



S5130-52S-PWR-EI 与主机ip地址冲突

MAC地址表 [陈启敏](#) 2021-06-30 发表

组网及说明

组网：无

设备：S5130-52S-PWR-EI 组网的终端ip地址均为静态ip地址，手动配置。

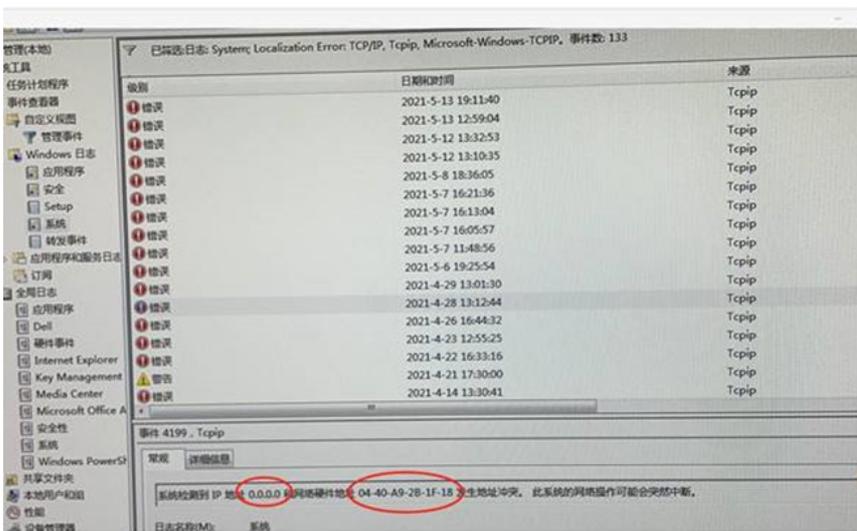
问题描述

故障现象：某局点整栋楼，每个楼层都有部分用户反馈，开机或者休眠后，电脑提示IP地址冲突等一会儿，又可以正常入网。

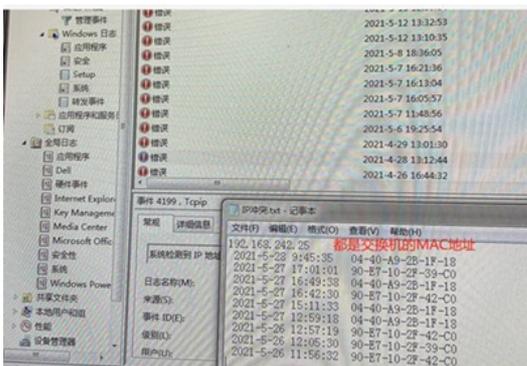
过程分析

第一：查看电脑上提示ip冲突，是什么ip发生的冲突，从下图可以看出是0.0.0.0的ip地址与某硬件设备发送了冲突

```
C:\Users\chenhang>netstat -ano
活动连接
协议 本地地址 外部地址 状态 PID
TCP 0.0.0.0:135 0.0.0.0:0 LISTENING 1268
TCP 0.0.0.0:443 0.0.0.0:0 LISTENING 10696
TCP 0.0.0.0:445 0.0.0.0:0 LISTENING 4
TCP 0.0.0.0:902 0.0.0.0:0 LISTENING 7244
TCP 0.0.0.0:912 0.0.0.0:0 LISTENING 7244
TCP 0.0.0.0:1027 0.0.0.0:0 LISTENING 632
TCP 0.0.0.0:3360 0.0.0.0:0 LISTENING 12648
TCP 0.0.0.0:3370 0.0.0.0:0 LISTENING 12648
TCP 0.0.0.0:3389 0.0.0.0:0 LISTENING 1588
TCP 0.0.0.0:5021 0.0.0.0:0 LISTENING 9120
TCP 0.0.0.0:5040 0.0.0.0:0 LISTENING 12024
TCP 0.0.0.0:5120 0.0.0.0:0 LISTENING 5444
TCP 0.0.0.0:5357 0.0.0.0:0 LISTENING 4
TCP 0.0.0.0:7680 0.0.0.0:0 LISTENING 4660
TCP 0.0.0.0:8680 0.0.0.0:0 LISTENING 17688
TCP 0.0.0.0:8889 0.0.0.0:0 LISTENING 7252
TCP 0.0.0.0:11512 0.0.0.0:0 LISTENING 5092
TCP 0.0.0.0:15000 0.0.0.0:0 LISTENING 12648
TCP 0.0.0.0:19329 0.0.0.0:0 LISTENING 5772
TCP 0.0.0.0:20377 0.0.0.0:0 LISTENING 2984
TCP 0.0.0.0:25097 0.0.0.0:0 LISTENING 3268
```



第二步：查找组网中该mac地址所对应的硬件设备，排查后，冲突地址均为S5130-52S-PWR-EI的mac地址



第三步对现象分析：通过分析出现问题的用户电脑系统日志，所有日志显示都是为：系统检测到IP地址为0.0.0.0和硬件地址冲突（硬件地址是S5130 H3C交换机的MAC地址）0.0.0.0最特殊的一个ip地址 普通windows的PC电脑，在电脑未正式入网以前或者拿不到IP时，系统的IP地址一般是会就是0.0.0.0或者169.254地址。

第四步抓包对流量进行分析：

第一次抓包

192.168.100.70/69 两台 S5130-28S/52S交换机发出的第一次ARP包，定向发至192.168.244.239 和28 (239 IP在1小时以前，就已经手动移除。28为领导的IP，持续时间10多分钟左右)

分析：S5130交换机向网络通告，我的0.0.0.0 IP地址，定向向192.168.244.28. 请求。但是244.28主机是不会回复“这种不合规”的报文。

此时239IP已经移除1个小时

初步定位:

通过分析判断原因因为，在用户电脑开机或者休眠恢复时，准备重新加入网的时候，电脑的IP为系统保留地址IP 0.0.0.0/169.254.XX，但在电脑入网之前，立即就收到H3C交换机定向发送的ARP报文（源：交换机MAC+源IP：0.0.0.0），此时电脑检测到0.0.0.0 IP地址和系统的保留地址一样，产生冲突提示。

因此需要看为什么设备会发出这样的arp报文

```

> Interface id: 0 (Device\MPF_{2CC54AA-BCF5-41A1-A770-A57874762530})
[Time shift for this packet: 0.000000000 seconds]
Epoch Time: 1622245644.005699000 seconds
[Time since reference or first frame: 0.238250000 seconds]
Frame Number: 8
  
```

终端都是配置的静态ip地址，没有dhcp的配置，走的dot1x认证

上文中的ip移除与现场确认过是ip直接手动修改掉

进一步定位:

第二次抓包

针对报告进行了配置的检查，配置比较干净，也没有查到日志中有异常机

192.168.100.69的S130交换机此再已经被替换为S120交换机，100.70交换机甚至开数个配置副本

vlan244 100.70 S5130-28S交换机发出的第一个包，后面持续定向发至192.168.236.238 (youlan@y00)

arp snooping enable

192.168.236.238向192.168.236.254发送arp包是正常的，当254不通。会一直发。

```

arp source-suppression enable
arp source-suppression limit 20
#
1100 179.445339 Dell_72:01:af Broadcast ARP
1101 179.445368 Dell_72:01:af Broadcast ARP
1122 180.339086 Dell_72:01:af Broadcast ARP
1123 180.339094 Dell_72:01:af Broadcast ARP
1142 181.339115 Dell_72:01:af Broadcast ARP
1145 182.155982 Dell_72:01:af Broadcast ARP
1149 182.44221 Dell_72:01:af Broadcast ARP
1152 183.339166 Dell_72:01:af Broadcast ARP
1161 183.339166 Dell_72:01:af Broadcast ARP
1168 184.157792 Dell_72:01:af Broadcast ARP
  
```

确认vlan244是用户vlan

也和代理商确认过s5120没有开启arp snooping

怀疑是arp snooping开启的缘故，但是查看配置指导并未指出arp snooping会主动发出arp报文，因此找产品线进行确认

最终定位:

现场5130上vlan224配置了arp snooping:

ARP Snooping表项的老化时间为25分钟，有效时间为15分钟。

如果一个ARP Snooping表项自最后一次更新后12分钟内没有收到ARP更新报文，设备会向外主动发送一个ARP请求进行探测；

但现场5130做二层交换机，vlan224并没有配置地址，因此发送这个arp探测时，使用的源地址只能填充0.0.0.0，实验室用三台交换机复现出来了类似的现象：

Sw1 (100.100.100.101) --sw2 (只二层透传，配置arp snooping) --sw3 (10.0.100.100.102)

在正常情况下在sw2上查看arp snooping表项为：

```

[2074-S7500E]dis arp snooping vlan 100
IP address    MAC address  VLAN ID  Interface    Aging Status
100.100.100.102 84d9-3123-a801 100     GE1/4/0/4    15 Valid
100.100.100.101 84d9-3123-b801 100     GE1/4/0/1    15 Valid
  
```

当老化时间到了12分钟，在SW1和SW2上可以收到如下arp报文：

```

<2072-s10504>*May 30 21:01:59:597 2021 2032-s10504 ARP/7/ARP_RCV: -
  
```

MDC=1-Chassis=1-Slot=4; Received an ARP message, operation: 1, sender MAC: 3c8c-40c6-7e00, sender IP: 0.0.0.0, target MAC: 84d9-3123-b801, target I