

- 
- 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



NLIC2970949966



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

网络分析与网络管理工程师用书

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 xdupfb001@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

如有印装问题可调换

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 1 章 某地税网上申报业务系统

故障分析报告 1

1.1 故障环境 1

1.1.1 网络拓扑 1

1.1.2 业务访问流程 1

1.2 故障现象 2

1.3 故障分析 2

1.3.1 前期分析 2

1.3.2 数据包分析 2

1.4 分析结论及解决方法 7

1.5 总结 7

第 2 章 某公安系统机房网络

丢包分析案例 8

2.1 故障描述 8

2.2 故障重现 8

2.3 数据分析 9

2.4 故障结论及解决办法 11

第 3 章 某保险公司 VPN 异常中断

故障分析报告 12

3.1 故障描述 12

3.1.1 故障现象 12

3.1.2 环境描述 12

3.2 分析过程 13

3.2.1 流量趋势分析 13

3.2.2 数据包解码分析 14

3.3 结论及建议 16

3.3.1 分析结论 16

3.3.2 建议 16

第 4 章 某供电局营销应用服务中断

问题分析案例 17

4.1 故障描述 17

4.1.1 故障现象 17

4.1.2 网络拓扑 17

4.2 问题分析过程 18

4.2.1 服务器流量分析 18

4.2.2 客户端流量分析 19

4.2.3 营销应用其他服务器的排查 23

4.3 分析结论 24

4.3.1 故障说明 24

4.3.2 优化后监测 24

第 5 章 某移动公司 BOSS 系统

故障分析 26

5.1 故障描述 26

5.1.1 故障现象 26

5.1.2 网络拓扑 26

5.2 分析过程 27

5.2.1 捕获数据包 27

5.2.2 分析数据包 27

5.3 结论及建议 31

5.3.1 分析结论 31

5.3.2 建议 31

第 6 章 某航空公司客服系统

故障排查 32

6.1 故障描述 32

6.1.1 故障现象 32

6.1.2 故障规律摸索 32

6.2 故障排查过程 33

6.2.1 排查思路 33

6.2.2 故障重现 33

6.2.3 IP 会话分析 33

6.2.4 软件界面连接分析 33

6.2.5 控制插件连接分析 34

6.2.6 故障原因分析 35

6.3 解决问题建议 35

第7章 同一网段部分电脑无法 Ping 通 网关故障分析	36
7.1 故障描述	36
7.1.1 故障现象	36
7.1.2 基本环境	36
7.2 分析方案设计	37
7.2.1 分析目标	37
7.2.2 分析设备部署	37
7.3 分析情况	37
7.3.1 客服中心抓包情况	37
7.3.2 分局办公楼抓包情况	38
7.4 分析结论	39
第8章 网络环路分析	40
8.1 故障描述	40
8.2 分析过程	41
8.2.1 详细分析	41
8.2.2 网络环路分析	42
8.3 分析结果	43
8.4 紧急处理办法及优化建议	43
第9章 某运营商客户系统访问 故障分析	45
9.1 故障描述	45
9.1.1 故障环境	45
9.1.2 故障现象	45
9.2 故障分析	46
9.2.1 分析思路	46
9.2.2 前期分析准备	46
9.2.3 分析过程	47
9.3 分析结论与建议	50
第10章 某应用间歇性无法访问 故障分析	51
10.1 故障描述	51
10.1.1 故障现象及环境	51
10.1.2 检测描述	51
10.2 分析内容	52
10.2.1 分析过程	52
10.2.2 分析结果	53
10.2.3 处理方法	54
10.3 分析总结	54

第11章 防火墙策略导致服务器访问 异常分析	55
11.1 故障描述	55
11.1.1 测试描述	55
11.1.2 故障现象	55
11.2 故障分析	56
11.3 测试总结	58
第12章 某单位部分用户 Web 无法 正常访问故障分析	59
12.1 故障描述	59
12.1.1 网络环境	59
12.1.2 故障现象	59
12.2 分析过程	59
12.2.1 故障点分析	59
12.2.2 分析设备部署	60
12.2.3 数据包分析	60
12.2.4 分析结论	61
12.3 总结	61
第13章 内外网核心对接故障 分析报告	62
13.1 故障描述	62
13.1.1 故障现象	62
13.1.2 基本环境	63
13.2 分析方案设计	63
13.2.1 分析目标	63
13.2.2 分析设备部署	63
13.3 分析情况	64
13.3.1 内网核心	64
13.3.2 外网核心	64
13.4 分析结论	65
第14章 某集团 LIMS 服务器访问 ERP 系统故障分析	66
14.1 故障描述	66
14.1.1 故障现象	66
14.1.2 网络拓扑	66
14.2 具体分析	67
14.2.1 捕获数据包	67
14.2.2 LIMS 访问 ERP 的 RFC 函数及 模块	67

14.2.3 疑问及故障原因	70	15.1 环境概述	74
14.3 推荐解决方法	73	15.2 故障分析	74
第 15 章 VoIP 通信受干扰故障分析	74	15.3 解决方案	76

第二部分 网络安全分析

第 16 章 某人民法院蠕虫问题		22.2.2 意外的 SMTP 主机扫描警报	111
分析报告	77	22.2.3 SMTP 会话统计分析	112
16.1 故障描述	77	22.3 SMTP 数据流解码分析	113
16.2 故障分析	77	22.4 案例总结	114
16.3 分析总结	81	第 23 章 由于攻击造成的网络	
第 17 章 数据库暴力破解分析	82	性能下降案例分析	116
17.1 分析背景	82	23.1 故障描述	116
17.2 故障描述及分析	82	23.1.1 故障现象	116
17.3 分析结论	86	23.1.2 基本环境	116
第 18 章 通过网络分析验证		23.2 分析方案设计	117
IPS 设备误报	87	23.2.1 分析目标	117
18.1 故障描述	87	23.2.2 分析设备部署	117
18.2 故障分析	87	23.3 分析情况	117
18.3 分析结论及建议	91	23.3.1 基本流量分析	117
第 19 章 通过科来网络分析系统		23.3.2 重点主机分析	119
查找蠕虫案例	92	23.3.3 其他流量分析	119
19.1 故障描述	92	23.4 分析结论	120
19.2 分析过程	92	第 24 章 BT 流量通过 TCP 80 端口	
19.3 分析总结	97	占用和蠕虫攻击	121
第 20 章 邮件系统攻击分析	98	24.1 故障描述	121
20.1 案例背景	98	24.2 分析过程	122
20.2 针对邮件系统的暴力破解	98	24.3 分析总结	127
20.3 邮件蠕虫攻击	100	第 25 章 利用黑客工具进行渗透的	
第 21 章 飞客蠕虫研究	102	数据分析	128
21.1 案例背景	102	25.1 背景	128
21.2 分析过程	102	25.2 分析过程	128
21.3 参考文档	108	25.3 总结	130
第 22 章 垃圾邮件行为分析	109	第 26 章 Web 服务器攻击分析	131
22.1 故障描述	109	26.1 故障描述	131
22.1.1 故障背景	109	26.1.1 故障现象	131
22.1.2 故障环境	109	26.1.2 基本环境	131
22.2 分析过程	110	26.2 分析方案设计	131
22.2.1 主机扫描警报的基本效果	110	26.2.1 分析目标	131

26.2.2 分析设备部署	131
26.3 分析情况	132
26.3.1 基本流量分析	132
26.3.2 总体通信情况分析	133
26.3.3 针对 Web 服务器访问流量 进行分析	134
26.4 分析结论	135
第 27 章 某局 ARP 欺骗故障分析	136
27.1 故障环境	136
27.2 故障现象	136
27.3 故障分析	136
27.3.1 分析测试	136
27.3.2 数据包捕获	137
27.3.3 数据包分析	138
27.3.4 分析结论	139
27.4 总结	139
第 28 章 通过协议分析理解端口 扫描原理	140
28.1 概述	140
28.2 扫描分析	140
28.2.1 TCP SYN 扫描	140
28.2.2 TCP connect 扫描	142
28.2.3 UDP 扫描	143
28.2.4 NULL 扫描	144
28.2.5 ACK 扫描	145
28.2.6 窗口扫描	146
28.2.7 IP 扫描	147

第三部分 网络应用性能分析

第 31 章 某银行网银系统访问缓慢 分析案例	165
31.1 故障描述	165
31.1.1 故障背景	165
31.1.2 网络拓扑	165
31.2 分析过程	166
31.2.1 分析思路	166
31.2.2 整体流量分析	166
31.2.3 网络延时分析	166

28.2.8 FIN/ACK 扫描	147
28.2.9 定制扫描	149
28.3 总结	149
第 29 章 虚假源地址网络攻击 分析案例	150
29.1 故障描述	150
29.1.1 故障现象	150
29.1.2 网络与应用结构	151
29.1.3 内网用户访问方式	151
29.2 分析方案及思路	152
29.2.1 基本分析思路	152
29.2.2 分析设备部署	152
29.2.3 分析档案与方案选择	152
29.3 分析过程	153
29.3.1 总体分析	153
29.3.2 问题分析	155
29.4 分析总结	157
29.4.1 分析结论	157
29.4.2 问题验证	158
29.4.3 解决方法	159
第 30 章 回溯式异常流量分析	160
30.1 故障背景	160
30.2 分析过程	160
30.2.1 流量突起分析	160
30.2.2 TCP 请求异常分析	162
30.3 结论	164

31.2.4 网银系统性能分析	167
31.3 分析结论	170
第 32 章 某金融机构行情查询系统 分析案例	171
32.1 故障描述	171
32.2 分析过程	171
32.2.1 TCP 交互延时分析原理	171
32.2.2 延时状况分析	172
32.2.3 有效数据传输分析	173

32.3 问题解决	174
第 33 章 某基金公司邮件服务器访问缓慢分析案例	175
33.1 故障描述	175
33.1.1 故障现象	175
33.1.2 网络拓扑	175
33.2 分析过程	176
33.2.1 整体流量状况评估	176
33.2.2 网络延时状况评估	176
33.2.3 应用层交互延时分析	178
33.3 分析结论	180
33.4 调整建议	180
第 34 章 应用服务器测试响应缓慢分析案例	181
34.1 故障描述	181
34.1.1 故障现象	181
34.1.2 检测描述	181
34.2 分析内容	181
34.2.1 分析过程	181
34.2.2 分析结果	183
34.3 处理方法及分析总结	183
第 35 章 门户服务器流量异常分析报告	185
35.1 故障描述	185
35.1.1 故障现象	185
35.1.2 检测描述	185
35.2 故障分析	185
35.2.1 基本分析	185
35.2.2 详细分析	186
35.2.3 处理方法	186
35.3 分析总结	186
第 36 章 某移动公司虚拟化迁移后应用缓慢分析案例	187
36.1 故障描述	187
36.2 分析过程	187
36.2.1 链路流量状况分析	188
36.2.2 故障应用管理平台通信数据分析	188
36.3 总结	194

第 37 章 广东省某学院网络测试分析报告	195
37.1 故障描述	195
37.1.1 故障环境	195
37.1.2 网络部署示意图	195
37.1.3 测试目标	196
37.2 故障分析	196
37.2.1 网络承载性能分析	196
37.2.2 Top 应用层协议分析	197
37.2.3 网络用户 IP 流量占用分析	198
37.3 分析总结	200
37.3.1 分析结果	200
37.3.2 优化解决建议	200
第 38 章 某市供电局网络性能分析报告	201
38.1 故障描述	201
38.2 故障分析	201
38.2.1 网络承载性能质量分析	201
38.2.2 网络异常行为分析	203
38.3 总结	204
第 39 章 某供电局内部网络分析	205
39.1 故障描述	205
39.2 故障分析	205
39.2.1 分析故障思路	205
39.2.2 解决步骤	205
39.2.3 对数据链路层进行分析	207
39.2.4 对网络层进行分析	208
39.2.5 对传输层进行分析	210
39.3 总结	213
第 40 章 税务系统问题分析	214
40.1 故障描述	214
40.1.1 故障现象	214
40.1.2 基本环境	214
40.2 分析内容	215
40.2.1 分析目标	215
40.2.2 分析过程	216
40.2.3 性能分析	216
40.2.4 安全性分析	217
40.2.5 异常情况分析	217

40.3 分析结论	218	43.2.3 流量信息验证	228
第 41 章 高校网络访问速度慢的 探究和分析报告	219	43.2.4 业务主动监控	230
41.1 故障描述	219	43.3 小结	231
41.1.1 基本环境	219	第 44 章 某局视频会议故障报告和 服务器运行分析	232
41.1.2 故障现象	219	44.1 视频会议故障描述	232
41.2 分析方案设计	219	44.1.1 网络环境	232
41.2.1 分析目标	219	44.1.2 故障现象	232
41.2.2 分析设备部署	220	44.2 视频会议故障分析	233
41.3 分析情况	220	44.2.1 分析方法	233
41.3.1 对招待所捕获的 Web 访问数据 进行分析	220	44.2.2 部署方式	233
41.3.2 在服务器端进行流量分析	221	44.2.3 具体分析	233
41.3.3 查找丢包点	222	44.3 服务器的运行分析	238
41.4 分析结论	222	44.4 总结	239
第 42 章 某 OA 系统访问缓慢 原因分析	223	第 45 章 某单位访问部分应用服务 缓慢故障分析	241
42.1 故障描述	223	45.1 故障描述	241
42.2 分析过程及结论	223	45.1.1 故障环境	241
42.2.1 客户端访问速度慢原因分析	223	45.1.2 故障现象	241
42.2.2 打开附件慢原因分析	224	45.2 故障分析	241
42.2.3 关于小包太多的原因分析	226	45.2.1 分析方法	241
第 43 章 IDC 出口流量梳理	227	45.2.2 部署方式	242
43.1 故障背景	227	45.2.3 捕包分析	242
43.2 IDC 出口流量梳理	228	45.2.4 分析结论	244
43.2.1 设备部署	228	45.3 总结	244
43.2.2 快捷历史数据回溯	228	附录 关于 CSNA 网络分析论坛	245

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。

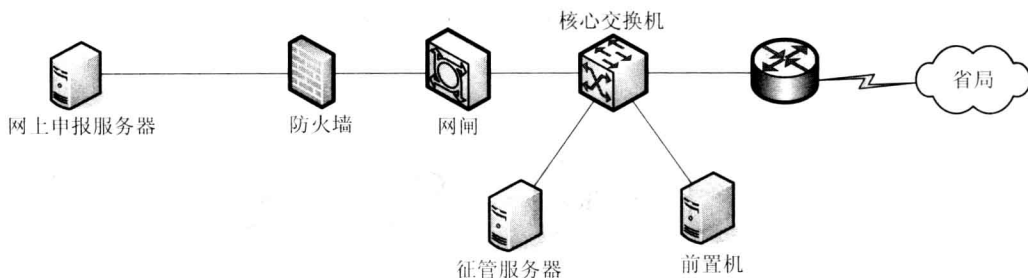


图 1-1

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。

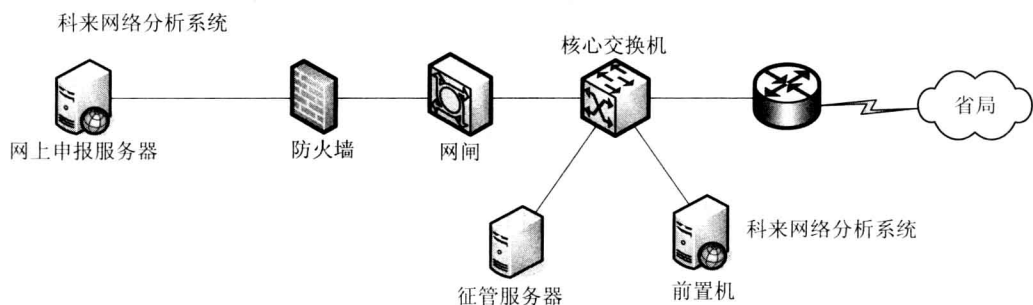


图 1-2

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
16.73.3999	16.56.9001	27	16.959 KB	00:02:02	16.123 KB	856 B	14	13
16.73.3770	16.56.9001	26	16.898 KB	00:01:57	16.119 KB	798 B	14	12
16.73.3857	16.56.9001	27	16.936 KB	00:01:52	16.100 KB	856 B	14	13
16.73.3919	16.56.9001	25	15.805 KB	00:01:49	15.031 KB	792 B	13	12
16.73.3848	16.56.9001	26	17.293 KB	00:01:47	16.514 KB	798 B	14	12
16.73.3907	16.56.9001	24	15.748 KB	00:01:29	15.031 KB	734 B	13	11
16.73.3891	16.56.9001	44	30.039 KB	00:00:32	5.898 KB	24.141 KB	22	22
16.73.3787	16.56.9001	41	27.979 KB	00:00:32	3.906 KB	24.072 KB	20	21
16.56.4336	16.73.23	81	5.246 KB	00:00:28	3.032 KB	2.214 KB	48	33
16.73.3779	16.56.9001	49	29.951 KB	00:00:12	5.650 KB	24.301 KB	25	24
16.73.3993	16.56.9001	49	29.957 KB	00:00:11	5.656 KB	24.301 KB	25	24
16.73.3915	16.56.9001	41	27.961 KB	00:00:02	3.889 KB	24.072 KB	20	21
16.73.4006	16.56.9001	24	14.358 KB	00:00:02	2.146 KB	12.213 KB	11	13
16.73.3795	16.56.9001	43	29.514 KB	00:00:02	5.373 KB	24.141 KB	21	22
16.73.3955	16.56.9001	43	29.500 KB	00:00:02	5.359 KB	24.141 KB	21	22
16.73.3926	16.56.9001	43	29.500 KB	00:00:02	5.359 KB	24.141 KB	21	22
16.73.3889	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
0.000152	16.73.3770	16.56.9001	序列号=0858950856, 确认号=0000000000, 标志=...S, 长...
0.000137	16.73.3770	16.56.9001	序列号=1817933311, 确认号=0858950857, 标志=A..., 长...
0.000372	16.56.9001	16.73.3770	序列号=0858950857, 确认号=1817933312, 标志=A..., 长...
0.071267	16.73.3770	16.56.9001	序列号=0858950857, 确认号=1817933312, 标志=A..., 长...
0.000075	16.73.3770	16.56.9001	序列号=0858952305, 确认号=1817933312, 标志=AP..., 长...
0.000022	16.56.9001	16.73.3770	序列号=1817933312, 确认号=0858953349, 标志=A..., 长...
0.002726	16.73.3770	16.56.9001	序列号=0858953349, 确认号=0000000000, 标志=...R,F, 长...
0.226054	16.73.3770	16.56.9001	[重传] 序列号=0858950857, 确认号=1817933312, 标志=A...
0.000014	16.56.9001	16.73.3770	序列号=1817933312, 确认号=1817933312, 标志=...R, 长...
0.459979	16.73.3770	16.56.9001	[重传] 序列号=0858950857, 确认号=1817933312, 标志=A...
0.000032	16.56.9001	16.73.3770	序列号=1817933312, 确认号=1817933312, 标志=...R, 长...
0.920005	16.73.3770	16.56.9001	[重传] 序列号=0858950857, 确认号=1817933312, 标志=A...
0.000028	16.56.9001	16.73.3770	序列号=1817933312, 确认号=1817933312, 标志=...R, 长...
1.839923	16.73.3770	16.56.9001	[重传] 序列号=0858950857, 确认号=1817933312, 标志=A...
0.000034	16.56.9001	16.73.3770	序列号=1817933312, 确认号=1817933312, 标志=...R, 长...
3.679965	16.73.3770	16.56.9001	[重传] 序列号=0858950857, 确认号=1817933312, 标志=A...
0.000018	16.56.9001	16.73.3770	序列号=1817933312, 确认号=1817933312, 标志=...R, 长...
7.359918	16.73.3770	16.56.9001	序列号=0858950857, 确认号=1817933312, 标志=A..., 长...
0.000040	16.56.9001	16.73.3770	序列号=1817933312, 确认号=1817933312, 标志=...R, 长...
14.71...	16.73.3770	16.56.9001	序列号=0858950857, 确认号=1817933312, 标志=A..., 长...
0.000037	16.56.9001	16.73.3770	序列号=1817933312, 确认号=1817933312, 标志=...R, 长...
29.43...	16.73.3770	16.56.9001	序列号=0858950857, 确认号=1817933312, 标志=A..., 长...
0.000041	16.56.9001	16.73.3770	序列号=1817933312, 确认号=1817933312, 标志=...R, 长...
58.87...	16.73.3770	16.56.9001	序列号=0858950857, 确认号=1817933312, 标志=A..., 长...
0.000020	16.56.9001	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。

Packet:	Num:2,292 Length:64
以太网 - II[Ethernet Type II]:	[0/14]
目标地址:[Destination Address]:	00:21:5E:54:7C:50
源地址:[Source Address]:	00:21:5E:82:AF:86
协议类型:[Protocol]:	0x0800
IP	版本:4 头长:5 DSF:00
TCP - 传输控制协议[TCP - Transport Control Protocol]:	[34/20]
源端口:[Source Port]:	3770 [34/2]
目标端口:[Destination Port]:	9001 [36/2]
序列号:[Sequence Number]:	858953349 [38/4]
确认号:[Ack Number]:	0 [42/4]
TCP偏移量:[TCP Offset]:	5 (20字节)
标志:[Flags]:	..00 0101 [47/1]
紧急位:[Urgent pointer]:	..0. [47/1]
确认位:[Acknowledgment number]:	...0 [47/1]
急迫位:[Push Function]:	 0... [47/1]
重置位:[Reset the connection]:	1.. [47/1]
同步位:[Synchronize sequence]:	0. [47/1]
终止位:[End of data]:	1 [47/1]
窗口:[Window]:	0 [48/2]
校验和:[Checksum]:	0x758B (正确)
紧急指针:[Urgent point]:	0 [52/2]
无TCP选项[No TCP Option]:	[54/0]

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。

[illegible]

图 1-6

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。

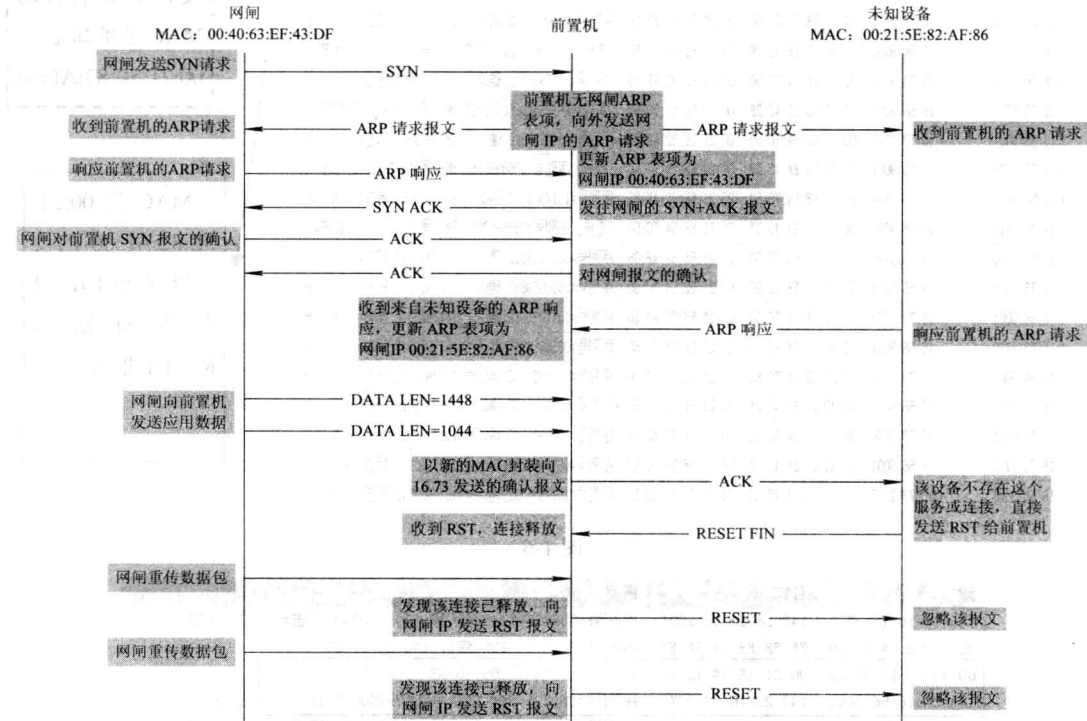


图 1-8

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。