第 5 章　计算机网络基础与应用

本章学习目标

- 了解计算机网络的发展历程。
- 掌握计算机网络的定义、功能及分类。
- 理解 OSI 参考模型及 TCP/IP。
- 理解 Internet 含义及发展阶段。
- 掌握 IP 地址的基本概念及分类。
- 了解常用的 Internet 服务。
- 熟练掌握无线路由器的使用。

本章首先介绍计算机网络的定义、发展历程及主要功能，从硬件和软件两方面对计算机网络的组成进行阐述，并描述常见的计算机网络分类及依据；其次针对全球最大的计算机网络 Internet，从其发展历程、接入技术及各类服务等方面进行介绍；最后结合实际应用介绍无线网络特别是无线局域网的相关知识及无线路由器的使用方法。

5.1　计算机网络基础

计算机网络是地理位置分散的、具有独立功能的多台计算机及其外部设备，利用通信设备和传输介质互相连接，在相应的网络软件及通信协议的管理和协调下，以实现数据通信和资源共享的计算机系统，如图 5.1 所示。其中，计算机技术和通信技术是计算机网络中的两大核心技术，二者的迅速发展及相互渗透，形成了计算机网络技术。因此，计算机网络是计算机技术与通信技术相结合，实现远程信息处理并达到资源共享的系统。

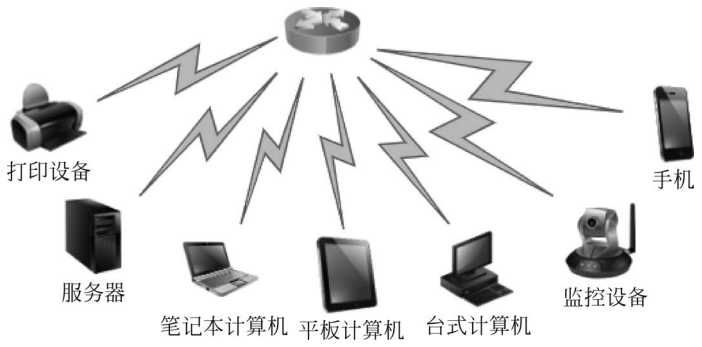


图 5.1　计算机网络示意图

5.1.1　计算机网络概述

1. 计算机网络的发展历程

计算机网络是计算机技术与通信技术相结合的产物。起初，计算机以单机模式被广泛

使用，然而随着计算机的不断发展，人们已不再局限于单机模式，而是将一个个计算机连接在一起，形成一个计算机网络。这样多台计算机连接后就可以实现信息共享，同时物理位置较远的计算机之间也可以即时传递信息。具体而言，计算机网络的发展大致经历了以下4个阶段。

1）面向终端的计算机网络

20世纪50年代初，美国麻省理工学院林肯实验室为美国空军设计被称为SAGE的半自动化地面防空系统，它用通信线路将远程雷达与测量控制设备连接到同一台IBM中央计算机上，由计算机进行集中的信息处理，再将处理好的数据通过通信线路送回到各自的终端设备，进而实现分布的防空信息能够集中处理与控制，这就是当今世界首次尝试将计算机技术与通信技术结合到一起。后来，20世纪60年代初，美国航空公司的飞机订票系统（即SABRE）又一次尝试通过一台中央计算机连接了遍布美国全境的2000多台终端设备，从而实现了分时多用户和集中控制处理，以计算机为中心的联机系统就这样产生了。

面向终端的计算机网络特点：以单个主机为中心，面向终端设备的星状网络结构。系统中除了中央计算机具有独立的数据处理功能外，系统中所连接的终端设备均无独立处理数据的功能。存在问题：主机负荷重，线路利用率低。

2）计算机通信网络

20世纪60年代中期，在美苏冷战期间，美国国防高级研究计划局（Defense Advanced Research Projects Agency，DARPA）提出要研制一种崭新的网络来对付来自苏联的核攻击威胁。于是，1969年美国国防高级研究计划局资助建立了一个名为ARPANET（即阿帕网）的网络，该网络当时只有4个节点，以电话线路作为主干通信网络，把位于洛杉矶的加利福尼亚大学，位于圣芭芭拉的加利福尼亚大学、斯坦福大学，以及位于盐湖城的犹他大学的计算机主机连接起来，这个ARPANET就是Internet最早的雏形，标志着计算机网络的发展进入了第二代。通信双方都是具有自主处理能力的计算机，而不是终端机，同时网络功能以资源共享为主，而不是以数据通信为主。

此后，ARPANET的规模不断扩大，到了20世纪70年代后期，网络节点超过60个，主机100多台，连通了美国东部和西部的许多大学和研究机构，而且通过通信卫星与夏威夷和欧洲地区的计算机网络互联。由此，ARPANET成为现代计算机网络诞生的标志，第一个真正意义上的计算机网络诞生。

计算机通信网络特点：采用分组交换技术的计算机网络，网络中的通信双方都是具有自主处理能力的计算机，功能以资源共享为主。存在问题：网络对用户不是透明的。

3）开放式标准化网络

为了促进网络产品的开发，各大计算机公司纷纷制定自己的网络技术标准。例如，IBM公司首先于1974年推出系统网络体系结构（System Network Architecture，SNA），1975年，DEC公司提出数字网络体系结构（Digital Network Architecture，DNA），1976年，UNIVAC公司也宣布了分布式通信体系结构（Distributed Communication Architecture，DCA）。有了网络体系结构，使得一个公司所生产的各种机器和网络设备可以非常容易地被连接起来。但是由于各个公司的网络体系结构是各不相同的，所以不同公司之间的网络不能互联互通。随着社会的发展，需要各种不同体系结构的网络互联，但是由于不同体系的网络很难互联。

针对上述情况，国际标准化组织（International Standard Organization，ISO）于 1977 年设立专门的机构研究解决上述问题，不久后提出了一个使各种计算机设备能够互连的标准框架——开放式系统互连参考模型（Open System Interconnection/Reference Model，OSI/RM），简称 OSI。OSI 共 7 层，1984 年正式发布了 OSI，各层的协议被批准为国际标准，给网络的发展提供了一个可共同遵守的规则，使各厂家设备、协议达到全网互联，计算机网络的发展走上了标准化的道路。

开放式标准化网络特点：网络体系结构的形成和网络协议的标准化，建立全网统一的通信规则，使计算机网络对用户提供透明服务。

4）面向全球互联的高速计算机网络

20 世纪 90 年代初至今都属于第四代计算机网络，自 OSI 参考模型推出后，计算机网络一直沿着标准化的方向发展，而网络标准化的最大体现就是 Internet（因特网）的飞速发展。Internet 的建立将分散在世界各地的计算机和各种网络连接起来，形成了覆盖世界的大网络。随着信息高速公路计划的提出和实施，它将当今世界带入了以网络为核心的信息时代，并成为世界上最大的国际性计算机互联网，计算机的发展已经完全与网络融为一体，计算机网络已经真正进入社会各行各业，为社会各行各业所采用，影响着人们工作生活的各方面。

面向全球互联的计算机网络特点：综合化、高速化、智能化和全球化。早期计算机网络是把许多计算机连接在一起。而在第四代互联网（internet）则把许多网络通过路由器等网络设备连接在一起，构成一个覆盖范围更大的计算机网络，即互联网是多个网络的互联。

2. 计算机网络的组成

按照计算机网络的功能，计算机网络可以划分为通信子网和资源子网两部分，如图 5.2 所示。其中，通信子网是由节点处理机和通信链路组成的一个独立的数据通信系统，提供计算机网络的通信功能。资源子网由主机、终端控制器和终端组成，提供访问网络和处理数据的能力。资源子网中主机负责本地或全网的数据处理，提供各种软硬件资源和网络服务。终端控制器用于把一组终端连入通信子网，并负责控制终端信息的接收和发送。

此外，全球最大的计算机网络 Internet 虽然其结构复杂，覆盖全球，但从工作方式上来看，可以分为边缘部分和核心部分两大块。其中，边缘部分是用户直接使用的，由所有连接在 Internet 上的主机组成，也称端系统，主要用于网络访问和资源共享；而核心部分则是由大量网络和连接这些网络的路由器等网络连接设备组成，是 Internet 中最复杂的部分，用于为边缘部分提供连通性和数据交换服务。

3. 计算机网络的功能

通过计算机网络的发展历程可以看出，计算机网络的功能主要体现在以下 4 方面。

（1）资源共享。资源共享是计算机网络的目的，也是计算机网络最核心的功能。可以使网络中各单位的资源互通有无、分工协作，大大提高了系统资源的利用率。共享的资源包括硬件资源、软件资源和数据资源。

（2）数据通信。数据传输是计算机网络最基本的功能，是实现其他功能的基础。数据通信主要指完成网络中各个节点之间的通信，包括各个计算机之间、计算机与网络连接设备之间以及各个网络连接设备之间的通信。

（3）分布式数据处理。分布式处理是指将分散在各个计算机系统中的资源进行集中控制与管理，从而将复杂的问题交给多个计算机分别同时进行处理，在均衡使用网络资源的同

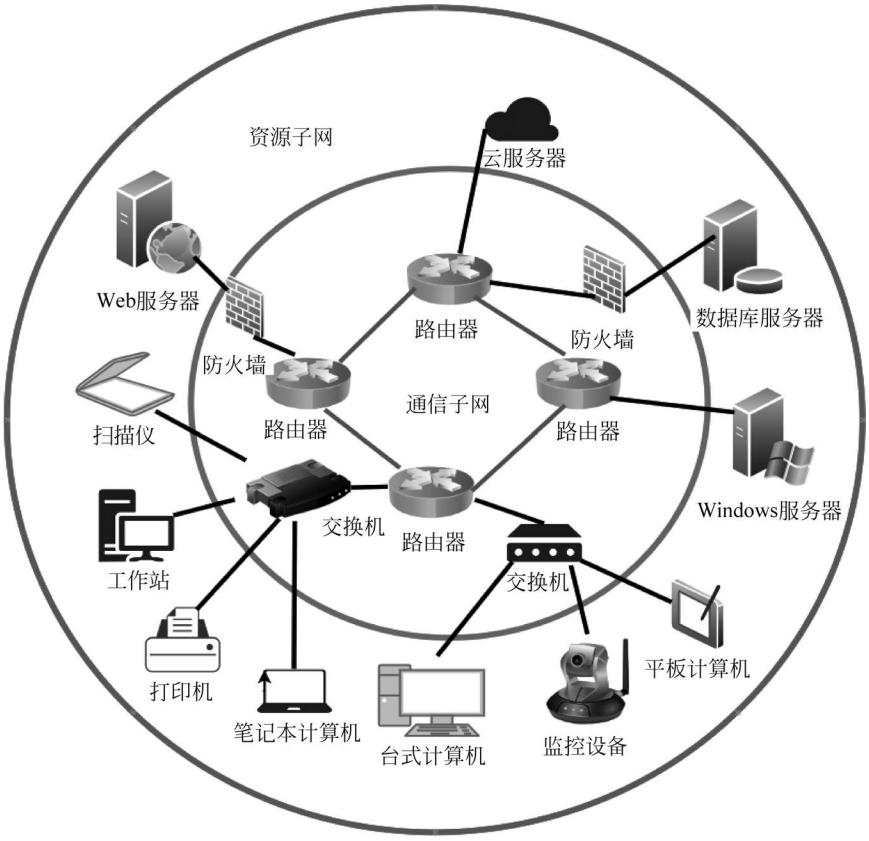


图 5.2　计算机网络的功能组成

时，提高工作效率。

（4）提高系统可靠性。在计算机网络系统中，可以通过结构化和模块化设计将大的、复杂的任务分别交给几台计算机处理，用多台计算机提供冗余，以使其可靠性大大提高。当某台计算机发生故障，不至于影响整个系统中其他计算机的正常工作，使被损坏的数据和信息得到恢复。

5.1.2　计算机网络系统

计算机网络系统由硬件系统和软件系统组成。其中，硬件系统包括主体设备（主机）、连接设备（网络节点）和传输介质（通信链路）三大部分；软件系统包括网络操作系统和应用软件等，网络中的各种协议也以软件形式表现出来。

1. 硬件系统

1）主体设备

计算机网络硬件中的主体设备——主机，也称计算机系统，担负数据处理工作，进行信息的采集、存储和加工处理等具体任务，无关计算机的规模，大型机、小型机、微型机均可。根据其具体功能可进一步分为服务器（中心站）和客户机（工作站）两类。其中，服务器是指提供网络服务和共享资源的主机，其性能通常优于客户机，一般是大型机、小型机等。根据所提供服务的不同，可进一步分为文件服务器、Web 服务器、邮件服务器等。客户机通常是

指用户访问网络的工作站，即用户通过客户机使用网络。与服务器相比，客户机配置低、性能指标要求不高，常见的客户机包括个人计算机、笔记本计算机、手机、平板计算机等。

2）连接设备

连接设备也称网络节点，作为计算机与网络的接口，负责网络中信息的发送、鉴别、接收和转发等功能。连接设备的性能直接影响网络的传输性能指标，如速率、延时、丢包率、稳定性等。在局域网中通常使用交换机、路由器等，大型网络中一般由一台通信处理机来担当，还具有存储转发和路径选择的功能。常见的连接设备包括网卡、集线器、中继器、网桥、交换机、路由器和网关等，如图 5.3 所示。

(a) 网卡

(b) 集线器

(c) 中继器

(d) 网桥

(e) 交换机

(f) 路由器

(g) 网关

图 5.3　常见网络连接设备

（1）网卡。

网卡(Network Interface Controller，NIC)也称网络适配器，是计算机连接到网络的核心硬件设备，是计算机与网络之间进行数据交换的桥梁。如图 5.3 所示，网卡一般插在机器内部的总线槽上，也可以集成在主板上，都有唯一固定的 MAC 地址。网卡接口类型有连接同轴电缆的 BNC 接口和连接双绞线的 RJ45 接口。

网卡作为主机连接网络的节点，负责把主机要向网络传输的数据按照一定的格式转换为网络设备可处理的数据形式，通过网线传送到网络。同时，接收网络传来的数据，并把数据转换为主机可识别和处理的格式，通过计算机总线传输给主机。作为一种物理层和数据链路层的设备，网卡提供网络通信的基础，承担数据缓冲、介质访问控制、主机数据的编解码等功能，减轻主机 CPU 负担。现代网卡通常支持全双工通信，能够同时进行数据的发送和接收，并支持 IPX/SPX、NetBEUI 和 TCP/IP 等多种网络标准和协议。日常使用中，可通过定期更新驱动程序，保持网卡的兼容性。

（2）集线器。

集线器(Hub)是连接多台计算机或其他设备的连接设备。它是计算机网络发展早期的重要设备，只包含物理层协议，主要提供信号放大和中转的功能，工作在物理层，采用广播式群发。一个集线器上往往有 4 个、8 个或更多的端口，端口彼此相互独立，所有连接在集线器上的主机都共用一条传输通道，共享带宽，各个主机的带宽由对应端口平均分配。

集线器的工作原理相对简单，当端口收到数据时，集线器就会将这个信号放大，然后广播到除接收端口之外的所有其他端口。这种广播方式导致集线器网络中的所有设备都在一

个冲突域内，无法隔离冲突域，易造成网络风暴。由于所有连接设备都能收到数据，安全性较差、效率低。当多个设备同时发送数据时，也会发生冲突，需要通过 CSMA/CD(载波侦听多路访问/冲突检测)机制来解决。

(3) 中继器。

中继器是一种用于接收、放大和重新发送信号，以克服信号在传输过程中的衰减问题，进而延长网络传输距离的设备。与集线器类似，中继器也工作在物理层，本质上看可以认为是一个放大器，承担信号的放大和传送任务，增加信号的有效传输距离。中继器通常只有两个端口，可以连接相同或不同的物理媒介。当信号通过传输媒介传输时，会因为各种因素，如电阻、干扰等，而逐渐衰减，中继器接收到该衰减信号后，会对其进行放大和整形，然后重新发送。其处理过程不对信号所携带的信息内容更改，只是增大了信号的强度和质量，即通过简单的信号处理来扩展网络的物理范围。

在计算机网络发展的早期，中继器在扩展以太网范围方面发挥了重要作用。它允许网络超过单一网段的限制，连接更远距离的网络设备。用中继器可以连接两个局域网或延伸一个局域网，它连起来的仍是一个网络，与集线器处于同一协议层次。然而，中继器存在不能隔离冲突域、不能连接不同的网络协议、级联使用时存在延迟累积问题、无法过滤或处理数据等不足，随着计算机网络的发展，其被更先进的设备所取代。在一些旧的网络系统中，中继器仍在使用，以便维持现有的网络结构。此外，一些需要长距离传输，但不需要复杂网络功能的工业环境中，中继器仍不失为一个简单有效的解决方案。

(4) 网桥。

网桥是一种工作在数据链路层的桥接器，用于连接两个局域网的一种存储/转发设备。主要功能包括过滤通信量、扩大物理范围、增加局域网上的工作站的最大数目、提高可靠性等。作为早期的两端口二层网络设备，网桥可将一个大的虚拟局域网(Virtual Local Area Network，VLAN)分割为多个网段，或者将两个以上的局域网(Local Area Network，LAN)互联为一个逻辑 LAN，使得 LAN 上的所有用户都可以访问服务器。

网桥通过接收、存储、地址过滤与转发的方式实现互联网络之间的通信。它可以将一个大的网络划分为多个小的冲突域，每个冲突域都有独立的带宽，从而提高网络的性能和可靠性。网桥的工作过程包括接收帧、检查帧和转发帧 3 部分。首先，网桥接收来自一个局域网的数据帧。其次，检查数据帧的目的地址，如果目的地址属于另一个局域网，网桥就将数据帧转发到该局域网；如果目的地址属于同一个局域网，网桥就丢弃该数据帧。网桥通过地址表记录每个局域网中设备的 MAC 地址和对应的端口信息，以便快速转发数据帧。

网桥能够隔离冲突域，提高网络的带宽利用率和性能。它还可以扩大网络的物理范围，增加局域网上的工作站的最大数目。此外，网桥还可以实现不同物理层网络和传输率网络的互联。但是，网桥在转发数据帧之前需要先进行存储和查找站表，增加了网络时延。当网络负荷较重时，可能因网桥缓冲区的存储空间不够而导致帧丢失。此外，当所连接设备数量较多时会产生较大的广播风暴。

网桥主要用于实现局域网之间的互联。在早期的网络环境中，网桥是连接不同局域网的主要设备之一。然而，随着交换机技术的发展和应用，网桥逐渐被拥有更多端口和功能的交换机所替代。但在某些特定场景下，如连接两个小型局域网时，网桥仍然具有一定的应用价值。

(5) 交换机。

交换机是现代计算机网络中最常用的连接设备之一,它工作在数据链路层,能够根据MAC 地址进行数据包的转发,将数据包转发到目标设备,完成信息交换功能,大大提高了网络的效率和性能。交换机的主要功能包括物理编址、错误校验、帧序列以及流控制。通过为每个端口相连的设备建立独立的电信号通路,避免了共享式网络的带宽争用问题,提高了网络性能。以太网交换机是最常见的交换机类型,此外还有电话语音交换机、光纤交换机等。

交换机的工作原理可以分为 3 个步骤:学习、转发和过滤。首先,交换机通过学习过程识别网络中设备的 MAC 地址,并建立地址表。在学习过程中,交换机监听网络中的数据包,并记录数据包的源 MAC 地址和端口号。其次,在转发过程中,交换机根据目标 MAC 地址查找地址表,确定数据包应该从哪个端口转发。如果地址表中没有目标 MAC 地址的记录,交换机会将数据包广播到所有端口。最后,过滤过程可以防止重复的数据包到达目标设备,提高网络的效率。

交换机提供了大量的端口,支持高速的数据传输和通信,避免了共享网络的带宽争用问题,提高了网络性能。交换机还可以实现网络分段,通过 MAC 地址表过滤不必要的网络流量,提高安全性。现代交换机还具备对 VLAN 的支持、链路汇聚等功能,部分甚至集成了防火墙的功能。交换机虽然提高了网络性能,但在某些情况下,如广播风暴发生时,仍然可能导致网络拥塞。此外,交换机本身并不具备路由功能,不能实现跨网络的数据包转发。

交换机广泛应用于局域网、城域网(Metropolitan Area Network,MAN)、广域网(Wide Area Network,WAN)等不同类型的网络。在局域网中,交换机可以连接计算机、终端和其他设备,提供高速的数据传输和通信。在城域网和广域网中,交换机可以作为汇聚层设备,将多个接入层交换机的流量汇聚到核心层交换机。此外,交换机还可以用于构建虚拟专用网(Virtual Private Network,VPN)、防火墙等网络安全设备。

(6) 路由器。

路由器是一种工作在网络层的网络连接设备,主要用于在网络中转发数据包,将数据从一个网络传输到另一个网络。作为构建现代网络的关键设备之一,路由器是互联网和企业网络的核心组件。路由器的主要功能包括路由选择和数据传输。路由选择是指路由器根据路由表选择最佳的路径,将数据包传输到目标地址。数据传输是指路由器将数据包从一个网络传输到另一个网络。路由器还具有网络隔离、安全检测、负载均衡、网络监控和流量分析等功能。

路由器的工作原理可以概括为两个基本过程:路由选择和数据传输。首先,路由器从网络上接收到一个数据包。其次,路由器从数据包中识别出目标地址,并根据路由表选择最佳的路径。最后,路由器将数据包传输到下一站路由器或目标设备。路由表是路由器的核心组件之一,它存储了网络地址和最佳路径之间的映射关系。路由表是根据路由协议生成的,常见的路由协议包括 RIP、OSPF 和 BGP 等。

路由器能够实现跨网络的数据包转发,支持大规模的网络和复杂的网络拓扑结构。路由器还具有网络隔离、安全检测、负载均衡、网络监控和流量分析等功能,提高了网络的安全性、可靠性和性能。与交换机等连接设备相比,路由器的配置和管理相对复杂,需要专业的网络知识和技能。此外,路由器的价格相对较高,对于小型网络来说可能成本较高。

目前，路由器广泛应用于互联网和企业网络中。企业可以使用路由器将本地网络连接到互联网，实现企业与客户、合作伙伴等的数据交换。路由器可以通过网络隔离实现安全隔离，防止网络攻击和恶意软件传播。此外，路由器还可以实现负载均衡，将数据包传输到多个网络，以提高网络性能和可靠性。

（7）网关。

网关是现代通信技术中不可或缺的一部分，它充当着互联网、局域网等不同网络之间的桥梁，使得不同网络之间的通信变得更加便捷、高效。网关可以将一个网络的协议格式转换为另一个网络可识别的协议格式，实现不同网络之间的数据传输。网关的主要功能包括协议转换、路由选择、安全检测、数据过滤等。网关需要具备转换不同协议格式的能力，支持数据缓存、分组、组装、再传输等功能，以保证数据的快速、稳定传输。此外，网关还能实现路由选择、防火墙、入侵检测等网络安全功能，保障网络安全。

网关的工作原理是将一个协议格式的数据包接收进来，在进行数据格式转换后再转发到另一个网络中。网关一般放置在网络边缘，与不同网络相连。当一个数据包在源网络中发送时，将首先被发送到网关。网关会对数据包进行协议格式的解析，然后再构建适合目的网络的协议格式，发送到目的网络中。

网关能够实现不同网络之间的无缝连接和数据传输，提高了网络的灵活性和可扩展性。网关还具有强大的安全性能，如防火墙、入侵检测等，保障了网络的安全。但网关的配置和管理相对复杂，需要专业的网络知识和技能。网关的价格与其他设备相比更高，相应网络成本较高。在某些特定场景下，如两个网络协议完全兼容时，可能不需要网关进行协议转换。

网关广泛应用于不同网络之间的连接和通信。例如，家庭路由器就是一种网关设备，它将家庭内部的设备与公网进行连接。企业内部的不同子网之间需要通信时，也可以使用网关设备来实现。此外，在跨地域的数据传输和通信中，网关也发挥着重要作用。

交换机、网桥、路由器和网关是现代计算机网络中不可或缺的连接设备。它们各自具有独特的功能和工作原理，在不同的网络场景中发挥着重要作用。交换机提供了高速的数据传输和通信能力；网桥主要用于实现局域网之间的互联；路由器实现了跨网络的数据包转发和安全隔离；网关则充当着不同网络之间的桥梁，使得不同网络之间的通信变得更加便捷、高效。这些设备共同构成了现代计算机网络的基础设施，支撑着各种网络应用和服务的发展。

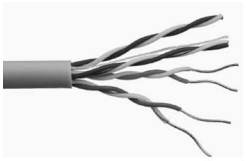
3）传输介质

传输介质是指连接各个网络设备和节点之间的通信信道（桥梁），是网络中进行数据收发的物理通道，也是信道传递的载体。负责数据的物理传输的这些介质，可以分为有线传输介质和无线传输介质两大类。常见的有线传输介质包括双绞线、同轴电缆和光纤等，如图5.4所示。常见的无线介质则包括无线电波、微波、红外线、卫星通信、蓝牙等。每类传输介质在传输距离、抗干扰性等性能指标上有所差异，根据自身的特点在相应场景进行应用。

（1）有线传输介质。

① 双绞线。

双绞线是最常见的有线传输介质之一，由多根细线组成，通常是将两根绝缘导线绞合在一起以减少电磁干扰。根据单位长度上绞合次数的不同，把双绞线分为不同的规格。绞合次数越高，则抗干扰能力越强。根据双绞线外是否有屏蔽层，双绞线可分为非屏蔽双绞线



(a) 双绞线

(b) 同轴电缆

(c) 光纤

图 5.4　常见网络有线传输介质

(Unshielded Twisted Pair,UTP)和屏蔽双绞线(Shielded Twisted Pair,STP)。UTP 没有金属屏蔽层,价格相对便宜,而 STP 在 UTP 的基础上增加了金属屏蔽层,以提高抗干扰能力。

根据双绞线的类别不同,传输率也有所不同,常见的有超五类线(Cat5e)、六类线(Cat6)等,传输率可达 1～10Gb/s。通常而言,双绞线的传输距离不超过 100m,对于更远距离的传输,需要加入中继器或交换机等设备。双绞线具有价格适中、安装简单、维护方便的优点,由于其传输距离较短,一般用于家庭网络、办公网络等短距离传输的局域网内。

② 同轴电缆。

同轴电缆由内外两层导体构成,包括内导体铜芯和外导体屏蔽层,中间夹着绝缘层以及最外层的塑料保护外层。借助屏蔽层的作用,同轴电缆具有很好的抗干扰能力。根据直径的不同,可分为粗缆和细缆。粗缆适用于长距离传输,而细缆成本相对较低。

同轴电缆的抗干扰能力强,能有效抵抗电磁干扰。因此,传输距离远,适用于长距离通信。传输率也可达到几百兆比特每秒至几吉比特每秒级别。但其安装和维护复杂,成本较高。多用于有线电视网络、城域网和宽带的接入等。

③ 光纤。

光纤是一种利用光的全反射原理(当光从光密介质射向光疏介质时,只要入射角超过某一角度,折射光完全消失,只剩下反射光线的现象)进行数据传输的传输介质。光纤通常由玻璃或塑料纤维组成,传输率高,传输距离远。

按传输模式可分为单模光纤和多模光纤。与单模光纤相比,多模光纤芯径较大,存在多种入射角度,光线以波浪形式传输,多种频率共存,其光源可选用较为便宜的发光二极管。而单模光纤比多模光纤的衰减更小,无中继传输距离更远,但其光源通常是较为昂贵的半导体激光器。

由于采用光传输信号,不受电磁干扰,与其他有线传输介质相比,光纤具有带宽高、传输损耗小、抗干扰能力强、传输距离远、传输率高、体积小、重量轻等优点。特别适用于长距离数据传输、高速网络、数据中心之间的连接等。但其连接需要专用设备,安装和维护复杂。

(2) 无线传输介质。

① 无线电波。

无线电波是一种通过空气传播的电磁波,频率范围很广,从低频到高频不等,按波长和频率可分为超长波、长波、中波、短波和超短波等波段。在无线通信中,无线电波是主要的传输介质。根据调制方式和频率不同,传输率有所不同,一般在几兆比特每秒至几吉比特每秒。不同波段的无线电波具有不同的传播方式和应用领域。其中,长波主要用于导航,引导舰船和飞机按预定线路航行,同时也有一部分用于高质量的调频广播;中波主要用于广播、

导航和通信等方面；短波可以沿地面以地波方式传播，也可通过电离层反射以天波方式传播；超短波指波长为1～10m的无线电波。

无线电波通信无需物理连接，灵活性强。但其信号强度易受距离衰减和障碍物干扰的影响，传输率相对有线传输较低，传输距离有限，根据环境状况，从几米到几万米不等。适用于移动通信网络、无线局域网(Wireless Local Area Network，WLAN)、广播、电视信号传输等。

② 微波。

微波是较低频率的电磁波，通常在几兆赫兹到几吉赫兹，波长在1mm～1m。微波通信利用微波在直线视线范围内进行数据传输，可以被地面或者空中的接收设备接收。由于微波是沿直线传播，而地球表面是一个曲面，因此，易受障碍物阻挡，传输距离有限，通常在50km左右。为能够进行远距离通信，需设立相应的中继器进行信号的放大转发，如很多高山上可以看到一些电视转播塔，维护成本较高，且通信的隐蔽性和保密性差。

微波通信具有较大的通信信道容量，传速率高，适用于移动电话、无线电视等数据传输领域。特别是远距离通信，微波通信比电缆通信成本小、可靠性高。

③ 红外线。

红外线是一种电磁波，频率高于可见光但低于微波。红外线传输利用红外光信号进行数据传输。通常以红外二极管或红外激光器作为发射源，以光电二极管作为接收设备。与微波相比，实现较为简单，无需复杂的微波调制，设备也相对便宜。但其传输距离短，不能透射不透明物，传输率较低。适用于近距离、低传输率的数据通信场景，如红外线遥控器等。

④ 卫星通信。

卫星通信是航天技术与电子技术相结合的重要技术，发展于19世纪60年代，利用空间轨道中运行的地球同步卫星作为中继站，地球站作为终端站，实现两个或多个地址站之间的远距离、大容量通信。由于信号需要经过卫星转发，卫星通信具有一定的传输时延。

卫星通信的覆盖范围广，部署灵活，通信可靠，不受地理环境条件限制等优点，可实现全球范围内的通信。例如，我国自行研制的北斗卫星导航系统，可在全球范围内全天候、全天时为各类用户提供高精度、高可靠定位、导航、授时服务，并且具备短报文通信能力。

⑤ 蓝牙。

蓝牙作为一种短距离无线通信技术，具备低功耗的特点，主要用于设备之间的数据传输和设备互连。如日常手机、计算机与蓝牙耳机、无线音箱等设备之间的连接。

计算机网络中的传输介质各有其特点和适用场景。在选择传输介质时，需要根据实际需求、成本、性能等因素综合考虑。有线传输介质适用于对稳定性和抗干扰能力要求较高的场景，如企业网络和长距离通信；而无线传输介质则适用于移动设备之间的快速通信以及临时构建的网络。

2. 软件系统

在计算机网络中，软件系统扮演着至关重要的角色，它们不仅支撑着网络的基本运作，还促进了信息的高效传输与应用。网络软件系统包括网络操作系统、网络管理软件、网络应用软件、网络安全软件等，只有正确合理地选择相应的软件，才能够相互配合，完成所要求的网络功能。

1) 网络操作系统

网络操作系统(Network Operating System，NOS)是计算机网络软件系统的核心，它是

建立在独立的操作系统之上，专门用于管理和控制网络资源的软件系统。网络操作系统不仅具备单机操作系统的基本功能，如内存管理、CPU 管理、输入输出管理、文件管理等，还扩展了一系列网络特有的服务和管理功能，以面向计算机网络用户提供各种网络服务。与其他操作系统相比，网络操作系统侧重于优化网络活动相关的特性，如通过网络管理相关的共享文件、软件应用和外部设备等资源，稳定性和安全性相对更好。

网络操作系统的主要功能包括以下 4 方面。

（1）网络通信管理：网络操作系统负责实现网络节点间的数据传输，确保数据包的正确发送和接收。

（2）网络远程管理：支持用户远程访问和操作网络资源，如远程文件访问、远程打印等。

（3）网络资源共享：管理网络中的各种共享资源，如磁盘空间、打印机等，确保资源高效利用。

（4）安全管理：提供网络安全策略的实施和监控，保护网络资源免受非法访问和攻击。

2）网络管理软件

网络管理软件是用于配置、监控和管理网络系统的工具。它可以帮助网络管理员轻松地管理网络设备、配置网络参数、监控网络状态、诊断网络故障等。

常见的网络管理软件包括以下 3 种。

（1）SolarWinds：一款功能强大的网络管理软件套件，支持多种网络设备的管理和监控。

（2）PRTG：一款易于使用的网络监控软件，提供实时网络性能监控和报警功能。

（3）Nagios：一款开源的网络监控和报警系统，支持多种监控插件和扩展功能。

网络管理软件的主要功能如下。

（1）网络配置：提供图形化界面或命令行接口，允许管理员配置网络设备的参数和设置。

（2）性能监控：实时收集和分析网络设备的性能数据，如吞吐量、延迟、丢包率等，帮助管理员了解网络运行状况。

（3）故障排查：提供故障检测和诊断工具，帮助管理员快速定位和解决网络问题。

（4）安全审计：记录网络访问和操作日志，提供安全审计功能，确保网络安全合规性。

3）网络应用软件

网络应用软件是指运行在计算机网络上，为用户提供各种网络服务和功能的软件。它们涵盖了浏览器、电子邮件客户端、即时通信软件、云存储服务、社交媒体平台、在线支付平台、在线教育平台、在线娱乐平台、在线办公软件等多个领域。如谷歌浏览器、火狐浏览器、微软 Edge 等，用于访问互联网并展示网页内容。微软 Outlook、苹果 Mail、谷歌 Gmail 等，用于发送和接收电子邮件。微信、QQ、Skype 等，允许用户通过网络实时地与其他用户进行文字、语音和视频交流。百度云、腾讯微云、阿里云等，提供文件和数据在云端的存储、共享和备份服务。微博、抖音、小红书等，允许用户分享信息、交流和互动。

随着云计算、大数据、人工智能等技术的不断发展，网络应用软件将呈现更加智能化、个性化和集成化的趋势。未来，网络应用软件将更加注重用户体验和数据安全，为用户提供更加丰富、便捷的网络服务。

4）网络安全软件

网络安全软件用于保护计算机和网络免受恶意软件和网络攻击的威胁。其通过实施各种安全措施和策略，确保网络系统的安全稳定运行，主要包括防火墙、入侵检测系统、加密技术等。

常见的网络安全软件包括360安全卫士、腾讯电脑管家、火绒安全、卡巴斯基等。其中，360安全卫士是一款功能全面的网络安全软件，提供防火墙、病毒查杀、系统修复等多种安全功能。腾讯电脑管家是腾讯公司开发的网络安全软件，集杀毒、管理、加速于一体，提供全方位的安全保护。此外，卡巴斯基安全软件也提供强大的病毒查杀和防护功能。

计算机网络的硬件系统和软件系统是密切且相互依存的。它们共同构成了完整的计算机网络系统，发挥不同的作用，但又相互协作以实现网络通信的功能。硬件系统提供物理基础设施，如网卡、交换机、路由器等；而软件系统提供协议实现、网络管理和应用支持。二者相互结合才能实现完整的网络功能。硬件系统的性能（如带宽、处理能力）直接影响网络的整体性能，而软件系统的效率（如协议实现、算法优化）则决定了如何充分利用硬件资源。硬件设备如交换机、路由器等需要相应的软件系统来配置和管理，以实现高级功能，如VLAN、路由选择、安全策略等。硬件系统的更新通常需要相应的软件支持，如新的驱动程序或固件更新。同时，软件系统的升级也需要考虑与现有硬件的兼容性。

网络问题的诊断和解决通常需要同时考虑硬件和软件两方面，因为问题可能出现在任何一个环节或二者的交互中。计算机网络中硬件系统和软件系统是紧密集成的整体，它们共同工作以提供可靠、高效的网络通信服务。

5.1.3 计算机网络的分类

从不同角度出发，计算机网络可以依据不同的标准进行分类。计算机网络的常见分类方式包括以下4种。

1. 按拓扑结构分类

拓扑（Topology）图是网络设计和管理中的一种图示工具，用于展示网络中各个设备（如交换机、路由器、防火墙等）及其连接关系，帮助理解网络结构和数据流向，是网络规划、故障排查和性能优化的重要参考。拓扑图就像是一张网络的“地图”，通过图形化的展示，网络管理员可以更直观地了解网络的整体结构，识别网络中的设备和它们相互连接的关系。

当网络出现问题时，拓扑图可以帮助快速定位故障点。在进行网络升级或扩展时，拓扑图有助于制定合理的规划方案。此外，拓扑图也是进行网络安全评估的重要参考依据。简言之，网络拓扑结构是指网络中通信线路（链路）和节点相互连接所构成的几何形式。其中，节点包括计算机、交换机或路由器等设备。按照拓扑结构的不同，可以将网络分为总线网络、环状网络、星状网络、网状网络和树状网络等，如图5.5所示。通过理解不同类型拓扑图的特点和用途，可以更好地根据实际需求选择合适的网络拓扑结构，以满足性能、可靠性和管理的要求。

1）总线拓扑

总线拓扑（Bus Topology）网络中，采用单一信道作为传输介质，所有节点都连接到一个单一连续的物理线路（总线）上。数据通过这一条总线传输到所有节点，每个节点都通过专门的连接器接到总线，如图5.5(a)所示。

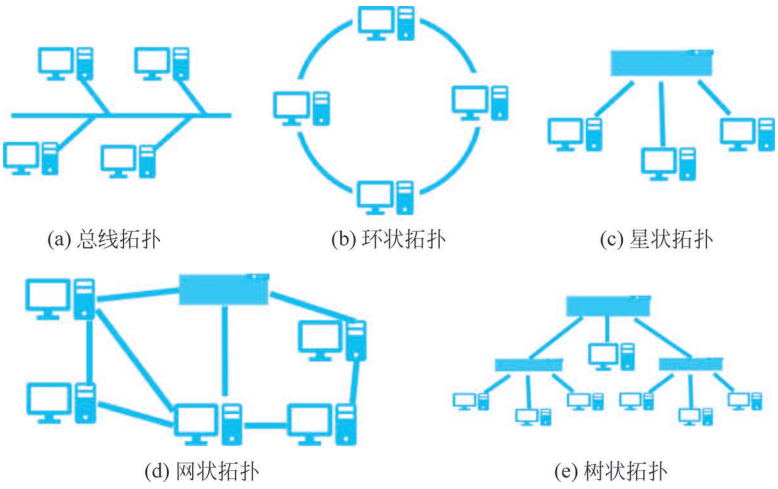


图 5.5　常见网络拓扑结构示意图

每个节点发送的数据都沿着总线向两个方向扩散，并且能够被连接在总线上的所有节点接收。各节点在接收数据时进行地址检查，看是否与自身的地址相符，相符则接收数据，反之丢弃。因此，总线拓扑网络的一个重要特征是可以在网络中广播信息，也称广播网。

总线拓扑网络的主要优点包括成本低、布线安装简单、入网灵活。只需要一条主干线缆，线缆和连接设备数量较少，节点扩张方便灵活，单个节点故障不会影响其他节点通信，可靠性高。总线拓扑网络的主要缺点包括故障排查困难、总线负载能力低、扩展受限等。一旦主干电缆出现故障，就会造成节点之间的隔离，整个网络都会受到影响；增加节点或扩展网络可能导致性能下降和发送冲突的问题。因此，总线拓扑网络适用于小型网络或低带宽需求的环境，常见的有 Ethernet、ARCNet 和 Token Bus 等。

2）环状拓扑

在环状拓扑(Ring Topology)网络中，每个节点都与两个其他节点相连，连接网络中各节点的线路形成了一个封闭的环，如图 5.5(b)所示。在该类网络中，数据必须沿着环路的节点单向传输，即每个节点都转发数据，直到数据到达目标节点。数据发送过程中，各节点识别数据中的目的地址，如与本节点的地址一致，则数据被接收；否则，将其传送给下一个节点。数据环绕一周后，由发送节点将其从环上删除。为避免数据冲突，环状拓扑网络通常使用令牌传递方式，也称令牌环网。

环状拓扑网络具有数据传输稳定、最大传输时延固定、传输机制简单、易于安装和监控等优点。由于每个节点都参与数据的发送，因此环状拓扑网络中每个节点都有相同的负载，能实现负载均衡。然而，环状拓扑网络中任何一个节点或连接的故障都会影响整个网络的通信，除非使用双环设计。此外，节点的增加和删除不方便，增加新节点需要断开网络环路，影响网络的稳定性。环状拓扑网络中的网卡等通信部件比较昂贵且管理复杂，其抗干扰能力比较强，主要用于工厂环境、数据中心等大型网络场景中，以满足高稳定性、高带宽的需求。

3）星状拓扑

在星状拓扑(Star Topology)网络中存在一个节点作为中心节点，所有其他节点都直接与中心节点相连，所有的数据都通过中心节点转发，如图 5.5(c)所示。常见的中心节点包

括集线器和交换机等，其中集线器的主要功能是对接收到的信号进行再生整形放大，进而扩大网络的传输距离。

星状拓扑网络属于集中控制型网络，中心节点对整个网络的通信进行集中式控制管理，各节点间的通信都要通过中心节点。即每个要发送数据的节点都需要将数据先发送到中心节点，再由中心节点负责将数据送到目的节点。

星状拓扑网络具有便于集中管理、方便扩展和故障排查的优点。只要中心节点正常，网络基本不受影响，单个设备故障不会影响其他设备；在网络中添加新节点时，只需将其连接到中心节点即可。然而，星状拓扑网络存在高度依赖中心节点、线缆成本高的缺点。由于所有通信都需经过中心节点，一旦中心节点出现故障，会导致整个网络瘫痪，中心节点是整个网络的瓶颈，必须具有高可靠性。同时，所有节点都需与中心节点相连接，进而需要较多的线缆来连接所有设备。因此，星状网络通常适用于小型企业网络、办公室网络或校园网等。

4）网状拓扑

网状拓扑（Mesh Topology）网络采用无规则的连接方式，每个节点都有一条或多条链路与其他节点相连，每个节点可以与任何节点相连，形成一个网状结构，如图 5.5(d)所示。

网状拓扑结构的主要优点是可靠性高、扩展性好、容错能力强。由于节点之间的路径较多，相应的碰撞问题、阻塞问题大大减少，数据的传送路径可以通过动态优化选择，多条路径确保数据能够绕过故障节点，不会因某个局部网络故障影响整个网络正常工作，添加新设备也不会影响现有网络。然而，网状拓扑网络也具有网络管理复杂、经济成本高等缺点。各节点的布线和配置复杂，需要大量的线缆和端口，管理成本高，路由选择、网络管理等技术也相对复杂。因此，网状拓扑网络主要用于关键任务和高可靠性需求的环境，如数据中心和广域网核心网络中。由于节点之间路径较多，因此局部故障不会影响整个网络的正常工作，具有较高的可靠性。

5）树状拓扑

树状拓扑（Tree Topology）网络是星状拓扑网络的扩展，当局域网的规模比较大，中心节点连接到多个子中心节点，每个子中心节点再连接到多个设备，即将原来用单独链路直接连接的节点通过多级处理主机进行分级连接，如图 5.5(e)所示。

当网络覆盖单位存在行政或业务隶属关系时，通常采用树状拓扑网络，便于进行层次化管理。在该网络中存在主干通信线路和分支通信线路，计算机和网络设备之间的连接存在分级关系。尽管其存在布线复杂（需要较多的布线工作）、中心节点依赖强，特别是根节点的故障会影响整个网络等缺点，但树状拓扑网络具有分层结构、扩展性强的优点，便于网络的管理和维护，对网络故障的定位较为容易，添加新的分支进行扩展方便。因此，树状拓扑网络适用于大型企业或校园网等需要进行层次化管理的网络环境。

2. 按覆盖范围分类

根据通信距离，即计算机网络的分布和覆盖的地理范围，可将计算机网络由近及远划分为局域网（LAN）、城域网（MAN）、广域网（WAN）等。

（1）局域网：局域网是一种在小区域内、局部的地理范围（如一个学校、工厂和单位内）使用的，由一个房间、一层楼或一座建筑物内的多台计算机、外部设备等组成的网络。其网络覆盖范围通常从几百米到几千米，属于一个单位或部门组建的小范围网。局域网的传输距离有限，但建设成本低、传输率高、可靠性高。此外，可通过数据通信线路或专用数据线

路，与其他局域网连接，构成一个大范围的网络。

（2）城域网：城域网是作用范围在广域网与局域网之间的网络，往往在一个城市内使用，其网络覆盖范围通常可延伸到整个城市，常使用与局域网相似的技术，采用通信光纤将同一城市不同地点的多个局域网联通形成大型城市网络，传输媒介主要是光缆，传输率通常在 100Mb/s 以上。能够在局域网内资源共享的基础上，进一步实现局域网之间的资源共享。

（3）广域网：广域网又称远程网，涉及长距离的通信，其覆盖范围最广，一般从几万米到几千万米，可以是一个国家或多个国家，甚至整个世界。由于广域网地理上的距离可以超过 100 万米，所以信息衰减非常严重，这种网络一般要租用专线，通过接口信息处理协议和线路连接，构成网状结构，以此解决寻径问题。由于其覆盖范围广，传输率相对较低，因此传输误码率相对较高。目前，世界上最大的广域网是因特网（Internet），它将世界各地的广域网、局域网等数万个网络互联，形成了一个最大的网络，实现全球范围内的数据通信和资源共享。

3. 按传输介质分类

按节点连接所使用的传输介质不同，可将网络划分为有线网和无线网。

（1）有线网是采用同轴电缆、双绞线、光纤或电话线作为传输介质进行连接的计算机网络。其中，双绞线和同轴电缆作为常见的联网方式，价格相对便宜，安装较为方便，但易受干扰，传输距离较短，灵活性较差，移动性受限。主要应用于办公室局域网或家庭宽带网络。光纤网采用光导纤维作为传输介质，其传输距离长，抗干扰性强，带宽大，传输率高，可达数千兆比特每秒，不会受到电子监听设备的监听，是高安全性网络的理想选择，多用于城市骨干网、长距离通信、高速互联网的接入等，但其安装成本较高、安装和维护需要专业技术。

（2）无线网主要以无线电波、红外线等电磁波作为载体来传输数据。与有线网相比，其联网方式灵活性高，部署方便，支持移动性；但受环境影响较大，安全性相对较低，传输速度不如有线网络稳定。常见有 Wi-Fi 网络、移动通信网络等。此外，无线网也包括利用通信卫星作为中继站传输数据的网络。由于通过卫星进行数据通信，其覆盖范围广，适用于偏远地区，如远程通信、航海通信、应急通信等；但网络延迟较高，受天气影响较大，且成本高。

4. 按使用性质分类

按照网络使用性质进行分类，计算机网络可以分为公用网（Public Network）和专用网（Private Network）。这两种网络在用途、管理、安全性和访问权限等方面存在显著差异。

（1）公用网，也称公共网络，是面向社会公众开放的网络系统，任何用户都可以通过适当的方式接入和使用公用网。通常由电信部门或其他提供通信服务的机构组建，属于经营性网络。公用网具有开放性、覆盖广、服务多样化、协议标准化、资源共享等特点。可以跨越地理边界，遵循公共的网络协议和标准，确保互操作性。网络资源被多个用户共享，提供如电子邮件、网页浏览等各种通用的网络服务。公用网最典型的例子是 Internet，它是全球最大的公用网。公用网也面临安全风险、隐私保护、网络拥塞、服务质量等一些挑战。由于其开放性，公用网更容易受到网络攻击和数据泄露的威胁，用户隐私保护成为重要议题。此外，可能出现网络拥堵，难以为所有用户提供一致的高质量服务，影响用户体验。

（2）专用网，也称内部网络，是为特定组织或用户群体设计和使用的封闭网络系统，通常不对外提供服务。常见的专用网包括企业内部网络、政府机构网络、电力系统网络、军事

通信网络等。专用网最主要的特征是封闭性，仅允许授权用户访问，对外部用户严格限制。采用更严格的安全措施，如防火墙、加密通信等技术，更好地保护敏感数据和重要信息，具有高安全性。其提供的服务和功能是根据用户的特定需求而专门设计和配置的，网络管理者可以根据需求更灵活地分配网络资源，调整网络配置，确保关键应用的性能。然而，专用网也存在建设和维护成本较高、扩展性不强、与外部网络互通性受限等一些局限性。

随着网络技术的发展，公用网和专用网的界限正在逐渐模糊，呈现融合趋势。许多组织采用混合网络策略，将公用网和专用网的优势结合起来。虚拟专用网络技术的应用，使专用网可以通过在公用网上构建安全的专用通道，实现安全连接。既保证了安全性，又利用了公用网的广泛覆盖。此外，越来越多企业也利用公有云构建自己的专用网环境，实现了灵活性和安全性的平衡。这种趋势反映了现代网络架构向着更加灵活、安全和高效的方向发展。

5.1.4 网络协议与体系结构

在计算机网络的相关概念中，网络协议与网络体系结构是两个最基本、最核心的概念，其抽象性较强，理解掌握其基本内容，有助于加深对计算机网络的认识。

1. 网络协议

计算机网络是一个非常复杂的系统，网络中的两个主机进行通信必须有一条传送数据的通道，但这远远不够，至少还有以下几项工作需要完成。例如，怎样识别要接收数据的计算机，如何保证要发送的数据不出错，当通信出现意外故障时采取何种措施恢复通信，以及不同操作系统、硬件架构的计算机之间由于信息表示格式不一致，如何实现二者之间的数据正确发送和接收等。网络协议能够使不同硬件、操作系统或应用软件之间进行有效的通信。

网络协议是网络实体之间交换信息时必须遵守的规则或约定的集合。在计算机网络中，网络协议是确保不同计算机之间能够顺利通信的基础。作为一组规则的集合，网络协议定义了网络中实体之间如何交换信息。这些规则不仅涵盖了数据传输的格式、顺序和速度，还规定了错误检测与纠正、流量控制等关键机制。网络协议的制定旨在实现不同系统间的互操作性，确保数据能够准确、高效地在网络中传输和交换。在计算机网络中，通信双方要做到有条不紊地交换数据，就必须遵守事先约定好的规则，协调一致地完成通信过程。

网络协议主要包含以下 3 个基本要素组成。

(1) 语法：定义用户数据和控制信息的结构或格式。例如，超文本传送协议(Hypertext Transfer Protocol，HTTP)规定了请求和响应消息的格式，包括起始行、头部字段和消息体等部分。

(2) 语义：解释数据或控制信息的具体含义，即需要发出何种控制信息，以及完成的动作与做出的响应。例如，HTTP 中，状态码 200 OK 表示请求已成功，而 404 Not Found 则表示请求的资源未找到。

(3) 时序：也称同步，是对事件实现顺序的详细说明。例如，传输控制协议(Transmission Control Protocol，TCP)通过三次握手建立连接，确保通信双方都已准备好进行数据传输，通过四次握手断开连接。

由于计算机网络通信是一个复杂的过程，从发送端计算机数据的处理，通信链路上数据的流转，到目的地计算机数据的正确接收。此外，还涉及网卡、集线器、网桥、交换机、路由器、网关等多种不同的设备。因此，计算机网络协议并不是单个协议，而是一套复杂的协议

集。尽管各个协议的具体功能有所不同，但核心目标在于实现网络中数据的可靠传输、错误检测与纠正、流量控制等。

网络协议通常采用分层设计，每层负责特定的功能。例如，当打开浏览器在地址栏输入学校网址访问学校官网时，背后起作用的应用层协议就包括域名服务（Domain Name Service，DNS）协议和 HTTP 等。其中 DNS 协议将所输入的便于记忆的域名转换为计算机能够理解的 IP 地址，使得不需要记住复杂的数字地址就能够顺利访问目标网站；而 HTTP 定义了客户端（浏览器）和服务器之间请求和响应的标准，确保能正确地获取网页内容。在这个过程还涉及传输层的 TCP、网络层的 IP 和链路层的相关协议。TCP 通过序列号、确认号和重传机制确保数据的可靠传输；互联网协议（internet Protocol，IP）则负责将数据包从源地址路由到目的地址，实现不同网络之间的互联。通过这些协议的协同工作，得以享受到便捷、高效的网络服务，无论是在线学习、资料检索、还是社交沟通，都离不开这些协议的支持。

计算机网络协议的分层设计，一方面，可以促进标准化发展，其通常由国际组织制定，确保全球范围内的一致性。分层后可精确定义每层所提供的服务及所需要的条件保障。相应的公司可根据自身优势，提供具备某一或某几个协议层次功能的产品，为计算机网络提供多样化软硬件产品的选择。另一方面，各层所提供的服务功能相对独立，某一层不需要知道它的下一层是如何实现的，仅需要知道该层所提供的服务及接口。因此，能够将一个难以处理的复杂问题分解为若干容易处理的小问题，降低系统设计的复杂度。同时，协议的分层设计还能够保障协议的可扩展性。只要在保证相邻层之间的接口不变、不影响现有功能的情况下，就可以使用最新的技术对某一协议层进行改进，也可为其添加新的功能特性，而且不影响其他层的工作，有助于技术的更新、迭代。

计算机网络体系结构是指用于组织和设计计算机网络的一种概念模型，是计算机网络所划分的层次结构模型与各层相应协议的集合。通过将复杂的网络通信过程分解为多个层次，每个层次负责特定的功能，实现了计算机网络通信的标准化和模块化。目前，主要有两种广泛使用的网络体系结构模型：OSI 参考模型和 TCP/IP 模型。

2. OSI 参考模型

开放系统互连（OSI）参考模型（简称 OSI）是国际标准化组织（ISO）在 1984 年提出的网络体系结构标准。其中，开放表示非独家垄断，只要遵循 OSI 标准，一个系统就可以和其他遵循这一标准的任一系统进行通信。在此之前，世界上第一个网络体系结构是由 IBM 公司于 1974 年提出的系统网络体系结构（SNA），后续其他组织机构也纷纷提出各自的网络体系结构。虽然这些网络体系结构都采用了分层的思想，但各自划分的层次及功能有差异，难以实现网络互联。

OSI 提供了一个网络分层结构及各层功能的统一标准，它将网络通信过程划分为 7 层，每层负责不同的功能。从低到高依次为物理层、数据链路层、网络层、传输层、会话层、表示层和应用层，如图 5.6 所示。分层设计不仅简化了复杂的通信过程，使各层协议更容易替换和扩展，还使不同厂商生产的计算机和网络设备可以互相通信。

物理层（Physical Layer）：作为 OSI 的最底层，负责物理介质上比特流的传输。计算机网络的传输介质种类繁多，通信方式也存在多种方式，物理层的主要作用就是尽可能屏蔽这些差异，使其上一层不必考虑具体的传输介质和通信方式。物理层主要定义数据在传输介

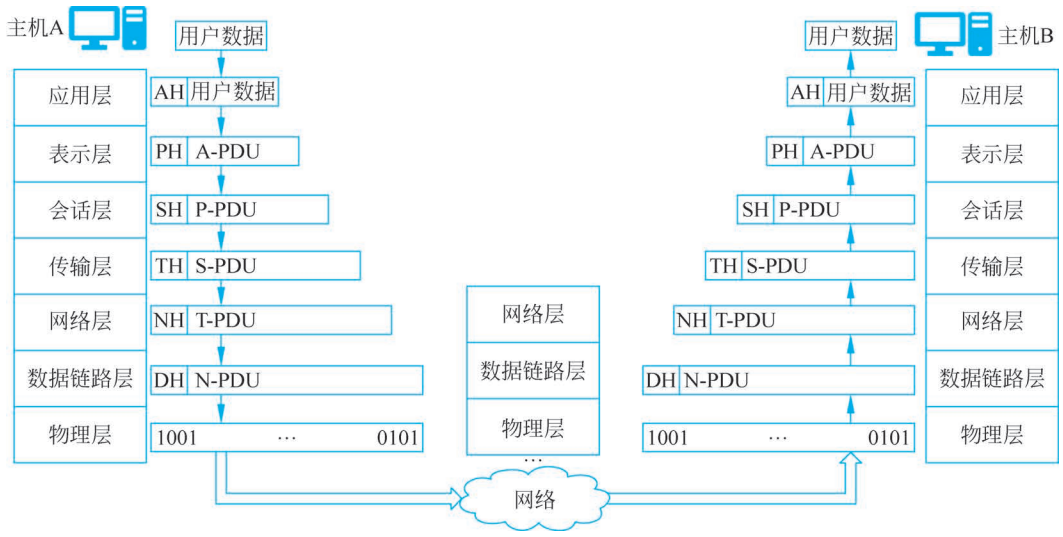


图 5.6　OSI 参考模型

质上的传输方式，以及电缆、光纤等传输媒介的机械特性、电气特性、功能特性、过程特性等，如在接口电缆的各条线上出现的电压的范围、某条线上出现的某一电平的意义、不同功能的各种可能时间的出现顺序等。物理层可以理解为一条高速公路，计算机网络通信的信道，负责数据的物理传输。

数据链路层(Data Link Layer)：链路就是从一个节点到相邻节点的一段物理线路，中间没有其他交换节点。通信时数据要经过这样的多条链路才能到达目的地，即若干条链路组成了发送方到接收方之间的路径。数据链路层工作在物理层之上，负责相邻节点之间传递数据帧。它将网络层传递来的数据包添加首部和尾部组成有序的数据帧，并从接收到的无差错帧中提取出数据包交给网络层。该层利用 MAC 地址识别不同的网络设备，通过错误检测和纠正、流量控制和数据帧同步等功能，确保数据帧能够准确无误地传输到目的设备。可以把它想象成高速公路上的车辆，负责将数据包(即货物)从一个节点(城市)运送到下一个节点。

网络层(Network Layer)：负责在网络中的不同节点之间传输数据包。该层定义了网络层地址(IP 地址)，以实现不同网络之间的互联。网络层的主要功能包括逻辑地址寻址、路由选择和流量控制，通过路由选择算法将数据包从源节点传输到目的节点。网络层提供的是尽最大努力交付的数据传输服务，不能保证数据的可靠传输。在网络层，传输的数据单位是数据包，路由器是核心设备，负责根据路由表转发数据包。网络层就像是高速公路上的导航系统，两台计算机之间通信中间可能经过多个节点和链路，也可能要经过多个通信子网络，而网络层主要负责完成通信路线的规划，即路由选择，确保数据包能够按照正确的路线到达目的地。

传输层(Transport Layer)：传输层的主要任务就是为上层应用提供可靠的端到端通信服务，包括数据分段、重组和流量控制等。一台计算机可以同时运行多个网络应用进程，如浏览器、微信、安全外壳(Secure Shell，SSH)等，不同的应用程序对应不同的端口，每个端口用一个称为端口号的正数表示，如 22 端口对应 SSH、80 端口对应 HTTP。传输层利用端口号区分不同的应用进程，实现复用和分用功能。当应用进程要发送数据时，就把数据发送到

其相应的端口，传输层从该端口接收数据并进行后续处理；当传输层收到数据后，就把数据送到相应的端口，应用进程从该端口读取数据。与数据链路层提供的节点之间比特率无差错传输不同，传输层负责发送端和接收端数据的无差错传输。即前者面向计算机之间的通信，后者侧重计算机进程之间的通信。传输层就像是快递服务，面向多种进程，提供通用的、端到端的通信服务，将应用层要发送的数据报文分割成较小的单元（如数据段），通过传输控制协议机制，确保数据能够完整无误地送达接收方。

会话层（Session Layer）：工作在传输层之上，在两个节点之间建立端连接，为应用程序之间的通信提供对话控制机制。会话层管理登录和注销过程，负责建立、管理和终止会话连接，确保两个用户或进程之间的对话顺利进行。它允许不同主机上的应用进程之间进行对话，并协调它们之间的通信过程。

表示层（Presentation Layer）：负责处理应用层的数据，提供数据格式交换、数据加密与解密、数据压缩与终端类型的转换等数据编解码服务，确保数据在发送方和接收方、不同系统间能够正确解释。表示层就像是翻译官，负责将不同语言（数据格式）之间的通信进行转换和解释。例如，JPEG 和 PNG 是表示层常用的图像编码协议，它们允许图像数据在不同系统间传输和显示。

应用层（Application Layer）：作为 OSI 的最顶层，应用层直接向用户提供各种网络服务和应用程序接口，是用户与网络之间的桥梁。常见的应用层协议有 HTTP、FTP、SMTP、POP3 等。HTTP 用于 Web 数据传输，FTP 用于文件传输，SMTP 和 POP3 则用于电子邮件的发送和接收。

OSI 为网络体系结构与协调发展提供了一种国际标准。它清晰地定义了网络通信过程中各层的功能和职责，有助于不同厂商开发的网络设备之间的互操作性。虽然 OSI 在理论上很完善，但由于其复杂性，在实际应用中，完全遵循 OSI 的网络系统并不多见。尽管如此，OSI 的思想对网络技术的发展仍然产生了深远影响。

3. TCP/IP 模型

TCP/IP（Transmission Control Protocol/internet Protocol）即传输控制协议/网际协议，最初由美国国防部高级研究计划局（DARPA）在 20 世纪 70 年代开发，旨在实现不同计算机网络之间的互联互通。作为互联网的基础协议，TCP/IP 并非单一协议，而是由多个协议共同组成的一个通信协议族。随着时间的推移，TCP/IP 逐渐成为全球互联网的标准通信协议，也被称为事实上的国际标准。TCP/IP 采用了一种简洁的分层结构，将网络协议划分为网络接口层、网络层、传输层和应用层 4 层（或者 5 层，将网络接口层细分为物理层和数据链路层）。

网络接口层：对应 OSI 的物理层与数据链路层，定义了数据传输的电气、机械、功能和过程标准，以及设备之间物理连接的特性。负责将 IP 数据包封装成适合在特定物理网络上传输的帧格式，并处理数据的实际传输。常见的物理层协议有 Ethernet、RS-232 等、数据链路层协议有 SDLC、HDLC、PPP 等。

网络层：对应 OSI 的网络层，负责在网络中的不同节点之间传输数据包。通过 IP 实现网络互联和路由选择，允许网间的报文根据目的地址通过路由器传递至另一个网络。常见的网络层协议有 ICMP、ARP、IP、IGMP 等。

传输层：对应 OSI 的传输层。传输层处理数据分段、重组和流量控制，负责为上层应用

提供端到端的通信服务。常见的传输层协议包括 TCP 和 UDP。其中，TCP 传送的数据单位称为 TCP 报文段，UDP 传送的数据单位称为 UDP 用户数据报。TCP 通过三次握手建立连接，并采用序列号、确认号和重传机制确保数据的可靠传输；UDP 则提供无连接的数据报服务，具有较低的延迟和较小的数据包头部开销。

应用层：对应 OSI 的应用层、表示层和会话层。应用层直接向用户提供各种网络服务和应用程序接口。常见的应用层协议有 HTTP、FTP、SMTP、POP3 等。这些协议共同构成了互联网丰富多彩的应用生态。

尽管 TCP/IP 和 OSI 在层次划分上有所不同，但它们都采用分层结构，每层都负责特定的功能，并通过层间接口与相邻层进行交互，尽管层级数量不同，但两种模型的功能层有对应关系，如表 5.1 所示。这种分层结构为网络通信提供了一个标准化的框架，使得不同层次可以独立开发和优化，提高了网络设计的灵活性和可扩展性，也使得不同厂商的网络设备和软件能够互相兼容和通信。

表 5.1　TCP/IP 与 OSI 关系对比

TCP/IP	OSI	主 要 功 能	常 见 协 议
应用层	应用层	面向用户，提供网络服务接口	HTTP、FTP、SMTP、POP3、SSH、DNS
	表示层	完成数据格式转换、压缩及加解密	
	会话层	负责进程间会话的建立、管理和维护	
传输层	传输层	确保可靠的端到端数据传输	TCP、UDP
网络层	网络层	完成数据通信的寻址及路由选择	ICMP、ARP、IP
网络接口层	数据链路层	相邻节点间无差错的数据帧收发	PPP、Ethernet CSMA/CD
	物理层	屏蔽底层细节建立通信的物理连接	

OSI 是一个纯粹的概念模型，由国际标准化组织制定，将网络通信划分为 7 层。TCP/IP 则是基于实际应用开发的，是应用较为广泛的网络协议集合，它将网络通信划分为 4 层。TCP/IP 以其简洁的分层结构、广泛的兼容性和强大的功能著称，可以在 OSI 的框架下工作，支持多种网络类型和拓扑结构，能够跨不同的操作系统和硬件平台实现互操作性，使得全球范围内的计算机能够相互通信和共享资源。总体而言，OSI 提供了一个全面的理论框架，而 TCP/IP 则是实际应用中广泛使用的标准。尽管有些差异，但二者都为理解和实现网络通信提供了重要指导。

计算机网络体系结构是计算机网络技术的重要组成部分，网络协议、OSI 和 TCP/IP 共同构成了网络通信的基石。通过深入理解这些概念和技术原理可以更好地设计和维护计算机网络系统，推动信息技术的发展和应用。

5.2　Internet 基础

因特网(Internet)作为人类历史发展中的一个标志性成就，无疑是科技革新与社会进步的重要标志。它通过其独特的优势，有效地打破了地理空间的限制，实现了全球范围内人群的高效连接。全球分布的服务器系统，承载着庞大的信息数据库，无论是深入的学术研究资料还是日常生活的小技巧，都能在短时间内为用户所获取。此外，Internet 还深刻改变了消费模式，电子商务平台的兴起使得商品和服务的选择更加多样化且易于获得。消费者可以

在家中舒适的环境中，通过简单的网络操作完成购物过程，所选商品随后将被快速配送至指定地点。这种购物方式不仅有效节约了时间与成本，同时也提供了更加个性化与便捷的服务体验。

5.2.1 Internet 的发展

1. Internet 的含义

Internet 是全球范围内由多个相互连接的计算机网络构成的庞大系统。基于 TCP/IP 的通信标准，Internet 实现了全球各地计算机网络的紧密互联，构建了一个广泛覆盖的信息交换网络体系。

该网络不仅提供了多样化的应用服务，而且由于其大规模的网络覆盖与广泛的应用领域，已成为支撑全球信息传播的关键基础设施。Internet 可以被形象地比喻为一个由无数条互联道路组成的复杂交通网络，这些“数字道路”连接了从个人计算机到高性能工作站乃至大型服务器等多种终端设备，同时也跨越地理界限，将政府网络、企业局域网、教育机构网络等不同类型和规模的网络紧密相连。在这个由 TCP/IP 构建的虚拟空间中，数据包作为信息载体，犹如高速公路上快速移动的车辆，在不同的网络节点间高效传输，最终到达目的地。这种高度互联的网络结构，构成了一个几乎无处不在的信息交流平台，支持着世界各地用户之间的即时沟通与资源共享。

值得注意的是，Internet 并非是任何一个特定机构或个人的专有资产，而是全人类共同创造并享有的科技成果。随着现代通信技术和信息技术的不断进步，Internet 已经成为一种高效、便捷且用途广泛的信息传播媒介，对促进全球经济一体化和社会信息化进程发挥了不可替代的作用。

Internet 采用了一种分层结构模型，由物理网、协议、应用软件和信息 4 层组成。每层都承担着特定的功能，共同协作以实现高效的信息传输。

1）物理网

物理网是 Internet 实现通信的基础，它类似于现实生活中的交通网络，如一个巨大的蜘蛛网般覆盖全球，并不断延伸和加密。物理网由各种硬件设备组成，包括计算机、服务器、路由器、交换机、电缆、光纤等。这些设备相互连接，形成了一个庞大的网络，使得数据能够在不同地点的设备之间传输。

2）协议

在 Internet 上传输的信息至少遵循 3 个主要协议：网际协议、传输协议和应用程序协议。

网际协议（IP）负责将信息发送到指定的接收机。它为每个设备分配一个唯一的 IP 地址，通过这个地址来确定数据的传输目的地。

传输协议（TCP）负责管理被传送信息的完整性。它确保数据在传输过程中不会丢失或损坏，并且能够按照正确的顺序到达接收端。

传统的 Internet Web 应用还是以面向连接 TCP 为主，更加关注数据的完整性和可靠性。而对更加关注实时性、能容忍少量数据丢包的应用，则会采用面向连接的 UDP。

应用程序协议众多，如 SMTP、Telnet、FTP 和 HTTP 等。每个应用程序都有自己的协议，这些协议负责将网络传输的信息转换成用户能够识别的信息，使得用户能够在应用程序

中进行各种操作，如发送电子邮件、远程登录、文件传输、浏览网页等。

3）应用软件

在实际应用中，用户通过一个个具体的应用软件与 Internet 进行交互。每个应用程序的使用代表着获取 Internet 提供的某种网络服务。例如，通过万维网（World Wide Web，WWW）浏览器可以访问 Internet 上的 Web 服务器，享受图文并茂的网页信息；使用电子邮件客户端可以发送和接收电子邮件；使用文件传输软件可以从远程服务器下载文件或上传文件到服务器等。

4）信息

信息是 Internet 的核心价值所在，涉及实际的信息内容及其表示方式。在网络世界中，信息就像货物在交通网络中一样，建设物理网（修建公路）、制定协议（交通规则）和使用各种各样的应用软件（交通工具）的目的都是传输信息（运送货物）。Internet 上的信息种类繁多，包括文本、图像、音频、视频、数据等，这些信息存储在各种服务器和数据库中，用户可以通过网络访问和获取这些信息，以满足自己的需求。

这种分层设计不仅简化了 Internet 的复杂性，提高了系统的灵活性和可扩展性，还促进了不同技术组件之间的兼容性和互操作性，是 Internet 能够持续发展和广泛应用的重要基础。

2. Internet 的发展

1）Internet 的起源与早期发展

1969 年，ARPANET 首次成功连接了四所美国大学的主机，该网络采用了先进的分组交换技术，即将数据分解为小块（即数据包），通过多个路径独立传输至目的地，然后再重新组装。这种技术显著提高了网络的可靠性和灵活性，为后续的网络发展奠定了基础。

随着技术的不断进步，ARPANET 逐渐扩大，吸引了更多的大学和科研机构加入。1974 年，TCP/IP 的推出成为 Internet 发展历程中的关键转折点。TCP/IP 定义了一套全面的网络通信规范，确保了不同网络之间的互联互通。其开放性和标准化的特性，使得 Internet 的应用范围迅速从军事和科研领域扩展到更广泛的社会公众。

进入 20 世纪 80 年代，美国国家科学基金会（National Science Foundation，NSF）推出了 NSFNET 项目，进一步推动了互联网的发展。NSFNET 利用 TCP/IP，连接了全美各地的超级计算机中心，形成了当时 Internet 的主干网络。这一举措极大地促进了 Internet 的普及与开放，使得大学、研究机构乃至普通民众都能够方便地接入，享受其带来的便利。

2）Internet 的商业化与普及

20 世纪 90 年代，Internet 开始向商业化方向转变。其中，WWW 的出现和普及是这一过程中的重要里程碑。WWW 通过 HTTP 将文本、图片、音频、视频等多种媒体形式有机结合，极大地丰富了网络内容的表现形式，促进了信息的广泛传播。随着个人计算机的普及和 Internet 接入成本的降低，越来越多的家庭用户能够方便地接入 Internet，享受电子邮件、即时通信、在线游戏等多样化应用带来的便利。同时，许多企业也开始利用互联网开展电子商务、在线广告、远程办公等业务，推动了互联网经济的快速发展。

3）技术创新与未来发展趋势

近年来，网络技术持续创新，云计算（Cloud Computing）、大数据（Big Data）、物联网（Internet of Things，IoT）、人工智能（Artificial Intelligence，AI）等新兴技术的兴起，为

Internet 的发展注入了新的活力。云计算技术允许用户通过 Internet 按需访问强大的计算资源和存储服务，降低了企业和个人使用高端 IT 设施的成本门槛。大数据分析技术帮助企业和组织从海量数据中挖掘有价值的信息，辅助决策制定。物联网通过将物理设备连接至 Internet，实现了设备间的智能交互与自动化管理。人工智能技术的应用，则为用户提供更加个性化和智能化的服务体验，如智能搜索、语音助手、图像识别等。

3. Internet 在中国的发展

1）Internet 在中国的起步阶段（20 世纪 90 年代）

中国 Internet 的发展历程体现了从无到有、从小到大的转变。自 1986 年起，中国开始探索 Internet 技术的研究与应用。初期，Internet 主要服务于科研和教育目的，仅限于少数科研机构和高等教育机构中的电子邮件服务。1994 年，中国实现了与国际 Internet 的全功能连接，标志着中国正式加入全球 Internet 大家庭。随后，中国陆续启动了多个 Internet 项目，包括公用计算机互联网、中国教育和科研计算机网等，Internet 开始渗透到普通民众的生活中，并在全国范围内快速扩展，开启了中国 Internet 发展的新篇章。

以下是我国四大主干网络的基本情况。

（1）公用计算机互联网（ChinaNet）。

ChinaNet 是由中国电信运营的基于 Internet 技术的公用计算机网络，作为中国主要的网络之一，通过高速数据专线在国内各节点之间建立了连接，并配备了国际专线，构成了中国 Internet 的关键基础设施。ChinaNet 提供多样化的 Internet 接入服务，如宽带和拨号接入，覆盖全国各区域，为政府、企业和个人用户提供高效稳定的网络连接。此外，ChinaNet 支持多种 Internet 应用，包括但不限于网页浏览、电子邮件、文件传输和远程登录，同时也为电子商务、在线教育和远程医疗等新兴领域提供了技术平台。随着技术的不断演进，ChinaNet 持续优化升级，致力于满足用户对更高速度和更高质量网络服务的需求。

（2）中国教育和科研计算机网（CERNet）。

CERNet 是一个由国家资助、教育部管理、多所高等学府共同参与建设和运维的全国性学术网络。该网络旨在建立一个覆盖全国主要高等教育机构和科研单位的高速网络，以提供先进的信息技术支持。经过多年的建设与发展，CERNet 已经成为中国教育信息化不可或缺的组成部分，对于人才培养、科学研究及学术交流产生了深远的影响。CERNet 的网络架构分为主干网、区域网和校园网 3 个层级，分别负责全国范围的数据传输、地区间的资源共享以及校内用户的网络接入。CERNet 不仅提供了稳定的网络连接，还支持多种应用服务，促进了教育资源的共享与科研合作，对于培养创新型人才、推动科技进步具有重要意义。

（3）中国科技网（CSTNet）。

CSTNet 旨在为中国科技界打造一个高效、稳定且安全的信息交流平台，以促进科技信息的共享与传播，加速科技创新的步伐。该网络由中国科学院主管，具体建设和运营管理由中国科学院计算机网络信息中心负责。CSTNet 的网络架构分为核心层、汇聚层和接入层，各层之间协同工作，确保了高效的数据传输和路由转发。CSTNet 凭借先进的网络技术和设备，实现了与国内外其他网络的互联互通，为全球范围内的信息交换和资源共享提供了可能。

（4）国家公用经济信息通信网（金桥信息网：ChinaGBN）。

建立在金桥工程之上的金桥网，是支持多项“金”字头工程项目（如金关、金税、金卡等）

的信息通信平台，同时也是中国经济社会信息化的重要基础设施之一。金桥网依托卫星通信和地面光纤传输网络相结合的方式，构建了一个天地一体化的网络体系，旨在为国家宏观经济管理和决策提供信息支持，同时也面向企业和公众提供经济信息服务。金桥网以其高速、高可靠性及安全性著称，对于推动经济发展、加速信息化进程及保障国家信息安全等方面发挥了关键作用。

2）Internet 在中国的初步普及阶段（2000—2010 年）

进入 21 世纪后，随着宽带网络的普及、技术成本的降低及 Internet 应用的日益丰富，中国网民数量呈现爆发式增长，从 2000 年的数百万网民到 2010 年突破数亿网民，Internet 开始从少数专业人士和科研人员的工具逐渐普及到普通大众。这一转型不仅标志着信息技术在中国社会中的渗透程度加深，也反映了信息化对社会经济结构产生的深远影响。

在此期间，新浪、搜狐、网易等门户网站迅速崛起，成为中国 Internet 发展的重要标志。这些平台通过整合新闻资讯、电子邮件、搜索引擎、论坛等多种服务，成为用户获取信息和参与网络社交的关键入口。门户网站的成功运营不仅促进了信息传播效率的提升，也为早期 Internet 商业模式的探索提供了宝贵经验。

2003 年，淘宝网的成立标志着中国电子商务进入了快速发展阶段。随后，京东、当当等电商平台相继涌现，共同推动了中国电商市场的繁荣。电子商务的兴起不仅改变了传统的商业销售模式，为消费者提供了更加便捷、多样化的购物选择，同时也为中小企业开辟了新的市场机遇。尽管初期电子商务的交易规模相对有限，但其展现出的巨大发展潜力不容忽视。伴随电子商务的成长，物流配送、在线支付等相关配套产业也开始逐步成熟，形成了一个完整的电商生态系统。

此外，以 QQ 为代表的即时通信软件在这一时期得到了广泛应用，成为中国网民进行网络社交的核心工具之一。即时通信软件不仅改变了人们的沟通方式，还促进了网络社区的形成与发展，进一步推动了电子商务、网络营销等行业的发展。

3）Internet 在中国的高速发展阶段（2010 年至今）

自党的十八大以来，中国 Internet 发展进入了全新的阶段，国家大力推进网络强国战略和数字中国建设。在技术创新领域，中国在 5G 通信、人工智能、大数据分析和物联网等前沿科技上取得了显著进展，为 Internet 的进一步发展提供了强有力的技术支撑。

在应用层面，中国互联网企业不断创新，推出了众多新产品和服务。例如，移动支付的广泛应用极大地简化了支付流程，促进了无现金社会的形成；共享单车模式有效缓解了城市交通的最后一公里问题，促进了绿色出行方式的发展；在线直播平台的兴起，极大地丰富了人们的休闲娱乐生活。这些创新不仅在国内受到了热烈欢迎，而且在国际上也产生了重要影响，引领了全球 Internet 应用的新趋势。

与此同时，Internet 与传统行业的深度融合，为数字经济的发展注入了强大动力。通过实施“互联网＋”战略，将信息技术与制造业、农业、服务业等多个领域紧密结合，推动了产业的转型升级。在制造业，工业互联网的应用提高了生产的智能化水平，增强了企业的市场竞争力；在农业领域，物联网技术的应用使农业生产更加精准高效；在服务业，互联网与旅游、金融、物流等行业的结合，为消费者提供了更加便捷的服务体验。这一系列变革，不仅促进了中国经济结构的优化调整，也加速了中国经济向高质量发展的转型。

4. Internet 的应用

Internet 作为一种全球性的信息网络，其应用范围广泛且深入，几乎渗透到了社会生活的每个角落。它不仅改变了个人的生活方式，也在商业、教育和公共服务等多个领域中扮演着至关重要的角色。

（1）个人使用。支持网页浏览、电子邮件收发、即时通信、视频流媒体播放、在线游戏等多种娱乐和社交活动。

（2）商业应用。助力企业实现办公自动化、电子商务交易、远程协作会议、高效的数据交换等功能，有助于提升工作效率和市场竞争力。

（3）教育领域。为在线学习和远程教育提供平台，帮助学生获得丰富的教育资源，消除地理障碍。

（4）公共服务。在医疗健康方面，可实现远程诊疗和医疗信息的共享，改善了医疗服务的可达性和质量；在智慧城市构建中，连接智能家居系统、智能交通管理和工业物联网等，促进了城市管理的智能化。

5.2.2 Internet 的接入技术

Internet 的接入技术是指用于连接终端用户（包括个人用户和商业实体）与因特网服务提供方（the Internet Service Provider，ISP，如电信运营商或有线电视公司）的数据通信系统。这项技术是实现全球范围内信息共享与通信交流的核心，它不仅使人们能够不受时间和地点的限制，获取和分享信息，而且还促进了经济、文化、教育等多领域的繁荣与发展。此外，Internet 接入技术还是现代社会发展数字化转型的基石，为诸如云计算、大数据、物联网等新兴技术的应用提供了必要的基础设施支持。Internet 接入技术的实现通常涉及以下 5 个关键步骤。

（1）物理连接。首先，需通过有线（如光纤、同轴电缆）或无线（如 Wi-Fi、蜂窝网络）方式将用户终端与接入点（如路由器、交换机、基站等）相连。

（2）信号传输。在此基础上，采用特定的通信协议（最常见的是 TCP/IP）将用户产生的数据包转换为可在传输媒介上传输的信号形式，这些媒介包括但不限于电缆、光纤和无线电波。

（3）网络寻址。为了确保数据包能准确无误地送达目标位置，接入技术必须为每个用户终端分配一个唯一的 IP 地址，并运用路由选择算法来决定最佳的数据传输路径。

（4）连接建立。用户终端与 Internet 上的目标服务器之间建立连接，这是进行后续数据交换的前提条件。

（5）数据传输。一旦连接成功建立，用户终端便可通过此通道发送或接收数据，从而实现各种 Internet 应用功能。

根据传输媒介的不同，Internet 接入技术主要可以划分为两大类别：有线接入技术和无线接入技术。

有线接入技术包括拨号接入（Dialup Access）、数字用户线（Digital Subscriber Line，DSL）接入、光纤接入（Fiber Access）、以太网接入（Ethernet Access）等，这类技术通常提供更高的带宽和更稳定的连接质量。

无线接入技术涵盖 Wi-Fi、蜂窝数据网络、蓝牙、卫星通信等，其特点是部署灵活、覆盖

范围广，尤其适用于移动设备和偏远地区的 Internet 接入需求。

1. 有线接入技术

有线接入技术是指通过物理线缆将用户设备与网络连接，实现数据传输的技术手段。这些物理线缆包括电话线、同轴电缆、双绞线和光纤等，每种线缆都有其独特的特性和适用场景，为用户提供了多样化的接入选择。以下是 4 种常见的有线接入技术。

1）拨号接入

拨号接入是一种利用公用电话交换网（Public Switched Telephone Network，PSTN）提供 Internet 服务的接入方式，也是最早的 Internet 接入方式之一。用户通过电话线和调制解调器（Modem）连接到 Internet 服务提供方（ISP）的远程接入服务器（Remote Access Server，RAS）。在发送端，调制解调器将计算机中的数字信号转换成能够在电话线上传输的模拟信号；在接收端，再将接收到的模拟信号转换回数字信号。这种方式使得用户能够通过电话线实现与 ISP 的连接，进而接入 Internet。

拨号接入的优点在于安装简单、成本低廉，但其下行速率较低（通常不超过 56Kb/s），且可靠性不高。随着宽带技术的发展，拨号接入已逐渐被其他方式取代，但在一些偏远地区或临时应急情况下仍可能被使用。对于网络速度要求不高的用户，或者在没有其他接入方式可选时，拨号接入可以作为备用方案。

2）数字用户线接入

数字用户线接入是一种基于普通电话线的宽带接入技术。它利用电话线路中未使用的高频频段，通过不同的调制方式实现数据传输和语音通信并行，互不干扰。常见的 DSL 技术包括非对称数字用户线（Asymmetric Digital Subscriber Line，ADSL）和超高速数字用户线（Very high-bit-rate Digital Subscriber Line，VDSL）等。

ADSL 是目前应用最广泛的 DSL 技术之一。其下行速率（从 ISP 到用户）一般为 1～8Mb/s，上行速率（从用户到 ISP）为 512Kb/s～1Mb/s，具体速率取决于用户与 ISP 机房的距离以及线路质量等因素。ADSL 采用先进的频分复用技术，将数据信号和电话音频信号分别调制在不同的频段上，使得用户在上网的同时可以进行电话通话，二者互不干扰。ADSL 技术具备高速传输能力，能够满足用户浏览网页、观看视频、下载文件等需求，同时提供独享带宽，确保网络使用的稳定性和流畅性。此外，ADSL 具有较高的安全可靠性，适用于小型商户的日常经营需求，如便利店、咖啡店等。

VDSL 是一种速度更快的 DSL 技术，下行速率最高可达 52Mb/s，上行速率最高可达 16Mb/s。相比 ADSL，VDSL 的传输率显著提升，能够满足用户对高清视频流、在线游戏、大型文件下载等高带宽应用的需求。VDSL 主要用于短距离的高速接入，一般在 1km 以内传输效果较好，适合在小区内或办公楼等相对较小的区域范围内提供高速宽带服务。例如，在一个多层办公楼内，运营商可以通过 VDSL 技术为每个办公室提供高速 Internet 接入，满足企业员工日常办公对网络的需求。

3）光纤接入

光纤接入是指终端用户通过光纤连接到局端设备，实现高速、大容量的数据传输。光纤接入技术以其传输容量大、传输质量好、损耗小、中继距离长等优点，在宽带网络中占据重要地位。根据光纤深入用户的程度不同，光纤接入可以分为多种类型。

（1）光纤到大楼（Fiber To The Building，FTTB）：光纤接入建筑物的某层或某个区域，

再通过其他方式(如双绞线)接入最终用户。

(2) 光纤到驻地/光纤到户(Fiber To The Premises/Fiber To The Home,FTTP/FTTH):将光缆直接接入家庭或企业用户,提供最高质量的光纤接入服务。

(3) 光纤到办公室(Fiber To The Office,FTTO):将光纤接入办公区域,满足企业用户对高速网络的需求。

(4) 光纤到路边(Fiber To The Curb,FTTC):光纤接入路边的光交接箱,再通过其他方式(如双绞线)接入用户家中。

光纤接入技术适用于对网络速度和稳定性要求较高的企业、学校、科研机构等。例如,现在很多新建小区都采用光纤接入的方式,让居民能够享受到快速的网络体验,无论是观看4K 甚至 8K 高清视频,还是进行多人视频通话,都能流畅进行。

4) 以太网接入

以太网接入是指将以太网技术与综合布线相结合,作为公共电信网的接入网,直接向用户提供基于 IP 的多种业务传送信道。它借用了传统以太网技术的帧结构和接口,采用异步工作方式,适于处理 IP 突发数据流。

以太网接入技术主要通过以下两种形式实现。

(1) 纯以太网接入。用户自己有一个 IP 地址,设置掩码和网关,通过网关所在的子网连接到 Internet 中。

(2) 以太网 VLAN 分段业务。VLAN 可以动态地把一些不同的节点绑定到一个网络中,增强网络管理的灵活性和安全性。

以太网接入技术作为一种成熟且广泛应用的宽带接入技术,具有诸多优点和应用前景。随着工业 4.0 的推进,智能工厂越来越依赖网络连接来实现自动化生产、设备监控和数据采集。以太网接入可以将工厂内的各种设备,如机器人、传感器、控制器等连接到网络中,实现设备之间的实时通信和协同工作。例如,在汽车制造工厂中,以太网接入可以实现生产线的自动化控制,提高生产效率和产品质量。

2. 无线接入技术

无线接入技术是指通过无线信号将用户设备连接到 Internet 或其他网络的技术手段。它利用无线电波作为传输媒介,无须铺设物理线缆,使得用户能够在一定范围内灵活地接入网络。无线接入技术涵盖了多种不同的标准和协议,适用于不同的场景和应用需求。以下是 4 种常见的无线接入技术。

1) Wi-Fi

Wi-Fi(Wireless Fidelity)是一种基于 IEEE 802.11 系列标准的高频无线局域网技术。它通过无线接入点(Wireless Access Point,WAP)将有线网络信号转换为无线信号,供支持 Wi-Fi 的设备连接上网。Wi-Fi 允许电子设备在没有物理连接的情况下进行高速数据传输,通常在开放性的许可频段内运行,如 2.4GHz 和 5GHz。

Wi-Fi 设备在一定范围内搜索可用的 WAP,并与信号最强的 WAP 建立连接。连接建立后,设备可以通过 WAP 访问 Internet。Wi-Fi 覆盖范围内自由移动,无须担心线缆的束缚,并且可以提供较高的数据传输速度,满足用户浏览网页、观看视频、下载文件等需求。家庭中各种智能设备(如手机、平板计算机、智能电视、智能音箱等)都可以通过 Wi-Fi 接入 Internet,实现智能家居的控制和多媒体内容的共享。例如,用户可以通过手机上的 App 远

程控制家里的灯光、空调、窗帘等设备，同时还可以在智能电视上观看在线视频、玩游戏等。

2）蜂窝数据网络

蜂窝数据网络是一种移动通信网络技术，将服务区域划分为若干相邻的小区，形状类似蜂窝，因此得名。每个小区都由一个基站提供服务，基站负责与小区内的移动设备进行通信。

蜂窝数据网络的主要特点是可以实现频率复用，即在不同的小区中使用相同的频率进行通信，从而提高了频谱利用率。这是因为小区之间的距离足够远，使得同一频率的信号在相邻小区之间不会产生明显的干扰。在蜂窝数据网络中，移动设备通过与基站进行无线通信来接入网络。当移动设备在小区之间移动时，它会自动切换到信号更强的基站，以保持连续通信。这种切换过程通常是无缝的，用户几乎感觉不到。

蜂窝数据网络的发展经历了多个阶段，从最初的模拟通信到现在的数字通信，技术不断升级。目前，广泛使用的蜂窝数据网络技术包括 2G、3G、4G 和 5G 等。

2G 网络主要提供语音通信和低速数据传输服务，如短信和彩信；3G 网络在 2G 网络的基础上增加了对高速数据传输的支持，使得用户可以浏览网页、使用电子邮件和下载一些小型文件；4G 网络进一步提高了数据传输速度，能够支持高清视频流媒体、在线游戏等对带宽要求较高的应用；5G 网络具有更高的速度、更低的延迟和更大的连接容量，为物联网、智能驾驶、虚拟现实等新兴技术的发展提供了有力支持。

3）蓝牙

蓝牙是一种短距离无线通信技术，允许设备在短距离范围内进行数据传输和连接到 Internet。大多数现代设备都支持蓝牙功能，使得蓝牙接入具有广泛的兼容性。蓝牙通常适用于在 10m 左右的范围内进行设备间的通信，并且蓝牙设备的功耗相对较低，适用于电池供电的移动设备。

在 Internet 接入方面，蓝牙可以通过与其他设备（如手机、平板计算机、笔记本计算机等）建立连接，然后利用这些设备的网络连接（如 Wi-Fi 或蜂窝数据网络）来实现间接接入 Internet。例如，蓝牙音箱可以通过与手机配对，使用手机的网络来播放来自 Internet 的音乐。此外，蓝牙还可以用于构建个人局域网，在这个局域网内，设备可以相互通信和共享数据。虽然蓝牙本身的传输速度和距离有限，但它在某些特定场景下，如智能家居、可穿戴设备等领域，发挥着重要的作用。

4）卫星通信

卫星通信主要依赖于卫星的宽带 IP 多媒体广播技术，该技术能够解决 Internet 带宽的瓶颈问题，尤其是在地理条件复杂或传统通信设施难以覆盖的地区。卫星通信具有覆盖面广、传输距离远、不受地理条件限制等优点，在自然灾害、突发事件等情况下，地面通信网络可能会遭到破坏，卫星通信可以作为应急通信手段，为救援人员、受灾群众提供 Internet 接入服务，方便救援指挥和信息传递。例如，在地震、洪水等灾害发生后，卫星通信可以快速建立通信链路，保障救援工作顺利进行。

卫星通信常采用非对称的传输方式，即上行速率较低，主要用于发送用户请求；下行速率较高，主要用于传输大量的数据信息。支持标准的 TCP/IP，以及 WWW、E-mail、NewsGroup、Telnet 等多种互联网应用协议，能够满足用户多样化的网络需求。卫星系统具有天然的广播优势，能够以非常低廉的价格实现广大区域内大数据量的分发。卫星通信接入 Internet 的所有传输数据都实现了数据加密标准（Data Encryption Standard，DES），确

保了数据传输的安全性。它不仅能够解决传统通信方式难以覆盖地区的 Internet 接入问题，还能够为用户提供高速、稳定、安全的网络体验。

5.2.3 IP 地址及域名系统

1. IP 地址的概念

在现实世界的通信中，精确的地址对于信件和包裹的成功投递至关重要。同样，在数字网络中，为了确保数据包能够准确无误地到达目的地，每台计算机、路由器以及其他联网设备都必须拥有一个独一无二的标识符，即 IP 地址(Internet Protocol Address)。IP 地址是一种逻辑地址，它在网络层面上标识了 Internet 上的每个节点，从而支持数据包在源地址与目的地址之间的有效传输。IP 地址分为 IPv4 和 IPv6 两种类型。

1) IPv4 地址

现有的网络是在 IPv4 的基础上运行的。IPv4 地址(以下简称 IP 地址)是基于 32 位二进制数的标准地址格式，它为网络中的每台设备提供了唯一的身份识别。无论是在局域网还是广域网环境中，任何希望接入 Internet 的设备都必须拥有一个独特的 IP 地址，以便于与其他网络节点进行通信。IP 地址通常采用点分十进制形式表示，即 4 个 0～255 的十进制数字，以“.”分隔。例如，二进制数

01110000.01010111.01000001.00111100

将其转换成十进制数，对应的 IP 地址为 112.87.65.60。

IP 地址结构上被划分为网络部分和主机部分，这一设计旨在实现对网络架构的有效管理。网络部分定义了设备所属的具体网络，而主机部分则标识了该网络内部的特定设备。根据这一原理，IP 地址可以被抽象地表达为一个二元组：＜网络号，主机号＞。这样的设计允许数据包根据其目的地的网络部分和主机部分被准确地路由至正确的接收方。

为了适应不同的网络规模需求，IP 地址被进一步细分为 5 类：A、B、C、D 和 E。A 类地址适用于大型网络，B 类地址适合中等规模的网络，C 类地址主要用于小型网络，D 类地址专门用于多播通信，E 类地址预留以备未来之需。每类地址都有其特定的前缀模式，这些模式不仅有助于确定地址的类别，还影响着可分配给网络和主机的数量。例如，A 类地址的第一个 8 位组以 0 开头，这意味着 A 类地址的网络部分占用了第一个 8 位组，而主机部分则占据了剩余的 24 位，如图 5.7 所示。

图 5.7 IP 地址编码示意图

值得注意的是，某些特殊的 IPv4 地址段具有特定用途。例如，全 0 的主机部分通常用来表示整个网络本身，而全 1 的主机部分则用于本地网络广播。此外，还有一些地址段被预留为私有地址空间，这些地址可以在私有网络中自由使用而不必担心与公网地址冲突。

A类地址的前8位用于标识网络号，其余24位用于标识主机号，最高位固定为0。所以，A类地址所能表示的网络数范围为0～127，但需要注意的是，数字0和127并不作为主机的IP地址。其中，数值0被视为预留地址，用于指代本地网络，而非特定主机；而数值127则被专门预留用于环回测试，例如，127.0.0.1通常作为本机循环接口的标准地址。因此，A类地址实际上可用的网络只有126个，范围为1.0.0.0～126.255.255.255。A类IP地址通常用于大型网络。

B类地址的前16位用于标识网络号，其余16位用于标识主机号，最高两位固定为10。B类地址范围为128.0.0.0～191.255.255.255。B类地址结构适用于中等规模的网络配置，如区域性的网络管理机构或企业内部网络。

C类地址的网络标识占据前24位，主机标识仅占最后8位，且最高3位固定为110。这导致C类地址的适用范围为192.0.0.0～223.255.255.255。由于其主机数量限制较小，C类地址尤其适合小型网络部署，如教育机构的内部网络。

综上所述，通过分析IP地址的第一组十进制数值，即可准确判断出地址所属的类别，这一过程在实际网络规划与管理中具有重要意义。表5.2提供了详细的分类指南，便于快速识别不同类型的IP地址。

表5.2 A、B、C类地址

类　　型	第一段数字范围	包含主机台数
A	1～126	16 777 214
B	128～191	65 534
C	192～223	254

IP地址池总计包含2^{32}个地址，即大约42.9亿个唯一标识符。然而，随着Internet技术的快速发展与全球连网设备数量的显著增长，IPv4地址资源日益稀缺，成为制约Internet扩展的关键因素之一。在Internet初期，IP地址的分配工作主要由因特网编号分配机构(Internet Assigned Numbers Authority，IANA)统一协调并实施。具体流程：IANA首先将大范围的地址块分配给五大区域因特网注册管理机构(Regional Internet Registries，RIRs)，包括但不限于亚太网络信息中心(Asia-Pacific Network Information Centre，APNIC)、欧洲IP网络协调中心(RIPE Network Coordination Centre，RIPE NCC)等。随后，这些RIRs依据各自区域内的需求，继续向下一级分配，直至ISP层面。ISP再根据终端用户的特定需求，如企业或个人，分配相应的IP地址，确保其能够顺利接入Internet并实现数据交换。

然而，在地址分配过程中，存在着一定的非最优分配及历史遗留问题，这些问题直接导致IP地址资源的浪费。例如，某些组织可能基于未来扩张的预期或是出于安全考虑，预先申请了远超实际所需数量的IP地址，而实际上并未充分利用这些资源。这种现象不仅限制了新入网设备获取独立IP地址的可能性，也加速了IP地址池的枯竭速度，进而促使业界积极探索新的解决方案，如IPv6协议的推广与应用，以应对即将到来的地址短缺挑战。

2) IPv6地址

IPv6，即Internet Protocol version 6，是为应对IPv4地址耗尽问题而设计的下一代Internet协议。IPv6采用了128位地址长度，理论上能够提供约3.4×10^{38}个唯一地址，极大地扩展了网络地址空间，满足了日益增长的互连设备数量的需求。IPv6地址格式为冒号

分隔的十六进制数，共包含 8 组 16 位数字，如示例地址 2001:0db8:85a3:0000:0000:8a2e:0370:7334。

IPv6 相对于 IPv4 具有多方面的优势，这些优势主要体现在以下 6 方面。

(1) 扩展的地址空间：通过 128 位地址长度的设计，IPv6 解决了 IPv4 地址资源有限的问题，能够为更多的设备分配唯一的网络地址，适应了 Internet 的快速发展。

(2) 提高的网络性能和效率：IPv6 支持大于 64KB 的数据包大小，优化了数据传输效率。此外，通过简化报文头部结构和改进的分段机制，IPv6 提高了数据包的处理速度和转发效率，从而增强了网络的整体性能。

(3) 强化的安全特性：IPv6 包括内置的 IPsec(Internet Protocol Security)支持，这提供了更强的网络安全性。IPsec 可以用于数据加密和身份验证，以保护通信的机密性和完整性。

(4) 优化的移动性和即插即用能力：IPv6 包括内置的支持移动设备的功能，使得移动设备可以更容易地切换网络，而无须更改 IP 地址，从而提高了设备的可用性。IPv6 引入了 SLAAC(Stateless Address Autoconfiguration)机制，允许设备自动获取 IPv6 地址，减少了网络管理员的配置工作，实现了即插即用。

(5) 改良的多播功能：相较于 IPv4，IPv6 的多播功能更加灵活，支持定义多播范围和区分永久性与临时性地址，有利于多播服务的有效实施。

(6) 增强的服务质量(Quality of Service，QoS)支持：IPv6 提供了更精细的流量控制选项，有助于网络管理员优化数据包的传输优先级，保障关键应用的服务质量。

尽管 IPv6 技术已经成熟并存在多年，其在全球范围内的广泛应用仍面临挑战。然而，随着 IPv4 地址资源的逐渐枯竭，向 IPv6 过渡成为必然趋势。目前，许多国家和地区正积极推广 IPv6 的部署，以促进 Internet 的可持续发展。

2. 子网掩码

在计算机网络架构中，子网掩码(Subnet Mask)是一个不可或缺的概念，它与 IP 地址紧密关联，共同承担着网络划分和管理的核心职责。子网掩码可被视为网络世界的“标尺”，通过其精准划分不同规模的网络区域，实现网络资源的合理配置和高效利用。具体来说，子网掩码是一个 32 位的二进制数，与 IP 地址具有相同的位数，主要用于区分 IP 地址中的网络部分和主机部分。为了便于人们的理解和配置，子网掩码通常采用点分十进制表示法。

在标准的 IP 地址分配体系中，子网掩码的主要功能之一是作为判断两台计算机是否处于同一子网络的关键依据。其实现方式是通过将两台计算机的 IP 地址与子网掩码进行按位逻辑与(AND)运算。如果运算后的结果完全一致，则表明这两台计算机位于同一子网内。例如，假设有一台计算机的 IP 地址为 192.168.1.100，子网掩码为 255.255.255.0，对其进行逻辑与运算(将 IP 地址和子网掩码的每位进行与运算，即只有当两个位都为 1 时，结果才为 1)后，得到的网络地址为 192.168.1.0。该网络地址定义了该 IP 地址所属的网络范围，而主机地址则可通过从完整 IP 地址中减去网络地址来确定。在此例中，主机地址为 0.0.0.100，即 IP 地址的最后一字节。明确网络地址和主机地址对于确保网络通信的准确性至关重要。当一设备准备向另一设备发送数据时，必须先确认目标设备的网络地址。若目标设备与发送方位于同一网络，数据包可直接在同一网络内传输；反之，若目标设备位于不同网络，则需通过路由器将数据包转发至目标网络。子网掩码的恰当设定与运用，确保了

设备能够准确辨识网络地址和主机地址，从而保障了网络通信的顺畅进行。

在基于分类的IP地址体系中，子网掩码是预设的，不允许用户自定义子网划分。例如，在A类地址中，前8位固定用于表示网络部分，而剩余的24位可供自由分配给主机。然而，在非分类的IP地址体系中，子网掩码的设置更为灵活，允许对主机地址部分进行进一步细分，从而实现更细粒度的网络管理。这种灵活性不仅提高了IP地址资源的使用效率，也为网络设计者提供了更大的操作空间，以适应多样化的网络需求。

子网掩码采用点分十进制表示法，其结构设计用于区分IP地址中的网络部分与主机部分。具体而言，在子网掩码中，1代表网络部分，0代表主机部分。基于此原则，不同类别的IP地址具有相应的默认子网掩码。

(1) A类地址的默认子网掩码为255.0.0.0，表明前8位(即第一个8位组)用于标识网络，剩余24位用于标识主机。

(2) B类地址的默认子网掩码为255.255.0.0，表明前16位(即前两个8位组)用于标识网络，后16位用于标识主机。

(3) C类地址的默认子网掩码为255.255.255.0，表明前24位(即前三个8位组)用于标识网络，最后8位用于标识主机。

在上述点分十进制表示中，每个数字实际上映射了子网掩码的一个8位二进制字段。例如，255在二进制下等同于8个连续的1(即11111111)，而0则对应8个连续的0(即00000000)。以255.255.255.0为例，该子网掩码的完整二进制形式为11111111.11111111.11111111.00000000，清晰地展示了前24位用于标识网络，最后8位用于标识主机的规则。这种机制确保了IP地址的有效解析，使得数据包能够准确无误地从源端传输到目标端。通过子网掩码的应用，网络管理员还可以进一步细分网络，提高IP地址资源的利用效率。

3. Internet域名系统

1) 域名概述

域名是在Internet上用于识别和定位特定资源(如网站、服务器等)的一种人类可读的地址形式。它充当了数字IP地址的友好替代品，使用户能够更加便捷地访问网络资源，而无须记忆复杂的数字序列。例如，通过输入www.example.com，用户即可轻松访问目标网站，而无须知晓其背后的IP地址。

(1) 顶级域名。

顶级域名(Top-Level Domain，TLD)位于域名体系结构的最高层级，主要分为两大类：通用顶级域名(Generic TLD，gTLD)和国家/地区代码顶级域名(Country Code TLD，ccTLDs)。

① 通用顶级域名：此类域名旨在全球范围内应用，涵盖多种组织类型，包括但不限于商业实体(.com)、网络服务提供商(.net)、非营利组织(.org)、政府机关(.gov)以及教育机构(.edu)。例如，域名www.google.com中的.com部分即为通用顶级域名，表明Google属于商业性质的企业。

② 国家/地区代码顶级域名：此类域名用于标识特定的国家或地区，如中国(.cn)、美国(.us)、日本(.jp)等。它们主要服务于各自国家或地区的网络资源。例如，www.sina.com.cn中的.cn部分指明新浪是中国注册并运营的网站。

(2) 二级域名。

二级域名位于顶级域名的左侧,通常由用户根据自身需求向相关注册机构申请注册。它有助于标识具体的组织、企业或个人,从而反映网站的品牌、名称或业务特性。以 www.example.com 为例,其中的 example 即为二级域名,代表了该网站的独特身份。

(3) 三级域名。

三级域名是在二级域名基础上的进一步细分,主要用于内部组织结构的划分或特定服务的指示。例如,www.example.com 中的 www 即为三级域名,常用于指向网站的主页面。

此外,还有一些特殊的域名类型,如子域名、泛域名等。

子域名:子域名是在二级或三级域名之下创建的,用于细化网站的各个部分或功能区。例如,mail.example.com 中的 mail 子域名可能指向邮件服务,而 blog.example.com 中的 blog 子域名则可能指向博客平台。

泛域名:是指使用通配符(*)来匹配所有子域名的域名。例如,*.example.com 可以匹配 www.example.com、blog.example.com 等所有以 example.com 为后缀的域名。

2) 域名系统

Internet 域名系统(Domain Name System,DNS)是一种分布式数据库系统,负责将人类友好的域名转换为机器可识别的 IP 地址。域名通常按照从右至左的顺序排列,依次为顶级域名、二级域名、三级域名等。其基本格式如下:

计算机名.[机构名.][网络名.] 顶级域名

这里,从右到左分别代表了国家或地区名称、网络类别、组织名称以及具体的主机名称。DNS 不仅简化了网络资源的访问过程,还促进了全球网络信息的高效管理和交换。

域名系统作为 Internet 的核心基础设施之一,承担着将易于人类记忆的主机名(即域名)转换为计算机可以直接处理的 IP 地址的重要任务。这一过程类似于现实世界中的电话簿,使用户能够通过简单的文本字符串(如 www.example.com)而非复杂的数字序列(如 192.168.11.100)来访问网络资源。即使目标服务器的 IP 地址因技术维护、迁移等因素发生变化,只要域名保持不变,用户依然能够通过相同的域名访问到所需的服务,而无须关注底层的技术细节。

5.2.4 Internet 的基本服务

1. 社交媒体

社交媒体是指依托于 Internet 平台的一系列在线服务和应用程序,其核心功能在于让用户能够创建个人资料、分享各种内容(包括但不限于文本、图像、视频等),并与他人进行交流互动,构建社交网络。社交媒体颠覆了传统媒体单向信息传递的模式,转而强调用户间的双向沟通和积极参与,从而为用户提供了一个开放、互动的虚拟社交环境。社交媒体的应用范围广泛,可用于信息的传播与获取、社交互动与人际关系的维护、商业营销与品牌形象的推广、社会舆论的形成与公共事务的参与等多方面。目前,较为流行的社交媒体形式包括但不限于社交软件、微信、微博、抖音、小红书等社交网络平台。

2. 流媒体

流媒体技术是指将连续的媒体数据经过压缩处理后,通过网络分段传输,以达到即时播放效果的技术手段。这项技术革新了传统的媒体消费模式——必须先下载完整文件才能开

始播放，而是实现了“边下载边播放”的用户体验，大大缩短了用户等待的时间，提升了观看或收听的便捷性。例如，在线视频观看过程中，视频数据会随着播放的进行不断从服务器端传输至客户端，用户无须等待整个视频文件下载完成即可开始观看。腾讯视频、爱奇艺、YouTube 等流媒体服务平台，为用户提供了丰富的影视内容，包括电影、电视剧、综艺节目及短视频等。除此之外，流媒体技术同样适用于游戏直播、体育赛事直播、新闻直播等领域。在这种场景下，直播者或内容提供方会将现场的音视频信号实时编码压缩并通过网络传输，观众则可以即时观看直播内容，并通过发送弹幕、点赞、评论等方式与主播或其他观众进行互动。

3. 电子商务和电子支付

电子商务是一种利用信息技术手段，围绕商品和服务交换开展的商务活动。它涵盖了通过 Internet、企业内部网络和增值网络进行的电子交易及其相关服务。电子商务的核心在于将传统商业活动的各个环节实现电子化、网络化和信息化，从而使得买卖双方能够在没有面对面接触的情况下完成各类商贸活动，包括但不限于消费者的在线购物、企业间的电子交易以及在线支付等。电子商务的主要模式包括企业对企业（Business to Business，B2B）、企业对用户（Business to Customer，B2C）、用户对用户（Customer to Customer，C2C）和线上线下商务（Online to Offline，O2O）。

B2B 电子商务模式是指企业之间通过 Internet 进行产品、服务及信息的交换和交易，如阿里巴巴。在这种模式下，交易双方均为企业，其交易规模通常较大，交易过程相对复杂。它具有交易频率相对较低，但每笔交易金额较大；交易关系较为稳定，合作周期较长等特点。

B2C 电子商务模式是企业通过 Internet 直接向用户销售商品和服务，如天猫、京东。此模式下，交易频率高，流程简单，消费者仅需在平台上选择商品、完成支付，随后等待商品配送即可。

C2C 电子商务模式是指用户之间通过 Internet 进行个人物品的交易，如二手交易平台闲鱼。这类模式的交易主体为个人，规模小且分散，价格灵活，买家可与卖家协商定价。

O2O 电子商务模式是结合线上营销与线下服务的一种商业模式，如美团、饿了么。O2O 模式强调线上线下互动，通过线上平台吸引顾客并提供预订、支付等服务，同时确保线下服务质量，提升用户体验。

电子支付则是指通过安全的电子手段，在消费者、商家和金融机构之间传输支付信息，以实现货币支付或资金转移的过程。电子支付系统是电子商务的重要组成部分，它简化了支付流程，提高了交易效率，保障了交易的安全性。

4. 网盘的应用

网盘，即网络硬盘，是一种基于 Internet 的数据存储服务，允许用户通过网络上传文件至服务器进行存储，并能从任何有网络连接的地方访问和管理这些文件。网盘为用户提供了灵活的存储解决方案，既适合个人用户存储和备份日常文件，也适用团队协作，支持文件共享、编辑等功能，有效促进远程工作和项目合作。

5. 搜索功能

搜索是 Internet 用户获取信息的基本途径之一，通过搜索引擎输入关键词或查询语句，可以高效地查找网页、文档、图片、视频等信息资源。搜索引擎的工作原理是通过索引

Internet 上的内容，根据用户的查询请求返回最相关的搜索结果。随着人工智能技术的进步，搜索引擎正变得更加智能，不仅能理解用户的自然语言查询，还能根据用户的搜索历史和行为偏好提供个性化服务，极大地提升了搜索的准确性和用户体验。

6. 电子邮件服务

电子邮件服务是 Internet 上最早且最基础的通信方式之一，主要用于个人与个人、个人与组织以及组织与组织之间的信息交流。电子邮件系统由邮件客户端软件、邮件服务器和通信协议构成，通过这些组件实现邮件的发送、接收和管理。电子邮件地址的标准格式为“用户名@电子邮件服务器域名”，例如，zhangsan@qq. com，其中，zhangsan 为用户名，qq. com 为电子邮件服务器的域名。电子邮件因其快捷、成本低廉、易于操作等优点，成为现代社会不可或缺的沟通工具。

5.3 无线网络

5.3.1 无线网络基础知识

1. 无线网络的定义

无线网络(Wireless Network)是一种利用无线通信技术进行数据传输和信息交换的计算机网络，不依赖于物理介质(如电缆连接)。无线网络通过无线电波、红外线等方式传输数据，使得设备在一定范围内可以自由移动而不会失去连接。无线网络具有灵活性、易于部署、扩展性强和成本效益高的特点。它允许设备(如智能手机、笔记本计算机和平板计算机等)在家中、办公场所或公共区域内方便地接入网络。无线网络按应用场景和覆盖范围主要分为无线个人域网(WPAN)，如蓝牙、红外通信；无线局域网(WLAN)，如 Wi-Fi；无线城域网(WMAN)，如 WiMAX；以及无线广域网(WWAN)，如蜂窝网络(3G、4G、5G)。这些网络类型满足了不同需求，从短距离的个人设备连接到广域的跨城市、国家的通信。

2. 无线网络的基本组成

无线网络的基本组成包括无线客户端设备、无线接入点、无线路由器，以及相关的网络基础设施。如图 5.8 所示。每个部分在无线网络中扮演不同的角色，共同实现了无线数据传输和通信。


无线客户端设备


无线接入点


无线路由器


交换机H3C

图 5.8 无线网络的基本组成设备

1) 无线客户端设备

无线客户端设备是无线网络的重要组成部分，指通过无线通信技术连接到网络的终端设备。常见的无线客户端设备包括智能手机、平板计算机、笔记本计算机，以及日益普及的智能家居设备，如智能音箱、智能门锁和可穿戴设备等。这些设备通常内置无线网卡或通过外接无线网卡来实现无线连接，利用 Wi-Fi、蓝牙、蜂窝网络(如 4G、5G)等技术进行数据的接收和发送。无线客户端设备能够随时随地访问网络资源，满足用户对互联网、文件服务

器、打印机等资源的需求。

在无线网络的架构中，客户端设备不仅是数据的终端接收方，也是信息的发出者。通过无线网络，这些设备能够与其他网络组件，如无线接入点和路由器建立连接，形成一个完整的网络通信链路。无线客户端设备的便携性和移动性，使得用户能够灵活地进行办公、学习和娱乐等活动，同时也推动了物联网的发展，使得智能家居、智慧城市等应用场景成为可能。这些设备与无线基础设施的紧密结合，构成了现代无线网络系统的基础，使得人们的生活方式与工作方式都发生了深刻的变革。

2）无线接入点

无线接入点（WAP）是无线网络中的核心组成部分，主要功能是将无线客户端设备与有线网络连接。作为无线和有线网络之间的桥梁，WAP 通过无线电波在特定频段（如2.4GHz 或 5GHz）进行数据的发送和接收，进而为无线客户端设备提供网络接入服务。用户通过 WAP 可以方便地访问互联网、公司内部网络等网络资源，而无须依赖传统的有线连接方式。WAP 通常通过有线方式连接到交换机或路由器，从而将无线设备引导到有线网络中，实现数据的双向传输。

在无线网络的实际部署中，WAP 的数量和位置对整个网络的覆盖范围和性能起着决定性作用。一个 WAP 可以支持多个无线客户端设备同时连接，然而，其性能会受到硬件配置、信号强度和网络带宽的影响。环境因素如墙壁、天花板以及其他障碍物都会对无线信号产生干扰，从而影响信号质量和网络速度。为了克服这些限制，通常在大面积的场所（如办公楼、校园、商场等）需要部署多个 WAP，形成一个覆盖广泛的无线网络。在这种情况下，漫游（Roaming）技术能够确保用户在不同 WAP 覆盖区域之间移动时，依然能够保持稳定的网络连接。此外，信道优化技术也用于减少 WAP 之间的干扰，确保每个 WAP 都能提供最佳的性能和传输效率。通过合理的 WAP 部署与配置，无线网络能够实现广泛的覆盖和高效的连接，满足多种应用场景的需求。

3）无线路由器

无线路由器是一种功能集成化的网络设备，结合了无线接入点和路由器的双重作用，广泛应用于家庭、小型办公室及其他小型网络环境中。作为无线接入点，路由器可以通过 Wi-Fi 技术连接多个无线客户端设备，如智能手机、平板计算机、笔记本计算机等，提供稳定的无线网络接入。而作为路由器，它能够管理数据包的传输路径，确保网络中的设备能够有效地与外部网络（如互联网）通信。无线路由器不仅可以通过有线方式连接到外部网络，还能通过其无线功能为局域网内的设备提供连接。

无线路由器还具备多项管理和安全功能，确保网络的正常运行和数据的安全性。通过其内置的动态主机配置协议（Dynamic Host Configuration Protocol，DHCP），路由器可以自动为网络中的设备分配 IP 地址，简化了设备的网络配置过程。同时，网络地址转换（Network Address Translation，NAT）功能能够隐藏内部网络设备的真实 IP 地址，提供额外的隐私和安全层。此外，路由器通常自带基本的防火墙功能，可以阻止未经授权的访问。用户可以通过路由器的网页管理界面进行配置，设置服务集标识符（Service Set Identifier，SSID）、密码以及安全协议（如 WPA3）等，确保网络的安全性。许多无线路由器还支持高级功能，如访客网络的设置、家长控制、带宽管理、以及虚拟专用网连接，以满足不同用户的个性化需求。这些功能使得无线路由器不仅提供了灵活的网络连接方案，还提升了网络的安

全性和管理便捷性。

4）其他网络基础设施

除了无线客户端设备、无线接入点和无线路由器，完整的无线网络还需要相关的网络基础设施，如交换机、网关和服务器。交换机用于连接多个无线接入点和有线设备，确保高效的数据传输和网络管理。网关通常连接到 ISP，充当本地网络与 Internet 之间的接口。服务器则提供各种网络服务，如 DNS、DHCP 和身份验证等，支持无线网络的正常运行和管理。通过这些组成部分的协同工作，无线网络能够提供灵活、便捷且高效的网络连接，满足现代生活和工作中的多样化需求。

5.3.2 无线局域网

1. 无线局域网的定义与类型

1）无线局域网概述

无线局域网（WLAN）是一种利用无线通信技术在局部区域内实现设备互连和资源共享的网络形式。WLAN 不需要传统的有线连接，通过无线电波在一定范围内传输数据，使得设备能够灵活地接入网络。WLAN 技术广泛应用于家庭、企业、学校和公共场所，极大地提升了网络的灵活性和便利性。

无线局域网的核心组成部分是无线接入点和无线客户端设备。无线接入点通过无线电波在 2.4GHz 或 5GHz 频段发送和接收数据，形成一个覆盖区域，称为服务集（Service Set）。无线客户端设备如智能手机、平板计算机、笔记本计算机等，通过内置的无线网卡与无线接入点进行通信，从而接入网络。无线局域网使用的主要协议是 IEEE 802.11 系列标准，包括 Wi-Fi 4（802.11n）、Wi-Fi 5（802.11ac）、Wi-Fi 6（802.11ax）等，这些标准不断演进，提供更高的传输速度和更好的网络性能。

无线局域网具有多种优势。首先，它提供了极大的灵活性和移动性，用户可以在无线信号覆盖范围内自由移动而不中断网络连接。其次，无线局域网的安装和部署相对简单，不需要铺设大量的网络线缆，降低了网络建设的成本和时间。此外，无线局域网能够支持多种设备接入，适应现代办公和生活中多设备同时在线的需求。

2）无线局域网的分类

无线局域网根据其应用场景和规模的不同，可以分为多种类型。主要包括家庭无线局域网、企业无线局域网、公共无线局域网和校园无线局域网等。每种类型的无线局域网都有其特定的需求和特点。

（1）家庭无线局域网。

家庭无线局域网是最常见的无线网络形式，主要用于家庭环境中。家庭无线局域网通常由一个无线路由器组成，负责将互联网连接扩展到家庭内的各种无线设备，如智能手机、平板计算机、笔记本计算机、智能家居设备等。家庭无线局域网的特点是设备数量相对较少，覆盖范围通常是一个家庭或公寓的内部区域。为了保证网络的稳定性和安全性，家庭无线局域网一般使用 Wi-Fi 标准，如 Wi-Fi 4（802.11n）、Wi-Fi 5（802.11ac）和 Wi-Fi 6（802.11ax），并通过加密技术（如 WPA2 或 WPA3）保护网络安全。

（2）企业无线局域网。

企业无线局域网广泛应用于各类办公环境，包括小型企业到大型企业。与家庭无线局

域网不同，企业无线局域网需要支持更高的设备密度和更广的覆盖范围。企业无线局域网通常由多个无线接入点组成，这些无线接入点通过有线网络连接到企业的核心交换机或无线路由器。企业无线局域网的特点包括高并发连接、高性能要求和网络安全性。企业通常使用 Wi-Fi 5 或 Wi-Fi 6 标准，以支持高速数据传输和多用户并发访问。同时，企业无线局域网还配备无线控制器，用于集中管理无线接入点、优化网络性能和实施安全策略。

（3）公共无线局域网。

公共无线局域网在公共场所提供互联网接入服务，如咖啡馆、商场、机场、酒店等。公共无线局域网的主要特点是对大量用户的支持和开放性。为了应对高密度的用户连接和提供稳定的服务，公共无线局域网通常部署多个无线接入点，并使用负载均衡技术来分配网络流量。由于公共无线局域网涉及众多用户，安全性是一个重要考虑因素，通常采用加密和认证机制来保护用户的数据安全。此外，公共无线局域网还可能提供访问限制和流量管理，以确保网络资源的公平分配和性能优化。

（4）校园无线局域网。

校园无线局域网应用于学校，支持师生的教学和学习活动。校园无线局域网需要覆盖整个校园，包括教室、实验室、图书馆、宿舍等区域。与家庭和企业无线局域网类似，校园无线局域网由多个无线接入点组成，并通过中央控制系统进行管理。校园无线局域网需要支持大量的设备连接和高带宽需求，同时提供安全的网络访问和管理功能。通常，校园无线局域网会采用更高级的无线标准，如 Wi-Fi 6，来满足教学和研究活动对高速和高稳定性的要求。某大学无线局域网分布如图 5.9 所示。

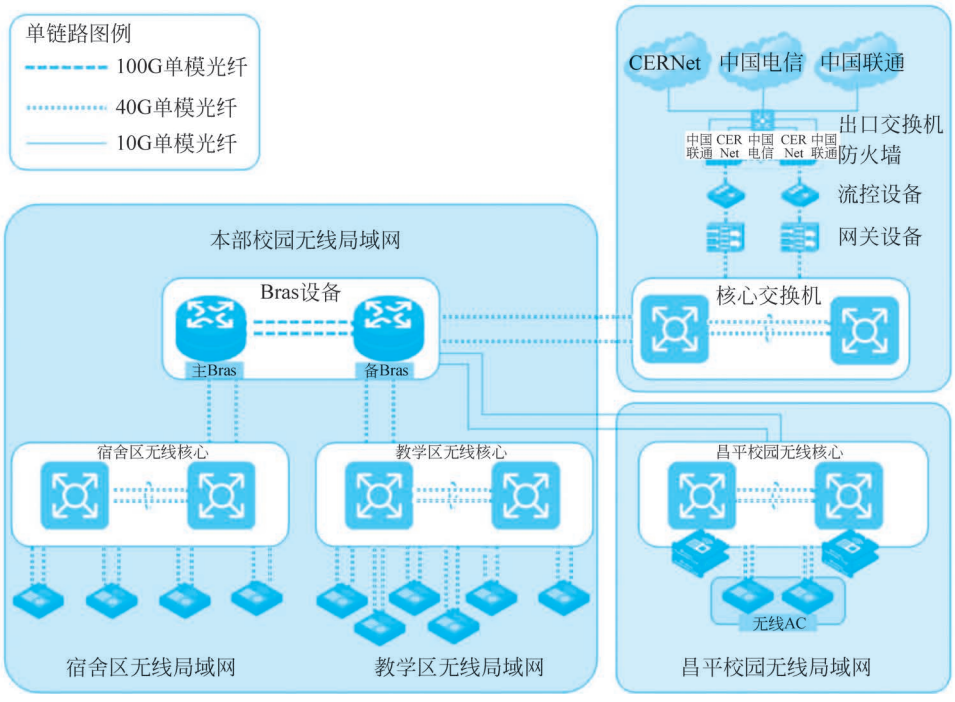


图 5.9　某大学无线局域网分布图

无线局域网的分类涵盖了从家庭到企业、公共场所和校园的多种应用场景。每种类型

的无线局域网根据其需求和规模的不同，具有不同的技术要求和配置方案，以实现高效、稳定的网络服务。

2. 无线局域网的架构与部署

在无线局域网中，无线接入点和客户端设备之间的关系是网络架构的核心。无线接入点和客户端之间的交互方式直接影响到网络的性能、覆盖范围和用户体验。

1）无线接入点

无线接入点（WAP）是 WLAN 架构中的关键组件，负责提供无线信号覆盖，并将无线通信转换为有线网络连接。WAP 通常连接到网络交换机或无线路由器，通过有线接口将无线网络与有线网络系统连接。它们负责处理客户端设备的无线信号，提供网络访问权限，并管理无线网络的流量。

WAP 通过无线电波广播网络信号，使得附近的客户端设备能够探测到信号并连接到无线网络。一个 WAP 的覆盖范围受物理环境的影响，如墙壁、家具和其他障碍物。为了扩大网络覆盖范围和提高网络容量，通常会部署多个 WAP，并通过无线信号或有线方式进行连接。这种多 WAP 部署模式通常称为无线网络的“蜂窝”架构，每个 WAP 称为一个蜂窝区域。

2）客户端设备

客户端设备是指连接到 WLAN 的各种终端，如智能手机、笔记本计算机、平板计算机和无线打印机等。这些设备通过无线网络适配器与 WAP 建立连接。客户端设备会扫描可用的无线网络，并选择一个 WAP 进行连接。连接后，客户端设备将通过该 WAP 访问网络资源和互联网。

客户端设备通过无线电波向 WAP 发送数据请求，WAP 接收数据并将其转发到有线网络上的目标地址。返回的数据同样通过 WAP 从有线网络发送回客户端设备。WAP 在数据传输过程中可能会遇到干扰和信号衰减等问题，因此需要有效的信号处理和干扰管理策略，以确保稳定的连接质量。

3）无线接入点与客户端设备之间的关系

WAP 与客户端之间的关系可以视为一种主从模式。在这种模式下，WAP 充当网络的主控点，而客户端设备则作为从属设备与 WAP 进行通信。WAP 的主要职责是提供网络访问、管理无线信号和处理数据流量，而客户端设备则依赖 WAP 来获得网络服务和资源。

在实际部署中，WAP 与客户端的有效配置和管理至关重要。WAP 的布置需要根据实际需求和环境进行优化，以确保良好的覆盖范围和信号强度。客户端设备的配置也需要确保正确连接到合适的 WAP，并配置正确的网络设置。此外，为了提升网络性能，WAP 通常会配备负载均衡和频谱管理功能，以优化客户端的连接体验。

无线接入点与客户端设备之间的关系是 WLAN 架构的核心，良好的 WAP 部署和客户端设备管理是确保无线网络高效、稳定运行的基础。

3. 无线局域网的安全性

1）无线局域网的安全威胁

无线局域网因其便捷性和灵活性，广泛应用于家庭、企业和公共场所。然而，WLAN 的无线性质也带来了多种安全威胁，这些威胁可能导致数据窃取、非法接入和其他安全问题。了解这些安全威胁有助于采取有效的防护措施，保障无线网络的安全性。

(1) 数据窃取。

数据窃取(Data Voyeur)是无线网络面临的主要安全威胁之一。由于无线信号可以被空气中的任何设备接收,攻击者可能会利用嗅探工具捕获传输中的数据包。如果网络中的数据传输未加密,攻击者可以轻易解读这些数据,从而窃取敏感信息,如个人身份信息、银行账户信息或企业机密。即使是加密的网络,弱加密或过时的加密标准也可能被破解,从而威胁到数据的安全性。

(2) 非法接入。

非法接入(Unauthorized Access)指未经授权的用户或设备连接到无线网络。这种情况可能发生在网络安全设置不严密的情况下,攻击者可以通过猜测或破解弱密码获得网络访问权限。一旦成功接入,攻击者可以利用网络资源进行非法活动,如监听网络流量、实施中间人攻击或发起网络攻击。此外,非法接入还可能导致网络带宽的滥用和网络性能的下降,影响正常用户的使用体验。

(3) 中间人攻击。

中间人攻击(Man-in-the-Middle Attack)是另一种常见的无线网络安全威胁。在这种攻击中,攻击者伪装成合法的无线接入点或网络节点,拦截和修改在网络上传输的数据。攻击者可以利用这一技术进行数据窃取、篡改数据或注入恶意代码。中间人攻击通常发生在未加密的无线网络中,使得攻击者能够读取和操控传输中的信息。

(4) 网络干扰与拒绝服务攻击。

无线网络的信号容易受到干扰,即网络干扰(Network Interference),可能导致网络性能下降或中断。干扰源可能是其他无线设备、物理障碍物或恶意攻击。拒绝服务(Denial of Service,DoS)攻击通过大量无用的流量占用网络带宽,导致合法用户无法访问网络服务。这类攻击通常通过发送大量数据包或伪造无线接入点进行,使网络瘫痪或性能显著下降。

(5) 恶意软件与僵尸网络。

无线网络也可能成为恶意软件(Malware)传播的渠道。攻击者可以通过无线网络传播病毒、木马或间谍软件,感染连接到网络的设备。这些恶意软件可以窃取用户信息、破坏系统文件或将感染的设备纳入僵尸网络,用于发起进一步的网络攻击。僵尸网络(Botnet)由大量受控设备组成,用于执行大规模攻击或其他恶意活动。

2) 无线局域网的安全措施

为了确保无线局域网的安全性,采取有效的安全措施至关重要。这些措施可以防止未经授权的访问、数据窃取和网络攻击。以下是8种常见的无线局域网安全措施及其特点。

(1) WPA/WPA2加密。

Wi-Fi保护接入(Wi-Fi Protected Access,WPA)和WPA2是无线网络中最常用的加密协议,用于保护无线通信的安全。WPA使用时限密钥完整性协议(Temporal Key Integrity Protocol,TKIP)加密数据,而WPA2则引入了更强的高级加密标准(Advanced Encryption Standard,AES)加密算法。WPA2提供更高的安全性,防止数据窃取和篡改。

WPA:最初的WPA标准采用TKIP加密,解决了有线等效保密(Wired Equivalent Privacy,WEP)加密技术的安全问题。尽管比WEP更安全,但WPA已经过时,不再满足当前的安全需求。

WPA2:作为WPA的增强版,WPA2使用AES加密算法,提供了更强的数据保护。它

引入了基于计数器模式密码块链接消息认证码协议(Counter Mode with Cipher Block Chaining Message Authentication Code Protocol,CCMP),显著提升了网络的安全性。WPA2 适用于家庭和企业环境,并在许多现代无线设备中得到广泛支持。

(2) WPA3。

WPA3 是最新的无线网络安全标准,进一步提升了 WPA2 的安全性。它引入了 SAE(Simultaneous Authentication of Equals)协议,增强了密码保护,即使在使用弱密码的情况下也能防止密码破解。此外,WPA3 改进了公开网络的加密保护,提供了更高的安全保障。

(3) MAC 地址过滤。

介质访问控制(Medium Access Control,MAC)地址过滤是一种基于设备硬件地址的网络访问控制方法。网络管理员可以在无线接入点上配置一个允许或拒绝特定 MAC 地址的列表。只有在白名单上的设备可以连接到网络,这种方法能够有效防止未经授权的设备接入。

虽然 MAC 地址过滤可以提高网络的安全性,但它并不是绝对安全的,因为 MAC 地址可以被伪造。它应作为其他安全措施的补充,而不是唯一的防护手段。

(4) 隐藏 SSID。

SSID 是无线网络的名称。隐藏 SSID 意味着无线网络不会广播其名称,从而减少了被发现的机会。虽然隐藏 SSID 不能完全防止被攻击者扫描和发现网络,但它可以使网络不那么显眼,从而减少自动扫描工具的发现概率。

(5) 强密码策略。

使用强密码是保护无线网络的基本措施之一。密码应至少包含 8 个字符,包括大小写字母、数字和特殊字符。避免使用易于猜测的密码,如 123456 或 password。强密码能够有效防止暴力破解和字典攻击,提高网络的安全性。

(6) 定期固件更新。

无线接入点和路由器的固件更新是维护网络安全的重要措施。制造商会定期发布更新以修补已知漏洞和改进安全性。管理员应定期检查并安装这些更新,以确保网络设备保持最新的安全状态。

(7) 网络监控与入侵检测。

部署网络监控工具和入侵检测系统(Intrusion Detection System,IDS)可以实时监测无线网络中的异常活动。通过分析网络流量和行为模式,这些工具可以检测到潜在的攻击或异常,及时采取措施保护网络安全。

(8) 强制使用 VPN。

在公共无线网络中,强制使用 VPN 可以增强数据传输的安全性。VPN 通过加密用户与网络之间的通信,防止数据在传输过程中被窃取或篡改。

通过实施这些安全措施,可以显著提升无线局域网的安全性,保护网络免受各种威胁和攻击,从而为用户提供一个稳定、安全的无线网络环境。

小结

本章对计算机网络的定义、发展历程、主要功能、系统组成及网络分类进行了详细介绍,

结合具体应用对常见的各类计算机网络做了阐述，并重点针对网络协议、OSI 及 TCP/IP 进行描述。同时，以全球最大的计算机网络 Internet 为例，从其发展历程、常见的接入技术、IP 地址、域名系统及各类服务等方面进行了系统阐述。最后，针对无线网络，重点就其网络组成、工作原理及其安全性等展开介绍。

案例一：从黑客攻击阴影到互联网治理新格局

2014 年 1 月 24 日下午三点，大量国内网站域名解析不正常，许多访问的请求被跳转到一个无响应的美国 IP 地址。全国将近三分之二的 DNS 服务器处于瘫痪状态，包括百度，新浪微博等网站都暂时无法访问，预计受影响的网站超过几十万个。经查网络故障是全球 DNS 根解析出现故障导致，该事件很有可能是黑客攻击行为。

2016 年中国主导雪人计划，在与现有 IPv4 根服务器体系架构充分兼容的基础上，在全球 16 个国家完成 25 台 IPv6 根服务器架设，事实上形成了 13 台原有根加 25 台 IPv6 根的新格局。中国部署了其中的 4 台，这打破了中国过去没有根服务器的困境，巩固了国家的网络主权和信息安全。也改变了美国在全球互联网治理中一家独大的现状，让更多的国家都参与到全球互联网治理中。2019 年 6 月 28 日，互联网域名系统国家工程研究中心（ZNDS）推出首款搭载龙芯芯片的域名服务器——红枫系统，这款服务器在软硬件上均实现了国产化，并从技术上突破了全球 13 个根服务器的数量限制，对于我国维护网络安全具有重要的意义。

当前网络空间已成为与海、陆、空同等重要的人类生活的新领域，网络安全也成为国家安全的重要组成部分，并与政治、经济、社会甚至每个人的人身安全紧密联系在一起。维护网络安全不仅是国家、企业的责任，也需要每位网民共同参与。大学生作为网络使用最为频繁的重要群体，应提高网络安全意识和防护技能，遵守网络空间的法律法规，做一个合格的网络公民。

案例二：华为的 5G 崛起之路

在 21 世纪 10 年代，中国科技企业在全球科技领域的崛起引人瞩目，而华为公司作为其中的领军者，经历了许多挑战与磨难。这个故事不仅展现了 5G 技术的突破，还深刻体现了国家力量与个人奋斗的结合，激励着无数年轻人。

21 世纪 10 年代初，全球正处于 4G 网络的高速发展阶段，5G 尚在概念探索之中。当时，世界各大科技巨头纷纷布局 5G 技术，尤其是美国和欧洲国家的企业占据了技术研发的主导地位。然而，华为公司作为中国企业，怀抱着对科技的追求和民族复兴的梦想，决定勇敢进军 5G 领域。

华为公司创始人任正非曾公开表示："我们要在 5G 时代，让中国掌握更多的话语权。"这不仅是企业发展的目标，更是为国家崛起贡献科技力量的愿景。在全球竞争异常激烈的背景下，华为公司 5G 研发团队不分昼夜地攻克一个又一个难题，逐步突破技术壁垒。

随着华为公司 5G 技术的不断成熟，华为公司成为全球 5G 网络设备领域的领军企业，掌握了全球范围内超过 20%的 5G 标准必要专利。然而，2018 年开始，华为公司遭遇了国际上的打压，尤其是美国发起了对华为公司的禁令，导致华为公司无法使用一些重要的技术和零部件。

面对这一严峻形势，华为公司并未退缩，而是更加坚定了自力更生的决心。在中国政府的支持和全国人民的关注下，华为公司通过自主研发和技术创新，逐步摆脱对外技术依赖，建立了自己的供应链体系。这一过程中，华为公司 5G 研发团队更是埋头苦干，最终推出了全球领先的 5G 商用网络设备，成为全球多个国家 5G 网络建设的合作伙伴。

华为公司的故事，不仅是一个企业发展的传奇，更是无数科研人员和工程师无私奉献、勇于挑战自我、不断突破的缩影。这个故事告诉我们，唯有坚持创新与拼搏，才能在全球舞台上获得尊重和话语权。华为公司的 5G 之路是一条艰难而光辉的路，正因为有这样的企业和个人在背后默默付出，中国才能在全球科技竞争中占据一席之地。新时代的青年，应该把个人梦想与国家发展紧密结合起来，投身于科技创新，勇敢追梦，为中华民族的伟大复兴贡献自己的智慧与力量。

习题 5

一、单项选择题

1. 以下_____最准确地描述了计算机网络的定义。

A. 计算机网络是连接多台计算机的系统，用于共享资源和信息

B. 计算机网络是一种硬件设备，用于连接互联网

C. 计算机网络是一种软件，用于管理计算机之间的通信

D. 计算机网络是一种通信协议，用于确保数据安全

2. 以下_____不是计算机网络的主要功能。

A. 数据通信　　B. 资源共享　　C. 实时天气预测　　D. 分布式处理

3. 计算机网络的分类中，以下_____是按照覆盖范围划分的。

A. 局域网、城域网、广域网　　B. 有线网、无线网

C. 专用网、公用网　　D. 客户端/服务器网络、对等网络

4. 计算机网络的 OSI 参考模型中，_____负责数据的加密和解密。

A. 网络层　　B. 传输层　　C. 表示层　　D. 应用层

5. IPv4 地址由_____位二进制数组成。

A. 16　　B. 32　　C. 64　　D. 128

6. 以下_____顶级域名通常用于商业机构。

A. .com　　B. .net　　C. .org　　D. .gov

7. 局域网中一台主机的 IP 地址为 192.168.1.23，子网掩码为 255.255.255.0，以下表述错误的是_____。

A. 此局域网中可正常上网的最多为 512 台主机

B. 这是一个 IPv4 格式的地址

C. 此局域网中其他主机 IP 地址一般为 192.168.1.*

D. 此 IP 地址是由 32 位二进制数组成的，但用点分十进制表示

8. 以下用于发送电子邮件的协议是_____。

A. SMTP　　B. OP3　　C. IMAP　　D. HTTP

9. 无线路由器在家庭网络中扮演着重要角色。以下关于无线路由器功能的描述，

_____是不正确的。

A. 提供无线接入点功能，允许多个设备通过 Wi-Fi 连接

B. 管理数据包的传输路径，实现内部网络与外部网络的通信

C. 通过 DHCP 自动为网络设备分配 IP 地址

D. 直接连接到 ISP，无须其他设备作为中介

10. 关于无线接入点的作用，错误的是_____。

A. 将无线客户端设备与有线网络连接

B. 通过无线电波在特定频段进行数据的发送和接收

C. 为无线客户端设备提供互联网访问服务

D. 自动为网络中的所有设备分配 IP 地址

11. 关于无线网络的特点，描述不正确的是_____。

A. 利用无线电波进行数据传输

B. 具有较高的灵活性和移动性

C. 通常比有线网络提供更高的带宽

D. 覆盖范围可通过添加无线接入点扩展

二、判断题

1. 计算机网络中，集线器工作在数据链路层，具有数据转发和过滤功能。（　　）

2. 在计算机网络中，路由器工作在网络层，可以根据 IP 地址进行数据包的路由选择。（　　）

3. OSI 参考模型和 TCP/IP 是完全相同的两套网络体系结构。（　　）

4. HTTP 属于 OSI 参考模型中的应用层协议。（　　）

5. 同一个 IP 地址可以有若干不同的域名，但每个域名只能有一个 IP 地址与之对应。（　　）

6. 光纤的信号传播利用了光的全反射原理。（　　）

7. 目前大量使用的 IP 地址中，A 类地址的每个网络的主机个数最多。（　　）

8. 公共场所利用无线路由器上网，IP 地址分配方法一般采用动态分配的方式。（　　）

9. Wi-Fi 7 相比 Wi-Fi 6 的主要优势仅在于传输率的提升。（　　）

10. 6G 网络将实现地面无线与卫星通信的集成，从而实现全球无缝覆盖。（　　）

三、填空题

1. 计算机网络的硬件系统主要包括计算机设备、通信设备和_____。

2. OSI 参考模型从下到上分为七层，分别是物理层、数据链路层、网络层、传输层、会话层、_____和应用层。

3. TCP/IP 中，_____协议负责将应用层数据分成较小的段，并添加必要的头部信息以便传输。

4. 计算机网络的_____是指网络中各实体间的连接形式，常见的有总线状、星状、环状等。

5. 中国教育和科研计算机网的英文简称是_____。

6. 子网掩码用于将 IP 地址划分为_____和主机地址两部分。

7. 在网络性能方面，_____网络通常提供更高的带宽和更低的延迟，适合需要大数据传输和高实时性的应用，如高清视频流、在线游戏和大规模数据中心。

8. IEEE 802.11ax 标准，也称为_____，在 2.4GHz 和 5GHz 频段上工作，支持最高 9.6Gb/s 的数据传输率。

9. 发布于 2009 年的 IEEE 802.11n 标准引入了_____技术和空间复用，使得信号质量和网络效率大大提高。它可以通过多条无线链路同时传输数据，显著改善了网络的稳定性和覆盖范围。

四、简答题

1. 简述计算机网络的定义及其主要功能。

2. 解释 OSI 参考模型和 TCP/IP 的区别与联系。

3. 列举至少 3 种常见的 Internet 接入技术，并简要介绍其特点。

4. 简述 IP 地址的分类及特点。

5. 简述无线网络在安全性方面的特点及相应的安全措施。