普通高等教育“十二五”创新型规划教材

网络管理与维护

WANGLUO GUANLI YU WEIHU

主　编　李光宇　陈　巍

北京理工大学出版社
BEIJING INSTITUTE OF TECHNOLOGY PRESS

普通高等教育“十二五”创新型规划教材

网络管理与维护

主　编　李光宇　陈　巍
主　审　齐彦力
副主编　杨　铭　刘志宝　杨颖辉
参　编　齐　宁　刘金明

北京理工大学出版社
BEIJING INSTITUTE OF TECHNOLOGY PRESS

图书在版编目（CIP）数据

网络管理与维护/李光宇，陈巍主编. —北京：北京理工大学出版社，2012.1

ISBN 978-7-5640-5444-1

Ⅰ.①网…　Ⅱ.①李…②陈…　Ⅲ.①计算机网络管理—高等学校—教材②计算机网络—维修—高等学校—教材　Ⅳ.①TP393.07

中国版本图书馆 CIP 数据核字（2011）第 275417 号

出版发行／北京理工大学出版社
社　　址／北京市海淀区中关村南大街 5 号
邮　　编／100081
电　　话／(010)68914775(总编室)　68944990(批销中心)　68911084(读者服务部)
网　　址／http：// www. bitpress. com. cn
经　　销／全国各地新华书店
印　　刷／北京市兆成印刷有限责任公司
开　　本／710 毫米×1000 毫米　1/16
印　　张／10.75
字　　数／197 千字
版　　次／2012 年 1 月第 1 版　2012 年 1 月第 1 次印刷　责任编辑／钟　博
印　　数／1～1500 册　责任校对／陈玉梅
定　　价／29.00 元　责任印制／王美丽

前言

Preface <<< <<<

计算机网络课程不仅是为了让学生掌握技术原理，更重要的是帮助学生运用所学的知识进行工程设计和实践，从而培养学生的创新能力、动手能力和解决问题的能力，能够为今后的实际工作打下基础。为此，我们站在实际网络管理和维护的角度，结合多年教学经验并参考许多同行的技术成果，编写了这本教材。

本书内容全面而完整，结构安排合理，图文并茂，通俗易懂，注重理论联系实际，能够很好地帮助读者学习和理解计算机网络管理和维护等方面的功能和应用技术。本书的可读性和实用性强，教程与实训合二为一，全面按照项目教学、单元设计的思路来组织教学，从实践中领悟、总结理论，用理论指导实践，切实提高学生的专业动手实践能力。本书共分为8个章节，第1章介绍网络管理基础，第2章讲解网络管理协议，第3章讲述网络操作系统及局域网常用通信协议，第4章介绍集线器与交换机，第5章讲述路由器，第6章介绍IP地址管理，第7章讲述服务器管理，第8章讲述网络故障的诊断与网络维护。每个章节后面都安排有本章知识小结、习题练习、综合实训等内容，便于学生自学和操作，提高实际动手能力。

本书适合高等院校计算机网络和计算机应用或相近专业的学生使用，也可作为从事网络管理、网络维护的科研人员和相关技术人员的参考书。

本书由李光宇、陈巍担任主编，杨铭、刘志宝、杨颖辉担任副主编，齐宁、刘金明参与编写了本书。其中第1章、第2章、第3章由李光宇、陈巍、刘志宝、杨颖辉合作编写，第4章、第5章由陈巍、齐宁、刘金明合作编写，第6章、第7章由李光宇、刘志宝、杨铭合作编写，第8章由杨铭、刘金明合作编写。齐彦力教授审阅了全书，并提出了宝贵意见。另外，本书在编写过程中，得到了学院领导的关心和支持，在此一并表示衷心的感谢。

由于网络管理和维护的技术发展非常快，本书的选材还有不尽如人意的地方，加上作者水平有限，书中难免存在不足之处，敬请读者批评指正。

编　者

目录

Contents <<< <<<

第1章 网络管理基础 …… 1
1.1 局域网管理 …… 1
1.1.1 了解网络 …… 2
1.1.2 网络运行 …… 3
1.1.3 网络维护 …… 4
1.2 网络管理功能 …… 7
1.2.1 配置管理 …… 8
1.2.2 性能管理 …… 8
1.2.3 故障管理 …… 9
1.2.4 安全管理 …… 9
1.2.5 计费管理 …… 10
小结 …… 11
习题 …… 11
实训 …… 11

第2章 网络管理协议 …… 15
2.1 网络管理协议简介 …… 15
2.1.1 SNMP …… 16
2.1.2 CMIS/CMIP …… 16
2.1.3 CMOT …… 17
2.1.4 LMMP …… 17
2.1.5 SNMP与CMIP的比较 …… 17
2.2 网络管理模型 …… 18
2.3 SNMP（简单网络管理协议） …… 19
2.3.1 SNMP概述 …… 19
2.3.2 SNMP管理控制框架与实现 …… 19
2.3.3 SNMP管理信息库MIB …… 21
2.3.4 SNMP的实现机制 …… 23
2.3.5 SNMP数据类型 …… 25
2.3.6 SNMP报文格式 …… 26

2.3.7 SNMP 网络管理工作站数据收集方法 …… 28
2.3.8 SNMP 的风险及防范 …… 29
小结 …… 32
习题 …… 32
实训 …… 33

第 3 章 网络操作系统及局域网常用通信协议 …… 35
3.1 网络操作系统基本概念 …… 35
3.1.1 计算机操作系统的概念 …… 35
3.1.2 计算机网络操作系统的概念 …… 36
3.1.3 UNIX 操作系统 …… 38
3.1.4 Linux 操作系统 …… 40
3.1.5 NetWare 操作系统 …… 41
3.1.6 Windows 操作系统 …… 42
3.2 网络操作系统的选择 …… 44
3.2.1 常用网络操作系统的比较 …… 44
3.2.2 选择操作系统时应考虑的因素 …… 44
3.3 局域网常用通信协议 …… 45
3.3.1 TCP/IP 协议 …… 45
3.3.2 NetBEUI 协议 …… 46
3.3.3 IPX/SPX 及其兼容协议 …… 46
3.3.4 如何选择通信协议 …… 47
小结 …… 48
习题 …… 49
实训 …… 49

第 4 章 集线器与交换机 …… 53
4.1 共享式与交换式以太网 …… 53
4.2 交换机的 MAC 地址表学习过程 …… 55
4.3 交换机的分类 …… 56
4.3.1 从网络覆盖范围划分 …… 56
4.3.2 根据传输介质和传输速度划分 …… 56
4.3.3 根据应用层次划分 …… 58
4.3.4 根据交换机的结构划分 …… 59
4.3.5 根据交换机工作的协议层划分 …… 60
4.4 交换机的性能 …… 61
4.5 交换机的选型 …… 63

4.6 交换机高级配置与使用 …… 64
4.6.1 广播域 …… 64
4.6.2 VLAN 的产生 …… 64
4.6.3 VLAN 的划分 …… 66
4.7 交换机的配置 …… 69
4.7.1 访问网络设备命令行接口的方法 …… 69
4.7.2 命令视图 …… 71
4.7.3 命令级别 …… 71
小结 …… 72
习题 …… 72
实训 …… 74

第5章 路由器 …… 79
5.1 路由器基础 …… 79
5.2 路由器的结构 …… 80
5.3 路由器分类 …… 81
5.4 路由原理 …… 82
5.5 路由表 …… 83
5.6 路由优先级 …… 85
5.7 路由器的配置 …… 86
小结 …… 87
习题 …… 88
实训 …… 88

第6章 IP 地址管理 …… 91
6.1 IP 地址与子网掩码 …… 91
6.1.1 IP 地址 …… 91
6.1.2 子网掩码 …… 93
6.2 IP 地址规划 …… 94
6.2.1 IP 地址的规划原则 …… 94
6.2.2 使用 Wildcard 实现局域网 IP 地址规划 …… 97
6.2.3 IP 地址规划案例 …… 100
6.3 IP 地址的冲突管理 …… 106
6.3.1 IP 地址与 MAC 地址 …… 106
6.3.2 IP 地址的冲突解决 …… 108
小结 …… 112
习题 …… 113

实训 …… 113

第7章 服务器管理 …… 116

7.1 服务器概述 …… 116

7.1.1 服务器的外观与性能 …… 116

7.1.2 服务器的分类 …… 117

7.1.3 中小企业如何采购服务器 …… 120

7.2 服务器的安全与管理 …… 122

7.2.1 提高服务器可靠性的方法 …… 122

7.2.2 服务器的安全使用 …… 123

7.2.3 企业服务器安全防护的要点 …… 124

7.2.4 服务器的管理 …… 127

小结 …… 134

习题 …… 135

实训 …… 135

第8章 网络故障的诊断与网络维护 …… 142

8.1 网络故障诊断的概述 …… 142

8.1.1 网络故障的分类 …… 142

8.1.2 网络故障的排除过程 …… 144

8.1.3 网络故障原因 …… 145

8.2 网络故障诊断的常用工具和命令 …… 146

8.2.1 网络故障诊断常用工具 …… 146

8.2.2 ping 命令 …… 147

8.2.3 Tracert 命令 …… 150

8.2.4 ipconfig 命令 …… 150

8.3 典型网络故障诊断、排查与维护 …… 152

8.3.1 连通性故障的表现、产生原因及排查 …… 152

8.3.2 协议故障的表现、产生原因及排查 …… 154

8.3.3 网络配置文件和选项故障的表现及排除 …… 155

8.4 网络故障维护及优化技巧 …… 156

8.4.1 网络故障维护技巧 …… 156

8.4.2 网络性能优化 …… 157

小结 …… 159

习题 …… 160

实训 …… 160

参考文献 …… 162

第1章 网络管理基础
Chapter 1

要 求

- 了解网络环境。
- 了解网络运行的基本要求。
- 了解网络维护的基本步骤。
- 了解网络管理功能。

知 识 点

- 网络硬件设备的特点与用途。
- 网络拓扑结构。
- 常用网络协议。

技 能 点

- 能够对局域网络进行简单配置。
- 能够对局域网络进行维护。

重 点 难 点

- 了解网络结构，能够对网络进行简单配置与维护。
- 熟悉网络通信协议。
- 了解网络管理各项功能。

1.1 局域网管理

传统的局域网管理主要针对一定范围的局域网络，在这样的局域网络中包括的主要管理对象有：服务器、客户机、各种网络线路与集线器以及各种网络操作系统。由于在这样规模的局域网中，网络管理的对象有限，网络管理一般包括三个方面：了解网络、网络运行和网络维护。

1.1.1 了解网络

要管好一个局域网，就必须对该局域网有清楚的了解。对该网络的清晰了解以及对各种网络信息的资源化管理记录，是保证网络正常运转以及进行各种网络维护的前提与基础。

（1）识别网络对象的硬件情况：局域网是由各种节点组成，这样的节点主要是服务器和客户机，因此首先需要识别这些节点的硬件组成。硬件识别包括了解服务器和客户机的品牌、它们的芯片速率、网卡品牌与配置情况，以及集线器的型号与品牌，这样就可以了解局域网中硬件设备的提供商并对硬件设备所能达到的性能有大体的了解。另外，对服务器的硬件还必须有进一步的了解，包括服务器的外设配置情况、硬盘驱动器的容量以及内存大小等。

（2）判别局域网的拓扑结构：了解了网络中的关键部件之后，须进一步了解它们是如何连接运行的，即网络结构下的实际布线系统。常见的三种布线的拓扑结构是星形、总线和环形，另外也有无线和点对点的拓扑结构，但不常用。在了解局域网的布线结构后，针对每种结构各自的优缺点，应注意其将导致的性能与故障差异。然后还须了解实现网络的传输方式——Ethernet（以太网）。它是一种支持广泛的传输协议以及多种布线形式的成熟标准。Ethernet 是非确定型的，网络传送任务越重，越有可能发生冲突，而冲突将导致影响响应时间。所以网络上有大量活动节点时性能就会大大降低，如果 Ethernet 集线器上总是出现冲突信号的话，在熟悉网络布局后可能就得重新考虑分布网络上的用户。Ethernet 的缆线包括：①粗缆 Ethernet，或叫 10Base5 Ethernet，使用大号的同轴电缆；②细缆 Ethernet，也叫 10Base2 Ethernet，使用小口径的 RG-58 同轴电缆；③10BaseT Ethernet，在星形结构中使用非屏蔽双绞线。对于采用 Ethernet 方式的局域网，网络管理员不仅要清楚 Ethernet 的原理，还必须了解组网所用的 Ethernet 缆线和插头以及它们的特点，这样在网络出现故障时可以帮助故障点的寻找与排除。除了 Ethernet 之外，其他的网络传输方式还有标记环（Token Ring）、光纤分布数据接口（FDDl）以及 ARCNet 等。了解局域网使用的传输方式是局域网管理的基本条件之一。

（3）确定网络的互联：首先需要确定网络连接的设备和接入网络的方式。这些设备与接入方式有使用调制解调器（Modem）、使用网络插座、使用 CSU/DSU 连接、使用网桥工作、使用路由器和使用网关。这些接入设备对于保证网络节点的连通以及该局域网与主干网连通有着重要作用，同时也是网络故障多发的故障点和影响网络性能的可能“瓶颈”所在。另一方面，还需要在网络服务器或其他网络设备上确定该局域网的所有子网和各客户机都能连通，并记录下网络中各子网以及客户机的 IP 地址分配。

（4）确定用户负载和定位：网络负载最重要的方面是用户的分布，因为每一网络和服务器上的用户数量是影响网络性能的关键因素，因此确定网络上有多

少用户以及他们各自的定位尤其重要。首先，查看文件服务器上的负载，了解文件服务器正常运行的时间，查看服务器 CPU 的使用率，以及服务器上网络连接的数目，这些数据提供了网络负载的直接数据；然后，利用这些数据分析众多服务器中哪个使用率最高，哪些网络的负担最重，最后对网络用户以及负载分布情况有个大致的了解。

1.1.2 网络运行

要使一个局域网顺利运转必须完成很多工作，这些工作包括：①配置网络，即选择网络操作系统，选择网络连接协议，并根据选择的网络协议配置客户机的网络软件；②配置网络服务器及网络的外围设备，做好网络意外预防处理；③网络安全管理、网络用户权限分配以及病毒的预防与处理。

（1）配置网络：配置网络就要选择网络操作系统。传统的网络操作系统包括 UNIX，Windows NT，NetWare，VINES，Windows for Workgroups，LANtastic，Personal Net-Ware 等，这些网络操作系统有各自的特点，相对而言，在局域网中 Windows-NT 和 NetWare 比较普遍。Windows-NT 最大的优势在于价格和支撑其发展的巨头 Microsoft。Windows-NT 支持 IPX 和 TCP/IP，因此在大多数网络环境中很受欢迎，另外，其安全性和网络管理功能也不错，在硬件完全兼容时安装也比较方便。在现有网络中，大约 70% 的网络操作系统采用了 Novell 公司的 NetWare 系列。NetWare 是一种快速而可靠的操作系统，十分类似于 DOS，它对多种网络协议和多种客户机操作系统有着完善的支持，其兼容性和模块化设计也使它领先于其他系统。

选择网络协议也是配置网络的重要组成部分。现在流行的局域网网络协议包括 IPX/SPX、TCP/IP、NETBIOS、NetBEUI 和 AppleTalk 等。比较普遍的协议是 IPX/SPX 和 TCP/IP，其中 IPX/SPX 是 NetWare 所采用的数据传输方式，在局域网中使用非常普遍；TCP/IP 是面向 Internet 所使用的网络协议，具有广泛的影响力。

在确定了网络操作系统和网络协议之后，需要配置该网络中每台客户机的网络软件。在 DOS 平台上，一般是安装相应网络协议的网络驱动软件，然后修改一些配置文件中的参数；在 GUI 的操作系统（如 Windows 系列、Macintosh 和 OS/2）中，主要是选择相应的对话框窗口配置网络参数；在 UNIX 系统中，则主要靠修改系统配置文件来配置网络。

（2）配置网络服务器：在局域网中，服务器往往具有重要作用，一个配置良好的服务器可以顺利保障网络的运行。①在服务器上用磁盘和卷根据内容的性质与空间大小分配来划分工作，这样可以把不同的程序和数据按照一种顺序存放在磁盘中；而卷的使用不仅可以按一定的层次存放数据，而且可以控制用户的访问权；②在服务器上启动网络服务进程，监测网络用户的访问。还有一些外围设

备如共享打印机、共享外接磁盘或驱动器等在服务器上都应正确配置。③预防网络意外发生，首先是保证电源特别是网络服务器的电源，一般的方式是配置 UPS 应急电源；然后是保证服务器的环境状况，如维持机房的温度与湿度在一定的范围；最后是做好重要数据和系统的备份工作。备份的硬件设备包括硬盘阵列和磁带、光盘驱动器等，备份的方法很多，常用的是磁盘镜像、磁盘双工或磁盘阵列等。在进行备份时一定要做好详细记录，对备份内容进行分类并做标记。

（3）网络安全控制：网络安全控制的首要任务是管理用户注册和访问权限。在局域网上，网络操作系统一般都提供用户管理和权限分配的工具。对于局域网内部用户，利用这些工具可以检查和设置用户信息、进行账号限制。例如，改变账号密码、设置组、确定组中的账号、修改组或账号的权限、设定账号有效时间等。定时对网络当前访问情况进行检查并做好记录，及时发现异常情况。另外，管理局域网外部权限和连接也很重要，一般局域网外部用户可能会访问该局域网，如查看已有文件、传递他们的文件或使用其他网络资源，因此对这种用户也需要建立账号，但应根据其使用网络的目的详细控制其访问权限，然后定期检查哪些用户最近没有注册，对一些不再需要的账号及时注销。

查找并消除病毒也是局域网管理的一项重要任务。病毒对局域网的危害非常严重，一种网络病毒可以通过网络迅速地传染到局域网的每一台客户机，因此及时发现并杀死病毒至关重要。有多种不同的方法可以识别病毒：在文件级上，用 CRC 技术可以将预期的文件大小或其他特征与文件被打开之前所看到的实际特征进行比较；最常用的方法是对文件进行扫描，发现已知病毒的标志、代码，从而辨认出每一种病毒的变形。一旦发现病毒，当然就要清除它。利用一些杀毒软件可以杀死病毒恢复原来的文件。另一种方法是删除有病毒的文件，然后用备份的无病毒文件替代。另外还必须对受病毒感染的服务器上的各卷进行扫描，如果在网络服务器之间或客户机之间存在通信联络，还必须去扫描其他系统。确定适当的持续的病毒防护是避免病毒侵害的最有效方法，这样的防护包括：建立和增强反病毒规则和程序；在客户机上安装和更新反病毒软件；安装基于网络的反病毒软件。

1.1.3 网络维护

网络维护是保障网络正常运行的重要方面，主要包括常见网络的故障和修复、网络日常检查及网络升级。

（1）常见网络的故障和修复：在局域网中，最重要的故障检测工作是文件服务器的维护。只要服务器正常工作，集中存储的数据就是安全的，用户可以在需要时访问这些数据。当然，网络连接设备应保证用户能持续工作，而客户机本身也应能正常工作。

故障处理过程有发现故障迹象、追踪故障的根源、排除故障和记录故障的解

决方法四个主要部分。网络故障处理经常需要进行大量的调查研究，但相对而言只有很少的问题是真正比较复杂的。常见的情况是，故障的解决方法是很简单的，只不过被其他问题或不完全的信息掩盖了。在处理故障期间，可以参考图1－1中的流程图，以确保能对网络故障进行逻辑的、有条理的分析。

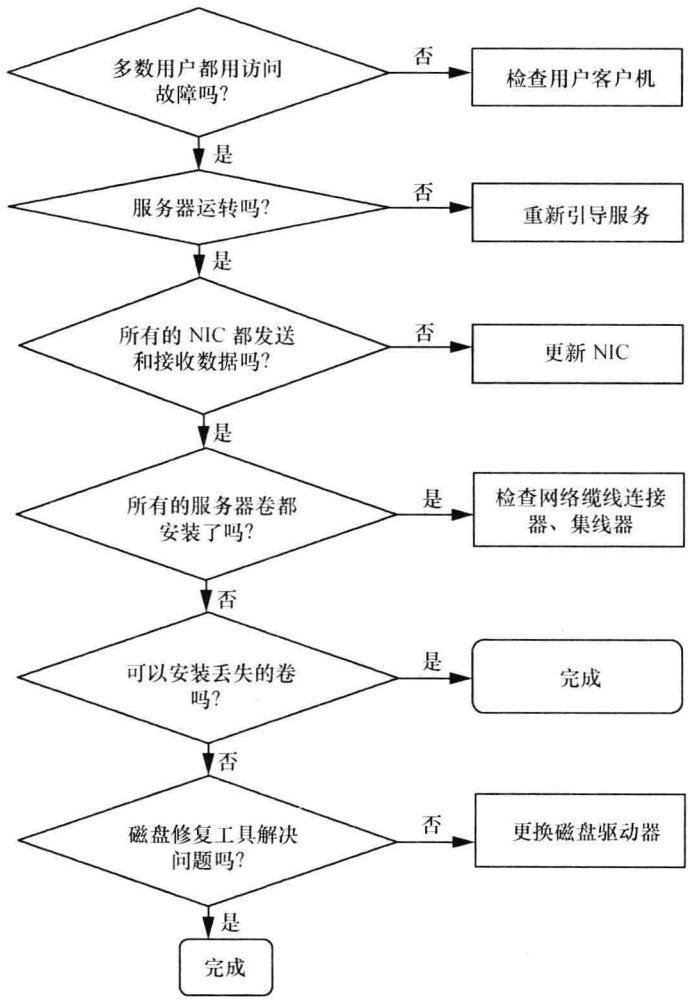

图1－1　故障检测流程图

当网络管理人员收到故障报告时，首先应该检查别的用户是否也遇到同一问题，如果有多个用户报告了同类问题，那么很可能是出现了服务器或缆线故障，而不是用户客户机所引起的故障。

排除文件服务器上的错误非常关键，因为它通常会影响到很多用户，因此首先要对服务器进行认真检查：服务器是否在运行？监视器是否显示信息？服务器是否响应键盘输入？服务器控制台是否显示异常终止或其他信息？服务器NIC

（网络适配器）是否发送和接收数据？服务器的卷是否已安装？

文件服务器通常是十分稳定的，但它们也特别容易出现以下三种类型的故障。

第一类，故障并不是网络操作系统本身的错误，而是由于配置的更改造成的，因此无论何时改变网络操作系统的配置都必须备份以前的配置并记录更改日期；

第二类，故障是部件失效，虽然 NIC 和磁盘失效是最为常见的，但从键盘端口到 SIMM 的任何部件都可能会发生故障，甚至在高品质服务器上也无法避免；

第三类，故障是服务器的软件模块引发的系统冲突故障，比如磁盘驱动程序或 LAN 驱动程序引发的内存故障等。

当服务器故障检查各方面都没有问题时，引起大量用户访问故障的问题很可能出现在网络缆线系统上。如果故障网络采用的是总线拓扑结构，那么故障检测工作可能会比较繁重；对于星形结构，则应检查集线器或 MAU 是否通电并能正常运行。如果连接设备本身运行良好，可检查它们与服务器的物理连接。一般而言，对于物理网络，电缆和接插件老化、电磁干扰、电缆长度限制是最常见的物理网络故障源；连接设备，如接插板、集线器和路由器也是故障多发点。

（2）网络检查：网络检查是在网络正常运转情况下对服务器状态和网络运行情况的动态信息收集和分析的过程。有些数据最好每天检查一次，而有些数据则较长时间检查一次即可，表 1－1 列出了一些需要定期检查的网络关键信息。

表 1－1　网络关键信息

频率	活动	频率	活动
每日	检查各服务器的卷空间	每日	去除旧用户
每日	列出前一天创建的文体	每月	检查用户账号安全性
每日	找出可被存档/删除的旧文件	每月	确保备份的完整性
每日	检查备份的执行情况	每月	更新服务器模块
每日	检查服务器错误记录文件	每月	更新客户文件

（3）网络升级：网络升级是一个持续的过程，它需要考虑一些财务和预算因素。一般在网络管理中需要考虑的是必须进行的升级，这些升级能够保证网络正常运转。虽然网络操作系统的升级通常是最迫切的，但硬件和软件也可能需要升级。

服务器升级是最重要的。必须的服务器升级有三种：第一种也是最简单的服务器升级是用户许可证升级，如果网络服务器的能力已达到最大限度，并需要容纳更多的用户，就需要进行许可证升级；第二种服务器升级是网络操作系统的升级，如果使用的是过时的或有故障的网络操作系统，就应该升级为最新的版本；第三种服务器升级所指的范围相对来说要广泛一些，主要指硬件升级，硬件升级

可能包括增加磁盘空间、改进容错措施或系统升级。另外，客户软件的升级有时也是很必要的，因为旧客户软件对于网络操作系统可能是一种沉重的负担。在确定了最重要的升级之后，应决定需要购买的产品，并对升级费用进行评估，然后制定实施升级的工作步骤，最后应从成本和效益两方面总结新配置的优点。

1.2 网络管理功能

在实际网络管理过程中，网络管理应具有的功能非常广泛，包括了很多方面。在 OSI 网络管理标准中定义了网络管理的 5 大功能，如下：

- ◆ 配置管理（configuration management）
- ◆ 性能管理（performance management）
- ◆ 故障管理（fault management）
- ◆ 安全管理（security management）
- ◆ 计费管理（accounting management）

这 5 大功能是网络管理最基本的功能。

事实上，网络管理还应该包括其他一些功能，如网络规划、网络操作人员的管理等。不过除了基本的网络管理 5 大功能，其他的网络管理功能实现都与具体的网络实际条件有关，因此我们只须关注以下 OSI 网络管理标准中的五大功能。

（1）配置管理：它是最基本的网络管理功能。主要负责：自动发现网络拓扑结构，构造和维护网络系统的配置。监测网络被管对象的状态，完成网络关键设备配置的语法检查，配置自动生成和自动配置备份系统，对于配置的一致性进行严格的检验。

（2）性能管理：它是采集、分析网络对象的性能数据。主要负责：监测网络对象的性能，对网络线路质量进行分析；同时，统计网络运行状态信息，对网络的使用发展作出评测、估计，为网络进一步规划与调整提供依据。

（3）故障管理：它是网络管理的核心。主要负责：过滤、归并网络事件，有效地发现、定位网络故障，给出排错建议与排错工具，形成整套的故障发现、告警与处理机制。

（4）安全管理：它结合使用用户认证、访问控制、数据传输、存储的保密与完整性机制，以保障网络管理系统本身的安全。主要负责：维护系统日志，使系统的使用和网络对象的修改有据可查。控制对网络资源的访问。

（5）计费管理：它是对网际互联设备按 IP 地址的双向流量统计。主要负责：产生多种信息统计报告及流量对比，并提供网络计费工具，以便用户根据自定义的要求实施网络计费。

下面将针对 5 大功能中每个部分的功能进行具体的描述。

1.2.1 配置管理

（1）配置信息的自动获取：在一个大型网络中，需要管理的设备是比较多的，如果每个设备的配置信息都完全依靠管理人员的手工输入，工作量是相当大的，而且还存在出错的可能性。对于不熟悉网络结构的人员来说，这项工作甚至无法完成。因此，一个先进的网络管理系统应该具有配置信息自动获取功能。即使在管理人员不是很熟悉网络结构和配置状况的情况下，也能通过有关的技术手段来完成对网络的配置和管理。在网络设备的配置信息中，根据获取手段大致可以分为三类：第一类是网络管理协议标准的 MIB 中定义的配置信息（包括 SNMP 协议和 CMIP 协议）；第二类是不在网络管理协议标准中有定义，但是对设备运行比较重要的配置信息；第三类就是用于管理的一些辅助信息。

（2）自动配置、自动备份及相关技术：配置信息自动获取功能相当于从网络设备中“读”信息；相应地，在网络管理应用中还有大量“写”信息的需求。同样根据设置手段对网络配置信息进行分类：第一类是可以通过网络管理协议标准中定义的方法（如 SNMP 中的 set 服务）进行设置的配置信息；第二类是可以通过自动登录到设备进行配置的信息；第三类就是需要修改的管理性配置信息。

（3）配置一致性检查：在一个大型网络中，由于网络设备众多，而且由于管理的原因，这些设备很可能不是由同一个管理人员进行配置的。实际上，即使是同一个管理员对设备进行的配置，也会由于各种原因导致配置一致性问题。因此，对整个网络的配置情况进行一致性检查是必须的。在网络的配置中，对网络正常运行影响最大的主要是路由器端口配置和路由信息配置。因此，要进行一致性检查的也主要是这两类信息。

（4）用户操作记录功能：配置系统的安全性是整个网络管理系统安全的核心，因此，必须对用户进行的每一配置操作进行记录。在配置管理中，需要对用户操作进行记录，并保存下来。管理人员可以随时查看特定用户在特定时间内进行的特定配置操作。

1.2.2 性能管理

（1）性能监控：由用户定义被管对象及其属性。被管对象类型包括线路和路由器；被管对象属性包括流量、延迟、丢包率、CPU 利用率、温度、内存余量。对于每个被管对象，定时采集性能数据，自动生成性能报告。

（2）阈值控制：可对每一个被管对象的每一条属性设置阈值，对于特定被管对象的特定属性，可以针对不同的时间段和性能指标进行阈值设置。可通过设置阈值检查开关控制阈值检查和告警，提供相应的阈值管理和溢出告警机制。

（3）性能分析：对历史数据进行分析，统计和整理，计算性能指标，对性能状况作出判断，为网络规划提供参考。

（4）可视化的性能报告：对数据进行扫描和处理，生成性能趋势曲线，以直观的图形反映性能分析的结果。

（5）实时性能监控：提供了一系列实时数据采集；分析和可视化工具，用以对流量、负载、丢包、温度、内存、延迟等网络设备和线路的性能指标进行实时检测，可任意设置数据采集间隔。

（6）网络对象性能查询：可通过列表或按关键字检索被管网络对象及其属性的性能记录。

1.2.3 故障管理

（1）故障监测：主动探测或被动接收网络上的各种事件信息，并识别出其中与网络和系统故障相关的内容，对其中的关键部分保持跟踪，生成网络故障事件记录。

（2）故障报警：接收故障监测模块传来的报警信息，根据报警策略驱动不同的报警程序，以报警窗口/振铃（通知一线网络管理人员）或电子邮件（通知决策管理人员）发出网络严重故障警报。

（3）故障信息管理：依靠对事件记录的分析，定义网络故障并生成故障卡片，记录排除故障的步骤和与故障相关的值班员日志，构造排错行动记录，将事件－故障－日志构成逻辑上相互关联的整体，以反映故障产生、变化、消除的整个过程的各个方面。

（4）排错支持工具：向管理人员提供一系列的实时检测工具，对被管设备的状况进行测试并记录下测试结果以供技术人员分析和排错；根据已有的排错经验和管理员对故障状态的描述给出对排错行动的提示。

（5）检索/分析故障信息：浏览并且以关键字检索查询故障管理系统中所有的数据库记录，定期收集故障记录数据，在此基础上给出被管网络系统、被管线路设备的可靠性参数。

1.2.4 安全管理

安全管理的功能分为两部分，首先是网络管理本身的安全，其次是被管网络对象的安全。网络管理过程中，存储和传输的管理和控制信息对网络的运行和管理至关重要，一旦泄密、被篡改或伪造，将给网络造成灾难性的破坏。网络管理本身的安全由以下机制来保证：

（1）管理员身份认证，采用基于公开密钥的证书认证机制；为提高系统效率，对于信任域内（如局域网）的用户，可以使用简单口令认证。

（2）管理信息存储和传输的加密与完整性，Web 浏览器和网络管理服务器之间采用安全套接字层（SSL）传输协议，对管理信息加密传输并保证其完整性；内部存储的机密信息，如登录口令等，也是经过加密的。