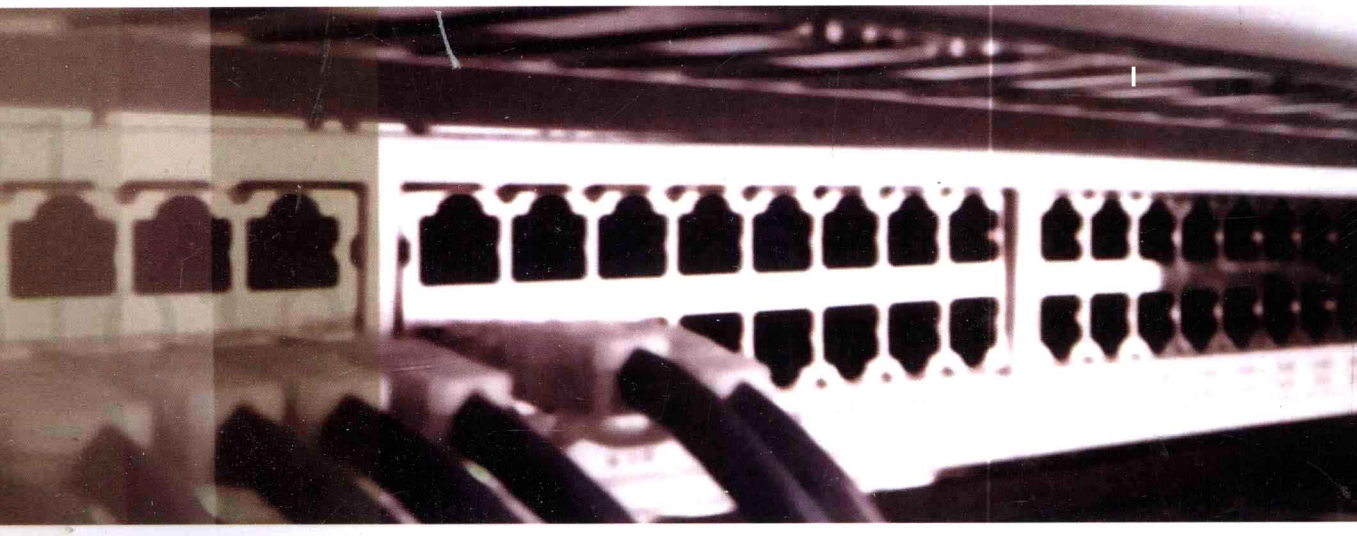
中小型企业

网络管理

实战宝典

——基于Windows平台

刘增杰　张俊斌　编著



全面讲解网络管理配置与部署

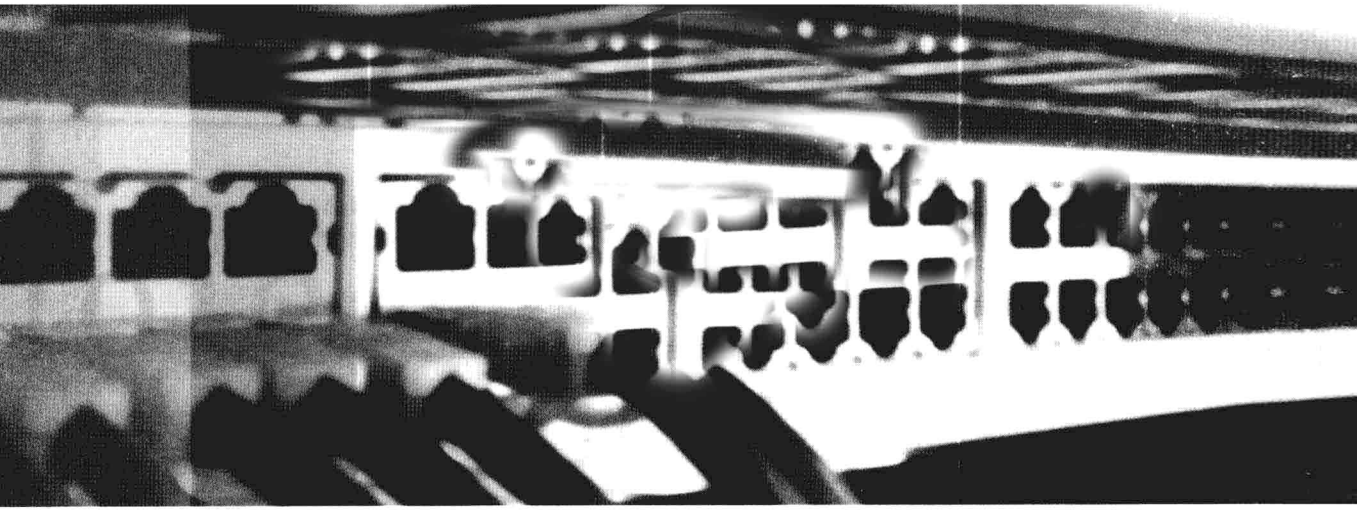
DVD 多媒体教学光盘

共66课全语音讲解
20小时视频教学

清华大学出版社

中小型企业
网络管理
实战宝典
——基于Windows平台

刘增杰　张俊斌　编著



清华大学出版社
北　京

内 容 简 介

本书主要介绍的是针对中小型企业的网络管理和网络安全技术，为了使读者清晰系统地认识网络管理和网络安全，本书将两者分为17章分别讲解。在内容组织上，网络管理首先从网管基础开始介绍，包括网络管理协议的介绍；其次以现实网络管理工程案例为背景进行需求分析及施工方案设计，给出网络管理过程中要实施的管理模块；然后，后面章节的内容根据前面需求分析给出的管理模块分别进行实现。网络安全的内容组织形式和网络管理相似。这种方式可以使读者循序渐进地学习，同时也可以让读者系统地了解现实网络管理及网络安全工程的施工流程等内容，便于读者举一反三，胜任中小型企业的网络管理工作。随书光盘中赠送了20小时培训班形式的视频教学录像，真正体现本书“完全”的含义，令其物超所值。

本书内容丰富全面，图文并茂，深入浅出，使读者能够理解网络管理的精髓，并能解决实际生活或工作中的问题，真正做到知其然更知其所以然。它适用于对中小型企业管理感兴趣的零基础读者，计算机网络技术、网络工程、网络安全相关专业的学生；以及具有一定的网络基础知识，熟悉网络路由交换技术，熟悉网络服务器技术，能够实现简单网络搭建，对网络管理技术、网络安全技术感兴趣的工程师。

图书在版编目（CIP）数据

中小型企业网络管理实战宝典：基于Windows平台/刘增杰，张俊斌编著.—北京：清华大学出版社，2011.11

ISBN 978-7-302-26837-6

I. ①中… II. ①刘… ②张… III. ①中小企业－计算机网络－管理 IV. ①TP393.18

中国版本图书馆CIP数据核字（2011）第187061号

责任编辑：夏非彼　马颖君
责任校对：闫秀华
责任印制：杨　艳
出版发行：清华大学出版社　　地　　址：北京清华大学学研大厦A座
http://www.tup.com.cn　　邮　　编：100084
社　总　机：010-62770175　　邮　　购：010-62786544
投稿与读者服务：010-62776969，c-service@tup.tsinghua.edu.cn
质　量　反　馈：010-62772015，zhiliang@tup.tsinghua.edu.cn
印 装 者：北京艺辉印刷有限公司
经　　销：全国新华书店
开　　本：190×260　**印　张**：34　**字　数**：871千字
附光盘1张
版　　次：2011年11月第1版　　**印　　次**：2011年11月第1次印刷
印　　数：1～4000
定　　价：69.00元

产品编号：043663-01

前　言

随着网络技术的发展，中小型企业对于网络的管理与安全越来越重视，因此很多企业希望能招聘到有较高技术水平、实践能力的工程师。面对这种社会需求，很多学校也开设了网络管理及网络安全课程，但是其中的网络管理课程一般都是简单网络扫描软件的介绍，而在网络安全课程方面，大都以安全技术为主要内容，比如加密、认证、安全协议介绍等，对现实中的企业安全管理设备环境的架设涉及比较少。除此之外，在校学生大都停留在技术学习层面，对现实网络工程了解甚少，设备选型、项目施工流程等内容大都处于空白状态。

结合以上问题，如何让有意向成为网络工程师、网络管理员、网络安全工程师的人，在负担较小经济压力的前提下学到有价值的东西，成为了社会的主要需求。

而本书就是针对这一需求定制的。作者在网络工程、网络管理、网络安全方面从事了多年研究及毕业生培训、实训工作，本书由实训经验和企业网络环境总结而来。

本书内容

本书主要介绍的是针对中小型企业的网络管理和网络安全技术，并基于 Windows 的操作系统平台。本书将利用理论联系实际的方法，通过典型的实例向大家介绍网络管理的知识。

第 1 章介绍网络管理的技术基础，包括网络管理的五大职能、体系结构和网络管理实现模式分析等内容。

第 2 章介绍 SNMP 网络管理协议及其配置等。读者想要高效的完成网络管理任务，首先需要掌握 SNMP 协议的运行原理及相关运用技术。

第 3 章介绍中小型企业网络管理项目的需求分析和实施流程。读者想要实现完善的网络管理体系，必须掌握网络管理方案的设计原理。

第 4 章介绍网络基本信息的获取方法，并通过两个项目实例进行详细讲解。

第 5 章介绍主流网络管理平台的架设和应用，使读者掌握高效管理网络的方法。

第 6 章介绍服务器远程监控与管理，使读者掌握高效管理远程服务器的方法。

第 7 章介绍网络流量监测分析的工具及其使用方法，使读者掌握利用流量监测分析工具发现网络异常的方法。

第 8 章介绍企业网络主流监控产品及其使用方法，使读者掌握利用网络监控产品进行网络监管的方法。

第 9 章介绍网络安全的基础知识，包括攻击类型及防护策略。

第 10 章介绍企业网络安全项目分析和实施流程，使读者掌握中小型企业网络安全方案的设计原理。

第 11 章介绍 Windows Server 2008 系统安全及策略，使读者掌握系统安全的配置方法。

第 12 章介绍网络设备安全概述及其配置。

第 13 章介绍无线网络安全现状及其实施措施，使读者掌握小型无线局域网的使用及安全配置。

第 14 章介绍企业防火墙架设及配置，使读者掌握中小型企业防火墙的架设与应用方法。

第 15 章介绍反病毒系统及其配置实例，使读者掌握解决企业病毒威胁的方法。

第 16 章介绍 VPN 技术的概述及分类，使读者掌握使用 VPN 技术保证信息在互联网安全传输

的方法。

第 17 章介绍入侵检测系统的概述及分类，使读者掌握网络入侵安全问题的解决方法。

本书特色

理论联系实际：网络管理及网络安全均添加中小型企业中用得到的案例，以基础知识开始引入，帮助读者了解该项网络技术。本书采用中小型企业中使用较多，安全性、稳定性较高的软硬件产品工具。

一步一图，图文并茂：注重操作，图文并茂，在介绍案例的过程中，每一个操作均有对应的插图。这种图文结合的方式使读者在学习过程中能够直观、清晰地看到操作的过程以及效果，便于更快地理解和掌握。

易学易用：颠覆传统“看”书的观念，变成一本能“操作”的图书。

举一反三：同一类技术或产品，大都会介绍至少两款主流工具产品供读者学习使用，从而更加深刻理解网络管理知识，达到触类旁通的效果。以中小型企业环境为基础，同时兼顾必备的基础知识及设计原理，进而达到“知其然，并知其所以然”的效果。

实训效果：本书采用案例介绍、需求分析、实施流程规划及分步施工的顺序组织内容，方便读者系统的、模块化的学习，使读者通过阅读此书，能够达到网络实习的效果。

超值光盘：随书奉送 20 小时的培训班形式的视频教学录像，使本书真正实现“自学无忧”，成为一本物超所值的好书。

读者对象

本书是一本完整介绍中小型企业网络管理应用知识的教程，内容丰富，条理清晰，实用性强，适合以下读者学习使用：

- 对中小型企业管理感兴趣的零基础读者；
- 计算机网络技术、网络工程、网络安全相关专业的学生；
- 具有一定的网络基础知识，熟悉网络路由交换技术，熟悉网络服务器技术，能够实现简单网络搭建，对网络管理技术、网络安全技术感兴趣的工程师；
- 各行各业需要学习网络管理知识的人员。

鸣谢

本书作者长期从事网络实训的培训工作。参与本书编写人员除了封面署名人员以外，还有王英英、苏士辉、肖品、张少军、孙若淞、宋冰冰、王维维、梁云亮、程铖、臧顺娟、刘海松、陈伟光等人。虽然倾注了编者的努力，但由于水平有限、时间仓促，书中难免有错漏之处，请读者谅解，如果遇到问题或有意见和建议，敬请与我们联系，我们将全力提供帮助，编者电子邮箱为 liuyu_200882@163.com。

编者

2011 年 7 月

目　录

1.1 网络管理概述.avi/5 分钟
1.2 网络管理的发展.avi/9 分钟
1.3 网络管理的五大职能.avi/26 分钟
1.4 网络管理体系结构.avi/8 分钟
1.5 网络管理实现模式分析.avi/14 分钟

2.1 SNMP 概述.avi/10 分钟
2.2 SNMP 管理系统.avi/4 分钟
2.3 SNMP 实现机制.avi/8 分钟
2.4 SNMP 管理信息库 MIB.avi/4 分钟
2.5 远程监视 RMON.avi/4 分钟
2.6 SNMP 安全分析与安全机制.avi/5 分钟
2.7 配置 SNMP 网络管理协议.avi/18 分钟
2.8 典型 SNMP 网络管理案例.avi/10 分钟

3.1 项目介绍.avi/7 分钟
3.2 需求分析.avi/16 分钟
3.3 项目实施流程.avi/16 分钟

4.1 网络基本信息概述.avi/8 分钟
4.2 获取网络基本信息.avi/3 分钟
4.3 IP/MAC 地址扫描工具.avi/18 分钟
4.4 项目实施 1.生成基本信息库.avi/5 分钟
4.5 项目实施 2.利用基本信息库防止 ARP 欺骗.avi/15 分钟

5.1 网络管理平台介绍.avi/12 分钟
5.2 项目实施：搭建 Spiceworks 网络管理平台.avi/51 分钟
5.3 项目实施：搭建 WhatsUp Gold 网络管理平台.avi/48 分钟

6.1 服务器管理需求分析.avi/11 分钟
6.2 服务器性能指标分析.avi/8 分钟
6.3 服务器远程控制工具介绍.avi/11 分钟
6.4 项目实施 1.使用 51MyPC 轻松管理办公室中的电脑.avi/8 分钟
6.5 项目实施 2.使用 RemotelyAnywhere 远程管理服务器.avi/38 分钟

7.1 网络流量分析的意义.avi/5 分钟
7.2 主流产品技术分析.avi/12 分钟
7.3 科来网络分析系统.avi/13 分钟
7.4 项目实施 使用 sniffer 进行网络流量监测分析.avi/40 分钟

8.1 网络监管系统的意义.avi/3 分钟
8.2 主流监管产品.avi/4 分钟
8.3 项目实施.使用网路岗进行网络监管.avi/40 分钟

9.1 网络安全的概述.avi/21 分钟
9.2 网络攻击的入口.avi/8 分钟
9.3 寻找木马的藏身之处——进程.avi/17 分钟
9.4 网络安全防护策略.avi/13 分钟

10.1 项目介绍.avi/8 分钟
10.2 需求分析.avi/11 分钟
10.3 项目实施流程.avi/24 分钟

11.1 Windows 系统漏洞安全.avi/16 分钟
11.2 Windows 端口安全.avi/20 分钟
11.3 Windows 组策略安全.avi/23 分钟
11.4 项目实施.加强 Inetnet 信息服务安全.avi/2 分钟

12.1 网络设备安全概述.avi/8 分钟
12.2 网络设备安全配置.avi/90 分钟

13.1 无线网络现状.avi/9 分钟
13.2 无线安全实施措施.avi/20 分钟
13.3 项目实施.媒体访问控制（MAC）地址过滤.avi/4 分钟

14.1 防火墙概述.avi/30 分钟
14.2 项目实施 1.架设 ISA 企业防火墙.avi/30 分钟
14.3 项目实施 2.利用 ISA 控制员工上网.avi/28 分钟
14.4 项目实施 3.利用 ISA 发布企业内网服务器.avi/15 分钟

15.1 反病毒系统概述.avi/10 分钟
15.2 项目实施 1.ESET NOD32 企业反病毒系统实战案例.avi/49 分钟
15.3 项目实施 2.趋势科技企业反病毒系统实战案例.avi/70 分钟

16.1 VPN 技术介绍.avi/13 分钟
16.2 基于 Windows 的远程访问 VPN.avi/32 分钟
16.3 基于 ISA 防火墙的 VPN.avi/41 分钟

17.1 入侵检测系统的概述.avi/18 分钟
17.2 入侵检测系统系统分类.avi/17 分钟
17.3 项目实施 1.入侵检测系统工具实战.avi/9 分钟
17.4 项目实施 2.提高网站服务器的安全.avi/12 分钟

第 1 章　网络管理技术基础

从上世纪 90 年代开始，国内网络事业蓬勃发展，网络技术也逐步普及。到目前为止，网络几乎无处不见，在生活、工作中越来越多的人离不开网络。由于网络环境不断的普及壮大，相应的网络管理问题也越来越被重视。在这种环境下，网络管理技术得到不断的更新、改善。

究竟什么是网络管理技术，应当如何进行网络管理呢？下面对这两个问题进行详细介绍。

1.1　网络管理概述

网络管理，是指网络管理员通过网络管理程序对网络的运行状态进行检测和控制，从而使网络有效、可靠、安全、经济运行的技术体系。从定义来看，网络管理主要包括两部分任务：检测网络运行状态和控制网络运行状态。通过这两部分任务可以了解网络运行是否正常、是否存在潜在危险和瓶颈，并通过控制调节做到优化网络、提高性能、保障服务。可以看出控制和检测是密不可分的，检测是基础，控制做补充。

随着企业信息化不断的发展，依赖于计算机网络和计算机终端的业务及应用越来越多。为了提高业务及应用质量，对于网络设备、终端客户机、服务器、应用程序的性能和可靠性要求越来越高，相应的网络维护管理工作也越来越复杂。

由于信息化发展迅猛，很多企业在应对需求、扩充网络环境及应用复杂性的同时，并不能及时的补充相应的管理人员。在这种相对不和谐的工作环境下，如果可以介入专业的管理技术，高素质的管理人才，会极大的提高网络环境的可靠性、网络应用的高效性。

企业业务对网络的依赖越来越大，一旦出现问题，会造成很多方面的损失。因此，对网络的稳定性、安全性、可靠性、可用性等特征的等级要求也越来越高。企业的业务运作是一整套的东西，如果某一个环节出现网络故障，很可能导致工作停滞。

想要保持网络的稳定性，需要在网络故障发生之前及时发现故障隐患，并能在故障发生之后及时地找出故障原因和解决办法。同时网络的稳定运行也和其性能息息相关，所以需要实时的监控其性能状态，及时地发现性能瓶颈、找到解决办法。

在网络管理过程中，由于网络设备繁杂，单靠人工管理很难应付，所以需要管理员能够智能化的对所有设备进行配置查看和修改。

网络管理是对网络上资源的集中管理，通过对管理内容的细化，可以分为以下五种管理职能：配置管理、性能管理、故障管理、计费管理、安全管理。

1.2 网络管理的发展

伴随网络环境的不断扩大，网络应用的增加，网络结构变得越来越复杂。在这个变化中，网络管理的工作内容也变得越来越有难度，越来越繁重。早期的完全依靠手工实现的网络管理时代早已不能满足网络可用性、稳定性、安全性的需求。紧接着，利用软件实现的简单集中式网络管理模式诞生了，但是网络不断扩大，复杂的网络环境逐步走向分层式网络结构，集中式的网络管理软件已经无法处理剧增的庞大网络管理信息，网络管理再次变得被动。面对广大企业网络管理的需求，分布式、分层的网络管理模型诞生。在这样的发展过程中，网络管理技术不断的被完善。网络管理技术发展至今，已经成为了一套完整的技术体系，并且还在不断的壮大中。

随着网络的壮大，网络应用技术的增加，网络复杂性的提高，网络管理水平和深度的需求，网络管理内容也在不断地增加，各种有针对性的网络管理系统软硬件设备纷纷涌现。根据网络管理内容的不同，网络管理技术可以划分为六个发展方向。

1. 网管系统（NMS）

这个方向产生的产品也可以称作网络运维系统或网络管理平台，主要致力于网络设备的实时监测、配置管理和故障诊断。可以实现网络拓扑自动发现、设备远程配置、各种性能图标的显示、故障报警和分析。目前市场上比较流行的网管系统产品有 HP OpenView、IBM Tivoli NetView、CiscoWorks2000 等。

2. 应用性能管理（APM）

主要用于实现企业关键性业务的性能监测和优化。从原来只监控服务器硬件及系统程序性能，发展到兼顾客户端相应速度，可以实现应用系统各个组件的性能监控，最终可以达到提高企业应用服务可靠性和客户服务质量的目的。目前市场上比较流行的应用性能管理产品有 BMC、Quest 系列产品、Topaz 和 SiteView 等产品。

3. 桌面管理系统（DMI）

主要用于实现对最终用户的全方位管理，包括计算机组件、操作系统、地址信息。可以实现对设备资产信息、软件分发和远程控制等方面的工作，减少了管理员的工作量，提高了工作效率。目前市场上比较流行的桌面管理系统有 CA Unicenter、NetInhandLANDesk Management Suite 7、Landesk 等。

4. 员工行为管理（EAM）

主要用于对员工上网及桌面操作行为的监控和管理。可实现规范员工工作习惯，提高员工管理水平。目前市场上比较流行的员工行为管理系统有 WebSense、NetManage 等。

5. 安全管理

主要用于实现保障合法用户对网络资源的安全访问，防止网络被恶意攻击和破坏。主要通过各种软硬件产品的身份验证、加密认证、访问控制、流量分析、漏洞扫描和安全日志等功能来实现

网络安全保护。

目前市场上比较流行的安全管理系统有：防火墙（Cisco ASA、天融信、NetScreem、Check Point）、IDS 入侵检测（RealSecure、ITA、ESM）、防毒墙（启明星辰、趋势科技）、流量监测分析（Sniffer Pro、科来）、VPN（安达通）、CA 认证等。

1.3　网络管理的五大职能

在进行网络管理时，需要管理的内容、信息繁多，综合起来可以实现五个方面的管理职能，分别是配置管理、性能管理、故障管理、计费管理、安全管理。这五大管理职能的具体内容介绍如下。

1.3.1　配置管理

配置管理在网络管理中非常重要，通过这项功能可以对网络里所有设备进行配置查看、调试、保存等操作，这样一方面提高了设备配置效率，另一方面确保了设备配置的准确性和安全性。配置管理系统需要具备以下功能。

1. 配置管理设备的配置信息

网络环境越来越大，需要配置管理的设备也越来越多，如果所有设备的配置信息全部由人工来完成，工作量会很大，同时由人工操作难免会出现配置错误。而且在设备配置结束后，即便是当初的配置人随着网络环境的逐渐扩充、变换，也不一定能一直掌握所有设备的配置情况，如果换了新的网络管理员，就更不可能掌握整个网络配置了。所以，在实施网络管理时需要架设一套可以实现设备远程配置并可以自动获得管理所有设备配置信息的程序。

当然并非所有配置内容都可以实现远程配置，比如网络设备初始安装时，远程管理端根本无法连接，最基本的连接配置还需要管理员手工操作完成。

2. 自动更新、保存配置

网络管理过程中经常会出现一些需要定期调整的配置内容，比如程序升级。还有设备的配置也会经常地被调整，一旦设备出现故障，原有的配置信息可能会丢失，必须对这些配置信息执行定期备份保存操作。这些周期性的工作内容，如果每次都需要管理员去操作很浪费时间，也很容易忘记。所以，需要专门的管理程序能够定期的自动执行任务计划，以完成这些工作。

3. 配置一致性校验

网络环境较大的情况下，需要配置的设备太多，一般都会由多人完成配置，虽然前期有详细的配置方案，但是在实施过程中难免会出现问题。再者，在日常网络维护中，网络环境或设备会经常被改动，在改动过程中也难免出现错误的配置。这些情况都有可能导致网络无法正常使用。所以，在网络管理过程中要经常对网络设备的配置进行一致性校验。其中对网络使用影响较大的配置内容主要是路由器、交换机、防火墙等关键设备的配置。

4. 配置变化记录

网络中有一部分设备需要被用户频繁使用，而这部分设备很容易被普通用户操作错误的配置信息，一旦设备出现故障在，在没有任何资料的情况下，网络管理员进行故障排查会很吃力。如果可以实时的记录设备配置信息的变化情况，管理员就可以通过这些记录信息迅速的查出导致故障的错误配置。这一般可以通过设备的系统日志功能来实现，管理员通过远程管理可以查看保存这些日志信息。

1.3.2 性能管理

性能是用来评价系统、设备和网络整体运行状况的重要信息。这些性能信息如果能被合理利用，网络管理员就可以及时地发现性能瓶颈、故障隐患及原因。而网络管理系统就可以提供性能管理机制，帮助管理员进行性能检测分析，并对异常现象报警。详细剖析，性能管理系统需要具备以下功能。

1. 性能监控

设备、系统和网络的性能需要由专业的工具统计产生，最终可能产生的性能信息有 CPU 使用率、空闲内存量、磁盘驱动器读写速率、网络流量、丢包率、网络延迟等，这些性能信息通过性能管理程序的处理可以生成性能报告。

2. 性能分析

获取性能信息和性能报告的意义在于查找性能瓶颈和故障隐患。这需要对已统计的性能信息进行整理、分析，并和性能指标做比较，最终得出分析结果和调整方案，使整个网络的性能得到最好的发挥。

3. 警报阈值控制

设备、系统和网络出现异常时，性能状态会有所改变，如果当时没有进行性能监控和分析，很可能使异常恶化。通过性能管理程序，可以设定性能阈值，一旦监控到的性能信息超过了设定的阈值，代表出现了异常，并向管理员发送警报提示。

1.3.3 故障管理

网络故障一直是网络管理员最头痛的问题，有些故障可能会造成巨大的损失，而有些故障不大，但却频繁发生。不过一般的网络故障都是一些小故障，这些小故障虽然危害不大，但是恢复起来也需要管理员费一番手脚，关键是这些小故障发生的频率都很高，时间长了就变成了占用管理员时间最多的、机械的、重复的工作。

其实网络里的每一个用户和管理员的期望都一样，希望故障彻底消失。但是这不可能，作为管理员能做的是尽量避免故障发生，尽快解决故障。当没有故障时，管理员需要实时的监控网络，分析故障隐患，让故障结束在萌芽状态。当故障发生后，管理员需要第一时间让网络畅通，然后再查找故障原因进行恢复。

要做到以上内容需要架设一套完善的故障管理系统，通过该系统实现故障检测、隔离和恢复。