面向21世纪

高职高专系列教材

网络管理与维护

◎王兴宝　主编

◎姜国忠　审

机械工业出版社
China Machine Press

面向21世纪高职高专系列教材

网络管理与维护

王兴宝　主编

姜国忠　审

机械工业出版社

本书针对 Windows NT 4.0 网络操作系统，系统、全面地介绍了计算机网络管理和维护的基本知识，内容包括网络管理概述、Windows NT 网络的安装与配置、用户管理、资源管理、服务器管理、磁盘管理和容错技术、性能监视、TCP/IP 协议和服务（包括 DHCP、WINS、DNS、RAS、IIS 等）的配置、Windows 2000 Server 网络新功能等，每章后均有一定数量的习题，书后附有实验参考资料。

本书在阐明网络管理基本概念的基础上，以网络管理的对象、内容为线索来组织材料，系统、全面地介绍了 Windows NT 网络管理的基本内容和操作技术，同时也融入了一般的网络管理理论，内容详实、条理清楚、深入浅出、可读性强，可作为高职高专院校计算机应用及相关专业网络管理课程的教材，也可供企事业单位计算机网络管理和使用人员及网络爱好者参考。

图书在版编目（CIP）数据

网络管理与维护/王兴宝主编. —北京：机械工业出版社，2001.6
面向 21 世纪高职高专系列教材
ISBN 7-111-08286-9

Ⅰ.网… Ⅱ.王… 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-维修-高等学校：技术学校-教材 Ⅳ.TP393.07

中国版本图书馆 CIP 数据核字（2001）第 20768 号

机械工业出版社（北京市百万庄大街 22 号 邮政编码 100037）
策　　划：胡毓坚
责任编辑：周艳娟
责任印制：郭景龙

北京京丰印刷厂印刷·新华书店北京发行所发行

2001 年 9 月第 1 版·第 2 次印刷
1000mm×1400mm B5·8.125 印张·373 千字
5 001—9 000 册
定价：22.00 元

凡购本图书，如有缺页、倒页、脱页，由本社发行部调换
本社购书热线电话（010）68993821、68326677-2527

面向21世纪高职高专
计算机专业系列教材编委会成员名单

顾问	曾玉崑　王文斌　陈瑞藻　李　奇　凌林海
	林　东
主任委员	周智文
副主任委员	周岳山（常务副主任）　詹红军　陈付贵
	穆天保　赵佩华　黄甘洲　武文侠　吕何新
委员	郭曙光　王德年　刘瑞新　陈丽敏　孔令瑜
	李　玲　鲁　辉　陶书中　赵增敏　马　伟
	孙心义　翟社平　廖常武　于恩普　王春红
	王娟萍　屈　圭　汤新广　谢　川　姜国忠
	汪赵强　董　勇　梁国浚　张晓婷
秘书长	胡毓坚
副秘书长	陈丽敏（兼）

出版说明

积极发展高职高专教育，完善职业教育体系，是我国职业教育改革和发展的一项重要任务。为了深化职业教育的改革，推进高职高专教育的发展，培养 21 世纪与我国现代化建设要求相适应的，并在生产、管理、服务第一线从事技术应用、经营管理、高新技术设备运作的高级职业技术应用型人才，尽快组织一批适应高职高专教学特色的教材，已成为各高职高专院校的迫切要求。为此，机械工业出版社与高职高专计算机专业、电子技术专业和机电专业教材编委会联合组织了全国 40 多所院校的骨干教师，共同研究开发了一批计算机专业、电子技术专业和机电专业的高职高专系列教材。

各编委会确立了“根据高职高专学生的培养目标，强化实践能力和创新意识的培养，反映现代职业教育思想、教育方法和教育手段，造就技术实用型人才为立足点”的编写原则。力求使教材体现“定位准确、注重能力、内容创新、结构合理和叙述通俗”的编写特色。

本套系列教材是由高职高专计算机专业、电子技术专业、机电专业教材编委会分别会同各院校第一线专业教师针对高职高专计算机、电子技术和机电各专业的教学现状和教材存在的问题开展研讨，尤其针对目前高职高专教学改革的新情况，分别拟定各专业的课程设置计划和教材选题计划。在教材的编制中，将教学改革力度比较大、内容新颖、有创新精神、比较适合教学、需要修编的教材以及院校急需、适合社会经济发展的新选题优先列入选题规划。在广泛征集意见及充分讨论的基础上，由各编委会确定每个选题的编写大纲和编审人员，实行主编负责制，编委会通过责任编委和主审对教材进行质量监控。

担任本套教材编写的老师们都是来自各高职高专院校教育第一线的教师，他们以高度的责任感和使命感，经过近一年的努力，终于将本套教材呈现在广大读者面前。由于高职高专教育还处于起步阶段，加上我们的水平和经验有限，在教材的选题和编审中可能出现这样那样的问题，希望使用这套教材的教师和学生提出宝贵的意见和建议，以利我们今后不断改进，为我国的高职高专教育事业的繁荣而共同努力。

高职高专系列教材编委会
机 械 工 业 出 版 社

前　言

本书的主要内容大致上包括网络系统的安装和配置、用户管理、资源管理、性能监视和系统维护等。对于大型计算机网络来说，需要有专门的“网络管理”软件对网络系统运行情况进行动态的监视和全面的管理，而在中、小型网络中，网络的各种功能是通过网络操作系统以及在此基础上运行的应用程序来实现的，网络管理的基本功能也是由网络操作系统提供的。因此，讨论网络管理的问题离不开具体的网络操作系统。

目前流行的网络操作系统种类比较多，在有限的篇幅内，只能选择一种较流行的系统来讲述。由于 Windows NT Server 4.0 具有功能强大、用户界面友好、易学易用等特点，不仅能够胜任局域网服务器，并且能够在网络的各个层次（包括从最简单的对等网到 Internet/Intranet 应用）上适应用户的需要，已成为目前市场上占主导地位的网络操作系统。通过学习 Windows NT，可以较好地掌握现代计算机网络管理与维护的基本概念和基本知识。因此，本教材以 Windows NT 4.0 为背景网络来讲述计算机网络管理和维护的基本知识。Windows NT Server 4.0 的后续版本是 Windows 2000 Server，它在 Windows NT 4.0 的基础上增加了许多新的网络功能，对原有的功能也进行了很大的改进，并引入了许多新的概念。为了便于读者学习，在本书中安排一章专门讲述 Windows 2000 Server 中的网络新功能和重要概念。

本书在概括性地介绍了网络管理与维护的基本知识之后，系统、全面地介绍了 Windows NT 网络管理与维护的基本概念和技术。书中以网络管理的对象、内容为线索来组织材料和安排章节，对网络管理的任务、目标、环境、条件的解释与具体操作步骤的描述相兼顾，书中的大部分插图取自作者的实际操作过程，对概念的论述力求准确、严谨，便于读者学习、理解和记忆。

本书是作为高职高专院校网络管理与维护课程的教材而编写的，也可作为 Windows NT 网络的参考书。为了便于教学，每章后都附有一定数量的习题，附录中还给出了实验参考资料。本课程的教学总时数（包括课堂教学和实验课时在内）以安排 60 学时左右为宜。

本书第 1、3、4、5、6、7、8、9、11、12 章由王兴宝编写，第 2 章由霍江明编写，第 10 章和附录由张晓琦编写，王兴宝担任主编并负责统编全书、定稿。在本书的编写过程中，得到了所在单位领导、师生的大力支持和帮助；姜国忠老师审阅了全部书稿，并提出了重要的修改意见，在此一并表示感谢。

限于作者的学术水平，错误和疏漏之处在所难免，敬请读者不吝赐教。

编　者

目　录

第 1 章　网络管理概述

网络管理是通过规划、监视、分析、扩充和控制网络来保证网络服务的有效实现。随着网络规模的扩大和复杂性的增加，网络管理已成为保证网络高效、稳定、安全可靠地运行的必要手段，是整个网络系统不可缺少的重要部分。

本章将介绍网络管理的目标、功能，以及网络安全和网络管理系统的基本知识。

1.1　网络管理的基本任务

1.1.1　网络管理的目标

网络管理的目标是最大限度地增加网络的可用时间，提高网络设备的利用率、网络性能、服务质量和安全性，简化多厂商混合网络环境下的管理和控制网络的运行成本，提供网络的长期规划。它可以在多厂商混合网络下通过单一的网络操作控制环境来管理所有的子网和被管理的设备，以集中、统一的方式远程控制网络，用于排除故障和重新配置网络设备。

一个网络管理系统应该满足以下要求。

1.提供网络监视和控制能力

网络监视功能可以使管理员掌握网络的当前状态，而网络控制功能可以使管理员采取措施影响网络的运行状态，网络管理功能应同时包含这两方面的能力。例如，在故障管理中，网络监视能力用来发现和诊断网络故障，网络控制能力用来隔离故障和定位故障，最终排除故障。

2.能够管理所有的网络协议

现代网络体系结构是分层设计的，网络的功能和完成这些功能的协议也是分层的，不同层次的协议完成不同的功能。通用的网络管理系统应该能够管理网络中尽可能多的协议。

3. 尽可能大的管理范围

不仅管理点到点的网络通信，还应管理端到端的网络通信；不仅管理基本的网络设备，还应管理应用层的网络应用。

4. 尽可能小的系统开销

管理尽可能多的网络协议和尽可能大的范围是以增大系统开销作为代价的，应该根

据实际情况对网络管理的范围和所需的系统开销作一个合理的分配和选择。在同样的网络管理下，尽可能减少系统开销，提高网络的运行效率。

5. 可以管理不同厂家的网络设备

现代大型计算机网络一般由不同厂家提供的设备连接而成，网络管理和运行应该不受具体厂家设备的限制。

6. 支持不同的网络管理系统

大型计算机网络一般会连接不同的城域网或局域网，这些网络可能由不同的网络管理系统来管理。尽可能支持不同的网络管理系统，形成全网统一的网络管理运行机制是十分重要的。

7. 网络管理的标准化

为了更好地管理不同厂家的网络设备，支持不同的网络管理平台，需要制定网络管理标准。国际标准化组织(ISO)十分重视网络管理的标准化工作，制定了一系列网络管理标准，Internet 体系结构委员会在实践中形成了一整套的网络管理工业标准，在设计和运行网络管理系统时，应该采用标准化的网络管理机制和协议。

1.1.2 网络管理的功能

网络管理涉及网络资源和活动的规划、组织、监视、计费和控制，在 OSI 网络管理模型中，基本的网络管理功能被划分成五个模块，这五个模块分别完成不同的网络管理功能，它们分别是：故障管理、配置管理、性能管理、记账管理和安全管理。

1.故障管理

故障(Fault)管理是基本的网络管理功能，它包括故障检测、故障诊断和故障恢复等工作，其目的是保证网络能够提供连续可靠的服务。

由于网络服务的意外中断往往会造成很大的影响，而且，在大型计算机网络中发现故障时，往往不能立刻确定故障的具体位置，这就需要故障管理提供逐步隔离和最后定位故障的一整套解决方案。有时候，发现的故障是随机性的，需要经过很长时间的跟踪和分析才能找到原因，要圆满地解决这些问题，需要一个故障管理系统，能够自动发现故障，自动报警，具体记录每一个故障的信息，跟踪分析，直到最后确定并排除故障。

2. 配置管理

配置(Configuration)管理负责监控网络的配置信息，使网络管理人员可以生成、查询和修改软件和硬件的运行参数及条件，以保持网络的正常运行。配置管理功能至少包括：识别被管理网络的拓扑结构；标识网络的各个对象；自动修改指定设备的配置；动态维护网络配置数据库等。

一个计算机网络是由各种各样的设备连接而成的，这些设备组成网络的物理结构和

逻辑结构。为更好地控制网络设备，要求网络管理系统能够定义、组织和管理各种设备的参数、状态和名字等信息，这对于一个大型计算机网络的运行是至关重要的。另外，网络运行的环境是经常变化的，网络系统配置也要随着用户的增加、减少或设备的维修而经常调整，使其更有效地工作，配置管理功能可以完成以上的任务。

3. 性能管理

性能(Performance)管理涉及到网络通信(信息流量、谁在使用、访问什么资源等)的收集、加工和处理等一系列活动，其目的是在使用最少的网络资源和达到最小延迟的前提下，保证网络提供可靠、连续的通信能力。

性能管理的具体内容包括从被管对象中收集与网络性能有关的数据，分析和统计历史数据，建立性能分析模型，评价被管对象行为和通信活动的有效性，预测网络性能的发展趋势，并根据分析和预测的结果，找出系统性能瓶颈，优化和调整网络拓扑结构及各种设备的配置和参数，以达到提高网络性能的目的。

4. 计账管理

计账(Accounting)管理的功能体现在两个方面：

(1) 在网络通信资源和信息资源有偿使用的情况下，计账管理能够统计到哪些用户利用哪些通信线路传输了多少信息以及访问了哪些资源等信息，经统计汇总后作为收费的依据。

(2) 在非商业化的网络上，计账管理可以统计不同线路的利用情况和不同资源的利用情况，为优化或扩充网络提供依据。譬如某条线路长期拥挤，那么应该考虑是否扩充；如果某些资源被频繁访问，那么应该考虑是否设置一个镜像服务器等。

对于商业化的计算机网络，记账系统要包含更多更详细的信息，如每次通信的开始时间、结束时间、通信中传送的数据等信息，并使用户能够查询这些信息，还要选择一种用户可以接受的计费方法。

5. 安全管理

安全管理有两层含义：一方面，安全管理要保证网络用户和网络资源不被非法使用；另一方面，网络安全管理也要确保网络管理系统本身不被非法使用。

网络安全管理的主要内容包括：与安全管理措施有关的信息分发(如密钥的分发和访问权设置等)；与安全有关的事件通知(如对网络的非法侵入、未授权用户对特定信息的访问企图等)；安全服务设施的创建、控制和删除；与安全有关的网络操作的记录、维护和查询等日志管理工作等。一个计算机网络的管理系统必须制定网络管理的安全策略，并根据这个策略设计和实现网络安全管理系统。

上述的网络管理功能不是互相孤立的，完成某项管理功能往往需要其他管理功能的配合，比如故障管理需要从性能管理得到当前的运行分析结果，从配置数据库得到设备的配置信息；一旦确认发生故障，通过配置管理修改配置参数，修复、替换或隔离故障部件；将网络故障情况作为网络状态数据移交性能，以分析网络的可用性参数。由此可见，网络

管理可看作是一组过程和任务的集成。

1.2 网络安全管理

随着计算机网络技术的发展，网络的安全和可靠成为不同使用层次的用户共同关心的问题，解决好网络的安全问题，是保证网络正常运行的前提和保障，也是计算机网络管理的重要内容之一。

1.2.1 影响网络安全的因素

影响计算机网络安全的因素多种多样，但归纳起来主要有如下几个方面。

1. 环境因素

计算机网络通过有线链路或无线电波连接不同地域的计算机或终端，线路中经常有信息传送，恶劣的自然环境对计算机网络会产生不良影响，例如温度、湿度、防尘条件、地震、风灾、火灾等天灾以及事故都会对网络造成严重的损害和影响；强电、磁场会毁坏传输中和信息载体上的数据信息；雷电能轻而易举地穿过电缆，损坏网络中的计算机，使网络陷于瘫痪。

2. 资源共享

计算机网络实现资源共享，包括硬件共享、软件共享、数据共享。各个终端可以访问经济的资源，各终端之间也可以相互共享资源。资源共享在为用户提供巨大方便的同时，也给非法用户窃取信息、破坏信息创造了条件。非法用户有可能通过终端或节点进行非法浏览、非法修改。此外，由于硬件和软件故障也会引起泄密，同时，大多数共享资源同它们的许多使用者之间有相当一段距离，例如网络打印机，这样就给窃取信息在时间和空间上提供了便利条件。

3. 数据通信

计算机网络通过数据通信来交换信息，这些信息是通过物理线路、无线电波以及电子设备进行传输的，在通信中传输的信息容易遭到窃听，例如通过搭线窃听、网络线路的辐射等。

4. 计算机病毒

计算机网络可以从多个结点接收信息，因而极易感染计算机病毒。病毒一旦侵入，在网络内再按指数增长进行再生传染，很快就会遍及网络各结点，轻则使系统的效率明显降低，严重时可以造成网络的瘫痪。

5. 网络管理

网络系统的正常运行离不开系统管理人员对网络系统的管理，所有的安全措施，都要

经管理人员进行配置后才能有效的实施。从技术的角度来说，不恰当的配置会增加系统管理、使用的复杂性或降低系统的安全性。另外，由于组织管理措施不当，会造成设备的损坏和保密信息的人为泄露等。

1.2.2 网络的安全级别

在增加计算机网络安全性的同时，也必然会增加系统的复杂性，并且使系统的管理和使用更为复杂，因此，并非安全性越高越好。为了帮助用户区分和解决计算机网络的安全问题，美国国防部公布了“可信计算机系统标准评估准则”(称为“桔黄皮书”)，对多用户计算机系统安全级别的划分进行了规定。

“桔黄皮书”将计算机网络的安全由低到高分为四类七级：即 D1、C1、C2、B1、B2、B3、A1。通过这些分类可以了解在一些系统中固有的各种安全风险，并能掌握如何减少或排除这些风险的方法，下面是各个级别的情况。

- D1 级。计算机网络的最低一级，不要求用户进行登录和密码保护，任何人都可以使用，整个系统是不可信任的，硬、软件都易被侵袭。常见的属于 D1 级的系统有：MS-DOS、MS Windows 3.x 等。
- C1 级。自主安全保护级，要求硬件有一定的安全措施(如计算机带锁)，用户必须通过登录认证方可使用系统，并建立了访问许可权机制。但 C1 级不能控制进入系统的用户访问级别，用户可以直接访问操作系统的根。常见的属于 C1 级的计算机系统有：早期的 UNIX、XENIX 以及 Windows 95/98 等。
- C2 级。受控垫取保护级，比 C1 级增加了如下几个特性：引进了受控访问环境(用户权限级别)，进一步限制了用户执行某些系统指令；授权分级使系统管理员给用户分组，授予他们访问某些程序的权限或访问分级目录，数据访问控制为目录级；采用系统审计，跟踪记录所有安全事件及系统管理员的工作。达到 C2 级的常见计算机系统包括：UNIX、XENIX、NOVELL Netware 3.x/4.x、Windows NT 等。
- B1 级。标记安全保护级，对网络上的每一个对象都实施保护；支持多级安全，对网络、应用程序、工作站实施不同的安全策略；对象必须在访问控制之下，不允许拥有者自己改变所属资源的权限。B1 级计算机系统的主要拥有者是政府机构和防御承包商。
- B2 级。结构化保护级，对网络和计算机系统中的所有对象都加以定义，分配一个固定的标签；为工作站、终端、磁盘驱动器等设备分配不同的安全级别；按照最小特权原则取消权力无限大的特权用户，任何一个人都不能享有操纵和管理计算机系统的全部权力。
- B3 级。安全域级，要求用户工作站或终端必须通过信任的途径连接到网络系统内部的主机上；采用硬件来保护系统的数据存储区；根据最小特权原则，增加了系统安全员，将系统管理员、系统操作员和系统安全员的职责隔离，将人为因素对计算机安全的威胁减至最小。
- A1 级。验证设计级，本级包括了以上各安全级别的所有措施，并附加了一个安全系统的受监视设计，合格的个体必须经过分析并通过这一设计；所有构成系统部件的来源都必须有安全保证，还规定了将安全计算机系统运送到现场安装所必须遵

守的程序。

综上所述，D1 级是不具备最低安全限度的等级；C1 级是具备最低安全限度的等级，适合在小范围内使用；C2 级是具备基本安全保护能力的等级，可以满足一般应用的安全要求，现在常用的网络操作系统（例如 Windows NT 和 Netware）基本上属于这一等级；B1 级和 B2 级是具有中等安全保护能力的等级，基本可以满足一般的重要应用的安全要求；B3 级和 A1 级属于最高安全等级，只有极其重要的应用才需要使用这类安全等级。

1.2.3 网络的安全保护措施

网络系统安全等级是一种大致的划分，网络的实际安全性与所采用的具体安全措施和这些安全措施的实施情况有关。网络的安全保护措施主要从物理安全、访问控制和传输安全等三个方面来考虑。

1. 物理安全

物理安全主要是防止对网络设备和电缆等的非法使用和意外损坏等，物理安全控制的原则如下：

（1）所有的网络节点（包括交换机、集线器、主机、网络打印机等）都要设有物理保护，不能随意让人接触。

（2）重要的主机和网络设备配备 UPS 电源保护和备份电源。

（3）室外的网络电缆要深埋，并加以标识；室内采用结构化布线，并尽量减少外露的电缆和接头。

（4）机房要设有火灾、烟雾自动报警装置及常备灭火器等设施。

（5）机房的保护地线安装要符合有关标准。

（6）主服务器要加带口令的屏幕保护或键盘锁。

（7）所有的系统备份磁带（或磁盘、光盘）要保存在主机房以外的安全地方。

2. 访问控制

访问控制识别并验证用户的身份，将用户限制于已授权的活动和资源，网络的访问控制可以从以下几个方面来考虑规划。

（1）口令。网络安全系统的最外层防线就是网络用户的登录，在登录注册过程中，系统会检查用户的登录名和口令的合法性，只有合法的用户（登录名和口令都输入正确）才能进入系统。因此，只要知道系统的登录名和口令，任何人都可以进入系统。因为用户的登录名一般是不保密的，所以，口令的安全就非常重要。保护口令安全的基本措施有如下几条：

1）采用不易猜测、无规律的口令，字符数不能少于 6 个。

2）不同的系统采用不同的口令。

3）定期更换口令，最长不超过半年。

4）采用加密的方式保存和传输口令。

5）对每次的登录失败作记录并认真查找原因。