某局点特殊时间段无线控制器CPU利用率高达100%，设备卡顿的经验案例

CPU　进程监控和维护配置　**张自成**　2017-03-15 发表

现场反馈最近网络出现每天上班时间八点半至九点半之间无线网络卡顿，故障时候登录设备，几乎无法操作，无法采集诊断信息。

由于故障时候无法操作设备，待网络正常之后采集了诊断信息发现：

==========display cpu-usage history==========
100%|　　#　## ########## ##　　　　###
 95%|　　## ### ########## # 　　　　######
 90%|　　### #### ########################## # #########
 85%|　　### ##
 80%|　　##
75%|　　##
70%|　　##
65%|　　##
60%|　　##
55%|　　##
50%|##
45%|##
40%|##
35%|##
30%|##
25%|##
20%|##
15%|##
10%|##
 5%|##
CPU的历史记录确认存在100%的情况，再查看具体的进程
 ==========display process==========

　　45　　45 23.1　0.0　D　115　　-　25:04:28 [Rcv-SingleCPU0]
　　46　　46 14.2　0.0　D　115　　-　17:26:07 [Rcv-SingleCPU1]
正常的时候设备cpu利用率主要进程是上面这两个，这两个是软件收包的进程，然后在接口下发现
Input (total):　720429141 packets, 424569144855 bytes
　　628430760 unicasts, 389678 broadcasts, 91608703 multicasts, 0 pauses
 Input (normal):　720429141 packets, 424569144855 bytes
　　628430760 unicasts, 389678 broadcasts, 91608703 multicasts, 0 pauses

有大量的组播报文，甚至超过了单播的数量。所有怀疑是组播类攻击或者业务，以至于存在异常报文冲击导致的软件收发报文进程CPU高。
想要具体定位故障时间点上送CPU报文的具体情况可以通过下面的方式来采集。
在probe模式下：

fpl-diag　showcpstat　　//该命令执行之后可以看到1到32号的协议
**********fpl showcpstat: start **********
Idx Proto　　Rx　　Drop　　RxSpeed(pps)
---
 1 dot1x　　0　　0　　0
 2 dhcp　　41182　　0　　0
 3 igmp　　170491　　0　　0
 4 ntp　　0　　0　　0
 5 arp　　2038531　　0　　9
 6 snmp　　0　　0　　0
 7 telnet　　64531　　0　　2
 8 icmp　　0　　0　　0
 9 icmpv6_nd　　0　　0　　0
10 icmpv6_other　0　　0　　0
11 iactp　　0　　0　　0
12 acsei　　0　　0　　0

13 http 0 0 0
14 udp 27943 0 0
15 tcp 9252126 0 22
16 ip 14721 0 0
17 ipv6 0 0 0
18 ethernet 14722 0 0
19 radius 0 0 0
20 vrrp 0 0 0
21 capwap_ctrl 10786932 0 22
22 capwap_data 506962669 0 4506
23 dot11_auth 0 0 0
24 dot11_assoc 777658 0 4
25 dot11_reassoc 90 0 0
26 dot11_null 231 0 0
27 dot11_disassoc 0 0 0 0
28 dot11_deauth 0 0 0 0
29 dot11_action 0 0 0 0
30 dot11_ctrl 224922 0 1
31 portal_syn 0 0 0
32 lacp 0 0 0

接着执行这条命令：

fpl-diag showcplog 5,9,8,30,50 //该命令查看5号协议的arp在日期9号 8点30分之后的50条记录

1分钟记录一条，比如下面：

[XESPY_ZD_AC1-probe]fpl-diag showcplog 5,9,8,30,80

idx proto date rx drop delta

7144 arp 08:30:12 02/09/2017 1821692 0 50

7145 arp 08:31:12 02/09/2017 1821742 0 50

7146 arp 08:32:12 02/09/2017 1821810 0 68

其中idx proto表示协议号，date为时间，delta为增长速度，我们需要知道CPU高的时候哪种协议报文上送CPU的增长速度快，依次来判断定位具体原因。

配合现场收集的现象8：30~9：30 这个时间段的CPU规律性变高，可以证明高峰期的时候存在大量报文冲击AC 造成设备繁忙。

目前计划如下优化策略：

1、 开启无线的二层隔离，广播隔离。

2、 检查vlan配置，AC对端设备接口不要配置没有必要的vlan，防止其余vlan报文上送AC。虽然AC不转发但是硬件还是会进行处理。

3、如果是异常报文或者某些固定终端IP发出的报文，可以采取包过滤的方式暂时消除故障，再去排查终端。

若复现CPU过高，可以通过dis cpu-usage history job + job号 来回溯进程一个小时内的使用情况，目前看来基本上就是软件收发报文这个进程过高导致的。

对于固定时间段设备CPU利用率高，设备卡顿的情况，无法采集实时信息的情况，可以通过上述方法来定位具体是哪种报文上送CPU导致的，另外也可以进行抓包，具体查看是否存在大量异常攻击报文，比如组播，比如icmpv6报文等等来定位网络中是否存在异常主机或者攻击。