新一代计算机与人工智能系列新形态教材

计算机网络

顾翔　王进　曹利　编著

南京大学出版社

内容简介

计算机网络是在不断设计方案解决网络通信各种问题的过程中发展起来的技术，本教材充分考虑计算机网络的课程特点，还原问题场景，以计算机网络通信中要解决的核心关键问题为引领，层层递进，逐步展开。本教材通过设问引导读者思考，然后阐述协议标准给出的解决方案，最后引导读者反思比较多种方案优缺点，讨论在多种方案中标准为什么选择现行协议。以这样的编排方式培养读者分析问题、解决问题的能力。

全书共分为九章，分为概述、物理层、数据链路层、网络层与 IP 协议、路由协议、传输层与 TCP 协议、TCP 的流量控制与拥塞控制、应用层以及计算机网络安全。该书可作为应用型本科高校计算机与人工智能相关专业使用。

图书在版编目(CIP)数据

计算机网络/顾翔，王进，曹利编著. -- 南京：
南京大学出版社，2026.8. -- ISBN 978-7-305-30326-5

Ⅰ. TP393

中国国家版本馆 CIP 数据核字第 20268EX527 号

出版发行　南京大学出版社
社　　址　南京市汉口路 22 号　　邮　　编　210093

书　　名　**计算机网络**
　　JISUANJI WANGLUO
编　　著　顾　翔　王　进　曹　利
责任编辑　刘　飞　　编辑热线　025－83592146

照　　排　南京布克文化发展有限公司
印　　刷　南京人文印务有限公司
开　　本　787mm×1092mm　1/16 开　印张 21.5　字数 497 千
版　　次　2026 年 8 月第 1 版　2026 年 8 月第 1 次印刷
I S B N　978-7-305-30326-5
定　　价

网　　址　http://www.njupco.com
官方微博　http://weibo.com/njupco
微信服务号　NJUYUNSHU
销售咨询热线　025－83594756

前言 PREFACE

自从计算机网络技术诞生以来，人类社会的生产模式、生活方式乃至社会结构都发生了巨大改变。近十年，移动互联网的高速发展，催生了众多新兴行业和商业模式。如今工业互联网、智能制造、智慧城市等各类现代工程系统，都依赖以网络为底层平台的联网协同。立足《教育强国建设规划纲要(2024—2035年)》战略部署和新工科建设发展要求，顺应新一轮科技革命与产业变革趋势，理工科专业学生无论主修方向为何，都有必要了解和掌握计算机网络的基本知识和数据传输的工作原理，以期在日后工作中，能够更好地理解和设计现代工程系统中的信息交互过程，适应万物互联时代的工程技术要求，有效利用网络资源优化系统设计与运维，更好服务新时代高等工程教育人才培养和教育强国建设大局。

计算机网络是计算机相关专业的一门核心专业课程，同时也是新工科背景下人工智能、物联网、智能制造等新兴交叉专业的重要基础课程，国内外已经出版过不少经典教材。本书编者在数十年的课程教学实践中，也曾经先后选用过多种版本的教材。这些教材各有其值得称道之处，但在实际使用中都或多或少存在一些问题。有鉴于此，我们对标教育强国建设对高校教材建设、新工科创新人才培养的总体要求，在总结课程教学经验的基础上，编写了此教材。在教材编写过程中，力求做到：

(1) 精炼课程内容。以数据封装和传输为主线，以通信协议为核心知识点，引导帮助学生理解“从发送端到接收端”的协议交互逻辑与数据流转过程，避免陷入技术细节，分散难点，使学生能够在有限学时内建立起清晰的网络通信整体框架。此外，在每章最后还附有本章知识点的思维导图。

(2) 精选课程习题。每章都附有20～30道的习题供学生作业使用。这些习题是从历年考研试卷或是教材习题集中精选出来的，难易程度适当，充分映射各章知识点，帮助学生更好掌握课程内容。

(3) 启发学生思考。从阅读与自学教材的角度，在各小节适当位置设置了多个思考性问题，让学生能够从功能实现者、协议设计者的角度来考虑问题，体会前人设计方案的精妙之处，逐步培养学生思考问题、解决问题的能力。

(4) 融入课程思政。紧扣《教育强国建设规划纲要(2024—2035年)》立德树人根本任务，从多个维度展现我国互联网从追赶到引领的奋斗历程，潜移默化地拓宽学生国际视

野，培育其参与全球互联网治理的使命担当，树立网络安全和国家安全的意识，力求实现“知识学习、能力培养与价值塑造”的同向同行。

本书为课程的理论部分，按五层体系结构展开，全书共分为九章，讲授约需 32～48 学时。第 1 章概述，主要讲述计算机网络的基本概念、体系结构与性能指标；第 2 章物理层，主要讲述数据通信基本概念、信道极限传输速率、复用技术与常用传输介质；第 3 章数据链路层，主要讲述点对点信道和广播信道的链路层数据封装与传输；第 4 章网络层与 IP 协议，主要讲述网络层协议与 IP 数据分组转发；第 5 章路由协议，主要讲述基本路由算法、内部网关协议、外部网关协议；第 6 章传输层与 TCP 协议，主要讲述 UDP 协议、TCP 协议及可靠传输问题；第 7 章 TCP 的流量控制与拥塞控制，主要讲述流量控制策略以及拥塞控制算法；第 8 章应用层，主要讲述多种网络应用；第 9 章计算机网络安全，主要讲述常用加密算法、数据加密应用技术、安全协议和安全法规。

我们另外编写了《计算机网络综合实训教程》一书作为课程的实验教材，形成理论与实训融合的完整教学体系，契合新工科产教融合、理实一体的育人理念。

本书由王进、曹利、何海棠、陈亮、顾翔、王丹丹、魏晓宁编写，由顾翔、王进、曹利统筹审稿。南通大学人工智能与计算机学院部分 2024 级和 2025 级研究生帮助完成了插图绘制工作。

本书可供普通高等学校计算机类、电子信息类专业本科生用作计算机网络课程的理论教材，也可供新工科相关新兴专业及其他理工科专业本科生自学使用。

在本书编写和出版过程中，得到了南通大学高质量教材建设培育专项的资助；南通大学人工智能与计算机学院、南通理工学院用友数智学院和信息工程学院的各位教师也提出了诸多宝贵意见；南京大学出版社给予了大力支持，在此表示衷心感谢！

由于时间紧迫和水平有限，书中难免存在不妥之处，真诚希望使用本书的读者能够给予批评指正。

编　者

2026 年 5 月

目 录 CONTENTS

第 1 章

概　述

在当今时代，计算机网络已深度融入日常生活方方面面，成为现代社会的神经中枢，支撑着社会各领域的高效运转。清晨醒来，我们通过手机上的新闻客户端浏览世界各地的时事资讯，这些信息从新闻服务器跨越千山万水瞬间呈现在我们眼前；上班途中，我们使用导航应用，实时获取交通路况，规划最优路线，背后是交通信息系统与地图服务器的数据交互；到了办公室，我们通过公司内部网络访问共享文件，与同事进行线上协作办公，还能借助视频会议系统与远程的合作伙伴沟通交流。企业依靠网络管理全球供应链，实现高效的生产与配送；科研机构通过网络共享实验数据，协同开展前沿研究。

这些司空见惯的场景表明，计算机网络就如水和电一样，无时无刻不在保障我们的生活，已经成为信息时代的关键基础设施。因此，我们有必要对计算机网络系统的结构和工作原理进行深入学习。

在本章概述中，我们将首先梳理计算机网络的基本概念，涵盖其发展历程、核心定义、主要功能及分类方式；同时，深入剖析计算机网络的体系结构，包括网络的组成要素、经典的 OSI 参考模型与 TCP/IP 参考模型，以及与之相关的协议、接口、服务等关键概念；此外，还将系统介绍网络的各类性能指标，重点阐释时延、带宽、速率等核心参数。

本章重点：

（1）计算机网络的概念、组成与分类；

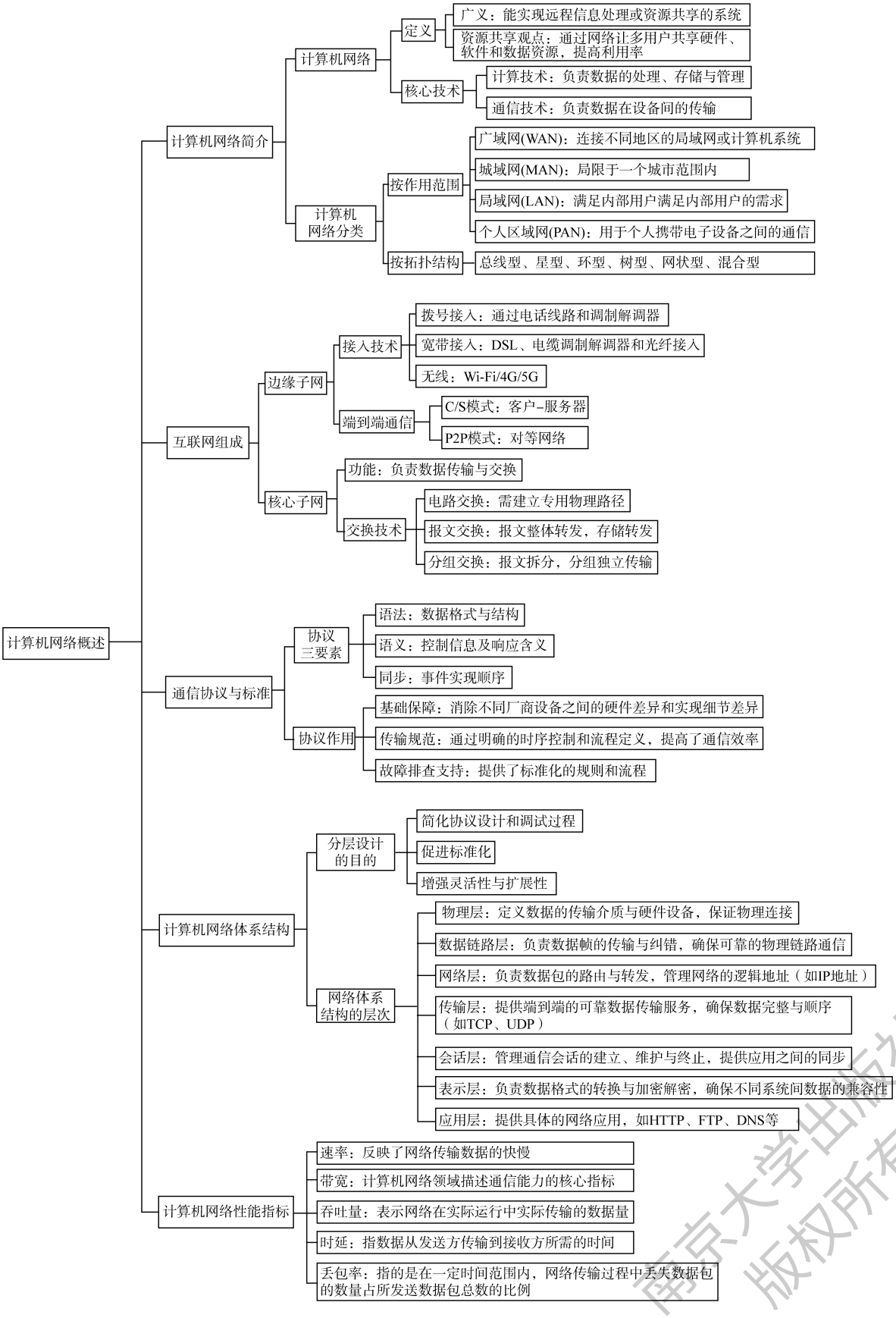
（2）计算机网络的标准化工作及相关组织；

（3）计算机网络体系结构与参考模型；

（4）计算机网络协议、接口、服务等概念；

（5）网络各类性能指标。

思维导图



1.1 计算机网络简介

1.1.1 计算机网络概念

在计算机网络的发展进程中，人们对计算机网络给出了不同的定义。

从广义的观点，认为凡能实现远程信息处理或进一步达成资源共享的系统，均属于计算机网络。此观点所定义的计算机通信网络，虽在物理结构上具备计算机网络的雏形，但资源共享能力较弱，属于计算机网络发展的初级阶段。

从资源共享的观点出发，可将计算机网络定义为：以能够相互共享资源的方式互联起来的自治计算机系统的集合，该定义包含三层含义：目的是资源共享；组成单元为分布在不同地理位置的多台独立自治计算机；网络中的计算机需遵循统一的网络协议。该定义符合当前计算机网络的基本特征。

从用户透明性的观点出发，认为存在一种可自动为用户管理资源的网络操作系统，能够调用用户所需的资源，而整个网络就像一个大的计算机系统一样对用户是透明的。用户使用网络就像使用一台单一的超级计算机，无须了解网络的存在、资源的位置信息。用户透明性观点的定义描述了一个分布式系统，它是网络未来发展追求的目标。

这些定义反映了当时计算机网络的发展水平和人们对计算机网络技术的理解。

从技术上，目前认为，计算机网络是将分布在不同地理位置的、具有独立功能的多台计算机及其外部设备，通过通信线路连接起来，并在网络操作系统、网络管理软件以及网络通信协议的管理和协调下，实现资源共享和信息传递的一种复杂的系统。简而言之，计算机网络就是一些互联的、自治的计算机系统的集合。

问题：

以上内容从不同时代、不同角度给出了计算机网络的不同定义。请思考基于不同的定义，计算机网络必须拥有哪些基本的共同特性？

尽管人们对计算机网络的认知随着时间变化而有所变化，但均认为计算机网络必须具有连通性和共享性的两大基本特性。连通性使网络中的计算机能够跨越距离实现通信，突破地域限制，实现信息的快速传递。共享性则允许网络中的硬件、软件和信息资源被不同用户共同使用，极大地提高了资源利用率，促进了知识传播和交流。为了更形象地理解这一概念，我们可以将计算机网络比作一张无形的大网。这张大网将分布在不同地点的计算机及相关设备紧密连接在一起，使它们能够相互交流、协同工作。因此，计算机网络不仅提高了信息处理的效率，还促进了信息交流与共享，可以极大改变我们的生活和工作方式。

计算机网络为实现信息处理和共享功能，其核心技术必须涵盖计算机技术和通信技

术两大领域。其中，计算机技术是网络的核心，主要负责数据的处理、存储与管理。以网络中的服务器为例，它凭借强大的计算能力，能够处理海量的数据请求。例如，在电商平台的后台，服务器需要处理来自全球用户的订单信息、商品查询请求以及支付数据等。这些数据的高效处理和存储，确保了用户能够快速浏览商品、下单购买并完成支付。如果没有强大的计算机技术作为支撑，这些复杂的操作将无法实现。而通信技术则是网络的桥梁，它负责保障数据在不同设备之间的传输，其功能由通信设备和通信介质共同实现。网络通信设备，典型的如路由器、交换机、网桥和中继器等，承担着数据转发、交换和传输控制的重要任务；而通信介质，包括光纤、双绞线、无线信号等，则是数据传输的物理通道，负责将数据信号从发送端传递到接收端。以校园网络的通信为例，当学生在图书馆电脑上访问教学资源时，数据通过网线传输到附近的交换机，交换机根据目标地址将数据转发到校园网的核心路由器，核心路由器再通过光纤链路将数据传输到服务器所在区域。通信设备和通信介质的协同工作，确保数据高效、准确地到达目标服务器。

理解了计算机网络的概念与功能，不妨聚焦最具代表性的实例——互联网。它作为全球规模最大的计算机网络，正是前述概念与功能的集中体现与实践载体。互联网由无数子网通过标准化协议互联而成，覆盖全球几乎所有国家和地区。它以 TCP/IP 通信协议族为核心，连接数十亿设备，支撑着网页浏览、即时通信、电子商务等海量应用，成为信息时代不可或缺的基础设施。

这里需要解释和区分一下“因特网”和“互联网”两个词汇，一般人常认为这两个词表达的是同一个概念，但它们在计算机网络中是不一样的术语。“因特网”特指必须采用 TCP/IP 协议族进行通信的全球最大的、开放的、由众多网络相互连接而成的计算机网络，我们所说的上网一般就是指此因特网。而“互联网”的概念更为宽泛，它泛指由多个计算机网络相互连接而成的网络集合。因此，我们可以理解“因特网”是互联网的一个典型代表，但两者之间没有等价关系。在计算机网络中，常用小写字母开头的“internet”表示“互联网”，而用大写字母开头的“Internet”表示“因特网”。在此说明后，后继章节本教材将不严格区分这两个概念，请读者根据情景把握和理解。

随着物联网和人工智能技术的蓬勃发展，产生了“互联网＋”的概念。“互联网＋”是指“互联网＋各个传统行业”的意思，但这并不是简单的两者相加，而是利用信息通信技术以及互联网平台，让互联网与传统行业进行深度融合，创造新的发展生态。以智能交通领域为例，通过物联网技术，将道路上的车辆、交通信号灯、监控摄像头等设备接入互联网，这些设备实时采集并上传交通流量、车辆行驶速度、信号灯状态等数据。然后，利用人工智能算法对这些海量数据进行分析处理，实现交通信号灯的智能调控，根据实时路况动态调整信号灯时长，以缓解交通拥堵。同时，为驾驶员提供精准的实时路况导航，引导车辆合理选择行驶路线。“互联网＋交通”通过互联网与传统交通行业的融合，提升了交通系统的智能化水平和运行效率。

“互联网＋”是互联网的新形态，它为传统行业的转型升级提供了新的思路和途径，并以不可阻挡的态势重塑各个领域，推动社会的快速发展。

1.1.2 计算机网络分类

计算机网络技术并不单一、在不同应用场景方面存在着显著差异。不同网络在技术上存在拓扑结构、传输介质、通信协议等方方面面的不同，这导致了计算机网络技术高度的复杂性和多样性。为深入学习和全面掌握计算机网络的工作原理，对其进行科学分类显得尤为重要。通过对不同类型的计算机网络技术的了解，有助于我们从多个角度对网络技术进行系统分析，构建完整且系统的网络技术版图。

计算机网络按作用范围分类，可分为局域网（LAN）、城域网（MAN）和广域网（WAN）等；按使用者分类，可分为公用网、专用网等；按网络拓扑结构分类，可分为总线型、星型、环型和网状型等；按传输技术分类，可分为广播式网络和点对点网络。这些不同分类方式从不同的维度揭示了网络的特征和应用场景。

1. 按作用范围分类

（1）广域网（Wide Area Network，WAN）

广域网覆盖的地理范围极为广泛，通常可以跨越城市、国家甚至全球。它主要用于连接不同地区的局域网或计算机系统，实现远距离的数据通信和资源共享。广域网一般由多个运营商共同构建和维护，借助电话线、卫星通信、光纤等多种通信线路，将分布在不同地理位置的网络节点连接起来。

国际金融机构的全球业务网络是典型的广域网应用。以花旗银行为例，其全球各地分支机构通过广域网相连，纽约总部服务器存储大量如客户账户信息、交易数据及金融分析模型等关键资源。分布在伦敦、东京、香港等地的分行，借助广域网实时访问这些数据，为当地客户服务。如香港分行客户进行外汇交易，交易信息瞬间经广域网传至纽约总部处理记录，确保全球业务一致准确。

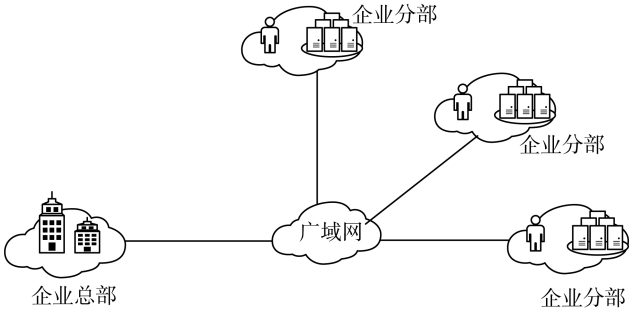


图 1-1 广域网示意图

（2）城域网（Metropolitan Area Network，MAN）

城域网覆盖范围介于广域网和局域网之间，通常局限于一个城市范围内，旨在为城市内的多个局域网提供高速连接，实现区域内的资源共享和数据通信。城域网一般由城市的电信运营商负责建设和运营，多采用光纤作为主要传输介质，以保证较高的带宽和传输速率。

例如，一个城市的教育网，连接了市内众多中小学、高校以及教育管理部门。学校之间可以通过该城域网共享教学资源，如优质的教学课件、在线课程视频等。

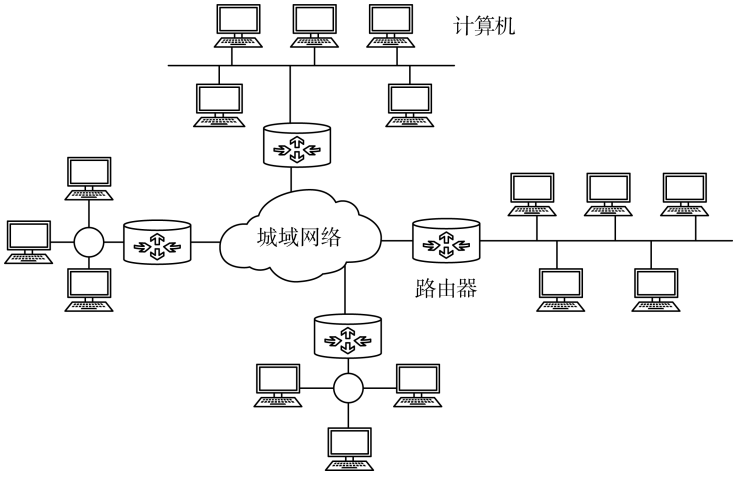


图 1-2　城域网示意图

（3）局域网（Local Area Network，LAN）

局域网属于较小覆盖范围，如一个办公室、一栋建筑物或一个校园内构建的计算机网络。它的特点是覆盖范围小、传输速率高、误码率低，主要用于满足内部用户之间的数据共享和通信需求。局域网通常由一个单位或部门自行建设和管理，常见的传输介质有双绞线、光纤等。

在一个企业的办公楼内，各个部门的计算机通过局域网连接在一起。员工可以在局域网内共享文件、打印机等资源。市场部的员工制作好一份产品推广方案文档，存放在局域网的共享文件夹中，销售部的同事就能直接访问并下载使用。同时，企业内部的办公系统、邮件服务器等也都部署在局域网上，方便员工协同办公。

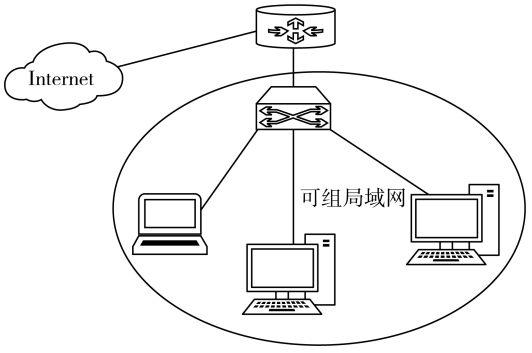


图 1-3　局域网示意图

（4）个人区域网（Personal Area Network，PAN）

个人区域网覆盖范围最小，主要用于个人携带电子设备之间的通信，如个人电脑、智能手机、平板电脑、无线耳机等设备之间的连接。个人区域网通常采用蓝牙、NFC、RFID

等无线通信技术，组建简单、使用便捷。

我们日常使用蓝牙耳机连接手机听音乐，手机与蓝牙耳机之间就构成了一个简单的个人区域网。当我们在办公室使用无线鼠标和键盘连接电脑时，它们与电脑之间也形成了个人区域网。这种网络方便个人在短距离内实现设备之间的数据传输和交互，满足个人在不同场景下的便捷使用需求。

2. 按使用者分类

（1）公用网

公用网一般由电信运营商或网络服务提供商构建和运营，向公众提供网络接入服务。社会公共用户可以根据自己的需求租用这些网络资源，实现上网功能。公用网的特点是服务对象广泛，资源共享程度高。

家庭使用的宽带网络就是公用网的一种典型形式。电信、联通等运营商铺设网络基础设施，用户通过申请办理宽带业务，接入运营商提供的公用网络，从而能够访问互联网上的各种资源，如浏览网页、观看在线视频、进行网络游戏等。不同用户在同一运营商的公用网络中，根据自己所购买的带宽套餐，共享网络资源。

（2）专用网

专用网是为特定的机构、组织或企业构建的网络，只有该机构内部的人员或授权用户能够使用。专用网通常对安全性和隐私性要求较高，会采取一系列安全措施，如防火墙、加密技术等，以保护网络中的数据和资源不被外部非法访问。

银行的内部网络是典型的专用网。银行的各个分支机构、自动取款机（ATM）以及后台业务系统都通过专用网连接。银行客户的账户信息、交易记录等高度敏感的数据在专用网内传输和处理。只有银行内部经过授权的工作人员才能访问和操作这些数据，确保客户资金安全和业务的正常运行。军事单位的网络也是专用网，用于军事指挥、情报传递等重要任务，对安全性和保密性有着极高的要求。

3. 按网络拓扑结构分类

网络拓扑结构是指由网中节点（路由器、主机等）与通信线路（网线）之间的几何关系（如总线型、环型）表示的网络结构。一般可分为总线型拓扑结构、星型拓扑结构、环型拓扑结构、树型拓扑结构、网状拓扑结构等。

其中，总线型拓扑结构采用一条共享的通信线路（称为总线）作为传输介质，所有的网络节点都通过相应的硬件接口直接连接到该总线上。信息在总线上以广播的方式传输，任何一个节点发送的数据都可以被总线上的其他节点接收。

星型拓扑结构以中央节点为中心，其他各个节点通过单独的通信线路与中央节点相连。中央节点通常为集线器（Hub）或交换机（Switch）等通信设备，负责数据的转发和控制。当一个节点要发送数据时，先将数据发送到中央节点，再由中央节点转发给目标节点。

环型拓扑结构的各个节点通过通信线路连接成一个闭合的环。数据在环中沿着一个方向逐点传输，每个节点都充当数据转发的中继站。当一个节点发送数据时，数据会依次经过环上的其他节点，直到到达目标节点。

树型拓扑结构是一种层次化的结构，它由总线型拓扑结构和星型拓扑结构演变而来。树型拓扑结构的网络像一棵倒置的树，有一个根节点，根节点下面可以连接多个子节点，每个子节点又可以作为下一级的根节点，连接更多的子节点，以此类推。数据在树型拓扑结构中通常按照层次进行传输。

网状拓扑结构中各个节点之间通过多条通信线路相互连接，形成一个复杂的网状结构。每个节点都可以与多个其他节点直接通信，数据传输路径有多条可选。

不同拓扑结构的网络工作原理请参考本教材的第 3 章数据链路层，此处仅简单介绍，不具体展开。

4. 按传输技术分类

（1）广播式网络

所有联网计算机都共享一个公共通信信道。当一台计算机利用共享通信信道发送报文分组时，所有其他的计算机都会“收听”到这个分组。接收到该分组的计算机将通过检查目的地址来决定是否接收该分组。局域网基本上都采用广播式通信技术，早期共享介质局域网常采用广播机制；现代交换式局域网主要采用点对点交换方式。

（2）点对点网络

点对点网络中，每条链路通常连接两个网络节点。如果通信的两台主机之间没有直接连接的线路，那么它们之间的分组传输就要通过中间节点的接收、存储和转发，直至目的节点。广域网基本都属于点对点网络。

互联网还可以进一步按传输介质分为有线网络和无线网络。有线网络可细分为双绞线、同轴电缆、光纤等不同网络；无线网络则可细分为无线局域网、无线广域网、无线个域网等不同网络。我们后继将结合传输介质的知识点进行教学。

1.1.3 互联网的发展历程

计算机网络的发展历程是从简单到复杂、从初级到高级的逐步演进过程。早期的阿帕网（Advanced Research Projects Agency Network，ARPANET）奠定了网络通信的基础，随后 TCP/IP 协议的出现使得异构网络能够互联互通，推动了互联网的广泛应用。在这一过程中，计算机技术与通信技术深度融合，共同促进了计算机网络技术持续进步。了解这一演变过程，有助于我们理解计算机网络的基本原理和架构，以及这些原理如何在实际应用中不断优化和发展。

1. 互联网的起源与发展

（1）ARPANET 的诞生

20 世纪 60 年代，正值冷战的紧张局势下，美国国防部高级研究计划局（ARPA）出于军事战略考虑，期望构建一种即便遭受核打击等极端状况，军事指挥系统仍能维持通信联络的计算机网络。1969 年，世界首个分组交换网络——ARPANET 宣告问世。起初，它仅连接了美国的四所高校与科研机构，即加州大学洛杉矶分校、斯坦福研究院、加州大学

圣巴巴拉分校以及犹他大学。这些节点间通过专门铺设的线路传输数据，每个节点配备一台名为接口消息处理器(IMP)的小型计算机，负责数据的接收、存储与转发等工作。

ARPANET的诞生，标志着计算机网络从理论研究迈向实际应用，为后续互联网发展奠定了基石。在ARPANET运行期间，人们意识到需一套统一标准实现不同计算机间可靠通信。于是，20世纪70年代至80年代，一系列网络协议逐步发展完善，其中最关键的是TCP/IP通信协议。TCP/IP协议为网络数据传输提供可靠的端到端通信及网络寻址功能，让不同类型计算机网络得以互联。

与此同时，计算机技术发展与普及，促使更多科研机构和高校渴望接入ARPANET。1985年，美国国家科学基金会(NSF)资助建立国家科学基金会网络(National Science Foundation Network，NSFNET)，其以56 Kbps的线路连接美国五个超级计算机中心，并向其他高校和科研机构扩展。NSFNET规模超越ARPANET，在网络架构与应用上也有突破，采用层次化网络结构，便于网络管理与扩展。

(2) 万维网的诞生

20世纪90年代，互联网迎来重大转折点——万维网(World Wide Web，WWW)诞生。1989年，英国计算机科学家蒂姆·伯纳斯-李(Tim Berners-Lee)在欧洲核子研究中心(CERN)工作时，提出基于超文本的信息系统，方便科研人员共享交流成果。1991年，首个万维网服务器和浏览器诞生，用户通过简单点击在不同文档和网页间跳转获取信息。万维网极大简化互联网使用方式，使其从科研与专业人员走向大众。

(3) 互联网商业化开启

随着互联网用户激增，商业机构看到其巨大潜力。1995年，NSFNET退役，互联网商业化全面开启。众多互联网服务提供商(ISP)涌现，提供网络接入服务。电子商务、搜索引擎、社交媒体等互联网应用蓬勃发展，互联网成为全球经济增长新引擎。

2. 国内互联网的发展历程

我国互联网发展起步稍晚。1987年9月14日，北京计算机应用技术研究所研究员钱天白通过国际互联网向前西德卡尔斯鲁厄大学发出中国第一封电子邮件——“越过长城，走向世界”，揭开国人使用互联网序幕，标志我国开始与国际互联网建立联系。尽管此时我国尚未实现全功能网络连接，但为后续发展奠定基础。

20世纪90年代，全球互联网快速发展，我国加快互联网基础设施建设。1994年4月20日，中国科学院高能物理研究所通过64 Kbps的国际专线，实现与国际互联网全功能连接，标志中国正式接入互联网。此后，中国公用计算机互联网(CHINANET)、中国教育和科研计算机网(CERNET)、中国科技网(CSTNET)和中国金桥信息网(CHINAGBN)四大骨干网相继建设。

(1) CHINANET由原邮电部于1995年开始建设，是我国首个面向公众的商业互联网，提供拨号上网、专线接入等多种方式，有力推动互联网在我国的普及。

(2) CERNET主要面向教育科研领域，连接众多高校和科研机构，为教育资源共享、学术交流提供平台，如高校间可通过CERNET共享学术数据库、开展远程教学。

(3) CSTNET依托中国科学院，为科研工作者提供高性能网络服务，促进科研成果交流

合作。

(4) CHINAGBN 致力于推动国民经济信息化建设,为企业和政府部门提供数据通信与信息服务。

进入 21 世纪,信息技术飞速发展,我国互联网进入快速发展阶段。宽带网络普及让用户享受高速稳定网络服务,家庭上网从拨号过渡到宽带。移动互联网兴起改变生活方式,2009 年我国发放 3G 牌照,智能手机普及,微信、支付宝等移动应用崛起,深刻影响社交、支付、出行等方面。

近年来,我国在 5G 技术、大数据、人工智能等领域成绩显著,推动互联网创新发展。如智能交通领域,借助 5G 网络与大数据技术实现交通流量实时监测与智能调控;医疗领域,远程医疗通过互联网实现优质医疗资源广泛共享。我国互联网产业不仅国内蓬勃发展,在国际也具竞争力,如字节跳动旗下的 TikTok 在全球获极高用户关注度。

3. 计算机网络基础结构的发展演变

计算机网络基础结构的发展演变是网络发展的核心脉络,它历经多个重要阶段,每个阶段都对网络的功能、规模和应用产生了深远影响。

(1) 面向终端的计算机网络

当时计算机价格昂贵,为充分利用计算机资源,人们将多个终端通过通信线路连接到一台中心计算机上。这些终端大多不具备独立处理数据的能力,仅作为输入输出设备,用户通过终端向中心计算机发送作业请求,由中心计算机集中处理后返回结果。

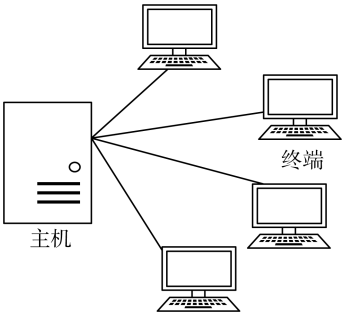


图 1-4　面向终端的计算机网络

20 世纪 50 年代,美国半自动地面防空系统(SAGE)就是一个典型的面向终端的计算机网络结构,它将远距离的雷达和其他传感器收集的信息,通过通信线路传送到一台中心计算机进行处理,实现对来袭敌机的监测和预警。这种结构虽简单,但开启了计算机与通信技术结合的先河。

(2) 分组交换网络

随着计算机技术的发展,多个计算机之间相互通信的需求日益增长。传统的电路交换方式在数据传输效率和灵活性方面存在局限,于是分组交换技术应运而生。分组交换网络将数据分割成一个个小的数据包(分组)进行传输,每个分组独立选择路径,到达目的地后再重新组装。

图 1-5　美国半自动地面防空系统

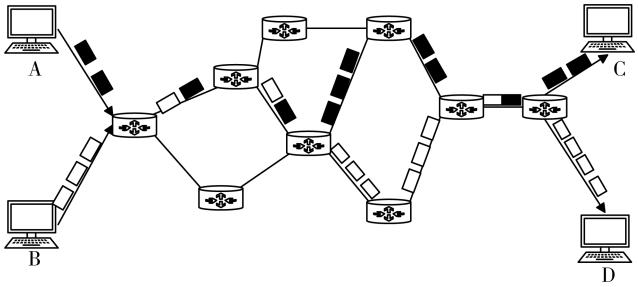


图 1-6　分组交换网络

1969 年诞生的 ARPANET 是分组交换网络的典型代表，它连接了美国多所高校和科研机构。如加州大学洛杉矶分校、斯坦福研究院等作为网络节点，通过专门的接口消息处理器(IMP)接入网络。当一个节点要发送数据时，数据被分成多个分组，这些分组在网络中通过不同路径传输，最终在目的地节点重新组合成完整的数据。ARPANET 的成功运行，标志着现代计算机网络雏形的形成，为后续互联网的发展奠定了基础。

(3) 多层次结构的网络

随着网络规模的不断扩大，简单的网络连接方式难以满足管理和扩展的需求，于是出现了多层次结构的网络。

以美国国家科学基金会网络(NSFNET)为例，它构建了一个三层结构的网络体系，包括主干网、地区网和校园网。

主干网由高速通信线路连接多个超级计算机中心，承担着大量数据的长距离传输；地区网则连接不同地区的高校和科研机构，并与主干网相连；校园网则是各个学校内部的局域网，为校内用户提供网络服务。

如图 1-7 所示，互联网的多层次结构使得网络的管理更加有序，不同规模的用户需求都能得到满足，同时也便于网络的扩展和维护。例如，一所高校的科研人员可以通过校园

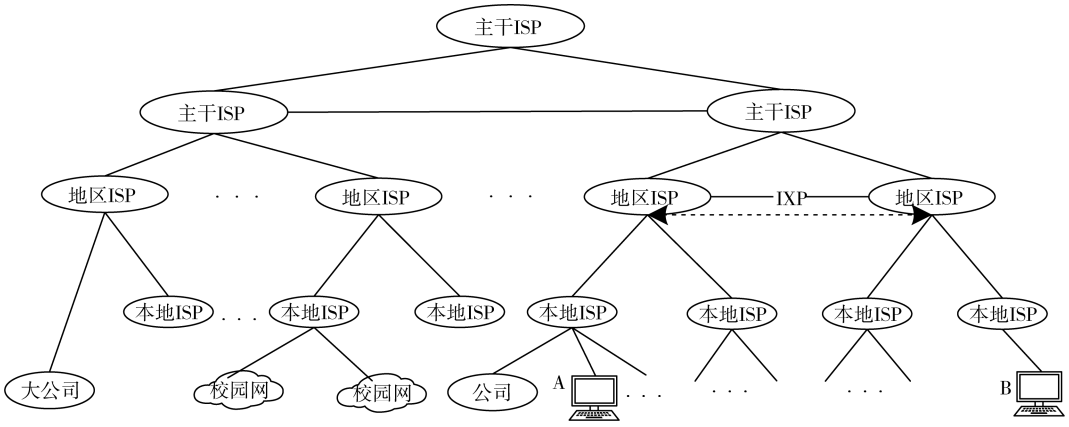


图 1-7　多层次结构网络

网、地区网接入主干网，与其他地区的科研团队进行数据共享和合作研究。

（4）商业化浪潮与技术融合创新

20 世纪 90 年代，互联网迎来了商业化与全球普及的浪潮，互联网服务提供商（ISP）如雨后春笋般涌现，为广大用户提供多样化的接入服务。不同国家和地区的网络借助各类通信线路紧密相连，构建起覆盖全球的互联网络。这使得互联网真正演变为全球信息交流与资源共享的核心平台。

进入 21 世纪，云计算、物联网、5G 等一系列新技术不断涌现，促使互联网基础结构持续演进。软件定义网络（SDN）与网络功能虚拟化（NFV）等新型网络架构理念应运而生。SDN 和 NFV 将网络的控制平面与数据平面相分离，借助软件定义的方式达成网络的灵活配置与管理。在云计算数据中心，SDN 技术可依据不同租户的需求，动态调配网络资源，显著提升资源利用率，降低运营成本。

与此同时，物联网的蓬勃发展促使大量物理设备接入互联网，构建起庞大的物物互联网络。而 5G 技术以其高速率、低延迟以及海量连接的卓越特性，为物联网及其他新型应用提供了坚实的网络支撑。在智能工厂中，借助物联网技术将生产设备互联互通，通过 5G 网络实现设备间的实时通信与协同控制。生产线上的传感器可实时采集设备运行数据，反馈至控制系统，实现生产流程的精准调控，极大提高生产效率与产品质量。

1.1.4　互联网的标准化工作

大家可以想象，若交通出行不遵守统一的交通规则，道路上的车辆将陷入混乱，交通事故频发，交通效率极低。交通规则的标准化确保了所有车辆和行人都遵循相同的规则，从而保障了交通安全和高效运行。互联网的标准化工作在网络中发挥着类似交通规则的关键作用，可以保障信息在各通信设备中遵循相同的传输规范从而有序传递。因此，学习互联网的标准化工作对理解计算机网络至关重要。

互联网的标准化并不是在网络诞生之初就被人们所重视。刚开始，由于用户使用来

自不同厂家的网络设备和操作系统，没有统一的标准化协议和规范，数据的传输与解读陷入混乱，不同系统之间无法进行信息交流。人们意识到，需要对不同网络系统进行标准化工作，以确保不同系统之间的无缝对接和各类应用的协同发展。标准化工作也不是一蹴而就，而是根据用户需求不断发展，例如，为解决 IPv4 协议标准的地址不足的问题，新的标准协议 IPv6 被制定。而 IPv6 协议的标准化确保了该协议能够被广泛接受和应用，从而推动了网络技术的进步。另外，标准化工作不仅针对通信领域，还涉及网络安全、隐私保护等重要领域。如标准化协议 SSL/TLS 是为了确保网络通信的安全性，保护用户数据免受窃取和篡改。

互联网的标准化工作并不仅由一个组织主导，而是由国际标准化组织（ISO）、国际电信联盟（ITU-T）等多个国际组织和机构共同负责。这些组织通过制定和维护一系列标准协议和技术规范，确保不同厂商的网络设备和软件能够无缝协作。主要的标准化组织如下：

1. 互联网协会（Internet Society，ISOC）

互联网协会成立于 1992 年，是一个全球性的非营利组织。ISOC 致力于推动互联网标准的制定与推广，支持 IETF（互联网工程任务组）和 IAB（互联网体系结构委员会）的工作。在标准化方面，ISOC 取得了显著成就。它的努力为互联网的全球普及和技术创新奠定了坚实基础，促进了其在全球范围内的广泛应用。

2. 国际标准化组织（International Organization for Standardization，ISO）

国际标准化组织成立于 1947 年，总部位于瑞士日内瓦，是一个非政府间国际组织。其宗旨是制定和推广国际标准，促进全球贸易、环境保护、社会责任和消费者权益。ISO 成员包括 160 多个国家的国家标准化机构，ISO 的标准覆盖了除电气和电子工程（由国际电工委员会 IEC 负责）之外的几乎所有技术领域，包括质量管理（如 ISO 9001）、环境管理（如 ISO 14001）、信息安全（如 ISO/IEC 27001）等多个领域。这些标准通过促进产品和服务的质量、安全性和互操作性，帮助组织提升效率、降低成本，并在全球范围内建立信任。

3. 国际电信联盟电信标准化部门（International Telecommunication Union Telecommunication Standardization Sector，ITU-T）

该部门是国际电信联盟（ITU）的一个重要组成部分，旨在促进全球电信网络的兼容性、互操作性和高效运行，主要负责研究技术、操作和资费问题，为电信标准化制定规则。其工作范围广泛覆盖电信网络的传输、交换、信令等各个层面，为互联网基础设施与服务质量相关标准的制定发挥了关键作用。

4. 电气和电子工程师协会（Institute of Electrical and Electronics Engineers，IEEE）

该协会是一个国际性、非营利性的电子技术与信息科学工程师协会，在电气和电子工程、计算机科学、信息技术等领域具有深远影响力，通过制定标准、组织学术会议、出版学

术期刊等方式，推动相关技术的发展与应用。其制定的众多标准，如 IEEE 802 系列局域网标准，广泛应用于网络通信等领域，对行业发展起到了关键的规范与引领作用。

下面以影响力较大的互联网协会(ISOC)为例，了解其网络协议标准的制定流程。如图 1-8 所示，互联网协会(ISOC)旗下有一个重要的技术组织互联网体系结构委员会(Internet Architecture Board，IAB)，主导标准制定审核。IAB 下设有两个工程部：互联网工程部(Internet Engineering Steering Group，IESG)和互联网研究部(Internet Research Steering Group，IRSG)。

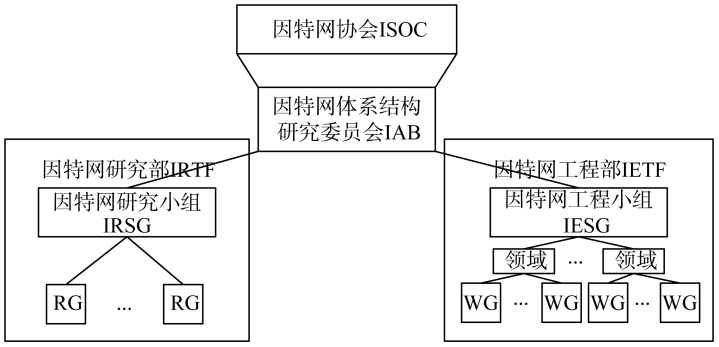


图 1-8　互联网协会基本结构

1. 互联网工程部

该部门主要针对互联网当前面临的实际技术问题，制定切实可行的解决方案和技术标准。例如，随着互联网用户数量的急剧增长以及网络应用的日益复杂，网络拥塞问题愈发严重。互联网工程部需组织专家团队，对网络拥塞的成因、影响进行全面分析，通过大量的实验和模拟，提出了一系列优化网络拥塞控制的算法和标准，并推动这些标准在互联网工程实践中的广泛应用，有效缓解了网络拥塞状况，提升了网络传输效率。

2. 互联网研究部

该部门侧重于对互联网未来发展趋势和前瞻性技术问题的研究。它关注那些可能对互联网架构和功能产生深远影响的新兴技术和理念，为互联网的长期发展奠定理论基础。例如，在量子计算技术逐渐兴起的背景下，互联网研究部敏锐地意识到其可能对互联网安全和加密技术带来挑战与机遇。于是，它需要组织相关领域的专家开展深入研究，探索如何提前布局和研发适应量子计算时代的新型互联网安全加密技术，为未来互联网的安全发展提供技术储备和理论指导。

网络协议标准的制定流程具有严谨且开放的特性，其过程为：

1. 问题提出：伴随互联网发展，如 5G 应用兴起带来网络适配问题，相关人员发现技术、应用等方面新的问题，提出标准化需求。

2. 草案撰写：IETF 组建工作组，成员来自全球，综合考量各方因素。例如，制定物联网设备通信标准草案，需兼顾不同设备特性与应用场景，详细描述协议等关键内容。

3. 公开征求意见：草案通过官方渠道面向全球发布。网络设备商、服务商等基于自

身经验提建议，指出草案技术实现难度或优化流量控制机制等建议。

4. 修订完善与发布：IETF 整理分析意见，工作组修订草案。经多轮完善审核后，正式发布成为权威标准。

互联网体系结构委员会的网络协议标准以请求评论（Request for Comments，RFC）文档为核心载体。RFC 文档起初作用是为了在技术专家之间交流想法、征求意见，随着互联网发展，RFC 文档主要用于描述互联网技术标准，但并非每个 RFC 都是网络协议标准，RFC 要上升为网络协议的正式标准需经过以下 4 个阶段。

（1）因特网草案（Internet Draft）。这个阶段还不是 RFC 文档。

（2）建议标准（Proposed Standard）。从这个阶段开始就成为 RFC 文档。

（3）草案标准（Draft Standard）。

（4）因特网标准（Internet Standard）。

下面以 HTTP 协议为例说明 RFC 文档的作用。HTTP 协议是互联网中规范网页传输的通信协议，该协议将在应用层详细学习。对该协议技术标准的描述包含一系列的 RFC 文档，其中具有代表性的经典文档有：

1. RFC9110 文档

规定了 HTTP 语义，详细说明了 HTTP 的各种概念、方法、状态码等，比如定义了 GET、POST 等方法的具体含义和用法。

2. RFC2616 文档

定义了 HTTP/1.1 协议，规定数据包请求头需包含 Content-Length 或 Transfer-Encoding 说明长度，引入了 keep-alive 和 pipeline 特性，提高了传输效率。该文档现已被新一代 RFC 系列文档替代。

3. RFC7540 文档

定义了 HTTP/2 协议，采用二进制分帧层等技术，实现了多路复用、首部压缩等功能，提升了性能和传输效率，像可在同一个连接中并行发送多个请求和响应。

1.2 互联网组成

完整的计算机网络由硬件、软件和协议三大部分构成，三者缺一不可。硬件作为网络的物理基础，主要包括主机（端系统）、通信链路（如双绞线、光纤）、通信设备（如路由器、交换机）等；软件是网络功能实现的载体，主要包含核心管理软件（如网络操作系统）和方便用户使用的工具软件（如邮件收发程序、FTP 工具、即时通信软件等），且多属于应用层；协议是计算机网络的核心，如同交通规则规范车辆行驶一般，它规定了网络数据传输所遵循的规范，是保障通信有序进行的关键。

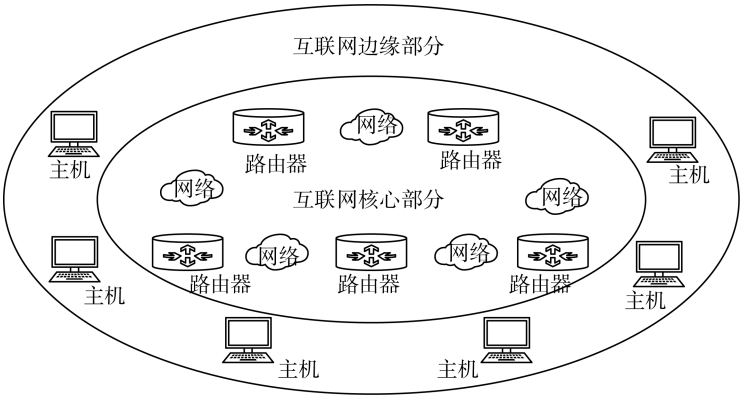


图 1-9　互联网的组成

互联网是一个由众多计算机子网络相互连接而成的全球性网络。如图 1-9 所示，从宏观层面上，互联网大致可以分为边缘部分和核心部分，分别对应着边缘子网和核心子网（也称为资源子网和通信子网）。

边缘子网主要由各种终端设备以及相关的接入网络组成，终端设备可以是个人计算机、服务器、智能手机、物联网设备等，它们是互联网服务的最终使用者或提供者。边缘子网负责将这些终端设备接入到互联网中，并为用户提供各种网络应用服务。

核心子网是互联网的骨干，由大量的路由器和高速通信链路组成，负责数据的高速转发和路由选择，确保数据能够准确、高效地从源端传输到目的端，为边缘部分提供连通性和交换服务。它就像是互联网的“交通枢纽”，承载着整个网络的大部分数据流量。

下面对这两个子网进行具体阐述。

1.2.1　边缘子网

1. 终端设备概述

终端设备是边缘子网的基本组成单元，其中，个人计算机（PC）是常见的终端设备之一，被广泛应用于办公、学习和娱乐等领域。服务器则是为网络用户提供各种服务的计算机，如 Web 服务器提供网页浏览服务，邮件服务器处理电子邮件的收发等。

随着移动互联网的发展，智能手机和平板电脑等移动终端设备也成了边缘子网的重要组成部分，它们通过无线通信技术接入互联网，满足用户随时随地获取信息和服务的需求。

此外，物联网设备的兴起进一步丰富了边缘子网的终端设备类型，如智能家居设备、智能传感器等，它们能够采集和传输各种环境数据，实现物与物、人与物之间的互联互通。

2. 接入网

接入网络是连接终端设备与核心子网的桥梁，它负责将终端设备接入到互联网中。请读者注意，有些教程并不将接入网作为边缘子网的一部分讲解，因在学术上并没有定论，本教程还将其作为边缘子网的组成部分。

常见的接入网络类型包括拨号接入、宽带接入、无线接入等。

（1）拨号接入

拨号接入是早期的一种接入方式，通过电话线路和调制解调器（Modem）实现用户计算机与互联网服务提供商（ISP）之间的连接。这种方式带宽较低，数据传输速度较慢，现已逐渐被淘汰。

（2）宽带接入

宽带接入包括数字用户线路（DSL）、电缆调制解调器（Cable Modem）和光纤接入等。DSL 利用现有的电话线路提供高速数据传输，通过不同的调制技术，可以实现不同的带宽速率。Cable Modem 则借助有线电视网络进行数据传输，适用于已经铺设有线电视线路的区域。光纤接入是目前最为先进的宽带接入方式，它利用光纤作为传输介质，能够提供极高的带宽，满足用户对高速网络的需求，如常见的光纤到户（FTTH）、光纤到楼（FTTB）等。

（3）无线接入

随着无线通信技术的发展，无线接入已成为重要接入方式之一。常见的无线接入技术包括 Wi-Fi 和蜂窝移动通信网络（如 4G、5G）。Wi-Fi 主要用于室内或局部区域的无线覆盖，通过无线路由器将终端设备连接到互联网，提供便捷的上网体验。蜂窝移动通信网络则具有更广泛的覆盖范围，能够支持用户在移动过程中保持网络连接，满足用户随时随地接入互联网的需求。

3. 端到端通信

边缘子网的通信一般被称为端到端通信，即数据从源端设备跨越多个网络节点与链路，最终抵达目的端设备的过程。不同主机间的进程通信是端到端通信的具体实现。根据通信双方的角色和交互模式，端到端通信可分为客户-服务器（Client-Server，C/S）方式和对等（Peer-to-Peer，P2P）方式。这两种方式在不同的应用场景下各有优势。

（1）客户-服务器方式

在客户-服务器方式中，通信的双方被明确区分为客户和服务器角色。客户是对服务和资源的请求方，它发起对特定服务和资源的请求，如访问网页、下载文件等。服务器则是服务和资源的提供方，它持续运行并等待客户的请求，一旦接收到请求，就根据请求的内容提供相应的服务和资源。客户-服务器方式如下图 1-10 所示。

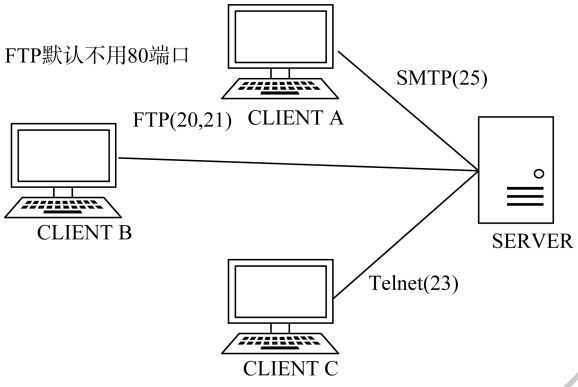


图 1-10　客户-服务器方式

我们日常生活中浏览网页的过程就是典型的客户-服务器通信方式。当我们在浏览器中输入一个网址(比如 www. ntu. edu. cn)并按下回车键时,我们的电脑(客户)就向该网址对应的网页服务器发起了访问请求,请求获取该网页的内容。

此时,那台存储着该网页数据的服务器(服务和资源的提供方)会接收到这个请求,然后从自身的存储中找到对应的网页数据,再将这些数据发送回我们的电脑。我们的浏览器接收到数据后,将其解析并展示出完整的网页,整个过程就像我们(客户)向商店(服务器)提出购物请求,商店根据请求提供商品一样。

(2) 对等方式

对等方式中,通信各个节点地位是平等的,既可以作为服务和资源的请求者,也可以作为服务和资源的提供者。每个对等方都具备类似的功能,它们之间直接进行通信,无需依赖专门的服务器。

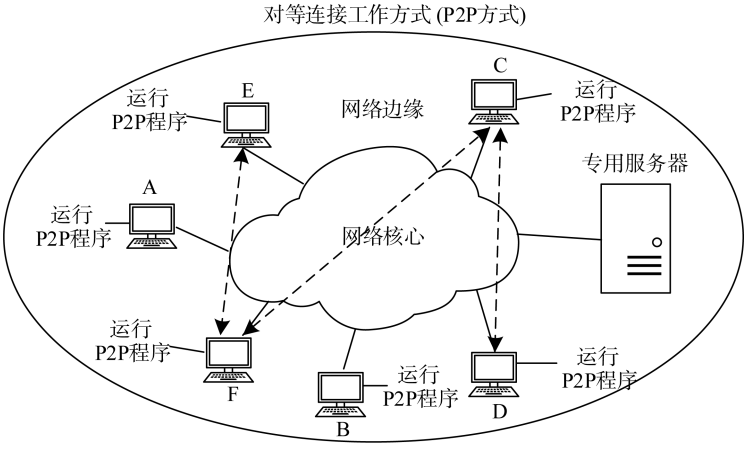


图 1-11　对等方式

常见的对等通信方式有 P2P 下载技术(如 BitTorrent 协议)。在 P2P 下载技术中,参与文件分享的所有设备(称为“对等点”)地位均等。每个下载者同时也是上传者:当用户下载某部电影时,其设备会从其他已获取部分文件的节点处获取数据,同时也向其他需要该部分数据的节点提供上传服务。这种模式无需集中式文件服务器,可通过节点间直接交互高效分发大文件,常见于影视资源、软件安装包的共享场景。

而区块链技术是对等通信模式在数字世界更典型的应用,其核心特点是“去中心化”,即网络中没有任何一个节点拥有绝对控制权,所有参与节点地位平等,共同维护系统的运行。

以大家熟悉的转账场景为例:在传统方式中,转账需要通过银行等中心机构验证和记录;而在区块链网络(如比特币、以太坊)中,当用户 A 向用户 B 转账时,这笔交易信息会被广播到网络中的所有节点。每个节点都会独立验证交易的合法性(比如,A 是否有足够余额),验证通过后,交易将被打包成“区块”,与其他节点生成的区块链接成链,形成不可篡改的公开账本。此时,A 既是交易的发起者(请求资源),也通过参与网络维护为其他交易提供验证服务(提供资源);其他节点同理,既接收和验证他人的交易请求,也向全网广

播自己的交易信息。

这种模式的优势在于：无需依赖第三方机构，交易过程透明可追溯，且单个节点的故障或恶意行为不会影响整个网络的安全运行。除了数字货币，区块链的对等通信特性还被应用于供应链溯源（如食品来源全程记录）、版权保护（数字作品确权与交易）等领域，本质上都是通过节点间的平等协作实现可信信息传递。

1.2.2 核心子网

核心子网也被称作通信子网，主要负责数据传输与交换，是互联网的“交通枢纽”。它的功能是将数据从源节点高效送达目的节点。核心子网若出现故障，互联网将大面积瘫痪。因此，核心子网必须具备以下特性：

（1）高可靠性，通过冗余链路和设备保障数据传输不中断；

（2）高带宽，能承载海量数据流量；

（3）良好的扩展性，以适应网络规模不断扩大。

核心子网并不关心数据内容，而是专注于数据的快速、准确传输，为边缘子网的端到端通信提供坚实支撑。它通过通信交换节点（如路由器），将数据从一个端口转发到另一个端口，从而实现跨越不同设备进行数据通信。

通信交换技术解决了众多设备之间高效、准确地传递信息的问题，“交换”可以理解为在网络节点之间建立临时的通信路径，就像交通指挥中心根据车辆的目的地调度车辆行驶路线一样。网络中的交换节点会根据数据的目的地址，决定将数据从哪个端口发送出去，以达到数据从源主机到目的主机的传输，实现不同设备之间资源共享和信息交互。

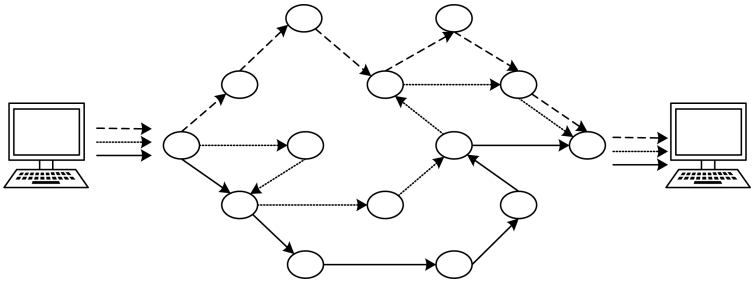


图 1-12 交换技术

常用交换技术有三种：电路交换、报文交换、分组交换。

1. 电路交换

电路交换（Circuit Switching，CS）是通信网中最早出现的交换技术，其核心特征是为通信双方建立一条专用的物理传输路径，该路径在通信全程被独占，直至通信结束才释放资源。这种“面向连接”的工作模式需经历建立连接、数据传输、释放连接三个不可分割的阶段。典型应用如传统固定电话通信系统，通话质量有保障，但资源利用率比较低。

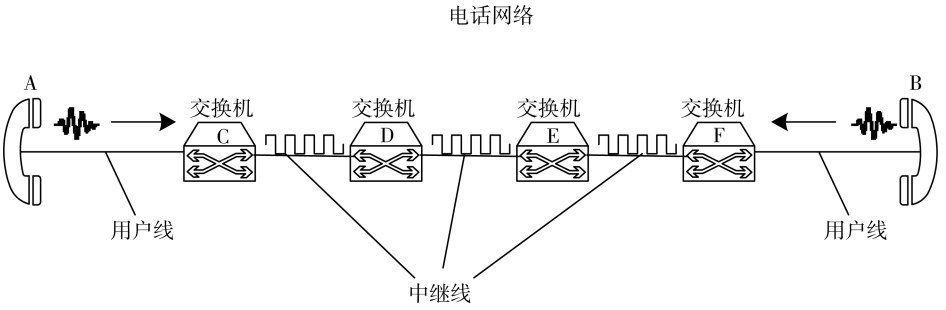


图 1-13　电路交换

在建立连接阶段，源结点需向网络发送连接请求，网络通过交换设备（如电话交换机）依据目的地址选择物理链路，逐步构建从源节点到目的节点的专用路径。这一过程涉及多设备间的信令交互，如同电话拨号时，本地交换机与长途交换机协同确定通话路由，确保链路中所有节点为该连接预留资源。此阶段的核心是“路径独占性”，即一旦建立连接，链路中的带宽、时隙等资源即被通信双方专用，其他用户无法占用。

数据传输阶段依赖已建立的专用电路，通信双方直接通过物理链路传输数据。由于资源独占，数据无需排队等待，传输延迟稳定且微小，且不受其他用户数据干扰。例如，固定电话通话中，语音信号通过专用电路连续传输，音质清晰、时延恒定，这也是电路交换适用于实时通信的关键原因。

通信结束后进入释放连接阶段，网络收到断开请求后，沿原路径释放各节点占用的资源（如交换机端口、链路带宽），使这些资源可被其他连接复用。若不及时释放，大量闲置连接会导致资源浪费，降低网络整体利用率。

电路交换的优势源于其专用性：

首先，实时性强，数据传输时延固定，适合语音、视频等对时延敏感的业务；

其次，传输质量高，独占链路避免了干扰和拥塞，可靠性有保障。

但其局限性也十分显著：

首先，资源利用率低，连接建立后无论是否传输数据，资源始终被占用，尤其在数据突发性强的场景（如 Web 访问、文件传输等突发业务）中，空闲时段的资源浪费问题突出；

其次，连接建立耗时较长，信令交互和路径选择过程可能产生明显建立时延，不适应快速通信需求；

最后，带宽固定且不可动态调整，无法匹配数据量的波动。若遇小数据量时易造成带宽闲置，而遇大数据量时则可能因容量不足导致阻塞。

正是由于互联网数据传输具有突发性强、流量波动大的特点，电路交换的固定资源分配模式难以满足其需求，这也为分组交换技术的发展提供了契机。

2. 报文交换

报文交换是继电路交换之后发展起来的一种基于“存储-转发”机制的通信技术，其核心是将数据以完整报文为单位在网络中传输，这一技术被视为分组交换的前身，为现代数

据通信奠定了重要基础。

与电路交换的“独占链路”不同，报文交换中，源节点会将待传输的数据封装为包含源地址、目的地址、控制信息及数据本身的完整报文。报文进入网络后，无需预先建立专用链路，而是采用“存储-转发”模式：每个中间节点（如交换机、路由器）先将接收到的报文完整存储在本地缓冲区，通过路由表查询目的地址对应的下一跳路径，待链路空闲时再将报文转发至下一个节点。这一过程逐节点重复，直至报文抵达目的节点，最终由目的节点解析报头并提取原始数据。例如，早期的电报通信网络，便是通过这种方式将完整电文从发送方经多个中转站点转发至接收方。

报文交换的优势集中体现在资源利用与网络灵活性上：

首先，链路资源采用时分共享模式，多个报文可交替使用同一条线路，避免了电路交换中链路空闲时的资源浪费，显著提升了线路利用率；

其次，中间节点可根据网络实时状态（如链路拥塞程度、节点故障）动态调整转发路径，当某条链路中断时，能自动切换至其他可用路径，增强了网络对拓扑变化的适应能力。

但其“存储-转发”特性也带来了固有局限：

首先，传输延迟较大，每个节点需完成报文接收、存储、校验、路由选择等操作。若报文长度较长或网络负载较重，累计延迟会显著增加，难以满足语音、视频等实时通信需求；

其次，节点需配备较大容量的存储设备以缓存完整报文，尤其在传输大文件时，对存储资源的需求更高；此外，报文在传输中若发生错误，需重新传输整个报文，导致效率低下。例如，一个 10 MB 的报文因某一比特错误而重传，会造成大量带宽浪费。

报文交换的出现，打破了电路交换对链路的独占性，为数据通信提供了更灵活的资源分配方式。但由于其对长报文的处理效率不足，逐渐被更高效的分组交换技术取代，不过其“存储-转发”核心思想仍在现代网络中发挥着重要作用。

3. 分组交换

分组交换是目前计算机网络中应用最广泛的交换技术，在交换方式上和报文交换类似，但它会首先将大的数据块分割成若干个小的数据分组，每个分组独立传输。分组交换技术又可分为数据报和虚电路两种方式。

（1）数据报交换

数据报交换是分组交换的主要模式，在此工作模式下，发送方首先把待传输的报文拆分成多个小的分组，每个分组都附带源地址、目的地址等关键信息。这些分组独立地在网络中传输，并各自依据网络的实时状态和路由算法独立选择最优路径，最终汇聚到目的节点。

如图 1-14，在数据报交换中，发送方首先将完整报文按照固定长度拆分为若干个分组（每个分组通常为几百至几千字节，具体长度由网络协议规定，如以太网中最大传输单元 MTU 通常为 1 500 字节）。这一拆分过程并非简单切割，而是需要遵循“边界对齐”原则，确保每个分组的长度不超过传输链路的最大承载能力，避免因分组过大导致的链路适配问题。

每个分组均独立封装为“数据报”，其结构包括两部分：控制信息报头，主要包含源地

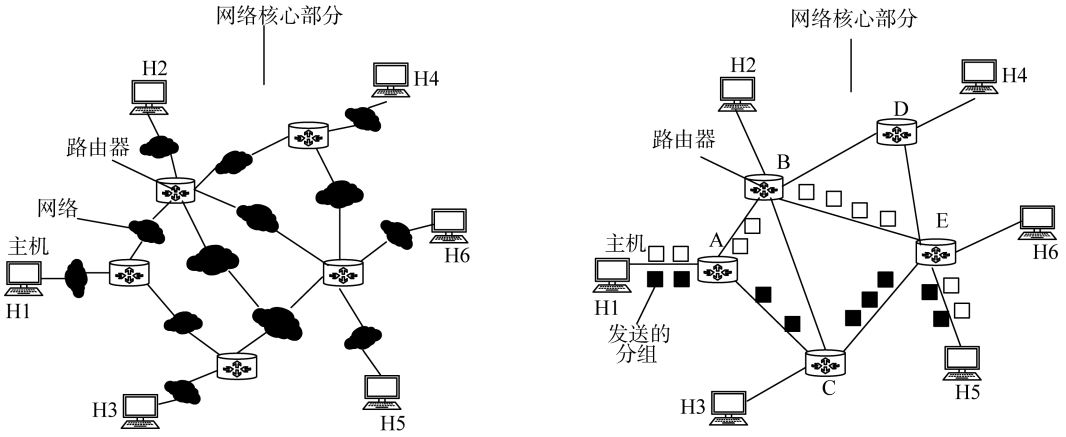


图 1-14　数据报交换技术

址、目的地址、校验和、生存时间等关键字段；数据部分，即原始报文的片段。

与报文交换的“完整报文传输”不同，这些数据报在网络中采用“独立路由＋独立传输”的模式。其核心特点体现在以下三个方面：

（1）无连接性：数据报传输前无需建立任何预先的连接，发送方可以随时向网络中发送数据报，接收方也无需提前准备资源，这种“即发即传”的模式极大简化了通信流程。

（2）节点独立决策：每个数据报到达中间节点（如路由器）后，节点会首先对其进行完整性校验（通过校验和比对），若发现错误则直接丢弃该数据报（由发送方后续重传）；校验通过后，路由器会查询本地路由表，结合当前网络拓扑、链路负载等实时状态，通过路由算法计算出最优转发路径，确定下一跳节点的物理接口。

（3）路径动态性：即使是同一报文拆分的不同数据报，也可能因网络状态变化而选择完全不同的传输路径。例如，同一批数据报中，先发送的分组可能走“链路 A”，而后发送的分组因“链路 A”突然拥塞，会自动切换至“链路 B”传输。这种动态调整机制无需人工干预，完全由网络设备根据预设算法自主完成，确保数据报始终沿着当前最优路径传输。

最终，所有数据报无论经过多少节点、选择何种路径，都会在目的节点重新汇聚，等待重组为完整报文。

我们以互联网中“用户访问南通大学校内新闻”为例，清晰理解数据报交换的运作逻辑：

当用户在浏览器输入网址并发送请求后，南通大学服务器接收请求，将新闻内容（含文字、图片、视频片段等）拆分为数十个甚至上百个数据报，每个数据报均分配唯一序号（如 1、2、…、n），并在报头中写入服务器源地址与用户设备目的地址。

这些数据报依次进入互联网，途经的每个路由器会独立处理：路由器通过路由表查询目的地址对应的下一跳地址，若某条链路因拥塞或故障不可用，会立即切换至其他路径。例如，序号为 5 的数据报可能经“本地运营商骨干网→省际光缆”传输，而序号为 6 的数据报可能因骨干网繁忙，改由“城域网→卫星链路”绕行。

各数据报到达用户设备后，设备根据报头中的序号对分组进行排序，通过校验和检测

数据完整性，最终重组为完整的新闻报文，由浏览器解析并展示。

数据报交换的技术特性优势如下：

动态适应性强：数据报可实时规避故障或拥塞链路，例如，某地区光缆中断时，后续数据报会自动选择其他路由，无需人工干预，这一特性使网络具备极强的抗毁性。

资源利用率高：无需预先分配链路资源，数据报仅在传输时占用链路，空闲时段资源可被其他数据报共享，解决了电路交换的资源浪费问题。

健壮性突出：单个数据报的丢失或损坏不会影响其他数据报传输，接收方可通过重传机制仅请求丢失的分组，避免了报文交换中“一错全重传”的低效问题。

但其也有固有局限如下：

传输延迟不确定：不同数据报的路径长度、链路质量存在差异，可能导致“分组失序”（如序号3的数据报晚于序号5到达），接收方需缓存所有分组并按序重组，增加了处理延迟。

协议开销较大：每个数据报需独立携带完整报头（含地址、序号等信息），相比报文交换的单报头，额外开销随分组数量增加而累积。

路由计算负担重：路由器需为每个数据报独立计算路由，在海量数据传输场景下，可能增加节点的处理压力。

总之，数据报交换通过“分组拆分-独立传输-动态路由-重组还原”的机制，完美适配了互联网“突发性、分布式、异构性”的特征。尽管存在延迟不确定性等局限，但其无需连接建立、抗故障能力强的优势，使其成为TCP/IP协议族的核心支撑技术，至今仍是全球互联网数据传输的主导模式。理解数据报交换的原理，是掌握现代计算机网络通信机制的基础。

问题：

试分析分组交换相比报文交换的优势，并说明分组交换中可能出现的“分组失序”问题及解决方法。

（2）虚电路交换

虚电路交换是分组交换技术中面向连接的典型实现方式，是一种通过建立逻辑通路实现数据传输的交换模式，其核心特征是融合了电路交换的连接导向性与分组交换的存储-转发机制，适用于对传输可靠性和时序一致性要求较高的通信场景。如图1-15所示，虚电路交换技术在数据传输前，源节点和目的节点会先建立一条逻辑连接，该逻辑连接被称为虚电路。之后传输的所有分组都沿着这条既定路径走，传输结束，虚电路便被释放。

虚电路交换以“逻辑连接”为核心的工作机制，包含三个关键阶段：

首先是虚电路建立阶段，源节点向目的节点发送连接请求分组，该分组携带源地址、目的地址等控制信息，沿途交换节点（如路由器）根据路由算法选择路径，逐跳转发并建立虚电路表项。表项中记录了输入端口、虚电路标识、输出端口及下一跳标识等映射关系，形成从源到目的的逻辑通路。

数据传输阶段，所有分组均携带虚电路标识而非完整地址，交换结点通过查询虚电路

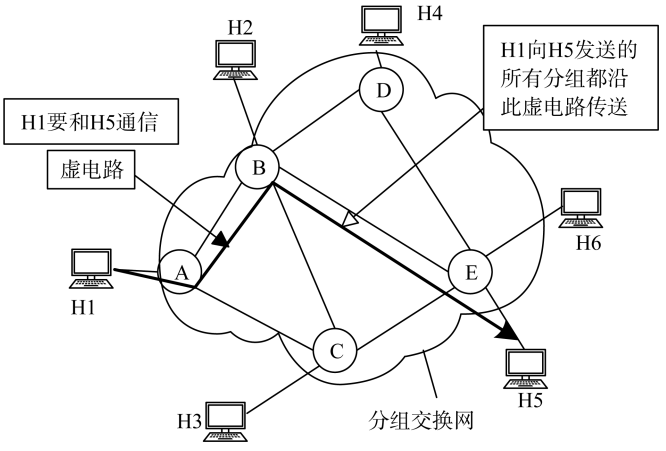


图 1-15　虚电路交换技术

表项即可完成转发，无需重新计算路由。由于分组沿预设路径传输，且节点按接收顺序转发，能够保证数据的有序性。

虚电路释放阶段，通信结束后源节点发送释放请求分组，沿途节点删除对应表项，释放缓存和带宽等资源，完成整个通信过程。

下面举例说明其工作原理，假设用户在使用在线游戏平台玩一款多人在线竞技游戏，用户的设备（源节点）需要和游戏服务器（目的节点）进行大量、稳定且有序的数据交互，比如用户的角色移动、攻击动作等指令要及时准确地发送到服务器，服务器也要实时把其他玩家的行动信息反馈给用户，这个过程就可采用虚电路分组交换技术来保障数据传输的可靠性。首先，当用户启动游戏并尝试连接服务器时，设备会向游戏服务器发送一个建立虚电路的请求报文。这个报文包含了用户的设备 IP 地址（源地址）和游戏服务器的 IP 地址（目的地址）等关键信息。网络中的交换设备，主要是路由器，根据这些信息，通过路由选择算法确定一条从用户的设备到游戏服务器的路径。例如，这个路径可能要经过用户所在地区的本地路由器、网络服务提供商的骨干路由器等。沿途的路由器会记录下这条虚电路的相关信息，像是虚电路编号等，为后续的数据传输做好准备。一旦虚电路建立成功后，用户在游戏中的各种操作会被设备转换成数据报文，并分割成多个分组。每个分组都带有虚电路标识，交换设备依据这个标识，按照预先建立好的路径将分组转发出去，直至到达游戏服务器。同样，服务器反馈给用户的数据分组也会沿着同一条虚电路返回。因为所有分组都走同一条路径，它们能按发送顺序到达，确保游戏画面和操作的连贯性。当用户结束游戏，设备会向服务器发送一个释放虚电路的请求报文。沿途的交换设备收到这个请求后，会清除之前为这条虚电路记录的信息，释放占用的网络资源，以便其他数据传输使用。

技术特性来看，虚电路交换的优势体现在三个方面：

（1）传输可靠性高：通过预先建立的逻辑通路和资源预留机制，降低了分组丢失概率，且能避免数据报交换的失序问题；

（2）转发效率高：基于虚电路标识的查表转发减少了节点处理开销，端到端延迟更

稳定；

（3）便于流量控制：可在连接建立时协商传输参数，实现基于虚电路的拥塞管理。

但其局限性也较为明显，如建立和释放连接的信令交互会产生额外开销，不适合短报文传输；路径固定导致灵活性不足，某段链路故障时需重建虚电路；资源预留虽保障了服务质量，但空闲时无法被其他连接复用，可能造成资源浪费。

在网络技术体系中，虚电路交换是电路交换与数据报交换的折中方案：既保留了电路交换的连接管理思想，又继承了分组交换的资源共享优势。这种特性使其在传统广域网（如 X.25、帧中继）和现代通信系统中均有应用，例如，ATM 网络通过虚通道和虚信道实现高速分组传输，本质上是虚电路技术的延伸。理解虚电路交换的工作原理，有助于把握分组交换技术的演化逻辑，为网络设计中的交换方式选型提供理论依据。

最后，给出三种交换技术的比较示意图：

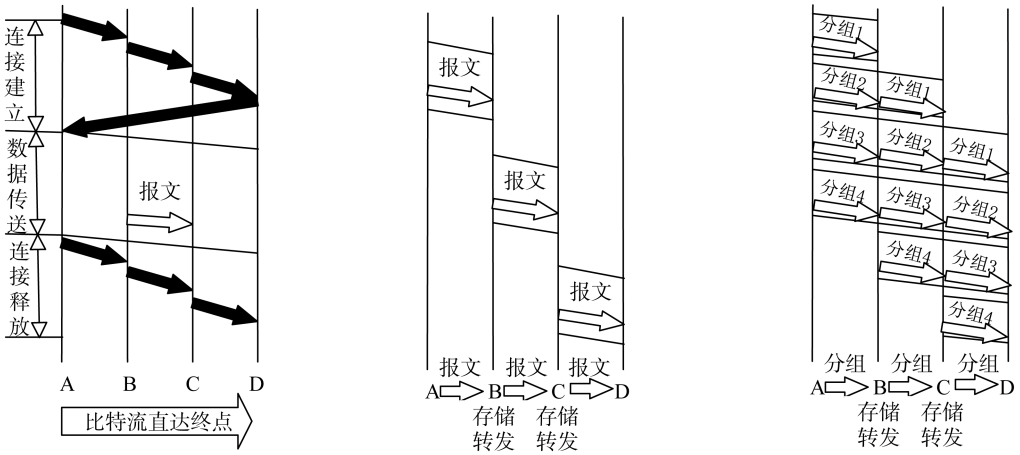


图 1-16　交换技术比较

从图中可知，电路交换在通信前需建立专用物理电路，通信时独占资源，实时性与可靠性高，但资源利用率低、建立连接慢且灵活性差。报文交换以报文为单位进行存储转发，线路利用率和灵活性好，却有传输延迟大、对节点存储要求高的问题。分组交换将数据进行分组，其数据报方式灵活但延迟不定、分组可能失序，虚电路可靠性高但建连与释放复杂，二者资源利用率均较高，适用于计算机网络数据传输。

1.3　通信协议与标准

1.3.1　通信协议基本概念

随着网络即时通信技术的发展，纸质信已经成为一种遥远的记忆。让我们一起回忆一下纸质信的发送过程吧，为了和朋友沟通，我们需要在纸上写下相关信息，然后塞进信

封，并在信封上写上朋友的地址后，投递给邮局。邮局根据信封上的地址帮你进行投递。

在这个过程中，我们其实都在默默遵循着一种通信规范，如写信得用双方都懂的文字，以明确表达自己的信息；信件格式也有讲究，开头有称呼，结尾有署名和日期；信封上收件人、寄件人的地址按正确位置填写；邮编采用国家标准填写。只有符合要求的信才能被准确送达并被朋友所理解。

计算机网络通信过程也遵循相同道理，异构计算机间要进行有效的数据交换，需要遵循一系列规则。想象一下，若 A 计算机和 B 计算机进行通信，A 计算机采用一种二进制编码来表示数据，而 B 计算机使用另一种编码方式。那么当 A 计算机向 B 计算机发送数据时，B 计算机是无法解读这些数据的含义。因此，A、B 两台计算机在通信前需要对信息的编码进行预先协商，比如双方共同约定采用 UTF－8 编码进行文字的表示，这就是通信协议与标准的一部分内容。

网络通信协议是在计算机网络中，为实现不同系统、不同设备之间的数据交换，而预先制定并共同遵循的一整套规则、标准与约定的集合。它不仅明确了通信双方在数据交换过程中采用的格式、顺序，以及动作执行的条件等，更是搭建起了一座跨越不同计算机系统差异的桥梁，以此确保数据能够在不同系统间准确、可靠地传输。在互联网中，全球各地不同品牌、型号的计算机与网络设备，正是依靠各类网络通信协议，才得以顺畅交换信息，构建起庞大复杂却又井然有序的网络体系。

网络协议主要由以下三要素组成：

（1）语法：语法规定了数据与控制信息的结构和格式。如同写信时，信封上收件人地址、寄件人地址等信息，都有各自固定的书写位置和格式要求。

（2）语义：语义定义了通信过程中需要发出的控制信息，以及对应的动作和响应。这和我们写信时，信件内容所表达的请求、询问等不同含义，对方会依据这些含义给出对应回复的道理是一样的。

（3）同步：同步确定了事件实现顺序的具体说明，也就是通信过程中各种操作的先后顺序。还以我们写信过程为例，对方收到信后会先阅读，然后再根据内容决定何时回信。

1.3.2 协议的分类与作用

1. 协议的分类

协议的分类方式多样，从功能层次角度划分具有鲜明的层级特征。

低层协议聚焦物理介质与数据传输基础环节。在工业自动化生产线中，大量设备通过现场总线连接，采用的 PROFIBUS 协议作为成熟现场总线协议，具有传输速度快、可靠性高的特点。它作为典型的低层协议，规定了数据在总线上的传输格式与访问方式，确保众多传感器、执行器等设备能有序地传输数据，协同完成生产任务，解决了工业环境中设备密集、数据交互频繁时共享物理传输介质的冲突问题。在家庭宽带接入场景中，调制解调器完成数模信号转换，PPPOE 协议依托该线路实现拨号认证，让家庭用户能借助电话线路等模拟信道，稳定地连接到互联网，将家中计算机、智能电视等设备产生的数字数据

转化为适合电话线传输的模拟信号，反之亦然。

高层协议则更侧重数据的处理与应用交互。在电商购物场景下，超文本传输协议（HTTP）支撑着整个交易流程的信息交互。用户在浏览器中浏览商品页面、将商品加入购物车、提交订单等操作，浏览器都遵循 HTTP 协议向电商服务器发送请求，服务器也依据此协议返回对应的页面数据、处理结果等，使得全球范围内的用户能顺畅地进行在线购物。

2. 协议的作用

协议在网络通信中发挥着不可替代的核心作用。

从基础保障层面，它通过统一的数据格式与交互规则，消除了不同厂商设备间的硬件差异与实现细节差异。例如，在大型数据中心，来自不同厂商的服务器、存储设备与网络交换机，只要都遵循相同协议，就能顺畅地构建起高速稳定的内部网络，实现数据的快速存储与读取。

在传输规范层面，协议通过明确的时序控制与流程定义提升了通信效率，如在无线传感器网络中，采用时分多址（TDMA）协议，通过为每个传感器节点分配特定的时间片来发送数据，避免了数据冲突，使有限的无线带宽得到有序利用，高效地收集环境监测数据。

同时，协议的规范性也为网络故障排查提供了依据，当通信出现异常时，技术人员可依据协议规则逐层定位问题，大幅降低了网络维护的复杂度。例如，在校园网络出现卡顿、部分网站无法访问等故障时，网络管理员可根据网络层的 IP 协议、传输层的 TCP/UDP 协议等规则，检查路由设置、端口状态等，快速找到故障点并解决，这种标准化的通信框架，既是网络设备互通的技术基础，也是网络规模扩张与功能升级的重要支撑。

1.4 计算机网络体系结构

1.4.1 网络体系结构的分层设计

两个系统中实体间的通信是一个很复杂的过程，为了降低协议设计和调试过程的复杂性，也为了便于对网络进行研究、实现和维护，促进标准化工作，通常对计算机网络的结构以分层的方式进行建模。

我们把计算机网络的各层及其协议的集合称为网络的体系结构（Architecture）。换言之，计算机网络的体系结构就是这个计算机网络及其所应完成的功能的精确定义，它是计算机网络中的层次、各层的协议及层间接口的集合。需要强调的是，这些功能究竟是用何种硬件或软件完成的，则是一个遵循这种体系结构的实现问题。体系结构是抽象的，而实现是具体的，是真正在运行的计算机硬件和软件。

计算机网络体系结构的分层需遵循以下基本原则：

（1）每层实现相对独立的功能，以降低大系统的复杂度；

（2）各层间界面应自然清晰、易于理解，且相互间的交互应尽可能少；

(3) 每层功能的精确定义需独立于具体实现方法,以便采用最合适的技术完成实现;

(4) 保持下层对上层的独立性,上层仅单向使用下层提供的服务;

(5) 整个分层结构还应能促进标准化工作。由于分层后各层相对独立且灵活性好,这种体系结构不仅易于更新(如替换单个模块)、调试、交流和抽象,也利于标准化工作的推进。

不过,层次过多会导致部分功能在不同层中重复出现,产生额外开销,降低整体运行效率;而层次过少则会使每层的协议过于复杂。因此,分层时需在层次的清晰程度与运行效率、层次数量之间进行合理折中。分层后的网络从低层到高层依次被称为第 1 层、第 2 层……第 n 层,通常还会为每层赋予特定名称,例如,第 1 层称为物理层。

采用分层结构设计的典型网络体系结构如下图 1-17 所示。

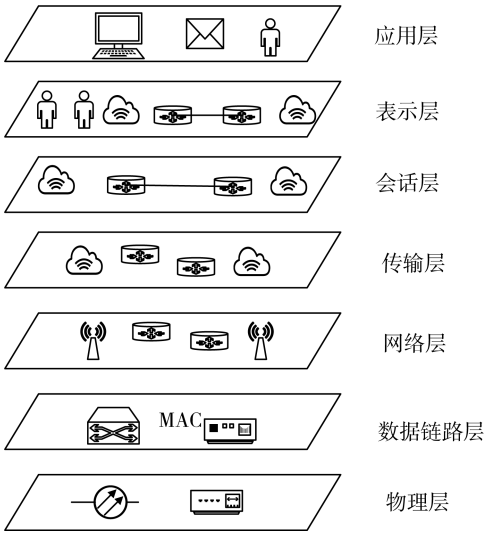


图 1-17　采用分层结构设计的典型网络体系结构

在计算机网络的分层结构中,第 n 层中的活动元素通常称为 n 层实体。具体来说,实体指任何可发送或接收信息的硬件或软件进程,可由软件或硬件功能模块实现。不同机器上的同一层称为对等层,同一层的实体称为对等实体。n 层实体实现的服务为 $n+1$ 层所利用。在这种情况下,n 层被称为服务提供者,$n+1$ 层则服务于用户。

在计算机网络体系结构的各个层次中,对等层次之间传送的数据单位称为该层的 PDU,第 n 层的协议数据单元记为 n-PDU。每个报文(PDU)均由服务数据单元(SDU)和协议控制信息(PCI)两部分组成。其中,服务数据单元(SDU)为完成用户所要求的功能而应传送的数据,协议控制信息(PCI)为控制协议操作的信息。

在实际的网络中,每层的协议数据单元都有一个通俗的名称,如物理层的 PDU 称为比特;链路层的 PDU 称为帧;网络层的 PDU 称为分组;传输层的 PDU 称为段或用户数据报。

在各层间传输数据时,发送方把从第 $n+1$ 层收到的 PDU 作为第 n 层的 SDU,加上第 n 层的 PCI,就变成了第 n 层的 PDU,接收方接收时做相反的处理,其变换过程如图 1-18 所示。

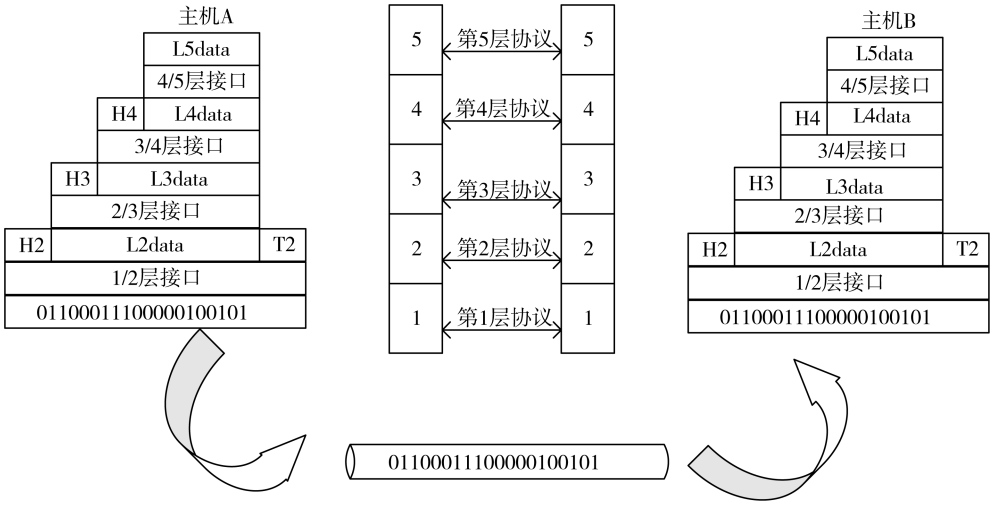


图 1-18　网络体系结构的各层次数据单元的关系

层次结构的含义具体可从以下几方面理解：

(1) 第 n 层的实体需借助第 $n-1$ 层的服务来完成自身功能，同时向第 $n+1$ 层提供服务，而该服务是第 n 层及其之下所有层次服务的总和。

(2) 最低层仅承担服务提供的角色，是整个层次结构的根基；中间各层具有双重身份，既是下一层服务的使用者，又是上一层服务的提供者；最高层则直接面向用户提供服务。

(3) 上一层只能通过与相邻下一层的接口获取服务，不可直接调用其他层次的服务；并且，下一层服务的具体实现细节，对上一层而言是不可见的(即透明)。

(4) 两台主机进行通信时，对等层可以认为在逻辑上存在一条直接的信道，能将信息直接传递给对方。

1.4.2　接口、服务的概念

1. 接口

在计算机网络协议的分层体系结构中，接口是同一节点相邻两层之间交互的边界，是实现层次间服务传递的关键机制，每层只能为紧邻的层次之间定义接口，但不能跨层定义接口。相邻两层的实体通过服务访问点(Service Access Point，SAP)进行交互。接口定义和规范了上层实体如何访问下层实体提供的服务，明确了服务请求的形式、参数格式及响应方式，为层次间的协作提供了交互标准。

接口的核心功能是实现服务的透明调用。上层实体无需知晓下层服务的具体实现细节，仅需通过接口规定的操作即可获取服务，这种隔离性使得各层可独立演进，下层可在不改变接口规范的前提下优化实现方式，上层也可基于稳定的接口扩展功能，极大提升了体系结构的灵活性与可维护性。

2. 服务

服务是指下层为紧邻的上层提供的功能调用，它是垂直的。上层使用下层所提供的服务时必须与下层交换一些命令，这些命令在 OSI 中称为服务原语。OSI 将原语划分为 4 类：

(1) 请求(Request)。由服务用户发往服务提供者，请求完成某项工作。

(2) 指示(Indication)。由服务提供者发往服务用户，指示用户做某件事情。

(3) 响应(Response)。由服务用户发往服务提供者，作为对指示的响应。

(4) 证实(Confirmation)。由服务提供者发往服务用户，作为对请求的证实。

这 4 类原语用于不同的功能，如建立连接、传输数据和断开连接等。有应答服务包括全部 4 类原语，而无应答服务则只有请求和指示两类原语。

需特别注意的是，接口与服务、协议存在本质区别：服务是下层为相邻上层提供的功能集合，协议是对等层实体间的通信规则，而接口则是服务的访问入口。

我们再进一步分析网络协议和网络服务在层次结构中的关系，可归纳为“协议是水平的，服务是垂直的”。

所谓协议是水平的，是因为协议是在同一层次上不同节点之间通信时所遵循的规则和约定。协议的作用是确保不同设备或系统在相同层次上能够正确地交换和理解数据。也就是说，协议只在同一层次的对等实体之间生效。

如何理解服务是垂直的呢？如前文所述，服务是指相邻层次之间提供的功能和接口。每一层通过上层提供的服务接口向上层提供服务，同时使用下层提供的服务接口来实现其功能。服务是垂直的，因为它涉及相邻层次之间的交互。

这种层次化的结构使得网络协议的设计更加模块化和易于管理，同时也提高了网络系统的灵活性和可扩展性。

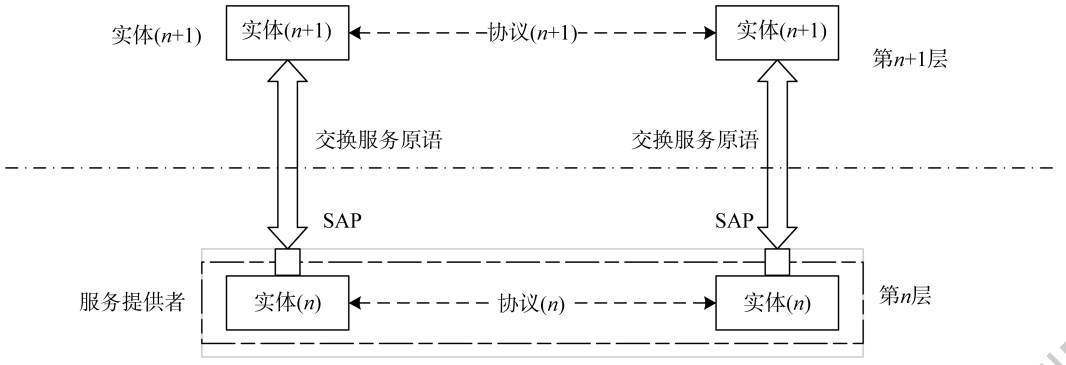


图 1-19　协议、服务、接口的关系

1.4.3　OSI 参考模型和 TCP/IP 参考模型

20 世纪 70 年代末，随着计算机网络应用的逐渐普及，不同网络系统之间的互操作性

问题变得日益突出。为了实现不同网络之间的无缝连接和通信，国际标准化组织（International Organization for Standardization，ISO）在 1984 年颁布了开放系统互连参考模型（Open System Interconnection Reference Model，OSI）。OSI 模型采用分层设计，共分为七个层次，从下到上分别为物理层、数据链路层、网络层、传输层、会话层、表示层和应用层。低三层统称为通信子网，它是为了完成数据的传输功能；高三层统称为资源子网，主要完成数据处理等功能；传输层则承上启下。

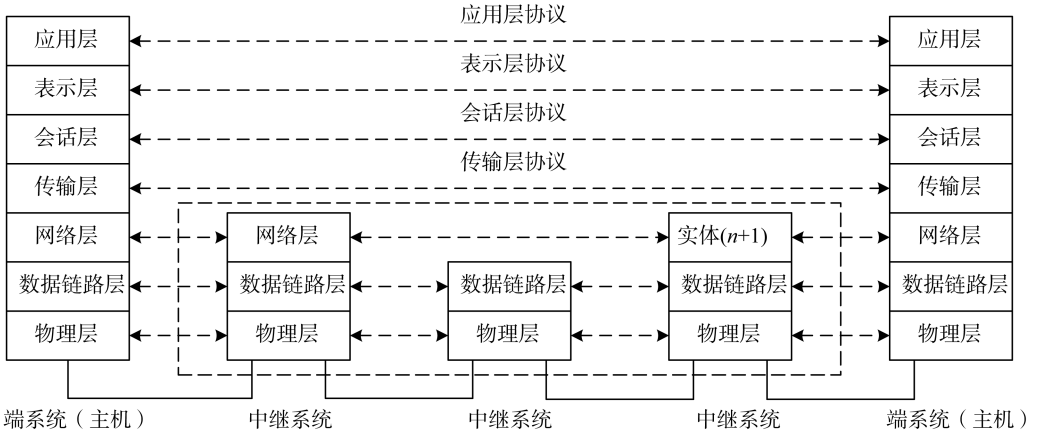


图 1-20　ISO/OSI 参考模型的层次结构

OSI 模型试图为全球范围内的计算机网络通信制定一套统一的标准，使得不同厂商的设备和软件能够在一个开放、兼容的环境下进行通信。尽管该模型在理论研究领域收获颇丰，为网络通信理论的发展贡献了清晰的分层架构、规范的通信概念等成果，但在市场化推广进程中却遭遇重大挫折，始终未能在实际应用市场中占据主导地位。其原因在于以下几点：

1. 协议设计过于复杂

由于 OSI 协议构建了七层结构，每一层的功能划分都极为严格与精细，从底层物理介质上的比特流传输，一直延伸到顶层应用程序间的交互，各层之间的交互流程极为繁杂。以会话层为例，不仅要处理会话的建立、维持和拆除等操作，还要应对不同应用场景下会话同步的各类复杂状况；而表示层则需承担数据编码转换、加密解密等多项功能。如此复杂的设计，致使在实际开发过程中，难度超乎想象。这不仅需要投入大量的人力、物力以及时间成本，在后续的调试与维护环节，也困难重重。许多企业在尝试实现 OSI 协议栈时，发现技术难度远超预期，开发周期大幅延长，产品成本急剧上升，这使得众多厂商对其敬而远之。

2. 与实际市场需求脱节

OSI 协议先构建理论模型，再依此开发具体协议，这一模式导致其在实际应用场景中与市场需求存在偏差。在制定模型时，过于追求理想化的通用性与全面性，却未能充分考

量当时市场上已有的网络技术和应用需求。在网络应用发展初期，企业和用户最为关注的是实现网络通信的基本功能，如文件传输、远程登录等，对于会话层和表示层的一些复杂功能，需求并不强烈。但 OSI 协议却在这些相对次要的功能上投入了大量精力，致使协议整体在满足市场核心需求方面表现欠佳，无法迅速、有效地解决实际网络通信问题，自然难以获得市场的认可。

3. 面临强大竞争对手

在 OSI 协议发展的同一时期，另外一种协议模型 TCP/IP 已在实践中逐步成熟并得到广泛应用。TCP/IP 协议从一开始就以满足实际网络互联需求为目标，历经美国国防部高级研究计划局（ARPA）网络项目的实践检验，不断优化改进。与 OSI 协议相比，TCP/IP 协议体系结构更为简洁，仅包含四个层次，却能更高效地实现网络通信功能。随着互联网的迅猛发展，TCP/IP 协议借助在互联网中的广泛应用，积累了庞大的用户和开发者群体，形成了成熟的生态系统。当 OSI 协议进入市场时，TCP/IP 协议早已占据先发优势，在市场份额和用户认知度方面具有压倒性优势，这使得 OSI 协议在竞争中处于极为不利的境地，难以突破市场壁垒，实现大规模推广。

TCP/IP 协议的四层结构为：应用层、传输层、网际层和网络接口层。实际上，TCP/IP 协议只定义了最上面的三层标准，最底层的网络接口层使用所属不同局域网的标准。

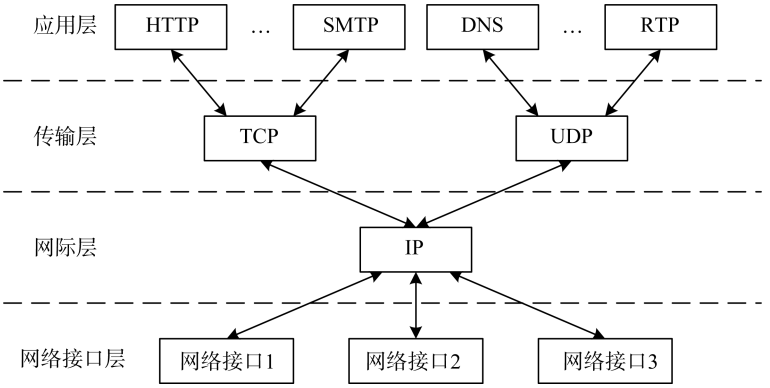


图 1-21　TCP/IP 模型的层次结构

在此需要说明的是，本教材既没采用 OSI 协议的七层结构，也没采用 TCP/IP 协议的四层结构进行教学，而是遵循大多数教材的思路，基于 OSI 和 TCP/IP 协议模型，生成如图 1-22 所示的一种原理协议的五层体系结构，以此去分析计算机网络通信的原理。请读者务必注意，五层体系结构的原理协议在实际中是不存在的，仅仅为了方便我们学习、掌握协议体系结构的原理。

如图 1-22 所示，OSI 协议模型的七层结构涵盖物理层到应用层，细致划分网络通信各环节。TCP/IP 协议模型的四层结构则把 OSI 协议模型的物理层与数据链路层合并为网络接口层，并将 OSI 协议模型的表示层和会话层功能纳入应用层，极大简化了模型的系统结构。本教材原理协议为清晰地分步讲解底层核心技术，让教学逻辑更明确，考虑到

TCP/IP 协议模型中网络接口层所包含的物理层和数据链路层，功能差异显著，将其拆分教学。原理协议的物理层负责比特流传输，数据链路层保障本地链路数据可靠，网络层负责路由，传输层提供端到端通信，应用层对接用户程序。设计理念上，OSI 重理论完备，TCP/IP 重实用，原理协议的五层结构兼顾理论与实践。

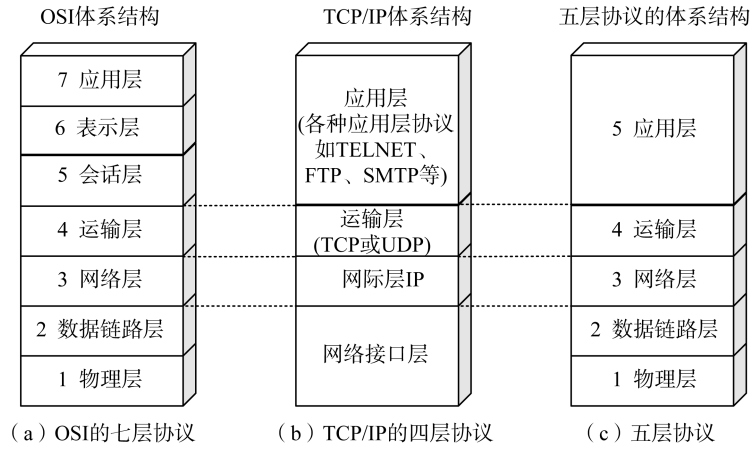


图 1-22　计算机网络体系结构

下面结合互联网情况，自上而下，简要介绍五层原理协议每个层次的主要功能。读者在此不需要拘泥每层的技术细节，而只需要建立整体的协议框架概念，了解协议层次结构，细节部分将在后继章节具体展开学习。

1. 应用层（Application Layer）

应用层是计算机网络五层协议模型中的最高层，是用户与网络的界面。其主要任务是通过规范应用进程间的交互来完成特定的网络应用。应用层协议就是规范的体现，其定义了应用进程之间的通信和交互规则，确保不同应用程序能够高效、安全地进行数据传输。

因为用户的实际应用多种多样，这就要求应用层采用不同的应用协议来解决不同类型的应用要求，因此，应用层是最复杂的一层，使用的协议也最多。应用层协议利用用户与网络之间的接口，为各种网络应用服务。例如，网页浏览需要快速响应和高可靠性，因此使用 HTTP 或 HTTPS 协议；文件传输需要高效率和数据完整性，因此使用 FTP 或 SFTP 协议；电子邮件需要可靠的传输和存储，因此使用 SMTP、POP3 或 IMAP 协议。此外，随着网络技术的发展，新的应用场景不断涌现，如物联网、实时通信等，也需要相应的应用层协议来支持。多种应用层协议的存在不仅满足了不同应用的需求，还促进了网络技术的创新和发展。如为了提高网络通信的安全性，HTTPS 协议在 HTTP 的基础上引入了 SSL/TLS 加密机制。

因五层结构的应用层实际还包含了 OSI 协议模型的表示层和会话层，在此简单进行功能介绍。

（1）表示层主要处理在两个通信系统中交换信息的表示方式。不同机器采用的编码

和表示方法不同，使用的数据结构也不同。为了使不同表示方法的数据和信息之间能互相交换，表示层采用抽象的标准方法定义数据结构，并采用标准的编码形式。另外，数据压缩、加密和解密也是表示层可提供的数据表示变换功能。

比如，当一台采用 ASCII 编码的 Windows 电脑与一台使用 EBCDIC 编码的大型主机传输文本时，发送方的表示层会将本地 ASCII 编码转换为双方约定的标准编码（如 Unicode），接收方的表示层再将标准编码转换为本地的 EBCDIC 编码，确保文本内容准确解读。这个过程就体现了表示层在数据格式转换方面的作用。

（2）会话层允许不同主机上的各个进程之间进行会话。会话层利用传输层提供的端到端的服务，向表示层提供它的增值服务。这种服务主要为表示层实体或用户进程建立连接并在连接上有序地传输数据，这就是会话。

会话层负责管理主机间的会话进程，包括建立、管理及终止进程间的会话。会话层可以使用校验点使通信会话在通信失效时从校验点继续恢复通信，实现数据同步。

比如，当用户通过视频会议软件进行在线会议时，会话层便发挥着关键作用。它会先在参与会议的各设备进程间建立会话连接，确保数据传输通道的有序开启；在会议进行中，会话层会持续管理该会话，比如通过设置校验点（如同视频会议中的定期画面同步标记），若因网络波动导致数据传输中断，恢复连接后可从最近的校验点继续传输，避免从头重传，保障会议内容的连贯性；当会议结束时，会话层则会终止该会话连接，释放相关资源。这一过程完整体现了会话层对进程间会话的建立、管理与终止功能，以及利用校验点实现数据同步的作用。

2. 传输层（Transport Layer）

传输层是计算机网络五层协议模型中的第二层，位于应用层和网络层之间。其主要功能是为应用层提供端到端（两台主机进程之间的通信）的可靠数据传输服务，确保数据能够准确、高效地从发送方传输到接收方。传输单位是报文段（TCP）或用户数据报（UDP）。

传输层允许多个应用进程共享同一网络连接，因此具有复用和分用功能。复用功能可将多个应用进程的数据流合并为一个传输层数据流发送；分用功能则在接收端将数据流正确分配到对应的接收应用进程。例如，用户可以在同一台计算机上同时浏览网页和发送邮件，传输层通过传输层的端口号区分这些应用的数据流。

为保证数据传输的可靠性，传输层还具有可靠传输、流量控制、拥塞控制等功能，可靠传输是通过序列号、确认应答和重传机制，确保数据按顺序、无错误地到达接收方。流量控制是通过调节发送方的数据传输速率，以匹配接收方的处理能力，避免接收方缓冲区溢出。拥塞控制是通过监测网络状态，动态调整数据传输速率，防止网络拥塞而丢弃数据。

传输层的两种主要协议：

（1）传输控制协议（Transmission Control Protocol，TCP）

TCP 是一种面向连接的协议，提供可靠的、有序的、错误检测的数据传输服务。TCP 通过三次握手建立连接，使用滑动窗口机制进行流量控制，并在检测到错误时重传丢失的数据段。

(2) 用户数据报协议(User Datagram Protocol,UDP)

UDP是一种无连接的协议,提供尽最大努力但不可靠的数据传输服务。由于UDP不建立连接,不保证数据的可靠传输,适用于对实时性要求较高的应用,如视频流和在线游戏。

因此,传输层通过复用和分用功能,实现了多个应用进程对网络资源的高效共享,同时通过TCP和UDP两种协议,满足了不同应用对可靠性和实时性的不同需求。

3. 网络层(network layer)

网络层是计算机网络五层协议模型中的第三层,支持异构网络互联,即不同类型的网络(如局域网、广域网)可以通过无连接的网际协议IP(Internet Protocol)实现互联互通。网络层主要功能是从通信子网选择合适的路径将源主机的数据传输到目的主机。

网络层核心任务包括路由选择和分组转发。

(1) 路由选择

路由选择是指网络层通过路由算法确定数据包在网络中传输的合适路径。常见的路由选择协议包括RIP(路由信息协议)、OSPF(开放最短路径优先)和BGP(边界网关协议)。

(2) 分组转发

分组转发指路由器接收数据包后,根据数据包的目的地址查找路由表,将数据包转发到正确的输出端口。这一过程是网络层实现数据传输的关键步骤。

完成网络层核心任务的通信设备是路由器,路由器具有连接不同网络、转发数据包、路径选择与优化等功能。

4. 数据链路层(Data Link Layer)

数据链路层是确保两个相邻节点间无差错的传输以帧为单位的数据。这边需要重点指出的是,数据链路层提供的是点到点的通信,传输层提供的是端到端的通信,两者完全不同。

假设两台计算机通过以太网电缆连接,那么传输数据的过程中可能会出现比特错误或帧丢失的情况。为了确保数据能够可靠传输,需要引入数据链路层功能。数据链路层将网络层交下来的IP分组组装成帧(Frame),每个帧包括数据和其他控制信息。控制信息实现帧同步、差错控制、流量控制、介质访问控制等功能。其中,帧同步负责将比特流封装成帧,并在帧的开头和结尾添加特殊的标志,以便接收方能够准确地识别帧的边界;差错控制通过循环冗余校验(CRC)等技术检测并纠正传输中的错误;流量控制则通过调节发送方的数据传输速率,以匹配接收方的处理能力,防止接收方缓冲区溢出;介质访问控制负责在共享介质(如以太网)中协调多个设备对共享介质的访问,避免冲突。

数据链路层的引入使得网络能够以帧为单位进行数据传输,提高了数据传输的可靠性和效率。

5. 物理层(Physical Layer)

物理层是计算机网络五层协议模型中的最底层,主要实现在数据链路层的实体间提供一个物理链路,通过网络接口和不同的传输介质实现比特流传输,其传输数据的单位是比特。

计算机网络中两台计算机进行数据传输时,数据从发送方的网络接口卡(Network Interface Card,NIC)发出,它需要以电或者光信号的形式在物理介质(如双绞线或光纤)上传播。然而,数据在物理介质上的传输会受到多种因素的影响,例如,信号衰减、噪声干扰和传输距离限制。如果没有一个专门的物理层来处理这些物理传输问题,数据将无法可靠传输。

物理层为完成物理介质上比特流的传输,如发送方发送 1 或者 0 时,接收方应该收到对应的 1 或者 0,需详细定义传输介质的物理特性,包括:规定多大电压表示 1,多大电压表示 0 以及电流和阻抗等参数,确保信号能够在物理介质上传输。定义连接器的形状、尺寸和引脚排列,确保设备之间的物理连接。说明哪些信号表示数据,哪些信号表示控制信息。规定数据传输的顺序和速率,以及如何建立和释放物理连接。

物理层的存在使得数据能够在不同类型的物理介质上传输,同时为上层协议提供了一个可靠的数据传输基础。例如,在以太网中,物理层定义了双绞线和光纤的电气和光学特性,确保数据能够在这些介质上高效、准确地传输。

有了以上对协议模型每层内容的了解,我们可以开始初步学习不同主机间应用进程通信过程。

由图 1-23 可知,主机 1 和主机 2 通过核心通信设备路由器进行连接。主机 1 的协议为 5 层,主机 2 的协议也对应 5 层。由于路由器工作在网络层,所以不需要应用层和传输层,因此协议为 3 层。路由器具有多个接口,每个接口可以连接不同局域网,在本图中路由器通过两个接口分别连接了主机 1 和主机 2,每个接口拥有 1、2 层功能。在 TCP/IP 协议中,1、2 层被合并叫作网络接口层。

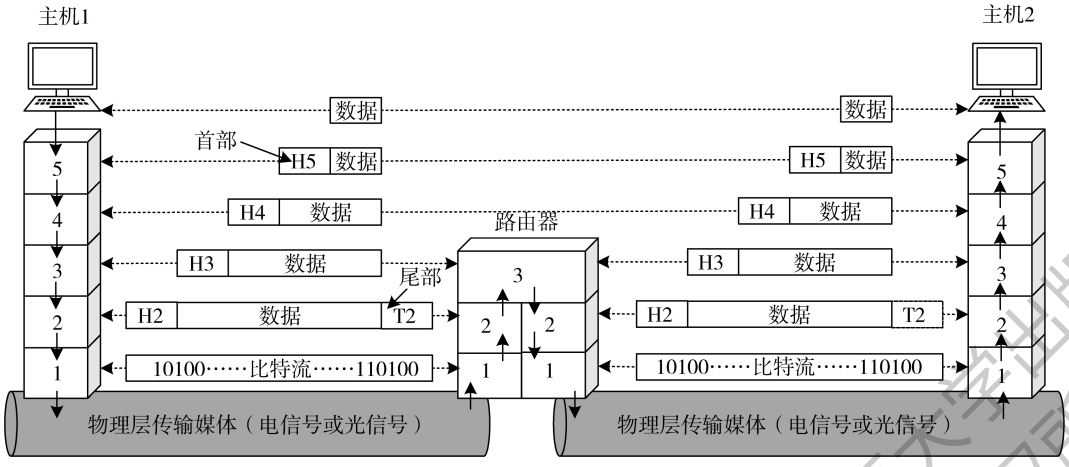


图 1-23　数据在各层间传递过程

我们分析主机1的进程AP1向主机2的进程AP2传输数据的过程，该过程中，主机1将数据发送给路由器，路由器将数据转发给主机2。

主机1的数据封装以及发送过程为：

(1) AP1首先将数据交给本机的第5层应用层。应用层协议(如HTTP、FTP、SMTP等)将用户数据封装成应用层报文。添加应用层头部H5，H5包含协议相关信息。

(2) 传输层协议(如TCP或UDP)接收上层的应用层报文，添加传输层头部H4(如TCP头部或UDP头部)，包含源端口、目的端口、序列号、确认号等信息，将应用层报文封装成传输层报文(TCP报文或UDP报文)。

(3) 网络层协议(如IP协议)接收上层的传输层报文，添加网络层头部H3(IP头部)，包含源IP地址、目的IP地址、协议类型等信息，将传输层报文封装成IP数据报。

(4) 数据链路层协议接收上层的IP数据报，添加数据链路层头部H2(如以太网帧头部)，包含源MAC地址、目的MAC地址等信息，并添加数据链路层尾部(如CRC校验码)。将IP数据报封装成数据链路层帧。

(5) 物理层将上层的数据链路层帧转换为比特流(电信号或光信号)，并通过物理介质(如双绞线、光纤)发送到网络。

路由器接口收到数据后，完成以下操作：

(1) 物理层接收比特流，并将其转换为数据链路层帧。

(2) 数据链路层解封装帧头部和尾部，提取IP数据报上传给网络层。

(3) 网络层根据IP头部中的目的IP地址，决定将数据报转发到下一跳，即目标主机2。

(4) 数据再次被封装成数据链路层帧，以比特流(电信号或光信号)形式发送给目标主机2。

主机2对数据接收和解封装过程为：

(1) 物理层接收比特流，并将其转换为数据链路层帧。

(2) 数据链路层解封装帧头部和尾部，提取IP数据报，并检查CRC校验码，确保数据的完整性。

(3) 网络层解封装IP头部，提取传输层报文，并根据IP头部中的协议类型，将数据传递给相应的传输层协议。

(4) 传输层解封装TCP头部或UDP头部，提取应用层报文，并根据目的端口号，将数据传递给相应的应用层协议。

(5) 应用层解封装应用层头部，提取用户数据，将用户数据交付给主机2的应用进程。

整个过程中，数据在发送方被逐层封装，在接收方被逐层解封装，确保数据能够正确地从主机1传输到主机2，并交付给目标应用进程。

1.4.4 云计算及边缘计算

前面我们学习了OSI七层模型和TCP/IP协议框架以及五层原理协议模型，这些经

典体系为计算机网络的标准化通信提供了基础。但随着物联网、大数据和人工智能技术的快速发展，终端设备数量激增，数据产生量呈指数级增长，传统的“终端-中心服务器”集中式通信模式开始面临新的挑战。例如，远程数据传输带来的延迟可能影响实时应用的体验，海量数据全部上传至中心服务器也会造成带宽压力和处理效率问题。为应对这些挑战，云计算与边缘计算两种新型计算模式逐渐成为主流，它们在经典协议的基础上，形成了适应不同场景的协议框架与通信逻辑。

1. 云计算

云计算的核心思想是将计算、存储等资源集中部署在远程数据中心（即“云端”），用户通过网络按需获取服务。其模型如图 1-24 所示。

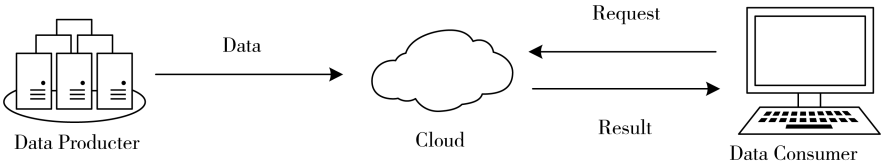


图 1-24　传统云计算模型

从协议框架来看，它以 TCP/IP 协议族为基础，形成了层次化的通信体系：

用户终端（如手机、电脑）作为服务请求方，通过 HTTP/HTTPS、WebSocket 等应用层协议向云端发送请求，比如我们在浏览器中访问在线文档、调用云服务器的数据分析接口时，使用的就是这些协议；

在网络传输层面，依赖 TCP 协议保证数据的可靠传输，通过 IP 协议完成路由选择，确保请求能够跨越复杂的网络环境到达云端数据中心；

在云端内部，为了高效管理海量服务器和资源，会采用分布式协议，如 Hadoop 的 HDFS 分布式文件系统用于数据存储，Kubernetes 的容器编排平台用于任务调度，这些协议使得云端能够像一个“超级计算机”一样协同工作。其通信过程遵循“请求-响应”模式，终端发起服务请求，云端处理后返回结果，就像我们向远方的图书馆借阅书籍，图书馆（云端）整理好书籍后通过快递（网络协议）送达我们手中。

云计算模式适用于对实时性要求不高、需要大规模计算或存储的场景，例如，云存储服务（如百度云）、在线办公软件（如腾讯文档）以及大规模数据分析（如电商平台的用户行为分析）等。

2. 边缘计算

与云计算不同，边缘计算则将部分计算任务从云端下沉到网络边缘——即靠近终端设备的节点，如基站、路由器、物联网网关等，从而减少数据传输距离和延迟。其模型如图 1-25 所示。

边缘计算的协议框架更强调“本地化处理”，在经典协议基础上增加了针对边缘场景的轻量级协议：物联网终端（如智能摄像头、工业传感器）通常通过 MQTT、CoAP 等协议

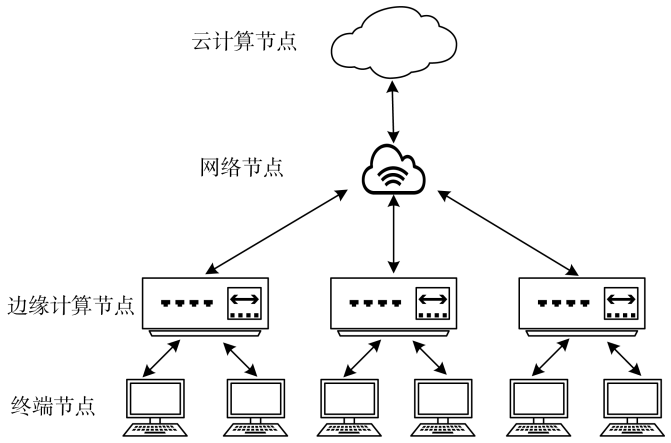


图 1-25　边缘计算模型

与边缘节点通信，这些协议设计简洁，适合低带宽、高延迟的环境，比 HTTP 更节省资源；边缘节点之间则通过 P2P 协议或局域网协议（如 Wi-Fi、蓝牙）协同工作，能够快速处理本地产生的数据，例如，智能摄像头通过边缘节点实时识别异常行为，无需等待云端响应；对于需要全局分析的数据，边缘节点会将汇总后的结果而非原始数据，通过 TCP/IP 协议上传至云端，由云端完成最终的存储和优化，比如，在城市交通系统中，路口的边缘节点处理实时车流数据，再将汇总信息上传至云端进行全局交通调度。

这种模式中，边缘节点既是本地服务的提供者，又可作为云端与终端的中转者，很好地满足了实时性要求高的场景需求，如自动驾驶（车辆需实时处理传感器数据以规避障碍）、工业物联网（生产线设备需实时监控运行状态）、智能安防（摄像头需快速识别异常情况）等。

值得注意的是，云计算与边缘计算并非相互替代，而是互补协同的关系。在实际应用中，两者常结合形成“云-边协同”体系：边缘节点处理实时、高频的本地任务，减轻云端压力；云端则负责全局数据的存储、长期分析和优化，为边缘节点提供策略支持。它们之间通过标准化协议实现数据交互，例如，边缘节点通过 MQTT 协议向云端上报汇总数据，云端通过 HTTPS 协议向边缘节点下发更新配置。这种协同模式既利用了边缘计算的低延迟优势，又发挥了云计算的大规模处理能力，是应对复杂场景的有效方案。

从本质上看，无论是云计算的集中式通信，还是边缘计算的分布式交互，都没有脱离 TCP/IP 等经典协议的支撑，而是根据具体场景对协议进行了针对性组合与优化。这也体现了网络协议的发展逻辑：经典体系提供基础规则，而新兴技术则在其之上，根据实际需求不断演化出更具适应性的框架。理解这一点，有助于我们更深入地把握网络技术的发展脉络。

1.5 计算机网络主要性能指标

计算机网络的性能指标是衡量网络系统运行效率和质量的关键参数。下面介绍常用的一些性能指标。

1.5.1 速率

在网络性能评估中，速率(Rate)通常指单位时间内传输的数据量，反映了网络传输数据的快慢，单位为 bit/s(比特每秒)或 B/s(字节每秒)，表示每秒传输的比特数或字节数。当数据量较大时，还可用千比特每秒、兆比特每秒、吉比特每秒、太比特每秒等单位，其换算方式如下：

千比特每秒(kbps)：1 kbps=1 000 bps

兆比特每秒(Mbps)：1 Mbps=1 000 kbps=1 000 000 bps

吉比特每秒(Gbps)：1 Gbps=1 000 Mbps=1 000 000 000 bps

太比特每秒(Tbps)：1 Tbps=1 000 Gbps=1 000 000 000 000 bps

需要提醒读者的是，计算机中存储单位一般是以字节 Byte 为单位，一般不使用 bit 为单位。为方便表达大容量存储，常使用 KB、MB、GB、TB 等。其换算方式速率不同：

1 KB=1 024 B；

1 MB=1 024 KB=1 024×1 024 B；

1 GB=1 024 MB=1 024×1 024×1 024 B

1.5.2 带宽

1. 基本概念

带宽(bandwidth)是计算机网络领域描述通信能力的核心指标，其概念在不同技术场景中具有特定内涵，需从信号传输与数据通信两个维度进行理解。

在模拟通信系统中，带宽最初被定义为信号所占据的频率范围，即信号中包含的各种频率成分的最高值与最低值之差。例如，传统电话线路传输的话音信号，其有效频率范围为 300 Hz 至 3.4 kHz，因此标准带宽为 3.1 kHz。这种频域视角下的带宽单位为赫兹(Hz)，常用衍生单位包括千赫(kHz)、兆赫(MHz)和吉赫(GHz)等。

对于通信线路而言，其带宽表示线路允许通过的信号频带宽度(又称通信频带)。在模拟信号传输时代，线路带宽直接决定了可传输信号的复杂程度：带宽越宽，能承载的信号频率成分越丰富，传输质量越高。

在数字通信场景中，带宽的含义已演变为网络通信线路在单位时间内所能传输的最

高数据率，这也是计算机网络领域对带宽的主流表述。其单位为比特每秒(bit/s)，实际应用中常使用千比特每秒(kbit/s，1 kbit/s＝10^3 bit/s)、兆比特每秒(Mbit/s，1 Mbit/s＝10^6 bit/s)、吉比特每秒(Gbit/s，1 Gbit/s＝10^9 bit/s)等单位。

例如，100 Mbit/s 以太网的带宽定义，即表示该网络链路的最高数据传输速率为100 兆比特每秒。需要注意的是，这里的“最高数据率”是理想条件下的理论上限，实际传输速率(吞吐量)会受噪声、干扰、协议开销等因素影响而降低(如 100 Mbit/s 以太网的典型吞吐量可能仅为 70 Mb/s 左右)。

频域带宽与数据率带宽虽分属不同技术维度(前者描述频率范围，后者描述传输速度)，但存在本质联系：通信线路的频域带宽越宽，其能支持的最高数据率也越高。这是因为更宽的频带可容纳更高频率的信号变化，从而实现更快的数字信号调制与传输。这种关联构成了从模拟通信到数字通信的技术衔接点。

2. 带宽对网络性能的影响

带宽是衡量网络性能的关键指标，其数值直接影响网络的吞吐量、时延等核心特性。例如，当网络利用率(实际吞吐量与带宽的比值)接近 100%时，网络时延会急剧增加，甚至趋于无穷大。这是由于数据帧排队等待时间随利用率升高而呈指数增长。因此，为保障网络服务质量，大型 ISP(互联网服务提供商)通常将主干网利用率控制在 50%以内，当超过该阈值时，需通过扩容(如提升线路带宽)降低拥塞风险。

综上，带宽不仅是描述网络传输能力的基础参数，更是网络规划、性能优化与资源调度的重要依据，其概念演化反映了通信技术从模拟到数字的发展历程。

1.5.3 吞吐量

吞吐量(Throughput)：表示网络在实际运行中实际传输的数据量，是网络性能的直接体现。因为网络中存在延迟、拥塞等因素，实际吞吐量通常低于理论带宽。

吞吐量是衡量计算机网络实际数据传输能力的重要指标，与带宽共同构成描述网络传输特性的核心参数。在计算机网络中，吞吐量直接反映了网络的实时运行效率。其单位与带宽一致，通常为比特每秒(bit/s)，常用的衍生单位有 kbit/s、Mbit/s、Gbit/s 等。比如，某以太网链路的带宽为 100 Mbit/s，但实际测量发现每秒仅能传输 70 Mbit 的数据，那么此时该链路的吞吐量就是 70 Mbit/s。

需要明确的是，吞吐量和带宽是两个既相关又不同的概念。带宽代表的是链路的理论最高传输能力，好比高速公路的最高限速；而吞吐量则是网络在实际运行中的传输效果，类似于高速公路上车辆的实际平均行驶速度。所以，吞吐量的数值总是小于或等于链路带宽，这是因为实际传输过程中会受到多种因素的影响。两者的比值，即吞吐量与带宽的比值，被称为网络利用率，这个指标常被用来判断网络是否出现拥塞，例如，当利用率超过 50%时，网络很可能会出现明显的时延。

影响吞吐量的因素有很多。首先是网络拥塞，当多个设备同时向链路发送数据时，数据帧需要排队等待传输，这会导致实际传输速率下降，像高峰时段的校园网，由于大量用

户同时访问，吞吐量可能只有带宽的 30%～40%。其次是传输损耗，信号在传输过程中会因噪声、干扰等产生误码，进而导致数据重传，这会间接降低有效吞吐量，尤其是无线链路，受环境影响更大，雨雾天气可能使吞吐量下降 20%～50%。再者是协议开销，TCP/IP 协议族中的首部信息、确认帧等控制数据会占用部分带宽，比如 TCP 报文的首部开销约为 5%～10%，这就使得实际数据吞吐量低于原始比特流速率。另外，设备性能也会对吞吐量产生影响，路由器、交换机等中间设备如果处理能力不足，就会成为吞吐量的瓶颈，例如，一台老旧路由器的转发速率仅为 100 Mbps，即便连接的是 1 Gbps 带宽的链路，实际吞吐量也会被限制在 100 Mbps。

在网络性能评估中，吞吐量有着重要的作用，它是网络规划与优化的重要依据。对于视频会议、在线游戏等实时应用来说，需要保证稳定的高吞吐量，比如 4K 视频流就需要 25 Mbps 以上的持续吞吐量才能流畅传输。网络管理员通过监测吞吐量的变化，能够及时发现网络中的拥塞点，当某段链路的吞吐量长期接近带宽值时，就需要采取扩容、负载均衡等措施来缓解拥塞。同时，在网络协议设计中，吞吐量也是衡量协议效率的核心指标，以 TCP 的拥塞控制算法为例，其设计目标就是在保证数据传输可靠性的同时，最大限度地提高吞吐量。

总之，吞吐量作为衡量网络实际数据传输能力的量化指标，与带宽一起构成了评估网络性能的基础维度，理解吞吐量的特性及其变化规律，对于掌握网络运行机制有着重要的意义。

1.5.4 时延

时延(Delay)是指数据从发送方传输到接收方所需的时间。它是衡量网络性能的重要指标之一，直接影响用户体验和网络效率。时延通常由以下几个部分组成：发送时延(Transmission Delay)、传播时延(Propagation Delay)、处理时延(Processing Delay)、排队时延(Queueing Delay)。

(1) 发送时延

发送时延是指将数据从主机的发送缓冲区传输到链路所需的时间。它主要取决于数据的大小和发送速率。

在这儿要注意区分发送速率和链路带宽，发送速率是指发送方实际将数据发送到链路的速率。它通常由发送方的网络接口卡(NIC)或发送方的网络配置决定，因此发送时延发生在机器的内部。当发送数据量一定时，发送速率决定了数据从发送方的缓冲区传输到链路所需的时间。而链路带宽是指链路的最大传输速率，即链路能够支持的最大数据传输速率，但发送方的实际发送速率可能低于这个最大值。

发送时延计算公式为：

$$\text{发送时延} = \text{数据长度(bit)} / \text{发送速率(bps)}$$

假设发送数据长度为 1 000 B(8 000 bit)，链路带宽为 200 Mbps(200 000 000 bps)，发送方的发送速率为 10 Mbps(10 000 000 bps)，则发送时延为 8 000 bit/10 000 000 bps＝

0.8 ms。

(2) 传播时延

传播时延是指电磁信号在物理介质(如双绞线、光纤、无线信号等)中传播所需的时间。这个时间取决于信号传播的距离和电磁波在该介质中的传播速度。传播时延发生在机器外的传播信道上,信号传输越远,传播时延就越大。

传播时延的计算公式为:

传播时延=距离/传播速度

电磁波在不同介质中的传播速度略有不同,在真空中的传播速度最快,约为 3×10^8 m/s。在空气中,电磁波的传播速度略小于在真空中的速度,约为 2×10^8 m/s。在铜线(如双绞线)中,电磁波的传播速度约为真空中光速的 2/3,大约为 2.2×10^8 m/s。

假设信号需要在 1 000 m 的光纤中传播,光纤中的传播速度为 200 000 000 m/s,则传播时延为 1 000 m/200 000 000 m=5 μs。

这种时延在高速网络中是非常重要的考虑因素,尤其是在设计广域网和高速通信系统时。

(3) 处理时延

处理时延是指数据在网络结点(如路由器、交换机、网关等)中被处理所花费的时间。这个过程包括对数据包头部字段的分析、查找路由表、更新数据包头部信息、执行安全检查等操作。处理时延的长短受多种因素影响,包括节点的处理能力、数据包的复杂性、协议的复杂性、网络拥塞情况等。在设计和优化网络时,减少处理时延是提高网络性能的重要方面。

(4) 排队时延

排队时延是指数据在网络节点(如路由器、交换机等)的缓冲区(队列)中等待被处理和转发所经历的时间。在网络负载较高的情况下。排队时延对网络性能有显著影响。

排队时延的产生和大小受几个关键因素的影响:

网络流量负载:当网络流量超出节点的处理能力时,会导致数据包在缓冲区中排队等待,从而增加排队时延。负载越高,排队时延通常越长。

节点处理能力:节点的处理能力决定了其处理数据包的速度。如果处理能力有限,即使网络流量未超负荷,也可能导致数据包排队,增加排队时延。

数据包到达模式:数据包到达的速率和模式也会影响排队时延。如果数据包以突发方式到达,即使平均到达速率未超过节点处理能力,也可能导致瞬时的排队时延增加。

缓冲区大小:缓冲区的大小决定了节点可以存储多少等待处理的数据包。较大的缓冲区可以容纳更多数据包,但也可能延长数据包在缓冲区中的等待时间,从而增加排队时延。

队列管理策略:不同的队列管理策略(例如,先到先服务 FCFS、优先级队列等)对排队时延有不同的影响。某些策略可能优化特定类型的流量,减少某些数据包的排队时延,但可能同时增加其他数据包的排队时延。

因此,为减少排队时延,可以通过增加网络带宽、优化路由算法,减少数据包的传输路

径、使用缓存技术、平滑网络流量，减少数据包到达的突发性等策略，有效减少排队时延，提高网络的整体性能和用户体验。

如图 1-26 所示，数据在网络中的总时延就是以上四种时延的总和：

总时延＝发送时延＋传播时延＋处理时延＋排队时延

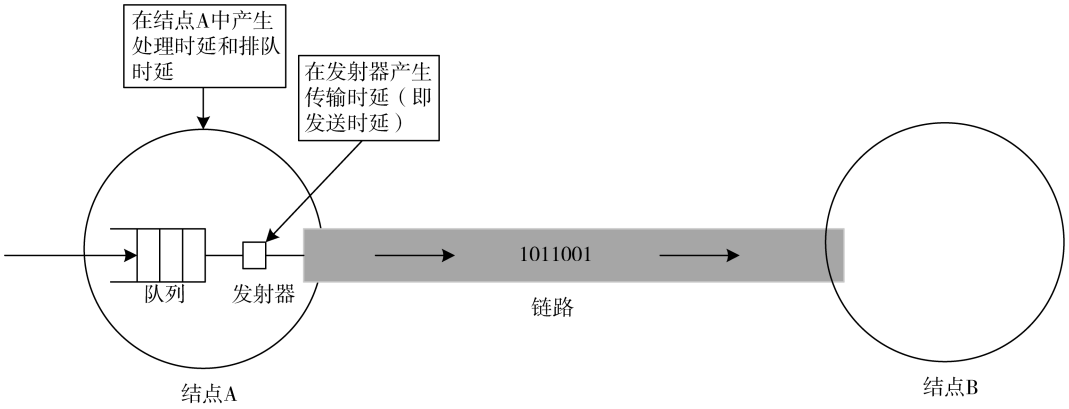


图 1-26　总时延的构成

那么在总时延中，究竟哪一种时延占据主导地位呢？这就必须具体分析。

考虑一个局域网(LAN)环境，其中数据包从一个计算机传输到另一个计算机，距离较短。在这种情况下，传播时延可能非常小，几乎可以忽略不计。如果网络设备(如交换机)的处理能力较强，处理时延也较小。如果网络负载不高，排队时延可能也不显著。因此，在这种情况下，发送时延可能是主导因素，尤其是当发送大数据包时。

相反，考虑一个广域网(WAN)环境，其中数据包需要跨越大陆甚至海洋。在这种情况下，传播时延由于长距离传输而变得显著，可能成为主导因素。

此外，如果网络节点(如路由器)的负载较高，排队时延也可能增加，进一步影响总时延。

由于总时延的主导因素取决于网络的具体配置、传输距离、网络负载和数据包大小等多种因素。理解和分析这些因素对于优化网络性能和减少时延至关重要。

1.5.5　丢包率

在大型校园网络中，学生在教室和宿舍之间移动时，由于无线网络连接不稳定，会导致视频流和在线游戏频繁出现卡顿和中断。经过调查，发现是由于无线信号在穿过墙壁和障碍物时衰减，导致数据包丢失。显然，数据包丢失将直接影响用户上网体验。

在计算机网络中，丢包率指的是在一定时间范围内，网络传输过程中丢失数据包的数量占所发送数据包总数的比例，通常用百分比表示。例如，若发送了 1 000 个数据包，其中有 10 个数据包未能成功抵达接收端，那么丢包率就是(10÷1 000)×100%＝1%。它直观地反映了网络传输的可靠性，丢包率越低，说明网络传输越稳定，数据丢失情况越少；反之，较高的丢包率则意味着网络存在问题，可能会严重影响依赖网络传输的各类应用的

正常运行。

丢包率的影响因素包括网络拥塞、链路故障、设备性能、电磁干扰等。

复习与思考

1. 请简述计算机网络的定义，并说明其与分布式系统的主要区别。

2. 从网络的组成部分来看，计算机网络通常包含哪些硬件和软件元素？请分别举例说明。

3. 计算机网络的主要功能有哪些？试结合实际应用场景，分析其中数据通信功能的重要性。

4. 按照网络的覆盖范围，计算机网络可分为哪几类？各类网络的典型覆盖范围和应用场景是什么？

5. 试论述计算机网络体系结构分层的必要性，并说明 OSI 七层模型与 TCP/IP 四层模型的对应关系。

6. 计算机网络中的“资源共享”具体指哪些资源的共享？这种共享对用户和社会产生了哪些积极影响？

7. 什么是网络协议？其三个基本要素是什么？请举例说明协议在计算机网络通信中的作用。

8. 在计算机网络的组成中，通信子网和资源子网的关系是怎样的？二者如何协同工作以实现网络功能？

9. 计算机网络发展过程中经历了哪些主要阶段？每个阶段的标志性事件或技术是什么？

10. 请分别阐述电路交换、报文交换和分组交换的基本工作原理，并对比它们在数据传输过程中的特点。

11. 在实时性要求较高的通信场景（如语音通话）中，哪种交换技术更为适用？请说明原因。

12. 比较电路交换和分组交换在建立连接、传输时延、资源利用率等方面的差异，并举例说明各自的典型应用场景。

13. 请简述计算机网络标准化工作的意义，并举出两个重要的网络标准例子。

14. 国际上有哪些主要的计算机网络标准化组织？它们各自的主要职责和代表性成果是什么？

15. 什么是计算机网络体系结构？它包含哪些核心要素？

16. TCP/IP 参考模型与 OSI 参考模型在层次划分上有何不同？两者之间存在怎样的对应关系？

17. 网络协议的三要素是什么？请分别对这三个要素进行解释。

18. 试论述 OSI 参考模型中服务、接口和协议三者之间的关系。

19. 在计算机网络体系结构中，为什么要采用分层结构？分层结构可能带来哪些潜在的问题？

20. 比较 OSI 参考模型和 TCP/IP 参考模型的优缺点。

21. 什么是网络体系结构的向下兼容？试结合 TCP/IP 协议族的发展说明其重要性。

22. 请分别给出计算机网络中协议、接口、服务的定义，并说明它们之间的联系。

23. 试分析在 OSI 参考模型中，相邻两层之间的接口如何实现服务的提供与调用，以及服务原语的类型和作用。

24. 论述协议与服务的区别和联系，并举例说明在协议族中某一层的协议如何为上层提供服务。

25. 请分别解释网络性能指标中时延、带宽、吞吐量的含义，并说明三者之间的区别与联系。

26. 网络中的时延主要由哪几部分组成？试分析在不同网络环境下，各部分时延对总时延的影响程度。

27. 什么是数据传输速率？它与带宽在概念上有何异同？通常用什么单位来表示？

28. 假设某链路的带宽为 10 Mbps，往返时间 RTT 为 100 ms，若要发送一个大小为 4 000 字节的数据包，忽略处理时延和排队时延，求总时延是多少？（注：1 字节＝8 比特）

29. 试论述影响网络吞吐量的主要因素，以及在实际应用中如何提高网络的吞吐量。

阅读与拓展

互联网双星的时空交响：文顿·瑟夫与罗伯特·卡恩的破壁之路

20 世纪 60 年代美苏冷战焦灼，核阴影下的美国因担忧集中式军事指挥系统脆弱性，催生了由通信网络连接分散指挥点、可抗损毁的分散式指挥系统设想。1958 年 2 月，美国国防部为落实分散式指挥系统设想组建 ARPA，随后将网络建设外包给波士顿的咨询公司 BBN，由其研发可接入四台主机、充当 ARPANET 网关且功能类同路由器的 IMP 设备。

1969 年 11 月，ARPANET 项目正式启动，最初仅有四个节点，分别设立在加利福尼亚州大学洛杉矶分校、加州大学圣巴巴拉分校、斯坦福大学和犹他大学的四台大型计算机上。选择这四个节点，部分原因是考虑到不同类型主机联网的兼容性。ARPANET 采用包交换机制，初期主要用于军事研究，在技术和安全层面都有严格考量，既要保证网络能经受故障考验，维持正常运行，又要在战争中部分网络受损时，其他部分仍能通信。此时的 ARPANET，从军事要求上受美国国防部高级机密保护，技术上也尚未成熟，不具备向外推广的条件。

随着时间推移，ARPANET 不断发展。1972 年，来自 BBN 公司的罗伯特·卡恩加入 ARPA，同年，他在国际计算机通信大会（ICCC）上成功演示 ARPANET 网络，这是 ARPANET 首次公开亮相。1973 年，ARPANET 借助卫星通信，实现与夏威夷、英国伦敦大学和挪威皇家雷达机构的联网，演变为国际互联网络。到 1976 年，其节点已增至 60 多个，连接 100 多台主机，覆盖美国大陆。不过，当时的 ARPANET 面临诸多挑战，尤

其是不同网络之间难以互联互通，如同一个个孤岛。彼时，ARPANET 虽在不断扩张，但不同网络有着各自的通信规则，就像不同国家使用不同的语言和文字，交流起来障碍重重。卡恩在 BBN 公司工作期间参与建立早期工业管理程序，又在 ARPA 深入接触 ARPANET 的运营，深刻体会到这种困境。他之前参与制定的“网络控制协议”(NCP)，只能在 ARPANET 内部勉强支撑通信，面对日益增多的不同类型网络，显得力不从心，无法实现真正意义上的互联。

在 ARPANET 发展的关键阶段，文顿·瑟夫与罗伯特·卡恩登上了历史舞台。1943 年 6 月 23 日，瑟夫生于洛杉矶，早产导致他自幼听力受损，需佩戴助听器。然而身体的障碍并未阻挡他对科学的热爱与求知的渴望。中学时，他结识了同样痴迷科学的好友斯蒂夫·克洛克，两人常在周末一起进行各类实验。瑟夫身材清瘦却精力充沛，性格热情外露。为躲避体操课，他加入后备军训练队，时常身穿制服或正装，手提棕色公文包。受白手起家成为公司高管的父亲影响，他广泛阅读、热爱数学与化学。在斯蒂夫的引荐下，他高中时便接触到加州大学洛杉矶分校的计算机实验室，甚至曾翻窗潜入，自此与计算机结下不解之缘。

高中毕业后，瑟夫凭借父亲公司提供的四年奖学金进入斯坦福大学主修数学，并迅速迷上计算机编程。他认为编程如同创造自己的世界，能掌控一切，这种奇妙感觉让他沉醉其中。大学毕业后，瑟夫在 IBM 担任系统工程师，支持 QUIKTRAN 工作两年，随后前往加利福尼亚大学洛杉矶分校攻读研究生学位，于 1970 年获得硕士学位，1972 年获得博士学位。在杰拉尔德·埃斯特林教授的指导下，瑟夫在莱昂纳德·克莱因洛克的数据包网络小组工作，参与连接 ARPANET 的前两个节点，为 ARPANET 贡献了主机到主机的协议。在此期间，他结识了正在研究 ARPANET 系统架构的鲍勃·卡恩，两人的合作就此拉开序幕。

罗伯特·卡恩 1938 年 12 月 23 日生于美国纽约布鲁克林。1960 年，他获纽约城市学院工程学士学位，后赴普林斯顿大学深造，于 1962 年、1964 年分别取得电气工程硕士与博士学位。1964 至 1966 年，卡恩任职于 AT&T 贝尔实验室，积累了扎实的实践经验。1966 年起，他同时担任麻省理工学院电子工程系助理教授，并在 BBN 公司工作至 1972 年，期间参与早期工业管理程序的建立。1972 年，卡恩加入美国国防高级研究计划局(DARPA)，历任信息处理技术办公室项目经理、主任及 IPTO 公司网络项目主任等职。在 DARPA 任职期间，他深刻洞悉网络互联的重要性与紧迫性，由此促成与瑟夫的合作，共同投身于网络互联难题的攻克。

1973 年 3 月的一个雪夜，卡恩带着写满想法的餐巾纸，敲响了瑟夫家的门。他提出了一个极具创新性的设想：将每个网络视为“黑箱子”。这意味着不再去深究各个网络内部的复杂构造，不管它采用了何种硬件设备、遵循怎样的内部协议，都把它当作一个独立的、不透明的整体。解决网络互联问题的关键，在于制定一套统一的数据交换规则，让这些“黑箱子”之间能够顺畅地传递信息。

卡恩提出的“黑箱子”理念，精准切中了当时网络互联的核心痛点。此前，人们为实现互联，一味追求让所有网络遵循统一的内部建设与运行标准，但不同网络的发展背景、技术路径差异悬殊，这种做法如同强令不同国家的人使用同一种语言文字，不仅难度极高，

更缺乏现实可行性。而“黑箱子”理念则另辟蹊径：它无需改变各网络的固有特性，只需像在不同网络间搭建一座通用桥梁——桥梁两端的网络可保留自身特色，只需在数据“过桥”时遵循统一规则即可实现顺畅互通。这套数据交换规则包含四大关键环节：以统一“包装”完成数据封装、为设备分配唯一“地址”实现精准寻址、依据网络实时状况动态选择传输路径，以及在数据传输出现问题时及时启动补救机制。

瑟夫对此深表赞同，两人在壁炉火光映照下，就如何给数据包贴“地址标签”、处理传输错误等问题展开推演。经过彻夜探讨，TCP 协议的核心框架初步成型。此后，卡恩凭借丰富的实践经验和对网络本质的深刻洞察，提出“端到端原则”，去除网络中冗余控制功能，将智能赋予终端设备；瑟夫则凭借扎实的理论基础和出色的代码能力，设计出用 20 个字节字段构建全球通用“数据护照”的 TCR 基础头部格式。1974 年，两人在《IEEE 通信学报》发表论文，阐述“网关”如同能听懂所有网络“方言”的翻译，帮助数据包找到目的地的观点，为网络互联指明方向。

然而，他们的技术探索并非一帆风顺。国防高级研究计划局（DARPA）的官员对为可能无法相连的网络设计通用协议表示质疑，认为成本过高且缺乏实际意义。瑟夫在办公室黑板上画下 Möbius 环，写下“最简单的结构，往往包容性最强”，表达对简单通用结构强大生命力的坚定信念。事实证明瑟夫是正确的，1983 年 1 月 1 日，ARPANET 正式切换到 TCP/IP 协议，异构网络间数据互通瓶颈被打破，效率大幅提升，TCP/IP 协议的优势尽显。

更值得称赞的是，瑟夫和卡恩坚守技术伦理。面对硅谷资本对协议专利的觊觎，瑟夫在公开演讲中强调 TCP 协议应像空气和水一样免费供大众使用；卡恩则推动成立互联网工程任务组（IETF），采用“请求评论（RFC）”的开放机制制定标准。直至今日，标注“RFC793”的 TCP 协议文档每月仍新增数十条注释，不断发展完善，如同充满生机的有机体。

如今，当我们用手机跨越山海视频通话，光纤中穿梭的数据包，仍携带着 20 世纪 70 年代瑟夫与卡恩的技术烙印。瑟夫晚年授课时，常展示一张旧照：他与卡恩俯身查看 IMP，屏幕数据流在黑暗中划出的绿色光带，恰似当年点燃世界连接的火种。

两位科学家的故事启示我们：真正的创新不是颠覆秩序，而是于差异中寻共性、化繁为简。下次敲击网址时，不妨回望那个用 20 个字节定义通信规则的夜晚——科学探索的魅力与坚持，终将化为我们推动进步的力量。

第 2 章

物理层

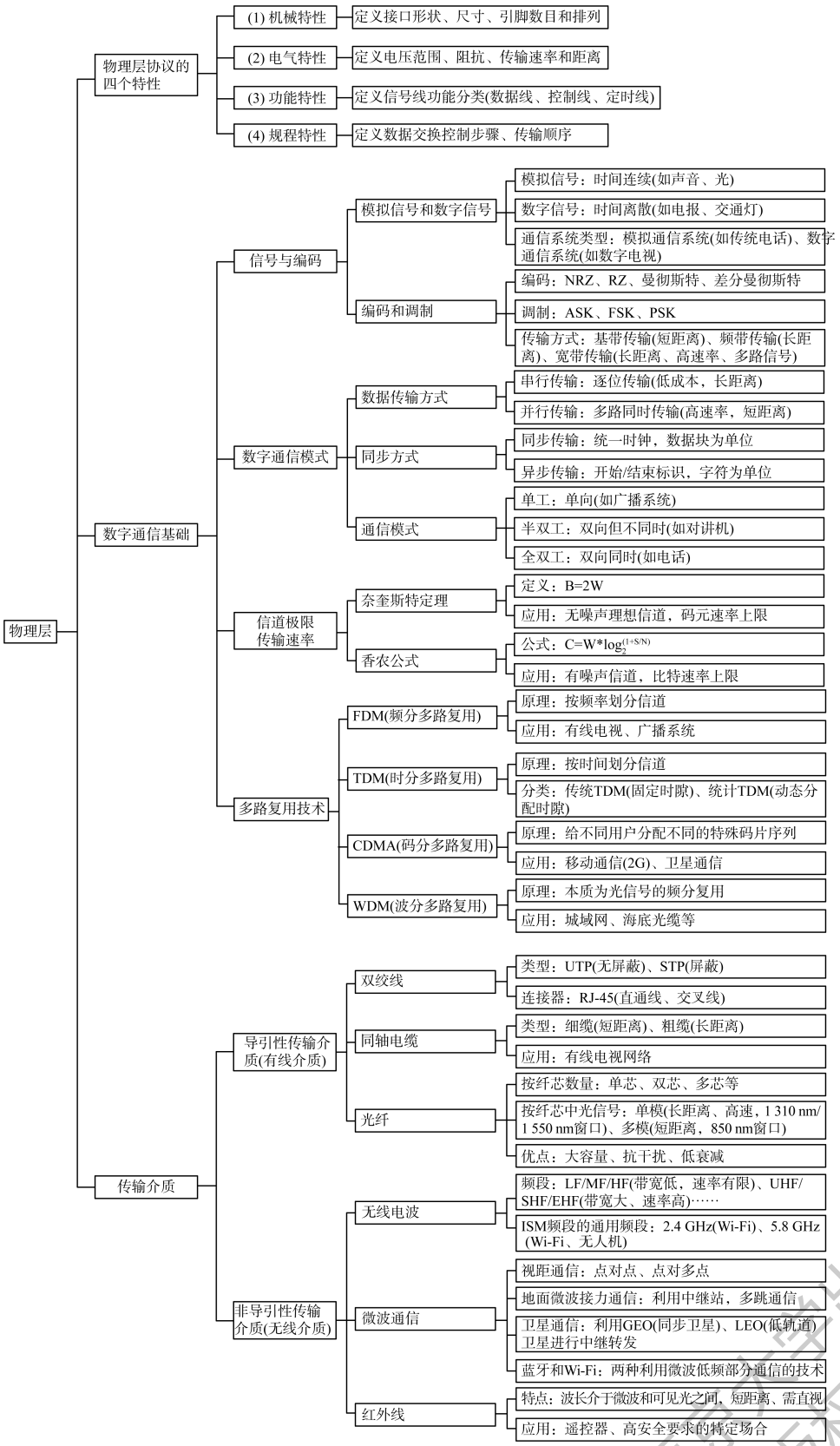
物理层处于 OSI 参考模型的最底层，其向下直接面对具体的传输介质，向上为数据链路层提供服务。物理层传输数据的单位是比特，表现为物理的电信号、光信号或无线信号。物理层的基本功能是在数据链路层的实体间提供一个物理链路，通过网络接口和不同的传输介质实现比特流传输。在实际的网络环境中，不同计算机网络使用的传输介质、通信协议和标准各异，为了更有效、更可靠地实现物理传输，更好地为数据链路层的透明传输提供服务，物理层还需要尽可能地屏蔽这些差异性、提供编码、传输方式转换等方面的功能。

在研究通信时，我们往往会思考这些问题：通信链路的连接方式是有形的还是无形的？传递的信号是光的、电的、还是无线的？要传输的数据如何转换成适合通信链路的信号形式？传输速率是多少？怎么提高传输链路的使用效率和降低传输成本？对这些问题的解答，不但需要我们对物理层的功能和相关技术细节进行理解，还需要我们在了解物理层协议外，有适当的数字通信的基础知识，本章我们就从这两个方面入手学习。

本章重点：

（1）物理层协议的四个特性；
（2）数据通信中的基本概念；
（3）数字通信模式；
（4）奈氏准则和香农公式；
（5）多路复用技术；
（6）常见的传输介质。

思维导图



2.1　物理层协议的四个特性

ISO 给出了 OSI 参考模型中物理层的明确定义：物理层为建立、维护、释放数据链路层实体间的传输二进制比特流的物理连接提供机械的、电气的、功能的和规程的特性。由此不难看出物理层协议（又称规程）作为各种网络设备进行互联时必须遵守的基础规范，其主要任务是标准化各种网络物理连接中接线器、接口的机械特性、电气特性、功能特性、规程特性，进而确保不同厂商生产的网络设备能在物理层上实现互联互通。中继器、集线器等为工作在物理层的设备，其接口的外观、结构、电气等特性直接体现了物理层协议的四个特性。

1. 机械特性

机械特性指明网络中的接线器、网络接口的形状和尺寸、引脚数目和排列次序、固定和锁定装置形式等。如 RJ－45 的 8 针结构、RS232 的 9 针双排结构。要注意的是，网络中设备的接口一般是插接式的，遵循一凸一凹的对称原则，一方是插针形式，另一方则会是插孔形式。例如，RJ－45 接头，俗称水晶头，它和路由器、交换机、网卡上的网线接口，就遵循这种对称原则。

2. 电气特性

电气特性指明传输二进制比特流时接口电缆上出现的电压范围、阻抗高低、正负逻辑、传输速率和传输距离等。如 RJ－45 以太网接口使用 100 Ω 特性阻抗的双绞线，差分信号电压为±2.5 V。

3. 功能特性

物理接口信号线一般分数据线、控制线、定时线和地线。功能特性指明了某条线上出现的某一电平的电压的意义及接口信号线的功能规定或作用分类。如 RJ－45 的 8 个引脚中，1/2 针用于发送数据（TX＋/－），3/6 针用于接收数据（RX＋/－），4/5 针保留（或用于 PoE 供电），7/8 针通常为备用（或在千兆以太网中用于双向数据传输）。

4. 规程特性

规程特性也被称为过程特性，指明各信号线进行数据交换时的控制步骤、传输数据的顺序、某事件发生的合法变化序列等。如理解 RJ－45 的物理层规程特性，可看作其体现在：在 10/100 M 以太网中通过快速链路脉冲（FLP）完成速率（10/100 Mbps）和双工模式的自动协商；在千兆以太网（1 000BASE-T）中，除兼容 FLP 机制外，还需通过更复杂的信道训练完成协商，在链路激活后通过一系列有序的信号交互维持时钟同步、监控链路状态等。

2.2 数字通信基础

通信系统是传输信息的系统，包括信源、发送器、传输系统、接收器、信宿几个要素，其一般模型如图 2-1 所示。传输系统是数据传输的通道，从物理上来看，它就是单纯的一条物理通路，从逻辑上来看，它由传输介质、相关协议、各种节点设备共同作用构成。信源是信息的发送端，信宿是信息的接收端。发送器将信源发出的信号经编码或调制后转换成需要的形式，以达到在传输系统中高效、可靠传输的目标。接收器则将从传输系统中接收到的信号解码或解调，还原后传送给信宿。由于通信通常是双向的，发送器的功能和接收器的功能往往会集成在同一设备中，如调制解调器、网卡。信号在传输的过程中受到的干扰是噪声，噪声既可以来自外部，也可以产生于传输过程中，其不可能避免，但可以通过有效技术或措施降低其对传输的影响。

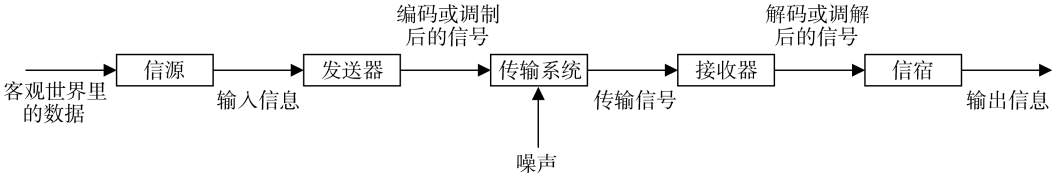


图 2-1 通信系统一般模型

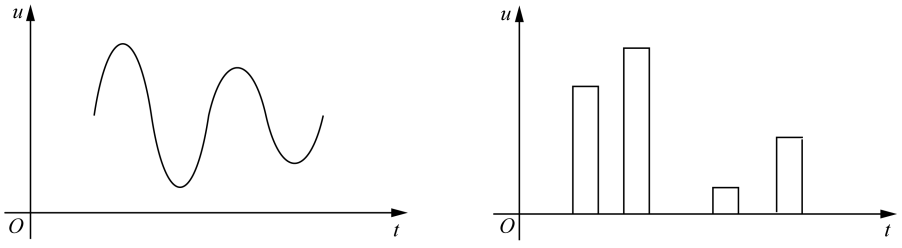
2.2.1 信号与编码

1. 模拟信号和数字信号

日常生活中，我们通过文字、语音、图像、视频等来交流和获取内容，这些未经加工的原始内容（如一段文字、一张图片、一段语音等）被称为数据。根据其状态与时间的关系，数据可分为连续型和离散型两种。信息是被加工处理后的有意义的数据，同样的数据对不同的对象可以被提炼出不同的信息。无论是数据还是信息，在计算机中进行存储和处理时，需要将其转换成二进制的形式。数据和信息具有相对性，在后续的学习中，不再严格对两者进行区分，均用数据一词表述。

信号是数据的表现形式，如在电信系统中，数据往往被转换成电信号（如电压、电磁波等）进行表示和传输。根据数据的形式，信号也有两种：模拟信号、数字信号。图 2-2 描述了这两种信号的特征。

模拟信号是时间上连续的信号，其描述数据的参数（如幅度、频率、相位）可以随时间连续变化。模拟信号是自然界中普遍存在的信号，光、声音都是模拟信号。模拟信号的生成和传输相对简单，但往往数据量大、不利于存储，在传输过程中容易受到干扰，长距离传输时信号衰减较为明显，若要保证传输质量则会增加传输系统的复杂性和成本。



(a) 模拟信号　　(b) 数字信号

图 2-2　两种信号

数字信号是在离散时间点上存在的信号，其描述数据的参数取值只在特定的时间点上存在。电报信号、交通中的红绿灯信号、计算机输出的高低电平信号都是日常生活中的数字信号。数字信号具有抗干扰能力强、易于存储、处理等优点。数字信号在传输过程中同样会有信号衰减和噪声干扰，但相对于模拟信号来说，其更易于再生，只要信号的离散变化在可识别的范围内，用合适的技术手段就能将其准确地还原。

无论是模拟数据还是数字数据，都可以用模拟信号或数字信号来表示和传输。根据传输和处理所基于的信号，可将通信系统分为模拟通信系统和数字通信系统。传统的电话系统就是基于模拟信号的通信系统，而数字电话、数字电视都是基于数字信号的现代数字通信系统。本章后续均基于数字通信进行讨论。

问题：

日常生活中，还有哪些模拟信号、数字信号？有哪些模拟通信系统、数字通信系统？

2. 编码和调制

在具体的通信中，由于传输介质的适配、抗干扰和保真、多路复用技术等各方面的要求，信源发出的数字信号或模拟信号并不能直接在物理链路上传输，需要经过编码或调制转换。

编码是将模拟数据或数字数据转换成适合传输的数字信号的过程。在数字通信系统中，对于模拟数据，可先通过模数转换(A/D)对其数字化，转换成二进制数据，再对转换成的二进制数据进行线路编码生成适合在物理介质上传输的数字信号波形。模数转换最常用的技术是脉冲编码调制(Pulse Code Modulation，PCM)技术，其基于采样原理，在规定的时间间隔里对模拟数据进行采样，将获取到的采样值用特定位数的二进制码来表示，从而实现数字化。对于数字数据，可以直接进行编码转换成物理层信号。在物理层，数字信号表现为离散的、不连续的物理量，如电压脉冲、光脉冲、电磁波等，最简单的情况下，一个数字信号就直接对应一个二进制位，如一个电压脉冲代表一位 0 或 1。整个编码过程的核心目标是将原始数据转换成适合特定传输介质的高效、可靠的信号形式。

信号的编码直接关系到数据在物理介质中的传输质量和效率，不同的编码方案会影响数据的传输速率、抗干扰能力和同步性能，进而影响整个通信系统的性能。常用的编码有不归零码(NRZ)、归零码(RZ)、曼彻斯特编码(Manchester Encoding)、差分曼彻斯特编码(Differential Manchester Encoding)。图 2-3 为几种常用编码的对比。

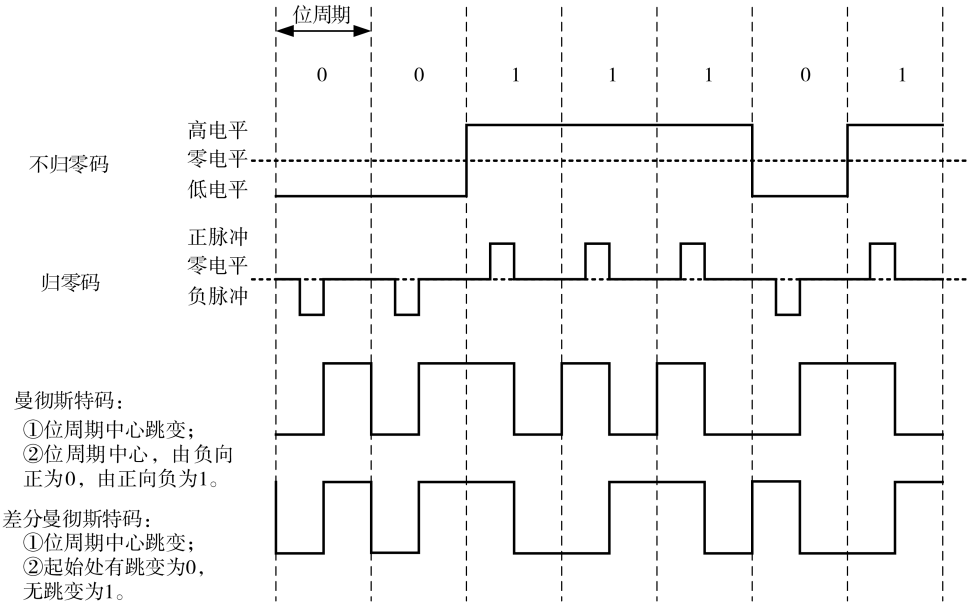


图 2-3　常用编码对比

不归零码(NRZ)：在每个位周期中，用两种不同的电平表示二进制编码的 0 和 1。这种编码方式简单，但当连续发送 0 或 1 时会使两个相邻信号间没有间隙，进而被误认为稳定的直流电平，产生直流分量，不利于在某些物理介质中传输。例如，在长距离的电缆传输中，直流分量会导致信号的积累和干扰。另外，采用这种方式时，难以确定一位的开始和另一位的结束，需要在收发双方间采用额外的方式进行定时和同步，保证数据传送。

归零码(RZ)：在一个位周期内(通常在 1/2 周期时)，信号脉冲电平必须回归到零电平(无电流)，通常用正脉冲表示 1，负脉冲表示 0(也可以相反)。归零码具有自同步能力，即接收端可以通过检测电平的回归来提取时钟信息、确定比特边界、实现位同步，但因为仍有零电平的存在，会产生零电平直流成分，不利于在某些介质中传输。另外，归零码在每个位周期内有两次电平跳变，在相同的数据传输情况下，归零码比不归零码的信号频率更高。

曼彻斯特编码(Manchester Encoding)：在每个位周期的 1/2 位置上发生电平极性跳变，由正向负为 1，由负向正为 0，也可以反过来定义。从编码方式可看出，曼彻斯特编码消除了直流分量，具有自同步能力(可以从每个位周期的中间位置的跃变提取出时钟信息)，相同的情况下的信号频率为不归零码的 2 倍，但对于接收端来说，无法从位开始的位置上确定当前位是 0 还是 1，容易在无极性跳变约定的情况下引起译码错误。早期的 IEEE 802.3 CSMA/CD 以太网中(如 10Base-T)采用的就是曼彻斯特编码。

差分曼彻斯特编码(Differential Manchester Encoding)：在每个位周期的 1/2 位置上必须发生电平极性跳变，且在位开始处通过有无跳变来确定 0 或 1，如有跳变为 0、无跳变为 1。差分曼彻斯特编码同样具有自同步能力，且其时钟信息和数据信息分离，便于数据提取。另外，相较于曼彻斯特编码，接收端可以通过位开始处有无跳变来确定 0 和 1，使得在译码时不易发生错误。

信源发出的未经调制的原始信号称为基带信号。计算机中的二进制数据转成的电平

信号就是基带信号，上述编码后形成的信号也是基带信号，这类信号的频谱通常集中在零频率附近，在传输中表现为含有大量的低频分量（甚至直流分量），这使得其只能在低通特性（只允许低于某个频率的信号通过）的传输媒介中传输，而大多数传输介质具有带通属性（只允许某个范围内的信号通过），另外，基带信号在传输过程中衰减严重，不适合于远距离传输。因此，为了适应信道特性并提高传输距离，需要考虑调制。

调制，从狭义上来说，即是带通调制（载波调制），是将基带信号加载到载波上、将其频率范围转换到更高的频段。“将基带信号加载到载波上”是用来自信源的基带信号去控制载波的参数，使载波的某一个或某几个参数按照基带信号的规律变化。这里，载波如果选用高频振荡的正弦波，可以进行控制的载波的参数有幅度、频率、相位，当基带信号为模拟信号时，通常采用幅度调制（AM）和频度调制（FM），当基带信号为数字信号时，对应的调制技术有幅移键控（ASK）、频移键控（FSK）、相移键控（PSK）。对数字信号的三种调制方式如图 2-4 所示。

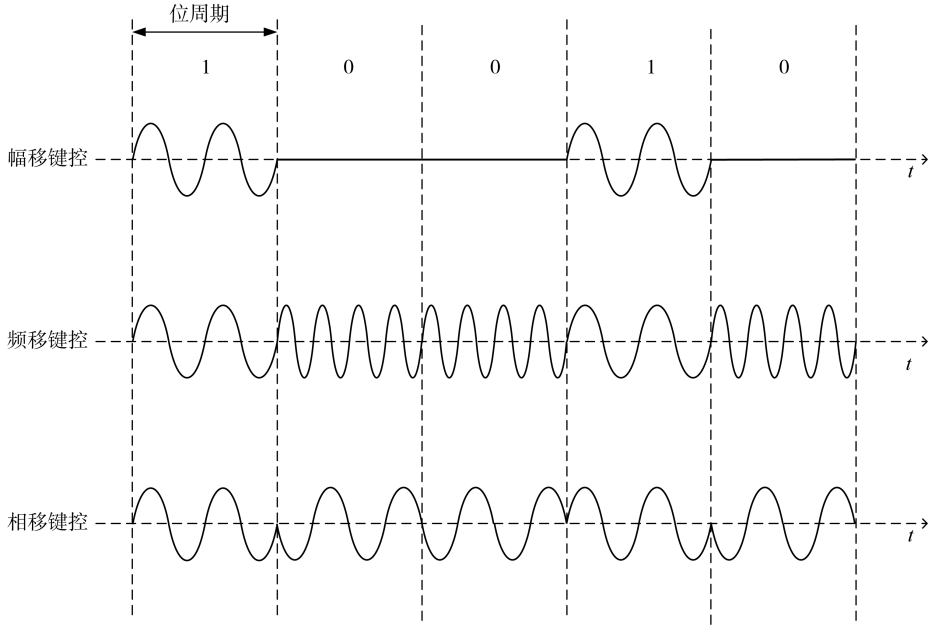


图 2-4　数字信号的三种基本的调制方法

经过调制，可以把基带信号的频谱搬至较高的频率上，以适合于远距离传输，也可以把多个基带信号分别搬移到不同的载频处，以实现信道的多路复用，提高信道利用率，还可以扩展信号带宽，提高系统抗干扰能力。

计算机网络中的数据传输，根据传的是未经调制的基带信号，还是调制后的频带信号，分为基带传输和频带传输。基带传输的信号频率范围较窄，传输简单，同一时间只支持单路线号，适合于短距离，如局域网内部的数据传输就采用基带传输。频带传输的信号频率范围较宽，通常在较高的频段，可以利用模拟信道进行传输，适用于长距离和高速率的数据通信。光纤通信、微波通信、卫星通信采用频带传输。另外，还有一种宽带传输方式，该方式也需要对从信源发出的信号进行调制，采用的是比音频更高的频带，包括大部

分电磁波频谱，适用于大规模、高速率的数据通信，可以在一个物理信道上分别传输音频、视频和其他数据等多路信号。宽带传输在实际应用中非常广泛，如互联网接入、有线电视网络、移动通信网络等。

2.2.2 数字通信模式

对数字通信模式进行了解，需要从三个方面进行着手，一是数据传输方式，二是同步方式，三是通信模式。这三个方面的交互作用对通信效果有着显著影响。

1. 数据传输方式

数据的传输方式有两种，串行传输和并行传输。

串行传输时，组成单位数据的比特位在一条传输线路（如一条芯线）上以串行的方式逐位、按序传输。这种传输方式传输速率低，实现简单、成本较低，适合于长距离传输。USB 接口、RS－232 接口、以太网中的双绞线数据传输，都采用串行传输。实际上，串行传输中会通过提供多条串行线路同时工作来提高速率，以 RS－232 接口为例，接口中的 TXD（发送数据线）和 RXD（接收数据线）就是两条可以同时工作的串行线路。

并行传输时，组成单位数据（如一个字节）的比特位通过多条并行的传输线路（多条芯线）同时传输。这种传输方式传输速率高，但易受干扰，成本高，适合于短距离传输。早期的打印机接口、DDR 内存总线，都采用并行传输。

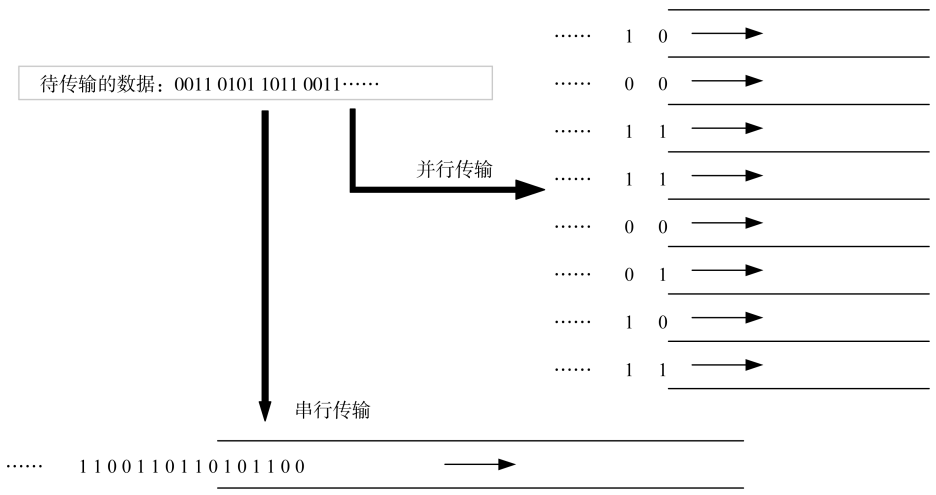


图 2-5 数据的传输方式

2. 同步方式

在通信中，同步是指收发双方在时间上保持协调一致，使接收方能准确识别出发送方发送的各单位数据的起止时间，从而保证接收数据的正确、可靠。为实现这一目标，通信协议中需明确定义同步方式。并行传输和串行传输都需要同步，但两者处理方式不同。

以下讨论串行传输中两种同步方式:同步传输机制和异步传输机制。

同步传输机制下,收发双方基于统一的时钟信号协调工作,数据按固定的时间间隔发送和接收,收发双方的时钟与传输的每个数据位都严格对应。该机制下,通常以数据块(或数据帧)作为数据传输的单位,发送方在有效数据(数据块或数据帧)的前后加上固定长度的同步字符序列和终止字符序列,接收方通过识别这些特殊序列来接收数据。同步机制下,为防止双方的计时漂移,统一的时钟信号可以是单独的,也可以掺在数据信号中(如曼彻斯特或差分曼彻斯特编码的数据)。同步机制适用于高速数据传输,如光纤通信和高速网络传输。

异步传输机制下,收发双方不需要同时工作,没有统一的时钟信号,但双方事先约定好相同的数据传输速率。该机制下,通常以字符作为数据传输的单位,发送方在每个字符前后添加开始和结束标识,每两个字符间的时间间隔可以是任意长,但每个字符所占用的时间固定。接收方通过识别开始、结束标识来接收字符数据。异步传输机制下,每个字符均需添加辅助位造成传输效率降低,只能适用于低速数据传输、间歇性数据传输,如键盘输入。

3. 通信模式

信道是信号传输的媒介或通路。根据信号在点对点通信信道中的传输方向,将通信模式分为三种:单工、半双工和全双工。

单工通信时信号只能在信道中单向传输。这种情况下,发送方只负责发送,接收方只负责接收。如图 2-6(a)所示。如在广播、电视系统中,信号从广播站、电视塔单向传输到用户的接收设备,用户只能接收而不能发送信号。

半双工通信允许信号双向传输,但同一时刻只能有一个方向传输。这种情况下,每一方既能发送也能接收,但同一时刻,每方只能执行一个功能,要么接收、要么发送。如图 2-6(b)所示。如对讲机机通信中,用户需要按下发送按钮才能发送信号,而松开按钮时则处于接收状态,该用户无法同时进行发送和接收。

全双工通信允许信号同时、双向传输。这种情况下,每一方既能发送也能接收,且能同时执行发送或接收功能。如图 2-6(c)所示。如电话通信中,双方可以同时说话和听对方的声音,实现了真正的双向同时通信。

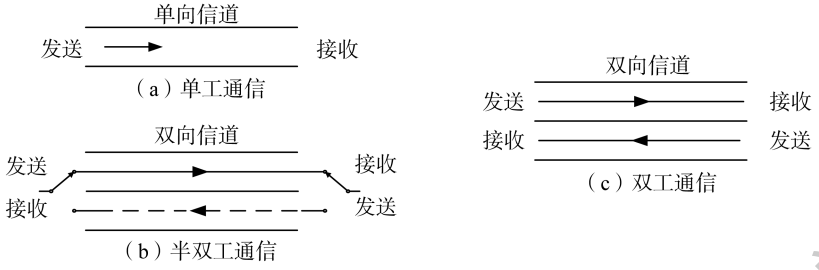


图 2-6　三种通信模式

问题：

结合上述的学习，讨论一下局域网中使用的是什么样的传输方式、同步机制、通信模式？为什么要如此设计？

2.2.3 信道极限传输速率

在这一节的学习中，我们的讨论前提是物理层用电信号来表示模拟信号和数字信号。为了保证信号接收的准确、可靠，传输模拟信号时，往往要求接收端收到的信号无波形失真，传输数字信号时，接收端收到的信号允许波形失真，但需要能无差错地识别、还原出原始信号。为了保证信号的不失真，前者需要对模拟信号到数字信号转换过程中的采样频率进行控制，后者需要对信号的传输速率进行控制。

不管什么信号，最终要在信道中传输。对于任一个信道，由于其固有的特性及通信中诸多因素的制约，允许通过的信号频率都是有限的，非允许频率范围内的信号会被滤出。信道中允许通过的信号频率带宽越宽，信道的数据传输速率越高。对信道的极限传输速率进行了解，有利于从资源分配、抗干扰处理、协议选择等方面为通信系统的设计提供理论依据。计算信道的最大数据传输速率有两个重要的理论：奈奎斯特定理、香农公式。

1. 奈奎斯特定理

数字信号传输中，可以在信道中传输的、代表数据的某种波形称为码元。一个码元可以对应一个比特，也可以对应多个比特的一个组合，接收方根据收到的波形确定收到的是哪种比特的组合。码元的传输速率（波特率）指单位时间内传输的码元数，单位是波特（Baud）。例如，1 波特表示每秒传输 1 个码元，若一个码元代表 2 个比特，那每秒传输 2 个比特（2 bps）。波特率和比特率的关系可见公式 2-1。

$$S = B\log_2 N \text{ 或 } B = \frac{S}{\log_2 N} \qquad \text{（公式 2-1）}$$

公式中，S——比特率，单位为 bps；B——波特率，单位为 Baud；N——调制后，一个码元所取的离散值个数，该值与具体的编码调制方案相关。

基带传输中，典型的电信号波形为矩形脉冲信号，这种信号的高频分量很丰富，在通过信道时，如果高频分量被信道过滤、产生衰减，则输出波形就产生失真，严重的情况下，会表现为码元间的明显界限消失、一个码元的波形展宽到另一个码元的位置或时间区域内，接收方无法正确地识别波形，这种情况称为码间串扰。要避免码间串扰就需要限制信道中的数据传输速率。

1924 年，美国的著名物理学家奈奎斯特经过反复实验提出一个结论：在理想的低通信道（无噪声、有限带宽）中，若信道带宽为 W 赫兹，则最高的无码间串扰的码元速率为 $2W$ 波特。换言之，传输速率如果超过此上限，则会出现严重的码间串扰问题，使接收端

对码元的识别成为不可能。

奈奎斯特定理结合公式 2-1 则有：

$$S = 2W\log_2 N \qquad \text{（公式 2-2）}$$

该公式能计算出理想情况下信道的最高数据传输速率，其中，S——比特率，单位为 bps；W——信道带宽，单位为 Hz；N——调制后，一个码元所取的离散值个数，也即是一个码元对应的波形为 N 种不同波形中的一种。

【例 2-1】在理想情况下，某通信信道的带宽为 4 kHz，分别计算：调制后离散电平数目是 2 或 8 的情况下，该通信信道的最高数据传输速率。

解：题干中的“离散电平数目是 2”意味着调制后一个码元可取的离散值个数为 2，即公式 2-2 中的 $N=2$，也就是一个码元对应 2 种不同波形中的一种，一种波形对应一位比特 0 或一位比特 1；而“离散电平数目是 8”则意味着公式 2-2 中的 $N=8$，也就是一个码元对应 8 种不同波形中的一种，一种波形对应一个 3 位比特的组合。具体计算如下：

“离散电平数目是 2”时，信道的最高数据传输速率：$S = 2W\log_2 N = 2\times 4\ 000\times \log_2 2 = 2\times 4\ 000\times 1 = 8$ kbps

“离散电平数目是 8”时，信道的最高数据传输速率：$S = 2W\log_2 N = 2\times 4\ 000\times \log_2 8 = 2\times 4\ 000\times 3 = 24$ kbps

由以上计算不难看出，根据奈奎斯特定理，若使用二进制信号传输，每赫兹信道带宽最多支持 2 波特的码元速率，无码间串扰的情况下，相同的信道带宽，若采用更好的编码调制技术提高码元所代表的比特数（如例题中将一个码元波形所对应的比特数从 1 位提升到 3 位），则可能增加数据的传输速率。

2. 香农公式

在实际应用中，信道不可能是理想的，不可避免地存在噪声。噪声具有随机性，会对码元的正确判决造成随机干扰，其影响程度由信噪比（S/N）的大小决定。信噪比（S/N）描述了信道中的噪声情况，其值为有用信号的平均功率与噪声的平均功率之比，可用 dB（分贝）作为单位来度量其大小，对应转换计算见公式 2-3，当 S/N 值为 1 000 时，对应为 30 dB。

$$\text{信噪比(dB)} = 10\log_{10} S/N \qquad \text{（公式 2-3）}$$

1948 年美国物理学家香农提出香农公式，考虑了噪声对信道传输速率的影响，给出了实际信道的极限数据传输速率。具体见公式 2-4。

$$C = W\log_2(1 + S/N) \qquad \text{（公式 2-4）}$$

该公式中，C——信道的极限数据传输速率；W——信道带宽（单位为 Hz）；S/N——信噪比。

由该公式可看出，带宽一定的情况下，信噪比越高，信道的极限数据传输速率越高。

以一个带宽为 3 000 Hz、信噪比为 30 dB 的信道为例，根据香农公式计算，最大数据传输速率约为 $3\ 000\log_2(1+1\ 000) \approx 29\ 910$ bps，即约 30 kbps，要注意的是，该值仅是信道

容量的理论上限，实际系统中需要通过高阶调制、纠错编码等技术手段才能逼近这个极限值。

奈奎斯特定理和香农公式，均是通信理论中关于信道的数据传输速率的重要定理，他们在通信模型中所作用的范围不同（如图 2-7 所示），意义不同。奈奎斯特定理给出了无噪声情况下的码元速率上限，而香农公式给出了有噪声情况下的比特速率上限。基于奈奎斯特定理，我们可以不断地探索编码调制技术，使一个码元能携带更多的比特信息（一个码元对应更多位的比特的组合），从而提高信道的最高数据传输速率，而基于香农公式，我们需要始终清醒地注意理论与现实的差异，要理解，在实际的通信信道中，由于噪声的客观存在，无论多复杂的编码调制技术，都不可能突破公式计算出来的极限数据传输速率。

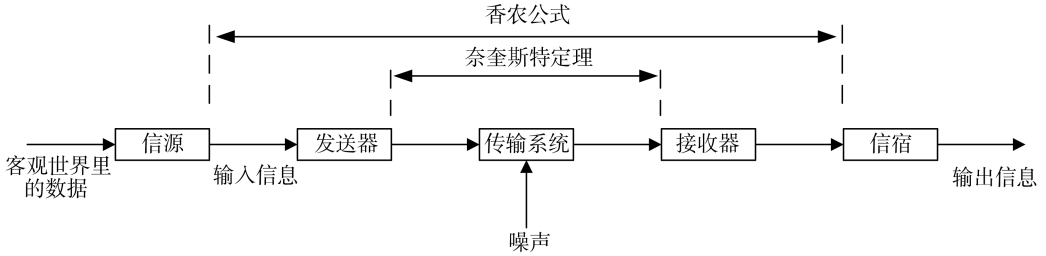


图 2-7　两个重要理论在通信模型中的作用

2.2.4　多路复用技术

数据通信是在物理链路的信道上传输数据信号，默认情况下一条信道中只传输一路信号，当实际信道的带宽远高于信号带宽时，会造成极大的浪费。如早期的模拟电话系统中，一条物理线路（如铜线）只能传输一路语音信号，铜线本身实际的可用带宽超过 1 MHz，而语音信号的带宽为 4 kHz（语音的频率为 300～3 400 Hz），这意味着近 99.6% 的带宽被浪费。因此，如何充分地利用信道，让多路信号或多个用户共享同一物理信道，提升信道的利用率、降低通信成本，是数据通信中多路复用技术致力实现的目标。

想象一下早高峰的地铁站：所有的乘客都需要进入地铁大厅（一个信道）后才能乘坐地铁，但是偌大的地铁大厅入口只有一个入站闸机，每个人得依次排队通过该闸机才能进入大厅，这使得队伍很长且入站效率极低。现实中，地铁站采用在入口设置多个入站闸机、分时段限流、不同的乘客通道（员工通道、无障碍通道）等多种措施来提高通行效率，这背后的逻辑正是多路复用技术（Multiplexing）的核心思想。

通信时，信道（如网线、光纤、无线频谱）就像地铁大厅，在有限的带宽资源下，需要传输更多的数据，可以考虑分时、分频、分码等多种不同的多路复用策略，让不同的数据流像“共享地铁大厅的乘客”一样，有序、高效地共用同一信道。在使用多路复用技术时，在发送方，需要有对应的复用器，就像地铁站的闸机一样，能对不同的多路信号处理以达到在同一信道中传输的要求，在接收方，需要有对应的分用器，将在同一信道中传输的多路信

号过滤、分离出来。在实际的应用中，由于通信的双方既需要发送也需要接收，因此复用器和分用器往往集成在同一个设备中。根据不同的信号和传输介质类型，通信中主要使用的信道复用技术有频分多路复用（FDM）、时分多路复用（TDM）、码分多路复用（CDM）、波分多路复用（WDM）。

1. 频分多路复用（FDM）

FDM 的技术思想是按一定的带宽值将一条信道划分成多个互不交叠的子信道，每个子信道可供传输一路特定频率范围内的信号，同一时刻该信道中可以传输不同的多路信号。FDM 的工作原理如图 2-8 所示。使用频分多路复用技术时，在发送方，频分多路复用器将不同的多路信号的工作频带调制、搬移到对应子信道的频带范围，以适合在同一信道中互不干扰的传输；在接收方，频分多路分用器通过滤波技术分离出各子信道中的信号，并解调还原成原始信号。实际应用中，每个子信道间通常会预留一段保护频带，一方面可以防止相邻子信道的频谱重叠、产生干扰，另一方面也方便接收端的滤波器对信号进行缓冲、识别。频分多路复用技术适用于模拟信号的多路复用，传统的有线电视系统、广播系统采用的就是频分多路复用。如无线电广播中，FM 电台频道间间隔为 200 kHz，但实际音频信号只占用 150 kHz，多出的部分为保护频带。

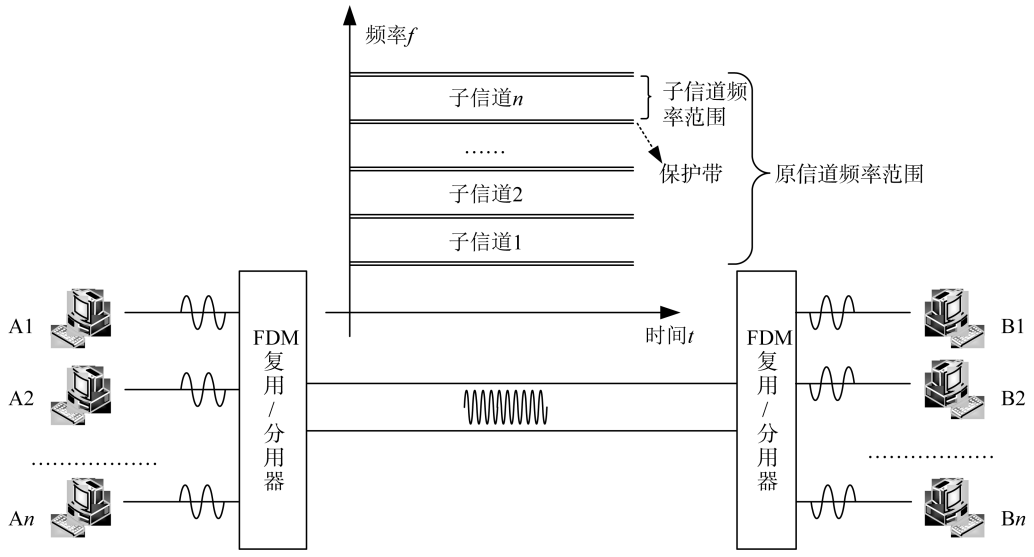


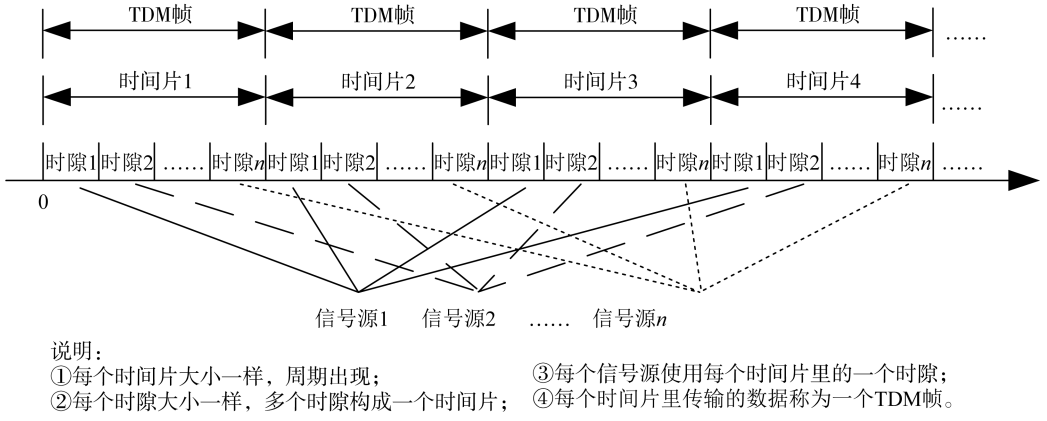
图 2-8　FDM 的工作原理

FDM 技术的优点是实现简单，但频带利用率较低，容易受到干扰。例如，在传统的有线电视系统中，每个电视频道占用一定的频带宽度，经过调制被分配到不同的频率段，多个频道可以在同一条同轴电缆中同时传输，用户通过调整接收设备的频率来选择收看不同的频道。然而，由于 FDM 技术下频带划分是固定的，会出现某些频道没有被充分利用的现象，导致频带资源浪费，另外，虽然保护频带隔离了不同的子信道，但仍可能因为频率漂移、同步误差等其他多方面的原因而产生子信道间的干扰，影响信号质量。

实际数据传输中，当单一信号传输需要的带宽占用不了整条信道的完整带宽时，考虑使用频分多路复用技术以提高信道的利用率，但有时发送方并非一直有数据传输需求，此时需要考虑从信道使用时间上来提高信道的利用率，即使用时分多路复用技术。

2. 时分多路复用(TDM)

TDM 的技术思想是将信道的使用时间划分为相等时长的多个时隙，每个时隙分配给一个独立的信号源，多个信号源轮流占用同一信道，从时间维度上实现信道的复用。多个信号源的一个完整轮次的时隙集合构成一个时间片，在该时间片中传输的数据称为一个 TDM 帧。在发送方，时分复用器将多路信号按时间顺序合并为复合信号；在接收方，时分分用器则将复合信号按时隙分离并还原为原始信号。时分复用能避免频分复用中可能存在的频带干扰问题，特别适合于数字化信号传输，数字电话系统、卫星通信中均有使用。但要注意的是，TDM 中对时钟同步的要求很高，一旦时钟出现偏差，就可能导致信号传输出错。TDM 的工作原理如图 2-9 所示。



说明：
①每个时间片大小一样，周期出现；
②每个时隙大小一样，多个时隙构成一个时间片；
③每个信号源使用每个时间片里的一个时隙；
④每个时间片里传输的数据称为一个TDM帧。

图 2-9　TDM 工作原理

根据时隙分配方式的不同，有传统的 TDM 和统计 TDM（STDM，也称为异步 TDM）。

传统的 TDM 采用固定时隙分配，时间片的长度固定，同一信号源在不同时间片中占用固定序号的时隙，即使当前某信号源没有数据传输，对应时隙也必须保留且不能分配给其他信号源使用。图 2-10 为传统的 TDM 工作原理图，图中信号源 1～4 在每个时间片中固定时隙占用信道，在第 2 个时间片中，即使 2 号信号源无数据传输，该时隙也得为 2 号信号源保留，不能给其他信号源使用。

基于传统 TDM 技术下仍存在时间浪费或信道空闲问题，STDM 技术进行了改进。STDM 技术下，信号源总数多于每个时间片中的时隙数，时隙被动态地分配给对应时间里有数据传输需求的信号源。当某时隙中有多个信号源有数据传输需求时，这些信号源根据指定的争用原则争用时隙。STDM 的原理如图 2-11 所示。该图中，有 4 个信号源，每个时间片中有 3 个时隙，根据每个时隙中的信号源数据的到达情况封装 STDM 帧，每

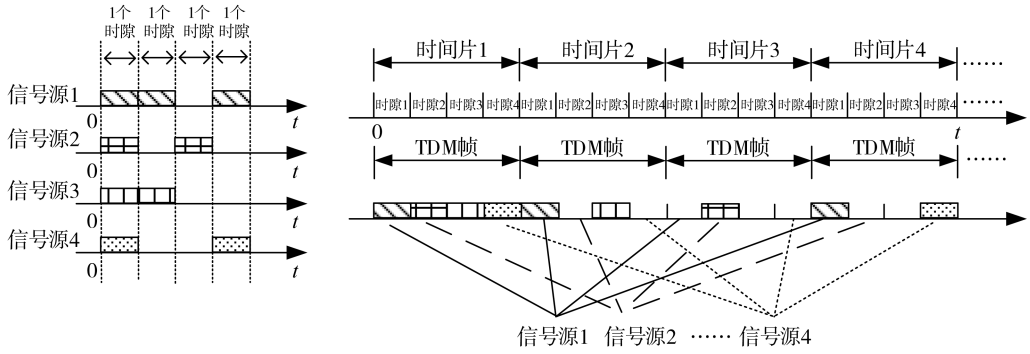


图 2-10　传统的 TDM 工作原理

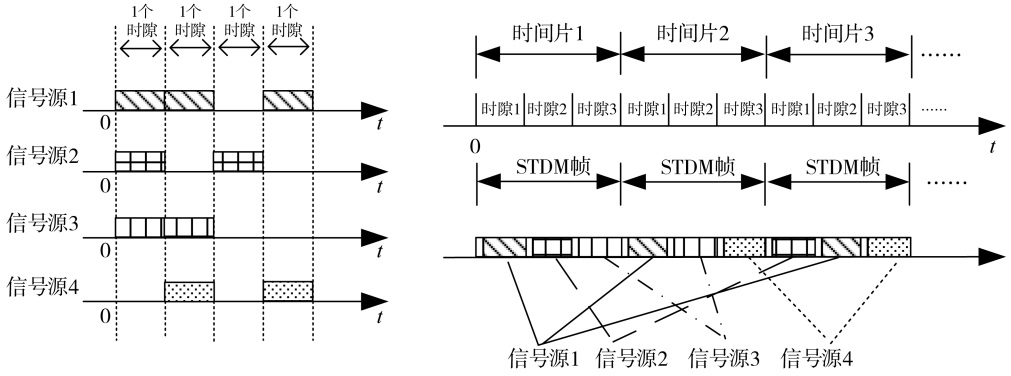


图 2-11　STDM 工作原理

个时间片中固定时隙对应的信号源不一定相同，如第 1 个时间片中第 2 个时隙里的信号源是 2 号信号源，而在第 2 个时间片中第 2 个时隙里的信号源是 3 号信号源。

时隙分配方式的不同，使得传统 TDM 适合于恒定速率的业务，如多路语音信号的传输，而 STDM 适合于突发性业务，如互联网的数据传输。也正因为时隙分配方式的不同，传统 TDM 又称为同步 TDM，发送方和接收方必须严格同步、以确保接收方能正确识别每个时隙所属的信号源，STDM 又称为异步 TDM，发送方在每个时隙的数据前添加特定数据标识信号源，接收方据此识别信号源，收、发双方无需严格同步。

时分多路复用技术的优点是能避免频分复用中可能存在的频带干扰问题，频带利用率高，特别适合于数字化信号传输，但具体实现复杂度较高。

3. 码分多路复用(CDMA)

CDMA 属于扩频通信形式，是完全不同于频分复用和时分复用的一种复用技术。扩频通信有两种，一种是跳频扩频，一种是直接序列扩频。CDMA 属于后者。CDMA 的技术思想是给每个用户分配独特的码片序列对其信号进行扩频处理，进而达到不同用户在同样的时间里使用同样的频带进行通信。

CDMA 技术下，每个比特的时间被进一步细分为 m 个更短的时间单元——码片。通常 m 的取值为 64 或 128，为了讨论方便，后续假定 m 的值为 4。另外，码片也是二进制，但为了跟要传输的数据比特区分，用－1、＋1（正好对应负电平、正电平）表示码片中的 0、1。对同一个信道有共享需求的用户，均被分配一个独特的码片序列（在此，只从原理上对 CDMA 进行学习，不去讨论如何生成这样的具体的码片序列），其独特之处在于：

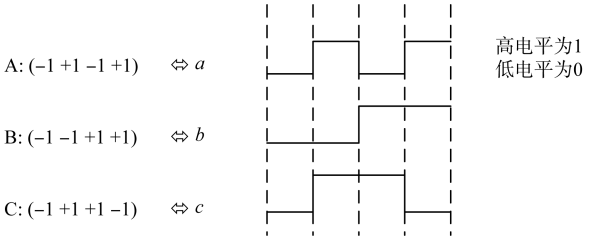
（1）任意两个不同用户的码片序列向量具有正交特性，即两者的归一化向量内积值为 0。a、b 两个向量的归一化内积公式如下：

$$a \cdot b = \frac{1}{m}\sum_{i=1}^{m} a_i b_i \qquad \text{（公式 2-5）}$$

（2）该码片序列向量自己和自己的归一化向量内积值为＋1，自己和自己的反码的归一化向量内积值为－1。

发送方，被分配到码片序列的用户若传输数据为 1 则传该码片序列，若传输数据为 0 则传该码片序列的反码，多个用户同时在信道中传输的信号会产生叠加，接收方将接收到的信号与发送方分配到的码片序列进行归一化向量内积运算，根据结果分离、还原出原始发送信号。如果运算结果为＋1，则原始为数据 1；如果为－1，则原始为数据 0；如果为 0，则发送方没有发送数据。

图 2-12 为 CDMA 的工作原理图。在图 2-12(a)所示复用状态下，用户 A 分到的码片序列为(－1 ＋1 －1 ＋1)(记为 a)，对应的反码为(＋1 －1 ＋1 －1)(记为 $\overline{a}$)，用户 B 分到的码片序列为(－1 －1 ＋1 ＋1)(记为 b，其反码记为 $\overline{b}$)，显然有 $a \cdot b = 0$。当用户 A 传输 1 时发送码片序列 a、传输 0 时发送码片序列 $\overline{a}$。如图 2-12(b)中 S2 所示，当用户 A 发送数据 1 的同时，用户 B 发送数据 0，即两者的码片序列从同一时刻开始传输，两者的信号在信道中产生叠加，即 $a+\overline{b}$，接收方接到的码片序列为(0 ＋2 －2 0)(记为 g)。如图 2-12(c)中所示，接收方计算 $a \cdot g = a \cdot (a+\overline{b}) = \frac{1}{4}\sum_{i=1}^{4} a_i g_i = 1$ 确定 A 用户发的数据 1，如图 2-12(d)中所示，接收方计算 $b \cdot g = \frac{1}{4}\sum_{i=1}^{4} b_i g_i = -1$ 确定 B 用户发的数据 0。



（a）每个用户分到的码片及码片的电信号波形

$S1 = a = (-1\ +1\ -1\ +1)$

$S2 = a + \overline{b} = (\ 0\ +2\ -2\ \ 0)$

$S3 = b + c = (-2\ \ 0\ +2\ \ 0)$

$S4 = \overline{a} + b + c = (-1\ -1\ +3\ \ -1)$

（b）信道中可能的部分信号组合

$a \cdot S1 = (1+1+1+1)/4 = 1$　发的1

$a \cdot S2 = (0+2+2+0)/4 = 1$　发的1

$a \cdot S3 = (2+0-2+0)/4 = 0$　未发送

$a \cdot S4 = (1-1-3-1)/4 = -1$　发的0

(c) 接收方判断用户 A 发送的原始数据

$b \cdot S1 = (1-1-1+1)/4 = 0$　未发送

$b \cdot S2 = (0-2-2+0)/4 = -1$　发的0

$b \cdot S3 = (2+0+2+0)/4 = 1$　发的1

$b \cdot S4 = (1+1+3-1)/4 = 1$　发的1

(d) 接收方判断用户 B 发送的原始数据

图 2-12　CDMA 工作原理

通过以上的学习，不难看出，采用 CDMA 后，每个用户需要发送的信息从 x b/s 增加到 mx chip/s；不同用户在扩频后可以同时共享同一信道的全部频谱资源；同一系统中，可以按需确定码片序列的长度，并使得不同用户的码片序列不同，实现编码隔离；CDMA 中的码片序列具有伪随机性，既码片序列与用户发送的数据不相关，对除目的接收方外的其他用户表现出随机性；解码时，只有拥有发送方码片序列的目的接收器才能正确分离、识别接收到的信号，其他非目的信号被认为是随机噪声。CDMA 技术的优点是频带利用率高、抗干扰能力强，但实现复杂度较高，需要精确的同步技术。其早期是为军事通信而开发，现在也应用于移动通信（如第二代移动通信系统 2G）、卫星通信等领域。

4. 波分多路复用（WDM）

WDM 的本质为光信号中的频分复用，因为光信号的频率很高，不便于表示，因而用波长描述。WDM 的技术原理是把不同波长的多路光载波信号通过复用器（也称“合波器”）复用到一根高速长途光纤上进行传输，在接收端，由分用器（也称“分波器”）将各种波长的光载波信号分离出来。

WDM 技术在 1970 年首次发表，1996 年，首个商用系统能将 8 个 2.5 Gbps 信道进行复合，复合后的总速率达到 20 Gbps，信道间的间隔为 200 GHz（约 1.6 nm）。其后随着技术发展，出现了 DWDM（密集波分复用）和超密集 DWDM。DWDM 技术下能实现 192 个 10 Gbps 信道或 64 个 40 Gbps 信道的复合，总速率达 2.56 Tbps，信道间的间隔压缩至 50 GHz（约 0.4 nm）；超密集 DWDM 技术下，单对光纤可支持 160 个信道，总容量超过 16 Tbps。

WDM 技术的不断发展离不开全光器件的发展。光信号在长距离传输过程中会产生衰减，早期每 100 公里就需要拆分所有信道，将每个信道转换为电信号单独放大后再转回光信号合并，而全光放大器可直接对光信号进行放大，无需多次光电转换。合适状态下，掺铒光纤放大器（Erbium Doped Fiber Amplifier）、拉曼放大器、光纤参量放大器分别能提供最长 120 km、250 km、500 km 的信号再生。

WDM 技术具有可灵活增加光纤传输容量、在同一根光纤中传输多个信号而与数据速率和调制方式无关、减少光纤的使用量而降低建设成本等优点，目前在城域网、海底光缆系统、数据中心互连等领域里应用较多。

问题：

结合上述的学习，你能更形象地结合生活中的实例来说明几种复用技术吗？

2.3 传输介质

传输介质是网络中传输数据的物理通道，用于连接各种网络设备，应用于不同的通信网络。对传输介质进行讨论，通常围绕传输介质中可传输的信号类型、信号传播的方式、传输距离、抗干扰能力、带宽和速率等。

基于信号的传播路径特性，传输介质分为导引性传输介质和非导引性传输介质。导引性传输介质往往能约束信号的传播，使其沿着固定物理路径（如铜线、光纤）传播。双绞线、同轴电缆、光纤均是导引性传输介质。非导引性传输介质中，信号通过自由空间传播，无固定传播方向，依赖天线调控，易受环境干扰。无线电波、微波、红外线均是非导引性传输介质。

工程实践中常基于介质形态，将导引性传输介质称为有线传输介质，将非导引性传输介质称为无线传输介质。前者需要物理布线，实施成本高但稳定可靠，适合于固定基础设施的构建，后者无需物理布线，灵活便捷，可按需临时构建满足移动需求，但需规划频段和覆盖范围。实际应用中则常结合两者，如现在家庭宽带大多采用“光纤入户＋室内Wi-Fi”的模式。

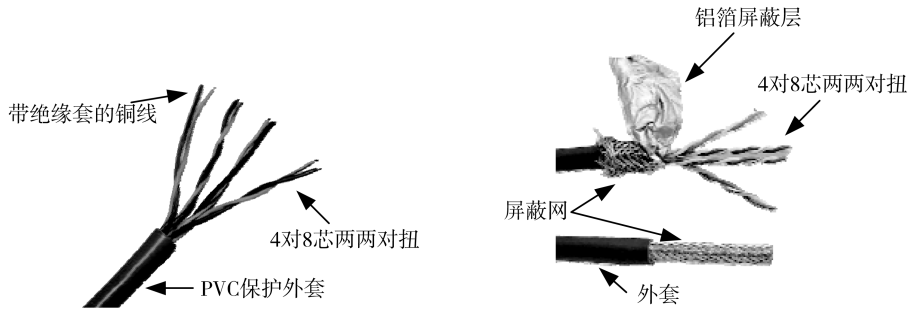
2.3.1 导引性传输介质

1. 双绞线

双绞线电缆的最外层是PVC或阻燃材料（LSZH）构成的护套，既保护内部结构，又提供机械强度；最内层是导体，由包裹绝缘材料的高纯度铜线组成，传输电信号。采用差分信号传输机制时，两根绝缘铜线按一定绞矩螺旋状绞合在一起，用于传输一路信号。为了达到双向传输，至少需要2对（4芯）这样相互绞合的铜线封装在一起，再进一步考虑传输速率的提高、抗干扰优化等问题，目前常用的一根双绞线电缆中包括了4对（共8根）芯线。

双绞线能传输模拟信号，也能传输数字信号，传输性能与其线径密切相关，线径越小，信号衰减和被干扰程度越高，无论哪种线径，均需要每隔几公里放置一中继放大器对信号进行放大或整形。双绞线中通过每对线的绞合来减少电磁干扰和串扰，绞矩越小，抗干扰的能力越强，数据的传输速率可以越高。为了增强抗干扰能力，部分双绞线会在绞合线的外面再加一层屏蔽层，屏蔽层可以是铝箔（Foiled，记为F）或金属网（Braid Screen，记为S）。根据是否有屏蔽层，双绞线分为无屏蔽双绞线UTP（Unshielded Twisted Pair）和屏蔽双绞线STP（Shielded Twisted Pair），根据屏蔽层位置和材料又可将STP进一步细分为S/UTP、F/UTP、SF/UTP、U/FTP、S/FTP、F/FTP等。其中“/”后的UTP表示内部线对无屏蔽，FTP表示每对线用铝箔屏蔽。如F/UTP表示内部每对线无屏蔽，所有线对

用铝箔总屏蔽；S/FTP 表示内部每对线用铝箔屏蔽，所有线对再用金属网总屏蔽。UTP 的安装比 STP 的安装简单，成本也较低，其安全性和抗干扰能力也可以满足常规应用需求，在以太网中使用较为广泛。STP 通常用在安全性能要求更高、电磁环境相对复杂的场所，如工业现场或医疗设备组网中。图 2-13 为市面上的 UTP 和 STP 中的 SF/UTP 的示意图。



(a) UTP　　(b) SF/UTP

图 2-13　UTP 和 STP 示意图

TIA(电信行业协会 Telecommunications Industries Association)、EIA(美国电子工业协会 Electronic Industries Association)、ANSI(美国国家标准化组织 American National Standards Institute)是制定双绞线标准的主要组织，其制定的 TIA/EIA - 568 系列、ISO/IEC 11801 系列中给出了不同应用中的双绞线技术标准，按这些标准，双绞线有 1 类线、2 类线、3 类线等，类别号越大，技术标准越新、带宽越高、价格越贵。其中 1 类线指最原始的 2 芯 UTP，用于电话语音通信，2 类线才是第一个用于计算机网络数据传输的双绞线，但数据传输速率只有 4 Mbps，用于旧的令牌网，4 类线标准已废止，表 2-1 中列出其他几类双绞线的相关信息和典型应用。

表 2-1　部分双绞线信息

类别	带宽	线缆特点	传输距离	最高传输速率	典型应用
3	16 MHz	UTP	≤100 m	10 Mbps	10BASE-T 以太网
5	100 MHz	UTP	≤100 m	100 Mbps	100BASE-TX
5e	100 MHz	UTP，改进防串扰性能	≤100 m	1 Gbps	千兆以太网
6	250 MHz	UTP/FTP	≤55 m	10 Gbps	10GBASE-T(短距离)
6A	500 MHz	UTP/FTP/SFTP	≤100 m	10 Gbps	万兆以太网
7	600 MHz	S/FTP	≤100 m	10 Gbps+	工业网络
8	2 000 MHz	F/FTP 或 S/FTP	≤30 m	25 Gbps/40 Gbps	数据中心高速互联

以太网中，双绞线连接网络设备时，使用的连接器为 RJ - 45(俗称水晶头)。RJ - 45 的引脚序号与双绞线中的芯线颜色根据 EIA/TIA 的 568A 或 568B 线序标准进行对应，若双绞线两端均使用 568B 线序，该线称为直通线，用于连接不同类型设备，如交换机和 PC；若双绞线两端分别使用 568A、568B 线序，该线称为交叉线，早期用于连接同类型设备(如 PC 与 PC、交换机与交换机)，以解决收发引脚无法自动匹配的问题。目前，由于

多数设备支持端口自动翻转，直通线已可替代交叉线用于绝大多数场景。图 2-14 为双绞线的水晶头示意图及两种不同的线序。

(a) RJ45 水晶头

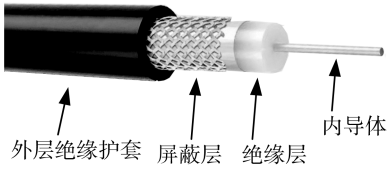
线序	1	2	3	4	5	6	7	8
T568A	白绿	绿	白橙	蓝	白蓝	橙	白棕	棕
T568B	白橙	橙	白绿	蓝	白蓝	绿	白棕	棕

(b) 两种线序

图 2-14　RJ45 接头和两种线序

2. 同轴电缆

同轴电缆可传输数字信号或模拟信号，其由内往外依次为：内导体、绝缘体、屏蔽层、外护套，其内导体为单股或多股的导电铜线，屏蔽层为一层薄的网状导电体，通常为铜或合金，用于防止信号干扰。图 2-15(a)为市面上的某种同轴电缆结构示意。根据电缆的直径大小，同轴电缆有细缆和粗缆之分。相较于粗缆，细缆安装方便，信号衰减相对较大，传输距离相对较短，常用于连接计算机，构建小型网络环境，粗缆常用于连接网络设备，构建大型局域网络。根据电缆的特征阻抗，有宽带同轴电缆和基带同轴电缆之分，宽带同轴电缆的特征阻抗为 75 Ω，用于传输模拟信号和数字信号；基带同轴电缆的特征阻抗为 50 Ω，用于传输数字信号。同轴电缆的传输速率一般在 10 Mbps 到 1 Gbps，具体取决于其类型和质量。以太网中常用的同轴电缆连接器有 BNC 连接器、AUI 连接器、Thicknet 连接器。图 2-15(b)为 BNC 连接器。



(a) 同轴电缆结构示意

(b) 50 Ω BNC 连接器

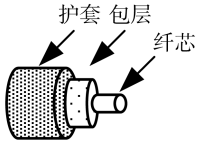
图 2-15　同轴电缆和 BNC 接头

同轴电缆曾是早期以太网的常用传输介质。然而，随着技术发展，在高速网络传输与长距离通信领域，它逐渐被传输距离、带宽以及抗干扰能力等方面更具优势的光纤所替代；在短距离网络连接场景中，又逐渐被低成本、易扩展和安装方便的双绞线所替代。但是，同轴电缆并未完全退出历史舞台，有线电视网络以及部分特定的工业控制网络里，同轴电缆依旧因其出色的抗干扰能力继续发挥着重要作用。

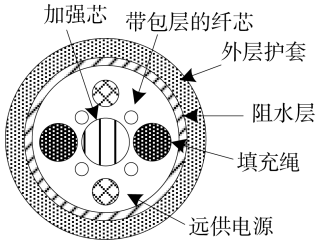
3. 光纤

光纤由纤芯、包层和护套组成，如图 2-16(a)所示。纤芯通常用纯度极高的石英玻璃

制成，包层紧密包裹在纤芯周围，为光的传输提供反射面，纤芯的折射率高于包层的折射率，当光信号以适当的角度入射到纤芯与包层的界面时，会发生全反射。护套由涂覆层和加强构件组成，起到保护光纤、增加光纤机械强度的作用。严格来说，我们平时所说的光纤应该指的是光缆，是将多根光纤用绝缘保护材料包裹在一起而成，根据光缆中包含的光纤数量分为单芯、双芯、多芯几种，这些光缆中，除添加加强芯和填充物以提高其机械强度外，有的还会放入远供电源线，为长距离通信中的光纤放大器等设备提供电力。图 2-16(b)为四芯光缆的剖面示意图，市面上的实物根据实际工程需要在结构上与之有一定差异。



(a) 单芯光缆结构示意

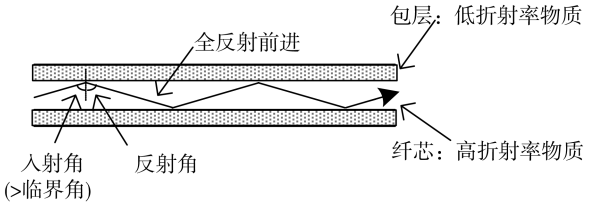


(b) 四芯光缆剖面示意

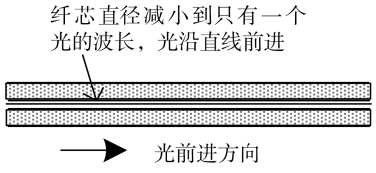
(说明：此为结构示意，实物根据需要不一定完全相同。)

图 2-16　单芯和多芯光缆结构示意

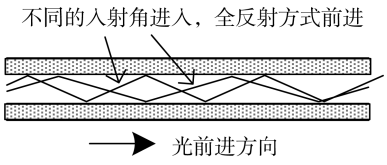
根据纤芯中光信号的传播模式，光纤被分为单模光纤和多模光纤。图 2-17(a)是光纤利用光的全反射原理传输光信号的示意图。单模光纤的纤芯很细，直径通常在 8～10 μm，与光的波长接近，且单模光纤的纤芯具有较高的折射率，而包层的折射率较低，当光信号进入光纤后，在全反射原理下，只能沿着基本模式(直线路径)传播，这种情况下，光信号的色散较小，带宽较宽，适合长距离、高速率的信号传输。多模光纤的纤芯直径较粗，通常为 50～62.5 μm，这使得光信号在以不同入射角度进入光纤后能在纤芯中以多种模式(多次全反射后沿着不同的路径向前)传播，这种情况下，光信号的色散较大，带宽相对较窄，适合短距离、中低速率的光信号传输。图 2-17(b)和(c)分别对应单模光纤和多模光纤的工作原理。



(a) 光纤全反射工作原理示意



(b) 单模光纤工作原理示意



(c) 多模光纤工作原理示意

图 2-17　多模和多模光纤工作原理示意

光纤通信是利用光纤传递光脉冲来实现数据通信，有光脉冲相当于 1，无光脉冲相当于 0，在发送端需要有光源在电脉冲的驱动下产生合适的光脉冲，在接收端需要有光检测器，将光脉冲信号再还原为电信号。发送端的光源设备主要有激光器（Laser）和发光二极管（LED）。激光器产生的光信号光谱窄、方向性强、高功率，适合高带宽、长距离传输，主要用于单模光纤；LED 产生的光信号光谱宽、设备成本低、可靠性高，适合低速率、短距离传输，主要用于多模光纤。

光纤中传输的光信号常用的三个低损耗窗口为 850 nm、1 310 nm 和 1 550 nm[①]，这些波长范围内的光信号在光纤中传输时损耗均较低。单模光纤使用 1 310 nm 窗口和 1 550 nm 窗口，前者适合中等距离的高速传输，后者适合长距离传输；多模光纤使用的波段在 850 nm 窗口和 1 300 nm 窗口，适合中等距离的信号传输。单模光纤可见于城域网、有线电视网络、FTTH（光纤到户）等应用中；多模光纤则多见于校园网、数据中心、工业网络等应用中。在实际应用中，单模光纤常见的数据传输速率有 10 Gbps、40 Gbps、100 Gbps，传输距离一般在数十公里到上百公里之间，如 1 550 nm 波段，配合有效放大器，无中继传输距离理论最远可达 120 公里。多模光纤的常见数据传输速率为 1 Gbps、10 Gbps，传输距离能达到几百米（在低速率或特殊优化条件下也能达到公里级别），如 OM4 多模光纤在 850 nm 波段、10 Gbps 速率下能支持 550 米的传输距离，40 Gbps 速率下能支持 150 m 的传输距离。

ITU-T 和 ISO/IEC 分别从不同的角度出发制定了光纤的标准，对光纤进行分类，如 G 标准中涉及的 G.652～G.657、ISO/IEC 11801 中涉及的 OM1～OM5。不同标准的光纤，物理特性、应用场景等各有所长，但总的来说，相较于其他导引型传输介质，光纤具有如下公认优点：

（1）通信容量大。无论是采用哪个波段的光信号进行传输，带宽均能达到 THz 级，如单模光纤采用 1 550 nm 窗口、波分复用的情况下理论上能达到 50 THz 的带宽、数据传输速率能达到 Tbps 级别，足够支持 5G 需求或其他高数据传输速率的场景。

（2）通信距离远。双绞线无中继传输距离一般在 100 m 以内，同轴电缆一般在 500 m 以内，而光纤中光信号的低衰减率使得其无中继传输距离很长，可达 100 km 以上，海底光缆更是在超低损耗（如 0.16 dB/km）和高灵敏接收的配合下能达到 300～400 km 的无中继传输。

（3）抗电磁干扰能力强、保密性好。光信号不同于电信号，不受电磁场影响、无串音干扰，且被约束在纤芯内传输，几乎不向外辐射，难以被非接触方式窃取或截获，因此光纤能适用于工厂、电力系统等复杂环境的布线，也能适用于军事、金融等安全要求高的情境。

（4）体积小、重量轻、安装后维护成本低。光纤的纤芯很细，单模光纤含护套在内的直径只有 0.125 mm，其直径远低于 Cat5e 双绞线的 5.8 mm 或标准同轴电缆 RG－6 的 1.02 mm，石英玻璃（SiO_2）的比重为 2.2 g/cm^3，远低于铜或铅（常用于同轴电缆屏蔽层）。光纤体积小、重量轻，还很柔软，易于弯曲，这使得其能被轻松铺设进拥挤的电缆管道中。

① 三个低损耗窗口的波段范围分别是：800～900 nm（850 nm 波段）、1 260～1 360 nm（O 波段）、1 520～1 565 nm（C 波段）和 1 565～1 625 nm（L 波段）。

虽然光纤有上述优点，但其也存在一些局限性，如过度的弯折会影响光信号的衰减，需额外供电，初期部署成本高，对光纤熔接技术要求高、光端机等设备昂贵等。但这些局限性并不妨碍其在各种复杂环境中使用。例如，在互联网骨干网中，光纤被用于连接不同的数据中心和网络节点，提供高速、稳定的长距离数据传输，满足了全球互联网数据传输的需求。在跨洋的海底光纤通信系统中，光缆被铺设在海底，连接不同大陆的通信网络，实现了全球范围内的高速数据传输，支撑了现代互联网的全球互联。

问题：

结合上述的学习，回想一下，你家里、宿舍或机房，使用的是哪种有线传输介质？具体是该有线传输介质中的哪种类型或型号？

2.3.2　非导引性传输介质

导引性传输介质能提供低衰减、高稳定、高可靠性的网络搭建，往往用于长期稳定性的部署，但是，在地理环境、技术发展和社会需求的多重驱动下，某些特定场景中采用非导引性传输介质搭建无线网络成为一种必需。例如，在峡谷、岛屿等复杂地形中，由于地质条件限制或硬件部署困难，铺设传统的有线传输介质不仅成本高昂，甚至可能无法实现，此时，无线网络凭借其无需物理连接的特性，能够绕过地形障碍，提供灵活可靠的通信支持。与此同时，随着智能化时代的到来，移动设备普及率激增，用户对随时随地接入网络的需求日益迫切，而依赖导引性传输介质的固定网络显然无法满足这种动态化、移动化的连接需求。此外，在灾难救援、灾后重建、野战部署、临时集会等情况下，无线网络可以更好地发挥其灵活性，快速响应。

非导引性传输也称无线传输，是通过不同频段的电磁波传输数据信息。图 2-18 为电磁波的频谱及应用领域。用于数据通信的电磁波有无线电波、微波、红外线、激光等。

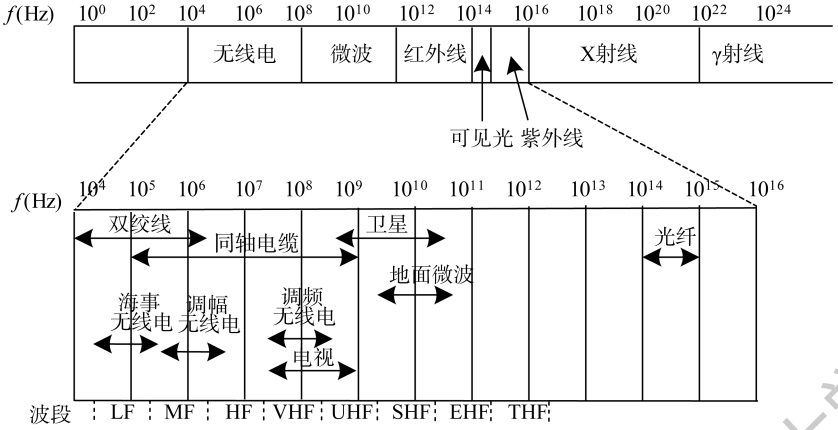


图 2-18　电磁波的频谱及应用领域

无线电波是应用最广的非导引性传输介质，基于 ITU 的定义，其频率范围覆盖不同频段对物质的穿透能力差异显著，且通常频率越高，可用带宽越大，所能支持的数据传输速率也越高。ITU 基于频率范围将无线电波分为多个频段，以便于合理利用无线电资源并避免干扰。表 2-2 列出数据通信中常用频段的名称及特点。无线电波的数据传输能力和信号覆盖能力与其频率相关，低于 30 kHz 的波有甚低频（VLF）、特低频（ULF）、超低频（SLF）和极低频（ELF），它们一般被应用于潜艇通信、地质勘探、地震检测等特殊领域的数据通信；在无线电波和红外间，还有一段称为至高频（THF）的电磁波，该波需要特殊器件来生成和接收，目前应用于实验性通信、分子光谱分析方向，未用于常见的数据通信；LF/MF/HF 频段的无线电波属于无线电波中相对低频的部分，波长长、绕射能力强、带宽低、数据速率有限，适合于远距离覆盖的需求，多用于无线广播、海事通信、导航等。UHF/SHF/EHF 频段的波，即是我们通常说的微波，属于无线电波中的高频部分，波长极短、带宽极大、数据速率高，但传播损耗也明显，需要通过中继来增加覆盖范围，常应用于卫星通信、雷达等方面。VHF/UHF 频段介于无线电波的低频和高频之间，其特点也兼顾两者的优点，在通信网络中既能提供相对较广的信号覆盖范围，又能支持较高的数据传输速率，从而在覆盖能力和传输效率之间取得较好的折中，应用于电视广播、4G/5G 移动通信、Wi-Fi（2.4 GHz）等。

表 2-2　常用频段名称及特点

频率名称	频率范围	波长范围	波段名称	传播方式	特点
低频（LF）	30 kHz～300 kHz	1 km～10 km	长波	地波	地表波传播
中频（MF）	300 kHz～3 MHz	100 m～1 000 m	中波	地波和天波	白天依赖地表波，夜间可通过电离层反射
高频（HF）	3 MHz～30 MHz	10 m～100 m	短波	天波	靠电离层反射，可实现全球通信
甚高频（VHF）	30 MHz～300 MHz	1 m～10 m	米波	近似直线传播	视距内直线传播，易受障碍物阻挡
特高频（UHF）	300 MHz～3 GHz	10 cm～100 cm	分米波	直线传播	穿透能力强，适合城市环境，易被雨水吸收
超高频（SHF）	3 GHz～30 GHz	1 cm～10 cm	厘米波		严格直线传播，易被大气吸收，高带宽
极高频（EHF）	30 GHz～300 GHz	1 mm～10 mm	毫米波		带宽极大，传播损耗高

ITU 和各国专门的监管机构（如美国的 FCC、中国工信部）通过划分专用频段、分配许可证、制定技术标准来对无线电通信进行管理，想使用某特定频段进行通信，需要向对应国家监管机构申请获得该频段的通信许可。但为了在无线电频谱资源日益紧张的背景下，为特定用途提供免许可（License-free）的无线通信频段，设立了 ISM（Industrial，Scientific，and Medical，工业、科学和医疗）频段，应用这些频段无需许可证或费用，只需要遵守一定的发射功率，且不对其他合法用户的通信造成干扰和伤害。主要的 ISM 频段包括：

- 2.4 GHz（2 400～2 483.5 MHz）：全球通用，用于 Wi-Fi（IEEE 802.11b/g/n）、蓝牙、ZigBee 等。
- 5.8 GHz（5 725～5 875 MHz）：用于 Wi-Fi（IEEE 802.11a/n/ac）、无人机遥控和射

频识别(RFID)等。

• 915 MHz(902～928 MHz):美洲/澳大利亚开放,用于 RFID、LoRa 无线传感网和部分物联网设备等。

• 433 MHz(433.05～434.79 MHz):欧洲/亚洲开放,用于遥控器、无线传感器和短距离通信等。

各国家具体的 ISM 频段的划分、允许的功率、具体的用途存在差异性,但大多数遵守并开放了 ITU 建议的全球通用的 2.4 GHz 和 5.8 GHz 这两个 ISM 频段。另外,我国除开放了与欧洲国家相同的 433 MHz 频段外,还开放了 783 MHz(779～787 MHz)用于部分物联网设备通信。

微波通信是利用 300 MHz～300 GHz 频段的电磁波进行数据传输,实际主要使用 2～40 GHz 的频率范围,ISM 中的 2.4 GHz、5.8 GHz 就是微波。微波的高频使得其不能像中波那样沿地球表面传播(会被吸收),也不能像短波那样经电离层反射后再传播,只能沿直线传播。微波通信采用视距通信和卫星通信两种传输方式。

微波视距通信时,使用的微波的典型频率为 2 GHz 以上,微波在发送端和接收端间以直线传播,收发天线间必须保持无障碍物的直视路径。微波视距通信有点对点、点对多点等不同形式,其中点对点形式在城市通信中具有独特的优势。一方面,城市通信需要高速、低延迟的数据传输,微波的高频段(24 GHz/60 GHz)可提供千兆级带宽,远超铜缆的数据传输性能。另一方面,建设好的城市中无线信号密集、基础设施固化,若想在某特定地区开展临时活动,利用微波视距通信,通过定向天线精准对准接收端,既能解决快速响应的需求,又能避免多径干扰和邻频干扰、实现可靠传输信号,同时还能免于搭建过多无长远意义的固定设施,节约成本。

考虑地球曲率和信号稳定性,纯视距通信(单跳)的传输距离通常为 30～50 km,实际上往往会通过地面微波接力(添加中继站,多跳)、增高天线(如架设铁塔)等方式来延伸数据传输距离。传统的电信骨干网就是采用地面微波接力,每隔 30～50 km 就设一个中继站。

卫星通信是利用微波进行接力通信的一种,但其通过地球同步卫星(GEO)、中轨道(MEO)或低轨道(LEO)卫星转发信号,使得通信覆盖范围更广,实现全球通信。卫星通信的基本工作原理是地面某站发出的无线电信号经通信卫星天线接收后,进行变频和功率放大后,再重新发到另一个地面站,进而实现地面站间的远距离通信。理论来说,只需要三颗同步定点轨道卫星(等距离相隔 120 度),就可以覆盖地球几乎全部面积,就可以实现全球 24 小时全天通信。卫星通信具有通信距离远(GEO 通信时单跳最远可达 40 000 km),频带宽、容量大、信号受干扰小、通信比较稳定、有效解决地面通信覆盖不足等方面优点,但通信中的传播时延和建设成本不容忽视,一般来说,GEO 系统的两个地球站间(与两站的地面距离相关不大)通过一颗卫星中继的单跳传播时延平均在 270 ms(250～300 ms)。

近年来,低轨道卫星通信技术迅速发展。低轨卫星通信相较于中高轨卫星通信具有低时延(信号往返时延可降至 20～50 ms)、高覆盖率、低成本等显著优势,且对于低轨道空间 ITU 制定了“先发先得”的频谱分配规则,这促使各国基于军事、导航等各个领域发展的需求加速了对低轨道空间的资源布局。美国太空探索技术公司 SpaceX 从 2015 年

1月开始着手的“星链”(Starlink)计划是低轨卫星通信发展的代表项目之一,计划部署大规模LEO星座,以实现全球范围内的互联网覆盖,截至2024年,该计划已发射超过7 500颗卫星。目前,我国也在加速布局LEO星座,2016年宣布的“鸿雁星座”和2018年底成功发射实验卫星的“虹云工程”均为相关的计划。

人们熟知的蓝牙和Wi-Fi是两种利用微波低频部分通信的技术,蓝牙基于IEEE802.15.1,工作在2.4 GHz频段,Wi-Fi基于IEEE802.11,工作在2.4 GHz/5 GHz/6 GHz。蓝牙通信具有低功耗、低成本、短距离的特征,其典型传输距离在10米以内,低功耗蓝牙(BLE)可扩展至百米级别,常用于耳机、键盘、鼠标等设备的通信。Wi-Fi拥有多个频段,速率远高于蓝牙,传输距离也更远(室内50～100米,室外更远),适合大容量数据传输,其功耗高、需持续供电,被用于高速、广覆盖的无线网络接入。

红外线也可用作数据传输中的非导引性传输介质。红外线的波长范围为0.75～1 000 μm(对应频率范围约为0.3～400 THz),介于微波和可见光之间,能沿直线传播,不受电磁干扰,但易被障碍物阻挡。日常生活中绝大多数传统电视遥控器、空调遥控器就是利用红外线进行通信。利用红外线进行无线通信(即红外通信),具有方向性强、安全性高、无需频段许可等优点,但其通信时的传输距离较短,一般不超过10米,且需要直视路径,中间不能有障碍物,因此,除在某些高安全要求的特定场合外,红外通信正逐渐被蓝牙等新技术所取代。

复习与思考

1. 物理层的主要功能是什么?物理层需要解决哪些通信中的问题?
2. 请简述物理层协议的四个特性,并对每个特性结合实例说明。
3. 请给出数据通信系统的模型,并说明其各个组成部分的作用。
4. 模拟信号和数字信号有什么区别?各举一个日常生活中的例子进行对比说明。
5. 解释曼彻斯特编码的工作原理,并说明其自同步能力的实现机制。
6. 在数字通信模式中,串行传输和并行传输的主要区别是什么?各举一个应用场景。
7. 在数字通信模式中,单工、半双工、全双工有什么区别?局域网使用的是哪种通信模式?
8. 一个理想低通信道带宽为4 000 Hz,根据奈奎斯特定理,其最高无码间串扰的码元速率是多少?若把码元的振幅划分为16个不同等级来传送,则可以获得的最大比特率是多少?
9. 一个信道带宽为3 000 Hz,信噪比为30 dB,求该信道的极限数据传输速率(需提供计算过程)。
10. 为什么要使用多路复用技术?常用的多路复用技术有哪些?
11. 比较频分多路复用(FDM)和时分多路复用(TDM)的优缺点,并说明各自适用的场景。
12. 描述码分多路复用(CDMA)的工作原理,并解释其归一化向量内积如何用于信

号分离。

13. 分析同步 TDM 和统计 TDM(STDM)的时隙分配差异,并解释为什么 STDM 更适合突发性业务。

14. 假设采用 CDMA 技术的情况下,有四个用户,各自分得的码片序列为:

A:(−1 −1 −1 +1 +1 −1 +1 +1)、B:(−1 −1 +1 −1 +1 +1 +1 −1)、

C:(−1 +1 −1 +1 +1 +1 −1 −1)、D:(−1 +1 −1 −1 −1 −1 +1 −1)。

现收到的码片序列为(−4 0 −2 0 +2 0 +2 −2),请问,哪些用户发送了数据,发送的是数据 1 还是数据 0?

15. 讨论双绞线中 UTP 和 STP 的差异,包括抗干扰能力、成本和典型应用场景。

16. 描述同轴电缆的结构组成,并解释其在现代网络中被光纤替代的原因。

17. 比较单模光纤和多模光纤在传输距离、带宽和应用场景上的区别,并说明光纤通信的优点。

18. 分析微波通信的两种传输方式(视距通信和卫星通信),并讨论低轨道卫星(如 Starlink)相较于地球同步卫星的优势。

19. 综合分析:一个企业网络需在复杂电磁环境中部署短距离通信,请你为其推荐合适的传输介质(如双绞线或无线),并基于文档说明理由(需考虑抗干扰、成本和速率)。

阅读与拓展

材料 1:中国光纤之父——赵梓森①

从狼烟烽火到智慧光网络,光通信深刻改变了人类生活。《科学美国人》杂志曾评价说:“光纤通信是二战以来最有意义的四大发明之一。如果没有光纤通信,就不会有今天的互联网和通信网络。”

在光纤通信上有几个重要的节点事件:1966 年,英/美籍华人高锟首次提出玻璃丝可用于通信。1970 年,美国研制出第一根实用光纤;1977 年,中国武汉的赵梓森带领团队拉出了中国第一根具有自主知识产权的实用光纤。

赵梓森 1932 年出生,1949 年至 1953 年期间先后就读于国立浙江大学、上海大同大学、上海交通大学,1954 年参加工作。1971 年,他负责国家的“激光大气传输通信”项目,成功将传输有效距离从 8 米提高到 10 千米,但由于该技术受天气影响严重,促使他寻找更可靠的传输介质。

1974 年,赵梓森提出石英光纤通信技术方案。他在深入研究后发现,降低光纤传输损耗关键在于控制过渡金属离子含量、改进拉丝工艺和热处理技术,于是,他在单位办公楼一厕所旁改造出的实验室里,带领几位年轻同事,采用最简易的实验设备(电炉、试管和酒精灯等)、最简单的工艺(烧烤)和最基础的原料(四氯化硅、氧气),在一年多时间里数千

① 本文根据《学习强国》“新华每日电讯”2019 年 7 月 22 日供稿,周甲禄、徐海波所写的《“中国光纤之父”:赵梓森》一文改写。

次的试验后，最终熔炼出高纯度的石英玻璃，并以此试验为基础，绘制出 300 多张图纸，利用旧车床和废旧机械零件制造出一台光纤拉丝机。

1977 年，赵梓森团队成功拉制出中国第一根实用型、短波长和阶跃型石英光纤。同年，“邮电部工业学大庆展览会”上，他用自研光纤成功传输了黑白电视信号，引起国家的重视。光纤通信因此被破格列为国家重点攻关项目。

光纤通信需三大要素：光纤、激光器、通信机。光纤能自制了，但另两项还是空白，赵梓森又组织团队继续攻关。1980 年 4 月，他带领团队将长波长光纤在 1.55 nm 处的损耗降至 0.29 dB/km，达到实用要求；他大胆起用年轻科研人员，历时两年多攻坚，最终在中方主导的长江激光里生产出我国第一个享有自己知识产权的长波长半导体激光器，摆脱了对美国技术的依赖；在 PCM 通信机方面，他创造性地通过“脉冲调相”来替代实现数字传输，后来又及时在引进国外集成块技术，指导团队研制和推动 PCM 机的迭代发展。

1982 年 12 月 31 日，中国第一条实用化光纤通信系统——“八二工程”在武汉开通并并入市话网，标志着中国正式进入光纤数字化通信时代。而在此之前的工程建设中，赵梓森常深夜赶赴现场，带领团队在几十公里线路上排查、修复光纤故障。

如今，中国已成为全球最大的光纤光缆生产国，部分技术领跑世界，赵梓森所在的武汉东湖高新区也已成为“中国光谷”，与世界科技高地齐名。“技术永远在发展，不努力就会落后，”赵梓森深感国际竞争之激烈，尽管被尊称为“中国光纤之父”，他始终谦逊勤勉，在科学报国的道路上奋力前行。他常说：“没有我，也会有别人来做。我只是早走了一步。只要对社会有用，我就很满足。”

2022 年 12 月 15 日，赵梓森因病医治无效在武汉逝世，享年 91 岁。

材料 2：单模光纤迈向空分复用新纪元

当前，光纤技术正迎来新一轮突破——空分复用（Space Division Multiplexing，SDM）技术成为国际研究热点，其旨在突破单模光纤香农极限，实现单纤容量数量级提升。

空分复用（SDM）技术的构想萌芽于 20 世纪 90 年代，旨在突破单模光纤的容量极限。与存在严重模间串扰的传统多模光纤不同，空分复用通过两种精准途径实现：一是在单根光纤中集成多个独立纤芯，构成多芯光纤（MCF），每个纤芯可作为一个并行传输通道；二是采用少模光纤（FMF），利用其有限数量的正交模式，通过模分复用（MDM）将每个模式作为独立信道传输。该技术依赖两个核心技术：一是模式复用与分离技术，即在发射端将信号耦合至不同模式或纤芯，在接收端再实现信号分离；二是多通道间的串扰抑制技术，确保空间并行传输的独立性。

空分复用的根本突破在于引入了空间维度这一新的自由度，通过多通道并行传输，绕过香农公式对单通道的容量限制，从而实现总容量的倍增。经过二十多年的发展，空分复用技术经历了从理论探索到实验室验证再到产业化尝试的历程。早期的技术瓶颈在于纤间串扰和复杂的光信号处理，近年来通过创新设计（如沟槽辅助型纤芯结构和先进的 MIMO 数字信号处理算法）得到了有效解决。2023 年，日本 NICT 利用 4 芯光纤实现了 1.02 Pbps 的传输速率，创造了新的世界纪录。我国在该领域也取得重大突破，2024 年世

界移动通信大会(MWC)上,中国信息通信科技集团有限公司旗下的烽火通信公司展示了自研的 19 芯空分复用光纤,该光纤此前已实现净传输容量 3.61 Pbps 的系统传输,刷新了单模多芯光纤传输容量的世界纪录,这项突破为下一代超高速光通信网络奠定了材料基础。

当前,空分复用技术正从实验室加速迈向实际应用,在跨洋海缆、数据中心互联及航空航天等特殊通信领域展现出巨大潜力。国际主流运营商正积极测试多芯光纤海缆方案,以应对全球数据洪流;华为等企业也已推出预商用产品,实现光纤数量不变而带宽跃升。在这一全球创新浪潮中,中国力量正扮演关键角色:以武汉“中国光谷”为核心,依托国家信息光电子创新中心,华中科技大学、烽火通信等单位协同推进多芯光纤的标准化与产业化进程。从半个世纪前赵梓森院士拉出中国第一根光纤,到今天我国自主研发 19 芯光纤刷新传输容量世界纪录,中国科研与产业界正持续为空分复用技术的全球发展贡献核心力量,为构建未来数字基础设施奠定坚实底座。

第 3 章

数据链路层

在计算机网络体系结构中，数据链路层位于物理层之上，网络层之下。数据链路层的主要作用是在相邻节点之间实现可靠的数据传输。数据链路层一方面负责将网络层的IP 数据报“组装”成数据帧，另一方面负责将数据帧无差错地传递至物理层。帧是数据链路层的基本传输单位，一个数据帧可以类比为一个包裹，里面装着待传输的数据以及一些必要的控制信息（如源地址、目的地址等）。有了数据帧这样的包裹形式，直连的通信双方可以方便传输载荷数据。此外，为应对传输过程中可能出现的差错，数据链路层可通过差错校验机制，检测数据在传输过程中是否出现错误。数据链路层还可根据不同的信道特性（例如，有线或无线），决定是否重传错误的数据帧。可见数据链路层的主要功能是保障数据在相邻节点之间有序、可靠地传输。

本章重点：

（1）帧的概念与结构：包括帧首部、帧尾以及数据部分的构成及其作用；

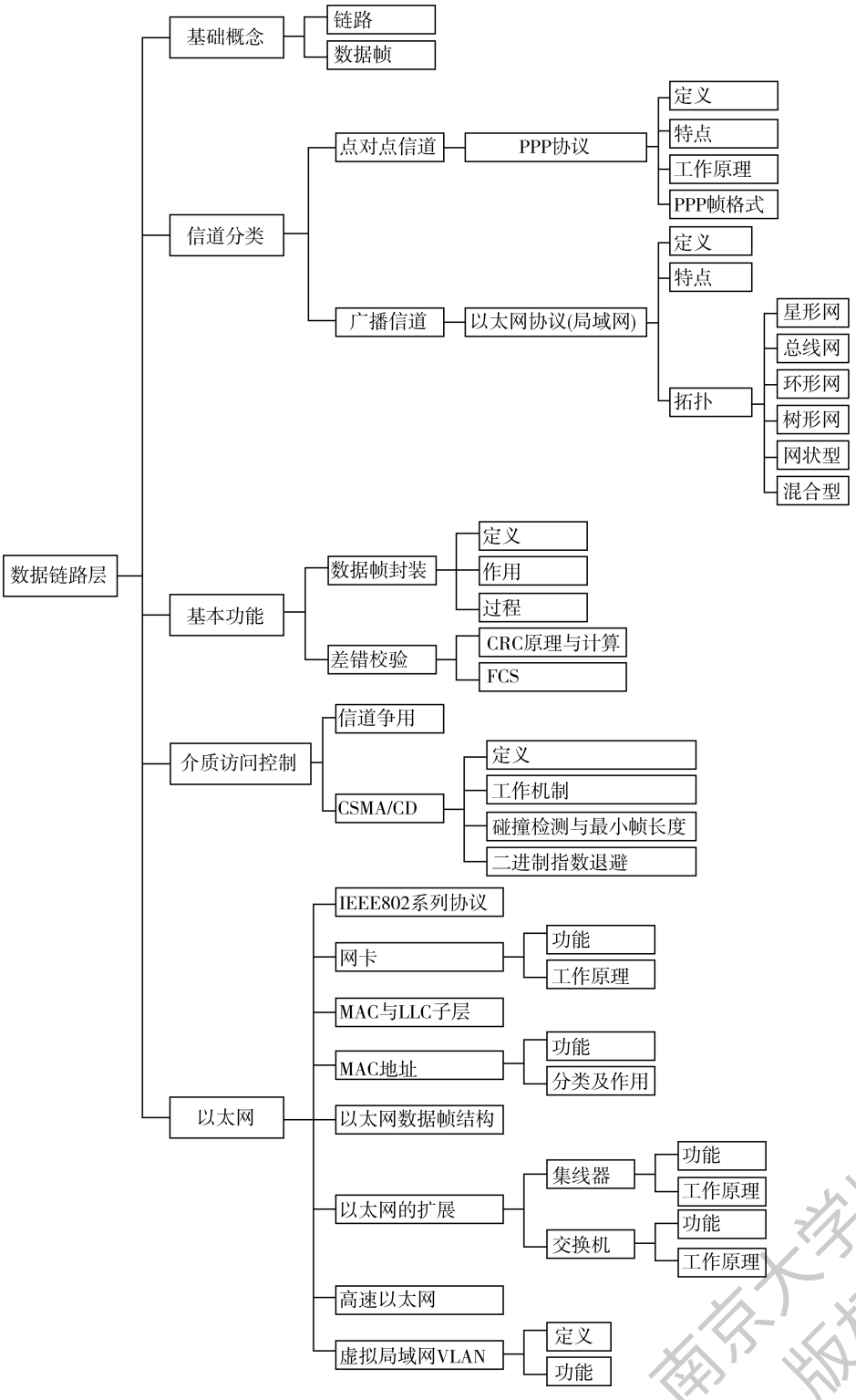
（2）数据帧封装的原理与作用；

（3）数据帧的差错控制：循环冗余校验（CRC）差错检测方法的原理和实现过程；

（4）介质访问控制（Media Access Control，MAC）层核心算法：以太网的载波监听多路访问/冲突检测（Carrier Sense Multiple Access/collision detection，CSMA/CD）协议的原理与作用，退避机制算法；

（5）集线器、交换机的工作原理和功能。

思维导图



3.1　数据链路层基础概念

3.1.1　链路

在计算机网络中，链路(link)是指从一个节点到相邻节点的一段物理线路，中间没有其他的交换节点。链路分为物理链路和逻辑链路。物理链路是指实际存在的物理线路(如光纤、双绞线及无线等)，它为数据传输提供了物理介质。逻辑链路是在物理链路上通过一些协议和技术建立起来的逻辑连接。在物理链路的基础上，逻辑链路通过添加各种控制信息和执行相应协议，实现数据的可靠传输。例如，可以通过封装成帧、差错控制等手段，将物理链路变成逻辑上可靠的链路。计算机网络技术通常将逻辑链路称为数据链路。概括而言，链路是网络中节点之间数据传输的路径，物理链路是“硬件基础”，逻辑链路则是在物理链路之上实现数据有效传输的“逻辑通道”。数据链路层在计算机网络体系结构中的地位如图 3-1 所示。

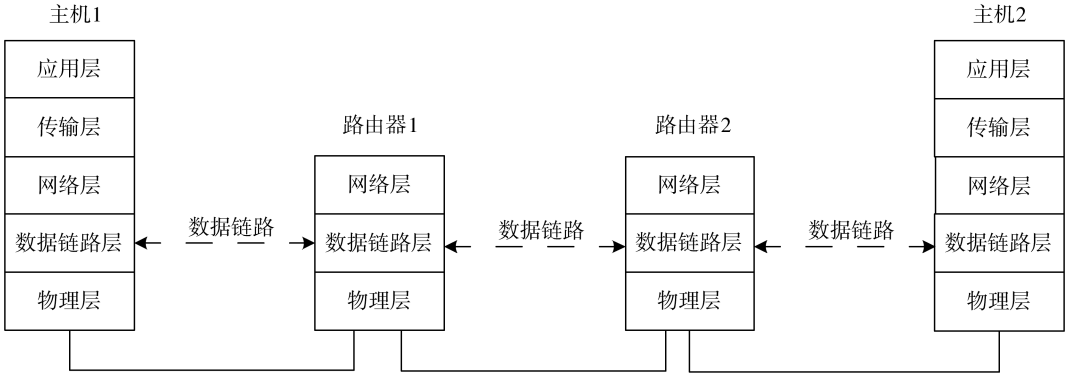


图 3-1　数据链路层在计算机网络体系结构中的地位

3.1.2　数据帧

数据帧(frame)是数据链路层的基本传输单元。在计算机网络中，当网络层将 IP 数据报向下传递，数据链路层会给上述 IP 数据报追加某些控制信息，将其封装成数据帧，再交给物理链路进行传输。数据帧具有特定的结构，具体包含帧头、数据部分和帧尾。帧头中包含了诸如目的地址、源地址、帧类型等控制信息，这些信息有助于数据帧在网络中的传输和处理。例如，目的地址告诉网络设备该数据帧要发送到哪里，源地址则表明数据帧来自何处。数据部分承载的是网络层传递下来的 IP 数据报。帧尾通常包含用于差错检测的校验序列，例如，循环冗余校验(CRC)码。通过校验序列，接收方可以检测数据帧在

传输过程中是否出现错误。通过将数据封装成数据帧，数据链路层能够实现有效的信息传输，确保数据在相邻节点之间准确、可靠地传递。

3.2 数据链路层的信道类型

数据链路层中的信道类型可以分为点对点信道和广播信道两种，下面分别进行介绍。

3.2.1 点对点信道

设想一个简单的组网需求，一台计算机需要与另一台计算机通信。如图 3-2 所示，当利用物理线缆将两者连接，就构成了一条点对点信道。该信道只存在两个端点，分别与两台计算机相连，可以认为该点对点信道仅被两台计算机独享。换言之，点对点信道为一对直连设备之间提供专用、可靠的数据传输通道。该类信道可以用于终端用户与 ISP 连接、路由器之间互联、移动网络基站与用户设备。

图 3-2 点对点信道示意图

点对点信道使用一对一的通信方式，数据传输在两个特定节点之间进行，链路两端的设备明确且固定。因为每次只有两个设备进行数据交互，通信过程简单，不易产生冲突。点对点信道支持全双工通信，两个设备可同时进行数据发送和接收。点对点信道适用于对数据传输的准确性和实时性要求较高的场景，例如，可用于互联网用户连接 ISP 或不同路由器之间通信，确保数据传输的可靠性。点对点(Point-to-Point Protocol，PPP)协议就是点对点信道的数据链路层通信协议。

问题：

既然存在简单而可靠的点对点信道，是不是只要通过点对点信道两两相连，计算机就可以组建各种规模的网络？

3.2.2 广播信道

将所有的计算机设备两两相连，一方面会带来线路复杂性的急剧膨胀，另一方面计算机等终端设备也无法增加大量的通信端口。因此，随着计算机网络的发展，出现多个设备

共享同一通信介质的需求。如图 3-3 所示，多台计算机可以通过共享信道连接并实现资源共享和通信，广播信道就是为满足这种多设备共享通信介质的需求而产生。该类信道可以用于传统以太网、无线局域网等。需要说明的是，为了方便初学者理解，图 3-3 仅是广播信道的一种拓扑实现方式，本章 3.4 节还会介绍广播信道的其他拓扑方式。

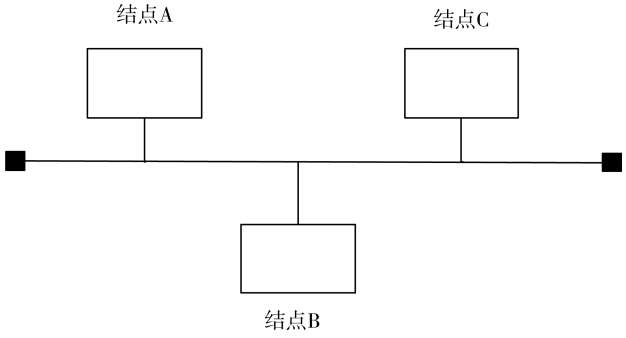


图 3-3　广播信道示意图

使用一对多的广播通信方式，一个设备发送的数据能被连接到该信道的所有其他设备接收。连接的主机数量众多，共享同一传输介质，容易发生信号冲突，需要专门的共享信道协议（如 CSMA/CD 协议）来协调各主机的数据发送。需要说明的是，广播机制的一对多通信，实际上也实现了一对一通信。要实现用户理解的一对一通信，只需要在各计算机终端设备增加一个判断机制，如果终端收到数据帧的目的地址是本机地址，则向上提交该数据帧。如果终端收到数据帧的目的地址不是本机地址，则直接丢弃该数据帧，即不向用户提交该数据。广播信道可以实现局域网内多台设备之间的通信，降低了网络建设成本，适用于网络中的广播消息、局域网内的设备发现等场景。

下面将分别在 3.3 节与 3.4 节介绍点对点信道与广播信道对应的通信协议。

3.3　PPP 协议

3.3.1　背景

在早期网络发展中，需要一种能在点到点信道上传输多种网络层协议数据的标准协议。不同厂商的设备和不同网络层协议（如 IP、IPX 等）之间缺乏统一的通信规范。为解决这些问题，PPP 协议应运而生。它旨在提供一种通用的、标准化的点到点链路通信解决方案，以实现不同设备和网络层协议之间的有效通信。

3.3.2　特点

PPP 协议支持多种网络层协议，能承载 IP、IPX 等多种网络层协议数据，使不同网络

层协议可在同一链路传输。PPP 协议链路控制功能具备链路建立、配置和测试机制，可自动协商数据链路层地址、最大传输单元等链路参数，确保链路正常工作。PPP 协议支持身份验证，提供多种身份验证方式，增强网络安全性，防止非法接入。PPP 协议支持数据压缩，可通过压缩算法对传输数据进行压缩，提高链路传输效率，减少传输延迟和带宽占用。PPP 协议支持灵活的配置选项，允许根据不同应用场景和需求，配置链路的各种参数，例如，是否启用加密、是否进行流量控制等。

3.3.3 PPP 协议的工作原理

PPP 协议的工作原理主要分为以下四个阶段。

1. 链路建立阶段

当两个设备之间的物理链路激活后，PPP 协议即开始启动。双方通过发送 LCP（Link Control Protocol）数据包来协商链路的参数，比如最大传输单元（Maximum Transmission Unit，MTU）、是否采用压缩等。只有当双方就所有协商参数达成一致后，链路建立阶段才成功完成，进入下一阶段。

2. 身份验证阶段（可选）

如果配置了身份验证，那么在链路建立后会进入此阶段。PPP 协议支持 PAP（Password Authentication Protocol）和 CHAP（Challenge Handshake Authentication Protocol）等身份验证方式。如果采用 PAP 方式，被认证方会将用户名和密码以明文形式发送给认证方进行验证，如果采用 CHAP 方式则更为安全，认证方会发送一个挑战消息，被认证方根据挑战消息和自身的密码计算出一个响应值，发送给认证方，认证方通过验证响应值来确定被认证方是否合法。

3. 网络层协议阶段

身份验证通过后，PPP 协议会针对不同的网络层协议进行相应的配置。通过 NCP（Network Control Protocol）协商网络层的参数，比如为 IP 协议分配 IP 地址等。当网络层参数协商完成后，双方就可以在链路上传输相应网络层协议的数据报。

4. 链路终止阶段

当一方想要终止链路时，与建立链路类似，会发送 LCP 数据包通知对方。双方完成释放资源、保存相关数据等必要的清理工作，再关闭物理链路，最终结束 PPP 连接。

3.3.4 PPP 协议帧格式

如图 3-4 所示，PPP 协议的帧格式由多个字段组成，具体介绍如下。

（1）标志字段（Flag）：占 1 字节，值固定为 0x7E，用于标识帧的起始和结束位置。

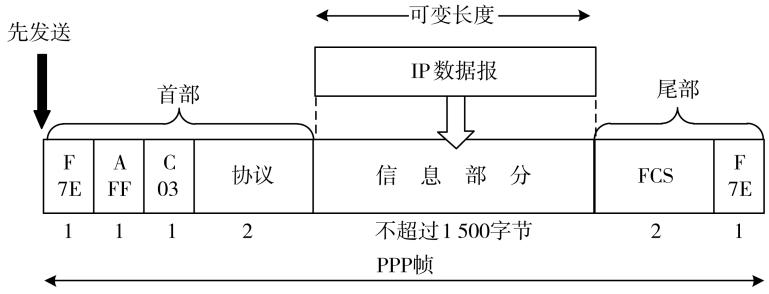


图 3-4　PPP 协议的帧格式

(2) 地址字段(Address):占 1 字节,通常设为 0xFF,由于 PPP 链路是点到点的,该字段一般无实际作用。

(3) 控制字段(Control):占 1 字节,常取值 0x03,代表无编号帧,主要用于实现基本的链路控制功能。

(4) 协议字段(Protocol):占 2 字节,用于指明帧中数据字段所承载的协议类型,例如,0x0021 表示承载的是 IP 协议数据,0xC021 表示承载的是链路控制协议(LCP)数据。

(5) 数据字段(Data):长度可变,包含了上层协议传来的数据,其具体长度由协议字段指定的协议以及链路层的最大传输单元(MTU)共同决定。

(6) 帧校验序列字段(FCS):通常为 2 字节或 4 字节,采用循环冗余校验(CRC)算法,用于接收方检测帧在传输过程中是否出现错误。

为保证数据传输的准确性,当数据字段中出现与标志字段 0x7E 相同的值时,会进行转义处理,将 0x7E 转为 0x7D、0x5E,0x7D 转为 0x7D、0x5D。

3.4　局域网

3.4.1　定义与特点

广播信道可以实现一对多和一对一的通信,20 世纪 70 年代诞生的局域网最初就广泛使用广播信道进行通信。局域网(Local Area Network,LAN)是指在某一区域内由多台计算机及相关设备通过网络设备连接而成的计算机网络,它覆盖的地理范围有限,且为一个单位所拥有。例如,南通大学的校园网是局域网,个人通过电缆直连两台计算机组建的网络也是局域网。

局域网具有如下特点。

(1) 覆盖范围小:一般覆盖范围在几十米到几千米以内,通常局限于一个建筑物内、一个校园或一个企业园区等较小的地理区域。如一个办公室、一栋教学楼或一个工厂车间内的网络。

（2）数据传输速率高：一般为 10 Mbps 到 1 000 Mbps，甚至可达 10 000 Mbps 及以上。例如，企业内部的局域网采用千兆以太网技术，能满足大量数据快速传输需求，支持多人同时高速下载文件、进行视频会议等。

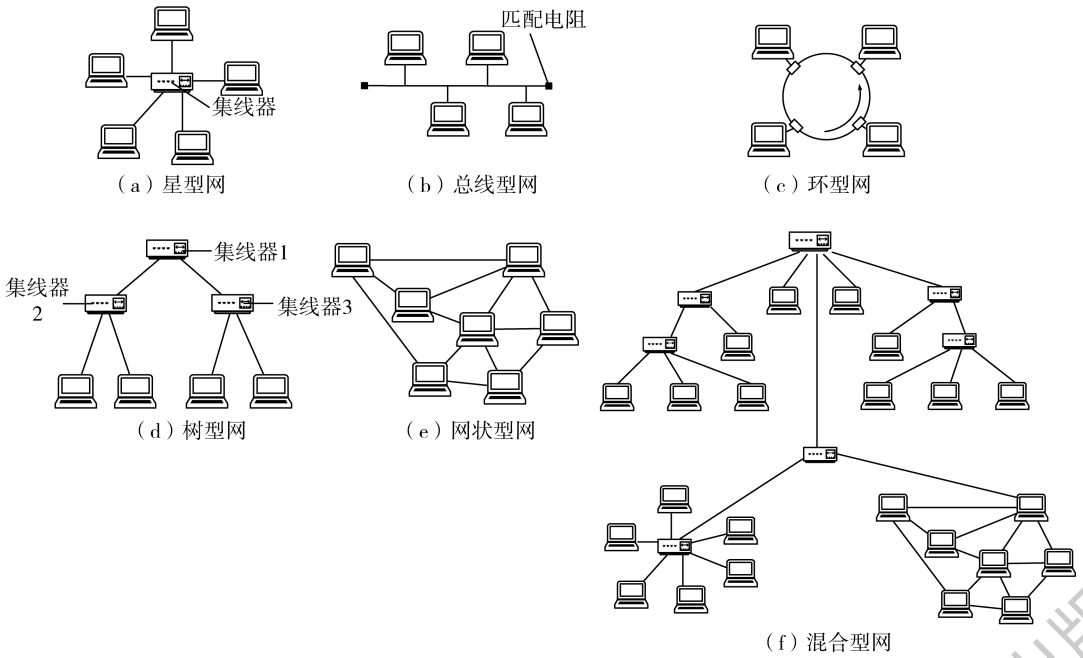
（3）传输延迟低：由于网络覆盖范围小，数据在网络中传输距离短，所以传输延迟通常较低，一般在几毫秒到几十毫秒。这使得局域网内的在线游戏、视频监控等实时应用能流畅运行。

（4）误码率低：局域网采用高质量的传输介质和可靠的通信协议，数据传输的误码率通常在 10^{-6} 到 10^{-8} 之间。例如，在使用光纤作为传输介质的局域网中，信号传输稳定，受外界干扰小，误码率很低，能保证数据准确传输。

（5）易于组建和维护：局域网的组建相对简单，只需购买网络设备如交换机、路由器等，将计算机等设备连接起来，并进行适当的配置即可，便于进行维护和管理。

3.4.2 局域网的拓扑结构

如图 3-5 所示，局域网的拓扑结构多样，常见的有星型、总线型、环型、树型、网状型与混合型等。例如，小型办公室网络常采用星型拓扑，以一台中心交换机为核心，连接多台计算机，这种结构便于扩展和管理。而校园网络则通常采用树型拓扑。



（a）星型网　（b）总线型网　（c）环型网

（d）树型网　（e）网状型网　（f）混合型网

图 3-5　局域网的常见拓扑结构

（1）星型拓扑结构

有一个中心节点（如交换机、集线器），其他节点都与该中心节点相连，所有数据均需通过中心节点进行转发。该结构的优点首先是易于扩展，添加新节点时只需将其连接到

中心节点，反之亦然；其次是便于集中管理和控制，中心节点可对各节点进行监测和管理。但缺点是中心节点负担较重，且一旦中心节点出现故障，会导致整个网络瘫痪。

应用：广泛应用于小型办公室与家庭网络等。如家庭中通过一台无线路由器连接多台电脑和手机，无线路由器就是中心节点。

（2）总线型拓扑结构

所有节点都连接在一条总线上，数据沿着总线进行传输，任何节点发送的数据都能被总线上的其他节点接收。该结构的优点是布线简单、成本较低。但缺点是由于所有数据都在同一条总线上传输，容易产生冲突，网络传输效率较低，而且总线出现故障，整个网络都会瘫痪。

应用：适用于家庭、办公室等计算机数目较少的局域网络，早期的一些小型网络多通过同轴电缆将多台计算机连接起来，就是典型的总线型拓扑。

（3）环型拓扑结构

网络中的结点通过点到点链路连接成一个闭合的环，数据在环中沿着一个方向逐站传输。该结构的优点是数据传输具有确定性，每个结点都有平等的访问权；但缺点是环中任何一个节点或链路出现故障，都会导致整个网络瘫痪，而且重新配置网络比较困难。

应用：早期的一些工业控制网络采用环型拓扑结构，例如，20 世纪 80 年代中期由 IBM 开发的令牌环网就是典型的环型拓扑。在一个自动化生产车间中，各个控制设备连接成环型网络。假设其中一个设备检测到生产线上的某个参数异常，它会将报警信息发送到环上，信息沿着环依次传递，最终到达控制中心进行处理。

（4）树型拓扑结构

本质上可看作一个多级星型拓扑，节点按照层次进行连接，形状像一棵倒置的树，顶端是根节点，向下分支连接多个子节点。该结构的优点首先是易于扩展，可以方便地增加新的分支和节点；其次是故障隔离较容易，某一分支出现故障不会影响其他分支。但缺点是对根节点的依赖性较大，如果根节点出现故障，会影响到其下属的多个分支。

应用：常用于企业园区网络，核心层、汇聚层和接入层的架构就类似于树型拓扑结构，便于对大型局域网进行分层管理和扩展。以一个大型企业的园区网络为例，企业总部的核心交换机作为根节点，连接各个办公楼的楼层交换机（子节点），每个楼层交换机又连接该楼层的各个办公室的接入交换机（孙节点），办公室的计算机再连接到接入交换机上。

（5）网状型拓扑结构

网络中的节点之间存在多条链路相互连接，形成一个网状结构。该结构的优点首先是可靠性高，任何一条链路出现故障不影响数据传输。其次是网络的冗余度高，容错能力强。但缺点是线路成本高，网络结构复杂，配置和管理难度大。

应用：主要用于对可靠性要求极高的骨干网络，如大型电信网络、国家级骨干网络等，以确保网络的稳定性和不间断运行。

（6）混合型网络拓扑结构

混合型网络拓扑结构指同时使用上面 5 种网络拓扑结构中的两种或两种以上的网络拓扑结构。这种网络拓扑结构是由星型结构和总线型结构的网络结合在一起的网络结构，这样的拓扑结构更能满足较大网络的拓展，解决星型网络在传输距离上的局限，而同

时又解决了总线型网络在连接用户数量的限制，兼顾了星型网与总线型网络的优点，在缺点方面得到了一定的弥补。

3.5 数据链路层基本功能

问题：

物理层处理的是位流，网络层处理的是 IP 数据报，数据链路层位于物理层与网络层之间。参考物流系统的快递寄送，思考数据链路层需要完成哪些工作？

为了实现网络层数据在数据链路上的传送，同时确保将物理层提交的比特流转换为数据链路层可以识别的传输单元，数据链路层主要需要解决两个主要问题，其一是高层载荷数据在本层如何完成封装，其二是如何检查本层传输中可能存在的错误。

3.5.1 数据帧封装

1. 定义

数据帧封装是指在计算机网络通信中，将上层协议传递下来的数据加上特定的帧头和帧尾信息，组成一个完整的数据帧的过程。这些添加的信息包含了诸如源地址、目的地址、帧类型及校验和等，使得数据能够在物理网络中正确地传输和被接收方识别。

2. 作用

通过将上层数据封装成帧，可以实现下面的三个功能。首先，封装实现了数据传输。封装后的数据帧包含了目标地址等信息，就像给数据贴上了“快递标签”，确保数据能准确无误地在网络中传输到目的地。其次，封装实现了错误检测，部分系统可能支持纠错。帧中包含的校验和字段，可让接收方检测数据在传输过程中是否发生错误，有的还能进行一定程度的错误纠正，保证数据的完整性和准确性。再次，封装实现了标识数据类型。通过帧类型字段，接收方可以知道所接收的数据是何种类型，如 ARP 请求帧、IP 数据包等，以便交给相应的上层协议进行处理。

3. 封装过程

数据帧封装过程如图 3-6 所示。首先添加帧头信息。在数据的前端添加帧头，帧头中包含目的 MAC 地址、源 MAC 地址、帧类型等字段。目的 MAC 地址和源 MAC 地址用于在局域网中标识数据的发送方和接收方的硬件地址。帧类型字段则指示了数据帧所承载的上层协议类型，例如，0x0800 表示 IP 协议。其次完成数据载荷装载。发送端将上层

传递下来的数据放入数据帧的有效载荷部分，最后添加帧尾信息。在数据的末尾添加帧尾，通常包含校验和字段。常用的校验算法如循环冗余校验（Cyclic redundancy check，CRC），发送方根据数据内容计算出一个 CRC 值，放在帧尾的校验和字段中。至此，发送端将整个数据帧发往物理层进行传输。接收端在收到数据帧后，会按照相同的算法重新计算 CRC 值，并与帧尾的校验和进行对比，若一致则认为数据传输正确，提取出原始数据并交给上层协议处理，否则判定数据有误。

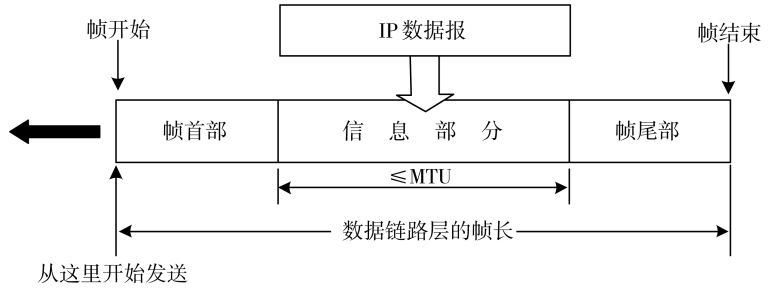


图 3-6　数据帧封装过程

3.5.2　差错校验

无论是信道介质还是物理层，都无法保证数据链路层收到的数据帧不会出现差错。如果 1 000 字节的数据帧中有若干比特传输过程中发送错误（比如 0 变为 1，或 1 变为 0），接收节点如何在数据链路层上发现上述传输错误，下面介绍数据链路层的另一个功能差错检测。

数据链路层的差错校验可以提高数据完整性保障能力。通过差错检测，能及时发现数据在传输过程中是否出现错误，确保接收方收到的数据与发送方发送的数据一致，避免信息丢失或误解。差错校验还可以提高传输效率。通过及时检测出错误，可以避免对错误数据进行不必要的后续处理，节省网络资源和时间，提高数据传输的整体效率。差错校验可以增强系统可靠性，是数据链路层的重要保护机制，有助于增强整个网络系统的可靠性，确保各种网络应用和服务能够稳定、准确地运行。

问题：

假如你是协议设计人员，如何检测数据帧是否在传输过程中发生了错误？

为了实现差错校验，容易设想的一个思路是“奇偶校验”算法，其原理是在数据位后添加一个奇偶校验位。若采用奇校验，那么添加校验位后，数据中“1”的个数为奇数。若为偶校验，数据中“1”的个数则为偶数。接收方通过检查接收数据中“1”的个数是否符合约定的奇偶性来判断数据是否出错。奇偶校验方法较为简单，但只能检测出错误而无法对其进行修正。此外，虽然双位同时发生错误的概率相当低，但奇偶校验却无法检测出双位错误。

因此需要考虑设计一个性能更强的差错校验。数据链路层广泛使用循环冗余校验(CRC)。发送方和接收方约定一个生成多项式 G(x)。发送方将待发送的数据 D(x)视为一个多项式的系数,在数据后面添加一定长度的冗余码(校验和),使得添加后的多项式能被生成多项式 G(x)整除。接收方收到数据后,用同样的生成多项式 G(x)去除接收到的多项式,如果余数为零,则认为数据无差错;否则,认为数据在传输过程中出现了错误。CRC 能检测出多种类型的错误,检测能力强,且实现相对简单,因此在数据链路层的差错检测中广泛应用。而上述添加的用来检错的冗余码被称为帧检验序列(Frame check sequence,FCS)。

下面通过一个具体的例子来说明循环冗余检验 CRC 的工作原理。假设发送方要发送的数据 D(x)为 110101,生成多项式 $G(x)=x^3+1$,对应的二进制位串是 1001。计算冗余码的具体步骤如下。

步骤 1:添加 0

在要发送的数据后面添加 n 个 0,n 是生成多项式的最高次数。这里多项式 G(x)的 n=3,所以在 110101 后面添加 3 个 0,得到 110101000。

步骤 2:除法运算,取余数作为冗余码

被除数:110101000

除数:1001

被除数 110101000 除以除数 1001,采用模 2 除法(即异或运算:当 A、B 不同时,输出 P=1;当 A、B 相同时,输出 P=0)。

①用 1101 除以 1001,商为 1,余数为 100。

②将余数 100 与下一位 0 组成 1000,再除以 1001,商为 1,余数为 001。

③重复上述过程,最终得到余数 011。

模 2 除法的计算过程如图 3-7 所示。

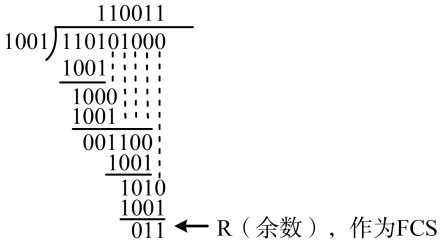


图 3-7　模 2 除法的计算过程

步骤 3:发送数据

把计算得到的冗余码(余数)011 添加到原始数据 110101 后面,得到要发送的数据 110101011。

步骤 4:接收方校验

步骤(4.1)

接收方收到数据后,用同样的生成多项式 1001 对收到的数据 110101011 进行模 2

除法。

步骤(4.2)

如果余数为 0,就认为数据在传输过程中没有出错。如果余数不为 0,就说明数据出现了错误,接收方会要求发送方重新发送数据。

以上就是循环冗余检验的工作过程,通过发送方计算冗余码并添加到数据中,接收方进行校验来判断数据传输的正确性。

如上所述,CRC 校验应用于数据通信,在以太网、PPP 等通信协议中,用于校验传输数据的完整性,确保接收端收到正确数据。它也可以用于存储设备(硬盘、U 盘、光盘等存储介质),检测数据在存储或读取过程中是否出现错误。此外,CRC 校验还可以应用于软件压缩与归档。ZIP 与 RAR 等压缩文件格式,利用 CRC 验证解压后的文件与原始文件是否一致,防止文件损坏或篡改。

需要指出的是,CRC 校验也存在一些缺陷。第一,虽然 CRC 能检测大部分常见错误(如单比特错误、双比特错误、奇数个比特错误等),但仍然无法识别一些特定错误。例如,对于与生成多项式存在倍数关系的错误,若错误序列恰好是 CRC 生成多项式的倍数,则校验会失效。对于某些长突发错误,当其长度超过 CRC 校验码的位数时,可能无法检测。第二,CRC 不具备纠错能力。CRC 仅能判断数据是否出错,无法定位错误位置,也不能自动纠正错误,需通过重传数据帧等方式解决。第三,CRC 存在生成多项式依赖性。校验效果依赖于生成多项式的选择,若多项式设计不合理,可能导致错误检测能力下降。

3.6　介质访问控制

3.6.1　信道争用

上文介绍了数据链路层的点对点信道和广播信道。对于前者,通信双方使用信道相对简单,无需考虑信道分配问题。但很显然,点对点信道并不适合节点规模逐渐增长的网络。而因为允许多对用户复用,广播信道在计算机网络发展过程中,曾经被广泛地应用。广播信道理论上属于所有连接该信道的用户,所以需要解决的关键问题是如何合理而高效地共享信道。

一种思路是静态划分信道资源,频分多路复用、时分多路复用等就属于静态划分。它的优点是用户只要获得了信道资源,通信时就不会与其他用户发生冲突。但缺点是实现代价较大,与可能造成信道资源浪费。

另一种思路是动态划分信道资源,这就需要解决谁可以获得信道资源以及如果多个用户争用信道如何解决冲突。因此,动态划分又可以细分为以下三类。

第一类是随机接入,也就是并不对节点发送做条件限制,有发送需求的节点都可以向共享信道发送数据。这样信道争用机制可以设计的比较简单,但需要解决多用户随机接入信道带来的信道冲突(也可称为碰撞)问题。具体内容下文在 3.6.2 节中会详细介绍。

第二类是通过令牌实现对信道的接入。令牌是一个特殊的帧，在环网中沿着物理链路依次传递。令牌有两种状态，空闲令牌和忙令牌。当网络中的某个站点有数据要发送时，它必须等待空闲令牌的到来。当收到空闲令牌后，该站点将其转换为忙令牌，并在令牌后面附加自己要发送的数据帧，然后将其发送到环网上。数据帧在环网中沿着各个站点依次传输，每个站点都会检查数据帧中的目的地址。如果目的地址与自己的地址匹配，则接收该数据帧，并在帧上做相应的标记，表示已经接收。数据帧继续在环中传输，直到回到发送站点。发送站点收到自己发送的数据帧后，将其从环网上删除，并释放令牌，将忙令牌转换为空闲令牌，继续在环网上传递，以便其他站点有机会发送数据。由于在任何时刻环网上只有一个令牌，因此只有拥有令牌的站点才能发送数据，这就避免了多个站点同时发送数据导致的冲突。因为令牌网不存在信道冲突，也就无需考虑如何解决冲突问题。

第三类是通过轮询实现对信道的接入。轮询机制通常由一个中心控制器（如基站、交换机等）来协调各个设备对信道的访问。中心控制器会按照一定的顺序依次询问每个设备是否有数据要发送。例如，控制器从设备 A 开始，询问 A 是否有数据发送，若有则允许 A 发送；接着询问设备 B，以此类推，直到轮询完所有设备；然后再从设备 A 开始下一轮轮询。轮询的优点是可以避免冲突，因为同一时刻只有被轮询到的设备才能发送数据，能有效管理多个设备对共享媒体的访问，适用于对实时性要求较高的场景，如工业自动化控制系统等，可保证每个设备都有机会在一定时间内发送数据。轮询的缺点是信道接入的效率不高，尤其是在设备数量较多且大部分设备没有数据发送时，会浪费大量时间在无数据设备的询问上，增加了传输延迟。而且中心控制器一旦出现故障，会导致整个系统瘫痪。

问题：

针对局域网的特点与用户需求，以上三种动态划分共享信道的方式中，哪一种更为合适？

由于局域网内的节点数量可能较大，各节点的发送需求也不一致，局域网主要选择第一种的随机接入，用以实现多节点高效利用共享信道。换言之，局域网优先选择了效率而非公平性。

3.6.2 CSMA/CD 协议

带冲突检测的载波侦听多路访问方法（Carrier Sense Multiple Access with Collision Detection，CSMA/CD）起源于美国夏威夷大学开发的 ALOHA 网所采用的争用型协议，并进行了改进。早期的局域网将许多计算机连接到一根总线上，采用广播通信方式，所有计算机共享传输介质。当多个设备同时尝试发送数据时，就会产生信号冲突，导致数据传输失败。为了解决多台计算机共享同一物理介质时的冲突问题，提高介质利用率，CSMA/CD 协议应运而生。

CSMA/CD 的基本原理是载波侦听（Carrier Sense，CS）、多点接入（Multiple Access，

MA)与冲突检测(Collision Detect,CD)。所谓载波侦听,每个站点在发送数据之前,通过检测总线上的信号电压变化,持续监听总线的状态,判断总线上是否有其他设备正在发送数据。若检测到总线上有载波信号,表示总线忙,站点需等待。若未检测到载波信号,则认为总线空闲,站点可发送数据。所谓多点接入,多个设备以多点接入的方式连接到同一根总线上,任何一个设备发送的数据都能被总线上的其他设备接收,形成广播式的通信环境。所谓冲突检测,在发送数据的同时,站点继续监听总线。如果监听到总线上的信号电压变化幅度超过正常发送信号的幅度,就说明传输过程中发生了冲突,此时有其他设备同时也在发送数据,导致信号相互干扰。接收方无法正确解析相互干扰的数据信号,继续发送数据帧只会浪费信道资源,因此,所有的发送节点立即停止发送。CSMA/CD 的算法流程如图 3-8 所示。

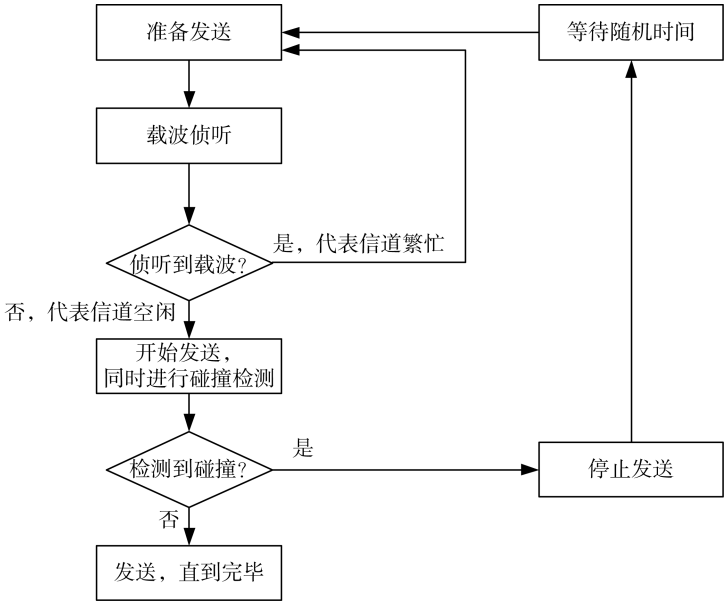


图 3-8　CSMA/CD 的算法流程

CSMA/CD 的工作机制可以概括为三点,即先听后发、边发边听与随机延迟重发。先听后发,站点有数据要发送时,先监听总线。若总线空闲,立即发送数据;若总线忙,则持续监听,直到总线变为空闲后再发送。边发边听,在发送数据过程中,持续检测总线,一旦检测到冲突,立即停止发送数据,并发送一个强化冲突的信号,让总线上的其他设备都能知道发生了冲突。随机延迟重发,发送站点在检测到冲突并停止发送后,会等待一个随机的时间间隔,再次尝试发送。这个随机时间间隔的选择,关系到下一次重传的碰撞概率。因此需要设计一个机制,尽量避免下一轮的重传冲突。CSMA 通常采用二进制指数退避算法,以减少再次冲突的概率,具体流程后文予以介绍。

如图 3-9,我们通过示例来说明 CSMA/CD 的工作流程。设有 A、B、C 三个站点连接在同一总线。A 站点准备发送数据,它先监听总线,发现总线空闲,于是开始发送数据。在 A 发送数据的过程中,B 站点也准备发送数据,它监听总线时,由于 A 正在发送,所以 B

判断总线忙，B 站点进入等待状态。如果此时 C 站点也有数据要发送，并且在 A 还未发送完时，C 站点监听到总线空闲（因为信号传播有延迟，C 站点可能还未收到 A 发送的数据信号），C 站点开始发送数据。这时总线上就发生了冲突，A 和 C 都会检测到冲突。A 和 C 检测到冲突后，立即停止发送数据，并发送强化冲突信号。此后 A 和 C 分别按照二进制指数退避算法计算出一个随机延迟时间，等待一段时间后再次尝试发送数据。例如，A 计算出的延迟时间较短，先再次尝试发送。如果此时总线空闲，A 就能成功发送数据；如果总线仍忙，A 就继续等待，直到总线空闲后再发送。

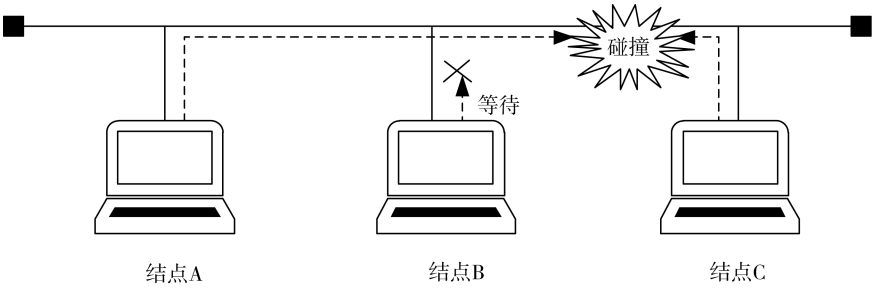


图 3-9　CSMA/CD 的工作流程示例

3.6.3　碰撞检测

为了确保冲突检测机制有效，以太网采用 CSMA/CD 协议，当一个站点发送数据时，需要先监听信道是否空闲，如果空闲则发送数据，并在发送过程中持续检测是否发生冲突。由于信号在网络中传播需要时间，为了让发送方能够在发送数据的过程中检测到冲突，就要求帧的长度足够长。考虑一个局域网中相距最远的两个站点，当一个站点发送的帧还未到达另一个站点时，另一个站点可能会误认为信道空闲而发送数据，从而导致冲突。只有保证数据帧的长度足够，使得信号在网络中传播一个来回的时间内，发送方还没有发送完整个帧，发送方才能够检测到冲突并进行相应处理，避免发送方检测不到数据帧碰撞。因此，为了实现碰撞检测，源节点发送的数据帧必须满足一个最小帧长度。

下面我们来尝试计算以太网的最小帧长度。考虑电磁波在铜缆中的传输速度略低于真空中的光速，设其传播速度为 200 000 000 m/s。那么 1 km 距离的传播时延约为 5 μs，考虑覆盖距离的上限，设一个大型局域网的端到端距离为 5 km（例如某大型校园网络的覆盖范围东西长度仅为 2 km）。上述局域网的单程传播时延为 25 μs，往返双程的传播时延为 50 μs。换言之，考虑最远距离情况，对于局域网中相距最远的 A 与 B 两结点，A 只有在自身开始发送数据帧并监听信道的时刻算起，约 50 μs 后才可能听到 B 发送的数据信号到达。已知以太网最初的标准速率 $R_{\min}$ 仅为 10 Mb/s。设以太网的最小帧长度为 $L_{\min}$ 字节，那么需要满足条件 $8\times L_{\min}/R_{\min}\geqslant 50\ \mu s$。简单计算可得，最小帧长度 $L_{\min}\geqslant 62.5B$。因此，当时以太网设定传输的数据帧长度不得小于 64B。如果结点 A 发送的数据帧低于这个最小长度，结点 A 可能在极短时间内（例如，20 μs）发送完自身的数据帧，就

取消了监听信道，导致无法监听到“姗姗来迟”（例如，传播时延为 49 μs）的节点 B 的数据信号。既然没有监听信道发生的信号冲突，节点 A 也就不会进入“随机延迟重发”阶段，最终造成数据帧的碰撞丢失。

问题：

通过设计帧碰撞检测与重传机制，是否就可以避免所有的碰撞？为什么？还需要设计其他机制吗？

3.6.4　二进制指数退避算法

在 CSMA/CD 协议中，当多个站点同时发送数据导致冲突后，如果这些站点立即重传，很可能会再次发生冲突，形成死循环。为了解决重传数据帧冲突，CSMA/CD 机制设计了一个随机延迟重发机制——二进制指数退避算法。它能让发生冲突的站点在等待一段时间后再重传，随着冲突次数的增加，等待时间会以指数方式增长，从而降低再次冲突的概率，使网络能够在重负荷情况下保持稳定。二进制指数退避的工作机制可以概括为以下四点。

1. 确定基本退避时间

把总线上的单程端到端传输时延记为 τ。一般取端到端的往返时间 2τ 作为基本退避时间，也称为冲突窗口或争用期。

2. 定义参数 k

k 与冲突次数 n 有关，规定 k 不能超过 10，即 $k=\min(\text{冲突次数 } n, 10)$。在冲突次数大于 10 且小于 16 时，$k$ 不再增大，一直取值为 10。

3. 计算随机等待时间

从离散的整数集合$\{0,1,2,\cdots,(2k-1)\}$中随机取出一个数 r，退避等待时间为 r 倍的基本退避时间，即 $r\times 2\tau$。

(1) 当冲突次数小于或等于 10 以后，从整数集合$\{0,1,2,\cdots,(2k-1)\}$中随机取出一个数 r，退避等待时间为 r 倍的基本退避时间，即 $r\times 2\tau$。

(2) 当冲突次数大于 10 以后，从整数集合$\{0,1,2,\cdots,(210-1)\}$中随机取出一个数 r，退避等待时间为 r 倍的基本退避时间，即 $r\times 2\tau$。

(3) 当冲突次数达到 16 次发送仍然失败，发送方丢弃传输的帧，向高层发送错误报告。

下面我们通过示例来说明二进制指数退避算法的工作流程。

假设站点 A 和 B 同时发送数据发生了冲突。

第一次冲突：冲突次数 $n=1$，$k=\min(1,10)=1$，从集合$\{0,1\}$中随机取数，若 A 取 0，

B取1，那么A等待$0\times2\tau=0$时间后尝试重传，B等待$1\times2\tau$时间后尝试重传，此时A先重传，若总线空闲则A重传成功。

第二次冲突：若A和B再次冲突，$n=2$，$k=\min(2,10)=2$，从集合{0，1，2，3}中随机取数，若A取2，B取3，A等待$2\times2\tau$时间后尝试重传，B等待$3\times2\tau$时间后再尝试重传。

多次冲突后：随着冲突次数n增加，k值不断增大，等待时间的取值范围按2的指数增大。当冲突次数n大于10且小于16时，k则仅能取10。站点等待随机时间后重传，直到成功发送或冲突次数超过16次发送失败。

3.7 以太网

3.7.1 IEEE802系列协议

局域网是一个基于覆盖范围的网络概念。20世纪70年代，以太网、令牌环网等实现局域网的多种不同技术陆续出现。这些技术在传输介质、访问控制方法等方面存在差异，导致不同厂商的设备难以相互兼容和通信。为了解决上述问题，电气和电子工程师协会(Institute of Electrical and Electronics Engineers，IEEE)于1980年2月成立了IEEE 802委员会，专门负责制定局域网的标准，以促进局域网技术的标准化和互操作性。1985年，IEEE802委员会正式推出IEEE802.3标准，规定了CSMA/CD的介质访问控制方式和物理层的技术规范。实现上述标准的以太网就此出现。

下面说明局域网与以太网的关系。局域网(LAN)是指在较小地理范围内(如办公室、校园、家庭等)连接设备的网络，属于按覆盖范围划分的网络类型。以太网(Ethernet)是实现局域网的一种具体技术标准。基于IEEE 802.3协议，以太网定义了数据链路层和物理层的规范(如数据帧格式、介质访问控制方式、传输介质等)。二者是“网络类型”与“具体技术”的关系。局域网概念出现以后，可以通过多种技术构建(如早期的令牌环网、ATM局域网、以太网及无线局域网Wi-Fi等)。但随着技术的发展和演进，以太网技术实现的局域网，应用最为广泛，占据了局域网市场的绝大多数份额。而其他可以实现局域网的网络技术(如令牌环网和ATM网络)则逐渐消失，目前在市场上几乎不再出现。所以准确来说，以太网是局域网的一种技术实现。而以太网凭借其优势成为局域网的绝对主流。因此现在很多非正式的场合，提到局域网，往往默认说的就是以太网技术实现的局域网。换言之，有时也可以比较宽泛地说，现在的局域网就是以太网。

需要额外说明的是，IEEE 802系列协议包括多个标准，每个标准针对不同的局域网技术或应用场景。例如，IEEE 802.3标准定义了以太网的介质访问控制方法和物理层规范。IEEE 802.11标准则是针对无线局域网的标准，规定了无线介质的访问控制和物理层传输方式等。通过IEEE 802系列协议的制定，局域网技术得到了统一和规范，不同厂商的设备能够实现互联互通，推动了局域网技术的广泛应用和发展。

3.7.2　网络适配器

网络适配器又称网卡，是连接计算机与网络的硬件设备。网卡的主要功能是实现数据的发送与接收、信号转换及网络协议处理。需要说明的是，网卡实现的功能包括数据链路层与物理层。网卡的数据收发过程如图 3-10 所示。

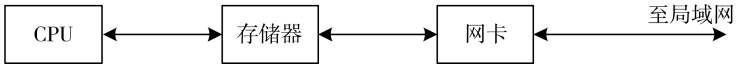


图 3-10　网卡的数据收发

1. 核心功能

（1）数据收发与格式转换

发送数据时将计算机中的二进制数据转换为网络信号（如电信号、光信号）。接收数据时将网络信号还原为计算机可识别的二进制数据。处理数据帧的封装与解封装（如添加 MAC 地址、校验码等）。

（2）信号处理与传输控制

实现物理层信号的放大、滤波等，确保信号稳定传输。遵循以太网协议，控制数据传输的时序（如 CSMA/CD 冲突检测）。

（3）网络地址识别

每个网卡有唯一的 MAC 地址（物理地址），用于网络中设备的身份标识与数据寻址。

2. 工作原理

（1）数据发送流程

数据封装，将网络层传下来的 IP 数据报添加帧头与帧尾，封装为 MAC 帧。信号转换，网卡将数据帧转换为电信号或光信号，通过传输介质发送至网络。

（2）数据接收流程

信号捕获，网卡接收网络传来的电信号或光信号，转换为数字数据帧。校验与过滤，验证数据帧的完整性（如 CRC 校验），并根据 MAC 地址过滤非目标数据。解封装与交付，剥除数据帧的协议头，将原始数据上交高层。

3.7.3　MAC 子层与 LLC 子层

如图 3-11 所示，IEEE 802 系列协议将局域网的数据链路层分为两个子层，分别是逻辑链路控制（LLC）子层和介质访问控制（MAC）子层。LLC 子层负责向网络层提供统一的服务接口，与传输介质无关。MAC 子层则根据不同的传输介质和访问控制方法，制定具体的规则，以实现对传输介质的有效访问和数据帧的正确传输。下面具体介绍数据链路层的 LLC 子层和 MAC 子层的功能与关系。

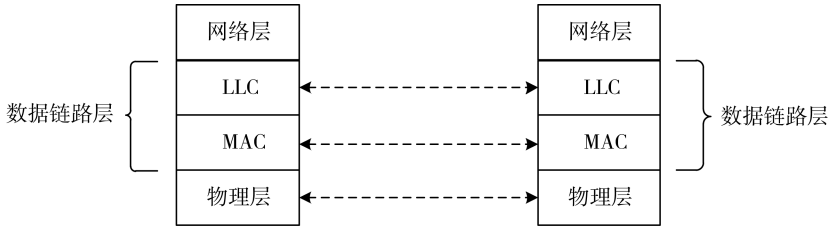


图 3-11　数据链路层的 MAC 子层与 LLC 子层关系

LLC 子层具体功能如下。首先向网络层提供统一的服务接口，屏蔽了底层不同物理网络的差异，使网络层无需关心具体的物理网络类型，增强了数据链路层的适应性和灵活性。其次实现差错控制，负责检测和纠正数据帧在传输过程中出现的错误。通过在帧中添加校验字段，接收方可以根据校验结果判断帧是否传输正确，发现错误时可要求发送方重传，以保证数据的可靠性。

MAC 子层具体功能如下。首先提供介质访问控制。根据不同的传输介质和网络拓扑结构，制定具体的介质访问控制方法，如 CSMA/CD、令牌环等，以确保多个站点能够公平、有序地访问共享的传输介质，避免数据冲突，提高信道利用率。其次实现帧的封装与解封。发送数据时，将网络层传来的数据封装成帧，添加 MAC 地址与帧校验序列等字段，以便交付物理层传输。接收数据时，对收到的帧进行解封，去除帧头和帧尾等信息，将数据传递给 LLC 子层。再次负责物理地址管理。物理地址即 MAC 地址。每个网络设备都有唯一的 MAC 地址，MAC 子层利用 MAC 地址来标识网络中的不同设备，实现数据帧的正确发送和接收。

LLC 子层和 MAC 子层相互协作，共同完成数据链路层的功能。需要说明的是，上述 LLC 与 MAC 的双子层划分是一种理想设计，以太网在工业界的发展与实现，最终并没有严格执行 IEEE802 委员会的 LLC 子层设计。可以理解为产业界（硬件制造商等）将 LLC 的部分功能省去，部分功能合并至 MAC 子层。所以现在提到数据链路层，可以仅指 MAC 子层，不再单独讨论或提及 LLC 子层。

3.7.4　MAC 地址

媒体访问控制（MAC）地址，也称为物理地址。下面介绍 MAC 地址的作用、结构与分类。

1. 作用

MAC 地址在局域网中用于唯一标识某个网络设备。它确保数据帧能够准确无误地发送到目标设备，就如同每个人的身份证一样，是设备在以太网中的“身份标识”。设备通过识别 MAC 地址来判断数据帧是否发送给自己。

2. 结构

MAC 地址是一个 48 位的二进制数(共 6 个字节),通常用十六进制表示一个字节,相邻字节之间用冒号或短横线隔开,如“00:16:3E:00:01:02”。前 24 位称为组织唯一标识符(Organizationally Unique Identifier,OUI),由 IEEE 分配给设备制造商,用于标识设备的生产厂商。后 24 位是由设备制造商自行分配的序列号,用于在同一厂商生产的设备中唯一标识每个设备。

3. 分类

(1) 单播地址

目的地址为单播 MAC 地址的帧会被发送到网络中唯一的一个设备。其特点是 MAC 地址的第一位为 0,如“00:01:02:03:04:05”。

(2) 广播地址

广播 MAC 地址为“FF:FF:FF:FF:FF:FF”。目的地址为广播地址的帧会被发送到局域网中的所有设备,所有设备都会接收并处理该帧。

(3) 组播地址

组播 MAC 地址用于标识一组设备。其特点是 MAC 地址首字节最低位为 1,如“01:00:5E:00:00:01”。目的地址为组播地址的帧会被发送到属于该组的所有设备。

3.7.5　以太网数据帧

如图 3-12 所示,以太网 MAC 帧包含 5 个字段,下面分别予以介绍。

目的 MAC 地址(Destination MAC Address):6 字节,用于标识帧的接收方设备 MAC 地址,该地址是唯一的,确保数据帧能准确无误地发送到目标设备。

源 MAC 地址(Source MAC Address):6 字节,标识发送方设备的 MAC 地址,使接收方能够知道数据帧的来源,以便进行响应或错误处理。

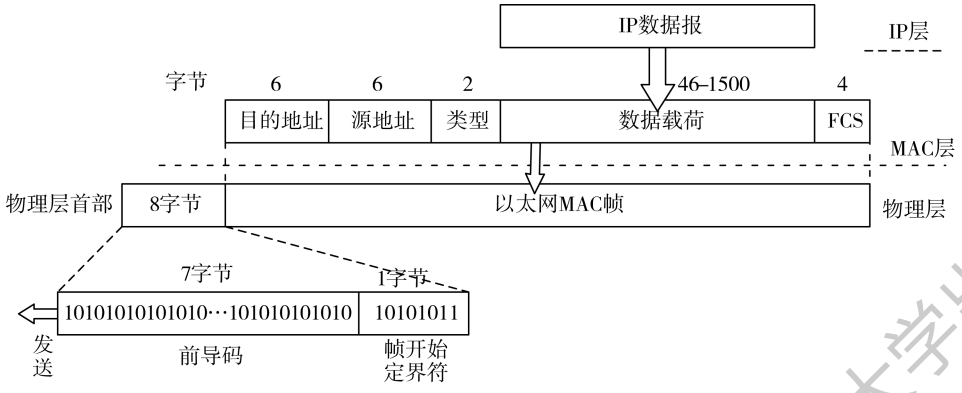


图 3-12　以太网数据帧结构

类型/长度(Type/Length):2 字节。如果该字段的值大于 0x0600,则表示上层协议的类型,如 0x0800 表示 IP 协议,0x0806 表示 ARP 协议;若小于等于 0x0600,则表示数据字段的长度。

数据字段(Data):长度在 46 到 1 500 字节之间,包含了要传输的上层协议数据,如 IP 数据报、ARP 请求或响应报文等。当数据长度小于 46 字节时,需要进行填充,以保证帧的最小长度为 64 字节。

帧校验序列(FCS):4 字节,采用循环冗余校验(CRC)算法生成,用于检测帧在传输过程中是否发生错误。接收方通过对收到的帧进行同样的 CRC 计算,并与 FCS 字段的值进行比较,若计算结果与 FCS 字段值不一致,则说明帧在传输过程中出现了错误。

目的 MAC 地址、源 MAC 地址与类型/长度三个字段组成数据帧的首部,数据字段为帧体,帧校验序列则为数据帧尾部。上述数据帧被数据链路层向下交付时,在物理层上还需在帧首部以前增加前导码与帧开始定界符。前导码(Preamble)由 7 个字节的 10101010 序列组成,用于实现接收端的时钟同步,使接收方的时钟与发送方的时钟保持一致,确保数据的正确接收。帧开始定界符(SFD)为 1 字节,固定值为 10101011,标志着一个帧的开始,通知接收方接下来的内容是一个以太网帧。

3.7.6 以太网的扩展

问题:

用户具备了网卡和线缆,是否就可以完全满足用户的组网需求?为什么?

以太网诞生以后获得了广泛应用,但也暴露出两个主要缺点。第一是覆盖范围有限。最初的以太网标准规定了网络的最大传输距离。例如,10Base-5 以太网中,粗同轴电缆的最大长度为 500 米。超过这个距离,信号会因传输损耗而变得难以识别,限制了以太网在大型场所的应用。第二是节点数量受限。每个以太网网段都有一个最大节点数限制。例如,10Base-2 以太网,一个网段最多连接 30 个节点。随着企业或机构中计算机数量的增加,单个以太网网段无法满足需求。因此考虑对传统的以太网进行扩展。需要说明的是,本节的所谓扩展仅限于数据链路层与物理层。在网络层看来,扩展的以太网仍然是一个网络。

1. 集线器扩展以太网

以太网技术的扩展,第一阶段使用了集线器(Hub)。作为工作在物理层的网络设备,集线器的主要功能是对信号进行放大和转发。当集线器的某个端口接收到信号时,它会将信号放大到合适的强度,然后向除接收端口外的其他所有端口广播该信号。这意味着连接到集线器的所有设备都能收到相同的信号,它们处于同一个冲突域中。

如图 3-13 所示,集线器通过增加端口数量来扩展以太网。它可以将多个以太网设备连接在一起,使原本分散的设备能够相互通信,从而扩大了以太网的覆盖范围和连接设备

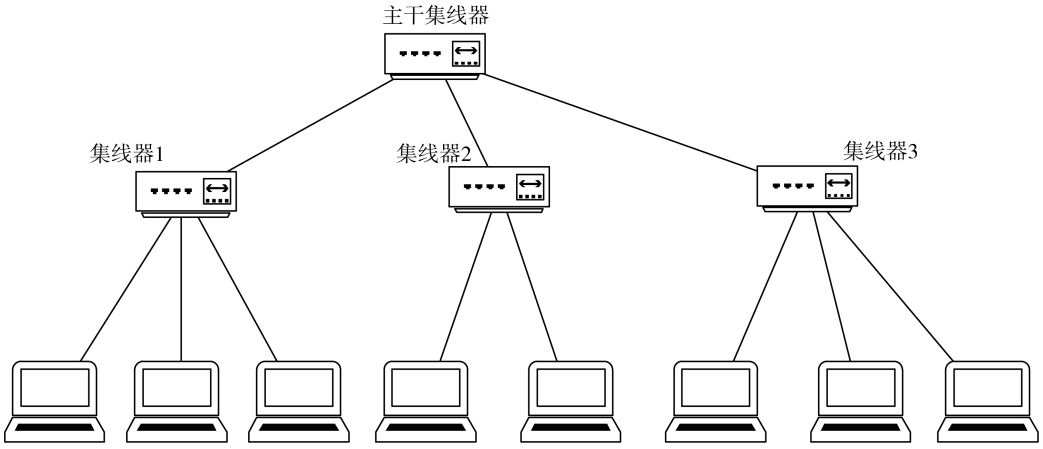


图 3-13　集线器扩展的以太网

的数量。例如，在一个小型办公室中，若有多台计算机需要联网，此时可以使用集线器连接这些计算机，将它们纳入同一个以太网网络中。

但是集线器扩展以太网也存在一些缺点。第一是冲突严重。集线器将所有连接的设备置于同一个冲突域中，任何时刻只能有一个设备发送数据，否则就会发生冲突。随着接入设备数量的增加，冲突的概率会大幅上升，导致网络效率降低。第二是带宽受限。集线器共享带宽，所有连接到集线器的设备共享同一带宽。例如，一个 100 Mbps 的集线器连接了 10 台设备，那么每台设备平均能使用的带宽只有 10 Mbps。因此，当多个设备同时传输数据时，可用带宽会降低。第三是安全性低。由于集线器采用广播方式转发数据，任何连接到集线器的设备都能接收到其他设备发送的数据帧，容易造成信息泄露，存在安全隐患。第四是网络管理困难。集线器对所连接的设备没有智能管理功能，无法对网络流量进行有效的控制和监测，网络出现故障时，排查问题也较为困难。第五是传输效率低。集线器不管数据帧的目的地址是什么，都会向所有端口广播，这会导致大量无效数据在网络中传输，占用了网络带宽，降低了传输效率。总之，由于集线器采用广播方式转发数据，随着连接设备增多，冲突概率增加，网络性能会下降，所以目前集线器已经很少应用于网络。

2. 交换机扩展以太网

针对上述集线器扩展以太网的问题，人们又提出了新的扩展设备——交换机（Switch）。作为一种工作在数据链路层的设备，交换机能够基于 MAC 地址转发和过滤数据帧。交换机拥有多个端口，每个端口都可以连接一台计算机终端，通过学习连接到端口设备的 MAC 地址，建立 MAC 地址表，然后根据数据帧中的目的 MAC 地址，将数据帧从源端口转发到对应的目的端口，实现设备之间的通信。

（1）交换机的功能与特点

交换机可以实现四方面功能。首先，隔离冲突域。交换机为每个端口提供独立的冲突域，使得连接到不同端口的设备之间的数据传输不会相互干扰，大大降低了冲突的发生概率，提高了网络性能。其次，提高网络带宽。交换机能够在多个端口之间同时建立并发

连接，实现多个数据帧的同时传输，使网络的总带宽得到了充分利用，每个设备都能获得相对独立的带宽，提高了数据传输速度。再次，学习与转发数据帧。交换机通过学习网络中设备的 MAC 地址，建立 MAC 地址表，根据目的 MAC 地址准确地转发数据帧，避免了像集线器那样的广播式转发，减少了网络中的无效数据传输，提高了传输效率。

相较于集线器，交换机具有以下特点。工作原理上，集线器是将接收到的信号向除接收端口外的所有端口广播，而交换机则是根据 MAC 地址表进行精准转发，只将数据帧发送到目的端口。冲突域上，集线器连接的所有设备处于同一个冲突域，而交换机每个端口都是一个独立的冲突域，大大降低了冲突概率，提高了网络性能。带宽利用上，集线器所有设备共享带宽，随着设备增多，每个设备可用带宽降低。交换机则能为每个端口提供独立的带宽，多个端口可同时传输数据，并发传输能力强，能更充分地利用网络带宽。安全性上，集线器以广播方式传输数据，所有设备都能接收数据帧，存在安全隐患。交换机基于 MAC 地址转发，只有目的设备能收到数据帧，提高了数据的安全性。

如图 3-14 所示，一个大型办公楼中有多个部门，每个部门都有若干台计算机。若采用传统的以太网，一个网段无法满足所有计算机的连接需求，且会因冲突过多导致网络性能下降。此时，可以使用交换机来扩展以太网。将每个部门的计算机连接到一台交换机的不同端口上，多台交换机之间再相互连接。这样，每个部门的计算机形成一个独立的冲突域，部门内计算机通信时不会影响其他部门，同时通过交换机之间的级联，实现了整个办公楼内计算机的互联互通，有效地扩展了以太网的覆盖范围和连接节点数量，提高了网络性能。

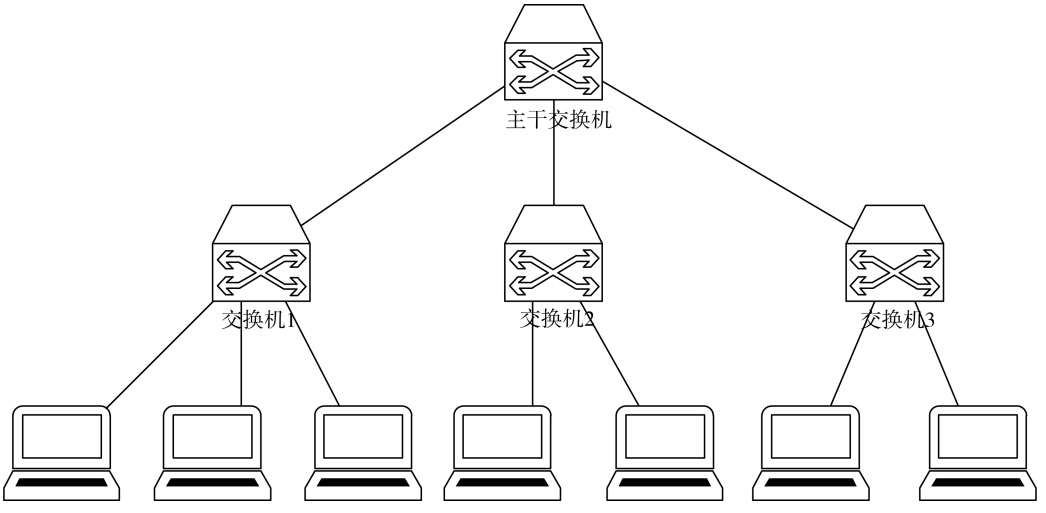


图 3-14　交换机扩展的以太网

(2) 交换机的工作原理

相较集线器广播数据帧给本网内的所有节点，交换机可以直接将 A 节点间数据帧直接发往节点 B。交换机能够自动转发数据帧，主要是基于交换机地址表(即 MAC 地址表)，用于存储 MAC 地址与交换机端口的对应关系。MAC 地址表结构主要包括三个内

容。首先是 MAC 地址字段，用于存储网络设备的 MAC 地址。其次是端口号字段，记录与 MAC 地址对应的交换机端口号，标识数据帧应从哪个端口转发出去。再次是老化时间字段，每一条 MAC 地址表项都有相应的老化时间，用于指示该表项在多长时间内未被更新就会被删除，一般默认值为 5 分钟。

显然交换机完成制作并出厂时，无法预知用于哪一个局域网，当然也不可能预存 MAC 地址表。因此，必须给交换机设计一个自动学习并更新 MAC 地址表的机制。我们称其为交换机的自学习功能，其具体过程如下。

学习过程。交换机初始启动时，其 MAC 地址表为空。当交换机的某个端口接收到一个数据帧时，它会检查该数据帧的源 MAC 地址，并将该地址与接收端口的信息记录到 MAC 地址表中。例如，一台计算机通过交换机的端口 1 发送数据帧，交换机就会将这台计算机的 MAC 地址与端口 1 对应起来，记录在 MAC 地址表中。

地址表更新。随着网络中数据帧的不断传输，交换机持续学习新的 MAC 地址与端口的对应关系，并更新 MAC 地址表。如果交换机发现一个已经在 MAC 地址表中的 MAC 地址对应的端口发生了变化，它会更新该条记录，以确保 MAC 地址表的准确性。

老化机制。为了保证 MAC 地址表的时效性，MAC 地址表中的每条记录都有一个生存时间。如果在一段时间内没有收到来自某个 MAC 地址的新数据帧，交换机就会自动删除该 MAC 地址与端口的对应记录。这样可以及时清除那些已经不再使用的 MAC 地址信息，为新的记录腾出空间。

随着网络中数据的不断传输，交换机逐渐学习到连接到各个端口的设备的 MAC 地址，从而构建起完整的 MAC 地址表。当交换机接收到一个数据帧时，它会根据数据帧中的目的 MAC 地址，在 MAC 地址表中进行查找。如果在 MAC 地址表中找到匹配的目的 MAC 地址，交换机就会将数据帧从对应的端口转发出去，实现数据帧的精准转发。如果在 MAC 地址表中未找到目的 MAC 地址，交换机会将数据帧向除源端口外的所有端口进行广播，以查找目的设备。当目的设备响应时，交换机就会学习到该设备的 MAC 地址与端口的对应关系，并更新 MAC 地址表，以便后续能够准确转发数据帧到该设备。交换机能够动态地建立和维护 MAC 地址表，准确地将数据帧转发到目的端口，提高网络的传输效率和性能。

下面通过一个具体示例说明交换机 MAC 地址表的自学习工作过程。如图 3-15 所示，设一个小型办公室网络中有一台交换机，连接了三台计算机 A、B、C，MAC 地址分别为 MAC-A、MAC-B、MAC-C，以下是交换机自学习的过程。

（1）初始状态：交换机的 MAC 地址表为空。

（2）当计算机 A 向计算机 B 发送数据帧时，交换机的端口 1 收到该数据帧。交换机检查数据帧的源 MAC 地址为 MAC-A，便将 MAC-A 与端口 1 的对应关系记录到 MAC 地址表中。此时 MAC 地址表中有一条记录：MAC-A 对应端口 1。

（3）随后计算机 B 向计算机 A 回复数据帧，交换机的端口 2 收到该数据帧。交换机学习到 MAC-B 与端口 2 的对应关系，将其添加到 MAC 地址表中，此时 MAC 地址表有两条记录：MAC-A 对应端口 1；MAC-B 对应端口 2。

（4）此后计算机 C 向计算机 A 发送数据帧，交换机的端口 3 收到该帧，交换机又将

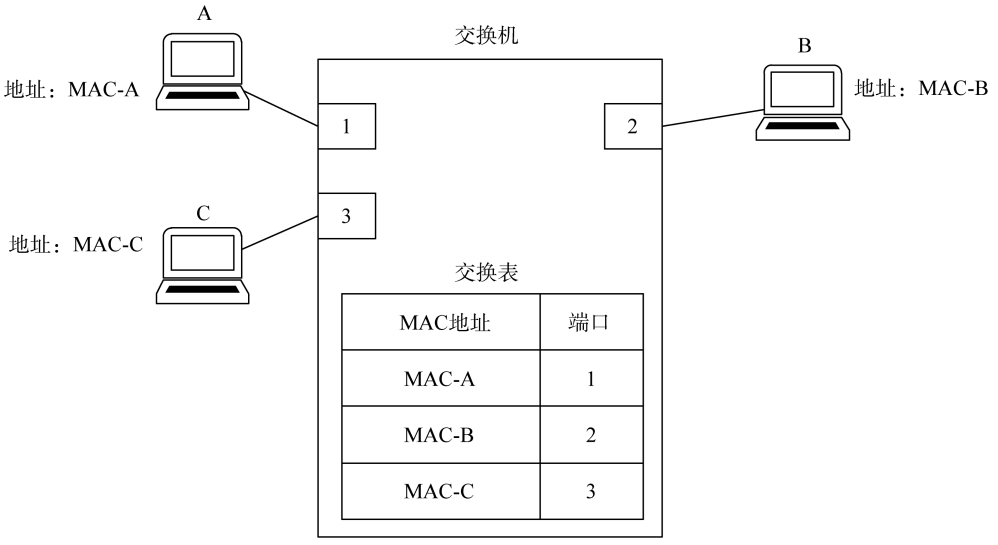


图 3-15　交换机 MAC 地址表的自学习工作过程

MAC-C 与端口 3 的对应关系记录到 MAC 地址表中，至此 MAC 地址表包含三条记录：MAC-A 对应端口 1；MAC-B 对应端口 2；MAC-C 对应端口 3。

(5) 若经过一段时间，计算机 B 关闭并从网络中断开，交换机在老化时间内未收到来自 MAC-B 的新数据帧，就会删除 MAC 地址表中 MAC-B 与端口 2 的对应记录。当计算机 B 重新连接到网络并发送数据帧时，交换机将再次学习其 MAC 地址与端口的对应关系并更新 MAC 地址表。

显而易见，交换机构建的以太网明显优于集线器构建的传统以太网。至此，采用交换机的星型结构成为以太网的主流，而传统以太网的总线型逐渐被淘汰。总线型以太网采用 CSMA/CD 协议，是一种半双工的通信。而交换机出现后，不再使用共享总线，也就没有碰撞问题，所以不再需要使用 CSMA/CD 协议，交换机以太网是一种全双工通信。但由于交换机构建的局域网仍然采用传统以太网的数据帧结构，所以继续沿用以太网这一称呼。

需要特别说明的是，尽管交换机构建的以太网已经完全不使用 CSMA/CD 协议，但教材仍然使用较大篇幅介绍传统以太网及其 CSMA/CD 协议，其原因有二。其一，以太网帧结构与传统以太网的 CSMA/CD 协议息息相关，不介绍 CSMA/CD 协议，将无法解释以太网帧结构的设计背景与思路。其二，CSMA/CD 协议的变体协议 CSMA/CA，仍被无线局域网 Wi-Fi 所使用，讲述 CSMA/CD 协议有助于学习者快速理解无线局域网的数据链路层通信原理。

3.7.7　高速以太网

随着计算机技术的发展，多媒体应用、视频会议等对网络带宽要求较高的应用不断涌现。传统以太网 10 Mbps 的速率无法满足数据快速传输的需求，促使高速以太网技术应

运而生。高速以太网能够满足企业对网络高带宽、低延迟的要求。互联网的普及使得网络用户数量急剧增加，网络服务提供商需要提升网络骨干链路的传输能力，以应对大量的数据流量。高速以太网为互联网骨干网络和数据中心网络提供了高速、可靠的连接，保障了互联网服务的稳定性和高效性。而光纤通信技术、半导体技术等相关技术的不断进步，为高速以太网的发展提供了技术支持。例如，光纤具有高带宽、低损耗的特点，能够满足高速以太网长距离传输的需求。新型的网络芯片和交换机技术也使得高速以太网设备的性能不断提升，成本逐渐降低，推动了高速以太网的广泛应用。

高速以太网是指速率达到或超过 100 Mbps 的以太网技术，其主要标准有如下几种。

快速以太网(100Base-T)：使用两对双绞线，一对用于发送，一对用于接收，数据传输速率为 100 Mbps。它又分为 100Base-TX(使用 5 类及以上非屏蔽双绞线或屏蔽双绞线)和 100Base-FX(使用光纤作为传输介质)等标准。

千兆以太网(1000Base-X)：数据传输速率为 1 000 Mbps，包括 1000Base-SX(多模光纤，短距离传输)、1000Base-LX(单模或多模光纤，长距离传输)和 1000Base-T(使用 4 对 5 类及以上非屏蔽双绞线)等。

万兆以太网(10 Gigabit Ethernet)：主要用于骨干网络连接等，速率高达 10 Gbps，通常采用光纤作为传输介质，有多种不同的物理层标准以适应不同的传输距离和应用场景。

高速以太网具有高带宽、兼容性好及易于部署的特点。首先，它能为网络中的设备提供更高的数据传输速率，满足视频会议、高清视频监控、大规模数据传输等对带宽要求较高的应用需求。其次，保留了传统以太网的帧格式、介质访问控制方法等，可与现有的以太网设备无缝连接，便于升级和扩展。最后，它的网络拓扑结构灵活，可采用星型、树型等结构，且设备安装和配置相对简单，降低了网络建设和维护的成本。

3.7.8　虚拟局域网

问题：

交换机出现后，冲突域受到了有效控制，但如果某个设备发送了广播消息，思考网络中的各台交换机将如何应对和处理？另外。一个单位往往拥有若干部门，各部门的数据往往需要保密，现有的以太网能否实现各部门内部的数据独享？

1. 背景

随着网络规模的扩大和复杂性的增加，传统局域网在管理、安全和性能等方面面临诸多问题。虚拟局域网(Virtual LAN，VLAN)应运而生，旨在解决这些问题。通过 VLAN 技术，可以将一个物理局域网划分成多个逻辑上相互独立的虚拟局域网，提高网络的灵活性、可管理性和安全性。如图 3-16 所示，利用 VLAN 构建的以太网结构。

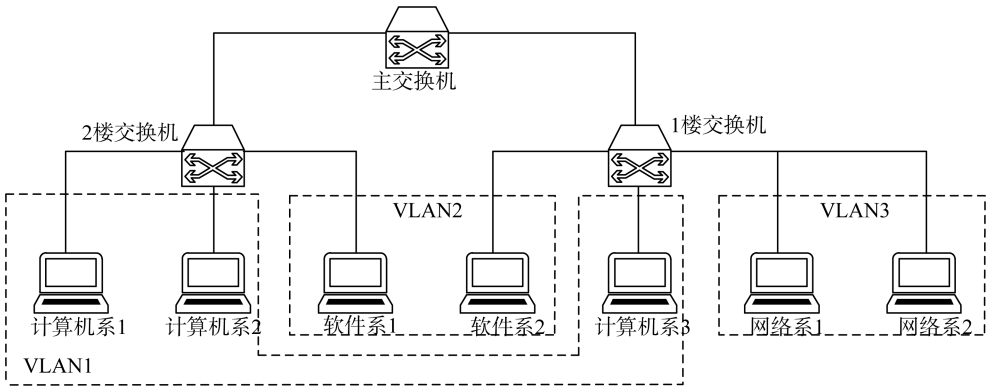


图 3-16　虚拟局域网示意图

2. VLAN 的作用

（1）隔离广播域

某公司网络中存在销售部、财务部、技术部等多个部门。若不划分 VLAN，当销售部的一台电脑发送广播消息时，整个网络中的设备都能收到，这会占用大量网络带宽，影响网络性能。通过划分 VLAN，每个部门处于不同的 VLAN 中，广播消息仅在本部门的 VLAN 内传播，不会扩散到其他 VLAN，从而有效隔离了广播域，提高了网络效率。

（2）增强网络安全性

在医院网络中，不同科室（如内科、外科、药房等）的业务数据具有不同的敏感性。将各科室的计算机划分到不同的 VLAN 后，未经授权的用户很难跨 VLAN 访问其他科室的数据。例如，药房 VLAN 中的设备无法直接访问内科 VLAN 中的患者病历数据，这在一定程度上防止了数据泄露和非法访问，增强了网络的安全性。

（3）灵活进行网络管理

在校园网络中，多个年级分布在不同的教学区域。通过 VLAN 技术，可以根据年级将网络设备划分到不同的 VLAN。例如，将每个年级的教室、办公室的网络设备分别划分到各自的 VLAN 中。当需要对某个年级的网络进行调整或维护时，只需针对该年级所在的 VLAN 进行操作，而不会影响到其他年级的网络。同时，也可以方便地为不同 VLAN 设置不同的网络访问权限和策略，实现灵活的网络管理。

3. 工作原理

（1）VLAN 的划分

VLAN 的划分方式有多种，常见的有基于端口、MAC 地址、网络层协议和 IP 子网等。基于端口划分是将交换机的端口划分到不同的 VLAN 中，同一端口下的设备属于同一个 VLAN。基于 MAC 地址划分则根据设备的 MAC 地址来确定其所属的 VLAN。基于网络层协议划分可依据不同网络层协议类型（如 IP、IPX 等）进行 VLAN 划分。基于 IP 子网划分是按照设备的 IP 地址所属子网来划分 VLAN。

（2）数据帧的标识与转发

当交换机收到一个数据帧时，会根据数据帧的源 MAC 地址和端口信息，以及已建立的 VLAN 映射表，为数据帧添加 VLAN 标签，标识其所属的 VLAN。带有 VLAN 标签的数据帧在交换机之间转发时，交换机根据 VLAN 标签来决定数据帧的转发路径，只将数据帧转发到同一 VLAN 的端口上，不同 VLAN 之间的数据帧相互隔离，不能直接通信。

（3）VLAN 间的通信

如果不同 VLAN 之间的设备需要通信，通常需要通过路由器或三层交换机来实现。路由器或三层交换机具有路由功能，能够在不同 VLAN 之间进行数据转发，实现 VLAN 间的网络层通信。

复习与思考

1. 数据链路层的主要功能是什么？

2. 计算 CRC 校验码：数据位 101101，生成多项式 $G(x)=x^3+x+1$。

3. 简述 CSMA/CD 的工作原理。

4. CSMA/CA 与 CSMA/CD 的主要区别是什么？

5. 以太网帧的最小长度是多少？为什么需要这个限制？

6. MAC 地址的长度是多少？通常如何表示？

7. 计算在以太网中，当发生第 3 次冲突时，可能的退避时间范围（假设基本退避时间为 51.2 微秒）。

8. 一个 PPP 帧的数据部分（十六进制）为 7D 5E FE 27 7D 5D 7D 5D 65 7D 5E，试解析真实数据。

9. 某 10Base-T 以太网使用 10 Mbps 共享式集线器连接 8 台计算机，所有设备同时向不同目标发送数据。问题：

（1）每台计算机实际可用的带宽是多少？

（2）若其中一台计算机持续占用信道传输数据，其他计算机的可用带宽变为多少？

10. 某网络使用全双工 100 Mbps 以太网交换机连接 4 台计算机，每台计算机分别与交换机的一个端口相连，且两两之间同时进行双向数据传输（例如，A→B 和 B→A 同时传输）。

问题：

（1）每台计算机的理论最大双向带宽是多少？

（2）整个交换机的背板带宽至少需要达到多少才能无阻塞传输？

11. 网络适配器的作用是什么？它工作在计算机网络体系结构的第几层？

12. 局域网的主要特点是什么？举例说明身边的计算机网络，哪些属于局域网。

阅读与拓展

材料1:二进制指数退避算法

在计算机网络数据链路层的介质访问控制协议中,二进制指数退避算法是CSMA/CD协议应对冲突的核心机制。当网络中的设备检测到数据传输冲突时,该算法通过指数级增长的随机退避时间,有效降低了再次冲突的概率,保障了网络通信的有序进行。算法不仅是技术领域的精妙设计,更蕴含着丰富的人生哲理与思政内涵。

二进制指数退避算法的工作原理基于“动态调整”与“概率优化”。当设备第一次检测到冲突时,它会在0和1两个时隙中随机选择一个作为退避时间。第二次冲突后,退避时间的选择范围扩大到0～3个时隙。第三次冲突则扩展到0～7个时隙。以此类推,退避时间的上限以2的指数幂形式增长。这种设计避免了多个设备在冲突后同时重传数据,如同交通路口发生拥堵时,车辆以不同的等待时间重新启动,有效缓解了道路压力。

在网络世界中,数据传输如同千万条河流并行流动,冲突不可避免。而二进制指数退避算法就像是一位智慧的管理者,通过动态调整重传时间,让每一条“数据河流”都能找到自己的节奏,避免了因无序竞争导致的网络瘫痪。这种“动态平衡”思维在现实生活中同样重要。无论是个人成长还是社会发展,我们都会面临各种“冲突”与矛盾。面对学业与兴趣的冲突、经济发展与环境保护的冲突等,我们需要学会动态调整自己的策略,在矛盾中寻找平衡,实现可持续发展。

二进制指数退避算法还彰显了“集体利益优先”的价值观。在网络环境中,每个设备都可能有传输数据的需求。但当冲突发生时,设备必须通过退避机制暂时放弃传输,以保障整个网络的稳定运行。为了整体网络的高效运行,个体设备需要做出一定的妥协和牺牲。这种集体主义精神在现实社会中不可或缺。在团队合作、社会治理等各个领域,我们都需要学会将个人目标与集体目标相结合。二进制指数退避算法通过个体的有序退让,实现了网络系统的整体优化,这为我们理解个人与集体的关系提供了生动的技术隐喻。

材料2:新一代移动通信技术6G

6G作为新一代移动通信技术,数据链路层在其中扮演着极为关键的角色。在6G网络里,数据链路层主要负责将物理层接收到的原始比特流,转化为可被网络层识别和处理的数据帧,并保障这些数据帧在相邻节点间可靠、高效地传输。

在功能上,6G数据链路层有着多方面的重要作用。首先,是介质访问控制(MAC)仍是6G的核心功能之一。在智能工厂与智慧城市等场景中,大量的传感器与智能设备需要接入网络。6G网络需要支持更多设备同时连接,因此6G的MAC需要通过合理的算法(如多址高速时分多址和正交频分多址),协调众多设备对无线频谱资源的访问,避免冲突,提升频谱利用率。其次,是差错控制。由于无线通信环境复杂,信号容易受到干扰,数据在传输过程中可能会出现错误。6G数据链路层采用自动重传请求(ARQ)、前向纠错编码(FEC)等技术来保障数据的准确性。一旦检测到数据错误,就会自动请求重传或者

利用冗余编码信息纠正错误，从而提高数据传输的可靠性。再次流量控制也是数据链路层的重要职责。它能够根据接收方的处理能力，动态调节发送方的数据发送速率，防止接收方因来不及处理数据而导致数据丢失，确保数据的稳定传输。

在技术创新上，6G 数据链路层有着新的突破。例如，采用更高效的链路适配技术，能够依据信道质量、信号强度等实时变化的网络条件，灵活调整数据传输的参数（调制方式、编码速率等），从而保障数据传输的稳定性和高效性。同时，6G 数据链路层还引入了网络编码技术，把多个数据包进行编码组合后再传输，这样不仅能提升数据传输的吞吐量，还增强了数据在复杂网络环境中的抗干扰能力。