



SUNDRAY  
信锐技术

# 无线业务不定时中断排查（控制器双机）

2021 年 8 月

信锐江西办黄立华

信锐技术

版权所有 侵权必究

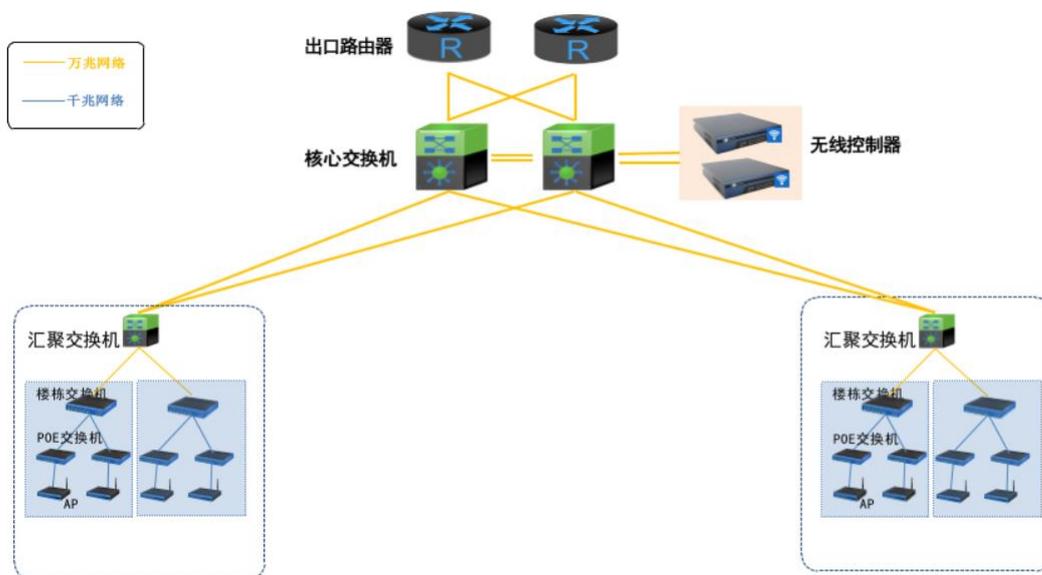
## 目录

无线业务不定时中断排查（控制器双机） .....	1
1、项目背景与需求 .....	3
2、拓扑图 .....	3
3、问题现象 .....	3
4、故障排查排错 .....	3
4.1、第一步 .....	4
4.2、第二步 .....	4
4.3、第三步 .....	4
4.4、第四步 .....	5
5、解决方法 .....	6
6、下一步计划 .....	7
7、结尾 .....	7

## 1、项目背景与需求

客户现场对网络要求高，放了两个控制器做双机，客户要求网络故障不能超过 30 分钟。

## 2、拓扑图



## 3、问题现象

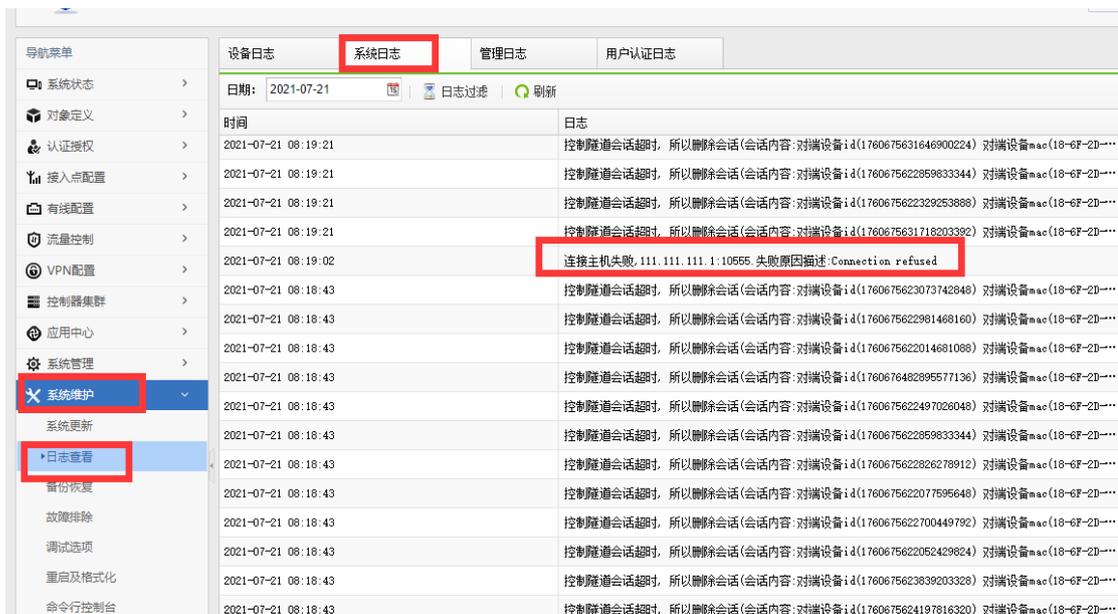
观察发现：

- 组双机，8:00-17:00 时间段一部分人连不上无线，持续 10 分钟左右；
- 不组双机，8:00-17:00 时间断偶尔发生中断全部连不上无线，持续 10 分钟左右。

## 4、故障排查排错

## 4.1、第一步

早上 8:19 开始控制器报心跳 VRRP 组频繁切换且发生心跳口连接失败，并开始出现部分无线终端连 wifi 获取不到地址，初步检查配置，发现很多 AP 的发现控制器 IP 不是虚拟 IP，定位可能双机断开时，一部分终端在备机上拿不到地址。



设备日志	系统日志	管理日志	用户认证日志
日期: 2021-07-21 日志过滤 刷新			
时间	日志		
2021-07-21 08:19:21	控制隧道会话超时, 所以删除会话(会话内容:对端设备id(1760675631646900224) 对端设备mac(18-6F-2D-...		
2021-07-21 08:19:21	控制隧道会话超时, 所以删除会话(会话内容:对端设备id(1760675622859833344) 对端设备mac(18-6F-2D-...		
2021-07-21 08:19:21	控制隧道会话超时, 所以删除会话(会话内容:对端设备id(1760675622329253888) 对端设备mac(18-6F-2D-...		
2021-07-21 08:19:21	控制隧道会话超时, 所以删除会话(会话内容:对端设备id(1760675631718203392) 对端设备mac(18-6F-2D-...		
2021-07-21 08:19:02	连接主机失败. 111.111.111.1:10555. 失败原因描述: Connection refused		
2021-07-21 08:18:43	控制隧道会话超时, 所以删除会话(会话内容:对端设备id(1760675623073742848) 对端设备mac(18-6F-2D-...		
2021-07-21 08:18:43	控制隧道会话超时, 所以删除会话(会话内容:对端设备id(176067562201468108) 对端设备mac(18-6F-2D-...		
2021-07-21 08:18:43	控制隧道会话超时, 所以删除会话(会话内容:对端设备id(176067562201468108) 对端设备mac(18-6F-2D-...		
2021-07-21 08:18:43	控制隧道会话超时, 所以删除会话(会话内容:对端设备id(1760676462895577136) 对端设备mac(18-6F-2D-...		
2021-07-21 08:18:43	控制隧道会话超时, 所以删除会话(会话内容:对端设备id(1760675622497028048) 对端设备mac(18-6F-2D-...		
2021-07-21 08:18:43	控制隧道会话超时, 所以删除会话(会话内容:对端设备id(1760675622859833344) 对端设备mac(18-6F-2D-...		
2021-07-21 08:18:43	控制隧道会话超时, 所以删除会话(会话内容:对端设备id(1760675622826278912) 对端设备mac(18-6F-2D-...		
2021-07-21 08:18:43	控制隧道会话超时, 所以删除会话(会话内容:对端设备id(1760675622077596648) 对端设备mac(18-6F-2D-...		
2021-07-21 08:18:43	控制隧道会话超时, 所以删除会话(会话内容:对端设备id(1760675622700449792) 对端设备mac(18-6F-2D-...		
2021-07-21 08:18:43	控制隧道会话超时, 所以删除会话(会话内容:对端设备id(1760675622052429824) 对端设备mac(18-6F-2D-...		
2021-07-21 08:18:43	控制隧道会话超时, 所以删除会话(会话内容:对端设备id(1760675623839203328) 对端设备mac(18-6F-2D-...		
2021-07-21 08:18:43	控制隧道会话超时, 所以删除会话(会话内容:对端设备id(1760675624197816320) 对端设备mac(18-6F-2D-...		

12 点将 AP 发现控制器全部改写为虚拟 IP，一直到下午 4:30，网络都均未出现问题。

## 4.2、第二步

客户 4:30 又发生一部分上不了网的情况，客户打电话说自己把备机的上联口和心跳口拔了，无线就好了，此时定位为备机存在问题，下午 5 点到第二天早上 9 点都没有出现问题。

## 4.3、第三步

客户 9 点 10 分打电话说所有人都上不了网了，核心直连 ping 控制器，发现不通，推断控制器和核心交换机及链路可能存在问题，通过镜像抓包分析日志，看流量是否正常，9:00-16:40 出现问题就获取抓包，发现控制器和核心交换机之间只有请求包，且发现流量属于正常范围，16:40-23:00 未出现问题，客户现场一直反馈有线正常，说要在安排新控制器做好替换准备，（链路和光模块全部更换；出现问题电脑直连 10.252.252.252 不通），此时推断可能控制器问题或流量问题。

#### 4.4、第四步

客户上午 8 点 20 反馈还是会有这种现象，此时核心直连 ping 和电脑直连 ping 都不通，转换思路，排查是控制进程卡死，后台查看会话数，发现被占满了。

The screenshot shows a terminal window with the following content:

```

1468 alg_protocol_table 0 0 0 128 1 0 0 0 1 31
1469 -----
1470 proxy_arp_hash_table 0 0 0 16 0 0 0 0 0 32
1471 -----
1472 proxy_ns_hash_table 0 0 0 16 0 0 0 0 0 0
1473 -----
1474 localhost#
1475 [ 20210722-115401 ]
1476 localhost# show table-statistics
1477
1478 | | | name | totality | use | free | bucket-num | node-num | slab-num | slab-use | slab-free | dynamic-num | dynamic-free
1479 -----
1480 session-table 309000 309000 0 65536 77662 0 0 0 77662 0
1481 -----
1482 ddos_white_list_table 512 0 512 64 0 0 0 0 0 0 0
1483 -----
1484 ddos_defender_table 131072 0 131072 16384 0 0 0 0 0 0 0
1485 -----
1486 qos_user_table 65536 0 65536 8192 0 0 0 0 0 0 0
1487 -----
1488 frag4_table 8192 0 8192 1024 0 0 0 0 0 0 190
1489 -----
1490 expect_hash_table 2048 0 2048 256 0 0 0 0 0 0 0
1491 -----
1492 arp_hash_table 32768 371 32397 4096 0 0 0 0 0 0 0
1493 -----
1494 nd6_neighbor_table 512 0 512 64 0 0 0 0 0 0 0
1495 -----
Find result - 107 hits
Line 945: session-table 309000 309000 0 65536 66834 0 0 0 66834 0
Line 1012: session-table 309000 294629 14371 65536 69875 0 0 0 69875 0
Line 1079: session-table 309000 309000 0 65536 76175 0 0 0 76175 0
Line 1146: session-table 309000 309000 0 65536 76563 0 0 0 76563 0
Line 1146: session-table 309000 309000 0 65536 76563 0 0 0 76563 0
Line 1213: session-table 309000 309000 0 65536 76837 0 0 0 76837 0
Line 1213: session-table 309000 309000 0 65536 76837 0 0 0 76837 0
Line 1280: session-table 309000 309000 0 65536 76981 0 0 0 76981 0
Line 1280: session-table 309000 309000 0 65536 76981 0 0 0 76981 0
Line 1347: session-table 309000 309000 0 65536 77242 0 0 0 77242 0
Line 1347: session-table 309000 309000 0 65536 77242 0 0 0 77242 0
Line 1414: session-table 309000 309000 0 65536 77438 0 0 0 77438 0
Line 1414: session-table 309000 309000 0 65536 77438 0 0 0 77438 0
Line 1481: session-table 309000 309000 0 65536 77662 0 0 0 77662 0
Line 1481: session-table 309000 309000 0 65536 77662 0 0 0 77662 0
Line 1548: session-table 309000 308998 2 65536 77879 0 0 0 77879 0
Line 1615: session-table 309000 308985 15 65536 78082 0 0 0 78082 0
Line 1682: session-table 309000 199799 109201 65536 65245 0 0 0 65245 0
Line 1749: session-table 309000 21066 287934 65536 16016 0 0 0 16016 0
Line 1816: session-table 309000 18512 290488 65536 13195 0 0 0 13195 0

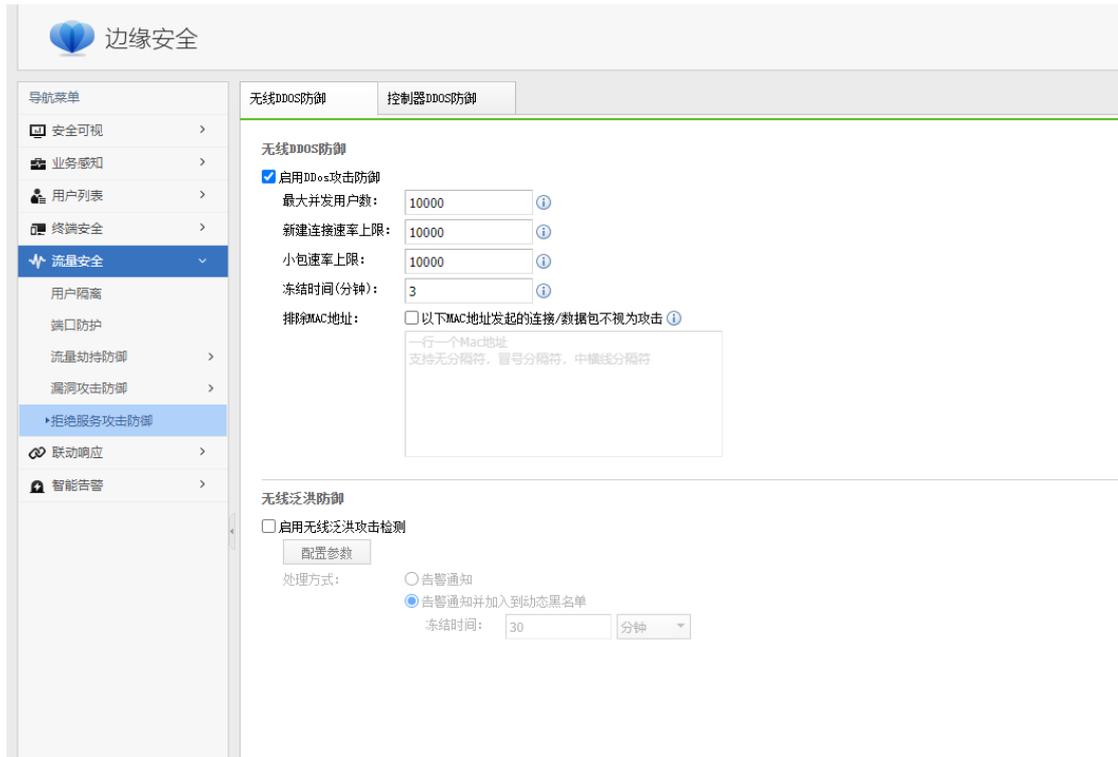
```

基本定位，异常流量导致会话数满，导致控制器不能正常工作。

## 5、解决方法

控制器开启 DDOS 防御和扫描防御。





## 6、下一步计划

- 1、在出现会话数高，后台会话数满通过 cli 进入数据面，使用 clear session 清除；
- 2、控制器后台挂进程，有异常流量自动保存，用于分析具体是哪些终端导致的异常；

```

-rw-r--r-- 1 root root 1106153 Jul 23 15:33 session.log
-rwxrwxrwx 1 root root 489 Jul 23 15:32 session.sh

```

- 3、定期进行巡检。

## 7、结尾

发生问题期间和客户一起留守观察到 11 点半，早上 8 点半到客户现场，加上定位问题是公司内部有部门会做压力测试，原因终归还是内部人员导致，把文档做好并向领导汇报，结果客户还算满意。