H3C无线控制器本地MAC认证典型配置举例（V7）

wlan接入 MAC地址认证 AAA 李晨光 2016-06-21 发表

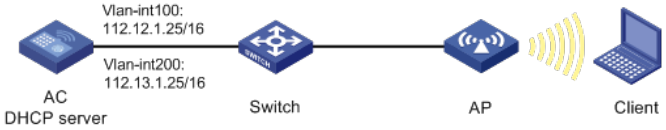
本文档介绍无线客户端通过本地认证方式进行MAC地址认证并访问外网的典型配置举例。

本文档不严格与具体软、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MAC地址认证、WLAN用户接入认证和WLAN接入特性。

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。



1.1 配置步骤

1.1.1 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。AP将获取该IP地址与AC建立CAPWAP隧道。

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。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

(2) 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

(3) 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

(4) 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3ca9f4144c20，密码为明文密码3ca9f4144c20，并指定用户可以使用lan-access服务。

[AC] local-user 3ca9f4144c20 class network

[AC-luser-network-3ca9f4144c20] password simple 3ca9f4144c20

[AC-luser-network-3ca9f4144c20] service-type lan-access

[AC-luser-network-3ca9f4144c20] quit

(5) 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

(6) 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service。

[AC-wlan-st-1] ssid service

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

开启无线服务模板。

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

[AC-wlan-st-1] quit

(7) 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绑定到Radio 2上。

[AC-wlan-ap-officeap] radio 2

[AC-wlan-ap-officeap-radio-2] service-template 1

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

1.1.2 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。

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

1.2 验证配置

完成以上配置后，无线用户Client连接到WLAN网络并进行MAC地址认证。在AC上通过命令**display wlan client**可以看见无线用户Client从VLAN 200上线。

```
[AC] display wlan client
 Total Number of Clients          : 1
                          Client Information
 SSID: service
--------------------------------------------------------------------------------
MAC Address    User Name           APID/RID IP Address                  VLAN ----------------------------
------------------------------------------------------------
3ca9-f414-4c20 3ca9f4144c20          1/2   112.13.0.2                   200
```

1.3 配置文件

· AC：

```
#
dhcp enable
#
vlan 1
#
vlan 100
#
vlan 200
#
dhcp server ip-pool vlan100
 gateway-list 112.12.1.25
 network 112.12.0.0 mask 255.255.0.0
#
dhcp server ip-pool vlan200
 gateway-list 112.13.1.25
 network 112.13.0.0 mask 255.255.0.0
#
wlan service-template 1
 ssid service
 vlan 200
 client-security authentication-mode mac
 mac-authentication domain local-mac
 service-template enable
#
interface Vlan-interface100
 ip address 112.12.1.25 255.255.0.0
#
interface Vlan-interface200
 ip address 112.13.1.25 255.255.0.0
#
interface GigabitEthernet1/0/1
 port link-type trunk
 undo port trunk permit vlan 1
```

```
 port trunk permit vlan 100 200
 port trunk pvid vlan 100
#
domain local-mac
 authentication lan-access local
 authorization-attribute idle-cut 15 1024
#
local-user 3ca9f4144c20 class network
 password cipher $c$3$KWMkvq/FnQ2opPqBnpSTs3NPhVKrSOvqFPLAECSiDQ==
 service-type lan-access
 authorization-attribute user-role network-operator
#
wlan ap officeap model WA4320i-ACN
 serial-id 210235A1Q2C159000019
 vlan 1
 radio 1
 radio 2
  radio enable
  service-template 1
#
```

- Switch：

```
#
vlan 1
#
vlan 100
#
vlan 200
#
interface GigabitEthernet1/0/1
 port link-type trunk
 undo port trunk permit vlan 1
 port trunk permit vlan 100
 port trunk pvid vlan 100
#
interface GigabitEthernet1/0/2
 port access vlan 100
 poe enable
#
```

- 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。
- 在AC上配置的MAC地址认证的用户名、密码需要与Client上配置的用户名、密码保持一致，即使用Client的MAC地址作为用户名和密码进行MAC地址认证。
- 配置Switch和AP相连的接口禁止VLAN 1报文通过，以防止AC上VLAN 1内的报文过多。