网络管理与防火墙技术

刘占全 编著

黎连业 审

人民邮电出版社

网络管理与防火墙技术

刘占全　编著

黎连业　　审

人 民 邮 电 出 版 社

图书在版编目(CIP)数据

网络管理与防火墙技术/刘占全编著. -北京：人民邮电出版社，1999.7
ISBN 7-115-07855-6

I.网… II.刘… III.① 因特网-管理② 因特网-防火墙 IV.TP393.4

中国版本图书馆 CIP 数据核字(1999)第 14284 号

内 容 提 要

本书从网络管理员角度出发，系统介绍了网络管理的基本知识，以及今后几年的热点——防火墙技术。作为网络管理员要管理什么？防火墙的核心技术是什么？堡垒主机、数据包过滤、代理主机技术有哪些内容？防火墙怎样建设？对这些问题书中均作了较为详细的叙述。

本书内容新颖、通俗易懂，可供网络管理人员、大专院校计算机专业的师生和计算机联网用户阅读参考。

网络管理与防火墙技术

◆ 编　　著　刘占全
审　　黎连业
责任编辑　张瑞喜

◆ 人民邮电出版社出版发行　北京市崇文区夕照寺街 14 号
北京密云春雷印刷厂印刷
新华书店总店北京发行所经销

◆ 开本：787×1092　1/16
印张：12.75
字数：310 千字　　1999 年 7 月第 1 版
印数：1－5 000 册　　1999 年 7 月北京第 1 次印刷
ISBN 7-115-07855-6/TP·1134

定价：20.00 元

前　言

随着计算机网络技术的发展和局域网、因特网的广泛应用，网络系统的管理责任越来越重大。网上“黑客”、计算机病毒等问题，使得网络管理人员不得不关注网络安全问题和防火墙技术。

防火墙是一种行之有效的网络安全机制，它是在网络内部与外部之间实施安全防范的系统。本书首先以 Windows NT 为背景叙述网络管理员的基本工作，在此基础上，再讲述防火墙技术，以便把网络管理与防火墙系统的管理结合起来。书中对 Windows NT 管理、用户帐户管理、网络安全性与研究对象等网络管理员的基本管理工作，以及防火墙技术的核心——堡垒主机、数据包过滤、代理服务，防火墙建筑实例等内容做了深入浅出的讲述。

本书写作过程中，得到原中科院计算所网络研究开发中心的王钢、刘春阳、杨一鸣、练子川、顾寿筠、刘凯、李宝红、张国清等同志的热情支持和帮助，作者在此一并表示感谢！

作者于联想科技公司

1999 年 2 月

目　录

第一章　网络管理概述 1

1.1　网络管理的功能与网络管理标准简介 1

1.1.1　性能管理 2

1.1.2　故障管理 3

1.1.3　配置管理 3

1.1.4　计费管理 4

1.1.5　安全管理 4

1.2　网络管理协议简述 6

1.2.1　SNMP 网络管理协议简述 6

1.2.2　CMIP 管理协议简述 9

1.3　网络管理诸因素的简析 10

1.4　网络管理解决方案 11

1.4.1　ManageWise 为网络提供全面管理 12

1.4.2　改进网络的可靠性和性能 12

1.4.3　适用于各种规模企业的可扩展解决方案 12

1.4.4　ManageWise 的主要功能 13

1.4.5　ManageWise 管理的三种方案 14

第二章　Windows NT 15

2.1　Windows NT 简述 15

2.1.1　Windows NT 的特点 15

2.1.2　Windows NT 的体系 17

2.1.3　管理安全策略 18

2.1.4　Windows NT 文件系统 18

2.2　Windows NT 网络结构 19

2.2.1　Windows NT 网络环境 19

2.2.2　Windows NT 系统结构 20

2.2.3　网络传输协议 23

2.3　Windows NT 功能和优化的性能 24

2.3.1　Windows NT 功能 24

2.3.2　Windows NT 优化的性能 25

第三章　Windows NT 管理简述 26

3.1　Windows NT 管理内容 26

3.2 Windows NT 的管理工具 27
3.3 Windows NT 网络管理的术语解释 27
3.4 登录到计算机 29
3.5 Windows NT 的安全对话 30
第四章 用户帐户管理 31
4.1 用户帐户设置的具体操作方法 31
4.2 文件夹放置 37
4.3 删除和重新命名用户帐号 38
4.4 组帐号的设置与具体操作方法 39
4.5 创建本地组和全局组 39
4.6 实现内置组 41
4.6.1 所有基于 Windows NT 计算机上的内置组 42
4.6.2 只存在于域的控制器上的内置组 42
4.6.3 内置的系统组 43
4.6.4 最佳方案 43
4.7 管理用户帐户和组帐户 44
4.7.1 管理帐户简介 44
4.7.2 创建用户帐户模板 45
4.7.3 实现帐户策略 46
4.7.4 重新设置用户帐户口令 48
4.7.5 解锁用户帐户 48
4.7.6 修改多个用户帐户 49
4.8 维护域控制器 49
4.8.1 提升一台备份域控制器 50
4.8.2 恢复域控制器的功能 50
4.8.3 同步域控制器 51
4.9 排除登录故障 52
第五章 网络安全性与研究对象 53
5.1 网络安全性面临的威胁 53
5.2 网络安全的内容 55
5.3 需要多大的安全性 56
5.4 OSI 安全性体系结构 58
5.5 计算机网络安全的研究对象 66
5.6 数据加密的基本概念 66
5.6.1 数据加密 67
5.6.2 常规密钥密码体制 67
5.6.3 数据加密标准 DES 69
5.6.4 公开密钥密码体制 74

5.6.5 数字签名 76
5.6.6 密钥分配协议 77
5.7 OSI 环境下的威胁和安全措施 80
5.7.1 对网络安全的威胁 80
5.7.2 实现通信安全的加密策略 81
5.7.3 在端到端加密下的若干措施 83
第六章 防火墙与防火墙的作用 85
6.1 防火墙的作用 85
6.1.1 Internet 防火墙 85
6.1.2 是购买现有的防火墙还是自己设计防火墙? 87
6.2 防火墙设计 88
6.3 防火墙体系结构 91
6.3.1 双重宿主主机体系结构 91
6.3.2 屏蔽主机体系结构 92
6.3.3 屏蔽子网体系结构 93
6.4 防火墙体系结构的组合形式 96
6.4.1 使用多堡垒主机 96
6.4.2 合并内部路由器与外部路由器 97
6.4.3 合并堡垒主机与外部路由器 98
6.4.4 合并堡垒主机与内部路由器 99
6.4.5 使用多台内部路由器 100
6.4.6 使用多台外部路由器 102
6.4.7 使用多个周边网络 103
6.4.8 使用双重宿主主机与屏蔽子网 104
6.5 内部防火墙 104
6.5.1 试验网络 104
6.5.2 低保密度网络 105
6.5.3 高保密度网络 106
6.5.4 联合防火墙 106
6.5.5 共享参数网络 107
6.5.6 内部防火墙的堡垒主机选择 107
6.6 防火墙的未来 108
第七章 堡垒主机 109
7.1 堡垒主机的种类 109
7.1.1 无路由双重宿主主机 109
7.1.2 牺牲品主机 109
7.1.3 内部堡垒主机 110
7.2 堡垒主机建设的诸因素的选择 110

7.2.1 选择操作系统 110
7.2.2 对机器速度的要求 110
7.2.3 堡垒主机的硬件配置 111
7.2.4 堡垒主机的物理位置 111
7.3 堡垒主机提供的服务 112
7.4 建立堡垒主机 114
7.4.1 系统日志的建立方法 116
7.4.2 关闭所有不需要的服务 116
7.4.3 如何关闭服务 117
7.4.4 哪些服务需要保留 117
7.5 堡垒主机的监控 120
7.5.1 监控堡垒主机的运行 120
7.5.2 自动监测堡垒主机 120
7.6 堡垒主机的维护和备份 121
第八章 数据包过滤 122
8.1 数据包 122
8.2 数据包过滤是怎样工作的 123
8.2.1 包过滤的优点 124
8.2.2 包过滤的缺点 125
8.2.3 包过滤规则的概念 125
8.3 包过滤处理内核 126
8.3.1 包过滤和网络策略 126
8.3.2 一个简单的包过滤模型 126
8.3.3 包过滤器操作 127
8.3.4 包过滤设计 129
第九章 代理服务 134
9.1 为什么要进行代理 134
9.2 代理服务的优点 135
9.3 代理服务的缺点 136
9.4 代理服务是如何工作的 137
9.4.1 使用定制客户软件进行代理 137
9.4.2 使用定制的客户过程进行代理 137
9.5 代理服务器的使用 138
9.5.1 应用级与回路级代理 138
9.5.2 公共与专用代理服务器 139
9.5.3 智能代理服务器 139
9.6 在因特网服务中使用代理 139
9.6.1 TCP 与其它协议 139

9.6.2 单向与多向连接 139
9.7 不使用代理服务器的代理 140
9.8 使用 SOCKS 进行代理 140
9.9 使用 TIS 因特网防火墙工具包进行代理 142
9.10 使用 TIS FWTK 的 FTP 代理 142
9.11 如果不能代理怎么办 143
9.12 因特网主要服务功能的服务代理特性 144
第十章 防火墙建筑实例 148
10.1 子网过滤结构的防火墙 148
10.2 主机过滤结构的防火墙 161
10.3 商用防火墙 FireWall-1 介绍 166
10.3.1 FireWall-1 的资源要求 167
10.3.2 FireWall-1 体系结构 167
10.3.3 FireWall-1 控制模块 169
10.3.4 网络对象管理器 171
10.3.5 服务管理器 173
10.3.6 规则库管理器 174
10.3.7 日志浏览器 178
10.3.8 FireWall-1 应用程序举例 179
10.3.9 FireWall-1 的性能 180
10.3.10 FireWall-1 规则语言 180
10.3.11 获得 FireWall-1 的信息 181
附录 A TCP/IP 183
附录 B 网络安全与级别 189
参考文献 192

第一章　网络管理概述

计算机网络从问世到今天，其技术发展之快，是人们始料不及的。从小型的局域网到Internet，网络结构更加复杂，人们不仅可以共享网上资源，还开发了各种网络应用，对网络的依赖性也越来越大。人们不仅要求网络能连续可靠地工作，最大可能地为用户提供服务，还要保证网上信息的安全。这就向人们提出了网络管理的问题，也就是说不但要用好网络，而且要管理好网络。

实际上，网络管理已存在很久了。从广义上讲，任何一个系统都需要管理，只是由于系统的大小、复杂性的程度不同，管理在系统中的重要性也不同而已。随着时间的推移，网络系统的结构越来越趋于复杂，管理也越加重要，以前的网络管理技术已不能适应网络的迅速发展。特别是以往的网络管理系统往往是厂商在自己的网络系统中开发的专用系统，很难对其他厂商的网络系统、通信设备软件等进行管理，这种现象已不适应网络异构互连的发展趋势。

网络管理系统主要涉及以下几个方面的问题：

• 系统的功能。即一个网络管理系统应具备哪些功能。

• 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。网络中的资源是指网络中的硬件、软件以及所提供的服务等。而一个网络管理系统必须将它们表示出来，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。网络管理信息如何表示和传递？传送的协议是什么？这些都是构成一个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。

本章分四点进行叙述：

(1) 网络管理功能与网络管理标准简介；

(2) 网络管理协议简述；

(3) 网络管理诸因素的分析；

(4) 网络管理解决方案。

1.1　网络管理的功能与网络管理标准简介

为实现开放系统的互连，国际电信联盟 ITU 制定了电信管理网标准（Recommendation

M.3010），该标准为网络管理规定了五个方面的任务，每种业务内又制定了相关的多个功能模块，极大地方便了管理软件的开发。这五个方面的任务是性能管理、故障管理、配置管理、计费管理和安全管理。

1.1.1 性能管理

性能管理（Performance Management，PM）是对网络性能的管理，要求做到对网络的特性、资源利用率以及有关通信活动进行分析，以帮助网络管理人员评价网络资源及相关的通信活动的情况和效率。有效的性能管理能优化网络的性能，最大限度地满足不同层次用户对网络的需求。

今天的企业网可以连接数千台设备，成百上千的用户在网上工作，实现性能优化是不容易的。因此人们对网络进行性能管理时将主干设备和较小的子网区分开，分别进行管理，可使整个网络利用率达到最高。

性能管理可以从三个方面着手：

① 建立对当前网络性能测量的基准；

② 寻找识别网络与应用软件不匹配的方法；

③ 进行分析测量，寻找可能改进网络性能的对策。

性能管理包括系统资源的运行状况及通信效率等系统性能，其能力包括监视和分析被管网络及其所提供服务的性能机制。性能分析的结果可能会启动某个诊断测试过程或重新配置网络以维持网络的性能。性能管理收集、分析有关被管网络当前状况的数据信息，并维护和分析性能日志，其典型的功能包括：

① 收集统计信息；

② 维护并检查系统状态日志；

③ 确定自然和人工状况下系统的性能；

④ 改变系统操作模式以进行系统性能管理的操作。

性能管理依靠软件工具可以测量服务器 CPU 处理数据的速率，测量文件服务器与工作站之间数据传输的速率，统计有多少工作站在工作等。

有些软件管理工具还可以监测磁盘利用率，例如有多少文件存在指定的目录里或卷里，这些文件归谁所有，文件的长度及存入时间等，从而可以帮助管理员了解是否有用户超越了权限，过多地使用了服务器硬盘空间，也便于硬盘容量的分配。

进行性能管理需要了解局域网上的全部业务，管理员可根据需要了解配置信息，查看服务器负载是否过重，是否使用了网桥、路由器将网络分段等。通过对这些信息的收集、统计，可进行故障诊断和对重大故障发出报警警告。

网络服务器对网络性能影响最大。服务器主要由三部分组成：CPU、内存和软件，磁盘子系统，网络输入输出子系统。

CPU 性能的提高除了使用功能强大的高速芯片外，还要有高速缓存（Cache）供给 CPU 处理所需的指令。使用对称多处理（SMP）技术不仅提高了处理能力，还具有容错功能。使用单驱动器的磁盘驱动子系统，可使用高速度处理器和增加磁盘容量来提高性能。若使用多处理器，可用多通道总线的智能驱动矩阵控制器来提高性能，也可以使用专用的文件服务器、打印服务器和数据库服务器来提高网络性能。网络的输入输出主要通过网卡，选用性能高的

网络接口卡也能提高服务器的性能。

1.1.2 故障管理

故障管理（Fault Management)是网络管理最基本的功能之一。当网络出现故障时，网络管理员必须迅速查找到故障并及时排除故障。但是通常不大可能迅速隔离某个故障，因为网络故障的产生原因往往相当复杂，特别是当故障是由多个网络共同引起时就更为复杂。在此情况下，一般先将网络修复，然后再分析网络故障的原因。分析故障原因对于防止类似故障的再发生相当重要。故障管理应包括以下五项典型功能：

① 维护并检查错误日志；
② 接受错误检测报告并作出响应；
③ 跟踪、辨认错误；
④ 执行诊断测试；
⑤ 纠正错误。

对网络故障的检测依据是对网络组成部件的监测。轻微故障通常被记录在错误日志中，并不做特别处理；而严重一些的故障则需要通知网络管理员，即所谓的报警。一般网络管理员应根据有关信息对故障进行处理，排除故障。当故障比较复杂时，网络管理员应能执行一些诊断测试程序来辨别故障原因。

故障管理主要对网络设备和服务器故障进行检测、诊断、故障排除、维修及报告。故障主要发生在三个方面：硬件、软件和电缆系统（包括网卡）。

网络硬件的故障可用诊断程序诊断，也可使用故障诊断设备，有经验的人员还可人工查错。无论用诊断程序还是诊断设备，主要检查网络参数，如帧头长度、帧顺序、CRC 错、冲突发生的频度等。

查找软件故障较困难，最好使用规程分析仪。这是一种高档设备，它作为一个特殊工作站连接在网上，收集、显示和分析 LAN 上传输的数据，并将这些数据保存起来。该仪器解决了大量的网络查错问题，但必须有高水平的专家才能评价其结果。

网卡、电缆和其他硬件对网络的操作、速度和网络吞吐量都有不同影响。如网卡工作不正常，或电缆接口、终端匹配器等接触不良，会出现大量的重发和丢包现象。网卡兼容性差，不同厂家的网卡不能在同一个网上正常工作时，可以使用网卡内带的诊断程序诊断。可以使用万用表、示波器和时域反射仪等测量电缆故障。

1.1.3 配置管理

配置管理（Configuration management)是维护网络正常有序运行的重要手段。它初始化网络、并配置网络，以使其提供网络服务。目的是为了实现某个特定功能或使网络性能达到最优。内容包括：

① 设置开放系统中有关路由操作的参数；
② 对被管对象或被管对象组名字的管理；
③ 初始化或关闭被管对象；
④ 根据要求收集系统当前状态的有关信息；

⑤ 获取系统重要变化的信息；

⑥ 更改系统的配置。

配置管理的任务是识别网上设备和用户，收集必要的数据，为通信系统的初始化提供数据，而且要提供连续可靠的连接。配置管理主要关心的是维护网上软件、硬件和电路精确清单，修改清单的能力以及响应改变业务需求的可靠方法。

配置管理与硬件、软件和电路维护清单相连，这些清单随配置改变而做相应的修改，配置改变也会影响网络性能。

网络设备的配置清单中不仅包括网上接入了什么设备，还包括这些设备选用了哪些参数。网络操作系统具有增加、删除和修改系统参数配置的能力。

文件管理的任务是帮助用户查询文件而不必使用文件的全名或具体的目录位置。有专门的文件管理工具使用户可根据文件主题、项目名称或生成日期调用文件，或根据任何信息段寻找保存在网上任何地方的文件。

一些用户工具能使管理人员访问远程工作站或从键盘或屏幕上采集数据，从而能帮助用户分析问题发生在哪里，有的系统还可以对接受帮助的用户进行统计。

1.1.4 计费管理

计费管理（accounting management)负责记录网络资源的使用，目的是控制和监测网络操作的费用和代价，它对一些公共商业网络尤为重要。它可以估算出用户使用网络资源可能需要的费用和代价，以及已经使用的资源。网络管理员还可以通过向用户收取费用来控制用户过多使用和占有网络资源。这也从另一方面提高了网络的效率。另外，当用户需要使用多个网络中的资源时，计费管理应能计算总计费用。

计费管理在局域网上不那么重要。因为局域网主要在一个单位内部使用，计费也不那么严格，所以计费系统比较简单，多数都包括在网络操作系统内。如 Novell 公司的 NetWare 中提供了一个计费模块，它包括费率计算、收费定价、确定收费内容等。一般包括对数据块读/写，连接服务时间、占有磁盘空间以及服务请求等方面收费。

计费管理是对网络资源和通信资源的使用进行计费，包括对用户使用的各种资源进行跟踪，统计用户对资源的使用数量和占用时间，计算费用及对已收费用户进行确认。该系统能对用户的访问活动建立详细记录，这既是对用户收费的依据，又是对网络极有用的信息，因为发生问题后可根据记录查找原因。

计费系统还具有安全管理功能。它能告诉网络管理员谁在网上的什么地方、什么时候做了什么工作，哪个用户在什么时间用了哪些资源等。管理员可以用它检查某个用户对某个服务器、目录或文件的操作。该系统还能提供错误报告清单，利于防止故障发生。

1.1.5 安全管理

安全管理（security management)是网络管理中非常重要的内容。安全性一直是网络的重要环节之一，而用户对网络安全的要求又相当高。网络中主要有以下几大安全问题：网络数据的私有性（保护网络数据不被侵入者非法获取）、授权（authentication，防止侵入者在网络上发送错误信息）、访问控制（控制对网络资源的访问）。相应地，网络安全管理应包括对

授权机制、访问控制、加密和加密关键字的管理，另外还要维护和检查安全日志。内容包括：

① 创建、删除、控制安全服务和机制；

② 与安全相关信息的分布；

③ 与安全相关事件的报告。

对任何一个网络而言，信息安全都是极为重要的。安全管理的任务主要是保护网上处理的信息不被泄露和修改，限制没有授权的用户或者具有破坏作用的用户对网络的访问，要能控制网上的合法用户只能访问自己访问权限范围内的资源，以保护网上信息不会在传输时泄露和被修改。

当前主要的网络操作系统是通过对文件服务器的公共接入使用集中式的存储。对数据的保护应从如下几个方面入手：

① 局域网上的关键设备是文件服务器、数据库服务器、工作站和电缆系统，还有打印服务器、通信服务器、网桥和路由器等，而承受安全危险最大的是工作站和电缆。因为本地工作站上的重要数据容易被盗，授权用户可以通过工作站获取服务器上的有用信息。

使用服务器不正确也可能引起信息丢失。Novell 公司与服务器提供商 NetFRAME 公司联手，从软、硬两个方面着手提供安全可靠的网络服务器，它们利用磁盘镜像和多硬盘同步等技术保证存储在硬盘上的数据的安全。此外经常进行磁盘备份可以防止信息丢失和破坏。远程工作站通过电话接入，其安全问题也应注意。

电缆系统也是信息泄露的途径。铜线容易被分接，还会造成电磁辐射，通过电磁感应的方法便可以获取网上信息，光纤在这方面安全得多。

② 网络操作系统对逻辑访问的管理包括两部分：一是控制用户对网络的访问；二是保护文件不被不该访问的用户访问，不被随意修改和删除。不同的操作系统有各自的逻辑访问控制方式，但不外乎使用用户名、口令、限制入网时间和地点等。

③ 访问控制的目的是控制用户对网上文件的访问。系统为用户授权，根据需要规定他可以访问哪个磁盘卷，哪些目录和文件，还对文件和目录设置了属性，即层层设防。用户欲对某目录下的文件进行某种操作，必须有相应的权限。

访问控制还能对非法入网的用户进行跟踪。在 NetWare 系统中，当用户欲入网而连续四次输入了不正确的口令时，系统即认为是非法用户，马上封锁该用户的入网请求并冻结其帐户。

④ 病毒是威胁信息安全的大敌，应受到高度重视。市场上虽有种类繁多的防病毒工具，但很难抵挡住每天 3～5 个新繁殖出来的病毒的进攻。因而严格禁止使用拷贝软件、加强对病毒的监测和及时清除病毒，也是保证网上信息安全的重要措施。许多厂家都提供防病毒的软、硬件。

网络管理业务功能虽然分为五个方面，但这五个方面是互相影响的，主要表现在：

(1) 性能与配置有关。如 CPU 处理速度不够快，这可能是由于缓冲区不够大造成的，可以通过配置管理去增大缓冲区；通信缓冲区不够，也会使信息传递的速度减慢。

(2) 性能管理与故障管理有关。当网上信息传输差错增多，出现过多的重发或信息包丢失时，最初表现为性能降低，当低到一定程度时，即成为故障。Novell 的管理软件中可以对某些参数设置门限值，实现故障自动报告。

(3) 故障与安全有关。无论网上硬件或软件发生故障，都可能影响信息安全。

(4) 安全与计费有关。因为计费管理要对用户在网上的活动进行跟踪和记录，万一出现

安全问题，即可查阅这些记录，从中找到问题所在。

1.2 网络管理协议简述

目前较为流行的网络管理协议有 SNMP 和 CMIP。

1.2.1 SNMP 网络管理协议简述

SNMP(Simple Network Management Protocol)是一个简单网络管理协议，是使用户能够通过轮询、设置一些关键字和监视某些网络事件来达到网络管理目的的一种网络协议。应该说，SNMP 是一个应用级的协议，而且是 TCP/IP 协议的一部分，工作于 UDP 上。在 SNMP 应用实体间通信时不需要事先建立连接，这样降低了系统开销，但不能保证报文的正确到达。

1. *初期的SNMP*

SNMP 有两个版本称之为 SNMP v1 和 SNMP v2。SNMP v1 是 SNMP 的早期版本，它的结构为 SNMP 管理者（SNMP Manager)和 SNMP 代理（SNMP Agents)。每一个支持 SNMP 的网络设备中包含一个代理，它随时记录网络设备的各种情况，网络管理程序再通过 SNMP 通信协议查询或修改代理所做的记录信息。

SNMP 的工作原理非常简单，它在 SNMP 的管理者（一般是运行了网络管理系统的计算机）和 SNMP 的代理（一般是包含了 SNMP 管理信息的计算机、网络设备）之间实时传递网络信息。这些网络信息在简单网络管理协议中被称为协议数据单元（PDU,Protocol Data Unit)。在 SNMP 中定义了 5 类协议数据单元。从高层角度，可以将协议数据单元看做包含了若干变量的对象，每个变量有它自己的变量名和变量值。当管理员要查看某个网络设备是否连接在网上时，就发出一个包含该请求的协议数据单元。如果相应设备的确连在网上，用户会接受到一个协议数据单元，该数据包中有“是的，我在网上”的信息；当设备关闭时，就会出现一个自陷（Trap)信息，使管理者知道出现了这样一个网络事件。在此，管理员所在的计算机就是 SNMP 管理者，而网上的网络设备就是 SNMP 代理。

在 SNMP 的网络通信模型中，SNMP 管理者负责向 SNMP 代理进行轮询。简单网络管理协议中定义了四种为轮询提供服务的报文操作原语：

① GetRequest SNMP 管理者发送给 SNMP 代理的“查询变量”请求，要求网络代理响应变量的具体值。例如，当你发出一条命令，要求获得某个路由器的某端口状态时，使用该原语。

② GetNextRequest SNMP 管理者发送给 SNMP 代理的“查询下一个变量”请求，要求网络代理响应下一个变量的具体数值。这个原语应用于当网络管理员遍历一个网络设备的 MIB 库的某一对象的一系列参数时。

③ GetResponse SNMP 代理对 SNMP 管理者的响应，并回送相应变量的具体数值。例如，当 SNMP 管理者询问 SNMP 代理的软件版本时，代理返回“V1.0”信息。

④ SetRequest SNMP 管理者发送给 SNMP 代理的“设置变量”请求，要求网络代理

设置本地管理信息库相应变量的值。例如，当使用网络管理系统将远程某一台路由器的某个端口状态从“Enable”设置为“Disable”时，就使用这一条原语。

此外，当 SNMP 代理的当前状态符合某种预先设定的状态时，它会主动向 SNMP 管理者发一种协议数据单元，这种报文称之为 Trap 。这些预先设定的状态包括连接或断开以及各种报警状态。Trap 报文在性能网络管理中尤为重要。当网络中出现网络设备故障时，管理者可根据 Trap 类型进行诊断和处理。

SNMP 对网络设备的管理采用轮询管理策略(Polling-based Management),而非事件管理策略（Event-based Management），SNMP 通信协议在数据查询和网络设备检测时占有较多的网络带宽，因此这种管理方式不适合大型广域网（WAN）。

在简单网络管理协议中，每一个网络代理者包含一个管理信息库。这个信息库是一个树型结构的数据库，是可被管理的对象组的集合，如图 1-1 所示。每一个对象又包含了若干个信息变量，每个信息变量包含以下信息：

① 变量名；

② 变量的数据类型；

③ 变量的属性；

④ 变量的值。

SNMP 的代理通过 MIB 来保存有关代理的各种配置信息和状态信息，并且在代理上运行一个称之为“守候”的进程。这个进程一方面等待来自 SNMP 网络管理者的请求报文，并作出相应反应，读取或修改 MIB 中的变量值；另一方面，守候进程检查本地的状态，发出 Trap 报文。

MIB 这个树型数据库的根结点是 Root，在 Root 下有若干个子结点，以后每一级都是一个一对多的映射，而且任何一个结点的子结点都按某个标准的序号排列。当管理者要访问某一指定的变量时，由一个序列标识号（Sequential ID）来确定这个变量。例如，在图 1-1 中，如果我们依次要访问 Root、ISO、Organizations、DoD、Internet、Management、MIB1&2、RMON、Hosts 时，应该使用 1.3.6.1.2.1.16.4 作为到达此结点的序列标识号。除此之外，MIB 厂商还可以在各标准子树下安装新的特殊的 MIB 结点，这种结点只允许特殊的管理者访问。这样大大提高了 MIB 的灵活性，当然同时也带来一定的兼容性问题。

在 SNMP 刚刚推出的时候，使用的是 MIB 1 管理信息库。它把对象的数量限制在 114 个之内，并把这些对象分成 8 个组，System、Interface、AT、IP、ICMP、TCP、UDP 和 EGP。MIB 2 扩展了 MIB 1 ,增加了 CMOT 和 SMNP 两个组，并把对象数增加到 185 个，使得 MIB 库的作用能力大大增强。

SNMP 是一个最流行的网络管理协议，但它也有许多不足之处，主要表现在：

① 由于 SNMP 是基于 TCP/IP 的一种网络管理协议，所以它不能超越 TCP/IP 的范畴。例如，它无法完成高层次的配置工作。另外，SNMP 仍然是一种应急的做法。它无法像 DEC 的 EMA 和 IBM 的 NMA 一样，提供一种整个网络的管理策略，而只是非常现实地把现有产品（如一些网桥和路由器）连接，并完成相应的管理工作。前面我们曾提到 SNMP 不适合在广域网上工作，也是这种限制的一种证明。

② 像所有 TCP/IP 协议族中的协议一样，SNMP 对安全问题考虑甚少。在安全性方面问题比较突出的是 SetRequest 协议数据原语。如果错误地使用这条原语，可能导致网络崩溃；如果各种网络管理系统使用不同格式的 SetRequest 原语，又会影响协议的一致性。

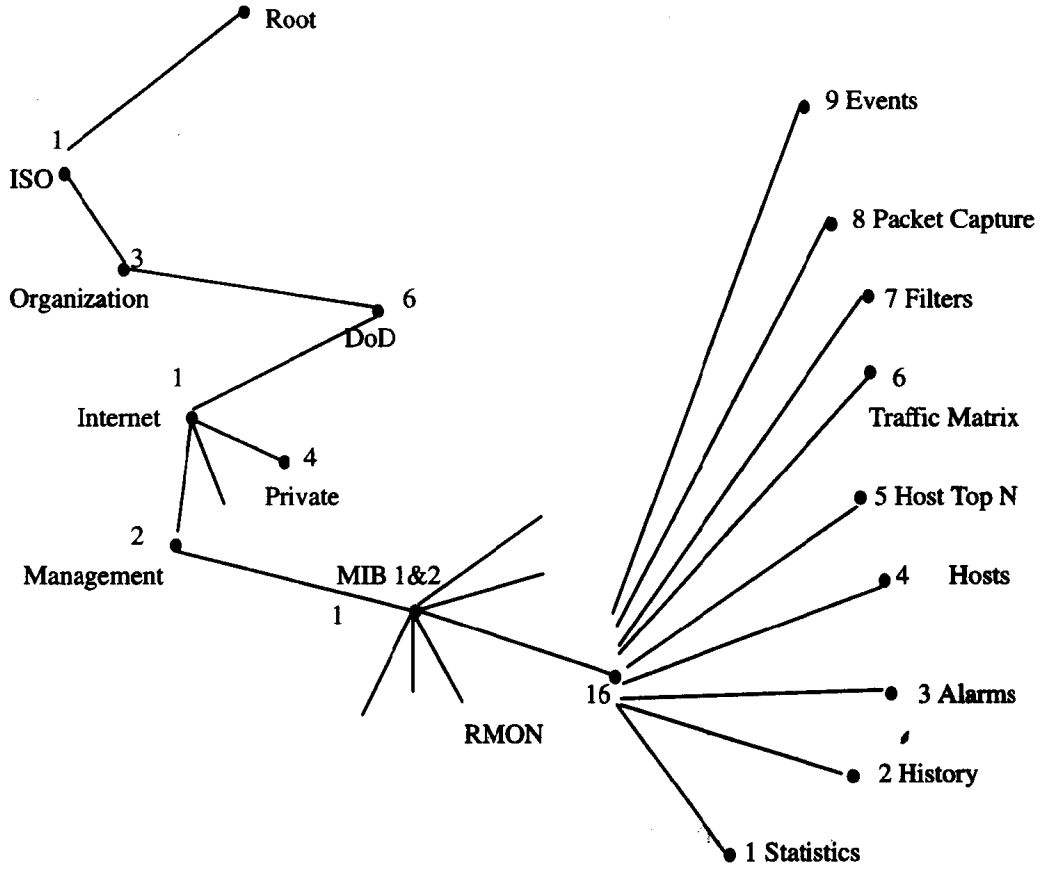

图 1-1 MIB 数据库的树型结构

③ 当 SNMP 刚刚面世时，几乎没有对管理程序到管理程序的通信提出任何需求。但从那时起，在一个网络中就已出现多个管理程序的情况。随着向客户/服务器计算和分布式网络管理的转移，一些组织在网络上采用多种管理程序。但 SNMP 没有提供允许这些管理程序共享信息和互相通信的机制。因此，带多个管理程序的 SNMP 用户可能需要考虑把网络分割为较小的部分，并且每个部分使用专用的管理站。这样大大降低了管理灵活性，并增加了网络负载。

2. 改进后的SNMP

由于早期 SNMP(SNMP v1)存在着不足之处，1993 年 IAB 对 SNMP 进行了改进，改进后的 SNMPv2 与早期的 SNMP 的不同之处郭继军等在 1996 年 4 月 29 日《计算机世界》的《网络管理协议 SNMP 和 CMIP 及其比较》一文中，叙述为：

① SMI (Structure of Management Information)描述的是 MIB 库的结构与定义方法。SNMP v2 支持几种 SNMP v1 所不支持的新的数据类，如 Integer32、Counter32、UInteger32 等。这些新增加的数据类型丰富了 MIB 库对网络设备的描述能力。在 SNMP v2 中还引入了信息模块（information modual）的概念，使 MIB 库中除了原先对象（object）、变量（variable）两个层次外，又多了一个层次。

② PDU (Protocol Data Unit) 在 SNMP v2 中定义了两种新的数据原语——InformRequest 原语和 GetBulkRequest 原语。其中，InformRequest 原语允许一个管理者发送一个 Trap 消息