某局点ARP刷新异常导致AP掉线的经验案例

wlan接入 ARP 余晨 2015-12-15 发表

2015年11月10日23点57分左右，该局点园区1号楼AC发生与AP不通并随后AP大面积掉线的情况，导致无线用户短时无法上网，40秒左右后自动恢复。在此过程中，1号楼AC的出现过CPU 100%的告警。无线网络中的其他7台AC没有出现问题。

一、对AC设备的分析

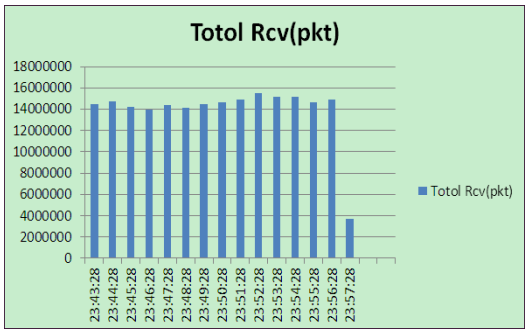
1号楼的AC上注册有502台AP，其中有426台发生掉线。但此时该AC与备AC的热备链路并未断开，与另外7台AC的漫游组隧道也没有断开，说明此时AC的数据平面和控制平面均能工作正常。从AC驱动的收报统计看此时也没有控制报文丢包的情况，所有的接收到的控制报文均送CPU进行处理了，驱动底层也未见硬件收发包异常的情况。

5724 lwapp_ctrl 23:57:28 11/10/2015 738376620 0(该列表示丢包数) 12175

5724 iactp 23:57:28 11/10/2015 62661655 0 921

5724 lwapp_data 23:57:28 11/10/2015 822075228 0 6785

AC驱动每分钟会统计一次从以太口接收的网络报文数量，如下图。

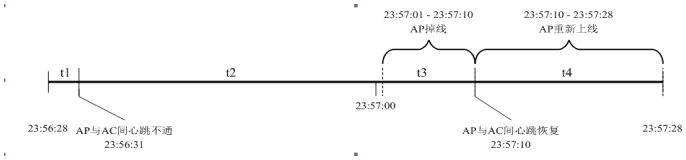


记录时间是每分钟的28秒，以23:56:28的统计为例，它记录的是从23:55:28到23:56:28这一分钟之内的AC以太口接收到的网络报文总数。从图中可以明显看出在23:56:28之前的收包统计基本上处于1400万~1500万这个范围（我们可以认定这是一个正常值的范围）。而在23:57:28秒记录的收包统计值只有300多万，与正常值相比明显少了太多。

通过分析所有掉线AP的log可以明确以下几点：

- 以该AC为主AC的AP掉线时间是从23:57:01开始，持续到23:57:09；
- 掉线的AP从23:57:10开始恢复上线；
- 期间没有掉线的AP（以故障AC为主AC的AP）为63台。

AP心跳默认超时时间为30秒，以此推算，AP与AC之间的心跳报文从23:56:31开始丢失。23:56:28到23:57:28这一分钟可以分成如下几个时间段：

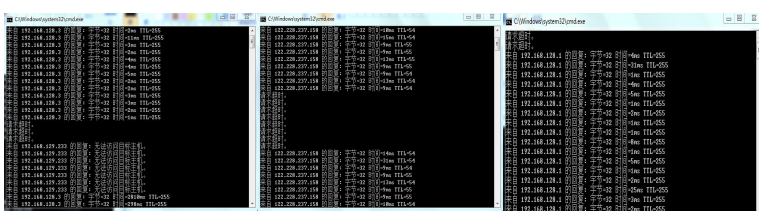


其中：

- t1（23:56:28-23:56:31）：3秒，AC与AP之间通信正常，心跳正常；
- t2及t3（23:56:31-23:57:10）：39秒，AC与AP之间心跳不通，AP在t3时间段内大量掉线；
- t4（23:56:10-23:56:28）：18秒，AC与AP之间通信恢复，AP开始重新上线；

t1和t4两段时间内产生的流量估计大概有100~200万个。减掉这部分流量，在t2及t3两段时间内，AC上接收到的网络报文量只有200万左右，明显少于正常水平。

另外，故障期间有63台AP始终没有掉线，恰好有一台无线客户连在其中的一个AP上并持续对网关设备、AC及外网服务器做ping操作。故障发生的过程中，所有的ping都不通，如下：



ping AC同网段地址 ping外网服务器www.163.com ping网关

依据上面的分析，我们推断在t2及t3时间内（即23:56:31到23:57:10之间）AC与AP之间的通信出现了中断，需要排查从AC到AP之间的上下行通路。

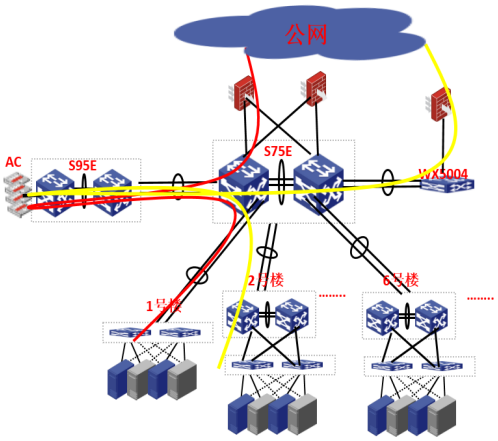
二、对AC-AP间通路的分析

1、对有线设备LOG的分析

故障恢复后，除收集AC侧相关信息后同时针对有线侧设备也进行了初步排查，包括对S36V2、S75E、S95E设备上的诊断信息、diaglog、logfile等信息的收集。通过对收集信息的分析，未发现关于硬件芯片复位、端口up/down、路由震荡、MAC漂移等可能影响流量转发的相关信息。

2、对AC-AP间上下行通路的分析

无线网络拓扑如下图所示：



其中

- 红色通路是SSID为 inc 无线用户访问公网流量，无线终端网关在S95E上
- 黄色通路是SSID为 guest 无线用户访问公网流量，访客无线终端网关在WX5004上
- 绿色通路为有线终端通过接入交换机上联至S75E并最终到公网的流量。
- 无线终端流量上送时由于S75E和各AC板卡都在vlan800内，所以S75E转发到AC板卡的流量是通过ARP进行转发。
- 从AC侧下行流量是通过AC侧默认路由指向S95E，再通过S95E上的默认路由指回S75E，该通路也是在vlan800内。

由于故障期间，所有有线终端的网络访问正常，因此可以首先排除从接入交换机S36到S75E之间的问题。那么造成AP与AC之间通信中断的原因，集中在S75E—S95E—AC这三点之间。

AP发送给AC的上行LWAPP隧道报文是在S75E上查询ARP表项后通过vlan800的二层转发到达AC的，因此如果上行通路发生终端，那么最大的可能是S75E上查询不到AC的ARP或者AC的ARP表项错误。

AC发送给AP的下行LWAPP隧道报文是在AC通过默认路由发送给S95E，然后S95E再通过默认路由发送给S75E。这里涉及到两次ARP表项的查询：

（1）AC通过默认路由发送给S95E：AC上要查询默认网关（S95E）的ARP表项，然后通过vlan800将报文发送S95E；

（2）S95E通过默认路由发送给S75E：S95E上要查询默认网关（S75E）的ARP表项，然后通过vlan800将报文发送S75E；

上述查询ARP表项的操作同样有可能存在查询不到ARP或者ARP表项错误的情况。由于S95E到S75E是所有AC下行公用的通道，因此可以排除上述（2）中ARP出问题的情况，（1）中出现ARP问题的可能是存在的。

由于vlan800属于核心网络设备间的vlan，不存在收到攻击的情况，也没有排查到有环路的存在，因此可以排除ARP表项错误的原因，仅有的可能就是ARP表项丢失（ARP老化并长时间无法学习到）。S75E上未见针对此AC的丢包。AC上在故障点附近收集到了ARP报文的丢包统计，如下：

idx	proto	date	rx	drop	delta
5722	arp	23:55:28 11/10/2015	80996878	7909	778
5723	arp	23:56:28 11/10/2015	80997733	7912	855
5724	arp	23:57:28 11/10/2015	80999511	9133	1778
5725	arp	23:58:28 11/10/2015	81001172	9835	1661
5726	arp	23:59:28 11/10/2015	81002853	9835	1681
5727	arp	00:00:29 11/11/2015	81003685	9835	832

从中可以看出在23点57分故障发生的1分钟时间里有约1200个的ARP丢包，这可能会引起AC上ARP表项的丢失。

三、 实验室模拟复现分析

在研发实验室对该局点无线网络搭建了一比一的模拟复现环境。通过在此环境上上模拟仿真，发现当AC上的网关ARP（即S95E的ARP）删除掉后，模拟大量无线客户端持续向外网发送流量会导致AC上数据核向控制核上报消息的队列持续拥塞并丢包，同时引起AC长时间学习不到网关的ARP，最终AP掉线。

复现过程如下：

1、AC上初始条件下正确学习到网关的ARP（10.64.200.42），并模拟大量无线客户端持续打流:

```
[AC1]dis arp all
               Type: S-Static    D-Dynamic    A-Authorized
IP Address       MAC Address    VLAN ID Interface              Aging Type
10.64.200.42     5866-ba81-cfe2  800     BAGG1                  13    D
1.1.0.1          0021-6330-0933  10      WLAN-DBSS100:0         20    D
```

2、删除AC上的网关的ARP:

```
[AC1]undo arp 10.64.200.42
[AC1]dis arp all
               Type: S-Static    D-Dynamic    A-Authorized
IP Address       MAC Address    VLAN ID Interface              Aging Type
1.1.0.1          0021-6330-0933  10      WLAN-DBSS100:0         19    D
```

3、此时查看上送控制CPU的报文队列，可以看到default会有大量的溢出，同时ARP也持续有丢包，网关ARP始终学习不到；

```
[AC1-hidecmd]fpl showcpufc
Proto          Rx                   Drop                 RxSpeed(pps)
-------------------------------------------------------------------------
1 default      877420               6380664              10192
2 udp          0                    0                    0
3 tcp          0                    0                    0
4 dot1x        0                    0                    0
5 dhcp         78                   0                    0
6 igmp         0                    0                    0
7 ntp          0                    0                    0
8 arp          679                  21                   0
9 snmp         0                    0                    0
10 telnet      0                    0                    0
11 icmp        0                    0                    0
12 lwapp_ctrl  1002                 0                    0
13 iactp       0                    0                    0
14 acsei       0                    0                    0
15 iec         0                    0                    0
16 stp         0                    0                    0
17 lwapp_data  488                  0                    0
18 ipc         0                    0                    0
19 http        0                    0                    0
20 ip          0                    0                    0
21 ipv6        0                    0                    0
22 ethernet    0                    0                    0
```

```
[AC1-hidecmd]fpl showcpufc
Proto          Rx                   Drop                 RxSpeed(pps)
-------------------------------------------------------------------------
1 default      1688420              13537060             10180
2 udp          0                    0                    0
3 tcp          0                    0                    0
4 dot1x        0                    0                    0
5 dhcp         78                   0                    0
6 igmp         0                    0                    0
7 ntp          0                    0                    0
```

```
[AC1-hidecmd]fpl showcpufc
Proto          Rx                   Drop                 RxSpeed(pps)
-------------------------------------------------------------------------
1 default      2710858              22558107             10180
2 udp          0                    0                    0
3 tcp          0                    0                    0
4 dot1x        0                    0                    0
5 dhcp         78                   0                    0
6 igmp         0                    0                    0
7 ntp          0                    0                    0
8 arp          697                  122                  0
9 snmp         0                    0                    0
10 telnet      0                    0                    0
11 icmp        0                    0                    0
12 lwapp_ctrl  1023                 0                    0
13 iactp       0                    0                    0
14 acsei       0                    0                    0
15 iec         0                    0                    0
16 stp         0                    0                    0
17 lwapp_data  548                  0                    0
18 ipc         0                    0                    0
19 http        0                    0                    0
20 ip          0                    0                    0
```

```
 8 arp         686                 66                  0
 9 snmp        0                   0                   0
10 telnet      0                   0                   0
11 icmp        0                   0                   0
12 lwapp_ctrl  1003                0                   0
13 iactp       0                   0                   0
14 acsei       0                   0                   0
15 iec         0                   0                   0
16 stp         0                   0                   0
17 lwapp_data  514                 0                   0
18 ipc         0                   0                   0
19 http        0                   0                   0
20 ip          0                   0                   0
21 ipv6        0                   0                   0
22 ethernet    0                   0                   0
23 radius      0                   0                   0
24 vrrp        0                   0                   0
```

```
[AC1-hidecmd]dis arp all
               Type: S-Static    D-Dynamic    A-Authorized
IP Address       MAC Address    VLAN ID Interface              Aging Type
1.1.0.1          0021-6330-0933  10       WLAN-DBSS100:0        18    D
```

4、只到AP掉线以后，网关的ARP可以再次学习到，之后AP重新关联上线。

```
[AC1-hidecmd]
#Dec  1 16:43:13:263 2015 AC1 LWPS/4/Tunnel Down:  Tunnel Down:1.3.6.1.4.1.2011.
10.2.75.1.3.0.2<h3cDot11ACMtTunnelDownTrap> Serial Id:210235A35U0087000023 DownI
nfo:1 AP Name:aaa IPv4:3.3.0.2 IPv6:-NA- Count:1 AP SysName:-NA- FirstTrapTime:2
#Dec  1 16:43:13:294 2015 AC1 IFNET/4/INTERFACE UPDOWN:
 Trap 1.3.6.1.6.3.1.1.5.3<linkDown>: Interface 12451847 is Down, ifAdminStatus i
%Dec  1 16:43:13:314 2015 AC1 LWPS/6/LWPS_AP_DOWN:
```

```
 Connection with AP aaa goes down by reason of Neighbor Dead Timer Expire.
%Dec  1 16:43:13:335 2015 AC1 WMAC/6/WMAC_CLIENT_GOES_OFFLINE:  Client 0021-
-0933 disconnected from WLAN 105343_ali. Reason code is 1.
%Dec  1 16:43:13:355 2015 AC1 IFNET/3/LINK_UPDOWN: WLAN-DBSS100:0 link statu
%Dec  1 16:43:13:365 2015 AC1 IFNET/3/LINK_UPDOWN: WLAN-ESS100 link status i
[AC1-hidecmd]dis arp all
               Type: S-Static    D-Dynamic    A-Authorized
IP Address       MAC Address    VLAN ID  Interface             Aging Type
10.64.200.42     5866-ba81-cfe2  800      BAGG1                 20    D
```

通过分析，产生上述现象的原因如下：

1、当AC上由于ARP老化等原因删除ARP时会同步删除与该ARP相关的所有快转表项。由于实验中删除的是网关的ARP，因此AC上的全部快转表项均会被删除。

注：快转表项是数据核上用来实现同VLAN内二个终端间的二层报文快速转发的cache表项。

2、当有要发往无线客户端的下行流量时，由于1中已经删除了所有快转表，因此报文会在数据核上走普通转发流程，并重新创建快转表。快转表的创建是数据核通过核间消息上报给控制核的，消息上报走的是default队列。控制核在收到消息并创建快转表的过程会由于查寻不到下一跳网关的ARP而失败。数据核上的下行数据报文也会因为没有ARP表项而发送失败被丢弃。由于下行持续有流量，就会有持续的学习快转表项的核间消息，从而造成default队列的持续拥塞。

3、AC定期会向AP发送LWAPP控制报文，该报文的发送过程由于查不到网关ARP表项触发ARP学习。网关回应的ARP报文首先由AC的数据核接收并通过核间消息队列上报给控制核。由于ARP报文上报所采用的硬件队列与default队列是同一个，并且ARP报文的数量远小于2中default队列的报文数量，因此ARP报文很容易被丢弃掉，导致网关ARP一直学习不到。

4、当AP由于长时间收不到心跳回应而大量掉线后，发往无线客户端的LWAPP下行流量会明显减少，通过defualt队列通知控制核建立快转表项的消息相应地减少，ARP报文的丢失概率也会降低。当有一个网关ARP回应通过核间通道被送到控制核后，AC上重新学习到网关的ARP，同时下发数据核转发表项，并删除控制核上的ARP黑洞。此时，AC到AP的下行通路恢复，掉线的AP重新上线。

上述实验室复现过程与该局点11月10日晚间的故障现象一致，因此可以确定导致10日晚间1号楼AC故障的原因就是AC上的网关ARP丢失。至于网关ARP丢失的原因，根据已有的现象推测是网关ARP表项在老化前（默认为该ARP表项学到后的第19分钟）向S95E网关发送单播ARP请求进行老化刷新时，S95E回应的ARP报文在AC上由于受到冲击而被丢掉（AC上23:57的ARP统计显示这一分钟内有大约1200个ARP丢包），导致刷新失败、ARP表项被老化。从现场11月11日00:03:29收集的诊断信息里显示，AC上S95E网关ARP表项的老化时间是14分钟（如下），说明该ARP表项是在11月10日23:57左右学习到或刷新的，时间上与前面的推断吻合。

```
IP Address       MAC Address     VLAN ID  Interface    Aging Type
10.64.200.42     7425-8a77-e300  800      BAGG1        14    D
```

四、对AC CPU高的分析

有关故障期间AC CPU出现100%的情况，通过分析现场11月11日03:29收集到的AC CPU历史记录可知，第一次100%高峰发生在59:29秒左右，此时正是前期掉线的AP重新上线的过程，同时伴有大量的无线客户端重新认证上线，CPU高是正常的。

```
    ===== CPU usage info (no:  0  idx: 18) =====
    CPU Usage Stat. Cycle: 60 (Second)
    CPU Usage              : 100%
    CPU Usage Stat. Time : 2015-11-10  23:59:54
    CPU Usage Stat. Tick : 0x13a52(CPU Tick High) 0x1ea9d94f(CPU Tick Low)
    Actual Stat. Cycle   : 0x0(CPU Tick High) 0xee6b9ec7(CPU Tick Low)
    TaskName         CPU         Runtime(CPU Tick High/CPU Tick Low)

INFO               16%                 0/26362da8
```

DT1X	4%	0/ 994f62f
RDS	10%	0/1957376f
PSEC	14%	0/229d5017
WMAC	27%	0/422d1c3b

问题结论

（1） 根据研发实验室模拟仿真结果及分析，确定本次1号楼AC故障是由AC上的网关ARP表项老化导致。

（2） 现网AC版本软件处理不合理，导致网关ARP老化后长时间学习不到，最终AP大面积掉线。

（3） 故障期间出现AC CPU达到100%的情况，是由于AP及无线客户端重新上线导致，属正常现象。

（1） 为了避免AC上再次出现由于网关ARP老化导致AP大量掉线的问题，建议在所有的AC板卡上通过静态ARP的方式将网关ARP绑定。另外，建议同时在S75E将所有AC板卡的ARP表配置为静态，避免由于AC上的ARP冲击导致S75E无法学习到AC的ARP的问题。

（2） 升级B109最新版本R2509P46，此版本中包含以下几部分修改：

·调整ARP报文上送控制核的优先级，调整后优先级高于default队列的优先级；

·针对上送CPU的协议报文，尤其是default队列中的报文，增加协议报文类型的细分识别；

·增加按协议类型对上送CPU的报文进行限速的功能；

·新增在CPU高时收集记录各种统计信息的功能，有助于后续的维护及问题定位，也可以为未来做进一步优化提供依据。