高职高专“十一五”计算机类专业规划教材

江苏省高等学校立项建设精品教材

网络管理与维护

实用教程

张家超 主编 吴国经 副主编

中国电力出版社
www.infopower.com.cn

高职高专"十一五"计算机类专业规划教材
江苏省高等学校立项建设精品教材

网络管理与维护实用教程

张家超 主编 吴国经 副主编

中国电力出版社
www.infopower.com.cn

内容提要

本书是江苏省高等学校立项建设精品教材。全书从技术的先进性与实用性出发，系统地介绍了计算机网络管理与维护的基础知识、基本理论、基本原理及基本技术。其中，第1、2章介绍了计算机网络管理与维护的基本概念、管理模型与体系结构；第3章介绍了网络操作系统的配置、管理与服务；第4、5、6章介绍了常用网络管理、维护以及网络安全所需软硬件环境的配置、管理与服务；第7、8章介绍了常用网络故障及其解决方法；第9章介绍了几个网络管理与维护的实例；第10章给出了网络管理与维护的实验指导。

本书采用通俗易懂的语言，注重理论联系实际，适合作为高职高专等应用型高等院校讲授计算机网络管理与维护知识的参考教材，也可作为全国计算机技术与软件专业技术资格（水平）考试“网络管理员”和“网络工程师”理论和实践部分的参考资料。

图书在版编目（CIP）数据

网络管理与维护实用教程 / 张家超主编. —北京：中国电力出版社，2007.3

高职高专“十一五”计算机类专业规划教材

ISBN 978-7-5083-5156-8

I. 网… II. 张… III. 计算机网络－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 011672 号

丛 书 名：高职高专“十一五”计算机类专业规划教材

书　　名：网络管理与维护实用教程

出版发行：中国电力出版社

地　　址：北京市三里河路 6 号　　邮政编码：100044

电　　话：（010）68362602　　传　　真：（010）68316497，88383619

服务电话：（010）88515918（总机）　　传　　真：（010）88518169

E-mail：infopower@cepp.com.cn

印　　刷：北京市同江印刷厂

开本尺寸：185×233　　**印　　张**：19　　**字　　数**：418 千字

书　　号：ISBN 978-7-5083-5156-8

版　　次：2007 年 3 月北京第 1 版

印　　次：2007 年 3 月第 1 次印刷

印　　数：0001—4000 册

定　　价：28.00 元

前　言

计算机网络技术的飞速发展，带来的不仅仅是技术上的更新，也是观念上的快速变革。在教学第一线的教师，经过多年的探索，结合“以服务为需求、以就业为导向，走产学研相结合之路”的高职办学指导思想和培养高素质技能型计算机网络技术专门人才的高职培养目标，以及全国计算机技术与软件专业技术资格（水平）考试网络部分的内容，将计算机网络课程的教学分为4个层面的内容。首先是基础知识部分，介绍计算机网络的体系结构等知识；其次是工程技术部分，介绍计算机组网及工程应用方面的知识；第三是网络管理与维护部分，详细介绍目前比较流行的Internet/Intranet上常用的网络管理、维护、安全和建站等方面的知识与技术；第四是应用技术部分，介绍常用的网页设计与网络数据库编程等方面的知识和技术应用。

本书从技术的先进性与实用性出发，采用通俗易懂的语言，注重理论联系实际，突出重点，内容丰富，深入浅出，比较系统地介绍了计算机网络管理与维护的基础知识、基本理论、基本原理及基本技术。其中第1、2章分别介绍了计算机网络管理与维护的基本概念、管理模型与体系结构；第3章介绍了网络操作系统的配置、管理与服务；第4～6章分别介绍了常用网络管理、维护与安全所需软硬件环境的配置、管理与服务；第7、8章分别介绍了常用网络故障诊断工具、常见网络故障及解决方法；第9章介绍了几个网络管理与维护的实例；第10章给出了网络管理与维护的实验指导。

本书是江苏省高等学校立项建设精品教材。

本书不仅可以作为高职高专以及应用型高等院校计算机网络管理与维护相关课程的参考教材，也可以作为应考全国计算机技术与软件专业技术资格（水平）考试“网络管理员”和“网络工程师”理论和实践部分的参考资料。

本书由张家超主编、吴国经副主编，参加编写的人员有马安龙、何洪磊、殷美、孙承庭、林雁、潘峰等，全书由张家超负责统稿、定稿。

本书在编写过程中，得到了许多高校同行们的大力支持和帮助，参考了许多已出版和未出版的教材、讲义等，在此不一一列举；本书是2005年江苏省高等学校立项建设精品教材，得到了江苏省教育厅的资助，也得到了江苏省教育科学研究院现代教育技术研究所的大力支持；本书出版时得到中国电力出版社编辑的大力帮助，没有他们热心的支持和辛勤的劳动，本书的出版是不可能的，在此一并表示衷心的感谢。

限于编者水平及时间，书中错漏和不妥之处在所难免，恳请专家和读者批评指正。

作　者

2006年12月

目　录

第 1 章　网络管理与维护概论

1.1　网络管理概念

随着计算机技术、通信技术和网络技术的发展，企业和政府部门开始大规模建立网络来推动电子商务和政务的发展。随着网络业务和应用的丰富，对计算机网络的管理与维护也就变得至关重要。当前计算机网络的发展特点是规模不断扩大，复杂性不断增加，异构性越来越高。一个网络往往由若干个大大小小的子网组成，集成了多种网络操作系统（Network Operating System，NOS）平台，包含了不同厂家、公司的网络设备和通信设备等，同时，还有许多网络软件提供各种服务。随着用户对网络性能要求的提高，如果没有一个高效的管理系统对网络系统进行管理，那么就很难保证向用户提供令人满意的服务。作为一种很重要的技术，网络管理对网络的发展有着很大的影响，并已成为现代信息网络中最重要的问题之一。

实际上，网络管理并不是新概念。19 世纪末的电信网络就已经有了自己相应的管理“系统”，这就是整个电话网络系统的管理员。而计算机网络的管理可以说伴随着世界上第一个计算机网络——ARPANET（Advanced Research Projects Agency，高级研究项目机构网络，美国国防部开始于1969年的一个项目，目的是为了向全国不同地区的超级计算机提供高速网络通信）的产生而产生的，当时，ARPANET 就有一个相应的管理系统。随后的一些网络结构，如 IBM 的系统网络结构体系（System Network Architecture，SNA）、DEC 的数字网络体系结构（Digital Network Architecture，DNA）、SUN 的 AppleTalk 等，也都有相应的管理系统。不过，虽然网络管理很早就有，却一直没有得到应有的重视。这是因为当时的网络规模较小，复杂性也不高，一个简单的网络管理系统就可以满足网络正常管理的需要，因而对其研究较少。但随着网络的发展，网络规模逐渐增大，复杂性增加，以前的网络管理技术已不能适应网络的迅速发展。

网络系统规模的日益扩大和网络应用水平的不断提高，一方面使得网络的维护成为网络管理的重要问题之一，例如排除网络故障更加困难、维护成本逐年上升等；另一方面，如何提高网络性能也成为网络系统应用的主要问题。虽然可以通过增强或改善网络的静态措施来提高网络的性能，比如增强网络服务器的处理能力、采用网络交换等新技术来拓宽网络的带宽等，但是网络运行过程中负载平衡等动态措施也是提高网络性能的重要方面。通过静态或动态措施提高的网络性能分别称为网络的静态性能和动态性能。而网络动态性能的提高是通过网络管理系统（即网管系统）来加以解决的。

关于网络管理的定义目前很多。一般来说，网络管理就是通过某种方式对网络进行管理，使网络能正常高效地运行。其目的很明确，就是使网络中的资源得到更加有效的利用。它应该能够维护网络的正常运行，当网络出现故障时能及时报告和处理，并协调、保持网络系统的高效运行等。国际标准化组织（International Standardization for Organization，ISO）在 ISO/

IEC7498-4（International Electrotechnical Commission，国际电工委员会）中定义并描述了开放系统互连参考模型（Open Systems Interconnection/Reference Model，OSI/RM）管理的术语和概念，提出了一个 OSI 管理的结构并描述了 OSI 管理应有的行为。它认为，开放系统互连参考模型管理是指这样一些功能，它们控制、协调和监视 OSI 环境下的一些资源，这些资源保证 OSI 环境下的通信。通常对一个网络管理系统需要定义以下内容：

- 系统的功能：即一个网络管理系统应具有哪些功能。
- 网络资源的表示：网络管理很大一部分是对网络中资源的管理。网络中的资源就是指网络中的硬件、软件及所提供的服务等。而一个网络管理系统必须在系统中将它们表示出来，才能对其进行管理。
- 网络管理信息的表示：网络管理系统对网络的管理主要靠系统中网络管理信息的传递来实现。网络管理信息应如何表示、怎样传递以及传送的协议是什么，都是网络管理系统必须考虑的问题。
- 系统的结构：即网络管理系统的结构是怎样的。

一般而言，网络管理有五大功能，分别是配置管理、故障管理、性能管理、安全管理和计费管理。这五大功能包括了保证一个网络系统正常运行的基本功能。

1.1.1 网络管理的基本要素

一个典型的网络管理系统包括 4 个要素：管理员、管理代理、管理信息数据库和代理服务设备。一般说来，前 3 个要素是必须的，第 4 个是可选项。

1. 管理员（Manager）

网络管理软件的重要功能之一，就是协助网络管理员完成管理整个网络的工作。网络管理软件要求管理代理定期收集重要的设备信息。收集到的信息将用于确定独立的网络设备、部分网络或整个网络运行的状态是否正常。管理员应该定期查询管理代理收集到的有关主机运转状态、配置及性能等信息。

2. 管理代理（Agency）

网络管理代理是驻留在网络设备中的软件模块，这里的设备可以是 UNIX 工作站或网络打印机，也可以是其他的网络设备。管理代理软件可以获得本地设备的运转状态、设备特性和系统配置等相关信息。管理代理软件就像是每个被管理设备的信息经纪人，它们完成网络管理员布置的采集信息的任务。管理代理软件所起的作用是充当管理系统与管理代理软件驻留设备之间的中介，通过控制设备的管理信息数据库（Management Information Base，MIB）中的信息来管理该设备。管理代理软件可以把网络管理员发出的命令按照标准的网络格式进行转化，收集所需的信息，之后返回正确的响应。在某些情况下，管理员也可以通过设置某个 MIB 对象来命令系统进行某种操作。

路由器、交换器和集线器等许多网络设备的管理代理软件一般是由原网络设备制造商提供的，它可以作为底层系统的一部分，也可以作为可选的升级模块。设备厂商决定管理代理软件可以控制哪些 MIB 对象，哪些对象可以反映管理代理软件开发者感兴趣的问题。

3. 管理信息数据库（MIB）

MIB 是一个关于被管理设备的信息存储库，这些网络设备（Network Equipment，NE）包

括计算机、集线器、路由器和交换机等。MIB 存储这些网络部件的配置信息，如这些设备运行软件的版本、端口及端口所分配的 IP 地址、可用磁盘空间的存储容量等。这样，MIB 充当了一个登记簿的角色，记录着被管理设备的设置和资源信息。现在已经定义了几种通用的标准 MIB，使用最广泛、最通用的 MIB 是 MIB-II。

在一个 MIB 中的简单网络管理协议（Simple Network Management Protocol，SNMP）数据被组织成树状分级形式。MIB 树的结构是由许多 Internet 工程任务组（Internet Engineering Task Force，IETF）标准来定义的，如图 1-1 所示，这些协议均包含在请求注释（Request for Comments，RFC）中。

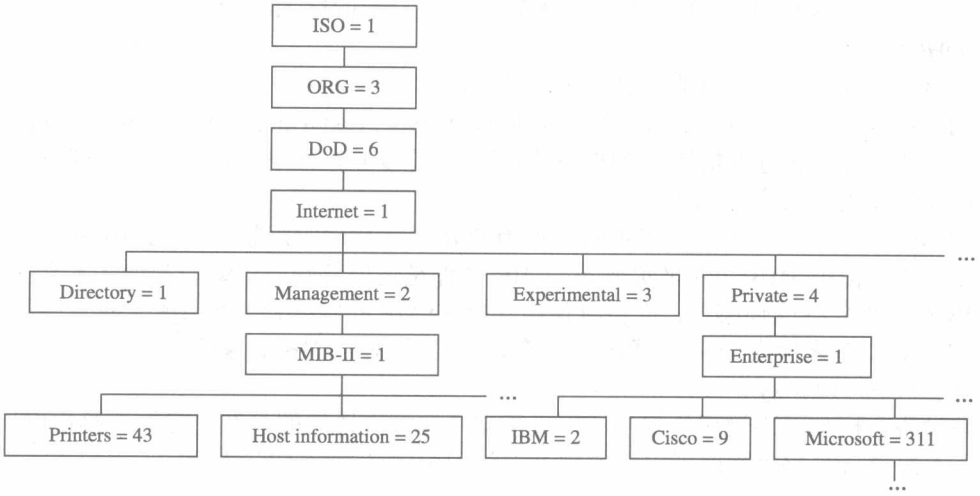

图 1-1　MIB 中 SNMP 数据的一般结构

广义的 MIB 树包含若干种分支：

（1）RFC 定义的公共分支，对所有的 SNMP 管理的设备是相同的。

（2）分配给公司和团体，由它们自己定义的专用分支。

图 1-1 描述了 MIB 树的一般结构，构成它的许多对象是用抽象语言符号 1（Abstract Syntax Notation One，ASN.1）来表示的。注意，每一台被管理的设备的信息通常只包含完整的 MIB 树的一部分，即与其具体操作相关的那部分。MIB 树的根是 ISO，接着是各类组织（ORGanization，ORG）、DoD（Department of Defense，国防部），然后是 Internet。主要的公共分支是 Management（简写为 mgmt），它定义了适用于所有厂家设备的通用网络管理参数。在 Management 下面是 MIB-II，它的下面是通用管理功能分支，如系统管理、主机资源、端口和打印机。比如，在图 1-1 中，包含着 SNMP 可管理打印机对象的 MIB 分支的根被称为 Printer，使用 MIB 记法，可通过文本字符串“.iso.org.dod.internet.mgmt.mib2.printer”来唯一定义该打印机对象。当然，也可以通过 MIB 为每个对象所分配的一个数字标识（即对象标识符，Object Identifier，OID）来简洁地表示该对象，即“.1.3.6.1.2.1.43”。

MIB 树包含有大公司和组织专用分支，这些分支组织在 Enterprise 对象下面，每个厂商在这个对象下面有一个分支根结点。例如，IBM 的分支根结点是 IBM（2），Cisco 公司是 Cisco（9），

Sun Microsystems 是 SUN（42），Microsoft LAN Manager MIB II 是 LANMAN（77），Microsoft 公司是 Microsoft（311）。厂商可以向 Internet 编号分配机构（Internet Assigned Numbers Authority，IANA）申请为它们公司保留特定的 MIB 编号。每个公司或组织，对于在自己的 MIB 树分支内产生什么对象，以及为每个对象分配什么 OID，有绝对的权利。所有的 MIB 对象必须遵守一个共同的 SNMP 信息定义，即管理信息结构（Structure of Management Information，SMI），它定义了所允许的各种数据类型。

把 Microsoft（.1.3.6.1.4.1.311）作为企业的实例，在它的根结点下定义的各种 MIB 分支如下所示。

- .1.3.6.1.4.1.311.1.3 代表动态主机配置协议（Dynamic Host Configuration Protocol，DHCP）。
- .1.3.6.1.4.1.311.1.7.2 代表文件传输协议（File Transfer Protocol，FTP）。
- .1.3.6.1.4.1.311.1.7.3 代表超文本传输协议（HyperText Transter Protocol，HTTP）等。

网络管理员可以通过直接控制 MIB 去控制、配置或监控网络设备。网络管理系统可以通过网络管理代理软件来控制 MIB。

在 SNMP 可管理设备上运行管理着被称为 SNMP 代理的专用软件，而 MIB 就集成在该软件内。这是通过使用 MIB 文件来实现的，MIB 文件是使用特殊格式编写的纯文本文件，一旦这些 MIB 对象被代理软件编译，就可以使用支持 SNMP 的网络管理系统来管理这些设备。可以使用 SNMP 命令来检索 MIB 对象的值，有时也可以修改 MIB 对象的值。

4. 代理设备（Proxy）

代理设备在标准网络管理员软件和不直接支持该标准协议的系统之间起桥梁作用。利用代理设备，不需要升级整个网络就可以实现从协议旧版本到新版本的过渡。

1.1.2 网络管理的目标和内容

网络管理的根本目标就是满足运营者及用户对网络的有效性、可靠性、开放性、综合性、安全性和经济性的要求。

- 网络应该是有效的。这是指网络要能准确及时地传递信息。这里所说的网络有效性与通信的有效性意义不同。通信的有效性是指传递信息的效率，而网络的有效性是指网络的服务要有质量保证。
- 网络应该是可靠的。这是指网络必须保证能够稳定地运转，不能时断时续，要对各种故障及自然灾害有较强的抵御能力和一定的自愈能力。
- 现代网络要有开放性。这是指网络要能够接受多厂商生产的异种设备。
- 现代网络要有综合性。这是指网络业务不能单一化，要由电话网、电报网、数据网分立的状态向综合业务数字网（Integrated Services Digital Network，ISDN）过渡，并且还要进一步加入图像、视频点播等业务，向宽带综合业务数字网（Broadband ISDN，B-ISDN）过渡。
- 现代网络要有很高的安全性。随着人们对网络依赖性的增强，人们对网络安全性的要求也越来越高。
- 网络要有经济性。网络的经济性有两个方面，一是对网络经营者而言的经济性，二是

对用户而言的经济性。对网络经营者而言，网络的建设、运营和维护等开支要小于业务收入，否则，其经济性就无从谈起。对用户来说，网络业务要有合理的价格，如果价格太高用户承受不起，或虽能承受得起但感到付出的费用超过了业务的价值，那么用户便会拒绝应用这些业务，网络的经济性也无从谈起。

网络管理的方式是随着网络的发展而变化的。早期以人工交换电话网为主的网络管理是采用人工方式进行的，由于网络设备构成和网络业务都比较简单，管理内容也比较简单。例如业务流量的控制以及转接路由的选择由话务员的接续来完成，不可能产生网络拥塞现象，设备和线路故障也比较好查找。自动交换机和计算机网络出现以后，情况发生了变化，即交换机和路由器等网络设备本身具有了一些网络管理功能，出现了人工与自动相结合的管理方式。但这时网络设备的管理功能还是很有限的，这时的管理方式主要是以网络管理中心为主的集中方式。随着计算机技术的进步和网络的高速发展，网络设备越来越复杂，因而要求网络设备自身要有较强的自我管理功能。由于网络设备自身具有了较强的网络管理功能，使网络管理方式从以集中为主变为以分散为主。为了能够综合管理整个网络，在网络之上又建立了管理网，使网络管理系统在体系结构上更加合理。

1.2　网络管理功能

ISO 在 ISO/IEC 7498-4 文档中定义了网络管理的 5 大基本功能，它们是配置管理、故障管理、性能管理、安全管理和计费管理。当然，在实际网络管理过程中，网络管理功能非常广泛，比如还包括了网络规划和网络操作人员的管理等。而这些网络管理功能的实现往往都与具体的网络实际条件有关，因此本书中只重点介绍 OSI 网络管理标准中的五大功能。

1.2.1　配置管理

配置管理用于管理网络的建立、扩充和开通，主要提供资源清单管理功能、资源开通功能、业务开通功能及网络拓扑服务功能。

配置管理是一个中长期的活动，它要管理的是因网络增容、设备更新、新技术的应用、新业务的开通、新用户的加入、业务的撤销、用户的迁移等原因而导致的网络配置的变更。网络规划与配置管理关系密切。在实施网络规划的过程中，配置管理发挥最主要的管理作用。

1. 资源清单管理功能

资源清单管理是配置管理的基本功能，它联机提供网络中的设备、器材、电路、服务、客户、设备厂商、软件和管理人员等资源的信息。利用标准的 SMI，将这些资源定义为被管对象，重点描述其属性、连接及状态。通过建立资源 MIB，提供对资源清单的提取、增加、删除和修改等功能。

2. 资源开通功能

网络资源的开通功能在保证所需资源的供应、开发和配置在经济上合理的前提下及时满足客户的业务需求。资源开通功能中所指的资源主要是指提供接入、交换、传输和 MIB 等功能的网络设备。这些网络设备由硬件和软件构成。硬件中包含基础设施、公用装置、插接件和跳线等接续元素。软件中包含一般的程序和软件包。

3. 业务开通功能

业务的开通从用户要求时开始，到网络实际提供业务时结束。它包含网络中装载和管理业务所需要的过程。业务的开通也具有向各用户或用户组分配物理或逻辑资源的能力。

4. 网络拓扑服务功能

网络拓扑服务提供显示网络及其各个构成层次的布局的功能。显示的网络布局有 3 种形式，即物理布局、逻辑布局与电气布局。为了支持各个层次各种形式的网络布局显示，需要网络配置数据库的支持。数据库不仅要存放当前的配置数据，还要存放历史的配置数据，以便能够显示网络布局的变化过程。

1.2.2 故障管理

故障管理的目的是迅速发现和纠正网络故障，动态维护网络的有效性。故障管理的主要功能有报警监测、故障定位、测试、业务恢复及修复等，同时还要维护故障日志。

网络发生故障后要迅速进行故障诊断和故障定位，以便尽快恢复业务。为此可以采用事后策略，也可以采用预防策略。事后策略重视迅速修复；预防策略可以采用配备冗余资源的方法，将发生故障的资源迅速地用备用资源替换。另一种预防策略是分析性能下降的趋势，在用户感到服务质量明显下降之前采取修复措施。

1. 报警监测功能

报警监测功能主要包含以下几个功能。

（1）网络状态监督：通过配置管理中的网络拓扑服务功能来进行分层配置显示或状态映射。利用业务量状态的实时显示和局部放大有助于确认和孤立问题。

（2）故障检测：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。其关键是检测手段是否有效。在一些情况下，为了防止故障漏检，往往采用多种检测手段。但这种方法不能过度使用，否则同一故障会产生过多的报警信息，反而不利于故障根源的确定。

（3）故障报警：接收故障检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。

（4）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、故障和日志构成逻辑上相互关联的整体，以反映故障产生、变化和消除的整个过程的各个方面。

（5）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。

（6）检索并分析故障信息：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和被管线路设备的可靠性参数。

2. 故障定位功能

故障定位功能的目的是确定设备中故障的位置。为确定故障根源，常常需要将诊断、测试及性能监测获得的数据结合起来进行分析。

故障定位的手段主要有诊断、试运行及软件检查。

（1）诊断：故障诊断一般利用专门的诊断程序进行。诊断常常是打扰性的，即在诊断进行期间，被诊断的设备不能运行正常的用户业务。

（2）试运行：试运行是将一部分网络设备隔离，利用设备正常的输入输出端口和测试器，系统地测试被隔离网络设备的所有服务特性。

（3）软件检查：利用软件进行的检查有核查、校验和运行测试、程序跟踪等。

3. 电路测试

测试功能与诊断功能不同。诊断可以在一个系统内进行，而测试常常涉及到位于不同物理位置的多个系统。

测试在业务导入和维护时使用。导入测试是检验功能或设备是否正常，其最有效的方式是端到端的测试方式。维护测试是检测及验证障碍，以及检验修复。提供测试入口的装置可以在电路、通道或传输媒体中设计。一般在不同维护区间的端口处需要设置测试入口。测试可以在电路、通道或传输线等各种层次上进行。

发生故障后，一般采用端到端测试检查故障。在端到端测试中，二分查找策略可以获得较高的效率。

4. 业务的恢复

为了在发生故障时继续提供业务，需要配备适当的预备资源。恢复策略主要有以下几种：

（1）隔离引起故障的设备，使其余的资源能够继续维持支持业务，虽然业务能力可能下降。

（2）将业务从故障设备切换到正常的预备设备，这可以通过 1:1 预备或 M:N 预备来实现。

（3）使用环或网状网络本身具有的异径功能。

1.2.3　性能管理

性能管理的目的是维护网络服务质量（Quality of Service，QoS）和网络运营效率。为此，性能管理要提供性能监测功能、性能分析功能及性能管理控制功能。同时，还要提供性能数据库的维护，以及在发现性能严重下降时启动故障管理系统的功能。

网络服务质量和网络运营效率有时是相互制约的。较高的服务质量通常需要较多的网络资源（带宽、CPU 时间等），因此在制定性能目标时要在服务质量和运营效率之间进行权衡。在网络服务质量必须优先保证的同时，就要适当降低网络的运营效率指标。相反，在强调网络运营效率的同时，就要适当降低服务质量指标。但一般在性能管理中，维护服务质量是第一位的。网络运营效率的提高主要依靠其他的网络管理功能，如通过网络规划管理和网络配置管理来实现。

在性能管理的各个功能中，性能监测功能联机监测网络性能数据，报告网络元素状态、控制状态、拥塞状态及业务量；性能分析功能对监测到的性能数据进行统计分析，形成性能报表，预测网络近期性能，维护性能日志，寻找现实的和潜在的瓶颈问题，如发现异常进行报警；性能管理控制功能控制性能监测数据的属性、阈值并报告时间表，改变业务量的控制方式，控制业务量的测量及报告时间表。

1. 网络性能指标

性能管理中需要一组能够准确、全面、迅速地反映网络性能的指标。OSI 系统管理标准中

定义了几种用于反映分组交换数据网络性能的指标，这些参数在性能管理中发挥重要作用。网络性能指标可以分为面向服务质量的指标和面向网络效率的指标两类。面向服务质量的指标主要包括有效性、响应时间和差错率。面向网络效率的指标主要包括吞吐量和利用率。

2. 性能监测功能

性能监测对网络的性能数据进行连续的采集。网络中多个设备单元的偶尔或间歇性的错误会导致服务质量降低，并且这种问题难以通过故障管理的方法检测出来。因此性能监测功能的主要目的就是通过连续采集性能数据监测网络的服务质量。同时性能监测也可用于在网络性能降低到不可接受的程度之前通过特征模式及时发现问题。

性能监测的主要用途有预防性服务、验收测试和监测合同业务的性能。

3. 性能分析功能

性能分析功能一是要对监测到的性能数据进行统计和计算，获得网络及其主要成分的性能指标，定期或在必要时形成性能报表，有时要生成性能趋势曲线，以直观的图形反映性能分析结果的可视化性能报告，为网络规划提供参考；二是要负责维护性能数据库，存储网络及其主要成分的性能的历史数据，为网络对象性能查询提供依据；三是要根据当前的和历史的数据对网络及其主要成分的性能进行分析，获得性能的变化趋势，分析制约网络性能的瓶颈问题；四是在网络性能异常的情况下向网络管理者报警，在特殊情况下，直接请求故障管理功能进行反应。

性能分析的基础是建立和维护一个有效的性能数据库。在此基础上，要解决的关键问题是设计和构造有效的性能分析方法。传统的方法是基于解析的方法，对于比较复杂的关系难以迅速得到正确结果。在这种情况下，基于人工智能的方法越来越受到重视。这种方法通过建立知识库和专家系统对网络性能进行分析，提高了分析的水平和速度。

4. 性能管理控制功能

性能管理控制功能包括监测网络中的业务量，优化网络资源的利用，调查网络的业务量处理状况。性能管理控制功能采集的业务量数据也被用于支持其他的网络管理功能，如故障管理和配置管理。数据采集时间间隔也由性能管理控制功能控制。例如，对于准实时的管理，5 分钟一次；对于一般的分析，1 小时或 24 小时一次。

1.2.4 安全管理

安全管理的目的是提供信息的隐私、认证和完整性保护机制，使网络中的服务、数据及系统免受侵扰和破坏。目前采用的主要网络安全措施包括通信伙伴认证、访问控制、数据隐私和数据完整性保护等。一般的安全管理系统包含风险分析功能，安全服务功能，报警、日志和报告功能，网络管理系统保护功能等。

需要明确的是，安全管理系统并不能杜绝所有对网络的侵扰和破坏，其作用仅在于最大限度地防范，以及在受到侵扰和破坏后将损失尽量降低。具体来说，安全管理系统的主要作用有：①采用多层防卫手段，将受到侵扰和破坏的概率降到最低；②提供迅速检测非法使用和非法初始进入点的手段，核查跟踪侵入者的活动；③提供恢复被破坏的数据和系统的手段，尽量降低损失；④提供查获侵入者的手段。

1. 风险分析功能

风险分析是安全管理系统需要提供的一个重要功能。它要连续不断地对网络中的消息和事

件进行检测，对系统受到侵扰和破坏的风险进行分析。风险分析必须包括网络中所有有关的部分。主要是用户端、交换机或局域网、本地网或城域网、长途网或广域网，以及有关的操作系统、数据库、文件、以及应用程序。

进行风险分析的一个方法是构造威胁矩阵，显示各个部分潜在的积极或消极的威胁。

2. 安全服务功能

网络可以采用的安全服务有多种多样，但是没有哪一个服务能够抵御所有的侵扰和破坏。只能通过对多种服务进行悉心的组合来获得满意的网络安全性能。网络安全服务是通过网络安全机制实现的。OSI 网络管理标准中定义了 8 种网络安全机制：加密、数字签名、数据完整性、认证、访问控制、路由控制、伪装业务流、公证。

（1）认证。可以使通信伙伴之间相互确认身份，防止侵入者插入通信过程。认证一般在通信之前进行，但在必要的时候也可以在通信过程中随机重复。认证有两种形式，一种是单方的标识被检查的单方认证，一种是通信双方相互检查对方标识的相互认证。认证服务可以通过加密机制、数字签名机制以及认证机制实现。

（2）访问控制。访问控制保证只有被授权的用户才能访问网络，进而利用资源。访问控制的基本原理是检查用户标识、密码，根据授予的权限限制其对资源的利用范围和程度。例如其是否有权利用主机 CPU 运行程序，是否有权对特定的数据库进行查询和修改等。访问控制服务通过访问控制机制实现。

（3）数据隐私。防止数据被无权者阅读。数据隐私既包括存储中的数据，又包括传输中的数据。隐私可以在特定文件、通信链路、甚至文件中指定的字段进行。数据隐私服务可以通过加密机制和路由控制机制实现。

（4）业务流分析保护。防止通过分析业务流，来获取业务量特征、信息长度、信息源和目的地等信息。业务流分析保护服务可以通过加密机制、伪装业务流机制、路由控制机制实现。

（5）数据完整性。保护存储中的和传输中的数据不被删除、更改、插入和重复。必要时该服务也可以包含一定的恢复功能。数据完整性保护服务可以通过加密机制、数字签名机制以及数据完整性机制实现。

（6）签字。用发送“签字”的办法来对信息的发送或信息的接收进行确认，以证明和承认信息是由签字者发出或接收的。这个服务的作用在于避免通信双方对信息的来源产生争议。签字服务通过数字签名机制及公证机制实现。

3. 报警、日志和报告功能

网络管理系统提供的安全服务可以有效地降低安全风险，但它们并不能排除风险。与故障管理相同，安全管理也要提供报警、日志和报告功能。该功能要以大量的侵扰检测器（可以由软件实现）为基础，在发现侵入者进入网络时触发报警过程，登录安全日志和向安全中心报告发生的事件。在报警报告和安全日志中，主要应包括事件的种类、发生的时间、事件中通信双方的标识符、有关的资源标识符和检测器标识符。

4. 网络管理系统的保护功能

网络管理系统是网络的中枢，大量的关键数据，如用户密码、计费数据、路由数据、系统恢复和重启规程等都存放在这里。因此网络管理系统是安全管理的重点对象，要采用高度可靠的安全措施对其进行保护。每个安全管理系统首先要提供对网络管理系统自身的保护功能。

1.2.5 计费管理

计费管理的主要目的是正确地计算和收取用户使用网络服务的费用。但这并不是唯一的目的，计费管理还要进行网络资源利用率的统计和网络的成本效益核算。对于以盈利为目的的网络经营者来说，计费管理功能无疑是非常重要的。

在计费管理中，首先要根据各类服务的成本和供需关系等因素制定资费政策，资费政策还包括根据业务情况制定的折扣率；其次要收集计费收据，如使用的网络服务、占用时间、通信距离和通信地点等计算服务费用。

1. 计费管理的主要功能

（1）计算网络建设及运营成本。主要成本包括网络设备器材成本、网络服务成本、人工费用等。

（2）统计网络及其所包含的资源的利用率。为确定各种业务各种时间段的计费标准提供依据。

（3）联机收集计费数据。这是向用户收取网络服务费用的根据。

（4）计算用户应支付的网络服务费用。

（5）账单管理。保存收费账单及必要的原始数据，以备用户查询和置疑。

2. 计费管理的功能模块

（1）服务事件监测功能模块：负责从管理信息流中捕获用户使用网络服务的事件。将监测到的事件存入用户账目日志供用户查询，同时将有关信息送至资费管理模块计算费用。此外，还要对计费事件的合法性进行判断，如发现错误，自动产生计费故障事件向故障管理功能模块通报。

（2）资费管理服务功能模块：按照资费政策计算为用户提供的网络服务应收取的费用。资费政策需要根据技术进步和业务状况不断进行调整；同时还要根据服务的时间、日期及服务性质制定折扣率。

（3）服务管理功能模块：根据资费管理功能模块和计费控制模块的控制信息，限制用户可使用的业务种类。例如，是否有权拨打长途电话，是否有权使用特殊服务等。

（4）计费控制功能模块：负责管理用户账号、调整费率及服务管理规则等。计费控制功能由操作员进行操作。

1.3 网络管理模型

网络管理模型定义网络管理的框架、方式和方法。不同的管理模型会带来不同的管理能力、管理效率和经济效益，决定网络管理系统的不同的复杂度、灵活度和兼容性。20 世纪 80 年代末期，ISO 提出的基于远程监控的管理框架是现代网络管理模型的基础。在此基础上，提出了建立综合网络管理系统（Integrated Netwok Mamagement System，INMS）的建议，并形成了两种主要的网络管理模型，即以 OSI 模型为基础的系统管理模型公共管理信息协议（Common Management Information Protocol，CMIP）和以 TCP/IP 模型为基础的网络管理模型（SNMP）。

1. 网络管理的分层模型

INMS 的思想就是按照通用标准制造网络设备，用统一的 INMS 取代众多不同的 NMS。