

21 世纪高等院校计算机网络工程专业规划教材

网络管理技术与实践教程

赵启升 毕野 张占强 姜宏岸 编著

可下载教学资料

<http://www.tup.tsinghua.edu.cn>

清华大学出版社



21世纪高等院校计算机网络工程专业规划教材

网络管理技术与实践教程

赵启升 毕野 张占强 姜宏岸 编著

清华大学出版社
北京

内 容 简 介

本书从实战出发,将基本理论与实践相结合,主要介绍了网络管理技术的基本概念,并分别以 CISCO 及 H3C 设备为实验室环境,介绍了交换机、路由器等网络设备的配置,内容涵盖了组建局域网、广域网所需要的从低到高的大部分知识,主要包括路由器与交换机配置基础、交换机高级配置、广域网协议原理及配置、路由选择协议及路由配置、访问控制列表及地址转换等技术,最后介绍了路由模拟器 Boson Netsim 5.13 的使用。

本书封面贴有清华大学出版社防伪标签,无标签者不得销售。

版权所有,侵权必究。侵权举报电话:010-62782989 13701121933

图书在版编目(CIP)数据

网络管理技术与实践教程/赵启升等编著. —北京:清华大学出版社,2011.6

(21 世纪高等院校计算机网络工程专业规划教材)

ISBN 978-7-302-24233-8

I. ①网… II. ①赵… III. ①计算机网络—管理—高等学校—教材 IV. ①TP393

中国版本图书馆 CIP 数据核字(2010)第 249520 号

责任编辑:魏江江 薛 阳

责任校对:梁 毅

责任印制:何 芊

出版发行:清华大学出版社

地 址:北京清华大学学研大厦 A 座

<http://www.tup.com.cn>

邮 编:100084

社 总 机:010-62770175

邮 购:010-62786544

投稿与读者服务:010-62795954, jsjic@tup.tsinghua.edu.cn

质 量 反 馈:010-62772015, zhiliang@tup.tsinghua.edu.cn

印 刷 者:北京市清华园胶印厂

装 订 者:三河市金元印装有限公司

经 销:全国新华书店

开 本:185×260 印 张:17 字 数:426 千字

版 次:2011 年 5 月第 1 版 印 次:2011 年 5 月第 1 次印刷

印 数:1~3000

定 价:29.00 元

产品编号:034170-01

前 言

本书从实战出发,将基本理论与实践相结合,主要介绍了网络管理技术的基本概念,并分别以 CISCO 及 H3C 设备为实验室环境,介绍了交换机、路由器等网络设备的配置,内容涵盖了组建局域网、广域网所需要的从低到高的大部分知识,适合作为网络系统设计与工程类课程的实践内容。本书共 11 章,各章的主要内容如下。

第 1 章介绍网络管理的定义及其目标、OSI 网络管理标准中定义的网络管理的 5 个基本功能,以及简单网络管理协议 SNMP 的管理模型、工作原理及特点。

第 2 章主要介绍计算机网络体系结构的分类及内容,重点介绍常见的网络介质特性。

第 3 章主要介绍交换机与路由器等网络互连设备的工作原理、分类以及接口连接,并介绍综合运用这些网络设备的一般原则。

第 4 章主要介绍路由器、交换机的配置方式、模式切换命令和查看命令的使用方法以及常用配置命令的使用。

第 5 章主要讨论交换机 VLAN 配置,介绍第 2 层交换机和第 3 层交换机 VLAN 的配置方法以及 VLAN 之间通过第 3 层交换机转发的配置方法。

第 6 章主要介绍广域网协议的基本工作原理、HDLC 协议的配置、PPP 协议身份验证的方法及配置、帧中继协议配置及广域网协议链路的查看和测试方法。

第 7 章主要介绍路由协议的概念、种类及静态路由的配置方法。

第 8 章介绍了 RIP 和 OSPF 动态路由协议的工作原理及配置方法。

第 9 章介绍了访问控制列表的工作原理与作用、标准访问控制列表的配置过程以及地址转换的配置。

第 10 章介绍了路由器、交换机系统管理诸如密码设置、恢复和文件管理的配置等有关内容。

第 11 章介绍了路由模拟器 Boson Netsim 5.13 的安装以及进行网络拓扑设计及网络设备配置的方法。

编者从多个大型的网络工程的实践经验出发,组织并选择了一些计算机网络管理技术和网络工程相关的关键技术内容作为本书内容。本书可作为计算机专业或通信专业的本、专科生“网络管理技术”教材,也可以作为网络工程师、网络管理员和对网络技术感兴趣的技术人员的参考资料。

本书由赵启升主编并对全书进行统稿,毕野、姜宏岸和张占强等为本书的编写付出了大



量的时间和精力,其中,第1、2、3章由赵启升编写,第5、9、11章由张占强编写,第7、8章由毕野编写,第4、6、10章由姜宏岸编写。本书在编写过程中参考了 CISCO 及 H3C 公司的有关著作和文献,并查阅了大量的网络资料,在此对所有的作者表示感谢。

由于编者水平有限,书中难免存在错误或不妥之处,欢迎广大读者批评指正。

编者

2010.10

目 录

第 1 章 网络管理	1
1.1 网络管理概述	1
1.1.1 网络管理的定义与目标	1
1.1.2 网络管理技术的特点及发展趋势	2
1.1.3 网络管理的功能	3
1.1.4 网络管理模型	6
1.2 网络管理协议	6
1.2.1 简单网络管理协议	6
1.2.2 公共管理信息服务/公共管理信息协议	9
1.2.3 公共管理信息服务与协议	9
1.2.4 局域网个人管理协议	9
1.2.5 电信管理网络	10
1.3 网络管理技术和软件	10
1.3.1 网络管理技术	10
1.3.2 常用网络管理软件	13
1.3.3 网络管理软件发展趋势及网管软件的选择	18
1.4 基于 Windows 的网络管理	19
1.4.1 SNMP 服务	19
1.4.2 SNMP 服务的运行	21
1.4.3 SNMP 服务的安装与配置	22
1.4.4 SNMP 服务的测试	25
第 2 章 TCP/IP 模型与传输介质	28
2.1 计算机网络体系结构概述	28
2.1.1 建立计算机网络体系结构的原因	28
2.1.2 计算机网络的分层次模型	28
2.1.3 国际标准化组织推荐的网络系统结构参考模型 ISO/OSI	29
2.1.4 开放系统互联参考模型的 7 层体系结构	30
2.1.5 TCP/IP 模型	31
2.2 传输介质	32
2.2.1 双绞线	33

2.2.2 光纤	35
2.3 双绞线制作	36
2.3.1 双绞线连接标准	36
2.3.2 设备连接	37
2.3.3 双绞线制作	38
第3章 交换机与路由器	42
3.1 交换机	42
3.1.1 交换机的作用	42
3.1.2 交换机的工作原理	43
3.1.3 三种交换技术	45
3.1.4 交换机的种类	46
3.1.5 交换机选型	49
3.1.6 交换机基本配置	50
3.2 路由器	54
3.2.1 路由器的作用	54
3.2.2 路由器的结构	55
3.2.3 路由器的功能	56
3.2.4 路由器的组成部件	56
3.2.5 路由器的性能指标	57
3.2.6 路由协议	58
3.2.7 路由器的种类	59
3.2.8 路由器的选型	60
3.2.9 路由器的配置	61
第4章 路由器、交换机配置基础	69
4.1 路由器、交换机的配置方式	69
4.2 命令行方式概述	72
4.2.1 系统配置对话	72
4.2.2 CLI 命令模式	73
4.2.3 帮助功能	74
4.2.4 编辑命令	77
4.3 常用基本命令	78
4.3.1 模式切换命令	78
4.3.2 查看类命令	79
4.3.3 常用全局配置命令	81
4.3.4 接口基本配置	82
第5章 交换机配置	87
5.1 交换机 VLAN 的端口划分及配置	87

5.1.1	常见的交换机类型	87
5.1.2	交换机系统与用户视图	88
5.1.3	VLAN 划分	92
5.1.4	配置步骤	93
5.2	交换机 VLAN 间路由协议配置	96
5.2.1	背景知识介绍	96
5.2.2	配置步骤	96
5.3	交换机端口 TRUNK 属性配置	98
5.3.1	背景知识介绍	98
5.3.2	配置步骤	100
5.4	三层转发交换机 VLAN 与路由器接口配置	101
5.4.1	背景知识介绍	101
5.4.2	配置步骤	101
5.5	交换机 STP 配置	103
5.5.1	生成树协议概述	104
5.5.2	STP 常用配置命令	106
5.6	交换机配置典型案例	107
5.7	练习	110
第 6 章	广域网协议原理及配置	111
6.1	广域网技术概述	111
6.2	HDLC 协议配置	113
6.2.1	HDLC 概述	113
6.2.2	HDLC 配置	114
6.3	PPP 协议配置	115
6.3.1	PPP 协议概述	115
6.3.2	PPP 身份验证	116
6.3.3	PPP 协议配置	117
6.4	帧中继配置	120
6.4.1	帧中继概述	120
6.4.2	帧中继的配置	121
第 7 章	路由选择基础与静态路由配置	127
7.1	路由选择基础	127
7.1.1	路由与路由表	127
7.1.2	路由的类型	128
7.1.3	路由器转发 IP 数据包的基本算法	129
7.1.4	管理距离与路由量度	130
7.2	静态路由及配置	131

7.2.1	静态路由简介	131
7.2.2	静态路由配置	131
7.2.3	静态路由配置案例	132
7.3	默认路由	136
7.3.1	默认路由简介	136
7.3.2	默认路由配置实例	137
7.3.3	路由环路	137
7.4	练习	138
第 8 章	动态路由协议及配置	139
8.1	动态路由协议概述	139
8.1.1	路由协议的基本工作原理	139
8.1.2	路由协议的分类	140
8.2	距离矢量路由协议	141
8.2.1	距离矢量路由协议概述	141
8.2.2	路由环路问题	144
8.2.3	解决路由环路问题的几种对策	146
8.3	RIP 路由协议及配置	147
8.3.1	RIP 路由协议概述	147
8.3.2	RIP 协议配置命令	148
8.3.3	RIP 协议配置实例	149
8.3.4	RIP 配置练习	154
8.4	OSPF 路由协议	154
8.4.1	OSPF 协议中单一区域路由生成的基本原理	155
8.4.2	OSPF 中与生成路由相关的几个概念	155
8.4.3	OSPF 的基本操作过程	158
8.4.4	OSPF 的 5 种协议报文	161
8.4.5	OSPF 区域划分	161
8.4.6	OSPF 中与区域相关的几个概念	162
8.4.7	划分区域后路由计算的基本原理	163
8.4.8	路由汇聚	167
8.4.9	OSPF 路由类型	168
8.4.10	OSPF 区域类型	168
8.4.11	OSPF 中 LSA 类型	172
8.4.12	常用 OSPF 命令简介	173
8.4.13	单区域 OSPF 配置实例	174
8.4.14	多区域 OSPF 配置实例	180
8.4.15	OSPF 综合配置实例	186
8.4.16	OSPF 配置练习	200

第 9 章 访问控制列表与地址转换	201
9.1 访问控制列表概述	201
9.1.1 IP 包过滤技术简介	201
9.1.2 访问控制列表作用	201
9.1.3 访问控制列表工作原理	202
9.1.4 访问控制列表分类	204
9.2 标准访问控制列表	204
9.2.1 标准访问控制列表简介	204
9.2.2 常用标准访问控制列表配置命令	204
9.2.3 反掩码技术	206
9.2.4 扩展访问控制列表	207
9.3 访问控制列表的应用	208
9.3.1 访问控制列表配置	208
9.3.2 标准 ACL 配置案例	210
9.3.3 扩展 ACL 配置案例	210
9.4 华为访问控制列表的运用	211
9.4.1 ACL 的配置命令	212
9.4.2 ACL 的配置	213
9.5 地址转换简介	215
9.5.1 私有地址与公有地址	215
9.5.2 地址转换原理	215
9.5.3 地址转换方式	216
9.5.4 地址转换的配置	217
9.5.5 使用地址池进行地址转换	219
9.5.6 地址转换的维护	221
9.6 访问控制列表与地址转换典型案例	221
9.7 练习	223
第 10 章 系统管理	224
10.1 密码的设置与恢复	224
10.1.1 Cisco 网络设备密码的设置	224
10.1.2 华为网络设备密码的设置	227
10.1.3 密码的恢复	229
10.2 文件操作	231
10.2.1 配置文件的操作	231
10.2.2 IOS 映像文件的操作	233
10.2.3 Cisco IOS 文件系统	235

第 11 章 路由模拟器 Boson NetSim	237
11.1 模拟软件 Boson NetSim 5.13 使用简介	237
11.1.1 Boson NetSim 的安装	237
11.1.2 Boson NetSim 的注册	238
11.1.3 Boson NetSim 的使用	239
11.1.4 Boson Network Designer 的应用实例	247
11.2 模拟器上的路由器配置	251
11.2.1 Boson NetSim 的界面	251
11.2.2 路由模拟器 Boson NetSim 中接口的配置	252
11.3 模拟器上路由配置	255
11.3.1 模拟器上的静态路由配置	255
11.3.2 模拟器上的 RIP 路由配置	257
11.3.3 模拟器上的单区域 OSPF 路由配置	258
11.3.4 NetSim 应用练习	260
参考文献	261

第 1 章

网 络 管 理

教学目标

(1) 明确计算机网络管理的定义及其目标、OSI 网络管理标准中定义的网络管理 5 个基本功能,理解网络管理模型。

(2) 正确理解简单网络管理协议的管理模型和工作原理,同时了解其他网络管理协议各自的特点。

(3) 了解基于 Web 的网络管理技术、远程网络监控技术,同时了解常用网络管理软件 HP OpenView、IBM NetView 等。

1.1 网络管理概述

1.1.1 网络管理的定义与目标

随着网络技术和应用的不断发展,人们对网络的依赖程度越来越大,用户已不再满足于网络连通性的要求,而是希望以更快的速度、更高的质量、更好的安全性访问网络。但是,随着网络用户数量的不断增多,为网络的日常管理与维护带来了巨大的挑战。为了维护日益庞大的网络系统的正常工作,保证所有网络资源处于良好的运行状态,必须有相应的网络管理系统进行支撑。

1. 网络管理的定义

网络管理,简称网管,是指对网络的运行状态进行监测和控制,使其能够有效、可靠、安全、经济地提供服务。简单地说,网络管理就是为保证网络系统能够持续、稳定、安全、可靠和高效的运行,对网络实施的一系列方法和措施。

网络管理的任务是收集、监控网络中各种设备和设施的工作参数、工作状态信息,将结果显示给管理员并进行处理,从而控制网络中的设备、设施、工作参数和工作状态,使其可靠运行。

2. 网络管理的目标

- (1) 减少停机时间,改进响应时间,提高设备利用率。
- (2) 减少运行费用,提高效率。
- (3) 减少或消除网络瓶颈。
- (4) 适应新技术。
- (5) 使网络更容易使用。
- (6) 使网络更安全。

可见,网络管理的目标是最大限度地增加网络的可用时间,提高网络设备的利用率、网络性能、服务质量和安全性,简化网络管理和降低网络运营成本,并提供网络的长期规划。

1.1.2 网络管理技术的特点及发展趋势

从已有的标准和技术发展趋势来看,网络管理标准主要是在管理体系结构、管理信息模型和管理协议方面提出一些规范和建议。关于管理框架和体系结构的标准有 NGOSS (TMF)、OSS through Java(OSS/j)、OSA/Parlay (ParlayConsortium, ETSI, 3GPP)、TMN (ITU-T)等。有关信息模型的标准有 TMF 的共享信息/数据模型(SID)、核心事务实体(OSS/j)、DMTF 的通用信息模型(CIM)、OMG 的 MDA 等。关于管理协议方面的标准有 IETF 的 SNMP、COPS、LDAP,ITU-T 的 CMIP,IPDR,以及另外一些用于通过 IP 传输数据的安全协议。

1. 网络管理软件技术热点

网络管理系统经过多年的发展,目前网络管理软件技术的热点集中在以下几个方面。

1) 开放性

随着用户对不同设备进行统一网络管理的需求日益迫切,各厂商也在考虑采用更加开放的方式实现设备对网管的支持。

2) 综合性

通过一个控制和操作台就可提供对各个子网的透视、对所管业务的了解及提供对故障定位和故障排除的支持,也就是说通过一个操作台实现对互联的多个网络的管理。此外,网络管理与系统管理正在逐渐融合,通过一个平台、一个界面,提供对网络、系统、数据库等应用服务的管理功能。

3) 智能化

现代通信网络的迅速发展,使网络的维护和操作越来越复杂,对操作使用人员提出了更高的要求。而人工维护和诊断往往花费巨大,而且对于间歇性故障无法及时检测排除。因此人工智能技术适时而生,用作技术人员的辅助工具。由此,故障诊断和网络自动维护也是人工智能应用最早的网络管理领域,目的在于解释网络运行的差错信息、诊断故障和提供处理建议。

4) 安全性

对于网络来说,安全性是网络的生命保障,因此网管软件的安全性也是热点之一。除软件本身的安全机制外,目前很多网管软件都采用 SNMP 协议,普遍使用的是 SNMP v1、SNMP v2,但现阶段的 SNMP v1、SNMP v2 协议对于安全控制还较薄弱,也为后续的 SNMP 协议发展提出挑战。

5) 基于 Web 的管理

基于 Web 的管理以其统一、友好的界面风格,地理和系统上的可移动性及系统平台的独立性,吸引着广大的用户和开发商。而目前主流的网络管理软件都提供融合 Web 技术的管理平台。

2. 网络管理技术发展趋势

通过现阶段网络管理软件中的一些技术热点,我们可以展望今后将在网络管理中出现的一些新技术,以期带动网络管理水平整体性能的提升。

1) 分布式技术

分布式技术一直是推动网络管理技术发展的核心技术,也越来越受到业界的重视。其技术特点在于分布式网络与中央控制式网络对比没有中心,因而不会因为中心遭到破坏而造成整体的崩溃。在分布式网络上,节点之间互相连接,数据可以选择多条路径传输,因而具有更高的可靠性。

2) XML 技术

XML 技术是一项国际标准,可以有效地统一现有网络系统中存在的多种管理接口。其次 XML 技术具有很强的灵活性,可以充分控制网络设备嵌入式管理代理,确保管理系统间以及管理系统与被管理设备间进行复杂的交互式通信与操作,实现很多原有管理接口无法实现的管理操作。

3) B/S 模式

B/S 网络管理结构模式简称 B/S 模式,是基于 Intranet 的需求而出现并发展的。在 B/S 模式中,最大的好处是运行维护比较简便,能实现不同的人员,从不同的地点,以不同的接入方式接入网络。其工作原理是网络中客户端运行浏览器软件,浏览器以超文本形式向 Web 服务器提出访问数据库的要求,Web 服务器接收客户端请求后,将这个请求转化为 SQL 语句,并交给数据库服务器,数据库服务器得到请求后,验证其合法性,并进行数据处理,然后将处理后的结果返回给 Web 服务器,Web 服务器再一次将得到的所有结果进行转化,变成 HTML 文档形式,转发给客户端浏览器以友好的 Web 页面形式显示出来。

4) 支持 SNMP v3 协议

SNMP 协议是一项被广泛使用的网络管理协议,是流传最广,应用最多,获得支持最广泛的一个网络管理协议。SNMP 最大的一个优点就是简单性,因而比较容易在大型网络中实现,可以帮助网管人员管理 TCP/IP 网络中各种装置,没有繁复的指令,概念上只有“存/取”两种命令。其优点是简单、稳定和灵活,也是目前网管的基础标准。

SNMP 协议经过多年的发展,已经推出的 SNMP v3 是在 SNMP v1、SNMP v2 两个版本的基础上改进后推出的,其克服了 SNMP v1 和 SNMP v2 两个版本的安全弱点,功能得到了极大的增强。SNMP v3 有以下优点。

(1) 适应性强:适用于多种操作环境,既可以管理最简单的网络,实现基本的管理功能,又能够提供强大的网络管理功能,满足复杂网络的管理需求。

(2) 扩充性好:可以根据需要增加模块。

(3) 安全性好:具有多种安全处理模块。

尽管新版本的 SNMP v3 协议还远未达到普及,但它毕竟代表着 SNMP 协议的发展方向,随着网络管理技术的发展,它完全有理由在不久的将来成为 SNMP v2 的替代者,成为网络管理的标准协议。

1.1.3 网络管理的功能

ISO 在 ISO/IEC 7498-4 文档中定义了网络管理的 5 大功能,并被广泛接受。这 5 大功能(FCAPS)分别介绍如下。

1. 故障管理

故障管理(Fault Management)又称失效管理,主要对来自硬件设备或路径节点的报警

信息进行监控、报告和存储,以及进行故障诊断、定位与处理。

所谓故障,就是那些引起系统以非正常方式运行的事件。它可分为由损坏的部件或软件故障引起的故障,以及由环境引起的外部故障。

用户希望有一个可靠的计算机网络。当网络中某个组成失效时,必须迅速查找到故障并能及时给予排除。通常,分析故障原因对于防止类似故障的再次发生相当重要。网络故障管理包括故障检测、故障诊断和故障纠正三方面。

1) 故障检测

维护和检查故障日志,检查事件的发生频率,看是否已发生故障或即将发生故障。

2) 故障诊断

执行诊断测试,以寻找故障发生的准确位置,并分析其产生的原因。

3) 故障纠正

将故障点从正常系统中隔离出去,并根据故障原因进行修复。

2. 配置管理

配置管理(Configuration Management)包括视图管理、拓扑管理、软件管理、网络规划和资源管理。只有在有权配置整个网络时,才可能正确地管理该网络,排除出现的问题,因此这是网络管理最重要的功能。配置管理的关键是设备管理,它由以下两个方面构成。

1) 布线系统维护

做好布线系统的日常维护工作,确保底层网络连接完好,是计算机网络正常、高效运行的基础。

对布线系统的测试和维护一般借助于双绞线测试仪、光纤测试仪、规程分析仪和信道测试仪等。

2) 关键设备管理

网络中的关键设备一般包括网络的主干交换机、中心路由器以及关键服务器。对于这些关键网络设备的管理除了通过网络软件实时监测外,更重要的是要做好它们的备份工作。

配置管理是一个中长期的活动。它要管理的是网络扩容、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、用户的迁移等原因所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。配置管理包括以下几方面。

- (1) 设置开放系统中有关路由操作的参数。
- (2) 被管对象和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。

3. 计费管理

计费管理(Accounting Management)主要管理各种业务资费标准,制定计费政策,以及管理用户业务使用情况和费用等。

计费管理对网络资源的使用情况进行收集、解释和处理,提出计费报告,包括计费统计、账单通知和会计处理等内容,为网络资源的应用核算成本并提供收费依据。这些网络资源

一般包括：网络服务，例如数据的传输；网络应用，例如对服务器的使用。

根据用户所使用网络资源的种类，计费管理分为三种类型，即基于网络流量的计费，基于使用时间的计费，基于网络服务的计费。

计费管理的作用为计算各用户使用网络资源的费用，规定用户使用的最大费用，当用户需要使用多个网络中的资源时能计算出总费用。通常计费管理包括以下几个主要功能。

(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。

4. 性能管理

网络性能(Performance Management)主要包括网络吞吐量、响应时间、线路利用率、网络可用性等参数。网络性能管理指通过监控网络运行状态、调整网络性能参数来改善网络的性能，确保网络平稳运行。它主要包括以下工作。

1) 性能数据的采集和存储

性能数据的采集和存储主要完成对网络设备和网络通道性能数据的采集与存储。

2) 性能门限的管理

性能门限的管理是为了提高网络管理的有效性，在特定的时间内为网络管理者选择监视对象、设置监视时间以及提供设置和修改性能门限的手段。当性能不理想时，通过对各种资源的调整来改善网络性能。

3) 性能数据的显示和分析

根据管理要求，定期对当前和历史数据进行显示及统计分析，生成各种关系曲线，并产生数据报告。

5. 安全管理

安全管理主要保护网络资源与设备不被非法访问，以及对加密机构中的密钥进行管理。安全管理是网络系统的薄弱环节之一。网络中需要解决的安全问题有以下几点。

(1) 网络数据的私有性，保护网络数据不被侵入者非法获取。

(2) 授权，防止侵入者在网络上发送错误信息。

(3) 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、访问机制、加密和加密密钥的管理等。

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、数据以及系统免受侵扰和破坏。一般的安全管理系统包含以下 4 项功能。

(1) 风险分析功能。

(2) 安全服务功能。

(3) 告警、日志和报告功能。

(4) 网络管理系统保护功能。

1.1.4 网络管理模型

在网络管理中,一般采用基于管理者-代理的网络管理模型,如图 1.1 所示。该模型主要由管理者、代理和被管对象组成。其中管理者负责整个网络的管理,管理者与代理之间利用网络通信协议交换相关信息,实现网络管理。

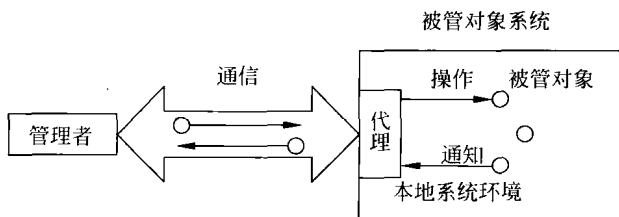


图 1.1 网络管理模型示意图

网络管理者可以是单一的 PC、单一的工作站或按层次结构在共享的接口下与并发运行的管理模块连接的几个工作站。

代理是被管对象或设备上的管理程序,把来自管理者的命令或信息请求转换为本设备特有的指令,监视设备的运行,完成管理者的指示,或返回所在设备的信息。另外,代理也可以把自身系统中发生的事件主动通知管理者。一般的代理都是返回它本身的信息,而另一种称为委托代理的,则可以提供其他系统或设备的信息。

管理者将管理要求通过管理操作指令传送给被管理系统中的代理,代理则直接管理设备。但是,代理也可能因为某些原因而拒绝管理者的命令。管理者和代理之间的信息交换可以分为从管理者到代理的管理操作和从代理到管理者的事件通知两种。

一个管理者可以和多个代理进行信息交换。一个代理也可以接受来自多个管理者的管理操作,在这种情况下,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。

1.2 网络管理协议

1.2.1 简单网络管理协议

简单网络管理协议(Simple Network Management Protocol, SNMP),是一种作为 TCP/IP 协议集一部分的应用层协议,它运行在用户数据报协议(User Datagram Protocol, UDP)之上,提供了一种从网络上的设备中收集网络管理信息的方法。它是在应用层进行网络设备间通信的管理协议,可以进行网络状态监视、网络参数设定、网络流量统计与分析、发现网络故障等。由于其开发及使用简单,所以得到了普遍应用。

1. SNMP 发展历史

1988 年,Internet 工程任务组(IETF)制定了 SNMP v1。1993 年,IETF 制定了 SNMP v2,该版本受到各网络厂商的广泛欢迎,并成为事实上的网络管理工业标准。SNMP v2 是 SNMP v1 的增强版。SNMP v2 较 SNMP v1 版本主要在系统管理接口、协作操作、信息格式、管理体系结构和安全性几个方面有较大的改善。1998 年 1 月,SNMP v3 发布,SNMP v3 涵盖了 SNMP v1 和 SNMP v2 的所有功能,并在此基础上增加了安全性。