

NSF

张宏 等编著

网络安全基础

国家信息化安全教育认证(ISEC)系列教材

 机械工业出版社
CHINA MACHINE PRESS



国家信息化安全教育认证(ISEC)系列教材

网络安全基础

张 宏 等编著



机械工业出版社

网络安全基础知识是接受网络安全教育和培训过程中首先要学习和掌握的内容。本书共包括计算机网络基础、网络安全基础知识、局域网的安全、互联网安全、网络管理实施、计算机病毒和操作系统安全等7章内容。全书以基本知识和基本概念为主,注重内容的全面性、系统性和准确性,目的是为学习后续信息安全方面的有关专业技术知识打下良好的基础。

本书为信息安全认证考试用书,也可作为高校信息安全教材,或者供从事信息安全工作的人员进行安全培训使用。

图书在版编目(CIP)数据

网络安全基础/张宏等编著. —北京:机械工业出版社,2004.4

(国家信息化安全教育认证(ISEC)系列教材)

ISBN 7-111-14165-2

I. 网... II. 张... III. 计算机网络—安全技术—资格考核—教材
IV. TP393.08

中国版本图书馆 CIP 数据核字(2004)第 019304 号

机械工业出版社(北京市百万庄大街 22 号 邮政编码 100037)

责任编辑:车 忱

责任印制:李 妍

北京蓝海印刷有限公司印刷·新华书店北京发行所发行

2004 年 4 月第 1 版·第 1 次印刷

787mm × 1092mm $\frac{1}{8}$ ·11.5 印张·281 千字

0001—5000 册

定价:20.00 元

凡购本图书,如有缺页、倒页、脱页,由本社发行部调换

本社购书热线电话:(010)68993821、88379646

封面无防伪标均为盗版

国家信息化安全教育认证(ISEC)专家组

- 卿斯汉 中国科学院信息安全技术工程研究中心主任 研究员
曲成义 中国航天科技集团公司第 710 研究所总工 研究员
许榕生 中国科学院高能物理研究所计算中心研究员
贾颖禾 国务院信息化工作办公室网络与信息安全组研究员
曹元大 北京理工大学软件学院院长 博士生导师
杨义先 北京邮电大学信息安全中心主任 博士生导师
林 鹏 国家计算机网络应急技术处理协调中心广东分中心副主任
教授级高级工程师
祁 金 公安部公共网络信息安全监察局管理监察处副处长
井乾元 公安部公共网络信息安全监察局安全对策处副处长
万平国 国际信息战略研究中心理事 中网通讯网络有限公司董事长
刘宝旭 中国科学院高能物理研究所计算中心副研究员

教材编委会

主任：宋 玲

副主任：赵小凡 张会生 欧阳满 蔡金荣 沈志工

成 员：洪京一 张宝泰 王 宏 孙论强 彭 澎 张晓伟

刘树安 刘 旻 马志谦 胡 铮 宁宇鹏 阎 慧

王 伟 薛静锋 辛 阳

出版说明

随着信息化在我国不断深入和发展,信息技术和网络给社会的经济、科教、文化和管理等各个方面注入了新的活力。人们在感受它所带来的新体验、享受它为我们带来高效率的同时,也面临着日益突出的信息安全问题。党和国家领导人多次强调,必须充分认识到做好信息安全保障工作的重要性,大力搞好技术开发和人才培养。

对信息安全专业人才的需求是多层次的。从信息安全基础理论研究到新技术的开发利用,再到各级网络信息系统信息安全保障体系的建设、运行,需要根据不同要求有针对性的进行人才培养。

国家信息化安全教育认证(ISEC)项目是由信息产业部信息化推进司推出的信息安全领域的国家级认证体系。该项目由中国电子商务协会监督,由 ISEC 国家信息化安全教育认证管理中心统一管理并实施。ISEC 国家信息化安全教育认证管理中心以行业为基础、以技术为核心制定了一套面向应用的教育方案。根据工作性质的不同,教育对象被划分为规划决策层、管理运营层和操作层三个层次。认证体系的设计,课程内容及相应的教学考试大纲的编写和指定是针对三个层次人员对信息安全知识和技能的不同需求和理解程度的不同而制定的。确保不同层次,不同需求的各类人员从各自的角度充分掌握和理解信息安全的知识和技能。

本系列教材是在国家信息化安全教育认证(ISEC)专家组的指导下,由国家信息化安全教育认证(ISEC)教材编委会组织编写的。始终以 ISEC 国家信息化安全教育认证管理中心制订的各级考试大纲为依据,坚持面向行业用户的需求和侧重技术应用两个基本原则,全面地介绍了信息安全各种主流技术和管理规范,以帮助读者深入了解信息安全本质,并熟练掌握相应的技能,从而建立完备的信息安全观念。本系列教材包括:《网络安全基础》、《防火墙原理与技术》、《入侵检测技术》、《VPN 技术》、《PKI 技术》、《数据备份与灾难恢复》、《网络隔离与网闸》、《信息安全法规与标准》、《信息安全策略与机制》、《信息安全团队构建与管理》,共计 10 本。

在写作过程中,北京正阳天马信息技术有限公司为本系列教材的编写提供了很多宝贵的建议和支持。

前 言

随着计算机网络的普及,计算机为人们的日常的生产和生活带来极大便利,可是,信息安全的问题也时时困扰广大的计算机用户。因此,人们迫切需要掌握计算机网络安全知识。

本书是根据国家信息安全认证中心培训大纲要求编写的教材,详细地介绍了网络安全所涉及的所有方面的问题。全书共分7章:

第1章介绍了计算机网络基础知识,包括计算机网络的定义、计算机网络的组成、计算机网络体系结构等;第2章介绍了网络安全基础知识;第3章介绍了局域网的安全知识,包括局域网基础知识及局域网所采用安全技术;第4章介绍了有关互联网安全的知识,包括互联网基础知识及在局域网安全技术上所采用安全技术;第5章介绍了网络管理的基础知识;第6章介绍了计算机病毒发生、发展和破坏案例,计算机病毒的种类及计算机病毒的防治。第7章介绍了操作系统安全。

本书体系完整,结构清晰,难度适中,适合大学相关专业作为教材和各种安全方面的培训使用。

本书主要由张宏编著,参加本书编写工作的还有凌丰、伍尔灿、丘蕾、周湛等。彭澎对全书进行了审阅并对部分内容进行了修改,在此表示感谢。本书在编写过程中,参考了大量资料,并得到多位同行的大力支持和帮助,在此一并表示感谢。

目 录

出版说明

前言

第 1 章 计算机网络基础	1
1.1 计算机网络的概念、分类和特点	1
1.1.1 计算机网络系统的产生与发展	1
1.1.2 计算机网络的定义	2
1.1.3 计算机网络的分类	2
1.1.4 计算机网络的特点	5
1.2 计算机网络的结构	6
1.2.1 计算机网络的基本结构	6
1.2.2 计算机网络的硬件与软件系统结构	6
1.2.3 计算机网络的拓扑结构	8
1.3 计算机网络的资源共享	10
1.3.1 硬件资源共享	10
1.3.2 软件和数据资源共享	10
1.3.3 通信信道资源共享	10
1.4 计算机网络体系结构	11
1.4.1 网络体系结构概述	11
1.4.2 计算机网络结构的模型	13
1.4.3 TCP/IP 参考模型	16
1.4.4 其他网络协议	18
1.5 习题	19
第 2 章 网络安全基础知识	21
2.1 网络安全涉及哪些方面	21
2.1.1 政策法规	21
2.1.2 组织管理	22
2.1.3 安全技术	22
2.1.4 其他因素	23
2.2 网络安全的定义	24
2.2.1 数据保密性	24
2.2.2 数据的完整性和可靠性	24
2.2.3 数据的可用性	25
2.3 安全隐患的产生	26
2.3.1 环境因素	26
2.3.2 数据通信中的隐患	26

2.3.3	资源共享带来的隐患	26
2.3.4	计算机病毒的危害	27
2.3.5	网络管理造成的隐患	27
2.4	网络面临的威胁	27
2.4.1	威胁的分类	27
2.4.2	网络可能遇到的威胁	28
2.4.3	产生威胁的原因	29
2.5	网络中的风险	30
2.5.1	安全风险的特点	30
2.5.2	常见的安全风险	30
2.5.3	风险的管理	31
2.6	习题	33
第3章	局域网的安全	34
3.1	局域网概述	34
3.1.1	什么是局域网	34
3.1.2	局域网的主要模式	34
3.1.3	局域网的基本类型	35
3.1.4	IEEE 802 LAN 简介	35
3.2	局域网的安全	36
3.2.1	来自内部的危害	36
3.2.2	组织管理因素	37
3.3	备份技术	38
3.3.1	数据备份技术	38
3.3.2	备份系统的组成及逻辑结构	40
3.3.3	系统备份	43
3.3.4	备份方案的基本要求	44
3.4	归档和存储的其他技术	45
3.4.1	归档	45
3.4.2	分级存储管理	49
3.4.3	存储区域网络	51
3.5	容错技术	52
3.5.1	容错系统的分类	52
3.5.2	容错技术的模型	53
3.5.3	容错系统实现方法	53
3.5.4	常用的容错系统	56
3.6	访问控制技术	59
3.6.1	访问控制机制	59
3.6.2	访问控制策略	62
3.7	虚拟网技术	62
3.7.1	虚拟网的定义	63
3.7.2	虚拟网的划分	63

3.7.3	虚拟网间的信息传递	65
3.7.4	虚拟网的标准	65
3.7.5	虚拟网的优势	66
3.8	局域网病毒防范	68
3.8.1	仅保护工作站	68
3.8.2	仅保护服务器	68
3.8.3	完全保护工作站和服务器	69
3.8.4	网络环境下的病毒防护	69
3.9	习题	70
第4章	互联网安全	72
4.1	互联网的基本结构	72
4.1.1	互联网的概念	72
4.1.2	互联网的特点	72
4.1.3	互联网的基本结构	74
4.1.4	互联网的主要接入方式	75
4.2	互联网安全技术	76
4.2.1	防火墙概念	76
4.2.2	防火墙的主要技术	77
4.2.3	数据加密技术	81
4.2.4	数据加密方式	83
4.2.5	认证技术	85
4.2.6	入侵检测技术	87
4.2.7	计算机病毒防范	91
4.3	习题	93
第5章	网络管理实施	94
5.1	网络管理的概念	94
5.1.1	什么是网络管理	94
5.1.2	网络管理的基本模型	95
5.1.3	网络管理协议	99
5.2	网络管理的基本内容	100
5.2.1	网络性能管理	100
5.2.2	网络的合理配置	101
5.2.3	网络故障的预警与诊断	103
5.2.4	网络安全管理	106
5.2.5	网络计费管理	107
5.3	简单网络管理协议及远程网络监控简介	108
5.3.1	简单网络管理协议简介	108
5.3.2	远程网络监视	112
5.4	习题	115
第6章	计算机病毒	117

6.1 计算机病毒概述	117
6.1.1 计算机病毒发展阶段	117
6.1.2 病毒分类	119
6.1.3 病毒特征	119
6.1.4 计算机病毒运行机制	121
6.1.5 计算机病毒检测	121
6.2 计算机病毒主要类型	123
6.2.1 引导型病毒	123
6.2.2 文件型病毒	124
6.2.3 蠕虫病毒及变体	125
6.2.4 计算机病毒发展趋势	125
6.3 计算机病毒防治	126
6.3.1 防止计算机病毒破坏的措施	126
6.3.2 病毒破坏后的修复	127
6.3.3 防病毒软件介绍	128
6.4 近年计算机病毒的破坏案例	131
6.4.1 影响较大的病毒	131
6.4.2 近年部分计算机病毒的特征及变种	133
6.5 习题	145
第7章 操作系统安全	147
7.1 操作系统安全基础	147
7.1.1 操作系统概述	147
7.1.2 网络操作系统的基本类型	147
7.1.3 操作系统安全机制	148
7.1.4 网络系统安全等级	148
7.2 Windows NT/2000 操作系统安全特性	149
7.2.1 Windows NT/2000 操作系统简介	149
7.2.2 Windows NT/2000 安全环境	150
7.2.3 Windows NT/2000 账号安全管理	151
7.2.4 Windows NT/2000 的安全访问控制	155
7.2.5 Windows NT/2000 资源安全管理	156
7.2.6 Windows NT/2000 网络安全管理	158
7.3 UNIX/Linux 操作系统安全特性	159
7.3.1 UNIX/Linux 操作系统简介	159
7.3.2 UNIX/Linux 系统的访问控制	161
7.3.3 UNIX/Linux 操作系统的安全管理	163
7.3.4 UNIX/Linux 的安全性	167
7.3.5 UNIX/Linux 的安全审计	169
7.4 习题	171
附录	172

第 1 章 计算机网络基础

本章导读：

本章介绍计算机网络的组成、计算机网络的资源共享、计算机网络的体系结构,以及网络协议等基础知识。本章重点是计算机网络的组成、网络体系结构和网络协议。

计算机网络是计算机技术和通信技术紧密结合的产物,它涉及通信与计算机两个领域。它的诞生使计算机体系结构发生了巨大变化,在当今社会经济中起着非常重要的作用。它对人类社会的进步作出了巨大贡献。

1.1 计算机网络的概念、分类和特点

1.1.1 计算机网络系统的产生与发展

计算机网络是随着计算机技术和通信技术的发展而发展起来的。

早期的计算机系统是高度集中的,所有的设备安装在独立的大房间中。后来出现了批处理和分时系统,分时系统所连接的多个终端必须紧接着主计算机。20 世纪 50 年代中后期,许多系统都将地理上分散的多个终端通过通信线路连接到一台中心计算机上,这样就出现了第一代计算机网络。

第一代计算机网络是以单个计算机为中心的远程联机系统。典型应用是由一台计算机和全美范围内 2000 多个终端组成的飞机票订票系统。其中,终端是一台计算机的外部设备,只包括 CRT 控制器和键盘,无 CPU、内存。

随着远程终端的增多,在主机前增加了前端处理机 FEP。当时,人们把计算机网络定义为“以传输信息为目的而连接起来,实现远程信息处理或进一步达到资源共享的系统”,这样的通信系统就构成了计算机网络的雏形。

第二代计算机网络是把多个主机通过通信线路互联起来,为用户提供服务的系统。它产生于 20 世纪 60 年代后期,典型代表是美国国防部高级研究计划局协助开发的 ARPAnet。

在 ARPAnet 中,主机之间不是直接用线路相连,而是经过接口报文处理机(IMP)转接后互连的。IMP 和它们之间连接的通信线路一起负责主机间的通信任务,这就构成了所谓通信子网。通信子网连接的主机负责运行程序,提供资源共享,从而组成了所谓的资源子网。

两个主机间通信时对传送信息内容的理解、信息表示形式以及各种情况下的应答信号都必须遵守一个共同的约定,即协议。在 ARPAnet 中,按功能将协议分成了若干层次。如何分层,以及各层中具体采用的协议的总和被称为网络体系结构。体系结构是个抽象的概念,其具体实现是通过特定的硬件和软件来完成的。

第二代网络以通信子网为中心。这个时期,网络概念为“以能够相互共享资源为目的互联起来的具有独立功能的计算机之集合体”。

第三代计算机网络是具有统一的网络体系结构并遵循国际标准的开放式和标准化的网络。

ISO 在 1984 年颁布了 OSI/RM, 该模型分为七个层次, 也称为 OSI 七层模型, 被公认为新一代计算机网络体系结构的基础。

第四代计算机网络从 20 世纪 80 年代末开始, 是一种网络与网络联接而形成的网络集合, 即互联网。

1.1.2 计算机网络的定义

早期制造的计算机, 一台机器由一人使用, 其使用效率非常低, 所以很快被“计算中心”的模式取代。在计算中心的模式下, 一台计算机同时可以被多个用户使用, 使多个用户得以共享一台计算机系统的资源。但是, 计算中心仍然把用户限制在一个地方和一台机器上。

计算机网络的出现, 则把许多计算机或计算中心连接起来, 其中每一台计算机都有可能通过网络为任何其他计算机上的用户提供服务。网络使用者摆脱了地域分隔的局限, 在网络覆盖的范围内能够实现计算机之间资源的共享。

为此, 可以把计算机网络定义为: 将若干具有独立工作能力的计算机系统通过通信设备和线路连接起来, 由功能完善的网络软件实现资源共享和数据通信的系统。

定义涉及三个方面的问题:

- 至少两台计算机互连。
- 通信设备与传输介质。
- 网络软件: 通信协议和网络操作系统(NOS)。

1.1.3 计算机网络的分类

目前不存在被普遍接受的所有计算机网络都适用的分类法, 但是有两个标准很重要: 传输技术和规模。

1. 按传输技术(通信方式)划分

按传输技术(通信方式)分类, 计算机网络可被分为广播方式网络和点对点方式网络两种。

广播方式网络(broadcast network)仅有一条通信信道, 由网络上的所有机器共享。网络中任何机器都可以发送或接收消息(按某种语法组织的分组或包(packet))。分组的地址字段指明此分组应被哪台机器接收。当一台计算机或控制转发节点收到分组后, 各机器将检查分组的地址字段。如果是发送给它的分组, 则处理该分组, 否则将分组丢弃。

广播系统通常也允许在地址字段中使用一段特殊代码, 以便将分组发送到所有目标。使用特殊代码的分组发出以后, 网络上的每一台机器都会接收和处理它。这种操作被称作广播(broadcasting)。某些广播系统还支持向机器的一个子集发送信息的功能, 即多点播送(multicasting)。一种常见的方案是保留地址字段的某一位来指示多点播送, 而剩下的各位地址字段存放组号。每台机器可以注册到任意组或所有的组。当某一分组被发送给某个组时, 它被发送到所有注册到该组的机器。

点对点网络(point-to-point network)是由一对对机器之间的多条连接构成的。为了能从源到达目的地, 网络上的分组可能必须通过一台或多台中间机器。传输路径通常是多条, 长度

可能不一样,因此在点对点网络中路由算法十分重要。一般来讲(当然也有例外),小的、处于同一地区的网络采用广播方式,而大的网络则采用点对点方式。

2. 按网络地理有效范围(网络规模)划分

表 1-1 列出了按地理有效范围分类的多处理器系统。

表 1-1 按连接距离分类的多处理器系统

处理器间的距离	多个处理器的位置	例子
0.1m	同一电路板	数据流机器
1m	同一系统	多计算机
10m	同一房间	局域网
100m	同一建筑物	
1km	同一园区	
10km	同一城市	城域网
100km	同一国家	广域网
1000km	同一洲内	
10000km	同一行星上	互联网

在表 1-1 中,最上面的是数据流机器(data flow machine),它是高度并行的计算机,具有多个处理单元为同一程序服务,接下来是多计算机(multi computers),即在非常短、速度很快的总线上发送消息,并进行通信的机器。在多计算机之后就是真正的网络,是能够在很长的电缆上交换消息进行通信的机器。

3. 按通信媒体划分

按通信媒体划分,计算机网络被分为有线网和无线网两大类。

有线网是采用如同轴电缆、双绞线、光纤等物理媒体来传输数据的网络。

无线网是采用微波、红外线、光波等形式来传输数据的网络。

4. 按通信速率划分

按通信速率划分,计算机网络被分为低速网、中速网和高速网三类。

低速网是借助调制解调器利用电话网来实现的。

中速网主要是传统的数字式公用数据网。

高速网主要用于互联网的主干网中。

5. 按数据交换方式划分

按数据交换方式划分,计算机网络被分为直接交换网、存储转发交换网和混合交换网三类。

直接交换网又称电路交换网。直接交换网进行数据通信交换时,首先申请通信的物理通路,物理通路建立后,通信双方开始通信传输数据。在传输数据的整个时间内通信双方始终独占所占用的信道。

存储转发交换网是这样一种网络:在进行数据通信交换时,先将数据在交换装置控制下放入缓冲器中暂存,并对存储的数据进行一些必要的处理,当指定的输出线空闲时,再将数据发

送出去。

混合交换网是在一个数据网中同时采用存储转发交换和电路交换两种方式进行数据交换的网络。

6. 按通信性能划分

按通信性能划分,计算机网络被分为资源共享计算机网、分布式计算机网和远程通信网三类。

资源共享计算机网是在网络系统中,计算机的资源可以被其他系统共享。

分布式计算机网是网络中的各个计算机进程可以相互协调工作和进行信息交换,来共同完成一个大的、复杂的任务。

远程通信网是主要起数据传输作用的系统,它的主要目的是使用户能使用远程主机。

7. 按使用范围划分

按使用范围划分,计算机网络被分为公用网和专用网两类。

公用网:是为公众提供各种信息服务的网络系统,如互联网是只要符合网络拥有者的要求就能使用的网络。

专用网:是为一个或几个部门所拥有的系统,它只为拥有者提供服务。这种网络不向拥有者以外的人提供服务。

8. 按配置划分

按配置划分网络是对不同局域网进行划分的一种主要方式。在局域网中,互连的计算机,根据它们的作用和地位被划分为服务器和 workstation 两类。服务器是指在系统中提供服务的计算机, workstation 是指接受服务器提供服务的计算机。按配置划分就是根据系统中服务器和 workstation 的组合方式划分网络。

同类网:又称对等网。如果在网络系统中,每台计算机既是服务器,又是 workstation,那这个网络系统就是同类网。在同类网中,每台计算机都可以利用其他计算机的资源。它要求每个用户必须掌握足够的计算机知识并对网络工作方式有深入了解,还要花费很多时间和精力用来搞清楚不同 workstation 用户之间的关系。所以这类网络系统只能局限在小范围内。

单服务器网:是客户/服务器结构的网络。如果在网络系统中,只有一台计算机作为整个网络的服务器,其他计算机全部是 workstation,那么,这个网络系统就是单服务器网。在单服务器网中,每个 workstation 都可以通过服务器享用全网的资源。每个 workstation 在网络中的地位是一样的,而服务器在网中也可以作为一台 workstation 使用。单服务器网是一种最简单、最常用的网络。

混合网:也是客户/服务器结构的网络。如果在网络系统中的服务器不只一个,同时又不是每个 workstation 都可以当作服务器来使用,那么,这个网就是混合网。混合网与单服务器网的差别在于网中存在不只一个服务器。混合网与同类网的差别在于并非每台计算机既是服务器又是 workstation。

由于混合网中服务器不只一个,因此,避免了在单服务器网上工作的各 workstation 完全依赖于一个服务器,当服务器发生故障后全网处于瘫痪的现象。所以,对于一些大型的、信息处理工作繁忙的、重要的网络系统,在设计时要注意这个问题,应采用混合网设计,这一点是非常重要的。

9. 按对数据的组织方式划分

数据的组织方式与计算机网络的性能有直接的关系。

分布式数据组织网络系统中的资源既是互连的,又是独立的。虽然系统要求对资源进行统一的管理,但系统中分布在各独立的工作站中的资源,由各独立的工作站独立支配。系统只能通过一个高层次的操作系统对各个分布的资源进行管理。

分布式数据组织网络系统的特点是:系统独立性强,用户使用方便、灵活。但对整个网络系统来说,管理复杂,保密性、安全性差。

集中式数据组织网络:将网络系统中的资源进行统一管理,系统中各独立的工作站独立性差,它们必须在主服务器或起决定作用的主计算机支配下进行工作。

集中式数据组织网络系统的特点是:对信息处理集中,系统响应时间短,可靠性高,便于管理,但整个系统适应性差。

在对数据组织上,比较理想的网络系统,特别是局域网,通常采用分布式与集中式相结合的系统,即分布集中式系统。这种网络系统通常是根据用户的需要和具体系统的特点,综合分布式和集中式的优点进行设计的。

10. 按计算机网络的拓扑结构划分

根据计算机网络中各计算机之间不同的连接方式归纳出的计算机网络的拓扑结构来划分计算机网络的类型,是一种非常重要的对计算机网络进行分类的方法。拓扑结构的有关知识将在1.2.3节中介绍。

1.1.4 计算机网络的特点

虽然各种网络系统的具体用途、系统连接结构、数据传送方式并不相同,但各种网络系统都具有一些共同的特点。

1. 数据交换

网络系统中相连的计算机能够相互传送数据信息,使相距很远的人能够直接交换数据。

2. 相对独立性

网络系统中相连的计算机既有相互联系又相互独立。

3. 建网周期短、见效快

建立一个网络系统只需把各计算机与通信媒体连接好,安装、调试好相应的网络软硬件即可。

4. 成本低、效益高

计算机网络使只有微机的用户也能分享大型机的功能。这一点充分体现了网络系统的“群体”优势。

5. 使用简单

对用户而言,掌握网络使用技术要比掌握大型机使用技术容易,实用性也非常强。

6. 易于分布处理

由于网络是将多台计算机连成具有高性能的计算机系统,所以,网络具有将较大型的综合性问题,通过一定算法把任务分配给不同的计算机完成,以解决大量复杂问题的能力。

7. 系统灵活性、适应性强

在计算机网络系统中能很灵活地接入新的计算机,以扩充系统,计算机网络的灵活性使其表现出对不同的用户、不同的任务具有很强的适应性。

1.2 计算机网络的结构

根据计算机网络的定义,可以知道计算机网络由计算机和通信线路组成。

1.2.1 计算机网络的基本结构

计算机网络在结构上包括两个部分。一部分是连接在网络上的供网络用户使用的计算机的集合。这些计算机称为主机(host),用来运行用户的应用程序,为用户提供资源和服务,这部分被称为资源子网。另一部分是用来把主机连接在一起并在主机之间传送信息的设施,称为通信子网。通信子网由传输线路和转接部件构成。其中,传输线路是实现信息实际传送的通道,转接部件是处理信息传送的处理机。从逻辑上看,网络是节点之间通过通道相连的一个连通域,它的通信方式可以采取点对点信道通信,或者广播信道通信。至于具体的连接,则有不同的拓扑结构。例如,在点对点通信方式下,可以取星型、环型、树型、全连接型或不规则型结构;在广播通信方式下则可用总线连接、卫星连接、无线电连接以及环型连接。

在计算机网络上的主机之间传送数据和通信是通过一定协议进行的。为了减少设计的复杂性,设计者用高度结构化的方法来分层制定协议。当两台计算机通信时,直接表现为应用级别上的服务请求和返回服务结果。从一台主机发出用过程语言表达的服务请求,到把请求转变为在物理线路上传送的比特(bit)信息流,中间要经过多个层次的转化。在信息到达另一端的目标计算机后,将按相反的次序逐层复原信息,最后变成提交给目标计算机执行的服务请求的初始形式。从目标机返回结果时,沿反方向经历同一过程。在网络的层次协议中,每一层协议建立在它的下层协议基础之上,下层为上层服务,保证上层的功能,而服务的细节对上层加以屏蔽。各层协议就是主机之间在各对等层上的对话规则和约定。

1.2.2 计算机网络的硬件与软件系统结构

1. 网络系统体系中硬件系统结构

计算机网络系统中硬件系统结构如图 1-1 所示。

其中:计算机主机是任何可以组网的计算机,包括大型机、中型机、小型机、PC 机等。网络接口通常指网卡,也包括 USB、RS-232、LPT 这些可以与外部相连的接口。传输介质有有线和无线两类。有线传输中指的是网线,包括光纤、同轴电缆、多股绞线等。无线传输中有无线电、红外线、光等。网络连接设备是指集线器、路由器、网桥等网络连接设备。

2. 网络系统体系中的软件系统结构

由于网络体系结构的多样化、网络硬件的多样化和复杂化,使网络软件系统所要解决的问题多而复杂,涉及的范围广,内容丰富,软件类型多种多样,难以标准化。网络软件系统的这些特点决定了网络软件系统的基本结构。

网络软件也同单机系统中的软件系统一样,是一种层次结构,网络软件系统的分层结构如

图 1-2 所示。

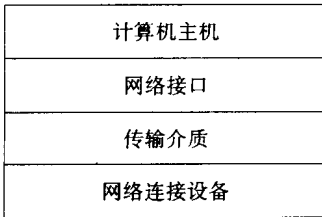


图 1-1 计算机网络系统硬件系统结构

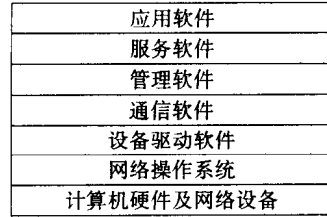


图 1-2 网络系统的分层结构

事实上,对网络软件来说没有明显的软件的分层结构,层与层之间没有明显的界线,也就是说,对许多网络软件来说,很难把它划分在某一确定的层次上。

3. 典型软件介绍

网络软件是实现网络功能所不可缺少的软环境,它主要包括如下几类:

(1) 协议软件。用以实现网络协议功能的软件就是协议软件。协议软件的种类非常多,不同体系结构的网络系统都有支持自身系统的协议软件,体系结构中不同层次上又有不同的协议软件。对某一协议软件来说,到底把它划分到网络体系结构中的哪一层是由协议软件的功能决定的。所以对同一协议软件,它在不同体系结构中所隶属的层可能是不一样的。

(2) 联机服务软件。联机服务软件是为网络用户提供获取联机信息的软件。联机服务软件有许多种,性能各异。

(3) 通信软件。在网络系统中,主计算机—主计算机或主计算机—终端连接有两种方式:

1) 主机通过通信接口单元与其他计算机连接。这种连接必须按照网络协议所规定的接口关系进行。

2) 主机直接通过通信媒体与主机或终端相连接。这种连接,由于所连接的终端和计算机种类不同,没有固定标准,并且连接接口关系不必一定与网络协议的规定一致。所以在网络环境下,在主机操作系统中除了要配置实现网络通信的低级协议软件外,还要为各种相连的终端或计算机配置相应的通信软件。

通信软件的作用就是使用户能够不必详细了解通信控制规程,很容易地控制自己的应用程序,同时能与多个机器进行通信,并对大量的通信数据进行加工和管理。

目前,所有主要的通信软件都能很方便地与主机连接,并具有完善的传真功能、传输文件功能和自动生成原稿功能。

(4) 管理软件。网络系统是一种复杂的系统,对管理者来说经常会遇到许多难以解决的问题。如要重新设置某个用户的 config.sys 文件、避免服务器之间的任务冲突、跟踪网络中用户工作状态、检查与消除计算机病毒、运行路由器诊断程序等。这就需要有一些软件,用这些软件来解决管理人员所遇到的问题。这就是管理软件。网络管理软件的种类很多,功能各异。

(5) 网络操作系统。网络操作系统是网络软件中最主要的软件。

(6) 设备驱动软件。设备驱动软件是一种控制特定设备的硬件级程序。设备驱动软件可以被看成是一个硬件的小型操作系统,每个驱动程序都包括确保特定设备相应功能所需的逻辑和数据。设备驱动软件通常以固件形式存在于它所操作的设备中。例如 NIC,它为主机的