

本书可作为本科、专科、高职高专院校计算机职业技能教育课程的教学用书

MyDEC[®] 专业教育机构

信息产业IT职业技术培训指定教材

企业网络管理

HE 实用教程

Enterprise Network and
Service Management

总策划 MyDEC专业教育机构
审 定 信息产业部电子行业职业技能鉴定指导中心
主 编 张景安
副主编 郭振民 张越新



中国青年出版社
中国青年电子出版社

<http://www.21books.com> <http://www.cgchina.com>

信息产业 IT 职业技术培训指定教材

企业网络管理实用教程

张景安 主 编

郭振民 张越新 副主编



中国青年出版社
中国青年电子出版社

<http://www.21books.com> <http://www.cgchina.com>

本书由中国青年出版社独家出版。未经出版者书面许可,任何单位和个人不得以任何形式复制或传播本书的部分或全部内容。

图书在版编目(CIP)数据

企业网络管理实用教程 / 张景安, 郭振民, 张越新编. —北京: 中国青年出版社, 2006

ISBN 7-5006-7027-3

I.企... II.①张...②郭...③张... III.企业—计算机网络—技术管理—教材 IV.TP393.18

中国版本图书馆 CIP 数据核字 (2006) 第 091614 号

书 名: 企业网络管理实用教程

主 编: 张景安

副 主 编: 郭振民 张越新

出版发行: 中国青年出版社

地址: 北京市东四十二条 21 号 邮政编码: 100708

电话: (010) 84015588 传真: (010) 64053266

印 刷: 中国农业出版社印刷厂

开 本: 787×1092 1/16 **印 张:** 26

版 次: 2006 年 9 月北京第 1 版

印 次: 2006 年 9 月第 1 次印刷

书 号: ISBN 7-5006-7027-3/TP·593

定 价: 38.00 元

企业网络管理实用教程编委会名单

主	任：	王耀光			
副	主	任：	李雅玲	蒋红兵	周 明
主	编：	张景安			
副	主	编：	郭振民	张越新	
委	员：	曹 丽	祝 丹	王 乾	陈朔鹰
		丁喜纲	丛迎九	邓文新	迟呈英
		李良俊	王 虹	张欣欣	郭 明
		杨振宇	刘墨德	谭 军	时秀波
		张润梅	折如义	王培麟	曹国红
		谷秀荣	刘 镇		

前 言

计算机网络的出现,使整个世界实现了信息化,使人们的生活、工作产生了巨大变化,工作效率更是提高了许多。随着计算机网络在各个领域的应用越来越广泛,网络管理工作也变得越来越重要。

网络管理工作要求从业者不仅要拥有很强的动手能力、丰富的实践经验,以迅速排除故障、恢复计算机和网络的正常运行,又要有扎实的理论基础、敏锐的洞察力、缜密的逻辑判断和分析能力,以解决出现的千奇百怪的未知难题。本书全面而系统地讲解了在网络管理工作中遇到的各种技术问题,并给出了细致而可行的解决方案。

全书系统详细地介绍了网络的系统规划与设计、网络布线与施工、设备选购与配置、服务搭建与管理以及网络排除等内容,涉及从规划、搭建、管理与维护的全部主要技术,是一整套紧贴实际应用的完全解决方案。

本书内容丰富,讲解深入浅出、图文并茂、范例实用性强,书中所有操作和组网实例均是作者从实际组网工作中得来,并最大限度地融会了新产品、新技术,更加符合网络管理者的实际需求。

本书为信息产业 IT 职业技术培训指定教材,重点面向所有参加信息产业 IT 职业技术培训的人员,同时也适合大中专院校相关专业师生以及对网络管理应用技能有不同程度培训需求的人员阅读学习。

参加本书编写的有:张昱、赵枫朝、赵伟、李大伟、张杰、张忠狮、马文喜、成保栋、朱东锋、王为、赵季卫、赵松岩、李平生、郑海员、刘航、王优胜、薛艳菊、李南、金碧云等。由于时间仓促加之水平有限,书中难免会有差错及不足之处,敬请广大专家和读者给予批评指正。

最后,祝广大读者学有所成、学习愉快!

编 者

2006年7月

目 录

第1章 网络管理基础

1.1 企业网络管理的概念	1
1.2 企业网络管理资源的表示	2
1.3 企业网络管理系统的组成	2
1.4 网络管理的类型及优缺点	3
1.5 网络管理的功能	3
1.6 网络管理技术	5
1.6.1 基于 Web 的网络管理技术	5
1.6.2 远程网络监控 (RMON) 技术	5
1.7 网络管理协议	6
1.7.1 SNMP 协议	6
1.7.2 CMIS/CMIP 协议	8
1.7.3 RMON 协议	8
1.7.4 AgentX 协议	9
1.8 网络管理软件的发展	9
1.9 常见的几种网络管理软件	10
1.9.1 HP 公司的 OpenView	10
1.9.2 IBM 公司的 NetView	11
1.9.3 SUN 公司的 SUN Net Manager	11
1.9.4 Cisco 公司的 Cisco Works	11
1.9.5 3Com 公司的 Transcend	12
1.9.6 美萍软件	12
1.9.7 远程控制软件 Remotely-Anywhere	13
1.9.8 NetSuper 和 NetRay 软件	15
1.9.9 "网路岗三代"软件	15
1.10 小结	16
1.11 习题	16

第2章 网络布线的工程设计技术

2.1 网络布线综述	17
2.2 网络布线的工程设计	19
2.2.1 网络布线工程的范围	19
2.2.2 网络工程的分析与设计	20
2.2.3 网络工程工作清单	20
2.3 网络布线系统的组成	22
2.4 工作区子系统的设计	23
2.4.1 工作区子系统设计概述	23
2.4.2 工作区子系统设计要点	24
2.4.3 信息插座连接技术要求	24
2.5 水平布线子系统的设计	25
2.5.1 水平布线子系统设计概述	25
2.5.2 水平布线子系统布线方案	28
2.6 管理间子系统的设计	30

2.6.1 管理间子系统设计概述	30
2.6.2 管理间子系统设计方案	30
2.6.3 管理间管理子系统的设计步骤	31
2.7 干线布线子系统的设计	32
2.7.1 干线布线子系统设计概述	32
2.7.2 干线布线子系统的拓扑结构	32
2.7.3 干线布线子系统的介质类型	33
2.7.4 布线子系统的设计方法	33
2.8 设备间子系统的设计	34
2.8.1 设备间子系统设计概述	34
2.8.2 设备间子系统的环境指标	34
2.9 建筑群子系统的设计	37
2.9.1 建筑群子系统设计概述	37
2.9.2 建筑群子系统的设计方法	37
2.9.3 建筑群子系统的布线方法	39
2.10 小结	40
2.11 习题	40

第3章 网络设备的选择与连接

3.1 网卡	41
3.1.1 网卡的类型	41
3.1.2 网卡的工作原理	42
3.1.3 网卡的选用	42
3.2 集线器	43
3.2.1 集线器的作用与工作原理	43
3.2.2 集线器的种类与选择	44
3.3 交换机	45
3.3.1 交换机的作用与工作原理	45
3.3.2 交换机的三种交换技术	45
3.3.3 交换机的种类及选择	46
3.4 路由器	46
3.4.1 路由器的工作原理与作用	46
3.4.2 路由器的选择	47
3.5 网关	47
3.6 其他设备	48
3.6.1 调制解调器 (Modem)	48
3.6.2 综合业务数字网 (ISDN)	48
3.6.3 非对称数字用户环路 (ADSL)	48
3.6.4 电缆调制解调器 (Cable Modem)	49
3.7 小结	49
3.8 习题	49

第4章 交换机的配置与管理

- 4.1 交换机概述50
 - 4.1.1 交换机基础50
 - 4.1.2 交换机与集线器的区别51
 - 4.1.3 交换机的工作原理52
- 4.2 交换机的分类54
 - 4.2.1 根据网络覆盖范围划分54
 - 4.2.2 根据传输介质和传输速度划分54
 - 4.2.3 根据交换机的结构划分56
 - 4.2.4 根据交换机工作的协议层划分57
- 4.3 交换机的配置58
 - 4.3.1 本地配置方式58
 - 4.3.2 远程配置方式61
- 4.4 交换机 VLAN 的配置62
 - 4.4.1 VLAN 基础62
 - 4.4.2 VLAN 的划分方法63
 - 4.4.3 VLAN 的优越性64
 - 4.4.4 VLAN 网络的配置实例65
- 4.5 小结68
- 4.6 习题68

第5章 路由器的配置与管理

- 5.1 路由器概述69
 - 5.1.1 路由器基础69
 - 5.1.2 路由器的主要功能70
 - 5.1.3 路由器的工作原理70
- 5.2 路由器的配置72
 - 5.2.1 路由器的启动过程72
 - 5.2.2 路由器的几种配置方式72
 - 5.2.3 路由器配置的用户模式73
 - 5.2.4 路由器的常用命令74
 - 5.2.5 简单配置实例76
- 5.3 路由器的高级配置78
 - 5.3.1 路由器的命令配置方式78
 - 5.3.2 对话方式下路由器的基本配置81
 - 5.3.3 局域网路由协议配置83
 - 5.3.4 路由器广域网协议配置86
- 5.4 小结88
- 5.5 习题88

第6章 IP 地址的管理

- 6.1 什么是 IP 地址89
- 6.2 IP 地址的形式与分类89
 - 6.2.1 IP 地址的表示89
 - 6.2.2 IP 协议中的网络90
 - 6.2.3 IP 地址分类90
- 6.3 IP 地址分配方法92

- 6.3.1 每个网络接口有一个地址92
- 6.3.2 多穴设备92
- 6.3.3 多网化——每个网络接口有多个地址92
- 6.3.4 示例93
- 6.4 子网划分93
- 6.5 子网掩码94
 - 6.5.1 掩码概述94
 - 6.5.2 掩码的组成95
 - 6.5.3 计算子网掩码95
- 6.6 IP 地址规划96
 - 6.6.1 三种规划方法97
 - 6.6.2 三种规划方法的选择98
- 6.7 IP 网络的安全管理100
- 6.8 小结100
- 6.9 习题101

第7章 网络系统服务

- 7.1 服务器概述102
 - 7.1.1 服务器基础102
 - 7.1.2 服务器的功能分类103
 - 7.1.3 服务器的主要特点103
- 7.2 域名服务器104
 - 7.2.1 Internet 命名机制104
 - 7.2.2 Internet 的域名结构105
 - 7.2.3 域名服务器工作原理105
 - 7.2.4 Windows 2000 中的 DNS 服务器106
- 7.3 DHCP 服务器112
 - 7.3.1 DHCP 工作原理112
 - 7.3.2 安装和配置 DHCP 服务器113
 - 7.3.3 管理 DHCP 服务器116
 - 7.3.4 设置 DHCP 客户机117
- 7.4 WINS 服务器118
 - 7.4.1 Windows Internet 命名服务原理118
 - 7.4.2 WINS 的运行方式119
 - 7.4.3 WINS 名称服务的优势120
 - 7.4.4 安装 WINS 服务器121
 - 7.4.5 配置 WINS 服务器122
 - 7.4.6 启用客户机的 WINS 功能124
- 7.5 Web 服务器126
 - 7.5.1 Web 服务原理126
 - 7.5.2 建立和配置 Web 服务器128
 - 7.5.3 管理 IIS131
- 7.6 网络文件存储系统131
 - 7.6.1 分布式文件系统131
 - 7.6.2 NTFS 文件系统134
- 7.7 活动目录与用户的管理135

7.7.1 活动目录 (Active Directory)	
概述	135
7.7.2 安装活动目录	136
7.7.3 用户/计算机账户的设置和管理	138
7.7.4 组账户的设置和管理	140
7.8 WINDOWS 群集的管理	141
7.8.1 群集的基本概念	141
7.8.2 群集服务的安装	142
7.8.3 安装群集服务软件	147
7.9 小结	150
7.10 习题	150
第 8 章 Windows 网络的管理与维护	
8.1 Windows IntelliMirror 技术	151
8.2 Windows 平台中组策略编辑器的使用 and 配置	152
8.2.1 组策略编辑器的启动	153
8.2.2 组策略编辑器的使用与配置	155
8.3 Windows 2000/Server 2003 下的常用系统维护工具及其配置	157
8.3.1 任务管理器	157
8.3.2 性能监视器	159
8.3.3 事件查看器	163
8.3.4 网络监视器	166
8.4 常用网络命令工具	168
8.4.1 Ping	168
8.4.2 Ipconfig	172
8.4.3 Netstat	174
8.4.4 nbtstat	177
8.4.5 tracert	179
8.4.6 Route	180
8.4.7 arp	182
8.4.8 net	183
8.5 小结	191
8.6 习题	191
第 9 章 网络硬件常见故障的诊断与排除	
9.1 主机常见故障	192
9.1.1 主机喇叭报警声诊断故障	192
9.1.2 计算机死机故障	193
9.1.3 主板常见故障	196
9.1.4 内存常见故障	197
9.1.5 硬盘常见故障	198
9.1.6 CPU 常见故障	199
9.2 网卡常见故障	200
9.3 集线器常见故障	201
9.4 交换机常见故障	202
9.5 路由器常见故障	203
9.6 服务器常见故障	204
9.7 小结	207
9.8 习题	207
第 10 章 网络软件常见故障的诊断与排除	
10.1 TCP/IP 的配置方法	208
10.2 TCP/IP 常见故障的原因和解决办法	210
10.3 紧急恢复盘的创建	212
10.4 Ghost 和 FinalData 的使用	213
10.4.1 Ghost 的使用	213
10.4.2 FinalData 的使用	215
10.5 系统自动拨号的方法	217
10.6 拨号上网常见故障的原因和解决方法	218
10.7 Internet Explorer 的配置和使用	221
10.7.1 Internet Explorer 的配置	221
10.7.2 Internet Explorer 的使用	225
10.8 垃圾邮件和乱码邮件的处理	226
10.8.1 垃圾邮件的处理	226
10.8.2 乱码邮件的处理	228
10.9 操作系统常见故障的原因和解决方法	229
10.9.1 Windows 常见故障	229
10.9.2 UNIX 常见故障	231
10.10 小结	235
10.11 习题	235
第 11 章 网络安全问题	
11.1 网络安全概述	236
11.1.1 网络安全的背景	236
11.1.2 网络安全的意义	236
11.2 策略和机制	237
11.3 物理安全措施	237
11.4 网络安全技术	238
11.4.1 网络隔离技术	238
11.4.2 访问控制技术	239
11.4.3 加密通道技术	241
11.4.4 入侵检测技术	242
11.5 数据加密技术	250
11.5.1 加密的历史	250
11.5.2 数据加密的基本概念	251
11.5.3 数据加密的标准	254
11.5.4 数据加密的应用	254
11.5.5 PGP 邮件加密软件	255
11.6 认证技术	256
11.7 反病毒技术	257
11.8 备份和灾难恢复技术	258
11.9 IPSec 技术	258

11.9.1	IPSec 简介	258	13.2.3	黑客攻击的工具	352
11.9.2	创建 IPSec 管理单元	260	13.3	常用的防黑客软件	354
11.9.3	配置 IPSec	262	13.3.1	Norton Personal Firewall	354
11.9.4	配置审核策略	264	13.3.2	BlackICE 防火墙	356
11.9.5	IPSec 统计	265	13.3.3	ZoneAlarm	358
11.10	加密文件系统实战	267	13.3.4	天网防火墙	362
11.11	证书实战	271	13.3.5	硬件防火墙	363
11.12	小结	285	13.4	木马及其破解	366
11.13	习题	285	13.4.1	木马概述	366
第 12 章	网络防病毒		13.4.2	木马的破解方式	366
12.1	计算机病毒概述	286	13.4.3	木马终结者	368
12.1.1	计算机病毒的发展史	286	13.5	Windows 2000/2003 Server 安全设置	368
12.1.2	计算机病毒的基本概念	287	13.6	Linux 安全设置	373
12.1.3	计算机病毒的特性	289	13.7	LockDown 2000	377
12.1.4	计算机病毒的分类	291	13.8	IIS 安全双剑客	379
12.1.5	计算机病毒的危害及症状	291	13.8.1	使用 IIS Lock Tool 快速设置 IIS 安全属性	379
12.2	计算机病毒技术	293	13.8.2	使用 URLScan Tool 过滤非法 URL 访问	382
12.2.1	计算机病毒的结构	293	13.9	Windows 2000/2003 Server 的入侵检测	384
12.2.2	计算机病毒的传染机理	295	13.10	小结	387
12.2.3	常见的计算机病毒技术	296	13.11	习题	387
12.3	计算机防毒技术	301	第 14 章	构筑安全的企业网络	
12.3.1	防毒的原则	301	14.1	企业网概述	388
12.3.2	深层病毒防护	301	14.1.1	局域网、部门网络与企业网	388
12.3.3	典型防病毒技术介绍	317	14.1.2	为什么要建立企业网	388
12.3.4	防病毒过程	322	14.1.3	企业网的应用	389
12.3.5	网络病毒的防御方式	324	14.1.4	企业网的基本构成	389
12.4	常见的杀毒软件介绍	325	14.1.5	Internet 与企业网	390
12.4.1	诺顿杀毒软件 2006	325	14.1.6	如何用好企业网	390
12.4.2	卡巴斯基 2006	329	14.2	构筑安全的企业网模型	391
12.4.3	金山毒霸 2005	333	14.3	企业网的安全策略	391
12.4.4	瑞星 2005	335	14.3.1	需求分析	392
12.4.5	在线病毒扫描工具	338	14.3.2	风险分析	396
12.4.6	几款常用杀毒软件的病毒库备份	339	14.3.3	安全计划	397
12.5	手机病毒	340	14.3.4	安全策略的制订	398
12.5.1	起源及其发展	340	14.3.5	对安全策略的评估和复查	399
12.5.2	特点	341	14.4	服务器的安全保护技术	400
12.5.3	原理	342	14.5	网络安全产品的选择	402
12.5.4	防御方法	342	14.6	紧急响应和事故处理	402
12.6	系统恢复	343	14.7	安全意识培训与安全技能教育	407
12.7	小结	347	14.8	企业网络安全综合管理	407
12.8	习题	347	14.9	小结	408
第 13 章	网络防黑客		14.10	习题	408
13.1	黑客概述	348			
13.2	黑客攻击技术	351			
13.2.1	黑客攻击的步骤	351			
13.2.2	应对黑客攻击的策略	352			

第 1 章 网络管理基础

本章重点:

- 企业网络管理资源的表示
- 企业网络管理系统的组成
- 网络管理的类型及优缺点
- 网络管理的功能
- 网络管理技术与协议
- 常见的网络管理软件

随着网络技术的不断发展和网络应用范围的不断扩大, 计算机网络在人们的日常生活中已经变得越来越普遍。特别是 20 世纪 90 年代以来, 随着 Internet 在世界范围的普及, 计算机网络逐渐成为人们获取信息、发布信息的重要途径。与此同时, 基于计算机网络的应用也越来越多, 人们生活中的许多重要环节都可以利用网络方便、快捷地实现。例如, 网络商店的出现, 使得人们在家里就可以选购到自己满意的商品; 金融网络的发展, 使得货币完全电子化, 人们再也不用在钱包中塞满纸币; 还有邮电网络、各种专业大型网络等。这些大到国家经济命脉, 小到个人日常生活的活动大多依赖于计算机网络, 因此网络运行的稳定性、可靠性就显得至关重要, 于是网络管理就应运而生。本章将介绍一些网络管理的基础知识及几种常见的网络管理软件。

1.1 企业网络管理的概念

对于一个企业网络来说, 首先应该把它建立起来, 并且实现网络设计的功能; 其次, 通过网络管理系统保证建立起来的网络持续、正常、稳定、安全和高效地运行; 再次, 当网络出现故障时, 网络管理系统能够进行及时地报告和处理, 以保证网络的正常运行。

按照国际标准化组织 (ISO) 的定义, 企业网络管理是指规划、监督、控制网络资源的使用和网络的各种活动, 以使网络的性能达到最优。企业网络管理的目的在于提供对计算机网络进行规划、设计、操作运行、管理、监视、分析、控制、评估和扩展的手段, 从而合理地组织和利用系统资源, 提供安全、可靠、有效和友好的服务。网络管理领域是随着通信和计算机技术的发展而发展的, 网络管理的技术也从最初的面向网络设备的管理发展到面向端到端的全面网络管理。

一般来说, 企业网络管理包含以下内容:

(1) 企业网络资源的表示。网络资源就是指网络中的硬件、软件及所提供的服务等。网络管理系统必须将它们表示出来, 才能对其进行管理。

(2) 企业网络管理信息的表示。对网络的管理主要是通过传递网络管理信息来实现的。

(3) 企业网络管理的功能。

(4) 软件资源管理和软件分发。该功能是指优化管理信息的收集, 此外, 软件资源管理还对企业所拥有的软件授权数量及安装地点进行管理。软件分发则是通过网络把新软件分发到各个站点, 并完成安装和配置工作。

(5) 应用管理。应用管理用于测量和监督特定的应用软件及其对网络传输流量的影响。网络管理员通过应用管理可以跟踪网络用户和运行的应用软件, 改善网络响应时间。

1.2 企业网络管理资源的表示

网络环境下，资源的表示是企业网络管理的一个关键问题。目前一般采用“被管对象 (Managed Object)”来表示网络中的资源。ISO 认为，被管对象是从 OSI 角度所看的 OSI 环境下的资源，这些资源可以通过使用 OSI 管理协议而被管理。网络中的资源一般都可用被管对象来描述，但通常要以多个被管对象的方式来描述。如网络中的一个路由器就可用一些被管对象来描述，说明它的制造厂商、路由表的结构等。对网络中的软件、服务及网络中的一些事件等都可用被管对象来描述。

被管对象的一个概念上的集合被称作 MIB (Management Information Base)，即管理信息库。所有相关的网络被管对象信息都放在其中。不过应当注意的是，MIB 仅是一个概念上的数据库，实际网络中并不存在这样的库。目前网络管理系统的实现主要依靠被管对象和 MIB，所以它们是网络管理中非常重要的概念。

1.3 企业网络管理系统的组成

企业网络管理的需求决定企业网络管理系统的组成和规模，任何企业网络管理系统一般都由 4 个基本部分组成，即网络管理软件、网络设备的管理代理、管理信息库 (MIB) 和代理设备，如图 1-1 所示。

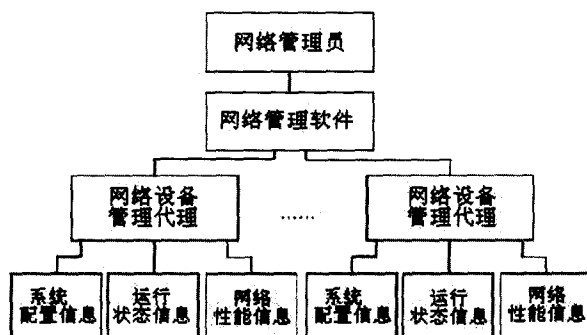


图 1-1 企业网络管理系统的组成

1. 网络管理软件

网络管理软件简称“网管软件”，它是协助网络管理员对整个网络或者网络中的设备进行日常管理的软件。

网络管理软件要求网络设备的管理代理定期收集用于管理的设备信息，并定期查询管理代理收集到的设备运转状态、配置及性能等方面的信息。这些信息将用于确定网络设备和网络整体运行状态是否正常。

目前大多数网管软件是在 Unix 或者 Windows 平台上实现的。用户在选择网络管理软件时一般应从以下几个方面考虑：是否与自身的管理规模和网络模式相一致；是否具有支持多协议、开放式操作系统和第三方管理软件的能力；是否具有良好用户界面；是否具有智能化的监视能力；是否具有基于用户策略的控制能力；是否具有较高的性价比。

2. 网络设备的管理代理

网络设备的管理代理简称“管理代理 (Agent)”，它是一种特殊的软件或固件，包含了一个特定设备及该设备所处环境的信息。

当一个管理代理被安装到一个设备上时,这个设备就被列为“被管理的”。管理代理可以获得所驻留设备的运转状态、设备特性和系统配置等相关信息。它就像是每个被管理设备的经纪人,完成管理软件布置的信息采集任务。管理代理行使网络管理系统与管理代理所驻留设备的中介职能,通过管理信息数据库(MIB)中的内容来管理该设备。管理信息数据库中所包含的数据,随着被安装设备的不同而不同。

3. 管理信息库(MIB)

MIB是管理信息库(Management Information Base)的缩写,它是由网络管理协议访问的管理对象数据库,包括可以通过网络设备的管理代理进行设置的变量。网管软件正是通过控制每个对象的MIB来实现对该网络设备的配置、控制和监视的。

4. 代理设备

代理设备是标准的网络协议软件和不标准的网络协议软件之间的一座桥梁,它在网络管理系统中是可选的。

1.4 网络管理的类型及优缺点

网络管理的类型主要有集中式网络管理(Centralized Network Management)、分级式网络管理(Hierarchical Network Management)和分布式网络管理(Distributed Network Management)。

1. 集中式网络管理

集中式网络管理可以统一管理全部网络,全网所有需要管理的数据均存储在一个集中的数据库中。集中式网络管理具有易于管理、维护和扩容的优点。但是它也存在缺点:频繁地进行数据交互使得网络管理系统链路承载的业务量过大,有时甚至会超出负荷能力,一旦出现故障,将导致全网瘫痪。

2. 分级式网络管理

分级式网络管理由多个网络管理系统构成,其中有一个核心网络管理系统用于管理其他所有非核心网络管理系统所分别管理的领域。分级式管理的优点在于分散了网络和资源的负荷,降低了核心网络管理系统需收集传送的业务量,从而减轻了网络管理系统链路的负担,使得可靠性高于集中式管理。但是它却有处理过程较为复杂的缺点,另外,系统设备价格也相应较高。

3. 分布式网络管理

分布式网络管理由多个网络管理系统构成,各个网络管理系统分别管理各自的领域。分布式管理的优点在于完全分散了网络和资源的负荷,具有很高的可靠性。缺点是系统设备更复杂一些。这是一种最有前途并且正在迅速发展的网络管理技术。

如上所述,这3类网络管理模式各有其优缺点,并各自的应用范围:集中式网络管理适用于规模较小的网络系统;分级式网络管理适用于单一业务和网络拓扑结构简单的网络系统;分布式网络管理适用于业务信息量大而且能灵活扩容、容易升级和能够异构处理的网络系统。

1.5 网络管理的功能

网络管理是控制一个复杂的网络使得它具有最高的有效性和可靠性的过程,网络管理系统则是网络管理者用来管理网络的有效工具。国际标准化组织(ISO)将网络管理的需求划分成5大类,通常将其说成是网络管理的5个功能。这5个功能分别是:故障管理FM(Fault Management)、配置管理CM(Configuration Management)、计费管理AM(Accounting Management)、性能管理PM(Performance

Management) 和安全管理 SM (Security Management)。

1. 故障管理 (FM)

故障管理的功能是检测、定位和排除网络硬件和软件中的故障。当出现故障时, 该功能确认故障的发生, 记录故障现象, 找出故障位置并尽可能排除这些故障。它包括 3 个步骤: 隔离问题、找出故障的原因和修复故障 (如有可能)。

显然, 确定一个网络设备是否处于正常的运行状态, 必须知道每个设备的“故障特性”。每个设备都有一个预先定义好的故障门限, 与配置管理结合在一起, 这些门限应该是可以设置的。

为了确定故障的存在, 需要收集与网络状态相关的数据。收集信息有两种方法: 设备向管理系统报告关键的网络事件、管理系统定期地查询网络设备。同时, 不是所有的故障都有同样的优先级。在信息收集过程中, 网络管理系统还需要决定对一个特定的设备中哪些故障进行管理, 对故障通知或报告进行优先级判别, 从而实现故障过滤功能, 防止过多的故障通知在网络上传送, 造成泛滥。网络管理者在做这个决定时, 应考虑到网络大小和对网络的控制范围这两个因素。

预防性的日常维护能够保证互联网络中的设备正常运行, 理想的故障管理还要包括故障预测。

2. 配置管理 (CM)

配置管理包括 3 个方面的内容: 获得关于当前网络配置的信息; 提供远程修改设备配置的手段; 储存数据、维护一个最新的设备清单并根据数据产生报告。

配置管理用于掌握和控制网络的状态, 包括网络内各设备的状态及其连接关系。

配置管理最主要的作用是它可以增强网络管理者对网络配置的控制。这是通过对设备的配置数据提供快速的访问来实现的。在比较复杂的系统中, 它能够使管理者将正在使用的配置数据与储存在系统中的数据进行比较, 并且可以根据需要方便地修改配置。

配置管理与故障管理之间有密切关系。配置管理的目的是为网络设备提供软件配置的初始化或更新能力, 包括可选的软件配置。

3. 计费管理 (AM)

计费管理的功能是度量各个终端用户和应用程序对网络资源的使用情况。这一方面可以维持网络的运行和发展, 另一方面管理者可以根据情况更好地为用户提供其所需的资源量, 并促使用户合理地使用网络资源。

计费管理主要的作用是: 网络管理者能够测量和报告基于个人或团体用户的计费信息, 分配资源并计算用户通过网络传输信息的费用, 然后据此数据给用户开具账单。它有一个附带的作用, 就是增加了网络管理对用户使用网络资源情况的认识, 这有助于创建一个更具生产能力的网络。

计费管理技术也能够帮助组织计算通过网络给规定用户发送信息的费用, 使用户了解为获得网络服务需要花多少钱。

实现计费管理有 4 个步骤: 确定计费原则、收集关于网络资源使用情况的数据、设置使用定额和为用户开具网络使用账单。

4. 性能管理 (PM)

性能管理保证计算机网络可以被访问, 从而使用户能有效地使用它。故障管理考虑的是网络运行是否正常, 而性能管理考虑的则是网络运行的好坏。运用性能管理信息, 管理者可以保证网络具有足够的容量以满足用户的需要, 保证网络保持在可通过和不拥挤的状态, 为用户提供更好的服务。它通过下列途径实现这一点:

(1) 监控网络设备和它们的相关连接以确定使用率和出错率;

(2) 保证设备和连接的容量不会被过度地使用以致对性能产生有害影响。

性能管理包括下面 4 个步骤：收集网络设备和连接的当前使用数据；分析相关数据，辨别使用趋势；设置利用率阈值；使用模拟方案确定如何调整网络达到最佳性能。

性能管理除了有利于为用户提供可持续高水平的服务之外，还可以帮助管理者对网络的未来做出规划。

5. 安全管理 (SM)

安全管理通过控制信息的访问点保护网络中的敏感信息。敏感信息是指一个组织想要保护的任何数据，比如与财务、顾客的账户及与研究和发展的计划相关的一些东西。

安全管理使得网络管理者可以通过以下途径来保护敏感信息：

- (1) 限制用户（包括组织内部和外部）对主机和网络设备的访问；
- (2) 在有人试图或实际突破安全控制时，报告给管理者。

这种安全管理和操作系统的安全或物理安全是不同的。网络安全管理是通过主机或设备的特殊配置控制网络中的访问点，它不处理如何保护实际安全敏感信息，因此不应该把它和物理操作系统安全等概念混淆起来。它主要的作用是保护敏感信息，并消除安全性的忧虑。

使用安全管理，网络管理者可以限制用户对主机和网络资源的访问，并获得相应的安全保护信息。它包括下面 4 个步骤：确定要保护的敏感信息；找出访问点；使用加密、信息过滤、主机认证、用户认证及密钥认证等方法来保护访问点；维护安全访问点。

1.6 网络管理技术

1.6.1 基于 Web 的网络管理技术

随着 Web 的流行和其技术的发展，可以考虑将网络管理和 Web 结合起来。基于 Web 的网络管理系统的根本点就是允许通过 Web 浏览器进行网络管理。

基于 Web 的网络管理模式 (Web-Based Management, WBM) 的实现有两种方式。第一种方式是代理方式，即在一个内部工作站上运行 Web 服务器 (代理)。这个工作站轮流与端点设备通信，浏览器用户与代理通信，代理与端点设备之间通信。在这种方式下，网络管理软件成为操作系统上的一个应用，它介于浏览器和网络设备之间。在管理过程中，网络管理软件负责将收集到的网络信息传送到浏览器 (Web 服务器代理)，并将传统管理协议 (如 SNMP) 转换成 Web 协议 (如 HTTP)。第二种实现方式是嵌入式，它将 Web 功能嵌入到网络设备中，每个设备有自己的 Web 地址，管理员可通过浏览器直接访问并管理该设备。在这种方式下，网络管理软件与网络设备集成在一起。网络管理软件无需完成协议转换，所有的管理信息都通过 HTTP 协议传送。

在未来的 Intranet 中，基于代理与基于嵌入式的两种网络管理方案都将被应用。大型企业通过代理来进行网络监视与管理，而且代理方案也能充分管理大型机构的纯 SNMP 设备；内嵌 Web 服务器对于小型办公室网络则是理想的管理方式。将两种方式混合使用，更能体现二者的优点。

现在人们花费许多精力扩展 Web 的范围和能力，但要使 Web 真正应用于网络管理，以取代传统的网络管理模式，还需要国际标准组织、网络设备供应商、网络管理系统供应商和用户做大量的基础工作。

1.6.2 远程网络监控 (RMON) 技术

远程网络监控 (RMON) 技术的采用，为主动和广泛的网络管理提供了方便的手段。在计算机网络中，被最广泛使用的网络管理协议是简单网络管理协议 (SNMP)，采用客户 / 服务器模式工作的 RMON 是对 SNMP 最重要的增强。在这里，客户是网络管理者，嵌入到网络交换机中的 RMON 被称为嵌入式

代理, 扮演服务器的角色。嵌入式 RMON 代理模块作为系统功能的一部分, 智能地采集数据。客户通过布置在网络重要节点的 RMON 代理获取网络的重要信息和系统事件, 使得网络管理者能够及时全面地掌握网络的工作状态。

1.7 网络管理协议

网络管理系统中最重要的部分就是网络管理协议, 它定义了网络管理器与被管代理间的通信方法。下面简单介绍几种网络管理协议。

1.7.1 SNMP 协议

简单网络管理协议 (SNMP: Simple Network Management Protocol) 是由互联网工程任务组 (IETF: Internet Engineering Task Force) 定义的一套网络管理协议, 该协议基于简单网关监视协议 (SGMP: Simple Gateway Monitor Protocol)。利用 SNMP, 一个管理工作站可以远程管理所有支持这种协议的网络设备, 包括监视网络状态、修改网络设备配置、接收网络事件警告等。虽然 SNMP 开始是面向基于 IP 的网络管理, 但作为一个工业标准也被成功用于电话网络管理。

1. SNMP 基本原理

SNMP 采用了 Client/Server 模型的特殊形式——代理/管理站模型。对网络的管理与维护是通过管理工作站与 SNMP 代理间的交互完成的, 每个 SNMP 从代理负责回答 SNMP 管理工作站 (主代理) 关于 MIB 定义信息的各种查询。如图 1-2 所示是 NMS 公司网络产品中 SNMP 协议的实现模型。

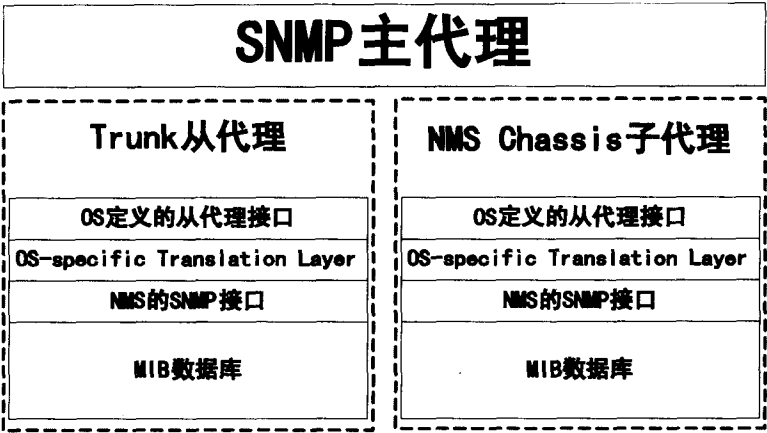


图 1-2 NMS 公司网络产品中 SNMP 协议的实现模型

SNMP 代理和管理站通过 SNMP 协议中的标准消息进行通信, 每个消息都是一个单独的数据报。SNMP 使用 UDP (用户数据报协议) 作为第四层协议 (传输协议), 进行无连接操作。SNMP 消息报文包含两个部分: SNMP 报头和协议数据单元 PDU。数据报结构如图 1-3 所示。



图 1-3 SNMP 数据报结构

(1) 版本标识符 (Version Identifier): 确保 SNMP 代理使用相同的协议, 每个 SNMP 代理都直接抛弃与自己协议版本不同的数据报。

(2) 团体名 (Community Name): 用于 SNMP 从代理对 SNMP 管理站进行认证。如果网络配置为要求验证, SNMP 从代理将对团体名和管理站的 IP 地址进行认证, 如果失败, SNMP 从代理将向管理站发送一个认证失败的 Trap 消息。

(3) 协议数据单元 (PDU): 其中 PDU 指明了 SNMP 的消息类型及其相关参数。

2. 管理信息库 MIB

IETF 规定的管理信息库 MIB (其中定义了可访问的网络设备及其属性), 由对象标识符 (OID: Object Identifier) 惟一指定。MIB 是一个树形结构, SNMP 协议消息通过遍历 MIB 树形目录中的节点来访问网络中的设备。

如图 1-4 所示给出了 NMS 系统中 SNMP 可访问网络设备的对象识别树结构。

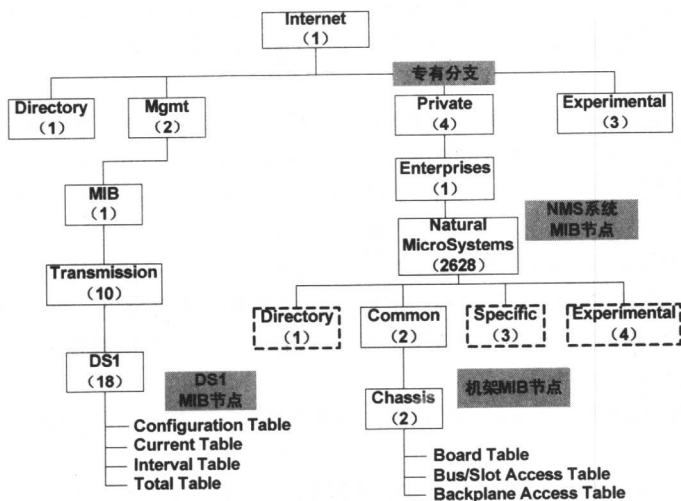


图 1-4 NMS 系统中 SNMP 可访问网络设备的对象识别树结构

如图 1-5 所示给出了对一个 DS1 线路状态进行查询的 OID 设置例子。

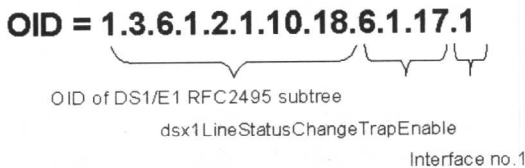


图 1-5 查询 DS1 线路状态的 OID 设置例子

3. SNMP 的 5 种消息类型

SNMP 中定义了 5 种消息类型: Get-Request、Get-Response、Get-Next-Request、Set-Request 和 Trap。

(1) Get-Request、Get-Response 与 Get-Next-Request: SNMP 管理站用 Get-Request 消息从拥有 SNMP 代理的网络设备中检索信息, 而 SNMP 代理则用 Get-Response 消息响应。Get-Next-Request 和 Get-Request 组合起来查询特定的表对象中的列元素。如首先通过下面的原语获得所要查询的设备的接口: {iso org (3) dod (6) internet (1) mgmt (2) mib (1) interfaces (2) ifNumber (2)}; 然后再通过下面的原语, 进行查询 (其中第 1 次用 Get-Request, 其后用 Get-Next-Request): {iso org (3) dod (6) internet (1) mgmt (2) mib (1) interfaces (2) ifTable (2)}。

(2) Set-Request: SNMP 管理站用 Set-Request 对网络设备进行远程配置 (包括指定设备名、设置

设备属性、删除设备或使某一个设备属性有效/无效等)。

(3) Trap: SNMP 代理使用 Trap 向 SNMP 管理站发送非请求消息,一般用于描述某一事件的发生。

1.7.2 CMIS/CMIP 协议

通用管理信息协议 (CMIP: Common Management Information Protocol) 是与通用管理信息服务 CMIS (Common Management Information Service) 并行的一种 ISO 协议,支持网络管理应用和管理代理之间的信息交换服务。CMIS 定义了一个网络管理信息服务系统,CMIP 接口支持 ISO 和定义用户 (user-defined) 管理协议。TCP/IP 网络中的 CMIP 规范称之为 CMOT (CMIP Over TCP),而 IEEE 802 LAN 中的版本称之为 CMOL (CMIP Over LLC)。此外,CMIP/CMIS 是作为 TCP/IP 协议组中简单网络管理协议 SNMP 的一种竞争协议提出的。

CMIP 是要为运行在 OSI 协议集上的开放系统提供一个网络管理框架。CMIP 出现的时间与 SNMP 差不多,但它所取得的成功非常有限。它只占领了采用 OSI 协议集网络的一小部分市场,以及几个大型电信网管理市场。

CMIP 是一个完全面向对象的模型,采用分布式、等级制的对象结构,使用面向连接、可靠的传输服务,并内置安全机制,其功能包括访问控制、认证和安全日志 (security logs)。管理对象 (Managed Objects) 负责交换网络管理应用和管理代理之间的管理信息。管理对象具备管理设备可以被监控、修改或控制等特征,并能完成各种作业。其体系结构由 4 个主要部分组成,它们结合在一起提供非常全面的网络管理方案。该体系结构给出了一个信息模型、一个组织模型、一个通信模型和一个功能模型,并提供丰富的服务。信息模型包括管理信息结构、命名等级体系和管理对象定义。通信模型采用 OSI 协议集,但其体系结构中包括系统管理,利用面向连接的服务。功能模型包括以前提到过的特定管理功能域:故障、配置、账务、性能和安全管理。

CMIP 并没有提供网络管理应用功能的规定,只定义了管理对象的信息交换机制,包括信息的使用和说明。

与 SNMP 相比,两种管理协议各有所长。SNMP 是 Internet 组织用来管理 TCP/IP 互联网和以太网的,由于实现、理解和排错很简单,所以受到很多产品的广泛支持,但是安全性较差。CMIP 是一个更为有效的网络管理协议,把更多的工作交给管理者去做,减轻了终端用户的工作负担。此外,CMIP 建立了安全管理机制,提供授权、访问控制、安全日志等功能。但由于 CMIP 是由国际标准组织指定的国际标准,因此涉及面很广,实施起来比较复杂且花费较高。

1.7.3 RMON 协议

远程监控 (RMON) 是分布式监视网络通信的工业标准,它可以在各种网络监控器和控制台系统之间交换网络监控数据。RMON 为网络管理员选择符合特殊网络需求的控制台和网络监控探测器提供了更多的自由。

RMON 是在互联网工程任务组 (IETF) 的帮助下,由用户组织定义的。它在 1992 年成为推荐标准,即 RFC1271,并在 1995 年成为草案标准,即 RFC1757,同时废除了 RFC1271。

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。RMON 中包含了一组网络统计数据 and 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。数据结果可用来监控网络效用,因而为网络规则及运行提供调控依据,同时协助网络错误诊断。

RMON 的目的在于更为有效、更为积极主动地监控远程设备。它是 RMON 探测器和 RMON 控制台管理器结合在网络环境中实施的。RMON 的监控功能有效,关键在于其探测器具有存储统计数据历史的能力,这样就不需要不停地轮询才能生成一个有关网络运行状况趋势的视图。RMON 探测器能够根据用户定义的参数来捕获特定类型的数据。当一个探测器发现一个网段处于一种不正常状态时,它会主动与