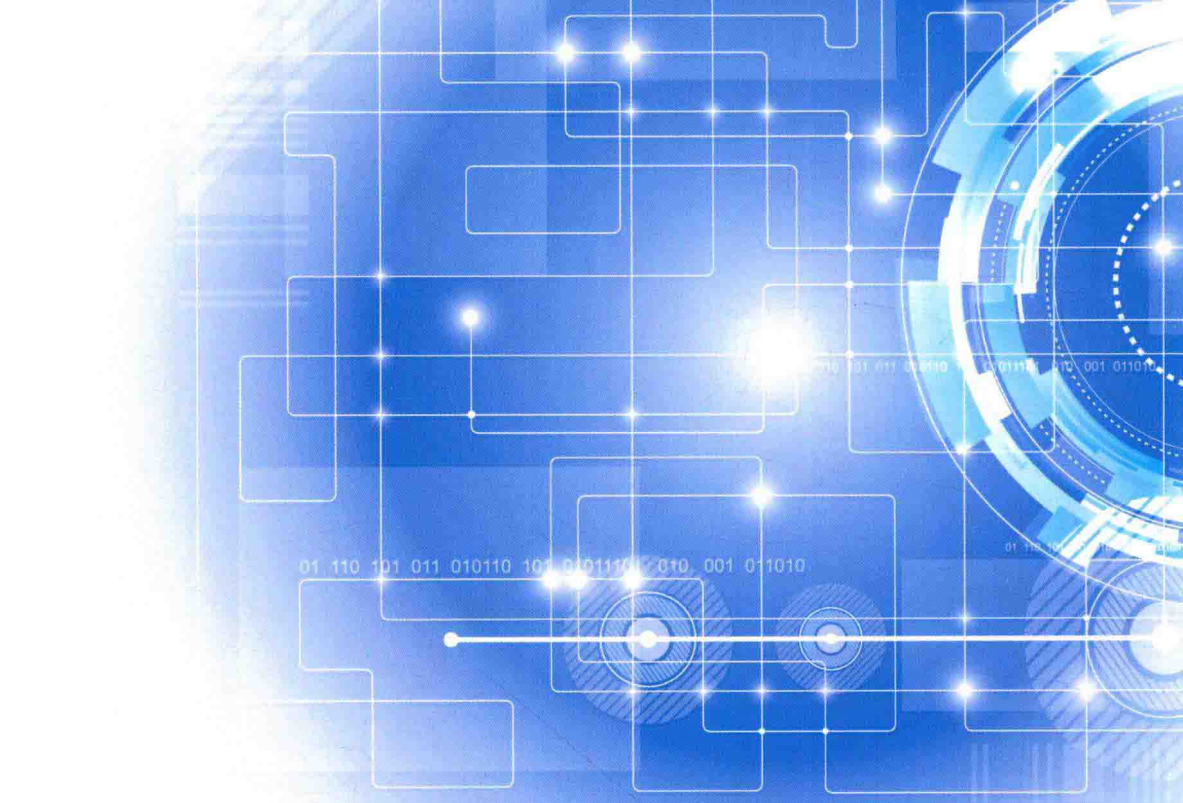

探索计算机网络协议与服务的奥秘

EXPLORING OF THE PROFOUND MYSTERIES OF COMPUTER NETWORK PROTOCOLS AND SERVICES

朱小明　孙　波　张冬慧　王　兵◎著

科学出版社

探索计算机网络协议与服务的奥秘

朱小明　孙　波
张冬慧　王　兵　著

科学出版社
北京

内 容 简 介

本书以协议分析为主线对计算机网络传输和服务展开探秘。在介绍计算机网络各层功能的同时，通过对捕获报文的分析，对每一层协议的工作原理和交互过程进行详细说明。

全书共分 5 章，主要内容有：计算机网络概要、计算机网络体系结构、OSI 和 TCP/IP 参考模型、TCP/IP 协议簇、应用层的 5 种典型应用（DNS、Web、FTP、Telnet、Mail）的协议基础和工作原理、网络测试工具的协议基础和使用、无线网络的基本知识和协议分析。

本书的出版旨在向广大青少年朋友普及网络知识，为国家的创新型人才培养做出贡献。为了让更多的年轻朋友在学习网络协议和服务时，不受抽象的理论困扰，本书选择了一个独特视角，即利用从网络中捕获到的数据来验证理论知识，让枯燥的数字鲜活起来，让读者感到神奇。

图书在版编目（CIP）数据

探索计算机网络协议与服务的奥秘/朱小明等著. —北京：科学出版社，2017

ISBN 978-7-03-051538-4

Ⅰ.①探… Ⅱ.①朱… Ⅲ.①计算机网络-通信协议-青少年读物 Ⅳ. ①TN915.04-49

中国版本图书馆 CIP 数据核字（2017）第 011181 号

责任编辑：吕燕新 王 惠 / 责任校对：刘玉靖
责任印制：吕春珉 / 封面设计：蒋宏工作室

科学出版社 出版
北京东黄城根北街 16 号
邮政编码：100717
http://www.sciencep.com

北京京华虎彩印刷有限公司 印刷
科学出版社发行 各地新华书店经销
*
2017 年 2 月第 一 版 开本：B5（720×1000）
2017 年 2 月第一次印刷 印张：15 3/4
字数：302 000

定价：69.00 元

（如有印装质量问题，我社负责调换〈京华虎彩〉）

销售部电话 010-62136230 编辑部电话 010-62135397-2052

序

《国家中长期教育改革和发展规划纲要（2010—2020年）》中明确提出提升中国青少年的科技创新能力的重要性及迫切性，然而我国在落实青少年科技创新培养方面仍然处于起步阶段。素质教育近年来得到国家和社会的广泛重视，我们强烈地意识到素质教育必须与培养青少年科技创新能力相结合，不仅要对培养方向进行准确定位，还要充分挖掘现代教育理论和教学策略与学科交叉、学科融合实践之间的关系，为培养青少年科技创新能力提供重要的支撑作用。

北京师范大学信息科学与技术学院在完成“基于机器人的中国青少年素质教育提升研究”课题的基础上，申请并获得了国家社会科学基金“十二五”规划2015年度国家一般课题“青少年科技创新能力培养研究”（BCA150050）的研究任务，该课题为我们探索在网络技术的学习和实践中培养青少年科技创新能力提供了良好的契机和平台。

本书是该课题的研究成果之一，用另外一种方式来揭示网络的结构和通信过程。本书的最大特点不是讲给你听，而是做给你看，用在网络中得到的数据包来验证理论知识，让广大青少年了解网络，应用网络，提高创新能力。本书旨在向广大青少年普及网络知识，为国家的人才培养做出应有的贡献。

“青少年科技创新能力培养研究”课题组

2016年11月8日

前　言

信息时代的发展，影响着世界的每一个角落。每个人的生活和工作几乎都离不开计算机。在运行速度越来越快的计算机硬件和日益更新的软件背后，网络作为中枢神经将分布在各地的计算机联系在一起。计算机网络已经成为支持现代社会运行的基础设施，深刻地影响着人们的生活和思维方式。计算机网络技术与应用水平已经成为一个国家经济、文化、科学与社会发展水平的重要标志之一。

目前介绍计算机网络知识的图书很多，大多是从理论知识入手来介绍网络协议和服务。我们认为学习计算机网络要从做中学，因为计算机网络作为一门工程学科，其实践性很强，要想学好网络就要多实践。另外，为了让更多的年轻朋友在学习网络协议和服务时，不受抽象的理论困扰，本书选择了一个独特视角，即利用从网络中捕获的数据来验证理论知识，让枯燥的数字鲜活起来，让读者感到神奇，这是本书的最大特点。

本书以协议分析为主线来组织内容，自底向上分为网络接口层、网际层、传输层和应用层。在介绍各层功能和原理的同时，通过对捕获报文的分析，对每一层协议的工作原理和交互过程进行详细说明。全书共分 5 章，各章主要内容如下：

第 1 章概要介绍计算机网络，包括计算机网络的分类、组成、传输介质等内容。

第 2 章介绍了计算机网络体系结构，讨论了 OSI 和 TCP/IP 参考模型，详细分析了链路层、网络层和传输层的原理、数据报文结构，并且在真实的网络环境中捕获多种报文，解读、分析报文，说明各层协议的工作过程。

第 3 章讨论了应用层的 5 种典型应用（DNS、Web、FTP、Telnet、Mail）的协议基础、工作原理，并且搭建出真实的网络环境，捕获相关报文，解读、分析报文，说明各种应用的工作过程。

第 4 章介绍了几种网络测试工具的使用、协议基础和工作原理，并且捕获相关报文进行解读和分析。

第 5 章介绍无线网络的基础知识、无线局域网的组成和协议分析。

本书具有以下特点：

（1）在内容安排上，循序渐进，深入浅出。

（2）在文字叙述上，简明扼要，通俗易懂。

（3）理论阐述有思考性和启发性，有助于提高读者的创新能力。

（4）实验数据真实、严谨，分析详尽。

本书第 1、2 章由朱小明、孙波撰写，第 3 章由张冬慧撰写，第 4 章由孙波、王兵撰写，第 5 章由张冬慧撰写。全书由朱小明、孙波、张冬慧统稿。

由于著者水平有限，编写时间仓促，书中难免有不妥之处，殷切希望广大读者批评指正。

作　者

2016 年 9 月于北京

目　录

第 1 章　计算机网络技术概述

1.1　计算机网络简介

计算机网络是计算机与通信技术相结合的产物，它是信息高速公路的重要组成部分。计算机网络使人们不受时间和地域的限制，实现资源共享。

1.1.1　什么是计算机网络

计算机网络可以从不同的角度来定义：

- 从技术上讲，计算机网络是计算机技术和通信技术相结合的产物，通过计算机来处理各种数据，再通过各种通信设备和线路实现数据的传输。
- 从组成结构来讲，计算机网络是通过通信设备和连线，将分布在相同或不同地域的多台计算机连接在一起的集合。
- 从应用的角度讲，只要将具有独立功能的多台计算机连接在一起，能够实现各计算机间信息的交换，并可共享计算机资源的系统便可称为计算机网络。

综上所述，将分布在不同地域的一群具有独立功能的计算机通过通信设备和传输介质互连起来，在通信软件的支持下，实现计算机间资源共享、信息交换的系统，称为计算机网络。

图 1-1-1 给出了一个简单网络系统的示意图，它将若干台计算机、打印机和其他外部设备互连成一个整体。连接在网络中的计算机、外部设备、通信控制设备等称为网络结点。

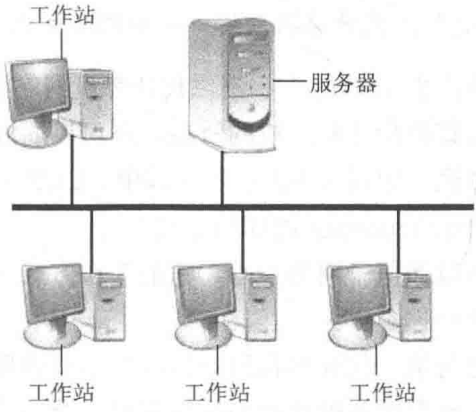

图 1-1-1　一个简单的网络系统

计算机网络从诞生至今经过多次重大的发展，根据不同时期的变化特点可将其分为以下 4 个发展阶段[1]。

1. 面向终端的第一代计算机网络——终端与主机互连

计算机网络产生于 20 世纪 50 年代，随着一种既能发送信息又能接收信息的终端设备（客户端不具备数据的存储和处理能力）的研制成功，实现了将穿孔卡片上的数据通过电话线路发送到远程计算机上。此后，电传打字机也作为远程终端与计算机实现互连，用户可以在远程的电传打字机上输入自己的程序，经计算机处理后，程序又指挥计算机将处理结果传送给电传打字机，并在电传打字机上输出，第一代计算机网络就这样问世了，并形成图 1-1-2 所示的通信形式。

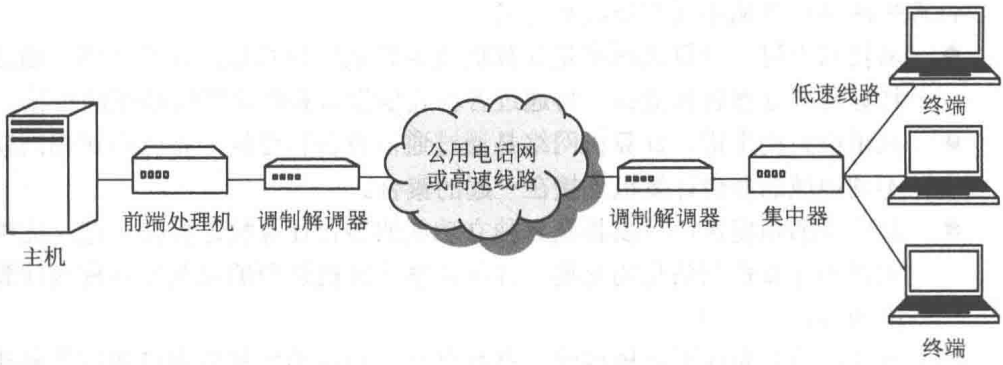

图 1-1-2　以主机为中心

第一代计算机网络是以单个主机为中心、面向终端设备的网络结构。由于终端设备不能为中心计算机提供服务，因此终端设备与中心计算机之间不提供相互的资源共享，网络功能以数据通信为主。

2. 强调整体性能的第二代计算机网络——主机与主机互连

第二代计算机网络产生于 1969 年。第二代计算机网络强调网络的整体性，用户不仅可以共享与网络直接相连的主机的资源，还可以通过通信子网共享其他主机或用户的软、硬件资源，如图 1-1-3 所示（其中，CCP 是指通信控制处理机，即 Communication Controc Processor 的缩写形式）。

第二代计算机网络以通信子网为中心，它的工作方式一直延续至今，即计算机网络=通信子网+资源子网。

第二代计算机网络与第一代计算机网络的区别主要表现在两个方面：其一，网络中的通信双方都是具有自主处理能力的计算机，而不是终端；其二，计算机网络功能以资源共享为主，而不是以数据通信为主。

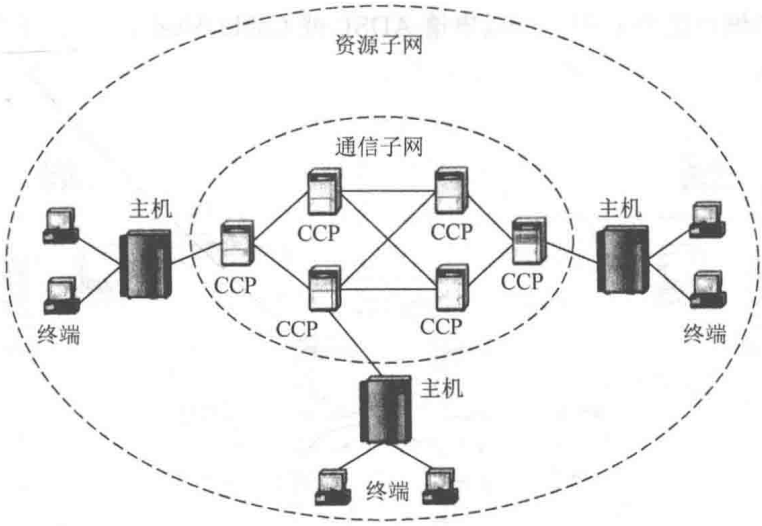

图 1-1-3　以通信子网为中心

3. 以 OSI 模型为基础的第三代计算机网络——网络与网络互连

早期计算机之间的组网是有条件的，即在同一网络中只能存在由同一公司生产的机器和网络设备，不同公司之间的网络不能互连互通。针对这种情况，国际标准化组织（International Organization for Standardization，ISO）于 1977 年设立了专门机构研究解决上述问题，不久后提出了一个使各种计算机能够在世界范围内互连的标准框架，即开放系统互连参考模型（Open System Interconnection/Recommended Model，OSI/RM），简称 OSI 参考模型。OSI 参考模型是一个开放体系结构，它规定将网络分为 7 层，并规定了每一层的功能。OSI 参考模型的出现，标志着计算机网络发展到第三代，如图 1-1-4 所示。

OSI 参考模型的提出，为计算机网络技术的发展开创了一个新的纪元，为计算机网络的互连奠定了理论基础。从此，计算机网络进入了标准化发展阶段。

4. 宽带综合化的第四代计算机网络——多媒体信息互连

第四代计算机网络是在进入 20 世纪 90 年代后，随着多媒体技术和数字通信的出现而产生的，其主要特点是综合化。

综合化是指将多种业务综合到一个网络中实现。例如，将语音、数据、图像等信息以二进制代码的数字形式综合到一个网络中进行传送，这样的网络就称作综合业务数字网（Integrated Service Digital Network，ISDN），电信部门所提供的“一线通”即为 ISDN 的一种通信方式。如果说 ISDN 开创了网络综合化的先河，那么同样以普通电话线作为传输介质的 ADSL（Asymmetrical Digital Subscriber Loop，非对称数字用户环路）技术和以有线电视作为传输介质的线缆调制解调器（Cable Modem）技术的广泛应用，将网络综合化的应用推向了高峰。

如今，许多城市的普通用户可以申请 ADSL 或 Cable Modem 以实现真正意义上的宽带接入。

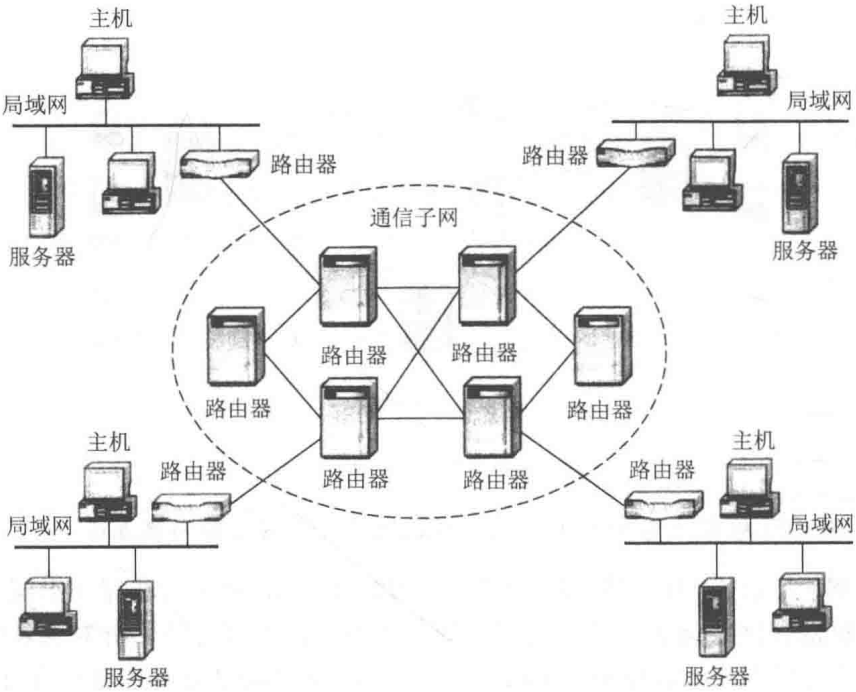

图 1-1-4　第三代开放的计算机网络

网络综合化的另一种形式是“三网合一”。简单来说，“三网合一”是指在宽带环境下，将传统的电信网、广播电视网和计算机网络这 3 个不同信道所实现的不同功能整合到一个信息平台上，提供文字、数据、影视、声音等无所不包的宽带服务，用户可以在一条线、一台电视机上享受打 IP 电话、看电视和快速上网冲浪。三网合一、宽带服务，代表着未来的信息生活。

5. 计算机网络和因特网的历史

计算机网络和因特网的发展可以追溯到 20 世纪 60 年代，当时电话交换网络是在全世界占有绝对统治地位的通信网络。电话网使用电路交换方式将信息从发送方传输到接收方。这种方式使得语音以一种恒定的速率在发送方和接收方之间传递。随着计算机技术的飞速发展，出现了分时计算机，使得很多终端可分时共享 CPU 资源。在很多小型以上的计算机上采用这种工作方式，但是这不是严格意义上的网络。它提出了两个问题：第一是如何更好地让不同地理位置的终端共享 CPU 资源；第二是如何解决通信问题，因为这些用户产生的流量具有“突发性”，有时信息量很大，有时又十分空闲。有人开玩笑说，输入一个命令后，喝一杯咖啡才收到响应。

当时全世界有 3 个研究小组提出了分组交换概念。分组交换技术是一种高效的电路交换的替代技术。这 3 个研究小组彼此并不知道其他小组的存在和工作内容。第一个分组交换技术的首次公开发表是由伦纳德·克兰罗克（Leonard Kleinrock）完成的（1961 年），那时他是美国麻省理工学院的一名研究生。他使用排队论，完美体现了利用分组交换方法处理突发性流量的有效方法。保罗·巴兰（Paul Baran）于 1964 年开始研究分组交换的应用，即在军用网络上安全地传输语音。同时，英国国家物理实验室的唐纳德·戴维斯（Donald Davies）也在研究开发分组交换技术。这 3 个小组的工作奠定了今天的因特网的基础。但是因特网也有很长一段时间的边构建边示范的发展历程。1969 年 11 月，美国国防部高级研究计划署（Advanced Research Projects Agency，ARPA）开始建立一个名为 ARPAnet 的网络，当时只有 4 个结点，分布在加利福尼亚大学洛杉矶分校、加州大学圣巴巴拉分校、斯坦福大学、犹他州大学 4 所大学的 4 台大型计算机。这是因特网的前身。到了 1972 年，ARPAnet 有了 15 个结点。1972 年的计算机通信国际会议首次对它进行了公开演示。第一个在 ARPAnet 端系统间的主机到主机的协议，被称为网络控制协议（NCP）。随着端到端协议的使用，第一个邮件程序于 1972 年诞生。早期的 ARPAnet 主要考虑不同类型的计算机互连。

1972—1980 年，各种不同网络不断涌现，人们开始考虑不同网络的互连问题，由此提出了网络互连的概念，并且提出了将网络连到一起的体系结构，这些体系结构的原则被具体表现在 TCP 中。然而早期的 TCP 和现在的 TCP 有很大的不同。TCP 的早期版本与数据可靠的顺序相结合，有转发功能和重传功能。目前转发功能由 IP 执行，重发功能仍由 TCP 完成。通过实验人们认识到，有些服务是不能用 TCP 完成，后来又发明了 UDP。到 20 世纪 70 年代，网络中最重要的 3 个协议：TCP、UDP 和 IP 都已完成。1983 年 1 月 1 日，TCP 作为新的标准主机协议正式实施，替代了 NCP。到了 20 世纪 80 年代后期，有几个重要的技术得到了应用，首先是拥塞控制技术，其次是 DNS。

1980—1990 年这 10 年中，计算机网络有了飞速的发展，到 20 世纪 70 年代末期与 ARPAnet 相连的计算机有 200 台，到了 80 年代，连接到公共因特网的主机增长到了 1 万台。1985 年，美国国家科学基金会（National Science Foundation，NSF）利用 ARPAnet 建立了用于科学研究和教育的骨干网络（NSFNET）。1990 年，NSFNET 代替 ARPAnet 成为国家骨干网。1987 年 9 月 20 日，钱天白教授通过意大利公用分组交换网在北京发出我国第一封电子邮件，与德国卡鲁斯尔厄大学进行通信，揭开了中国人使用因特网的序幕。

1990—2000 年是因特网发展暴发的 10 年，这主要基于以下技术得到了应用，首先是万维网的出现，它将因特网带入世界上数以千万计的家庭和企业。作为一个

平台，Web 也引入并设置了数百个新的应用程序。网络在教育、股票、银行、流式媒体等行业得到了广泛的应用。1992 年，Internet（因特网）学会成立，该学会把因特网定义为“组织松散的、独立的国际合作互连网络”，“通过自主遵守计算协议和过程支持主机对主机的通信”。1993 年，美国伊利诺伊大学国家超级计算中心成功开发网上浏览工具 Mosaic（后来发展成为 Netscape），使得各种信息都可以方便地网上交流。1993 年克林顿宣布正式实施美国国家信息基础设施计划。

这个时期在因特网上也有其他服务得到应用，如 BBS、FTP 和 Telnet 等服务。此时计算机也从神坛上走下来，计算机应用从一门科学转换为计算机文化，人们无论男女老幼、各行各业都在使用计算机。从目前来看，计算机网络技术的发展远远跟不上应用的发展。当前没有一个领域不用计算机网络，而且计算机网络在各个领域得到极大的发展。

1.1.2　计算机网络的主要功能

计算机网络的功能主要体现在数据通信、资源共享、增强可靠性和分布式处理 4 个方面。

1. 数据通信

数据通信是计算机网络最基本的功能，主要完成网络中各个结点之间的信息交换。如文件传输、IP 电话、E-mail、视频会议、信息广播、交互式娱乐、电子商务、远程教育等活动。

2. 资源共享

网络上的资源包括硬件、软件和数据（数据库）资源。网络内的各种输入/输出设备、大容量的存储设备、高性能的计算机等都是可以共享的网络资源，对于一些价格昂贵又不经常使用的设备，可通过网络共享提高设备的利用率和节省重复投资。

网上的数据库和各种信息资源是共享的主要内容。任何用户都不可能把需要的各种信息收集齐全，况且也没有必要这样做，计算机网络提供了这样的便利，全世界的信息资源都可通过 Internet 实现共享。

3. 增强可靠性

利用计算机网络可替代的资源，可提供连续的高可靠服务。在单一系统内，单个部件或计算机的失效会使系统难于继续工作。但在计算机网络中，每种资源（尤其是程序和数据）可以存放在多个地点，而用户可以通过多种途径来访问网络内的某个资源，从而避免了单点失效对用户产生的影响。

4. 分布式处理

所谓分布式处理是指在分布式操作系统的统一调度下，各计算机协调工作，共同完成一项任务，如并行计算。这样可将一项复杂的任务划分成许多部分由网络内的各计算机分别完成，从而使整个系统的性能大大提高。

1.1.3 计算机网络的拓扑结构

拓扑学是几何学的一个分支。拓扑学首先把实体抽象成与其大小、形状无关的点，将连接实体的线路抽象成线，进而研究点、线、面之间的关系，从而使人们对实体有明确的全貌印象。例如，人们看到铁路交通图、航空线路图等。计算机网络的拓扑结构是网络中的结点（计算机或设备）和通信线路的几何排列形式。

计算机网络有很多拓扑结构，最常用的网络拓扑有如下几种。

1. 总线型结构

总线型结构采用一条通信线路（总线）作为公共的传输通道，所有的结点都通过相应的接口直接连接到总线上，并通过总线进行数据传输，如图 1-1-5（a）所示。

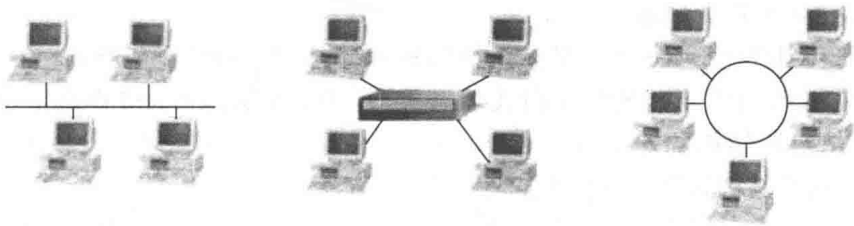

图 1-1-5　总线型、星形、环形结构

总线型网络使用广播式传输技术，总线上的所有结点都可以发送数据到总线上，数据沿总线传播。但是，由于所有结点共享同一条公共通道，在任何时候只允许一个站点发送数据。当一个结点发送数据并在总线上传播时，数据可以被总线上的其他所有结点接收。各结点在接收数据后，分析目的物理地址再决定是否接收该数据。同轴电缆以太网就是这种结构的典型代表。

总线型拓扑结构具有如下特点：

- 结构简单灵活，易于扩展；共享能力强，便于广播式传输。
- 网络响应速度快，但负荷重时性能迅速下降；局部结点故障不影响整体，可靠性较高。但是，若总线出现故障，则影响整个网络。
- 易于安装，费用低。