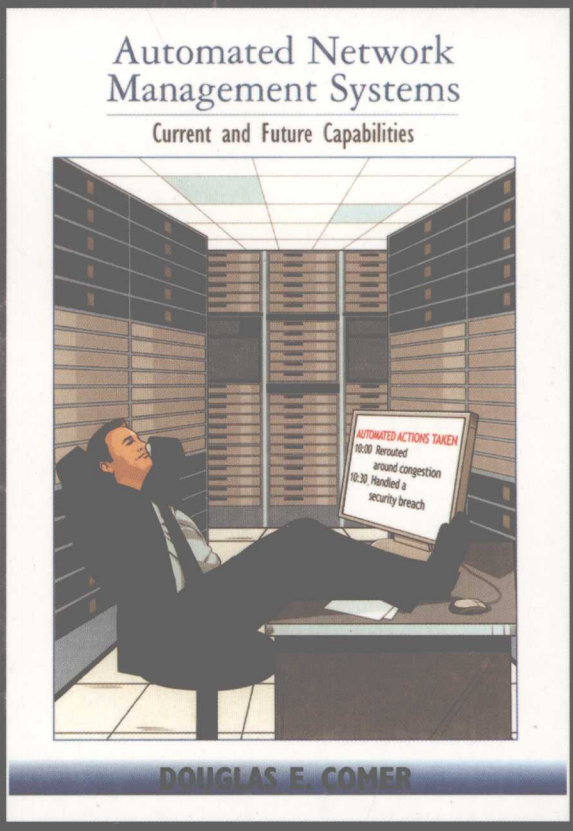
HZ BOOKS 华章教育

PEARSON Prentice Hall

计 算 机 科 学 丛 书

自动网络管理系统

(美) Douglas E. Comer 普度大学 著 吴英 南开大学 等译



Automated Network Management Systems

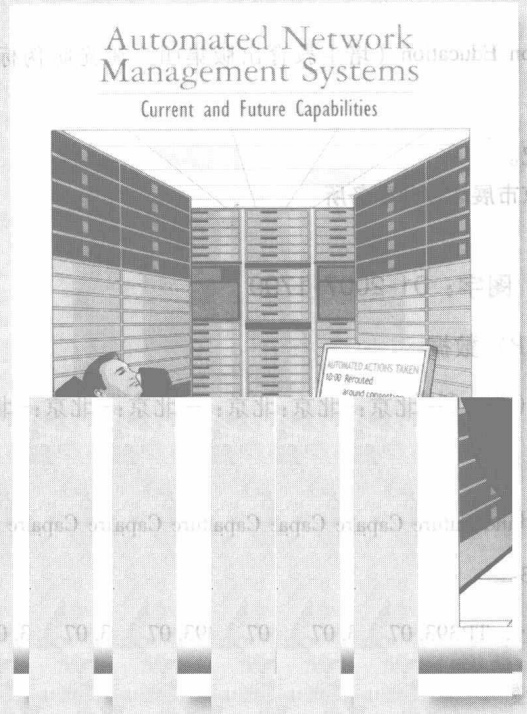
Current and Future Capabilities

机械工业出版社
China Machine Press

计 算 机 科 学 丛 书

自动网络管理系统

(美) Douglas E. Comer 普度大学 著
吴英 南开大学 等译



Automated Network Management Systems

Current and Future Capabilities

机械工业出版社
China Machine Press

本书对自动网络管理进行了全面介绍，全书包括三个部分。第一部分对网络管理的问题进行定义，并给出重要的背景知识；第二部分介绍进行网络自动化管理的工具与技术；第三部分介绍网络自动化管理的发展趋势并提出了开放性的问题。

本书层次清晰、概念准确、语言通俗易懂，既适合高等院校计算机及相关专业作为教材，也适合从事网络管理的技术人员阅读。

本书版权登记号：图字：01-2007-1799

图书在版编目（CIP）数据

自动网络管理系统/（美）科默（Comer, D. E.）著；吴英等译. —北京：机械工业出版社，2009.1

（计算机科学丛书）

书名原文：Automated Network Management Systems: Current and Future Capabilities

ISBN 978-7-111-25393-8

Ⅰ. 自… Ⅱ. ①科… ②吴… Ⅲ. 计算机网络－管理 Ⅳ. TP393.07

中国版本图书馆 CIP 数据核字（2008）第 079466 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：朱　劼

北京慧美印刷有限公司印刷

2009 年 1 月第 1 版第 1 次印刷

184mm×260mm · 14.25 印张

标准书号：ISBN 978-7-111-25393-8

定价：38.00 元

凡购本书，如有倒页、脱页、缺页，由本社发行部调换

本社购书热线：（010）68326294

出版者的话

文艺复兴以降，源远流长的科学精神和逐步形成的学术规范，使西方国家在自然科学的各个领域取得了垄断性的优势；也正是这样的传统，使美国在信息技术发展的六十多年间名家辈出、独领风骚。在商业化的进程中，美国的产业界与教育界越来越紧密地结合，计算机学科中的许多泰山北斗同时身处科研和教学的最前线，由此而产生的经典科学著作，不仅擘划了研究的范畴，还揭示了学术的源变，既遵循学术规范，又自有学者个性，其价值并不会因年月的流逝而减退。

近年，在全球信息化大潮的推动下，我国的计算机产业发展迅猛，对专业人才的需求日益迫切。这对计算机教育界和出版界都既是机遇，也是挑战；而专业教材的建设在教育战略上显得举足轻重。在我国信息技术发展时间较短的现状下，美国等发达国家在其计算机科学发展的几十年间积淀和发展的经典教材仍有许多值得借鉴之处。因此，引进一批国外优秀计算机教材将对我国计算机教育事业的发展起到积极的推动作用，也是与世界接轨、建设真正的世界一流大学的必由之路。

机械工业出版社华章分社较早意识到“出版要为教育服务”。自1998年开始，华章分社就将工作重点放在了遴选、移译国外优秀教材上。经过多年的不懈努力，我们与Pearson，McGraw-Hill，Elsevier，MIT，John Wiley & Sons，Cengage等世界著名出版公司建立了良好的合作关系，从他们现有的数百种教材中甄选出Andrew S. Tanenbaum，Bjarne Stroustrup，Brain W. Kernighan，Dennis Ritchie，Jim Gray，Afred V. Aho，John E. Hopcroft，Jeffrey D. Ullman，Abraham Silberschatz，William Stallings，Donald E. Knuth，John L. Hennessy，Larry L. Peterson等大师名家的一批经典作品，以“计算机科学丛书”为总称出版，供读者学习、研究及珍藏。大理石纹理的封面，也正体现了这套丛书的品位和格调。

“计算机科学丛书”的出版工作得到了国内外学者的鼎力襄助，国内的专家不仅提供了中肯的选题指导，还不辞劳苦地担任了翻译和审校的工作；而原书的作者也相当关注其作品在中国的传播，有的还专程为其书的中译本作序。迄今，“计算机科学丛书”已经出版了近两百个品种，这些书籍在读者中树立了良好的口碑，并被许多高校采用为正式教材和参考书籍。其影印版“经典原版书库”作为姊妹篇也被越来越多实施双语教学的学校所采用。

权威的作者、经典的教材、一流的译者、严格的审校、精细的编辑，这些因素使我们的图书有了质量的保证。随着计算机科学与技术专业学科建设的不断完善和教材改革的逐渐深化，教育界对国外计算机教材的需求和应用都将步入一个新的阶段，我们的目标是尽善尽美，而反馈的意见正是我们达到这一终极目标的重要帮助。华章分社欢迎老师和读者对我们的工作提出建议或给予指正，我们的联系方法如下：

华章网站：www.hzbook.com
电子邮件：hzjsj@hzbook.com
联系电话：(010) 88379604
联系地址：北京市西城区百万庄南街1号
邮政编码：100037

译者序

21 世纪的一个重要特征是数字化、网络化与信息化，而它的基础是支持全社会的强大的计算机网络。计算机网络技术对社会发展和科学技术的进步产生了不可估量的影响。计算机网络已经与电力、电话一样，成为支持现代社会整体运行的基础设施，人们时刻都不能离开。随着人们对网络服务需求的增加与网络规模的扩大，企业管理者与用户对网络的依赖程度越来越高，如何保证网络持续、有效、安全地运行已经成为关键性问题，这就使得网络管理成为现代网络技术中的重要研究课题。

Douglas E. Comer 是国际著名的网络技术专家，他的很多著作已经被翻译成多种文字在世界各国发行，并且被广泛应用于很多大学的计算机专业教学中。他对网络管理的概念和工作原理有独到的见解，这与他在计算机系统（包括硬件与软件）方面具备广泛的研究背景是分不开的。在本书中，作者用清晰的层次结构、准确的概念与通俗易懂的语言，为读者准确地剖析了网络管理的工作机制，以及自动化网络管理的相关研究、技术与未来发展方向。

本书的最大特点是能够满足不同程度的读者需求。对于网络管理方面的背景知识不是很多的读者，本书是一本适宜的入门教材和参考书，他们可以循序渐进地学习网络管理基础知识，了解网络管理的新的发展动态。对于讲授计算机网络和网络管理课程的教师，或者对网络管理有一定了解的高年级本科生与研究生，本书是一本适宜的提高教材与参考书，他们可以从中获得所需知识来完成教学与研究，并学会利用相关工具来完成基本的网络管理任务。

本书的前言、第 1 ~ 2 章与第 16 ~ 18 章由吴英翻译，第 3 ~ 5 章及第 12 ~ 15 章由许昱玮翻译，第 6 ~ 11 章由孙琳翻译，全书由吴英审校。

在翻译这本书的过程中，我们希望尽可能地尊重原著的思想，但是译者的学识有限，加之时间仓促，书中难免有疏漏之处，敬请读者指正。

译者

2008 年 8 月 1 日

于南开大学信息技术科学学院

前 言

网络管理仍是人类在网络领域了解最少的方面。研究人员已成功设计出整套的 Internet 通信协议，网络行业已开发出整套高速处理数据包的创新性系统。与此同时，网络管理高度依赖于人类的创造力来诊断问题，并通过人工干预来修复问题。

网络在商业应用上的成功使网络管理的难度增加。一方面，对网络服务需求的增加意味着网络规模要不断扩大。另一方面，高需求正在创造着一种环境，促使运营商开发创新性的产品与技术。由于管理员倾向于采用最先进的网络元素与机制，因此这种扩展导致网络管理发生显著变化。结果，在网络中包含多种以 ad hoc 方式结合的新技术，这意味着网络基础设施变得杂乱无章。

即使对于一个小型 ad hoc 网络，也很难对它进行监视与控制。随着网络规模不断扩大，出现的问题常常让管理员一筹莫展。大型的企业网络通常相当复杂，管理员很难独立胜任管理任务。简而言之，我们没有足够的能力来设计、部署、配置、控制、监视、测试与管理大型网络，因此需要实现网络管理自动化。

网络管理自动化是本书的中心议题。我们既将全面的自动化管理视为对人类智力的挑战，又视为在商业上可行的努力。本书各章将会考虑这个问题，评价现有的工具与技术，并研究自动化能够以哪种方式得到扩展。

本书内容可以分为 3 个部分。第 1 章是全书概述。第一部分包括第 2 章至第 8 章，这部分将对网络管理的问题进行定义，并对重要部分的背景进行介绍。第 2 章与第 3 章介绍基本网络元素，描述网络管理的问题，并介绍工业标准——FCAPS 模型。后续几章将分别介绍 FCAPS 模型的各个方面。

本书第二部分包括第 9 章至第 13 章，该部分将对可用于自动化管理各方面的工具与技术进行介绍。这部分讨论的例子包括：集成平台、SNMP 协议、数据流量分析（NetFlow）、路由与流量管理、管理脚本等。该部分中的各章主要关注概念，而不是介绍处理特定任务的商用产品与研究原型。例如，脚本一章中的概念是随着 expect 脚本提出，并且通过一个可扩展 DHCP 服务器的几个脚本例子加以解释。

本书第三部分包括第 14 章至第 18 章，该部分对自动化管理的未来进行了展望。首先，将描述全面的自动管理系统应具备的特点，并考虑可能使用的软件体系结构。接着，探讨信息表示与语法方面及设计权衡的难点问题。最后，提出一系列开放式问题与研究性问题。

本书既适合产业界也适合学术界的读者阅读。对于产业界读者来说，本书为网络管理者提供了很好的背景知识，有助于网络管理者定义任务的范围。对于学术界读者来说，本书可用于高年级本科生或研究生教学。在本科生层次，教学目标是使学生了解网络管理任务的困难，并向学生展示一些有效的工具。在研究生层次，本书可以提供足够的背景知识，以帮助他们承担相关的研究工作。

无论本科生层次还是研究生层次，实际动手的实验都是必不可少的。本科生应该学习手工配置已有的网络元素，并使用配置与故障监控的工具。研究生除了掌握概念之外，还要具有设计、实现与测量自动化工具的经验，这些工具可处理配置、故障监控、流量分析或安全等不同

方面。

很多人为本书做出了贡献。Cisco 公司的同事提供了编写思路、鼓励与反馈信息。Nino Vidovic 建议了这个项目，Dave Oran 提供了精辟的评论，David Bainbridge 提出了信息模型的语义与复杂性方面的原则，Fred Serr 为第 7 章中性能方面的讨论提供了很大帮助，Ralph Droms 审校了大纲与几章内容，Thad Stoner 提供了典型企业网规模方面的信息，Brain McGovern 提供了工具方面的建议，Jim Brown 提供了第 13 章中的脚本例子，IP 服务规划组听取介绍与产生思路。最后，Cliff Meltzer 邀请我访问 Cisco 公司，并为本书中的一些工作提供资助。Cisco 公司的其他同事也为本书做出了贡献。Craig Wills 与 James Cernak 审校了所有章节，并提出了很多建议。Ethan Blanton 编写了第 13 章中的单机监控脚本。Jennifer Rexford 提供了一些参考意见。Brent Chapman 与 Ehab Al-Shaer 审校了部分初稿的内容。Jon Saperia 除了审校部分章节之外，还与我讨论了模型、层次与交互关系。特别感谢我的妻子与伙伴 Christine，她的支持、编辑与建议帮助我克服了所有困难。

Douglas E. Comer

2006 年 7 月

关于作者

Douglas E. Comer 是美国普度大学计算机科学系的杰出教授与 Cisco System 公司的研发副总裁[⊖]。他是计算机网络、TCP/IP 协议与 Internet 领域的国际知名专家。他著有很多学术文章与技术书籍，还是网络开发和网络系统教学和科研方面的先驱者。

作为一位作品众多的作者，Douglas E. Comer 的畅销书籍已被翻译成 16 种语言，并被广泛应用于世界各地的产业界，以及高等院校的计算机科学、工程与商务等院系。他的具有里程碑意义的三卷本教材《TCP/IP 网络互联技术》，引发了组网与网络教育方面的变革。他的教材与创新实验室手册已经并且继续影响着本科生与研究生教学。

Douglas E. Comer 的书籍表现出的准确性与洞察力反映出他在计算机系统方面具备丰富的经验。他的研究工作横跨硬件与软件部分。他曾经开发过一个完整的操作系统，编写过设备驱动程序，完成了传统计算机与网络处理器的网络协议软件。由此产生的软件已被产业界应用到多种产品中。

Douglas E. Comer 曾经开设与讲授网络协议与计算机技术方面的多门课程，包括为工程师或学术界受众开设的课程。他的创新实验室使他与学生能设计、实现大型、复杂系统的原型，并测试原型系统的性能。他一直在世界各地的企业、大学与学术会议中授课。另外，他还为产业界提供计算机网络与系统设计方面的咨询。

在超过 19 年的时间里，Douglas E. Comer 是计算机研究杂志《软件：实践与经验》的主编。他是 ACM 高级会员、普度大学学术委员会的成员。他获得过很多奖项，包括 Usenix 终身成就奖。

Douglas E. Comer 的其他信息可从以下网址获得：

www. cs. purdue. edu/people/comer

有关 Douglas E. Comer 书籍的信息可从以下网址获得：

www. comerbooks. com

⊖ 在编写本书时，Comer 是 Cisco 的 Network Management Technology Group（网络管理技术组）的客座教授。

目 录

第 1 章　网络管理的挑战

1.1　简介

从商业网络出现时开始，如何有效管理通信网络的问题就一直困扰着产业界。网络设备需要安装、配置、操作、监控与维护，而用于连接设备的铜缆与光纤基础设施需要购买或租赁。用户需要付费使用这些服务。另外，管理员必须考虑如何保护网络，以避免网络遭到无意或恶意的破坏。

令人惊讶的是，尽管已经对网络管理问题进行了研究，并创建出很多用于帮助管理者的技术，但很多网络管理活动仍然需要人工完成。这些可行的技术是网络管理的基础，人类智慧被用于解决复杂性的问题。因此，存在一个令人兴奋的机会：找到一种方式来构造软件系统，以便自动完成网络管理任务。这个问题形成我们讨论的焦点，自动化管理是对智力的挑战，但其成果可能获得商业上的成功。

1.2　Internet 与网络管理

Internet 的出现从根本上改变了网络管理的方式。与传统电话系统由一个大的电话公司拥有，并管理包括通信线路到服务的整个网络不同，Internet 连接着很多由不同机构拥有并管理的网络。因此，不是由单一的电话公司来集中管理整个网络，Internet 要求每个机构独立维护自己的内部网络。随着越来越多的机构建立数据网络，自动管理的需求变得越来越迫切。

过去，网络研究组织与网络产业界一起工作以解决问题。早期的工作主要是探索基本技术，例如信号与调制、数字编码、基本通信协议等。第二阶段是提出一些用于创建现代通信网络（例如局域网与广域网、交换机、路由器、Internet 协议、网络应用等）的技术。第三阶段是由网络科学研究向商业方面转变，包括 Internet 服务提供商以合同形式明确用户获得服务，而自己是为用户提供服务。

根据网络管理的紧迫性与重要性，我们可以预测：

> 网络研究的下一阶段将会集中在找到自动管理方式，以便规划、配置、控制与运营计算机网络和 Internet。

1.3　Internet 结构

要理解网络管理的难度，我们首先需要了解网络的底层结构。在一个层次上，Internet 可以被看作一个扁平结构的“网中网”，大量独立的数据包交换网络之间通过路由器互联起来。尽管互联网络的抽象给我们一个清晰的图片，但是现实情况比想象中要复杂得多。网络与路由器被划分为子网，每个子网由一个管理实体拥有与运营，并且子网基于不同目的提供服务。网络结构随着覆盖网与隧道技术的出现而变得复杂，这些技术用于在物理网络中实现成组的逻辑连接。管理实体（administrative entity）这个术语已变得相当模糊，这是由于实体可小（例如个人）可大（例如跨国公司），也可能是支持内部业务、电子商务或全部业务的 Internet（例如为其他用户提供 Internet 服务的服务提供商）。网络下层结构也发生了变化：Internet 服务提供商的边缘部分

连接终端系统，例如桌面计算机或便携式设备，而 Internet 服务提供商的核心部分通过路由器提供数据包传输服务。

1.4　管理一个实体

从概念上将 Internet 划分为管理实体是重要的，这是由于它意味着自治，即每个实体可以自
2 由设计并实现自己的使用策略。因此，所有权的概念成为网络管理和控制的关键因素：

> 尽管 Internet 中的设备需要协同工作以保证网络功能正常，但是每个管理实体独立操作与控制属于自己的 Internet 部分。

也就是说，每个实体配置、监视与控制自己的交换机、路由器或网络，以实现本地策略而不依赖于通用的控制机制。因此，这种自治提供了选择策略的自由，但是要求每个管理实体确保它的策略得到执行。

1.5　内部与外部策略

我们将学习很多复杂网络管理的问题与细节。由自治的概念引出一个问题：在不同管理实体之间存在着边界，位于边界上的实体必须协同执行双方的策略。例如，在一个典型的公司中，公司员工可以访问内部设备与服务，而公司以外的用户则没有这个权限。因此，公司策略就会包含“内部”与“外部”的规则，而这些规则之间的交互变得复杂。

管理边界为服务提供商带来复杂的问题，这是由于服务提供商必须建立多种策略，以便满足个人用户与其他服务提供商的需要。因此，当我们讨论服务提供商的网络管理时，要充分认识到复杂性问题大多是由边界引起的。

1.6　网络管理状态

正如我们将要学到的那样，网络管理目前处于一种不乐观的状态。管理员[⊖]都在抱怨很难理解运营条件与通信量、故障诊断、实现策略与验证安全规定。现有的工具与协议只能提供基本功能，并不能处理跨越多设备的全局策略或服务。每个网络设备都是独立配置与控制的，这就意味着如果要实现一个穿越整个管理域的策略，管理员必须配置每个设备以完成期望的策略。另外，由于设备通常由某个特定供应商提供，现有的工具很难在异构环境中使用，也很难与其他工具进行交互。这点主要表现在：

> 当前的网络管理工具主要集中在单个设备：诊断一个问题或实现一个策略要求管理员
> 3 一次只能检测或配置一个设备。

另外，网络产业界采用了一种手工管理的范型，即一个管理人员与一个设备进行交互。由一个人来配置、监视与控制单个设备是不够的，这主要是由两个原因造成的。第一个原因是人工进行交互相对较慢，这种方式无法适合大规模的网络。第二个也是更重要的原因是人容易犯错误，这种方式无法保证在所有设备上实现管理策略。这点主要表现在：

⊖ 在本书中，我们使用网络管理员这个术语来描述从事网络管理活动的人，例如网络设计、配置、运行、测试，以及问题检测或修复。我们没有对 network manager 与 network administrator 加以区分。

> 由于依赖人去控制与测试单个设备，当前用于网络管理的方法对大型网络，或在多个设备上实现复杂策略的网络是不够的。

1.7　Gartner 模型中的网络管理

Gartner 公司曾经提出过一个关于信息技术处理的成熟度模型[⊖]。根据 Gartner 模型的描述，成熟度包括 4 个主要阶段。相对于网络管理，这 4 个阶段可以描述为：

- 第 1 阶段：被动的人工控制与响应。
- 第 2 阶段：被动地借助自动化工具。
- 第 3 阶段：主动地对问题自动响应。
- 第 4 阶段：适应于自治系统处理问题。

在 Gartner 模型的阶段中，网络管理可以达到第 2 阶段：尽管已有工具可以帮管理员做出决策，但是最终的行动依赖于管理员。问题是网络管理如何以及何时能达到第 3 阶段。

1.8　自动化的优点

自动网络管理具有以下几个优点：

- 减少实现某个任务所需要的时间。
- 减少人工处理出错的可能性。
- 保证在整个网络中实现一致的策略。
- 提供对改变的责任制。

减少完成一个任务所需时间是最显著的优点，而减少人工处理出错的可能性特别重要，这是因为很多网络问题是由简单错误引起。人工处理出错也与第 4 项相关，如果策略的改变引起了错误，系统记录所有改变会有助于确定出错的原因。

第 3 项的保证一致性可能是最重要的。ad hoc 方法用于管理网络意味着对一致性有较低层次保证。因此，即使是一个简单的自动化系统，就算只能完成多个网络设备的复制配置，这也是一件很有用的工作。为了保证有意义的一致性，系统要处理的不只是重复的、机械性的任务。也就是说，有意义的一致性要求人工完成的任务自动完成。

1.9　缺乏产业界的响应

为什么网络产业界更加关注网络管理的人工范型上？为什么没有开发出软件系统自动完成大部分管理功能？我们将会看到这个问题非常复杂，并且实现自动化还有很多研究要做。从科学的观点来看：

> 网络管理是对计算机网络了解最少的方面。

我们还可以看到，在实现网络管理自动化之前，首先需要改变范型。由于当前的方式依赖于人工智能，我们很难构造软件来实现相同的功能。因此，在我们创建软件系统与计算机程序来执行网络管理任务之前，要找到新方式来表示与存储有关计算机的信息，将策略转换为配置，以及收集和分析有关网络操作与性能的信息。

⊖ Gartner 信息技术处理成熟度模型的描述可以在以下网址找到：http：//www. gartner. com/DisplayDocument? doc_cd = 131972。

1.10　对商业的影响

如果对自动化管理系统的研究失败将会怎样？在商业上的后果是明显的。随着网络规模变得越来越大，对网络进行管理变得越来越难。实际上，我们应该对网络规模进行限制，以将它控制在现有工具可以处理的范围内。服务提供商发现安装、配置与控制设备与服务是困难的。大型
5 企业网络的管理员会抱怨网络超过他们处理问题的能力。

由于企业越来越依赖于数据网络作为与用户、其他企业的主要连接，这个情况变得更加严重。网络管理的一个特定方面——网络停机变得突出。对于很多企业来说，网络停机或阻塞将会造成损失。具有讽刺意义的是，随着企业的发展与其网络达到一定的规模，用于诊断与修复问题的时间将会快速增加。因此，越成功的企业将会承担越多的风险。我们可以总结出：

> 由于企业越来越依赖于数据网络，并且网络规模接近现有管理工具的限制，因此研究自动网络管理系统变得非常关键。

1.11　分布式系统与新的抽象

网络管理研究是普通网络研究的一个部分。我们发现，对自动网络管理系统的研究需要了解基本网络之上的计算机科学的几个方面。当然，这就需要熟悉各种网络设备与它们在实际网络中的角色，以及用来配置这些设备的参数。另外，我们需要了解如何创建各种必要的、供软件使用的抽象。最后，创建网络管理软件需要熟悉大规模分布式系统的概念：通信应用、两阶段提交与并发数据访问控制。

实际上，当我们讨论创建网络管理系统与网络管理软件可能的体系结构时，关注点将会从网络与协议转移到系统方面。特别是，我们需要考虑如何收集与处理跨越多个站点的管理数据，以及很多管理功能都要使用的数据存储技术，例如分布式数据库系统。

在设计自动网络管理系统时，会遇到与分布式系统相同的问题：大规模。包括很多设备与服务的大型网络会跨越多个站点。例如，在很多网络中有上万台设备需要管理。更重要的是，大规
6 模会由于异构变得更复杂，很多大型网络包含很多类型的设备。

1.12　本书的其他部分

本书分为三个部分。第一部分介绍基础与背景知识。前面的章节描述了一组网络元素与它们在网络系统中角色的例子，说明了网络管理问题的范围与复杂性，以及对网络管理功能的工业标准定义。后面的章节将详细介绍网络管理的各个方面，并提供了有关功能要求与基本特点的例子。

本书的第二部分通过研究现有的工具与技术，将目标集中在现有的网络管理系统上。各章节将介绍工具与用于管理特定设备的接口的演变，简单网络管理协议的角色与基本模型，以及对 NetFlow 数据的分析。第 13 章提供了几个用于管理网络设备的脚本例子。

本书的第三部分将介绍网络管理的未来。各章节讨论了下一代系统应具有的特点、可能的体系结构与在设计上的权衡。第三部分提出了一系列问题与思考。

1.13　总结

网络管理是人类对网络了解最少的方面，并且是需要进行深入研究的课题。本书将介绍这个问
7 题，回顾已有的工具与技术，并概括用于构造完成自动网络管理的软件系统的可能体系结构。