新世纪应用型高等教育
网络专业系列规划教材

新世纪

网络管理与维护

新世纪应用型高等教育教材编审委员会　组编
主 编　寇海洲　陈宏明

大连理工大学出版社

新世纪应用型高等教育
网络专业系列规划教材

新世纪

网络管理与维护

WANGLUO GUANLI YU WEIHU

新世纪应用型高等教育教材编审委员会　组编
主 编　寇海洲　陈宏明
副主编　章　慧　单劲松　刘泉生

大连理工大学出版社

图书在版编目(CIP)数据

网络管理与维护 / 寇海洲，陈宏明主编. —大连：大连理工大学出版社，2013.11

新世纪应用型高等教育网络专业系列规划教材

ISBN 978-7-5611-7979-6

Ⅰ. ①网… Ⅱ. ①寇… ②陈… Ⅲ. ①计算机网络管理－高等职业教育－教材②计算机网络－计算机维护－高等职业教育－教材 Ⅳ. ①TP393.07

中国版本图书馆 CIP 数据核字(2013)第 133241 号

大连理工大学出版社出版

地址：大连市软件园路 80 号　邮政编码：116023

发行：0411-84708842　邮购：0411-84703636　传真：0411-84701466

E-mail：dutp@dutp.cn　URL：http://www.dutp.cn

大连美跃彩色印刷有限公司印刷　　大连理工大学出版社发行

幅面尺寸：185mm×260mm　印张：18.5　字数：450 千字

印数：1～1500

2013 年 11 月第 1 版　　2013 年 11 月第 1 次印刷

责任编辑：马　双　　责任校对：鲍雪梅

封面设计：张　莹

ISBN 978-7-5611-7979-6　　定　价：39.50 元

前　言

计算机技术和通信技术的紧密结合形成了当今发展最迅速、应用最广泛、技术最先进的计算机通信设施——计算机网络。网络管理是计算机网络发展的必然产物，它随着计算机网络的发展而发展。最早的网络管理是局域网管理，局域网管理主要保证在局域网内的所有计算机能够顺利传输和共享文件，其管理系统与网络操作系统密不可分。随着 Internet 的普及，网络管理不再局限于保证文件的传输，而是保障连接网络的网络对象（路由器、交换机和线路等）的正常运转，同时监测网络的运行性能，优化网络的拓扑结构。网络管理系统也因此越来越独立，越来越复杂，功能越来越完备，网络管理也发展成为计算机网络中的一个重要分支，国际上各种网络管理的标准也相继制定，网络管理逐步变得规范化、制度化。

网络管理理论抽象，术语众多。本教材以网络管理的四大模型为基础，以五大功能为主线，按理论、技术、产品及功能展开叙述。本教材内容组织有条理，逻辑关系清楚，论证充分，通俗易懂。本教材重点章节都有针对理论的一个或多个相应的实验教学案例，注重学生动手能力的培养，同时，也注重教材习题的配套。

本教材共分为 8 章：第 1 章，网络管理概论，讲述了网络管理的基本概念、网络管理的功能和目标、网络管理模型与协议、网络管理系统的类型及特点、新型的网络管理模型。第 2 章，域和活动目录，讲述了活动目录简介、活动目录的创建与配置、活动目录的管理、用户和用户组的管理。第 3 章，网络连接设备的管理，讲述了 TCP/IP 体系结构与介质基础、网络连接设备概述、交换机的配置、路由器的配置与管理、网络配置管理案例。第 4 章，网络安全与攻击防范，讲述了网络安全的基本概念、网络安全评价标准、网络攻击技术、入侵检测概述、网络安全的防范技术、计算机病毒的防护、黑客攻击与防范。第 5 章，防火墙与 VPN 技术，讲述了防火墙概述、防火墙的工作方式、防火墙的分类、防火墙的设置、防火墙注意事项、VPN 技术、VPN 的配置与管理。第 6 章，数据恢复和备

新世纪

份，讲述了文件恢复简介、数据库文件恢复、常用文件恢复、系统故障恢复、数据备份、磁盘阵列、服务器数据备份与恢复。第7章，网络调测与故障排查，讲述了网络综合测试、交换机测试、路由器测试、局域网故障维护、网络故障检测、交换机和路由器等网络设备故障恢复。第8章，网络管理系统，讲述了网络管理系统简介、网络管理系统平台、LinkManager系列网络管理系统，并且比较详细地介绍了物联网的相关知识。

本教材由淮阴工学院的寇海洲和陈宏明任主编，淮阴工学院的章慧、单劲松和南宁学院的刘泉生任副主编。其中，第1章由章慧编写，第2章由陈宏明编写，第3章由单劲松编写，第4、5、6、7章由寇海洲编写，第8章由刘泉生编写。全书由陈宏明统稿。

由于作者水平有限，书中难免存在缺点和不足，恳请读者提出宝贵意见。

编　者

2013年11月

所有意见和建议请发往：dutpbk@163.com

欢迎访问教材服务网站：http://www.dutpbook.com

联系电话：0411-84707492　84706104

目　录

第1章 网络管理概论

随着网络技术的发展、网络规模的逐渐增大以及复杂度的不断增加，网络的异构性也越来越强。网络的异构性是指网络的形态和网络设备伴随网络技术的发展而产生，并且它们能够共存在一个体系中。计算机网络管理技术的发展是与互联网的发展同步进行的，网络管理技术目前也得到了迅速的发展。时至今日，计算机网络和全球信息化时代已经到来，网络管理和网络安全性等问题的重要性日益突出。计算机网络一旦崩溃，将会给企业、公司、单位、学校以及人们的工作、学习和日常生活带来巨大的损失。因此，网络管理成为网络技术发展中的一项重要技术，它对网络技术的发展有着重要的影响，是现代信息网络中最重要的研究课题之一，并为越来越多的人所重视。计算机网络维护与管理是为了提高网络的稳定性、安全性。网络管理的任务是监测和控制组成整个互联网的硬件和软件系统，监测并纠正导致网络通信低效，甚至不能进行通信的问题，并且尽量降低这些问题再度发生的可能性。硬件或软件的错误都能导致这些问题，所以要同时对硬件和软件进行管理。

本章学习要点

- 理解网络管理的基本概念
- 熟悉网络管理的功能和目标
- 掌握网络管理模型与协议
- 重点掌握网络管理的类型及特点
- 了解新型的网络管理模型

1.1 网络管理的基本概念

网络管理是指监督、控制网络资源的使用和网络各种活动，从而使网络性能达到最稳定的过程，即对计算机网络的配置、运行状态和计费等所从事的全部操作和维护性活动。它提供了对计算机网络进行规划、设计、操作运行、监测、控制、协调、分析、测试、评估和扩展的各种手段，维护整个网络系统正常、高效运行，使网络资源得到更加有效的利用，当网络出现故障时能及时报告和处理。简单地说，网络管理实际上就是通过合理的方法和手段使网络综合性能达到最佳状态。网络管理实际上还包括电信管理。为了与传统网络管理区分开，可以把目前的网络管理称为现代网络管理，其追求的是集成化、开放型、分布式的网络管理模型。

对于不同的网络，管理的要求和难度也不同，局域网管理相对简单，因为局域网运行相同的操作系统，只要熟悉网络操作系统的管理功能和操作命令就可以管理好一个局域网。对于异构型网络，由于运行多种操作系统，管理起来就很复杂，而且特别困难，如 Internet，就需要跨平台的网络管理技术。在 TCP/IP 网络中有一个简单的管理工具——Ping 程序，它可以确定通信目标的连通性及传输时延。如果网络规模很大，互联设备很多，Ping 返回的信息很少，这种方法就不太适用，另外用 Ping 程序对很多设备逐个测试检查，工作效率很

低。在这种情况下出现了用于 TCP/IP 网络管理的标准——简单网络管理协议(Simple Network Management Protocol,SNMP)。这个标准适用于任何支持 TCP/IP 的网络,包括任何厂商生产的设备,以及运行任何操作系统的网络。

国际化标准组织 ISO 也推出了开放系统互联 OSI(Open System Interconnection)系统管理标准 CMIS/CMIP,它更适合结构复杂、规模庞大的异构型网络,但由于其技术开发缓慢,所以尚未进入实用阶段,也许它代表了未来网络管理发展的方向。网络管理标准的成熟刺激了制造商的开发活动,市场已经出现了符合国际标准的商用网络管理系统。有主机厂家开发的网络管理系统开发软件(如 IBM Net View,HP Open View),有网络新产品制造厂商推出的与硬件相结合的网络管理工具(如 CiscoWorks 2000,Cabletron Spectrum)。这些产品都可以称之为网络管理平台,在此基础上开发适合用户网络环境的网络管理应用软件,才能实施有效的网络管理。

1.2 网络管理的功能和目标

网络管理的目的是协调、保持网络系统高效、可靠地运行,当网络出现故障时,能及时地报告和处理。ISO 建议网络管理应包含以下基本功能:故障管理、计费管理、配置管理、性能管理和安全管理。

(1)故障管理(Fault Management)。故障管理是网络管理中最基本的功能之一。当网络发生故障时,①必须尽可能快地找出故障发生的确切位置;②将网络其他部分与故障部分隔离,以确保网络其他部分不受干扰继续运行;③重新配置或重组网络,尽可能降低隔离故障对网络带来的影响;④修复或替换故障部分,将网络恢复为初始状态。对网络组成部件状态的监测是网络故障检测的依据。不严重的简单故障或偶然出现的错误通常被记录在错误日志中,一般无需做特别处理;而严重一些的故障则需要通知网络管理器,即发出报警。因此网络管理器必须具备快速和可靠的故障监测、诊断和恢复功能。

(2)计费管理(Accounting Management)。在商业性有偿使用的网络上,计费管理功能统计哪些用户、使用何信道、传输多少数据、访问什么资源等信息;另一方面,计费管理功能还可以统计不同线路和各类资源的利用情况。由此可见,计费管理的根本依据是网络用户占用资源的情况,例如,信息传输量、占用线路的时间等统计量。

(3)配置管理(Configuration Management)。配置管理也是网络管理的基本功能。计算机网络由各种物理结构和逻辑结构组成,这些结构中有许多参数、状态等信息需要设置并协调。另外,网络运行在多变的环境中,系统本身也经常要随着用户的增减或设备的维修而调整配置。网络管理系统必须具有足够的手段支持这些调整,使网络更有效地工作。

(4)性能管理(Performance Management)。性能管理的目的是在使用最少的网络资源和具有最小延迟的前提下,确保网络能提供可靠、连续的通信能力,并使网络资源的使用达到最优化的程度。网络性能管理有监测和控制两大功能,监测功能实现对网络中的活动进行跟踪,控制功能,实施相应调整来提高网络性能。性能管理的具体内容包括:从被管理对象中收集与网络性能有关的数据;分析和统计历史数据;建立性能分析的模型;预测网络性能的长期趋势;根据分析和预测的结果,对网络拓扑结构、某些对象的配置和参数做出调整,逐步达到最佳运行状态。如果需要做出的调整较大,还要考虑扩充或重建网络。

(5)安全管理(Security Management)。安全管理的目的是确保网络资源不被非法使用,防止网络资源由于入侵者攻击而遭受破坏。其主要内容包括:与安全措施有关的信息分发(如密钥的分发和访问权设置等);与安全有关的通知(如网络有非法侵入、无权用户对特定信息的访问企图等);安全服务措施的创建、控制和删除;与安全有关的网络操作事件的记录、维护和查询日志管理工作等。一个完善的计算机网络管理系统必须制定网络管理的安全策略,并根据这一策略设计实现网络安全管理系统。

最初的网络管理往往指实时网络监控,以便在不得已的条件下(如过载、故障)使网络仍能运行在最佳或接近最佳状态。监测是从网络中获取信息,而控制则是改变网络状态。如今的网络管理范围已经扩大到了网络中的通信活动以及与网络的规划、组织、实现、运营和维护等相关的几乎所有过程。

网络管理的目的就是最大限度地增加网络可利用的时间,合理地组织和利用系统资源,提供安全、可靠、有效和优质的服务,保证网络正常、经济、可靠和安全地运行。或者说网络管理的目标就是对网络资源(硬件和软件)进行合理分配和控制,以满足业务提供者的要求和网络用户的需要,使网络资源得到最大限度的利用,整个网络更加经济地运行,同时能够提供连续、可靠和稳定的服务。

现代网络管理的内容通常可以用运行、管理、维护和提供来概括。

运行(Operation):针对向用户提供的服务而进行的面向管理的活动,如用户质量管理和用户计费等。

管理(Administration):针对向用户提供的有效服务,为满足服务质量要求而进行的管理活动,如对整个网络的管理和网络流量管理。

维护(Maintenance):为保障网络及其设备的正常、可靠、连续运行而进行的管理活动,如故障检测、定位和恢复,其中还有对设备单元的测试。维护又可分为预防维护和修正维护。

提供(Provision):针对网络资源的服务而进行的管理活动,如安装软件、配置参数等。为实现某种特定服务而提供资源、向用户提供某种服务等都属于这个范畴。

1.3　网络管理模型与协议

只要存在网络就必然要进行网络管理,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、异构性不断提高。根据 ISO 的定义,网络管理是为了使网络的性能达到最优所进行的监督、规划、网络资源的控制和使用等各种网络活动。目前,有影响的网络管理技术有 SNMP(简单网络管理协议)、CMIS/CMIP(公共管理信息服务和协议)、RMON(远程监控)和基于 Web 的网络管理技术。

1.3.1　网络管理模型

在网络管理中,网络管理人员通过网络管理系统对资源(如网桥、网关、路由器、集线器、工作站、微机、机柜中的插件板、通信软件等)进行管理,普遍遵循的结构都是管理者-代理(Manager-Agent)的管理模型,如图 1-1 所示。从图中可以看出,一个网络管理系统从逻辑上可以认为是由管理进程(Management Process)、管理协议(Management Protocol)、代理

管理(Agent)和管理信息库(MIB,Management Information Base)四要素组成的。其中MDB为管理信息库的数据库物理存储。

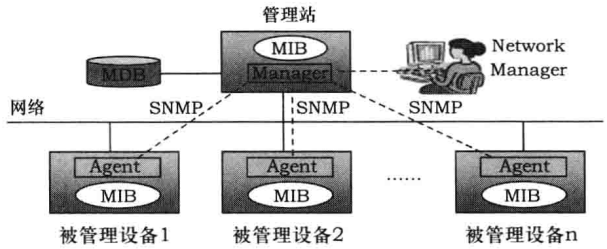

图 1-1 网络管理模型

管理者(Manager),即管理进程,可以是工作站、微机等对网络设备进行全面管理和控制的软件,一般位于网络系统的主干位置,运行于网络管理中心工作站上,负责发出所有的控制与管理操作命令,实现对管理代理的操作与控制,并接收来自代理的信息。代理是网络系统的一部分,位于工作站或其他网络设备(称为管理元素)中,收集信息反馈给这些设备的管理系统。管理系统在中心位置运行,但在分布式管理系统中,管理子系统可能位于网络的各节点,以收集周期性地传输给主管理系统的本地信息。每次网络管理活动都是通过网管请求的给予(网络管理中心的管理者进程)和网络请求的接收(代理系统中的代理进程)之间的交互式会话实现的。

网络管理员首先通过特定的请求窗口向管理者提交网管请求,然后通过本地的网络通信模块把该请求送给指定的远程代理,并等待执行结果的返回。远程代理在接收到该请求后,向被监控的网络资源发出执行网管请求的命令。此时,远程代理将等待执行结果,或在被监控的网络资源出现异常情况时产生事故报告(该报告是由于系统故障或者阀值自动产生的,与该网管请求无关)。然后,远程代理通过其网管通信模块向网管中心发回网管结果。网管中心的管理者在接收到网管结果或事件报告后,经过分析处理再通过指定窗口把结果显示出来。

一个管理可以和多个代理进行信息交互,同时一个代理也可以接受来自多个管理者的管理操作,但此时代理需要处理来自多个管理者的多个操作之间的协调问题。

一般的代理都是返回它本身设备的信息,在网络管理中还有另一种代理——转换代理。例如,SNMP要求所有代理的设备和管理站都必须实现TCP/IP,对于不支持TCP/IP的设备(如某些网桥、调制解调器和可编程控制器)不能直接用SNMP进行管理,为此提出了转换代理(也叫委托代理),实际上委托代理起到了协议转换的作用。

每一个管理代理都拥有自己的管理信息库,管理代理的本地MIB不一定具有ISO或Internet定义的MIB的全部内容,而只需包括与本地设备相关的管理对象。MIB中的变量对应着相应的管理对象。管理者与代理之间的通信协议为SNMP和CMIP,它们分别为Internet标准和ISO标准,其不同之处在于各自定义被管理对象和对被管理对象进行分类的原则与标准不同,前者较简单实用,后者较严格与规范。

网络管理者与管理代理之间共同用一个管理信息模型来统一对被管理网络资源的认识,协调管理两端的管理操作与动作。网络管理信息模型的主要作用是描述物理的或逻辑的网络资源,模型中规定管理系统中有关的资源特性。在ISO标准中定义了如下管理信息结构:要管理的资源抽象为管理对象(Manager Object,MO);资源的有关信息抽象为被管理

对象的属性(Attribute);资源之间的关系定义为对象之间的关系(Relationship);具有相同属性的管理对象集合称为对象类(Object Class),具体的某一管理对象称为对象的实例(Object Instance)。其中,对象类的定义包括:从外部看到的属性、作用于管理对象上的网络操作、管理对象对操作所做出的反应(即行为,Behavior),以及操作完毕后管理对象向管理者发回的通报(Notification)。

MIB 仅是一个概念上的数据库,实际中并不存在这样的数据库。它应理解为分布在网络管理中的 MIB(即中央数据库),以及所有代理系统中的本地 MIB 库的集合。因此,数据库用于记录网络中管理对象的信息。例如,状态类对象的状态代码、参数类管理对象的参数代码值等。

1.3.2　网络管理协议

网络管理具体的实现方法有命令行、SNMP/CMIP、Web 管理和 CORBA 管理等。其中 SNMP 是 Internet 管理标准,主要是基于 TCP/IP 协议的,现在已经被其他协议实现,如 IPX/SPX、DECNET 以及 Apple Talk 等。CMIP 是 ISO 标准,其基于 ISO/OSI 七层协议模型,是一个更为有效的网络管理协议。CORBA (Common Object Request Broke Architecture)的中文意思是公共对象请求代理,它是 OMG(Object Management Group)为解决分布式处理环境下硬件和软件系统的互联互通而提出的一种解决方案。基于 Web 的网络管理 WBM(Web-Based Management)模型是在 Internet 不断普及的背景下产生的,实际得用 Web 浏览器来监控和管理网络资源,模型就是将 Internet 技术与现有的网络管理技术相融合,为网络管理人员提供更有分布性和实时性、操作更方便、能力更强的网络管理方法。

1. 基于 SNMP 的网络管理

(1)SNMP 的发展

TCP/IP 网络管理系统最初使用的是 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 SNMP 第一版,陆续公布在 1990 年和 1991 年的几个 RFC(Request For Comments)文档中,即 RFC155(SMI),RFC1157(SNMP),RFC212(MIB 定义)和 RFC1213(MIB-2 规范)。由于其简单性和易于实现,SNMPv1 得到了许多制造商的支持和广泛的应用。

当初提出 SNMP 的目的,是将其作为弥补网络管理协议发展阶段之间空缺的一种临时性措施。SNMP 出现后显示出了许多优点,最主要的是简单、容易实现,而且是基于人们熟悉的 SGMP。在 1988 年,为了适应当时紧迫的网络管理的需求,开发了网络管理标准双轨制的策略:一是 SNMP 可以满足当前网络管理的需要,用于管理和配置简单的网络并且在将来可以平稳地过渡到新的网络管理标准。二是 OSI 网络管理(CMIP Over TCP/IP,CMOT)作为长期的解决办法,可以应对未来的更复杂的网络配置,提供更全面的管理,但是需要较长的开发过程,以及开发商和用户的接受。然而,这个双轨制策略很快停止了实施,其主要原因如下:

①原来的想法是 SNMP 的 MIB 应该是 OSI MIB 的子集,以便顺利过渡到 CMOT。但是 OSI 定义的管理信息库是比较复杂的面向对象模型,在此基础上实现 SNMP 几乎是不可能的,所以很快放弃了这个想法,让 SNMP 使用简单的标量 MIB。

②OSI 系统管理标准和符合 OSI 标准的网络管理产品的开发进展缓慢，而在此期间，SNMP 却得到了制造商广泛的支持，出现了很多 SNMP 产品，并得到广大用户的接受。

SNMP 的体系框架是围绕以下 4 个概念和目标进行设计的：

①保持管理代理的软件成本尽可能低。

②最大程度地保持远程管理的能力，以充分利用 Internet 的网络资源。

③必须保留原来的扩充余地。

④保持 SNMP 的独立性，不依赖于具体的计算机、网关的网络传输协议。

SNMP 的设计原则是简单性和扩充性。为了简单，SNMPv1 只提供了 4 类操作：

①Get 操作用来读取特定的网络信息。

②Get-Next 操作通过遍历活动来提供强大的管理信息读取能力。

③Set 操作用来对管理信息进行控制(修改、设置)。

④Trap 用来报告重要的事件。

SNMP 的开发工作首先是在美国几所大学的实验室中进行的，最早的 SNMP 产品在 1988 年出台以后，几乎所有的 Internet 网络设备和设施的厂家都在开发与 SNMP 有关的产品并投放市场。支持 SNMP 的产品中最广泛的是 IBM 公司的 Net View、Cabletron 公司的 Spectrum 和 HP 公司的 Open View。

SNMP 虽然被广泛应用，但 SNMP 的缺点也是显然的：没有实质性的安全设施、无数据源认证功能、不能防止偷听。面对这样不可靠的管理环境，许多制造厂商不得不废除了 Set 命令，以避免网络配置被入侵者恶意篡改。为了修补 SNMP 的安全缺陷，1992 年 7 月出现了一个新标准——安全 SNMP(S-SNMP)，这个协议增加了以下安全方面的功能：

①用报文摘要算法 MD5 保证数据完整性和进行数据源认证。

②用时间戳对报文进行排序。

③用 DES 算法提供数据加密功能。

但 S-SNMP 没有改进 SNMP 在功能和效率方面的缺点。与此同时，有人又提出了另一个协议 SMP(Simple Management Protocol)，这个协议由 8 个文件组成，它可以运行在 TCP/IP 网络上，也适合 OSI 系统和其他通信协议的网络，并保持了 S-SNMP 的安全功能，能够管理任意资源，不仅是网络资源，还可以用于应用管理、系统管理。SMP 可以实现管理站点之间的通信，保持了 SNMP 简单性的原则，更容易实现，并提供了数据块传输能力，因而速度和效率更高。在安全性方面结合了 S-SNMP 提供的安全功能，并且可以运行在 TCP/IP 网络上，也可以运行在 OSI 系统和其他通信协议的网络上。

最后，Internet 研究人员决定对 SNMP 的安全功能进行扩充，决定以 SMP 为基础开发 SNMP 第 2 版，即 SNMPv2。

1992 年 10 月，IETF(The Internet Engineering Task Force，互联网工程任务组)组织了两个工作组并开始工作，一个组负责协议功能和管理信息库的扩展，另一个组负责 SNMP 的安全方面。1993 年 1 月，工作组完成工作，在 1993 年 5 月发布了 12 个 RFC 文件作为草案标准。后来有人认为 SNMPv2 安全机制实现起来太复杂，对代理的配置很困难，限制了网络发现功能，失去了 SNMP 的简单性。

(2)SNMPv3

使用 SNMPv1、SNMPv2 进行网络管理时，由于安全功能限制，面临着假冒、信息篡改、

信息暴露、报文序列和定时机制的修改等几种安全威胁。所以 SNMPv1、SNMPv2 的安全性总是不能满足人们的期望。1998 年 1 月，Internet 工作组正式发布了 SNMPv3 协议文档：RFC1271～RFC2275，主要对 SNMP 的安全性进行了很大的改进。

在 SNMPv1 和 SNMPv2 中，实现协议功能的进程称为协议引擎或协议机，而在 SNMPv3 中，实现 SNMP 协议功能的软件称为协议实体(SNMP Entity)，SNMP 引擎是协议实体的一部分。实体是体系结构的一种实现，由一个 SNMP 引擎(SNMP Engine)和一个或多个有关的 SNMP 应用模块(SNMP Application)组成，如图 1-2 所示表示了 SNMPv3 协议实体结构。

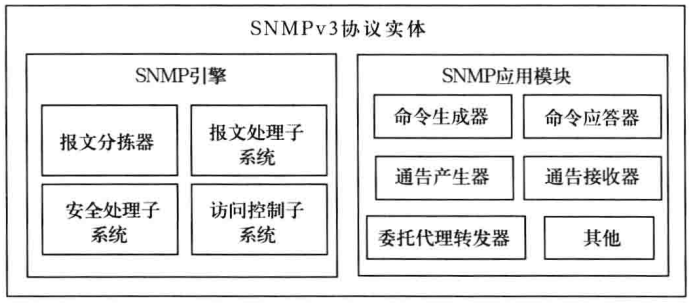

图 1-2　SNMPv3 协议实体结构

RFC2271 定义的 SNMPv3 体系结构，体现了模块化的设计思想，SNMP 引擎和它支持的应用程序被定义为一系列独立的模块。SNMP 实体的功能由在模块中的多个模块决定，每个实体仅仅是模块的不同组合，每个模块具有相对独立性，当改进或替换某一个模块时，不会影响整个结构，这样就可以简单地实现功能的增加和修改。

应用模块主要有：命令生成器(Command Generator)、通告接收器(Notification Receiver)、委托代理转发器(Proxy Forwarder)、命令应答器(Command Responder)、通告产生器(Notification Originator)和一些其他的应用。

SNMPv3 中命令生成器的主要功能是监控和操作管理数据，一般在管理进程一方实现；命令应答器的功能是实现管理数据的访问，一般在管理代理一方实现；通告产生器的功能是发送异步的通知报文(如 Inform Request，Trap 等)；通告接收器的功能是接收并处理异步的通知报文，一般在管理进程一方实现；委托代理转发器的功能是向不支持 SNMP 的设备转发报文，一般在管理代理一方实现。

作为 SNMP 实体核心的 SNMP 引擎用于发送和接收消息、对消息进行解密和加密以及对管理对象进行访问控制。SNMPv3 协议的引擎是由报文分拣器、安全处理子系统、报文处理子系统和访问控制子系统组成的。

SNMP 引擎中的报文分拣器的功能是接收和发送报文，确定报文版本号并将该报文发送给相应的报文处理模块，并为接收和发送 PDU 的 SNMP 应用提供一个抽象的接口。

报文处理子系统是由若干个报文处理模块(Message Processing Model)组成，不同的模块处理不同版本的报文，它的功能是按照预定的格式准备要发送的报文，或者从接收的报文中提取数据，如图 1-3 所示。

安全处理子系统提供安全服务，如报文的认证和加密。一个安全处理子系统可以有多个安全模块，以便提供不同的安全服务，如图 1-4 所示。安全处理子系统是由安全模型和安

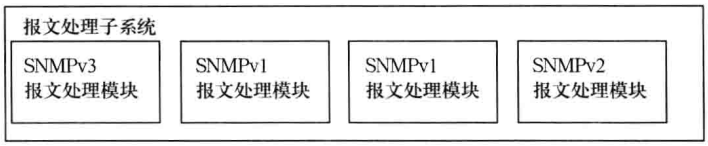

图 1-3 报文处理子系统

全协议组成。每一个安全模块定义了一种具体的安全模型，说明它提供安全服务的目的和使用的安全协议。而安全协议则说明了用于提供安全服务（如认证和加密）的机制、过程以及 MIB 对象。

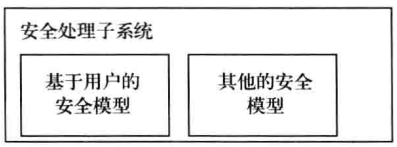

图 1-4 安全处理子系统

访问控制子系统通过访问控制模块（Access Control Model）提供授权服务，即确定是否允许访问一个管理对象，或者是否可以对某个管理对象进行特殊的管理操作，如图 1-5 所示。每个访问控制模块定义了一个具体访问决策功能，用以支持访问权限的决策。SNMPv3 目前定义了基于视图的访问控制模型 VACM（View-based Access Control Model），VACM 是由 RFC2275 定义的，且允许访问控制进行非常灵活的配置。

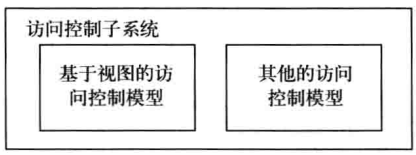

图 1-5 访问控制子系统

（3）SNMPv3 的安全机制

在网络环境中，管理实体之间传递的管理信息会受到多种威胁，最常见的包括修改、伪装和窃听。

修改是指在信息传递过程中非授权用户对其内容进行修改。这种修改不包括对消息的源地址和目的地址的修改。管理实体收到消息后，不知道其中的内容已被修改。

伪装是指非授权用户假冒授权用户向另一个用户发送消息。这种攻击可以通过修改消息的源地址实现。通过伪装的和修改的信息，非授权用户可以执行未被许可的操作。非授权用户还可以通过重排分组的顺序来改变消息的意义。

窃听是指在消息传递过程中非授权用户对其进行拷贝，通过获得副本来窃取消息中的信息。窃听不改变消息的正常传递通路，也不改变消息中的内容。

在 SNMPv3 中需要实现以下安全目标：

①验证接收到消息的完整性，确认在传输过程中没有被修改。

②验证源发送者的身份，确认其不是伪装。

③根据报文中的生成时间，确认从发送到接收之间的延迟在限定的时间窗口内。

为了实现以上目标，SNMPv3 的安全机制由鉴别模块、时标模块和加密模块三个部分组成。鉴别模块实现数据的完整性鉴别和数据源的身份鉴别。时标模块用于检验报文的传

输时延，确认报文时延在规定的时间窗口内。加密模块实现报文内容的加密。

在 SNMPv3 的体系结构中，安全模型为消息处理模型提供接口，对去往和到来的各类消息进行安全服务。为了防止非法授权用户对管理信息的修改、伪装和窃听，安全模型通过认证（Authentication）、保密（Privacy）和时限（Timeliness）模块，提供了安全性（Data Integrity）、数据源认证（Data Origin Authentication）、数据保密（Data Confidentiality）和消息时限（Message Timeliness）共四种服务。

当两个管理实体进行安全通信时，需要确定根据哪一方的信息判断接收的消息是安全的，例如，根据发送实体的时钟或是根据接收实体的时钟来判断消息是否超时。因此，SNMPv3 提出了权威 SNMP 引擎（Authoritative SNMP Engine）的概念，即相互通信的两个引擎中有一个被确定为权威的，另一个为非权威的。当 SNMP 消息要求应答时，接收消息的引擎是权威的，当 SNMP 消息不要求应答时，发送消息的引擎是权威的。

在安全模型中，认证模块提供数据完整性服务和数据源认证服务。发送端的数据完整性服务对消息的内容和顺序的完整性信息进行签发，接收端的数据完整性服务根据发送端签发的数据完整性信息对收到的数据进行认证，以鉴别数据在传输过程中是否被修改。数据源认证服务保证消息发送者声称的身份是真实的，认证模块通过在消息中加入与权威 SNMP 引擎相联系的一个唯一标识符来实现这个服务。

保密模块提供数据保密服务。发送端的数据保密服务对消息进行加密；接收端的数据保密服务对消息进行解密，以保证数据在传输过程中不被窃听。

时限模块提供消息时限服务，以防止消息被转向（Redirection）、延迟（Delay）和重播（Replay）。这个服务将消息的传输时间规定在时间窗口内，超时的消息被认为是不安全的。

2. 远程网络监测

SNMP 为远程网络监测提供了基础，利用 SNMP，网络操作中心（Network Operation Center）可以方便地进行配置和故障管理。但是，对网络性能进行管理却受到一定的限制，网络的性能是由不同时刻的统计特性反映的，这是不能直接利用 SNMP 获得的数据，因此，需要在 NOC 基础上开发监测网络重要参数的技术，即远程网络监测 RMON（Remote Network Monitoring）。开发 RMON 的目的是使 SNMP 更为有效、更为积极主动地监控。

对网络流量统计是网络管理的重要内容。虽然利用 MIB-II 可以获得各个代理所在节点各种协议数据的分组计算值，但是却不能获得全网的流量信息。当然，理论上讲，管理站可以通过不断地轮询各个节点的 MIB-II 来计算网络流量，但在实际上这是不太可行的：一方面会导致网络中传递大量的管理信息，使网络不堪负荷；另一方面也会由于承载管理操作命令和操作结果的分组的丢失而使得统计结果不准确。

因此，为了对网络流量进行监测，人们将一些专用设备配置在各个节点，并将这些设备称为网络监测器（Network Monitor 或 Prober），由此产生了 RMON 的概念。一般监测器工作在“混杂”模式下，即对网络中各种类型的分组进行观察，从而得到网络的总体信息，包括长度不足的分组、冲突数等错误事件统计以及每秒传递的分组数、分组大小的分布等性能统计。监测器还可将一些分组存储下来，以备事后分析。在网络互联环境下，为了达到监测网络流量的目的，一般每个子网需要一个监测器。监测器通常是一个独立的设备，专用于捕获和分析流量。

RMON 有许多先进之处。首先，每个 RMON 设备都对本地网段进行监测和分析，既可

被动也可主动地向网络管理系统传递信息。例如，当它发现严重的分组丢失和过高的冲突时，可以主动地向管理站报警。由于监测是在本地进行的，所以得出的分析结果是非常可靠的。同时这种工作方式大大降低了 SNMP 的流量。其次，RMON 降低了对网络管理操作和维护以及引擎的特殊要求。引擎常常会因为网络过载等原因而联系不上，如果没有 RMON 设备，此时引擎到底发生了什么情况事后是难以调查的。因此，往往引擎越是联系不上，网络管理系统越要与它联系。最后，RMON 设备对本地子网的监测几乎可以做到连续不断，这会显著提高统计和控制的精度，使得故障能够及时被发现、报告和诊断。

为了给 RMON 技术提供标准，IETF 发布了 RFC1757 和 RFC1513 分别对 Ethernet LAN 和 Token Ring LAN 的 RMON 进行了规范，形成了第一版的 RMON，这个规范的发布，使互联网的管理向前迈进了非常重要的一步。RMON 虽然只是一个 MIB 规范，并未对 SNMP 协议进行任何修改，但却显著地扩展了 SNMP 的功能。RMON 开发之初便确定了如下几个目标：

脱机操作：尽量减少网络管理者对监测器的轮询，使监测器能自主工作，积累数据，在必要时向管理站报告。

提前监测：监测器要能够不断地对网络进行诊断并记录日志，以便在必要时向管理站提供对诊断故障有帮助的信息。

问题监测和报告：监测器能够连续不断地对网络及网络资源的消耗进行监测，以便及时检查错误和其他意外情况。

增值数据：监测器要能对数据进行有针对性的分析，以减少管理站的工作。例如，监测器可以分析子网的流量以确定哪些主机产生的流量和错误最多。

多管理者：为了提高可靠性、完成不同的功能以及为不同的部门提供不同的管理能力，监测器需要具备同时处理多个管理站操作请求的能力。

尽管不是所有的监测器都能满足上述目标，但 RMON 规范为支持这些目标提供了基础。

图 1-6 是基于 RMON 的远程监测的一个配置实例，它是一个拥有 5 个子网的互联网。图中左边 3 个子网配置在一个楼内，另外 2 个子网里有两个不同的远程站点。一个具有 RMON 管理能力的专门管理站被连接到中心 LAN 上。另外两个子网 RMON MIB(远程监控管理信息库)分别被配置在两个 PC 上，专门用于远程监测。具有 RMON 管理能力的管理站被连接到 FDDI 骨干网上，成为在此网络中的第二个管理站。Token Ring LAN 的 RMON MIB 功能由该 LAN 的路由完成。RMON 最初的设计是用来解决从一个中心点管理各局域分网和远程站点的问题。RMON 规范是由 SNMP MIB 扩展而来的。RMON 中，网络监视数据包含了一组统计数据和性能指标，它们在不同的监视器(或称探测器)和控制台系统之间相互交换。结果数据可用来监控网络利用率，以用于网络规划、性能优化和协助网络错误诊断。

当前 RMON 有两种版本：RMONv1 和 RMONv2。RMONv1 在目前使用较为广泛的网络硬件中都能发现，它定义了 9 个 MIB 组服务于基本网络监控；RMONv2 是 RMON 的扩展，专注于 MAC 层以上更高的流量层，它主要强调 IP 流量和应用程序层流量。RMONv2 允许网络管理应用程序监控所有网络层的信息包，这与 RMONv1 不同，后者只允许监控 MAC 层以下层的信息包。