Broadview®
www.broadview.com.cn

安全技术大系

Sniffer Pro Network Optimization & Troubleshooting Handbook

Sniffer Pro 网络优化与故障检修手册

[美] Robert J. Shimonski , Wally Eaton
Umer Khan , Yuri Gordienko 著

陈逸 谢婷 等译

SYNGRESS®

電子工業出版社
PUBLISHING HOUSE OF ELECTRONICS INDUSTRY
http://www.phei.com.cn

安全技术大系

Sniffer Pro

网络优化与故障检修手册

Sniffer Pro

Network Optimization & Troubleshooting Handbook

[美] Robert J. Shimonski, Wally Eaton, Umer Khan, Yuri Gordienko 著

陈 逸 谢 婷 等译

電子工業出版社

Publishing House of Electronics Industry

北京 · BEIJING

内 容 简 介

Sniffer Pro 是美国 Network Associates 公司出品的一种网络分析软件，可用于网络故障与性能管理，在网络应用界应用非常广泛，现已占到网络分析软件市场的 76%。

本书可帮助读者了解 Sniffer Pro 的机理，掌握使用 Sniffer Pro 的技术。全书共分 12 章。第 1 章详细介绍网络工作的基本问题、Sniffer Pro 的功能，以及 SCP 认证考试的内容。第 2 章和第 3 章介绍 Sniffer Pro 程序的安装、配置和 Sniffer 界面的各个方面。第 4 章介绍如何监测应用程序，特别是在微软和 Novell Netware 网络中运行的应用程序。第 5 章介绍对网络进行实时性能监测和分析变化趋势的情况。第 6、7、8 三章分别介绍用于分析的网络数据捕获、网络问题的分析，以及使用过滤器进行网络流量捕获与分析的方法。第 9 章阐述如何在网络中使用触发与警告功能。第 10 章描述如何报告分析过的网络数据。第 11 和第 12 章介绍 Sniffer Pro 在探测和补救网络安全漏洞，以及网络优化与故障检修方面的应用。

本书适合于网络管理人员及其他相关领域的专业技术人员、管理人员阅读，也可作为大专院校相关课程的核心参考书。

版权贸易合同登记号　图字：01-2003-6400

图书在版编目（CIP）数据

Sniffer Pro 网络优化与故障检修手册 /（美）西蒙斯基（Shimonski, R. J.）等著；陈逸等译.
北京：电子工业出版社，2004.8
（安全技术大系）
书名原文：Sniffer Pro Network Optimization and Troubleshooting Handbook
ISBN 7-121-00007-5

Ⅰ. S…　Ⅱ. ①西… ②陈…　Ⅲ. 计算机网络－安全技术－应用软件，Sniffer Pro　Ⅳ. TP393.08

中国版本图书馆 CIP 数据核字（2004）第 057665 号

责任编辑：顾慧芳
印　　刷：北京智力达印刷有限公司
出版发行：电子工业出版社
　　北京市海淀区万寿路 173 信箱　邮编　100036
经　　销：各地新华书店
开　　本：787×980　1/16　印张：36.25　字数：686 千字
印　　次：2004 年 8 月第 1 次印刷
印　　数：4000 册　　定价：65.00 元

凡购买电子工业出版社的图书，如有缺损问题，请向购买书店调换。若书店售缺，请与本社发行部联系。联系电话：（010）68279077。质量投诉请发邮件至 zlts@phei.com.cn，盗版侵权举报请发邮件至 dbqq@phei.com.cn。

译 者 序

如今网络已经风行于世，但如何对网络进行管理，恐怕很多人还知之甚少。在计算机网络的质量体系中，网络管理是一个关键环节，网络管理的质量也会直接影响网络的运行质量。网络管理系统的功能就是为网络把脉，查看网络连接关系，检查各种设备可能出现的问题，检测网络性能瓶颈出在何处，并进行自动处理或远程修复，促进网络的高效运转。

自 20 世纪 80 年代之后，网络开始飞速的发展，网络管理人员的任务也日益艰巨。在接触这本书之前，我一直以为对一个网管而言，对网络的管理和故障的处理是建立在他的个人能力和经验之上的。如果网络出现什么问题，或者发生了瘫痪，如果网管有丰富的处理此类事件的经验，那么就会不动声色地轻松解决。而对于一个新手来说，即使是满头大汗地从头到尾对每个环节全部检测一遍，或许还是不能解决问题。另外对于一个庞大复杂的系统来说，即使是经验丰富的网络管理人员，想要排查和解决一个问题也将是一项极为繁重和令人讨厌的工作。现在，在看到本书之后，我完全改变了看法，原来，网络的管理与故障检修并非如此神秘，这就好像找到了新的武器，可去对付那些老缠着你的问题。

这本书的作者讲述了 Sniffer Pro 是利用计算机的网络接口截获网络数据并分析、生成统计结果和报告，以及对数据进行高级分析来发现问题的一种工具。在网络中，Sniffer Pro 的存在对系统管理员是至关重要的，系统管理员通过 Sniffer Pro 可以诊断出大量不可见的模糊问题，这些问题涉及两台乃至多台计算机之间的异常通信，有些甚至牵涉到各种的协议。借助于 Sniffer Pro，系统管理员可以方便地确定出多少的通信量属于哪个网络协议、占主要通信协议的主机是哪一台、大多数通信目的地是哪台主机、报文发送占用多少时间、或者主机的相互报文传送间隔时间，等等，这些信息为管理员判断网络问题、管理网络提供了非常宝贵的信息。

正如本书作者所言，目前出版的关于如何解决网络故障的著作少之又少，当网络出现问题时，人们通常是一筹莫展，或者只能借助网络管理人员的经验解决问题，这样就导致了故障检修具有一定程度的盲目性，也为网络管理与检修蒙上了一层神秘的面纱。但读过本书之后，你就会发现：它不仅能够帮助你熟练掌握 Sniffer Pro，并将其用于网络管理与故障检修；更重要的是，它还为如何检修网络故障提供了很多有益的思路，帮助你面对以前未曾碰到过的问题。

本书作者 Robert J Shimonski 是一家居世界领先地位的制造公司的首席网络和安全工程师。他擅长进行网络基础结构设计、防火墙的网络安全性设计和管理，网络优化和故障排除，并撰写过很多关于网络安全的文章，出版了很多相关书籍。Shimonski 在 Sniffer Pro 的应用方面具有丰富的经验，书中也提供了很多实际例子供读者参考。阅读本书，就好像有一位老师正在从旁指点你寻找网络故障一样，相信每位读者读过之后都会感觉受益匪浅。

Sniffer Pro 是一种比较新的工具，相关的中文参考资料不多，加之译者水平有限，译文中必定存在很多错误与不当之处，恳请读者不吝赐教。

陈　逸

2004.6.1 于北京

致　谢

我们将感谢下面这些人，因为有了他们的支持，本书才有可能完成。

Ralph Troupe、Rhonda St.John、Emlyn Rhodes 和 Callisma 的小组，他们为设计、部署和支持全世界的企业网络做出了卓越贡献。

Group West 出版社的 Karen Cross、Lance Tilford、Meaghan Cunningham、Kim Wylie、Harry Kirchner、Kevin Votel、Kent Anderson、Frida Yara、Jon Mayes、John Mesjak、Peg O'Donnell、Sandra Patterson、Betty Redmond、Roy Remer、Ron Shapiro、Patricia Kelly、Andrea Tetrick、Jennifer Pascal、Doug Reil、David Dahl、Janis Carpenter 和 Susan Fryer，他们和我们一起分享了他们宝贵的市场经验和专业知识。

Elsevier Science 的 Jacquie Shanahan、AnnHelen Lindeholm、David Burton、Febea Marinetti 和 Rosie Moss，他们帮助我们了解世界范围内的相关情况。

Transquest 出版社的 David Buckland、Daniel Loh、Wendi Wong、Marie Chieng、Lucy Chong、Leslie Lim、Audrey Gan 和 Joseph Chan，他们很热情地对我们的书稿进行了处理。

Acorn 出版社的 Kwon Sung June 也为我们提供了支持。

Jackie Gross & Associates 的 Jackie Gross、Gayle Voycey、Alexia Penny、Anik Robitaille、Craig Siddall、Darlene Morrow、Iolanda Miller、Jane Mackay 和 Marie Skelly，他们为我们提供了帮助，并在加拿大积极地宣传我们的作品。

Lois Fraser、Connie McMenemy、Shannon Russell 和 Jaguar Book Group 的其他人，他们帮助我们在加拿大发行 Syngress 系列丛书。

特别要感谢澳大利亚的 Woodslane 的人们！要感谢 David Scott 和那里的每一个人，我们最初就是通过 Woodslane 在澳大利亚、新西兰、巴布亚新几内亚、斐济汤加、所罗门群岛和库克群岛来销售 Syngress 的书籍的。

本书贡献者

Wally Eaton（CNX、BSCS、CCNP、CCDP、MCSE、MCP+I、NETWORK+、FCC）是佛罗里达州 Jacksonville 城的总安全长官。Wally 是 Unisys 公司的高级系统领域工程师，将在 20 年后退休。在 Unisys，他的职责包括为 Unisys 的主机安装、调试并维护硬件和系统软件。现在他正在攻读马里兰州首府学院的研究生课程，希望获得网络安全科学的硕士学位。

Yuri Gordienko（CCNP、CCNA、CCDA、MCSE）是加拿大最大的 ISP 之一——AT&T Canada 的中枢线路工程师。他负责为国家的中枢线路进行设计并提供支持。他的专长包括 Cisco 路由器和交换机，网络架构和优化，在蒙特利尔、多伦多和温哥华设计和建立了因特网数据中心（IDC），并负责部署加拿大 AT&T 的路由服务器。Yuri 还是 RCC 大学的兼职导师，这座大学位于多伦多，他教授计算机通信课程。他对几本 Syngress 资格认证的书籍都做出了贡献，其中包括《Cisco Certified Design Associate Study Guide and Cisco Certified Network Associate Study Guide》的第二版。Yuri 有计算物理学的学位。

Eric Ouellet（CISSP）是安全系统设计小组的重要合作伙伴，安全系统设计小组是加拿大渥太华的一个网络设计与安全咨询机构。他擅长实现网络和安全基础设施，并且同时满足设计和实用方面的要求。他曾经负责使用 Cisco、Nortel 和 Alcatel 设备来设计、安装并解决 WAN 的问题，通过地面、卫星中继、无线和受信通信链接来支持声音、数据和视频会议服务。

Eric 还曾经负责设计一些先进的公共密钥基础结构的部署，这些结构目前正在使用。他还提出了一些具有可操作性的策略来满足电子签章法（E-sign）和健康保险便利及责任法案（HIPAA）的要求。他向金融、商业、政府和军方的客户提供服务，包括美国财政部、加拿大财政部和 NATO。他经常在安全会议上作报告，并教授网络与 CISSP 课程。他与其他人合作完成了《Hack Proofing Your Wireless Network》（Syngress Publishing，ISBN：1-9289884-59-8）和《Building A Cisco Wireless LAN》（Syngress Publishing，ISBN：1-9289994-58-X）。Eric 要对他的家人和朋友在他写作本书期间给予的理解与支持表示感谢，还有 PK、FS、SJ、MW、ATN、SM 和那些“孩子们”。

技术评审人

Randy Cook（MCSE、SCSA）是 Sapphire Technologies 公司的高级 UNIX 系统管理人员和网络工程师。Randy 能够为高危险环境中的操作系统和关键任务应用程序提供支持。Randy 与其他人合作完成了几本 Syngress 出版的书籍，也担任了几本书的评审人，这些书包括《Sun Certified System Administrator for Solaris 8.0 Study Guide》（ISBN：007-212369-9）和《Hack Proofing Sun Solaris 8》（ISBN：1-928994-44-X）。他还在 IT 杂志上发表了一些技术文章，并且主持一个联合广播新闻节目。

技术编辑

Robert J. Shimonski（SCP、CCDP、CCNP、Nortel NNCSS、MCSE、MCP+I、Master CNE、CIP、CIBS、CWP、CIW、GSEC、GCIH、Server+、Network+、Inet+、A+、eBiz+、TICSA、SPS）是一家领先的制造公司的一名高级网络工程师和安全分析专家，这家公司提供线性运动产品和工程设计。Robert 最初的职责是用多种网络分析工具（包括 Sniffer Pro）每天对企业网络进行监控、基准设定和故障检修，这个网络是由多种协议和媒体技术组成的。Robert 多年来一直进行高级和低级的网络设计与分析，他现在不仅能够使用故障检修和分析方法为大型企业提供服务，而且可以帮助中小型公司优化 WAN、LAN 和安全基础设施。

Robert 在 TechTarget.com 上有一个网上论坛，称做“网络管理答案大全”，在那里，他每天回答一些网络分析和管理的问题。Robert 还擅长其他技术，包括用 Cisco 和 Nortel 产品为企业进行网络结构设计。Robert 还可以用 Sniffer Pro、Etherpeek、CiscoSecure 平台（包括 PIX 防火墙）和 Norton 的防病毒软件进行网络安全分析。

Robert 为很多文章、学习指导和资格认证预修软件，以及网站和世界级的各种组织都作出了贡献，包括《MCP Magazine》、TechTarget.com、Brainbuzz.com 和 SANS.Org。Robert 在 Avis Rent-A-Car 和 Cendant Information Technology 公司担任过网络架构师。他具有 SUNY 的学士学位，是纽约 Garden 城 Computer Career Center 的兼职技术指导，教授基于 Windows 的网络技术。Robert 还是《Configuring & Troubleshooting Windows XP Professional》（Syngress Publishing，ISBN：1-928994-80-6）和《BizTalk Server 2000 Developer's Guide for .NET》（Syngress，ISBN：1-928994-40-7）的作者之一。

Umer Khan（SCE、CCIE、MCSE、SCSA、SCNA、CCA、CNX）是 Broadcom Corporation（www.broadcom.com）的网络与安全负责人。目前，Umer 的部门正负责设计并实现 99.9%以上的时间都可利用的全球 LAN/MAN/WAN 方案，还要处理 Brodacom 公司所有的信息安全问题。Broadcom 的网络包括 Cisco 可交换端对端技术、暗光纤（dark fiber）、OC-48 SONET、DWDM、802.11 无线技术、多供应商 VPN 的整合和 VoIP。其信息安全小组主要处理策略问题、侵入探测与响应、鉴定和防火墙等问题。Umer 在 Illinois Institute of Technology 获得了计算机工程的学士学位。

前　言

在今天以业务为基础的网络基础设施中，几乎无时无刻都会出现新的问题，或者是网络速度太慢，或者就是有一些功能不能正确地执行。在这个问题不断涌现的时代，很多网络管理人员都采用了一种具有针对性的故障检修（troubleshooting）技术。这种技术在任何一本教科书里都没有提到过，课堂上也没有传授过，任何一种资格认证考试中也没有出现过。它主要是一种寻找故障的观察能力。很多人对这种方法都有一些认识，你们可能都看到过这种情形：高级的网络管理人员不需要进行任何分析，就能够找到网络问题出在哪里。他们可能会闭上眼睛，靠在椅子上，做几下深呼吸，几秒种之后就会得出结论："是服务器上的网卡出了问题——它至少已经用了5年了。可能驱动器也该换了。"你见过这种高超的技术吗？你自己是否也能做到这些呢？事实上你也可以——这并不困难。

作为一个网络管理人员，你是不是想过自己能够只瞟一眼跳线面板（patch panel）上的各种线，就可以解决一些高难度的网络问题呢？如果这一直是你的梦想的话，那么这本书就是为你写的。我曾经和一些初级的网络管理人员开玩笑，故弄玄虚地把手指插在空的 Hub 端口上，闭一会儿眼睛，然后脱口而出一个解决问题的方法。在解决问题之前，他们通常都以为我在骗他们——直到我确实解决了问题。但他们不知道，其实我已经花了一个上午的时间，用 Sniffer Pro 分析软件和其他一些工具来解决网络的问题。

你也许想过，要是能把头伸到电缆、Hub、交换机（switch）或者其他网络配件中就好了，这样就可以确切地指出问题所在了。本书和 Network Associates 公司的 Sniffer Pro Network Analysis 软件，将帮助你进行网络和网络协议标准的分析。Sniffer Pro 是一个与众不同的故障检修工具，根据我的个人观点，它还有很大的应用空间。如果我告诉你，用这种工具，你可以解决很多最棘手的常见网络问题，你会怎么样做？你会去用它吗？答案当然是肯定的。本书不仅能为你开拓网络分析的视野，还会传授给你一种工具的每一个使用细节，使你获得最详尽的数据。这种工具就是 Sniffer Pro。用这本书和 Sniffer Pro，你就可以很轻松地成为一名网络分析技术人员和 Sniffer 认证专家（Sniffer Certified Professional, SCP），这远比获得绝佳的观察能力更吸引人。

几年前，因为受到了一些挫折，我立志要写这本书。当时我的网络出了问题，

但是我没能自己找出原因，所以我找到了最近的一家书店。我漫无目的地闲逛，只想找到一本能帮助我的书，使我能够找到专门的方法，解决我遇到的这个神秘的网络问题——或者至少给我指明一个方向。我看了很多书，但没有一本是专门讲网络故障检修的。哎呀！现在怎么办？我仔细地翻阅了至少 700 本关于 HTML 和 MCSE 的书，而所有这些书对我也并没有什么帮助。我还打电话给一个可能会给我帮助的朋友，但同样一无所获。我本来以为这应该是一本针对常见问题的常用书，但却找不到，这让我很失望。我需要的是这样的一本书，告诉人们如何用 Sniffer Pro 网络分析软件来根据类型建立捕获过滤器，并分析传送量。这次经历使我意识到，完成《Sniffer Pro 网络优化与故障检修手册》是我的使命。

对新手和经验老道的网络管理人员来说，Sniffer Pro 产品都是一根救命稻草，它可以观察混乱的代码，从而发现网络问题的线索。但是，很多技术人员在错误地使用这些产品——把所有东西都捕获过来，再逐一筛选有用的——然后，因为没能学会如何建立正确进行分析的应用程序而很快就失败了。本书就是针对这种情况而完成的。

本书提供了一种基本方法，可帮助读者了解使用 Sniffer Pro 的机理，以及掌握使用 Sniffer Pro 的方法和技术。千万不要犯这样的错误，认为这种工具一定会解决你遇到的问题。作为一名网络分析人员，应该是在 Sniffer Pro 工具的帮助下，由你自己来解决问题，而且本书作者也在书中确保能使你逐渐朝这个方向前进。例如，在某些章中，会要求你用 Sniffer Pro 了解一些以太网问题，比如过度冲突，并发现网络的问题出在哪里。你不仅要了解出现的问题，还要知道如何用 Sniffer Pro 发现它。本书还重点介绍了其他工具和技术（包括作者了解的所有工具和技术）、如何进一步诊断问题，并得到完整的解决方法。掌握这些技术对你来说非常重要，本书将确保你能够完全掌握它们。

下面我们来逐章了解本书内容：

- 第 1 章“关于 Sniffer Pro”，详细介绍了网络工作的基本问题、Sniffer Pro 的功能，以及 SCP 认证考试的基本问题。这章的内容很重要，因为它包括了很多要灵活使用 Sniffer Pro 所需要了解的理论知识。如果你在阅读本书的后面部分时需要了解一个你不太清楚的概念，比如 IPX 寻址问题或者如何使用基于 hex 的寻址概念，这章还可以作为你的参考资料。
- 第 2 章“安装 Sniffer Pro”，它详细介绍了安装和配置 Sniffer Pro 程序的过程，以及 Sniffer Pro 正常运行需要的驱动程序。很多对 Sniffer Pro 略有所闻的技术人员真的认为在一个工作站上安装并运行了 Sniffer Pro 就可以为他们解决

问题了。但事实并非如此简单。例如，使用了错误的驱动程序会带来冲突，使你不能及时发现问题。此外，问题还可能会一直从你的电脑影响到整个网络，因为你在网络中的关键位置，你可能会丢失一些未处理的数据。这一章阐述了这样以及那样的一些错误概念。另外，本章还包括了建立技术工具箱的内容，使你了解你需要用什么来强化 Sniffer Pro 的功能，提高你检修故障的能力。

- 第 3 章“深入了解 Sniffer Pro 界面”，它深入介绍了 Sniffer Pro 界面的各个方面。这章有三个主要目的。第一，你需要了解如何在程序中移动，从而使用它。第二，这章使你熟悉基本界面配置，这样你就能够在今后建立并使用更高级的配置。我们提过，本书为你提供一种基本方法，使你知道你在做什么，同时了解配置步骤的原理。最后，如果要通过 SCP 考试，你就需要记住这一章的内容。考试中有很多问题都与如何从程序中一个位置到另一个位置，以及每个对话框的作用等问题直接相关。你必须不断复习这章内容，直到你能够熟练进行布局的配置。你进行的每一次网络分析都不同，所以你应该了解各种情况下 Sniffer Pro 的使用。
- 第 4 章“设置 Sniffer Pro 来监测网络应用程序”，它的内容建立在你刚刚对 Sniffer Pro 界面的掌握的基础上，教你如何监测应用程序，特别是在微软和 Novell NetWare 网络中运行的应用程序，还包括了 Sniffer Pro 捕获过程的基本问题，然后介绍了捕获与翻译流量信息代码之间的细微差别。这里要强调，本书提供一种基本方法，你在每章中都要学习新技术，这些新技术都是建立在前面内容的基础之上的。在这一章，你要学习捕获流量信息并加以分析。你需要了解如何定位 Sniffer Pro，用它来捕获客户端之间进行的特殊会话并分析它们。接着，这章会介绍捕获非常特殊的协议的过程，以及如何分析它们的代码。你将了解到（不仅限于此）SAP、NCP、微软登录、邮送器（mail slot）和 NetBIOS 的内容。这章的内容是要提醒你，使你清楚由电缆传输的是什么。
- 第 5 章“用 Sniffer Pro 监控网络性能”，它指导你进行性能监测、实时监测、制定基准并分析变化趋势。你必须精通这些用于网络与性能分析的技术。这章设计了一个有问题的网络，然后详细介绍了如何针对这个问题，专门进行监测并改进网络性能的步骤。在这一章结尾，你将有机会看到重新设计后的网络以最佳的状态运行。对于想要用 Sniffer Pro 进行性能分析的技术人员来说，这章至关重要。它包括了可以同时用于以太网与令牌环网络的实时表盘，这章设计的网络存在基于 LAN 的性能问题，你将发现网络的设计不正确，而

且配置也很差。

- 第 6 章“捕获网络数据用于分析”，它对如何用 Sniffer Pro 捕获数据，如何保存捕获结果和建立基本过滤器与剖面图的基本问题等——用 ARP 和 TCP 这样的协议来分析例子——都进行了深入的阐述。
- 第 7 章“分析网络问题”，这章进入了更高级的网络问题领域，更重要的是，这章将教给你如何用 Sniffer Pro 来发现、分析并尽可能消除这些问题。这章将分析 NIC chatter、网络访问与登录过慢问题、DHCP 问题、令牌环问题等等各种问题。这章的内容比较高级。
- 第 8 章“使用过滤器”，这章建立在第 6 章内容的基础上，第 6 章已经讲过了建立过滤器来进行网络流量捕获与分析的基本问题。技术人员最常碰到的问题是如何理解并建立过滤器。这个问题听起来很容易，但当你开始建立并调整过滤器时，就会发现并非如此。本章为你了解如何建立过滤器提供了必需的基本知识，并介绍了建立你自己的过滤器的机理。这章的结尾将简单介绍 Cisco CDP 与 RIP 分析方法。
- 第 9 章“了解触发并使用警告功能”，首先向你展示了一些 Sniffer Pro 中附加的、但是通常人们都不了解的功能。这章详细介绍了如何使用触发与警告功能。
- 第 10 章“报告”，详细介绍了如何报告你分析过的数据。Sniffer Pro 具有很强的功能，可以帮助你建立网络分析报告，来向管理人员或者客户解释网络中出现了什么问题。
- 第 11 章“用 Sniffer Pro 探测并补救安全漏洞”帮助你了解用 Sniffer Pro 进行分析的缺点。你可能已经听说过 Sniffer Pro 可以当做黑客的工具来攻击网络。在这一章中，你可以看到这一切是如何发生的，并学习怎样保护你的网络免受攻击。这章还将简单介绍对病毒与蠕虫的分析、Telnet、SNMP、电子信箱和其他明文密码协议及其危险性。在这里，我们可以检查 DNS 区域传送（zone transfer）捕获结果，还可以监听与重放。
- 第 12 章“检修传输故障以优化网络”介绍如何使用 Sniffer Pro 的所有属性来发现你网络中的一个问题，并用结果来优化你的网络，从而要把本书提到的所有概念都联系起来。每个网络都有某种形式的问题存在，在这章中，你在本书中学到的所有知识都将连接起来。用 Sniffer Pro 从开始到终止，完整地优化一个网络问题。

总而言之，本书对 IT 组织具有重要意义。就像任何一个想涵盖网络分析所有问

题的讨论主题一样，本书同样无法解答所有的问题。但是，我们希望这本书将帮助你使用 Sniffer Pro 网络分析应用程序，发现并研究问题，以进行更深入的分析。帮助完成这本书的作者们都有着丰富的经验，用他们各自的实际工作经验完成了每一章的写作，他们是用各种教训换来了对网络分析的了解。你将会看到，网络分析与故障检修是需要时间来培养的技术。

从某种程度来讲，网络分析与故障检修更像是一种武器。在你开始准备战斗时，你需要用最好的武器来武装自己。你会选择弹弓这样的武器来帮助你分析网络吗？我想不会。Sniffer Pro 才是更好的选择。所以，在你下一个网络问题出现之前，用技术、Sniffer Pro 和这本书来武装自己。我保证你会取得胜利。

——Robert J.Shimonski

CCDP, CCNP, SCP, NNCSS, MCSE, MCP+I,
Master CNE, CIP, CIBS, CWP, CIW, GSEC, GCIH,
A+, Inet+, Server+, Network+,eBiz+, TICSA

solutions@syngress.com

我们的 MCSE、MCSD、CompTIA 和 Cisco 的学习指导材料已经印刷了至少 150 万份，我们还会继续寻求更好的方法来为读者服务，提供更多信息。其中一种方法就是听取意见。

读者们已经告诉我们，他们需要基于因特网的服务，这样可以扩展并增强我们的出版物的价值。根据读者的反馈和我们自己的策略规划，我们已经建立了网站，希望借此来达到预期目的。

Solutions@syngress.com 是一个互动式的信息宝库，主要包括我们的书中的内容和相关技术。这个网站具备下列功能：

- 如果产品升级换代，在一年期限内可以进行内容更新。你可以对任何发生变化的内容进行在线更新。
- “向作者提问”的顾客提问表格，使你可以向作者和编者提出问题。
- 每月发出邮件，我们的专家将就读者提问做出回答，并对复杂的内容进行详尽的解释。
- 编者特别为读者推荐一些相关网站，并定期更新到这些网站的链接。

最重要的是，本书是访问这个网站的钥匙。登录 **www.syngress.com/solutions**，并且在注册时需要用这本书来确认你确实购买了此书。

非常感谢您给我们这个机会为您服务。如果还有其它事情需要我们帮助，请一定告诉我们，我们将让您的参与给您带来最大的收益。我们一直在听取您的意见。

目　录