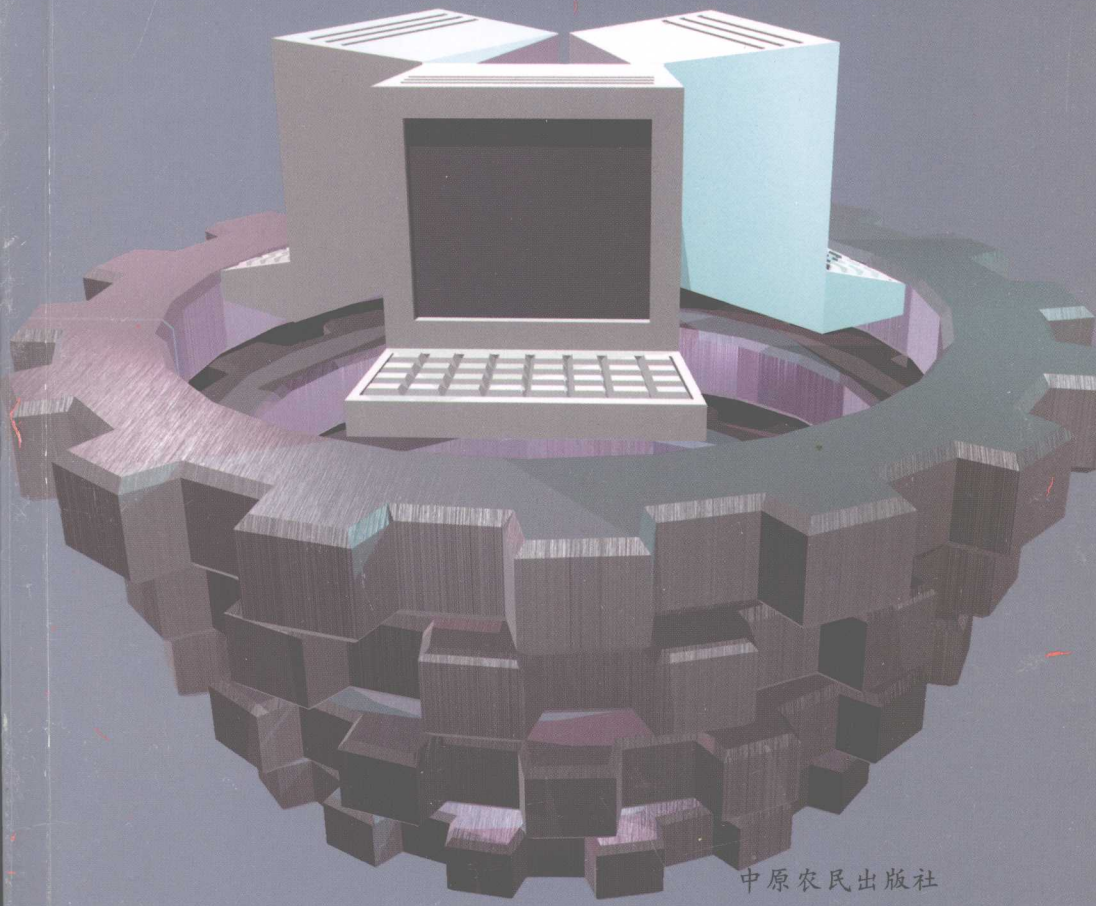
网络安全和网络行为研究

徐向阳 著



中原农民出版社

网络安全和网络行为研究

徐向阳 著

中原农民出版社

图书在版编目(CIP)数据

网络安全和网络行为研究/徐向阳著.—郑州:中原农民出版社,2008.8
ISBN 978-7-80739-338-2

Ⅰ.网… Ⅱ.徐… 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(2008)第 118271 号

出版社:中原农民出版社
(地址:郑州市经五路 66 号　电话:0371—65751257
邮政编码:450002)
发行单位:河南省新华书店
承印单位:河南省诚和印制有限公司
开本:890mm×1240mm　A5
印张:9　**字数**:280 千字
版次:2008 年 8 月第 1 版　**印次**:2008 年 8 月第 1 次印刷

书号:ISBN 978-7-80739-338-2　**定价**:20.00 元
本书如有印装质量问题,由承印厂负责调换

前　言

从世界上第一台计算机诞生到今天互联网的日益普及，计算机的发展速度可谓突飞猛进，从而也把人类文明带入数码时代。计算机网络的出现，使人们在获取和传递信息时，又多了一种选择，而且是一种能够提供空前“自由化”的选择。它使信息的传播速度、质量与范围在时间和空间上有了质的飞跃，从而使人们的许多梦想变成了现实。但是，任何事物都是矛盾对立的统一体，尤其对于正在发展中的新事物来说，更是如此。计算机网络也不例外。人们在享受着网络传输带给我们便利的同时，也对日露端倪的网络负面影响越发担忧。

随着计算机在社会各个领域中的广泛应用和快速发展，网络的普及速度超出了人们的想象，通过网络传输、存储和处理的信息呈几何级数增长，网络已经成为信息社会不可或缺的基础设施。但是网络安全以及网络应用安全一直以来都是人们密切关注的焦点，由于网络尤其是 Internet 网络的开放性、系统的缺陷与漏洞、恶意攻击、计算机病毒、工作人员的误操作以及安全意识淡薄等安全威胁的存在，使得基于网络的各种应用如电子商务、电子政务等的安全性受到了严重挑战。因此，加强网络安全管理，提高网络安全性和可用性已经成为关系国家安全、经济发展和社会稳定的一个重大课题，具有重要的战略意义。

网络时代的到来，虚拟空间出现“道德真空”，对传统的社会生活秩序造成很大冲击。2008 年 1 月，中国互联网络信息中心公布的第二十一次中国互联网络发展状况统计报告表明，学生占 2.1 亿网络用户的 28.8%，其中大专以上用户占 34.8%。由此可见，大学生是网络用户的重要组成部分。调查获悉，随着高校信息化进程加快

和校园内网络接入条件改善，大学生的网络行为越来越普遍，上网成为大学生的学习、交往、娱乐等生活的重要内容。同时，由于网络上的犯罪现象越来越多，网络犯罪已成为发达国家和发展中国家不得不关注的社会公共安全问题。据统计，1999 年中国公安机关立案侦查的计算机违法犯罪案件仅为 400 余起，2000 年剧增为2 700余起，2001 年达到4 500余起（其中 90% 以上的计算机违法犯罪案件牵涉网络）。规范网络行为，防治网络犯罪，已成为整个社会必须面对的课题之一。

本书是作者结合多年来对网络安全与网络行为的研究进行编写的。全书共分十章。第一章计算机网络概述，阐述了计算机网络相关的概念、网络分类与功能等基本内容；第二章网络体系结构，在阐述网络体系结构、OSI 模型及 TCP/IP 模型的基础上，重点对 OSI 参考模型与 TCP/IP 参考模型进行了分析与比较；第三章计算机网络安全，重点探讨了网络面临的安全威胁、网络安全内容及安全要素、OSI 网络安全体系结构、TCP/IP 网络安全体系结构及网络安全模型等内容；第四章网络安全技术概述，就网络安全技术所涉及的内容进行了较为详细的讨论，主要包括：信息加密技术、密钥管理、网络加密方式、访问控制技术、防火墙技术、安全扫描技术、入侵检测技术及病毒防范技术等；第五章网络的攻击行为和防范研究，详细介绍了黑客的历史、网络攻击技术的发展与演变、网络攻击与防范的方法、网络攻击与防范模型、网络攻击身份欺骗、网络攻击行为隐藏等；第六章网络行为中的网络犯罪态势，分析了网络犯罪的现状、特点及发展趋势；第七章网络行为中的网络犯罪分析，对网络行为中的网络犯罪原因进行了详细的阐述，重点对侦破和打击网络犯罪的困难进行了分析；第八章立法规范网络行为分析，对规范网络行为的立法问题进行了讨论；第九章网络时代我国高校文化建设面临问题与对策，研究了网络时代我国高校文化建设面临的机遇、问题及应对对策；第十章网络时代我国高等院校思想政治工作研究，对如何在网络时代加强高校学生的思想政治工作进行了探讨。

由于本书涉及内容较多，参考了大量的书籍、论文和网络资源，书后列出了较为详尽的参考文献，但由于涉及面太广，难免挂一漏万，如有遗漏，敬请谅解。限于作者水平有限，书中难免有疏漏和错误之处，恳请读者批评指正。

作　者

2008 年 2 月

目　录

第一章　计算机网络概述 …… 1
第一节　计算机网络的产生与发展 …… 1
第二节　计算机网络定义 …… 5
第三节　计算机网络分类 …… 5
第四节　计算机网络功能 …… 10
第二章　网络体系结构 …… 11
第一节　网络协议 …… 11
第二节　计算机网络的体系结构 …… 12
第三节　OSI 参考模型 …… 14
第四节　TCP/IP 参考模型 …… 20
第五节　两种参考模型的比较 …… 23
第三章　计算机网络安全 …… 25
第一节　网络安全的重要性 …… 25
第二节　网络面临的安全威胁 …… 26
第三节　网络安全内容及安全要素 …… 29
第四节　OSI 网络安全体系结构 …… 31
第五节　TCP/IP 网络安全体系结构 …… 39
第六节　网络安全模型 …… 40
第四章　网络安全技术概述 …… 45
第一节　信息加密技术 …… 45
第二节　密钥管理 …… 53
第三节　网络加密方式 …… 57
第四节　访问控制技术 …… 59
第五节　防火墙技术 …… 65

第六节　安全扫描技术 …… 72
第七节　入侵检测技术 …… 74
第八节　病毒防范技术 …… 77
第五章　网络的攻击行为和防范研究 …… 81
第一节　黑客的历史 …… 81
第二节　网络攻击技术的发展与演变 …… 85
第三节　网络攻击与防范的方法 …… 88
第四节　网络攻击与防范模型 …… 98
第五节　网络攻击身份欺骗 …… 103
第六节　网络攻击行为隐藏 …… 115
第七节　网络攻击的技术分析 …… 126
第六章　网络行为中的网络犯罪态势 …… 141
第一节　网络传播的负面效应分析 …… 141
第二节　网络犯罪的现状 …… 144
第三节　网络犯罪的特点 …… 149
第四节　网络犯罪的发展趋势 …… 153
第七章　网络行为中的网络犯罪分析 …… 156
第一节　网络犯罪的原因 …… 157
第二节　侦破网络犯罪存在的困难 …… 162
第三节　打击网络犯罪的困难 …… 168
第四节　网络犯罪的社会心理因素 …… 171
第八章　立法规范网络行为分析 …… 173
第一节　各国网络犯罪刑事立法比较 …… 173
第二节　我国刑法规定的几种计算机犯罪 …… 183
第三节　防范和打击网络犯罪的立法建议 …… 207
第九章　网络时代我国高校文化建设面临的问题与对策 …… 211
第一节　网络时代给高校思想政治工作带来的机遇 …… 211
第二节　网络时代教育工作者的素养建设 …… 213
第三节　建设健康网络文化的对策研究 …… 221

第四节　网络文化的发展趋势研究…… 228
第十章　网络时代我国高校思想政治工作研究…… 234
第一节　网络时代我国高校学生工作的思考…… 234
第二节　网络时代我国高校肩负着培养千万优秀人才的重任…… 240
第三节　抓住机遇加强思想政治工作的新思路…… 244
第四节　建设良好网络道德和网络行为的建议…… 251
附录一…… 257
附录二…… 261
附录三…… 264
附录四…… 269
参考文献…… 275

第一章　计算机网络概述

目前，人类社会正在从工业经济时代转向知识经济时代，知识经济时代的一个重要特征就是数字化、信息化和全球化，而信息化和全球化实现的核心基础离不开计算机网络。网络已经成为衡量一个国家综合实力的重要标志，它的产生与发展已经对人类社会的政治、经济、文化、科学技术和社会生活产生了深刻影响。

第一节　计算机网络的产生与发展

计算机网络是计算机技术与通信技术相互渗透、密切结合的产物，是人类社会进步和发展的一个显著标志。计算机网络经历了从简单到复杂，从低速到高速，从局部应用到全球范围的发展过程。众所周知，计算机是信息加工和处理的工具，具有速度快、精度高、存储容量大等显著特点。但是，单个计算机的处理能力无法满足远距离的信息加工处理和共享要求，而通信技术为远距离的信息传递和共享提供了可能，将二者相互结合，既能够实现信息的加工处理、远程传递和共享，又能够满足提高计算机系统性能、增强可靠性和可用性的要求。因此，随着计算机技术与通信技术的相互融合渗透，就产生并逐渐形成了计算机网络。

计算机技术与通信技术的发展融合，为计算机网络的产生奠定了技术基础，而强烈的社会需求则是推动计算机网络产生与发展的最重要因素。计算机网络的诞生最早可以追溯到20世纪50年代初由美国麻省理工学院为美国空军设计的SAGE半自动地面防空系统，该系统能够将分布在17个防区内的雷达观测站、机场、防空导弹

和高炮阵通过通信线路连接,形成一个联机的计算机系统。联机的计算机系统被用作辅助决策,自动引导飞机和导弹进行拦截等。

SAGE 系统通常被认为是计算机技术与通信技术相结合的先驱,然而名声最响、影响最大的现代计算机网络(Internet)的鼻祖——ARPANET(阿帕网络)则诞生于 20 世纪 60 年代末,是美苏冷战时期的产物。

ARPANET 是由美国国防部高级研究计划管理局(ARPA,Advanced Research Project Agency)于 1969 年创建的。当时研究的目的是为了对付来自苏联的核攻击威胁,在战争中保障计算机系统工作的不间断性。目标是在军事上建立一个分散的指挥系统,一旦战争爆发,若部分指挥点被摧毁,通过网络使信息仍然能够自动转接到正常工作的指挥点上,使指挥系统仍然能够保持正常运转。

ARPANET 采用分组交换技术,以电话网作为主干网络,最初只连接了 4 台计算机,两年后接入的计算机达到了 15 台。随后 ARPANET 规模的不断扩大,1972 年接入 ARPANET 的计算机达到了 40 多台,1983 年达到了 300 多台。网络跨越了整个美洲大陆,连通了美国东西部的许多高等院校和研究机构,并且利用通信卫星实现了与夏威夷及欧洲等国家和地区的计算机网络系统的连接,同年 ARPANET 建设基本完成。

ARPANET 之所以能有如此大的规模与影响,主要因为它具有如下一些重要特性,而其中的大部分特性通常被认为是现代计算机网络应当具备的基本特性。

(1)采用分组交换技术。

(2)采用专用的通信控制处理机。

(3)采用分层协议。

(4)采用分散控制。

(5)实现了资源共享。

继 ARPANET 之后,从 20 世纪 70 年代开始,西方许多发达国家也纷纷开始建立和发展各自的分组交换式网络。例如,英国邮政局

的 EPSS 公用分组交换网、加拿大的 DATAPAC 公用分组交换网、法国信息与自动化研究所的 CYCLADES 分布式数据处理网等。这些网络的联网目的主要是为了实现远程的数据传输、处理和资源共享，网络的覆盖范围广，接入网络的多数为大型计算机或中小型计算机，这些网络通常被称为广域网。

在分组交换式网络大力发展，并积累了很多经验的同时，20 世纪 70 年代中期出现了局域网。特别是到了 20 世纪 80 年代，随着微型计算机的普及应用，局域网技术得到了空前快速发展。局域网不同于广域网，它以实现共享数据、软件和昂贵的外部设备为主要目的。局域网是将一个单位内部或一个相对独立的局部区域内的各种微型计算机和通信设备连接起来的通信网络。局域网的主要特点是范围小、速度快、可靠性高，被广泛应用于办公自动化、工厂自动化、过程控制、企业管理、辅助教学、军事指挥、医疗管理、银行业务处理和商业信息处理等领域。

从 20 世纪 80 年代初开始，Internet 的发展引起了世人的瞩目。Internet 是一个覆盖全球范围的互联网，它的前身就是 ARPANET。ARPANET 是一个成功的计算机网络系统，它在概念、功能、结构和系统设计等方面为 Internet 的产生和发展奠定了基础。特别是随着 TCP/IP 协议的标准化和公开化，在 ARPANET 中也将 TCP/IP 协议作为网络互连的标准协议，极大地促进了 Internet 的发展。这一阶段是属于 Internet 的实验研究阶段，Internet 以 ARPANET 作为主干网络。

从 20 世纪 80 年代中期至 90 年代中期，Internet 进入了实用发展阶段。在这一时期，NSFNET 取代了 ARPANET 成为 Internet 的主干网络。NSFNET 是由美国国家科学基金会（NFS，National Science Foundation）于 1984 年开始组建的广域网络。NSFNET 所采用的网络硬件技术与 ARPANET 基本相同，但是它在软件技术和体系结构等方面都有了新的发展与突破。NSFNET 也采用基于 TCP/IP 的网络通信协议，它利用层次型结构方法把全美国 5 个超级计算中心的

计算机与分布于全国范围内的大学和研究所的大量的计算机彼此连接起来，构成了一个范围广泛、功能强大的计算机网络系统，并且NSFNET对全社会开放，资源可以为全社会所共享。各大学和研究院所的积极参与，极大地丰富了Internet的信息资源，于是各种Internet信息服务项目（如Gopher、FTP、WWW等）被相继开发出来，使得Internet真正发展成为以信息服务为主要目的的计算机互连网络。由于在这一时期Internet主要用于教育和科研院所的非商业应用，因此网络安全没有引起足够重视，这也给后来基于Internet的商业应用留下了安全隐患。

自20世纪90年代中期开始，Internet呈现出爆炸性增长的发展势头，不仅网络的规模在迅速扩大，而且网络的应用领域也从最初的科研和教育领域扩展到了文化、产业、政治、经济、体育、娱乐、商业及服务业等领域，使得Internet真正发展成为一个国际性的涉及多领域的互连网络。尤其是一些有远见的企业和公司在意识到Internet的商业价值后，纷纷加入Internet，并通过Internet开展产品宣传、技术支持、用户培训、产品销售和服务等工作，进一步推动了Internet的快速发展，使Internet进入了一个商业化阶段。在这一时期，Internet主干网络也由原来的政府资助转变为公司的经营与管理。

综观计算机网络的发展历史，可以看出虽然它的历史并不长，但是它的发展同样经历了从简单到复杂，从低级到高级的发展过程。计算机网络的发展与演变过程大致可以概括为三个基本阶段，即具有通信功能的单一计算机系统阶段、以通信子网为中心的计算机网络阶段和以开放系统互连（OSI，Open System Interconnection）参考模型为代表的采用分层体系结构的计算机网络阶段。

目前，计算机网络进入了一个高速发展的时期，随着计算机技术、通信技术、微电子技术和光电子技术等高新技术的不断创新和迅猛发展，计算机网络正朝着高速化、集成化、多媒体化和智能化等多个方向发展。网格计算、移动网络、网络存储及网络分布式对象计算等已经成为网络新的研究与应用的热点问题，新一代的网络正在酝

酿和发展之中。

第二节　计算机网络定义

在计算机网络发展的不同阶段，人们对计算机网络有不同的需求和认识，因此就产生了不同的定义。一般计算机网络的定义可以分为三类：一是强调信息传输为主要目的，二是强调资源共享为主要目的，三是强调用户透明性为主要目的。而强调资源共享为主要目的的计算机网络定义是目前最常用的定义，也是能够比较准确反映计算机网络基本特征的网络定义。

强调资源共享为主要目的的计算机网络定义是“以能够相互共享资源的方式互连起来的自治计算机系统的集合”。其中，“共享资源”中的“资源”包括硬件、软件和数据等；“互连”是指各计算机之间能够通过某种介质相互连接起来，并且相互之间能够交换信息；“自治”功能是指每台联网的计算机都是一个完整的计算机系统，它能够独立地进行工作，所有的计算机都是平等独立的，任何一台计算机都不能干预其他计算机的工作；“计算机系统的集合”是指计算机网络是由多台计算机组成，是一个计算机系统的集合体。

通过此定义可以看出，计算机网络，首先，是以实现“资源共享”为主要目的；其次，“互连”的计算机可以是分布在不同地理位置的多台具有“自治”功能的“计算机系统的集合”；最后，网络中计算机在信息交换时必须遵循相同的协议。

第三节　计算机网络分类

计算机网络种类繁杂，划分标准也很多，依据不同的分类标准，同一个计算机网络可以划归到不同类型的网络中，如按照网络拓扑结构来划分，网络可以分为星型网、树型网、环型网、总线型网、全连通型网和不规则型网；按照信息交换方式来划分，网络可以分为线路

交换网、报文交换网、分组交换网和信元交换网；按照网络的带宽来划分，网络可以分为窄带网和宽带网；按照网络传输介质来划分，网络可以分为有线网和无线网，等等。以上给出的这些分类标准，大多数只是按照网络的某一方面的特征来划分网络，并不能比较全面地反映计算机网络技术的本质特性。而目前最为常用的网络类型划分标准主要有两大类，即按照网络传输技术分类和按照网络覆盖范围分类。

一、按照网络传输技术分类

计算机网络所采用的传输技术决定了网络的主要技术性能和特点。按照网络传输技术来划分，计算机网络可以分为广播式网络和点对点式网络两类。

1. 广播式网络

广播式网络是用一个共享通信信道把所有的计算机连接起来，网络中任何一台计算机发出的信息都能够被所有其他计算机接收到的计算机网络。目前，大多数的局域网和城域网都采用这种技术，并且以微波、卫星通信方式传播的广域网也采用这种技术。

2. 点对点式网络

在点对点式网络中，一条通信线路只连接两台计算机，直接的数据交换仅仅发生在直接连接的两台计算机之间。在计算机网络中，通常是源计算机与目的计算机之间并没有直接通路，于是源计算机发出的信息一般要经过中间若干节点的转发，才能够到达目的计算机。由于从源计算机到目的计算机的信息传输的路径可能不止一条，并且比较大的报文还需要分解为若干小分组才能够在网络中正常传输，因此，路径选择和分组存储转发是点对点式网络中必须解决的主要问题。目前，大多数的广域网都采用这种技术。

二、按照网络覆盖范围分类

按照网络覆盖范围来划分，计算机网络可以分为局域网、城域网和广域网三大类。

1. 局域网

局域网(LAN,Local Area Network)顾名思义就是局部区域内的网络,它是指在一个有限范围内的各种计算机设备和通信设备互连起来的通信网络。局域网以实现共享数据、软件和昂贵的外部设备为主要目的。

局域网是计算机网络技术中应用最为广泛的技术之一,也是计算机网络技术成功应用的一个范例。局域网常用于政府机关、企事业单位和校园网的组建,接入局域网络的设备主要包括个人计算机、工作站、打印机、扫描仪、绘图仪及各种网络通信设备(如集线器、交换机、路由器)等。目前许多单位都有自己的局域网,甚至有的家庭中也都有自己的小型局域网。

局域网具有速度快、可靠性高、区域有限、组网方便、使用灵活、投资少等特点,可以归纳为以下几个方面:

(1)网络的覆盖范围有限。局域网的覆盖范围小,一般在数千米以内,网络属于一个部门或一个单位所有。网络的覆盖范围与使用的传输介质密切相关,目前局域网常用的传输介质主要有双绞线、同轴电缆和光纤等。使用双绞线和同轴电缆作为网络的传输介质时,网络的覆盖范围在1千米左右。而使用光纤时,网络的覆盖范围可以达到30千米左右。

(2)网络拓扑结构灵活多样。局域网的网络拓扑结构主要采用总线型、环型和星型三种,如图1-1所示。以往采用最多的是总线型网络拓扑结构的局域网,但是20世纪90年代后期随着交换型局域网网络技术的飞速发展,采用星型拓扑结构的局域网已经取代了采用总线型网络拓扑结构局域网的统治地位,成为局域网的主流形式。

(3)传输速率高且误码率低。局域网的传输速率一般为10~100Mb/s,在高速局域网中速率可以达到1 000~10 240Mb/s,误码率在10^{-8}~10^{-11}范围内。它的低延时和高可靠性,能够很好地支持计算机间的高速通信。

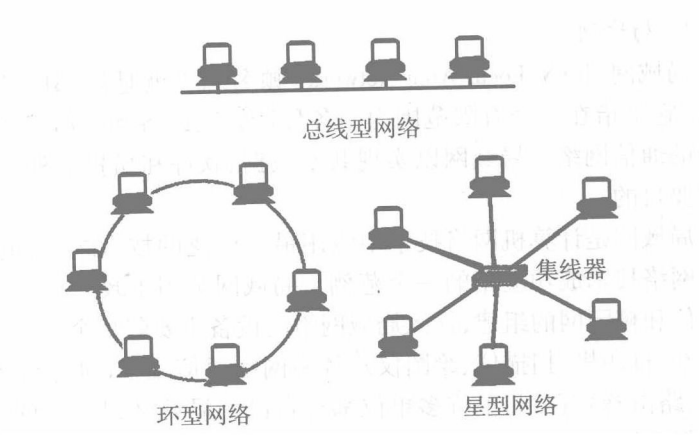


图 1-1　总线型、环型和星型网络拓扑结构

(4)支持多种介质访问控制方式。局域网支持的介质访问控制方式主要有:CSMA/CD(载波侦听多路访问/冲突检测)介质访问控制方式、Token Bus(令牌总线)介质访问控制方式和 Token Ring(令牌环)介质访问控制方式等三种。目前应用最多的是采用广播式的 CSMA/CD 介质访问控制方式的以太网(Ethernet)。

2. 城域网

城域网(MAN, Metropolitan Area Network)顾名思义其网络的覆盖范围是一个大的城市区域,一般在几十千米以内。城域网是一种介于局域网和广域网之间的高速网络,它采用的技术与局域网类似,只是网络的覆盖范围比局域网更大一些,可以说是局域网的延伸,连接的计算机数量更多,一个城域网通常连接着多个局域网。

城域网的主要特征可以归纳为以下几个方面:

(1)网络的覆盖范围较大。城域网的网络覆盖范围在一个大的城市区域内,最大范围一般不超过 100 千米。城域网的建设、使用和管理可以是由一个单位或部门完成,也可以由政府统一规划管理。

(2)网络拓扑结构简单,且采用无竞争的介质访问控制方式。城域网是一种标准成熟、结构简单的计算机网络。其网络标准采用