网络分析与管理工程师用书

拓展网络视野 精细网络管理

CSNA

CSNA网络分析认证专家实战案例

CSNA Network Analysis Certified Experts-Case Studies

科来软件 编著

西安电子科技大学出版社
http://www.xduph.com

网络分析与管理工程师用书

拓展网络视野　精细网络管理

CSNA网络分析认证专家实战案例

科来软件　编著

西安电子科技大学出版社

内 容 简 介

本书集中整理和编写了国内网络分析专家的大量实际分析案例，包括各种经典的网络故障分析、网络安全分析和网络应用性能分析等方面的实际案例。通过故障现象描述、分析方法、分析设备部署、数据获取与分析等完整的步骤来描述网络分析过程及细节，可为技术人员实际的网络故障诊断工作提供有效的借鉴，也有助于其网络安全管理水平的提升。

本书是为了满足从事网络建设、管理和维护服务的技术人员，以及从事网络安全管理的技术人员的实际需要而编写的，同时也可作为志在网络安全领域发展的各高等院校相关专业学生的自学读物以及专业培训机构的培训教材。

图书在版编目(CIP)数据

CSNA 网络分析认证专家实战案例/科来软件编著. —西安：西安电子科技大学出版社，2013.10
网络分析与管理工程师用书
ISBN 978-7-5606-3209-4

Ⅰ. ① C… Ⅱ. ① 科… Ⅲ. ① 计算机网络—网络分析 Ⅳ. ① TP393.02

中国版本图书馆 CIP 数据核字(2013)第 224902 号

策　　划　李惠萍
责任编辑　李惠萍　史鹏腾
出版发行　西安电子科技大学出版社(西安市太白南路 2 号)
电　　话　(029)88242885　88201467　　邮　　编　710071
网　　址　www.xduph.com　　电子邮箱　xdupfxb001@163.com
经　　销　新华书店
印刷单位　陕西天意印务有限责任公司
版　　次　2013 年 10 月第 1 版　　2013 年 10 月第 1 次印刷
开　　本　787 毫米×1092 毫米　1/16　印　张　16
字　　数　374 千字
印　　数　1～3000 册
定　　价　30.00 元
ISBN 978-7-5606-3209-4/TP

XDUP 3501001-1

前　言

随着关键业务越来越多地运行在网络上，网络中的关键数据也越来越多。如何保障关键业务的持续、高效和安全运行以及业务数据的安全性，已成为网络运维中非常关键的工作。实践证明，利用网络分析技术能实时地监控分析网络运行情况，及时发现网络异常和安全异常行为，快速定位分析网络和应用问题，同时还能提供强有力的网络安全分析手段，是保障网络持续、高效和安全运行的非常有效的方法。

在网络性能分析、网络故障分析和应用故障分析以及网络安全问题分析等领域，网络分析技术的应用都会大大提高分析的效率和准确度，熟练地运用网络分析技术能大大提高网络技术人员的工作效率和技术水平，在网络运维工作中运用网络分析技术，也可使网络运维的水平得到有效的提高。实际上，学习各种网络分析的实战经验，对提升网络管理技术人员和安全管理技术人员自身的网络分析能力有极大的帮助。

本书完全取材于CSNA网络分析技术专家们在实际工作中的实际网络分析案例，这些案例都是近几年在典型网络环境中产生的。全部案例按照相应的技术领域，分为网络故障分析、网络安全分析和网络应用性能分析三部分。

网络故障分析包括各种网络故障的故障现象描述、分析方法、分析设备部署、数据获取、数据分析、分析结论等完整的网络分析过程细节，对技术人员实际的网络故障诊断工作有很强的借鉴效用。

网络安全分析包括蠕虫病毒、木马、DoS攻击、ARP攻击、垃圾邮件、端口扫描等各种危害网络安全的行为的发现、分析、取证过程。掌握这些安全分析技术有助于提高网络安全管理技术人员的管理水平。

网络应用性能分析介绍了各种应用性能问题的现象、引起应用性能下降的原因定位分析方法和详细的分析过程，以及如何排查网络对应用性能的影响，对技术人员解决实际应用问题有很大的帮助。

本书中的案例来源于专业网络技术人员工作实践，都非常有代表性，每个案例都有可能在各用户单位网络中重现，所以很值得广大技术人员在实际网络分析工作中借鉴。我们对提供这些案例的技术人员表示衷心的感谢。

由于时间紧、任务重，文中难免有不足之处，欢迎大家多提宝贵意见。

科来软件公司

2013年5月21日

目　录

第一部分　网络故障分析

第二部分 网络安全分析

第三部分 网络应用性能分析

第一部分　网络故障分析

第 1 章　某地税网上申报业务系统故障分析报告

1.1　故 障 环 境

1.1.1　网络拓扑

该故障环境大体的网络拓扑如图 1-1 所示。

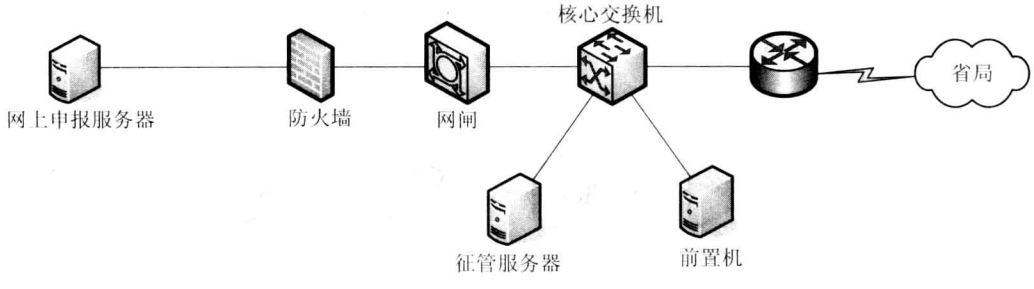

图 1-1

说明：

(1) 网上申报服务器的地址是 192.168.1.1，经过网闸后转换为 X.X.16.73。

(2) 前置机的 IP 地址为 X.X.16.56，征管服务器的 IP 地址为 X.X.16.200。

1.1.2　业务访问流程

(1) 纳税人通过互联网登录网上申报服务器，提交相关纳税信息。

(2) 网上申报服务器将这些纳税信息转发给前置机的同时，将相关信息写入征管服务器数据库。

(3) 如果网上申报服务器与前置机的数据交互出现问题，那么网上申报服务器会将征管服务器数据库相关的信息锁死。

1.2 故障现象

(1) 网上申报业务系统运行时，每天总有一部分纳税人的申报表单数据无法正常上传，通过征管服务器的业务软件可以看到这些用户的申报数据处于锁死状态。

(2) 在没有网闸的情况下，网上申报服务器与前置机直接通信，则故障现象消失，网上纳税系统全部恢复正常。

1.3 故障分析

1.3.1 前期分析

(1) 结合故障现象与业务流程，我们可以清晰地发现，问题应该就是出现在网上申报服务器经过网闸的地址转换后与前置机交互的过程中。

(2) 当网上申报服务器不通过网闸的地址转换而是直接与前置机交互的时候，业务应用一切正常，那么很可能是网闸在进行地址转换的时候对某些数据报文作了修改，或者是网闸直接丢弃了某些业务报文导致的故障。

(3) 网闸是最为可疑的故障关键点，我们决定在网闸前后部署网络分析系统(在此环境下，可直接在申报服务器和前置机上分别安装网络分析系统)，对网上申报业务数据交互过程分别进行抓包，如图 1-2 所示。

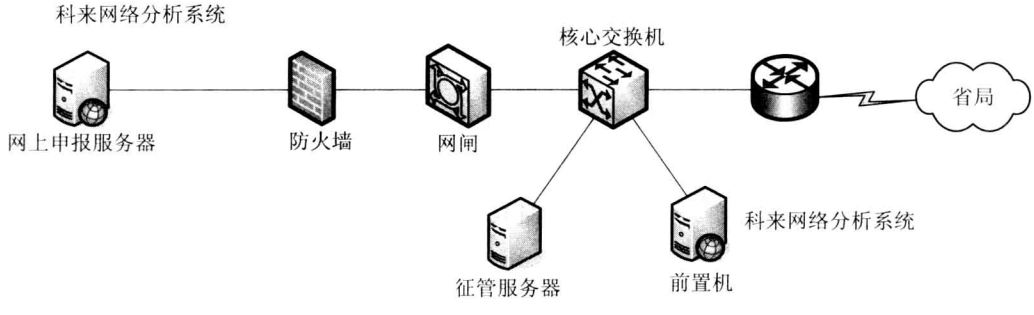

图 1-2

抓取数据报文后，可以为下一步的深入分析或对比分析提供原始数据。

1.3.2 数据包分析

(1) 我们通过科来网络分析系统捕获前置机交互的数据包，一段时间后，我们在“TCP 会话”视图中发现有几个 TCP 会话持续的时间比一般的 TCP 会话长很多(这是与正常情况下的业务会话持续时间作对比发现的，属于对比分析法应用方式的一种)，如图 1-3 所示。

节点1->	<-节点2	数据包	字节	持续时间	字节->	<-字节	数据包 ->	<- 数据包
3.16.73:3999	3.16.56:9001	27	16.959 KB	00:02:02	16.123 KB	856 B	14	13
3.16.73:3770	3.16.56:9001	26	16.898 KB	00:01:57	16.119 KB	798 B	14	12
3.16.73:3857	3.16.56:9001	27	16.936 KB	00:01:52	16.100 KB	856 B	14	13
3.16.73:3919	3.16.56:9001	25	15.805 KB	00:01:49	15.031 KB	792 B	13	12
3.16.73:3848	3.16.56:9001	26	17.293 KB	00:01:47	16.514 KB	798 B	14	12
3.16.73:3907	3.16.56:9001	24	15.748 KB	00:01:29	15.031 KB	734 B	13	11
3.16.73:3891	3.16.56:9001	44	30.039 KB	00:00:32	5.898 KB	24.141 KB	22	22
3.16.73:3787	3.16.56:9001	41	27.979 KB	00:00:32	3.906 KB	24.072 KB	20	21
3.16.56:4336	3.16.73:23	81	5.246 KB	00:00:28	3.032 KB	2.214 KB	48	33
3.16.73:3779	3.16.56:9001	49	29.951 KB	00:00:12	5.650 KB	24.301 KB	25	24
3.16.73:3993	3.16.56:9001	49	29.957 KB	00:00:11	5.656 KB	24.301 KB	25	24
3.16.73:3915	3.16.56:9001	41	27.961 KB	00:00:02	3.889 KB	24.072 KB	20	21
3.16.73:4006	3.16.56:9001	24	14.358 KB	00:00:02	2.146 KB	12.213 KB	11	13
3.16.73:3795	3.16.56:9001	43	29.514 KB	00:00:02	5.373 KB	24.141 KB	21	22
3.16.73:3955	3.16.56:9001	43	29.500 KB	00:00:02	5.359 KB	24.141 KB	21	22
3.16.73:3926	3.16.56:9001	43	29.500 KB	00:00:02	5.359 KB	24.141 KB	21	22
3.16.73:3889	3.16.56:9001	40	26.812 KB	00:00:01	2.739 KB	24.072 KB	19	21

这几个TCP会话持续的时间均超出其他的会话时间很多

图 1-3

(2) 双击其中一个 TCP 会话，打开详细的数据包视图，以查看其具体交互过程，如图 1-4 所示。

时间差	源	目标	概要
	3.16.73:3770	3.16.56:9001	序列号=0858950856, 确认号=0000000000, 标志=....S., 长...
0.000152	3.16.56:9001	3.16.73:3770	序列号=1817933311, 确认号=0858950857, 标志=.A..S., 长...
0.000137	3.16.73:3770	3.16.56:9001	序列号=0858950857, 确认号=1817933312, 标志=.A...., 长...
0.000372	3.16.56:9001	3.16.73:3770	序列号=1817933312, 确认号=0858950857, 标志=.A...., 长...
0.071267	3.16.73:3770	3.16.56:9001	序列号=0858950857, 确认号=1817933312, 标志=.A...., 长...
0.000075	3.16.73:3770	3.16.56:9001	序列号=0858952305, 确认号=1817933312, 标志=.AP..., 长...
0.000022	3.16.56:9001	3.16.73:3770	序列号=1817933312, 确认号=0858953349, 标志=.A...., 长...
0.002726	3.16.73:3770	3.16.56:9001	序列号=0858953349, 确认号=0000000000, 标志=...R.F, 长...
0.226054	3.16.73:3770	3.16.56:9001	[重传] 序列号=0858950857, 确认号=1817933312, 标志=.A...
0.000014	3.16.56:9001	3.16.73:3770	序列号=1817933312, 确认号=1817933312, 标志=...R., 长...
0.459979	3.16.73:3770	3.16.56:9001	[重传] 序列号=0858950857, 确认号=1817933312, 标志=.A...
0.000032	3.16.56:9001	3.16.73:3770	序列号=1817933312, 确认号=1817933312, 标志=...R., 长...
0.920005	3.16.73:3770	3.16.56:9001	[重传] 序列号=0858950857, 确认号=1817933312, 标志=.A...
0.000028	3.16.56:9001	3.16.73:3770	序列号=1817933312, 确认号=1817933312, 标志=...R., 长...
1.839923	3.16.73:3770	3.16.56:9001	[重传] 序列号=0858950857, 确认号=1817933312, 标志=.A...
0.000034	3.16.56:9001	3.16.73:3770	序列号=1817933312, 确认号=1817933312, 标志=...R., 长...
3.679965	3.16.73:3770	3.16.56:9001	[重传] 序列号=0858950857, 确认号=1817933312, 标志=.A...
0.000018	3.16.56:9001	3.16.73:3770	序列号=1817933312, 确认号=1817933312, 标志=...R., 长...
7.359918	3.16.73:3770	3.16.56:9001	序列号=0858950857, 确认号=1817933312, 标志=.A...., 长...
0.000040	3.16.56:9001	3.16.73:3770	序列号=1817933312, 确认号=1817933312, 标志=...R., 长...
14.71...	3.16.73:3770	3.16.56:9001	序列号=0858950857, 确认号=1817933312, 标志=.A...., 长...
0.000037	3.16.56:9001	3.16.73:3770	序列号=1817933312, 确认号=1817933312, 标志=...R., 长...
29.43...	3.16.73:3770	3.16.56:9001	序列号=0858950857, 确认号=1817933312, 标志=.A...., 长...
0.000041	3.16.56:9001	3.16.73:3770	序列号=1817933312, 确认号=1817933312, 标志=...R., 长...
58.87...	3.16.73:3770	3.16.56:9001	序列号=0858950857, 确认号=1817933312, 标志=.A...., 长...
0.000020	3.16.56:9001	3.16.73:3770	序列号=1817933312, 确认号=1817933312, 标志=...R., 长...

网闸地址73首先发送RESET报文

网闸地址向前置机发送(重传)报文，前置机直接发送RESET报文重置连接，这个过程导致了该TCP会话持续时间很长

图 1-4

在图 1-4 的视图中我们发现，这些 TCP 会话中存在大量的 TCP 重置报文，而且第一个发送 RESET 报文的是网闸的 IP 地址。

(3) 网闸为什么会突然给前置机发送 RESET 报文呢？我们双击打开这个 RESET 报文的详细解码视图，如图 1-5 所示。

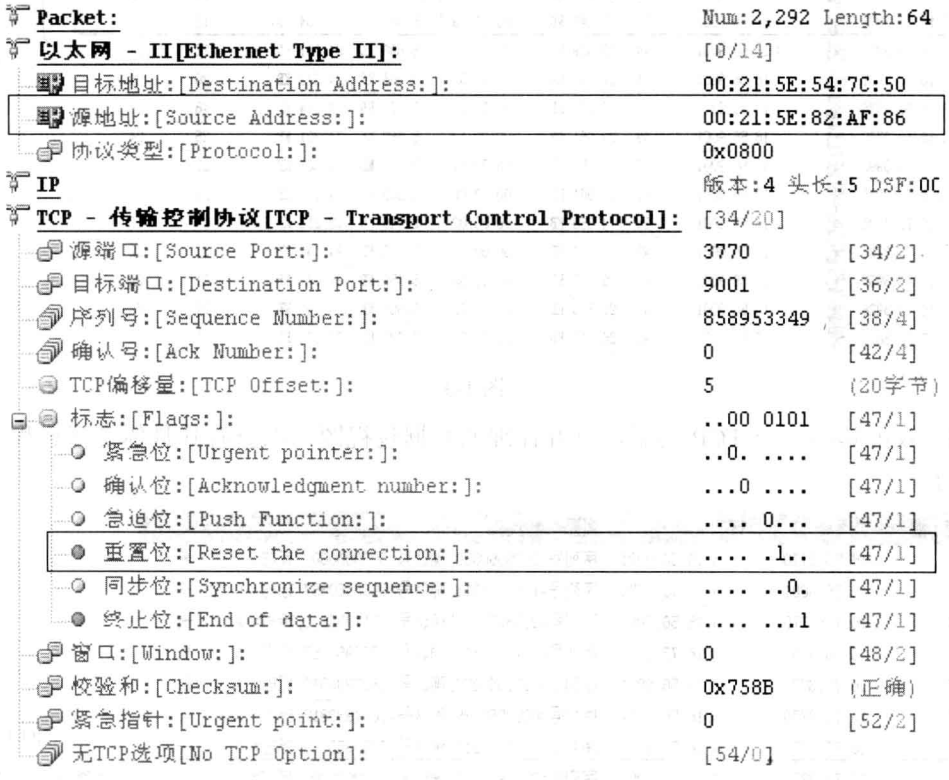

图 1-5

我们发现，这个数据报文的源 MAC 地址并非网闸的 MAC，真实的网闸 MAC 地址是 00:40:63:EF:43:DF，而这个数据报文的源 MAC 地址却是 00:21:5E:82:AF:86，难道是网内存在某些设备针对该业务数据进行会话劫持攻击？

(4) 通过进一步的分析发现，在这个 RESET 报文之前，是前置机发送给网闸地址的确认报文，这个报文封装的目的 MAC 地址就是 00:21:5E:82:AF:86，如图 1-6 所示。

(5) 前置机为什么会在数据交互的过程中突然出现了这种状况呢？一般而言，主机是根据其 ARP 表项来封装要发送的数据报文的目的 MAC 地址的，那么，这里前置机发往网闸数据报文的目的 MAC 地址出现改变是否是因为前置机的 ARP 表项内容变化了呢？我们在前置机的 DOS 窗口下，使用“arp –a”命令查看异常时的 ARP 表项内容，发现网闸 IP 对应的 MAC 地址的确变成了 00:21:5E:82:AF:86。

(6) 能够导致 ARP 表项更新的只可能是 ARP 报文，是前置机收到 ARP 欺骗报文导致了 ARP 表项的更新吗？由于前面都是针对 TCP 层面的数据交互来分析的，看不到 ARP 报文，因此我们决定在科来网络分析系统的“数据包”视图中查看交互过程的所有数据报文，如图 1-7 所示。

源	目标	源物理地址	目标物理地址	概要
3.16.73:3770	3.16.56:9001	00:40:63:EF:43:DF	00:21:5E:54:7C:50	序列号=0858950856,确认号=0000000000,标志=....S.,长...
3.16.56:9001	3.16.73:3770	00:21:5E:54:7C:50	00:40:63:EF:43:DF	序列号=1817933311,确认号=0858950857,标志=.A..S.,长...
3.16.73:3770	3.16.56:9001	00:40:63:EF:43:DF	00:21:5E:54:7C:50	序列号=0858950857,确认号=1817933312,标志=.A....,长...
3.16.56:9001	3.16.73:3770	00:21:5E:54:7C:50	00:40:63:EF:43:DF	序列号=1817933312,确认号=0858950857,标志=.A....,长...
3.16.73:3770	3.16.56:9001	00:40:63:EF:43:DF	00:21:5E:54:7C:50	序列号=0858950857,确认号=1817933312,标志=.A....,长...
3.16.73:3770	3.16.56:9001	00:40:63:EF:43:DF	00:21:5E:54:7C:50	序列号=0858952305,确认号=1817933312,标志=.AP...,长...
3.16.56:9001	3.16.73:3770	00:21:5E:54:7C:50	00:21:5E:82:AF:86	序列号=1817933312,确认号=0858953349,标志=.A....,长...
3.16.73:3770	3.16.56:9001	00:21:5E:82:AF:86	00:21:5E:54:7C:50	序列号=0858953349,确认号=0000000000,标志=...R.F,长...
3.16.73:3770	3.16.56:9001	00:40:63:EF:43:DF	00:21:5E:54:7C:50	[重传]序列号=0858950857,确认号=1817933312,标志=.A...
3.16.56:9001	3.16.73:3770	00:21:5E:54:7C:50	00:21:5E:82:AF:86	序列号=1817933312,确认号=1817933312,标志=...R..,长...
3.16.73:3770	3.16.56:9001	00:40:63:EF:43:DF	00:21:5E:54:7C:50	[重传]序列号=0858950857,确认号=1817933312,标志=.A...
3.16.56:9001	3.16.73:3770	00:21:5E:54:7C:50	00:21:5E:82:AF:86	序列号=1817933312,确认号=1817933312,标志=...R..,长...
3.16.73:3770	3.16.56:9001	00:40:63:EF:43:DF	00:21:5E:54:7C:50	[重传]序列号=0858950857,确认号=1817933312,标志=.A...
3.16.56:9001	3.16.73:3770	00:21:5E:54:7C:50	00:21:5E:82:AF:86	序列号=1817933312,确认号=1817933312,标志=...R..,长...
3.16.73:3770	3.16.56:9001	00:40:63:EF:43:DF	00:21:5E:54:7C:50	[重传]序列号=0858950857,确认号=1817933312,标志=.A...
3.16.56:9001	3.16.73:3770	00:21:5E:54:7C:50	00:21:5E:82:AF:86	序列号=1817933312,确认号=1817933312,标志=...R..,长...
3.16.73:3770	3.16.56:9001	00:40:63:EF:43:DF	00:21:5E:54:7C:50	[重传]序列号=0858950857,确认号=1817933312,标志=.A...
3.16.56:9001	3.16.73:3770	00:21:5E:54:7C:50	00:21:5E:82:AF:86	序列号=1817933312,确认号=1817933312,标志=...R..,长...
3.16.73:3770	3.16.56:9001	00:40:63:EF:43:DF	00:21:5E:54:7C:50	序列号=0858950857,确认号=1817933312,标志=.A....,长...
3.16.56:9001	3.16.73:3770	00:21:5E:54:7C:50	00:21:5E:82:AF:86	序列号=1817933312,确认号=1817933312,标志=...R..,长...
3.16.73:3770	3.16.56:9001	00:40:63:EF:43:DF	00:21:5E:54:7C:50	序列号=0858950857,确认号=1817933312,标志=.A....,长...
3.16.56:9001	3.16.73:3770	00:21:5E:54:7C:50	00:21:5E:82:AF:86	序列号=1817933312,确认号=1817933312,标志=...R..,长...
3.16.73:3770	3.16.56:9001	00:40:63:EF:43:DF	00:21:5E:54:7C:50	序列号=0858950857,确认号=1817933312,标志=.A....,长...
3.16.56:9001	3.16.73:3770	00:21:5E:54:7C:50	00:21:5E:82:AF:86	序列号=1817933312,确认号=1817933312,标志=...R..,长...
3.16.73:3770	3.16.56:9001	00:40:63:EF:43:DF	00:21:5E:54:7C:50	序列号=0858950857,确认号=1817933312,标志=.A....,长...
3.16.56:9001	3.16.73:3770	00:21:5E:54:7C:50	00:40:63:EF:43:DF	序列号=1817933312,确认号=1817933312,标志=...R..,长...

网闸源 MAC 地址为 00:40:63:EF:43:DF

前置机发往网闸的确认数据报文，封装的目的 MAC 地址却是 00:21:5E:82:AF:86

MAC 为 00:21:5E:82:AF:86 的设备以网闸的 IP 向前置机发送 RESET 报文

图 1-6

源	目标	概要
143.28.16.73:3770	143.28.16.56:9001	序列号=0858950856,确认号=0000000000,标志=....S.,长度= ...
00:21:5E:54:7C:50	FF:FF:FF:FF:FF:FF	谁是 143.28.16.73? 告诉 143.28.16.56
00:40:63:EF:43:DF	00:21:5E:54:7C:50	143.28.16.73 在 00:40:63:EF:43:DF
143.28.16.56:9001	143.28.16.73:3770	序列号=1817933311,确认号=0858950857,标志=.A..S.,长度= ...
143.28.16.73:3770	143.28.16.56:9001	序列号=0858950857,确认号=1817933312,标志=.A....,长度= ...
143.28.16.56:9001	143.28.16.73:3770	序列号=1817933312,确认号=0858950857,标志=.A....,长度= ...
00:21:5E:82:AF:86	00:21:5E:54:7C:50	143.28.16.73 在 00:21:5E:82:AF:86
143.28.16.73:3770	143.28.16.56:9001	序列号=0858950857,确认号=1817933312,标志=.A....,长度=14...
143.28.16.73:3770	143.28.16.56:9001	序列号=0858952305,确认号=1817933312,标志=.AP...,长度=10...
143.28.16.56:9001	143.28.16.73:3770	序列号=1817933312,确认号=0858953349,标志=.A....,长度= ...
143.28.16.73:3770	143.28.16.56:9001	序列号=0858953349,确认号=0000000000,标志=...R.F,长度= ...
143.28.16.73:3770	143.28.16.56:9001	[重传]序列号=0858950857,确认号=1817933312,标志=.A...,...
143.28.16.56:9001	143.28.16.73:3770	序列号=1817933312,确认号=1817933312,标志=...R..,长度= ...
143.28.16.73:3770	143.28.16.56:9001	[重传]序列号=0858950857,确认号=1817933312,标志=.A...,...
143.28.16.56:9001	143.28.16.73:3770	序列号=1817933312,确认号=1817933312,标志=...R..,长度= ...
143.28.16.73:3770	143.28.16.56:9001	[重传]序列号=0858950857,确认号=1817933312,标志=.A...,...
143.28.16.56:9001	143.28.16.73:3770	序列号=1817933312,确认号=1817933312,标志=...R..,长度= ...
143.28.16.73:3770	143.28.16.56:9001	[重传]序列号=0858950857,确认号=1817933312,标志=.A...,...
143.28.16.56:9001	143.28.16.73:3770	序列号=1817933312,确认号=1817933312,标志=...R..,长度= ...
143.28.16.73:3770	143.28.16.56:9001	[重传]序列号=0858950857,确认号=1817933312,标志=.A...,...
143.28.16.56:9001	143.28.16.73:3770	序列号=1817933312,确认号=1817933312,标志=...R..,长度= ...
143.28.16.73:3770	143.28.16.56:9001	序列号=0858950857,确认号=1817933312,标志=.A....,长度=14...
143.28.16.56:9001	143.28.16.73:3770	序列号=1817933312,确认号=1817933312,标志=...R..,长度= ...

图 1-7

我们发现，在网闸向前置机发送连接请求之后，前置机立即向网络中发送 ARP 请求，请求网闸 IP 对应的 MAC；在网闸响应了前置机的 ARP 请求之后，前置机开始与网闸进行 TCP 三次握手交互；这时，来自 MAC 地址为 00:21:5E:82:AF:86 的 ARP 响应到达了前置机，前置机更新其 ARP 表项；在此之后，前置机在收到来自网闸的数据报文时，都会向 00:21:5E:82:AF:86 地址发送确认报文。

为了便于大家理解，我们将这个交互过程中网闸、前置机以及未知设备的数据交互情况和状态变化作一个图示，如图 1-8 所示。

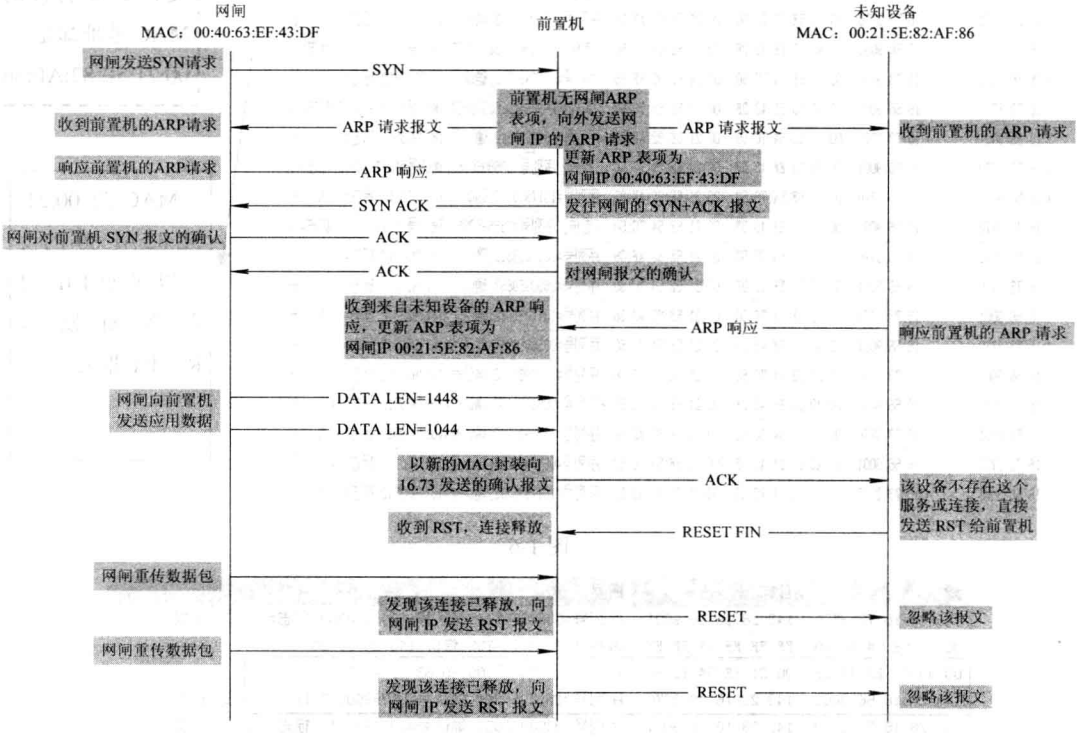

图 1-8

通过上面的图示可以清楚地看到，导致该业务故障的原因是网络内有一台设备使用了和网闸一样的 IP 地址。

另外，分析前置机的状态可以知道，前置机之所以会在交互的过程中向网络内发送目的 IP 为网闸的 ARP 请求报文，是因为前置机 ARP 表中网闸 IP 的 ARP 表项老化了。在前置机 ARP 表中网闸 IP 的 ARP 表项未老化之前，网闸与前置机交互数据是正常的，而网闸与前置机的业务数据交互间隔时间是随机的(这取决于网上纳税用户登录网上申报服务器提交纳税信息的时间)，这就可以解释为什么是部分网上申报业务表单出现异常了。

(7) 网络内有 2 台设备使用了同一个 IP 地址，应该很容易被发现，为什么一直没有被发现呢？其实，这是因为网闸的这个 IP 只有网上申报业务使用，而那个未知的网络设备设置的这个 IP，很可能仅仅是用来管理的，这个设备长期在线，又很少有人管理(至少信息中心的人都不知道该设备的存在)，因此不会主动向网络中发送 ARP 报文，不会影响到网络内其他主机和应用的正常运行。但是，它会响应其他主机对其 IP 地址的 ARP 请求。我们

可以通过交换机的MAC地址表找到这个设备所在的位置。

1.4 分析结论及解决方法

通过上面的综合分析，我们可以得出结论：此次业务故障的原因完全跟网闸无关，是由于内网的一台MAC地址为00:21:5E:82:AF:86的设备和网闸映射的地址冲突导致的。

问题原因定位之后，我们至少可以通过以下三种方式解决该故障：

(1) 由于是ARP表更新导致的，我们可以手动绑定网闸的ARP，或者修改注册表，将前置机的ARP表老化时间调大。

(2) 找出使用了网闸映射IP的设备，修改该设备的IP地址，或修改网上申报服务器通过网闸后映射的IP地址。

(3) 还可以让该业务系统在应用层面设置一个检测模块，当发现有表单提交异常时，等待一段时间，重新向前置机提交表单。

1.5 总　　结

在刚接触到这个故障时，我们以为是网闸的原因导致的，但是通过数据包分析后发现是由于网络中IP地址冲突导致的。所以在接触到故障时，不要主观地臆测故障原因，而是要通过分析的手段找到根本的原因，以便提高故障解决的效率。