

# 知 S7506E跨网段转发丢包经验案例

孙兆强 2017-12-20 发表

服务器和pc直连S7506E，网关都在交换机上，arp都能学习到。PC ping网关不丢包，ping服务器丢包。如果把电脑地址配置成和服务器同网段的地址ping就不丢包。交换机流统报文确实丢在设备上。排查设备可能存在的问题：接口都是电口且无错包丢包，接口不存在拥塞，没有mac漂移记录，接口广播包不大，内存和cpu正常，查看版本也无相关软件问题。

检查S7506E未发现异常，底层的arp学习也都是正常的：

PC:

34.36.129.129 f0de-f1b9-9722 14 GE1/2/0/24 5 D

Server:

34.36.128.31 70e2-840a-93dc 10 GE1/2/0/5 N/A S

34.36.129.129 ping 34.36.128.31开始时有问题，过一段时间又通了，流统也是在S7506E上丢弃的。

接口抓包看，最开始ping时，服务器34.36.128.31 请求网关地址34.36.128.254的arp，S7506E回应了，接着服务器34.36.128.10也回应了，导致服务器34.36.128.31学习到错误的的arp信息。导致服务器封装报文的目的mac地址不对，交换机接收到该报文后，查询目的mac不是本机mac，直接将报文丢弃。后面，S7506E交换机发送免费arp广播请求34.36.128.249的地址，服务器34.36.128.31收到后arp更新，后面的ping过程就正常了。

```
10 2017-12-19 12:48:31.881864000 34.36.129.129 34.36.128.31 ICMP 74 Echo (ping) request id=0x0001, seq=2695/34570, ttl=64
11 2017-12-19 12:48:31.881877000 34.36.129.129 34.36.128.31 ICMP 74 Echo (ping) request id=0x0001, seq=2695/34570, ttl=63 (reply in 14)
12 2017-12-19 12:48:31.882839000 70:e2:84:0a:93:dc Broadcast ARP 60 who has 34.36.128.254? Tell 34.36.128.31
13 2017-12-19 12:48:31.882839000 70:e2:84:0a:2a:9d 70:e2:84:0a:93:dc ARP 60 34.36.128.254 is at 70:e2:84:0a:2a:9d
14 2017-12-19 12:48:31.883039000 34.36.128.31 34.36.129.129 ICMP 74 Echo (ping) reply id=0x0001, seq=2697/34570, ttl=64 (request in 1)
...
Frame 14: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface 0
Ethernet II, Src: 70:e2:84:0a:93:dc (70:e2:84:0a:93:dc), Dst: 70:e2:84:0a:2a:9d (70:e2:84:0a:2a:9d)
Destination: 70:e2:84:0a:2a:9d (70:e2:84:0a:2a:9d)
Source: 70:e2:84:0a:93:dc (70:e2:84:0a:93:dc)
Type: IP (0x0800)
Internet Protocol Version 4, Src: 34.36.128.31 (34.36.128.31), Dst: 34.36.129.129 (34.36.129.129)
Internet Control Message Protocol
```

70:e2:84:0a:2a:9d是另一台服务器的，地址是34.36.128.10:

34.36.128.10 70e2-840a-2a9d 10 GE1/2/0/23 20 D

后面S7506E发arp广播请求128.249时，服务器收到后arp更新正确，恢复正常：

```
100 2017-12-19 12:49:26.437183000 60:0b:03:e9:24:01 Broadcast ARP 60 who has 34.36.128.249? Tell 34.36.128.254 (duplicate use of 34.36.128.254)
101 2017-12-19 12:49:26.705096000 wistron_b9:97:22 60:0b:03:e9:24:01 ARP 60 who has 34.36.129.254? Tell 34.36.129.129
102 2017-12-19 12:49:26.714440000 34.36.129.129 34.36.128.31 ICMP 74 Echo (ping) request id=0x0001, seq=2706/37386, ttl=64
103 2017-12-19 12:49:26.714440000 34.36.129.129 34.36.128.31 ICMP 74 Echo (ping) request id=0x0001, seq=2706/37386, ttl=63 (reply in 104)
104 2017-12-19 12:49:26.715120000 34.36.128.31 34.36.129.129 ICMP 74 Echo (ping) reply id=0x0001, seq=2706/37386, ttl=64 (request in 103)
105 2017-12-19 12:49:26.715120000 34.36.129.129 34.36.129.129 ICMP 74 Echo (ping) reply id=0x0001, seq=2706/37386, ttl=63
106 2017-12-19 12:49:26.778597000 70:e2:84:05:e3:13 Broadcast ARP 60 who has 34.36.128.254? Tell 34.36.128.222
...
Frame 104: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface 0
Ethernet II, Src: 70:e2:84:0a:93:dc (70:e2:84:0a:93:dc), Dst: 60:0b:03:e9:24:01 (60:0b:03:e9:24:01)
Destination: 60:0b:03:e9:24:01 (60:0b:03:e9:24:01)
Source: 70:e2:84:0a:93:dc (70:e2:84:0a:93:dc)
Type: IP (0x0800)
Internet Protocol Version 4, Src: 34.36.128.31 (34.36.128.31), Dst: 34.36.129.129 (34.36.129.129)
Internet Control Message Protocol
```

在连到70:e2:84:0a:2a:9d的GE1/2/0/23口镜像抓包，也能抓到上面错误的arp报文，确认是服务器发出的

- 1. 排查34.36.128.10这个服务器，解决错误回应arp的问题。
- 2. 在服务器上静态绑定网关的arp