普通高等教育“十一五”国家级规划教材

高职高专计算机系列

计算机网络管理与安全技术

李艇 编著

人民邮电出版社
POSTS & TELECOM PRESS

普通高等教育“十一五”国家级规划教材

高职高专计算机系列

计算机网络管理与安全技术

李 艇 编著

人民邮电出版社
POSTS & TELECOM PRESS
北 京

图书在版编目（CIP）数据

计算机网络管理与安全技术 / 李艇编著. —北京：人民邮电出版社，2008.4
普通高等教育“十一五”国家级规划教材，高职高专计算机系列
ISBN 978-7-115-17216-7

Ⅰ. 计… Ⅱ. 李… Ⅲ. ①计算机网络—管理—高等学校：技术学校—教材②计算机网络—安全技术—高等学校：技术学校—教材 Ⅳ. TP393

中国版本图书馆 CIP 数据核字（2007）第 179302 号

内 容 提 要

本书分为网络管理和网络安全两部分，共 9 章。主要内容包括网络管理概述、管理信息结构与管理信息库、SNMP 通信模型与 RMON 规范、网络管理系统、网络安全概述、网络安全技术、防火墙技术、Windows 操作系统安全和 Linux 操作系统安全。通过本书的学习，读者可以掌握计算机网络管理与安全的基本概念，熟悉现行的网络管理标准和网络安全技术应用，并具有网络管理系统和网络安全工具的实践操作能力。

书中每个实训内容都进行了屏幕录像，读者可以通过相关的辅助教学演示软件观看，非常适合于教学和自学。录像与电子课件等教学资源可在 www.ptpress.com.cn 下载区免费下载。

本书适合高职高专院校和应用本科院校计算机专业学生使用，也适合从事网络管理工作的读者学习参考。

普通高等教育“十一五”国家级规划教材
高职高专计算机系列
计算机网络管理与安全技术

◆ 编　　著　李　艇
责任编辑　张孟玮
◆ 人民邮电出版社出版发行　　北京市崇文区夕照寺街 14 号
邮编　100061　　电子函件　315@ptpress.com.cn
网址　http://www.ptpress.com.cn
北京隆昌伟业印刷有限公司印刷
新华书店总店北京发行所经销
◆ 开本：787×1092　1/16
印张：18.25
字数：443 千字　　2008 年 4 月第 1 版
印数：1 – 3 000 册　　2008 年 4 月北京第 1 次印刷

ISBN 978-7-115-17216-7 /TP

定价：28.00 元

读者服务热线：(010)67170985　印装质量热线：(010)67129223
反盗版热线：(010)67171154

编者的话

目前，无论是企业或事业单位的内部网络，还是IT业的运营公司，都迫切需要能够从事网络管理和网络安全技术应用的人才。高等院校开设“计算机网络管理与安全技术”课程的目的，就是让学生在这个重要的领域掌握新的技能以拓展自己的发展空间。

本书从高职高专与应用本科学生为培养目标组织编写，内容重点放在网络管理系统和网络安全工具的使用上，同时加强实践操作，以展现本书将理论、技术、应用、实际及产品融于一体，将教材的先进性、实用性和可读性融为一体的特色。本书力求尝试从理论到实践、从实训到技能的统一，使学生看得懂、可操作、可实现，以强化学生自主学习和职业能力的培养。

本书分为网络管理和网络安全两部分，选用了NetWin2000作为教学演示和实训的网络管理软件，并选用了若干免费版的网络安全工具作为教学实训软件平台。

本书参考课时为64学时，其中实训占24学时。本书内容安排如下：第1章网络管理概述，第2章管理信息结构与管理信息库，第3章SNMP通信模型与RMON规范，第4章网络管理系统，第5章网络安全概述，第6章网络安全技术，第7章防火墙技术，第8章Windows 操作系统安全和第9章Linux操作系统安全。书中的每个实训内容均配有屏幕录像，读者可以通过相关的辅助教学演示软件观看，非常适合于教学和自学。

本书还提供辅助教学资料，有需要的读者可与人民邮电出版社教材推广部联系（Teacher@ptpress.com.cn，010-67143005）。

本书得到了北京华信亿码科技发展有限公司技术总监董为群先生的指导并提供支持与帮助，在此谨表示衷心的感谢。

张峰晓、臧源、王田等同志为本书实训中的许多实验做了大量的基础性工作，郝芸、齐光磊、孟庆铂、庞莹和李楠同志为书稿的编辑和整理也做了许多工作，在此一并表示真诚的感谢。

限于本人的学术水平，书中难免存在错误和不当之处，敬请读者批评指正。

编　者
E-mail：litingcn@sina.com
2007 年 10 月　于天津

此为试读，需要完整PDF请访问：www.ertongbook.com

目　录

此为试读，需要完整PDF请访问：www.ertongbook.com

第 1 章 网络管理概述

随着计算机网络的普及和发展，各行各业都利用网络进行各种社会活动。而网络的正常运行是其生存和发展的有力保证。网络管理变得越来越重要，网络管理的质量直接影响网络的效益。另一方面，计算机网络的构成越来越复杂，互连的规模越来越大，而且连网的设备多为异构型、多制造商环境和多协议栈。这些都增加了网络管理的难度。从而，学习和研究网络管理技术是十分必要的和迫切的任务。

学习目标

- 掌握网络管理、网络管理系统和网络管理功能的基本概念
- 了解网络管理标准及其协议的发展
- 熟悉 SNMP 管理结构及工作机制

1.1 网络管理与网络管理系统

在早期的 ARPAnet 中，若网络运行不正常时，管理员通常使用一个简单的管理工具 Ping 对可能有问题的网络设备发 ICMP 报文，根据返回的 ICMP 报文头部的时间戳来确定通信目标的连通性和传输时延。由于当时的网络规模很小，网络设备不多，这种方法还是很有效。但随着网络规模的不断扩大，设备越来越多，这种方法就显得力不从心了。这是因为一方面 Ping 返回的信息很少，无法获取被管理设备的详细情况；另一方面用 Ping 程序对很多设备逐个测试检查，工作效率很低。在这种情况下，真正意义上的网络管理方案和实用系统才逐渐产生。可见，网络管理是控制一个复杂的计算机网络使其具有最高的效率和生产力的过程。而网络管理系统由一组软件组成，帮助网络管理人员完成日常的任务，大大提高了网络运行的效率和服务质量。

1.1.1 网络管理功能

国际标准化组织（ISO）定义了网络管理的关键功能且被标准和非标准的网络管理系统所广泛接受。其功能分类如下。

- 配置管理：提供互连服务的连续操作，执行控制、识别，从被管理对象采集数据。
- 故障管理：探测、隔离和纠正不正常操作。

- 性能管理：对被管理对象的行为和通信活动的效率进行评价。
- 安全管理：正确操作网络管理和保护管理对象。
- 计费管理：对使用的被管理对象进行识别和使用计费。

下面分别进行简要介绍。

1. 配置管理（Configuration Management）

配置管理是指网络中每个设备的功能、相互间的连接关系和工作参数，它反映了网络的状态。配置管理是用来识别、定义、初始化、控制与监测通信网中的管理对象。其功能有：

- 定义配置信息；
- 设置和修改设备属性；
- 定义和修改网络元素间的互连关系；
- 启动和终止网络运行；
- 发行软件；
- 检查参数值和互连关系；
- 报告配置现状。

2. 故障管理（Fault Management）

对一个复杂网络要维持正常操作，就必须将该系统视为一个整体来处理，每一个重要设备都要正常工作。网络故障管理包括及时发现网络中发生的故障，找出网络故障产生的原因，必要时启动控制功能来排除故障。其功能有：

- 检测管理对象的故障现象，接收其故障报警；
- 利用空余网络对象为故障对象提供临时网络服务；
- 创建与维护差错日志，对差错日志进行分析；
- 进行故障诊断，明确故障性质和解决方案；
- 维修和排除对象故障，恢复正常网络服务。

3. 性能管理（Performance Management）

网络性能管理活动是持续地评测网络运行中的主要性能指标，以检验网络服务是否达到了预定的水平，找出已经发生或潜在的瓶颈，报告网络性能的变化趋势，为网络管理决策提供依据。其功能有：

- 从管理对象中收集与性能有关的数据；
- 对与性能相关的数据进行分析与统计；
- 根据统计分析的数据判断网络性能，报告当前网络性能，产生性能警告；
- 将当前统计数据的分析结果与历史模型进行比较，以便预测网络性能变化趋势；
- 形成并调整性能评价标准与性能参数标准值，根据实测值与标准值的差异去改变操作模式，调整网络管理对象的配置；
- 实现对管理对象的控制，以保证网络的性能达到设计要求。

4. 安全管理（Security Management）

安全管理功能是用来保护网络资源的安全。安全管理活动能够利用各种层次的安全防卫

机制，使非法入侵事件尽可能少发生；能够快速检测未授权的资源的使用，并查出侵入点，对非法活动进行审查与追综；能够使网络管理人员恢复部分受破坏的文件。其功能有：

- 系统数据的保密性，即保护系统数据不被侵入者非法获取；
- 用户账号管理，即建立合法的用户账号；
- 用户授权，即防止非法侵入者在系统上发送错误信息；
- 访问控制，即控制用户对系统资源的访问；
- 对授权机制和关键字的加密/解密作业管理。

5. 计费管理（Accounting Management）

对于公用分组交换网和各种网络信息服务系统来说，用户必须为使用网络的服务而缴费，网络管理系统则需要对用户使用网络资源的情况进行记录并核算费用。

在大多数企业内部网中，内部用户使用网络资源并不需要缴费，但是计费功能可以用来记录用户对网络的使用时间，统计网络的利用率与资源使用等情况，使网络管理员处于一个有利的位置来计划网络的发展。其功能有：

- 通过网络的利用率确定不同时期与时间段的资费标准；
- 根据用户使用资源的情况来分摊费用；
- 支持采用信用记账方式收取费用方式；
- 当用户在一次服务时使用了多种信息资源时，能够将分别计费的各个资源的费用累加。

1.1.2 网络管理系统

网络管理系统提供了一组进行网络管理的工具，网络管理人员对网络的管理水平在很大程度上依赖于这组工具的能力。网络管理软件可以位于主机内，也可以位于传输设备中。一个网络管理系统应该提供5种网络管理功能，并提供图形化的用户界面，这样的网络管理系统也称为网络管理平台。简单的网络管理系统则可以完成一部分或某一方面的网络管理功能。网络管理系统把整个网络看成一个统一的结构，每个节点有自己的地址和特有的属性，它们通过路由或交换设备连接在一起。

1. 网络管理系统的作用

- 协助网络管理者完成常规任务。
- 对于大型异构网络，可跟踪大量的关键信息以确定网络的运行状况。

总之，网络管理系统帮助网络管理者有效地控制和维护网络设备。在复杂的网络环境中给网络管理者提供更高水平的帮助，使得网络更加适合于用户的需要。

2. 网络管理平台简介

对于高度复杂的信息技术基础设施，需要一个强大的系统工具来管理。目前主要的系统管理软件有：HP公司的OpenView、IBM公司的NetView、SUN公司的SunNet、Cisco公司的CiscoWorks以及华信亿码公司的NetWin 2000。

目前，国际上的网络管理软件主要分三类：专用网络管理软件、通用网络管理软件及网络应用管理软件。NetWin 2000，OpenView，SunNet 和 NetView 等属于通用网络管理软件，而像 CiscoWorks 则属于专用网络管理软件。它们各有其优缺点：专用网络管理软件是为自家网络设备专门设计的，具有较强的管理功能，而通用性一般较差；而通用网络管理软件具有较好的开放性和兼容性，可用于对不同厂商产品的分布式管理，但在设备的配置和深度管理方面却无法与专用网络管理软件相比。

1.2 网络管理标准

随着网络应用系统的日益浩繁，产生了对网络管理系统的迫切需求，从而推动了网络管理技术的进步。ISO 在 1989 年颁布了第一个关于网络管理的国际标准性文件，即 ISO DIS 7498-4（X.700）。其定义了网络管理的基本概念和总体框架，后来在 1991 年发布的两个文件中规定了网络管理提供的服务和网络管理协议，ISO 9595 公共管理信息服务定义（Common Management Information Service，CMIS）和 ISO 9596 公共管理信息协议规范（Common Management Information Protocol，CMIP）。1992 年公布的 ISO 10164 和 ISO 10165 两个文件中分别定义了系统管理功能（System Management Functions，SMFs）和管理信息结构（Structure of Management Information，SMI）。这些文件共同组成了 ISO 的网络管理标准。其管理信息采用了面向对象的模型，管理功能包罗万象，另外还有一些附加功能和一致性测试方面的说明。由于其过于复杂，有关 ISO 管理的实现进展缓慢，至今还没有真正实用的网管产品。

另一方面，随着 Internet 的迅猛发展，有关 TCP/IP 网络管理的研究活动十分活跃，其网络管理标准的广泛应用已达到了普及化的程度。

TCP/IP 网络管理最初使用的是 1987 年 11 月提出的简单网关监控协议（Simple Gateway Monitoring Protocol，SGMP）。在此基础上改进成简单网络管理协议第一版（Simple Network Management Protocol，SNMPv1）。在 20 世纪 90 年代初又公布了几个 RFC（Request For Comments）文件，即 RFC1155（SMI），RFC1157（SNMP），RFC1212（MIB 定义）和 RFC1213（MIB-Ⅱ规范）。由于其简单性和易于实现，SNMPv1 得到了许多厂商的支持和广泛的应用。几年后在此基础上改进其功能并增加安全性，产生了 SNMPv2。由于 SNMPv2 没有达到“商业级别”的安全要求，1999 年 4 月发布了最新的网络管理标准 SNMP v3。

在计算机网络异常迅猛发展的过程中，由于网络管理标准的制订，使计算机网络系统的管理技术不断取得突破性的进展，并成为特色鲜明的里程碑。目前正处于通信设备网络管理和综合网络系统管理的阶段。

1.2.1 通信网络设备的管理

随着网络规模的增大，复杂性的增加和异构性增强，简单专用的网络管理技术已不能适应网络的迅速发展，特别是不能适应网络异构互连的发展趋势。研究开发者们开展了对网络管理的广泛研究，并提出了多种网络管理解决方案。通信网络设备管理阶段的代表是基于 SNMP 的网络管理体系结构。

SNMP 已成为网络管理领域中事实上的工业标准，大多数网络管理系统和平台都是基于 SNMP 的体系结构。

通信设备管理阶段的特点是集中式网络管理体系结构，采用 SNMP 网络管理协议，管理的对象主要是针对网络互连设备，例如：路由器、交换机、打印机、UPS 等设备。

1.2.2　综合网络系统的管理

在通信网络设备的管理阶段，许多优秀的网络管理软件产品对网络通信设备本身出现的各种故障、性能、安全、计费和配置都能进行良好的管理。但是随着通信网络质量的不断提高，应用服务的不断增加，网络规模的日益扩大和复杂，原来基于 SNMP 的网络管理解决方案越来越不能满足网络发展的需要。如何在管理好通信网络的基础上，管理好数据库、操作系统、应用程序等服务；如何让 SNMP 集中式的管理策略转向分布式的管理策略；如何减少人为干扰，形成自动的、智能的网络管理系统则是综合网络系统的管理问题。

目前，综合网络系统的管理特点是采用分布式/分层式网络体系结构，网络互连设备与网络应用程序的集成，多种网络管理协议的集成。同时将系统管理和网络统一成一个管理平台，使得管理范围包括服务器、客户端硬件和操作系统平台的管理、网络管理、数据库管理、Internet/Intranet 管理以及其他应用程序的管理。

1.3　网络管理协议的发展

在网络发展的很长时间里，网络管理者都要学习各种从不同网络设备获取数据的方法。这是因为不同厂商开发出的网络产品有着各自专有的获取数据的方法。这样对于两个具有相同功能的设备，但由于来自不同的生产厂商，其提供的数据收集方法可能大相径庭。

在 Internet 发展的早期并没有专门的网络管理协议，唯一可用于网络管理的协议是 ICMP。当网络运行不正常时，管理员使用 Ping 程序向可能有问题的网络设备发送 ICMP 报文，根据返回的 ICMP 报文头的时间戳来确定问题的性质和方位。虽然利用 Ping 能够检测网络的连通性，但是也有许多问题。例如，不可靠的传送和返回信息有限等。另外，在确定了问题之后，网络管理者还需要依赖于其他的方法分离并修复问题。

然而，网络管理协议提供了一种可访问任何网络设备并获得一系列标准值的一致性方式。标准网络管理协议可以对网络设备进行查询，包括设备的名字、设备中软件的版本、接口数和接口每秒的包数；还可以对网络设备进行参数的设置，包括设备的名字及运行状态和接口地址及运行状态。

以下是几种标准网络管理协议。

（1）简单网络管理协议（SNMP）。

（2）OSI 网络管理协议公共管理信息服务（CMIS）和公共管理信息协议（CMIP）。

CMIS 定义了每个网络组成部分提供的网络管理服务，而 CMIP 是实现 CMIS 服务的协议。CMIS/CMIP 是用于所有网络设备的完整的网络管理协议簇。其功能远比 SNMP 复杂。

（3）在 TCP/IP 协议簇之上实现 CMIS 服务的公共管理信息服务与协议 CMOT。

（4）IEEE 802.1b 局域网个人管理协议（LMMP），为 LAN 环境提供一个网络管理方案。该协议由 3Com 和 IBM 公司开发，它直接位于 IEEE 802 逻辑链路层之上而不依赖于任何特定的网络层协议进行网络传输。LMMP 比 CMIS/CMIP 或 CMOT 易于实现。

1.4 SNMP 管理结构及工作机制

在网络管理中一般采用管理站—代理模型，如果各个厂商提供的管理者和代理之间的通信方式各不相同，将会大大地影响网络管理系统的通用性以及不同厂商设备之间的连通性。因此需要制订一个管理站和代理之间通信的标准，这就是网络管理协议。其中 SNMP 提供了一个标准化的网络管理框架，使得互连网络的监视和控制成为可能。SNMP 是一个简单的但可扩展的标准集。其采用管理站/代理模式，管理协议在应用层上运行。SNMP 的成功主要在于它的简单性、灵活性和可扩展性。

1.4.1 网络管理模式

网络运行中心对网络及其设备的管理有 3 种方式：本地终端方式、远程仿真终端登录（telnet 命令）方式和基于 SNMP 的代理/服务器方式。

1. 本地终端方式

本地终端方式是通过被管理设备的 RS-232 接口与网管机相连接，进行相应的监控、配置、计费、性能和安全等管理的方式。这种方式一般适用于管理单台重要的网络设备，例如路由器等。

2. 远程仿真终端登录方式

远程仿真终端登录方式是通过计算机网络对已知地址和管理口令的设备进行远程登录，并进行各种命令操作和管理。这种方式也只适用于对网络中的单台设备进行管理。其与本地终端方式管理的区别是远程仿真终端登录方式可以异地操作，不必亲临现场。

3. 基于 SNMP 的代理/服务器方式

在 SNMP 管理模型中，有 3 个基本组成部分：管理站（manager）、代理（agent）和管理信息库（MIB）。SNMP 的管理模式如图 1-1 所示。

管理站是一个或一组软件程序，它一般运行在网络管理中心的主机上，它可以在 SNMP 的支持下命令代理执行各种管理操作。

代理是一种在被管理的网络设备中运行的软件，负责执行管理进程的管理操作。管理代理直接操作本地信息库，可以根据要求改变本地信息库或将数据传送到管理进程。

管理信息库是一个概念上的数据库，它是由管理对象组成的，每个管理代理管理 MIB 中属于本地的管理对象，各管理代理控制的管理对象共同构成全网的管理信息库。

此为试读，需要完整PDF请访问：www.ertongbook.com