



Troubleshooting
Campus Networks

网络专业人员书库

园区网 故障排除

Priscilla Oppenheimer
Joseph Bardwell

著

刘耀明 王海峰 等译



机械工业出版社
China Machine Press

网络专业人员书库

园区网故障排除

(美) Priscilla Oppenheimer 著
Joseph Bardwell

刘耀明 王海峰 等译



机械工业出版社
China Machine Press

本书是一本有关园区网络故障分析与排除方法的实用参考大全。从讲述相关的网络基础知识和故障分析方法入手,在此基础上结合实际的网络分析工具及实践经验讲述对各种网络故障的识别和排除方法。本书不仅能够直接指导网络故障的分析和排除,而且能够帮助读者掌握网络的工作方式、故障原因、现象和分析方法。本书既是实用的故障排除手册,又是讲述网络协议的理论书籍,确实是本不可多得的好书。

本书适合于网络工程师、管理员和技术人员,同时也适合于认证报考人员,特别是准备报考Cisco认证以及网络分析专家认证的读者。

Priscilla Oppenheimer and Joseph Bardwell: Troubleshooting Campus Networks (0-471-21013-7)
Authorized translation from the English language edition published by John Wiley & sons, Inc.
Copyright © 2002 by Priscilla Oppenheimer and Joseph Bardwell.
All rights reserved.

本书中文简体字版由约翰-威利父子公司授权机械工业出版社独家出版。未经出版者书面许可,不得以任何方式复制或抄袭本书内容。

版权所有,侵权必究。

本书版权登记号:图字:01-2002-4818

图书在版编目(CIP)数据

园区网故障排除/(美)奥本海默(Oppenheimer, P.), (美)巴德维尔(Bardwell, J.)
著;刘耀明等译.-北京:机械工业出版社,2003.3

(网络专业人员书库)

书名原文: Troubleshooting Campus Networks

ISBN 7-111-11526-0

I. 园… II. ①奥… ②巴… ③刘… III. 局部网络-故障修复 IV. TP393.1

中国版本图书馆CIP数据核字(2003)第001677号

机械工业出版社(北京市西城区百万庄大街22号 邮政编码 100037)

责任编辑:李炎

北京第二外国语学院印刷厂印刷·新华书店北京发行所发行

2003年3月第1版第1次印刷

787mm×1092mm 1/16·29.5印张

印数:0 001-4 000册

定价:49.00元

凡购本书,如有倒页、脱页、缺页,由本社发行部调换

译者序

本书讲述的园区网是指一个企业、政府部门、学校等所属的网络，通常跨越多个建筑物，并涉及多种网络技术，例如有线和无线网络技术。一句话，园区网也正是我们自己管理的网络。

本书是本针对园区网故障排除的书，并不是解决一个简单的局域网中电缆是否断开的问题，相反，本书关心的是如何为一个有几十个、几百个，甚至几千个用户的复杂互连网络排除故障。因而它是一本为网络工程师、管理员和技术人员排忧解难的参考书。

本书包括了园区网可能涉及的所有网络技术，包括以太网、无线局域网、生成树协议的故障排除与分析，园区IP网络和IP路由协议的故障排除与分析，TCP、UDP以及网络上层的故障排除与分析，以及对Novell Netware的IPX、Apple的AppleTalk和Windows连网的故障排除，此外还包括与LAN工程师有关的WAN的故障排除方法。涉及面之广是同类书籍难以企及的。

本书的最大特点是理论与实践相结合。书中从讲述相关的网络基本知识和故障分析的方法入手，在此基础上结合实际的网络分析工具及实践经验讲述各种网络故障的现象的识别和排除方法。该书不仅能够直接指导网络故障的分析和排除，而且还使得读者对网络的工作方式、故障的原因、现象和分析方法有了深刻、清晰的认识。这使得本书既是本实用的故障排除手册，又是本讲述网络协议的理论书籍，确实是不可多得的好书。

本书的两位作者均是网络设计和故障排除方面的专家，书中的知识基于其多年对真实的、各种各样复杂网络的分析。书中的讲述思路清晰，语言表达明确，并且还具有丰富的示例，安排具有条理性，易于理解和掌握。使人读完有豁然开朗的感觉。

全书由刘耀明、王海峰等进行翻译，参与翻译工作的还有程尔红、邵玉珍、王冉、王欣、方翎、牛飞宇、肖杰谦、唐立卫、吴新鸣、张小冰、李海涛、文静、李祥、刘海宁、丁镇兴、万仁伟、刘晶晶、方平、邓盛骋、陈小冲、郭龙永、王治、李鹏君、常欣、李桦、时丁、迟可可、付睿等。本书的出版是集体劳动的结晶，前导工作室全体工作人员共同完成了本书的录排、校对等工作。由于时间仓促，且译者的水平有限，在翻译过程中难免会出现一些错误，请读者批评指正。

译者

2002年10月

目 录

译者序

第1章 引言	1
1.1 为什么写作本书	1
1.2 读者范围	2
1.2.1 Cisco认证	3
1.2.2 NAX认证程序	3
1.3 本书的组织	4
1.4 网站	4
第2章 故障排除方法	5
2.1 当今网络环境的挑战	5
2.2 使用系统的故障排除方法	6
2.2.1 将OSI模型用于故障排除	7
2.2.2 通用问题解决模型	9
2.2.3 Cisco的故障排除方法	10
2.3 主动故障排除与定基准	12
2.3.1 用文档记录网络	13
2.3.2 协议分析	17
2.3.3 理解网络流量	20
2.3.4 统计性监控	25
2.3.5 模拟与建模	27
2.4 主动与反应式故障排除	27
2.4.1 用于物理层故障排除的工具	27
2.4.2 用于物理层之上的故障排除工具	28
2.4.3 其他的故障排除命令	34
2.5 小结	38
第3章 以太网的故障排除与分析	41
3.1 以太网历史和结构	41
3.2 以太网物理层	43
3.2.1 协议分析仪与以太网介质	45
3.2.2 信号编码	45
3.2.3 时钟同步	48
3.3 以太网MAC层	48

3.3.1 带有冲突检测的载波侦听多路访问	49
3.3.2 冲突域	50
3.3.3 全双工操作	52
3.3.4 增强Gigabit以太网的以太网 媒体访问控制	56
3.4 以太网帧	57
3.4.1 以太网II或IEEE 802.3帧头部的域	58
3.4.2 以太网帧尺寸	64
3.5 收集与理解以太网性能数据	68
3.5.1 远程监控	68
3.5.2 Cisco的show interface ethernet命令	68
3.5.3 帧讹误	73
3.5.4 广播与多播速率	74
3.6 小结	75
第4章 IEEE 802.11无线网的故障排除 与分析	77
4.1 本章的范围与深度	77
4.2 无线网络入门	79
4.2.1 无线网络的基本原理	79
4.2.2 什么是无线网络	80
4.2.3 无线网络设计的挑战	80
4.2.4 无线网络里的协议分析	82
4.3 无线网络技术	82
4.3.1 窄带无线电传输	82
4.3.2 跳频扩频 (FHSS)	82
4.3.3 直序扩频 (DSSS)	83
4.3.4 红外线 (IR)	83
4.3.5 蓝牙 (Bluetooth) 和个人 局域网 (PAN)	83
4.3.6 其他的无线标准	84
4.4 WLAN环境的组成	84
4.4.1 基本服务组 (BSS)	85

4.4.2 扩展服务组 (ESS)	85	4.12 WLAN故障排除的场地调查技术	114
4.4.3 计时同步功能 (TSF)	87	4.12.1 估计有效范围	114
4.5 站点初始化行为	87	4.12.2 AP位置的考虑	114
4.5.1 信道选择	88	4.13 网络设计问题的故障排除	115
4.5.2 验证	89	4.13.1 大数据包与冲突	116
4.5.3 关联到BSS	90	4.13.2 同时存在的大量用户与冲突	116
4.5.4 初始化过程的分析	90	4.13.3 配置设置	117
4.6 802.11介质访问控制	91	4.14 理解802.11数据包的解码	118
4.6.1 帧间间隔	91	4.15 小结	120
4.6.2 网络分配向量 (NAV)	92	第5章 生成树协议的故障排除与分析	121
4.6.3 请求发送/清除发送机制	93	5.1 诗歌的配合	121
4.6.4 802.11环境摘要	93	5.2 透明桥接	122
4.7 射频传输	94	5.2.1 桥接任务	125
4.7.1 频率分配	95	5.2.2 桥接回路	125
4.7.2 RF工程学中的数学	95	5.3 STP行为	128
4.7.3 增益或损耗的规范	99	5.3.1 网桥协议数据单元	128
4.7.4 分贝和分贝毫瓦量度的应用	101	5.3.2 STP收敛	133
4.8 影响802.11传输的环境因素	104	5.4 STP的主动故障排除	140
4.8.1 反射	104	5.4.1 记录交换网络	141
4.8.2 吸收	104	5.4.2 监控STP	141
4.8.3 折射	104	5.5 STP的反应式故障排除	144
4.8.4 衍射	105	5.5.1 单向连通性	146
4.9 场地调查的故障排除	105	5.5.2 减少在Cisco交换机端口上的 启动延迟	146
4.9.1 无障碍信道功率估计	106	5.6 优化生成树的实现	149
4.9.2 RF信号传输的限制	106	5.6.1 上行链路加速与骨干加速	149
4.9.3 Shannon (仙农) 信道容量定理	106	5.6.2 负载共享	150
4.9.4 Gaussian (高斯) 噪音	107	5.6.3 明确地选择根网桥	151
4.9.5 多路传输	107	5.7 小结	154
4.9.6 真实世界的路径损耗	108	第6章 VLAN的故障排除与分析	155
4.9.7 最大覆盖的天线定位技术	108	6.1 VLAN框架	155
4.9.8 信号强度的协议分析仪报告	109	6.1.1 VLAN定义	156
4.10 确定供应商规范的意义	110	6.1.2 VLAN设计	156
4.10.1 输出功率	111	6.1.3 互连交换机	157
4.10.2 接收器灵敏度	111	6.1.4 在VLAN环境中的协议分析	158
4.11 环境噪音的影响	111	6.1.5 VLAN成员	158
4.11.1 网络利用率	113	6.2 配置VLAN	159
4.11.2 信号强度、坏数据包和网络利用率	113		

6.2.1 分配一个VTP域	160	8.3.2 使用多种路由协议	239
6.2.2 生成一个VLAN	161	8.4 IP路由故障排除的总的意见	241
6.2.3 给VLAN分配端口	161	8.5 协议分析示例中使用的示例网络	241
6.2.4 验证VLAN的配置	162	8.6 路由信息协议 (RIP)	242
6.3 VLAN中继	164	8.6.1 RIP协议分析	243
6.3.1 ISL与802.1Q的比较	165	8.6.2 RIP计时器	246
6.3.2 路由器和VLAN中继	166	8.6.3 RIPv2	246
6.3.3 Cisco的交换机间链路	169	8.6.4 RIP使用的Cisco显示和调试命令	247
6.3.4 IEEE 802.1Q	173	8.7 内部网关路由协议 (IGRP)	248
6.4 Per-VLAN生成树	175	8.7.1 IGRP协议分析	249
6.5 Cisco VTP的故障排除	178	8.7.2 IGRP触发更新和毒性逆转	251
6.5.1 VTP名字与口令	178	8.7.3 Cisco为IGRP使用的显示和 调试命令	253
6.5.2 VTP剪枝	179	8.8 增强型IGRP (EIGRP)	254
6.5.3 分析与监控VTP	180	8.8.1 EIGRP协议分析	255
6.6 小结	184	8.8.2 EIGRP使用的Cisco显示和调试命令	261
第7章 园区IP网络的故障排除与分析	187	8.9 开放最短路径优先 (OSPF)	262
7.1 TCP/IP的历史	187	8.9.1 OSPF网络结构	263
7.2 TCP/IP协议栈	188	8.9.2 OSPF协议分析	264
7.3 网际协议 (IP)	189	8.9.3 为OSPF使用的Cisco显示和 调试命令	270
7.4 IP编址	204	8.10 边界网关协议 (BGP)	272
7.4.1 将前缀边界右移 (子网化)	205	8.10.1 BGP协议分析	272
7.4.2 将前缀边界左移 (超网化)	209	8.10.2 BGP使用的Cisco显示和调试命令	272
7.4.3 地址解析协议 (ARP)	211	8.11 小结	275
7.4.4 动态主机配置协议	213	第9章 TCP、UDP和上层IP协议的 故障排除与分析	277
7.4.5 私有IP地址	219	9.1 上层IP协议分析	277
7.4.6 IP多播地址	220	9.2 传输控制协议 (TCP)	278
7.5 IPv6	223	9.3 用户数据报协议 (UDP)	294
7.5.1 IPv6协议分析	224	9.4 应用层协议	295
7.5.2 IPv6的自动配置	225	9.4.1 域名系统	296
7.6 小结	226	9.4.2 服务定位协议	301
第8章 园区网IP路由协议故障排除与分析	229	9.4.3 超文本传输协议	303
8.1 主机路由	229	9.4.4 文件传输协议	307
8.1.1 热备份路由器协议	231	9.4.5 电子邮件协议	315
8.1.2 主机路由监控与故障排除	232	9.5 小结	317
8.2 静态路由和默认路由	233		
8.3 动态路由	234		
8.3.1 距离向量和链路状态路由	236		

第10章 园区IPX网络故障排除与分析319

10.1 Novell NetWare思想319

10.1.1 IPX编址321

10.1.2 IPX数据包322

10.1.3 NetWare核心协议327

10.1.4 看门狗欺骗330

10.2 IPX服务通告协议331

10.2.1 SAP过滤器335

10.2.2 获得最近服务器335

10.3 IPX路由337

10.3.1 IPX路由信息协议338

10.3.2 IPX使用的增强内部网关路由协议340

10.3.3 NetWare链路服务协议343

10.4 过渡中的IPX网络345

10.5 IPX故障排除349

10.5.1 应用协议分析仪349

10.5.2 IPX ping和trace350

10.5.3 显示IPX路由350

10.5.4 显示IPX服务器351

10.5.5 显示IPX接口351

10.5.6 显示IPX流量352

10.5.7 显示IPX EIGRP353

10.5.8 显示IPX NLSP353

10.5.9 调试IPX包354

10.5.10 调试IPX路由354

10.5.11 调试IPX SAP354

10.6 小结354

第11章 园区AppleTalk网络故障

排除与分析357

11.1 AppleTalk思想357

11.1.1 AppleTalk体系结构358

11.1.2 AppleTalk编址361

11.1.3 数据报传输协议 (DDP)365

11.1.4 名称绑定协议 (NBP)367

11.1.5 Apple档案协议 (AFP)368

11.2 AppleTalk路由372

11.2.1 路由表维护协议 (RTMP)372

11.2.2 区域信息协议 (ZIP)376

11.2.3 AppleTalk基于更新的
路由协议 (AURP)377

11.2.4 AppleTalk中使用的EIGRP379

11.3 控制AppleTalk通信384

11.3.1 静态路由384

11.3.2 AppleTalk访问列表385

11.4 过渡中的Macintosh网络386

11.4.1 Mac OS X386

11.4.2 Mac OS X Server网络管理工具390

11.5 AppleTalk故障排除390

11.5.1 AppleTalk ping (Echo)391

11.5.2 Cisco AppleTalk NBP测试392

11.5.3 为AppleTalk使用的Cisco IOS
显示命令39311.5.4 为AppleTalk使用的Cisco IOS
调试命令394

11.6 小结395

第12章 Windows连网故障排除与分析397

12.1 Windows连网概念397

12.2 Windows连网的NetBIOS基础398

12.2.1 NetBIOS的历史398

12.2.2 NetBIOS函数调用399

12.2.3 NetBIOS的重要性399

12.2.4 NetBIOS不同实现的一致性400

12.2.5 NetBIOS命名传统401

12.2.6 NetBIOS不同实现之间的差异405

12.2.7 NetBIOS名称管理机制413

12.2.8 NetBIOS数据移动417

12.3 工作组模型和域模型421

12.3.1 工作组验证过程分析421

12.3.2 Windows NT域模型中的验证423

12.3.3 控制复制的NT注册表参数424

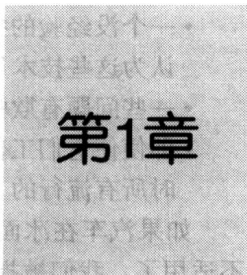
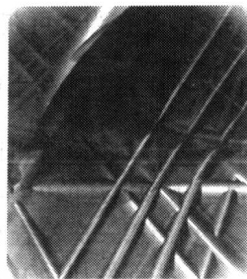
12.3.4 Browse (浏览) 协议424

12.4 Windows 2000模型427

12.5 小结428

第13章 为LAN工程师提供的

WAN故障排除	429	13.2.1 租赁线路	437
13.1 WAN思想	429	13.2.2 高级数据链路控制 (HDLC)	437
13.1.1 WAN标准	430	13.2.3 点对点协议 (PPP)	439
13.1.2 WAN组件	431	13.2.4 帧中继	441
13.1.3 端到端WAN的思考	432	13.2.5 综合业务数字网	446
13.1.4 从路由器接口角度对WAN 进行故障排除	434	13.2.6 异步传输模式 (ATM)	452
13.1.5 提供WAN容量	435	13.3 本章和本书总结	456
13.2 WAN技术	436	参考文档	459



引言

第1章

世纪之交，计算机应用进入了一个激动人心的发展时代。计算机网络技术与商业、教育、政府机构，甚至是私人家庭相融合的创新方式，已经取代实现计算机系统互相对话的基础工程而成为新的焦点。可是，当系统不能互相对话的时候，人们要说的第一件事情就是：“网络出问题了！”本书讨论了处理这些问题的方法，并解释了网络实际上是如何工作的。详细地描述了用于分析、诊断和修正错误的Cisco和行业标准的故障排除方法。本书也涉及了使用协议分析仪——例如WildPackets的EtherPeek和AiroPeek产品——来识别和隔离发生故障的网络行为的技术。

1.1 为什么写作本书

我们写作本书是为技术人员提供技术性的信息，他们能将这些信息用于生产环境、日常的网络配置、支持和故障排除。在20世纪80年代和90年代，我曾和许多计算机界的专家一起工作，有一些经常来往，有一些只是偶尔碰到。专家是什么人很显而易见，因为他们都知道网络是如何真正工作的。这些人从不说“TCIP”，他们都知道网桥是在第二层起作用，而路由器是在第三层。他们还知道许多其他的事情。

然而，在计算机业界的许多人并不是专家。他们认为他们知道许多事情，但是他们缺乏基础知识。在缺乏正规计算机网络教育，并且被迫去使用、实现、支持和维护复杂系统的情况下，他们做出了许多错误的结论，并且有时候又将这些错误传授给他们的同伴。

本书集中在许多经常被误解的技术和工程问题上。在阅读这些内容的时候，可能会遇到一些概念，这些概念与别人曾告诉过你的相矛盾。我们试图以书面形式记下一些核心的信息，它们对于成功的故障排除和协议分析是至关重要的。这些信息是来自著名的标准化组织的文档为基础的，这些组织包括Internet Engineering Task Force (Internet工程任务组, IETF) 和 Institute of Electrical and Electronics Engineers (电气与电子工程师协会, IEEE)。更重要的是，这些信息是基于对现实世界中各种不同的、复杂网络的多年分析。本书具有以协议层为中心的

特点，这在当今可获得的大量的技术文献上是找不到的。

保证不生锈、操作出错或收进垃圾

计算机网络和旧汽车较相像，而且，就像到了一个旧车市场一样，必须小心，不要拿到次品。下面描述的内容可以同时适用于网络和旧汽车：

- 当第一次检查它们的时候，它们可能会看起来很好，但是当最需要它们的时候，它们的一些部件却会失灵。
- 一个没经验的技术员能胡乱地修复它们，掩盖明显的问题，这导致了错误的结论，人们会认为这些技术员是专家。
- 一些问题有欺骗性的症状，只有一个真正的专家才能辨别真正的原因。
- 即使使它们工作的基本系统和技术好多年了都没有变化，但是它们都结合了在它们被设计时所有流行的工程模式。

如果汽车在冰面上打滑，我们被教导要踩住刹车，但在使用防锁式的刹车时，这个规则就不适用了。我们被提醒要采用手动刹车，但当汽车有前轮驱动时，这个又不适用了。自动化技术的变革完全改变了我们对驾车的一些基本方面的思考方式。

我们曾学过，有三种用于惟一识别主机的Internet Protocol（网际协议，IP）地址类（A、B和C）。但是当出现无类别编址时，这个就不适用了。我们经常听说，在Ethernet（以太网）上网络的利用率不应该超过40%，然而，对全双工以太网连接，这一点就不再正确了。计算机网络技术的革新改变了我们对于设计和故障排除基本方法的思考方式。

无论是检查一个旧汽车，还是给一个计算机网络排除故障，都要注意隐藏的问题、来自无经验帮助者的建议、易混淆的症状，以及设计的革新所带来的术语和功能上的改变。

1.2 读者范围

本书的读者是管理Cisco以及多供应商园区网的网络工程师、管理员和技术人员。园区网是指跨越多个建筑，并由连接客户和服务器的有线和无线技术组成的网络。虽然单词campus经常指的是学院或大学，并且这本书完全适合学院网络管理员的需要，但本书并不只是针对学院网络管理员，它也适合管理基于下列技术的园区网的任何一个管理员：

- 1) 10 Mbps、100 Mbps和1000 Mbps以太网连接。
- 2) 802.11无线通信。
- 3) 单个网络内部机器之间的交换连接。
- 4) 将网状拓扑结构的网络进行分隔的虚拟局域网（Virtual Local Area Network，VLAN）。
- 5) 在园区网环境中，网络之间的路由连接。
- 6) 园区网之间的广域网（Wide Area Network，WAN）连接（虽然本书集中讨论局域网，但也提供了广域网的信息）。
- 7) 传输控制协议（TCP）/网际协议（IP）、AppleTalk、Novell NetWare和Windows网络协议族的高层协议。

本书并不是解决一个简单的局域网中电缆是否断开的问题，而是如何为一个有几十个、几

百个,甚至几千个用户的复杂互连网络排除故障。本书写给管理和配置互连网络设备的网络工程师。虽然没有涉及工作站或服务器配置,但书里的一些信息会对台式机的技术支持人员和服务器管理员有所帮助。

最后,这本书也是写给认证报考人员的,特别是Cisco认证,以及由WildPackets Academy发起的与供应商无关的网络分析专家(NAX)认证程序。

1.2.1 Cisco认证

在Cisco领域,本书重点讨论CCNP(Cisco Certified Network Professional, Cisco认证网络专业人员)认证和CCIE(Cisco Certified Internetwork Expert, Cisco认证互连网络专家)认证。

CCNP认证表明掌握了对于网络的高级或技师级的知识。有了CCNP认证就等于向老板表明,您能为一个有100到500个节点的机构安装、配置、操作和故障排除多协议的局域网、广域网和拨号访问服务。要取得CCNP身份,必须通过五个测试。本书重点讨论最高级的测试——技术支持测试。Cisco中关于技术支持的所有主题列表本书都会涉及。

本书也适用于CCIE报考者。要取得CCIE身份,必须同时通过资格笔试考试和动手实验考试。本书会在下述的CCIE路由与交换资格考试主题上提供帮助。

- Cisco设备操作
- 普通网络理论
- 局域网编址
- 10 Mbps、100 Mbps和1000 Mbps以太网封装、介质访问控制、拓扑结构、错误和限制
- 逻辑链路控制(LLC) 802.2
- 桥接和局域网交换
- TCP/IP
- IP路由协议
- 台式机协议,包括Novell NetWare和Windows networking
- 性能管理
- 广域网编址、信令和帧

因为本书集中介绍故障排除,它也能帮你准备CCIE实验测试。既然Cisco已经将实验测试从两天改为一天,应用高效的故障排除方法比以前更为重要了。本书教授的方法会帮助你隔离和修正问题,这些问题在你执行CCIE实验测试人员需要的复杂任务时会出现在实验网络上。

关于Cisco认证程序更多的信息请参考www.cisco.com/warp/public/10/wwtraining。

1.2.2 NAX认证程序

NAX认证程序是由WildPackets Academy发起的一个工业标准的、与供应商无关的程序。从1990年开始,WildPackets一直在开发用户友好的、花费不大的工具,用于设计、维护、故障排除和优化计算机网络。WildPackets的产品包括用于以太网络分析的EtherPeek和用于802.11无线网络分析的AiroPeek。这两个产品都包括用于自动问题分析的NetSense实时专家系统技术。TokenPeek分析仪符合802.5令牌环用户的需求。

为了通过NAX认证测试, 报考者可以使用WildPackets或业界认可的其他协议分析仪。报考者下载一个分析仪追踪文件并回答实际的网络问题。这个考试测试报考者对协议的理解, 以及使用协议分析技术分析典型网络问题的能力。完成NAX认证包括三个步骤:

- 1) Applied Analysis Technician (应用分析技术员, AATech) 认证。
- 2) Protocol Analyzer Specialist (协议分析仪专家, PAS) 认证。
- 3) NAX认证。

这些认证需要通过知识考试和实践技术考试。知识考试需要报考者展示对于协议分析的概念、开放系统互连(OSI)参考模型, 以及在这个模型的不同层次上起作用的协议的完全理解。实践技术考试需要报考者展示对于协议分析仪的精通程度。要完成NAX认证, 报考者也要写一篇专题报告, 主题是从WildPackets Academy批准的主题列表里选出来的。除了提供许多其他工业认证中协议相关方面的完整的基础知识外, 本书也会为NAX认证程序中所有的考试知识提供帮助。

要得到关于NAX认证程序的完整的细节, 请到www.nax2000.com下载Pre-Test Study Guide (考前学习指南) 和Test-Taking Instructions (参加考试指导) 文档。

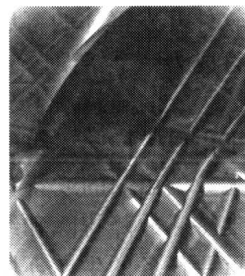
1.3 本书的组织

本书采用自下而上的组织方式。首先介绍故障排除方法的要点, 然后开始介绍OSI参考模型, 从物理和数据链路层开始, 到高层结束。章节组织如下所示:

- 第2章涉及问题隔离的方法和工具, 包括Cisco和行业标准的故障排除程序, 以及使用WildPackets或其他分析仪进行的协议分析。还涉及了OSI参考模型和ICMP (Internet Control Message Protocol, Internet控制消息协议)。
- 第3、4章解释了以太网和802.11无线网络是如何工作的, 以及当它们不工作时如何排除故障。第3章也涉及了802.2 LLC。
- 第5、6章仍然介绍数据链路层, 涉及了用于桥接和交换网络的Spanning Tree Protocol (生成树协议), 以及虚拟局域网的配置和故障排除。
- 第7到8章讲述网络层及其以上各层, 涉及IP编址、IP路由协议、TCP的详细分析和上层TCP/IP协议的概述。
- 第9到12章讲述对于最流行的台式机协议——Novell NetWare、AppleTalk和Windows连网的故障排除和协议分析。
- 第13章讨论了广域网技术, 并从一个局域网网络工程师的角度讨论了它的故障排除。

1.4 网站

我们已经建立了一个网站, 希望你能经常访问它, 当有关于故障排除的新的信息时, 网站就会有更新。它也包含到实际测试的连接, 以帮助认证考试的学习, 还有一些练习的建议, 你可以在实验网络上尝试, 以增强故障排除的熟练程度。参考手册的网站地址是www.troubleshootingnetworks.com。



第2章

故障排除方法

计算机网络并不是新的东西。各种机构将计算机连接起来，用于发布信息，交换消息，备份数据，以及共享外围设备，如打印机和调制解调器，已经有许多年了。然而，与早先的网络相比，现在的网络是复杂的，也是不可或缺的。如今的应用程序包括控制空间站机器人、为外科医生提供医学图像、出售产品以及管理生产资源。用户基于他们的网络进行日常的操作、研究开发和制定策略。作为一个网络技术支持工程师，可能意识到了对于应用支持和可靠性的不断增长的需求。本章将讲述用于解决网络问题的实践方法，而不是去考虑新的应用程序或高层服务。

2.1 当今网络环境的挑战

在20世纪80年代，一个由大约20个工作站组成的基于大型个人电脑（PC）的网络被连接起来，这样，用户就能共享打印机和高容量的硬盘（可能就5M大）。一般情况下，网络管理员是一些比较聪明的、并愿意去修补台式电脑的人。一个专职的负责维护网络的技术支持工程师在当时只是幻想。

在20世纪90年代早期，网络发生了巨大的变化。双绞线电缆取代了老式的同轴以太网电缆。交换机开始取代网络集线器，所有大型的网络已经有了专门的技术支持人员队伍。少量用户共享一个磁盘驱动器的单个文件服务器逐渐演化为一个园区网络，它将多个部门和多个建筑连接成一个多协议和多供应商的资源，这个资源对于生产目标是至关重要的。然而，全球的连网以及声音、图像与数据的集成在当时就和幻想差不多。

在20世纪90年代中期，随着万维网（WWW）的产生，进入了一个新的网络时代。地理上分散的园区网络的连接选择得到了发展，提供对雇员、商业伙伴和客户的访问的大型互连网络开始变得普及。90年代的最后几年集中在Y2K（2000年）问题的解决上。在2000年1月1日，当几乎所有预言中的Y2K问题都没有真正发生时，没有启动这项工作的人都自鸣得意地笑了，然而

软件开发群体的幕后英雄们、精疲力尽的网络支持工程师们知道是他们的努力才使得毁灭的预言成为一个错误。

Y2K问题来了又去了。网络产业加速了它的发展,呈现白热状态。如今,全球广域网连接了由以太网与无线设备、真实与虚拟局域网、交换机和路由器、Windows与UNIX服务器和其他无数的由旧的或新的技术组成的园区网,它们必须无缝地、可靠地一起工作。负责设计、实现、支持、故障排除和维修最新网络的人面临着各种层次的挑战。我们必须在维护和故障排除一个重要任务的生产环境的同时,紧跟加速发展的技术和商业变化的步伐。而那些生产环境可能是建立在20或30年前开发的技术的基础上的。

在20世纪60年代和70年代发明的核心工程技术现在仍在使用。以太网版本II,是70年代的以太网版本I的直接进化品,在1982年被标准化。以太网II的框架仍然是如今大多数IP园区网络中典型使用的。IP自从20多年前发明以来没有太大的变化。当然它做了一些修补,新的服务如动态主机配置协议(DHCP)增强了它的功能。聚集和分隔机器到一个可到达的位置的问题,以一种协议初建时相同的方式,给园区网的设计者、工程师和管理员提出了挑战。以太网和IP是与我们共处了15、20或30年的许多实现工具中的两个。如今的网络专家必须对已成为现代网络基础的核心工程技术有完全的理解。

本质上,如今所有的园区网络都实现TCP/IP协议,但许多大型的网络也混合使用AppleTalk和Novell NetWare。在商业和教育环境中,台式电脑典型地基于Microsoft Windows或Mac OS,当比尔·盖茨以不可抗拒的力量驱动这个行业时,UNIX/Linux不得不一直提升它们产品的优势。另一方面,服务器基于Microsoft Windows和UNIX/Linux,以及Mac OS。

将所有这些东西结合在一起需要开发一个牢固的、高效的故障排除方法。“跌倒了再交换”、希望问题消失是不行的(“跌倒了再交换”是在美国常用的一个短语,意思是直到累得跌倒在地上时才替换网络组件的一种故障排除方法)。当走向一个更快的、更加自动化的和更加复杂的未来时,一个好的方法的重要性会变得更加明显。

2.2 使用系统的故障排除方法

在其领域里已经成为专家的网络工程师在排除故障时使用系统的处理过程。这些专家也许不能解释这些过程,但在问题出现时他们能凭直觉使用它。其他的专家宣讲他们的系统方法,有时候甚至达到失去理智地批评工作得很好的不同方法的程度。所有的专家方法,无论是否描述得很准确,都能归结为一套排除问题起因的逻辑步骤。专家使用那些合理的、高效的、实用的和适合大多数情况的方法。在作改动之前,改动之时,改动之后,他们将网络结构和设备配置记录在文档中。在排除故障以确保问题被修复,并且没有新的问题被引入时,他们会测试他们所作的改动。

系统的故障排除方法与网络领域里的新手使用的方法会有显著的不同。新手经常会使用没有计划、没有文档、没有测试的随机的方法。他们的方法在网络用户需要的时间段里经常无法找到真正的问题,他们的努力经常使情况有所变化,但仍然是坏的。另一方面,一个专家能很快地缩小可能性、隔离问题、修正问题并在一个合理的短时间内测试所作的修改。

一个专家会有意或无意地定义下列的术语,并使用它们以提高效率。以下定义基于在线的

Merriam-Webster's Collegiate Dictionary中的定义：

Component (组件) 整体的一个要素部分或组成部分。

Function (功能) 一个事物特别适合或使用的行为。

System (系统) 一组经常交互或互相依赖地构成一个完整整体的组件。

Troubleshoot (故障排除) 在机器和技术设备上定位故障并作修理；预见和解决问题。

Upgrade (升级) 提升质量。

系统，包括网络系统，是由相关的组件组成的。系统和组件能够通过它们执行什么样的功能来描述。故障排除和升级系统要考虑系统的组件、它们的功能以及它们是如何影响整个系统的。任何组件的故障会导致整个系统的失效。网络领域的许多新手可能没有考虑这些基本的概念。缺少对于系统、组件及其功能中任何一个的理解，新手在故障排除时会非常困难。走到下一步——从考虑系统到使用系统的方法——对于新手来说也是困难的，特别是现在网络已经变得非常复杂、网络组件之间的关联也不像以前那样清晰的情况下。

区别专家和新手的一个因素是专家研究过协议是如何工作的。专家使用协议分析仪研究帧的结构、协议行为、连接建立、可靠性机制、路由协议等等。然而，学会所有的协议以及它们是如何结合在一起，是不可能的。协议设计工程师引入一个新的协议，以及引入使用旧协议的新方法是经常的事。在网络工程师领会一个协议时，新的协议或使用旧协议的新方法会使问题变得混乱。在当今网络协议疯狂混合和匹配的世界里，从高层来考虑网络行为和故障排除是必要的。

2.2.1 将OSI模型用于故障排除

用于故障排除和理解协议的一个高效的方法是使用国际标准化组织（ISO）的开放系统互连（OSI）参考模型作为指南。图2-1显示了OSI模型。

OSI模型有七层。每一层与运行在另一个系统上的对等层通信。然而，各层并不是直接做这件事情。除了最底层，各层都将它们的数据传给下一层以做进一步的处理。每一层为上一层提供服务。表2-1描述了模型中每一层提供的服务。

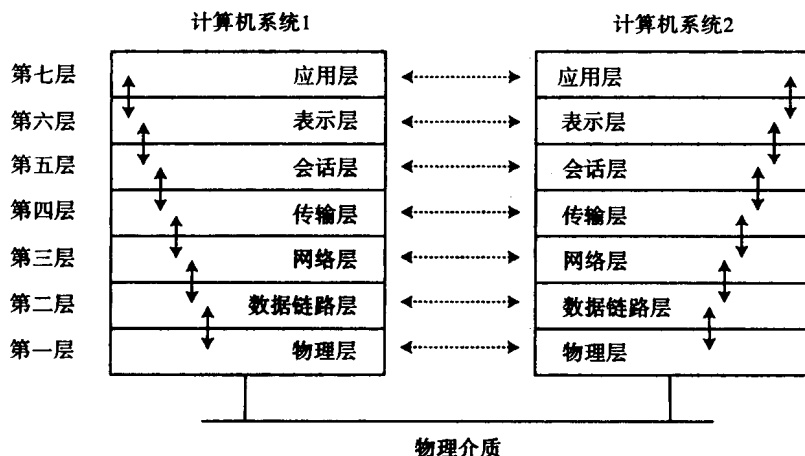


图2-1 OSI模型

表2-1 OSI各层提供的服务

层	服 务
应用层	处理文件和消息传递、目录查找、命名、验证和应用程序需要的其他服务
表示层	确保由一个系统发送的信息能在另一个系统的应用层上可读
会话层	建立、管理和终止应用程序间的会话
传输层	提供端到端的通信、错误恢复和流控制
网络层	提供网络间的连接和路径选择
数据链路层	提供通过物理链路的数据传送
物理层	为系统间的物理链路定义电子和机械规范

理解由OSI模型各层提供的服务，以及各层上的典型问题是重要的。分离问题的起因时，应该以自底向上的方式进行。从最底层开始，首先检查电缆和物理接口。然后在数据链路层检查封装选项和介质访问控制的任何问题。上移一层考虑路由协议问题和网络层编址问题。在高层，检查缓冲区耗尽、软件bug、命名、加密、压缩、数据表示和用户错误问题。剩下的章节将提供关于这些建议的更多的细节。

网络领域的新手如实地记住了OSI模型及其功能。当新手进一步学习网络时，他们发现许多协议并没有参考这个模型来设计，并且没有完全符合这个模型。一些协议根本就不符合线性栈，而且偏离了管理和控制界面的主列表。尽管存在这些告诫，模型仍然很好地解释了网络协议需要的功能，在故障排除中是一个很好的路标。

OSI模型为理解现有的和将来的协议行为提供了一个框架。当专家看到处理一个数据包（从数据链路层，通过网络层，到传输层）的过程时，他们能利用对OSI模型的理解来抽取数据包的含义和功能。结合OSI各层的网络设备（第二层的交换机，第三层的路由器，第四层及其上各层的文件服务器），工程师能将网络的症状与网络问题的潜在原因关联起来。网络层的症状可能表明了路由器上的路由协议的错误配置。传输层的重传可能表明文件服务器上的内存或计算能力的短缺。这种思考方式可以推广到无数的网络问题上。

另一个与汽车的类比

一个协议分析专家与一个自动化机械专家类似。大家都知道汽油从汽车外部的一个孔中进去。然后气体物质在发动机的汽缸里混合并爆炸，使得发动机运转起来。然后传送部分将发动机连接到车轮，等等。当我们听到奇怪的杂音时，我们会说“哦，听起来好像没有汽油了，”或者“听起来好像车胎漏气了”。毕竟我们不是机械专家。

然而，训练有素的机械师知道汽车的燃料系统、点火系统、驱动链、车闸和电子系统等等之间的细微差别和联系。虽然不同的汽车制造在许多方面不同，但是机械师可以处理许多他们不经常使用的汽车系统。因此，对于OSI参考模型和网络专家也是一样的。专家理解流量控制、消息编码、确认、路由等等，不管他们是否使用以太网、异步传输模式（ATM）、TCP/IP或是Internet工程任务组（IETF）之外的新协议。

OSI模型帮助网络工程师理解协议的设计是模块化的。模型的每一层以半独立的方式运行，为其上面的一层提供服务接口。当独立层没有遵循OSI原理时，就会出现問題。考虑文件传输协