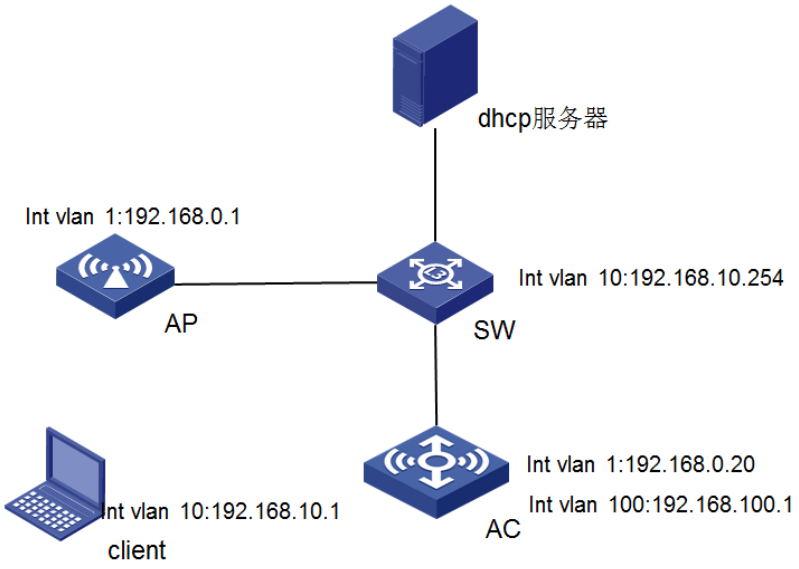
本地Portal无感知本地转发典型配置（V7）

Portal 杨攀 2017-07-31 发表

本案例介绍本地Portal认证无感知的典型配置,当客户端数量较少，且没有Portal服务器时，那么可以采用本地Portal认证无感知的方式来实现客户的无感知需求。
本案例不严格与具体软、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。
本案例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。
本案例假设您已了解Portal认证的特性。

如图1所示，DHCP服务器为AP和Client分配IP地址。现要求：
·AC同时承担Portal Web服务器、Portal认证服务器职责。
·采用直接方式的Portal认证



AP用VLAN 1进行注册，客户端获取的为VLAN 10的地址，网关在交换机上，为192.168.10.254。

一、配置AC

（1）配置AC的接口

创建VLAN1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 1
[AC-vlan100] quit
[AC] interface vlan-interface 1
[AC-Vlan-interface100] ip address 192.168.0.20 24
[AC-Vlan-interface100] quit
在交换机上配置路由，保证启动Portal之前各Client和AC之间的路由可达。（略）
(2)配置无线服务
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 localportal
配置本地转发的VLAN为10。
[AC-wlan-st-st1] client forwarding-location ap vlan 10
配置接入的Portal用户使用认证域为localportal。
[AC-wlan-st-st1] portal domain localportal
[AC-wlan-st-service] quit
#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
(4)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RADIUS。
[AC-isp-dm1] authentication portal local
为Portal用户配置AAA授权方法为RADIUS。
[AC-isp-dm1] authorization portal none
为Portal用户配置AAA计费方法为none，不计费。
[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
(5)配置Portal认证
配置Portal Web服务器的URL为http://192.168.100.1:8080/portal。
[AC] portal web-server newpt
[AC-portal-websvr-newpt] url http://192.168.100.1:8080/portal
配置设备重定向给用户的Portal Web服务器的URL中携带参数wlanuserip。
[AC-portal-websvr-newpt] url-parameter wlanuserip source-address
配置Portal Web服务器类型为imc。
[AC-portal-websvr-newpt] server-type imc
[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PortalWeb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
开启无线Portal漫游功能
[AC] portal roaming enable
#配置无感知的名字为localportal，无感知服务器为192.168.100.1，开启本地无感知功能，设置无感知绑定表项的老化时间为1小时
[AC]portal mac-trigger-server localportal
[AC-portal-mac-trigger-server-localportal]ip 192.168.100.1
[AC-portal-mac-trigger-server-localportal]local-binding enable
[AC-portal-mac-trigger-server-localportal]local-binding aging-time 1
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
(6)配置本地Portal认证的用户名和密码
 # 配置用户名为 123。
[AC] local-user 123 class network
配置密码为123，并调用为portal服务。
[AC-luser-network-123]password simple 123
[AC-luser-network-123]service-type portal
(6)在服务模板下调用mac-trigger,调用web-server，并且使能portal认证。
[AC-wlan-st-service] portal web-server newpt
[AC-wlan-st-service] portal apply mac-trigger-server localportal
[AC-wlan-st-service] portal enable method direct
[AC-wlan-st-service] service-template enable
二、给AP下发MAP文件。
sys-view
vlan 10

int g1/0/1
port link-type trunk
port trunk permit vlan 10 1

三、配置交换机。

创建VLAN 10，用于转发Client无线报文。
[Switch] vlan 10。
[Switch-vlan200] quit。
配置Switch与AP相连的GigabitEthernet1/0/1接口的属性为Trunk，允许VLAN 10通过。
[Switch] interface gigabitethernet 1/0/1。
[Switch-GigabitEthernet1/0/1] port link-type trunk。
[Switch-GigabitEthernet1/0/1] port trunk permit vlan 10 1。
[Switch-GigabitEthernet1/0/1] quit。
#在交换机上配置客户的DHCP
[switch]dhcp server ip-pool vlan10。
[switch-dhcp-pool-vlan10]network 192.168.10.0 24。
[switch-dhcp-pool-vlan10]gateway-list 192.168.10.254。
[switch-dhcp-pool-vlan10]dns-list 8.8.8.8。

四、实验结果。

第一次进行无感知认证时，首先会输入用户名和密码，认证成功之后可以通过命令查看。
[IRF]display portal user all
 Total portal users: 1
 Username: 1234
 AP name: ap1
 Radio ID: 1
 SSID: localportal
 Portal server: N/A
 State: Online
 VPN instance: N/A
 MAC IP VLAN Interface
68db-ca64-23fd 192.168.10.1 10 WLAN-BSS2/0/8
 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
查看本地MAC无感知的表项，当有本地portal无感知表项之后，说明无感知生效，接下来就客户端可以实现无感知。
[IRF]display portal local-binding mac-address all
 Total mac-address number: 1
 Mac-address User-name
 68db-ca64-23fd 1234

1. 客户端和AC能ping通，也就是客户端的网关要和AC能通。
2. AC上必须要配置portal host-check enable，来通过客户端的表项来检查客户端信息。
3. 给AP下发MAP文件放通客户端的相应VLAN。