H3C无线控制器无线客户端静态黑名单配置举例(V7)

wlan接入 wlan射频 wlan安全 用户隔离 **李晨光** 2016-06-23 发表

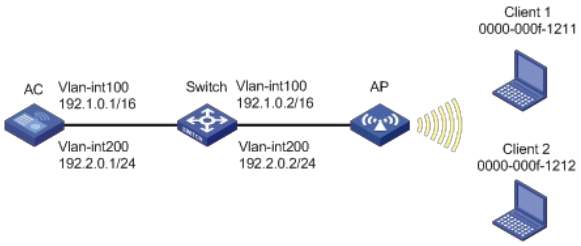
本文档介绍无线客户端静态黑名单典型配置举例。

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无线客户端静态黑名单特性。

如图1所示，AC和AP通过三层交换机Switch连接，三层交换机Switch作为DHCP server为AP和无线客户端分配地址。无线网络采用集中式转发。Client 1为已知非法客户端，通过将Client 1的MAC地址0000-000f-1211加入到静态黑名单中，拒绝该客户端接入无线网络。不对其它客户端的接入做限制。



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 192.1.0.1 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 192.2.0.1 24

[AC-Vlan-interface200] quit

配置与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) 配置无线服务模板

创建服务模板service，并进入无线服务模板视图。

[AC] wlan service-template service

配置SSID为service。

[AC-wlan-st-service] ssid service

配置无线服务模板VLAN为200。

[AC-wlan-st-service] vlan 200

开启无线服务模板。

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

[AC-wlan-st-service] quit

创建AP，配置AP名称为officeap，型号名称选择WA4320i-ACN，并配置序列号210235A1GQC158004457。

[AC] wlan ap officeap model WA4320i-ACN

[AC-wlan-ap-officeap] serial-id 210235A1GQC158004457

进入Radio 1视图。

[AC-wlan-ap-officeap] radio 1

将无线服务模板service绑定到Radio 1，并开启射频。

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

[AC-wlan-ap-officeap-radio-1] radio enable

[AC-wlan-ap-officeap-radio-1] quit

[AC-wlan-ap-officeap] quit

配置将Client 1加入静态黑名单。

[AC] wlan static-blacklist mac-address 0000-000f-1211

1.1.2 配置Switch

创建VLAN 100，用于转发AC和AP间CAPWAP隧道内的流量。

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 100接口的IP地址。

[Switch] interface vlan-interface 100

[Switch-Vlan-interface100] ip address 192.1.0.2 16

[Switch-Vlan-interface100] quit

配置VLAN 200接口的IP地址。

[Switch] interface vlan-interface 200

[Switch-Vlan-interface200] ip address 192.2.0.2 24

[Switch-Vlan-interface200] quit

开启DHCP功能。

[Switch] dhcp enable

配置DHCP地址池100，用于为AP分配IP地址。

[Switch] dhcp server ip-pool 100

[Switch-dhcp-pool-100] network 192.1.0.0 mask 255.255.0.0

[Switch-dhcp-pool-100] gateway-list 192.1.0.1

[Switch-dhcp-pool-100] quit

配置DHCP地址池200，用于为Client分配IP地址。

[Switch] dhcp server ip-pool 200

[Switch-dhcp-pool-200] network 192.2.0.0 mask 255.255.255.0

[Switch-dhcp-pool-200] gateway-list 192.2.0.1

[Switch-dhcp-pool-200] quit

1.2 验证配置

AP与AC正常连接后，在AC上可以通过**display wlan blacklist static**命令查看静态黑名单表项，发现Client 1已被加入静态黑名单。

```
[AC] display wlan blacklist static
Total number of clients: 1
 MAC addresses:
  0000-000f-1211
```

在AC上可以通过**display wlan client**命令查看无线客户端的信息，从显示信息中可以看出，Client 2成功接入无线网络，而Client 1被禁止接入。

```
[AC] display wlan client
Total number of clients: 1

MAC address     Username          APID/RID  IP address              VLAN ID
0000-000f-1212  N/A               1/1       192.2.0.3               200
```

1.3 配置文件

- AC：

```
#
vlan 1
#
vlan 100
#
vlan 200
#
wlan service-template service
 ssid service
 vlan 200
 service-template enable
#
interface Vlan-interface100
 ip address 192.1.0.1 255.255.0.0
#
interface Vlan-interface200
 ip address 192.2.0.1 255.255.255.0
#
interface GigabitEthernet1/0/1
 port link-type trunk
 port trunk permit vlan 1 100 200
#
wlan ap officeap model WA4320i-ACN id 1
 serial-id 210235A1GQC158004457
 radio 1
  radio enable
  service-template service
#
wlan static-blacklist mac-address 0000-000f-1211
#
```

- Switch：

```
#
vlan 1
#
vlan 100
#
vlan 200
#
dhcp server ip-pool 100
 network 192.1.0.0 mask 255.255.0.0
 gateway-list 192.1.0.1
#
dhcp server ip-pool 200
```

```
 network 192.2.0.0 mask 255.255.255.0
 gateway-list 192.2.0.1
#
interface Vlan-interface100
 ip address 192.1.0.2 255.255.0.0
#
interface Vlan-interface200
 ip address 192.2.0.2 255.255.255.0
#
interface GigabitEthernet1/0/1
 port link-type trunk
 port trunk permit vlan 1 100 200
#
interface GigabitEthernet1/0/2
 port link-type access
 port access permit 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。