开启二层隔离后终端有时无法访问服务器地址

wlan接入 用户隔离 裴锐霖 2016-03-23 发表

二层隔离的作用是减少网络中的广播报文，特别是无线网络中，一般做无线优化都建议开启二层隔离功能，减少无线网络中的广播报文。
某局点用户配置了二层隔离，放通了服务器的MAC地址，服务器也是通过无线连接到网络当中，但是出现同VLAN下的部分PC无法访问到服务器，关闭二层隔离功能后是正常的。

无

通过实验及问题分析

基于VLAN的二层隔离，要实现无线终端访问某台接入无线网络的固定主机，添加该主机MAC为隔离组里面允许通过的MAC，只有该主机触发ARP后，才可以实现其他无线终端访问该主机，一般现实网络环境中，如果主机为FTP/WEB Server都不会主动触发，因此该方案不能满足用户二层隔离的情况下访问服务器的需求。
因此建议采用基于VLAN二层隔离+ MAC-VLAN，在接入同一个ssid的情况下，把服务器划分到特殊的vlan，通过三层实现无线终端可以访问服务器，但无线终端之间不能互通。
由于mac-vlan的优先级最高，所以即使服务器和客户端接入的是同一个ssid和ap，但可以根据服务器的mac地址，把服务器划分到特殊的vlan内。

关键配置如下：

```
 #把服务器的mac地址通过mac-vlan划分到 vlan 10
mac-vlan mac-address acfd-ce43-7c18 vlan 10 priority 0
#基于VLAN的二层隔离开启，并允许网关地址通过，vlan10为给服务器划分的vlan，vlan11为普通客户端的vlan
user-isolation vlan 10 enable
user-isolation vlan 10 permit-mac 80f6-2e96-f0b2
user-isolation vlan 11 enable
user-isolation vlan 11 permit-mac 80f6-2e96-f0b2

#创建VLAN
vlan 10 to 11

#配置基于VLAN的地址池
dhcp server ip-pool vlan10
network 10.0.0.0 mask 255.255.255.0
gateway-list 10.0.0.1
dhcp server ip-pool vlan11
network 11.0.0.0 mask 255.255.255.0
gateway-list 11.0.0.1

#配置VLAN接口地址或网关
interface Vlan-interface10
ip address 10.0.0.1 255.255.255.0
interface Vlan-interface11
ip address 11.0.0.1 255.255.255.0

#配置WLAN-ESS接口，使能MAC-VLAN功能
interface WLAN-ESS2
port link-type hybrid
undo port hybrid vlan 1
port hybrid vlan 10 to 11 untagged
mac-vlan enable

#配置服务模板，绑定WLAN-ESS2接口
wlan service-template 2 clear
ssid test-h3c
bind WLAN-ESS 2
service-template enable

#AP2配置信息
wlan ap ap2 model WA4620i-ACN id 3
serial-id 210235A1BSC145001796
```

```
radio 1
  max-power 1
  service-template 2 vlan-id 11
  radio enable
radio 2
  max-power 1
  service-template 2 vlan-id 11
  radio enable
```

如上配置后，客户端接入后会划分到vlan10，服务器接入后会划分到vlan11，客户端和服务器通过三层互访，客户端与客户端之间不能互访。

当无线网络中开启二层隔离，并且服务器也是通过无线接入的，建议采用基于VLAN二层隔离+ MAC-VLAN，在接入同一个ssid的情况下，把服务器划分到特殊的vlan，客户端划分到普通业务vlan，客户端访问服务器通过三层互访，客户端与客户端之间不能互通。