

知 H3C 无线控制器 本地MAC认证+Access-Control 典型配置举例(V7)

wlan接入

MAC地址认证

丁犁

2020-07-24 发表

组网及说明

如图1所示，集中式转发架构下，AP和Client通过DHCP server获取IP地址，要求在AC上使用MAC地址用户名格式认证方式进行用户身份认证，以控制其对网络资源的访问。同时要求终端A仅能通过SSID1进行MAC地址认证；终端B仅能通过SSID2进行MAC地址认证。

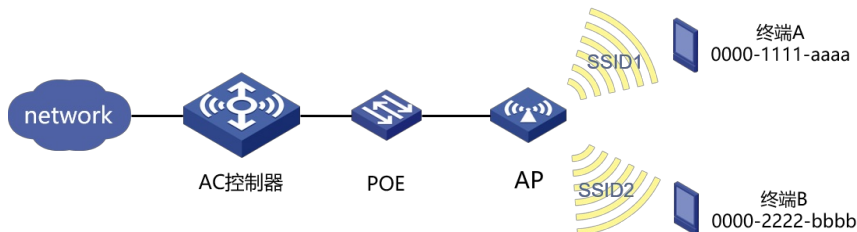


图1

配置步骤

配置AC

• 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。AP将获取该IP地址与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 112.12.1.25 16
[AC-Vlan-interface100] quit
```

创建VLAN 200及其对应的VLAN接口，并为该接口配置IP地址。终端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 112.13.1.25 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
```

• 配置DHCP server

开启DHCP server功能。

```
[AC] dhcp enable
```

配置DHCP地址池vlan100为AP分配地址范围为112.12.0.0/16，网关地址为112.12.1.25。

```
[AC] dhcp server ip-pool vlan100
[AC-dhcp-pool-vlan100] network 112.12.0.0 mask 255.255.0.0
[AC-dhcp-pool-vlan100] gateway-list 112.12.1.25
[AC-dhcp-pool-vlan100] quit
```

配置DHCP地址池vlan200为终端Client分配地址范围为112.13.0.0/16，网关地址为112.13.1.25。

```
[AC] dhcp server ip-pool vlan200
[AC-dhcp-pool-vlan200] network 112.13.0.0 mask 255.255.0.0
[AC-dhcp-pool-vlan200] gateway-list 112.13.1.25
[AC-dhcp-pool-vlan200] quit
```

• 配置本地认证域

创建一个名称为local-mac的认证域，为lan-access用户配置认证方法为local。

```
[AC] domain local-mac
```

```
[AC-isp-local-mac] authentication lan-access local
# 配置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-local-mac] authorization-attribute idle-cut 15 1024
[AC] quit
```

• 配置本地用户

配置一个网络接入类的本地用户，名称为客户端的MAC地址 00001111aaaa，密码为明文密码 00001111aaaa，并指定用户可以使用lan-access服务。

```
[AC] local-user 00001111aaaa class network
[AC-luser-network- 00001111aaaa] password simple 00001111aaaa
[AC-luser-network- 00001111aaaa] service-type lan-access
[AC-luser-network- 00001111aaaa] quit
```

配置一个网络接入类的本地用户，名称为客户端的MAC地址 00002222bbbb，密码为明文密码 00002222bbbb，并指定用户可以使用lan-access服务。

```
[AC] local-user 00002222bbbb class network
[AC-luser-network- 00002222bbbb] password simple 00002222bbbb
[AC-luser-network- 00002222bbbb] service-type lan-access
[AC-luser-network- 00002222bbbb] quit
```

• 配置本地MAC地址认证的用户名格式

配置MAC地址认证的用户名和密码均为用户的MAC地址（该配置为缺省配置）。

```
[AC] mac-authentication user-name-format mac-address without-hyphen lowercase
```

• 配置MAC地址ACL列表

创建MAC地址ACL列表4001和4002，分别匹配终端A 0000-1111-aaaa 和终端B 0000-2222-bbbb MAC地址。

```
[AC] acl mac 4001
[AC-acl-mac-4001] rule 0 permit source-mac 0000-1111-aaaa ffff-ffff-ffff
[AC-acl-mac-4001] rule 1 deny
[AC-acl-mac-4001] quit
[AC] acl mac 4002
[AC-acl-mac-4002] rule 0 permit source-mac 0000-2222-bbbb ffff-ffff-ffff
[AC-acl-mac-4002] rule 1 deny
[AC-acl-mac-4002] quit
```

• 配置无线服务

创建无线服务模板1，并进入无线服务模板视图。

```
[AC] wlan service-template 1
```

配置SSID为SSID1。

```
[AC-wlan-st-1] ssid SSID1
```

配置客户端从无线服务模板1上线后会被加入VLAN 200。

```
[AC-wlan-st-1] vlan 200
```

配置客户端接入认证方式为MAC地址认证。

```
[AC-wlan-st-1] client-security authentication-mode mac
```

配置MAC地址认证用户使用的ISP域为local-mac。

```
[AC-wlan-st-1] mac-authentication domain local-mac
```

配置Access-Control功能，基于ACL的接入控制为4001，仅允许MAC地址为0000-aaaa-1111的终端接入

```
[AC-wlan-st-1] access-control acl 4001
```

开启无线服务模板。

```
[AC-wlan-st-1] service-template enable
```

```
[AC-wlan-st-1] quit
```

创建无线服务模板2，并进入无线服务模板视图。

```
[AC] wlan service-template 2
```

配置SSID为SSID2。

```
[AC-wlan-st-2] ssid SSID2
```

配置客户端从无线服务模板2上线后会被加入VLAN 200。

```
[AC-wlan-st-2] vlan 200
```

配置客户端接入认证方式为MAC地址认证。

```
[AC-wlan-st-2] client-security authentication-mode mac
```

配置MAC地址认证用户使用的ISP域为local-mac。

```
[AC-wlan-st-2] mac-authentication domain local-mac
```

配置Access-Control功能，基于ACL的接入控制为4002，仅允许MAC地址为0000-bbbb-2222的终端接入

```
[AC-wlan-st-2] access-control acl 4002
```

开启无线服务模板。

```
[AC-wlan-st-2] service-template enable
```

```
[AC-wlan-st-1] quit
```

• 配置AP

```
# 创建手工AP，名称为officeap，型号名称为WA4320i-ACN。  
[AC] wlan ap officeap model WA4320i-ACN  
# 设置AP序列号为210235A1Q2C159000019。  
[AC-wlan-ap-officeap] serial-id 210235A1Q2C159000019  
# 进入AP的Radio 2视图，并将无线服务模板1和服务模板2绑定到Radio 2上。  
[AC-wlan-ap-officeap] radio 2  
[AC-wlan-ap-officeap-radio-2] service-template 1  
[AC-wlan-ap-officeap-radio-2] service-template 2  
# 开启Radio 2的射频功能。  
[AC-wlan-ap-officeap-radio-2] radio enable  
[AC-wlan-ap-officeap-radio-2] quit  
[AC-wlan-ap-officeap] quit
```

配置Switch

```
# 创建VLAN 100和VLAN 200，其中VLAN 100用于转发AC和AP间CAPWAP隧道内的流量，VLAN 200用于转发Client无线报文。  
<Switch> system-view  
[Switch] vlan 100  
[Switch-vlan100] quit  
[Switch] vlan 200  
[Switch-vlan200] quit  
# 配置Switch与AC相连的GigabitEthernet1/0/1接口的属性为Trunk，禁止VLAN 1报文通过，允许VLAN 100通过，当前Trunk口的PVID为100。  
[Switch] interface gigabitethernet1/0/1  
[Switch-GigabitEthernet1/0/1] port link-type trunk  
[Switch-GigabitEthernet1/0/1] undo port trunk permit vlan 1  
[Switch-GigabitEthernet1/0/1] port trunk permit vlan 100  
[Switch-GigabitEthernet1/0/1] port trunk pvid vlan 100  
[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 gigabitethernet1/0/2  
[Switch-GigabitEthernet1/0/2] port link-type access  
[Switch-GigabitEthernet1/0/2] port access vlan 100  
# 开启PoE接口远程供电功能。  
[Switch-GigabitEthernet1/0/2] poe enable  
[Switch-GigabitEthernet1/0/2] quit
```

配置关键点

通过在服务模板中使能 access-control acl 功能，可实现仅ACL rule规则中 permit 匹配的MAC地址允许无线接入。