无线终端切换楼栋后无法上网经验案例

wlan优化 范书珩 2023-06-28 发表

组网及说明

现场组网：1号楼和2号楼使用不同厂商的设备，相同的SSID，不同网段，1号楼部署我司无线AC+AP，2号楼部署友商设备，使用802.1x认证，出口使用防火墙做控制

1号楼网段：10.2.0.0/16

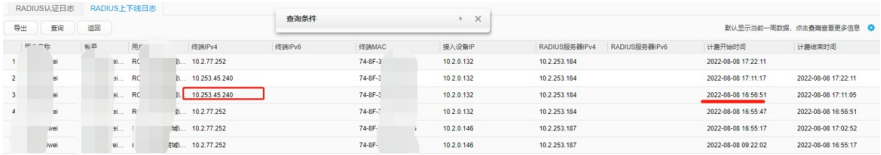
2号楼网段：10.253.0.0/16

问题描述

终端从2号楼切换到1号楼偶发出现无法上网

过程分析

终端从2号楼切换到1号楼后偶发出现无法上网，从radius服务器上的日志分析发现终端在1号楼的时候依然使用2号楼的ip地址10.253.45.240，推测AC通过ARP学习收到了终端使用10.253.45.240发送的arp报文，所以AC也用终端在2号楼获取的ip地址10.253.45.240向radius服务器发送了计费更新报文，radius服务器联动出口防火墙放通了10.253.45.240可以继续上网，但是由于在1号楼上线的终端无法与2号楼的网关进行通信，因此终端后续通过dhcp将ip地址更新为了1号楼的10.2.77.252，但是这个地址未在防火墙上进行放通所以无法进行上网。



通常遇到这个问题我们有以下两个解决思路：

1.当AC检测到终端的ip地址发生变化时会立即向服务器发送计费停止报文，随后发送计费更新报文，这样就可以保证终端切换楼栋后正常使用，相关命令如下:
client-security accounting-restart trigger ipv4 [delay interval]
delay interval：重新发送计费开始报文的延迟时间，取值范围为0～20，单位为秒，缺省取值为15秒。但是这个方法的缺点就是网络中可能产生大量的计费报文，radius服务器的性能可能无法承受，因此不建议使用这个方法。
2.关闭AC的arp学习功能（Undo client ipv4-snooping arp-learning enable），保证AC只通过dhcp学习到正确的ip地址从而发送正确的计费更新报文，这个方法可以避免AC用错误的ip地址发送计费更新报文的情况，但是关闭了AC的arp学习功能后，终端在漫游过程中如果无法及时触发dhcp流程，ac又无法通过arp学习到终端的IP地址，那么就可能出现短暂网络中断的情况，因此也不建议采用这个方法。

针对这个问题的场景，上述两个解决方案都有相应的缺陷，可以配置基于ACL规则学习终端IP地址，这个功能可以根据指定的acl配置的规则对新接入的无线客户端进行ip地址学习控制。当无线客户端接入无线网络时，设备学习终端IP地址时，会判断无线客户端的IP地址是否在ACL访问控制列表的规则中，具体的过滤机制如下：
·如果在permit规则中，则学习无线客户端的IP地址；
·如果在deny规则中，则拒绝学习无线客户端IP地址；
·如果未匹配任何已配置的规则，则拒绝学习无线客户端IP地址。
可以参考如下配置

```
 acl basic 2001
 description white_list
 rule 5 permit source 10.2.0.0 0.0.255.255
 rule deny

wlan service-template 10
 ssid JD
client ip-snooping acl 2001
service-template enable
```

终端携带2号楼的ip地址接入我司1号楼的设备，AC拒绝学习2号楼的ip地址，只学习1号楼的ip地址10.2.0.0/16，避免AC用2号楼的ip地址发送计费报文给防火墙，并且这个功能也不影响终端的正常漫游，不会给服务器发送大量的计费报文，可以解决这个问题。

解决方法

配置基于ACL规则学习终端IP地址规则，避免AC学习到错误的ip地址，将正确的地址段放通：

```
 acl basic 2001
 description white_list
 rule 5 permit source 10.2.0.0 0.0.255.255
 rule deny

wlan service-template 10
 ssid JD
client ip-snooping acl 2001
service-template enable
```