全国信息技术人才培养工程指定培训教材
信息安全理论与实用技术丛书

信息安全应用基础

信息产业部电子教育中心　组编
戴宗坤　主编

XINXI ANQUAN YINGYONG JICHU

重庆大学出版社

全国信息技术人才培养工程指定培训教材

信息安全理论与实用技术丛书

信息安全应用基础

信息产业部电子教育中心　　组编
戴宗坤　　主编
罗万伯　刘嘉勇　戴宗坤　等　编著

重庆大学出版社

内 容 提 要

本书作为《信息安全理论与实用技术丛书》中的基础篇，对信息安全的应用基础进行了全面、简明通俗的介绍，包括必要的网络基础知识，安全基础，操作系统基础，主流操作系统的安全问题及其解决办法，密码学基础，加密技术、数字签名技术以及散列算法等在信息安全的机密性、完整性、访问控制、鉴别和抗抵赖等方面的应用，开放系统互联安全体系、互联网络安全体系和信息系统安全体系结构，以及安全服务的配置原理和技术方法等。

本书可作为全国信息技术人才培养工程信息安全专业技术指定培训教材，亦可作为信息安全和计算机应用本专科教材；对从事信息安全管理、信息系统管理以及信息安全咨询服务的专业技术人员也具有参考价值。

图书在版编目(CIP)数据

信息安全应用基础/戴宗坤主编. —重庆：重庆大学出版社，2005.5
(信息安全理论与实用技术丛书)
ISBN 7-5624-3389-5

Ⅰ.信… Ⅱ.戴… Ⅲ.计算机网络—安全技术 Ⅳ.TP393.08

中国版本图书馆 CIP 数据核字(2005)第 043898 号

全国信息技术人才培养工程指定培训教材
信息安全理论与实用技术丛书
信息安全应用基础
信息产业部电子教育中心 组编
罗万伯 刘嘉勇 戴宗坤 等 编著
责任编辑：王海琼 黄 鑫 刘国良 吴庆佺 版式设计：王 勇 王海琼
责任校对：李定群 责任印制：秦 梅

*

重庆大学出版社出版发行
出版人：张鸽盛
社址：重庆市沙坪坝正街 174 号重庆大学(A 区)内
邮编：400030
电话：(023) 65102378 65105781
传真：(023) 65103686 65105565
网址：http://www.cqup.com.cn
邮箱：fxk@cqup.com.cn (市场营销部)
全国新华书店经销
重庆升光电力印务有限公司印刷

*

开本：787×1092 1/16 印张：16.75 字数：364 千
2005 年 5 月第 1 版 2005 年 5 月第 1 次印刷
印数：1—3 000
ISBN 7-5624-3389-5 定价：25.00 元

丛书序

当今世界，随着信息技术在经济社会各领域不断深化的应用，信息技术对生产力以至于人类文明发展的巨大作用越来越明显。党的“十六大”提出要“坚持以信息化带动工业化，以工业化促进信息化”，“优先发展信息产业，在经济和社会领域广泛应用信息技术”。明确了我国经济发展的道路，赋予了信息产业新的历史使命。近年来，日新月异的信息技术呈现出新的发展趋势，各类信息技术加快了相互融合和渗透的步伐，信息技术与其他技术的结合更加紧密，信息技术应用的深度、广度和专业化程度不断提高。

我国的信息产业作为国民经济的支柱产业正面临着有利的国际、国内形势，电子信息产业的规模总量已进入世界大国行列。但是我们也清楚地认识到，与国际先进水平相比，我们在产业结构、核心技术、管理水平、综合效益、普及程度等方面，还存在较大差距，缺乏创新能力与核心竞争力，“大”而不强。国际国内形势的发展，要求信息产业不仅要做大，而且要做强，要从制造大国向制造强国转变，这是信息产业今后的重点工作。要实现这一转变，人才是基础。机遇难得，人才更难得，要抓住本世纪头二十年的重要战略机遇期，加快信息产业发展，关键在于培养和使用好人才资源。《中共中央、国务院关于进一步加强人才工作的决定》指出，人才问题是关系党和国家事业发展的关键问题，人才资源已成为最重要的战略资源，人才在综合国力竞争中越来越具有决定性意义。

为抓住机遇，迎接挑战，实施人才强业战略，信息产业部启动了“全国信息技术人才培养工程”。该项工程旨在通过政府政策引导，充分发挥全行业和全社会教育培训资源的作用，建立规范的信息技术教育培训体系、科学的培训课程体系、严谨的信息技术人才评测服务体系，培养造就大批行业急需的、结构合理的高素质信息技术应用型人才，以促进信息产业持续快速协调健康发展。

由各方专家依据信息产业对技术人才素质与能力的需求，在充分吸取国内外先进信息技术培训课程优点的基础上，信息产业部电子教育中心精心组织编写了信息技术系列培训教材。这些教材注重提升信息技术人才分析问题和解决问题的能力，对各层次信息技术人才的培养工作具有现实的指导意义。我谨向参与本系列教材规划、组织、编写同志们致以诚挚的感谢，并希望该系列教材在全国信息技术人才培养工作中发挥有益的作用。

王耀先

二〇〇四年四月十日

全国信息技术人才培养工程教材

通讯地址：北京4356信箱教育中心

http://www.ceiaec.orgl/

前 言

短短几年时间，信息安全问题已经从教学和科学研究领域渗透到社会各个领域，引起人们的深切关注。人们对信息安全的认识和理解正在不断深化中。信息安全问题不是凭空出现的，它是信息化技术高速发展、伴随信息网络化和社会信息化发展进程中与生俱来的产物。一般认为，信息安全问题的源头是信息系统及其组件在客观上存在脆弱性和漏洞，在主观上存在利用这些脆弱性和漏洞来达到某种目的或获得某种利益的系统内外部的威胁。这些问题之所以引起全社会的高度重视，是因为国际互联网络技术的出现并大规模普及应用后，社会各领域从上到下都感到了问题的严重性。这是因为，信息化正在改变着人类社会的生活方式、生产方式、管理方式、思维方式和行为方式，而这种变化是渐进的、不以人们主观意志为转移的。人们在长期的社会生活中，知道如何规范自己的行为和自我保护，是因为有成熟的法律体系保障，而且人们从小就受到学校、家庭和社会的系统安全教育，加之整个社会具有维护传统社会秩序的强大的道德和文化氛围，使得人们有明确的是非判断能力和行为控制能力，因而具有强烈的安全意识。但当信息化渗透到社会各个领域时，由于信息化进程的高速发展，人们来不及对信息化社会的安全问题——即信息系统自身的脆弱性和漏洞，以及针对它们的威胁进行认识或根本不认识，人们没有从法律体系、从道德和文化素质，以及信息安全意识上做好适应信息化社会的心理和技术准备。针对我国信息化进程中这一普遍性问题，近年来党和政府一方面加强对信息安全有关的法律、法规建设，以及发展信息安全产业；另一方面从教育和培训做起，采取措施加快信息安全学科建设和人才培养，加强信息安全技术和技能培训，强调全面培养和提高全民族的信息安全道德素质和信息安全意识。

1998 年以来,四川大学信息安全研究所在信息安全学科建设和多层次学历教育上进行了系统的探索和研究,在多年教学和科研成果基础上编辑出版了用于本科和硕士研究生的教材和参考书。2003 年开始与国家信息安全产业成果化(四川)基地联合进行信息安全非学历教育和技能技巧的培训。为适应日益增长的培训和信息安全人员需求,我们在原编写的本科和研究生教材和参考书基础上,结合在职继续教育的经验和特点,编写了第 1 批(共 3 本)培训教材——《信息安全应用基础》、《信息安全实用技术》和《信息安全法律、道德规范及管理》作为重庆大学出版社信息安全丛书的开篇出版,以起抛砖引玉之作用。

本书共 5 章,第 1 章介绍网络基础知识,对各种网络拓扑和技术进行了全面介绍,并着重对与信息安全有关的子网络、TCP/IP 协议栈以及 IPv6 等概念和技术进行了系统介绍;第 2 章介绍信息安全的若干基本概念;第 3 章在从理论上介绍密码学的基础上,着重对加密技术、数字签名技术以及散列算法等在信息安全的机密性、完整性、访问控制、鉴别和抗抵赖等方面的应用进行了介绍,注重理论与实践的结合;第 4 章介绍常用计算机的主流操作系统的安全问题及其解决办法,并附示例以便于实践;第 5 章介绍信息系统安全体系结构问题,在对信息、信息技术和信息系统的沿革和现实定义进行系统介绍的基础上,对信息系统及其组件的脆弱性和漏洞以及其面临的威胁进行了分层分类介绍,并介绍了导出安全需求的方法,紧接着按照开放系统互联安全体系、互联网络安全体系和信息系统安全体系的逻辑关系层层提升,系统地介绍了信息系统安全体系的结构、安全服务的配置原理和技术方法。

本书第 1,2 章由罗万伯主笔完成,第 3 章由刘嘉勇主笔完成,第 4 章由罗万伯和韩立共同编写,戴宗坤修改完成,第 5 章由戴宗坤和欧晓聪共同完成。全书由戴宗坤和罗万伯审校定稿。在此对为本书出版提供帮助的所有人,表示衷心的感谢!

本书可作为信息安全专业技术培训教材,亦可作为信息安全和计算机应用本专科教材,并对从事信息安全管理、信息系统管理以及信息安全咨询服务的专业技术人员具有很高的使用价值和参考意义。

由于作者水平和时间限制,书中难免会有需要商榷之处,恳请读者不吝赐教。

编　者

2004 年 8 月

目 录

1 网络基础 …… 1

1.1 通信模型 …… 2

1.1.1 简单通信模型 …… 2

1.1.2 数据通信 …… 4

1.1.3 数据通信网络连接 …… 5

1.1.4 交换方式 …… 5

1.2 计算机网络概述 …… 8

1.2.1 计算机网络的定义 …… 8

1.2.2 计算机网络的发展阶段 …… 9

1.2.3 计算机网络的分类 …… 10

1.3 计算机网络的组织结构 …… 15

1.3.1 基本结构 …… 15

1.3.2 网络的硬件与软件系统结构 …… 16

1.3.3 计算机网络的拓扑构型 …… 19

1.4 网络体系结构 …… 22

1.4.1 网络体系结构概述 …… 22

1.4.2 计算机网络结构的模型 …… 24

1.5 TCP/IP 协议 …… 31

1.5.1 IP 协议 …… 31

1.5.2 UDP 协议 …… 36

1.5.3 TCP 协议 …… 37

1.6 IPv6 …… 38
1.6.1 IPv6 简介 …… 38
1.6.2 IPv6 包 …… 39
1.6.3 IPv6 地址 …… 39
2 信息安全概述 …… 41
2.1 基本概念 …… 42
2.2 常见的安全威胁与攻击 …… 46
2.2.1 窃取型攻击 …… 46
2.2.2 非法访问 …… 47
2.2.3 恶意攻击 …… 48
2.2.4 社会学工程 …… 51
2.2.5 计算机病毒 …… 52
2.3 信息安全问题溯源 …… 52
2.3.1 自然及物理安全问题 …… 52
2.3.2 方案设计缺陷 …… 53
2.3.3 系统安全漏洞 …… 53
2.3.4 人为因素 …… 54
2.4 网络通信的威胁 …… 56
2.5 信息安全对策 …… 58
2.5.1 基本对策 …… 58
2.5.2 信息安全模型 …… 60
3 密码技术 …… 85
3.1 密码学的发展 …… 86
3.2 密码学的基本概念 …… 87
3.2.1 密码学的主要任务 …… 87
3.2.2 密码学的基本要素 …… 87
3.2.3 密码体制的原则 …… 90
3.3 密码体制 …… 90
3.3.1 对称密码体制 …… 91
3.3.2 非对称密码体制 …… 96
3.4 网络中的两种主要加密方式 …… 100
3.4.1 链路加密 …… 100
3.4.2 端—端加密 …… 101
3.5 密钥管理 …… 102

3.5.1 密钥的管理问题 …… 102
3.5.2 密钥的种类和作用 …… 103
3.5.3 密钥的生成 …… 105
3.5.4 密钥的分配、注入、存储与更换 …… 105
3.5.5 公钥管理与 PKI …… 108
3.6 散列函数与数字签名 …… 111
3.6.1 散列函数 …… 111
3.6.2 数字签名 …… 113

4 操作系统安全 …… 119

4.1 操作系统与计算机安全 …… 120
4.1.1 普通操作系统 …… 120
4.1.2 可信操作系统 …… 122
4.1.3 操作系统的安全级别与安全操作系统 …… 125
4.2 主流操作系统的安全特性 …… 126
4.2.1 操作系统的典型缺陷 …… 126
4.2.2 UNIX 系统的安全特性 …… 127
4.2.3 Linux 系统的安全特性 …… 134
4.2.4 Windows 系统的安全特性 …… 140
4.3 Windows 2000 服务器的安全 …… 143
4.3.1 Windows 2000 服务器安全技术简介 …… 143
4.3.2 Windows 2000 Server 的安全配置 …… 150
4.4 Windows XP 系统安全 …… 156
4.4.1 Windows XP 系统新的安全特性 …… 156
4.4.2 Windows XP 系统的安全设置建议 …… 159
4.4.3 Windows XP 系统的防火墙功能 …… 161
4.4.4 配置 Windows XP 的安全策略 …… 162

5 信息安全体系结构 …… 165

5.1 信息系统安全体系 …… 166
5.1.1 开放系统互联安全体系结构 …… 166
5.1.2 信息系统安全体系框架 …… 177
5.2 安全服务和技术基础知识 …… 180
5.2.1 鉴别框架 …… 181
5.2.2 鉴别信息和设备 …… 187
5.2.3 访问控制框架 …… 191

5.2.4 抗抵赖框架 …… 205
5.2.5 机密性框架 …… 211
5.2.6 完整性框架 …… 217
5.2.7 安全审计和报警框架 …… 222
5.2.8 密钥管理框架 …… 222

参考文献 …… 233

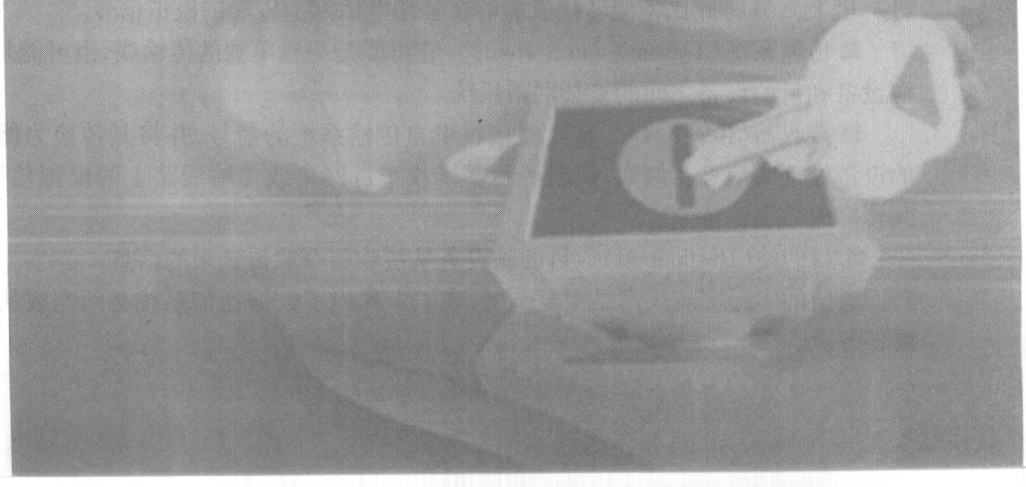
附录 …… 235

附录1 信息安全常用缩略语 …… 236
附录2 名词与术语 …… 249

1

网络基础

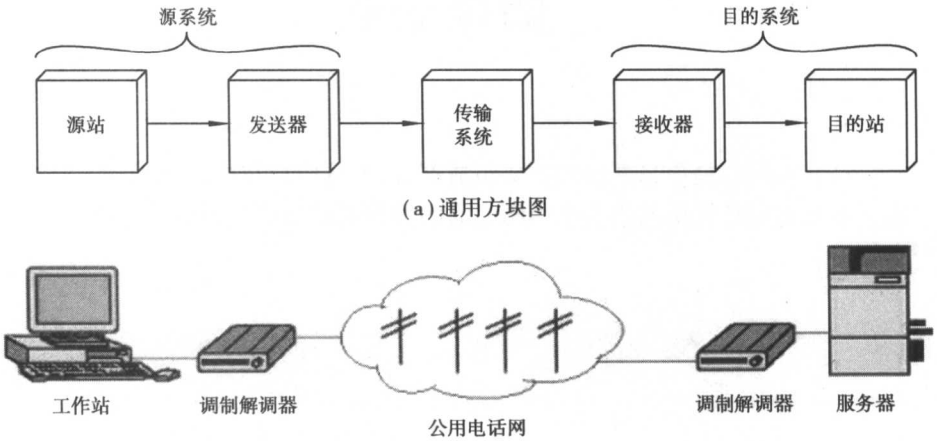
计算机网络是信息系统的重要组成部分，大量信息在网络中处理、存储和传输。本章将对计算机网络安全中所必需的网络基础知识进行简单介绍。



1.1 通信模型

1.1.1 简单通信模型

一个通信系统要达到的最基本目的就是完成双方的数据交换，这可以通过一种简单的通信模型来说明（如图 1.1 所示）。



(a) 通用方块图

(b) 示例

图 1.1 简单通信模型

这个简单的通信模型中有几个要素，分别是：

■ 源站（Source） 源站设备产生传输的数据，例如电话机和个人计算机。

■ 发送器（Transmitter） 通常源站生成的数据不会以它最初生成时的格式直接传输，而是通过一个发送器将这些信息转化并编码成能够在各种传输系统中进行传输的电磁信号。例如，调制解调器从与之相连的设备上获得一个数字比特流（如从个人计算机上），并将此比特流转化成能够在公用电话网上传输的模拟信号。

■ 传输系统（Transmission System） 它可能是一根单独的传输线，也可能是连接在源设备和目的设备之间的复杂网络系统。

■ 接收器（Receiver） 接收器接收来自传输系统的信号，并将其转换为能够被目的设备处理的信号。例如，调制解调器接收来自网络或传输线路上的模拟信号，并将其转换成数字比特流。

■ 目的站（Destination） 目的站设备从接收器获取传送来的信息。

通信的实际实现技术是很复杂的，表 1.1 列出了数据通信系统必须完成的一些主要任务。

图 1.1(b)为工作站和服务器之间通过公用电话网进行通信的示意图;更为简单的例子是在两部电话机之间通过同样的网络来交换话音信号。

表 1.1 通信的主要任务

	任 务	内 容
1	传输系统的利用	指的是如何充分利用传输设施,通常传输设施会被多个正在通信的设备共享,有多种技术(称为复用)可在多个用户之间分配传输系统的总传输能力。为了保证传输系统不会因过量的传输服务请求而超载,就需要引入拥塞控制技术
2	接口	即传输系统的接口。实际上,计算机通信离不开在传输媒体上传播的电磁信号。因此,一旦有了接口,要进行通信还需要信号的产生。信号的性质,如信号格式及信号强度,必须做到 2 点:①能够在传输系统上进行传播;②能够被接收器转换为数据
3	信号的产生	
4	同步	仅根据传输系统和接收器的要求生成信号还是不够的,必须要在发送器和接收器之间达成某种形式的同步。如接收器必须能够判断信号在什么时候开始到达,什么时候结束,以及每个信号单元的持续时间等
5	交换管理	要使双方顺利通信,除了决定信号的特性和定时这些基本要求之外,系统还要收集很多其他信息,一般归纳为“交换管理”。如果在一段时间内数据的交换是双向的,那么双方必须合作。例如,双方进行电话交谈,一方必须拨打另一方的电话号码,拨号产生的信号引起被叫方电话振铃。被叫方拿起电话双方就完成了连接。对数据处理设备来说,仅仅建立简单的连接还不够,在此基础上必须还完成其他一些协商工作,如同步问题
6	差错检测和纠正	差错检测和纠正以及流控制也可看作交换管理,但由于十分重要,有必要将它们独立分列出来。任何通信系统都有出现差错的可能,如传送的信号在到达终点之前失真过度。在不允许出现差错的环境中就需要有差错检测和纠正机制,这种情况通常发生在数据处理系统中
7	流控制	为了保证目的站设备不会因源站设备数据发送太快以致无法及时接收和处理而导致超载,就需要流控制
8	寻址	寻址和路由选择是两个相关但又截然不同的概念。当传输设施被两个以上的设备共享时,源站系统必须给出其目的站系统的标识。传输系统必须保证只有目的站系统才能接收到数据。此外,传输系统本身还可能是一个复杂的网络系统,那么还必须在这个网络中选择某条特定的传输路径
9	路由选择	
10	恢复	恢复(Recovery)与纠错(Error Correction)是两种不同的概念。当信息正在交换(如数据库处理或文件传输)时,由于系统发生故障而导致传输中断,那么就需要使用恢复技术。它的任务就是从中断处开始继续工作,把系统被涉及的部分恢复到数据交换开始之前的状态
11	报文的格式化	它是双方必须就数据交换或传输的格式达成一致的协议。例如,双方都使用同样的二进制字符编码
12	安全措施	在数据通信系统中采取某些安全措施常常是很重要的。例如,发送数据方可能希望确保只有它期望的接收方才能接收到数据,而数据接收方则可能希望保证接收到的数据在传送过程中没有被改变过,且此数据确实来自正确的发送方
13	网络管理	数据通信系统是一个十分复杂的系统,它不可能自动创建或运行,需要各种网络管理来设置系统,监视系统状态,在发生故障和过载时进行处理,并为系统进一步发展进行合理的规划

1.1.2 数据通信

为了更加形象地说明数据通信，将从一个新的角度来考察图 1.1(a)中的通信模型(如图 1.2 所示)。

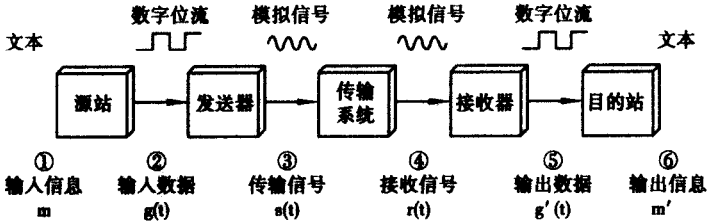


图 1.2 从一个新的角度考察通信模型

假设图 1.2 中的输入设备和发送器都是一台个人计算机的组件，使用这台 PC 机的用户希望向另一用户发送一条消息 m。用户激活 PC 机上的电子邮件程序，并用键盘(输入设备)录入这条消息。此时字符串暂时保存在主存储器里，将此字符串视为主存储器中的一比特序列 g。PC 机通过 I/O 设备(如局域网收发器或调制解调器)与某种传输媒体(如局域网或电话线)相连接。输入的数据以一连串高低变化的电压 g(t)的形式传递给发送器，这个电压变化代表了某些通信总线或缆线上的比特序列。发送器直接与传输媒体相连，并将输入的电压序列 g(t)转换成适于传输的模拟信号 s(t)。

传输媒体上传送的模拟信号 s(t)在到达接收器之前会受到多种形式的损伤。因此，接收到的信号 r(t)很可能与 s(t)不完全相同。接收器将根据 r(t)以及它对该传输媒体的了解，尽力估算出 s(t)的原貌，并转换比特序列 g′(t)。这些比特序列 g′(t)被送到输出端的个人计算机上，在这里它们以比特块 g′的形式暂存在主存储器中。一般情况下，目的站系统会试图判断是否有差错产生，如果有，它将与源站系统合作，并最终获得没有差错的完整数据块。然后，通过输出设备(如打印机或屏幕)将这些数据展现在用户面前。在正常情况下，用户看到的消息 m′是与原消息 m 完全一样的副本。

现在假设电话交谈的情况。在这种情况下，消息 m 以声波的形式输入电话机。电话机将声波转换成同频率的电信号，这些信号不经过任何形式的改变直接在电话线上传输。因此，输入信号 g(t)与被传输的信号 s(t)是一致的。信号 s(t)在传输媒体上会产生某些形式的失真，因此接收到的信号 r(t)与 s(t)并不完全一样。然后，信号 r(t)不经过任何形式的差错纠正或信号质量的提高，直接被转换成回声波。因此 m′与 m 并不完全一致。但是，对收听者来说，接收到的声音消息通常是可以理解的。

实际应用时，还涉及到数据通信的其他几个关键性问题，包括控制数据流并检测纠错的数据链路控制技术，以及用于提高传输效率的复用技术等。

1.1.3 数据通信网络连接

一般说来,两个通信设备点对点地相互直接连接在事实上是不可行的。例如:

①两个设备之间的距离很远。如要在两台相距几千千米远的设备之间用一条专线连接,其花费将惊人地昂贵。

②有一组设备,例如全世界的所有电话机或是某个组织拥有的所有终端和计算机,其中每台设备都可能需要在不同的时间与不同的设备连接。除非设备很少,否则要在每两台设备之间提供一条专线是不实际的。

解决此问题的办法是将所有设备都连接到一个通信网络上。图 1.3 表示图 1.1(a)的通信模型在这种情况下的模型,同时图 1.3 也展示出通信网络被传统地分为两大类:广域网(WAN)和局域网(LAN)。广域网和局域网的概念,将稍后讨论。近年来,不管是从技术的角度还是从应用的角度,这两种网络之间的区别已经变得越来越模糊,但不管怎样,对这种划分的讨论还是很有用的。

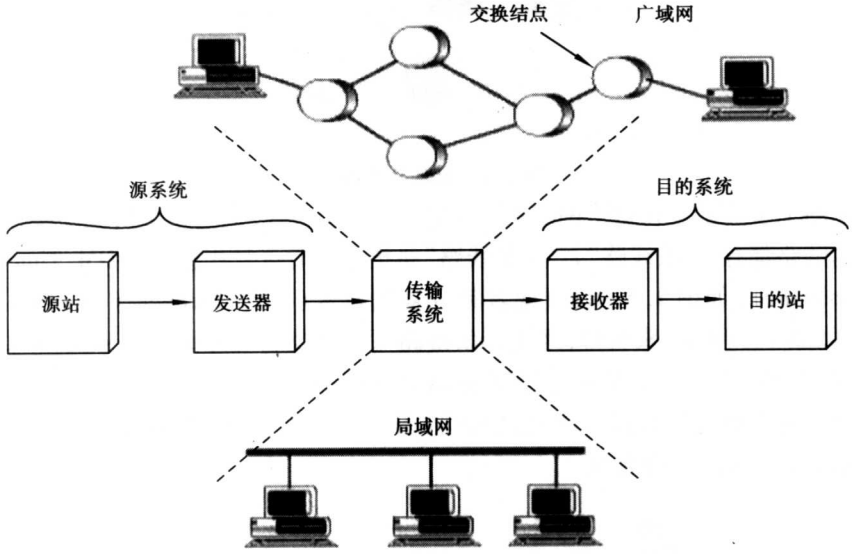


图 1.3 简化的网络模型

1.1.4 交换方式

目前,用于数字通信网的交换方式包括电路交换、报文交换、数据包交换 3 种,每种交换方式均有自己的特点和应用领域。

1)电路交换

在电路交换(Circuit Switching)方式中,交换网根据应用要求将通信终端连接起