普通高中教科书

信息技术

选择性必修2

网 络 基 础

浙江教育出版社
ZHEJIANG EDUCATION PUBLISHING HOUSE

普通高中教科书

信息技术

选择性必修2

网络基础

闫寒冰 主编

浙江教育出版社·杭州

主　　编：闫寒冰
副 主 编：赵　健　魏雄鹰

本册主编：林　强
编写人员（按姓氏笔画排列）：
叶敏红　李玉杰　陈　胜　林　强
赵明阳　胡家智

前　言

信息技术作为当今先进生产力的代表，已经成为我国经济发展的重要支柱和建设网络强国的战略支撑。在这样的大背景下，教育部全面修订并颁布了《普通高中信息技术课程标准（2017年版）》，为这门课程设定了与新时代相符的育人目标：帮助学生掌握信息技术基础知识与技能、增强信息意识、发展计算思维、提高数字化学习与创新能力、树立正确的信息社会价值观。

本套教材依据《普通高中信息技术课程标准（2017年版）》编写，包括两本必修教材《数据与计算》《信息系统与社会》，六本选择性必修教材《数据与数据结构》《网络基础》《数据管理与分析》《人工智能初步》《三维设计与创意》《开源硬件项目设计》，两本选修教材《算法初步》《移动应用设计》。

本套教材的编写组汇集了来自信息技术、课程与教学、教育技术等领域的高校学者与教学一线专家。编者们通力合作，从课程内容、教材体例、技术选择、教学方法、学习方法等方面精心打磨，期待以最专业的样态帮助学生达到课程预期的育人目标。

具体而言，本套教材体现了如下特点：

1. 体例上——为核心素养的培养创造空间和条件：将核心学习内容与支持学习的方法有机融合在一起，支持学生在自主、合作、探究的学习情境下发展核心素养。

2. 内容上——体现概念、内容与方法的精准与专业：在增强教材可读性的同时，精炼提升综合素养所必需的核心内容，强调所有概念、内容与方法的精准与专业。

3. 活动上——着力提升学生的高级思维能力：精心设计与布局教材中的练习、思考、讨论、实践与项目学习，追求对高级思维能力的培养。

4. 案例上——体现信息科技的多层需求与多维格局：把案例的呈现作为开阔视野的重要手段，帮助学生理解信息技术对于社会发展所具有的价值与意义。

5. 技术上——引领学生拓宽视野与发展思维：将每种具体应用软件都作为解决某些问题的一条路径来看待，期待学生通过具体的技术操作体验，理解其背后的原理与格局、特点与局限，拓宽视野、发展思维。

本册教材是选择性必修《网络基础》，是在信息技术必修课程基础上的深化学习。通过本册教材的学习，希望同学们掌握计算机网络的核心概念与发展历程，了解常用网络设备的功能，能通过网络命令查询网络及设备的工作状态，排除常见联网故障，认识到物联网对社会发展的影响，能使用典型的网络服务解决生活与学习中的问题，利用信息技术分享网络资源，具备网络应用安全意识，逐步成为信息社会的积极参与者。

就教材本身讲述的知识内容而言，我们相信，只要同学们潜心自学就可以基本掌握。但“知识内容”只是发展信息技术核心素养的基础部分，所以，我们希望同学们不要仅满足于对具体知识与具体技术的掌握，还要重视教材中的各类学习活动，与老师和学友一起，更多地去创造、研究、解决问题、制作、交流、合作和评价，唯有如此，同学们才能藉由这门课程的学习全面地提升信息素养，增强在信息社会的适应力与创造力，为实现中华民族伟大复兴的宏伟目标做出更大贡献！

本册教材在编写过程中得到了各方面的大力支持。北京大学计算机系李晓明教授、浙江大学计算机学院卜佳俊教授和翁恺教授、北京航空航天大学欧阳元新副教授在百忙之中对书稿内容进行了审阅。胡小伟老师为本书的撰写提供了相关资料与编写建议，叶巧蕊、叶璐婷、朱新葵、胡承丰四位高中教师对书稿内容提出了宝贵的修改意见。

由于水平有限，本书可能还存在不足之处。希望大家在教材使用过程中，能够及时将意见和建议反馈给我们，对此，我们深表谢意。

目　录
MULU

第一章 网络概述

1.1 网络的起源与发展 …… 4
1.2 网络的分类 …… 11
1.3 网络与社会 …… 15
1.4 “互联网＋” …… 19

第二章 网络技术基础

2.1 网络拓扑结构 …… 32
2.2 网络体系结构与TCP/IP协议 …… 35
2.3 网络传输介质与设备 …… 44
2.4 网络命令与简单故障排除 …… 49

第三章 网络服务

3.1 网络服务概述 …… 62
3.2 常见网络服务 …… 66
3.3 网络服务的发展 …… 80

第四章 物联网

4.1 感知物联网 …… 94
4.2 物联网的相关技术 …… 102
4.3 物联网搭建实例 …… 110

第五章 网络安全

5.1 网络安全威胁与防范 …… 124

5.2 数据加密与安全认证 …… 127

5.3 网络安全协议 …… 134

5.4 防火墙 …… 139

第一章 1

网络概述

当今世界，随着计算机、网络通信等技术的高速发展，特别是因特网在全球范围内的迅速普及，计算机和网络已渗透到人类社会的各个角落。计算机网络突破了人们在传统信息交流方式中受到的时空限制，已成为人们获取、交换信息的重要途径和工具，对社会发展和人们的生活产生了深刻的影响。

问题与挑战

- 随着移动网络和电子商务的快速发展，移动支付已经进入日常生活中的衣食住行等各个领域，现金的使用频次越来越低。在电商平台上网购，支付宝、微信支付和银联是主要支付手段；网约车、共享单车等的付费，都以移动支付为主。在不久的将来，移动支付会不会完全替代现金支付？

- 智能家居在日常生活中越来越常见。长期在外工作的人若想了解留守家中父母的实时情况，他可以通过手机、平板电脑或其他终端在任何一个有网络的地方查看并管理家中的电器、门窗、其他设备及老人的居家情况等。这些功能是如何实现的？需要哪些类型网络的支撑？

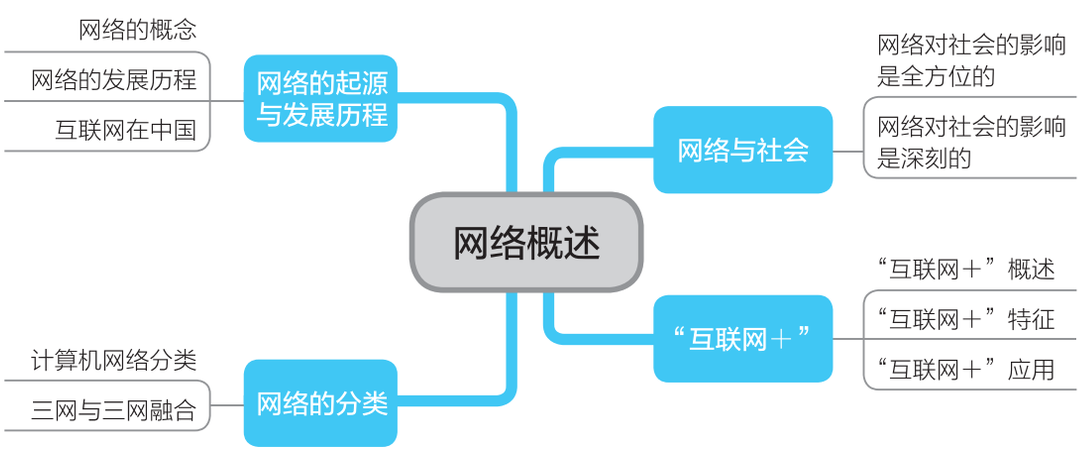
- 2016年8月16日，随着世界首颗量子科学实验卫星“墨子号”的成功发射，我国成为全球第一个实现卫星和地面之间量子通信的国家。量子通信进一步提升了信息传输的安全性。那么，量子通信网络会有怎样的应用前景？

- 目前，计算机网络已经深入人们生活的方方面面，但网络中也存在各种问题。结合实际，分析网络技术目前存在哪些问题，并思考解决策略，展望未来网络的发展。

学习目标

1. 知道计算机网络的概念、结构、特征及发展历程。
2. 掌握计算机网络的分类及其特征。
3. 理解移动互联网、物联网及三网融合。
4. 熟悉网络对社会的影响，了解“互联网＋”概念及其典型应用。

内容总览



1.1 网络的起源与发展

网络已经深刻地改变了人们的生活，特别是近年来智能终端和移动互联网的普及以及云计算和大数据的运用，促进并加速了新一轮的科技革命，对人类社会的发展产生了广泛而深远的影响。

1.1.1 网络的概念

计算机网络是通信技术与计算机技术密切结合的产物，它具有数据通信、资源共享、分布处理等功能。1970年，美国信息处理学会联合会（AFIPS）提出，计算机网络是以相互共享资源（硬件、软件和数据）方式连接起来，且各自具有独立功能的计算机系统的集合。具体地讲，就是指将地理位置不同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，在网络操作系统、网络管理软件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计算机系统集合。

计算机网络包含以下三个组成部分：

（1）计算机系统。它主要用于完成数据的收集、存储、处理和输出等任务，并提供各种网络资源，是计算机网络的基本模块，可分为服务器和终端。

服务器是网络资源的主要构成部分，负责数据处理和网络控制。网络软件和网络的应用服务程序主要安装在服务器中，为终端提供各种服务。终端是网络中数量大、分布广的设备，是用户进行网络操作，实现人机对话的工具，它可以是计算机、手机、平板电脑等各类设备。

（2）数据通信系统。它构成了计算机与通信设备、计算机与计算机之间的数据通信链路，主要由传输介质和网络连接设备等组成。

传输介质是传输数据信号的物理通道，用于连接网络中的各种设备。常见传输介质有双绞线、光纤、激光、微波等。网络连接设备主要用于实现网络中各计算机之间、网络与网络之间的互联，主要包括网卡、交换机、路由器等。

（3）网络软件及协议。创建计算机网络的主要目的是为了实现数据通信和资源共享，要实现这一目的，网络中需配备功能完备的网络软件，包括网络操作系统（如Unix、Linux、NetWare、Windows Server等）、网络通信协议（如TCP/IP、IPX/SPX等）、通信软件以及管理和服务软件等。

网络操作系统负责整个网络的软件资源、硬件资源的管理以及网络通信和任务的调度，并提供用户与网络之间的接口，它是网络管理系统软件和通信控制软件的集合。网络中各结点之间互相通信或交换信息需要有某些约定和规则，这些约定和规则的集合称为协议，各节点之间的逻辑互联依赖协议来实现，它是计算机网络正常工作的基础。

当今大型超市的日常数据管理一般都通过网络系统来实现，它就是一个较为典型的计算机网络应用，如表1.1.1所示。收银员用扫描枪获取商品的二维码，前台销售终端再通过数据通信链路获取数据服务器中相应商品的信息，当完成收款操作后，销售终端通过超市管理系统将数据服务器中的数据更新，打印机打印凭条，完成销售结账。

表1.1.1　超市网络系统分析

组成部分	具体对应设备	功能
计算机系统	数据服务器、后台计算机、销售终端、扫描枪、电子条码秤、打印机等	负责数据的收集、存储、处理、输出等
数据通信系统	构成网络的交换机、路由器、网线等设备	负责提供各设备之间的数据通信链路
网络软件及协议	网络操作系统、超市管理系统及通信协议	管理整个系统的软硬件及数据资源

1.1.2　网络的发展历程

从20世纪60年代兴起，到20世纪90年代形成全球互联的因特网，再到今天互联网与各行业有机融合，计算机网络已经成为当代科技发展最快的领域之一，对信息时代的人类社会发展有着巨大的影响。

随着计算机应用的发展，用户希望通过多台计算机互联实现资源共享。20世纪60年代，美国军方开始研究计算机技术和通信技术的结合，并由美国国防部高级研究计划署（ARPA）成功研制出ARPAnet网络，它通常被认为是现代计算机网络的起源，同时也是互联网的起源。

1. 计算机网络的发展历程

随着计算机技术和通信技术的不断发展，计算机网络也经历了从简单到复杂，从单机到多机的发展过程，其演变过程经历了以下四个阶段，即面向终端的计算机网络、分组交换式的计算机网络、开放的标准化计算机网络、互联网络和高速计算机网络。

第一阶段，面向终端的计算机网络。此时的网络是指以计算机为中心的远程联机系统，充分利用分时多用户系统支持多个用户通过多台终端共享单台计算机的资源，使得一台主机可以让几十个甚至上百个用户同时使用，如1963年美国推出SABRE-1飞机票订购系统，该系统由一台计算机和分布广泛的2000多个终端组成。严格地说，这类简单的“终端—通信线路—计算机”系统与以后发展成熟的计算机网络相比较，存在着本质的不同。因为除了中心计算机外，其他终端均没有数据处理的功能，这种系统被称为“面向终端的计算机通信网”。

拓展链接

分时多用户系统

分时多用户系统是指一台主机连接若干终端组成的计算机系统。多用户分时共用一台主机，主机承担所有用户的信息处理任务，实行集中管理。

第二阶段，分组交换式的计算机网络。1969年诞生的世界上第一个网络系统——ARPAnet，标志着计算机网络的兴起，实现了真正意义上的计算机网络。它的主要特点是分组交换、资源共享及分散控制，它是计算机网络技术发展中的里程碑。到了20世纪70年代，该网络的节点超过60个、主机超过100台，实现了通信卫星与计算机网络的互相连通。这一阶段的计算机网络使得整个网络系统性能大大提升，而且不会因为单个节点故障影响整个系统，甚至导致系统瘫痪。

第三阶段，开放的标准化计算机网络。这个阶段解决了计算机网络间互联标准化的问题，要求各个网络具有统一的网络体系结构，并遵循开放式标准，以实现“网与网互联”。由此，两种国际通用的最重要的体系结构应运而生，即TCP/IP体系结构和国际标准化组织的OSI体系结构。

第四阶段，互联网络和高速计算机网络。进入20世纪90年代，因特网的形成促使计算机网络技术和网络应用迅猛发展，各种类型的网络全面互联，并向宽带化、高速化、智能化方向发展。以下一代互联网为中心的新一代网络成为新的技术热点，目前IPv6技术的研究和发展成为构建高性能的下一代网络的基础工作。网络互联和高速计算机网络正成为最新一代计算机网络的发展方向。

2. 因特网（Internet）的发展历程

因特网起源于20世纪60年代，TCP/IP协议为它的发展奠定了基础，20世纪90年代的商业化应用促进它的飞跃。世界各地无数企业和个人纷纷加入，成就了今天的因特网。因特网的发展可以分为以下几个阶段：

第一阶段，从单一的ARPAnet发展为互联网。 ARPAnet只是一个单个的分组交换网，人们意识到不可能仅使用一个单一的网络来解决所有的通信问题。美国高级研究计划署（ARPA）开始研究多种网络的互联技术，于是出现了互联网。1983年TCP/IP协议成为ARPAnet上的标准协议，使得所有使用TCP/IP协议的计算机都能利用互联网相互通信，因而人们把1983年定为因特网的诞生时间。

第二阶段，建成三级结构的因特网。 1985年，美国国家科学基金会（NSF）建立了国家科学基金网NSFNET。它是一个三级计算机网络，分为主干网、地区网和校园网。这种三级计算机网络覆盖了美国主要的大学和研究所，并成为因特网的主要组成部分。1992年因特网上的主机超过100万台，1993 年因特网主干网的传输速率提高到 45Mb/s。

第三阶段，形成多层次ISP结构的因特网。从1993年开始，因特网服务提供商ISP出现，用户通过因特网服务提供商ISP上网。1994 年起，因特网逐渐演变成多层次ISP结构的网络。现在，因特网已经发展成全世界无数ISP所共同拥有的网络。

3. 移动互联网

随着计算机网络技术和移动通信技术的进一步融合，尤其是像移动互联网等一些新型网络技术和网络服务的发展，计算机网络技术正面临一次新的理论发展和技术革新，开放

化、集成化、高性能化的趋势越来越明显，其发展和应用有着光明的未来。

移动互联网不同于传统意义的网络，它是移动通信技术和互联网技术二者结合的产物。只要在移动网络信号的覆盖范围内，用户就可以通过手机等智能终端连接到公共网络。

移动互联网的个人业务包括移动支付、位置服务、移动社交、在线游戏、文件下载等业务。移动互联网具有可识别、便携等特点，使其支持的服务朝着更个性化和定制化的方向发展，新闻阅读、视频节目、电商购物、公交出行等热门应用都出现在移动终端上，移动用户规模更是超过了PC用户。

企业级用户的进入加快了移动应用市场的发展。一方面，传统互联网企业已经开始运用移动互联网技术和概念拓展新业务和方向，HTML5、多平台/多架构应用开发工具、可穿戴设备、高精度移动定位技术等都推动了移动互联网的发展。另一方面，移动互联网行业正在向传统产业加速渗透。传统制造企业正在积极拥抱移动互联网，深化移动互联网在企业各环节的应用，着力推动企业转型升级。

4. 物联网

物联网（Internet of Things，简称IoT）就是“物物相连的互联网”。它是通过射频识别（RFID）、传感器、全球定位系统、激光扫描器等信息传感设备，按约定的协议，把任何物体与互联网相连接，进行信息交换和通信，以实现对物体的智能化识别、定位、跟踪、监控和管理。

图1.1.1　物联网的发展

物联网是在互联网的基础上延伸和扩展的网络。先进的硬件设计制造技术及互联网为物联网的发展奠定了基础。目前，很多国家已经开始在工业、农业、军事、医疗、环境监测、建筑、空间和海洋探索等领域开展物联网应用的实践，全球物联网市场规模增长迅速，如图1.1.1所示。

随着“物联网十二五发展规划”“中国制造2025”等政策的提出，物联网的发展已经成为国家层面技术及产业创新的重点方向。我国目前在物联网应用中的工业、医疗、交通、金融以及安防等方面都取得了一定的成果。以智能交通为例，虽然智能交通产业在我国还处于起步阶段，但智能交通系统（ITS）作为新的经济增长点和交通系统建设的必然选择，已受到国家相关部门的高度重视。

问题与讨论

为了增强校园安全管理，实验室、财务室等场所设置了门禁系统，必须通过刷卡或刷脸方可进入，这都是物联网技术的应用。请分析讨论，除此之外还有哪些措施是通过物联网技术来提升校园安全系数的。

1.1.3 互联网在中国

中国互联网的产生虽然比较晚，但是经过几十年的发展，中国互联网已经成为国际互联网的重要组成部分，并且拥有最大的互联网用户群体，许多互联网应用服务已经走在世界前列。

20世纪80年代中期，中国的科技人员了解到国外采用电子邮件互相交流信息，十分方便、快捷，一些机构单位便开始研究。1987年9月，中国学术网（CANET）在北京计算机应用技术研究所内建成中国第一个国际互联网电子邮件节点，并于9月14日发出了中国第一封电子邮件："Across the Great Wall we can reach every corner in the world（越过长城，走向世界）"，由此揭开了中国人使用互联网的序幕。

1996年，中国公用计算机互联网（CHINANET）的诞生标志着中国的互联网用户从科技教育界转向其他行业，从而拉开了全民使用互联网的序幕，为中国互联网的发展奠定了坚实的基础。随着四大互联网主干网（中国公用计算机互联网CHINANET、中国科学技术网CSTNET、中国教育和科研计算机网CERNET、金桥信息网CHINAGBN）的建设与互联互通，互联网在中国飞速发展，开启了铺设中国信息高速公路的发展历程，也开启了中国互联网的商用化阶段。

1997年，中国的三家互联网公司（搜狐、网易、新浪）引领了中国互联网的第一波浪潮，先后在美国股市上市，奠定了中国的三大门户网站的重要地位。1998年，腾讯将"人"和"人"进行了连接；1999年，阿里巴巴将"人"和"商品"进行了连接；2000年，百度将"人"和"信息"进行了连接，形成了中国互联网的三足鼎立之势。之后，中国网民开始成几何级数增长，截至2017年底，我国网民规模达到7.72亿，其中手机网民规模占97.5%，互联网普及率为55.8%。通过图1.1.2可以明显看出我国互联网普及率的增长趋势。

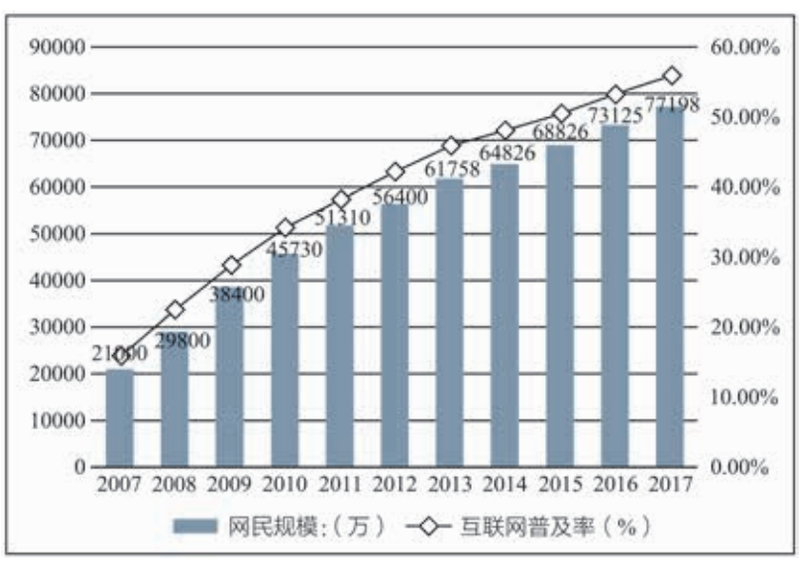


图1.1.2 2007—2017年中国网民总规模及互联网普及率走势

2017年，在全球各大市场中，中国的电商增长最快，占全国社会商品零售总额的15%，而美国仅占10%左右。根据艾瑞咨询集团的数据显示，中国移动支付规模远超出其

他国家，超市、餐馆、商场及线下交易正全面被移动支付占领，普及率和渗透率遥遥领先。现在中国的互联网产业和美国并驾齐驱，已经成为世界公认的互联网强国。

实践与体验

体验网络预订服务

当前，许多网络平台打出了“吃喝玩乐全都有”的口号。网络预订服务由于其独有的便捷性和直观性，已经迅速被人们认同接受。如图1.1.3，人们可以通过网站所提供的服务信息方便快捷地完成网上预订和支付。

图1.1.3　网络预订服务

实践内容：

1. 选择合适平台注册账号。
2. 体验并分析网络预订服务的流程。

实践步骤：

1. 选择一个网络预订平台（比如携程、美团、网易公开课等）。

2. 利用计算机或者智能终端（手机、Pad等）在该平台注册可用账号，已有账号的同学可跳过该步骤。

3. 体验网站提供的各种服务（点餐、订门票、订酒店、订网络课程等）。分

析用户从查询到预订成功需要经历哪些流程、提供哪些必要个人信息，并填表记录。

记录各个环节需要提供的个人信息（选填）						
	注册	订餐	订车票	订酒店	订景点门票	订网络课程
1						
2						
3						
4						

思考与练习

1. 请分析学校一卡通系统的网络构成，并完成下表。

组成部分	具体对应设备	功能
计算机系统		
数据通信系统		
网络软件及协议		

2. 利用思维导图软件制作网络发展历程图例。

1.2 网络的分类

在网络应用范围越来越广泛的今天，各种各样的网络越来越多，对网络进行分类，可以让我们了解计算机网络的类型及其特征，是熟悉计算机网络技术的重要方法之一。

1.2.1 计算机网络分类

计算机网络可以根据作用范围、传输技术、拓扑结构、交换方式等来分类。根据作用范围划分是一种普遍认可的通用网络划分标准，按这种标准可以把网络划分为局域网、城域网和广域网。

局域网（Local Area Network，简称LAN）可以将较小范围内（如一个办公室、一幢大楼，一个单位等）的各种终端互联成网，如图1.2.1所示。局域网可实现文件管理、软件共享、打印机共享、电子邮件和传真通信等功能。局域网根据传输介质可以分为有线局域网和无线局域网两种。局域网技术发展迅速，应用日益广泛，小到家庭中的几台设备，大到上万台计算机设备，都可以组成局域网。

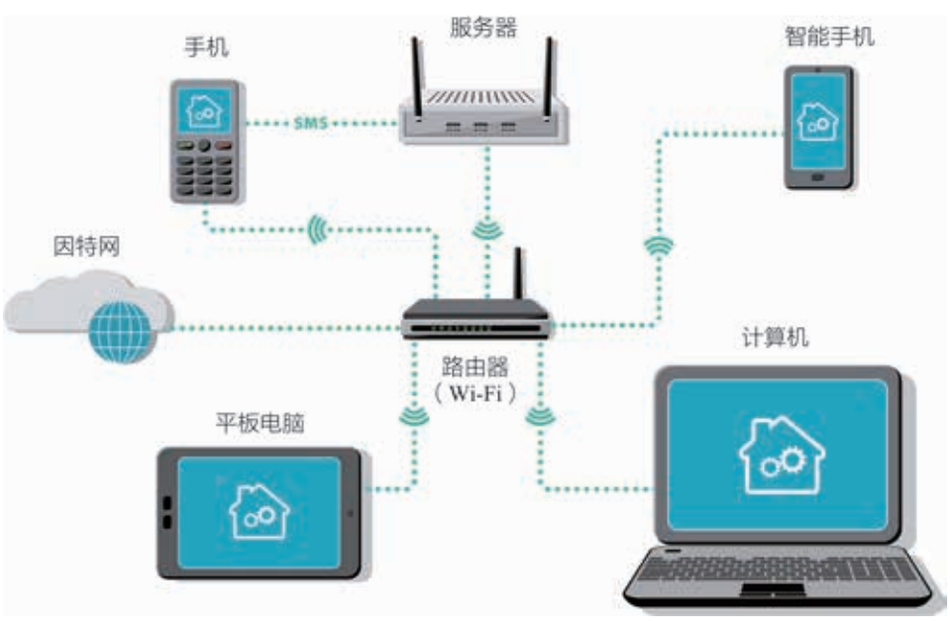


图1.2.1　局域网

城域网（Metropolitan Area Network，简称MAN）是在一个城市几十千米范围内所建立的计算机通信网，传输媒介主要采用光纤，并采用有源交换元件的局域网技术，网中传输时延较小，传输速率较高，如图1.2.2所示。城域网的一个重要用途是用作骨干网，通过它将位于同一城市内不同地点的服务器、主机及局域网等互相连接起来。

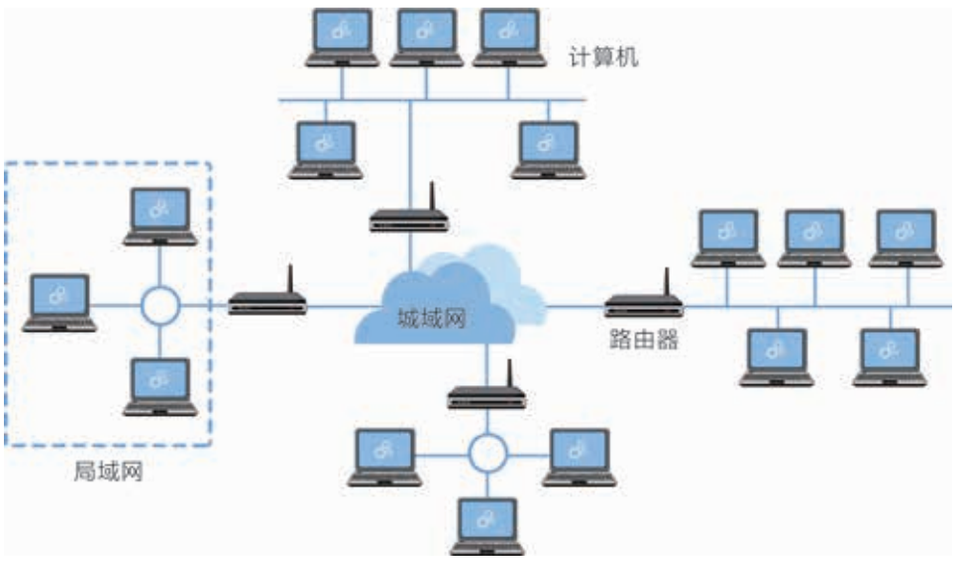


图1.2.2　城域网

广域网（Wide Area Network，简称WAN）覆盖的范围比局域网和城域网都广，其覆盖范围从几十千米到几千千米，能连接多个城市或国家，甚至横跨几个洲提供远距离通信，形成国际性的远程网络，如图1.2.3所示。广域网可以利用公用分组交换网、卫星通信网和无线分组交换网，将分布在不同地区的局域网或计算机系统互联起来，达到资源共享的目的。因特网是世界范围内最大的广域网。

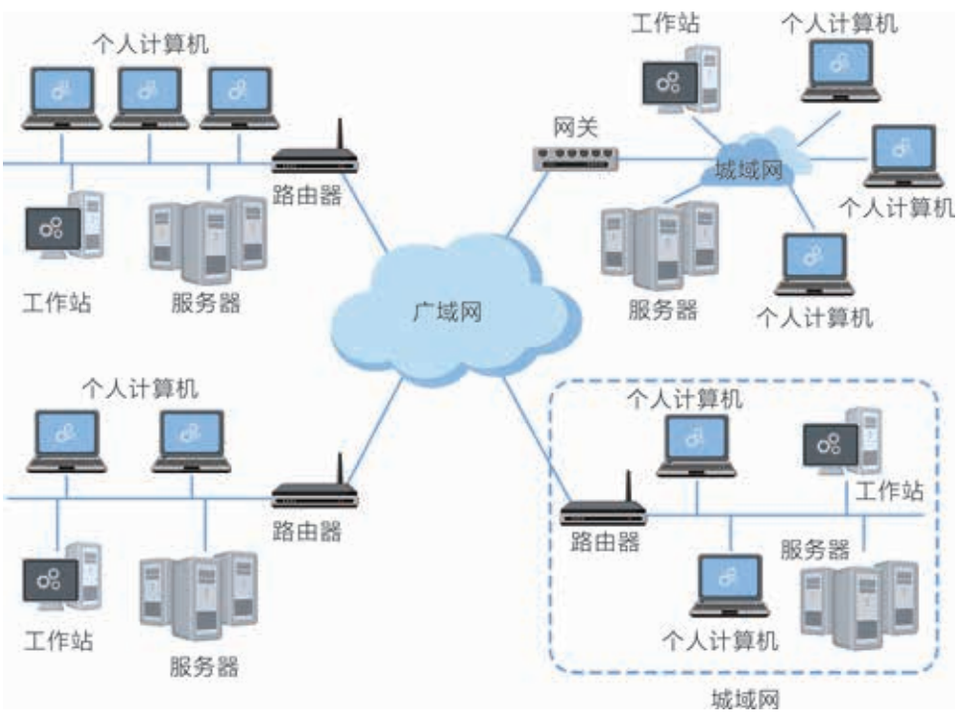


图1.2.3　广域网

依据不同的传输技术，相应的计算机网络又可以分为广播式网络和点对点式网络；依据不同的拓扑结构，可以分成总线型结构、环型结构、星型结构等；而依据不同的交换方

式，又可以分成线路交换网络、报文交换网络、分组交换网络等；依据不同的使用者来分，还可以将网络分成公用网络和专用网络。

1.2.2 三网与三网融合

三网指的是互联网、电信网和广播电视网。它们在人们生活中随处可见。2006年3月，《国民经济和社会发展第十一个五年规划纲要》提出推进电信网、广播电视网和互联网三网融合，构建下一代互联网，加快商业化应用。

互联网是网络与网络之间互联所形成的庞大网络，这些网络以一组通用的协议相连，形成逻辑上的单一巨大国际网络。这种将计算机网络互相连接在一起的方法可称作“网络互联”，在这基础上发展出的全球性互联网络称互联网。

电信网（Telecommunication Network）是构成多用户相互通信的多个电信系统互连的通信体系，是人类实现远距离通信的重要基础设施，它利用电缆、无线、光纤或者其他电磁系统，传送、发射和接收标识、文字、图像、声音等信号。电信网由终端设备、传输链路和交换设备三要素构成。目前我国主要有中国电信、中国移动、中国联通等运营商。

广播电视网（Cable Television，CATV）是利用光缆或同轴电缆来传送广播电视信号的网络。它具有频带宽、容量大、功能多、成本低、抗干扰能力强、支持多种业务等特点。同时，由于其免去了铺设线缆的麻烦，只需要在用户端增加设备即可访问网络，极大地促进了网络的普及。

“三网融合”又叫“三网合一”。通过技术改造，使得三网的技术功能趋于一致，业务范围趋于相同，三网互联互通、资源共享，三者之间相互交叉，你中有我，我中有你。三网融合并不意味着三大网络的物理合一，而主要是指业务应用的融合。融合应用广泛，遍及政府工作、公共安全、环境保护、智能交通、平安家居等多个领域。

交互式网络电视（Internet Protocol Television，IPTV）是“三网融合”的典型应用，如图1.2.4所示。它有效地利用网络资源，集互联网、多媒体、通信、广播电视及下一代网络等基本技术于一体，提供各种数字媒体交互型业务，实现宽带IP多媒体信息服务，它将成为未来家庭娱乐的核心。

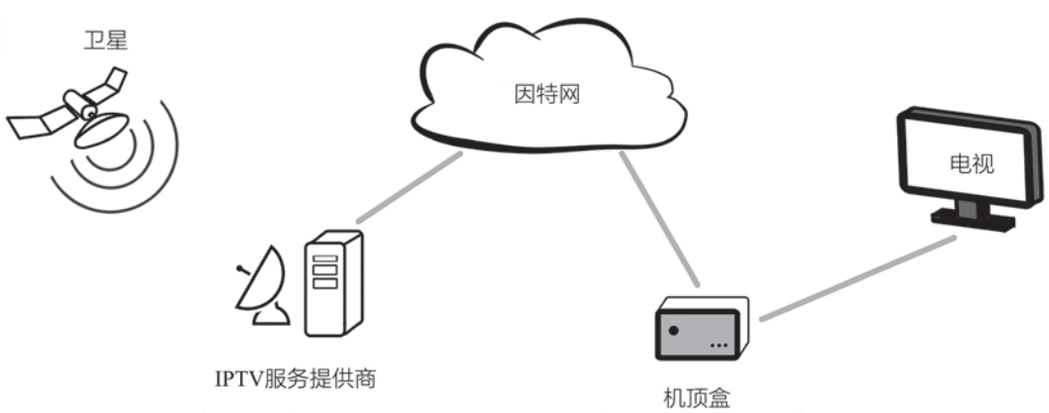


图1.2.4 IPTV

问题与讨论

随着第五代移动通信技术（5G）的出现，5G网络的理论下行速度为10Gb/s（相当于下载速度1.25GB/s），届时5G网络将怎样改变我们的世界？

思考与练习

1. 将你所在学校的计算机网络按照作用范围分类。
2. 思考并描述IPTV与普通有线电视或网络视频资源的区别。

1.3 网络与社会

互联网不仅大大提高了人类对数据收集、存储、处理的能力和效率，更重要的是改变了人们的思维方式。进入基于互联网的大数据时代后，人们不再依赖抽样分析法进行研究和决策，可以直接利用全样本的大数据，充分挖掘数据之间、事件之间的关联，发现更多以前从未意识到的各事物之间的联系。

1.3.1 网络对社会的影响是全方位的

网络从个人行为、社会交往、文化市场、社会制度和国际关系等层面影响了文化的发展；它促使科学技术的创新和生产技术的进步，推动生产方式发生变革；它渗透到了社会的各个行业领域，形成了网络虚拟社会。

1. 改变了人类的社会文化

互联网呈网状结构，没有中心节点，也不是一个层级结构，虽然不同的点有不同的权重，但没有一个点是绝对的权威。这种技术结构决定了它内在的精神是分布式的，是平等的。

互联网涵盖了个人行为、社会交往、文化市场、社会制度及国际关系这五个层面的文化元素。

在个人行为层面，它促使人们的行为方式与价值观念发生了深刻的革命，使得人们对于许多事物的认识得以扩展与深化，同时也使人们认识到，以往被视为确定的、理所当然的东西都是可以被质疑的，是可以被赋予不同的角色与含义的。在个人行为层面重要的影响是自我重塑，自我重塑的意义在于解放思想，这是互联网文化创新的内在原动力。

在社会交往层面，互联网的开放性赋予了社会弱势群体平等地传播信息、表达观点的权利，反映了社会文化形态与文化思潮多元化的现实，有利于社会文化朝着更加丰富多彩的方向发展。

在文化市场层面，互联网的出现大大促进了文化的传播与发展，也促进了文化市场的繁荣。互联网的传播模式简化了文化流通的环节、拓宽了文化流通的渠道，也打破了传统文化流通的等级观念、时空界限，使每个人都可以快捷方便地获取文化信息。

在社会制度层面，互联网有自己的规范，这既是网络交往的根本保障，更是互联网文化构建的基本条件。不仅要在制度文化层面创新一些行为规则和礼仪，更要在精神文化层面促进个人与群体、权利与责任等价值观念的有机结合。

在国际关系层面，由于互联网对外开放且对内平等的特性，决定了它终究不可能为某

一个国家、某一种文化所独占。随着互联网在全世界的普及，各个民族、各个国家都会在互联网上找到适合自身的文化发展空间，各种文化彼此沟通，相互交流，共同发展，形成一种和而不同的世界文化新格局。

2. 促使生产方式发生改变

互联网促进了科学技术的创新及生产技术的进步，加快了产品更新换代的速度。随着互联网技术的普及应用，传统的生产组织形式逐渐暴露出效率低下、反应滞后等缺陷，随之产生了适应信息化要求的网络化生产组织形式，使原本独立的经济体通过互补协作、相互关联，实现了共赢。网络通过改变劳动方式，打破了信息资源的界限，加强了社会分工的专业化程度，推动了生产方式的变革。

互联网的发展影响了实体经济，让传统商业、传媒业、金融业和教育业发生了重大改变。传统行业的互联网化是大势所趋，特别是在如何服务消费者、如何获得更多的用户、如何在竞争中发展等方面，互联网提供了许多全新的解决方案。

将互联网的创新成果深度融合于经济社会的各领域之中，可以充分发挥出互联网在生产要素配置中的优化和集成作用。“互联网＋”是互联网思维的进一步实践成果，它推动了知识社会的用户创新、开放创新、大众创新、协同创新，改变了人们的生产、工作和生活方式，也引领了创新驱动发展的“新常态”。

3. 形成了新的社会形态——虚拟社会

虚拟社会是指不同的人经由互联网相互连接以进行信息共享、互动交流，并在其中进行社会交往、社会活动而形成的一种亚社会性质的网络虚拟空间。它是随着计算机网络遍布各个行业而产生的一种新的社会形态。虚拟社会由符号化或数据化了的人和社会群体组成，成员之间的互动原则是自由、平等、民主、自治和共享。它克服了时间和空间的障碍，将信息从传统的地域限制中解放出来，使现实世界与虚拟社会紧密地联系起来，人与人之间的距离缩短，彼此之间仅相距几个超链接，如图 1.3.1 所示。

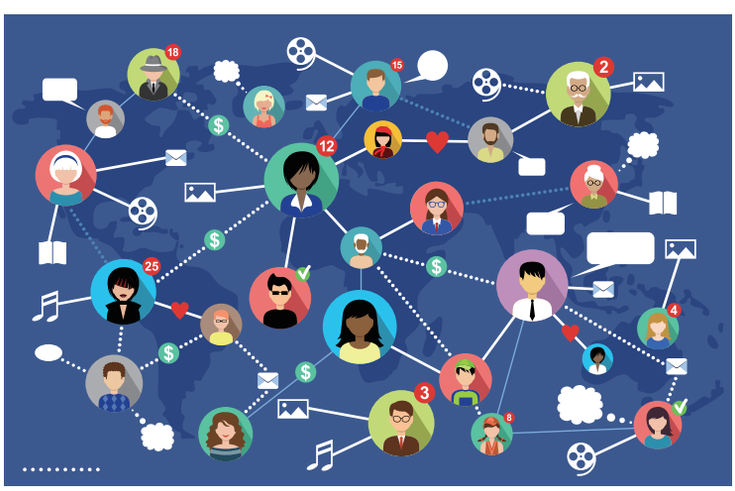


图1.3.1　虚拟社会

虚拟社会形成和发展的客观基础是现实社会。从构成要素来看，无论是人还是互动交往所依靠的人类创造物，都来源于现实社会，所以虚拟社会并不是凭空出现的，也不是存在于人们的思想意识中的，而是一个看得见、感受得到、体验得到的社会。人与人在虚拟社会中所建构的各种联系和关系本身是现实社会的一部分，是现实社会在虚拟社会中的反映。

虚拟社会对现实社会具有一定的反作用。在虚拟社会中形成的生活方式、思维方式等影响着现实社会中人们的工作和生活方式，越来越呈现出虚拟社会与现实社会的趋同化，进而影响到政治、经济、文化等各个领域。虚拟社会已成为一种来源于现实社会，又反作用于现实社会的力量。

问题与讨论

1. 讨论互联网企业（如阿里巴巴集团、百度公司、腾讯公司等）的出现与发展对社会的影响。

2. 随着电商和微商的快速发展，实体店受到了非常大的冲击，实体店会消失吗？实体店应该如何面对电商和微商带来的影响？

1.3.2 网络对社会的影响是深刻的

网络技术的发展，在许多领域产生了革命性的成果，拓展了人们的认知范围，并改写与重塑了人们思维认识的方方面面。

1. 实现即时交流

随着互联网的覆盖范围迅速扩大、网络应用的迅速普及，新的应用层出不穷。论坛、电子邮件和即时通信成为互联网的三大基础应用。

（1）论坛

论坛已经成为网民表达个人情感、观点和诉求的重要平台。通过论坛的方式，网民们可以在不违反相关法律、法规的前提下针对各种各样的事物发表自己的意见和观点，并和他人进行交流。

（2）电子邮件

电子邮件是互联网应用最广的服务之一，通过电子邮件系统，用户可以免费与世界上任何一个角落的网络用户即时通信。绝大部分网民恐怕早已记不起“鸿雁传书”的感觉了，电子邮件以其快速、便捷、免费等特性已然成为网民们通信的主要方式之一，极大地改变了人们的交流方式。

（3）即时通信

除了电子邮件，另外一个重要的网络通信应用——即时通信，更是成为网民们通信和交流的首选。即时通信工具，包括QQ、微信、钉钉等，可以让远隔重洋的人们通过文字、语音或者视频进行实时的交流，相比电话等传统通信工具，即时通信工具有着方便、多样化和廉价等优势。

2. 改变了人们获取信息的方式

搜索引擎是人们获取信息的最常用的工具之一。互联网极大地丰富了人们获取信息的途径、扩展了人们搜索信息的范围，但同时其过分庞大的信息量也使得用户难以从海量信息中获取有用数据。搜索引擎是一种智能的、高效的工具，帮助人们在互联网巨大的信息库中搜索出有用的内容，使得互联网储存的海量信息能真正服务用户。小到生活点滴，大到国计民生，搜索引擎的内容无所不包。有了搜索引擎，互联网俨然已成为网民生活中的百科全书。

3. 开启了新经济时代

随着移动互联网的飞速发展，移动支付快速进入人们的日常生活中，二维码、NFC等支付方式都在不断地扩展自己的市场占有率。移动支付的发展不仅让支付更便捷，也促进了网络购物、共享单车等业务的快速发展。移动支付、远程认证、生物识别等技术正在改变人们的消费和生活习惯。购物、发红包、理财、资金转账、充值缴费等，移动支付随时、随地、随身的特点给人们的生活带来了更多的便捷，越来越多的人出门已经不需要携带钱包，只需要拿上手机就能轻松支付。在深刻改变人们生活的同时，移动支付也走进了公共服务领域，帮助提高政府公共服务的效率和质量，让群众至少在缴费环节少跑腿、少排队，甚至一次都不用跑。

思考与练习

1. 列举网络改变生活的例子。
2. 思考青少年网络成瘾的应对策略。

1.4 “互联网＋”

“互联网＋”就是“互联网＋传统行业”，但这并不是简单的两者相加，而是利用信息技术以及互联网平台，让互联网与传统行业深度融合，创造新的发展生态。

“互联网＋”是互联网的创新成果与经济社会各领域的深度融合，它可以推动技术进步、效率提升和组织变革，提升实体经济创新力和生产力，形成更广泛的以互联网为基础设施和创新要素的经济社会发展新形态。

1.4.1 “互联网＋”概述

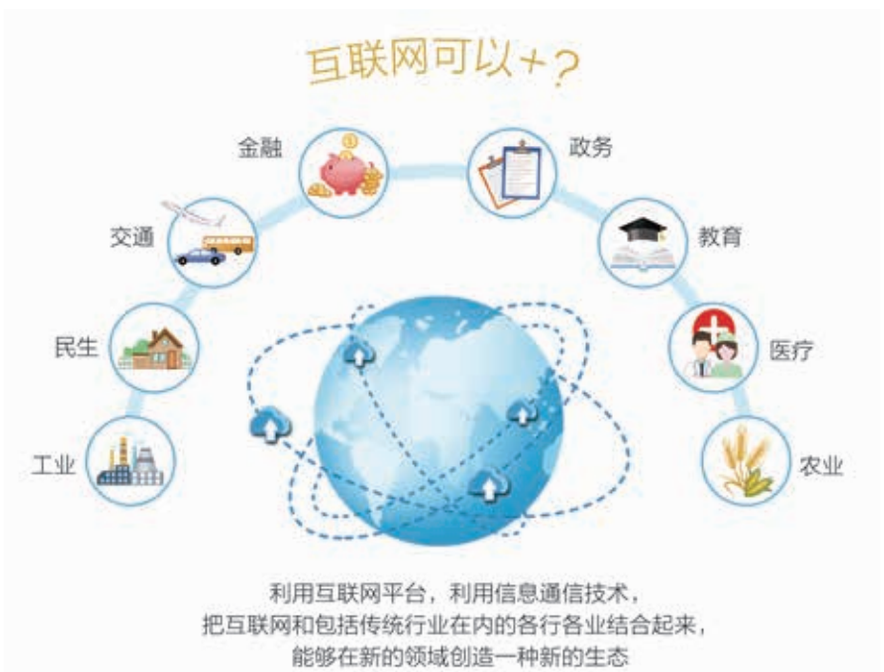


图1.4.1 “互联网＋”的一些应用领域

2015年3月5日，我国提出“‘互联网＋’行动”计划，到7月4日正式发布《国务院关于积极推进“互联网＋”行动的指导意见》，前后不到4个月时间。这4个月，“互联网＋”热潮席卷我国大江南北，几乎成为每一个人耳熟能详、津津乐道的话题。图1.4.1列出了目前“互联网＋”的一些应用领域。

“互联网＋”具体可分为两个层次。一方面，“＋”代表着添加、联合，这表明了“互联网＋”的应用范围为互联网与传统产业，针对互联网与传统产业进行联合和深入融合；另一方面，是通过传统产业的互联网化完成产业升级。在传统产业中运用开放、平等、互动等网络特性，并通过大数据的分析与整合，理清供求关系，改造传统产业的生产方式、产业结构，增强经济发展动力，提升效益，从而促进国民经济健康有序发展。

1.4.2 “互联网＋”特征

理解“互联网＋”，除了要知道它的本质是什么，要研究“互联网＋”和时代之间有怎样的关系，还要了解“互联网＋”的六大核心特征。

1. 跨界融合

“＋”代表跨界，意味着变革与开放、重塑与融合。敢于跨界，创新的基础就更坚实；融合协同，群体智能才会实现，从研发到产业化的路径才会更畅通。融合本身也指代身份的融合，客户消费转化为投资，伙伴参与创新等。

互联网已经与很多行业融合。互联网＋传统商场，出现了淘宝与京东等网络购物平台；互联网＋传统交通，出现了滴滴打车和美团打车等网约车平台；互联网＋传统银行，出现了支付宝等电子理财平台；互联网＋通信，出现了微信、QQ等即时通信工具。互联网思维的落地必须依靠实体企业，而传统企业也需要吸收互联网的创新思想实现转型升级。只有双方不断融合，才能发挥出更大的优势。

2. 创新驱动

“互联网＋”促进产业形态创新。随着互联网技术的发展，云计算、大数据、物联网等新技术不断融入传统产业，出现了互联网电商、互联网金融、互联网医疗、互联网教育等新的产业形态，并促进传统制造业、服务业甚至农业进行创新升级，从而促进经济结构调整，增强经济活力，实现经济有效益、有质量、可持续的增长。

2014年，我国提出“中国制造2025”，这是政府实施制造强国战略的第一个十年行动纲领。“中国制造2025”的总体思路是以促进制造业创新发展为主题，促进产业升级，实现制造业由大变强的历史跨越。“互联网＋”概念与“中国制造2025”的结合，符合当前互联网科技发展的趋势，有利于新兴产业的发展，将促进企业创新，提高市场效率。

3. 重塑结构

信息革命、全球化、互联网已经打破了原有的社会结构、经济结构、地缘结构、文化结构。结构被重塑的同时带来了很多要素的转变，比如关系、权力、连接、规则和对话方式等。

以“互联网＋”重塑现代农业产业体系为例。运用互联网技术对农业生产进行实时监测与精准管理，可以实现控制风险、提高产量及提升农产品品质。分散的小规模农户通过在线互联管理实现规模聚集，通过集体采购、集团营销、集约服务等手段来节约成本。通过全程互联强化品质控制，促进转型升级。农业生产过程周期长、难以控制的因素多，传统农户不具备标准化生产的管控能力，生产者没有动力去改进生产。农产品电商采取了产地直采、垂直整合、供应商扶持等多种方式利用信息技术加强全过程管理，保障产品品

质，成为推动我国农产品标准化和品质提升的重要力量。

4. 尊重人性

人性的光辉是推动科技进步、经济增长、社会进步、文化繁荣的重要力量，互联网之所以能够迅速深入人们的生活，是因为它有着对人性的最大限度的尊重、对人的体验的敬畏、对人的创造性发挥的重视。

“互联网＋”体现了以人为本的理念。例如分享经济，是透视人性、尊重人性的产物，这也是它的魅力和活力所在。传统的行业要转型和升级，最根本的出发点也都基于人性。

5. 开放生态

生态是“互联网＋”非常重要的特征，而生态本身就是开放的。推进“互联网＋”的一个重要的方向就是要化解过去制约创新的环节，打穿孤岛式创新的隔阂，让研发由人性决定的市场驱动，让创业者有机会实现自身的价值。

“互联网＋”行动计划的核心是生态计划，要重塑教育生态、创新生态、协作生态、创业生态、虚拟空间生态，优化资源配置机制、价值实现机制和价值分配规则。

6. 连接一切

互联网的本质就是连接。人与人的连接让我们更亲近，人与物的连接让我们更方便，物与物的连接让我们的生活更智能。

“互联网＋”构建了连接一切的新生态，推动产业转型升级，并不断创造出新产品、新业务与新模式。例如微信公众号平台可以整合多项民生服务功能，把政府政务服务大厅建在智能手机上，推动“智慧城市”的建设。

如今的互联网已经对传统行业产生了强烈的冲击，网络购物冲击了传统零售行业、互联网理财对银行产生了影响、互联网打车不断吞噬出租车行业的市场份额……各行各业都在思考如何添加互联网元素，找到企业发展的新方向。

在“全民创业”时代，越来越多的项目诞生时就是“互联网＋”的形态，不需要像传统企业一样转型与升级。“互联网＋”促进了更多的互联网创业项目的诞生，无需再耗费更多的人力、物力及财力去研究与实施行业转型。可以说，每一个社会及商业阶段都有一个常态以及发展趋势，

拓展链接

分享经济

分享经济（Sharing Economy）是指将社会中海量、分散的闲置资源，平台化、协同化地集聚并再分配，从而实现经济与社会价值创新的新形态。分享经济强调的两个核心理念分别是“使用而不占有”（Access over Ownership）和“不使用即浪费”（Value Unused is Waste）。

“互联网＋”提出之前的常态是千万企业需要转型升级的大背景，后面的发展趋势则是大量“互联网＋”企业的涌现以及传统企业的“破与立”。

1.4.3 “互联网＋”应用

我国积极推进“互联网＋”行动计划，该行动计划既涵盖了制造业、农业、金融、能源等具体产业，也涉及环境、养老、教育、医疗等与百姓生活息息相关的方方面面。

1.“互联网＋教育”

一所学校、一间教室、一位老师，这是传统教育；互联网、移动终端，几百万学生，学校任你挑、老师由你选，这是“互联网＋教育”。“互联网＋教育”，从教学手段、教学方法、教学过程到教学内容，乃至教育观念和教育目的都发生了深刻变革。教与学围绕互联网进行，教师在互联网上教，学生在互联网上学，数据在互联网上流动，知识在互联网上成型，线下的活动成为线上活动的补充与拓展，如图1.4.2所示。

图1.4.2 “互联网＋教育”应用

随着移动互联网相关技术的快速发展，“互联网＋教育”呈现出多形态的创新，已不再是依赖线下教育的资源分享平台，并正在改变传统教育以教学权威为核心的教育模式，进入了具有用户原创内容、自主学习、互动游戏等特点的新模式。

“互联网＋教育”有下面几个特征：

教育资源从封闭到开放。传统模式下，教育资源局限于课堂、图书馆、实验室等场所，满足有限人群的需求。而互联网以其存储和交互方面的优势，在短时间内迅速吸纳了海量的知识和信息，成为人类历史上前所未有的巨大“信息库”，并且这个信息库还在源源不断地扩容。借助互联网，教育资源可以走出校园，覆盖到世界每个角落，使得人们能够共享优质的教育资源。

教育机构从单一到多元。社会教育机构、新型教育组织，借助“互联网＋”对教育资源重新配置和整合，依靠灵活、免费等优势给学校教育带来了强烈冲击，教育组织形态呈现多元化的趋势。

学习从被动到自主。传统模式下，学习者必须按照学校的课程安排到教室听课，而在互联网环境下，学习成为无时不可、无地不可的事情，只要连接网络就可以学习，不再依赖课堂和书本，真正实现了时空上的自由。

教学过程互动环节明显增加。互联网改变了传统的授课模式，学生对教师授课的依赖性明显减弱，教师从教学的主导者变成学生学习的辅助者、服务者，教学向更加注重互动对话的“翻转课堂”转变。

“互联网＋教育”实现了知识学习的生活化。所谓学习的生活化，就是在生活中学习，用户在任何时间点都能学习。这种学习不再是一种被排除在生活时间之外的额外学习，而成为日常生活的有机组成部分。

2.“互联网＋医疗健康”

2018年4月，国务院出台《关于促进“互联网＋医疗健康”发展的意见》，确定发展“互联网＋医疗健康”措施，强调加快发展“互联网＋医疗健康”，缓解看病就医难题，提升人民健康水平。

智慧医疗有效解决了“看病难”与“就医烦”的问题。借助“互联网＋”应用，医院拓展了医疗服务的时间和空间，提高了医疗服务供给与需求的匹配度。以挂号难为例，很多医院不仅开发了专用APP，还加入了卫生健康行政部门搭建的预约挂号平台，如图1.4.3所示，把医院的号源放在号池里，患者通过互联网、手机、电话就可以挂号。另外，患者可以在线完成候诊、缴费、报告查阅等多个环节，大大节省了精力。

图1.4.3　手机端网上预约挂号

跨时空均衡配置医疗资源。利用“互联网＋”把医疗资源配置到一些匮乏的地区，特别是一些偏远地区、中西部地区和农村地区，在一定程度上改变了资源不均衡的情况。例如通过建立互联网医院，把大医院与基层医院、专科医院与全科医生连接起来，帮助老百姓在家门口及时享受优质的医疗服务。针对基层优质医疗资源不足的问题，通过搭建互联网信息平台，开展远程会诊、远程影像诊断等服务，促进检查检验结果实时查阅。借助人工智能等技术，面向基层开展预约诊疗、远程医疗等服务，帮助缓解老百姓看病难问题。

建立大健康管理模式，实现“我的健康我能管”。在“互联网＋”的助力下，健康管理正逐步迈向个性化、精确化。通过建立物联网数据采集平台，居民可通过智能手机、平板电脑、腕表等移动设备，全面记录个人的运动、生理数据。通过建立健康管理平台，依托

网站、手机客户端等载体，家庭医生可随时与签约患者交流，为签约居民提供在线健康咨询、预约转诊、慢性病随访、延伸处方等服务，真正发挥家庭医生的健康“守门人”作用。

问题与讨论

1. 讨论“互联网＋人工智能”将会在哪些层面改变社会。
2. “互联网＋金融”的发展，给你的学习和生活提供了哪些便利？

实践与体验

体验“互联网＋交通”

“互联网+交通”利用互联网技术解决城市交通的诸多问题，提高了市民的出行效率。人们可以通过各种地图网站或APP、打车软件等，根据各自的需求来选择交通工具、规划出行路线，如图1.4.4。

图1.4.4　百度地图与高德地图

实践内容：

利用地图网站或手机APP规划一条出游线路，并在网站或APP中切换公交、步行或打车等方案，比较其异同。

实践步骤：

1. 用搜索引擎搜索各种地图软件（百度地图、高德地图、凯立德地图等），或在手机中安装相应的APP。

2. 选择路线功能并输入起点和终点。

3. 比较系统提供的驾车、公交、步行、打车等方案，说说哪种最经济、哪种最快捷、哪种最方便。

4. 查看道路拥堵情况，记录目前哪一段路最拥堵。

结果呈现：

条目	结果
地图平台的域名及网址	
你选择的起点、终点以及出行方式（驾车、公交、步行、打车）	
系统提供的方案中，哪个方案最适合你？写出具体方案	
查看道路拥堵情况，记录目前哪一段最拥堵	
该平台还提供了哪些服务	

思考与练习

1. 移动互联网、大数据在“互联网＋”中起到了什么作用？

2. “互联网＋教育”突出了哪些技术的应用（如移动互联网、大数据等）？

巩固与提高

1. 互联网具有传播快捷和高效的特点。“互联网＋教育”实现了学习的泛在化，人们产生学习需求时就能立即学习。如同学们打算利用假期向“舞林高手”小田学习舞蹈，但学习时间很难统一，于是小田决定利用互联网平台进行教学辅导。他具体该怎样实现？需要的设备和技术支持有哪些？

2. 移动支付，就是允许用户使用其智能移动终端（通常是手机）对所消费的服务或商品进行账务支付的一种服务方式。移动支付需要网络的支持，人们需要在不同的情境中考虑选择使用不同的网络。试分析不同的环境中，该如何从有线网络、Wi-Fi无线网络、移动网络（中国电信、中国移动、中国联通）中选择合适的网络？说明理由。

3. 据统计，2017年全球互联网用户数已超34亿，同比增长10%，互联网全球渗透率达到46%。请查阅资料并预测至2050年，全球互联网用户数可以达到多少。你的结论是什么？请说明理由。

项目挑战

分析网络发展现状，展望未来网络

目前，计算机网络已经深入人们的工作、学习生活中，但网络中也存在各种问题。结合实际分析网络发展的现状，指出目前存在哪些问题并思考解决策略，展望未来网络的发展。

项目任务

请以小组的形式完成调查分析报告来阐述你的结论。

过程与建议

要完成这项挑战任务，你必须查阅资料并分析目前网络存在的各种问题，有哪些新技术可能能解决这些问题。

1. 调查分析网络发展现状，发现目前网络存在的问题

分析时要关注以下问题：（1）非人为因素引发的问题。（2）人为因素引发的问题。（3）其他类型的问题。

2. 通过查阅资料并展开讨论

以上问题是否已有应对的技术？如果没有，讨论可能会有哪些相应的新技术。

	存在的问题	已有或可能会有的技术	未来的网络特征
非人为因素	例：信息数据中心因自然灾害等因素损毁	多重数据存储，异地备份	
人为因素	例：黑客	量子通信	
其他	例：传输速率低		

3. 整理

按照调查分析结果，整理出一篇调查分析报告。其中应该包括如下内容：（1）分析调

查的目的和团队的分工情况。（2）网络发展现状的客观分析。（3）对已有的技术给出简要的说明并举例，阐述如何解决相应的网络问题；对未来的技术阐述部分依据。

4. 展示交流

每个小组派代表以演示文稿的形式向大家展示，并进一步完善分析报告。

评价标准

请根据项目实施的过程、效果以及成果展示交流的结果，对自己完成项目的情况进行客观的评价，并思考后续完善的方向。把评价结果和完善方案填写在下面的表格中。

评价条目	说明	评分（1～10分）	评分主要依据阐述	后续完善方向
调查	调查结论全面、提出的问题典型且有依据			
解决方案	至少提出三个问题的解决方案			
新型技术要求	已经存在的技术需要结合例子阐述，未成熟的技术给出部分依据			
完成并展示报告	表述准确，简明扼要，逻辑关系清晰，演示文稿制作美观大方			
团队合作	所有的团队成员都积极参与，对自己团队工作充满热情			

拓展项目

1. 学校希望将现在的食堂改造成“智慧食堂”，请你从网络建设的角度，给出一些合理的建议。

2. 社会上出现了很多“无人超市”，目前大致有三类：以计算机识别为基础的人工智能路线、以RFID为基础的物联网路线、以售卖机(二维码)为载体的互联网路线。随着科技的进步，还会出现其他的模式。假设你想投资一个“无人超市”，你会选择什么样的模式？怎样规划超市中的网络设备才能方便、快捷、安全地为人们提供服务？

3. 无人驾驶汽车是智能汽车的一种，也称为轮式移动机器人，主要依靠车内的以计算机系统为主的智能驾驶仪来实现无人驾驶。它利用车载传感器来感知车辆周围环境，并根据感知所获得的道路、车辆位置和障碍物信息，控制车辆的转向和速度，从而使车辆能够安全、可靠地在道路上行驶。如果希望无人驾驶汽车能够实时获取前方道路的路况来自动规划路线，该怎样改进？请你根据传感技术、网络技术等设计一个可行的方案。

第二章 2

网络技术基础

计算机网络是由计算机系统、数据通信系统以及网络软件和协议共同组成的一个复杂系统，计算机与计算机之间有不同的连接方式，并且可以用不同的传输介质进行连接。连在一起的计算机之间要实现互相通信，还需要约定共同的通信规则。利用分层设计的思想，能够使网络系统更容易实现，同时也更有利于促进网络的标准化工作。

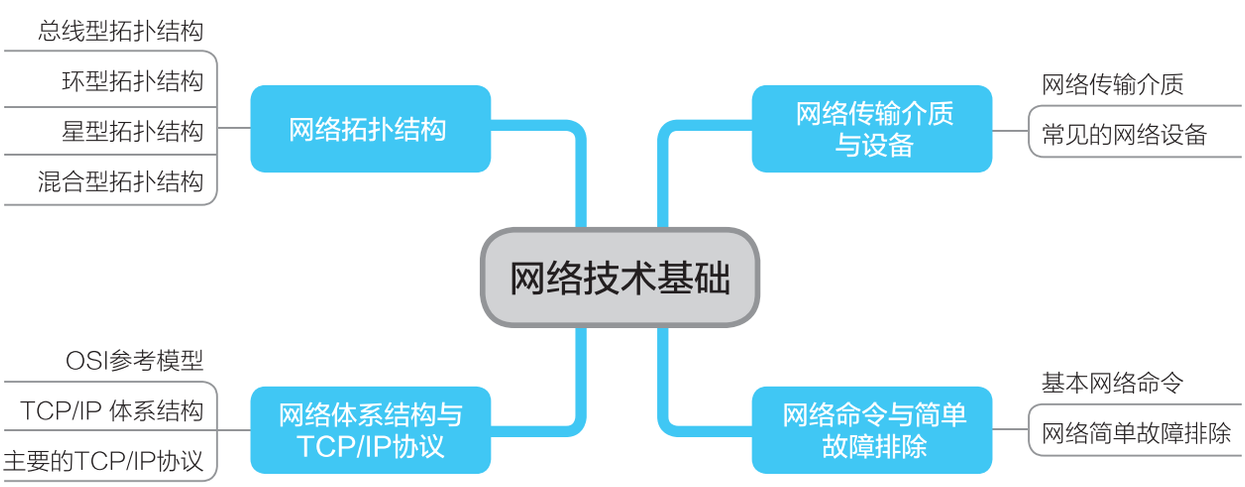
问题与挑战

- 无线网络和移动网络的覆盖范围越来越广，并且正朝着速度更快、应用更安全的方向发展，人们也越来越习惯通过无线网络或移动网络来上网。那么，在不远的将来，有线网络是否会被无线网络完全取代？有线网络的发展前景会怎样？
- 技术的发展促进了光纤到户，人们对千兆网络产品与千兆无线网已不再陌生，智能家居也方兴未艾，不同家庭对网络的需求呈现多元化趋势。传统的以提供接入为主的、百兆及以下的家庭网络越来越不适应未来家庭的需要，如何根据不同的网络需求和经济实力来升级家庭网络？
- 几乎所有人都碰到过网络故障，这会给生活与工作带来很大不便。对于身边常见的家庭与小型办公环境的网络，在没有专业的网络管理员的情况下，普通用户如何排除网络故障？

学习目标

1. 理解网络拓扑结构。
2. 了解常见网络传输介质的特性，理解影响网络传输质量的主要物理因素。
3. 理解网卡、交换机和路由器的作用和工作原理。
4. 了解分层设计的思想。
5. 了解OSI/RM参考模型及七层结构。
6. 了解TCP/IP体系结构，理解TCP/IP协议的主要功能和作用。
7. 掌握基本网络命令的使用方法。
8. 掌握小型网络简单故障排除的一般方法与步骤。

内容总览



2.1 网络拓扑结构

计算机和网络设备等节点的不同连接形式，构成不同的计算机网络拓扑结构。最基本的网络拓扑结构有三种：总线型拓扑结构、环型拓扑结构及星型拓扑结构。实际应用较多的还有混合型网络拓扑结构。

拓展链接

拓扑学

拓扑学（Topology）是几何学中的一门分支，是一种研究与大小、距离无关的几何图形特性的方法。若把网络中的计算机与网络设备抽象成点，把传输介质抽象成线，就可将计算机网络抽象成由点与线组成的表示节点连接方式的几何图形，这种几何图形具有拓扑学的一些特征，称为网络拓扑结构图。

2.1.1 总线型拓扑结构与环型拓扑结构

总线型拓扑结构网络是将各个节点设备用一根公共主线相连，网络中所有节点都通过公共主线传输信息，如图2.1.1所示。环型拓扑结构是指网络中各节点通过一条头尾相连的通信链路连接起来形成一个闭合的环形结构，如图2.1.2所示。这两种拓扑结构的网络目前已不多见。

拓展链接

FDDI

FDDI（光纤分布式数据接口）是20世纪80年代中期发展起来的一项局域网技术，速度为100Mbps。FDDI的基本结构为逆向双环，一个环为主环，另一个环为备用环，属于环型拓扑结构。

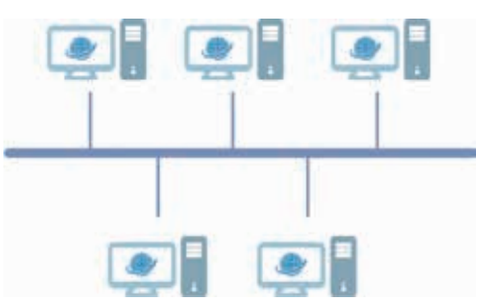


图2.1.1 总线型拓扑结构

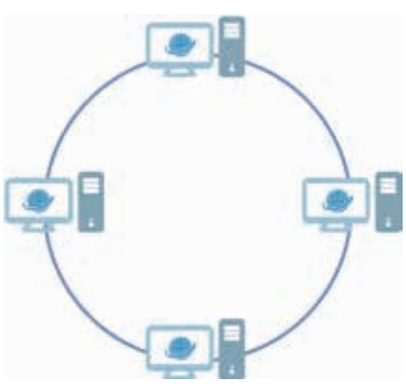


图2.1.2 环型拓扑结构

2.1.2 星型拓扑结构

星型拓扑结构由中心节点和分支节点构成，各分支节点与中心节点之间均有点到点的物理通路相连，分支节点之间没有直接的物理通路，如图2.1.3所示。分支节点之间的信息传输必须通过中心节点进行转发，或者由中心节点周期性地询问各分支节点，协助分支节点转发信息。

图2.1.3 星型拓扑结构

学生机房网络大多是星型拓扑结构，机房中的计算机都通过独立的网线与机房的交换机相连，数据都通过交换机转发。星型拓扑结构是目前应用最广、实用性最好的一种拓扑结构，这主要是因为它非常容易实现网络的扩展。

星型拓扑结构的主要优点：

①节点扩展与移动方便。在星型拓扑结构网络中，节点扩展时只需要同中心节点（如交换机）的空余端口建立链接即可，而移动一个节点只需要把该节点从原有端口断开，然后再移到新端口即可。节点的扩展与移动不影响已有设备的连接和使用，这是星型拓扑结构的突出优势。

②网络传输速度快。因为整个网络呈星形连接，所以每个节点的数据传输对其他节点的数据传输的影响比较小，因此网络数据传输速度较快。

③容易维护。在星型拓扑结构网络中，每个节点相对独立，一个节点的故障不会影响其他节点的连接。

星型拓扑结构的主要缺点：

①中心节点工作负荷重。星型拓扑结构网络中所有分支节点都连接到中心节点，中心节点特别是核心节点设备工作负荷重，对设备的性能要求也就非常高。另外，如果中心节点出现故障，就会导致整个网络的瘫痪。

②有线网络布线复杂。星型拓扑结构网络中每个分支节点都直接用专门链路与中心节点相连，这样整个网络中就需要用到与所有节点数目相同的电缆，电缆数量多，布线复杂。

③广播传输影响网络性能。因为星型拓扑结构的网络中经常要采用广播方式传输信息，即任何一个节点发送的信息在整个网络中的其他节点都可以收到，这种广播传输方式严重影响了网络性能。

2.1.3 混合型拓扑结构

实际网络结构中单纯的星型拓扑比较少见，总线型拓扑与环型拓扑几乎已看不到，最常应用的是基于基本拓扑结构而形成的混合型拓扑结构，如树型拓扑结构（星型拓扑结构的扩展）。如图2.1.4所示。

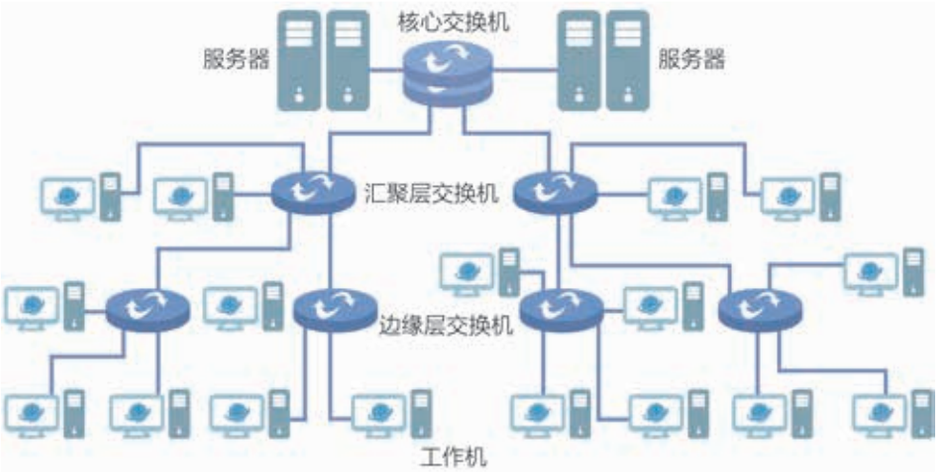


图2.1.4　混合型拓扑结构

思考与练习

1. 请对比分析总线型拓扑结构、环型拓扑结构与星型拓扑结构各自的优缺点。

	优点	缺点
总线型拓扑结构		
环型拓扑结构		
星型拓扑结构		

2. 为什么总线型拓扑结构与环型拓扑结构目前已不常见？

2.2 网络体系结构与TCP/IP协议

为了实现计算机之间的联网通信，人们把联网通信的功能划分出明确的层，同时规定了相同层之间的通信规则，以及相邻层之间的接口和服务种类。这种网络层次结构模型和层次之间通信规则的集合被称为网络体系结构。国际标准化组织（ISO）的OSI参考模型与TCP/IP体系结构是两种最重要的网络体系结构，其中TCP/IP体系结构所对应的TCP/IP协议系统在实践中应用非常广泛。

2.2.1 OSI参考模型

1974年，美国的IBM公司提出了世界上第一个系统网络体系结构SNA，随后其他厂商也纷纷提出了自己的体系结构。不同体系结构的网络之间不能或者很难实现互连，为了解决互连问题，ISO在1978年提出了开放系统互连参考模型（OSI/RM，也叫OSI参考模型）。

1. 分层与网络体系结构

OSI/RM参考模型采用分层设计的思想。分层设计使系统更容易实现与维护，也有利于促进标准化工作。分层的思想在第一个网络ARPAnet就已经被采用，随后IBM公司按照分层的方法研制并公布了著名的SNA网络标准，此后分层思想就成为网络标准研制的基本思想。

拓展链接

协议三要素

计算机进行网络通信时主要涉及三个问题：一是要实现什么样的网络服务（语义），二是如何实现这些网络服务（语法），三是如何与对方实现协同（同步）工作。语法、语义和同步是协议的三个基本要素。

分层思想的核心是每层完成一项相对独立的功能，并通过接口（interface）向上层提供服务（service），同层之间为完成本层的功能而必须遵守的一系列通信规则和约定称为协议（protocol），其结构如下页图2.2.1所示。

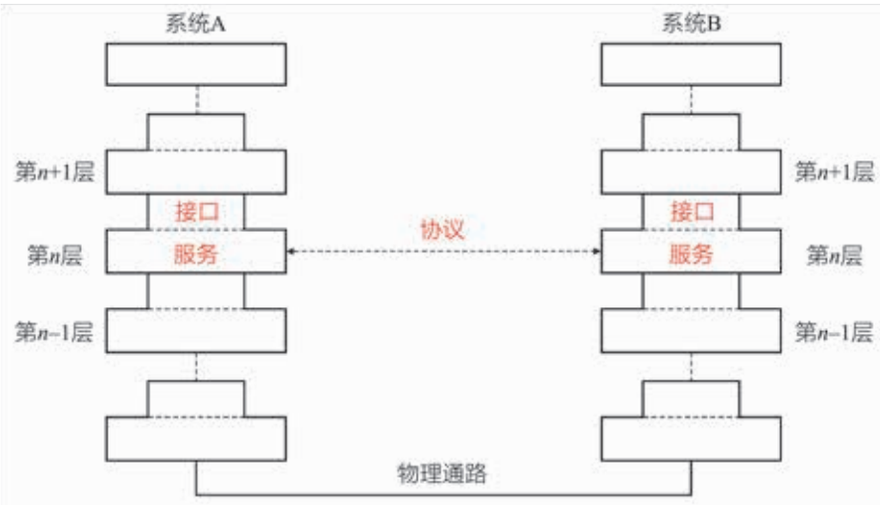


图2.2.1　计算机网络分层结构

问题与讨论

还有哪些领域应用体现了分层思想？

拓展链接

通信协议的连接方式

通信协议有两种连接方式：有连接通信方式与无连接通信方式。

有连接通信方式在传输数据之前首先建立并保持逻辑通道，再通过确认重传等机制提供可靠的数据传输服务；无连接通信方式事先不建立连接，只是尽最大努力传输数据，不保证可靠传输。

无连接通信方式是有连接通信方式的基础，虽然传输可靠性略差，但占用资源少，通常性能更好，还支持一对多传输，并且可靠性可在其他层加以弥补，所以无连接通信方式也是一种重要且常用的通信方式。

2. 七层结构与数据传输过程

OSI参考模型是一个七层模型。该模型一方面说明了通信的过程，另一方面规定了各层标准的制定方法。七层模型详细描述了OSI参考模型的三大核心概念，即各层提供的服务、层与层之间的接口以及对等层之间的协议。

七层分别为物理层（Physical Layer）、数据链路层（Data Link Layer）、网络层（Network Layer）、传输层（Transport Layer）、会话层（Session Layer）、表示层（Presentation Layer）

以及应用层（Application Layer）。发送数据时，数据从应用层逐层向物理层传输，数据到达每层后都会被“贴上该层的标签”或“装进该层的信封”，到达物理层后，所有的信息都被转化为“0”或“1”组成的比特流，进而转换成电信号通过物理媒介传输到接收端。在接收端数据从物理层逐层向上往应用层传输，数据向上传输到每一层，都会在该层被“撕去本层的标签”或“拆开本层的信封”后被传输到其上一层。每层都按照本层协议的规定来“封贴”或“撕拆”。如图2.2.2所示。

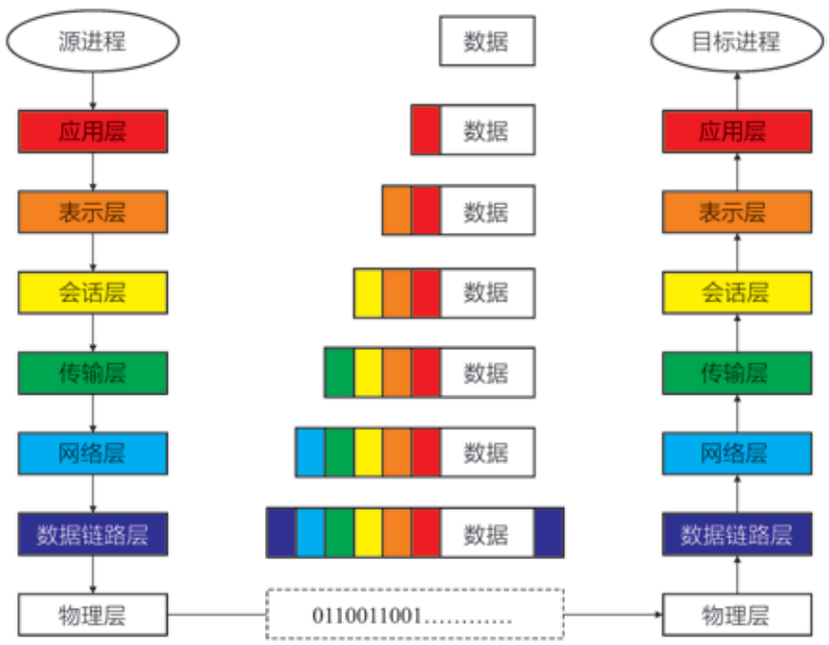


图2.2.2　OSI七层结构及数据传输过程

拓展链接

OSI七层模型

物理层：物理层定义了建立、维护和拆除物理链路所需的机械、电气、功能等特性，仅负责将“0”和“1”组成的比特流从一台计算机传输到另一台计算机。

数据链路层：数据链路层将比特流“打包”成称为“帧”的“协议数据单元”，并在相邻的节点间传输。数据链路层又进一步分为介质访问控制（MAC）子层和逻辑链路控制（LLC）子层。

网络层：网络层主要在非相邻节点之间建立数据传输“通道”，以实现网络互连的功能。

传输层：传输层主要功能是实现数据的发送端（源计算机中发送数据的程序）与接收端（目标计算机中接收数据的程序）之间的连接，即用“特定的编号”（端口号）来实现“端到端”的连接。

会话层：会话层的主要功能是组织和同步不同主机上各种正在运行的程序之间的通信。

表示层：表示层执行协议转换、数据翻译、压缩与加密、字符转换以及对图形命令的解释等功能。

应用层：应用层主要提供多种网络服务。

通常一个局域网内的不同计算机属于相邻节点，数据链路层（第二层）的一个主要功能就是实现相邻节点之间的可靠数据传输；位于不同局域网的两台计算机属于非相邻节点，非相邻节点之间的数据传输需要用到网络层（第三层）的路由选择功能；当数据传输到目标计算机后，还需要利用“特定的编号”即传输层（第四层）的端口号才能把数据传送到目标计算机上某个正在运行的程序中。

拓展链接

通信子网与资源子网

物理层、数据链路层、网络层（低三层）负责创建网络通信所需的网络连接（面向网络），通常称为通信子网；传输层、会话层、表示层以及应用层（高四层）负责端到端的用户数据通信（面向用户），通常称为资源子网。

2.2.2 TCP/IP 体系结构

TCP/IP体系结构也被称为因特网体系结构，因特网就是基于TCP/IP协议簇而构建起来的。TCP/IP协议簇包含了上百个各种功能的协议，TCP与IP是它的两个主要协议，如图2.2.3所示。TCP（Transmission Control Protocol）是传输控制协议，位于OSI参考模型的第四层即传输层；IP（Internet Protocol）是互联网协议，位于OSI参考模型的第三层即网络层。

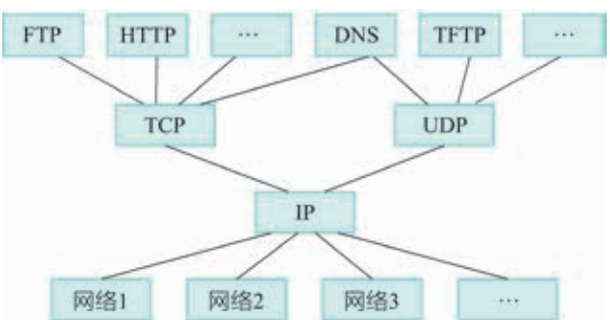


图2.2.3 TCP/IP体系结构协议图

TCP/IP体系结构通常用四层模型来描述，从低到高分别为网络接口层（Network Interface Layer）、网络层（Internet Layer）、传输层（Transport Layer）和应用层（Application Layer）。TCP/IP四层模型与OSI/RM七层模型的对应关系以及各层的主要协议及其实现途径如图2.2.4所示。

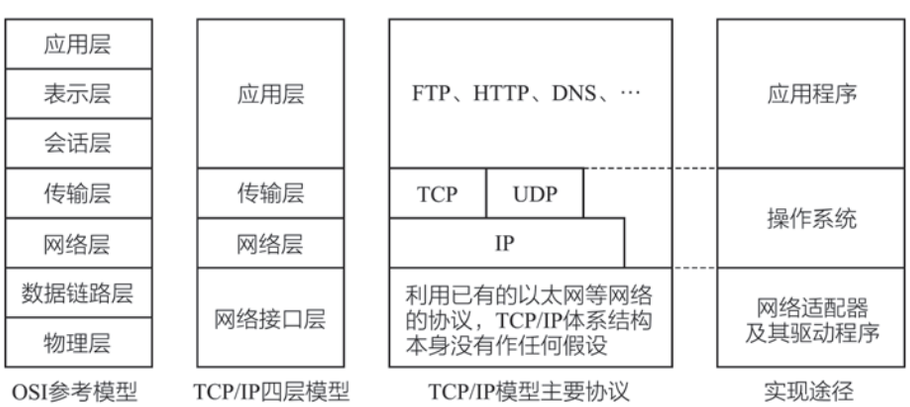


图2.2.4 OSI/RM七层模型与TCP/IP四层模型

网络接口层对应OSI/RM七层模型的物理层与数据链路层，这一层主要是利用已有的各种网络技术，如常见的以太网技术、无线局域网技术、点到点网络技术等。

网络层与传输层分别对应OSI/RM七层模型的网络层与传输层，网络层中的网际协议（Internet Protocol，IP协议）支持将多种网络互联为一个逻辑网络。传输层主要包括两个重要协议：传输控制协议（TCP）和用户数据报协议（User Datagram Protocol，UDP）。TCP与UDP为连接双方的应用程序提供可选的逻辑信道：TCP为有连接通信方式，能提供可靠的字节流信道；UDP为无连接通信方式，提供不可靠的数据报传送信道。

拓展链接

两种体系结构的连接方式

OSI参考模型的网络层同时支持有连接与无连接两种通信方式，传输层只支持有连接通信方式。TCP/IP体系结构在网络层只支持无连接通信方式，传输层则同时支持两种通信方式。

应用层对应于OSI/RM七层模型的会话层、表示层和应用层三层，常见的协议有FTP、HTTP、DNS、SMTP等，该层向用户提供一组常用的应用程序。

传送数据时，数据从源进程经应用层、传输层、网络层、网络接口层的数据链路子层逐层传递，每经过一层都会被“贴上该层的标签”或“装进该层的信封”，源进程的数据也相应地被转变成应用层的报文、传输层的报文段、网络层的数据包、网络接口层的数据链路子层的帧，帧在物理子层以0与1组成的比特流传送。接收端依次通过对应的“撕”“拆”操作后还原为目标进程的数据。

问题与讨论

为什么OSI七层模型概念清楚，理论也比较完整，但实际应用中远不如TCP/IP结构广泛？

2.2.3 主要的TCP/IP协议

TCP/IP协议通常指的是TCP/IP协议簇，由几百个协议构成，其中最重要的是网络层的IP协议与传输层的TCP协议和UDP协议。

IP协议以相同的规则给所有联网的计算机编上互不重复的“号码”（即IP地址），并在源计算机与目标计算机之间选择恰当的数据传输“通路”。TCP协议与UDP协议实现数据发送端点与数据接收端点之间的通信，即源计算机中的应用进程与目标计算机中的应用进程间的通信。

1. IP协议

（1）IP协议概述

IP协议将上层的报文段分割成适当大小的分组，再将分组根据当前路由选择的“路径”传送到目的地，不同的分组通过的“路径”可能完全不同，送达的先后顺序也不一定，也不保证能送达，即IP协议具有“无连接性”和“不可靠性”。这两个特性有助于提高整个网络通信链路的利用率，而把可靠性交给上层协议处理。

（2）IP地址

IP协议根据IP地址来标识网络上的主机，并且通过IP地址来发送和接收分组。当前广泛使用的IP协议是第四版的协议，称为IPv4，对应的地址为IPv4地址，通常称为IP地址。

IP地址是一个32位的二进制数，为了便于表示，按字节可以分成4组，再按组转换成十进制数并用圆点相连，即点分十进制表示法，如下表。

32位IP地址	11000000101010000000101000001011			
按字节分组	11000000	10101000	00001010	00001011
转十进制数	192	168	10	11
点分十进制表示	192.168.10.11			

拓展链接

IPv6

IPv6是Internet Protocol Version 6的缩写，是替换IPv4的新一代IP协议。IPv5是一个实验性的资源预留协议，它与IPv4一起运行，但与IPv6没有关系。

不同于32位的IPv4地址，IPv6采用128位的地址，解决了IPv4的最大问题——地址资源不足。IPv6甚至可以为地球上的每一粒沙子编上一个地址。

IP地址的前面若干位用于表示主机所在网络的网络地址，后面余下的位数表示该主机在本网络中的地址，称为主机地址，因此IP地址由网络地址和主机地址组合而成。

拓展链接

确定网络地址与主机地址的方案

确定IP地址中的网络地址部分与主机地址部分的最初方案是把地址分类，这种方案把地址分成A类、B类、C类等类别，每个类别的IP地址都规定了相应的网络地址部分与主机地址部分，这种方案现在已基本不再使用。

第二种方案是采用子网掩码技术，通过引入子网掩码来帮助确定网络地址与主机地址。最初的子网掩码技术是在分类地址的基础上进行的，现在基本上已放弃地址的分类，而采用任意长度即网络前缀来分割IP地址的网络地址部分与主机地址部分，即“无类型域间路由（CIDR）”。

2. TCP协议

TCP协议是传输控制协议的简称，位于传输层。TCP协议的主要功能是提供有连接的、可靠的、数据流式与端到端的传输服务。所谓有连接是指传送数据的双方必须事先沟通并确定已建立好连接后，才能传输数据。可靠是TCP协议很重要的一个特性，主要通过三条规则实现：第一条，若接收端接收的数据正确，则返回确认报文给发送端，发送端发送下一个等待发送的报文；第二，若接收端接收到的数据不正确，则返回要求重传的报文给发送端，发送端重新发送该报文；第三，若发送端在设置的时间内没有收到接收端的回应报文，则发送端自动重传该报文。数据流式是指TCP协议的数据传输是依次序一个接一个地传送分组。发送端实际发送数据的主体是应用进程，接收端实际接收数据的主体也是应用进程，而IP协议只负责把分组传送到目标主机的网络层但没有交付给主机中的应用进程，这个任务由传输层利用协议端口号（Protocol Port Number，简称为端口）来实现。端口号是一个16位的二进制数，因此共有65536个不同的端口，不同的端口对应着不同的应用进程，因此利用IP地址与端口号的结合实现了应用进程到应用进程间的通信——端到端的传输。IP地址与端口的结合被称为套接字（Socket），通常以冒号分隔，如“192.168.10.11:21”。部分端口号已被指派给了一些重要的TCP/IP应用程序，这些端口号被称为默认端口号（Well-Known Port Number）或系统端口号，如下表列出一些默认端口号。

应用程序	HTTP	HTTPS	SMTP	POP3	FTP	DNS	TELNET	SSH
默认端口号	80	443	25	110	21	53	23	22

3. UDP协议

UDP协议（User Datagram Protocol）是用户数据报协议的简称，是与TCP协议并列的传输层协议。UDP协议提供无连接的、尽最大努力交付的、面向报文的、端到端的传输服务。无连接意味着传送数据之前不需要建立连接，因此提高了传送效率。尽最大努力交付意味着主机不需要维持复杂的连接状态，并且也不需要等待确认以及重传等流量控制的机制。面向报文表示UDP对应用层交下来的报文不进行处理，只是在报文的前面添加首部后就直接传给下面的网络层。UDP协议同样也利用端口号来实现应用进程到应用进程即端到端的传输。UDP协议比TCP协议简单，传输效率更高，非常适合应用于通信实时性要求高

而通信数据完整性要求不是很高的场合，如QQ这样的即时通信软件。与之相对应，TCP协议适合应用于通信数据完整性要求高而通信实时性要求不是很高的场合，如文件传输。

实践与体验

查看IP参数

在使用计算机的过程中，有时会需要查看本机的IP地址等参数。对Windows系统来说，有多种查看方法，其中一种方法是通过查看连接状态的详细方式来实现的。

实践内容：

掌握一种查看IP地址等参数的方法。

实践步骤：

1. 打开“控制面板”窗口（按组合键Win + R，然后输入“control”后按回车键），单击“查看网络状态和任务”链接，如图2.2.5①所示，打开“网络和共享中心”窗口，如图2.2.5②所示。

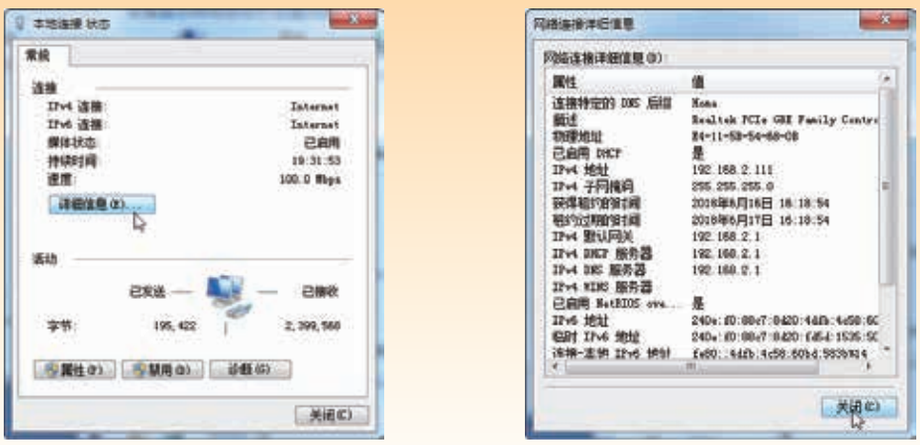
2. 在查看活动网络中单击连接名称（如“本地连接”“无线网络连接”“以太网”等），如图2.2.5②所示，打开“本地连接 状态”窗口，如图2.2.5③所示。

3. 查看并记录连接速度与持续时间，然后单击“详细信息(E)”按钮，如图2.2.5③所示，打开“网络连接详细信息”窗口，如图2.2.5④所示。

4. 查看并记录IP地址等参数，如图2.2.5④所示。

①

②



③ ④

图2.2.5 查看IP参数

结果呈现：

整理记录结果，完成下页表。

项目	内容
活动网络连接名称	
连接速度	
连接持续时间	
是否自动获取IP参数	
IP地址	
子网掩码	
默认网关	
DNS服务器	

思考与练习

在有关网络的讨论中，经常会提及“服务”和“协议”这两个术语。请查阅资料，了解这两个术语的区别与联系。

2.3 网络传输介质与设备

网络传输介质与设备连接节点计算机组成计算机网络，因此介质与设备的特性在很大程度上决定了整个网络的类型与性能。常见的网络传输介质有双绞线、光纤等，常见的网络设备有网络适配器（网卡）、交换机、路由器等。

2.3.1 网络传输介质

网络传输介质是网络中传输数据的物理线路，分为导向性传输介质和非导向性传输介质两类。

1. 导向性传输介质

导向性传输介质是指信号在其内部会沿着确定的方向传输的介质，通常指有线计算机网络中使用的传输介质，如同轴电缆、双绞线电缆和光纤电缆等。

（1）同轴电缆

同轴电缆由同一轴心的内外两层导体组成，两层导体间有绝缘层，外层导体外面包裹有绝缘保护套，结构如图2.3.1所示。

图2.3.1 同轴电缆

拓展链接

两种常用的同轴电缆

常用的同轴电缆有两种：一种是50欧姆的同轴电缆，也叫基带同轴电缆（又分粗缆与细缆），用于数字信号的传输，目前已很少使用；另一种是75欧姆的同轴电缆，也叫宽带同轴电缆（主要用在有线电视系统中），用于宽带模拟信号的传输。

（2）双绞线电缆

双绞线电缆是把两根互相绝缘的铜导线按一定规则绞合在一起，以减少彼此的电磁干扰。通常4对双绞线组成一根双绞线电缆，简称双绞线。

双绞线最初使用在电话系统中（主要是3类及更早的版本），后来移植到计算机网络中。在计算机网络中使用的双绞线默认都是指非屏蔽双绞线（Unshielded Twisted Pair，UTP），如图2.3.2所示。屏蔽双绞线以金属箔包裹线对组，能进一步减少干扰，性能更好一些，但价格昂贵，实际使用相对较少。

双绞线依其性能可分为不同的类别，当前比较常见的有5类、超5类、6类、超6类以及较新的7类，超5类及以上的双绞线支持千兆网，7类线支持10千兆网。双绞线的长度超过100米时传输性能会显著下降，因此双绞线一般用在同一楼层或同一幢楼内，如果几幢楼之间的距离较近，有时候也会用双绞线联网。

图2.3.2　双绞线

（3）光导纤维

光导纤维（Optical Fiber）简称光纤，由能传导光波的石英玻璃等材料制造而成。光纤通信是利用光纤传递光脉冲来进行数据通信的，通常一个光脉冲表示二进制中的一个1，而无光脉冲则表示二进制中的一个0。平常所说的光缆是指由光纤、加强件和保护层等组成的线缆，按光缆中所含光纤的数量可分为单芯、双芯以及多芯，如图2.3.3所示。

图2.3.3　光纤与光缆

光纤的分类标准很多，常见的分类标准是按传输模式划分，可分为多模光纤（Multi-Mode Fiber,MMF）和单模光纤（Single-Mode Fiber,SMF）。多模光纤允许多条不同角度入射的光线在同一条光纤中传输，这些光线通过光纤包层的全反射向前传输，如图2.3.4所示，多模光纤纤芯较粗，能够传输多个模式的光波，但是色散大，损耗也大，所以传输距离较短。单模光纤的纤径很小，只有基模能够在其中传输，如图2.3.5所示，光在单模光纤中能够沿纤芯中心轴线方向直线传播，色散和损耗也很小，因此适合长距离传输。

图2.3.4　多模光纤

图2.3.5　单模光纤

拓展链接

全反射

全反射又称全内反射，指光由光密介质（即光在此介质中的折射率比较大）射到光疏介质（即光在此介质中折射率比较小）的界面时，全部被反射的现象。光导纤维是全反射现象的重要应用。

光纤作为传输介质有许多优点。首先，光纤有很高的数据传输速率、极宽的频带、低误码率和低延迟；其次，光传输不受电磁干扰，安全性和保密性好；此外，光纤还具有质量轻、体积小、容易铺设等优点。

2. 非导向性传输介质

非导向性传输介质，是指信号在其中传输时没有固定方向的传输介质。电磁波在空间中的传播就属于非导向性传输，无线通信利用的就是这种传输方式。电磁波按照波长的不同可以分为无线电波、微波、红外线、可见光等，日常无线通信中常见的电磁波是Wi-Fi与移动网络的无线信号，这两类电磁波都属于微波。卫星通信一般用在国家的主干网络上，地面微波接力通信一般用在山区、海岛、草原等不太适合铺设有线线缆和使用卫星通信的场合，如图2.3.6所示。另外，还有一些近距离点对点通信的场合，如蓝牙、近场通信、红外线传输等，也采用了非导向性传输介质。

图2.3.6　微波通信

2.3.2　常见的网络设备

计算机要通过网卡来连接网络，多台计算机通常用交换机连接起来组成网络，多个网络需要用路由器连接起来组成更大的网络，因此网卡、网络交换机与路由器是常见的网络设备。

1. 网卡

网卡也叫网络适配器，是用来连接网络的最基础的网络设备。网卡按照主机接口（即与计算机主机的连接方式）的不同可进一步分为PCI接口网卡、PCI-E接口网卡、USB接口网卡、主板集成网卡等，按照网络接口（即与网络的连接方式）的不同可分为有线网卡与无线网卡，如图2.3.7所示。

图2.3.7　网卡

有线网卡主要有双绞线接口（又称为RJ-45口）与光纤接口两种类型，双绞线接口的网卡一般用在客户机与服务器上，如图2.3.8所示，光纤接口的网卡一般用在服务器上。按照网卡所支持的网络标准的不同，还可以分为10/100Mbps自适应网卡和10/100/1000Mbps自适应网卡等。服务器上一般配备多个千兆及以上的网卡，个人计算机一般配备千兆网卡。

图2.3.8　双绞线接口

2. 网络交换机

网络交换机是把多台计算机连接起来组成网络的重要网络设备，如图2.3.9所示。网络交换机简称交换机，是工作在OSI模型的第二层——数据链路层上的网络设备，具有多个端口用于连接计算机等设备，如图2.3.10所示。交换机采用储存转发技术传输数据，即交换机首先接收并存储数据，然后根据目标计算机网卡的MAC地址（即物理地址）将数据转发到相应的端口。

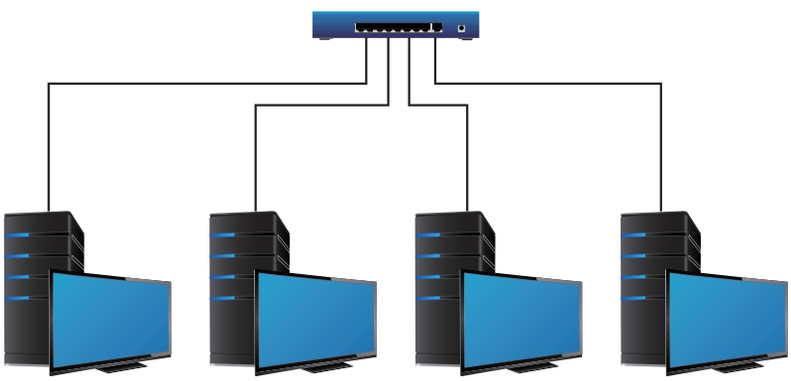


图2.3.9　网络交换机连接电脑组成网络

图2.3.10　网络交换机

网络交换机按端口数的不同可分为8口、16口、24口、48口等；按速度不同可分为百兆交换机、千兆交换机、万兆交换机等；按是否支持网络管理可分为网管型交换机和非网管型交换机；按是否支持三层路由可分为两层交换机与三层交换机。

拓展链接

三层交换机

最初的网络交换机是两层交换机，也就是说两层交换机只能在同一个网段内部实现数据传输。而实际应用中一个组织内通常有多个部门，各个部门往往用不同的网段形成不同的部门网络，这些部门网络大多是同类网络并且也比较简单，为了满足这种网络的互联需求，厂商通过在传统两层交换机的基础上增加基本的三层路由功能开发出了三层交换机。

3. 路由器

路由器是把不同的网络连接起来并实现互相访问的关键设备，如图2.3.11所示，图中路由器把四个网络连接起来然后再与外网相连。路由器通常端口数较少但端口的种类比较多，以适应连接各种不同的网络，如图2.3.12所示，专业的路由器通常还具有可更换的模块以适应不同的需求。

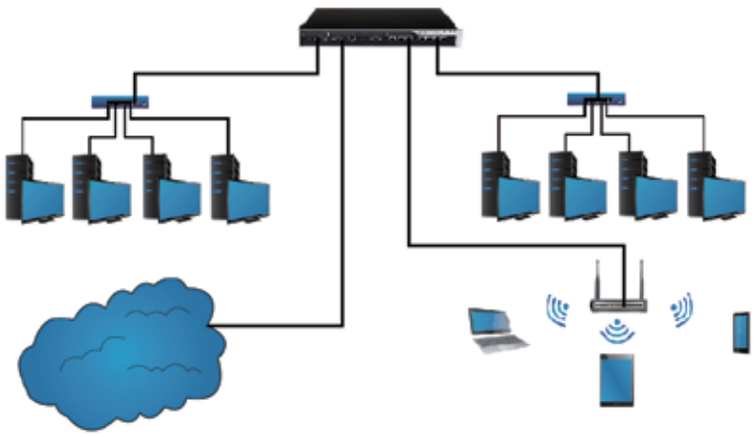


图2.3.11　路由器连接不同网络

图2.3.12　路由器

路由器是工作在OSI模型的第三层——网络层上的网络设备，与两层交换机类似，路由器也采用存储转发技术，但两层交换机是根据MAC地址进行转发，而路由器是根据IP地址进行转发的，路由器能够根据路由选择，将分组发送给下一个目标路由器。路由器还具有分担网络负荷的作用，有些路由器具备一定的网络安全等功能。因为路由器要处理的信息量比两层交换机要大得多，所以处理速度比两层交换机要慢。

拓展链接

小型无线路由器

常见小型无线路由器的性能和功能比专业的路由器差得多，并且通过无线连接的终端数量一般都有限制，超过该限制会使网络性能大幅下降。

例如一个5端口的无线路由器实际上可看成是一个5（4+1）端口的小型交换机与一个2（1+1）端口简易路由器的组合，交换机与路由器各有一个端口在内部连接起来，所以从外部看就是4个局域网口和1个广域网口。

思考与练习

1. 如果计算机的网卡是千兆网卡，是否就能实现千兆速度的传输？如果不能，还需要满足哪些条件？

2. 列表分析传输介质、网卡、交换机与路由器分别对应于OSI七层结构的哪一层。IP协议对应哪种网络设备？

2.4 网络命令与简单故障排除

在日常的网络维护中，经常需要查看网络配置、设置网络参数、诊断与排除网络故障，这个过程通常需要用到各种网络命令。

2.4.1 基本网络命令

基本的网络命令有ipconfig、ping、tracert、telnet等。

1. ipconfig

可以用ipconfig命令来查看本机的IP地址、网关、DNS等参数。常见的用法是在“命令提示符”窗口内输入“ipconfig”后按回车，该命令将列出本机所有网络适配器（网卡）基本的TCP/IP配置值，如图2.4.1所示。

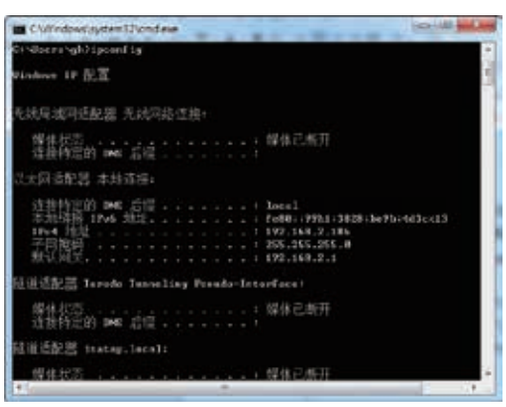


图2.4.1 ipconfig命令

从图中可知“本地链接”连通网络，IP地址是192.168.2.186，默认网关是192.168.2.1。如果想要查看更详细的内容可输入带“all”选项的命令，即“ipconfig /all”。利用“?”选项（即“ipconfig /?”）可以获取ipconfig命令本身的帮助信息。很多命令都可以用相同的方法来获取帮助信息。

拓展链接

打开“命令提示符”窗口

打开“命令提示符”窗口的一种方法：按组合键Win + R，输入“cmd”后回车。

在“命令提示符”窗口中输入“exit”命令后回车，即能退出。

拓展链接

默认网关

一台主机要访问其他网络上的主机，就需要利用网关转发数据。主机把数据发给事先指定的网关，再由这个网关转发数据，该网关就是这台主机的默认网关。

2. ping

ping命令是最常见的测试网络是否连通的命令，并且还能利用该命令大致判断网络连接速度。ping命令通常的用法是在“命令提示符”窗口内输入“ping”目标IP地址或域名，如图2.4.2所示。

从图中可知，本机与网关（192.168.2.1）之间是连通的，并且速度较快，时间均小于1毫秒（“时间＜1ms”），网络连接的质量也比较高［“丢失=0(0%丢失)”］。如果网络不通，将会出现“请求超时”的提示，若完全不通则丢包率的值为100%。

不带选项的ping命令默认发4个数据包，加上“–t”选项（如：ping –t 192.168.2.1）ping命令将持续发包，直到按Ctrl + C组合键停止。利用–t选项可持续监测一段时间内网络的连通情况。

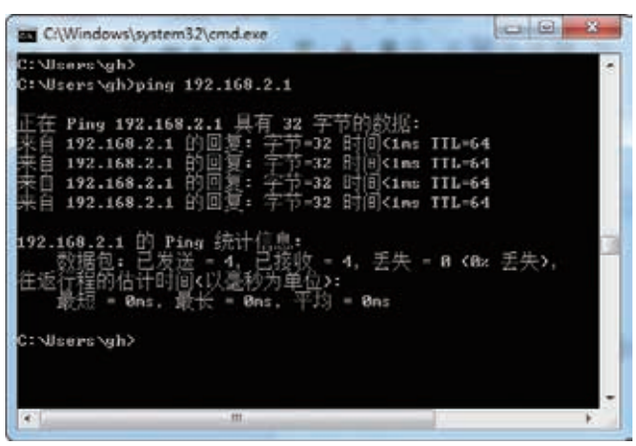


图2.4.2　ping命令

拓展链接

ping不通与网络不通

如果ping命令返回信息是“请求超时”，仅表明ping命令发出的数据包没有在规定的时间内收到对应的回包。其原因可能是网络完全不通，回包永远回不来了；也可能是回包还在路上，但规定的等待时间已到，回包被丢弃；也可能是数据包经过太多的中间路由器节点（超过规定数）而被丢弃；等等。

所以，如果网络不通，那么ping命令返回信息肯定是“请求超时”或类似信息，但是如果返回信息是“请求超时”，那么网络不一定不通（如对方设置了防火墙，拦截了ping包），但实践中一般判断为网络不通。

3. tracert

tracert命令是路由跟踪实用程序，用于确定IP数据包访问目标节点所采取的路径。实践中常用tracert命令来大致判断中间路由器节点的连通情况。tracert命令最常见的用法是在“命令提示符”窗口中输入：tracert 目标IP地址或域名。如图2.4.3所示。

图中显示数据包经过13个中间节点后最后到达目标节点（115.239.211.112）。

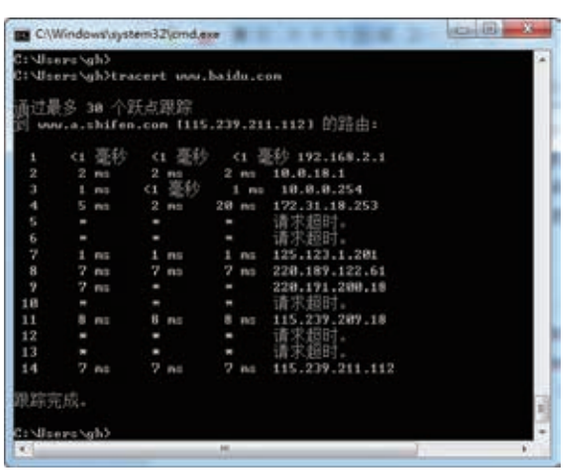


图2.4.3　tracert命令

问题与讨论

tracert命令中出现“请求超时”，是否表示该节点不通？如果该节点不通，是否一定会出现“请求超时”或类似信息？

4. telnet

telnet命令是远程登录程序，用于登录远程主机进行操作或者测试某个端口是否处于打开状态。在实践中常利用telnet命令连接交换机或路由器进行初始化配置或查看端口情况。

某些用户的Windows系统中Telnet客户端程序可能未安装，可在“控制面板”的“程序和功能”中单击“打开或关闭Windows功能”，再勾选“Telnet客户端”，然后单击“确定”进行安装，如图2.4.4所示。

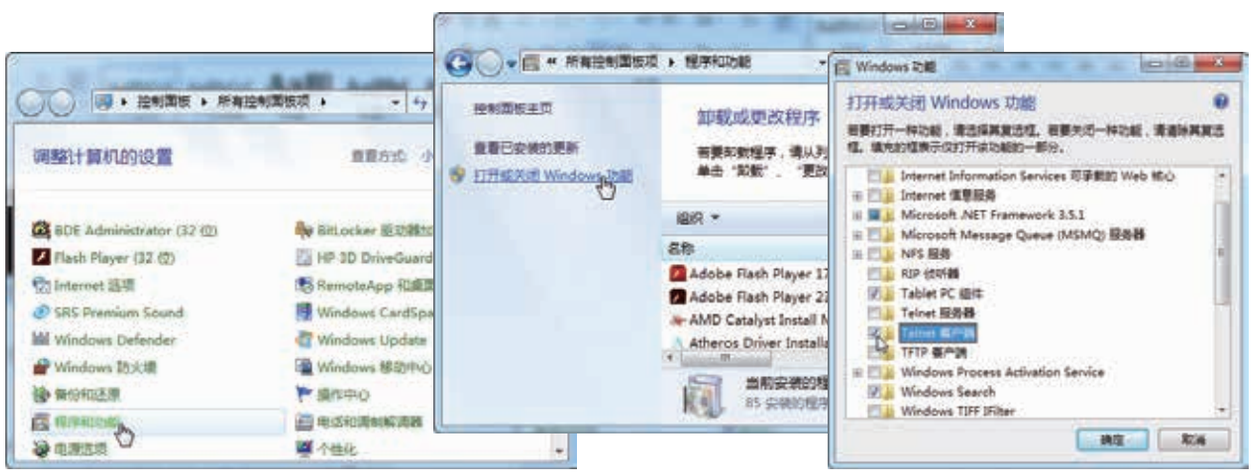


图2.4.4　安装Telnet客户端程序

用telnet命令查看端口的方法是在“命令提示符”窗口中输入：telnet 目标IP地址或域名 端口号。如图2.4.5所示。

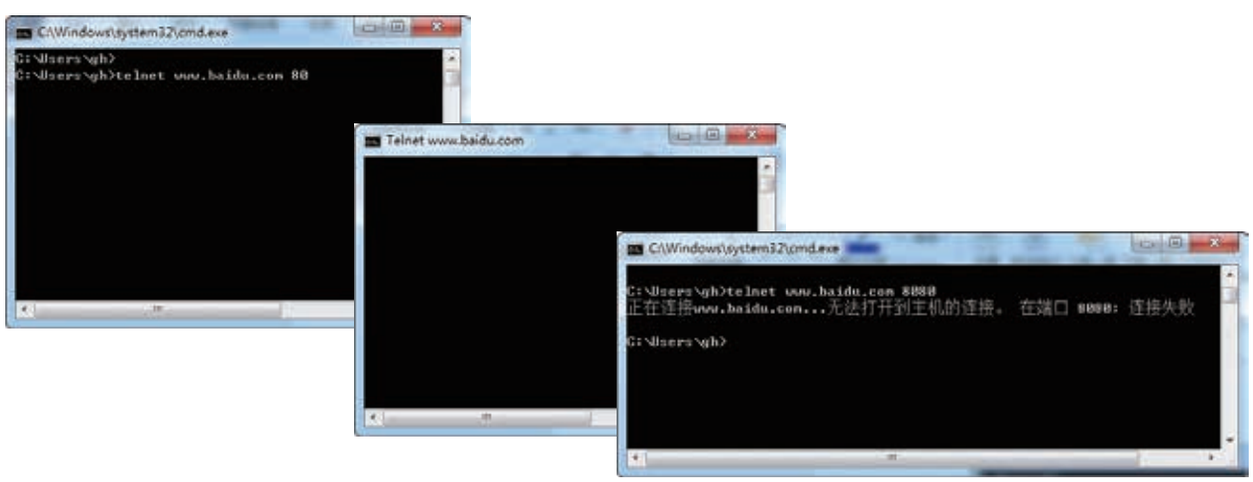


图2.4.5　telnet命令

如果端口已打开，那么会出现黑色的空窗口，如图2.4.5中间窗口。在黑色的空窗口中输入组合键Ctrl +]，再输入“quit”后回车即可退出telnet。如果端口已关闭，那么会出现“连接失败”的提示。

2.4.2 简单网络故障排除

因网络故障给生活和工作带来不便的现象时有发生。要快速准确地解决简单的网络故障，首先需要根据故障现象判断是本机原因、内网原因还是外网原因，再进一步细致分析，由近到远逐级检测，确定故障原因，最终排除故障。

下面以解决一个实际的网络故障为例，介绍诊断与排除简单网络故障的一般方法。

●●● 例

某家庭网络通过光纤接入社区网，再通过社区网访问外部网络。家庭网络内部有一台无线路由器，这台路由器通过网线连接了一台台式计算机和一台笔记本，通过Wi-Fi连接了另一台笔记本和若干部手机、平板电脑。近期发现播放社区网站的视频不流畅，有时甚至无法连接，但外部网络的视频可以正常播放。今天，用户发现台式机无法上网，所有网站都无法访问。

1. 初步界定网络故障的范围

首先确定家庭中其他终端是否能够上网，如果其他终端上网正常，那么基本上可以把网络故障确定在本机。如果家庭内所有终端都不能上网，那么故障最有可能出现在路由器上，也有可能是外网出了问题。

2. 检查本机网络是否存在故障

首先检查本机网络连接是否正常。查看任务栏右侧的系统托盘区是否有异常的连接图标，若有则表明本机网络连接有问题，然后再根据是有线连接还是无线连接做进一步判断。如果是有线连接可进一步检查计算机网卡与交换机或路由器的网线插口旁的灯是否正常工作，如果怀疑不正常，可尝试插拔网线或者换一根网线等；如果是无线连接，可以尝试重启或更换交换机或路由器。直到连接显示正常为止。

然后检查本机的IP协议是否正常。进入“命令提示符”窗口，输入命令：ping 127. 0.0.1。如果显示正常，那么说明本机IP协议正常。如图2.4.6所示。

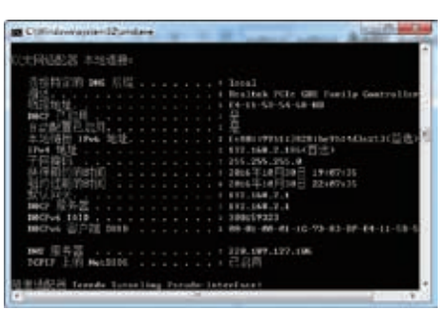


图2.4.6 测试本机IP协议

最后检查本机的IP地址设置是否正确。在“命令提示符”窗口输入命令“ipconfig /all”，如图2.4.7所示。记下IP地址（192.168.2.186）、网关（192.168.2.1）以及DNS（220.189. 127.106）。

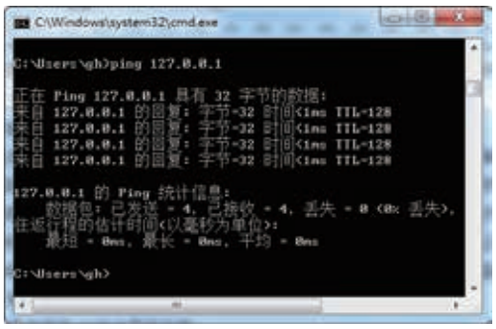


图2.4.7　查看本机IP参数

ping本机的IP地址，即输入命令“ping 192.168.2.186”，如图2.4.8所示。如果能通，说明IP地址设置正确，如果不通则可以尝试重设IP地址或者向DHCP服务器重新续订IP地址。

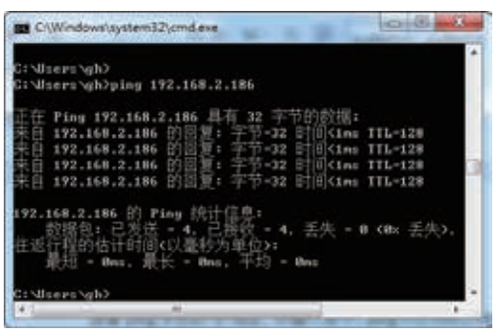


图2.4.8　ping本机IP地址

3. 检查本机与网关（路由器）间的连接是否正确

ping网关的地址，如输入命令“ping 192.168.2.1”。如果连接正确，那么基本可以断定是路由器或者外网出了故障。如果不通，那么尝试重新插拔、换插网口、更换网线甚至更换路由器等。

4. 检查本机与DNS间的连接是否正确

ping DNS地址，如输入命令“ping 220.189.127.106”，如图2.4.9所示。如果DNS能ping通，那么基本可以断定网络已无问题。如果DNS地址ping不通，那么咨询本地的网络接入服务提供商。

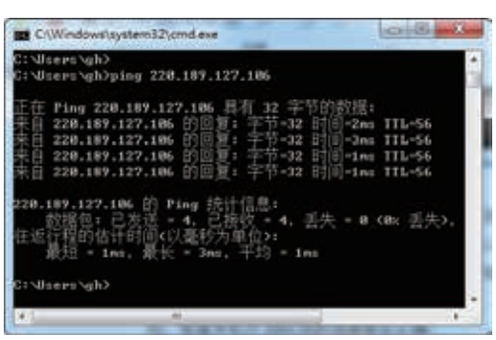


图2.4.9　ping DNS服务器

5. 检查本机与常用网站之间是否连通

继续在“命令提示符”窗口中输入一些经常访问的公共网站，如百度、新浪等。如果连接正常，那么基本可以断定网络正常。如果DNS能ping通但常用网站的域名ping不通，那么可以用telnet命令进一步查看DNS的端口是否打开，输入命令“telnet 220.189.127.106 53”。如果出现黑色的空窗口，那么说明端口正常，可能是DNS服务出问题；如果出现连接失败，那么说明DNS服务的端口没打开。不管哪种情况，通常需要咨询本地网络接入服务提供商，如果有其他DNS地址，也可以尝试更换DNS地址。

6. 检查个别网站特别慢甚至时断时续的原因

利用tracert命令可粗略判断问题大致出在哪些节点上，如社区视频网站的地址为10.10.10.2，则在“命令提示符”中输入命令“tracert 10.10.10.2”，如图2.4.10所示，大致可判定问题出在“请求超时”的那些节点上。

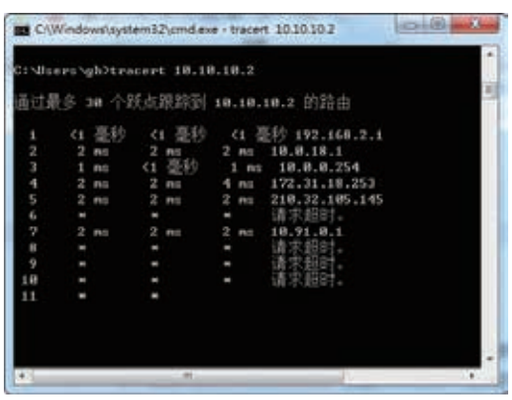


图2.4.10　tracert查看路由路径

实践与体验

常用网络命令与选项

在进行网络维护和网络故障诊断与排除的过程中，经常要用到网络命令。熟练掌握常用的网络命令以及这些命令的一些实用选项，可以提高网络维护的效率。

实践内容：

1. 通过查看常用网络命令的联机帮助，整理出常用网络命令的实用选项。
2. 通过上网搜索，整理出其他一些常用网络命令以及对应的实用选项。

实践步骤：

1. 在命令提示符窗口中用“/?”选项查看ipconfig、ping、tracert命令的联机

帮助，并记录部分实用选项。

2. 上网搜索并筛选出若干个常用的网络命令以及相应的一些实用选项，并把内容记录下来。

结果呈现：

记录并整理实用命令以及对应的实用选项，然后完成下面的表格。

命令	选项	应用场合

思考与练习

对于自动获取的IP地址，如果向DHCP服务器重新续订IP地址，要如何操作？查阅资料然后写出三种方法。

巩固与提高

1. 分层设计思想的应用比较普遍，良好的分层设计能使复杂问题变得相对简单。请根据网络层次模型分析，良好的分层设计要注意哪些方面。

2. 查阅资料，列举双绞线与光纤两种传输介质各自的优缺点以及较典型的应用场所。

3. TCP与UDP的功能有何不同？

4. 查阅资料，结合例子说明两层交换机、三层交换机以及路由器的典型应用场所。

项目挑战

家庭网络升级

某用户想改造自己的家庭网络，目前该用户的家庭网络配置是：由1台老旧的无线路由器通过双绞线连接1台台式机，再通过Wi-Fi连接2台笔记本电脑以及3部手机，外部网络通过光纤接入因特网。该用户对于升级的目标不明确、所需经费不清楚，希望专业人员提供多套升级方案以供选择。

项目任务

要求设计3套家庭网络升级方案，经费从低到高、功能与性能从弱到强。每套升级方案均包括经费、功能、配置清单等内容。

过程与建议

1. 确定升级目标

利用下表梳理不同方案的升级目标所包含的要素，明确升级方向。

方案	所需费用	功能	内部网络	扩展性
方案一	低			
方案二	中			
方案三	高			
示例	高	10TB文件存储空间，多终端视频与音频播放	千兆有线连接到终端，千兆无线连接覆盖整个家庭	有线连接数20个以上，有效无线连接数50个以上

2. 列出设备清单

根据升级目标上网搜索所需的设备，列出每套升级方案所需设备的品牌、型号与价格，并摘录主要的功能与性能。

3. 撰写升级方案

撰写3套升级方案，每套升级方案要包括升级目标、所需设备、功能与性能、经费预算以及升级步骤五个方面的内容。从用户的角度去审视和修订升级方案，确保好理解、易操作、可选择。

4. 向用户（模拟用户）展示升级方案

以一定的形式（如PPT、简报等）向模拟用户进行展示，要求在规定的时间内完成展示、回答模拟用户的问题，确保模拟用户能够理解升级方案。

评价标准

请根据项目实施的过程、效果以及成果展示交流的结果，对自己完成项目的情况进行客观的评价，并思考后续完善的方向。把评价结果和完善方案填写在下面的表格中。

评价条目	说明	评分（1～10分）	评分主要依据阐述	后续完善方向
升级目标	3套升级方案目标明确，有明显梯度，能体现升级价值			
设备清单	设备恰当有效，能恰好满足升级目标			
升级方案	结构完整，逻辑清晰，内容精练全面，具有很强的可读性			
展示交流	在规定时间内能清晰地解释整个方案，能很好地回答用户的问题			

拓展项目

1. 校园网通常是由多个不同网段的网络互相连接而成的比较复杂的网络，是学校不可缺少的基础设施，请在调查了解与实地察看的基础上绘制出校园网络整体拓扑图，并在图中注明传输介质与网络设备的类型，以及各网络的IP地址范围。

2. 以现有校园网主要网络设备购置金额总和的三分之一为额度，提出现有校园网主要网络设备的升级方案，并说明升级理由。

第三章 3

网络服务

网络服务采用互联网通用标准，使人们可以在不同的地方通过不同的终端设备访问网上的数据（如网上订票、网上购物、电子银行等），因此网络服务在电子商务、电子政务、公司业务等领域有着广泛的应用，这也使得网络生活变得丰富多彩。一般情况下，网络上不同的应用都有对应的服务器提供服务，如电子邮件由邮件发送服务器和邮件接收服务器提供服务，万维网由Web服务器提供服务，网上购物、即时聊天、云存储等也都有对应的服务器提供服务才能正常运转。

问题与挑战

- 随着数码摄影设备的大量普及，数码影像的共享问题日益凸现，由于影像容量较大，采用传统的文件拷贝方式在灵活性和便捷性上都难以满足需要。如何在各种家庭设备之间更加方便地共享数码影像，便于家庭成员在不同影像终端上随时欣赏呢？

- 万维网是因特网中使用最广泛的应用，其服务内容丰富多彩。很多服务都含有浏览、查询和评价等功能，如照片分享网站、文档共享网站、服务点评网站等。这些服务是如何实现的？

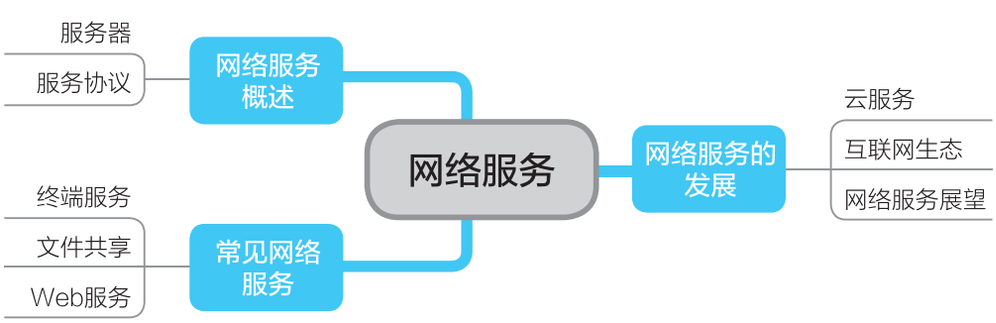
- 网络服务器一般是由管理人员远程管理的。在管理过程中经常需要上传大量的资源，如网页、图片、视频等，如何才能快捷地将这些资源传输到服务器上去呢？

- 云存储是一种专业的互联网存储技术，它通过互联网为企业和个人提供信息的储存、读取、下载等服务，具有稳定、海量的特点。但考虑到数据安全问题，有一些个人或团队专属的资料是不适合采用第三方云存储的，需要借助私有云存储，那么，该如何创建此类服务呢？

学习目标

1. 了解网络服务的相关概念。
2. 理解常用网络服务的实现原理。
3. 根据网络服务原理，能搭建简单的文件共享、Web及FTP服务器。

内容总览



3.1 网络服务概述

从技术角度看，网络服务是计算机通过网络为其他计算机提供数据处理的过程，提供数据处理的计算机通常叫服务器，接受数据处理结果的计算机称为终端。常见的网络服务有终端服务、文件或打印机共享服务、文件传输服务、域名服务、万维网服务、动态主机配置服务及电子邮件服务等。不同的网络服务一般都对应一种或多种网络协议，为了方便起见，有时也用协议名来表示服务，如文件传输服务也称FTP服务。

3.1.1 服务器

服务器通常由硬件和软件两部分组成，一般都用服务器的硬件部分来指代服务器。

服务器的硬件部分是指专门提供网络服务的计算机，根据安装方式不同，可以分为塔式服务器和机架式服务器，如图3.1.1所示。由于服务器一般要求全天候工作，24小时不关机，所以服务器的软硬件和普通计算机相比有较大的差别，这些区别主要体现在以下几个方面。

图3.1.1 硬件服务器

高稳定性：服务器要求长时间不间断工作，所以要求其硬件非常稳定，甚至为了追求稳定性而不惜增加冗余的硬件设备。

高处理能力：服务器要响应网上众多客户端计算机的请求，所以其处理能力通常要好于普通计算机。

高扩展性：服务器通常要配备大量的内存、硬盘、网卡等硬件设备，所以其扩展性要非常好。

网络操作系统简称NOS，是为了与网络上其他计算机便捷、有效地共享网络资源而开发的各种服务软件和有关规程的集合。网络操作系统与通常的操作系统有所不同，它以使网络相关特性达到最佳为目的，除了通常操作系统所具有的处理器管理、存储器管理、设

备管理和文件管理功能外，NOS还应具有以下两大功能：

1. 提供高效、可靠的网络通信能力。

2. 提供多种网络服务，如：远程作业录入处理服务、文件传输服务、电子邮件服务、远程打印服务等等。

常见的网络操作系统有Windows Server系列、Linux、Unix等。由于人们一般只会在服务器上进行维护操作，而不会进行类似普通计算机的应用操作，因此人们对服务器显示要求不高，有时会让多台服务器通过切换装置共享一个显示器。当具体的网络应用服务对服务器的性能要求不高时，也可以用普通计算机来替代服务器。

服务器的软件部分是指运行在服务器上的提供各种网络服务的软件。这些服务软件通常不会在服务器上显示复杂信息，而是通过网络对客户的请求进行响应。一台服务器可以同时安装多个网络服务软件，分别提供不同的网络服务。

服务器自身的特性决定了其对环境的特殊要求，因此通常置于专用的机房内，配以机柜、空调、UPS（不间断电源）等辅助设施，保证其能长时间不间断运行。

拓展链接

阿里云服务机房

走进阿里云机房，首先看到的是UPS系统。该UPS系统的部署是阿里自己设计的，保证在切断外部电源的情况下，服务器也能正常运行。

接下来看到的是服务器。一排排整齐的服务器，如同一面墙，墙上闪烁的灯光，如同繁星闪烁在夜空，给人无限遐想。这些是实实在在的物理服务器，而“云服务器”就存在于它们构成的虚拟世界中。这些服务器组成了一个集群，任何单个服务器出现故障都不会影响虚拟世界的正常运转。它们是阿里云根据高可用性和高性能的要求定制的，每台服务器都没有自己的电源模块，由专门的电源模块系统统一供电。

最后看到的是帮助服务器降温的空调系统。服务器很怕热，对环境的要求比较苛刻，因此，散热性能是机房设计中的重要指标。这里除了功能强劲的空调，还有自然风冷系统，当室外温度低于20℃时，自然风冷系统会自动启动，将室外的空气过滤后送入机房内，让服务器“呼吸”凉爽的新鲜空气。

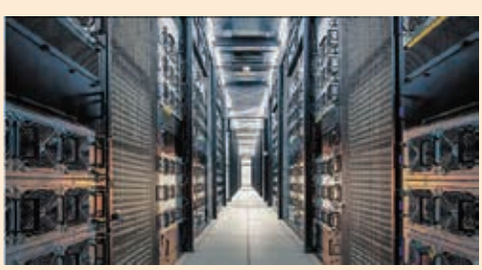


图3.1.2　阿里云服务机房

3.1.2　服务协议

网络服务协议是专门用于网络服务的协议。常见的网络服务协议有：HTTP、SMB、FTP、SMTP、POP3、DNS、DHCP，它们都属于应用层协议，这些协议规定了应用层数

据的交换方式。这些协议的使用都是建立在TCP/IP协议之上的。

表3.1.1　常见网络服务

服务类型	协议	服务软件
终端服务	Telnet	Telnet Server
文件共享	SMB	Samba、Windows操作系统
文件传输服务	FTP	IIS、ProFTPD
域名服务	DNS	DNS、Bind
万维网服务	HTTP	IIS、Apache、Nginx
电子邮件服务	SMTP、POP3	Exchange
动态主机配置服务	DHCP	DHCP Server
安全外壳协议	SSH	ssh

不同的网络服务使用不同的应用层协议。例如文件共享服务使用了SMB协议，网页浏览使用了HTTP协议，文件传输使用了FTP协议，等等。端口号用于区分不同的网络服务，应用层的不同应用各自绑定特定的TCP或UDP端口号。

网络服务一般有约定的端口号，但也可以按需要修改。与之连接的客户端程序也需要分配端口，这些端口号通常是随机分配的（见图3.1.3）。

协议	端口号
FTP	21、20
HTTP	80
Telnet	23
SMTP	25

图3.1.3　服务协议及端口

IP地址与端口的关系就好比房子与门窗的关系：如果把服务器的IP地址看作一座房子，端口是开在这个房子上的门，而且这样的门有很多，服务程序就是通过这些门与外界客户端程序进行数据交流。

服务端软件与客户端软件进行数据交流一般有两种模式：C/S模式和B/S模式（见图3.1.4）。C/S模式即客户端和服务器结构。这种结构通过将任务合理地分配到客户端和服务器端，降低了系统的通信开销，但

拓展链接

P2P模式

P2P是peer to peer的简写，是一种对等网络服务。位于两端的计算机既作服务器又作客户端。

软件需要针对不同的应用端设计不同的版本，QQ、微信就是典型的C/S模式。B/S模式即浏览器和服务器结构。这种模式其实是建立在C/S模式之上的，只是客户端用浏览器来代替，好处是大部分工作都由服务器来完成，客户端负荷较轻，维护成本低，软件设计只要设计服务端即可。缺点是对服务器性能要求较高，通信量大。常见的B/S应用有各种网站、论坛等。

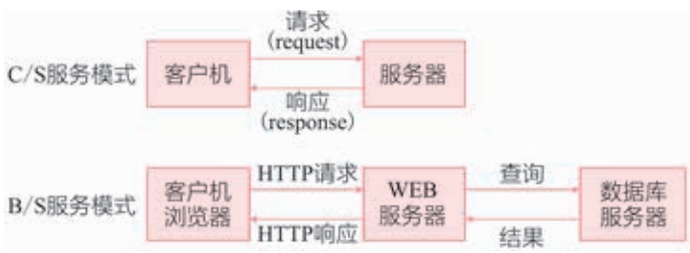


图3.1.4　服务模式的常见形式

思考与练习

结合网络服务的功能，说明为何有些网络服务使用TCP协议，有些使用UDP协议。

3.2 常见网络服务

网络服务在电子商务、电子政务及公司业务流程电子化等领域有着广泛的应用，是构建这些应用的基础技术，不同的应用使用一种或多种网络服务，如网上购物、网上就医、网上教育、电子银行用到了WWW服务和数据库服务，电子邮件用到了SMTP服务和POP3服务，等等。

3.2.1 终端服务

终端服务（Terminal Services）的客户机通过TCP/IP协议和网络与服务器互联，通过客户端的鼠标、键盘等的输入传递到终端服务器上，再把服务器上的显示传递回客户端。在终端服务中，客户端不需要具有计算能力，至多只需提供一定的缓存能力。终端服务主要包括客户端和服务器端两款软件，两款软件都可以安装在普通的计算机上，而非一定要将服务器端软件安装在服务器上。双方通过网络连接实现通信。

常见的终端服务有三种，第一种是命令行方式，如telnet、ssh等，通过网络远程登录到服务器，对服务器进行管理和维护。图3.2.1就是通过Telnet终端登录交换机的情况，这里的交换机充当了服务器的角色。此方式可以实现多用户登录。

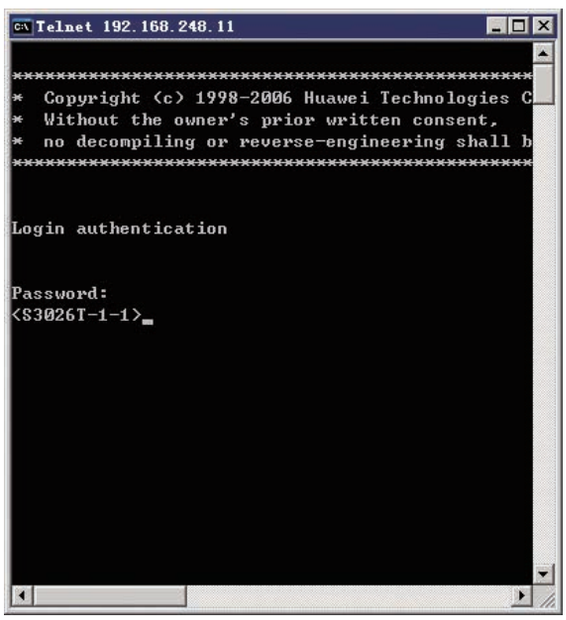


图3.2.1 Telnet登录交换机

第二种类似Windows远程桌面或Linux的Xmanager等软件（如图3.2.2）。该软件登录服务器后，服务器端的显示界面和终端的显示界面通常是不一样的。该方式也可以实现多用户登录，且每个用户的界面可以是不一样的。

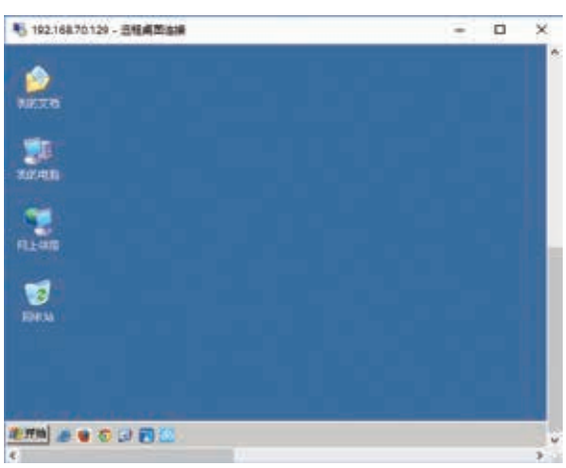


图3.2.2 Windows远程桌面

第三种类似Radmin软件（见图3.2.3）或虚拟网络控制台（Virtual Network Console，VNC），在该终端登录服务器后，终端屏幕

显示是与服务器屏幕同步的，该特点可以实现远程协助，协助者的操作都会在服务器端的屏幕中展现。该终端服务也可以实现多用户登录，但由于不同用户使用的是同一个界面，所以同一时刻只能由一个用户操作。

图3.2.3　Radmin软件界面

实践与体验

体验Windows远程桌面

目前使用的Windows系统都支持远程桌面，且操作系统缺省安装了客户端和服务器端软件，因此理论上客户端可以去登录任何一台联网的安装有Windows系统的计算机。

实践内容：

使用Windows远程桌面软件登录到同学的计算机。

实践步骤：

1. 启用计算机的远程桌面功能。

为了安全起见，缺省的Windows设置是不允许远程桌面连接的，需要进行如图3.2.4的设置。通过在“系统属性”窗口的“远程”选项卡中，勾选“远程桌面”栏，选中“启用这台计算机上的远程桌面”选项，启用远程桌面功能。

2. 由于Windows系统的安全性设计，密码为空的用户是无法通过远程桌面登录到系统的，因此需要设置登录用户名的密码，并将用户名和密码告诉登录者。

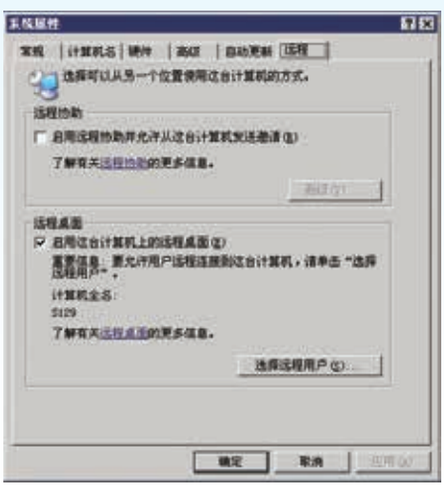


图3.2.4　远程桌面设置

3. 启动远程桌面客户端，输入同学计算机的IP，输入用户名和密码进行登录。
4. 查看对方计算机。

结果呈现：

同学之间轮流登录对方的计算机，展示登录后的界面。

3.2.2 文件共享

常用的文件共享包括基于SMB服务的文件共享和FTP文件共享。基于SMB服务的文件共享通常是指Windows系统中的文件共享，但在Linux系统中也可以使用，用户在共享目录中执行与普通目录几乎相同的操作，可以直接在共享目录中修改文件而无需下载和上传，该共享使用SMB协议，一般用于局域网。FTP可以用在局域网或因特网，但若想要修改FTP共享的文件，则需要先下载，待修改好后再上传，该共享使用了FTP协议。

在日常生活中，用户经常需要将文件从一台计算机拷贝到另外一台计算机，除了用U盘或移动硬盘拷贝外还可以使用文件共享的方式来实现文件的传输。

1. SMB协议

SMB（Server Message Block，服务器报文块）协议是共享文件（目录共享）和打印机的一种协议，它是Microsoft和Intel在1987年制定的主要用于Windows网络的通信协议，后来有人将其移植到Linux系统。SMB不仅提供目录和打印机共享，还支持认证、权限设置等。使用SMB协议的服务软件主要有Windows系统自带的文件共享软件和Linux系统中的Samba软件。

Windows中的文件共享一般和打印机共享合称为“文件和打印机共享”，是局域网络的一项重要应用（见图3.2.5）。Samba是在Linux系统上实现SMB协议的一个免费软件，由服务器及客户端程序构成，需要在系统中进行安装和配置。安装了Samba软件的Linux系统可以和Windows共享文件和打印机。

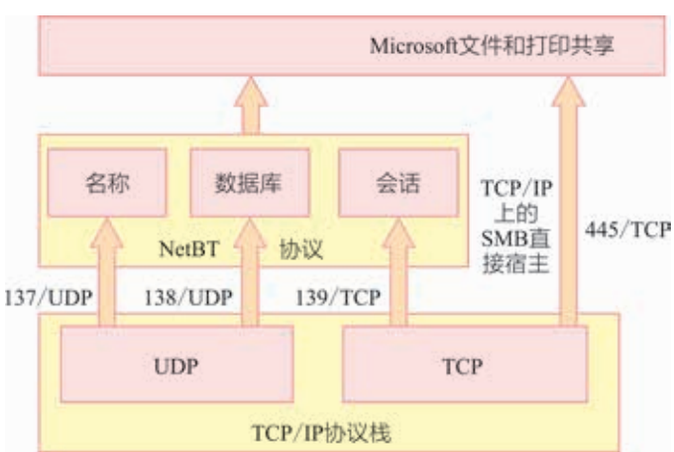


图3.2.5 文件和打印机共享协议

文件和打印机共享的工作模式是典型的C/S模式，只是Windows安装完成后，服务端和客户端软件一般都已经安装在计算机中，任意一台计算机都既可以成为服务端也可以成为客户端。

Windows文件和打印机共享一般需要三个程序：网络发现程序、文件和打印机共享程序、客户端程序。要正常使用文件共享功能，需要确保上述三个服务程序已启动，并开启了相应的功能。

2. FTP协议

FTP是文件传输协议（File Transfer Protocol）。在FTP的使用过程中，用户经常遇到两个概念：“下载”（Download）和“上传”（Upload）。“下载”文件就是从远程主机拷贝文件至本地的计算机上，“上传”文件就是将文件从本地的计算机中拷贝至远程主机上。

FTP服务器是在网络上提供文件存储和访问服务的计算机，它们依照FTP协议提供服务。FTP支持两种模式，一种是主动模式（PORT），另一种是被动模式（PASV）。一般使用的是被动模式。被动模式的FTP传输示意图如图3.2.6所示。

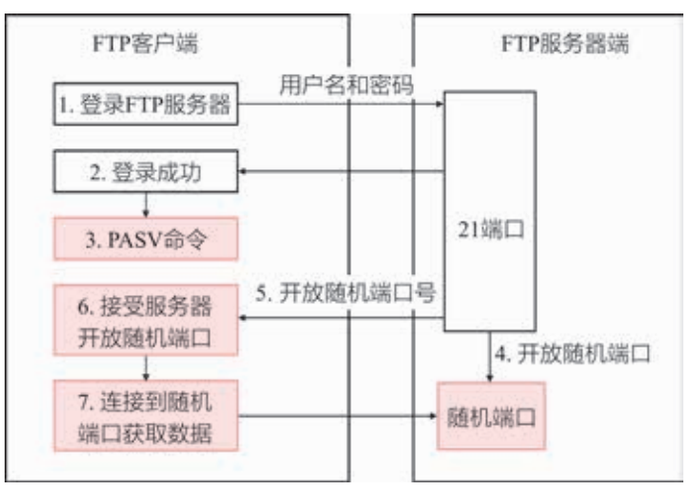


图3.2.6　FTP被动模式传输示意图

FTP服务类似于文件共享服务，但使用了不同的协议，所以其使用场景与文件共享并不完全重叠（见表3.2.1）。

表3.2.1　文件共享与FTP的比较

比较项	文件共享	FTP
协议	SMB	FTP
主要功能	打印机、文件共享	发布网站，文件共享
主要支持平台	Windows为主	Windows、Linux
主要使用范围	局域网	局域网、互联网
端口	137/138/139/445	21
权限设置	复杂	简单
在线编辑	可以	不可以

3. 共享过程

（1）共享资源列表

只有发现了资源，才可以有选择地进行访问。文件共享的网络发现程序定时对共享资源进行轮询并刷新网络共享资源列表，FTP客户端则是通过访问服务器获得。当共享文件有更新时，文件共享的资源列表一般会自动更新，而FTP资源列表则要手动刷新后才能更新。

（2）计算机名称解析

当用户访问共享资源列表时会发生一个名称解析过程。文件共享的名称解析使用DNS服务系统或基于TCP/IP的NETBIOS协议，而FTP则一般使用DNS服务进行解析，将共享计算机名称转换为该计算机的IP地址。

（3）访问计算机

当获得提供共享计算机的IP地址后，就可以开始访问该计算机了。在访问过程中首先要确定目标服务器上的协议、端口、组件是否齐备，服务是否已启动；其次要进行用户的身份验证。

另外，访问还受到被访问计算机的安全策略和权限限制，只有在这些限制都不存在的情况下，才能成功共享文件。其工作过程如图3.2.7所示。

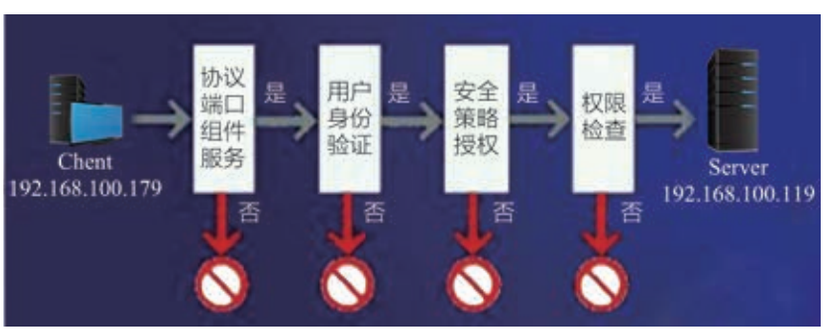


图3.2.7　共享资源的访问过程

问题与讨论

1. 怎样的情况下适合使用文件共享？怎样的情况下适合使用FTP？
2. 如何提高FTP服务器的访问安全性？

实践与体验

建立班级资源库

科技节、文化节等活动中，学校要求班级制作各种展示板卡进行展示。展示板卡是图文混排的，需要同学们分工合作，分别在互联网上搜索图片、文本等素材，然后编辑图片、编写文档，完成最后的作品。

实践内容：

1. 根据文件共享的特点，在计算机上创建班级资源库。根据实际需要，分别创建具有“完全控制”“读取/写入”“读取”权限的文件夹。

2. 让同一局域网的计算机访问该共享文件夹。

实践步骤：

1. 开启文件共享。

要确保所有共享资源的计算机都打开了“启用文件和打印机共享”“启用网络发现”等功能，如图3.2.8所示。

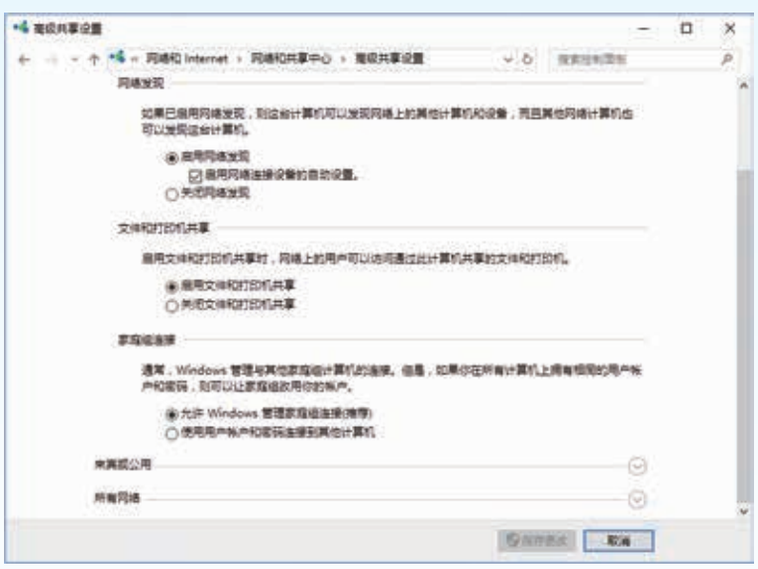


图3.2.8　共享设置

2. 完成文件夹的创建。

根据需要创建相应的文件夹，创建时要确保该文件夹所在的存储器有足够的容量。

3. 设置文件夹的共享权限。

可以在计算机内选择共享资源进行共享。在计算机中找到要共享的文件夹或打印机，在其上面单击右键，选择“属性”，在“属性”窗口中选择“共享”选

项卡，选择要与其共享的用户后就完成了共享设置，该文件夹就会出现在共享资源列表中。共享的文件资源一般有“完全控制”“读取/写入”“读取”三种权限，用户可以根据实际需要进行设置，如图3.2.9所示。

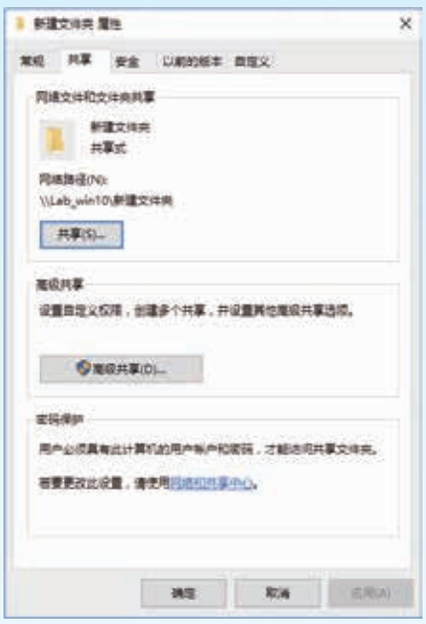


图3.2.9　共享权限设置

4. 通过局域网上的其他计算机访问共享文件夹，并在文件夹中进行新建文件、修改文件和删除文件操作。

结果呈现：

根据上面的操作，让其他同学通过局域网进行相应的测试，并填写表格。可以操作画“√”，无法操作画“×”。

操作	完全控制	读取	写入
创建新文件			
拷贝文件到该文件夹			
删除文件			
修改文件的权限			

3.2.3　Web服务

Web服务是目前互联网上应用最广的一种服务。浏览器通过HTTP协议访问Web服务器上的网页，网页文件可以很方便地从一个信息页连接到另一个信息页，不仅能查看文字，还可以欣赏图片、音乐、动画等。

1. HTTP 协议

HTTP（Hypertext Transfer Protocol，超文本传输协议）是目前互联网上应用最为广泛的一种网络协议，所有的WWW应用都必须遵守这个标准。

HTTP是客户端和服务器端之间的请求和应答的标准。通过使用Web浏览器、网络爬虫或者其他的工具，客户端发起一个到服务器上指定端口（默认为80端口）的HTTP请求，应答服务器根据请求将相关资源（HTML文件、图像文件等）发送给客户端。

一般客户端访问Web服务器要经过三个阶段：建立连接、传输内容、关闭连接。首先客户端使用HTTP命令向服务器发出Web请求（GET、POST等），服务器接收到Web请求后，就发送一个应答，并在客户端和服务器之间建立连接。然后服务器根据客户端的请求，查找相关文档，若找到，就会将该文档传送给客户端，否则就发送一个相应的错误提示文档给客户端。客户端接收到文档后，对文档进行解释并显示在屏幕上。最后，待传输完成后，服务器与客户端的连接就会关闭（见图3.2.10）。

拓展链接

HTTP请求

HTTP请求有两种最常用的方法：GET和POST。GET从指定的资源请求数据。POST向指定的资源提交需要被处理的数据。

图3.2.10　HTTP协议

HTTP协议使用明文传输，容易被窃听，为了弥补这一缺陷，需要使用另一种协议——安全套接层超文本传输协议HTTPS。HTTPS在HTTP的基础上加入了SSL协议，SSL依靠证书来验证服务器的身份，并为浏览器和服务器之间的通信加密。

2. URL

通过HTTP或者HTTPS协议请求的资源由统一资源定位器（Uniform Resource Locator，URL）来标识，URL是以统一的格式来描述信息资源（包括文件、服务器的地址和目录等）的字符串。互联网上的每个文件都有一个唯一的URL，它包含的信息指出文件的位置以及浏览器应该怎么处理它。

3. HTML

HTML（HyperText Markup Language，超文本标记语言），标准通用标记语言下的一个应用。“超文本”就是指页面内可以包含图片、链接，甚至音乐、程序等非文字元素。超文本标记语言的结构包括“头”部分（Head）和“主体”部分（Body），其中“头”部分提供关于网页的信息，“主体”部分提供网页的具体内容。（见图3.2.11）

```
<html>
    <head>
        <meta http-equiv="Content-Type" content="text/html; charset=gb2312">
        <title>标题</title>
    </head>
    <body>
        我的网页
        <a href="www.baidu.com">百度</a>
        <img src="images/photo.jpg">
    </body>
</html>
```

图3.2.11　网页的HTML代码

网页是网站的基本信息单位，使用HTML标准编写而成。网站通常是拥有相关内容的网页的集合，这些网页存放在一个或多个服务器内。通常把进入网站首先浏览到的网页称为首页，可以把首页看成是网站的门户。

拓展链接

HTML5

HTML5是对HTML标准的第五次修订，它可以在移动设备上支持多媒体。HTML5手机应用的最大优势是可以在网页上直接调试和修改。

4. Web服务器

Web服务器是可以向发出请求的浏览器提供文档的软件。Web服务器是一种被动程序，只有当互联网上其他计算机中的浏览器发出请求时，服务器才会响应。

Web服务器中的网页有静态网页和动态网页之分。静态网页也称为普通网页，静态网页不是指网页中的元素都是静止不动的，而是指服务器将网页文件不做改动，原样传输给浏览器，一般其文件扩展名为.htm、.html、.shtml或.xml等。在静态网页中，可以包括GIF动画、Flash动画或JavaScript程序。

动态网页是指在网页文件中除了HTML标记以外，还包括一些实现特定功能的程序代码，这些程序代码使得浏览器与服务器之间可以进行交互，即服务器端可以根据客户端的不同请求动态产生网页内容。动态网页的扩展名通常根据所用的程序设计语言的不同而不同，如.asp、.aspx、.cgi、.php、.perl、.jsp等。动态网页可以根据不同的时间、不同的浏览者显示不同的信息。常见的留言板、论坛、聊天室都是用动态网页实现的。

动态网页相对复杂，其运作流程分为以下四个步骤：

①用户在浏览器的地址栏中输入该动态网页的URL并按回车键（Enter），浏览器发送访问请求到Web服务器。

②Web服务器找到此动态网页。

③根据网页中的程序代码动态建立HTML流，并将其传输到用户浏览器。

④浏览器根据接收到的HTML流，显示网页的内容。

从整个工作流可以看出，用户浏览动态网页时，需要在服务器上动态执行该网页文件，将含有程序代码的动态网页转化为标准的静态网页，最后把静态网页发送给用户。其工作原理如图3.2.12所示。

图3.2.12　动态网页工作原理图

常用的Web服务器有Microsoft的互联网信息服务器IIS（Internet Information Services）、Nginx、Apache、Tomcat等。

IIS是Microsoft的Web服务组件，其中包括Web服务器、FTP服务器、NNTP服务器和SMTP服务器，分别用于网页浏览、文件传输、新闻服务和邮件发送等方面，它使得在网络上发布信息成了一件很容易的事。

Apache是Apache软件基金会的一个开放源码的网页服务器，可以在大多数计算机操作系统中运行，由于其多平台和安全性好而被广泛使用，是较流行的Web服务器端软件之一。

Nginx是一款轻量级的Web服务器、反向代理服务器及电子邮件（IMAP/POP3）代理服务器。它具有软件小巧、功能简单、占用内存少及并发能力强等特点，许多著名网站都使用了该服务软件，如百度、京东、新浪、网易、腾讯、淘宝等。

Tomcat服务器是开放源码的Web服务器，属于轻量级应用服务器，在中小型系统被普遍使用。Tomcat是Apache服务器的扩展，支持解释Java语言的动态网页。

问题与讨论

1. 在浏览器地址栏中只输入Web服务器的IP地址，会显示哪个网页文件的内容？

2. 当Web服务器的网页存储目录中有子文件夹时，该如何访问放在子文件夹中的网页？

3. 当用浏览器访问IIS服务器中的RAR文件时，浏览器将会如何处理？

实践与体验

在线商店

在线商店是目前使用非常广泛的一种Web应用，包括淘宝、京东等都是在线商店。在线商店通常由一台或多台Web服务器提供服务，用户通过浏览器发出浏览货物的请求，Web服务器发送货物清单；用户选择货物后，Web服务器根据选择的货物进行结算。现在，尝试用Nginx搭建一个简易的在线商店Web服务器。

实践内容：

尝试创建Web服务器，并实现简单的在线商店功能。

实践步骤：

1. 安装Nginx服务器。

从Nginx官网下载Nginx服务软件，下载完毕解压到C盘或D盘的根目录下，然后双击其中的nginx.exe可执行文件启动服务，如图3.2.13所示。

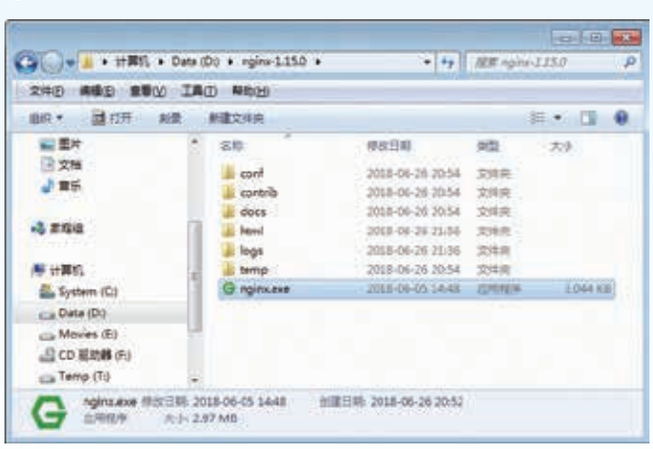


图3.2.13　Nginx服务软件目录

由于nginx.exe是服务程序，启动后没有任何显示，但可以通过任务管理

器查询到nginx进程。如果要结束服务，可以在nginx目录下，在命令行中输入“nginx -s quit”来结束。

2. 访问网站。

只要在浏览器中输入http://服务器IP，若显示“欢迎”的页面，则说明Nginx服务器运行正常。如果是在本机上测试，可以输入“127.0.0.1”。

3. 发布在线商店。

接下来要把在线商店的HTML文档和链接图片等文件放入网站主目录中，Nginx的缺省主目录位于html目录下，也可以根据实际需要进行调整。在线商店的首页index.htm文档的HTML代码如下所示。

首页index.htm代码：

```
<html>
<head>
<meta http-equiv="Content-Type" content="text/html; charset=gb2312">
<title>在线商店</title>
<style type="text/css">
div{
        float: left;
        width: 25%;
        text-align: center;
}
p {
        text-align:center;
}
</style>
</head>

<body>
 请选择要购买的商品:
 <hr>
<form action="submit.htm" method="get">
  <div>
   <img src="cup.jpg"><br>
   <input name="cup" type="checkbox" value="10.5">
   10.50元/只</div>
  <div>
   <img src="kiwifruit.jpg"><br>
   <input name="kiwifruit" type="checkbox" value="5">
   5.00元/个</div>
  <div>
   <img src="milk.jpg" ><br>
   <input name="milk" type="checkbox" value="4.4">
   4.40元/盒
```

```
  </div>
  <div>
    <img src="pen.jpg" ><br>
    <input name="pen" type="checkbox" value="5.7">
    5.70元/支</div>
  <hr>
  <p>
    <input type="submit" value="提交">
 </p>
 </form>
</body>
</html>
```

提交页 submit.htm 代码：

```
<html>
<head>
<meta http-equiv="Content-Type" content="text/html; charset=gb2312">
<title>在线商店</title>
<style type="text/css">
#total {
        font-size: 18px;
        font-weight: bold;
        text-align: center;
}
</style>
</head>
<body>
所选商品价格合计:
<hr>
<div id="total"></div>
</body>
<script>
 var urlinfo = window.location.href;
 var len = urlinfo.length;
 var offset = urlinfo.indexOf("?");
 var info = urlinfo.substr(offset+1, len)
 var ids = info.split("&");
 var t = 0;
 var i = 0;
 while (typeof(ids[i]) != "undefined") {
        t = t + parseFloat(ids[i].split("=")[1]);
        i = i + 1;
 }
 document.getElementById('total').innerHTML = t.toFixed(2) + " 元";
</script>
</html>
```

结果呈现：

当在浏览器地址栏里输入网站的IP或域名时，Web服务器会把首页文档发送给浏览器。上面的首页显示效果如图3.2.14所示。当用户选择相应的商品后单击“提交”按钮，浏览器又会把商品的选择信息发送给Web服务器，Web服务器会返回submit.htm文档给浏览器，显示商品的总价，如图3.2.15所示。

图3.2.14　在线商店主界面

图3.2.15　在线商店价格页面

思考与练习

1. 如果一个共享文件夹的共享权限设置为“读取/写入”，而安全权限设置为“读取”，那么网络用户对这个文件夹拥有怎样的操作许可？共享权限与安全权限之间是什么样的关系？

2. 创建一个Web服务器，并存放一个显示自己照片和姓名的网页，将网页的URL分享给其他同学，进行相互访问。

3.3 网络服务的发展

日新月异的信息技术推动网络服务不断向前发展。目前网络服务主要向云服务、生态链、智能化、区块链等方向发展，但其基础还是建立在传统的网络服务之上。

3.3.1 云服务

云服务，也叫云计算服务。云计算通过互联网云服务平台按需提供计算能力、数据库存储、应用程序和其他IT资源，包括云主机、云空间、云开发、云测试和综合类产品等。目前著名的云服务包括阿里云、AWS（Amazon Web Services，亚马逊云服务）、Azure（微软云服务）等。

我们平时提及的云服务，则是在云计算技术支撑下的对外提供的按需分配、可计量的一种IT服务模式。这种服务模式可以替代用户本地自建的IT服务。例如：用计算机处理文档、存储资料，通过电子邮件或U盘与他人分享信息。在这种服务模式下，如果计算机硬盘坏了，用户会因为资料丢失而束手无策。而在“云计算”时代，“云”会替用户做存储和计算的工作，我们只需要一台能上网的手机，一旦有需要，可以在任何地点用手机快速地找到所需要的资料并处理它们，再也不用担心资料丢失。

另外，云服务足够智能，能够根据用户的位置、时间、偏好等信息，实时地对需求做出预期。在这一全新的模式下，信息的搜索是“为用户而做”，而不再是“由用户来做”。无论用户采用什么设备，无论用户需要哪种服务，用户都将得到一个一致且连贯的良好体验。

1. 云服务类型层次

云服务包含三个主要层次，通常称作基础设施即服务（Infrastructure as a Service，IaaS）、软件即服务（Software as a Service，SaaS）和平台即服务（Platform as a Service，PaaS）。这三个层次组成了云计算技术层面的整体架构，这中间可能包含了一些虚拟化的技术和应用、自动化的部署以及分布式计算等技术，这种技术架构的优势就是可以对外表现出非常优秀的并行计算能力以及具有大规模的伸缩性和灵活性等特点。

（1）IaaS

IaaS是把数据中心、基础设施等硬件资源通过Web分配给用户的商业模式。消费者通过互联网可以从完善的计算机基础设施获得服务。

（2）SaaS

SaaS是一种通过互联网提供软件的模式，用户无需购买软件，而是向提供商租用基于Web的软件来管理企业的经营活动。SaaS模式大大降低了软件尤其是大型软件的使用成本，并且由于软件在服务商的服务器上托管，因此减少了客户的管理维护成本，可靠性也更高。

（3）PaaS

PaaS将软件研发的平台作为一种服务，以SaaS的模式提交给用户。因此，PaaS也是SaaS模式的一种应用。但是，PaaS的出现可以加快SaaS的发展，尤其是加快SaaS应用的开发速度。PaaS服务使得软件开发人员可以在不购买服务器等设备环境的情况下开发新的应用程序。

2. 虚拟化

虚拟化或虚拟技术（Virtualization）是一种资源管理技术，是将计算机的各种实体资源（CPU、内存、磁盘空间、网络适配器等），予以抽象、转换后，使其成为可供分割、组合为一个或多个计算机的资源单位。由此，打破实体结构间不可切割的障碍，使用户可以用比原本的配置更高效的方式来应用这些计算机硬件资源。这些资源的虚拟部分不受现有资源的架设方式、地域或物理配置所限制。一般所指的虚拟化资源包括计算能力和数据存储。

云服务相当于把分布于各处的资源集中在一起统一管理和分配，而虚拟技术则把硬件设备分拆成可以分配的虚拟单元。所以从某种程度上讲，虚拟化技术是云服务的基础。如图3.3.1所示，虚拟技术将一台计算机虚拟成六台虚拟计算机，这六台虚拟计算机拥有各自虚拟的CPU、内存、磁盘、网卡等，可以安装不同的操作系统，操作上同普通计算机没有什么区别。常见的虚拟化有虚拟主机、虚拟桌面、虚拟网络等。

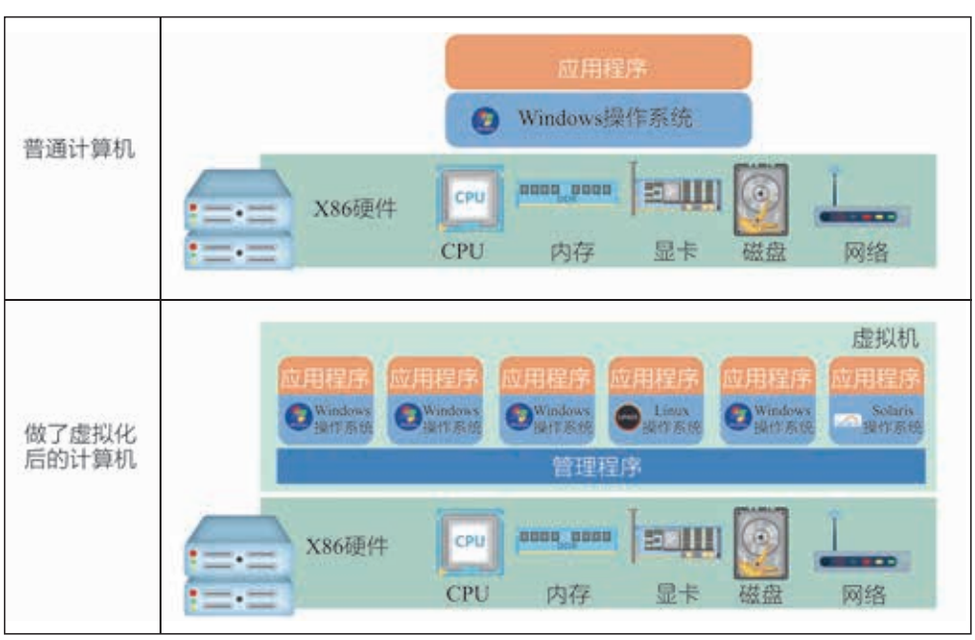


图3.3.1　虚拟化示意图

3. 云服务应用

常见的云服务应用包括云计算、云存储、人工智能、物联网等方面。

（1）云计算

云计算应用相当于把原来的计算机虚拟化后放置在云端，以实现可弹性扩展、安全、稳定、易用的计算服务。常见的云计算应用包括云服务器、批量计算、高性能计算、负载均衡等。

（2）云存储

云存储是指通过集群应用、网络技术或分布式文件系统等功能，将网络中大量不同类型的存储设备通过应用软件集合起来协同工作，共同对外提供数据存储和业务访问功能的系统。

当将大量数据的存储和管理作为云计算系统运算和处理的核心时，就需要配置大量的存储设备，云计算系统就转变成为一个云存储系统，所以云存储是一个以数据存储和管理为核心的云计算系统。简单说来，云存储就是将储存资源放到云上，使用者可以随时随地通过任何可联网的装置连接到云上并方便地存取数据。

（3）人工智能

人工智能包括智能识别（见图3.3.2）、人工大脑、各种智能解决方案等，常见的应用有城市智能化管理、智能医疗、图片识别、机器学习等。用户通过与云服务接口对接，可以方便地快速实现各种人工智能分析。

图3.3.2　人脸属性识别

（4）物联网

云端和物联设备进行稳定的双向通信，并提供规则引擎互联物联网设备与众多云产品，用户只需在Web上配置规则即可享受数据采集、数据计算、数据存储等服务，快速灵活构建物联网应用体系（见图3.3.3）。

图3.3.3　小米物联网

总之，传统的网络服务都可以放到云端，然后再通过网络提供相应的云服务，以达到节约资源、灵活部署、安全可靠、方便管理的目的。

实践与体验

体验人脸识别

人脸识别（Face Recognition）实现了图像或视频中人脸的检测、分析和比对，包括人脸检测定位、人脸属性识别和人脸比对等独立服务模块，开发者通过在线云服务，实现人脸AR、人脸识别和认证、人脸检索、照片管理等各种场景。（见图3.3.4）

图3.3.4　人脸比对

实践内容：

注册登录阿里云平台，选择“产品”菜单下的“人脸识别”，点击“免费体验”进入免费体验页面（见图3.3.5）。体验人脸识别功能及查阅接口文档。

图3.3.5　人脸识别页面（图片来自阿里云）

实践步骤：

1. 准备几张带有人脸的照片，其中一些是同一个人的不同照片。
2. 进入“人脸识别”下的“免费体验”界面。

3. 进行“人脸监测定位”“人脸属性识别”“人脸比对”等体验。
4. 分小组讨论该云服务的各种应用场景。

结果呈现：

描述小组讨论后的“人脸识别”应用场景。

3.3.2 互联网生态

网络服务商和传统企业在互联网上通过数据链路相互发生联系，它们既彼此依赖、相互合作，又激烈竞争、互相兼并，这种新兴的、复杂的关系称为互联网生态。互联网生态一般由多条生态链构成，如互联网出行生态由“平台＋内容＋应用＋终端”的服务链构成其中的多条生态链，生态链中同一层次的不同系统间构成行业竞争关系。

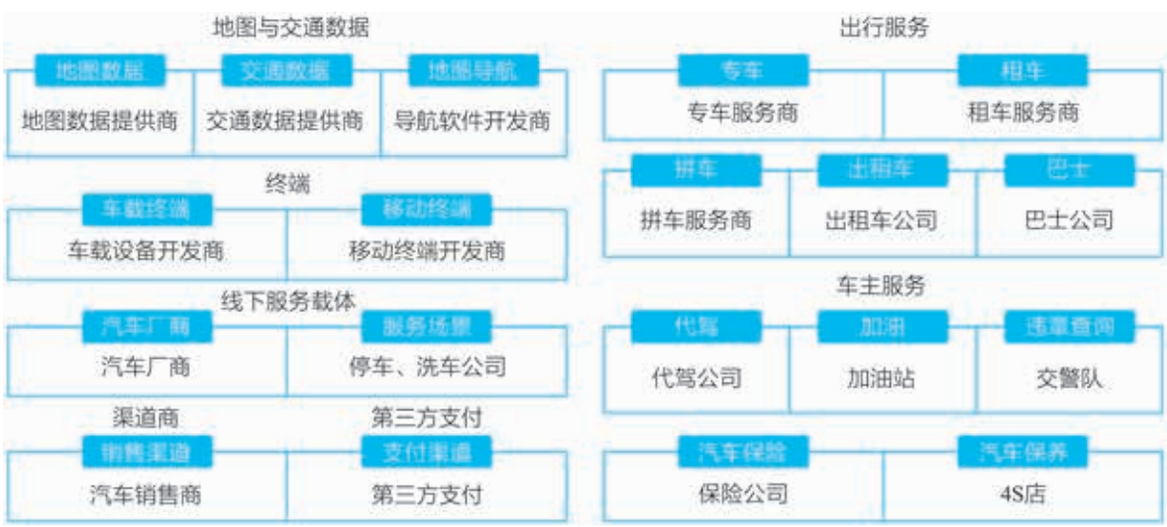


图3.3.6　互联网出行产业生态

互联网生态的生产者产生数据，如地图数据提供商通过卫星遥感、人工测量等方式收集数据并绘制地图，交通部门通过大数据分析产生车辆拥堵数据，导航软件开发商开发的软件本身也是数据的一种，如图3.3.6 所示。

消费者通过生产者或下层消费者产生的数据实现服务，服务过程中产生的数据又可以提供给上层消费者去实现新的服务。如车载设备商的导航终端通过安装导航软件、下载地图数据和交通数据，生成实时的导航数据，为用户提供导航服务，同时又将行驶数据反馈给导航公司，用于导航软件改进和交通大数据分析。在这里，车载设备商既是消费者，也是生产者。

同一行业的服务商，不管是生产者还是消费者，都会产生竞争关系，如专车服务商之间、共享单车提供商之间的竞争就非常激烈。如果服务商能保持合法、正当的竞争关系并

不断提高服务水平，将有利于行业的健康发展，反之，则有可能形成行业垄断，对行业造成不利影响。

问题与讨论

观察社会生活，通过与生物学有关知识的类比，分小组讨论其中有关互联网生态的实例，根据讨论结果填写下面的表格。

_____生态		
生产者	消费者	生产者与消费者的关联途径

3.3.3 网络服务展望

随着世界数字经济发展进入快车道，作为塑造全球数字化格局的重要力量，中国将顺应互联网发展带来的历史机遇，以数字经济为重要驱动力，在产业投资、商业模式和全球治理等多个领域引领全球新趋势，相关的网络服务可能会向以下五个方向深入发展。

（1）基础网络服务将得到升级。随着互联网在物联领域的拓展，现有的IPv6将获得普及，互联网体量将获得极大的扩张，物联时代的来临对现有的网络服务提出了更高的要求，使其不断获得提升和发展，Web标准、网络传输协议、HTML标准都将不断完善。

（2）新的网络服务将会涌现。虚拟现实、自动驾驶、3D打印、机器人、无人机、人工智能、物物相联等众多技术的进步和分布式网络服务思想的普及，促使人们研发新型网络服务。

（3）云服务将更加普及。云服务提供的大量服务足够专业和有效，可以让原来高端的服务触手可及，如人脸识别、大数据、人工智能等。

（4）互联网将与各行各业深度融合。“互联网＋”经济已获得了巨大的社会效益，得到了各行各业的认可。接下来，互联网的触须将会伸到行业的各个角落，与其深度融合，让传统行业得到升华，而这一切都和网络服务是密不可分的。

（5）大数据服务将实现对社会的反馈。大数据的反馈包括三个方面：一个是生产与消费之间的反馈，就是根据消费进行生产，如通过淘宝、京东等电商平台的农产品的消费指导农民进行生产；第二个是行为与管理的反馈，让管理更加科学和智能，如根据交通的拥

堵状况，管理道路导向；第三个是需求与服务之间的反馈，根据大数据分析可以获知人们的需求，从而可以有的放矢地提供相应的服务。物联网、云计算与大数据相结合可以产生更大的价值。

思考与练习

1. 要把Web服务转为云服务，实现与普通Web服务同样的功能，一般需要由哪些云服务构成？

2. 你认为未来的网络服务会包括哪些方面？

巩固与提高

1. 从网上下载VNC软件，将其服务软件安装到计算机，客户端软件安装到另一台计算机，尝试进行远程访问。

2. FileZilla Server是一款免费开源的FTP服务软件，请尝试使用FileZilla Server创建FTP服务器，并用FTP客户端远程访问该服务器。

3. 从网上下载Apache，在Windows下安装配置一个基于Apache的Web服务器。

4. IIS拥有域名绑定功能，可在同一个IP下运行多个网站应用，请你在IIS中找出对应功能，并进行多域名配置。

项目挑战

创建团队云

私有云是用户单独构建的云服务器，由于其核心资源都属于用户自己，因此具有安全和可控的特点，特别适合企业和团队的使用。

项目任务

我们的团队（班级、社团、兴趣小组等），在活动过程中经常会产生一些专有资料，为保证这些资料的安全，同时方便团队成员的交流与分享，需创建团队私有云。

过程与建议

1. 选择开源私有云

目前因特网上的开源私有云主要有Seafile、ownCloud等。这些私有云的功能类似，但又有自身特点。请下载相关说明文档，填写下表，并对它们的功能进行比较。

注：阅读说明文档，如软件具有相应功能，就在对应的单元格中画“√”，否则画“×”。

	Seafile	ownCloud	其他
云存储			
分享功能			
消息通信			
群组讨论			
跨平台同步			
其他：			
其他：			

根据团队的需要，基于以上分析，确定最终使用的私有云软件并说明原因。

2. 下载并部署私有云

（1）下载安装。为了防止系统被篡改，要从官方网站下载相应软件，可以通过校对验证码来进一步保证软件的安全性。

（2）配置调试。不同的软件都有不同的配置方式，可以通过参考软件配置文档，按照文档说明，结合团队需求进行配置。

（3）个性化。团队文化往往可以通过Logo、文字、符号、仪式化活动等来传递，具

体到私有云上也会有体现团队个性的空间。

3. 讨论确定团队沟通规则

团队云从技术上给我们提供了便利，但想要解决问题，纪律性也是不可或缺的要素。在使用团队云时，我们可以约定哪些规则？可以从文件命名、分享规则、点评原则等方面集体讨论，制订团队云使用规则。

4. 展示交流

请从任务完成过程、完成情况、团队沟通规则等方面与其他团队进行交流分享，一起查找问题，借鉴优点，继续完善。

评价标准

请根据项目实施的过程、效果以及成果展示交流的结果，对自己完成项目的情况进行客观的评价，并思考后续完善的方向。把评价结果和完善方案填写在下面的表格中。

评价条目	说明	评分（1～10分）	评分主要依据阐述	后续完善方向
软件选择	选择的开源私有云软件与团队云需求的契合程度			
安装部署和调试	成功安装部署并通过调试运行，保证团队云的正常使用			
个性化	团队云部署精致，契合团队文化			
团队沟通规则	团队沟通规则的可操作性			
展示分享	展示方式的合理性（是否能让人较好地了解项目的意义以及问题解决过程中的亮点）			

拓展项目

阿里云是全球知名的云计算及人工智能科技公司，其服务对象不乏制造、金融、政务、交通、医疗、电信、能源等众多领域的领军企业。现在请你分析阿里云所提供的各种服务，结合某IT公司的网络需求，在阿里云中配置符合该公司需求的服务系统。需求包括：

（1）有公司网站的发布空间，能在因特网上展示公司。

（2）可以方便地维护公司网站，易于上传/下载网页或文件。

（3）估计上述配置的成本，包括一次性成本和周期性成本（如包月费用）。

第四章 4

物联网

互联网渗透到信息社会的方方面面，已成为人与人交流沟通、传递信息不可或缺的纽带；在互联网基础上产生的物联网，依托传感技术、嵌入式技术和分布式处理技术，借助各类传感器、射频模块和通信网络，实现了人与物、物与物之间的通信与交流。随着互联网和物联网的进一步融合，将实现整个生态体系的高度智能化。

问题与挑战

- 网络监控系统通过安装在家里的摄像头，借助手机等移动终端随时远程查看家里情况，给我们的生活带来极大的便利。从技术层面分析，构建一个家用网络监控系统需要哪些硬件设备和软件系统？

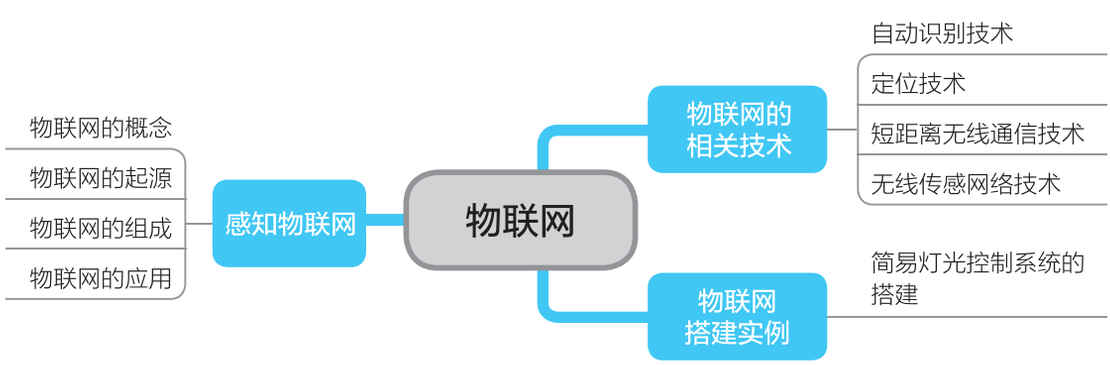
- 1995年比尔·盖茨（Bill Gates）提出了“未来屋”的概念，当时人们觉得那是在很遥远的将来才能实现的事，但在二十多年之后的今天，其中的大多数构想已经实现，特别是近年来，物联网更是快速发展。那么，物联网会对我们学习与生活的方式带来怎样的影响？

- 物联网技术使“智能家居”由概念走向现实。现在很多的系统可以帮助我们随时随地实现各类控制，比如说灯具、窗帘及电器控制等。这些“智能家居”是如何搭建和实现的？

学习目标

1. 了解物联网的发展历程，理解物联网的概念。
2. 了解日常生活中物联网相关设备，理解物联网的工作原理。
3. 探讨物联网对生活、工作与学习的影响。
4. 了解如何搭建简单的物联网系统。

内容总览



4.1 感知物联网

在电影《阿凡达》中，生活在潘多拉星球的“纳美人”只要用自己的辫子与大鸟相连，就可以乘大鸟展翅高飞，物物相通的科幻场景给观众留下深刻印象。物联网自从其诞生以来，引起了巨大关注，被认为是继计算机、互联网、移动通信网之后的又一次信息产业浪潮，被广泛应用于医疗、农业、家居、交通等领域。阿凡达式的世界并不遥远，物联网时代正在到来。

4.1.1 物联网的概念

物联网（Internet of Things，简称IoT）是在互联网基础上延伸和扩展的网络，是各种传感技术的综合应用，通过射频识别、红外感应器、全球定位系统、激光扫描器等传感设备，依据相关协议，把物品与互联网相连接，方便识别和管理。

世间的万事万物，大到整个城市、楼房、汽车，小到一部手机、一块手表甚至一把钥匙，只要在里面嵌入一个感应器，这个物品就可以“成活”，随时可以和你“对话”，也可以和其他物品“交流”。自从人们运用物联网技术后，似乎万物被“拟人化”了，每个物体都可寻、可控、可连。

例如智慧养老系统（如图4.1.1所示），系统会通过各类传感器向家人告知家中老人的生活起居和身体健康情况，使老人的日常生活处于远程监控状态，让老人的需求触手可及。在智慧养老系统中，如果老人想休闲，系统会自动告知老人当天的电视节目、社区开展的活动等内容。如果安装了智慧开关，老人睡觉时也不用起床关灯，晚上起夜也不用摸黑，即使老人忘记关灯，即便子女不在家，甚至远隔千里，子女也可以通过手机关灯。一旦老人住所内的水龙头连续24小时没有开启，报警系统就会通过电话或短信提醒其亲友，看看老人是否外出或出现意外。

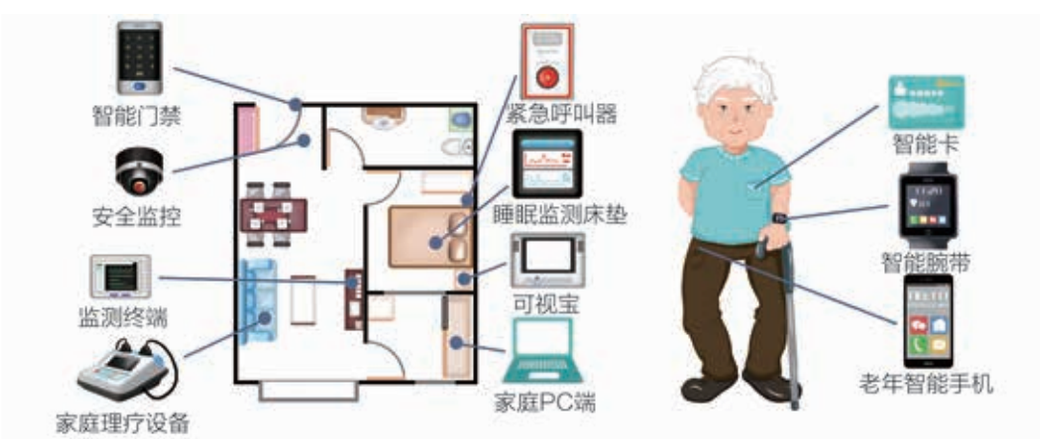


图4.1.1 智慧养老系统

智慧城市物联网系统，能随时获取信息并通过数据中心整合物联网，真正实现智能化、自动化及精细化的“未来城市”，而与人们生活息息相关的智能家居的普及更不是梦想。

4.1.2 物联网的起源

物联网的起源要追溯到1991年，当时剑桥大学特洛伊计算机实验室的科学家常常要下楼去看咖啡煮好了没有，但又怕影响工作，为了解决这一问题，他们在咖啡壶旁边安装了一个便携式摄像头，并编写了一套程序，利用终端计算机的图像捕捉技术，以3帧/秒的速率传递到实验室的计算机上，以方便工作人员随时查看咖啡是否已煮好，这就是物联网的雏形。就网络数字摄像机而言，确切地说，其市场开发、技术应用以及日后的种种网络扩展都是始源于这个世界上最负盛名的“特洛伊咖啡壶”，如图4.1.2所示。

图4.1.2 特洛伊咖啡壶

1995年，比尔·盖茨（Bill Gates）在《未来之路》一书中提到了“物联网”的构想，指出“互联网仅仅实现了计算机的联网而没有实现万事万物的互联”，而这在当时并没有受到关注，正如书中写的一样，“虽然现在看来这些预测不太可能实现，甚至有些荒谬，但是我保证这是本严肃的书，绝非戏言。十年后我的观点将会得到证实”。

从1999年凯文·艾什顿（Kevin Ashton）的那句“万物皆可通过网络互联”开始，物联网不断汲取各方面技术，快速成长。

2005年11月17日，在突尼斯举行的信息社会世界峰会上，国际电信联盟（International Telecommunication Union，ITU）发布了《ITU互联网报告2005：物联网》，报告指出，无所不在的物联网通信时代即将来临，世界上所有的物体从轮胎到牙刷、从房屋到纸巾都可以通过互联网主动进行数据交换。射频识别（Radio Frequency Identification，RFID）技术、传感器技术、纳米技术、智能嵌入这四项技术将得到更加广泛的应用。

2005年，物联网已经不再局限于RFID技术，开始扩展到任意物与物之间的信息互联，物联网的覆盖范围有了更大的拓展。2009年，物联网诞生10周年，时任国务院总理温家宝公开表示，物联网是中国的一个重要产业，并宣布将对物联网产业进行巨额投资，“智慧地球”“中国式物联”等一系列概念被搬上历史的舞台。

得益于物联网技术的飞速发展，人们即将进入一个万物互联的新世界，预计未来几年内，物联网连接的设备数量将会达数百亿，该产业也因此被视作全球经济增长的新引擎。

拓展链接

中国信息通信研究院物联网白皮书

2009年国家提出发展物联网之后，中国信息通信研究院在2011年5月发布了第一本白皮书，当时中国信息通信研究院重点从系统梳理的角度进行了原创性的梳理工作，提出了整个物联网发展的概念、内涵，还有架构体系、技术体系和关键要素等。之后中国信息通信研究院每年都会发布《物联网白皮书》。

4.1.3 物联网的组成

按照功能划分，物联网设备可划分为感知层、网络层和应用层，如图4.1.3所示。全面感知、可靠传送、智能处理是物联网的三大基本特征。

图4.1.3 物联网的组成

感知层是物联网发展和应用的基础，包括条码识读器、传感器、摄像头等数据采集设备和数据接入网关前的传感器网络等。

传感器是一种检测装置，能将被测信息按一定规律转换成电信号输出，以满足信息的传输、处理、存储、显示、记录和控制等要求。例如，测量体温的电子体温计就是常见的传感器，它将人体温度转换成电信号，利用显示器显示温度数字，如图4.1.4所示。传感器是感知层的核心部件，一般由敏感元件、转换元件、测量电路三部分组成。

图4.1.4 电子体温计

感知层以RFID、传感与控制等短距离无线通信为主要技术，识别物体和采集系统中的相关信息，从而实现对物的认识与感知，类似于人的感知器官。

网络层是物联网的中间层，主要负责传送感知层获取到的各种感知数据，实现共享与有效处理。通信技术，尤其是无线通信技术的发展，为物联网提供了可靠的传输通道，如图4.1.5所示。

图4.1.5　通信技术

网络层基本上综合了已有的各种网络形式来构建更加广泛的互联网络。网络层设备主要包括各种网络交换机、路由器、网络传输设备及Wi-Fi设备等。

应用层将感知到的数据进一步加工处理，与行业需求结合，为用户提供丰富的特定服务，实现物联网的智能应用。例如在智能电网中的远程电力抄表应用，安置于用户家中的读卡器是感知层的传感器，这些传感器在收集到用户的信息后，通过网络发送并汇总到核心处理设备上。该处理设备及其对应的工作属于应用层，将分析用户用电信息，并自动采取相关措施，如图4.1.6所示。

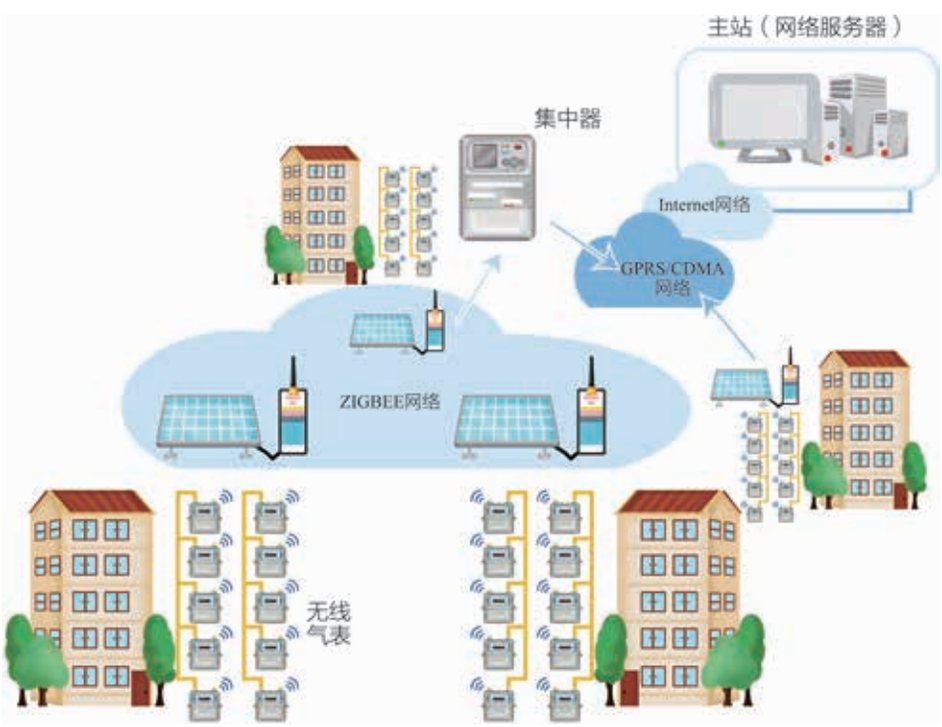


图4.1.6　基于物联网技术的全无线自动抄表系统

应用层主要由中间件、应用和云计算组成。应用层设备主要包括服务器、云存储、各种中间件及各种软件。

4.1.4 物联网的应用

现如今，物联网已广泛应用于公共事务管理、公众社会服务及经济发展建设等多个领域，如图4.1.7所示。接下来，我们将围绕“智能医疗”“智能农业”“智能家居”和“智能交通”四方面展开应用分析。

图4.1.7 物联网应用领域

1. 智能医疗

智能医疗是通过打造健康档案区域医疗信息平台，利用传感器等物联网技术，实现患者与医务人员、医疗机构、医疗设备之间的互动等，使医疗逐步达到信息化和智能化。

依靠物联网技术，在不同的医疗机构建立起医疗信息整合平台，将医院之间的业务流程进行整合，使得医疗信息和资源可以共享与交换，跨医疗机构也可以进行在线预约和双向就诊。智能医疗还将实现对医院资产、血液、医疗废弃物、医院消毒物品等的管理，在药品生产上，通过物联网技术实施对生产流程、市场的流动以及病人用药的全方位的检测等。图4.1.8所示为我们对智能医疗的展望。

图4.1.8 智能医疗图解

2. 智能农业

传统农业生产活动中的灌溉、施肥及打药等作业，农民只能依靠经验。而通过物联网的应用，这些作业都会在信息化智能监控系统的控制下实现实时定量的“精确”把关，农民只需按个开关，或是完全听从“指令”，就能种好菜、养好花。

“智能农业”系统及其整体解决方案，可以实现农产品从选种、育苗，到生产管理、订购销售、物流配送、质量安全溯源等产、供、销全过程的高效感知及管控，促进传统农业向智能农业转变。它涵盖农业规划布局、生产、流通等环节，主要由以下三大子系统构成：农产品溯源系统、精准农业生产管理系统和农业专家服务系统（如图4.1.9所示）。

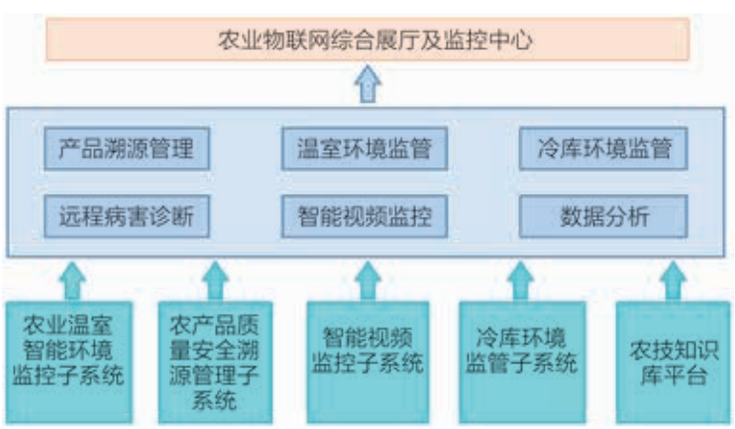


图4.1.9　智能农业系统结构图

3. 智能家居

智能家居是利用先进的计算机技术、网络通信技术、综合布线技术、自动控制技术及音视频技术等，依照人体工程学原理，融合个性需求，将与家居生活有关的各个子系统，如安防、灯光控制及煤气阀控制等有机地结合在一起，通过网络化综合智能控制和管理，

构建高效的住宅设施与家庭日程事务的管理系统，提升安居安全性、便利性及舒适度，同时又贯彻了环保节能理念。

通过智能家居，可智能控制移动报警、热水器、电视影音、温度、亮度等，如图4.1.10所示。

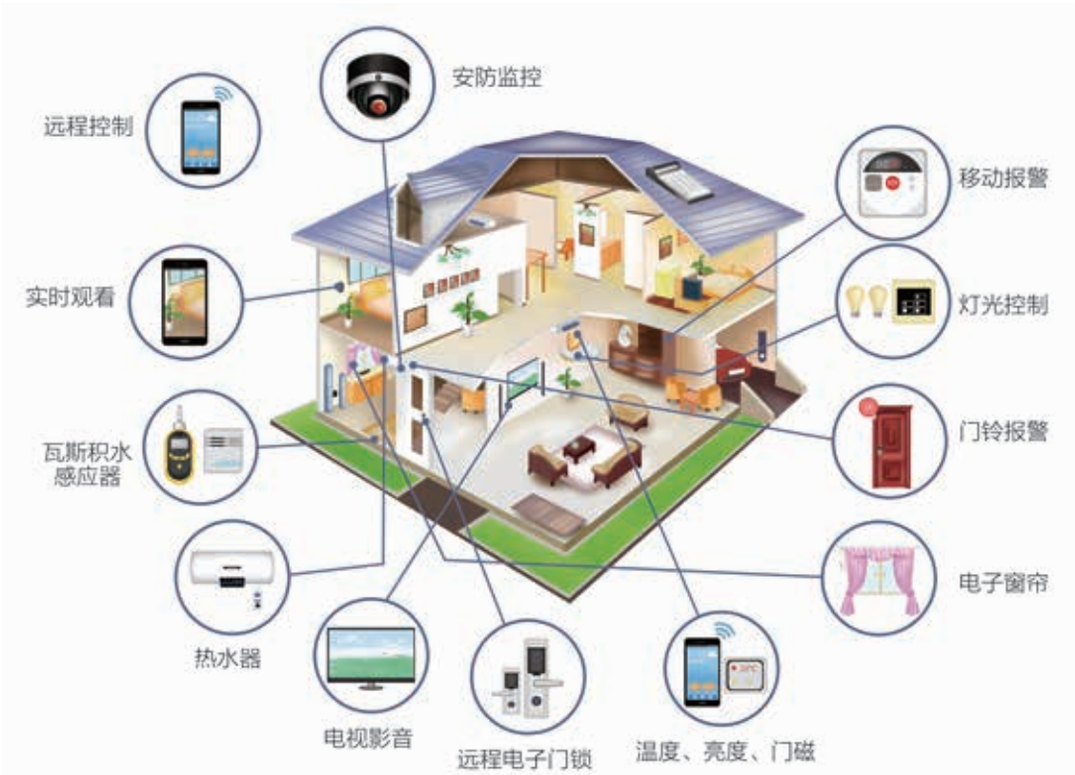


图4.1.10　手机控制智能家居

4. 智能交通

智能交通系统（Intelligent Transportation System,简称ITS）是由运输工具、运输道路和运营管理组成的一个庞大而复杂的系统，是运用高科技手段解决当今交通运输问题的新技术，是计算机、人工智能、图像处理、视觉理论、电子及交通运输管理等技术的综合应用。

道路交通信息通信系统主要是向驾驶员提供必要的最新道路交通信息，其涉及的硬件设备有很多，包括设置在醒目位置的可变信息板、车载导航设备、车上FM（调频）广播接收设备等。

智能交通系统包括智能导航系统、不停车收费系统（Electronic Toll Collection，简称ETC）、道路救援系统等。在这些系统当中，高效、安全地反馈信息是关键。

思考与练习

1. 列举我国物联网推动计划主要事件。

序号	年份	事件
1	1999年	中科院启动传感网的研究，建立了一些适用的传感网

2. 列举生活中物联网应用的典型案例，分析其实现的主要功能。

3. 智能手机能支持各种应用，与其自身分布大量的传感器是分不开的，请列举智能手机中的传感器。

4. 简述智能家居控制系统的组成及其功能。

4.2 物联网的相关技术

要实现物联网的智能化识别、定位、跟踪、监控和管理，需要强有力的技术支撑，如自动识别技术、定位技术和通信技术等。

4.2.1 自动识别技术

自动识别技术是指应用一定的识别装置，自动地获取被识别物品的相关信息，并提供给后台的计算机处理系统来完成相关后续处理的一种技术。自动识别技术为计算机提供了快速、准确的采集和输入手段，解决了计算机通过键盘手工输入数据速度慢、错误率高等问题。例如：商场售货员通过扫描仪扫描商品的条码，获取商品的名称、价格，输入数量，后台POS系统即可计算出该批商品的价格，从而快速完成结算。

现有的自动识别技术主要包括条码识别技术、射频识别技术、生物特征识别技术及图像识别技术等。

1. 条码识别技术

条码识别技术的核心是条码符号。条码是将宽度不等的多个黑条和空白，按一定的编码规则排列，用以表示一组信息，其中“条”指对光线反射率较低的部分，“空”指对光线反射率较高的部分。这种用条、空组成的数据编码可以供机器识读，也容易译成二进制数和十进制数。条码一般分为一维条码、二维条码两种。

（1）一维条码

一维条码种类繁多，每种条码都有自己的一套编码规则，规定了每个字母由几根线条（Bar）、几个空格（Space）组成及排列方式。目前较为流行的一维条码有EAN码、39码、UPC码、128码，以及用于书刊管理的ISBN、ISSN等。

EAN码是国际物品编码协会制定的一种条码，广泛应用于90多个国家和地区，超市中最常见的就是EAN码。EAN码符号有标准版和缩短版两种，标准版由13位数字构成，即EAN-13（如图4.2.1所示），缩短版由8位数字构成，即EAN-8。用数字“1”表示条码的一个“暗”或“条”部分，用“0”表示条码的一个“亮”或“空”部分。标准条码由厂商代码、商品项目代码、校验码三部分组成。

图4.2.1 EAN-13码

（2）二维条码

二维条码是目前应用较为广泛的条码技术。它采用特定的几何图形按一定规律在平面分布的黑白相间的图形中记录数据符号信息。在代码编制上巧妙地利用构成计算机内容逻辑基础的“0”“1”比特流概念，使用若干个与二进制相对应的几何体来表示文字数值等信息，通过图像输入设备或光电扫描设备自动识读以实现信息自动处理。

常见的二维条码是线性堆叠式二维码和矩阵式二维码。线性堆叠式二维码典型的码制有Code 16K、Code 49和PDF417等，矩阵式二维码典型的码制有QR码、Data Matrix条码、龙贝码、汉信码等。

矩阵式二维条码整体呈正方形，只有黑白两色。4个角落中的3个印有“回”字形图案，用来帮助解码软件定位，使用者不需对准，经任何角度扫描，资料均能被正确读取。二维条码能够在横向和纵向两个方位同时表达信息，因此能在很小的面积内表达大量的信息。图4.2.2为二维条码表示文字信息“浙江教育出版社”。

图4.2.2　表示文字信息“浙江教育出版社”的二维码

2. 射频识别技术

射频识别即RFID。RFID是一种非接触式的自动识别技术，通过无线射频信号识别特定目标并读写相关数据。RFID主要用来识别和跟踪物体上绑定的标签，从而实现对物体的管理。RFID系统主要由电子标签、读写器和后台管理系统组成。电子标签由耦合元件、芯片和天线组成，附着在物体上，每个标签都有唯一的电子编码，在标签中一般保存有被识别物体的相关电子数据。读写器是读取电子标签数据信息的设备。后台管理系统是计算机网络系统，其功能是对读取的数据进行处理和传输。

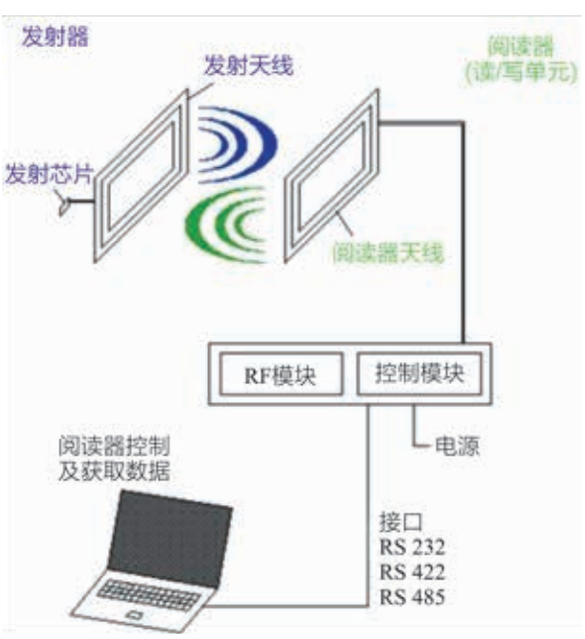


图4.2.3　RFID工作原理

RFID系统的工作原理是阅读器通过天线发送出一定频率的射频信号，当标签进入磁场时产生电流获得能量（无源），或者依靠自身的供电系统（有源）主动地向阅读器发送自身编码等信息，然后由阅读器采集并解码，最终将数据发送到计算机系统进行处理。如图4.2.3所示。

射频技术应用广泛，常见的应用有钞票及产品防伪技术、身份证、门票、电子收费系统、电子病历、仓储物流（如图4.2.4所示）等，其产品主要包括无源RFID产品、有源RFID产品和半有源RFID产品，如表4.2.1所示。

表4.2.1　RFID产品分类

类别	特性	应用领域
无源RFID产品	发展最早，最成熟、市场应用最广的产品，属于近距离接触式识别类	公交卡、食堂饭卡、银行卡、宾馆门禁卡、二代身份证等都属于无源RFID产品
有源RFID产品	发展比较晚，具有远距离识别特性，未来市场空间巨大	应用在远距离自动识别领域，如智能医院、智能停车场、智能交通、智能城市等
半有源RFID产品	也称低频近距离精确定位，通过微波远距离识别和上传数据，以解决单纯的无源、有源没有办法实现的功能	短距离射频产品，不怕油渍、灰尘污染等恶劣环境，可替代条形码，如用在产品流水线上跟踪物体。长距离射频产品多用于交通，如自动收费等

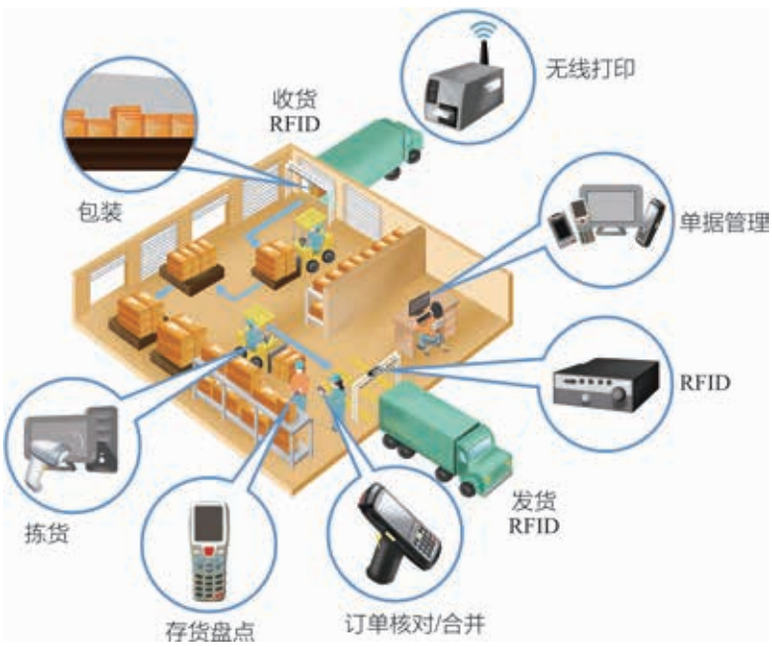


图4.2.4　RFID技术应用于仓储物流系统

3. 近场通信技术

近场通信即NFC。NFC是手机常见的一个通信接口，通过相互靠近的方式来交换数据，如图4.2.5所示。

通俗地说，NFC是RFID的演进版本。RFID由阅读器和标签组成，只能实现信息的读取以及判定；NFC将非接触读卡器、非接触卡和点对点功能整合进一块单芯片，强调的是信息交互。具有NFC功能的手机内置了NFC芯片，它是组成RFID模块的一部分，可以当作RFID无源标签使用；也可以当作RFID读写器，用作数据交换与采集；还可以用于NFC手机之间的数据通信。

NFC传输范围比RFID小，RFID的传输范围可以达到几米、甚至几十米，但由于NFC采取了独特的信号衰减技术，相对于RFID来说NFC具有距离近、带宽高、能耗低等特点。NFC技术一般应用于消费类电子设备间的相互通信，如图4.2.6所示。

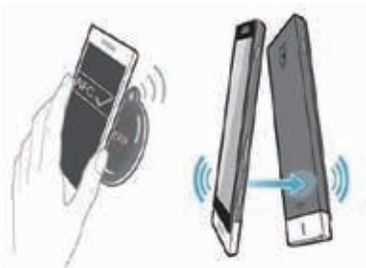


图4.2.5　NFC通信方式

图4.2.6　NFC技术被广泛应用于支付场景

4.2.2　定位技术

在未来复杂的异构网络（指由不同制造商生产的计算机、网络设备和系统组成的网络，在不同的协议下运行不同的应用）环境下，要实现全面、灵活及可靠的人与物通信、物与物通信，就须对物进行精准的定位、跟踪和操控。定位是指通过声光以及无线电等方式对目标当前位置信息的获取。这里的位置信息并不仅仅是单纯的物理空间坐标，还涉及处在该位置的时间等。常见的定位技术有GPS卫星定位技术、北斗卫星导航系统、Wi-Fi定位技术及蓝牙定位技术等。本节主要介绍卫星定位技术。

1. 全球定位系统

全球定位系统即GPS，是美国从20世纪70年代开始研制的利用导航卫星进行测时和测距的技术。全球卫星定位系统以全天候、高精度、自动化及高效益等特点，成功地应用于大地测量、工程测量、航空摄影、运载工具导航和管制、地壳运动测量、工程变形测量、资源勘察及地球动力学等多种学科，具有良好的经济效益和社会效益。

GPS主要由空间部分、地面监控部分和用户部分组成，如图4.2.7所示。

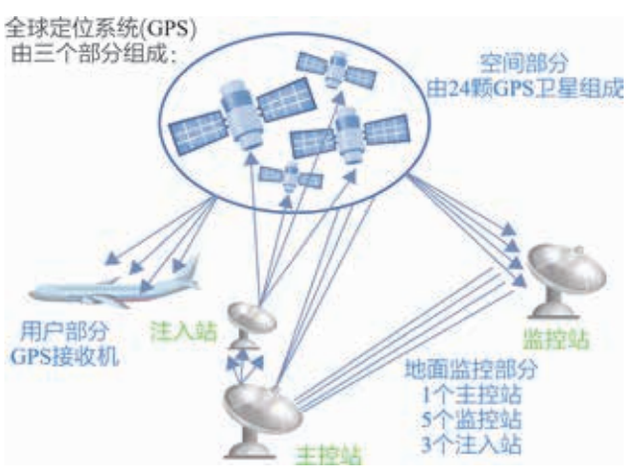


图4.2.7　GPS的组成

（1）空间部分

GPS的空间部分由24颗工作卫星组成，位于距离地表20200km的上空，均匀分布在6

个轨道面上（每个轨道面4颗），轨道倾角为55°。此外，还有4颗有源备用卫星在轨运行。卫星的分布使得在全球任何地方、任何时间都可观测到4颗以上的卫星，并能保持良好的定位解算精度，提供了在时间上连续的全球导航能力。

（2）地面监控部分

地面监控部分由1个主控站、5个全球监测站和3个地面控制站（注入站）组成。监测站均配装有精密的铯原子钟和能够连续测量到所有可见卫星的接收机。监测站将取得的卫星观测数据经过初步处理后，传送到主控站。主控站从各监测站收集跟踪数据，计算出卫星的轨道和时钟参数，然后将结果送到3个地面控制站。地面控制站在每颗卫星运行至上空时，把这些导航数据及主控指令注入卫星。

（3）用户部分

用户部分即GPS接收机。其主要功能是能够捕获到按一定卫星截止角所选择的待测卫星，并跟踪这些卫星的运行。当接收机捕获到跟踪卫星信号后，即可测量出接收天线至卫星的伪距离和距离的变化率，解调出卫星轨道参数等数据。在日常生活中，GPS主要的应用方向有车辆跟踪、出行路线规划和导航服务、信息查询及紧急援助等。

通过GPS定位，很多公交公司率先将一些线路的调度站和行驶中的公交车联网。随后，营运中的车辆的一举一动都可以通过卫星实时传送，并实时反映到调度室的计算机上，调度员可以将路况、乘车人数等信息尽收眼底，然后根据实际情况安排发车时间等事项，如图4.2.8所示。

图4.2.8　公交GPS系统

2. 北斗卫星导航系统

北斗卫星导航系统（BeiDou Navigation Satellite System，BDS）是中国自行研制的全球卫星导航系统，是继美国全球定位系统（GPS）、俄罗斯格洛纳斯卫星导航系统（GLONASS）之后第三个成熟的卫星导航系统。北斗卫星导航系统由空间段、地面段和用户段三部分组成，可在全球范围内全天候、全天时为各类用户提供高精度、高可靠性定位、导航服务。

北斗卫星导航系统空间段包括5颗静止轨道卫星和30颗非静止轨道卫星，根据总体规划，将于2020年前后覆盖全球。系统的主要功能包括：

①短报文通信。用户终端具有双向报文通信功能，民用可以一次传送40～60个汉字的短报文信息，军用可以一次传送120个汉字信息，在远洋航行中有重要的应用价值。

②精密授时。北斗系统具有精密授时功能，可向用户提供20～100纳秒（ns）时间同步精度（1ns=10^{-9}s）。

③定位精准。水平精度为100m，设立标校站之后为20m，工作频率为2491.75MHz。

④系统容纳的最大用户数：540000户/时。

北斗卫星导航系统应用范围广泛，主要应用领域包括气象应用、道路交通管理、海运和水运、航空运输、应急救援等。

4.2.3 短距离无线通信技术

短距离无线通信技术帮助人们摆脱了各种电缆的束缚，为小范围内的设备建立起无线通信网络，使设备之间的协同工作变得更加方便快捷。

1. Wi-Fi技术

Wi-Fi技术是一种允许电子设备连接到一个无线局域网（WLAN）的技术，通常使用2.4G Hz或5G Hz射频频段。多数无线局域网是有密码保护的，也有一些是开放的，允许WLAN范围内的任何设备连接。Wi-Fi是一个无线网络通信技术的品牌，由Wi-Fi联盟所持有。

2016年，Wi-Fi联盟公布的802.11ah Wi-Fi标准——Wi-Fi HaLow，使得Wi-Fi可以被运用到更多地方，如小尺寸、电池供电的可穿戴设备；同时也适用于工业设施内的部署，以及介于两者之间的应用。HaLow采用900MHz频段，低于当前Wi-Fi的2.4GHz和5GHz频段。同时HaLow的覆盖范围可以达到1千米，信号更强，且不容易被干扰。

2. 蓝牙技术

蓝牙技术最早始于1994年，由电信巨头爱立信公司创制。它采用调频技术，通信频段为2.402GHz～2.480GHz，通信半径从几米延伸到百米。

在微信和百度云还不太普及的时候，人们习惯打开手机里的蓝牙设备，把手机上好玩好看的东西分享给周围的朋友。手机、平板电脑等移动设备以及大量的无线外围设备（蓝牙耳机、蓝牙键盘等）都应用了蓝牙技术。

蓝牙技术紧跟物联网的发展脚步，蓝牙4.2数据传输速率可达1Mbps、隐私功能更强大，并可以将设备通过IPv6和6LoWPAN接入互联网。在智能家居领域，采用了Bluetooth Smart技术的蓝牙支持设备与设备之间的“对话”技术。在意外断网没有Wi-Fi的情况下，智能家居设备仍可继续工作。

3. ZigBee技术

ZigBee是一种新兴的短距离无线通信技术，用于传感器应用，其主要特点是近距离、低复杂度、低功耗、高数据速率等。ZigBee又称紫蜂协议，该名称来源于蜜蜂的八字舞，因为蜜蜂（Bee）是靠飞翔和“嗡嗡”（Zig）地抖动翅膀的“舞蹈”来向同伴传递蜜源信息的，而ZigBee也依靠这样的方式来构成群体中的通信网络。ZigBee技术广泛应用于家庭和楼宇网络、商业智慧型标签、传感器自动化控制、公共场所烟雾探测器等。

ZigBee网络中的设备可分为管理节点、汇聚节点、传感器节点三种，如图4.2.9所示。

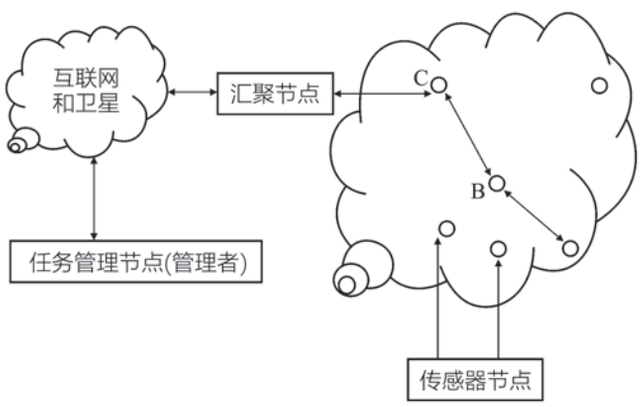


图4.2.9　ZigBee网络示意图

使用ZigBee技术，可以对矿井下的人员进行定位。矿井下人员通过佩戴基于ZigBee技术的定位卡，使得系统能对井下坑道作业工作人员精确定位，并能准确地提供井下人员的数量和分布情况，为事故处理和救援工作提供可靠的数据。

4.2.4　无线传感器网络技术

无线传感器网络（Wireless Sensor Networks，WSN）是由部署在监测区域内的大量微型传感器节点组成，通过无线通信的方式形成一个多跳的自组织网络。所谓自组织网络是区别于传统的客户端—服务器模式的一种新型网络模式，在该模式下，各种接入设备是对等的，在信息交互过程中，既可以作为客户端，又可以作为服务器。当信息从A经过B转发到C时，信息从A到B可以看作一跳，从B到C可以看作另一跳，所以多跳就是多次转发。无线传感器网络包括传感器节点、汇聚节点和管理节点，如图4.2.10所示。无线传感器网络具有十分广阔的应用前景，如生态环境监测（包括监测气候、土壤、森林、海洋以及各类生物等）、工业生产监控（包括公共设施的安

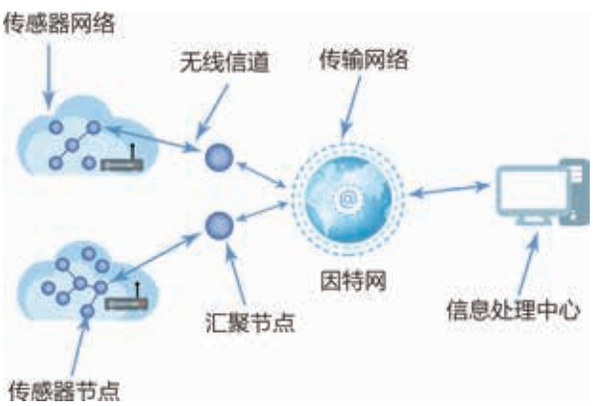


图4.2.10 无线传感器网络系统

全防卫、建筑结构的状态监控、智能交通督查以及物流跟踪管理等）、医疗卫生保健（包括抢险救援、病人监护以及远程医疗等）以及其他商业应用领域（包括智能家居、遥控玩具等）。

与传统的无线网络相比，无线传感器网络具有以下几个特点：

①大面积的空间分布。比如在军事应用方面，可以将无线传感器网络部署在控制区域内，随时发现异常情况并形成大面积的监视网络。

②能源受限制。由于布置传感器的区域有些是在无人区或者对人体有害的恶劣环境中，几乎不可能更换电源，而网络中每个节点的电源是有限的，因此为了延长网络的寿命，网络的能耗就不能太高。

③网络自动配置。无线传感器网络是一种具有无中心、自组织、快速展开和移动等特点的对等网络，管理和组网都非常简单灵活。

④网络的自动管理和高度协作性。传感器可以分布在很广泛的地理区域，感知的范围也很大。在无线传感器网络中，数据处理由节点自身完成，每个节点仅知道自己邻近节点的位置和标识，传感器网络通过相邻节点之间的相互协作来进行信号处理和通信，具有很强的协作性。

⑤传感器网络的拓扑结构变化快。传感器网络自身的特点使得传感器网络的拓扑结构变化很快，这对网络各种算法的有效性提出了挑战。此外，如果节点具备移动能力，也有可能带来网络的拓扑变化，导致网络拓扑结构十分复杂。

⑥通信能力有限。传感器网络的通信覆盖范围只有几十到几百米，通信带宽窄且经常变化，而且由于更多地受到地理、地势、地貌以及天气等自然条件的影响，传感器可能会长时间脱离网络，不能正常工作。

思考与练习

1. 什么是自动识别技术？举例说明你见过的条码识别系统的组成及识别方法。
2. 如何为校园内的介绍标签设计二维码？
3. 简述射频识别系统的构成、工作原理及应用领域。
4. 简述短距离定位技术。
5. 列举手机上网技术的发展历程。

4.3 物联网搭建实例

物联网系统的搭建主要包括硬件搭建和软件开发两个方面。在搭建系统时，必须先进行周密的分析，然后进行架构设计，方案要充分发挥各个环节的作用，使系统具备良好的适用性和扩展性。在设计基础上进行硬件搭建和软件开发，最终在进行系统测试后投入实际应用。物联网的搭建步骤如图4.3.1所示。

图4.3.1　物联网搭建步骤

4.3.1　前期分析

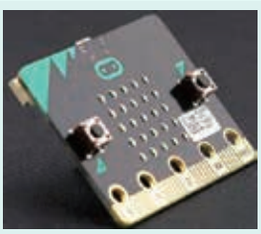
前期分析是为了确定用户需求。由于用户往往是非信息技术专业人员，他们所提出的问题通常不是从技术角度来表述的，如“希望有个设备能够知道室内环境是否适宜”，这时就需要技术人员对其重新表述，并与用户确认。下面就以一个简单的家庭远程灯光控制系统为实例来探讨如何搭建物联网系统。

例1　“家庭远程灯光控制系统”前期分析

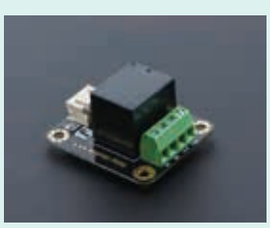
远程灯光控制物联网系统的搭建，可以帮助人们实时监测外界环境中光线的亮度并上传到服务器进行及时干预控制或自动分析。服务器端应用程序界面显示各种传感器数据，能根据实时数据做出判断或人工干预控制。本例中我们主要对灯光亮度进行采集，所以主要采用模拟环境光线传感器。

采集不仅需要传感器，还需要其他设备。针对远程灯光控制的物联网系统，还有如下资源需求：

①硬件资源。

名称	名称	图片	功能
核心板块	Micro:bit板		搭载了5×5可编程LED点阵、两颗可编程按键、加速度计、电子罗盘、温度计、蓝牙等电子模块。可以通过鳄鱼夹与各种电子元件互动，支持读取传感器数据，控制舵机与RGB灯带，能够轻松胜任各种与编程相关的教学与开发场景

续表

名称	名称	图片	功能
传感器模块	亮度传感器		可以用来对环境光线的强度进行检测。通常用来制作随光线强度变化产生特殊效果的互动作品
硬件中间件	物联网模块		OBLOQ是一款基于ESP8266设计的串口转Wi-Fi物联网模块，用以接收和发送物联网信息
硬件中间件	micro:mate多功能微型扩展板		micro:mate是一款为micro:bit设计的微型多功能IO传感器扩展板，其彩色3Pin接口支持DFRobot百款Gravity系列电子模块，可直插传感器或电子元件，省去了烦琐的鳄鱼夹接插步骤，为micro:bit添加新的玩法和扩展可能性
执行器模块	继电器		进行电源、电机电源等控制，连接在硬件中间件上
USB连接线			将硬件中间件与计算机进行连接，进行程序下载、调试等
无线AP			将硬件中间件数据进行网络传输
服务器			存储数据、发送信号
电机或电灯			被控制对象

②软件资源。

名称	功能
Python	编写服务器等应用程序使用

预算主要包括购买硬件和开发软件的费用。硬件由终端设备和服务器等组成，购置各种传感器、执行器、通信模块、扩展板等终端设备。网络设备需要一个无线AP，能接入因特网保证可上网就可以。服务器完全可以用家里闲置的PC机替代，无需购置。若要实现异地监测、实时互联，则对服务器性能要求较高，建议购买云服务器。软件则由使用者凭兴趣改写，无须购买。

综上所述，做一个远程控制灯光的物联网系统确实可行。

4.3.2 架构设计

传感器的数据通过无线及网络设备汇总到数据库服务器中，客户端通过访问服务器获得各种数据信息，数据的统计、分析、呈现等功能主要在服务器中完成，当环境信息出现异常，也由服务器直接发出各种报警信息，如邮件或短信。智能终端(硬件中间件)主要负责采集信息并执行命令，大部分的工作都在服务器端完成。如图4.3.2所示。

图4.3.2 C/S模式结构图

架构设计主要包括模块结构设计、系统物理配置和数据库设计三大部分。

在模块结构设计部分，主要包括划分系统模块、确定模块功能、决定模块间的调用关系、制定模块间的接口即数据传递。

在系统物理配置部分，主要包括硬件设备配置、通信网络的选择和设计、数据库管理系统的选择等。

在数据库设计部分，设计开发的信息系统规模越大，数据库设计就越重要。数据库用于存储信息系统的各种数据。信息系统的数据流转方式和数据交换的格式，都需要在这个环节进行确定。这些都将直接影响数据交换的工作效率，进而影响数据挖掘、分析功能的实现。

●●● 例2 “家庭远程灯光控制系统”模块结构

“家庭远程灯光控制系统”模块结构主要划分为三块，分别针对物联网的三层结构。感知层结构主要是传感器信息获取模块以及执行器执行模块，主要完成的是信息获取以及指令执行。“家庭远程灯光控制系统”主要使用Wi-Fi进行连接并通过因特网进行传输。“家庭远程灯光控制系统”直观演示接收到的数据，并对数据进行处理显示，未对数据进行保存，所以未配置数据库存放数据。

4.3.3 硬件搭建

“远程灯光控制的物联网系统”的硬件搭建包含两个部分，第一部分是将micro:bit与扩展板、OBLOQ模块、亮度传感器及继电器进行连接，以获取传感器数据和执行指令。连接方式如图4.3.3 红线框所示。

第二部分是先将USB线连接到计算机上，安装好驱动程序，通过串口测试传感器是否能获取亮度数据，同时测试能否控制继电器。然后连接好家中的网络设备，配置好无线AP或无线路由器，确保能连上因特网，如图4.3.4所示。

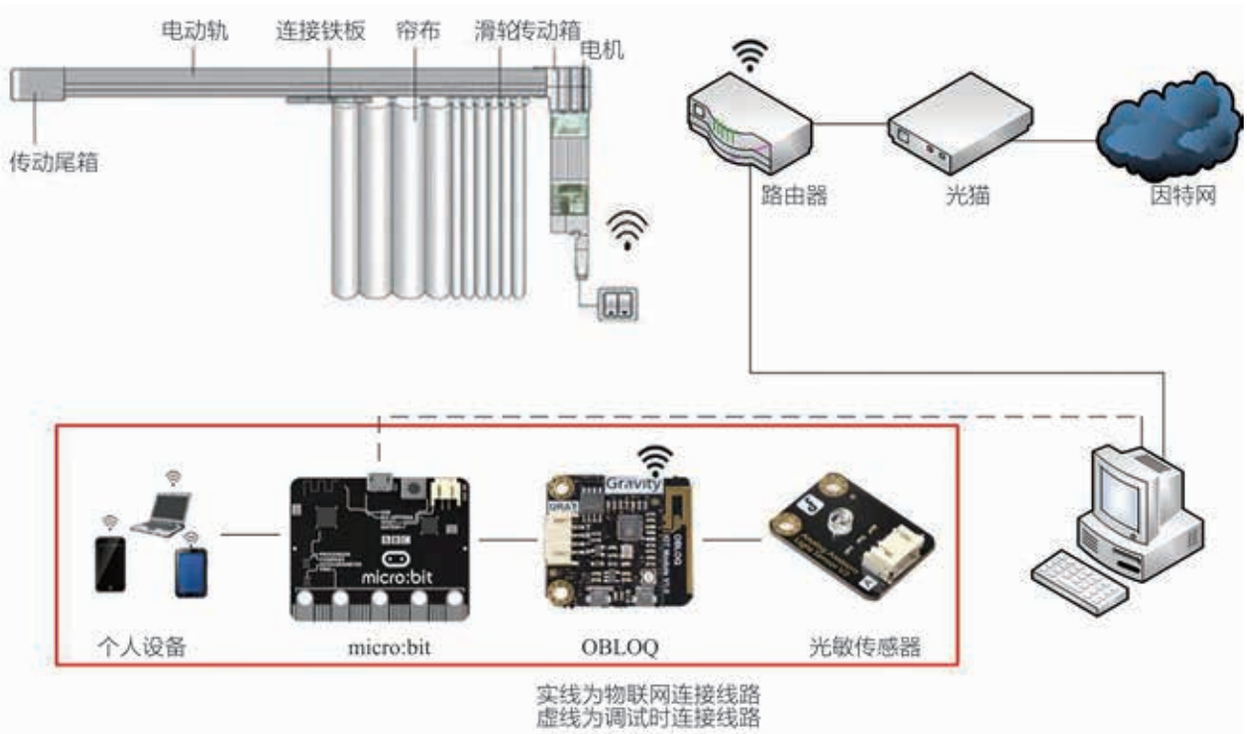


图4.3.3　家庭网络设备连接图

连接完成后，需要先进行设置才可将传感器收到的数据上传到网络。在这一步中，需要配置硬件中间件的无线参数，配置好SSID和密码，填入需要连接到服务器的IP地址和端口号，定义好传送到服务器上的数据格式。

例3　“家庭远程灯光控制系统”连接

在“家庭远程灯光控制系统”中，micro:bit板与micro:mate之间采用弹针连接，安装时，应将螺丝拧紧，防止接触不良。micro:mate和OBLOQ模块之间接线方式如图4.3.4所示，可以采用4Pin接线和双股杜邦线连接。micro:mate板的8、12、16接口和继电器之间可以通过3Pin接线连接，USB口仅作供电用。micro:bit板通过USB口与计算机连接，并安装驱动程序。

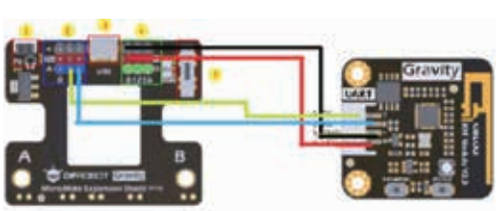


图4.3.4　接线方式

4.3.4　软件开发

软件开发分为两部分，一部分为客户端程序，一部分为服务器端程序。客户端程序的作用为收集数据并根据服务器返回的指令控制执行器。服务器端程序的作用是接收数据并

发出控制指令。为了将获取的数据传输至服务器，需将获取传感器数据程序、网络驱动程序编制后下发至硬件中间层。

●●● 例4 “家庭远程灯光控制系统”核心代码（该代码部分实现了灯光控制，完整的代码文件可从教学资源网站下载）：

OBLOQ模块联网工作的代码：

```
from microbit import *
import Obloq                                        #导入物联网模块库

IP="192.168.0.1"                                    #运行服务器端软件的IP地址
PORT="8080"                                         #服务器端软件的端口号
SSID="******"                                       #无线网络名称
PASSWORD="******"                                   #无线网络密码

uart.init(baudrate=9600, bits=8, parity=None, stop=1, tx=pin16, rx=pin12)

while Obloq.connectWi-Fi(SSID,PASSWORD,10000) != True:
    display.show(".")                               #无线连接不成功在板载LED上显示“.”

display.scroll(Obloq.ifconfig())
Obloq.httpSet(IP,PORT)

while True:
    errno,resp=Obloq.get("switch/led",10000)
    if errno == 200:
        c = str(resp)[0]
    if c == '1':
        pin0.write_digital(1)                       #打开LED灯
    else:
        pin0.write_digital(0)                       #关闭LED灯
    else:
        display.scroll(str(errno))                  #滚动显示出错信息
    sleep(1)
```

“家庭远程灯光控制系统”的服务器端代码：

```
from flask import Flask, render_template, jsonify
from flask import request
from flask_restful import Resource, Api
from flask_bootstrap import Bootstrap
from flask_moment import Moment
from flask_wtf import FlaskForm
from wtforms import RadioField, SubmitField
from wtforms.validators import DataRequired
```

```
from flask_nav import Nav
from flask_nav.elements import *
app = Flask(__name__)
app.config['SECRET_KEY']='xxx_ssss'
api = Api(app)
bootstrap = Bootstrap(app)
moment = Moment(app)

nav = Nav()
nav.register_element('top', Navbar('系统',
                            View('主页', 'index'),
                            View('系统监测', 'check'),
                            Subgroup('远程控制',
                                View('灯光远程控制', 'control', todo_id='led'),
                                Separator,
                                View('远程窗帘控制', 'control', todo_id='curtain'),
                                ),
                            )
                    )
nav.init_app(app)                                                    #建立网页导航菜单

todostatus = {'led': 0, 'curtain': 0}                                #设备及状态参数
todotitle = {'led': '照明', 'curtain': '窗帘'}                        #设备标题文本
todotxt = {'led': '0|关灯|1|开灯', 'curtain':  '0|关闭窗帘|1|打开窗帘'}  #设备状态文本

class MyForm(FlaskForm):
    switch = RadioField('开关状态：', choices=[], default='0', validators=[DataRequired()])
    submit = SubmitField('提交')

class TodoSomething(Resource):                                       #建立WEB API
    def get(self, todo_id):
        data = todostatus[todo_id]
        return jsonify(data)
    def post(self, todo_id):
        mtxt = request.json
        if mtxt is None:
            return '0'
        else:
            todostatus[todo_id] = mtxt[todo_id]
            return '1'

api.add_resource(TodoSomething, '/switch/<string:todo_id>')
@app.route('/')
def index():
    stxt = '智能家居远程控制系统'
    return render_template('index.html', txt=stxt)
```

```
@app.route('/check')
def check():
    return render_template("checkview.html", mstatus=todostatus, mtitle=todotitle)

@app.route('/control/<string:todo_id>', methods=['GET', 'POST'])
def control(todo_id):
    form = MyForm()
    ltxt = todotxt[todo_id].rsplit('|')
    form.switch.choices = [(ltxt[0], ltxt[1]), (ltxt[2], ltxt[3])]
    if form.validate_on_submit():
        switchdata = int(form.switch.data)
        todostatus[todo_id] = switchdata
      return render_template("controlview.html", form=form, mstatus=todostatus[todo_id],
mid=todo_id)

if __name__ == '__main__':
    app.run(host='0.0.0.0', port=8080, debug=True)  #脚本运行的IP地址和端口
```

程序运行后，通过Web页面进入，点击【系统监测】可以看到当前状态，此时如果外界光线变化明显，既可以通过传感器侦测到数据进行控制，也可以通过Web页面进行人工干预，开关电灯或者窗帘。如图4.3.5所示。

图4.3.5　灯光及窗帘控制界面

4.3.5　系统测试和调试

编写软件程序的过程中，难免会有错误。软件系统运行时会自动提醒语法错误，可立即进行修改。但有一类错误，是因为不正确的调控或数据运算逻辑导致的，这类错误比较隐蔽，不易察觉，一般可以用多种不同的数据输入形式进行测试，并检查算法结构以发现问题。

例5 “家庭远程灯光控制系统”测试和调试

“家庭远程灯光控制系统”的测试和调试包括硬件方面和软件方面。硬件有无连接错误、软件有无设计错误等都是通过不断地测试和调试来纠正的。测试过程中得不到要求的数据，就需调整软件或硬件来查找原因。

“家庭远程灯光控制系统”的测试和调试一般通过串口和板载LED进行。

1. 通过micro:bit串口显示器测试传感器数据有无正确获取、传感器环境数据是否会改变，来检查接口及程序是否正确、传感器有没有数据或者是串口是否选错等。如果连接及程序上都没有错误，串口显示器上应该显示获得传感器数值。

2. 通过micro:bit的LED显示有无连接到路由器、服务器，网络通信是否连通，控制指令是否有返回等。

测试和调试系统完成后，就可以应用到实际工作和生活中。

思考与练习

1. 物联网系统由哪些基本模块组成？
2. 简述搭建简易物联网系统的基本流程。
3. 设计一个智慧农业大棚物联网系统，并分析其实现的主要功能。

巩固与提高

1. 为解决食堂就餐排队问题，某中学引进了“智慧餐台”快速结算系统，让师生食堂就餐变得快速、便捷。该“智慧餐台”基于RFID技术，主要由配套餐具和智能结算台两部分组成。其中配套的每一个餐具底部都植入了RFID电子标签，颜色不同价格不同；智能结算台集成了射频读写装置、读卡器、显示屏等多个设备，可实现对进入结算区餐具的批量快速识别，顾客自助完成核对、刷卡支付，完全无需人工干预，极大地提升了结算效率，缓解了结算排队、拥堵的问题。请思考并讨论：

（1）分析本系统中的组网设备有哪些，各属于物联网中的哪一层。

（2）分析本系统中的数据流。

2. ETC是不停车电子收费系统，ETC专用车道是给那些装了ETC车载器的车辆使用的，采用电子收费方式。通过安装在车辆挡风玻璃上的车载电子标签与在收费站ETC车道上的微波天线之间的微波专用短程通信，利用计算机联网技术与银行进行后台结算处理，从而达到车辆通过路桥收费站不需停车而能交纳路桥费的目的。请分析ETC系统的工作原理。

项目挑战

构建基于物联网的智慧校园模型

智慧校园指的是以物联网为基础的智慧化的校园工作、学习和生活一体化环境，这个一体化环境以各种应用服务系统为载体，可以将教学、科研、管理和校园生活进行充分融合。随着信息技术的不断发展，智慧校园已不再只是一个美好的愿望，越来越多的学校正在借助物联网技术提升校园的智慧化程度。

项目任务

以概念图为呈现形式，为自己所在的学校构建智慧校园模型，并选择其中的一个功能，去具体实现它。

过程与建议

1. 构想物联网所能实现的智慧校园功能

建议从物联网技术和学校需求两个角度出发，来设计智慧校园。

从技术出发		以需求出发		
物联网技术	可能实现的功能	场景	功能需求	可能的技术支持
人脸识别	自动签到、安防	校门口	安防、签到	人脸识别、指纹识别、卡牌识别

反复讨论并丰富从不同角度构想出来的系统功能，并思考是否还有其他角度。

2. 梳理智慧校园功能，将其制成概念图

在制作概念图时要注意以下几点：

（1）建议选择合适的分类依据，以便条理清晰；

（2）同一类节点的图标标识尽可能保持一致，增加图形的辨识度；

（3）可以借助一定的图形与图片，增强概念图的可视化效果；

（4）概念图上呈现出来的文字要精练，使图形便于阅读。

3. 具体实现其中的一个功能

（1）计划具体实施的功能是：_____

（2）需要用到的硬件是：_____

请编写相关代码以实现这一功能。

4. 展示交流

每个小组打印自己的概念图，并将具体的功能呈现出来。在展示时，每组留下一名同学介绍和演示自己小组的成果，其他成员依次浏览和听取其他小组的情况。最后，大家坐下来一起为各个小组的表现评分。

评价标准

请根据项目实施的过程、效果以及成果展示交流的结果，对自己完成项目的情况进行客观的评价，并思考后续完善的方向。把评价结果和完善方案填写在下面的表格中。

评价条目	说明	评分（1～10分）	评分主要依据阐述	后续完善方向
功能分析	能满足可操作性需求、技术支撑可实现、遵循科学原理与依据			
概念图表达	概念图所呈现的各项功能符合智慧校园的特点，且有创意；条理清晰，可视化强，效果好			
具体功能实现	通过合理的硬件配置，成功地实现了功能			
展示交流	代表的表述清晰、准确，能够很好地呈现小组的工作成果；其他小组成员积极参与小组间的交流学习，并提出有价值的建议			

拓展项目

在同学们交流智慧校园需求分析可行性方案的基础上，选取合适的模块着手实施。

第五章 5

网络安全

当前，我国的互联网应用已经呈现出规模化和多元化的发展态势，共享经济、网络商店、移动支付等正在深刻地改变着人们的学习、工作及生活方式，促进了社会的发展。与此同时，有关网络的各种安全问题也日益突出，网络泄密、网络攻击、网络诈骗等问题时时侵犯人们的合法权益，威胁社会的安全稳定，影响经济的健康发展。

问题与挑战

- 作为网上查找、浏览信息的主要手段，万维网的使用者正面临越来越多的安全威胁，数据被窃取的事件时有发生。由于万维网上Web服务器是以一对多的方式为客户机提供服务的，因此加强Web服务的安全就可以在很大程度上确保被服务者的安全。如何在Web服务过程中保护用户数据的安全性，让用户的数据不易被窃取呢？

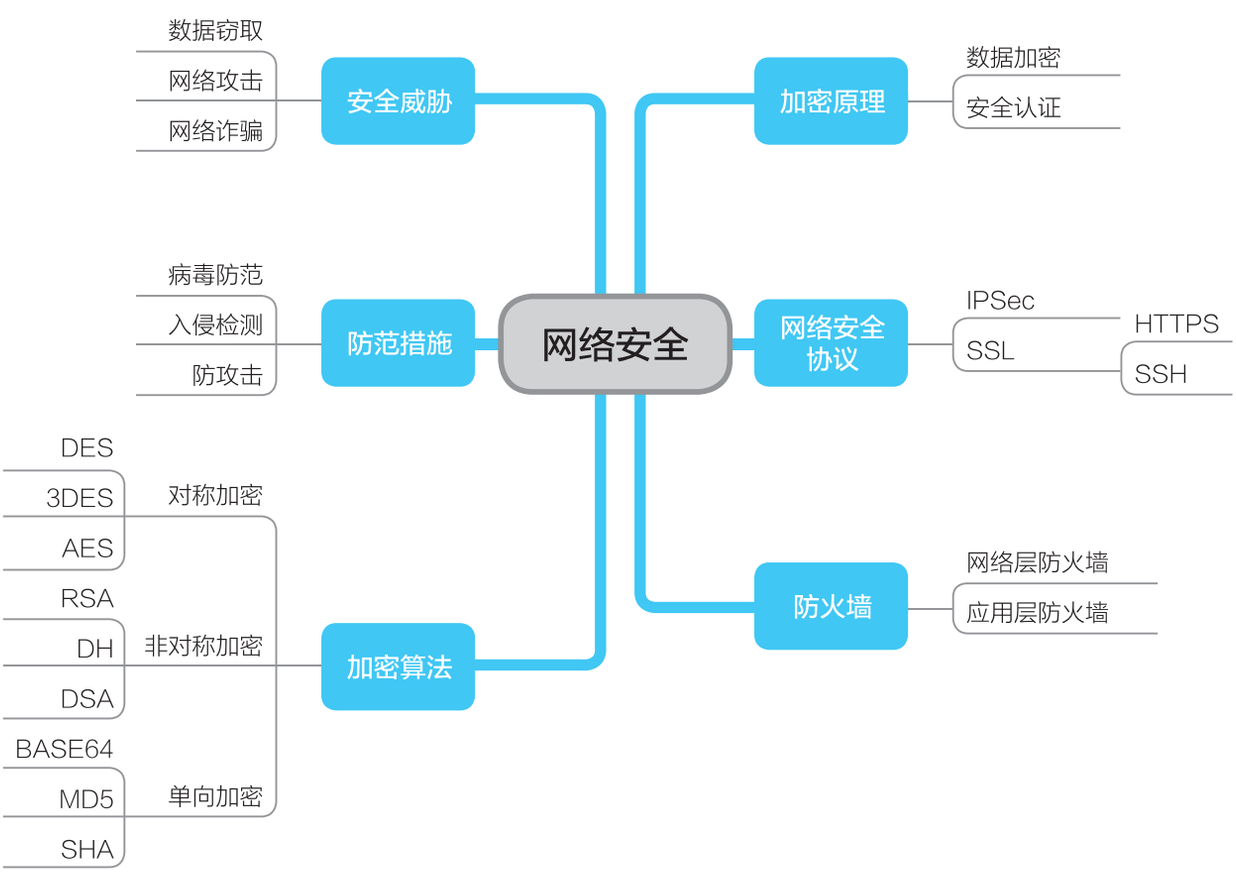
- 同一品牌的零售店连锁经营是一个普遍的业态。各连锁店分散在不同区域，在总部的组织领导下，采取共同的经营方针、一致的营销行动。现在的连锁店及其总部通常通过公共网络相互连接，其连接的安全性显得尤为重要。请分析这种连接中的安全隐患主要是什么？如何提升其安全度？

- 居家办公具有节约资源、兼顾家庭、提高效率等优点，正逐渐被各行各业所接受。开展居家办公的企业一般会配置专门的服务器为局域网外的员工提供特定服务，该过程可能为非法访问和攻击提供了可乘之机。该使用怎样的技术手段来提高该服务器的安全性呢？

学习目标

1. 了解加密原理，学会使用加密方法防范网络威胁。
2. 了解网络安全协议IPSec和SSL，学会使用安全协议防范网络威胁。
3. 了解防火墙的防护原理，掌握防火墙配置的基本方法。

内容总览



5.1 网络安全威胁与防范

在日常生活中经常会遇到各种各样的网络安全问题。比如：服务器硬件的损坏造成数据丢失，访问不安全网络而造成账户密码被窃，病毒或木马造成数据泄露或破坏等。随着互联网的广泛应用，全社会对网络的依赖程度越来越高，网络安全问题变得日益突出。

5.1.1 安全威胁

网络安全是指网络系统的硬件、软件及其系统中的数据受到保护，不会遭到破坏、更改及泄露。网络安全从本质上来讲就是网络上的信息安全。凡是涉及网络上信息的保密性、完整性、可用性、真实性和可控性的相关技术和理论都是网络安全的研究领域。因此，网络安全是一门涉及计算机科学、网络技术、通信技术、密码技术、信息安全技术、应用数学、数论和信息论等多种学科的综合性学科。

网络安全的主要特征有：

①保密性：信息不泄露给非授权用户、实体或过程，或供其利用的特性。

②完整性：数据未经授权不能进行改变的特性，即信息在存储或传输过程中保持不被修改、不被破坏和不丢失的特性。

③可用性：可被授权实体访问并按需求使用的特性，即当需要时能否存取所需的信息。

④可控性：对信息的传播及内容具有控制能力。

⑤可审查性：为出现的安全问题提供审查的依据与手段。

根据上述特征，一般来说，网络安全威胁可以分为以下几种：

①非授权访问。指对网络设备及信息资源进行非正常使用或越权使用等。如黑客通过系统漏洞，入侵控制他人计算机。

②冒充合法用户。主要指利用各种假冒或欺骗的手段非法获得合法用户的使用权限，以达到占用合法用户资源的目的。如通过窃取微信、QQ账号进行行骗。

③破坏数据的完整性。指使用非法手段，删除、修改、重发某些重要信息，以干扰用户的正常使用。如2017年感染全球150多个国家的Wannacry勒索病毒。

④干扰系统正常运行。指改变系统的正常运行状态，减慢系统的响应时间等手段。如分布式拒绝服务（Distributed Denial of Service，DDOS）攻击。

⑤恶意攻击。指通过网络传播病毒或恶意代码等。如利用操作系统和应用程序的漏洞主动进行攻击的蠕虫病毒“红色代码”“尼姆亚”及“求职信”等。

⑥线路窃听。指利用通信介质的电磁泄漏或搭线窃听等手段获取非法信息。如通过架设私人免费Wi-Fi进行数据窃听的行为。

拓展链接

DoS和DDoS

DoS拒绝服务攻击也称洪水攻击，就是用大量的访问使得服务器承受不了而瘫痪。随着服务器性能的提高，这种方式的攻击已难以奏效，这样就有了DDoS——分布式拒绝服务攻击。DDoS须有大量计算机共同参与攻击服务器，这些计算机通常是被黑客入侵的“僵尸”计算机，如果大量计算机参与攻击同一台服务器，一般服务器是难以抵挡的。

5.1.2 防范措施

对于不同的网络威胁，可以通过针对性的技术措施进行防范。

①访问控制：通过对特定网段、服务建立的访问控制体系，将绝大多数攻击阻止在到达攻击目标之前。交换机的ACL（访问控制列表）、防火墙、服务器的安全认证等都可以达到访问控制的目的。

②检查安全漏洞：通过对安全漏洞的定期检查和修补，即使攻击可到达攻击目标，也可确保绝大多数攻击无效。很多网络病毒、木马是通过系统漏洞进行传播或攻击，因此通过对系统“打补丁”的方式修补漏洞就可以起到一定的免疫效果。

③攻击监控：通过对特定网段、服务建立的攻击监控体系，可实时检测出绝大多数攻击，并采取相应的行动（如断开网络连接、记录攻击过程、跟踪攻击源等）。对于DoS、DDoS类攻击，最好的方式是对网络输入流进行监控，分析访问行为，自动切断攻击类连接，确保正常连接的通畅。

④加密通信：主动的加密通信，可使攻击者不能了解、篡改敏感信息。加密通信适合于防范数据的泄露，确保信息在通信过程中的安全。

⑤身份认证：良好的认证体系可防止攻击者假冒合法用户。网站的登录、手机的指纹开锁等都属于身份认证。

⑥备份和恢复：良好的备份和恢复机制，可在攻击造成损失时，尽快地恢复数据和系统服务。定期的数据备份可以确保在系统被破坏的时候，还可以在一定范围内恢复系统，减少损失。

对于不同的安全威胁，可以有针对性地使用一种或多种相应的防范措施进行应对。如对于非授权访问，可以通过设置系统或数据的访问权限阻止非法访问，来达到防范的目的。对于冒充合法用户威胁，可以通过加密通信、多重身份认证等手段，防止密码被窃取，或加大验证要求来达到目的。此外，可以综合运用多种防范措施，如多层防御，使攻击者在突破第一道防线后，延缓或阻断其到达攻击目标；隐藏内部信息，使攻击者不能了解系统内的基本情况，设立安全监控中心，为信息系统提供安全体系管理、监控、保护及紧急情况服务等。

为提高网络安全，在实施防范措施时，可从以下几方面入手：

①要用各种系统漏洞检测软件定期对网络系统进行扫描分析，找出可能存在的安全隐患，并及时加以修补。

②从路由器到用户逐级建立完善的访问控制措施，安装防火墙，加强授权管理和认证。

③利用RAID5等数据存储技术加强数据备份和恢复措施。

④对敏感的设备和数据要建立必要的物理或逻辑隔离措施。

⑤对在公共网络上传输的敏感信息要进行高强度的数据加密。

⑥安装防病毒软件，加强内部网的整体防病毒措施。

⑦建立详细的安全审计日志，以便检测并跟踪入侵攻击等。

思考与练习

1. 下面的事件属于哪类网络威胁？请说出理由。

①网上注册的个人信息被网站出售。

②黑客通过钓鱼攻击获取用户名和密码。

③QQ密码过于简单，结果被人猜到后登录QQ群发诈骗信息。

④由于系统升级不及时，网络病毒通过系统漏洞感染计算机。

2. 阅读下面的材料，说说这起安全事件可以通过什么措施进行防范？请从网站管理角度和从个人使用网站角度进行分析。

2016年8月的一天，徐玉玉（化名）接到骗子伪装的教育部门电话，通知她可以领到其申请的助学金，但须把学费打到指定的账号。当天下午徐玉玉将9900元人民币存入骗子的账户，待其发现被骗后昏厥死亡。事后调查发现犯罪嫌疑人杜某利用技术手段攻击了“山东省2016年高考网上报名信息系统”并在网站植入木马，获取了网站后台登录权限，盗取了包括徐玉玉在内的大量考生报名信息，然后进行诈骗。

5.2 数据加密与安全认证

数据加密，是一门历史悠久的技术，指通过加密算法和加密密钥将明文转变为密文，而解密则是通过解密算法和解密密钥将密文恢复为明文，它的核心是密码学。数据加密目前仍是计算机系统对信息进行保护的一种最可靠的办法。它利用密码技术对信息进行加密，实现保护信息安全的目的。

5.2.1 数据加密

数据加密技术主要有三种：对称加密、非对称加密和单向加密。

1. 对称加密

对称加密有很多种算法，其特点是加密密钥和解密密钥一致，加密效率较高，应用广泛。对称加密过程如图5.2.1所示。常见的对称加密算法有：

DES（Data Encryption Standard，数据加密标准）：曾经是应用最广泛的加密方案，使用56位密钥，但已于1998年被破解，所以现在基本不再使用。

3DES：也叫三重DES，使用3个密钥并执行3次DES算法。3DES对密码破解有较强的抵抗力，但其算法软件的运行速度较慢，影响了加解密效率。

AES（Advanced Encryption Standard，高级加密标准）：又称Rijndael加密法，使用128位、192位和256位三种长度的密钥。这个标准用来替代DES，已经被全世界广泛接受与使用。

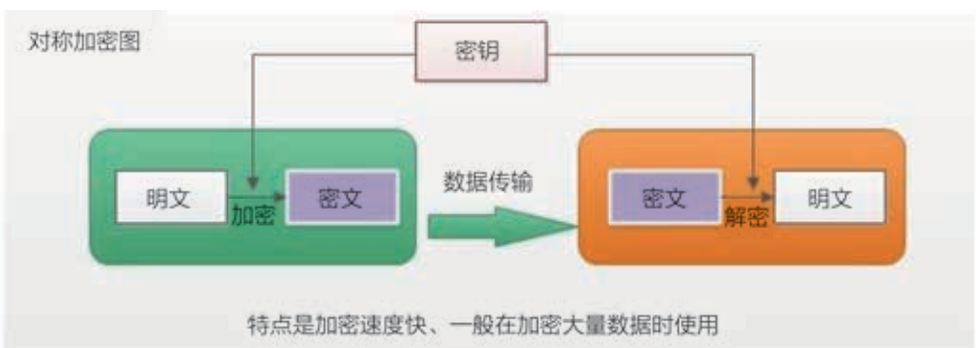


图5.2.1　对称加密算法示意图

2. 非对称加密

非对称加密为数据的加密与解密提供了一个非常安全的方法，它使用了一对密钥，

即公钥（public key）和私钥（private key）。私钥只能由一方保管，不能外泄，而公钥则可以发给任何请求者。非对称加密使用这对密钥中的一个进行加密，而解密则需要另一个密钥。

比如，A要向B发送一份加密信件，A拥有B的公钥，A先用B的公钥加密信件，然后发送给B，B收到信件后用自己的私钥解密信件，就可以看到里面的内容了。这样加密有个好处：由于B的公钥是公开的，所以任何拥有B公钥的人都可以向B发送加密信件，而拦截到加密信件的人（无论是否拥有B的公钥）是看不到信件内容的，只有发信人和B自己能看到信件内容（B的私钥只有B拥有），因此安全性大大提高。非对称加密过程如图5.2.2所示。常见的非对称加密算法有RSA、Elgamal等。

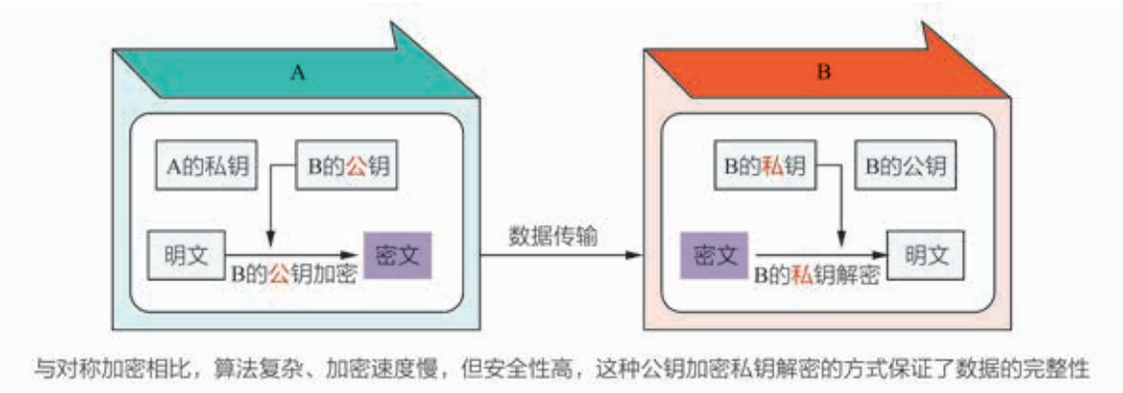


图5.2.2　非对称加密算法示意图

非对称加密长度通常有512位、1024位、2048位和4096位，常用的是2048位，增加长度可以增强安全性但是需要花很长时间来进行加密、解密，和对称加密相比，加密、解密的时间差不多是对称加密的1000倍，所以人们通常用其作为用户认证，用对称加密来实现数据的加解密。

3. 单向加密

单向加密也称非可逆加密，就是不可解密的加密方法。常见的单向加密算法有BASE64、MD5、SHA、HMAC等。单向加密算法通常用于数据的验证。如为了防止网上提供下载的软件被篡改，软件公司通常会提供与软件包对应的MD5（Message-Digest Algorithm）码，利用MD5软件获取下载软件包的MD5码与网上提供的MD5码进行比较，若不一致，则说明软件受到篡改（见图5.2.3）。

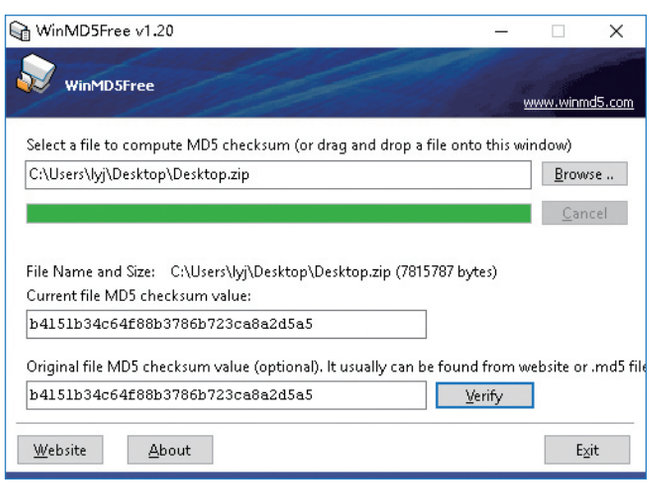


图5.2.3　MD5校验软件

实践与体验

非对称加密体验

RSA是目前最常用的非对称加密算法，目前的许多数字加密和身份验证一般都建立在该算法基础上。

实践内容：

通过RSA-Tools来体验非对称加密和解密操作。（见图5.2.4）

实践步骤：

1. 首先用“RSA KeyGen”菜单生成一个随机私钥和公钥，可以用随机方式生成密钥。

2. 把公钥发给同桌同学，同时接收同桌同学的公钥。

3. 然后用“Encrypt & Decrypt”菜单的“Encrypt”对输入的信息用同学的公钥加密。

4. 和同学交换密文。

5. 最后用“Encrypt & Decrypt”菜单的“Decrypt”解密密文，获得信息的内容。

结果呈现：

把解密获得的文字信息与同桌同学输入的明文进行对比，结果应该是一致的。

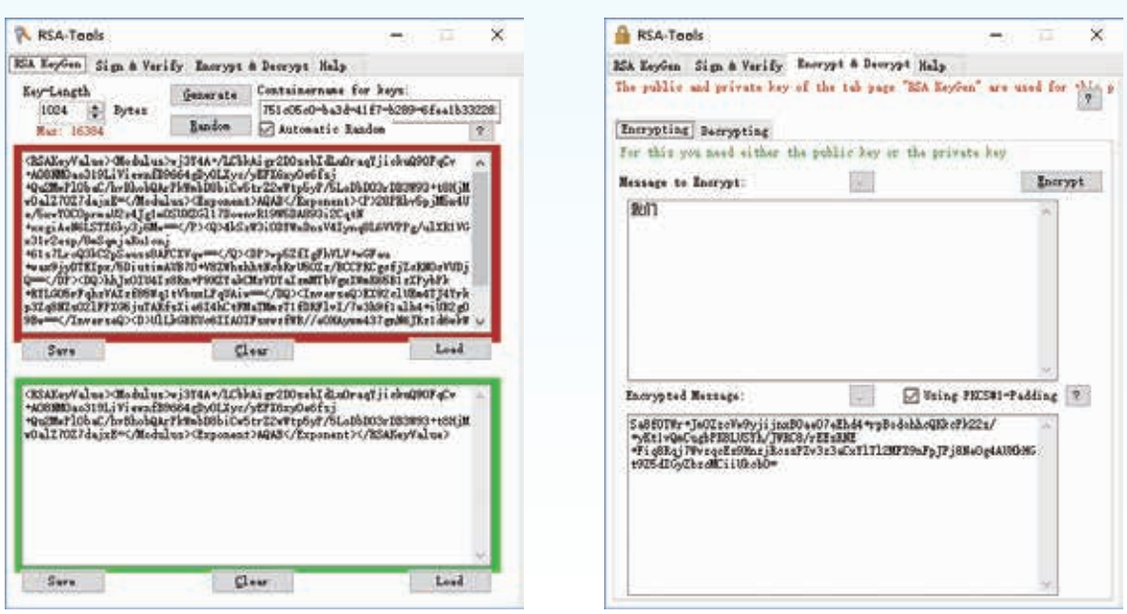


图5.2.4　RSA-Tools软件

5.2.2 安全认证

非对称加密除了可以进行数据加密，还可以用于安全认证，但其加密方式和数据加密的加密方式有所不同（见图5.2.5）：数据加密使用公钥加密、私钥解密，而安全认证使用私钥加密，公钥解密。

1. 认证过程

如有人发送了一封加密信给B，并声称发件人是A，那么B要怎样确定发件人真的为A？此时B只要用A的公钥对加密信件进行解密，若能解密，则可以肯定是A发送的。当然在做安全认证时不需要用冗长的信件，只要用简单的几个文本（通常用报文摘要，即信息的MD5校验码）让认证方进行加密，然后用对方的公钥进行解密即可。

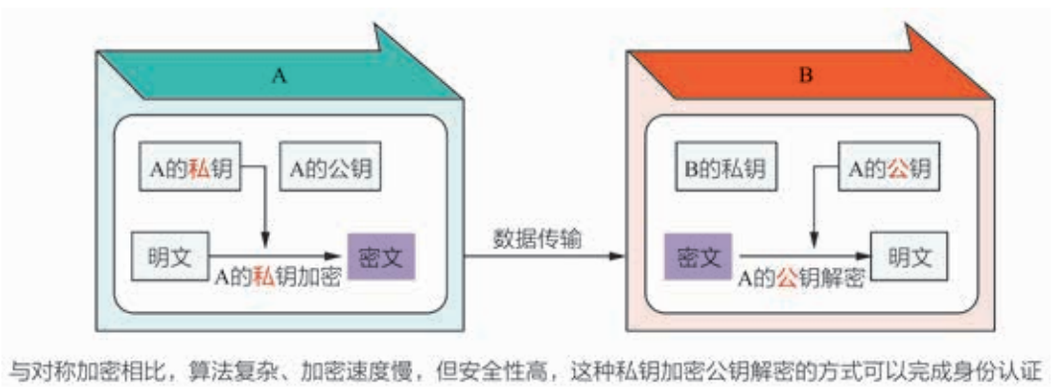


图5.2.5 使用非对称加密实现安全认证

除了RSA算法之外，DSA（Digital Signature Algorithm）也可以用于安全认证。

2. 数字签名

数字签名是目前最常用的安全认证方式，又称公钥数字签名、电子签章。数字签名类似写在纸上的普通的物理签名，但是使用了公钥加密领域的技术实现，用于鉴别数字信息的方法。一套数字签名通常定义两种互补的运算，一个用于签名，另一个用于验证。

数字签名过程如下：

发送报文时，发送方用一个哈希函数（如MD5）从报文文本中生成报文摘要，然后用自己的私人密钥对这个摘要进行加密，这个加密后的摘要将作为报文的数字签名和报文一起发送给接收方，接收方首先用与发送方一样的哈希函数从接收到的原始报文中计算出报文摘要，接着再用发送方的公用密钥来对报文附加的数字签名进行解密，如果这两个摘要相同，那么接收方就能确认该数字签名是发送方的（如图5.2.6所示）。

拓展链接

哈希函数

哈希函数（Hash）就是找到一种数据内容和数据存放地址之间的映射关系。Hash是主要用于信息安全领域中的加密算法，它把一些不同长度的信息转化成杂乱的128位编码，叫作Hash值。

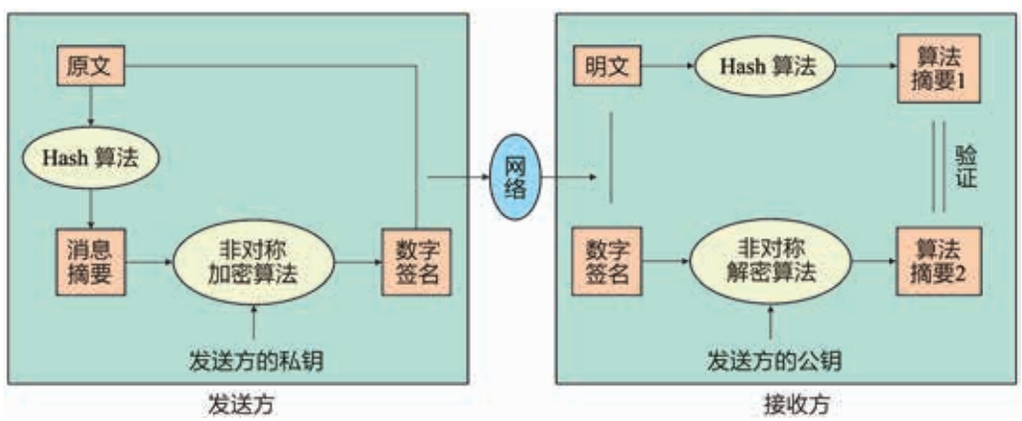


图5.2.6　使用非对称加密实现数字签名

数字签名有两种功效：①能确定消息确实是由发送方签名并发送的，因为别人假冒不了发送方的签名。②数字签名能确定消息的完整性，因为数字签名加密的是信息报文摘要，它代表了文件的特征，文件如果发生改变，数字摘要的值也将发生变化。

一次数字签名涉及一个哈希函数、发送者的公钥、发送者的私钥等。

3. 数字证书

数字证书也是非对称加密的一种应用。数字证书一般由独立的证书发行机构颁发，也可以自己颁发，自己颁发的证书称为自签名证书，颁发过程如图5.2.7所示。

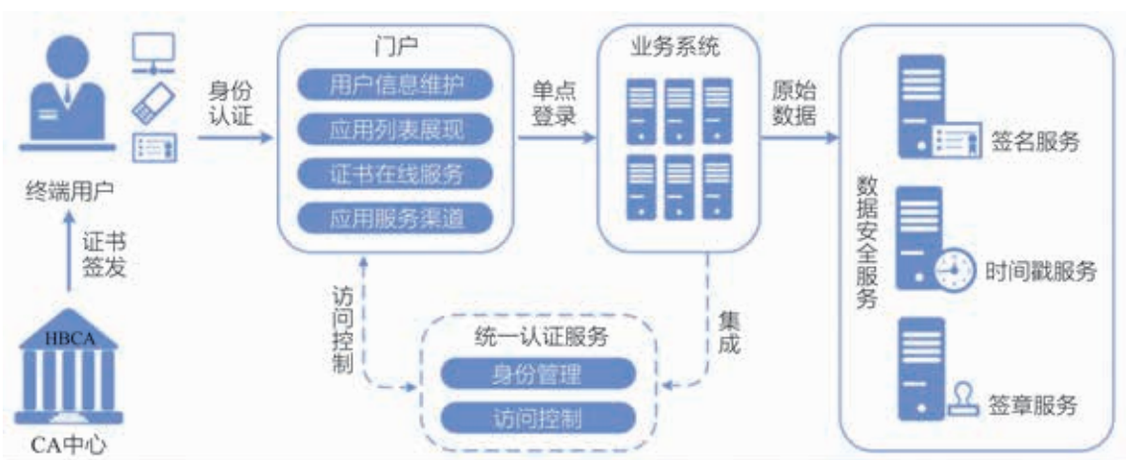


图5.2.7　数字证书的发放与使用

首先，用户生成密钥对，并将公共密钥及部分个人身份信息传送给认证中心。认证中心在核实身份后，将执行一些必要的步骤，以确信请求确实由用户本人发送而来。然后，认证中心将发给用户一个数字证书，该证书内包含用户的个人信息和他的公钥信息，同时还附有认证中心的签名信息。用户就可以使用自己的数字证书进行相关的各种活动。

由于目前各种软件如浏览器等都内置信任了证书颁发机构的根证书，所以浏览器对由此证书颁发机构发行的证书都认为是可以信任的，保证了信息的安全。

网银盾（USB Key）（见图5.2.8），是银行推出的安全产品，通过将制作好的电子证书存储在U盘而制成。客户在网上银行操作时，插入USB Key后，使用存储其中的证书来确保网上银行账户的安全，由于电子证书是有有效期的，过了有效期的网银盾就需要及时更新证书，更新证书的方式有网上下载或到银行更换。

图5.2.8　某银行网银盾

实践与体验

数字签名

可以通过RSA-Tools来体验数字签名。

实践内容：

通过RSA-Tools来体验数字签名，并用于信息的验证（见图5.2.9）。

实践步骤：

1. 首先用“RSA KeyGen”菜单生成一个随机密钥和公钥，可以用随机方式生成密钥；

2. 把公钥发给同桌同学，同时接收同桌同学的公钥；

3. 然后用“Sign & Verify”菜单下面的“Sign”菜单和本人的私钥生成信息的签名；

4. 和同学交换数字签名；

5. 最后用“Verify”菜单和同学的公钥验证同学的签名。

结果呈现：

验证成功，则可以确定签名是该同学所发，验证失败，则说明签名是伪造的。

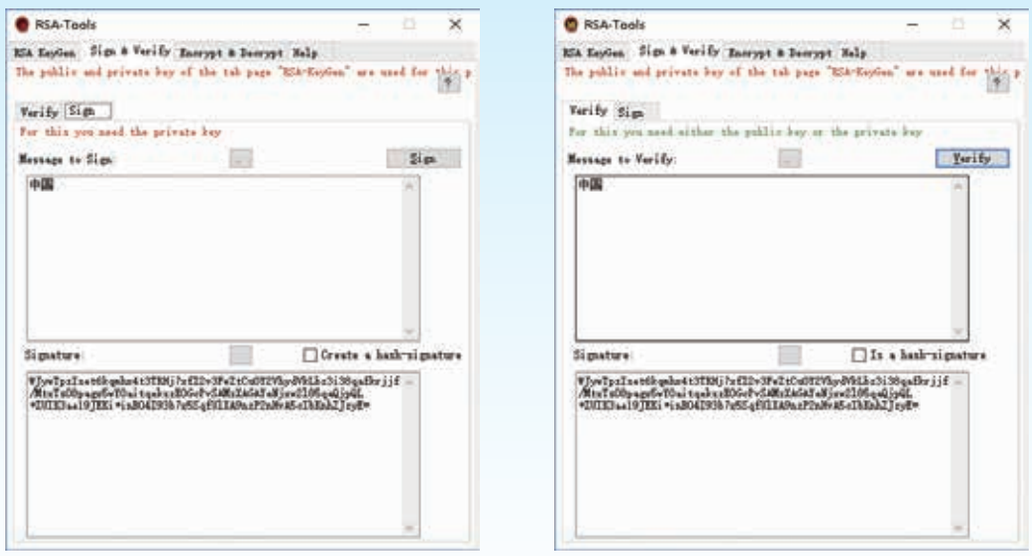


图5.2.9　使用RSA-Tools实现签名和验证

5.3 网络安全协议

建立计算机网络的目的是为了实现数据通信和共享，但是原始网络协议在安全性方面的不足造成了很多问题，需要在原有网络协议的基础上，增加一套有利于安全的协议，这就是网络安全协议。网络安全协议是营造网络安全环境的基础，是构建安全网络的关键技术，常见的网络安全协议如表5.3.1。

表5.3.1　网络安全协议

OSI模型	协议	安全协议
应用层	HTTP、FTP、TELNET、DNS	HTTPS、SSH
表示层		
会话层		SSL
传输层	TCP/UDP	
网络层	IP	IPSec
数据链路层	ARP	PPTP、L2TP
物理层	IEEE802.2	

网络传输安全的底层协议主要有PPTP、L2TP等，网络层协议有IPSec等，传输层协议有SSL等，应用层协议有HTTPS、SSH等，应用层协议一般是通过底层安全协议来加密的。由于对称加密的密钥容易泄露但加密速度快，而非对称加密的安全性高但加密速度慢，因此网络安全协议结合了这两种加密的特点。一般情况下，对称加密用于双方的数据传输，而非对称加密用于对称加密密钥的交换（用非对称加密技术对对称加密的密钥进行加密后再传输给对方），再结合单向加密用于信息的验证。由于对称密钥交换次数较少，不会耗费太多的时间，而具体的数据传输使用对称加密/解密速度较快，因此如此安排既提高了数据传输效率，又保证了数据的安全。

5.3.1　IPSec协议

IPSec通过使用加密的安全服务以确保在TCP/IP网络上进行保密而安全的通信。IPSec协议工作在OSI 模型的第三层，使其在使用时适合于保护基于TCP或UDP的协议。使用IPSec的好处在于：IPSec位于传输层之下，对所有应用和终端用户都是透明的，所以使用IPSec时既不需要对用户系统和服务器系统的软件做任何改变，也不需要对用户进行额外的安全培训。

1. IPSec应用模式

IPSec有两种应用模式：隧道模式（见图5.3.1）和传输模式（见图5.3.2）。隧道模式适用于两个安全网关之间的通信，如公司总部与分部之间通过公共网络的安全连接。传输模式适用于两台主机或一台主机和一个安全网关之间的通信，如公司外部计算机通过公共网络安全连接公司的内部局域网。

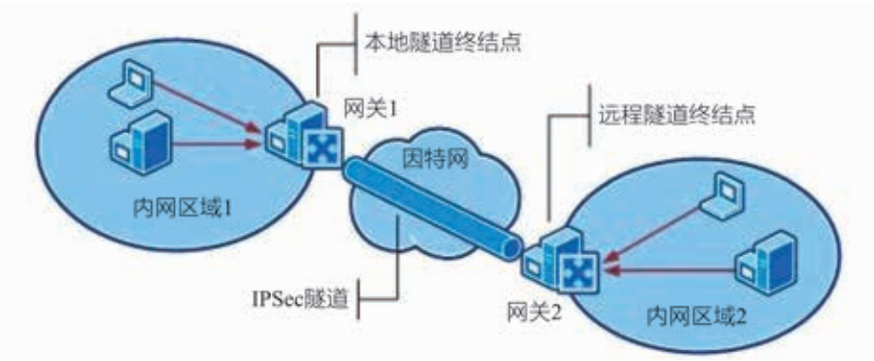


图5.3.1　IPSec隧道模式

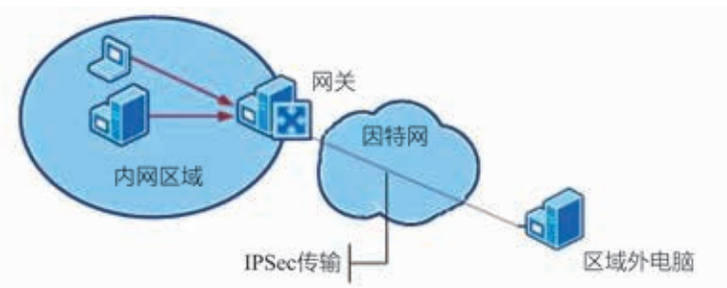


图5.3.2　IPSec传输模式

2. IPSec安全机制

IPSec提供了两种安全机制：认证和加密。认证机制使IP通信的数据接收方能够确认数据发送方的真实身份以及数据在传输过程中是否遭篡改。加密机制通过对数据进行编码来保证数据的机密性，以防数据在传输过程中被窃听。基于上述安全机制的IPSec拥有以下安全特性：

①合法性。数据源发送信任状，由接收方验证信任状的合法性，只有通过认证的系统才可以建立通信连接。

②不可否认性。当IPSec采用公钥技术通信时，可以证实消息发送方是唯一可能的发送者，发送者不能否认发送过消息。不可否认性是采用公钥技术的一个特征，当使用公钥技术时，发送方用私钥产生一个数字签名随消息一起发送，接收方用发送者的公钥来验证数字签名。

③反重播性。确保每个IP包的唯一性，保证信息万一被截取、复制后，不能被重新利用、重新传输回目的地址。该特性可以防止攻击者截取、破译信息后，再用相同的信息包获取非法访问权。

④数据完整性。防止传输过程中数据被篡改，确保发出数据和接收数据的一致性。IPSec利用哈希函数为每个数据包产生一个加密校验和，接收方在打开包前先计算检查校验和，若包遭篡改导致校验和不相符，数据包即被丢弃。

⑤数据可靠性。在传输前，对数据进行加密，可以保证在传输过程中，即使数据包遭截取，信息也无法被读取。

5.3.2 SSL协议

SSL（安全套接层协议）是由Netscape公司提出的安全交易协议，提供加密、认证服务和保证报文的完整性（见图5.3.3）。SSL协议建立在可靠的传输协议（一般为TCP）之上，为高层协议提供数据封装、压缩、加密等基本功能的支持。SSL相对于IPSec更容易穿越防火墙和内网，所以SSL一般用于客户端通过公共网络安全连接服务器，如HTTPS、SSH等。

图5.3.3 HTTPS协议

SSL协议提供的安全通道有以下三个特性：

机密性：SSL协议使用密钥加密通信数据。

可靠性：服务器和客户端都会被认证，其中客户端的认证是可选的。

完整性：SSL协议会对传送的数据进行完整性检查。

基于安全协议的网络安全技术：

①安全超文本传输协议（HTTPS）。依靠密钥对的加密，保障Web站点间的交易信息传输的安全性，是HTTP的安全版。因此HTTPS的安全基础是SSL。目前，重要的网站如银行网站、电子商务网站等的访问都适用HTTPS。

②安全外壳协议（SSH）。SSH是目前较可靠，专为远程登录会话和其他网络服务提供安全性的协议。利用SSH协议可以有效防止远程管理过程中的信息泄露问题。SSH客户端包含

拓展链接

密钥安全

现有的安全协议还是有一个漏洞：对称加密的密钥是通过非对称加密进行传输的，如果非对称加密的密钥在交换过程中被窃取，加密信息就可以被破解。为了解决这个问题，科学家提出了使用量子技术来分发密码。

量子通信的安全性基于量子物理基本原理，单光子的不可分割性和量子态的不可复制性保证了信息的不可窃听和不可破解，从原理上确保身份认证、传输加密以及数字签名等的安全，以更好地解决信息安全问题。

scp（远程拷贝）、slogin（远程登录，类似telnet）、sftp（安全文件传输，类似ftp）等应用程序。

5.3.3 虚拟专用网（VPN）

一个企业或团体可能在世界各地都有分支机构，如何让这些分支机构通过现成的互联网构成一个专用网络，就像是一个内部局域网一样？虚拟专用网络就是这样一种技术。

VPN在公用网络上建立专用网络，进行加密通信。VPN网关通过对数据包的加密和数据包目标地址的转换实现远程访问。按协议分，VPN主要有四种方式，基于PPTP协议、基于L2TP协议、基于IPSec协议和基于SSL协议。其中PPTP和L2TP协议工作在OSI模型的第二层，IPSec工作在第三层，SSL则工作在第四层，工作在不同层的VPN有不同的特点。

例

如果要将处于不同地域的局域网，通过专用的路由器、光纤等设备进行连接将是一笔非常大的投入。若使用VPN，则会大大节约成本，VPN通过公共网络将各处的局域网连接成一个大的局域网，可以使用基于IPSec隧道模式的VPN技术（如图5.3.4所示）进行连接。

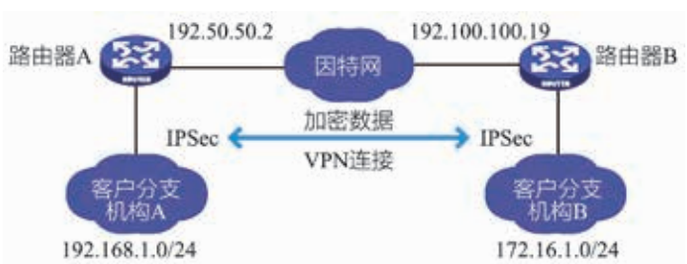


图5.3.4 隧道模式的VPN应用

问题与讨论

查询有关资料，讨论基于IPSec的VPN与基于SSL的VPN的优缺点，将讨论结果填写在下面的表格中，并探讨适合这些技术使用的场景。

表5.3.2 不同类型VPN比较

VPN	优势	不足
2层VPN		
IPSec VPN		
SSL VPN		

实践与体验

用SSH连接服务器

SSH软件正逐渐替代Telnet软件，成为网络管理员管理服务器的安全客户端。

SSH软件分为服务端软件和客户端软件。Linux操作系统服务器缺省安装一般都会包括服务端软件和客户端软件，可直接使用，但Windows操作系统中需要自己安装。

SSH客户端除了可以访问服务器外，也可以用于访问交换机、路由器等设备。

实践内容：

使用两台计算机，一台做服务器，一台做客户端，分别安装对应的SSH软件。用SSH客户端远程访问服务器，SSH客户端界面见图5.3.5。

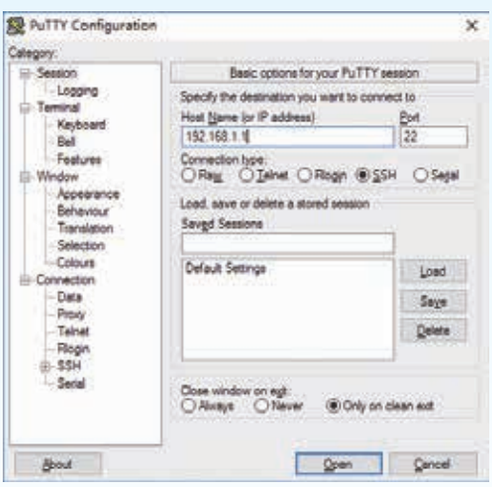


图5.3.5　SSH客户端界面

实践步骤：

1. 从http://www.freesshd.com/下载软件。
2. 分别在两台计算机上安装服务端和客户端。
3. 用客户端软件访问服务端。

结果呈现：

同学计算机之间相互访问。

思考与练习

列举日常生活中的哪些领域用到了网络安全技术，说说这些技术使用了哪些网络安全协议。

5.4 防火墙

防火墙（Firewall）是一种协助确保信息安全的设备或软件（见图5.4.1），它位于两个或多个网络之间（比如专网与公网，内网与外网），对两个网络之间的通信进行管理与控制，依照特定的规则，选择允许或是限制传输的数据通过，以保障系统的安全，是最重要的网络防护设备之一。

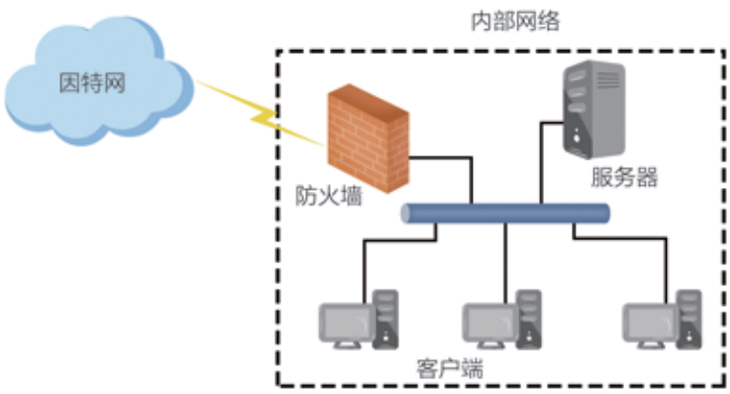


图5.4.1　防火墙示例图

5.4.1　防火墙主要功能

1. 网络安全的屏障

防火墙可通过过滤不安全的服务而减低风险，极大地提高内部网络的安全性。它可以禁止诸如不安全的协议进出受保护的网络，使攻击者不可能利用这些脆弱的协议来攻击内部网络。防火墙同时可以保护网络免受基于路由的攻击，如IP选项中的源路由攻击和ICMP重定向路径。防火墙能够拒绝所有以上类型攻击的报文，并将情况及时通知防火墙管理员。

2. 强化网络安全策略

通过以防火墙为中心的安全方案配置，能将所有安全软件(如口令、加密和身份认证等)配置在防火墙上。与将网络安全问题分散到各个主机上相比，防火墙的集中安全管理模式更加经济。

3. 对网络存取和访问进行监控统计

由于所有的访问都必须经过防火墙，所以防火墙不仅能够记录完整的日志，而且还能

够提供网络使用情况的统计数据。当发生可疑动作时，防火墙能进行适当的报警，并提供网络是否受到监测和攻击的详细信息。

4. 防止内部信息的外泄

通过利用防火墙对内部网络的划分，可实现内部网中重点网段的隔离，限制内部网络中不同部门之间互相访问，从而保障了网络内部敏感数据的安全。

防火墙通常使用的安全控制手段主要有包过滤、状态检测和代理服务等。包过滤技术是一种简单、有效的安全控制技术，它通过在网络间相互连接的设备上加载规则，允许、禁止来自某些特定的源地址、目的地址、TCP端口号等的数据包。包过滤的最大优点是对用户透明，传输性能高。状态检测是比包过滤更为有效的安全控制方法。对新建的应用连接，状态检测检查预先设置的安全规则，允许符合规则的连接通过，并在内存中记录下该连接的相关信息，生成状态表。对该连接的后续数据包，只要符合状态表，就可以通过。

5.4.2 防火墙分类

防火墙既可以是一台专属的硬件（硬件防火墙），也可以是架设在一般硬件上的一套软件（软件防火墙）。根据其作用范围，可以将防火墙分为个人防火墙和网络防火墙。根据其控制所用的协议，可以将防火墙分为网络层防火墙和应用层防火墙等。

1. 网络层防火墙

网络层防火墙也称包过滤防火墙。对每一个接收和发送的IP包应用一些规则，根据规则决定传递还是丢弃该包。过滤规则所包含的网络信息有源IP地址、目标IP地址、源目标端口号、接口（出站、入站、网卡）等（见图5.4.2）。

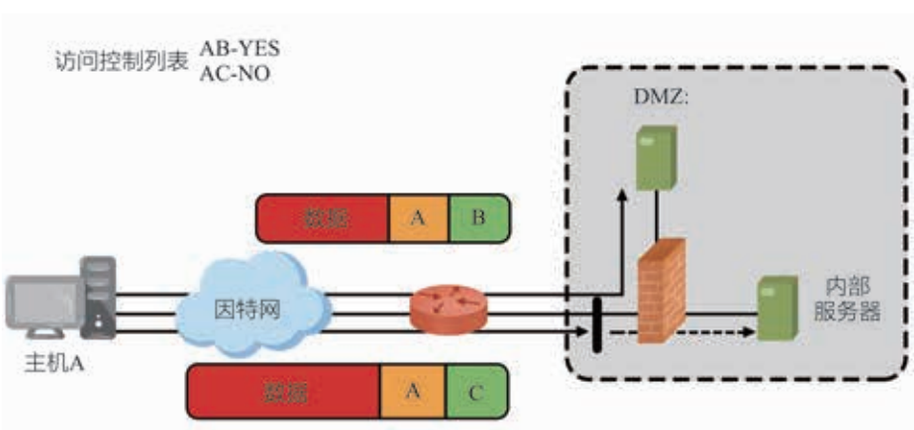


图5.4.2 包过滤防火墙示意图

传统的包过滤防火墙只对单个数据包进行判断，不考虑更高层的上下文信息。而带状

态检测的包过滤防火墙通过创建一个出站TCP连接目录来加强对TCP连接的控制。即在包过滤防火墙的基础上，增加了对历史和当前连接情况的分析，能进一步加强网络安全。

2. 应用层防火墙

应用层防火墙也称应用层网关，与网络层防火墙相比更安全但效率更低，属于服务型防火墙（见图5.4.3）。应用层防火墙是在TCP/IP协议族的“应用层”上运作的，使用浏览器或使用FTP时的数据流都属于这一层。应用层防火墙可以拦截进出某应用程序的所有封包，并且封锁其他的封包（通常是直接将封包丢弃）。理论上，这一类的防火墙可以完全阻绝外部的数据流进入受保护的机器。借由监测所有的封包并找出不符规则的内容，可以防范计算机蠕虫或是木马程序。

拓展链接

WAF防火墙

WAF（Web Application Firewall，Web应用防护系统），属于新兴的应用层防火墙，使用了先进的信息安全技术，可以对来自Web应用程序客户端的各类请求进行内容检测和验证，确保其安全性与合法性，对非法的请求予以实时阻断，从而更有效地解决Web应用的安全问题。

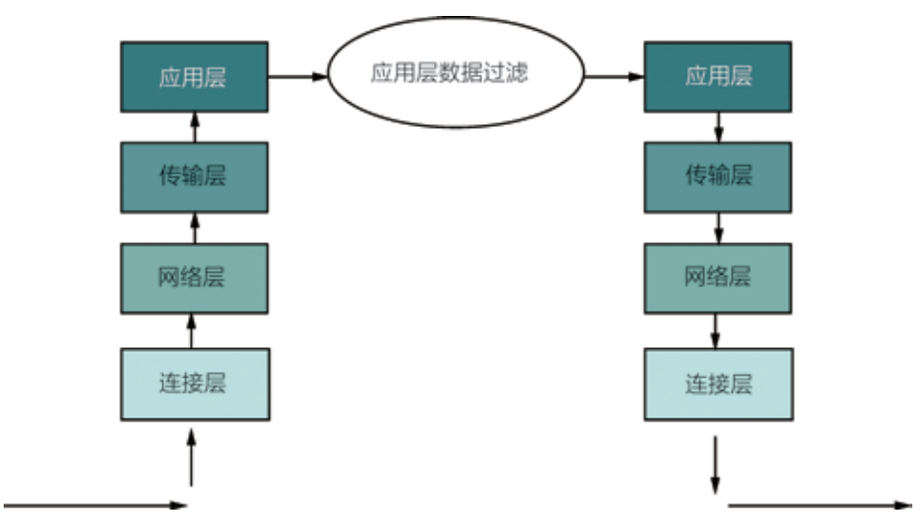


图5.4.3　应用层防火墙示意图

应用层防火墙关键技术包括Raw（数据包状态跟踪）、Nat（网络地址转换）、Filter（ip包过滤）、Mangle（路由标记），具体见表5.4.1。这四者之间的关系如图5.4.4所示。

表5.4.1　应用层防火墙规则表

规则	说明
Raw	确定是否对数据包进行状态跟踪
Mangle	为数据包设置标记
Nat	修改数据包的源/目标
Filter	确定是否放行该数据包

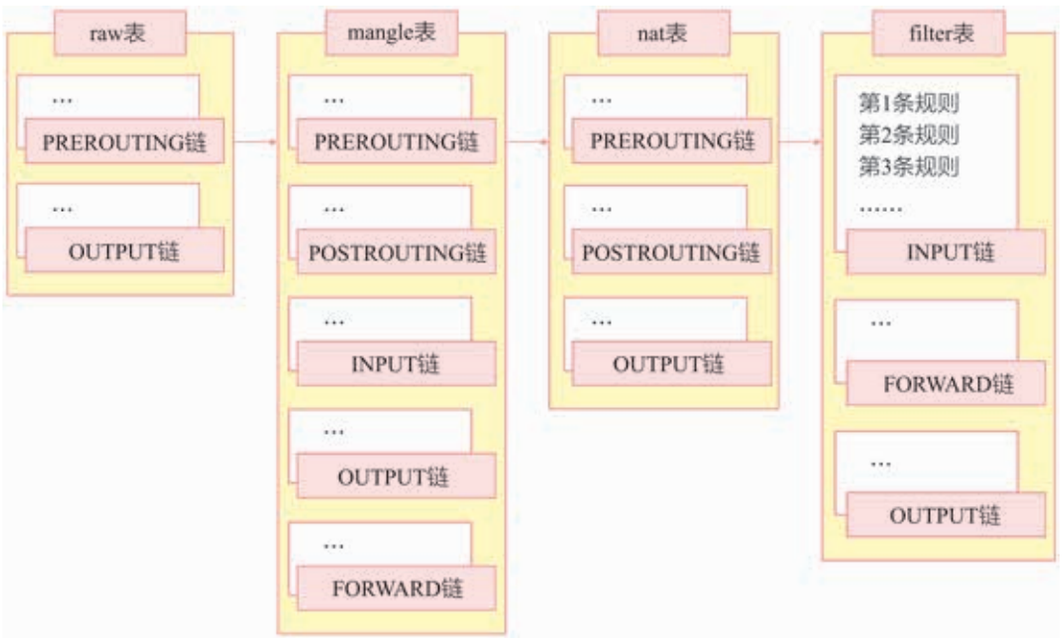


图5.4.4　应用层防火墙工作原理

数据包通过链的顺序如下：

入站操作：从外部主机访问本机或本网络。

PREROUTING→INPUT

出站操作：从本机或本网络访问外部主机或网络。

OUTPUT→POSTROUTING

转发操作：从外部网络或主机经由本地路由访问其他外部网络或主机。

PREROUTING→FORWARD→POSTROUTING

当多个规则表中都存在同一个规则链时，按以下顺序匹配：

Raw→Mangle→Nat→Filter

所有链的初始默认规则均为ACCEPT，设定规则只能是ACCEPT（允许）或DROP（阻止），若规则适配ACCEPT，则允许数据包通过，进入下一链，否则丢弃数据包，实行网络数据的拦截。

实践与体验

Windows防火墙的设置

Windows10系统都自带软件防火墙（图5.4.5），可以通过启用防火墙来增强系统的安全，考虑到某些应用的联网需要，可以开放部分端口或程序文件。

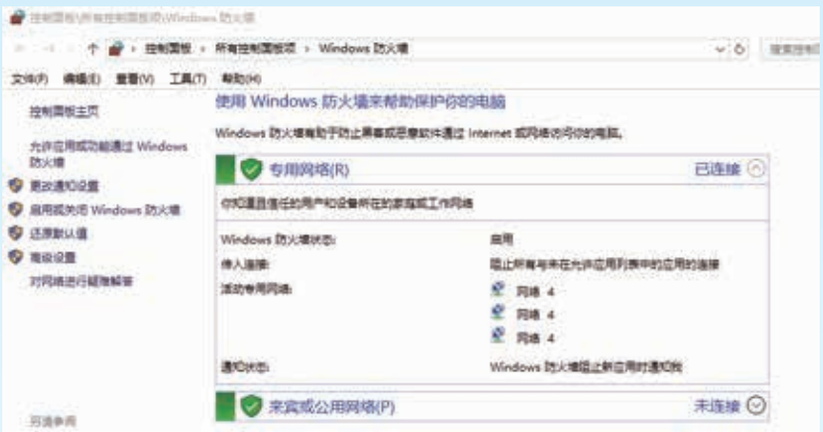


图5.4.5　Windows防火墙

实践内容：

通过设置Windows的防火墙来保障家庭上网的安全，包括IP地址过滤、端口和协议过滤、接口选择等。

实践步骤：

1. 设置“允许程序或功能通过Windows防火墙”即进入如图5.4.6界面，这个是最基础的配置，添加规则很简单，点击“允许其他应用”，选择你想要添加的程序即可，但是这里要区分专用网络和公用网络。这里只有最基础的通行或者不通行，不用端口等详细配置。因为对于普通用户来说，只是需要设置程序是否需要联网，不需要关心详细的规则。

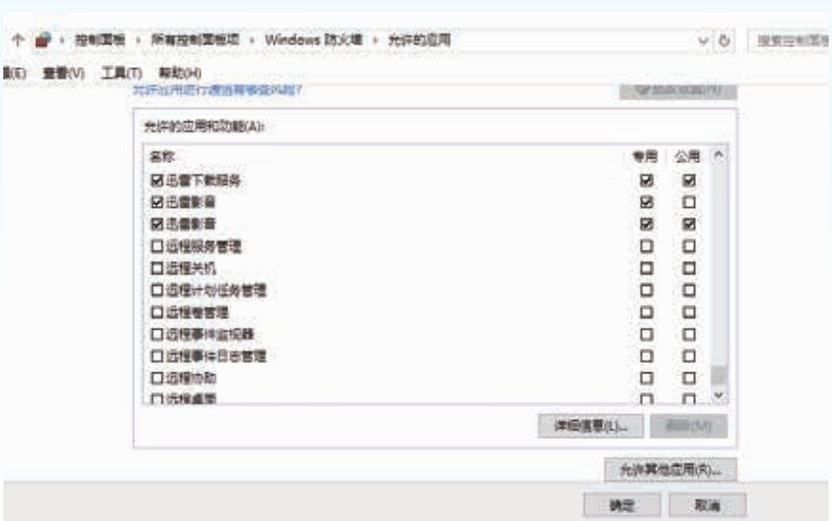


图5.4.6　Windows防火墙防护应用程序

2. 更改通知设置和打开或关闭Windows防火墙效果一样，出来的是如下界面，可以在这里选择启用或关闭Windows防火墙（图5.4.7）。

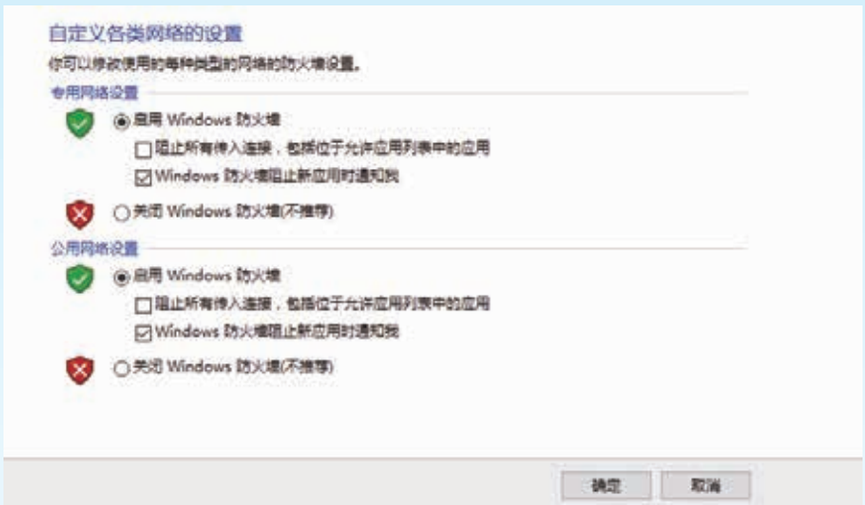


图5.4.7　启用Windows防火墙

在该界面选择对应区域的“启用Windows防火墙”启用相应区域的防火墙。此外，系统提供了防火墙还原默认设置功能，可以将防火墙还原到初始状态。

3. Windows防火墙进入“高级设置”选项中可以进行更加详细全面的配置，包括出入站规则、连接安全规则等都可以从这里进行自定义配置。“入站规则”（其他终端访问本机的规则）和“出站规则”（本机访问其他终端的规则）里，针对每一个程序都为用户提供了三种实用的网络连接方式：

允许连接：程序或端口在任何情况下都可以被连接到网络。

只允许安全连接：程序或端口只有IPSec保护的情况下才允许连接到网络。

阻止连接：阻止此程序或端口在任何状态下连接到网络。

结果呈现：

同学之间通过访问共享文件的方式，互相测试对方的防火墙。

思考与练习

请尝试配置Windows防火墙，实现在本地计算机限制某些程序（比如迅雷、QQ等）连接因特网。

巩固与提高

1. 在2016年，黑客的钓鱼攻击造成了乌克兰70万家庭断电，具体过程如下：黑客仅仅是在电子邮件之外使用了一些小手段，就在机构的系统上种植了黑色能量（blackenergy）木马。攻击者研究目标机构的员工，分辨哪些人会打开钓鱼邮件，并使用假冒的电子邮箱地址向其发送含excel表格的邮件，并引诱其点击恶意软件。通过感染了恶意软件的员工计算机让系统的一部分断线，导致了停电。

请你根据该事件，分析该发电厂应该采取的安全措施。

2. 对称加密和非对称加密的特点分别是什么？

3. 使用个人商店或宾馆提供的免费Wi-Fi一般具有较大的风险，但在不得已必须使用免费Wi-Fi时，可以采取哪些措施保证安全？请你说出使用这些措施的理由。

4. 目前的防火墙按照运行所在协议层可以分为4层防火墙和7层防火墙，尝试运用TCP/IP协议来分析不同类型的防火墙在防护不同网络应用时需要开启的功能，比如禁用QQ、微信该用哪一类防火墙。

项目挑战

让智慧校园更安全

物联网由于包含了服务器、终端、感应器、软件及相关数据，系统复杂。由于物联网通常连接网络设备，对安全性要求更高。

面对初步完成的智慧校园项目，其安全性令人担忧。试想，如果有人入侵了智慧校园网络服务器，就可以对校园内连接上智慧校园系统的各种设备进行控制，制造各种安全事端。

项目任务

通过一系列技术手段，让智慧校园网更加安全。

过程与建议

1. 分析网络的安全隐患

通过对网络协议、网络服务器、终端的分析，查出智慧校园网的安全隐患。

安全对象	安全隐患	结论
网络协议	有无加密	
网络服务器	有无防火墙	
终端1：	有无身份认证	
终端2：	有无身份认证	
终端3：	有无身份认证	
终端4：	有无身份认证	
终端5：	有无身份认证	
……		

在上面表格的“结论”栏中填写“有”或“无”。

2. 确定信息安全等级

《信息安全等级保护管理办法》规定，国家信息安全等级保护坚持自主定级、自主保护的原则。信息系统的安全保护等级应当根据信息系统在国家安全、经济建设、社会生活中的重要程度，信息系统遭到破坏后对国家安全、社会秩序、公共利益以及公民、法人和其他组织的合法权益的危害程度等因素确定。

信息系统的安全保护等级分为以下五级：

第一级，信息系统受到破坏后，会对公民、法人和其他组织的合法权益造成损害，但不损害国家安全、社会秩序和公共利益。第一级信息系统运营、使用单位应当依据国家有关管理规范和技术标准进行保护。

第二级，信息系统受到破坏后，会对公民、法人和其他组织的合法权益产生严重损害，或者对社会秩序和公共利益造成损害，但不损害国家安全。国家信息安全监管部门对该级信息系统安全等级保护工作进行指导。

第三级，信息系统受到破坏后，会对社会秩序和公共利益造成严重损害，或者对国家安全造成损害。国家信息安全监管部门对该级信息系统安全等级保护工作进行监督、检查。

第四级，信息系统受到破坏后，会对社会秩序和公共利益造成特别严重损害，或者对国家安全造成严重损害。国家信息安全监管部门对该级信息系统安全等级保护工作进行强制监督、检查。

第五级，信息系统受到破坏后，会对国家安全造成特别严重损害。国家信息安全监管部门对该级信息系统安全等级保护工作进行专门监督、检查。

根据分析结果，对于智慧校园安全防范措施进行规划，划分具体的操作步骤，并进行步骤的优化，减少不必要或重复的操作。

根据上述分级，确定智慧校园系统的系统等级为_____。

3. 系统整改方案

根据上述的安全隐患，创建一个切实可行的安全整改方案，具体整改项目如下：

对象	安全隐患	整改方案

可以通过使用安全协议、配置防火墙、进行身份验证等手段来提高系统的安全性。

4. 展示交流

与其他团队交流分享，从任务完成过程、完成情况、团队沟通规则等角度发现问题，相互借鉴优点，继续完善。

评价标准

请根据项目实施的过程、结果和交流效果，对自己完成项目的情况进行客观的评价，并思考后续完善的方向。将评价结果和完善方案填写在下面的表格中。

评价条目	说明	评分（1～10分）	评分主要依据阐述	后续完善方向
分析网络的安全隐患	网络安全隐患的查找是否全面			
确定信息安全等级	信息安全等级的确定是否符合实际需要			
系统整改方案	系统整改方案是否全面、可行			
展示分享	展示方式的合理性（项目成果的展示方式选择能让人较好地了解项目的意义以及问题求解的特点）			

拓展项目

1. 分析阿里云里面的安全服务，结合某IT公司的网络需求，为该公司配置安全网络Web服务和防火墙。

2. 列举当前社会生产生活中可以利用安全网络应用的例子，编写项目方案。