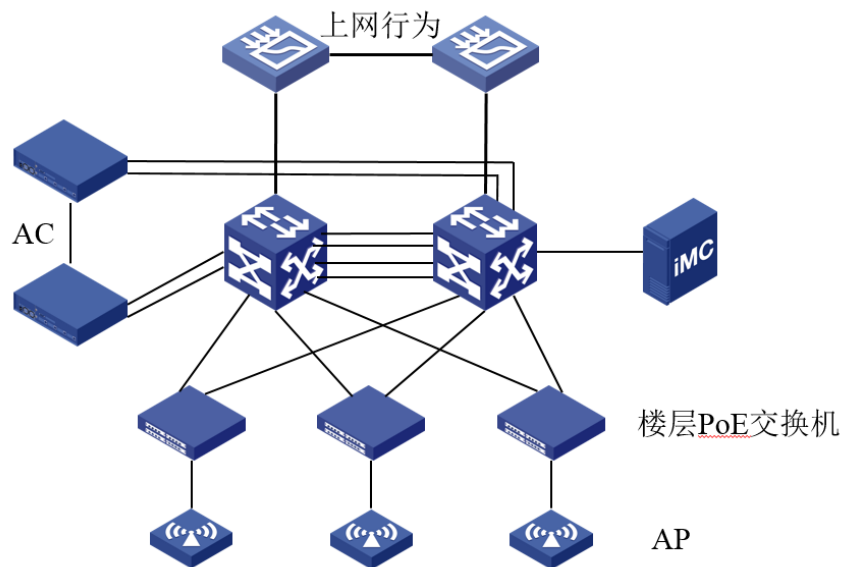


知 某局点无线Portal认证重定向失败问题经验案例

Portal 尹灵康 2018-03-09 发表

客户无线控制器结合IMC进行Portal无感知认证，有两个SSID，并各自起了Portal认证。在使用中发现，在两个SSID间切换多次时，会弹出认证页面，重新进行认证，且无法访问网络：即当用户连接ssid1时，进行常规Portal认证，可以正常使用网络；当用户切换到ssid2时，同样进行Portal认证，正常使用网络；当用户再切换回ssid1时，用户会进行重新认证，但推送的url是由上网行为设备给出的，且不能正常使用网络。

组网：



组网如上图，核心交换机上联上网行为设备，上网行为设备中也有Portal认证，用于控制整个网络中用户访问外网的情况。AC上配置了两个SSID：ssid1和ssid2，分别对应两个不同的VLAN：vlan10和vlan20，并在vlan接口下起了Portal+MAC-trigger无感知认证。

配置如下：

```
#
interface Vlan-interface10
description ssid1
ip address 10.6.15.253 255.255.248.0
portal server imc method direct
portal domain portal
portal nas-port-type wireless
portal backup-group 3
portal nas-ip 10.1.11.253
portal mac-trigger enable
portal mac-trigger server ip 10.1.11.5
#
interface Vlan-interface20
description ssid2
ip address 10.6.23.253 255.255.248.0
portal server imc method direct
portal domain portal
portal nas-port-type wireless
portal backup-group 4
portal nas-ip 10.1.11.253
portal mac-trigger enable
portal mac-trigger server ip 10.1.11.5
#
interface WLAN-ESS10
port link-type hybrid
undo port hybrid vlan 1
port hybrid vlan 10 untagged
port hybrid pvid vlan 10
```

```

mac-vlan enable
#
interface WLAN-ESS20
port link-type hybrid
undo port hybrid vlan 1
port hybrid vlan 20 untagged
port hybrid pvid vlan 20
mac-vlan enable
#
domain portal
authentication portal radius-scheme portal
authorization portal radius-scheme portal
accounting portal radius-scheme portal
access-limit disable
state active
idle-cut enable 30 512
self-service-url disable
#
wlan service-template 10 clear
ssid ssid1
bind WLAN-ESS 10
service-template enable
#
wlan service-template 20 clear
ssid ssid2
bind WLAN-ESS 20
service-template enable
#

```

当用户由ssid2切换回ssid1时，设备会进行重定向，弹出Portal认证页面，但此Portal页面并不是IMC上配置的，而是上网行为设备中的认证页面。但在AC上debug，并没有看到此重定向过程的信息，设备上从vlan10获取的IP地址的Portal用户信息也一直存在。因此怀疑是IMC服务器在进行认证时出现问题。

经分析，IMC服务器上有如下机制：当服务器上存在同一MAC地址对应多个IP地址时，会将前几个IP地址对应的用户下线，并删除其用户记录，仅保留最新的用户信息，然后服务器会将用户下线的信息上报给上行设备，不会通知接入设备。此机制只在nas-ip相同的情况下有效，当同一MAC地址对应不同IP地址且nas-ip不同时，所有的用户表项均不会被删除。

因此在此问题中，当用户由ssid2切换回ssid1后，之前分配的vlan10的IP地址，在IMC服务器上被删除表项信息，用户下线，但AC设备上还记录有Portal表项，用户数据会直接被转发到上行设备，上行的上网行为设备中没有此用户的表项，于是触发认证，给用户返回Portal登录页面。

此问题的解决方法有两种：

1. IMC上删除用户表项必须在同一nas-ip下，因此配置Portal认证时，可以指定不同的nas-ip。
2. 此问题出现的原因是IMC上已无用户表项，但AC接入设备上还记录有其Portal用户表项，可以配置强制用户下线命令：portal wlan ssid-switch logoff //当用户断开连接时，即删除其Portal表项。