
设置设备发送 RADIUS 报文时使用的源 IP 地址 138.100.1.101。
```
[AC-radius-office] nas-ip 138.100.1.101
[AC-radius-office] quit
```
创建 ISP 域并进入 ISP 域视图。
```
[AC] domain office
```
为 lan-access 用户配置认证方案为 RADIUS 方案，方案名为 office。
```
[AC-isp-office] authentication lan-access radius-scheme office
```
为 lan-access 用户配置授权方案为 RADIUS 方案，方案名为 office。
```
[AC-isp-office] authorization lan-access radius-scheme office
```
为 lan-access 用户配置计费为 none，不计费。
```
[AC-isp-office] accounting lan-access none
[AC-isp-office] quit
```
(3) 配置无线服务

创建无线服务模板 1。
```
[AC] wlan service-template 1
```
配置无线服务的 SSID 为 service。
```
[AC-wlan-st-1] ssid service
```
配置无线服务的 VLAN 为 200。
```
[AC-wlan-st-1] vlan 200
```
配置身份认证与密钥管理模式为 dot1x 模式，并配置 dot1x 认证域。
```
[AC-wlan-st-1] akm mode dot1x
[AC-wlan-st-1] client-security authentication-mode dot1x
[AC-wlan-st-1] dot1x domain office
```
配置 CCMP 为加密套件，配置 RSN 为安全信息元素。
```
[AC-wlan-st-1] cipher-suite ccmp
[AC-wlan-st-1] security-ie rsn
```
使能无线服务模板。
```
[AC-wlan-st-1] service-template enable
[AC-wlan-st-1] quit
```
(4) 配置 AP

创建 AP，名称为 ap1，并将无线服务模板 1 绑定到 ap1 的 Radio 1 接口。
```
[AC] wlan ap ap1 model WA4320i-ACN
[AC-wlan-ap-ap1] serial-id 210235A1GQC14C000225
[AC-wlan-ap-ap1] radio 1
[AC-wlan-ap-ap1-radio-1] service-template 1
[AC-wlan-ap-ap1-radio-1] radio enable
[AC-wlan-ap-ap1-radio-1] quit
[AC-wlan-ap-ap1] quit
```
(5) 创建 ACL 并设置包过滤规则

配置 ACL 规则 3001，禁止 Client 访问 8.1.1.5。
```
[AC] acl advanced 3001
```

```
[AC-acl-ipv4-adv-3001] rule 1 deny ip destination 8.1.1.5 0
[AC-acl-ipv4-adv-3001] quit
```

(6) AC 上配置静态路由

配置 AC 的默认路由，下一跳地址为 138.100.1.100。

```
[AC] ip route-static 0.0.0.0 0.0.0.0 138.100.1.100
```

3.3.2 配置Switch

(1) 配置 Switch 接口

创建 VLAN 100，并为该接口配置 IP 地址，用于和 AC 进行通信。

```
<Switch> system-view
[Switch] vlan 100
[Switch-vlan100] quit
[Switch] interface vlan-interface 100
[Switch-Vlan-interface100] ip address 138.100.1.100 16
[Switch-Vlan-interface100] quit
```

创建 VLAN 200 作为 Client 接入的业务 VLAN，并配置 VLAN 200 的接口 IP 地址，用于和 Client 进行通信。

```
[Switch] vlan 200
[Switch-vlan200] quit
[Switch] interface vlan-interface 200
[Switch-Vlan-interface200] ip address 138.200.1.100 16
[Switch-Vlan-interface200] quit
```

创建 VLAN 8，并配置 VLAN 8 的接口 IP 地址，用于和 RADIUS 服务器通信。

```
[Switch] vlan 8
[Switch-vlan8] quit
[Switch] interface vlan-interface 8
[Switch-Vlan-interface8] ip address 8.1.1.100 16
[Switch-Vlan-interface8] quit
```

配置 Switch 与 AC 连接的物理接口类型为 Trunk，允许所有 VLAN 通过。

```
[Switch] interface GigabitEthernet 1/0/1
[Switch-GigabitEthernet1/0/1] port link-type trunk
[Switch-GigabitEthernet1/0/1] port trunk permit vlan all
[Switch-GigabitEthernet1/0/1] port trunk pvid vlan 100
[Switch-GigabitEthernet1/0/1] quit
```

(2) 配置 DHCP 服务器

开启 DHCP 功能

```
[Switch] dhcp enable
```

创建名为 vlan100 的 DHCP 地址池，配置地址池动态分配的网段为 138.100.0.0/16，网关地址为 138.100.1.100，为 AP 分配 IP 地址。

```
[Switch] dhcp server ip-pool vlan100
[Switch-dhcp-pool-vlan100] network 138.100.0.0 mask 255.255.0.0
[Switch-dhcp-pool-vlan100] gateway-list 138.100.1.100
[Switch-dhcp-pool-vlan100] quit
```

创建名为 vlan200 的 DHCP 地址池，配置地址池动态分配的网段为 138.200.0.0/16，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 138.200.1.100，为 Client 分配 IP 地址。

```
[Switch] dhcp server ip-pool vlan200
[Switch-dhcp-pool-vlan100] network 138.200.0.0 mask 255.255.0.0
[Switch-dhcp-pool-vlan100] gateway-list 138.200.1.100
[Switch-dhcp-pool-vlan100] dns-list 138.200.1.100
[Switch-dhcp-pool-vlan100] quit
```

3.4 RADIUS服务器的配置

说明

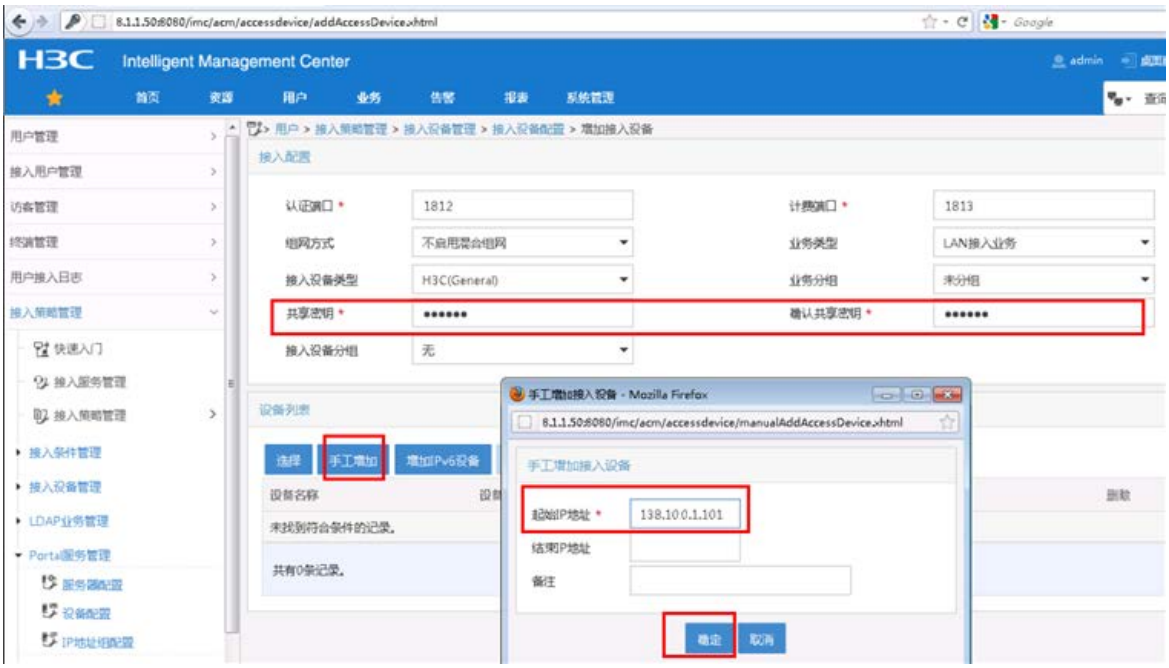
下面以 iMC 为例（使用 iMC 版本为：iMC PLAT 7.1(E0302)、iMC WSM 7.1(E0303)），说明 RADIUS 服务器的基本配置。

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，进入接入设备配置页面，在该页面中单击<增加>按钮，进入增加接入设备页面。

- 设置与 AC 交互报文时使用的认证、计费共享密钥为“12345678”；
- 选择手工增加接入设备，添加 IP 地址为 138.100.1.101 的接入设备；
- 其它参数采用缺省值，并单击<确定>按钮完成操作。

图2 增加接入设备

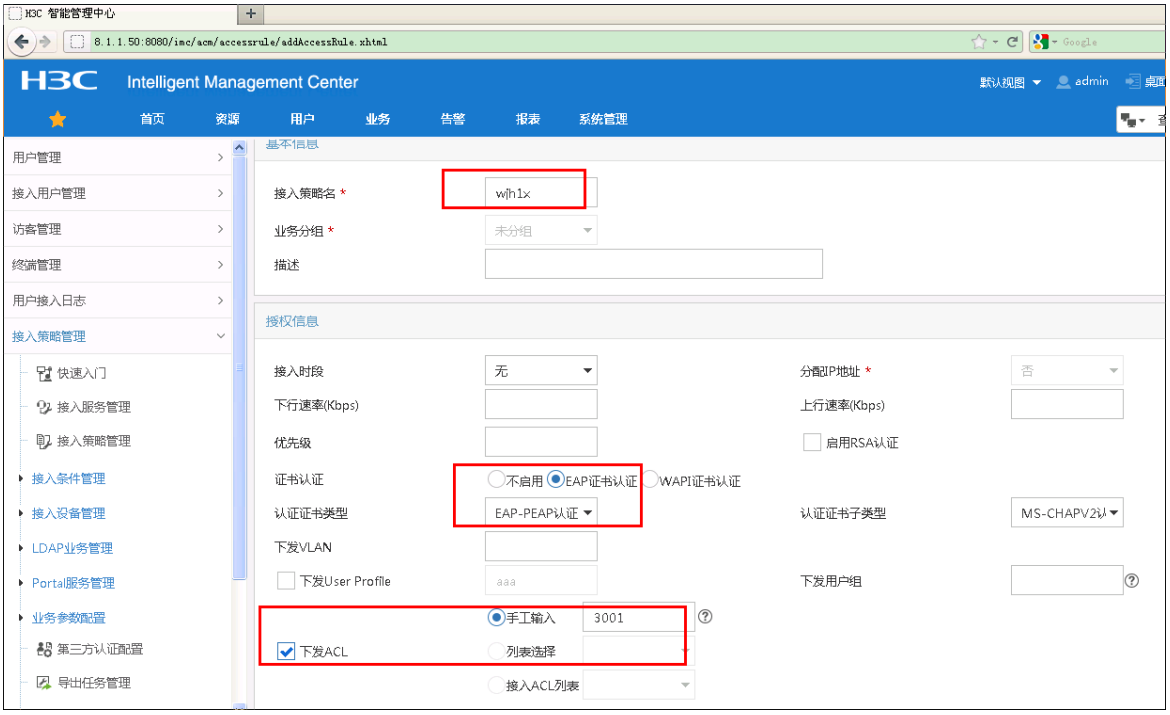


增加接入策略。

选择“用户”页签，单击导航树中的[接入策略管理/接入策略管理]菜单项，进入接入策略配置页面，在该页面中单击<增加>按钮，进入增加接入策略页面。

- 接入策略名输入“wjh1x”；
- 证书认证选择所需要认证的类型；
- 勾选上下发授权 ACL，并输入与设备上配置一致的 ACL 名称
- 其它参数采用缺省值，并单击<确定>按钮完成操作。

图3 增加接入策略

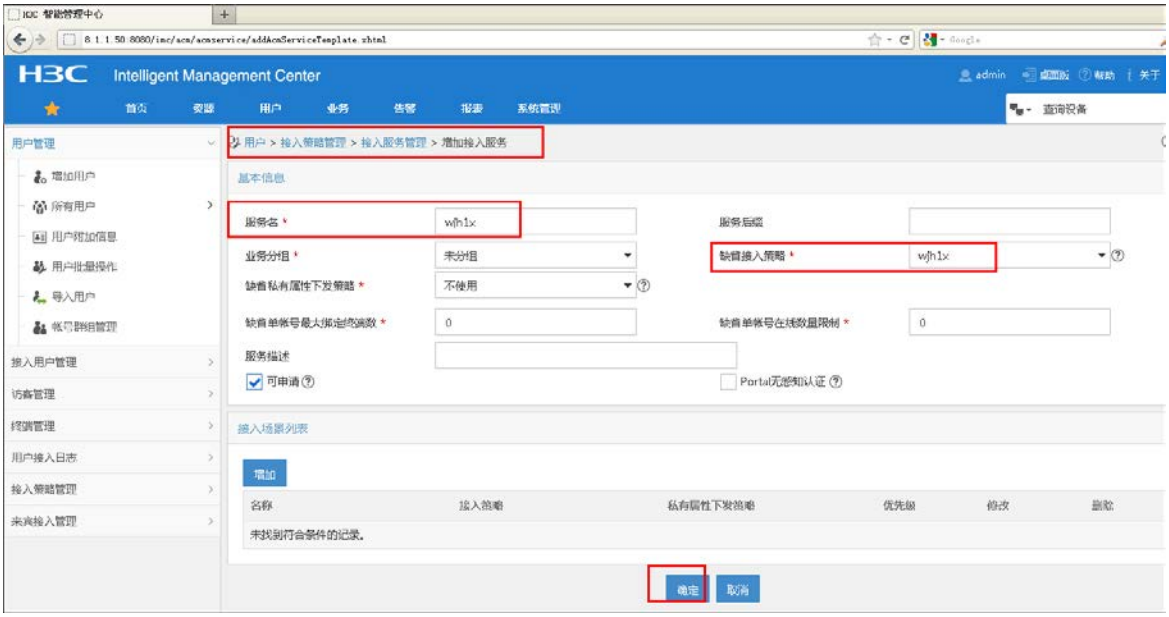


增加接入服务配置。

选择“用户”页签，单击导航树中的[接入策略管理/接入服务管理]菜单项，进入接入服务配置页面，在该页面中单击<增加>按钮，进入增加接入服务页面。

- 服务名输入“wjh1x”；
- 缺省接入策略选择上一步配置的 “wjh1x”；
- 其它参数采用缺省值，并单击<确定>按钮完成操作。

图4 增加接入服务

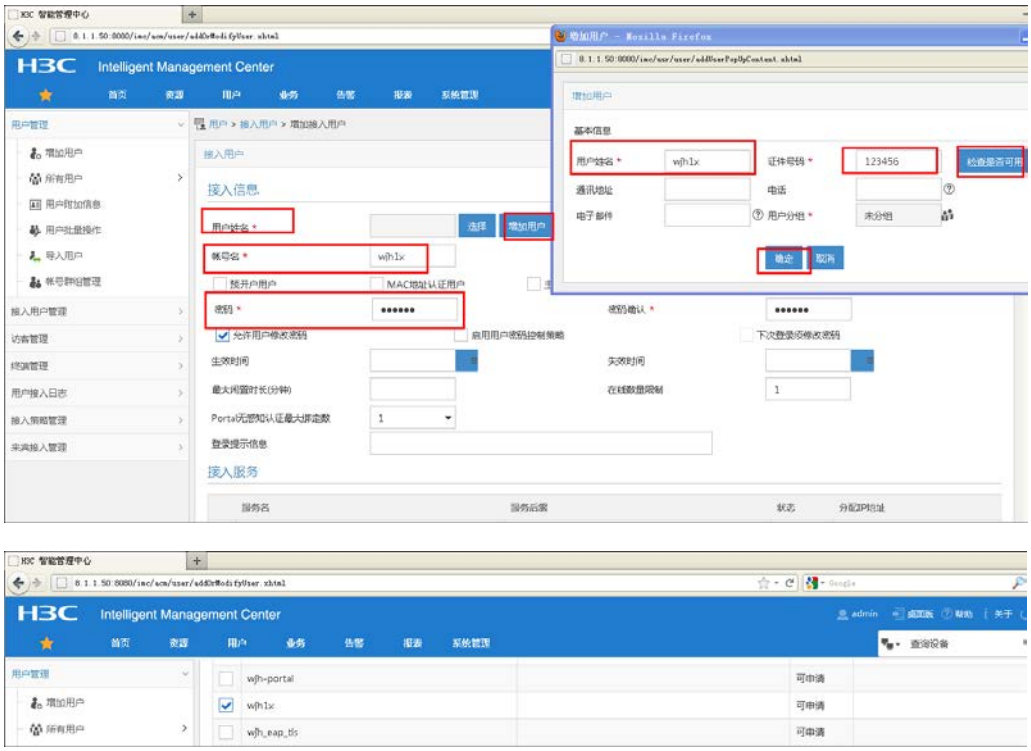


增加接入用户。

选择“用户”页签，单击导航树中的[接入用户管理/接入用户]菜单项，进入接入用户列表页面，在该页面中单击<增加>按钮，进入增加接入用户页面。

- 在增加接入用户页面，单击<增加用户>按钮弹出增加用户窗口；
- 输入用户名“wjh1x”，以及证件号码“12345678”；
- 单击<检查是否可用>按钮，户姓名和证件号码可用，单击<确定>按钮完成操作。
- 输入账号名“wjh1x”及用户密码“12345678”；
- 在接入服务处选择“wjh1x”，最后单击<确定>按钮完成操作。

图5 增加接入用户



3.5 验证配置

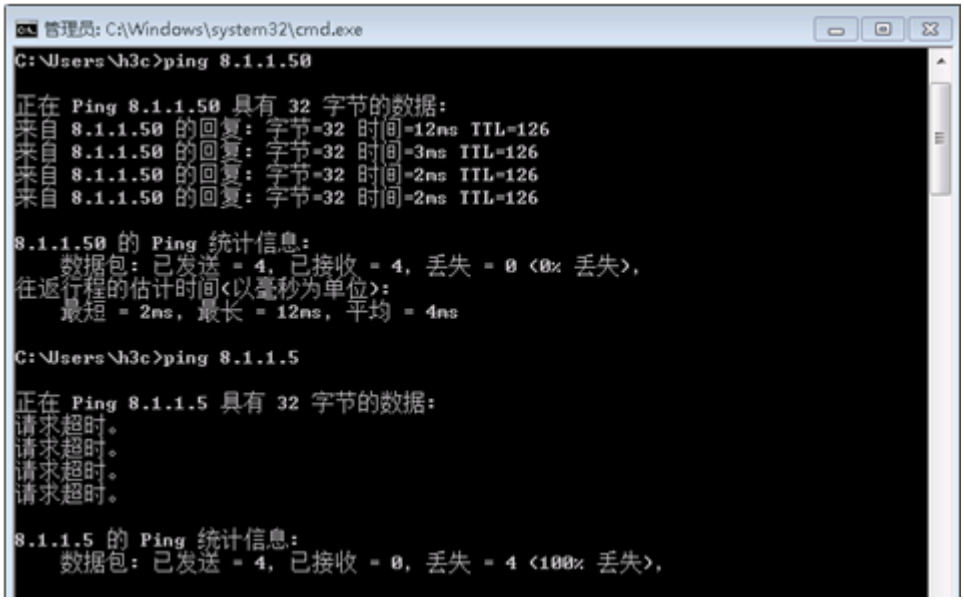
(1) 操作 Client 上线，输入 RADIUS 服务器上设置的用户名和密码完成接入，在设备 AC 上执行 **display wlan client verbose** 命令，可以查看 Client 信息。

```
<AC> display wlan client verbose

Total number of clients: 1
MAC address                          : 0015-00ba-0428
 IPv4 address                        : 138.200.0.1
 IPv6 address                        : N/A
 Username                            : wjh1x
 AID                                 : 1
 AP ID                               : 1
 AP name                             : ap1
 Radio ID                            : 1
 SSID                                : service
 BSSID                               : 5866-ba71-3960
 VLAN ID                             : 200
 Sleep count                         : 0
 Wireless mode                       : 802.11ac
 Channel bandwidth                   : 40MHz
 SM power save                       : Disabled
 Short GI for 20MHz                  : Supported
 Short GI for 40MHz                  : Supported
```

```
STBC RX capability                : Supported
STBC TX capability                : Not supported
LDPC RX capability                : Not supported
Block Ack                         : N/A
Supported HT MCS set              : 0, 1, 2, 3, 4, 5, 6, 7,
                                    8, 9, 10, 11, 12, 13, 14,
                                    15
Supported rates                   : 6, 9, 12, 18, 24, 36,
                                    48, 54 Mbps
QoS mode                          : WMM
Listen interval                   : 250
RSSI                              : 0
Rx/Tx rate                        : 0/0
Authentication method             : Open system
Security mode                     : RSN
AKM mode                          : 802.1X
Cipher suite                      : CCMP
User authentication mode          : 802.1X
Authorization ACL ID              : 3001
Authorization user profile        : N/A
Roam status                       : N/A
Key derivation                    : SHA1
PMF status                        : N/A
Forwarding policy name            : N/A
Online time                       : 0days 0hours 0minutes 17seconds
FT status                         : Inactive
```

(2) Client 成功上线后，从 Client Ping 8.1.1.50 是可以通的，但是 Ping 8.1.1.5 是不通的。



3.6 配置文件

- AC

```
#
port-security enable
#
dot1x authentication-method eap
#
vlan 100
#
vlan 200
#
wlan service-template 1
 ssid service
 vlan 200
 akm mode dot1x
 cipher-suite ccmp
 security-ie rsn
client-security authentication-mode dot1x
 dot1x domain office
service-template enable
#
interface Vlan-interface100
 ip address 138.100.1.101 255.255.0.0
#
interface Vlan-interface200
 ip address 138.200.1.101 255.255.0.0
#
interface GigabitEthernet1/0/1
 port link-type trunk
 port trunk permit vlan 100 200
 port trunk pvid vlan 100

#
ip route-static 0.0.0.0 0.0.0.0 138.100.1.100
#
acl advanced 3001
 rule 1 deny ip destination 8.1.1.5 0
#
radius scheme office
primary authentication 8.1.1.50
 primary accounting 8.1.1.50
 key authentication simple $c$3$h7ouSYGGL5EgJZ6HpwIIgRdgiLKJCd6zZxE4
 key accounting simple $c$3$qf3E+i6hAgx/rpYxDApL0E0NSDWHZCZ3OI1g
 nas-ip 138.100.1.101
#
domain office
 authentication lan-access radius-scheme office
```

```
 authorization lan-access radius-scheme office
 accounting lan-access none
#
wlan ap ap1 model WA4320i-ACN
 serial-id 210235A1GQC14C000225
 radio 1
  radio enable
  service-template 1
 radio 2
```

- Switch

```
#
vlan8
#
vlan 100
#
vlan 200
#
dhcp server ip-pool vlan100
network 138.100.0.0 mask 255.255.0.0
gateway-list 138.100.1.100
#
dhcp server ip-pool 200
network 138.200.0.0 mask 255.255.0.0
gateway-list 138.200.1.100
dns-list 138.200.1.100
#
interface Vlan-interface8
 ip address 8.1.1.100 255.255.0.0
#
interface Vlan-interface100
 ip address 138.100.1.100 255.255.0.0
#
interface Vlan-interface200
 ip address 138.200.1.100 255.255.0.0
#
interface GigabitEthernet1/0/1
 port link-type trunk
 port trunk permit vlan all
 port trunk pvid vlan 100
#
dhcp enable
```

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”。