科来

第 27 章
如何分析无盘客户端无法正常启动

科来官微
CSNA 公众号
400-6869-069
www.colasoft.com.cn
support@colasoft.com.cn

随着网络架构的不断升级，数据流通经过的中间设备也日益增加。面对客户端出现的异常情况，常规分析手法难以确定故障原因。本案例将介绍如何使用网络流量分析技术精准定位客户端异常启动的根因。

27.1 问题描述

据某学校的教学老师反馈，X.X.84.*网段无盘客户端频繁出现无法正常启动的情况，而无法启动的客户端需改为同网段其他地址就能够正常启动。该校网络运维人员通过网络、无盘应用等多方排查仍未能定位故障原因，该故障已经存在数月，这严重影响了正常的教学进程。

根据该校网络运维人员所描述的故障现象，科来网络分析工程师决定在“主核心交换机”以及“5700 接入交换机”处配置端口镜像，将最接近客户端和最接近服务器的两段流量镜像到科来网络回溯分析系统，以采集流量并进行分析，如下图所示。

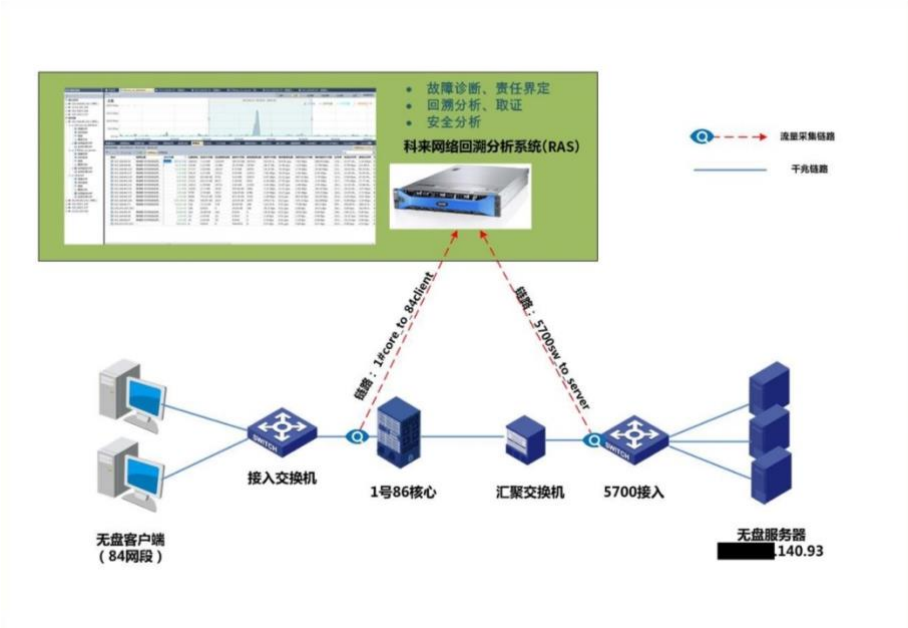


图 27-1

27.2 分析过程

首先抓取能够正常启动的无盘客户端的全部流量，分析并理解无盘启动过

程的详细原理，再模拟客户端无法启动的异常情况，通过对比分析两者的流量差异，找出无法启动的原因。

27.2.1 对正常启动的无盘客户端的数据分析

客户端 X.X.84.59（下文简写*.59）可以正常启动。

首先，通过科来网络回溯分析系统对 1#core_to_84client 链路中*.59 客户端进行数据回溯分析，发现该客户端流量峰值达到 75Mbps。再对所有 UDP 会话按开始时间升序排列后，从视图中看到客户端先和 X.X.140.93 无盘服务器单播交互了 DHCP，随后服务器立刻通过 TFTP、UDP 等方式将操作系统的文件推送至客户端。之后，*.59 客户端向广播地址（X.X.255.255）发出 DHCP 报文，同时和电信 DNS 服务器 X.X.152.99 产生 DNS 流量，此时表明客户端*.59 已经正常启动并成功登录操作系统，如下图所示。

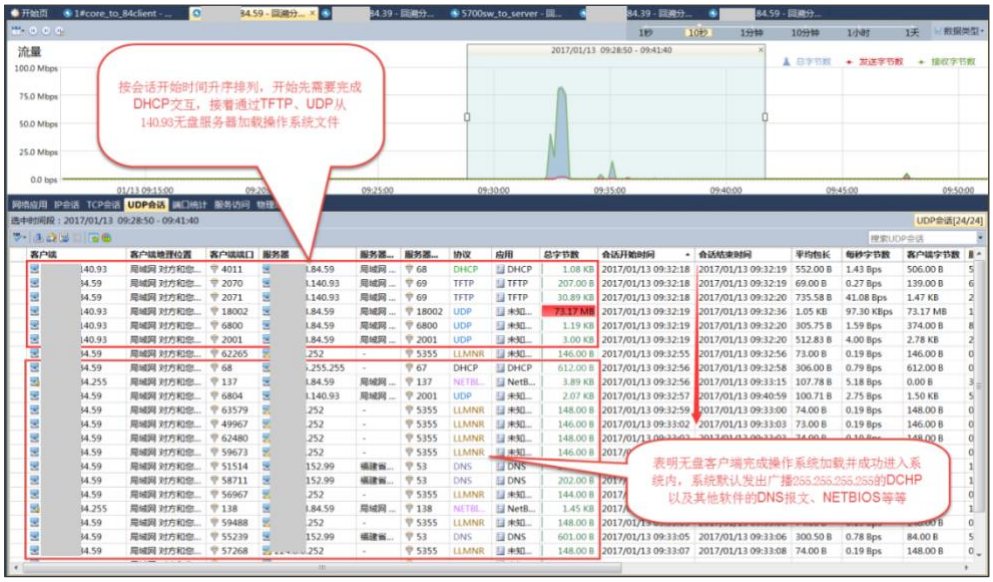


图 27-2

在后面分析中我们发现了客户端无法正常启动与第一个 DHCP 报文有关，所以本节着重分析 DHCP。*.59 客户端开机后，首先向 X.X.140.93：4011 发送 DHCP 请求，内容含“服务器名”、“引导文件名”等请求字段，1.5ms 后服务器返回消息报文——服务器 IP 地址为 X.X.149.93、引导文件名为 0600，如下图所示。

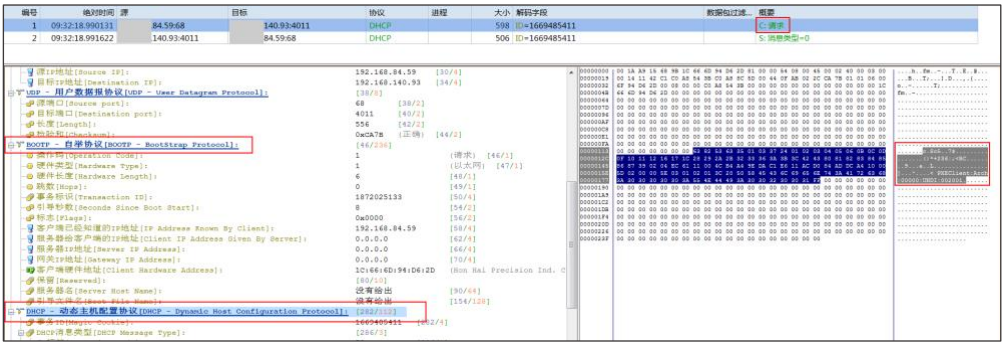


图　27-3

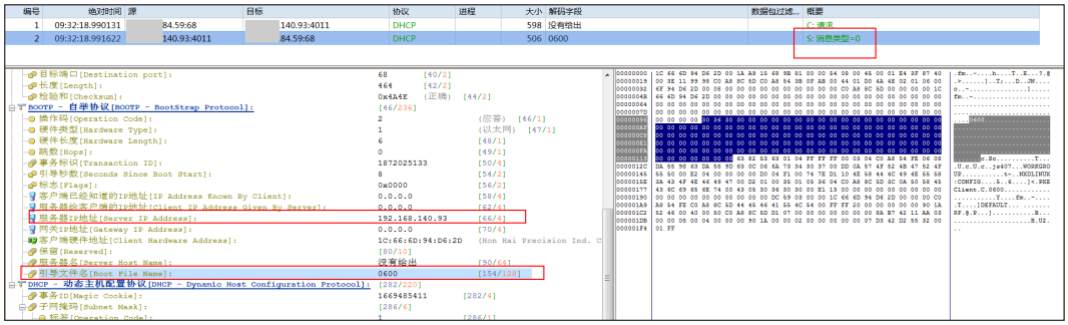


图　27-4

从上文分析中得知：*.59 客户端收到服务器返回的 DHCP 消息报文并获知引导文件名为 0600，*.59 客户端依此向服务器发送 tftp 请求下载 0600 文件。当客户端下载 0600 文件完毕后，便能根据 0600 文件配置要求，向服务器请求下载操作系统文件直至加载成功。

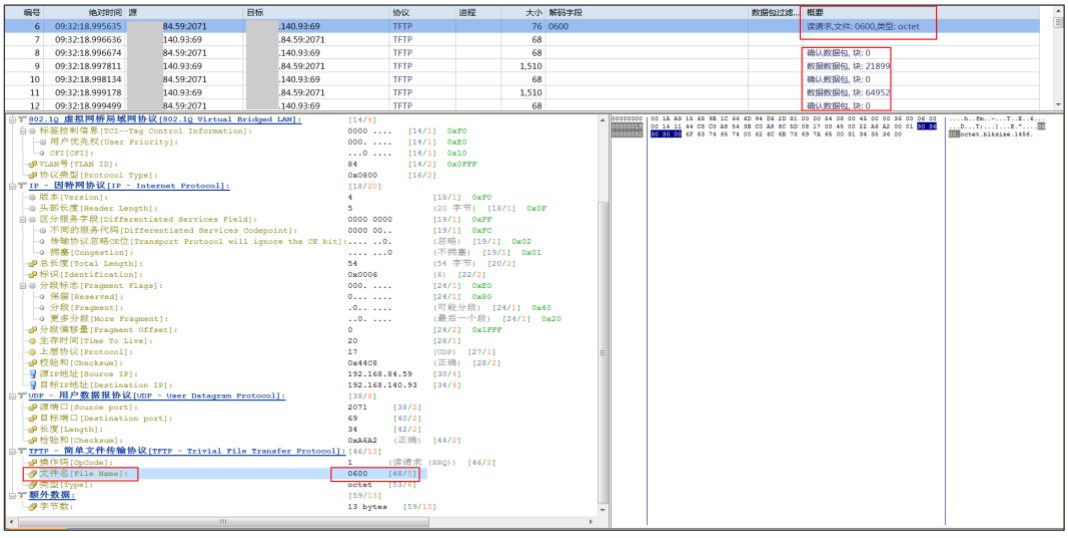


图　27-5

通过以上分析，我们对无盘启动过程原理进行总结：

客户端开机后首先需向服务器单播 DHCP 请求引导文件名

服务器收到客户端请求后将返回含引导文件名 0600 的报文

客户端获知引导文件名为 0600 后，便通过 TFTP 向服务器请求下载文件 0600

客户端成功下载引导文件 0600 后，启动程序根据该文件配置便从服务器下载操作系统文件

无盘客户端最终成功下载操作系统后，顺利进入系统

27.2.2 对无法启动的无盘客户端的数据分析

IP X.X.84.39（下文简写*.39）的无盘客户端无法正常启动。通过回溯分析，可以看到*.39 客户端流量峰值为 4Kbps，而在该时段内链路 1#core_to_84client 的流量峰值为 155Mbp，链路 5700sw_to_core 流量峰值为 155Mbp。因为客户端、服务器网口带宽都是千兆，因此不存在网络链路拥塞情况，所以无盘客户端无法启动的原因可以排除是网络拥塞造成的。

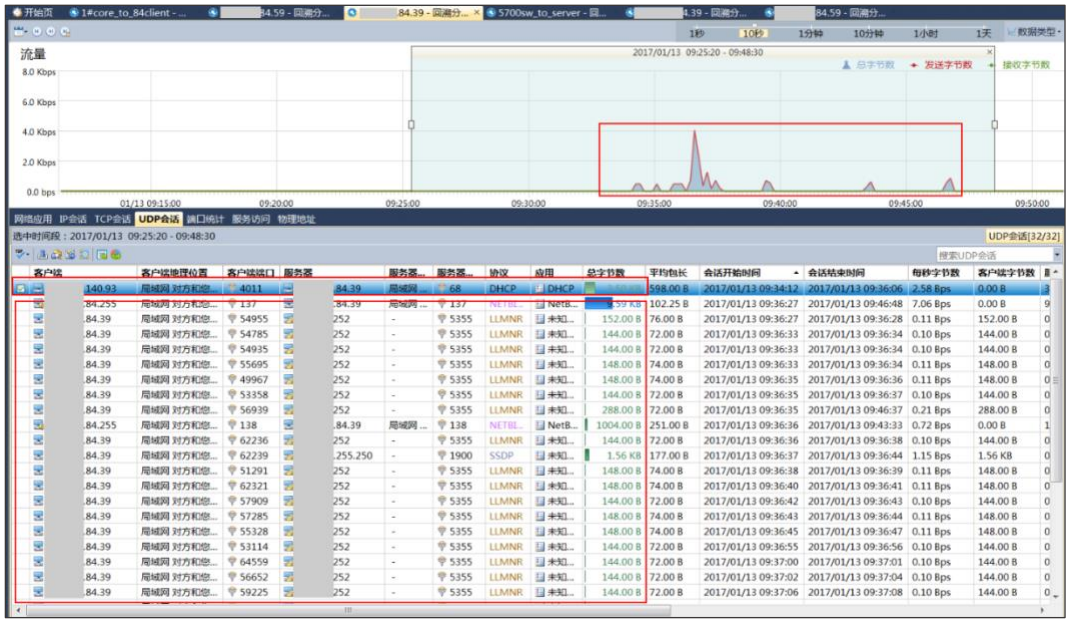


图 27-6

图　27-7

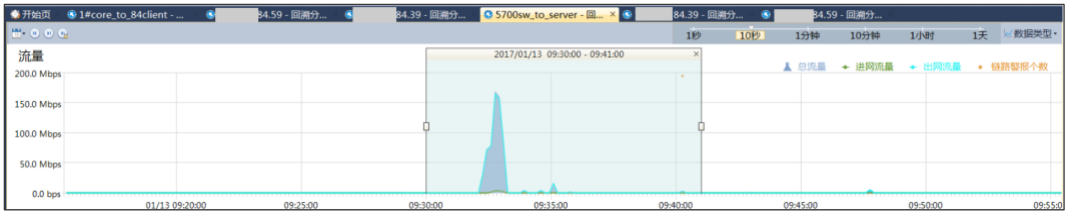


图　27-8

根据对正常启动的无盘客户端的数据分析小结，我们知道无盘启动顺序首先与 DHCP 有关，因此提取了 DHCP 流量，进行数据挖掘与精细化分析。*.39 客户端连续向 X.X.140.93 无盘服务器发送 DHCP 请求，但均未收到服务器返回的消息报文，所以*.39 客户端无法获知引导文件名，更无法向服务器下载引导文件。至此基本上断定：由于客户端未收到服务器 DHCP 返回消息，导致其无法获知引导文件名，从而造成客户端无法启动，如下图显示。

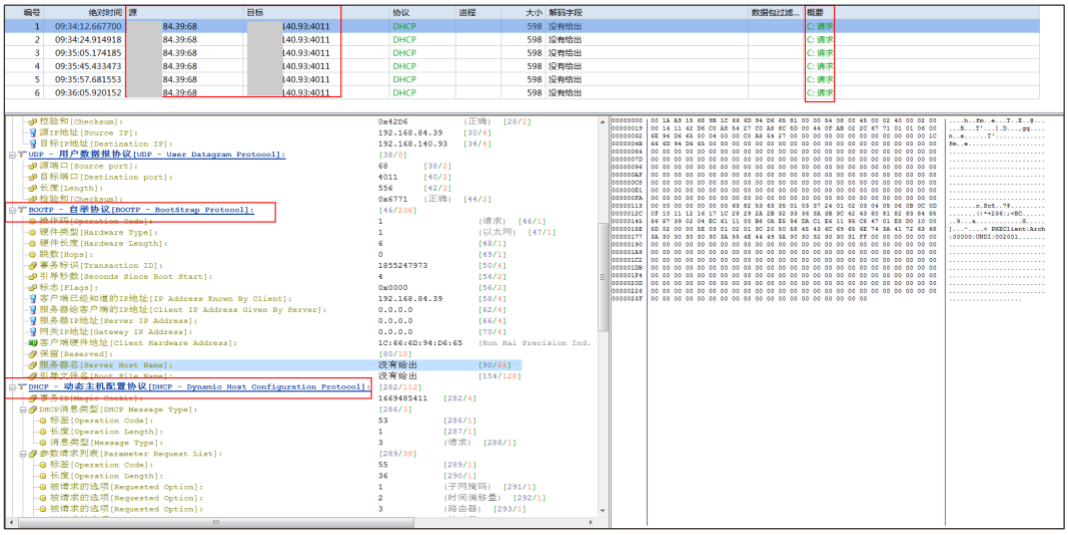


图　27-9

通过以上分析，无盘启动失败的客户端未收到服务器 DHCP 返回消息报文的可能原因有：

1、网络中的核心交换机、汇聚交换机、接入交换机转发造成的服务器回应报文丢包；

2、客户端发出 DHCP 请求内容有误，导致服务器收到消息但不回应；

3、若非前两点原因，可得出无盘服务器收到了客户端 DHCP 正确请求，由于无盘应用某种原因而不回应 DHCP 消息报文。

针对第一点，分析方法：在“靠近”服务器端的地方采集流量，观察服务器返回 DHCP 消息报文情况便可判断是否是网络问题。

在链路 5700sw_to_core 采集接入交换机的上行流量，该流量是最靠近服务器的流量数据，观察到客户端发送了 DHCP 请求后并未收到回应，这表明客户端无法启动问题不是核心交换机及汇聚交换机转发丢包造成的。

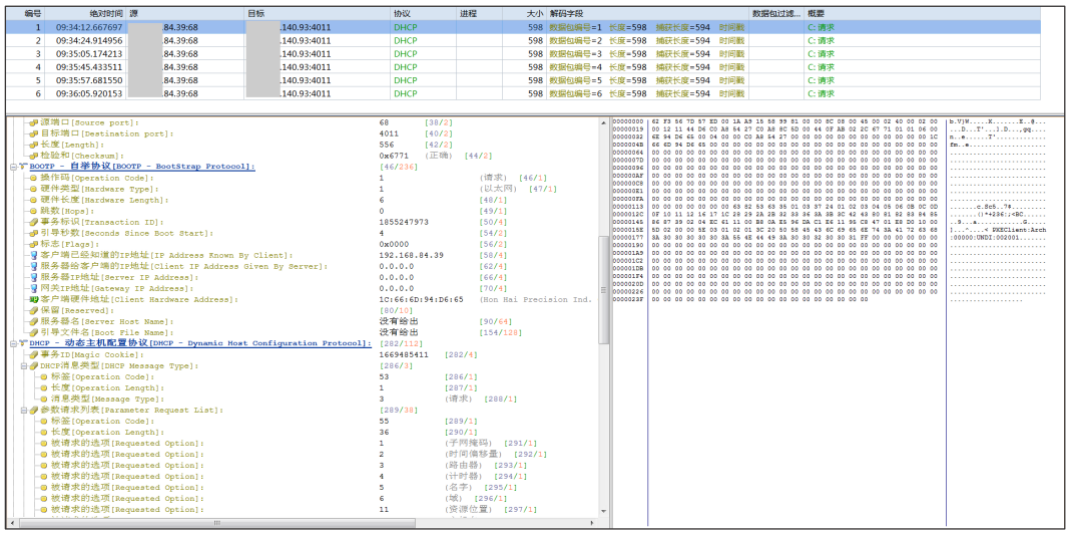


图 27-10

将镜像口手动调整到 5700 接入交换机并下联到无盘服务器接口，依然可见客户端发送了 DHCP 请求但服务器未回应，这表明导致客户端无法启动的问题并非是接入交换机转发丢包造成的，如下图所示。

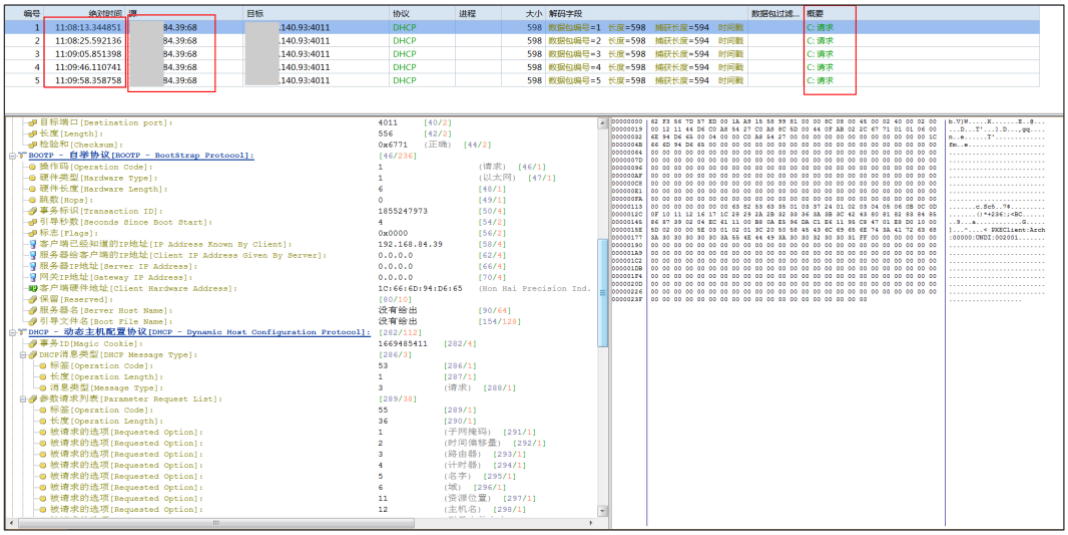


图　27-11

针对第二点，分析方法：对比正常启动与无法启动的 DHCP 请求报文字段值，便可判断客户端发出的内容是否有误。

*.39 客户端无法启动，1 分钟后将该客户端 IP 地址改为 X.X.84.3，便能顺利启动无盘。我们对 X.X.84.3 进行流量回溯分析，可以看到启动过程与 X.X.84.59 客户端一致，过程详细如下图。

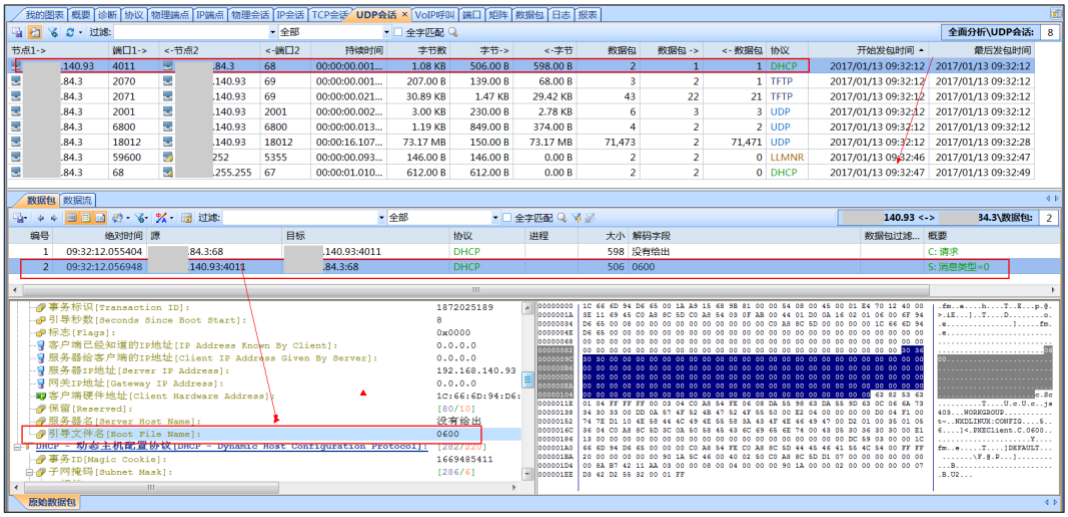
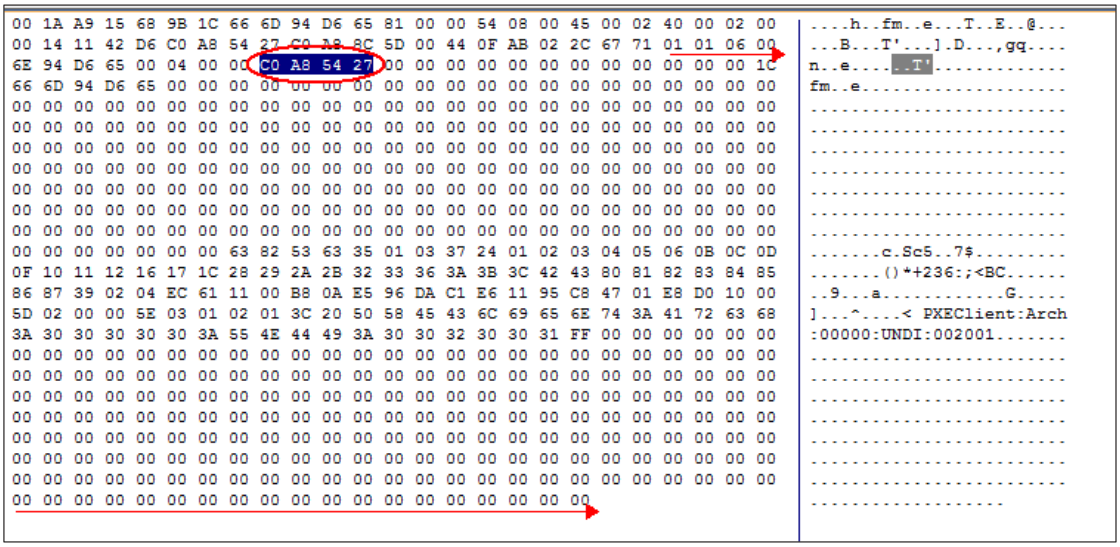


图　27-12

该客户端在 IP 为 X.X.84.39 时无法启动，在 IP 为 X.X.84.3 时正常启动，比对两个 IP 发出的 DHCP 请求内容，可以准确判断故障原因是否与客户端请求有关。通过比对信息，发现除了“客户端已经知道 IP 地址”不同外，其他字段值均



一致。所以,可以排除第二点可能的原因，如下图所示。

X.X.84.39 向 X.X.149.93 发送 DHCP 请求中载荷 HEX 字段值：

其中 C0 A8 54 27 为客户端已经知道 IP 地址 X.X.84.39。

```
00 1A A9 15 68 9B 1C 66 6D 94 D6 65 81 00 00 54 08 00 45 00 02 40 00 02 00   ....h..fm..e...T..E..@...
00 14 11 42 D6 C0 A8 54 27 C0 A8 8C 5D 00 44 0F AB 02 2C 67 71 01 01 06 00   ...B...T'...].D...,gq....
6E 94 D6 65 00 04 00 00 C0 A8 54 27 00 00 00 00 00 00 00 00 00 00 00 00 1C   n..e......T'.............
66 6D 94 D6 65 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   fm..e....................
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   .........................
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   .........................
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   .........................
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   .........................
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   .........................
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   .........................
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   .........................
00 00 00 00 00 00 00 63 82 53 63 35 01 03 37 24 01 02 03 04 05 06 0B 0C 0D   .......c.Sc5..7$.........
0F 10 11 12 16 17 1C 28 29 2A 2B 32 33 36 3A 3B 3C 42 43 80 81 82 83 84 85   .......()*+236:;<BC......
86 87 39 02 04 EC 61 11 00 B8 0A E5 96 DA C1 E6 11 95 C8 47 01 E8 D0 10 00   ..9...a............G.....
5D 02 00 00 5E 03 01 02 01 3C 20 50 58 45 43 6C 69 65 6E 74 3A 41 72 63 68   ]...^....< PXEClient:Arch
3A 30 30 30 30 30 3A 55 4E 44 49 3A 30 30 32 30 30 31 FF 00 00 00 00 00 00   :00000:UNDI:002001.......
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   .........................
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   .........................
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   .........................
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   .........................
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   .........................
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   .........................
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   .........................
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00                     ...................
```

X.X.84.3 向 X.X.149.93 发送 DHCP 请求中载荷 HEX 字段值:

其中 C0 A8 54 03 为客户端已经知道 IP 地址 X.X.84.3。

```
00 1A A9 15 68 9B 1C 66 6D 94 D6 65 81 00 00 54 08 00 45 00 02 40 00 03 00   ....h..fm..e...T..E..@...
00 14 11 42 F9 C0 A8 54 03 C0 A8 8C 5D 00 44 0F AB 02 2C 66 B5 01 01 06 00   ...B...T....].D...,f.....
6F 94 D6 65 00 08 00 00 C0 A8 54 03 00 00 00 00 00 00 00 00 00 00 00 00 1C   o..e......T..............
66 6D 94 D6 65 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   fm..e....................
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   .........................
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   .........................
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   .........................
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   .........................
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   .........................
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   .........................
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   .........................
00 00 00 00 00 00 00 63 82 53 63 35 01 03 37 24 01 02 03 04 05 06 0B 0C 0D   .......c.Sc5..7$.........
0F 10 11 12 16 17 1C 28 29 2A 2B 32 33 36 3A 3B 3C 42 43 80 81 82 83 84 85   .......()*+236:;<BC......
86 87 39 02 04 EC 61 11 00 B8 0A E5 96 DA C1 E6 11 95 C8 47 01 E8 D0 10 00   ..9...a............G.....
5D 02 00 00 5E 03 01 02 01 3C 20 50 58 45 43 6C 69 65 6E 74 3A 41 72 63 68   ]...^....< PXEClient:Arch
3A 30 30 30 30 30 3A 55 4E 44 49 3A 30 30 32 30 30 31 FF 00 00 00 00 00 00   :00000:UNDI:002001.......
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   .........................
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   .........................
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   .........................
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   .........................
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   .........................
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   .........................
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   .........................
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00                     ...................
```

总结：两者除了 IP 地址的 hex 字段不同，其它一致。表明发出的请求内容都一致。

图 27-13

综上分析，可以判定服务器因某种原因未回应正常的 DHCP 请求，从而造

成此类问题。建议在无盘服务器回查对比 X.X.84.3、X.X.84.39 两个 IP 配置差异性，便能找出某些客户端 IP 无法启动的原因。

27.3 分析结论及建议

根据上文分析，判断是服务器收到了客户端发出的 DHCP 正确请求但未回应，导致客户端无法获知“引导文件名”，造成启动失败。通过数据包级精细分析，我们可以确定无盘客户端 IP 无法正常启动原因与服务器有关。建议详查无盘服务器。

27.4 价值

繁杂网络环境中的操作系统启动异常现象，时常并非客户端的环境问题，有可能与之配套的服务器、网络等环境因素有关。运用网络原始流量分析技术，对当前问题事件进行数据包级别的深入分析，以及对网络多段数据详情对比，能帮助网络运维人员迅速精准定位事件发生原因及唯独，可视化网络运维性能，从而优化网络运营水平。

培训报名

科来网络流量分析技术资料

网络攻击与防范图谱

科来网络通讯协议图

科来网络故障诊断图

CSNA 网络分析经典实战案例

数据包样本

网络分析过滤器

术语表

科来网络流量分析产品下载(免费版)

科来网络分析系统

科来 MAC 地址扫描器

科来 Ping 工具

科来数据包播放器

科来数据包生成器

科来介绍

科来成立于 2003 年，是专注于网络流量分析技术研究与产品开发的高新技术企业，在这一领域有着几十项专利技术和完全独立的自主知识产权。科来研发的产品广泛应用于国内外用户的网络安全分析及网络智能运维等关键领域。科来连续入围 GartnerNPMD 魔力象限，并荣获“远见者”称号，是唯一入选“远见者”象限的中国企业。科来产品还曾被美国权威评测机构 PC Magazine 评选为《全球最佳科技产品》。

科来专业的技术服务在用户的业务保障上起到关键作用，已经成为对网络时效性高要求的企业的最佳选择，得到了社会各界的广泛认可。同时，科来创办的《CSNA 网络分析认证培训》是我国广具影响力的网络分析认证体系，为国家培养了大量的网络分析技术高级人才。

由于科来公司在网络安全领域的技术优势，受邀为青岛“上合峰会”、多届“两会”、“十九大”、杭州“G20 峰会”、“九三”阅兵、“世界田径锦标赛”、多届“数博会”等重大国家级活动做网络安保工作，做出突出贡献。

- 100 余家世界 500 强企业选择科来
- 为全球 10000 余家商业客户提供网络分析解决方案
- 全球 90 余万用户正在使用科来的产品
- 科来的技术服务于世界 110 个国家和地区