如何在交换机上流统AC和AP之间的管理报文

AP管理 谭奇伟 2023-01-09 发表

组网及说明

遇到AP在AC无法注册上线，或者AP频繁掉线问题，无线侧通过debug wlan capwap报文交互或者查看掉线AP自动生成的ap-diag.txt(掉线时有ping AC记录), 可能给出中间设备丢包的初步结论, 此时, 如何在中间设备(AC和AP的中间设备主要是交换机)排查丢包的位置就成为下一步排查的关键.

交换机上提供了流统这样一种非常有效的手段,用于辅助排查链路丢包.

那么针对AP无法注册上线/AP频繁掉线这类主要涉及AC和AP之间管理报文交互的情形, 如何进行流统配置了, 本案例给出了参考的配置方案.

本案例按照如下示意图进行配置:

配置步骤

现假设AP(MAC地址：b044-14bf-4a2) 无法在AC上注册上线, 而无线侧通过在AC和AP同时开启wlan capwap debug, 发现AP发出了discover request请求, 却没有收到AC侧的discover response报文, 与此同时, AC侧的wlan capwap debug打印记录中没有对应不上线AP发过来的discover request报文, 因此怀疑capwap报文丢在中间链路了, 于是在AC和AP之间的交换机上进行流统. (这里AC和AP之间一般有多级交换机, 但配置原理类似)

首先, 控制AP在AC注册和AP掉线的是CAPWAP-Control(管理报文), 其属于UDP报文, 交互时AC固定采用5246端口, 而AP则采用一个随机端口.

因此流统的时候, 指定5246端口分别为源端口或目的端口, 同时添加AP的MAC地址, 就能双向流统到AC和AP之间的管理报文交互.

如果AP是二层注册，由于二层注册一般不配置option 43或者138指定AC的IP地址，AP一般通过广播或者组播发现AC，因此CAPWAP管理报文discover request中的源目IP不一定是AC和AP的IP地址。因此acl不建议指定AC和AP的IP地址进行筛选，而是指定AP的MAC作为筛选条件。可以参考如下配置:

```
#
acl advanced 3010
rule 0 permit udp destination-port eq 5246
#
 acl advanced 3011
 rule 0 permit udp source-port eq 5246
#
traffic classifier ap-in operator and
 if-match acl 3010 if-match source-mac b044-14bf-4a20
#
traffic classifier ap-out operator and
 if-match acl 3011 if-match destination-mac b044-14bf-4a20
#
traffic behavior ap-in
 accounting packet
# traffic behavior ap-out
 accounting packet
#
qos policy ap-in
 classifier ap-in behavior ap-in
#
qos policy ap-out
 classifier ap-out behavior ap-out
#
interface GigabitEthernet1/0/2
 port access vlan 100
 qos apply policy ap-out inbound
 qos apply policy ap-in outbound
#
interface GigabitEthernet1/0/7
 port link-type trunk port trunk permit vlan 1 100 300
 port trunk pvid vlan 100
 qos apply policy ap-in inbound
 qos apply policy ap-out outbound
 poe enable
#
```

如果AP是三层注册，AP一般通过单播discover request请求发现AC，此时由于三层依靠路由转发，discover request或者response及后续管理报文的源目MAC会在网关处跨vlan时发生变化，因此建议使用AC和AP的IP地址作为筛选条件，此时筛选条件中不能再携带AP的MAC，可将ACL改为：

```
#
acl advanced 3010
 rule 0 permit udp source [AP-ip] 0 destination [AC-ip] 0 destination-port eq 5246
#
acl advanced 3011
 rule 0 permit udp source [AC-ip] 0 destination [AP-ip] 0 source-port eq 5246
```

#
traffic classifier ap-in operator and
 if-match acl 3010 if-match   // 这里不能再携带AP的MAC地址
#
traffic classifier ap-out operator and
 if-match acl 3011 if-match   // 这里不能再携带AP的MAC地址

配置关键点

查看流统结果命令：

[SW] dis qos policy interface g 1/0/2
[SW] dis qos policy interface g 1/0/7
[SW] dis qos policy interface inbound
[SW] dis qos policy interface outbound
注意流统前清空对应端口流量统计:
reset counters int g 1/0/2
reset counters int g 1/0/7