H3C 无线控制器

本地 Portal MAC-Trigger 快速认证典型配置举例(V7)

资料版本：6W100-20191125

目 录

1 简介

本文档介绍本地 Portal MAC-Trigger 快速认证配置举例。

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、WLAN 特性。

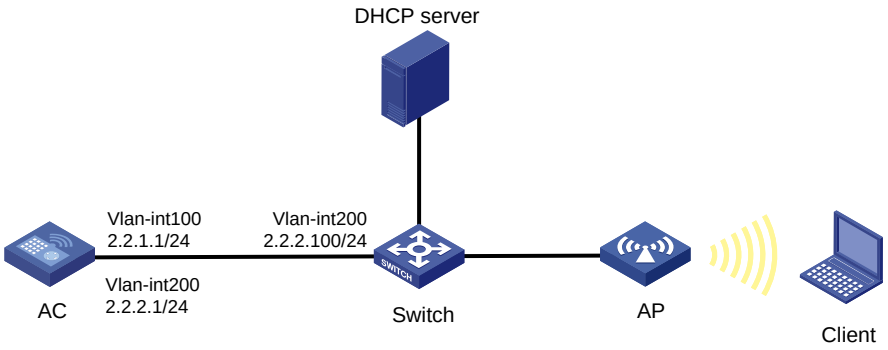
3 配置举例

3.1 组网需求

如图 1 所示，AP 和 Client 通过 DHCP 服务器获取 IP 地址，AC 同时作为 Portal 认证服务器和 Portal Web 服务器、MAC 绑定服务器，要求：

- AC 采用直接方式的 Portal 认证。
- Client 在通过 Portal 认证前，只能访问 Portal Web 服务器；Client 通过 Portal 认证后，可以访问外部网络。
- 在 Client 的流量达到 1024000 字节之前，允许 Client 访问外部网络资源，一旦流量达到 1024000 字节，则触发 MAC 快速认证。
- 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。

图1 本地 Portal 基于 MAC 地址的快速认证组网图



3.2 配置思路

- 为了使用户正常访问 Portal Web 服务器，必须配置 Portal 免认证规则，放行访问 Portal Web 服务器的流量。

- 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。

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。
- 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
- 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。

3.4 配置步骤

3.4.1 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。

```
<AC> system-view
[AC] vlan 100
[AC-vlan100] quit
[AC] interface vlan-interface 100
[AC-Vlan-interface100] ip address 2.2.1.1 24
[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 2.2.2.1 24
[AC-Vlan-interface200] quit
```

(2) 配置认证域

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 Local。

```
[AC-isp-dm1] authentication portal local
```

为 Portal 用户配置 AAA 授权方法为 none。

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

为 Portal 用户配置 AAA 计费方法为 none。

```
[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
```

(3) 配置 Portal 认证

配置 Portal Web 服务器的 URL 为 http://2.2.2.1:8080/portal。

```
[AC] portal web-server newpt
[AC-portal-websvr-newpt] url http://2.2.2.1:8080/portal
```

配置设备重定向给用户的 Portal Web 服务器的 URL 中携带参数。

```
[AC-portal-websvr-newpt] url-parameter wlanuserip source-address
[AC-portal-websvr-newpt] quit
```

创建本地 Portal Web 服务器，进入本地 Portal Web 服务器视图，并指定使用 HTTP 协议和客户端交互认证信息。

```
[AC] portal local-web-server http
```

配置本地 Portal Web 服务器提供的缺省认证页面文件为 abc.zip（设备的存储介质的根目录下必须已存在该认证页面文件，否则功能不生效）。

```
[AC–portal-local-websvr-http] default-logon-page abc.zip
[AC–portal-local-websvr-http] tcp-port 8080
[AC–portal-local-websvr-http] quit
```

配置本地 Portal 认证的用户名和密码。

```
[AC] local-user portaluser class network
[AC-luser-network-portaluser] password simple abc123
[AC-luser-network-portaluser] service-type portal
[AC-luser-network-portaluser] 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
```

(4) 配置 Portal 基于 MAC 地址的快速认证

创建 MAC 绑定服务器 mts，并进入 MAC 绑定服务器视图。

```
[AC] portal mac-trigger-server mts
```

配置用户免认证流量的阀值为 1024000 字节。

```
[AC-portal-mac-trigger-server-mts] free-traffic threshold 1024000
```

配置 MAC 绑定服务器的地址为 2.2.2.1。

```
[AC-portal-mac-trigger-server-mts] ip 2.2.2.1
```

开启 Portal 本地 MAC Trigger 认证功能，并配置本地 MAC Trigger 绑定表项的老化时间为 60 分钟。

```
[AC-portal-mac-trigger-server-mts] local-binding enable
[AC-portal-mac-trigger-server-mts] local-binding aging-time 60
[AC-portal-mac-trigger-server-mts] quit
```

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 200。

```
[AC-wlan-st-st1] vlan 200
```
在无线服务模板 st1 上开启直接方式的 Portal 认证。
```
[AC-wlan-st-st1] portal enable method direct
```
配置接入的 Portal 用户使用认证域为 dm1。
```
[AC-wlan-st-st1] portal domain dm1
```
在无线服务模板 st1 上引用 Portal Web 服务器 newpt。
```
[AC-wlan-st-st1] portal apply web-server newpt
```
在无线服务模板上应用 MAC 绑定服务器 mts。
```
[AC-wlan-st-st1] portal apply mac-trigger-server mts
```
开启无线服务模板。
```
[AC-wlan-st-service1] service-template enable
[AC-wlan-st-st1] quit
```
(5) 配置无线服务

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
```
3.4.2 配置Switch

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 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 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 200 接口的 IP 地址。

```
[Switch] interface vlan-interface 200
[Switch-Vlan-interface200] ip address 2.2.2.100 255.255.255.0
[Switch-Vlan-interface200] quit
```

3.5 验证配置

通过执行以下显示命令可查看 MAC 绑定服务器配置。

```
[AC] display portal mac-trigger-server name mts
Portal mac trigger server name: mts
  Version                     : 1.0
  Server type                 : IMC
  IP                          : 2.2.2.1
  Port                        : 50100
  VPN instance                : Not configured
  Aging time                  : 300 seconds
  Free-traffic threshold      : 1024000 bytes
  NAS-Port-Type               : Not configured
  Binding retry times         : 3
  Binding retry interval      : 1 seconds
  Authentication timeout      : 3 minutes
  Local-binding               : Enabled
  Local-binding aging-time    : 60 minutes
  aaa-fail nobinding          : Disabled
  Excluded attribute list     : Not configured
  Cloud-binding               : Disabled
  Cloud-server URL            : Not configured
```

用户通过网页方式进行 Portal 认证。用户在通过认证前，发起的所有 Web 访问均被重定向到 Portal 认证页面（http://2.2.2.1:8080/portal），在通过认证后，可访问非受限的互联网资源。

用户在首次进行 Portal 认证时，需要手工输入用户名和密码。当用户再次上线时，将可以直接访问互联网资源，不会感知到 Portal 认证过程。

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: portal
  Portal server: newpt
  State: Online
  VPN instance: N/A
  MAC             IP                  VLAN    Interface
  0021-6330-0933  2.2.2.2              200     Vlan-interface200
  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
 portal enable method direct
 portal domain dm1
 portal apply web-server newpt
 portal apply mac-trigger-server mts
 service-template enable
#
interface Vlan-interface100
 ip address 2.2.1.1 255.255.255.0
#
interface Vlan-interface200
 ip address 2.2.2.1 255.255.255.0
#
domain dm1
 authorization-attribute idle-cut 15 1024
 authentication portal local
 authorization portal none
 accounting portal none
#
portal host-check enable
#
 portal roaming enable
 undo portal refresh arp enable
#
 portal web-server newpt
 url http://2.2.2.1:8080/portal
 server-type imc
 url-parameter wlanuserip source-address
#
portal server newpt
 ip 2.2.2.1
 server-type imc
#
portal mac-trigger-server mts
 ip 2.2.2.1
```

```
 server-type imc
 free-traffic threshold 1024000
#
wlan ap office model WA4320i-ACN
 serial-id 219801A0CNC138011454
 radio 1
 radio 2
  radio enable
  service-template st1
#
```

- Switch：

```
#
vlan 100
#
vlan 200
#
interface Vlan-interface200
 ip address 2.2.2.100 255.255.255.0
#
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 vlan 100
 poe 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”。
- 《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”。