网络故障分析与排除

主编 夏 磊

WANG LUO GU ZHANG
FEN XI YU PAI CHU

中国石油大学出版社
CHINA UNIVERSITY OF PETROLEUM PRESS

网络故障分析与排除

主 编 夏 磊

中国石油大学出版社
CHINA UNIVERSITY OF PETROLEUM PRESS

图书在版编目(CIP)数据

网络故障分析与排除/夏磊主编. —东营:中国石油大学出版社,2016.5

ISBN 978-7-5636-5205-1

Ⅰ. ①网… Ⅱ. ①夏… Ⅲ. ①计算机网络—故障诊断 ②计算机网络—故障修复 Ⅳ. ①TP393.07

中国版本图书馆 CIP 数据核字(2016)第 078575 号

书　　名:网络故障分析与排除

作　　者:夏　磊

责任编辑:曹秀丽(电话 0532—86981532)

封面设计:青岛友一广告传媒有限公司

出 版 者:中国石油大学出版社(山东 东营　邮编 257061)

网　　址:http://www.uppbook.com.cn

电子信箱:shiyoujiaoyu@126.com

排 版 者:汇英文化传媒

印 刷 者:沂南县汶凤印刷有限公司

发 行 者:中国石油大学出版社(电话 0532—86981531,86983437)

开　　本:180 mm × 235 mm　印张:10　字数:206 千字

版　　次:2016 年 9 月第 1 版第 1 次印刷

定　　价:30.00 元

前言 Preface

现有的网络故障分析与排除相关教材的内容大多是根据分层进行故障分析而编写的。比如物理层故障分析与排除、数据链路层故障分析与排除、网络层故障分析与排除等，都属于传统的知识学科式讲授。这类教材讲解抽象，学生在学完后不能实际应用，甚至在工作中无法分清具体故障属于哪一层故障，因此在高职高专教学中使用效果很差。

本书以“方法—工具—按不同现象处理故障”为主线，通过方法和工具的使用奠定学生学习的基础。书中内容的设置和选取更加注重学习者技能训练和职业竞争力的培养，几乎涵盖了所有的网络故障现象，使读者能够通过7个任务的相关知识的学习和技能训练，熟练掌握网络故障分析与排除的方法。

本书采用基于工作过程的项目化方式编写，以图文并茂、通俗易懂的方式讲解了大量的企业工程案例，同时介绍了理解和学习这些案例所需的理论知识和操作技能。由成都科来软件有限公司提供的网络分析案例集也被部分引入书中，这些案例均来源于一线专业网络技术人员的实际工作，很具有代表性，值得在教学工作中借鉴和使用。本书的使用将促进案例教学、基于工作过程的项目式教学改革，提高学生的实践应用能力。书中融合了新的课程考核方式，可以更好地培养学生的职业能力、学习能力、团队协作能力等。

全书共有7个任务，从基础到综合、由浅入深地介绍网络故障分析与排除的全部内容，主要包括：网络故障分析与排除的方法，常见网络故障诊断工具的使用，互联设备故障分析与排除，网络性能故障分析与排除，网络连通性故障分析与排除，网络服务故障分析与排除，网络安全性故障分析与排除等。

本书可作为高职高专院校计算机及相关专业“网络故障分析与排除”课程的教材，也可用作相关技能培训、计算机从业人员和爱好者的参考用书。

本书是由具有丰富一线教学经验的教师集体编写而成的，由夏磊担任主编并对全书进行统稿，周连兵、孙艳玲担任副主编，王丽华、蒋莉莉、姜甜甜也参与了部分编写工作。本书参考和引用了大量的文献资料，在此向相关作者表示衷心的感谢，同时感谢成都科来软件有限公司的大力支持。

由于时间仓促，书中难免存在不妥之处，敬请读者见谅，并提出宝贵意见。

编者

2016 年 3 月

目录 Contents

课程导学 …… 1

任务一　典型网络故障案例分析 …… 4

1.1　典型网络故障描述 …… 4
1.2　典型网络故障分析 …… 5
1.3　相关知识 …… 10
1.4　任务实施 …… 34
1.5　学习效果测评 …… 35

任务二　常用诊断工具的使用 …… 36

2.1　任务说明 …… 36
2.2　任务分析 …… 36
2.3　相关知识 …… 36
2.4　任务实施 …… 47
2.5　学习效果测评 …… 48

任务三　互联设备故障分析与排除 …… 49

3.1　任务说明 …… 49
3.2　任务分析 …… 49
3.3　相关知识 …… 49
3.4　典型故障案例 …… 59
3.5　任务实施 …… 68
3.6　学习效果测评 …… 69

任务四　网络性能故障分析与排除 …… 70

4.1　任务说明 …… 70
4.2　任务分析 …… 70
4.3　相关知识 …… 70
4.4　典型故障案例 …… 77
4.5　任务实施 …… 82
4.6　学习效果测评 …… 83

任务五　网络连通性故障分析与排除 …… 84

5.1　任务说明 …… 84
5.2　任务分析 …… 84
5.3　相关知识 …… 84
5.4　典型故障案例 …… 100
5.5　任务实施 …… 108
5.6　学习效果测评 …… 109

任务六　网络服务故障分析与排除 …… 110

6.1　任务说明 …… 110
6.2　任务分析 …… 110
6.3　相关知识 …… 110
6.4　典型故障案例 …… 114
6.5　任务实施 …… 122
6.6　学习效果测评 …… 123

任务七　网络安全性故障分析与排除 …… 124

7.1　任务说明 …… 124
7.2　任务分析 …… 124
7.3　相关知识 …… 124
7.4　典型故障案例 …… 131
7.5　任务实施 …… 147
7.6　学习效果测评 …… 148

附录 1　课程考核方式 …… 149

附录 2　课程学习参考资源 …… 152

参考文献 …… 153

课程导学

1. 课程整体概述

网络故障分析与排除课程通过校企合作共同开发了新的体系，课程设计以培养学生的职业竞争力为导向，实施能力本位的人才培养方案。教学中结合德国先进的基于工作过程的教学理念，以职业标准和岗位任职要求为指导，以知识技能、职业素养和职业能力为培养目标，与成都科来软件有限公司、山东瑞华颂安信息科技有限公司合作进行课程开发与设计。

2. 课程体系结构(图 1)

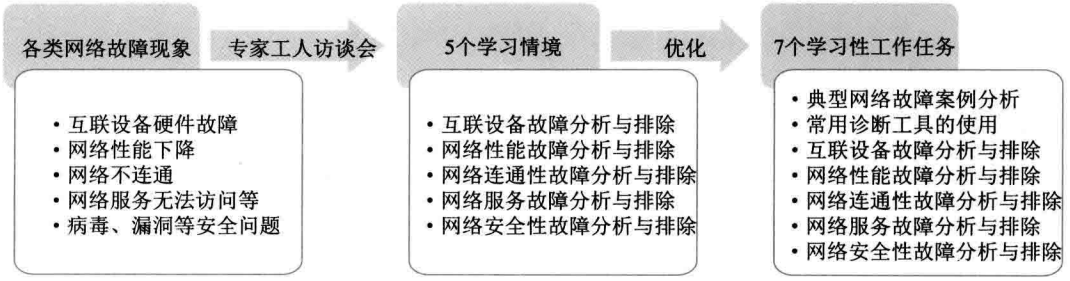


图 1

课程以“方法—工具—按不同现象处理故障”为主线，经过课程组与企业用户多次召开访谈会探讨与修订，根据教学规律进行优化，最终形成 5 个学习情境。

为了适应教学，作者在这 5 个学习情境的基础上，加上网络故障分析与排除的基本方法与使用工具，最终形成 7 个学习性工作任务(图 2)。每个任务按照工作过程的流程进行组织，更加重视学生实践能力和解决实际问题能力的培养。通过系统学习，学生能够通过对故障的分析，使用相关方法和工具排除故障。

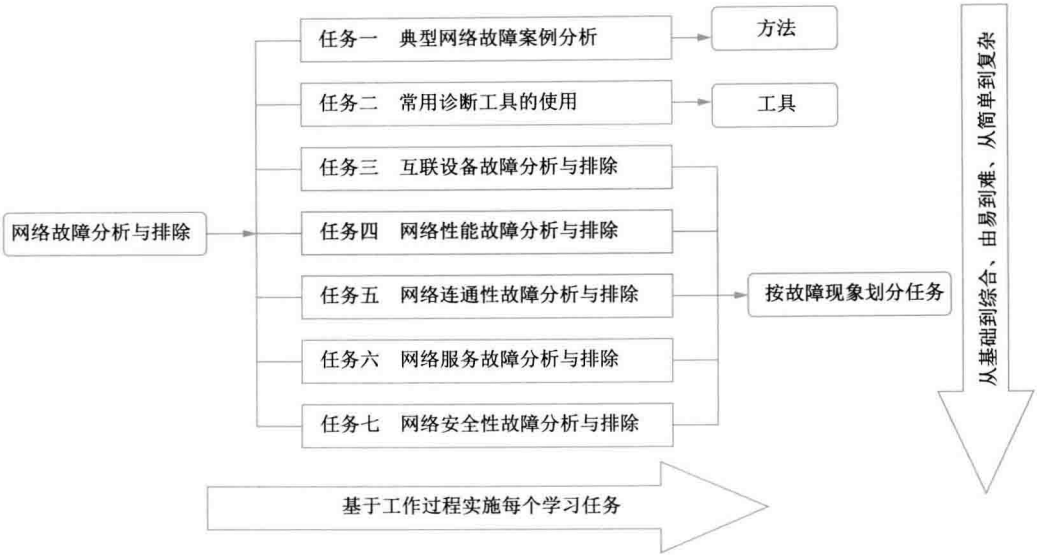


图 2

基于上述教学改革，传统的教材已无法满足课程教学需要，迫切需要编写一本适合教学改革的项目式案例教材。本书根据职业竞争力培养的要求，引入工作过程系统化的理念和大量的一线工程案例，以能力培养和实践操作为主线讲解内容。书中以丰富的企业一线工程案例，为学生进行理论学习和实践训练打下良好的基础。

3. 核心知识点和技能点（表 1）

表 1

章　节	知识点与技能点	掌握程度	考核方式	各教学环节学时分配		
				理论教学	实践教学	课内小计
任务一：典型网络故障案例分析	科来网络通讯分析系统 2010 使用技巧 TCP 头部选项功能详解	记忆 / 理解	过程考核、目标考核、小组答辩式考核	2	4	4
任务二：常用诊断工具的使用	常用网络测试命令的使用 Windows 故障诊断工具的使用 硬件故障诊断工具的使用 软件故障诊断工具的使用	记忆 / 理解 / 运用	过程考核、目标考核、小组答辩式考核	2	4	4
任务三：互联设备故障分析与排除	网卡故障分析与排除 服务器故障分析与排除 交换机故障分析与排除 路由器故障分析与排除 防火墙故障分析与排除 无线设备故障分析与排除	记忆 / 理解 / 运用	过程考核、目标考核、小组答辩式考核	3	6	4

续表

章　节	知识点与技能点	掌握程度	考核方式	各教学环节学时分配		
				理论教学	实践教学	课内小计
任务四：网络性能故障分析与排除	网速变慢故障分析与排除 网络间隙性故障分析与排除 帧差错故障分析与排除 冲突增多故障分析与排除 无线网络性能故障分析与排除	记忆／理解／运用	过程考核、目标考核、小组答辩式考核	3	6	4
任务五：网络连通性故障分析与排除	单点连接故障分析与排除 网段连接故障分析与排除 Internet 接入故障分析与排除 无线网络连通性故障分析与排除	记忆／理解／运用	过程考核、目标考核、小组答辩式考核	2	6	4
任务六：网络服务故障分析与排除	文件和打印服务故障分析与排除 IIS 服务故障分析与排除 DNS 服务故障分析与排除 DHCP 服务故障分析与排除 Apache 故障分析与排除 Samba 故障分析与排除	理解／运用	过程考核、目标考核、小组答辩式考核	2	4	4
任务七：网络安全性故障分析与排除	网络安全性测试 网络健康检查	理解／运用	过程考核、目标考核、小组答辩式考核	2	8	4
合　计				16	38	28

4. 学习本课程达成目标

（1）专业能力目标：使学生能够对具体的网络故障现象进行分析，找出可能的故障原因，进而使用各种办法排除故障。

（2）职业能力目标：培养学生开拓创新的能力、良好的职业道德和岗位责任感、团队协作与沟通能力、自主学习能力、分析问题和解决问题的能力。

（3）工程能力目标：使学生可以熟悉网络工程的实施步骤，熟练进行文档的书写等。

任务一　典型网络故障案例分析

网络故障分析与排除是网络工程师在工作中必须具备的一项重要技能。

当今的信息化社会对计算机网络的依赖程度越来越高，但网络随时都可能发生故障，影响人们正常工作和生活。有些单位如电信、电子商务公司、游戏运营商等使用的网络一旦发生故障，若不能及时排除，就会产生很大的损失。这些单位一般会安装网络故障管理软件，通过软件来管理和排除网络的故障。

网络故障管理一般包括5方面内容：

（1）对网络进行监测，提前预知故障；

（2）发生故障后，找到故障发生的位置；

（3）解决故障；

（4）记录故障产生的原因，找到解决方法；

（5）故障分析预测。

下面通过一个典型的网络故障分析与排除案例来了解网络故障分析与排除的常见方法。

1.1　典型网络故障描述

某运营商为3G手机用户提供Web portal系统，在每天业务高峰时段（22:30～23:30）都会接到大量的用户投诉：网站访问不了！

在故障时段，Web服务器和各网络设备的进程、资源开销与平时相比并无异常；事后查看各设备的日志，也找不到故障的原因。

用户基本网络拓扑如图1-1所示。3G手机用户经过无线网络后，通过3G核心网访问Web portal系统，Web portal系统内部由多台服务器上联到一台交换机，通过Redware做负载均衡，再通过出口路由器和防火墙上联到3G核心网。

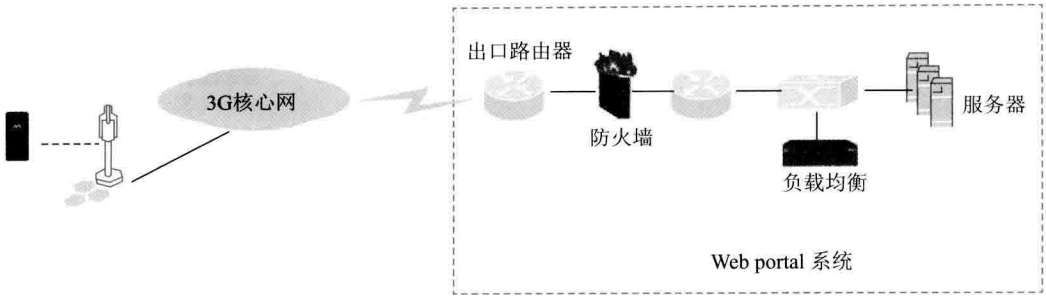


图 1-1　网络拓扑图

系统管理员一直尝试通过监控服务器和网络设备本身的状态、进程和日志来解决问题，但这种传统的网管方式存在以下几个难点。

（1）系统结构复杂：系统管理员没有 3G 核心网的管理权限，而 Web portal 系统内部需要监控的设备很多，工作量大，无法迅速定位是 Web portal 系统内部还是 3G 核心网端的问题；

（2）无法关联分析：无法对不同设备的监控数据进行有效的关联分析，无法拿出一个整体解决方案；

（3）缺乏故障回溯数据：各设备的日志系统内容有限，无法对故障进行回溯；

（4）监控网络设备时无法获取应用信息，监控应用服务器时无法获取网络信息。

1.2　典型网络故障分析

1.2.1　分析方案设计

1）分析目标

借助网络协议分析工具，能够从网络的角度分析应用信息，实现对 Web portal 系统端到端的性能监控；分析 Web portal 系统在故障时段与平时相比有何异常，最终定位有问题的设备节点。

2）分析设备部署

在 Web portal 的出口路由器上抓包分析，如图 1-2 所示，能够迅速地定位到底是 Web portal 系统内部问题还是 3G 核心网端的问题。

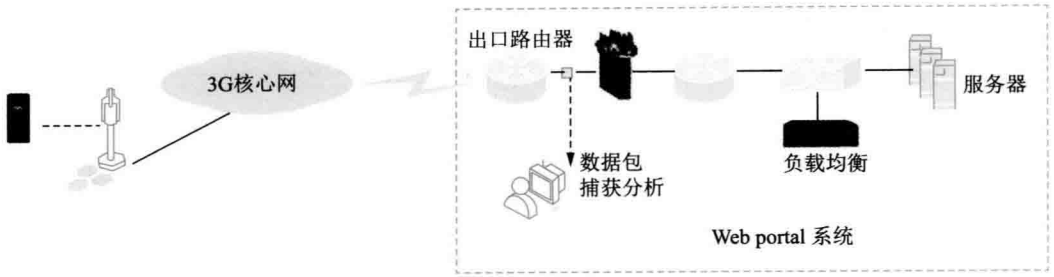


图 1-2　分析设备部署示意图

1.2.2　分析情况

1）基本流量分析

（1）流量负载分析。由图 1-3 可见，Web portal 系统的平均流量为 8.060 Mb/s，与平时相比并无异常，也没有发现异常爆发的广播和组播流量；平均包长为 718 507 B，并无异常。

流量统计	字节数	数据包数	利用率	每秒位	每秒包数
总流量	641.477 MB	936,160	0.806%	8.060 Mbps	1,406
广播流量	402 B	7	0.000%	0 bps	0
多播流量	0 B	0	0.000%	0 bps	0
平均包长					718.507 字节

图 1-3　流量统计

（2）流量突发分析。由图 1-4 可见，在故障时段并未发现明显的流量突发。

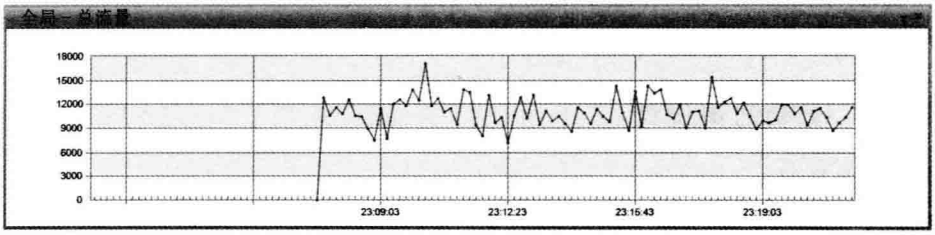


图 1-4　流量突发分析

（3）包尺寸分析。由图 1-5 可见，未发现异常。

数据包大小分布	字节数	数据包数	利用率	每秒位	每秒包数
<=64	1.473 MB	27,091	0.135%	13.520 Kbps	30
65-127	32.178 MB	411,093	4.133%	413.320 Kbps	627
128-255	2.537 MB	15,501	0.322%	32.232 Kbps	23
256-511	12.781 MB	36,513	1.492%	149.184 Kbps	51
512-1023	91.528 MB	111,376	12.162%	1.216 Mbps	176
1024-1517	441.915 MB	317,174	55.021%	5.502 Mbps	471
>=1518	59.066 MB	17,412	7.337%	733.736 Kbps	28

图 1-5　包尺寸分析

小结：通过流量的负载和突发分析，没有发现异常现象，排除了网络异常流量原因，可进一步分析网络层以上的信息。

2）TCP 连接分析

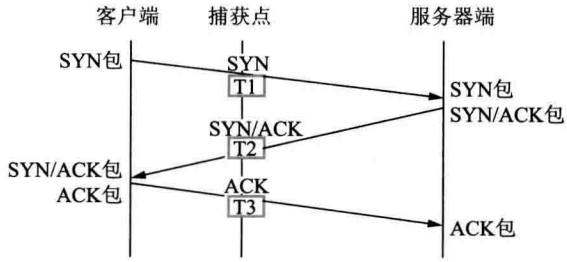
如图 1-6 所示，通过 TCP 统计信息发现：在故障时段总共有 135 个用户访问了该 Web 服务器，建立的 TCP 连接数为 5 235 个，而可疑的是在这些连接中有 2 213 个是通过 TCP 复位发送（RST）来结束连接，而不是通过正常的“四次握手”。

数据流统计	数量
物理会话	14
IP会话	135
TCP会话	5,235
UDP会话	3
TCP统计	**数量**
TCP同步发送	5,263
TCP同步确认发送	5,257
TCP结束连接发送	7,734
TCP复位发送	2,213

图 1-6　TCP 连接分析

3）通过“三次握手”分析网络时延技巧

如图 1-7 所示，业界通过“三次握手”来分析网络时延。



- T2-T1可以看作服务器端到捕获点的RTT
- T3-T2可以看作客户端到捕获点的RTT

图 1-7　“三次握手”

用户可以利用网络时延分析的技巧，为正常的 TCP 连接建立模型，以便在对异常连接分析时能够提供对比。

4）成功连接的分析模型

某成功的 TCP 连接时序图如图 1-8 所示。

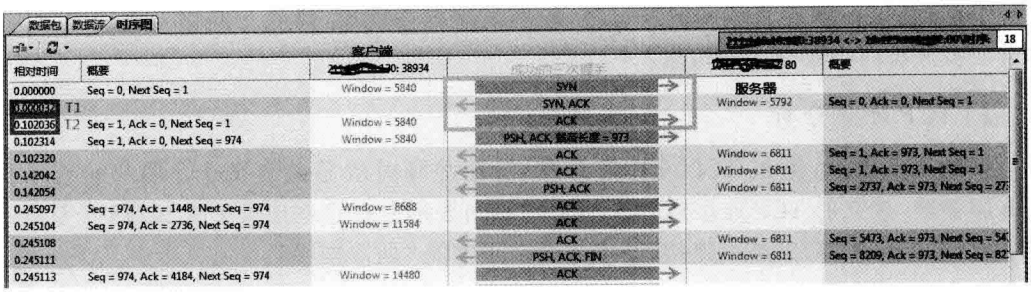


图 1-8　成功的 TCP 连接分析

由上图可见，该客户端通过“三次握手”与服务器建立连接，再进行数据传输。其中，第二个数据包“SYN，ACK”与第一个数据包“SYN”的时间差 T1 = 0.032 ms，可视为 Web portal 系统内部网络时延；第三个数据包“ACK”与第二个数据包“SYN，ACK”的时间差 T2 = 102.036 ms，可视为手机用户到 Web portal 系统的网络时延，包括了出口路由器、3G 核心网端的网络时延。

通过以上分析可以得出结论：正常情况下，Web portal 系统内部网络时延大致在 1 ms 以内，而 3G 核心网端（包含出口路由器）的网络时延为 100 ms 左右。

5）失败连接快速发现

失败的连接一般数据量较少，因此可以根据“字节”进行排序，能够快速定位到那些响应失败的连接，如图 1-9 所示。

图 1-9　根据字节排序示意图

6）失败原因分析

图 1-10 为某对失败连接的 TCP 连接时序图。从图中可以看出，该客户端向服务器发起了三次建立连接的请求，三次都以失败告终。服务器回应客户端同步请求的“SYN，ACK”数据包都是在 1 ms 内完成的，由此可见，Web portal 系统能够快速地响应客户端的连接请求，所以说系统并非连接失败的原因。

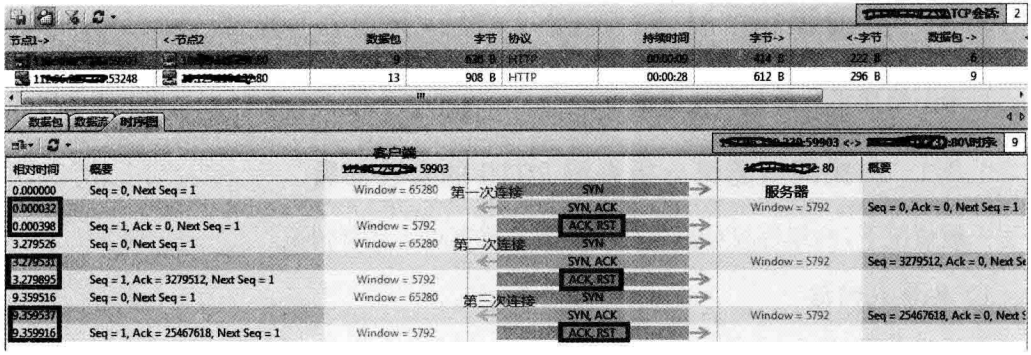


图 1-10　失败的 TCP 连接示意图

在服务器同步确认后，客户端反而发送“RST（TCP 复位发送）”数据包中断了连接，从而导致在 10 s 内三次连接都没有成功，从手机用户的角度来看就是“网页打不开”。在之前的 TCP 连接统计中，发现 5 235 个连接中的 2 213 个是这种连接失败，于是便有大量的用户投诉。

由于 RST 数据包来自客户端方向，就可以初步确定问题出自 Web portal 系统出口路由器或者 3G 核心网端。

进一步查看图 1-10，发现这三次 RST 网络时延分别为：

（1）（0. 398 － 0. 032）ms ＝ 0. 366 ms。

（2）（3. 279 895 － 3. 279 531）s ＝ 0. 000 364 s ＝ 0. 364 ms。

（3）（9. 359 916 － 9. 359 537）s ＝ 0. 000 379 s ＝ 0. 379 ms。

这三次 RST 网络时延全部都在 1 ms 以内，结合之前建立的分析模型，如果该 RST 是由 3G 核心网端发起的，响应时延应该在 100 ms 左右，而只有在本地网络的出口路由器的 RST 数据包能够在 1 ms 内到达数据分析点。

通过时延的判定，可以确认出口路由器就是导致本次故障的根源。

1.2.3　分析结论

Web portal 系统管理员将分析结果提交给出口路由器的厂家支持人员，厂家支持人员很快发现这是路由器的 Bug，最后通过升级路由器解决问题。

运营商、政府、金融企业及大型企业的网络业务系统结构复杂、网络节点及设备繁多，且业务量日益增长，系统管理员碰到的问题也会越来越复杂。当遇到问题时，很难迅速定位出问题的节点，通过传统的网管方式独立地分析每一台网络设备或服务器就像管中窥豹，往往消耗很多时间也解决不了问题。而通过网络协议分析工具，用“旁观”的方式、从网络角度对业务应用进行端到端的分析，就能更快速、更有效地定位出问题的节点。

1.3 相关知识

科来网络通讯分析系统使用技巧。

1.3.1 科来网络通讯分析系统 2010 的安装部署

一般情况下，网络协议分析软件的安装部署有以下几种情况。

1）共享式网络

使用集线器（Hub）作为网络中心交换设备的网络即共享式网络，集线器以共享模式工作在 OSI 层次的物理层。如果局域网的中心交换设备是集线器，就可将网络协议分析软件安装在局域网中的任意一台主机上，此时软件可以捕获整个网络中所有的数据通讯，如图 1-11 所示。

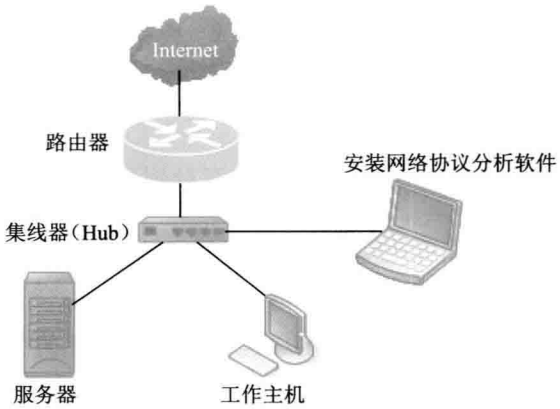


图 1-11 共享式网络安装部署图

2）具备镜像功能的交换式网络

使用交换机（Switch）作为网络中心交换设备的网络即交换式网络。交换机工作在 OSI 模型的数据链接层，它的各端口之间能有效分隔冲突域，由交换机连接的网络会将整个网络分隔成很多小的网域。

如果网络中的交换机具备镜像功能，可在交换机上配置好端口镜像，再将网络协议分析软件安装在连接镜像端口的主机上，此时软件可以捕获整个网络中所有的数据通讯，安装简图如图 1-12 所示。

3）不具备镜像功能的交换式网络

一些简易的交换机可能并不具备镜像功能，不能通过端口镜像实现网络的监控分