普通高中教科书

信息技术

选择性必修 2

网络基础

人民教育出版社　中国地图出版社

微信公众号：电子课本大全

普 通 高 中 教 科 书

信息技术

选择性必修 2

网络基础

人民教育出版社课程教材研究所信息技术课程教材研究开发中心
中国地图出版社教材出版分社 编著

总主编 祝智庭 樊 磊

人民教育出版社 中国地图出版社
·北京·

微信公众号：电子课本大全

总 主 编：祝智庭　樊　磊
副总主编：郭　芳　高淑印　李　锋

本册主编：慈黎利　熊雪亭
编写人员：梁南燕　武　迪　王集伟　佟松龄　王学红

责任编辑：梅栾芳　杨聪晖
美术编辑：李　媛　徐海燕

微信公众号：电子课本大全



前言

同学们，欢迎探索信息技术这个神奇而充满魅力的世界。

在以往的学习、生活中，你们已经积累了许多信息技术方面的知识与技能，例如：在网上查阅资料，用手机与亲朋好友保持联系，使用移动终端、自动柜员机等设备……你们知道这些应用中都包含哪些关键技术，涉及哪些领域吗？怎样有效地利用这些技术帮助我们培养信息意识，提升计算思维，进而通过数字化学习与创新，承担起信息社会责任呢？即将开始的这门课程，会帮助你们对信息技术有更多的认识和思考，获得更丰富的体验和感受。

为了很好地掌握信息技术，希望同学们按以下三个要求去努力。

1. 认真阅读教科书，理解基本概念和原理。信息技术发展非常迅猛、各类信息系统不断涌现，但信息系统的基础和运行体系相对稳定，离不开算法的设计及对数据的利用。只有夯实基础，才能学好本领，跟上时代发展的步伐。

2. 敢于动手，勤于实践。信息技术是一门实践性较强的课程。实践能帮助同学们熟练操作技能，进一步掌握知识。因此，要认真阅读理解每章的主题学习项目，并逐步完成“实践活动”“思考活动”“技术支持”“阅读拓展”等栏目的学习内容，在实践中获取知识和经验。

3. 要有积极探究、锲而不舍的精神。掌握信息技术的知识与技能需要一个过程，不可能一蹴而就。信息技术学科内容非常丰富，各知识点之间联系密切，但名词术语多，有可能令人感到繁杂，甚至产生畏难情绪。学习新知识，首先要知其然，接着通过不断学习，积极动手操作，大胆请教，加深对知识的理解，然后才能知其所以然，在不断的探索过程中取得进步。

本书中涉及的配套资源，可在教科书配套教学资源平台的信息技术栏目中获得。让我们开始一段信息技术新旅程，成长为信息社会中合格的中国公民！

微信公众号：电子课本大全

目录



第 1 章　网络概述　1

主题学习项目：网络基础探究竞　2

1.1　网络与生活　3

1.1.1　计算机网络　4

1.1.2　移动互联网　6

1.1.3　网络在现代社会中的应用　7

1.1.4　网络对社会生活的影响　12

1.2　网络的类型　14

1.2.1　按覆盖范围分类　15

1.2.2　按传输介质分类　16

1.2.3　按拓扑结构分类　18

1.2.4　按传输方式分类　20

1.2.5　按服务方式分类　21

1.2.6　影响网络传输质量的主要物理因素　22

总结评价　26



第 2 章　网络协议、设备与操作系统　27

主题学习项目：安全组建局域网　28

2.1　网络通信基础　29

2.1.1　数据交换技术　30

2.1.2　TCP/IP 协议　33

微信公众号：电子课本大全

2.1.3 IP地址 36
2.1.4 域名 40
2.2 网络设备与操作系统 46
2.2.1 常见的网络设备 47
2.2.2 网络操作系统 52
2.2.3 局域网的安全策略 53
总结评价 56



第3章 网络安全与网络资源 57
主题学习项目：安全分享细细说 58
3.1 加密技术与安全 59
3.1.1 网络通信面临的威胁 60
3.1.2 数字摘要及网络应用 61
3.1.3 加密技术及网络应用 65
3.1.4 身份认证 83
3.1.5 防火墙 84
3.2 网络资源分享 88
3.2.1 网络资源简介 88
3.2.2 网络资源分享实例 90
总结评价 98

微信公众号：电子课本大全



第4章　物联网与创新网络服务　99

主题学习项目：创新网络与社会　100

4.1　物联网简介　101

4.1.1　认识物联网　102

4.1.2　物联网的发展历程　103

4.1.3　相关设备　104

4.1.4　感测技术简介　107

4.1.5　联网技术简介　109

4.1.6　服务器端技术简介　113

4.2　创新网络服务与隐私保护　116

4.2.1　网络服务新案例　117

4.2.2　信息社会中的个人隐私保护　119

总结评价　124

项目评价　125

微信公众号：电子课本大全



第 1 章
网络概述

网络是数据传输的物理基础，是支撑信息社会的重要基础设施。它已经渗透到社会的方方面面，正在改变着每个人的工作、学习和生活，各国政府治理国家的方式也因网络的普及而发生着变化。掌握“网络生存”的相关知识与技能，是信息社会对每一位成员提出的基本要求。

微信公众号：电子课本大全

01 主题学习项目：网络基础探究竟

项目目标

网络已经应用到社会的方方面面，了解网络的历史、作用以及网络的类型、拓扑结构等基础知识，可以帮助我们更好地理解网络，面对网络。本章通过阅读课本、上网搜索、动手实践等方式，收集资料，完成名为“网络，我来说”的主题作品。

1. 围绕项目问题，收集资料，归纳总结网络的发展历史、应用现状和社会影响。

2. 知道网络类型、拓扑结构、传输介质等知识。

项目准备

为了完成项目，需要做以下准备。

- 4到6人组建一个小组，各组确定一名组长，按小组学习的方式展开项目活动。
- 小组成员应分工协作，共同收集相关资料，然后汇总成一份电子作品。
- 准备中国互联网络信息中心最新发布的《中国互联网络发展状况统计报告》，以及与互联网相关的资料和调研报告。

项目过程

为了保证顺利完成本章的学习活动，在不同学习阶段，小组长要注意检查组员项目学习的进度，并做好协调互助工作。

1 收集资料

通过不同途径，收集介绍计算机网络和移动互联网的相关资料。 P5

2 归纳总结

根据获取的资料，归纳总结互联网的发展历史、应用现状和社会影响。 P13

3 整理分析

整理网络类型特征；分析影响网络通信质量的主要物理因素。 P24

4 制作作品

根据自己的理解，制作活动所需的电子作品，并在全班展示交流。 P25

项目总结

汇集组员学习心得，并对比任务目标进行分类、归纳和提炼，进一步认识网络和网络的作用，然后在全班进行展示和交流。具体内容包括：了解计算机网络的发展历史，知道网络的结构、类型、特征及演变过程；理解计算机网络与通信、互联网及移动互联网对现代社会的重要意义；认识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；描述网络的拓扑结构及不同类型网络的主要特点。

微信公众号：电子课本大全

1.1 网络与生活

学习目标 ▶▶▶

- 了解计算机网络的发展历史。
- 熟悉常见网络服务的应用场景，知道这些服务的特点。
- 理解计算机网络与通信、互联网及移动互联网对现代社会的重要意义。

体验探索

回顾网络浏览和收发电子邮件的过程



图1.1.1 网络浏览和发送电子邮件示意图

观察图1.1.1，结合已经学过的内容，完成以下任务。

· 描述一封电子邮件在图1.1.1所示网络中的传送过程。

· 尝试描述网络浏览的过程，以及网络浏览所使用的通信协议。

微信公众号：电子课本大全

1.1.1 计算机网络

特征：
1. 包含多台计算机；
2. 以实现信息交换和资源共享为目标；
3. 使用统一的通信协议。

计算机网络的发展历程

计算机网络是用通信线路把若干台计算机互相连接起来，遵照某些通信协议，用于实现信息交换和资源共享的系统。一般认为计算机网络经历了四个发展阶段：诞生阶段、形成阶段、互联互通阶段和高速网络阶段（图1.1.2）。

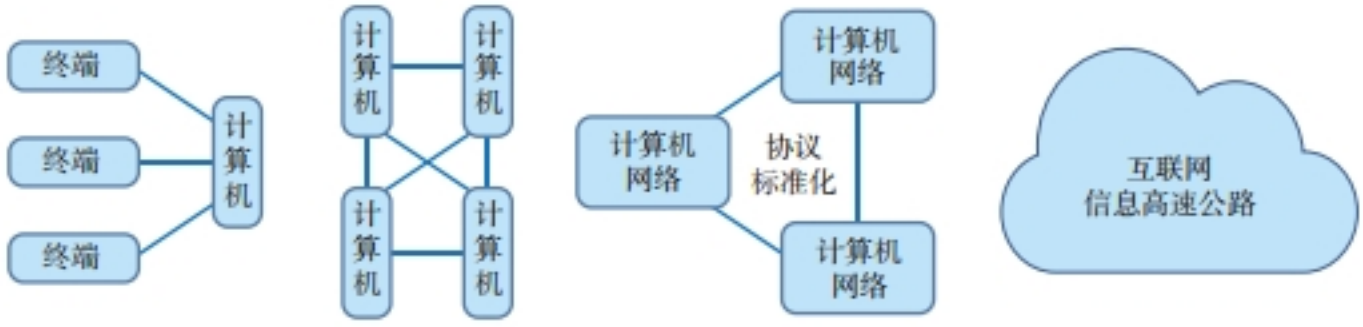


图1.1.2　计算机网络的发展

在诞生阶段，计算机的数量很少，这个阶段的特征是多个终端共享一台计算机，因此也被称为“面向终端的计算机通信网”；在形成阶段，其主要特点是实现了计算机之间的互联，诞生了真正意义上的计算机网络，如阿帕网（ARPANET）；在互联互通阶段，其特点是实现了通信协议的标准化，TCP/IP协议走上了历史的舞台；在高速网络阶段，作为“信息高速公路”的互联网，在社会中的应用日益普及，并诞生了覆盖全球的计算机网络——因特网。图1.1.3列出了互联网发展的主要事件。

严格来说，诞生阶段的面向终端的联机系统，不属于计算机网络，因为终端没有独立的数据处理能力。

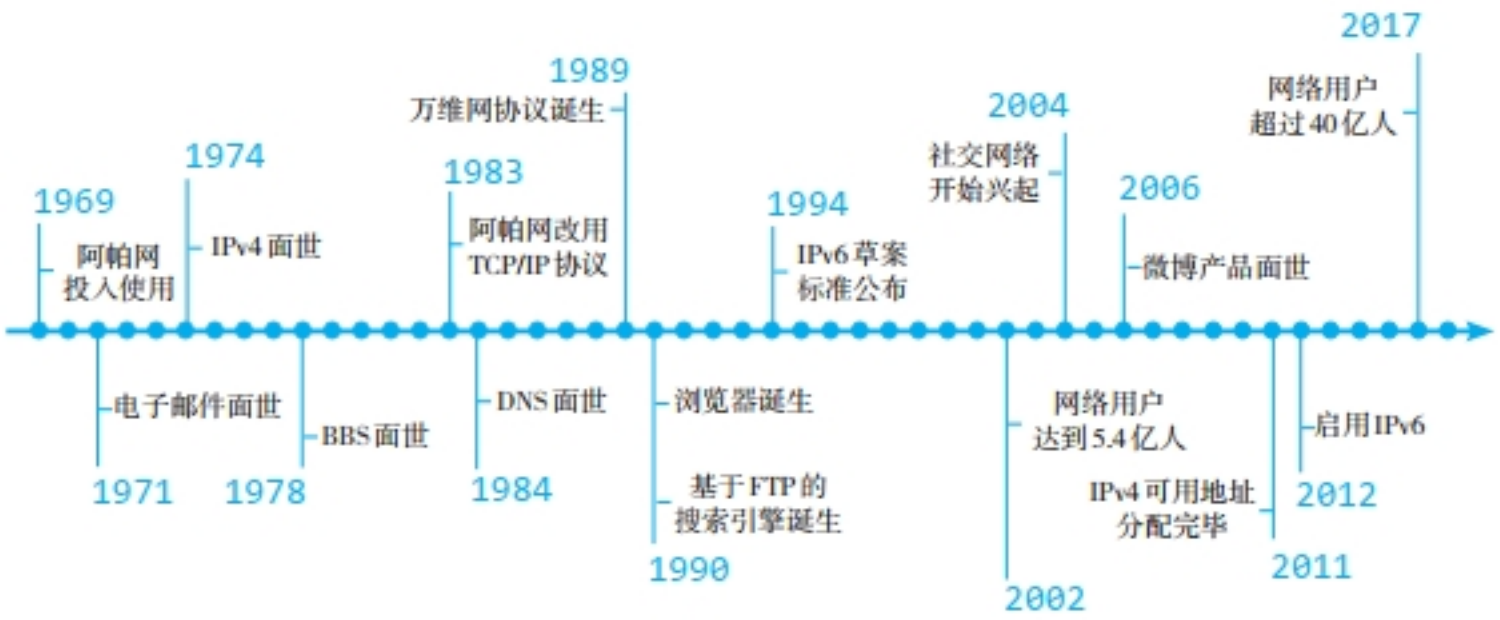


图1.1.3　互联网发展大事记

微信公众号：电子课本大全

我国互联网的发展历程

1987 年，北京计算机应用技术研究所建成我国第一个国际互联网电子邮件节点，揭开了中国人使用互联网的序幕；1994 年，我国实现与国际互联网的全功能连接，成为真正拥有全功能互联网的国家。从此，互联网开始在我国迅猛发展。

项目实施

了解互联网在我国的发展历程

搜索、阅读有关我国互联网发展情况的资料，然后选取你觉得最重要的事件，填入图 1.1.4 中，并谈一谈这些事件对你的影响。

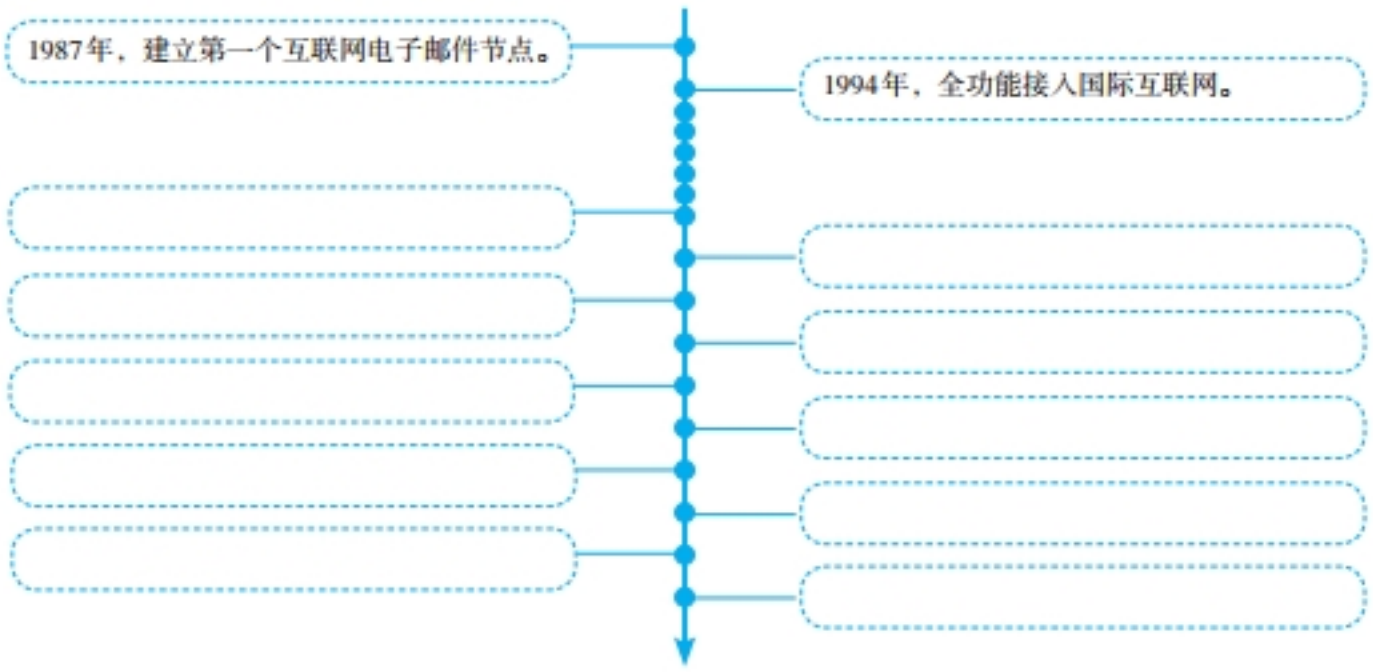


图 1.1.4 “我心中的中国互联网发展大事记”

思考活动

探讨互联网的发展及影响

汇总小组成员收集到的资料，尝试回答以下问题。

1. 我国网民总数哪一年超过了 1 000 万人？哪一年超过了 1 亿人？哪一年位居世界第一？当前的网民总数是多少人？

2. 我国曾经面临过哪些严重的网络威胁？采取了哪些措施加以应对？就你个人的感受而言，你觉得应对的效果如何？

3. 你知道“互联网 +”是什么意思吗？

微信公众号：电子课本大全

1.1.2 移动互联网

随着移动通信技术的发展，以智能手机为代表的移动终端也大量接入互联网，形成了日益普及的移动互联网。

第一代移动通信网（简称1G），主要用于提供语音业务，用的是模拟信号；2G改用数字信号，不仅可以语音通话、收发短信，还可以进行简单的网络操作；大力推广3G时，各种智能手机随之出现，网速的提升和移动设备性能的提高，使得移动互联网得到了快速发展（图1.1.5）。

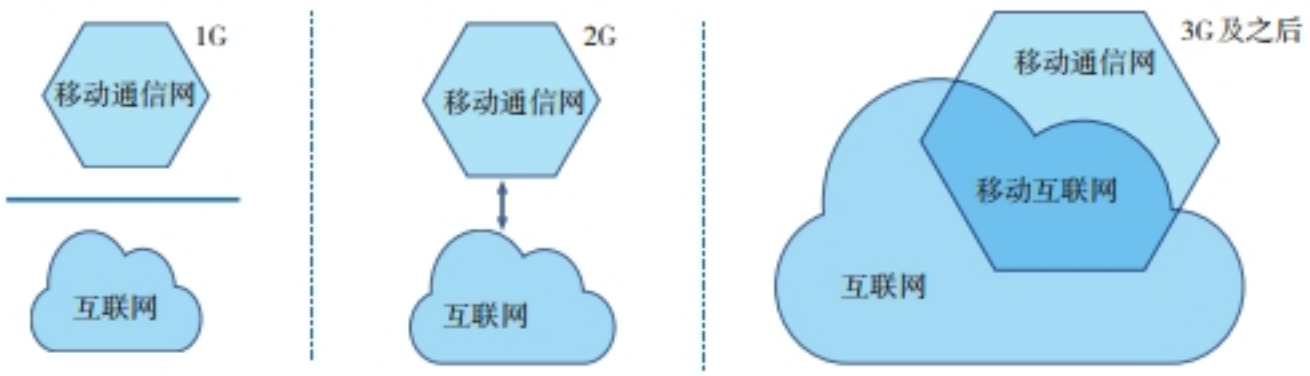


图1.1.5 移动互联网发展示意图

移动互联网也离不开传统互联网和计算机。例如，手机等移动终端中的网络应用软件（图1.1.6），工作时通常都要连入传统的互联网，寻求各种计算机服务器的支持。



图1.1.6 几种手机应用及界面

微信公众号：电子课本大全

思考活动

总结我国移动互联网的发展

我国的移动互联网从何时开始迅猛发展？手机“上网”后都能用来做什么？总结一下你所知道的手机应用软件以及它们的功能。

1.1.3 网络在现代社会中的应用

数据通信是网络最基本的功能，也是实现其他应用功能的基础；而资源共享是网络应用的主要目标，包括软件、硬件和数据资源的共享。在信息社会，网络已经成为连接个人、企业、机构、政府等社会成员的最重要的信息交流方式。

从我国网民的网络应用看，可以归纳为基础应用、商务交易、网络金融、网络娱乐和公共服务五类，具体可细分为搜索引擎、电子邮件、网络新闻、即时通信、网络音乐、网络游戏、网络购物等。

项目实施

了解我国网民互联网应用情况

1. 查阅最新的《中国互联网络发展状况统计报告》，了解我国网民使用互联网的现状，并填写下列表格。

表 1.1.1 互联网应用的使用情况

类别	应用	网民使用率	年增长率
基础应用	即时通信		
	搜索引擎		
	网上支付		

微信公众号：电子课本大全

表 1.1.2　手机互联网应用的使用情况

应用	网民使用率	相关的手机应用程序
手机即时通信		

2. 谈一谈你用过或知道的互联网应用，以及这些应用带来的改变。



图 1.1.7　用手机进行语音搜索

基础应用主要包括即时通信、搜索引擎、网络新闻、社交应用等，用于解决信息获取和交流沟通等问题。近年来，基础应用一直保持稳定增长。

即时通信是目前使用最广泛的网络应用，相关产品在不断创新。比如，有些侧重于提供更有效的分发方式，有些侧重于游戏、直播等应用的连接，还有些主攻商务办公。

搜索引擎的移动化趋势越发明显。随着人工智能技术，特别是自然语言问答技术的发展和完善，越来越多的人开始利用语音进行搜索（图 1.1.7）。

网络新闻的影响力进一步扩大，相关的法律法规进一步健全，越来越多的传统媒体开始利用网络发布采编的新闻。

以微信朋友圈、QQ 空间、微博等为代表的社交类应用的传播影响力在显著上升。越来越多的机构纷纷以官方微博、微信公众号等形式发布权威信息、扩大传播范围。

思考活动

了解我国信息服务的相关规定

搜索查阅《互联网群组信息服务管理规定》《互联网新闻信息服务管理规定》等法律法规，了解近年来国家在规范互联网基础应用方面所做的努力，并结合身边的事例，谈一谈你对这些规定的看法。

微信公众号：电子课本大全

商务交易具体包括网络购物、旅行预订等应用，这类应用正在加速线上和线下的融合，具体形式包括传统的零售企业与电商企业合作开店，电商企业独自开办体验店、专卖店等。

通过网络进行商务交易时，买方足不出户就可以货比三家，购买时通过网上支付、网上银行等缴纳货款；卖方在平台上展示相关商品的信息，然后通过快递（图1.1.8）、邮寄等方式发送实体产品，或者提供预订机票、预订酒店房间等服务。无论是对买方，还是对卖方来说，网络商务交易的便利性都非常突出，因此广受人们的欢迎。



图1.1.8　收快递

实践活动

了解电子商务类型

目前在网络中开展的电子商务活动，可以划分成B2B、B2C等类型。查阅相关资料，并填写表1.1.3。

表1.1.3　常见的电子商务类型

简称	全称	实例
B2B		
B2C		
C2C		
O2O		

网络金融主要包括互联网理财、网上支付等。互联网理财多元化发展趋势明显：一方面，银行、基金公司等传统机构，开始提供越来越多的在线理财产品；另一方面，互联网催生出了余额宝等新式的网络理财方式。

网上支付，特别是移动支付，在社会中的应用越发深入，它已经跨过了水、电等生活缴费的范围，开始向公共交通、医疗等领域扩展。

安全问题，是困扰移动支付快速发展的重要因素。近年来，随着指纹识别、面部识别等身份识别技术的发展，移动支付的安全性和便捷性，都得到了很大提升。关于网络中使用的身份识别技术，将在第3章进行介绍。

微信公众号：电子课本大全



图1.1.9　不要沉迷网络游戏

网络娱乐类应用多种多样，如网络音乐、网络文学、网络视频、网络游戏等。网络娱乐可以缓解压力、愉悦心情，但也存在很多问题。网络音乐、网络文学和网络视频等经常引发版权保护问题，网络游戏的争议更大，国家出台了多项法律法规来规范网络游戏的运营（图1.1.9）。例如，经营网游的机构必须采取技术措施，预防未成年人沉迷；未经用户同意，不得强制对战；不得为未成年人提供虚拟货币交易服务；虚拟货币不得用于支付、购买实物或兑换其他产品和服务，等等。然而在现实生活中，网络游戏引发的问题仍然层出不穷。

思考活动

阐述对网络游戏的看法

阅读下面关于网络游戏的论述，谈一谈你怎么看待网络游戏。如果由你来管理网络游戏，你会采取怎样的措施？

1. 网络游戏拖累学业，损害身心健康，诱发青少年犯罪，是一种新型的“毒品”，应当坚决取缔。

2. 网络游戏不是问题产生的真正根源，封杀它只是堵住了一个出口，这些问题还会从其他地方冒出来。

3. 网络游戏的“罪”不在游戏自身，而在玩游戏的人。

4. 一些网络游戏中含有暴力、迷信等不健康内容，这些网络游戏本身确实存在问题，应当予以规范。

公共服务的典型例子包括网约车和在线教育等。网约车，让预约出行等行为习惯越来越深入人心，同时，也有利于调动更多的社会交通资源，缓解人们“出行难”这一问题。在线教育正在以一对一、一对多、多对多等方式满足着人们多样化的学习需求。

思考活动

了解我国的网络公共服务

你接触过哪些公共服务类的网络应用？这些网络应用的功能是什么？能给使用者或社会带来什么样的便利？又可能会造成哪些问题？国家出台了哪些措施来应对新出现的问题？

微信公众号：电子课本大全

为了更好地满足信息社会的发展需求，很多社会管理和公共服务的开展都采用了在线的方式。这些举措都属于在线政务。

在线政务（图1.1.10）可以帮助政府及时、便捷、充分地获取、分析民众的需求，有助于决策过程和方法的科学化；可以更加便捷地公布各类信息，有助于政务的公开与透明；可以提高公文、资料的流转速度，提高办事效率；可以让民众和政府方便地进行互动，从而促进彼此的理解，帮助达成共识。



图1.1.10　在线政务

近年来，我国的在线政务得到了长足的发展，线上办公的使用率显著提升，在线政务正朝着智能化、精细化方向发展。

项目实施

了解我国在线政务的发展情况

查阅相关资料，了解我国在线政务服务的发展情况，并回答以下问题。

1. 从技术实现上看，我国在线政务服务都有哪些形式以及具体实例？

- 政府网站，实例：_____
- 官方微博，实例：_____
- 微信公众号，实例：_____
- _____，实例：_____
- _____，实例：_____

2. 从服务领域看，我国在线政务包括哪些服务类型？能提供什么服务？

- 气象信息，简介：_____
- 生活缴费，简介：_____
- 驾驶员服务，简介：_____
- _____，简介：_____
- _____，简介：_____
- _____，简介：_____

3. 在线政务的开设机构具体都有哪些？是否已经覆盖人们日常生活的需求？你对当前的在线政务发展情况有什么意见或建议？

微信公众号：电子课本大全

1.1.4 网络对社会生活的影响

目前，网络已广泛应用于教育、科研、商业等多个领域。网络可以促进社会平等，促进文化融合，增强社会联系；同时，它又可能加速文化侵蚀，拉大数字鸿沟，加剧社会隔离。

网络的出现打破了信息垄断，任何人，无论出身、民族、肤色、地域、学历、职位……在它面前都是平等的，都可以把各种“好事情”“坏消息”发布到网上，也可以方便地获取信息为己所用。



图 1.1.11　网络交流

一个网络群体的成员可能来自不同的国家、属于不同的民族、有着不同的文化背景……现实中他们可能无法面对面地交流，但借助网络，他们可以针对共同关心的话题畅所欲言，让各方意见得到充分展现（图 1.1.11）。比如，通过小区论坛与邻居讨论小区建设问题，利用即时消息与远方的亲戚朋友联络感情，发送电子邮件为各种公共政策献计献策……



图 1.1.12　参与社会活动

现在，越来越多的人通过网络参与各种活动（图 1.1.12）。网络已经成为人们参与社会活动、拓展人际关系的重要工具，近年来甚至出现了力图在虚拟世界中重建现实人际关系的社交类网站。

与此同时，网络也加快了强势文化对弱势文化的侵蚀。众所周知，语言是交流的工具，也是特定文化的载体。目前，英语在网络中占据强势地位，其他语言在网络交流中处于弱势地位，这些语言所承载的文化更容易被忽略，甚至是被排斥。越来越多的处于网络文化弱势的国家开始通过法律、法规等手段，有意识地维护本国的传统文化，抵制外来强势文化的侵蚀。



图 1.1.13　数字鸿沟

数字鸿沟（图 1.1.13）的存在，使得新的不平等正在逐渐形成。这是因为，世界各国的经济条件和技术水平不同，网络基础设施建设能力不同；在同一个国家，人们使用网络的条件和能力也各不相同。国与国之间、人与人之间在信息处理能力上的差距不断增大。在信息社会中，信息资源的不平等往往就意味着财富、权利上的不平等，数字鸿沟一直是困扰人们的社会问题。

微信公众号：电子课本大全

此外，网络引发的身心健康问题也日益受到关注。网络提供了一个便捷的交流平台，很多人通过网络认识了更多的新朋友，但网络交流却难以拉近心灵的距离，很多网民产生了“网络使我更孤独”（图1.1.14）的心理现象。网络给很多人带来了距离感，加重了社会隔离现象。这种情况在低龄网民中更加突出。



图1.1.14　网络孤独

实践活动

了解“非网民”人群

时至今日，还有很多人游离于网络之外。查找相关信息，了解一下“非网民”人群主要包括哪些人，他们不上网的原因以及由此可能给他们带来的影响。

项目实施

归纳总结自己对网络的认识

在了解网络发展历程、应用现状，以及社会影响的基础上，结合自己使用网络的感受和心得，归纳总结自己对网络的认识。

提示：

1. 可以宏观、全方位地介绍对网络的认识，也可以选择一个切入点，就某一具体问题进行阐述，如“互联网+”现状、网络对科学研究的推动等；

2. 观点鲜明，内容严谨；

3. 文字精练，语言生动。

练习提升

1. 计算机网络的发展可划分为哪几个阶段？每个阶段的特点是什么？

2. 简述网络的功能以及它对社会的影响。

3. 查阅关于青少年上网情况的调查报告，然后谈谈你对上网成瘾的看法。

4. 了解在线教育的发展情况，选择感兴趣的数字学习平台尝试进行在线学习，体会在线教育的优势和不足。

微信公众号：电子课本大全

1.2 网络的类型

学习目标 ▶▶▶

- 熟悉网络的类型及其特点。
- 认识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。

体验探索

分析计算机教室网络类型

根据计算机教室网络的特点，某同学绘制了图1.2.1所示的分类图。

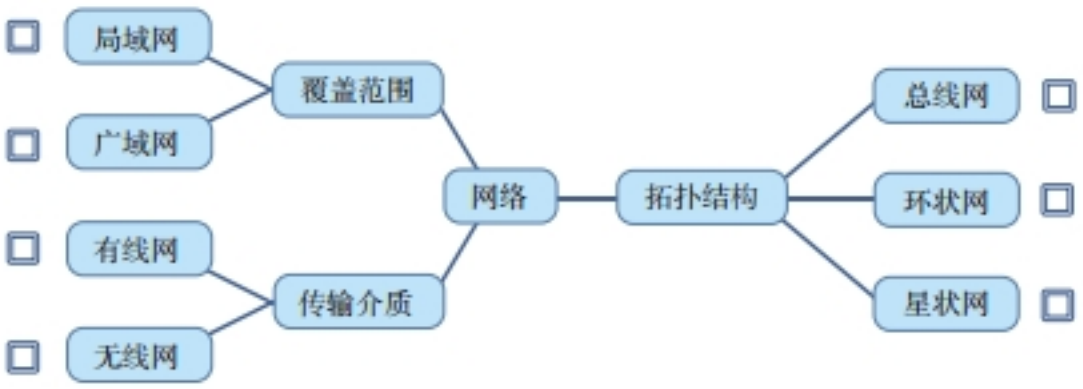


图1.2.1 网络分类图

请思考以下问题。

1. 图中展示了几种分类方式？
2. 每种分类方式具体包括哪些类型？
3. 每种具体的类型都有什么样的特点？

从不同的角度看，网络可以划分成不同的类型，每种类型又对应各自不同的特点和应用场合。下面就来介绍常见的网络类型。

微信公众号：电子课本大全

1.2.1 按覆盖范围分类

按网络覆盖的地理范围大小，可以把网络划分为局域网和广域网。

局域网，是覆盖局部地域的网络（图1.2.2）。比如，计算机教室中的网络。组成局域网的计算机多则数百台，少的可能只有两三台，这些计算机一般可以同时访问网上的各种信息系统。现在，无线局域网已经在生活中普及，智能手机、平板计算机等设备大多具备了接入无线局域网的功能。局域网这个“大家庭”中的“新面孔”已经越来越多了。

广域网，一般用于把不同地区的网络连接起来，覆盖的地理范围比较大（图1.2.3）。例如，一个公司在各地的分支机构所组建的网络可以看作局域网，而把这些分支机构的局域网连接起来，就形成了跨越多个地域的广域网。因特网可以看作覆盖范围最大的广域网。

也有人把网络划分为局域网、城域网和广域网。其中城域网的覆盖范围介于局域网和广域网之间，通常覆盖一座城市或一个地区。



图1.2.2 局域网



图1.2.3 广域网



阅读拓展

个域网简介

近年来，个域网开始受到关注。个域网主要由计算机和外部设备等组成，设备之间采用的无线通信技术，并非无线局域网的相关技术，而是更侧重于短距离传输的蓝牙等通信技术。个域网的覆盖范围比局域网还要小，大多数设备之间的距离不超过1米。

例如，一台计算机的键盘、鼠标、音箱等外部设备，通过蓝牙技术与计算机实现了无线连接，就可以认为组成了个域网（图1.2.4）。



图1.2.4 个域网

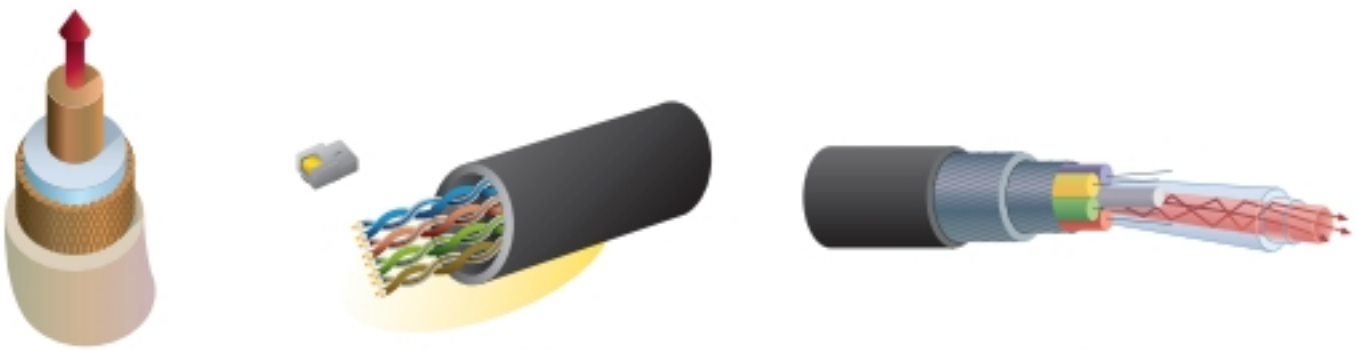
微信公众号：电子课本大全

1.2.2 按传输介质分类

按照传输介质的不同，可以把网络分为有线网和无线网两大类。

有线网指通过有形线缆连接的网络，常用的线缆包括同轴电缆、双绞线和光纤等（图1.2.5）。同轴电缆屏蔽性较好、抗干扰能力较强，但制作工艺复杂。双绞线易受干扰、传输率较低，但价格便宜，安装方便。目前，组建计算机网络时常用双绞线，同轴电缆主要用于有线电视网络。

光纤传输距离长、传输率高、抗干扰性强，是高性能、高安全性网络的最佳选择。但光纤制作费用高、安装难度大，相应的配套设备昂贵，近几年才开始广泛使用。



(a) 同轴电缆　(b) 双绞线　(c) 光纤

图1.2.5　常见线缆示意图



阅读拓展

光纤如何传递二进制数字信号

光纤设备会根据信号中的0或1改变电压的高低，从而控制设备内的激光二极管等设备闪亮。这样，二进制数字信号就变成了可以在光纤内传输的光信号。到达接收端后，接收端设备上的光敏元件会根据光信号的闪灭，产生不同的电压，从而形成二进制数字信号。图1.2.6为光纤通信原理示意图。



图1.2.6　光纤通信原理示意图

微信公众号：电子课本大全

无线网是通过无线的方式，以电磁波为载体来传输数据的（图 1.2.7）。无线网中的计算机不受线缆的长度限制，可以根据需要在一定范围内自由移动。

相对于有线网来说，无线网的稳定性稍差，传输速率较低，一般用作有线网的补充，但无线网使用起来灵活便捷。近年来，无线网的稳定性和传输速率得到了很大改善，越来越多的单位和个人开始使用无线网。



(a) 基于 Wi-Fi　　(b) 基于移动通信网　　(c) 基于蓝牙技术

图 1.2.7　常见的无线网

思考活动

交流使用无线网的感受

说一说你听说过的或接触过的无线网，聊一聊在使用无线网时，你最大的感受是什么。

阅读拓展

可见光无线通信简介

可见光无线通信（light fidelity，Li-Fi）这一概念是在2011年首次提出的，其原理是利用电信号控制发光二极管高速闪烁来传输信息（图 1.2.8）。可见光无法穿透墙壁，因而Li-Fi的穿透性不好，但这同时也意味着，可以比较容易地把信号控制在特定区域内，从而提高安全性。

另外，Li-Fi具有不产生电磁辐射、不受电子干扰等优势。目前，Li-Fi仍处于发展初期，设想的应用场合主要包括矿井、医疗设备工作区、飞机机舱等。

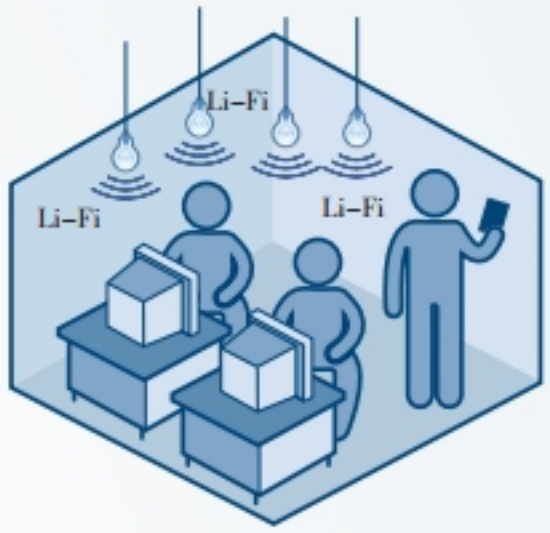


图 1.2.8　可见光通信设想图

微信公众号：电子课本大全

1.2.3 按拓扑结构分类

网络拓扑一般用来表示网络中各种设备的物理布局，特别是计算机的分布情况。常见的网络拓扑有线状、星状、环状、树状、网状等。

线状

在线状结构的网络中，所有的计算机共享一条数据通道（图1.2.9）。网络中的某台计算机出现故障，一般不会影响整个网络的通信，但如果共享的数据通道发生了故障，整个网络就会瘫痪。

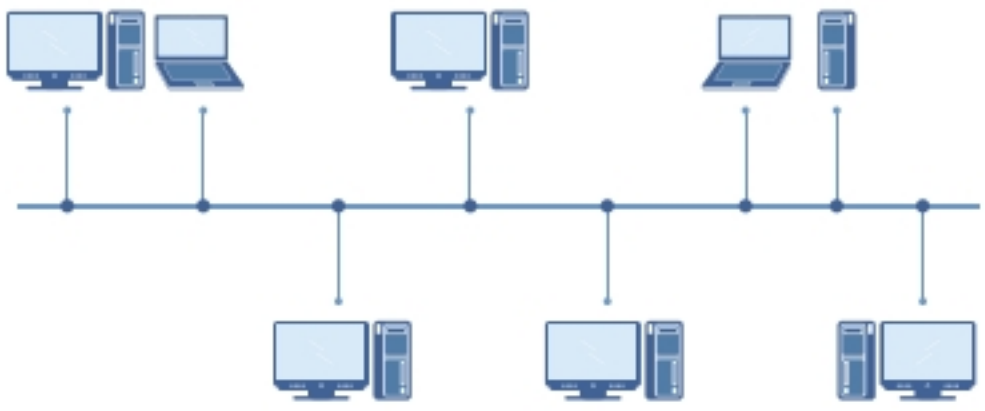


图1.2.9 线状



图1.2.10 环状

环状

在环状结构的网络中，所有的计算机通过传输介质连成一个封闭的环（图1.2.10）。环状结构的网络易于安装，但能够容纳的设备数量有限，难以根据需要随时增加或撤除连入网络的计算机，而且网络中的任何一台计算机出现故障，都可能会影响整个网络的正常运行。

星状

在星状结构的网络中，计算机会分别与同一个中心设备相连（图1.2.11）。这种网络容易增加新的节点，通过中心设备可以方便地监控网络，而且中心以外的计算机出现故障一般不会影响网络的使用。但中心设备必须非常稳定，一旦发生故障整个网络就会瘫痪。

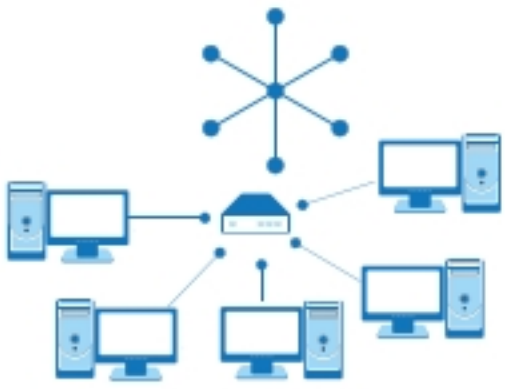


图1.2.11 星状

微信公众号：电子课本大全

树状

树状结构可以看作是星状结构的拓展，设备间呈现出清晰的层次关系（图1.2.12）。



图1.2.12　树状

树状网络的优点是易扩充，而且可以比较容易地把出现故障的区域与整个网络隔离开。这种网络的缺点是结构复杂、对根节点依赖性很大，一旦根节点发生故障，整个网络都无法工作。

网状

网状结构分为全连接网状和不完全连接网状两种形式（图 1.2.13）。在全连接网状中，每一个节点和网中其他节点均有链路连接；在不完全连接网状中，两节点之间不一定有直接链路连接，它们可以依靠其他节点转接。

网状网没有中心设备，局部的故障不会影响整个网络的正常工作，因而可靠性较高。但这种网络关系复杂，局域网很少采用，广域网常常使用不完全连接网状结构。

大型网络的拓扑结构比较复杂，其中包含多种基本的拓扑类型，因此也称为混合型。

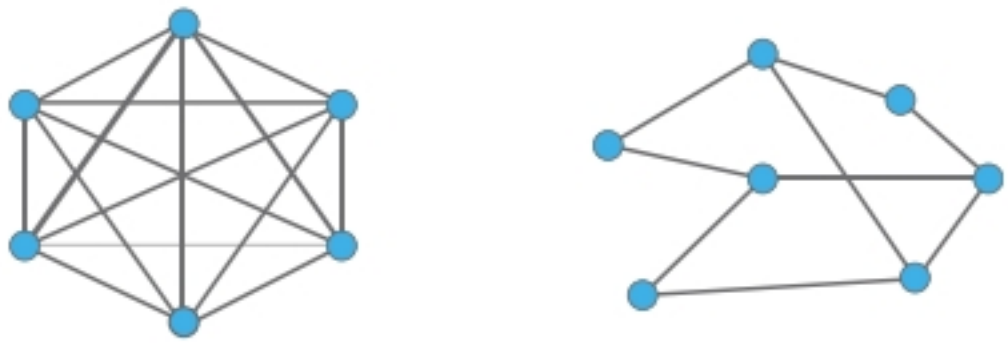

(a) 全连接　　(b) 不完全连接

图1.2.13　网状

阅读拓展

拓扑简介

此处所说的拓扑，源自数学的拓扑学。1736年，有人请数学家欧拉解答“七桥问题”，欧拉用一种独特的方法给出了解答，而这种解答的第一步，就是把现实问题进行简化。欧拉把目的地简化成了点，把不同的桥简化成了线（图1.2.14），这个简化过程，被认为是拓扑学的“先声”。

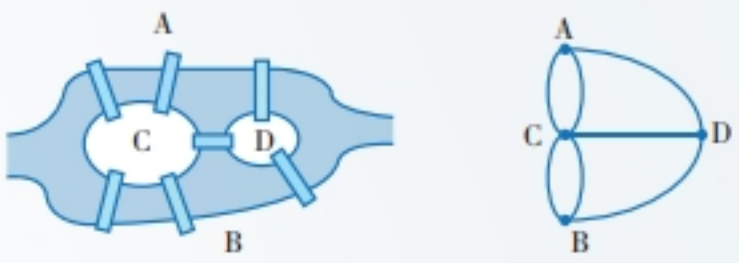


图1.2.14　七桥问题

研究计算机网络时，也可以借用类似的思想，把网络设备简化成一个点，连接线路简化成一条线。这样，网络设备的分布情况、彼此的连接关系等就清晰明了了。

微信公众号：电子课本大全

1.2.4　按传输方式分类

情境：

赵明要告诉王红一个消息，他可以采用哪些方法来告知王红呢？

具体的方法很多，这些方法大体可以归为两类：一是在其他人不知道的情况下，“悄悄”地告诉王红；二是当着大家的面，大声地告诉王红。与此类似，网络中信息的传输方式也可以分为两种：点对点式和广播式。

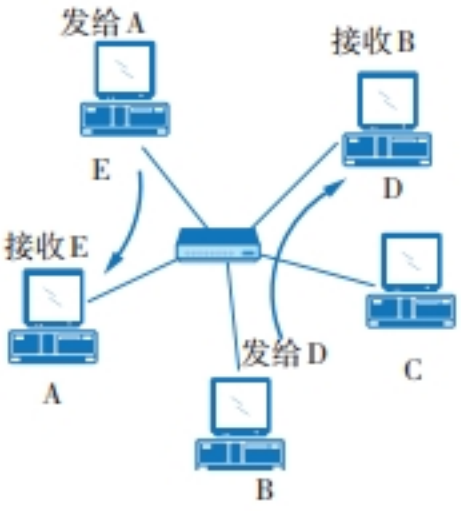


图1.2.15　点对点式

点对点式

在点对点式的网络中，数据一般只在要通信的计算机之间传输。在这个过程中，只有一个发送者和一个接收者，有时也称为单播（图1.2.15）。

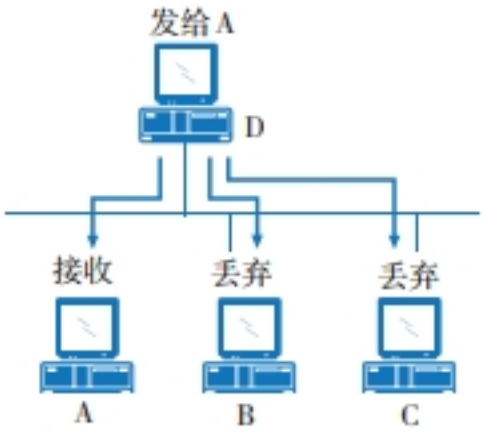


图1.2.16　广播式

广播式

在广播式的网络中，计算机共享一个信道。一台计算机发送信息时，网络中的计算机都能“听”到。计算机“听”到信息后，要根据其中标明的“目的地”进行判断，如果是发给自己的就接收，否则就丢弃（图1.2.16）。

这就跟赵明在班里大声说“王红，老师让我们去学校广播站”一样：其他人听见了不会加以理睬，而王红则会做出回应。

如果同一时间有多台计算机需要通信，那就会发生通信冲突。不难想象，网络中的计算机数量越多，产生通信冲突的概率就越大，网络的传输效率就越低。因此，广播式网络的规模一般不会太大。日常组建的无线局域网属于广播式网络。

阅读拓展

广播式传输的安全问题

广播式传输时，每一台计算机都可以“接听”网络中传输的所有信息，如果进行特殊处理，就可以把“接听”的信息都记录下来，从而窃取隐私或机密。因此，相对而言，广播式网络不如点对点式网络的安全性好。为了解决网络窃听问题，可以在网络通信时采用加密技术。关于加密，将在第3章进行介绍。

微信公众号：电子课本大全

1.2.5 按服务方式分类

按网络中计算机之间的服务方式，可以把网络分成主从式和对等式。

主从式

主从式网络中（图1.2.17），“主”代表服务器，指提供服务的高性能计算机或专用设备；“从”代表客户，指普通计算机、智能手机等设备。在这种模式下，资源集中在服务器中，客户需要从服务器那获取。这种结构称为“客户/服务器”（client/server，C/S）结构。

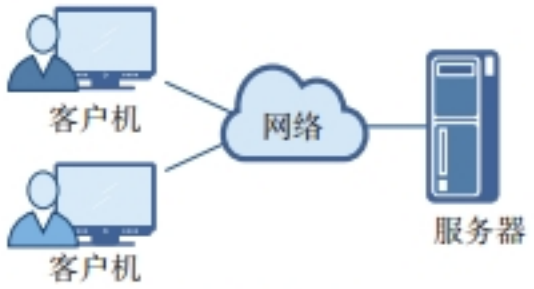


图1.2.17　主从式

要使用不同的网络服务，一般需要安装不同的软件，如即时通信软件、电子邮件客户端软件等。随着技术的发展，越来越多的服务可以通过万维网形式访问，客户机只要安装了浏览器就可以使用它们，而不必安装专门的软件，这样就可以形成“浏览器/服务器”（browser/server，B/S）结构。由此可以看出，B/S结构是C/S结构的特例。

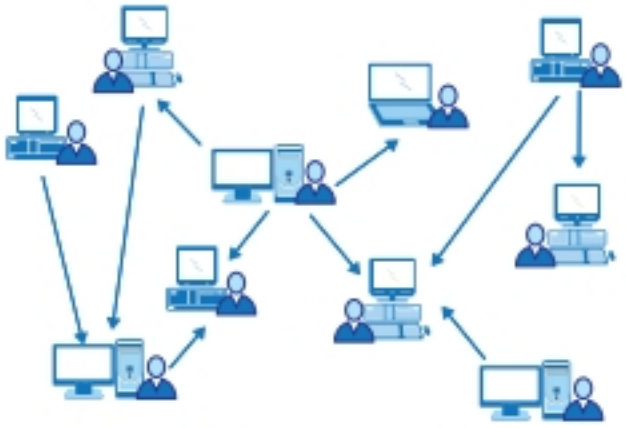


图1.2.18　对等式

对等式

在对等式网络（图1.2.18）中，每台计算机都与其他计算机共享彼此的信息资源或硬件资源，没有类似服务器和客户机的固定分工。这种网络常用于共享音乐和视频，P2P（peer-to-peer，对等网络）下载是其最典型的应用。

阅读拓展

服务方式的转变

服务方式会随使用的网络服务而发生改变，一台计算机可以既属于主从网，又属于对等网。例如，在一台计算机上用Foxmail软件收取电子邮件时，还可以用P2P软件下载资料，这样它就同时身处两种网络中了。实际上，很多网络服务是混合式的。例如，启动即时通信软件时，一般需要先登录到服务器上验证身份，这时，计算机和服务器之间构成了主从关系，属于主从网；登录后再收发消息就可能不通过服务器了，这样计算机间可以形成对等网。

微信公众号：电子课本大全

1.2.6　影响网络传输质量的主要物理因素

现实世界中，网络信号传输是受很多因素影响的，如果出现了干扰信号，网络就会不稳定；如果信号越来越弱，网络同样也无法使用。下面介绍影响网络传输质量的主要物理因素：噪声和衰减。

噪声

网络传输中的噪声，不是指嘈杂的声音，而是指引起信号质量下降或失真的影响因素。大家在物理课上都学过电磁感应：导体放置在变化的磁场中，导体内部就会产生电流（图1.2.19）。传输电信号的网线是导体，当外界有磁铁或散发电磁场的设备时，内部就可能因电磁效应产生电流，从而形成噪声。

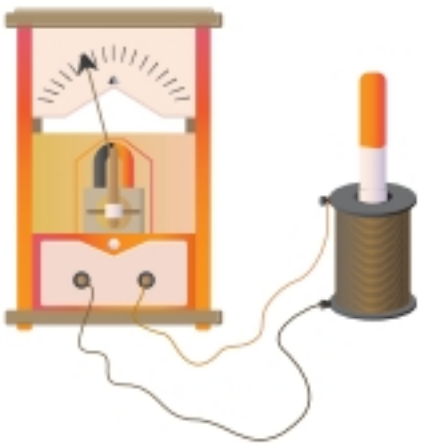


图1.2.19　电磁感应

噪声主要有两种来源：外界电磁干扰引发的噪声和内部串扰引发的噪声。如何对抗噪声呢？可以通过移除噪声源、给网线加屏蔽层等办法来消减噪声。

光纤传输的是光信号，它不是导体，不受电磁感应的影响，所以抗噪能力非常好；同轴电缆的屏蔽层比较厚实，它的抗噪能力也不错。

组建局域网时普遍使用双绞线，其单条线路的抗噪能力较差，但双绞线有自身的抗噪办法。双绞线里面共有八根线，两两缠绕形成4组。一根导线的某一段因电磁感应产生顺时针电流时，相邻的区域就会产生逆时针电流，从而抵消噪声（图1.2.20）。

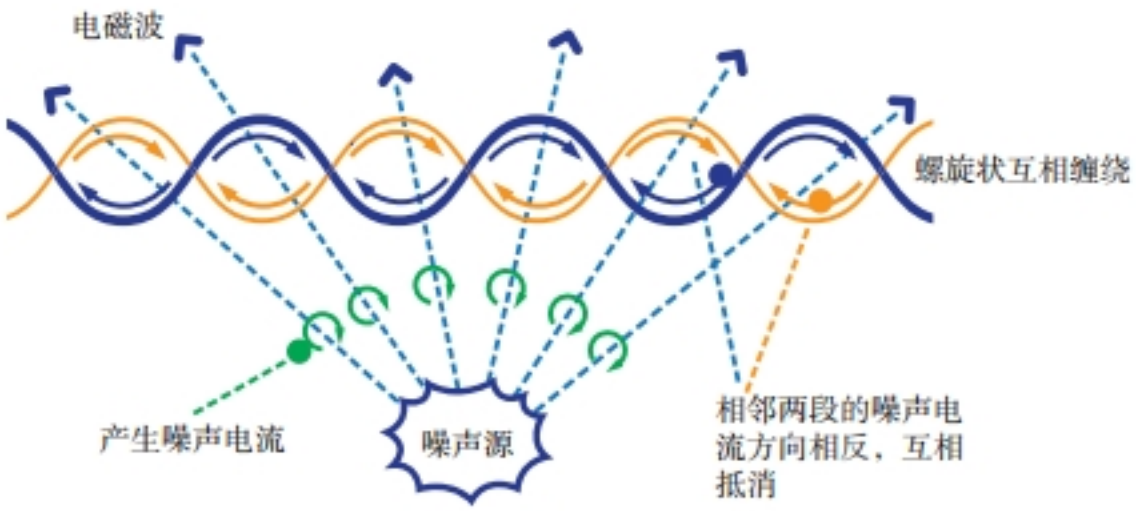


图1.2.20　双绞线消减外部噪声影响示意图

微信公众号：电子课本大全

距离很近的信号线之间也会出现电磁感应，从而造成噪声干扰，这是来自通信线路内部的噪声（图1.2.21）。

双绞线内部缠绕形成的4组线，每组的缠绕节距是不一样的。这样一来，串扰就会在相邻的区域形成相反的电流，从而从整体上消减串扰形成的噪声（图1.2.22）。

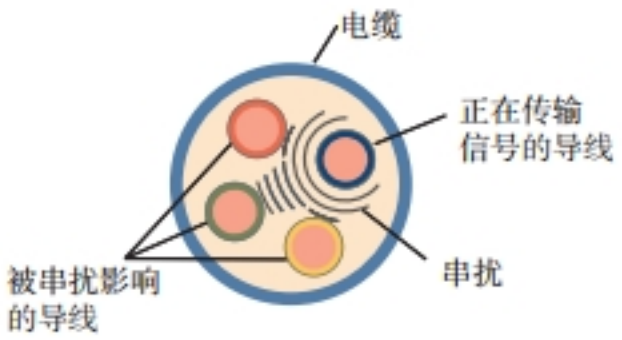


图1.2.21　串扰示意图

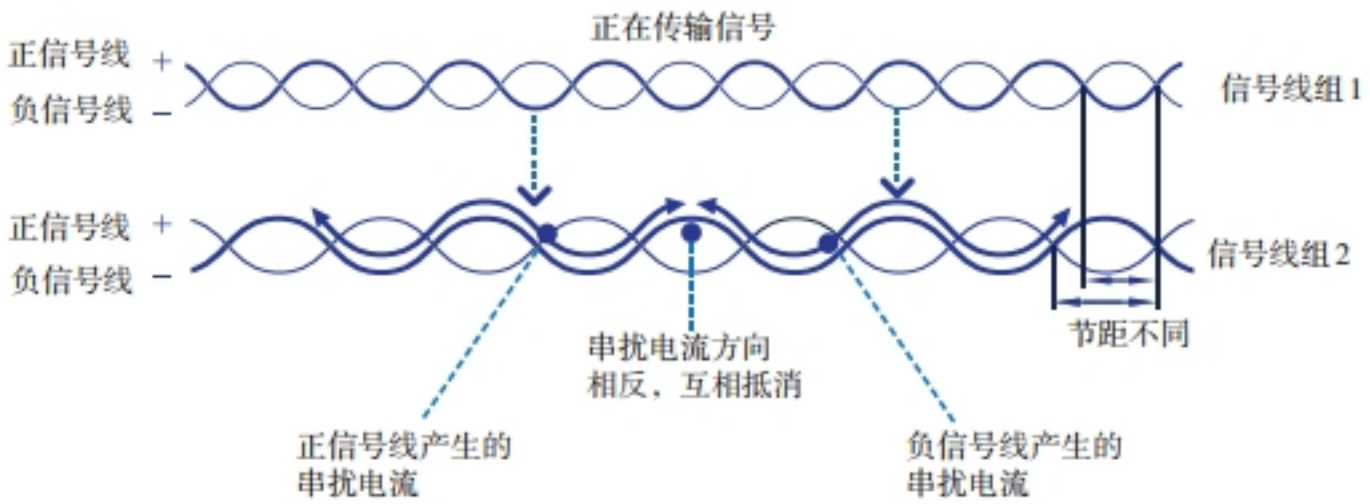


图1.2.22　双绞线消减串扰影响示意图

衰减

信号在传输介质中传播时，将会有一部分能量转换成热能或者被传输介质吸收，从而造成信号强度不断减弱，这种现象称为衰减（图1.2.23）。衰减也是影响网络传输质量的重要物理因素。

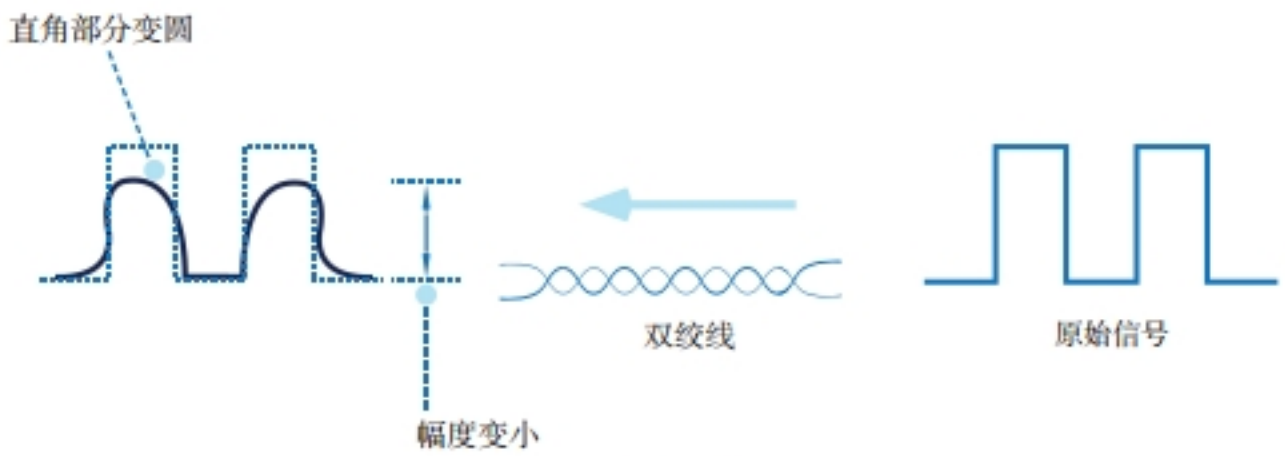


图1.2.23　信号衰减示意图

衰减现象在无线网中更为常见，无线信号每一次穿越墙壁或绕行障碍物时都会不可避免地产生大量衰减。衰减到一定的程度后，就无法使用了，这时人们就会说“信号不好”或者“没有信号”。

微信公众号：电子课本大全

通过缩短传输距离、提高网线通信质量、减少障碍物等方式，可以在一定程度上减轻衰减带来的影响。必要时，可以增加专门用来增强信号的设备——中继器，来对抗噪声或衰减带来的影响（图1.2.24）。

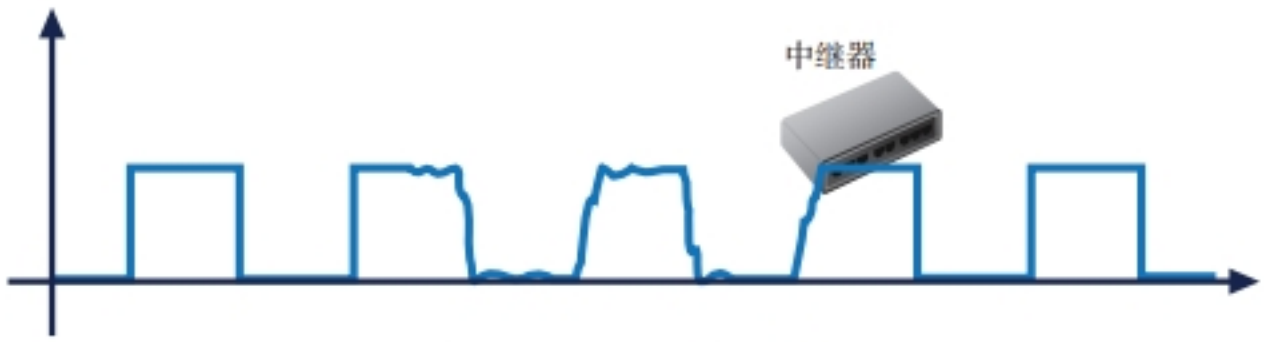


图1.2.24　用中继器增强信号

项目实施

填写项目报告

完成下面的项目报告，检查自己这个阶段的学习情况。

报告人：_____　　时间：_____

主题：网络的基础知识

1. 总结计算机网络的分类方法。

_____

_____

2. 认识常见的网络传输介质，总结它们的特性。

· 介质：双绞线，特性：_____

· 介质：光纤，特性：_____

· 介质：_____，特性：_____

· 介质：_____，特性：_____

3. 总结网络拓扑的特点。

· 类型：线状，特点：_____

· 类型：星状，特点：_____

· 类型：环状，特点：_____

· 类型：_____，特点：_____

· 类型：_____，特点：_____

4. 描述影响网络传输质量的主要物理因素。

_____

_____

微信公众号：电子课本大全

项目实施

制作主题作品

在了解互联网的发展历史、应用现状和重要意义，以及网络类型、网络拓扑等知识的基础上，制作主题为“网络，我来说”的电子作品。

制作要求：

1. 可以宏观地、全方位地介绍对网络的认识，也可以选择一个切入点，就某一具体的问题进行阐述，如探讨影响网络传输质量的因素；

2. 观点鲜明，内容严谨，语言精练。

阅读拓展

差错的检测

受各种因素的影响，在网络传输过程中，传输的数据出现差错，也就是接收端收到的数据和发送端发送的数据不一致，是不可避免的。为了及时发现差错，人们采取了很多技术手段。

奇偶校验码就是一种简单的检测技术。简单地说，奇偶校验码就是在二进制数据块的后面加上一位校验位，使得总数据块中的1始终为奇数或偶数。前者称为奇校验，后者称为偶校验。

元数据：　101010100010100

奇校验：　1010101000101001　　偶校验：　1010101000101000

接收端按照奇数或者偶数规则进行检查，如果与规则不符，就说明传输出现了差错。这种方法容易实现，对设备要求不高，但漏检率比较高。

循环冗余码在差错检测中的应用更为普遍，它的工作原理相对复杂，感兴趣的同学可以自行查阅相关资料。

练习提升

1. 与双绞线、同轴电缆相比，光纤具有什么优势？是否存在不足？

2. 某人说他使用的网络是“千兆光纤星状网”，从这个描述中，你能获知这个网络的哪些特点？

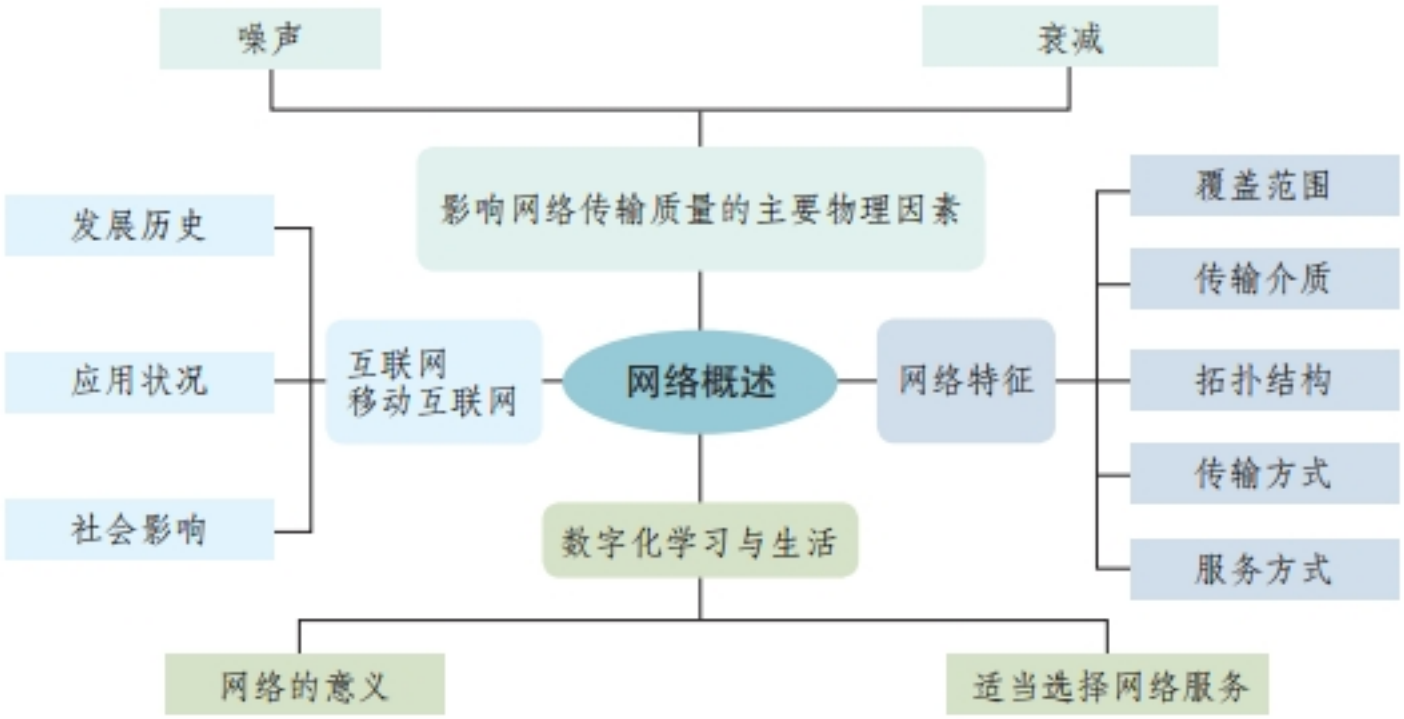
3. 调查校园网或身边的其他网络，完成以下任务。

- 绘制网络拓扑图，标出主要设备的名称。
- 说出这些网络使用的传输介质。
- 说出这些网络所拥有的特征。

微信公众号：电子课本大全

总结评价

1. 下图展示了本章的核心概念与关键能力，请同学们对照图中的内容进行总结。



2. 根据自己的掌握情况填写下表。

学习内容	掌握程度		
计算机网络的发展历史	□ 不了解	□ 了解	□ 理解
网络的演变过程	□ 不了解	□ 了解	□ 理解
网络的类型	□ 不了解	□ 了解	□ 理解
常见的网络拓扑	□ 不了解	□ 了解	□ 理解
常见的网络传输介质	□ 不了解	□ 了解	□ 理解
影响网络传输质量的主要物理因素	□ 不了解	□ 了解	□ 理解
网络对现代社会的重要意义	□ 不了解	□ 了解	□ 理解

3. 回答以下问题，完成活动反思。

（1）关于网络，你觉得它对我们的现代生活产生了什么推动作用？又给人类社会带来了哪些问题？

（2）在本章的学习过程中，你或同学遇到了什么问题？是如何解决的？你觉得自己有什么样的收获？尝试列举几点与同学分享。

微信公众号：电子课本大全

第 2 章

网络协议、设备与操作系统

网络协议是网络通信的基础，联网的各种设备必须遵照一定的协议，才能彼此传输数据。而要实现网络协议规定的各种功能，又离不开各种软硬件的支持。在本章的学习过程中，我们将进一步认识目前使用最广泛的 TCP/IP 协议的主要功能和作用，理解常见网络设备的工作原理，还将了解网络操作系统，学会使用基本的网络命令查询网络设备的工作状态。



微信公众号：电子课本大全

02 主题学习项目：安全组建局域网

项目目标

现在很多人家里都有计算机、智能手机、平板计算机等信息设备，而且通常需要把这些设备同时连入互联网。本章将通过组建一个局域网，并让网络中的设备共享上网的项目活动，介绍组网的相关软硬件，以及需要注意的安全事项。

1. 熟悉需要连入同一局域网的信息设备。
2. 能够比较、分析常用网络设备的优势和不足。
3. 能够提升局域网的安全性。

项目准备

为了完成项目，需要做以下准备。

- 本章活动涉及的网络基本命令、组网测试等诸多操作实践，都需要小组成员之间互相配合才能完成。小组活动时，组员之间一定要彼此协调好。
- 准备一些关于TCP/IP协议的资料，以备活动时使用。
- 准备组网活动所需的路由器、网线、智能手机等硬件设备。
- 本章活动需要使用路由器、交换机、智能手机等硬件设备，使用时应严格遵守使用规范，以免造成自身危险或设备损坏。

项目过程

为了保证顺利完成本章的学习活动，在不同学习阶段，小组长要注意检查组员项目学习的进度，并做好协调互助工作。

1 实践感受

完成关于数据包分析、网络通信等实验操作，感受网络协议的作用。 P34

2 归纳总结

根据使用心得，自行整理对TCP/IP协议的认识，熟悉它的功能和作用。 P45

3 组建网络

组建局域网，及时发现、排除联网故障，了解网络操作系统的功能。 P52

4 活动思考

回顾总结所使用的各种网络设备，反思组网过程中的安全问题。 P55

项目总结

学完本章后，及时分析活动时遇到的问题，归纳解决问题的方法。通过项目学习活动，熟悉TCP/IP协议（传输控制协议/互联网协议）的主要功能和作用，理解网卡、交换机、路由器等基本网络设备的作用和工作原理，了解网络操作系统的功能，能使用基本网络命令查询联网状态、配置情况，发现故障。

微信公众号：电子课本大全

2.1 网络通信基础

学习目标 ▶▶▶

- 理解网络中使用的数据交换技术。
- 熟悉TCP/IP协议的主要功能和作用。
- 理解IP地址与域名的关系。

体验探索

回顾所学知识，思考浏览网页的过程



图2.1.1 浏览网页过程示意图

1. 图2.1.1中，计算机之间通过什么技术互相交换数据？

☐ 电路交换 ☐ 报文交换 ☐ 分组交换

2. 浏览网页时，主要使用了哪个网络协议？主要涉及哪些软硬件？

微信公众号：电子课本大全

2.1.1 数据交换技术

网络中的计算机，要不时地发送请求或接收反馈，也就是说，计算机之间必然要交换数据，这就要用到数据交换技术。数据交换技术可分为三类：电路交换、报文交换和分组交换。

电路交换

采用电路交换技术时，需要在通信双方之间建立一条通道，所有的数据都通过这条通道实时传输（图2.1.2）。电路交换的实时性非常好，适合需要持续交互的应用场景。比如，传统的电话网就采用了这种交换技术。

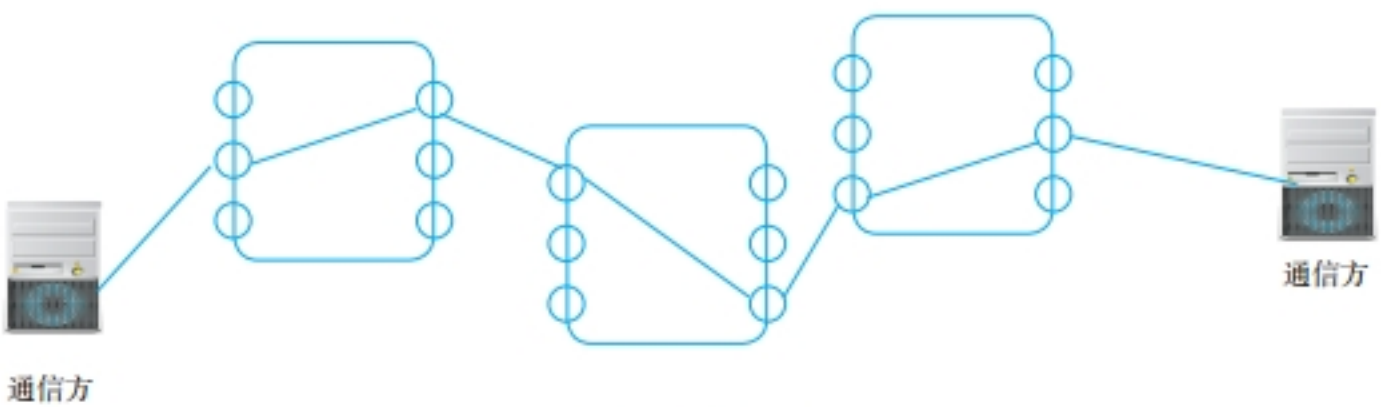


图2.1.2 电路交换

在电路交换的通信过程中，无论通信双方是否在传输数据，建立的通信通道都会被双方一直占用着，因而使用率比较低。

报文交换

报文交换技术不要求在通信双方之间建立物理通道，发送方把发送的数据作为整体发给网络中的交换设备，这些交换设备依次传递，最终把数据发送到目的地。收发电报时，主要采用这种交换技术（图2.1.3）。

采用报文交换技术时，每次转发数据只占用网络中的一小段线路，空闲的线路段可供其他通信任务使用。这样就可以提高整个网络的使用效率。不过由于需要不断地存储和转发，报文交换的延时比较严重，不适合实时性要求高的应用场景。

微信公众号：电子课本大全



图2.1.3　报文交换

每个报文通常由报头、正文和报尾三部分组成，报头中含有发送端地址、接收端地址等信息；正文就是具体的发送内容；报尾则包含一系列用于验证和控制的数据。

分组交换

分组交换与报文交换相似，但分组交换时每次传送的数据长度是有限的，原来的信息会按照限定大小分成许多个“小包”，这些“小包”可以沿同一线路按顺序发送和接收，也可以沿不同的线路随机发送和接收。按顺序收发属于虚电路交换，随机收发属于数据报交换。

采用虚电路交换时，需要在发送方和接收方之间建立一条逻辑通道，通道上的每个节点都要服从安排，按顺序传输数据“小包”，就好像有一条专用通道一样。虚电路在数据交换结束后会自动释放（图2.1.4）。

与电路交换不同，虚电路交换各节点不是某虚电路独占的，它们仍可用于传输其他数据。

采用数据报交换时，不同的数据“小包”可以通过不同的路径到达目的地，而且先发的“小包”不一定先到，后发的“小包”不一定后到。“小包”中含有关于次序的信息，接收“小包”的设备根据次序，把收到的“小包”重新组装起来，恢复成原来的信息（图2.1.5）。

微信公众号：电子课本大全

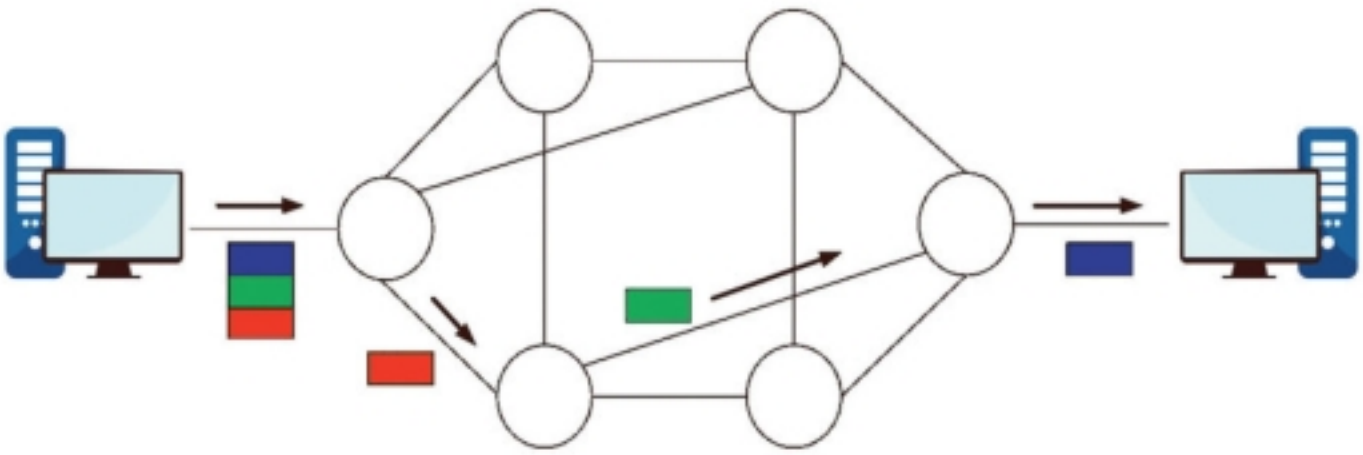


图2.1.4　虚电路交换

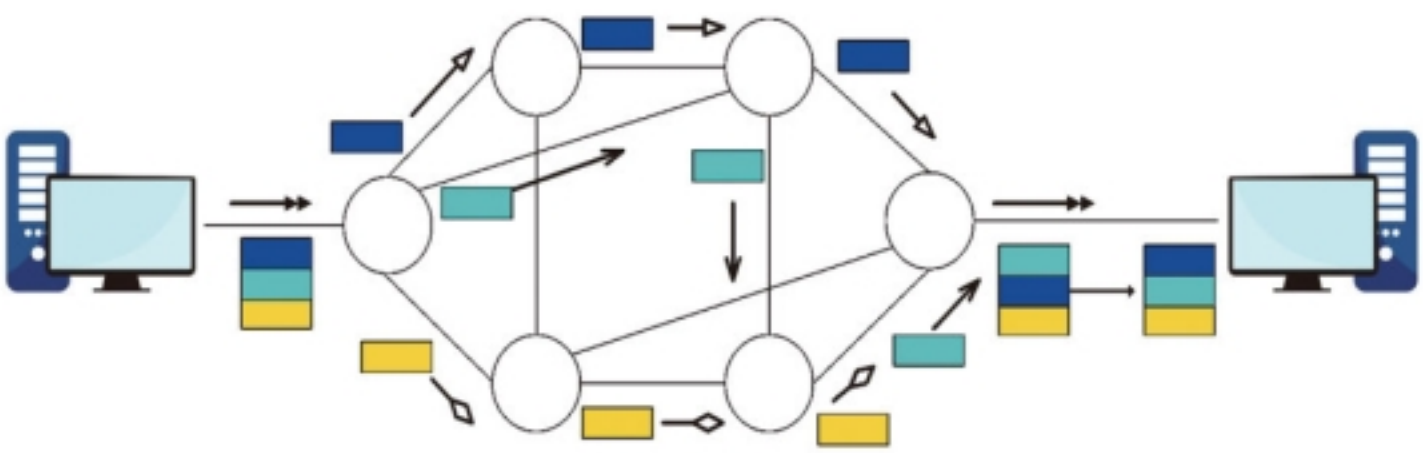


图2.1.5　数据报交换

以上三种数据交换技术各有特点。对于实时性要求高的交互式传输，电路交换最合适，不宜采用报文交换；对于实时性要求不高的传输任务，报文交换最经济合算；分组交换技术则兼具前两者的某些优点。

思考活动

分析数据交换方式

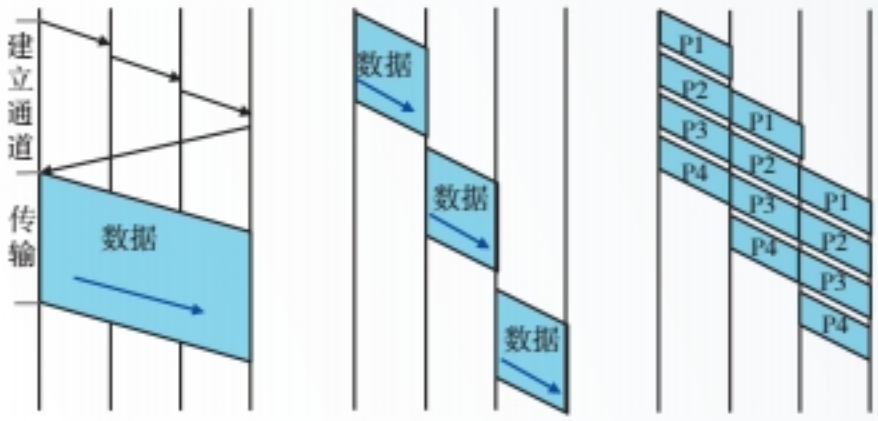


图2.1.6　数据交换方式示意图

有一位同学画了图2.1.6展示电路交换、报文交换和分组交换的特点，你觉得这些图分别代表了哪种数据交换方式？

微信公众号：电子课本大全

2.1.2 TCP/IP协议

TCP/IP协议包含两个基础性的通信协议：TCP协议（transmission control protocol，传输控制协议）和IP协议（internet protocol，互联网协议）。其中，IP协议保证数据传输，TCP协议保证数据传输质量。

因特网的前身——阿帕网在1983年改用第4版TCP/IP协议，当阿帕网“进化”成因特网后，TCP/IP协议也随之击败了其他的竞争对手，成为网络的通信基石。后来，人们又根据需要，不断地在其基础上研制各种网络协议。

发展到现在，TCP/IP协议已经演变成包含上百个网络协议的协议簇。为了便于分析和理解，通常把TCP/IP协议划分为4层（表2.1.1）。

表2.1.1 TCP/IP协议的层次结构

名称	描述	主要协议
应用层	规定使用各种服务要遵循的规范	HTTP、DNS
传输层	负责传输数据	TCP、UDP
网络互联层	负责连接网络和传输数据	IP
网络接口层	规定连接网络设备的接口	其他通信网络接口，如以太网等

项目实施

查看计算机所用的网络协议

1. 进行几个网络操作，如访问几个网站，使用即时通信软件等。
2. 用netstat命令，查看网络连接情况（图2.1.7）。

```
C:\>netstat

活动连接

  协议   本地地址          外部地址        状态
  TCP    10.50.16.99:53684      1.192.193.47:http      ESTABLISHED
  TCP    10.50.16.99:54104      180.163.235.136:https  ESTABLISHED
  TCP    10.50.16.99:54119      101.199.97.91:http     ESTABLISHED
  TCP    10.50.16.99:54140      10.50.16.1:http        ESTABLISHED
  TCP    10.50.16.99:54310      101.226.211.46:8080    ESTABLISHED
  TCP    10.50.16.99:54916      hk2sch130021518:https  ESTABLISHED
  TCP    10.50.16.99:63145      182.254.12.16:https    CLOSE_WAIT
  TCP    10.50.16.99:63990      pepapp:1352            ESTABLISHED
```

图2.1.7 某计算机网络连接情况

微信公众号：电子课本大全

依照TCP/IP协议发送数据时，数据将从上到下，依次在不同层流动。每一层接到上一层传来的数据后，都会加上含有本层控制信息的头部，形成TCP包、IP包等，再交给下一层。TCP包、IP包等数据包主要由头部和数据两部分组成。

如果应用层传来的数据很长，可能还要在传输层先拆分成若干个数据包，再添加头部。

下面以传送网页为例进行介绍（图2.1.8）。

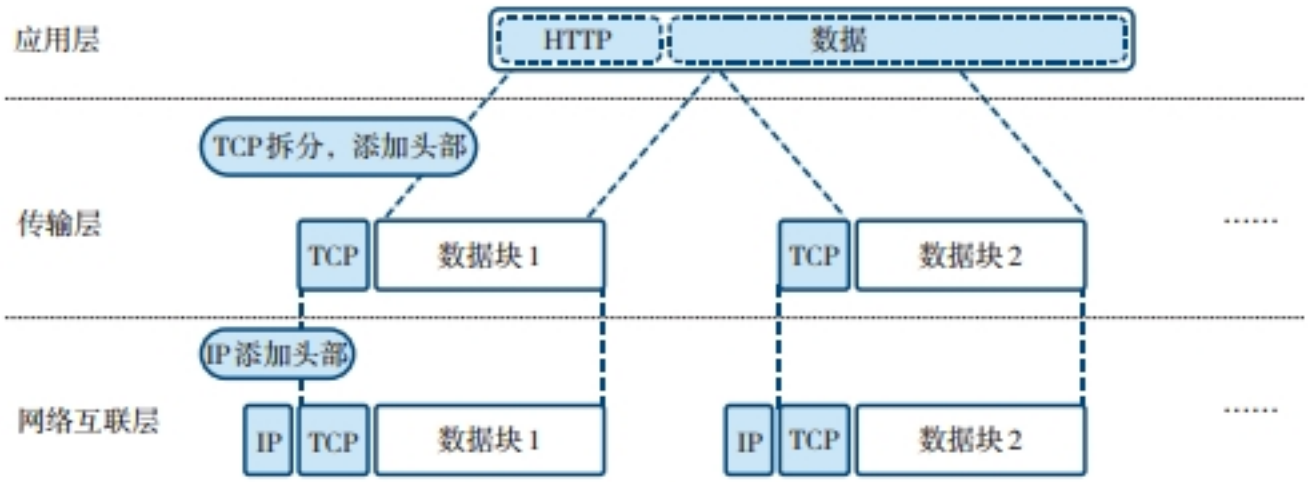


图2.1.8　数据分包示意图

项目实施

分析使用HTTP协议浏览网页时的数据包

1. 关闭正在运行的浏览器、即时通信、电子邮件等网络应用软件。

2. 启动Wireshark软件，单击 按钮，监测网络通信情况（图2.1.9）。

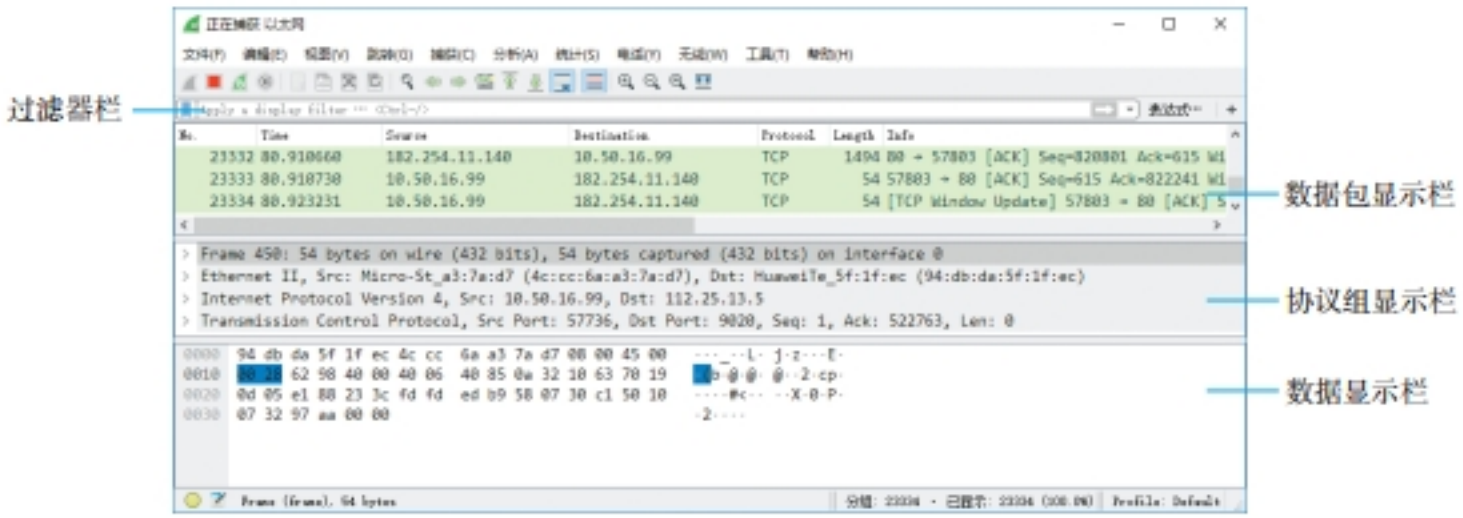


图2.1.9　Wireshark界面

3. 在过滤器栏中输入http，观察是否有软件在使用HTTP协议进行通信。如果有，把它们都关闭。然后单击 按钮，停止监测。

微信公众号：电子课本大全

4. 重新启动监测，接着用浏览器访问一个网站，然后停止监测。

5. 在数据包显示栏中选择一个数据包，然后通过协议组显示栏，观察它的内部结构。

6. 查看IP头部，找出目的计算机的IP地址（图2.1.10）。

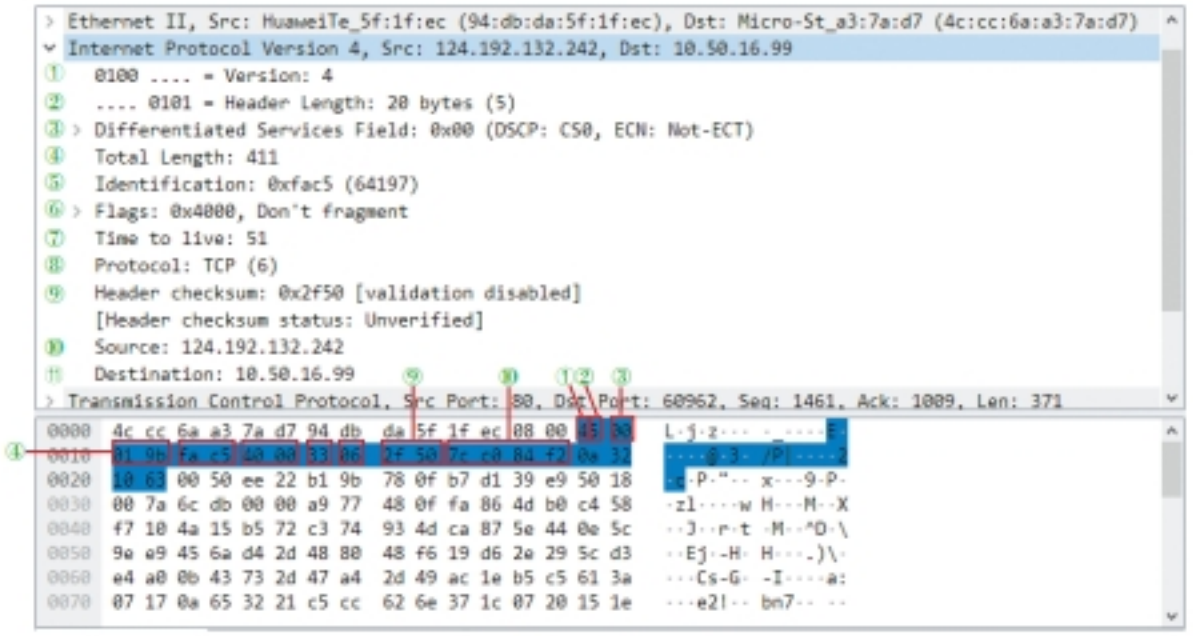


图2.1.10　查看IP头部

7. 查看TCP头部的组成（图2.1.11）。

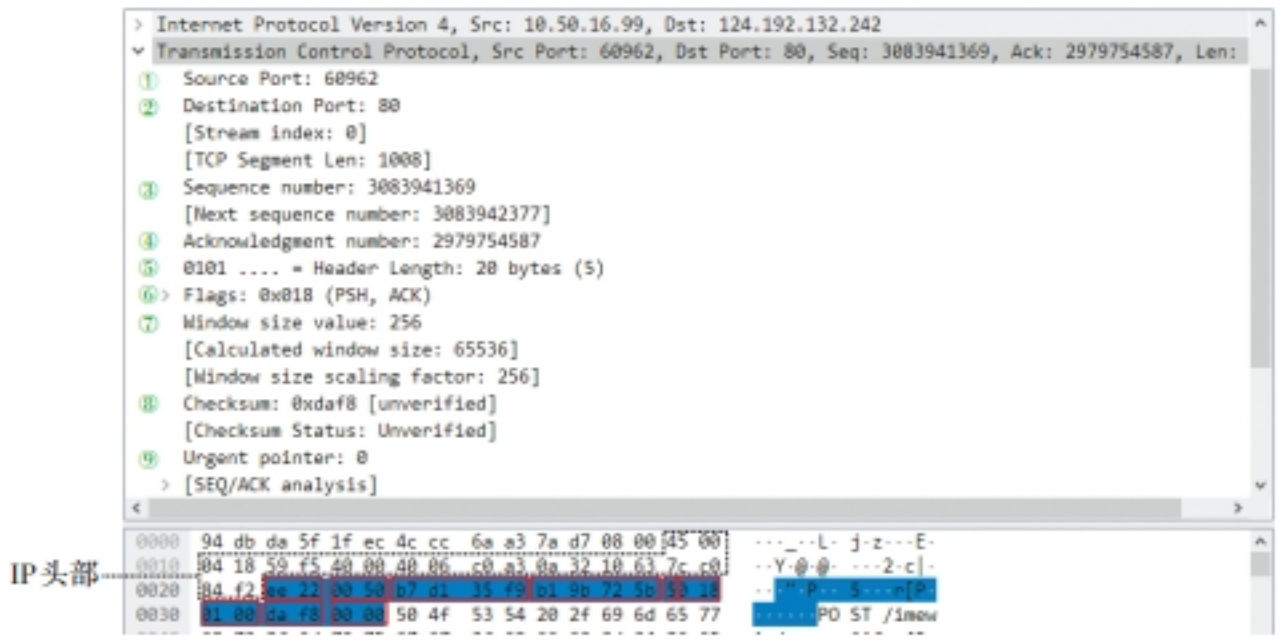


图2.1.11　查看TCP头部

8. 观察其他的头部，想一想数据是如何一层层封装起来的。

传送网页时，在应用层，会增加关于HTTP协议的头部；在传输层，会进行数据拆分，并增加关于TCP协议的头部；在网络互联层，会增加关于IP协议的头部……就这样一层层向下，不断增加相关协议的控制信息。

接收方收到信息后，自下而上，在不同层顺次解读数据包，最终获得传送的信息。

微信公众号：电子课本大全

2.1.3 IP地址

情境1：

2002年7月，江西省公安机关查获了一起利用网络赌博的案件。经侦查发现，用于赌博的计算机服务器的IP地址位于某市。根据这一线索，专案组迅速出击，抓获了主要的犯罪嫌疑人。这是我国破获的首例利用网络聚众赌博案。

那么，办案组为什么能根据IP地址查出计算机的位置呢？

互联网连接着难以计数的计算机，为了区分它们，人们给计算机设置了数字形式的标识，即IP地址。从表面上看，IP地址由用“.”隔开的4个十进制数来表示，这种表示方法被称为“点分十进制”法。但实际上IP地址是1个32位长的二进制数，比如：

219.239.238.40　11011011111011111111011100101000

这种IP地址源自第4版的TCP/IP协议，因此也被称为IPv4地址。

显然，采用“点分十进制”法表示的IP地址更容易记忆。需要注意的是，采用这种表示法，各个位置上的十进制数必须是自然数，而且最大值不能超过255。

IP地址的组成

电话网由分散在各地的电话网组成，各地的电话网都有相应的区号，区号和号码结合起来就可以完整表示国内的一个电话号码。

例如，010–58758200中的010表示北京市的电话网，58758200表示其中的某个电话号码。类似的，互联网是由各种网络连接而成的庞大网络，这些网络也要有自己的标识，IP地址中就含有这样的标识。实际上，IP地址一般由网络号和主机号两部分组成（图2.1.12）。

网络号	219 . 239 . 238 . 0
主机号	40
IP地址	219 . 239 . 238 . 40

图2.1.12　IP地址组成示意图

微信公众号：电子课本大全

网络通信时，计算机一般会先根据IP地址中包含的网络号找到相应的网络，再根据主机号，找出特定的计算机。如果知道了一个网络的网络号，那么就可以根据它查询计算机所处的网络，进而查出计算机所处的位置了。

实践活动

查询IP地址对应的地理位置

1. 执行 netstat 命令，查看本机连接过的IP地址。
2. 访问IP地址查询网站，查询某个IP地址对应的机构等信息（图2.1.13）。

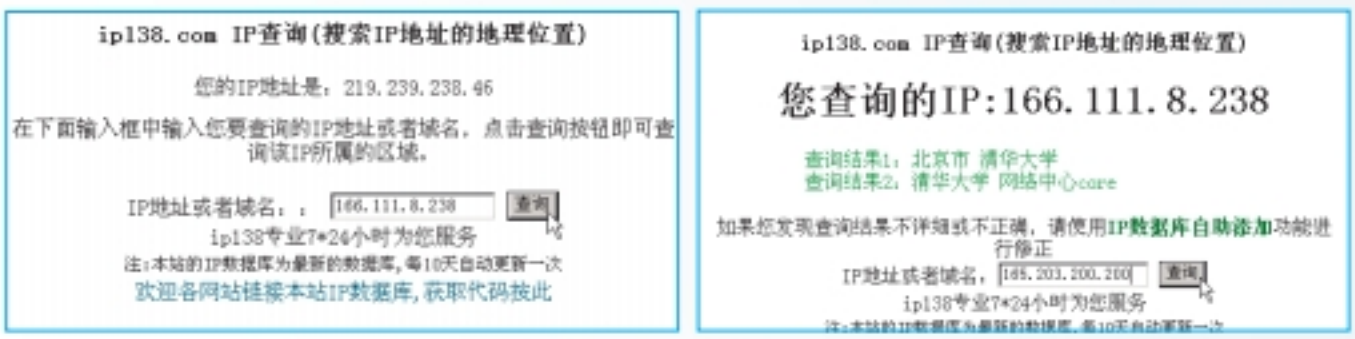


图2.1.13　IP地址的信息

IP地址的类型

常用的IP地址包括3类：A类、B类和C类。不同类的IP地址，网络号和主机号占用的位数不同（图2.1.14）。

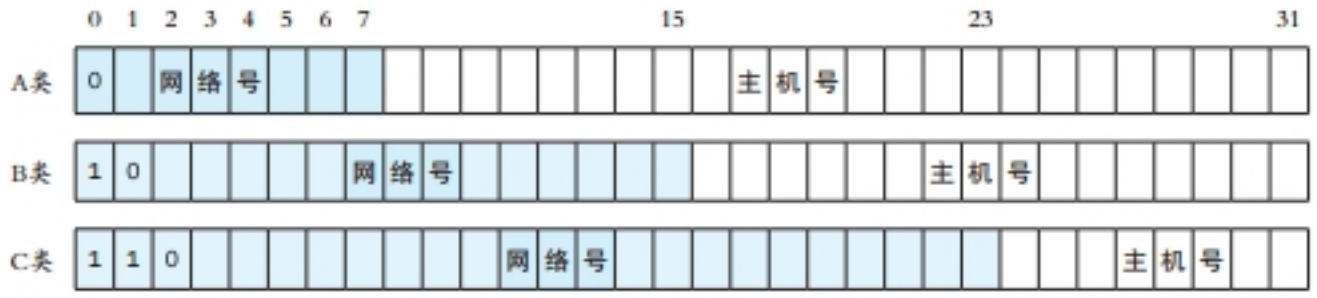


图2.1.14　常用IP地址分类

一般把使用A类地址的网络叫作A类网，使用B类地址的网络叫作B类网，依此类推。A类IP地址中的主机号用24位二进制数表示，B类IP地址中的主机号用16位二进制数表示，C类IP地址中的主机号用8位二进制数表示。

依照用途，IP地址还可以分为公用IP地址和私有IP地址。公用IP地址可以在互联网中使用，由专门的机构负责统一分配；私有地址只能用于单位、家庭组建的内部网，可以由组网人员自行分配。在常用的三类IP地址中，各保留了一些区域作为私有地址（表2.1.2）。

微信公众号：电子课本大全

表2.1.2　私有IP地址

类别	地址范围
A	10.0.0.0－ 10.255.255.255
B	172.16.0.0－172.31.255.255
C	192.168.0.0－ 192.168.255.255

此外，用“点分十进制”法表示时，第一个数大于223的IP地址和网络号为127的A类IP地址有特殊用途，一般不用于标识网络中的计算机。



思考活动

辨别公用IP地址

以下哪几个不可能是互联网中的IP地址。

☐ 121.121.121.3　☐ 266.216.5.225　☐ 127.127.23.1

☐ 165.25.23.200　☐ 252.252.252.3　☐ −3.134.60.127

子网掩码

制定IP地址规范时，制定者把它划分成A、B、C三类来应对不同规模的网络，但在实际应用中发现，这种分法难以充分利用地址资源。比如，一个B类网能容纳6万多台计算机，如果分配给一个公司，利用率可能还不到十分之一。为此，可以根据实际需要再次对网络进行划分，这就要用到子网掩码。

例如，在表2.1.3中，通过设置子网掩码，原来的主机号被划分为子网网络号和子网主机号两部分，其中的子网网络号可以是“00、01、10、11”中的任何一个，即利用这个子网掩码可以获得4个子网。

表2.1.3　子网掩码与子网号

项目	网 络 号			主 机 号	
				部分1	部分2
IP地址	11011011	11101111	11101110	10	101000
子网掩码	11111111	11111111	11111111	11	000000
“与”运算	11011011	11101111	11101110	10（子网网络号）	000000

微信公众号：电子课本大全

如果不需要划分子网，A类网的子网掩码是255.0.0.0，B类网的子网掩码是255.255.0.0，C类网的子网掩码是255.255.255.0。

IP地址的发展

常见32位长的IP地址叫作IPv4地址，即第4版IP协议规定的地址。这种地址理论上最多有2^{32}个。随着网络的飞速发展，IPv4的地址资源已经枯竭。为了应对这种状态，研究者在20世纪90年代中期提出了第6版IP协议，即IPv6。IPv6的地址长度有128位，从理论上讲最多可以提供约3.4×10^{38}个IPv6地址。假设全世界一微秒（一秒的百万分之一）要消耗100万个地址，那么需要10^{19}年才能用完所有的地址。

如果用“点分十进制”法记录IPv6，需要16个数：

```
219.239.238.42.0.0.0.0.0.0.17.128.0.10.255.255
```

可见，用“点分十进制”法已经不能方便地表示IPv6地址了。为了使地址更简洁，有人提议采用“16位二进制数为一组，将其转换为十六进制数，再用冒号隔开”的方法表示。例如，上面的地址可以记为：

```
DBEF:EE2A:0000:0000:0000:1180:000A:FFFF
```

事实上还可以进一步简化：每一组去掉头部的0，连续的0用“::”表示，以上地址可简化为：

```
DBEF:EE2A::1180:A:FFFF
```

注意，IPv6地址简化后，地址中只能有一个“::”。



实践活动

查看所用计算机的IP地址

执行 ipconfig 命令，查看IP地址等网络配置信息（图2.1.15），并填空。所用计算机的IPv6地址是_____，IPv4地址是_____，子网掩码是_____。

提示：图2.1.15中IPv6地址最后的“%9”用于标识网络接口。

```
连接特定的 DNS 后缀 . . . . . :
本地链接 IPv6 地址. . . . . : fe80::b0f3:543a:d34:2d8c%9
IPv4 地址 . . . . . : 10.50.16.99
子网掩码 . . . . . : 255.255.255.0
默认网关. . . . . : 10.50.16.1
```

图2.1.15　地址相关信息

微信公众号：电子课本大全

2.1.4 域名

数字形式的IP地址，难以直观地记忆。因而，人们又采用了字符型的标识——域名。

例如，www.moe.gov.cn就是一个域名，其中cn表示中国，gov表示政府机构，moe表示中华人民共和国教育部，www是服务器的名称，合起来可以理解为“中国政府机构之一的中华人民共和国教育部的一台名为www的服务器”（图2.1.16）。



图2.1.16 域名结构示意图

域名可以用来表示一个地域、一个单位或一个机构的网络系统，也可以用来表示网络中的某台计算机。例如，tsinghua.edu.cn是清华大学网络系统的名称，这个网络系统中可能包含多台计算机；www.tsinghua.edu.cn是清华大学网络系统中名为www的计算机，拥有这个域名的计算机通常负责提供万维网服务……

域名中包含的很多字符串都有其特定的含义。比如，com表示商业机构，hk表示中国香港，mail表示邮件服务，blog表示网络博客服务，等等。

域名解析

情境2：

- 王红输入www.baidu.com，访问了百度网。
- 赵明使用61.135.169.105，同样可以访问百度网。

为什么两个人使用不同的方式，能访问同一个网站呢？

通过一个域名访问网站，计算机必须先获得域名对应的IP地址。把域名转换成IP地址的过程称为域名解析。在网络中，有一些服务器专门用于提供域名解析服务，这些服务器被称为域名服务器。实际应用时，往往同时指定多个域名服务器，第一个叫作主域名服务器。

微信公众号：电子课本大全

实践活动　查看域名服务器

执行 ipconfig /all 命令，查看更详细的本机配置信息（图2.1.17）。其中“DNS服务器”标明了服务器的IP地址。DNS是domain name service的缩写，意为域名服务。

```
DNS 服务器  . . . . . . . . . . . . : 192.168.168.150
                                      192.168.168.20
                                      192.168.168.22
```

图2.1.17　查看DNS信息

你所使用的域名服务器的IP地址是：_____。

事实上，互联网中的域名解析服务是由不同层级的服务器协作完成的。

实践活动　分析域名解析过程

参照图2.1.18，描述域名解析过程中各级域名服务器如何协同工作。

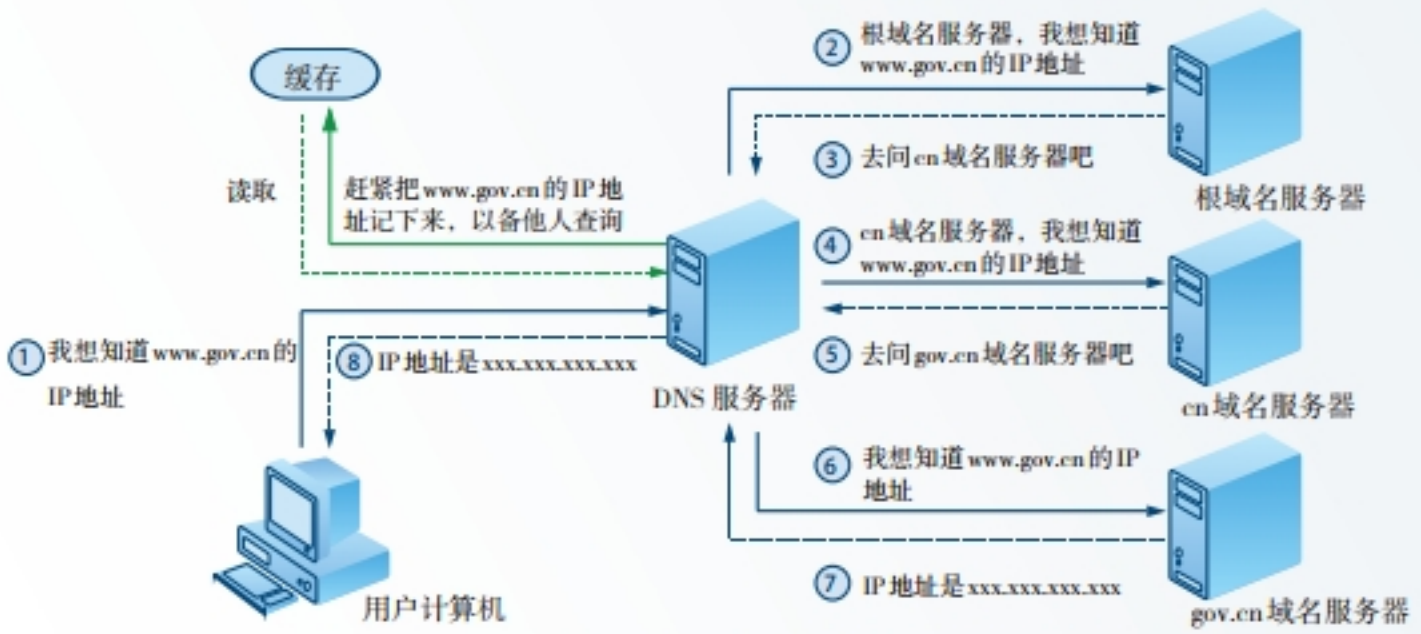


图2.1.18　域名解析过程示意图

阅读拓展　根域名服务器

根域名服务器，也称根服务器，位于域名解析系统的最顶端，负责管理其他域名服务器。根服务器对网络通信的影响巨大，一旦这些服务器发生故障或遭遇攻击，就可能造成大面积的网络通信故障。

在IPv4体系中，全球的根服务器有13台，其中10台在美国，2台在欧洲，1台在日本。随着IPv6体系的正式启用，这一状况得到了改变。截至2017年，我国牵头发起的“雪人计划”已经在全球各地部署了25台IPv6根服务器，其中4台在我国。

微信公众号：电子课本大全

项目实施

编程体验架设域名服务器

1. 参照下面的代码编写Python程序。

```
#引入网络编程库
import dnsserver

if __name__ == "__main__":
      #指定端口，DNS服务默认使用53号端口
      sev = dnsserver.DNSServer(53)

      #增加域名和IP地址的对应关系
      sev.add('www.sina.com.cn', '219.238.4.9')
      sev.add('www.baidu.com', '119.75.216.20')
      sev.add('www.qq.com', '182.254.50.164')
      sev.add('www.163.com', '116.242.0.145')

      #其他域名默认对应的地址
      sev.add('*', '0.0.0.0')
      sev.start()
```

2. 小组内一名成员运行刚刚编写的程序，并公布所用计算机的IP地址，其他成员把主域名服务器设成相应的IP地址，并浏览相应的网站，看看能否正常访问。

3. 修改程序中域名所对应的IP地址，比如调换上下两条的IP地址，然后进行网页浏览，观察此时出现的情况。

4. 恢复原有的网络设置。

阅读拓展

DNS欺骗

DNS欺骗是一种利用DNS服务实施欺骗的攻击行为。其手段通常是：在域名解析过程中，把用户原本要访问的IP地址，偷偷替换成特定的IP地址，从而使用户在不知不觉中访问假冒的网站。比如，在前面的程序中，故意输错域名对应的IP地址，就可以把用户引入错误的网站。

DNS欺骗并不是“攻破”了相应的网站，而是冒名顶替，且假冒的网站一般与原网站极其相似，因而具有很强的欺骗性，使用者很难察觉到，往往只有在欺诈发生后，比如接到被扣款的银行通知后，才会发觉上当受骗了。

为了有效地抵御DNS欺骗，科研人员正在研制更安全的DNS技术，如DNSSEC（domain name system security extensions，域名系统安全扩展），它可以通过数字签名等手段来抵抗DNS欺骗的攻击。

微信公众号：电子课本大全

域名与IP地址的对应关系

一个IP地址可以对应多个域名吗？一个域名可以对应多个IP地址吗？下面来验证一下。

实践活动

验证域名与IP地址的对应关系

1. 执行 ping 命令，获取域名 www.sina.com.cn 和 news.sina.com.cn 对应的IP地址，可以发现，这两个域名对应同一个IP地址。

2. 执行 nslookup 命令，查询一个域名对应的IP地址，如域名 www.baidu.com 对应的IP地址。可以看到，这个域名至少对应了两个IP地址（图2.1.19）。

```
C:\>nslookup www.baidu.com
服务器:  UnKnown
Address:  10.143.22.118

非权威应答:
名称:    www.a.shifen.com
Addresses:  115.239.210.27
          115.239.211.112
Aliases:  www.baidu.com
```

图2.1.19　查看域名对应的IP地址

3. 在浏览器地址框中输入这些IP地址，看看访问的是否为同一个网站。

4. 查看下列域名对应的IP地址。

www.gov.cn	www.mct.gov.cn	www.ccyl.org.cn
www.tsinghua.edu.cn	www.pku.edu.cn	www.sohu.com

可以发现，一个IP地址可以对应多个域名，一个域名也可以对应多个IP地址。前者可以更加充分地利用IP地址资源，后者则可以通过分流，提高用户访问的流畅性。

抢注域名

情境3：

2005年10月9日，国家刚公布珠穆朗玛峰的新高度，数秒后 88444.net、884443.com 等域名就被注册了，几分钟后，cn、us 等域内的相关域名也被注册了。2006年，赠台大熊猫“团团”“圆圆”的名字刚在春节联欢晚会上确定下来，没过几天，与这对大熊猫名字有关的域名就被注册了……

为什么会出现这样的事情呢？

微信公众号：电子课本大全

大家知道，域名中往往包含国家、行业、拥有者等信息，可以成为拥有者的“网上名片”。一个简单、易懂、有意义的域名容易得到人们的认可，有助于提高网站的知名度。对于一些商业机构，由代表自身形象的字母组成的域名，是其不可或缺的“网络商标”。

随着网络的普及，人们对域名越来越重视，注册的域名数量迅猛增加，抢注域名的现象也越来越严重。

想要注册一个辨识度高的域名本无可厚非，但如果恶意抢注和使用知名企业、单位的域名，就可能会侵犯他人的权益。同样地，如果不主动注册域名保护自己的权益，就有可能被他人抢注。



思考活动

如何保护企业的“网络商标”

由于以前大家对域名的认识不足，国内很多知名企业的代表性域名被他人抢先注册，引发了很多纠纷。如果你是一家企业的负责人，你将采取哪些措施来保护企业的“网络商标”呢？

假冒域名

有些字符很相近，比如o和0、i和1等；有些字符的组合很容易混淆，如bea和bee、go和goo等。一些别有用心的人，就利用这些相近的字符或字符组合，注册与知名网站相近的域名。

例如，中国银行原域名是bank-of-china.com，有人故意申请了域名bank-off-china.com；工商银行使用的域名是icbc.com.cn，有人故意申请了1cbc.com.cn……这些故意假冒的域名具有很强的欺骗性，一旦看错、输错就会访问那些假冒的网站，就可能泄露账号和密码。

现在，一些机构开始启用新的简短域名，希望通过减少输入的字符来降低输错的可能性。例如，中国银行就启用了新域名boc.cn。

此外，一些单位或机构把和自己相关、相似的域名都进行了注册，并把这些域名指向同一个网站。例如，微软公司同时注册了www.bing.com和www.bingg.com。

微信公众号：电子课本大全

思考活动

反思遏制假冒域名的方法

你认为还有哪些能够遏制假冒域名的方法？这些方法能够彻底解决问题吗？为什么？

项目实施

总结自己对TCP/IP协议的认识

在了解TCP/IP协议的主要功能和作用的基础上，结合自己的使用感受，总结自己对TCP/IP协议的认识。

提示：

1. 尽可能全面地介绍自己对TCP/IP协议的认识，同时可以选择一个重点进行详细介绍，如IP地址、域名、域名解析等；

2. 观点鲜明，内容严谨；

3. 文字精练，描述生动。

练习提升

1. 讨论域名mail.163.com中包含的信息。

2. 有人提出了一种新的域名——数字域名，它借鉴了电话号码的编码体系，由类似电话号码的国家代码、地区代码和终端代码组成。例如，某出版社网站的域名可以由086（中国代码）、010（北京地区代码）、58758866（企业电话号码）组成，即08601058758866。有人反对这种域名，他们认为域名是因为IP地址难于记忆才产生的，而数字域名又重新回到了数字形式，这是一种倒退。

有必要研发数字域名系统吗？谈谈你的看法。

3. 有人认为，IP地址的长度越长越好，比如256位甚至512位，这样就可以提供更多的地址。你怎么看这个问题？

4. 想象一下，假设有一天出现了下面描述的某种情况，到时候网络访问会出现怎样的景象，说出你的理由。

- 某台根域名服务器突然无法运行了。
- 所有的根域名服务器突然都无法运行了。

微信公众号：电子课本大全

2.2
网络设备与操作系统

学习目标 ▶▶▶

- 熟悉常见的网络设备，理解它们的作用和工作原理。
- 认识网络操作系统，会使用基本的网络命令。
- 能发现简单的网络故障，并能提出相应的解决方案。

体验探索

组建局域网，并实现共享上网

在之前的学习中，我们已经学过如何组建小型无线网络，并把智能手机、平板计算机等连入了网络。参照图2.2.1和图2.2.2的提示，利用路由器，组建一个同时包括有线和无线连接的局域网，并实现设备共享上网。



图2.2.1　有线连接

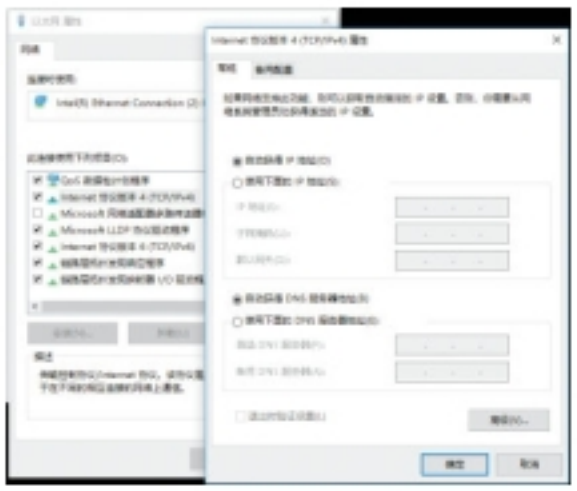


图2.2.2　查看网络设置

在组建过程中，回顾、思考以下问题。

1. 网络的拓扑结构是怎样的？网络的传输介质是什么？
2. 使用了哪些网络设备？这些设备的作用是什么？
3. 你认为，组建的网络由哪些要素构成？

微信公众号：电子课本大全

2.2.1 常见的网络设备

用于组建计算机网络的设备有很多，既有用于某台计算机通信的网卡、调制解调器等设备，也有用于连接不同设备的设备，如交换机、路由器等。

网卡

网卡也叫网络适配器，用来连接计算机等信息设备和网络。网卡分为无线网卡、有线网卡两大类。在智能手机、平板计算机等移动设备的内部，一般都有一块无线网卡，因而可以连接无线局域网。

每块网卡拥有独有的而且一般不能改变的地址，叫作MAC（medium access control，介质访问控制）地址或物理地址。通常也把设备中含有的网卡的物理地址，看作这个信息设备的物理地址。图2.2.3就展示了一部智能手机所配置的网卡的MAC地址。



图2.2.3 查看手机的MAC地址

实践活动

查看网卡的物理地址

1.执行 ipconfig /all 命令，查看网络配置信息。找到“物理地址”那一行，观察物理地址的组成（图2.2.4）。

```
连接特定的 DNS 后缀 . . . . . :
描述. . . . . : Intel(R) Ethernet Connection (2) I219-LM
物理地址. . . . . : 4C-CC-6A-A3-7A-D7
```

图2.2.4 查看网卡的物理地址

2.执行 arp -a 命令，查看IP地址对应的物理地址（图2.2.5）。

```
接口: 10.50.16.99 --- 0x9
  Internet 地址         物理地址              类型
  10.50.16.1            94-db-da-5f-1f-ec     动态
  10.50.16.80           00-e0-4c-36-1c-8b     动态
  10.50.16.125          4c-cc-6a-a3-89-1e     动态
  10.50.16.128          4c-cc-6a-a3-7a-e8     动态
  10.50.16.210          00-10-c6-b0-a7-dd     动态
  10.50.16.221          68-f7-28-b9-1c-73     动态
  10.50.16.222          44-37-e6-52-cc-a2     动态
  10.50.16.251          00-21-b7-56-d2-e1     动态
  10.50.16.252          00-21-b7-43-49-08     动态
  10.50.16.253          00-21-b7-fd-3f-56     动态
```

图2.2.5 查看IP地址对应的物理地址

3. 算一算，网卡的物理地址占多少比特。

微信公众号：电子课本大全

前面介绍过，依据TCP/IP协议传输的数据经层层封装后，形成IP包。IP包若想在局域网中传输，一般还需要加上MAC地址信息等，从而组成以太网帧（图2.2.6）。



图2.2.6　一种以太网帧

实践活动

运行Wireshark软件，了解MAC头部

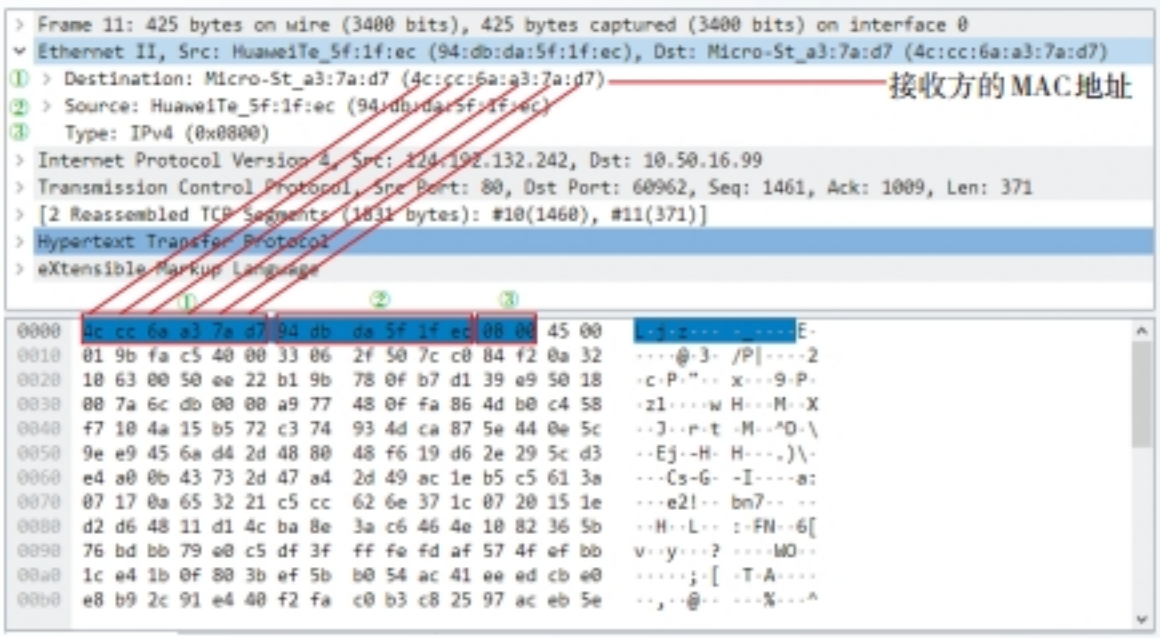


图2.2.7　了解MAC头部

思考活动

分析封装过程

参照图2.2.8，以用HTTP协议访问一个网页为例，回答以下问题。

- 数据需要进行拆分和组装吗？为什么？
- 数据如何一层层进行封装？

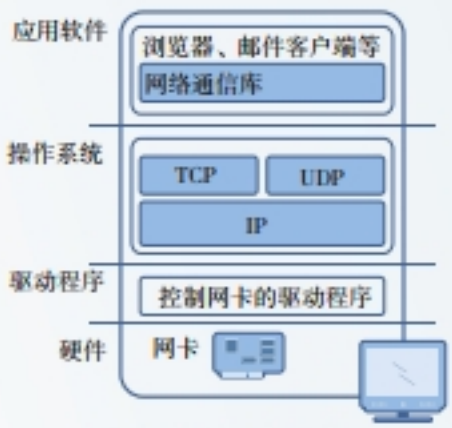


图2.2.8　数据包处理

网络中还有一类重要的硬件设备——通信连接设备。日常使用的通信连接设备主要是交换机和路由器。这两种设备从外观上看非常相似，但它们的工作特点却很不同。

微信公众号：电子课本大全

交换机

交换机（图2.2.9）的内部会记录连接每个端口的计算机的物理地址，两个端口间的计算机传输数据时，不会占用整个传输线路，而是在端口之间采用“点对点”的方式进行传输（图2.2.10）。也就是说，交换机同一时间允许多个端口之间互相通信。这样既提高了网络传输的效率，又增强了网络的安全性。



图2.2.9　交换机

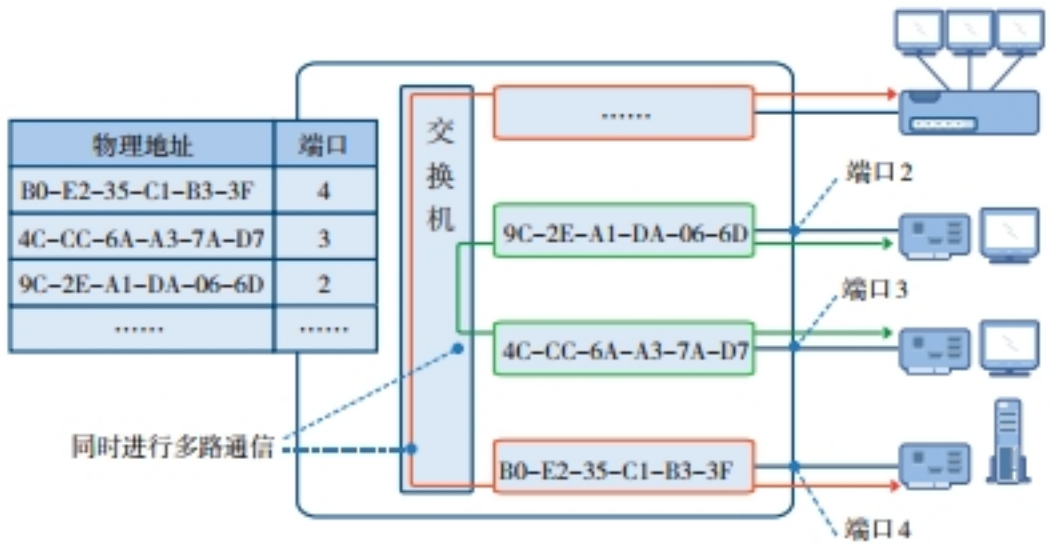


图2.2.10　交换机工作原理示意图

交换机具有较好的网络传输性能，很多单位和机构采用交换机组建规模较大的局域网。

路由器

路由器（图2.2.11）主要用途是连接不同的网络，工作的依据是IP地址。路由器常常拥有多个IP地址，分别对应连接的不同网络。分布在各处的路由器协同工作，从而根据IP地址在网络中找到传输路径（图2.2.12）。

可以说，路由器是互联网通信的基础设备，没有路由器，就无法实现网络互联。



图2.2.11　路由器

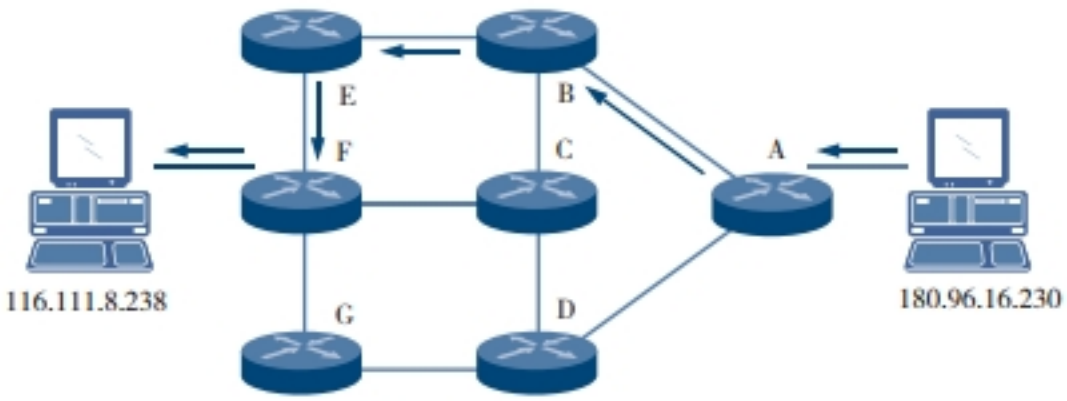


图2.2.12　路由器工作过程示意图

微信公众号：电子课本大全

项目实施

查看访问一个网站时需要经过的路由器

1. 执行 ipconfig 命令，观察窗口中的显示。其中“默认网关”一行中标注的地址，就是通信时经过的第一个路由器。

本机所在网络的默认网关是：_____

2. 用 tracert 命令，查看信息经过的路由器。执行 tracert www.baidu.com 命令，观察窗口中的显示（图2.2.13）。

```
通过最多 30 个跃点跟踪
到 www.a.shifen.com [119.75.216.20] 的路由:

  1     2 ms     1 ms     1 ms  10.50.16.1
  2     *        *        *     请求超时。
  3     1 ms     1 ms     1 ms  172.30.200.9
  4     1 ms     5 ms     1 ms  218.241.241.81
  5     1 ms     1 ms     1 ms  124.205.98.121
  6    61 ms    80 ms     1 ms  14.197.177.13
  7     2 ms    20 ms     3 ms  168.160.254.222
  8     *        *        4 ms  182.61.253.117
  9     *        *        *     请求超时。
 10     2 ms     2 ms     2 ms  127.0.0.1 [119.75.216.20]

跟踪完成。
```

图2.2.13　正常访问

如果访问失败，窗口中可能会出现类似图2.2.14的显示内容。

```
 10    38 ms    38 ms    40 ms  124.65.46.141
 11    47 ms    49 ms    44 ms  124.65.56.225
 12    41 ms    39 ms    40 ms  124.65.194.77
 13     *        *        *     请求超时。
 14     *        *        *     请求超时。
 15     *        *        *     请求超时。
 16     *        *        *     请求超时。
 17     *        *        *     请求超时。
 18     *        *        *     请求超时。
 19     *        *        *     请求超时。
 20     *        *        *     请求超时。
 21     *        *        *     请求超时。
 22     *        *        *     请求超时。
 23     *        *        *     请求超时。
 24     *        *        *     请求超时。
 25     *        *        *     请求超时。
 26     *        *        *     请求超时。
 27     *        *        *     请求超时。
 28     *        *        *     请求超时。
 29     *        *        *     请求超时。
 30     *        *        *     请求超时。
```

图2.2.14　访问失败

3. 利用 tracert 命令追踪访问其他网站。

路由器大体可分为专用路由器和家用路由器两种。专用路由器主要用于国家之间、城市之间的网络互联。家用路由器通常具备拨号上网、地址转换等功能，可以看作一台具有网络连接与访问控制功能的计算机，可用于连接互联网，并实现共享上网。

微信公众号：电子课本大全

局域网内的信息设备没有公用IP，不能直接用于互联网通信，这时可以借助路由器的地址转换功能实现网络通信（图2.2.15）。

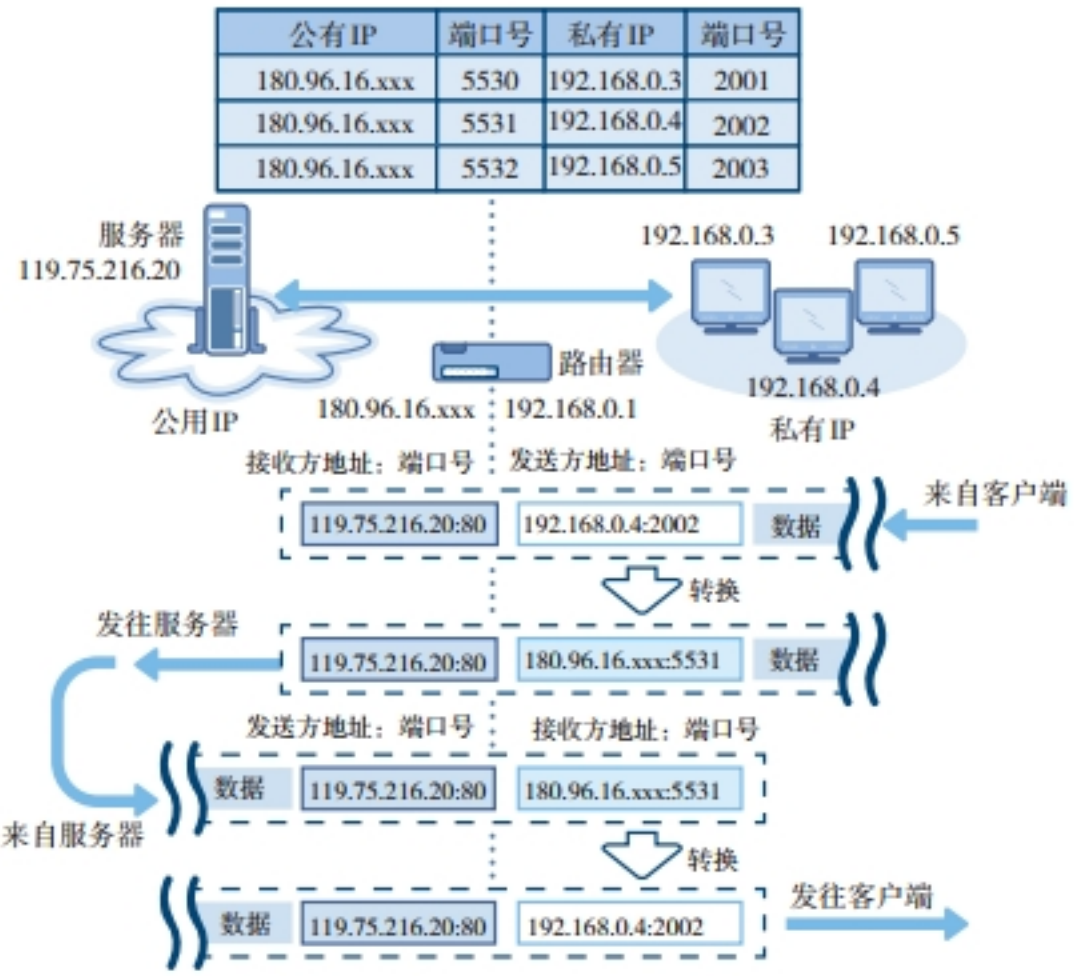


图2.2.15　地址转换示意图

在图2.2.15中，路由器连接着一个外网和一个内部的局域网。局域网内的设备发出通信请求后，路由器会把其中的私有IP地址和端口号，替换成自己的公用IP地址和端口号，并记录两者的对应关系，然后向服务器发送请求。

收到服务器的回复后，路由器再根据之前的记录，把数据包中的接收地址和端口号转换成局域网中设备的地址和端口号，并把数据发送过去。这样，局域网内的计算机就可以访问互联网了。

实际应用时，可能需要经过多台路由器层层转发，这时就要经历多个地址转换过程。

思考活动

分析路由器和交换机的功能

1. 参照图2.2.15，尝试描述路由器如何支持局域网内的多台信息设备同时访问互联网。

2. 交换机和路由器有什么区别？

3. 路由器具有哪些功能？

微信公众号：电子课本大全

2.2.2 网络操作系统

通常认为，网络操作系统（network operating system）主要包括两种：

一、运行在路由器等通信设备上，只用于完成特定的数据处理任务，力求保证网络通畅的操作系统；

二、运行在网络服务器上，侧重于实现文件共享、打印机共享、网络用户管理等功能的操作系统。

网络操作系统和单机操作系统曾经有明显的区分，如DOS、CP/M等都是非常典型的单机操作系统，而同一时期的NetWare则是典型的网络操作系统。

不过，随着软件技术的提升，目前常用的操作系统，如Windows、FreeBSD、UNIX和Linux等，都已经具备了网络操作系统的基本功能（图2.2.16）。

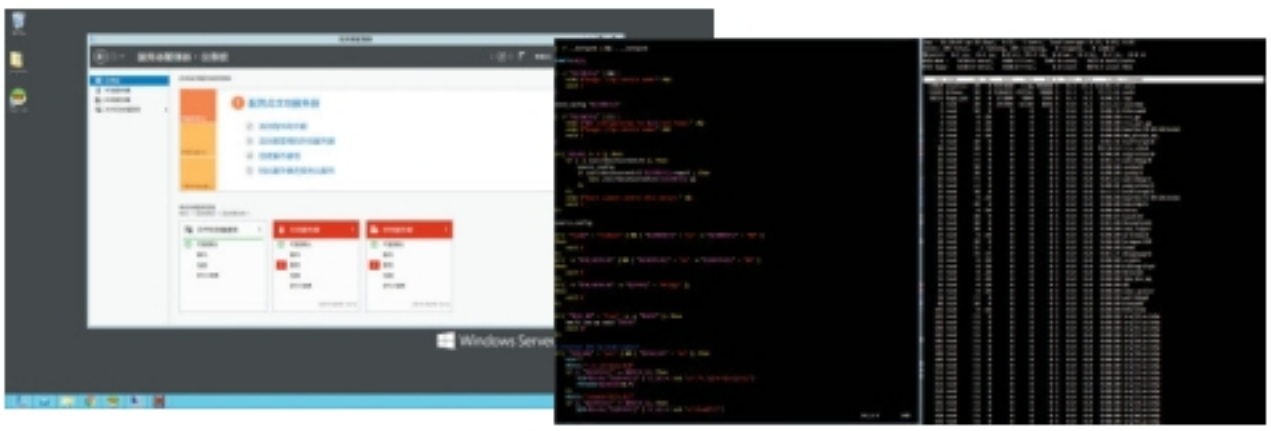


图2.2.16 网络操作系统

项目实施

回顾网络操作的基本命令

网络操作系统会提供很多网络操作命令，请根据学习体验填写表2.2.1。

表2.2.1 网络基本命令

命令	用途	例子
ping	用于检查网络是否能连通	ping 10.16.50.66
ipconfig		
nslookup		
netstat		
arp		

微信公众号：电子课本大全

2.2.3 局域网的安全策略

一个网络由多个环节组成，某一处出现问题，就可能引发安全问题。作为网络的设计者，应从整体出发进行考虑，采用适当的安全措施提升网络的安全性。之前介绍了如何设置无线网密码，接下来再介绍两种局域网安全策略。

情境1：

赵明和组员们想进一步增强所组建局域网的安全性，他们希望通过路由器完成这样的功能：只让得到授权的计算机、智能手机等设备连入网络，没有得到授权的设备，即使知道无线网密码，也不能连入网络。

想一想该怎么实现呢？

设置MAC地址过滤

前面说过，每一块网卡都有独一无二的MAC地址，如果能让路由器记住一张记录着MAC地址的表格，一旦发现表格外的设备试图连入，就自动拒绝，这样就可以满足前面的需求了。

目前，大部分路由器都有MAC地址过滤功能。这个功能又可分为两类：允许表格中的设备接入的白名单功能和阻止表格中的设备接入的黑名单功能。

项目实施

在路由器上设置白名单

1. 查询要联网设备的MAC地址，并记录下来。
2. 参照图2.2.17，在路由器上设置MAC地址过滤列表。

提示：过滤规则应该类似“允许下面的MAC地址访问”。

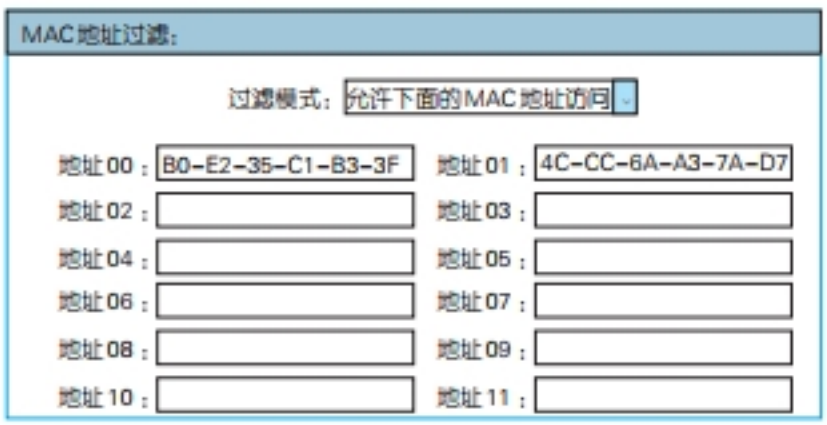


图2.2.17 MAC地址过滤

3. 分别用表中的设备和之外的设备，以有线和无线的方式接入局域网，观察接入效果。

微信公众号：电子课本大全

思考活动

探讨“蹭网”行为

“蹭网”指未经允许私自连接他人的网络，从而实现免费上网的行为。结合这一行为，谈一谈使用MAC地址过滤功能的好处以及可能引发的问题。

情境2：

赵明收集了一个名单，里面有很多钓鱼网站和假冒网站，但是很多同学不知道，仍可能访问那些网站。让每位同学访问网站时都去查单子，也很不方便。

有什么办法，能让局域网内的计算机无法访问那些网站呢？

域名过滤

前面介绍过，局域网内的计算机访问互联网中的服务器时，都要通过路由器。如果让路由器记住一张禁止访问的网站的清单，不对它们提供连接服务，自然就可以保证局域网内的计算机无法访问相应网站了。这个功能称为域名过滤功能。

项目实施

在路由器上设置域名过滤功能

1. 选择一些域名。
2. 参照图2.2.18，在路由器上设置域名过滤列表。

域名过滤：

通过域名过滤来限制局域网中计算机对某些网站的访问。

域名过滤功能 ○关闭 ●开启

ID	生效时间	域名	状态	操作
00	00:00–23:59	www.***.com	生效	编辑 删除
01	00:00–23:59	www.***.us	生效	编辑 删除
02	08:00–16:00	www.***.info	生效	编辑 删除
03	08:00–16:00	www.***.net	生效	编辑 删除
04	00:00–23:59	www.***.mil	生效	编辑 删除

添加新条目 使所有条目生效 使所有条目失效 删除所有条目

图2.2.18 域名过滤

3. 让局域网内的计算机访问含有过滤域名的网站，看看能否正常访问。

微信公众号：电子课本大全

项目实施

网络检查与总结

1. 检查组建小型局域网活动的完成情况。

· 检查小组组建的网络是否畅通。

检测方法是：_____

· 检查接入的计算机、智能手机等设备能否共享上网。

检测方法是：_____

2. 总结网络配置情况。

· 局域网支持的传输介质包括：_____

· 主要的联网设备包括：_____

· 主要使用的软件包括：_____

3. 总结采取的安全措施。

· 设置无线网密码，作用是：_____

· _____，作用是：_____

· _____，作用是：_____

练习提升

1. 在其他局域网中可以正常使用的信息设备，无法连入自己组建的局域网了，这种情况可能是什么原因造成的？该如何检查和解决？

2. 用路由器实现共享上网时，数据如何在局域网内的计算机和服务器之间传输？请简要描述。

3. 调查校园网或身边的其他网络，调查内容主要包括以下几点。

· 了解所使用IP地址的类型，以及IP地址是如何分配的。

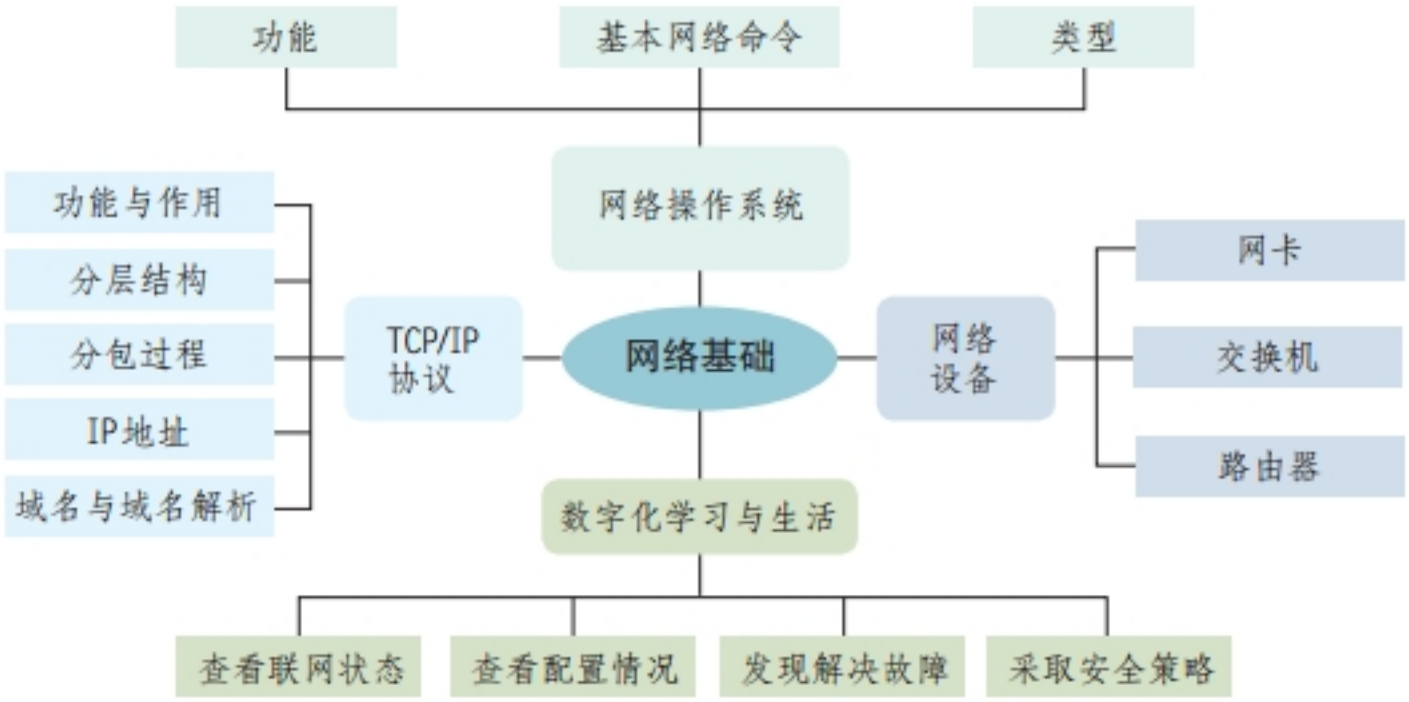
· 使用的主要网络设备和软件。

· 网络采取的安全措施。

微信公众号：电子课本大全

总结 评价

1. 下图展示了本章的核心概念与关键能力，请同学们对照图中的内容进行总结。



2. 根据自己的掌握情况填写下表。

学习内容	掌握程度		
TCP/IP协议的主要功能和作用	□ 不了解	□ 了解	□ 理解
网卡、交换机和路由器等基本网络设备	□ 不了解	□ 了解	□ 理解
基本网络设备的作用	□ 不了解	□ 了解	□ 理解
基本网络设备的工作原理	□ 不了解	□ 了解	□ 理解
网络操作系统	□ 不了解	□ 了解	□ 理解
用基本网络命令查询联网、配置情况	□ 不会	□ 会	□ 熟练
增强局域网安全	□ 不会	□ 会	□ 熟练

3. 回答以下问题，完成活动反思。

（1）有观点认为：“尽管IPv6协议已经正式启用，但在较长的一段时间内，它将和IPv4协议共存。”对于这个观点，你怎么看？

（2）在本章的学习过程中，你或同学遇到了什么问题？是如何解决的？你觉得自己有什么样的收获，尝试列举几点与同学分享。

微信公众号：电子课本大全

第 3 章
网络安全与网络资源

网络正在改变着社会和人们生活的方方面面，给人们带来了丰富的网络资源，带来了各种便捷的获取和使用资源的手段，方便着人们的工作、学习和生活。不过，网络在给人们带来惊喜和奇迹的同时，也给个人、企业、社会、国家等各方面带来了巨大的安全挑战。网络空间已成为继海、陆、空、天之外的“第五疆域”，网络安全与政治安全、经济安全、军事安全等传统安全融合交织。



微信公众号：电子课本大全

03 主题学习项目：安全分享细细说

项目目标

现在，人们经常通过网络分享各种信息，如照片、视频、学习文档等，但在分享的过程中经常会遇到各种安全问题。本章将通过利用网络安全分享图文等资源的项目活动，探讨网络加密和网络分享策略。

1. 通过项目活动，体会常用加密技术的特点。
2. 掌握智能手机、平板计算机等分享网络资源的方法。
3. 反思分享过程，提高网络分享的安全性。

项目准备

为了完成项目，需要做以下准备。

- 本章涉及的加密、资源分享等活动，需要小组成员互相配合协同完成。在开展这些活动时，既要积极完成分配给自己的任务，也要兼顾其他组员的进展。
- 本章的部分操作实践活动，需要不同小组之间互相配合才能完成。在开展这些活动时，各小组间应该事先商定好合作步骤。
- 开展本章设定的辩论活动前，每个人都应当熟悉活动规则，以便保证辩论活动的顺利进行。

项目过程

为了保证顺利完成本章的学习活动，在不同学习阶段，小组长要注意检查组员项目学习的进度，并做好协调互助工作。

1 学习实践

阅读有关加密技术的资料，认真完成关于网络安全的实践操作。P65

2 辩论明理

了解辩论规则，与其他组同学开展主题为“网络安全攻防战”的辩论赛。P86

3 安全分享

整理资源的类型和网络分享的常用方法；完成网络分享的实践操作。P95

4 活动反思

填写关于网络资源分享的项目报告，及时检查报告的完整性和准确性。P96

项目总结

学完本章后，及时分析活动时遇到的问题，归纳总结解决问题的方法。通过项目学习活动，认识网络应用中信息安全的重要性，熟悉常用的加密技术和网络安全协议，能够设置简易防火墙，能利用适当的工具对数据和终端设备进行加密，能识别网络资源的类型，能利用适当的工具在计算机和移动终端上生成与分享网络资源。

微信公众号：电子课本大全

3.1
加密技术与安全

学习目标 ▶▶▶

- 了解常用的加密技术，了解常用网络安全协议的作用。
- 能够设置及使用简易防火墙。
- 能够使用适当工具对数据和终端设备进行加密。

体验探索

回顾网络安全事件

近年来，网络安全问题层出不穷。

2017年3月，在公安部的统一指挥下，北京、安徽、辽宁、河南等14个省、直辖市的公安机关开展集中收网行动，抓获犯罪嫌疑人96名，查获被窃的公民个人信息达50多亿条，涉及交通物流、医疗、社交、银行等多个领域。

2016年8月，一位高中毕业生的个人信息被泄露，并被骗走了上大学的学费。该学生报警后突然离世。数日后，案件告破，查获被泄露的考生信息达10万多条。

2015年，我国首例黑客盗刷信用卡案告破，警方查获160多万条公民个人信息和银行卡账号，涉案金额14.98亿元。

你遭遇或者听说过哪些网络安全事件？这些事件给当事人带来了哪些影响？你觉得这些事件产生的原因是什么？

网络安全涉及的范围非常广，既包括计算机、路由器等硬件设备的安全，也包括操作系统、数据库、应用软件等软件的安全；既涉及国家机密信息的保护，也涉及个人隐私信息的保护；既需要规范的行为习惯，也需要稳定可靠的安全技术……在这一节，将重点介绍通过加密技术增强网络信息传输安全性的知识与方法。

微信公众号：电子课本大全

3.1.1　网络通信面临的威胁

思考活动

探讨网络通信面临的威胁

信息安全面临的风险有很多，但仅就网络通信而言，主要面临哪些安全威胁呢？

在网络通信过程中，信息安全时时面临各种威胁。如果进行适当的归纳整理会发现，这些威胁主要包括非法阻断、窃听、篡改和伪造等（图3.1.1）。

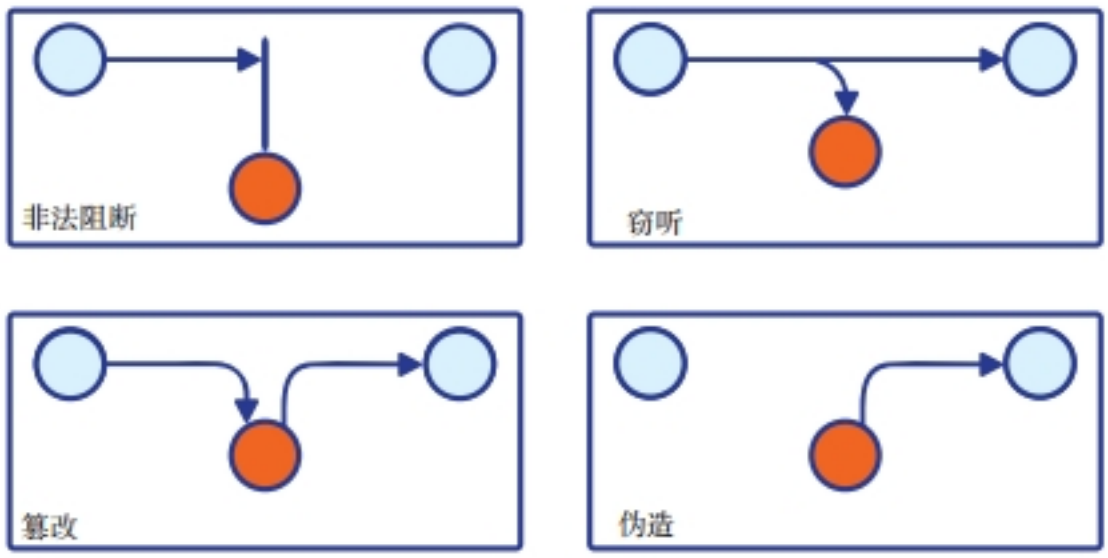


图3.1.1　网络通信面临的威胁

非法阻断问题，多与网络设备、通信线路、服务器设置等密切相关。本节不讨论这个问题。

与这些威胁相对应，网络安全就是要尽量保证数据的可用性、保密性、完整性和真实性。可用性，即得到授权的用户、实体或程序能顺利获取所需的信息，而不被非法阻断；保密性，即防止未授权的用户、实体或程序窃取信息；完整性，即尽可能保证数据不会被未授权的一方私自修改；真实性，即确保信息不被伪造。

如果把信息安全问题比作一场战争，那么维护信息安全的一方通常被视为防守方，而破坏者则被视为攻击方。防守方无论怎样做，也无法提前针对每一个可能存在的威胁做出相应的对策，而攻击方只要找到一个不起眼的漏洞，就可以攻破整个防守体系。用户作为信息系统中的不可控因素，其行为会对信息安全产生不可预估的影响。

尽管如此，研究人员仍然找到了很多可靠的技术手段来增强网络通信的安全性。

微信公众号：电子课本大全

3.1.2 数字摘要及网络应用

情境1：

王红下载文件时，发现在下载链接的旁边还有一串奇怪的字符串，赵明说那是文件的数字摘要，可以用来检测文件是否被篡改过。

数字摘要是什么？如何用它来检测信息是否被篡改过呢？

数字摘要

数字摘要是一种认证技术，它采用某种算法对信息中的若干重要元素进行某种变换，最终得到固定长度的摘要值。用于生成数字摘要的算法主要有MD5、SHA等。

项目实施

感受数字摘要算法

1. 阅读下面的程序。

```
# 引入编程库
import hashlib
message= input("input:")
m = hashlib.md5()
m.update(message.encode('utf-8'))
print('MD5:'+m.hexdigest())
```

2. 运行程序，输入不同的字符串，计算它们的MD5值。

```
input:hello,word!
MD5: 9702d6722a0901398efd4ecb3a20423f
input:hello,world!
MD5: c0e84e870874dd37ed0d164c7986f03a
input:b
MD5: 92eb5ffee6ae2fec3ad71c777531578f
```

3. 试一试，能不能通过MD5值获得跟字符串相关的信息，如内容、长度等。

4. 试一试，是否会遇到字符串不同，但MD5值相同的情况。

5. 参照提示，尝试采用SHA1、SHA256、SHA512等算法计算字符串的摘要值。

提示：`m = hashlib.sha1()`　`m = hashlib.sha256()`　`m = hashlib.sha512()`

数字摘要是根据信息生成的二进制数，为了便于表示，常常把它转换成字符串形式。数字摘要具有三个特征：

- 不同信息的数字摘要几乎不可能重复；
- 无法通过数字摘要反向推导生成这个摘要的信息；
- 同一算法的数字摘要长度是固定的（图3.1.2）。

微信公众号：电子课本大全

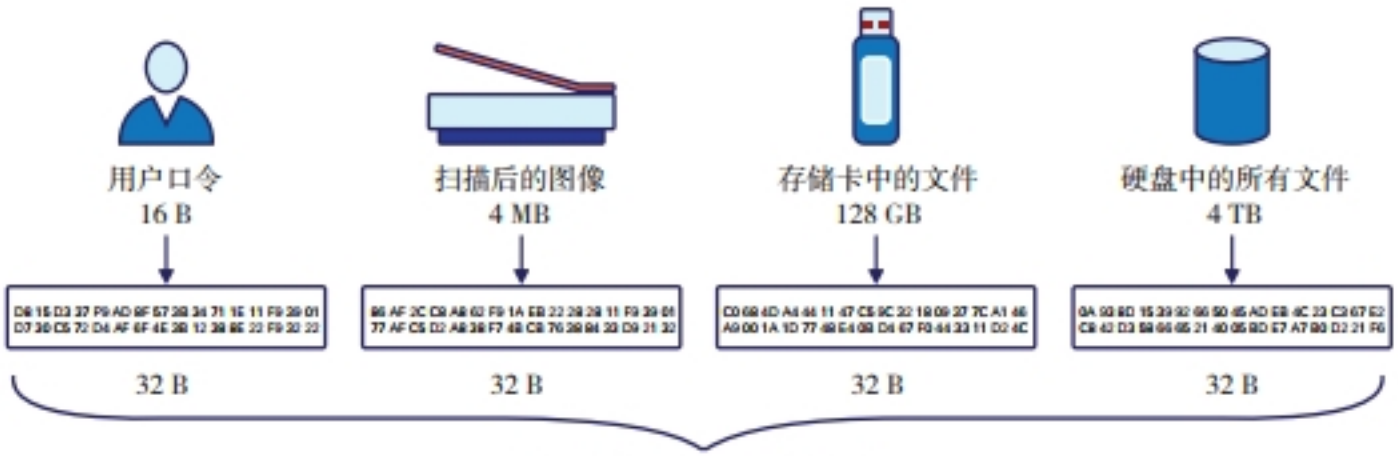


图3.1.2　数字摘要

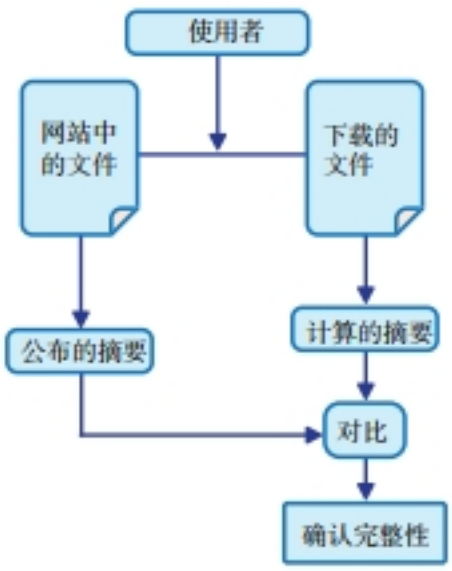


图3.1.3　用数字摘要验证文件的完整性

数字摘要的应用

数字摘要与文件下载。不同信息的数字摘要几乎不可能相同，也就意味着，不同文件的数字摘要通常是不同的，哪怕是文件中的一个0变成了1，数字摘要也会发生变化。这个特性正好用来验证文件的完整性（图3.1.3）。

很多网站提供文件下载服务时，往往会附上数字摘要算法和文件对应的摘要值。下载了某个文件的用户，只要验证一下所下载文件的数字摘要，就能知道文件在下载过程中是否发生了传输错误，或者是否被篡改过。

项目实施

验证文件的数字摘要

1. 从网上下载一个文件，如Python的安装文件，并记录网站公布的该文件的数字摘要，如MD5值（图3.1.4）。

Version	Operating System	Description	MD5 Sum	File Size	GPG
Gzipped source tarball	Source release		ab25d24b1f8cc4990ade979f6dc37883	22994617	SIG
XZ compressed source tarball	Source release		9f49654a4d6f733ff3284ab9d227e9fd	17049912	SIG
macOS 64-bit/32-bit installer	Mac OS X	for Mac OS X 10.6 and later	bf319337bc68b52fc7d227dca5b6f2f6	28093627	SIG
macOS 64-bit installer	Mac OS X	for OS X 10.9 and later	37d891988b6aeedd7f03a70171a8420d	26987706	SIG
Windows help file	Windows		be70202d483c0b7291a666ec66539784	8065193	SIG
Windows x86-64 embeddable zip file	Windows	for AMD64/EM64T/x64	04cc4f6f6a14ba74f6ae1a8b685ec471	7190516	SIG
Windows x86-64 executable installer	Windows	for AMD64/EM64T/x64	9e96c934f5d16399f860812b4ac7002b	31776112	SIG
Windows x86-64 web-based installer	Windows	for AMD64/EM64T/x64	640736a3894022d30f7babff77391d6b	1320112	SIG
Windows x86 embeddable zip file	Windows		b0b099a4fa479fb37880c15f2b2f4f34	6429369	SIG
Windows x86 executable installer	Windows		2bb6ad2ecca6088171ef923bca483f02	30735232	SIG
Windows x86 web-based installer	Windows		596667cb91a8fb20e6f4f153f3a213a5	1294096	SIG

图3.1.4　下载文件与数字摘要

微信公众号：电子课本大全

2. 利用下面的程序计算所下载文件的MD5值。

```
import hashlib
m = hashlib.md5()
#二进制形式读取文件
with open ('d:/python-3.6.5-amd64.exe','rb') as f:
    m.update(f.read())
print('MD5: '+m.hexdigest())
```

运行结果：MD5: 9e96c934f5d16399f860812b4ac7002b

3. 利用Windows系统中的工具CertUtil，计算文件的MD5值（图3.1.5）。

```
certutil -hashfile d:/python-3.6.5-amd64.exe MD5
```

```
D:\>certutil -hashfile d:/python-3.6.5-amd64.exe MD5
MD5 的 d:/python-3.6.5-amd64.exe 哈希:
9e96c934f5d16399f860812b4ac7002b
CertUtil: -hashfile 命令成功完成。
```

图3.1.5　计算MD5值

4. 比较一下，前面用不同方法获得的MD5值是否相等。

5. 更改文件的名称，然后重新计算MD5值，看看是否会发生变化。

数字摘要与密码保护。信息系统中的用户密码通常保存在数据库中，如果直接按密码的原样进行保存，那么数据库的管理人员就可以轻松看到这些隐秘信息，从而带来密码泄露的隐患。

这时，可以采用摘要算法对密码进行保护，即数据库中存放的是密码的数字摘要，管理人员即使看到数字摘要，也无法获悉用户的密码，甚至连密码的长度也无法知道。使用时，用户输入密码后，信息系统根据用户输入的密码计算数字摘要，然后与系统中已保存的数字摘要进行比对，就能决定是否允许用户登录了。

思考活动

数字摘要技术与密码安全

1. 讨论使用数字摘要技术后，一个信息系统是如何校验用户密码的，并把图3.1.6补充完整。

2. 用户丢失密码后，信息系统A的客服人员很热情，他表示自己虽然不能查看，但可以通过短信等方式，告知原来使用的密码；信息系统B的客服人员则表示，他无法提供原来的密码，只能帮用户申请一个临时密码。这两个信息系统，哪一个在密码安全方面做得更好？为什么？

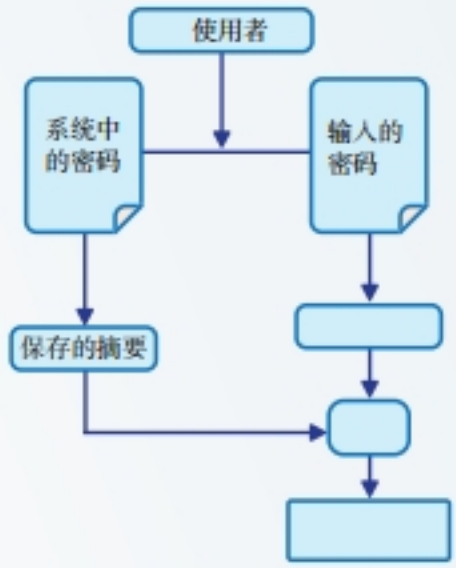


图3.1.6　数字摘要与密码验证

微信公众号：电子课本大全

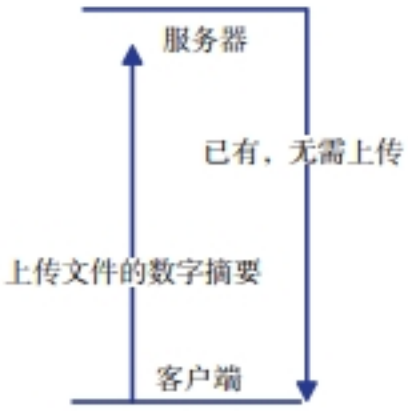


图3.1.7 “秒传”原理

数字摘要与云存储。现在，云存储的使用已经非常普及了，作为云存储的运营者，难免会遇到这样的问题：不同的用户上传了同样内容的文件，而作为一个系统，其实只要存一份就够了。如何才能快速判断系统中是否已经有相同文件了呢？

这时，可以先在客户端计算相关文件的数字摘要，并把数字摘要传给服务器，查看系统中是否已有相同文件。如果有了，就无需用户继续上传，只要用链接的技术，让用户的云盘中出现这个文件就可以了（图3.1.7）。

思考活动

探讨数字摘要技术的应用

数字摘要还可以用在哪些方面？

数字摘要的局限与应对

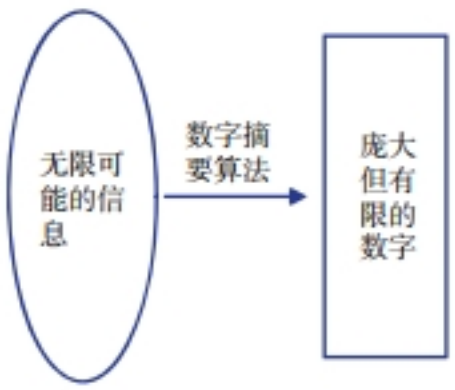


图3.1.8 生成数字摘要过程示意图

首先，数字摘要只能用来验证信息的完整性，但完整的信息不一定真实可靠。实际上，如果攻击方同时替换了要传输的数据和数字摘要，那么接收方就很难察觉。

其次，不同信息的数字摘要存在重复的可能。计算数字摘要，其实是把无限可能的信息，归纳为有限数字的过程，必然存在信息不同但数字摘要相同的情况（图3.18）。这就意味着，攻击者虽然不知道用户的密码，但他有可能用数字摘要相同的密码登录信息系统。

不过也无需对此过于担心。一方面，这种现象出现的可能性极低，如果想人为地根据一个特定的数字摘要反推出一个相应的字符串，是一件非常困难的事情，普通攻击者很难做到。

另一方面，研究人员在不断研制更安全的摘要算法。现在，很多信息系统开始改用SHA1等新算法，特别敏感的部门甚至会采用更安全的SHA256或SHA512算法。

当然，更安全的算法，通常需要更多的计算资源或者更长的运算时间。因此，确定数字摘要算法时，要根据实际需求进行选择，而不能一味地强求安全。比如，虽然MD5算法已被认为不安全了，但由于其计算过程相对简单，所以在不太敏感的领域仍广泛使用。

到目前为止，世界上还没有绝对安全的技术。一种技术，只要能保证在相对较长的时间里不被攻破，就可以认为是安全的。

微信公众号：电子课本大全

3.1.3 加密技术及网络应用

项目实施

体验加密过程

1. 准备4张纸板，上面有8行8列共64个空心圆。

2. 参照图3.1.9中的图a和图b，把第1张和第2张纸板的部分空心圆涂成实心圆。

3. 比对第1张纸板和第2张纸板，如果某一位置的圆一个为空心圆，一个为实心圆，则把第3张纸板的对应位置的圆涂成实心圆（图c）。

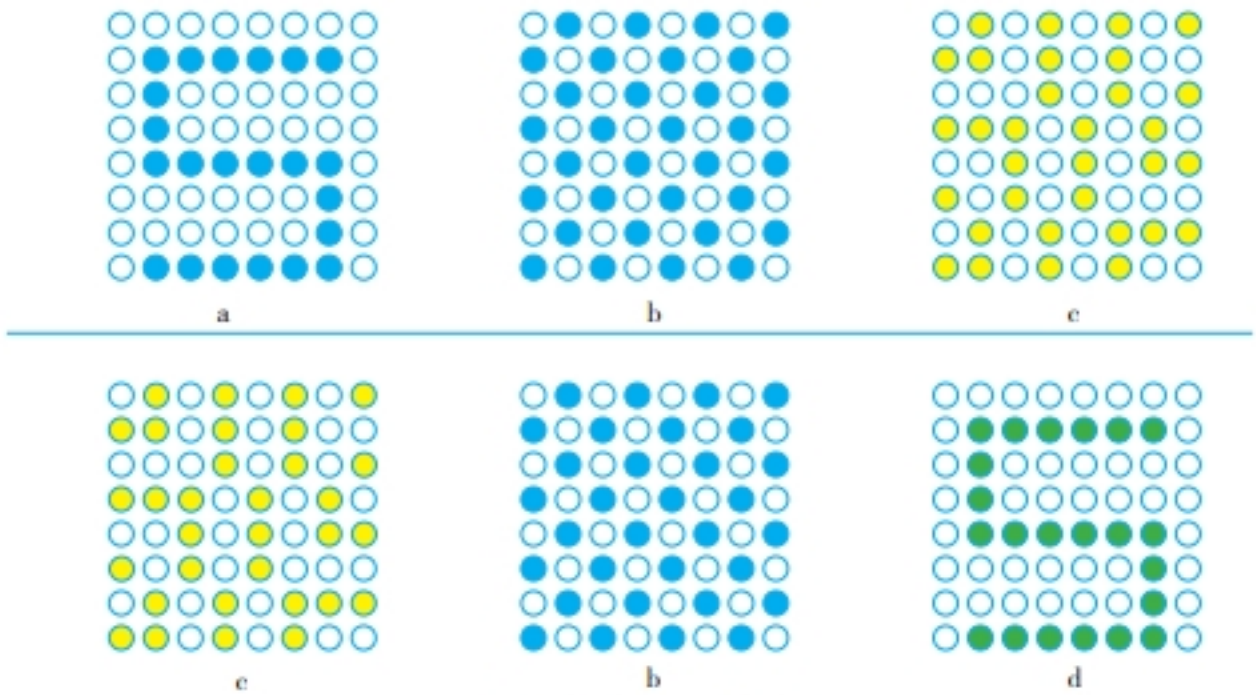


图3.1.9 活动过程示意图

4. 只把第3张纸板交给另一位同学，看看他（她）能否猜出原本的记号。

5. 把第2张纸板也交给那位同学，让他（她）与第3张纸板进行比对，并按照同样的规则涂第4张纸板，看看最后的结果（图d）。

上面这个活动，其实展示了一个简单的加密过程。其中图a相当于明文，图b相当于密钥。由图a和图b得出图c的过程相当于加密过程，由图c和图b得出图d的过程，相当于解密过程。加解密过程可抽象为图3.1.10。



图3.1.10 加密与解密

现在使用的加密技术，主要包括对称密钥加密和非对称密钥加密两种。

微信公众号：电子课本大全

实践活动

编程加密

在前面的活动中，如果把纸板上的空心圆看作0，实心圆看作1，那么纸板上的图形就可以看作是个64位的二进制数，相应的加密和解密过程，实际上采用了“异或”运算。“异或”是一种二进制运算，其特点是：“相同为0，不同为1”。参考下面的代码，尝试编程重现上面的加密和解密过程。

```
a = 0b10101010          # 前面加 0b 表示这是二进制数
c = a^b                 # a、b 两个数进行异或运算，相当于加密
d = c^b                 # c、b 两个数进行异或运算，相当于解密
print(bin(d))           # 二进制形式显示数字
```

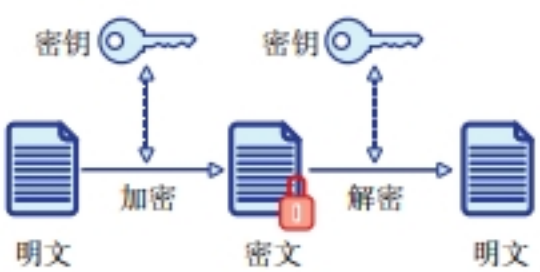


图3.1.11　对称密钥加解密

对称密钥加密

对称密钥加密的特点是加密和解密过程使用相同的密钥（图3.1.11）。前面进行的活动，可归属于对称密钥加密。目前常使用的对称密钥加密算法包括DES（data encryption standard，数据加密标准）、AES（advanced encryption standard，高级加密标准）等。

项目实施

体验AES加密

1. 打开下面用于加解密的程序。

```
# 导入 AES 加密库
from Crypto.Cipher import AES
# 导入 AES 加密所需的工具库
from Crypto.Util.Padding import pad,unpad

# 输入加密密钥
passwd = input('加密密钥：')
# 利用 pad 工具，生成适合 AES 算法要求的密钥
key = pad(passwd.encode('utf-8'),16)
print('密钥：'+str(key))

# aes 加解密准备
aes = AES.new(key, AES.MODE_ECB)

# 输入要加密的明文
message = input('输入明文：')
# 利用 pad 工具，整理明文，以满足 AES 算法的要求
text = pad(message.encode('utf-8'),16)

# 加密
etext = aes.encrypt(text)
print("密文：",str(etext))
```


微信公众号：电子课本大全

```
#输入解密密钥
passwd2 = input('解密密钥：')

#利用 pad 工具，生成适合 AES 算法要求的密钥
key2 = pad(passwd2.encode('utf-8'),16)

# aes 加解密准备
aes = AES.new(key2, AES.MODE_ECB)

#解密
de = unpad(aes.decrypt(etext1),16)
print('明文：',str(de,'utf-8'))
```

2. 运行程序体验加解密过程，并回答下面的问题。

- 你能否从密文看出明文的长度等特征？
- 如果输入了错误的密钥，能否解开密文？

与数字摘要不同，密文的长度一般随明文长度而变，明文越长，密文一般也越长。如果输错了密钥，则无法解开密文。

对称密钥加密拥有AES等可靠的加密算法，但也面临一个棘手的问题：如何把密钥安全地传递给接收方。在网络通信过程中，攻击者完全有可能通过网络窃听，获得密钥，从而获取机密信息（图3.1.12）。

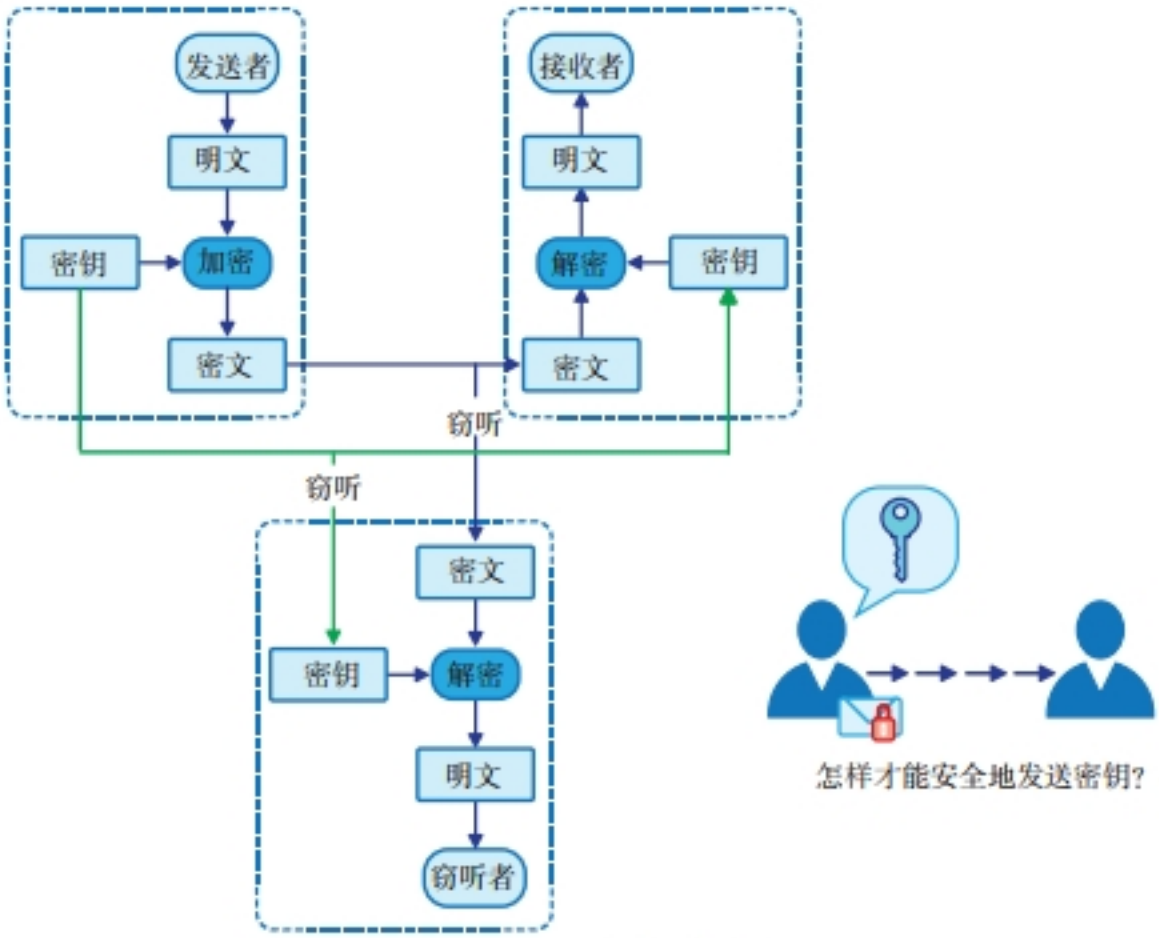


图3.1.12　对称密钥配送问题

微信公众号：电子课本大全

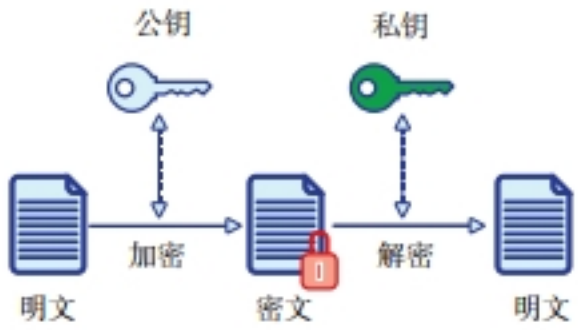


图3.1.13　非对称密钥加解密

非对称密钥加密

非对称密钥加密的特点是，加密和解密过程分别使用不同的密钥。这一对密钥中，一个公开发给他人，称为公钥，用于加密；一个自己保留，称为私钥，用于解密（图3.1.13）。RSA算法是目前最常用的非对称密钥加密算法。

项目实施

体验RSA非对称密钥加密

1. 打开下面用于加解密的程序。

程序1：生成RSA公钥和私钥

```
# 导入 RSA 加密库
from Crypto.PublicKey import RSA

# 生成私钥与公钥
key = RSA.generate(2048)
pr_key = key.export_key()
pb_key = key.publickey().export_key()

# 保存私钥和公钥
file_out = open("pr_key.bin", "wb")
file_out.write(pr_key)
file_out.close()

file_out = open("pb_key.bin", "wb")
file_out.write(pb_key)
file_out.close()
```

程序2：RSA加密

```
from Crypto.PublicKey import RSA
from Crypto.Cipher import PKCS1_OAEP

# 读取公钥
key_data = open("pb_key.bin", "rb").read()
key = RSA.import_key(key_data)

# 生成 RSA 加密器
cipher = PKCS1_OAEP.new(key)

# 加密
message ='密码不等于密钥。'
etext = cipher.encrypt(message.encode('utf-8'))
print(etext)

# 密文保存到文件
file_out = open("en_message.txt", "wb")
file_out.write(etext)
file_out.close()
```


微信公众号：电子课本大全

程序3：RSA解密

```
from Crypto.PublicKey import RSA
from Crypto.Cipher import PKCS1_OAEP

#读取私钥
key_data = open("pr_key.bin", "rb").read()
key = RSA.importKey(key_data)

#生成RSA加密器
cipher = PKCS1_OAEP.new(key)

#读取密文
file_in = open("en_message.txt", "rb")
en_data = file_in.read()

#解密
text = cipher.decrypt(en_data)
print(str(text,'utf-8'))
```

2. 把自己的公钥发给组内其他成员。

3. 请其他同学用自己的公钥进行加密，然后把密文传给自己，再用自己的私钥进行解密。

4. 思考以下问题。

· 能否使用不成对的公钥和私钥进行加密或解密操作？

· AES算法和RSA算法相比，哪一个速度更快？

非对称密钥加密、解密的过程，可以参见图3.1.14。



图3.1.14　非对称密钥的使用

在非对称密钥加密技术中，公钥原本就是要广而告之的，任何想给A发送机密信息的人，只要用A公布的公钥进行加密操作就可以了，因而不害怕密钥被窃听的问题。

不过这一技术也有弱点，比如，B收到一个号称来自A的公钥，B还必须想办法验证这确实是A的公钥，否则传输过程就可能被攻击（图3.1.15）。

微信公众号：电子课本大全

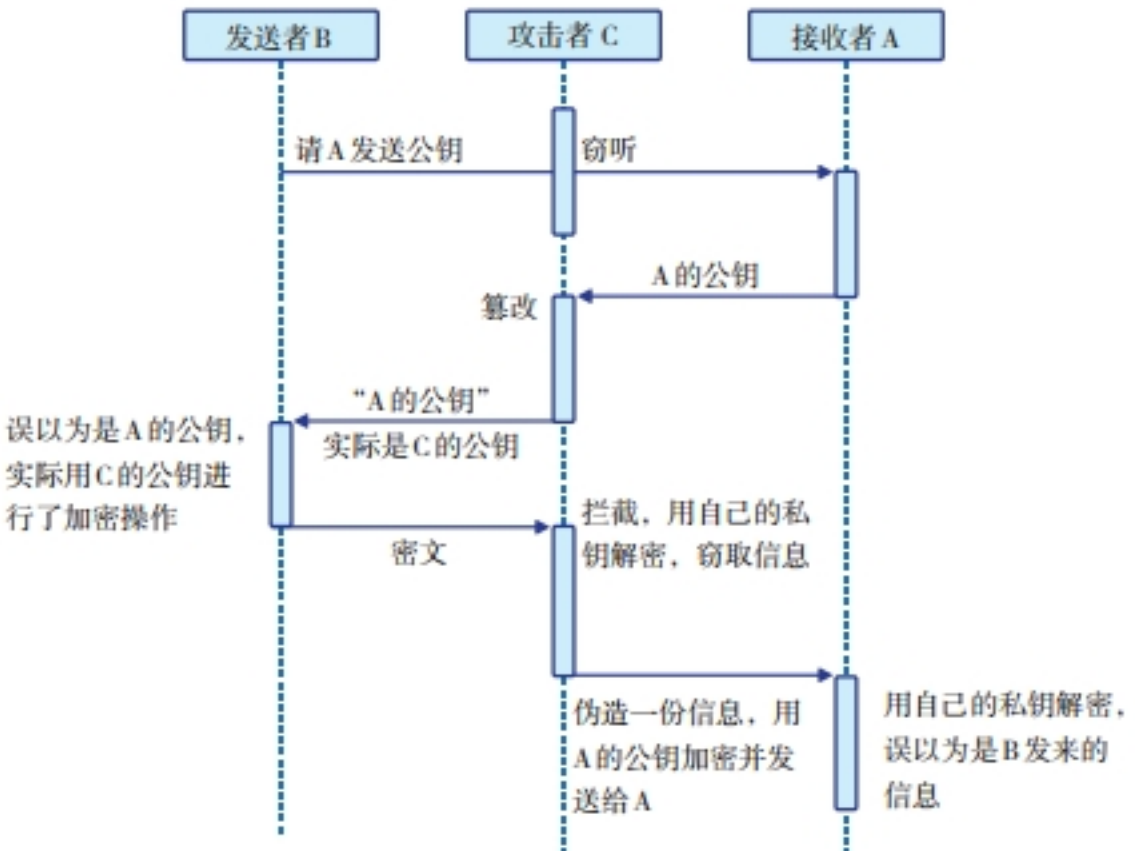


图 3.1.15　一种针对公钥的攻击

在图 3.1.15 演示的过程中，攻击者 C 悄悄截获了 A 发出的公钥，并把自己的公钥发给了 B；B 误以为是 A 的公钥，用其完成了加密操作，并发送密文；攻击者 C 截获 B 发出的密文，并用自己的私钥解开，从而实现窃听，甚至还可以伪造一份信息发给 A，从而进行欺诈。

把公钥交由权威的第三方，由第三方通过其他手段确认公钥的可靠性后，再放到网上供大家下载，可以比较好地解决公钥认证问题。具体过程见图 3.1.16。

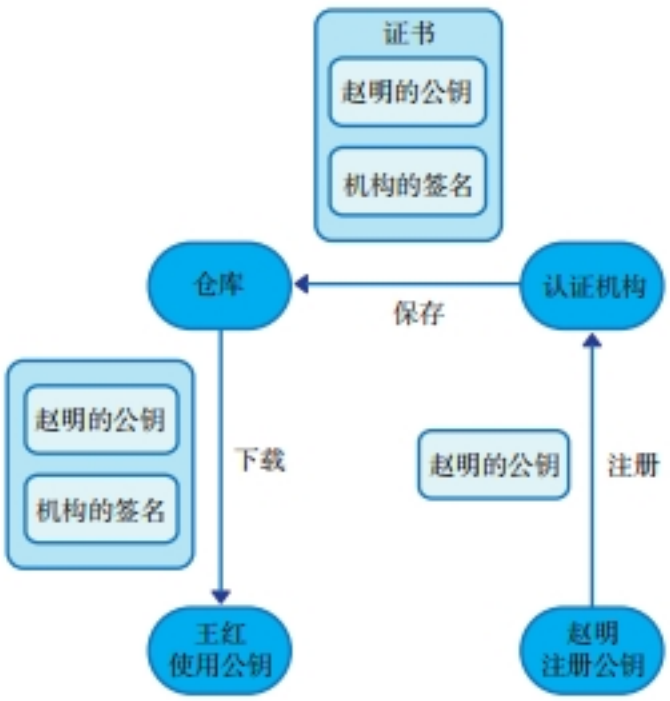


图 3.1.16　公钥认证过程示意图

微信公众号：电子课本大全

RSA算法原理简介

RSA算法是信息安全领域广泛使用的一种非对称密钥加密算法，其公钥和私钥的生成需要事先给出两个不同的大素数，然后通过一系列的计算得出两个互相关联的数对，分别作为公钥和私钥（图3.1.17）。

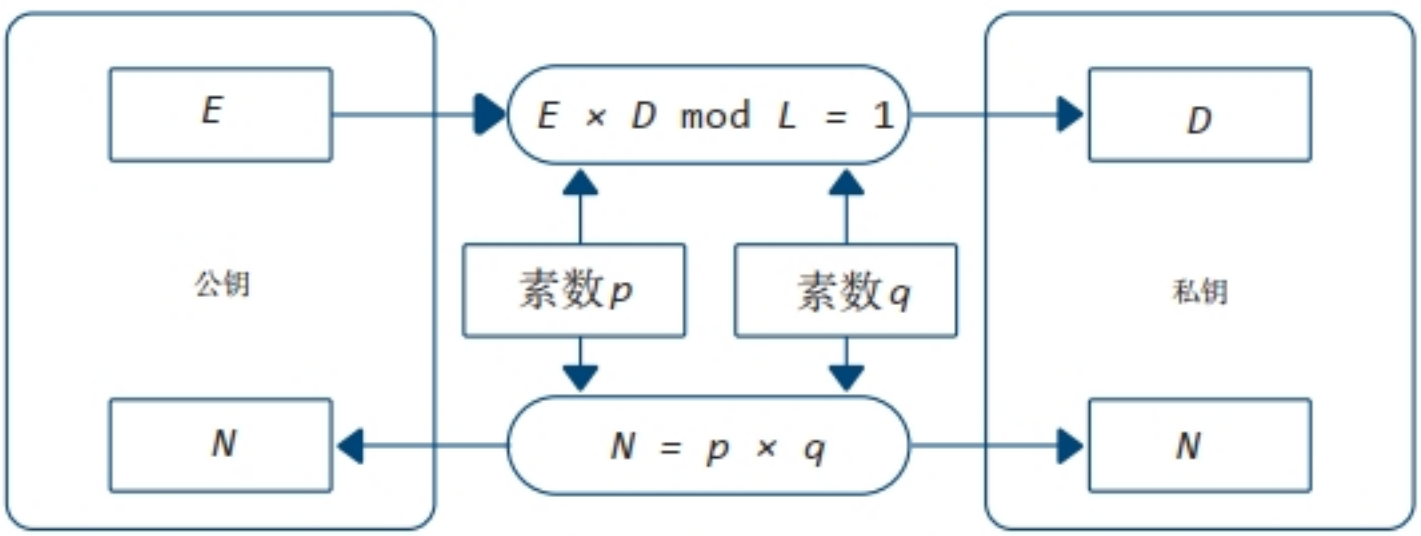


图3.1.17　RSA密钥生成示意图

产生公钥和私钥的过程，主要包括以下五步：

第一步，找两个素数p和q，求这两个数的乘积N。

第二步，求数L，L是$p-1$和$q-1$的最小公倍数。

第三步，找一个数E，要求E和L互质。

第四步，求数D，要求E和D的乘积除以L，余数是1。

第五步，把E和N作为一组，形成公钥；把D和N作为一组，形成私钥。

项目实施

体验RSA的工作原理

1. 启动Python的交互界面。
2. 选取两个素数，给变量p和q赋值。

```
>>> p=23
>>> q=29
```

3. 计算变量N。

```
>>> N=p*q
>>> print(N)
667
```

4. 计算变量L。

微信公众号：电子课本大全

```
>>> import math
>>> t=math.gcd(p-1,q-1)   #求p-1和q-1的最大公约数
>>> L=int((p-1)*(q-1)/t)  #求p-1和q-1的最小公倍数
>>> print(L)
308
```

5. 给变量E赋值。E和L互质，有很多种可能，随便选取一个，如5。

```
>>> E=5
```

6. 计算变量D。要求E和D的乘积除以L，余数是1。D也可能有多个，我们可选取一个，比如185。

```
>>> D=185
```

至此，生成公钥所需的变量E和N，生成私钥所需的变量D和N都已经确定了。

7. 加密。计算方法为：要加密的数的E次方除以N，并求余数。

```
>>> num=21
>>> enum=(num**E) % N
>>> print(enum)
60
```

8. 解密。计算方法为：密文的D次方除以N，并求余数。

```
>>> dnum=(enum**D) % N
>>> print(dnum)
21
```

9. 对比求得的余数和进行加密的数，看看是否完成了加解密过程。

公钥中包含了N，那是不是可以通过对N进行素因数分解，得到p和q，从而推导出私钥呢？在实际加解密时，p和q都是非常大的素数，可能在1 024比特以上。可以想象，其乘积N将是个非常大的整数。到目前为止，人们还没有找到能够对大整数进行质因数分解的高效算法。所以，即使公钥中有N，也很难通过质因数分解的方法获得p和q。正是因为这个原因，RSA很难被破解。

简单地说，RSA之所以安全，其背后依赖的原理是：求两个素数的乘积比较容易，反过来，对一个大整数进行素因数分解则非常困难。



实践活动

与同学一起体验RSA加密

仿照前面的操作过程，自行选择两个素数生成相应的公钥和私钥，然后把公钥交给旁边的同学，请他（她）对一个数进行加密操作，并把加密结果告诉你，你再利用手中的私钥进行解密操作。

微信公众号：电子课本大全

加密技术的混合使用

对称加密算法，加解密速度快，但密钥容易被窃听；非对称加密算法，发送的公钥不怕被窃听，但加解密的速度慢。

在实际应用中，人们常常混合使用这两种加密技术。对于一般的、长的信息交由AES等对称加密技术来处理，以适应网络交互的特点；而短的、关键性的信息用RSA等非对称加密技术进行处理（图3.1.18）。

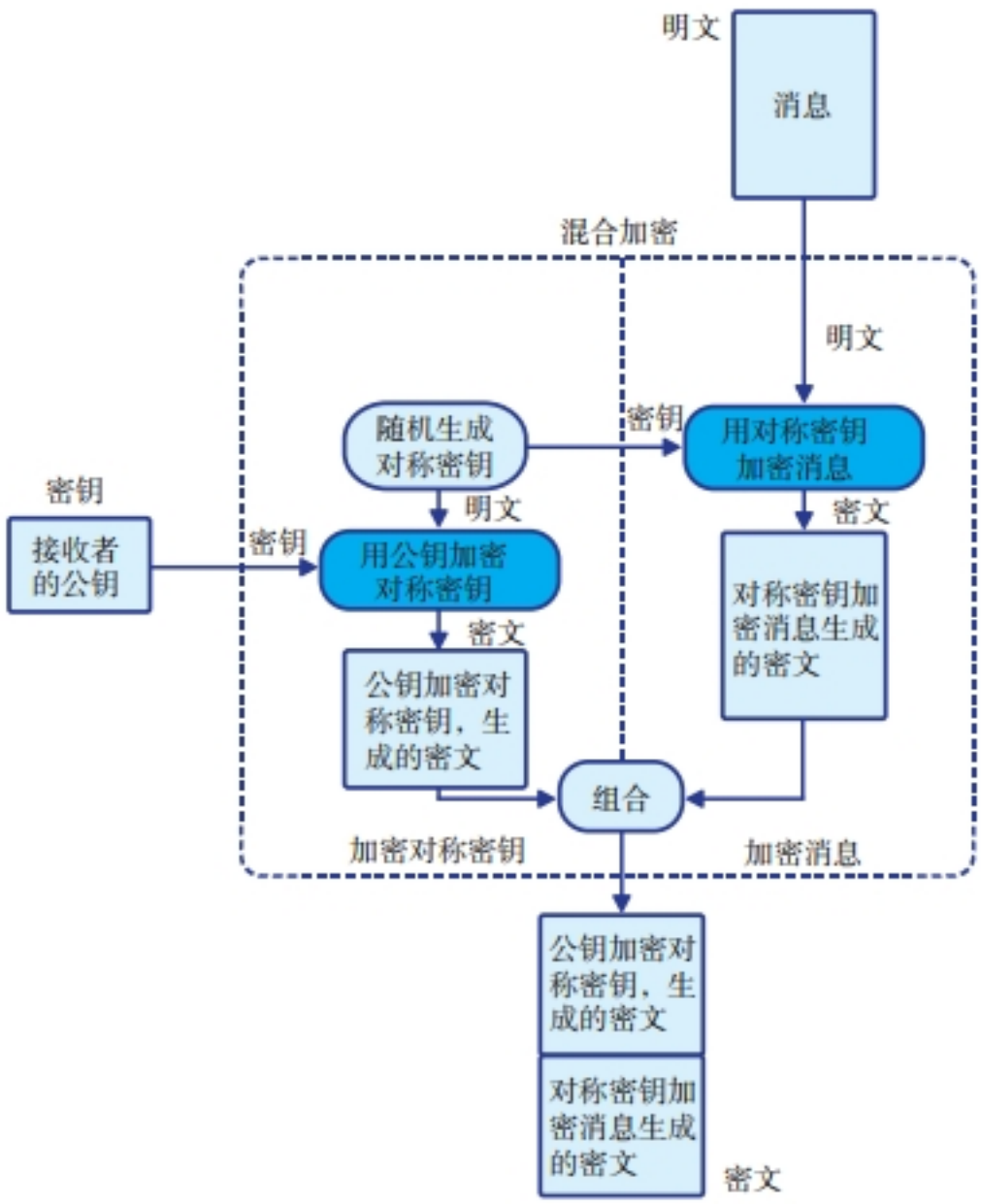


图3.1.18　混合加密过程示意图

在这个过程中，发送方利用对称加密速度快的特点，对消息明文进行加密操作；同时利用公钥为对称密钥进行了加密，这样就可以利用非对称加密系统的特点，解决秘钥传送可能被监听的问题。最后把两种密文组合起来，发送出去。

微信公众号：电子课本大全

解密时，先按照事先的约定，把组合的信息分解成密钥密文和消息密文；接着，用私钥解开密钥密文，获取对称密钥；最后，用对称加密密钥对消息密文进行解密操作（图3.1.19）。

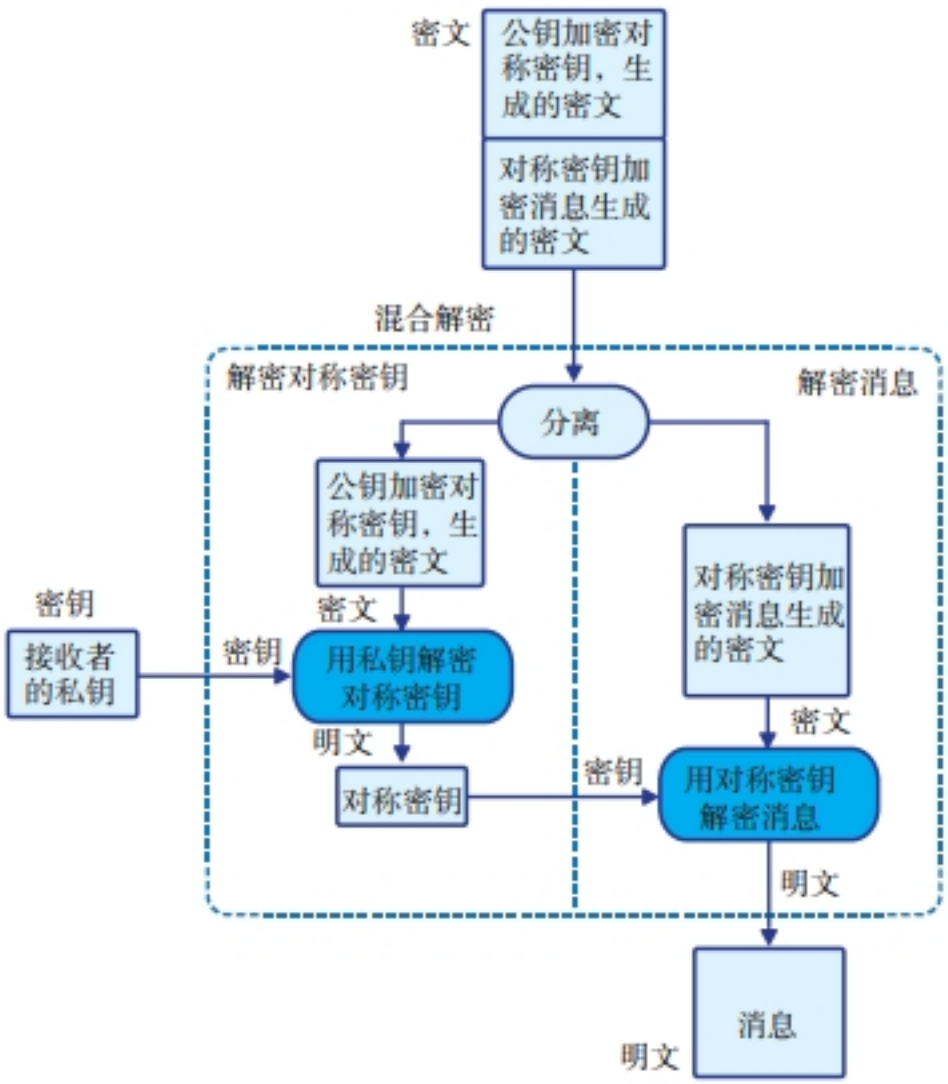


图3.1.19　混合解密过程示意图

实践活动

尝试混合加密

参考下面的代码和前面编写的程序，体验混合加密过程。

```
#引入编程库，用于随机生成指定长度的字符串
from Crypto.Random import get_random_bytes
#随机生成AES加密密钥
aes_key = get_random_bytes(16)
```

思考活动

分析混合加密的注意事项

1. 由于混合加密的过程中，对称加密密钥会用公钥进行加密，因此可以指定非常简单的密钥，如全是1、全是a等，这种做法可取吗？为什么？

2. 混合加密过程中，使用“随机生成的密钥”和使用“事先指定的密钥”这两种方法相比，你认为哪一种更好？为什么？

微信公众号：电子课本大全

情境2：

赵明收到了一份据称来自王红的加密文档和文档的MD5值，他用自己的私钥解密了文档，并重新计算MD5值进行了比对，一切看起来都很正常。

赵明正准备按文档要求行事，正好王红打来电话。在聊天中，赵明惊讶地发现，王红说自己没有发送过这份文档！

这一切是怎么回事呢？

在非对称加密过程中，王红如果想给赵明发送信息，就会用赵明公开的公钥加密，等赵明收到后，再用他的私钥解密（图3.1.20）。

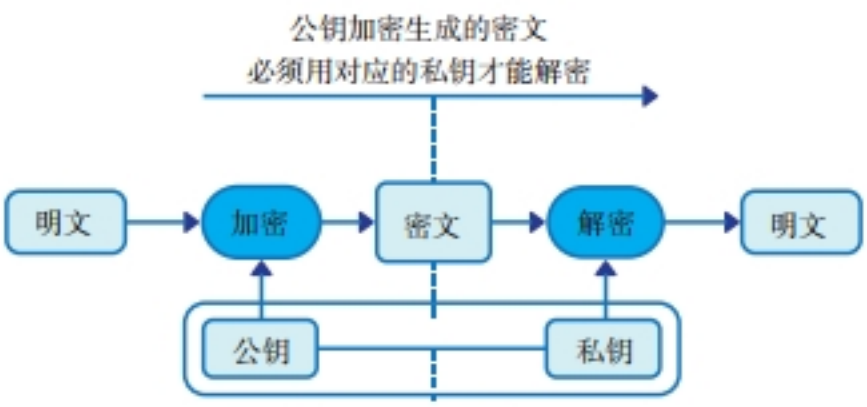


图3.1.20　加密与解密

公钥加密保证了信息的机密性、完整性等要求，但赵明的公钥是公开的，赵明无法确认信息肯定来自王红，王红也可以随时否认自己发送过信息。不过，如果公钥和私钥反过来用，就可以起到不一样的效果。

私钥是每个人单独保存的，因此王红用自己的私钥加密，相当于给文档添加数字签名；赵明用王红的公钥解密，相当于验证签名（图3.1.21）。

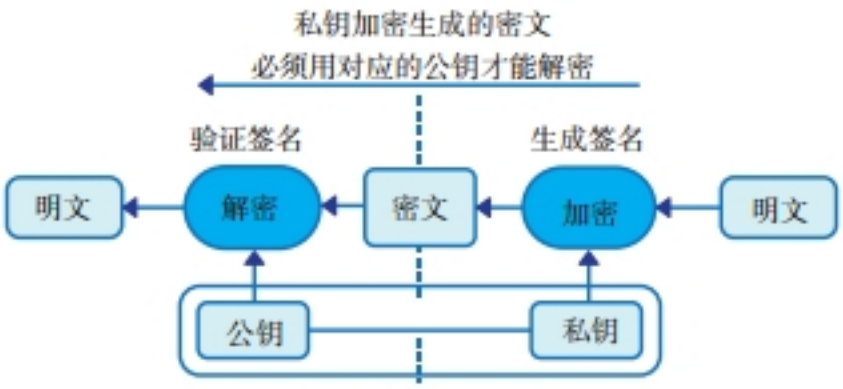


图3.1.21　数字签名

微信公众号：电子课本大全

数字签名能比较好地解决网络传输中信息的真实性问题，即能保证信息来自真实的发送者，而且发送者也没法否认自己发送过相关的信息。

项目实施

加密传输文稿

王红和赵明之间想通过网络安全传送比较大的文稿，通信过程既要保证机密性、完整性，同时也要保证真实性。请先判断已有方案是否合适，然后提出自己的解决方案。假定发送方为A，接收方为B。

【方案一】

操作：发送方A用自己的私钥加密，接收方B用A的公钥解密。

理由：加密后，密文不可阅读，保证了机密性，改动密文会造成解密过程失败，因而保证了完整性，同时私钥加密可以保证数据的真实性。

可行性：☐可行　☐不可行

解释：_____

【方案二】

加密过程：

①用接收方B的公钥对消息进行加密，得到密文1。

②用发送方A的公钥对密文1进行加密，得到密文2。

解密过程：

①用发送方A的私钥对消息进行解密，得到密文1。

②用接收方B的私钥对密文1进行解密，得到原文。

可行性：☐可行　☐不可行

解释：_____

【自定的方案】

加密过程：

_____

解密过程：

_____

解释：_____

加密技术与网络安全协议

默认情况下，网络以明文方式传输数据。用户输入的账号、密码等隐私信息，随时可能被人监听。现在主要有两种方法用于增强网络传输的安全性。

微信公众号：电子课本大全

一种是在现有传输层之上插入可以安全传输信息的层（图3.1.22），如SSL（secure socket layer，安全套接字层）。信息传输到这一层后，由相关软件自动进行加密和解密，从而实现安全传输。很多应用层的安全协议，如HTTPS（hypertext transfer protocol secure，超文本传输安全协议）就工作在SSL的基础上（图3.1.23）。



图3.1.22　SSL的位置

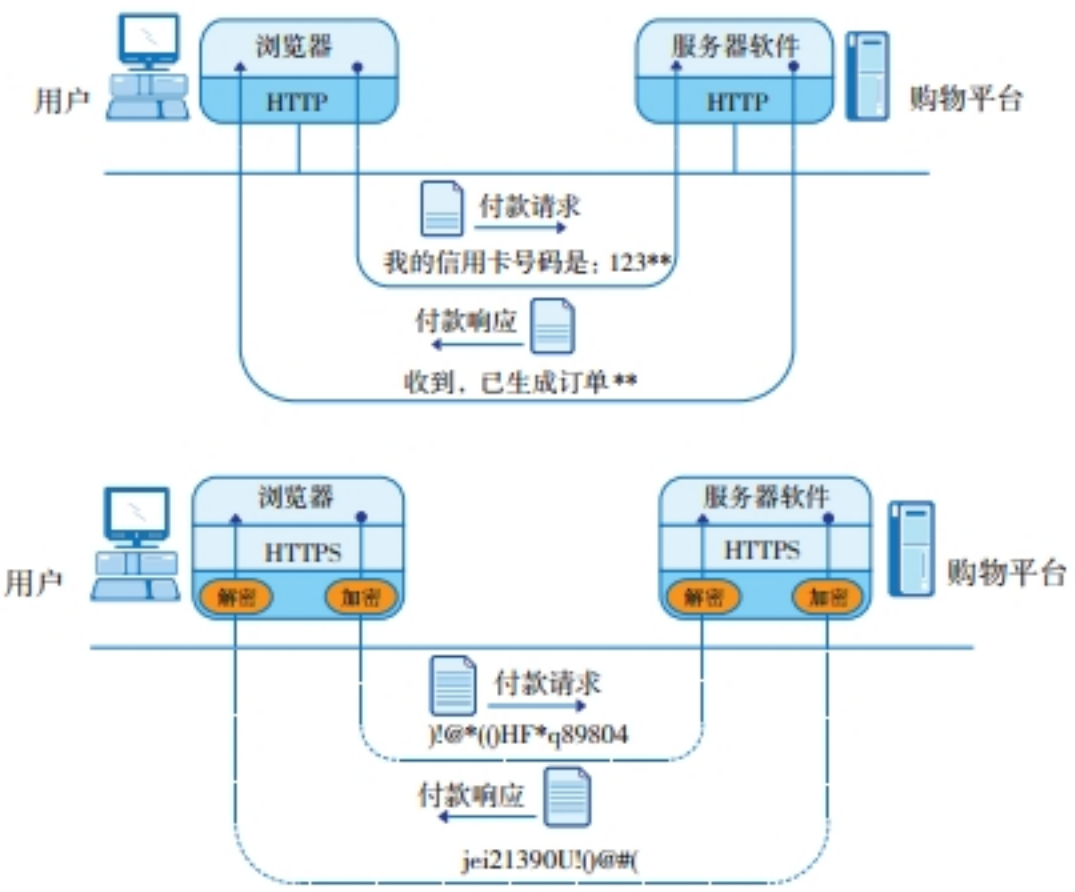


图3.1.23　HTTP与HTTPS

这个过程混合使用了多种安全技术。网站服务器会提前到管理机构申请公钥证书。实际运行时，服务器把证书和公钥发给用户；用户接收后，利用证书验证公钥是否合法，如果合法就随机生成一个对称密钥，并用服务器的公钥加密后传回服务器；服务器用私钥解密，获得对称密钥。此后，双方就可以利用随机生成的密钥实现加密通信了（图3.1.24）。

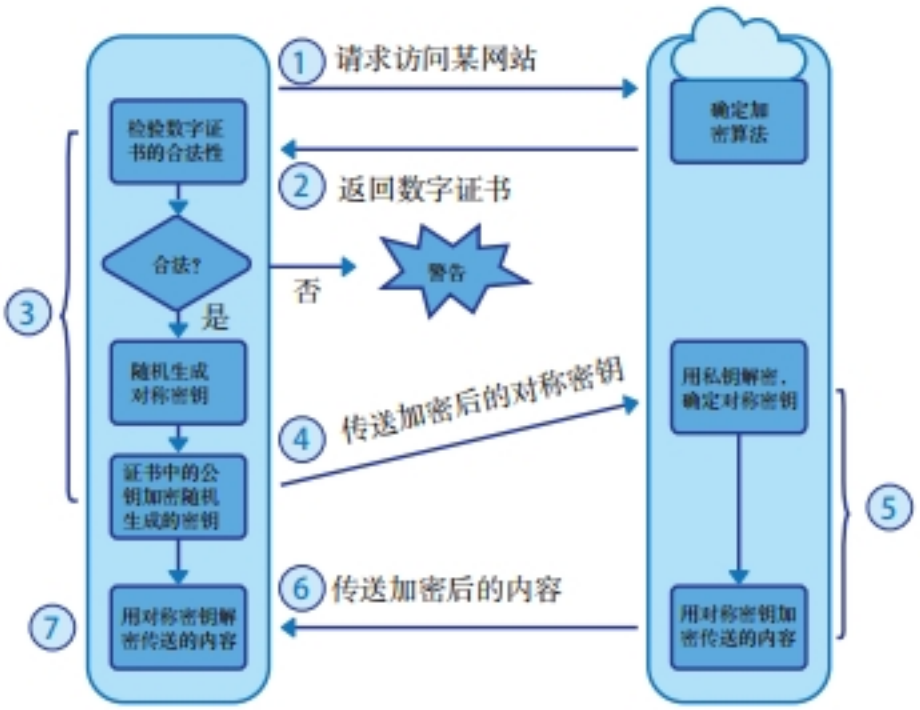


图3.1.24　HTTPS工作过程示意图

微信公众号：电子课本大全

项目实施

体验HTTPS服务

1. 改写下面的程序，用前面生成的私钥，制作服务器所需的证书。

```
from OpenSSL import crypto

#读取私钥
key_file=open("pr_key.bin", "rb")
key_data=key_file.read()
key=crypto.load_privatekey(crypto.FILETYPE_PEM,key_data)

#X509是一种证书格式
cert = crypto.X509()

#添加关于证书的信息
cert.get_subject().O = "XINHUA HIGH SCHOOL"
#证书对应的网站
cert.get_subject().CN = "127.0.0.1"
cert.set_issuer(cert.get_subject())

#设置证书的有效期
cert.gmtime_adj_notBefore(0)
cert.gmtime_adj_notAfter(60 * 60 * 24 * 10)

#添加密钥
cert.set_pubkey(key)
#签名
cert.sign(key, "MD5")

#保存证书文件
data=crypto.dump_certificate(crypto.FILETYPE_PEM, cert)
with open('abc.pem','wb') as f:
    f.write(data)
```

2. 打开能提供HTTPS服务的程序。

```
import http.server
import socketserver
import ssl

#端口
PORT=8000
Handler = http.server.SimpleHTTPRequestHandler
httpd = socketserver.TCPServer(("127.0.0.1", PORT), Handler)
print("serving at port", PORT)

#增加对SSL的支持，keyfile是私钥，cerfile是证书
httpd.socket = ssl.wrap_socket(httpd.socket, keyfile='pr_key.bin',
        certfile='abc.pem', server_side=True)
httpd.serve_forever()
```

3. 分别用http://127.0.0.1:8000和https://127.0.0.1:8000进行访问，看看访问时浏览器中的显示，并参照前面的讲解想一想，为什么会这样。

微信公众号：电子课本大全

使用HTTP协议访问时，会显示无法访问，而使用HTTPS协议时就可以访问（图3.1.25）。进一步查看会发现，这是因为所使用的证书没有经过专业机构的认证，因此浏览器认为证书存在造假的可能，不安全。但也可以看出，采用SSL，无论对于服务器端还是客户端来说，改动都不大，能够比较轻松地纳入已有的信息系统。



图3.1.25　访问刚刚创建的HTTPS服务器

另一种方法则关注于在IP层架构一个新的安全体系，如IPsec（internet protocol security，互联网络层安全协议）。IPsec提供了认证和加密两种安全机制。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；加密机制可以用来保证数据的机密性，防止数据在传输过程中被窃听。IPv6协议已经增加了对IPsec的支持。IPsec的实现方式可见图3.1.26。

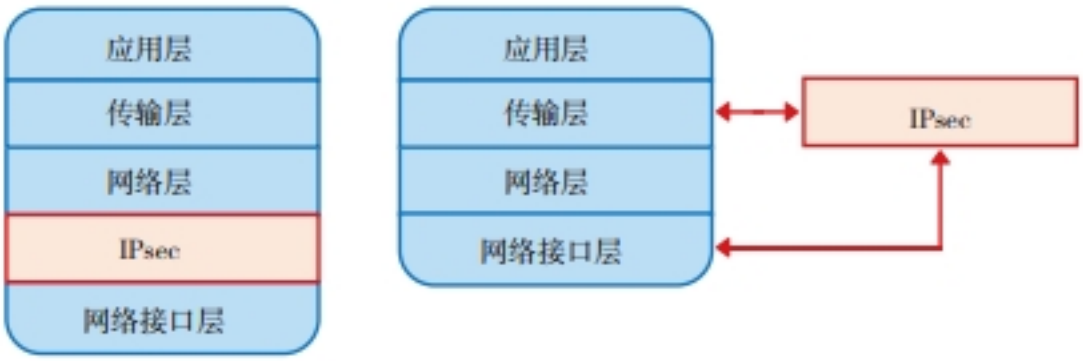


图3.1.26　IPsec的两种实现方式

思考活动

总结网络安全协议

你都知道哪些网络安全协议？这些网络安全协议的特点是什么？是否都用到了加密技术？

微信公众号：电子课本大全

常用的加密工具

PGP（pretty good privacy，颇好保密性）是目前广泛使用的加密技术体系，它混合使用了对称加密、非对称加密、数字摘要、数字签名等多种安全技术。

开源运动的软件工程师们根据PGP的相关标准，开发出了开源的GPG（GNU privacy guard）软件，随后又有人在GPG的基础上，开发出了带有操作界面的Gpg4win软件。

项目实施

体验GPG加解密过程

1. 启动Kleopatra软件，参考图3.1.27，生成个人使用的公钥和私钥，并选择合适的密码，保护存在本地的密钥对。



图3.1.27　创建个人密钥

2. 把公钥导出到文件中，或者上传到服务器上（图3.1.28）。

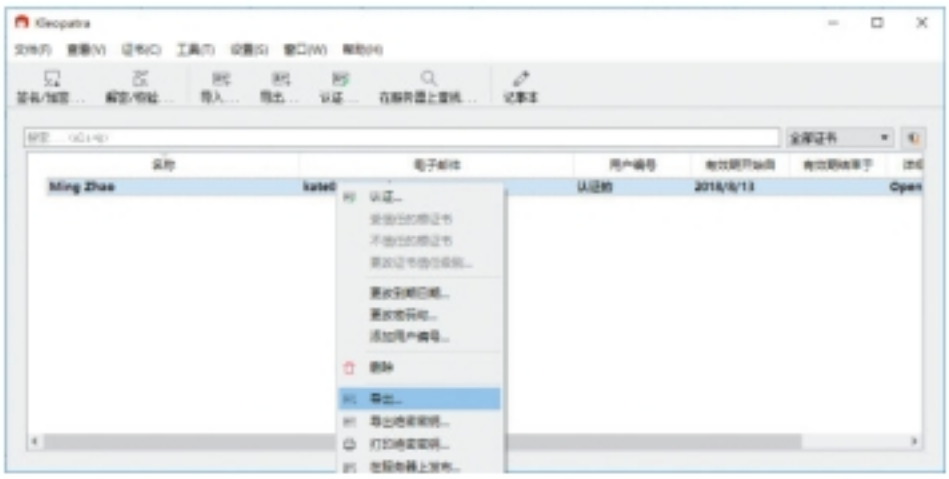


图3.1.28　发布自己的公钥

微信公众号：电子课本大全

3. 导入同学发来的公钥文件，或从服务器获取他们发布的公钥（图3.1.29）。



图3.1.29　获取他人的公钥

4. 选择导入的公钥，单击“认证”按钮，然后通过公钥的“指纹”，看看你所得到的公钥与某位同学实际发布的公钥是否一致。如果一致，就信任它（图3.1.30）。



图3.1.30　信任获取的公钥

5. 用同学的公钥文件进行加密操作，然后把加密后的文件，传给相应的同学。收到加密文件的同学，利用自己的私钥进行解密（图3.1.31）。



图3.1.31　加密与解密

思考活动

反思上述活动过程

- 为什么要对导入的公钥进行认证？上述操作中，对公钥认证的依据是什么？
- 上述操作过程使用了哪些安全相关技术？分别用来实现哪些功能？

微信公众号：电子课本大全

个人日常应用中，对每一个文件都人为加密比较烦琐，为此，人们开发出了很多可以自动加密硬盘的软件，如Windows系统自带的BitLocker。

项目实施

用BitLocker对移动硬盘进行加密

1. 选定移动硬盘，然后启用BitLocker加密功能，见图3.1.32。

2. 根据屏幕中的提示，选定加密方式、恢复密钥的保存方式、是否对整个盘进行加密等选项后，计算机系统就会开始加密操作（图3.1.33）。



图3.1.32　启动BitLocker加密功能

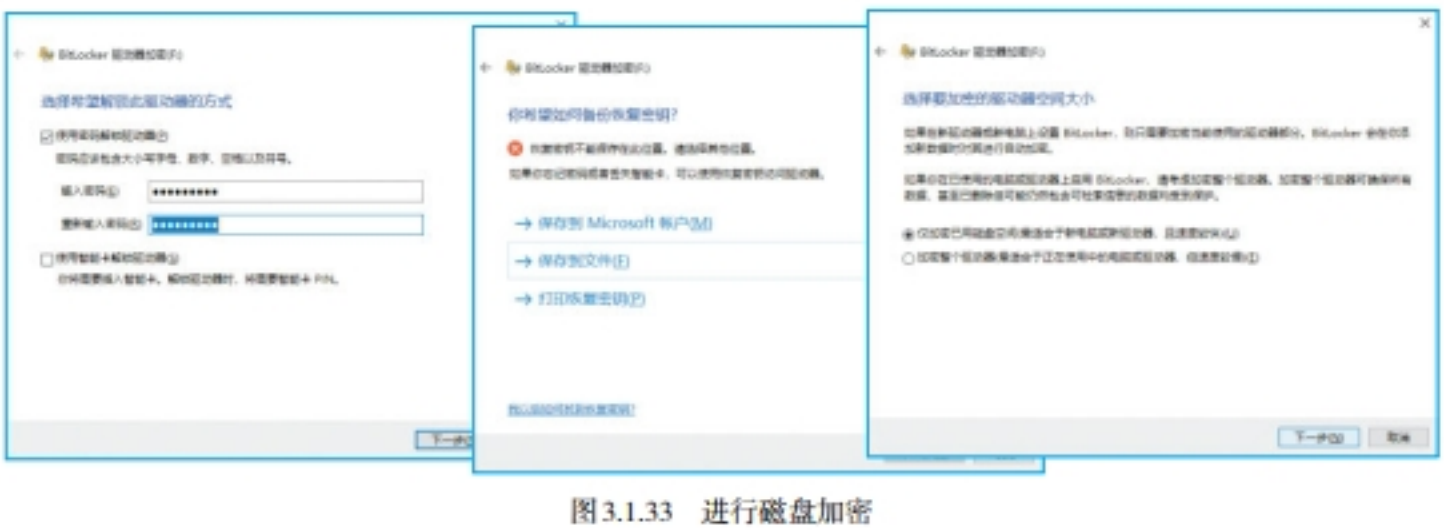


图3.1.33　进行磁盘加密

3. 拔下移动硬盘，然后再插上去，计算机就会提醒，需要输入密码才能使用（图3.1.34）。此后，再使用这个移动硬盘，计算机就会自动完成加密或解密操作。

提示：要保管好第2步操作得到的恢复密钥，一旦关于某个移动硬盘的BitLocker密码忘记了，就只能依靠它进行恢复。



图3.1.34　磁盘解密

思考活动

使用BitLocker的注意事项

王红启用了BitLocker来保护移动硬盘中的数据，为了更好地保护存有恢复密钥的文件，她决定把恢复文件也放到那个移动硬盘中。赵明听说后，连忙对王红说："不能那样做！"

赵明这么说有道理吗？为什么？

微信公众号：电子课本大全

3.1.4 身份认证

日常生活中经常要输入各种密码，如即时通信软件的登录密码、使用手机时的手势密码、使用云服务的密码等（图3.1.35）。



图3.1.35 输入密码

事实上，这时候输入的密码主要用于身份验证。也就是说，服务器接收到密码（通常是密码的数字摘要）后，并不是用于加密或解密，而是与数据库中已有的信息进行比对，信息符合的才允许进入系统，使用相应的信息资源。基于密码的认证，是使用最普遍的认证方式。



有一些信息系统进行用户认证时，用户光有账号和密码还不行，还得提供特殊的认证文件，或者磁卡、U盾等物理设备。此外，还有一些基于生物特征的认证方式，如指纹认证、声音认证、虹膜认证等（图3.1.36）。





图3.1.36 身份认证

微信公众号：电子课本大全

思考活动

私钥是否能用来验证身份

回想前面所学的知识，说一说非对称密钥加密中的私钥，是否可以用来作身份验证的依据？为什么？

3.1.5 防火墙

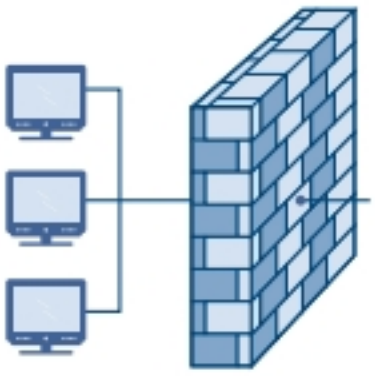


图3.1.37 防火墙示意图

防火墙这个概念来自古代。当时人们为防止火灾的发生和蔓延，会将坚固的石块堆砌在木制房屋周围，这种防护性的墙被称为防火墙。现在，很多机构或单位会在内部网络和互联网之间建立一道维护安全的屏障，这个屏障的作用是阻断来自外部网络的威胁和入侵（图3.1.37）。

防火墙可以由软件构成，也可以由硬件构成。安装了防火墙，可以使系统具备网络访问控制功能，从而抵御外来的攻击，过滤禁止访问的站点，提高系统的安全性。家庭和个人使用的防火墙一般都是软件防火墙，常用的有《费尔个人防火墙》《瑞星个人防火墙》等（图3.1.38）。



图3.1.38 两种个人防火墙软件

安装了防火墙软件后，可以规定哪些程序能够访问网络，哪些程序不能，这些规定也叫“网络访问规则”。使用不在网络访问规则中的软件进行网络通信时，计算机会弹出一个询问窗口，让操作者决定是否允许它访问网络。这样，通过防火墙软件，可以阻止那些不经用户同意就悄悄进行网络通信的程序，如“木马”程序。但防火墙软件有时也会因误判而阻止正常的网络访问，这时需要适当调整防火墙软件中的网络访问规则。

事实上，前面组网时使用的路由器，也能起到防火墙的作用。路由器通常运行在内网和外网之间，当路由器接

微信公众号：电子课本大全

收到内网计算机访问某个站点的请求后，就会检查这个请求是否符合规定，如果符合，就会去相应站点取回所需信息再转发给相应的计算机。

也就是说，路由器会像一堵墙一样挡在内网和外网之间，一般情况下，从外部只能看到路由器而无法获知内网的资源。

项目实施

设置防火墙中的网络访问规则

1. 打开《瑞星个人防火墙》软件的窗口，然后打开“访问控制”选项卡。

2. 选定一条访问规则，单击“修改”按钮，在“常规模式”下拉列表中选定“放行”“禁止”或“自定义规则”选项，调整访问规则（图3.1.39）。



图3.1.39　操作示意图

3. 根据实际需要，调整其他的网络访问规则。然后运行相应的程序，看看防火墙软件是否按照规则进行阻挡或放行。

阅读拓展

防火墙软件的基本功能

从总体上看，防火墙软件通常具有以下五大基本功能：

- 过滤进出网络的数据；
- 管理进出网络的访问行为；
- 封堵某些禁止的业务；
- 记录通过防火墙的信息内容和活动；
- 遇到网络攻击，及时显示警告信息。

微信公众号：电子课本大全

项目实施

网络安全攻防战

任务目标：防守方要快速传送大量的文件，但传输网络并不安全。防守方要设计一个传输策略，尽可能保证信息传输的完整性、机密性和真实性。

攻防过程：防守方先提出一个方案，然后由攻击方尝试攻击，列举攻破或驳回的理由。如果防守策略被攻破或被驳回，则防守方修改传输策略，再进行一个回合；如果攻击理由不充分，则由攻击方继续尝试。直到一方认输为止。

守方条件：拥有不可被破解的加密算法、摘要算法，但每次最多只能在现有安全体系的基础上，增加或撤换一项技术。备用的安全技术罗列如下：

☐ 数字摘要 ☐ 对称加密 ☐ 非对称加密

其他：_____

攻方条件：可以监听网络传输的所有信息。

---

1. 参照下面的提示，攻防双方开始网络安全的攻防战。

回合一：

防1：【技能】给要传输的文件都增加数字摘要。

攻1：【攻破】通过窃听，获得所有的文件内容。

回合二：

防2：【技能】增加RSA加密技术，对文件进行加密。

攻2：【驳回】这种加密技术速度比较慢，不适于快速加密大量的文件，驳回。

回合三：

防3：【技能】改为采用对称加密技术，对文件进行加密。

攻3：【质询】对称加密密钥如何传输？

防3：【回复】现有条件下，只能通过网络传输。

攻3：【攻击】窃听对称加密密钥，从而窃听文件。

防3：【回击】加密密钥是加密后才传输的。

攻3：【攻击】不管涉及几层加密，必然可以通过窃听，得到加密密钥。

回合四：

……

2. 根据网络攻防战的过程，体会网络安全技术的特点和应用场合。

微信公众号：电子课本大全

练习提升

1. 参照图3.1.40，谈一谈自己对内容加密密钥（contents-encrypting key，CEK）和密钥加密密钥（key-encryption key，KEK）的理解，说一说它们的作用以及可能采用的加密技术是什么。

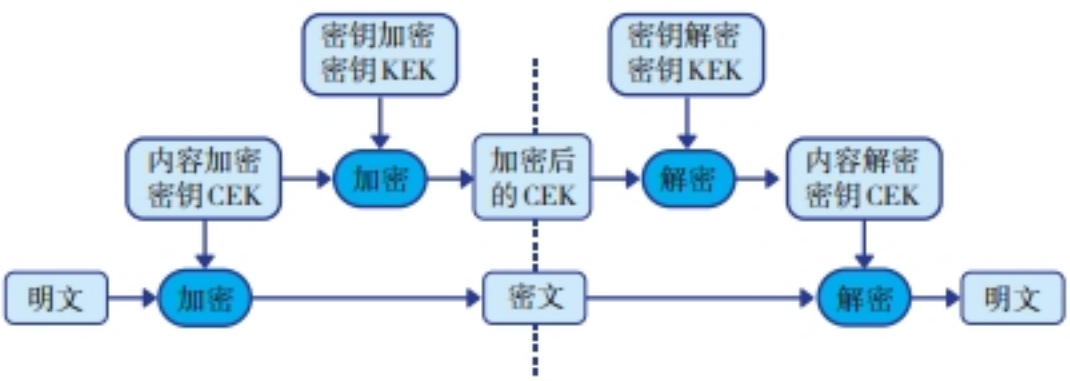


图3.1.40　CEK与KEK

2. 密码的作用是什么？为什么网站通常要求密码具有一定的长度和复杂度？

3. 某人说，他的资料都已经加密好了，密钥就是手机中拍摄的一张关于名画《星空》的照片。根据这个人的描述，回答以下问题。

- 手机拍摄的照片能用来作为密钥吗？为什么？
- 用自己的手机重新去拍一下《星空》，或者下载相关的图像，能用来解密吗？
- 这个人采用的加密手段，有可能面临什么风险？哪些人有可能解密他的资料？

微信公众号：电子课本大全

3.2 网络资源分享

学习目标 ▶▶▶

- 能识别网络资源的类型。
- 能利用适当的工具在计算机和移动终端生成和分享网络资源。
- 提高分享资源时的安全意识。

体验探索

回顾网络分享

萧伯纳曾说："如果你有一个苹果，我有一个苹果，彼此交换，我们每个人仍然只有一个苹果；如果你有一种思想，我有一种思想，彼此交换，我们每个人就有了两种思想，甚至多于两种思想。"这句话形象地描述了信息所具有的共享性特征。网络是目前人们所发明的最便捷的信息分享途径（图3.2.1）。



图3.2.1　常用的分享信息的方式

回忆你用网络分享过哪些资源，常用的分享手段都有哪些。

3.2.1　网络资源简介

在日常使用中，网络资源主要指网络信息资源，也就是通过计算机网络可以利用的各种信息资源的总和。

微信公众号：电子课本大全

很多人把网络资源分为图、文、声、像等类型。比如，使用搜索引擎时，很多时候就在搜索某种特定类型的资源（图3.2.2）；但更多的时候，人们获取的是由多种媒体组成的综合型信息资源（图3.2.3）。



图3.2.2　单一媒体型



图3.2.3　综合型

也可以按网络协议，将网络资源分为万维网资源、FTP网络资源、telnet网资源等。其中，万维网基于HTTP协议，目前使用最为广泛；FTP网基于FTP协议，主要用于文件传输，可用来共享各种文件；telnet网基于telnet协议，可借助网络中的计算机完成计算任务。

还可以按来源，把网络资源分成政府信息资源、企业信息资源、公众信息资源等（图3.2.4）；按主题，分为关于旅游的资源、关于学习的资源、关于体育运动的资源等。



图3.2.4　按信息来源分

除了信息资源外，IP地址数量、域名数量、国际出口带宽等可以视为网络基础资源。网络基础资源是信息社会的“大动脉”，是关乎建设网络强国的战略性资源。经过多年的努力，我国网络基础资源建设进步显著。表3.2.1展示了近年来我国网络基础资源的建设情况。

表3.2.1　互联网基础资源发展

项目	2017年12月	2018年12月	年增长量
IPv4/个	338 704 640	338 924 544	219 904
IPv6/（块/32）	23 430	41 079	17 649
域名/个	38 480 355	37 927 527	−552 828
CN域名/个	20 845 513	21 243 478	397 965
国际出口带宽/Mbps	7 320 180	8 946 570	1 626 390

来源：中国互联网络信息中心

微信公众号：电子课本大全

3.2.2 网络资源分享实例

通过网络分享资源的方式有很多，如把信息发布到微博或朋友圈中，用邮件传送图文资料等。实际使用时，应当根据资源和应用场景的要求，选择适当的方式。

分享文件

情境1：

王红所在小组的几位同学想分享他们手机、计算机中的照片、视频等，他们列出了几种方案：

- 通过移动硬盘复制文件；
- 通过局域网内的共享文件夹共享文件；
- 发到QQ群或微信群中；
- 发到云盘中，然后创建加密分享链接。

你认为哪种方式更合适？为什么？

网络发展过程中，出现过不少分享文件的方式，如专门用于传送文件的FTP服务、电子邮件附件、局域网共享文件夹等。近年来，网络云盘服务逐渐流行。通过云盘，不仅个人的各种信息终端可以方便地分享各种文件，而且还可以与其他人的各种设备分享。

项目实施

利用云盘分享文件

1. 小组同学选定一个网络云盘服务，并分别完成账号注册等必要操作。

2. 在自己的不同设备间实现文件分享，并描述自己的操作步骤（图3.2.5）。

3. 尝试与小组成员之间分享一个比较大的视频文件。注意，要创建加密的分享链接。

4. 把视频文件改名后再次上传，看看能否实现秒传，并讨论一下，秒传背后的机理是什么。

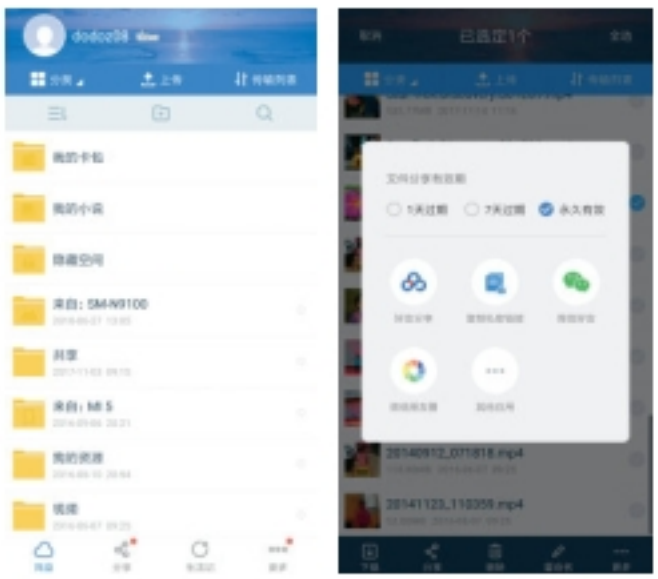


图3.2.5 云盘共享文件

微信公众号：电子课本大全

基于二维码的分享

情境2：

王红想在学校活动中和同学们分享她制作的关于保护濒危动物的宣传片，并已经利用云盘服务设好了共享链接。她发现，向好友发布这个消息比较容易，可以利用QQ等工具把网址传给对方，但如何才能让不熟悉的同学，特别是使用智能手机的同学，方便地打开链接呢？

把指定网址打印或展示出来，让使用手机的人照着网址输入访问，虽然可行，但显然很不方便。一个更方便的办法是，利用二维码来实现网址的分享。

信息设备扫描二维码后，可以把它转换成二进制数据，从而获取其中的信息。目前，经常可以见到各种基于二维码的应用（图3.2.6）。





图3.2.6　二维码的使用

生成二维码的方式有很多，可以用专门的软件，可以借助生成二维码的网站，还可以采用编程的方式。

项目实施

运行程序生成二维码

1. 打开生成二维码的程序。

```
#引入编程库
import qrcode
#要转换成二维码的内容
s='扫码须谨慎！'
#生成二维码
img = qrcode.make(s)
#保存二维码
img.save("ewm01.png")
```

2. 用智能手机扫描生成的二维码，观察扫描结果。
3. 把云盘分享文件的网址转换成二维码并扫描，观察扫描结果。

微信公众号：电子课本大全

分享计算资源

通过网络，不仅可以分享文件，分享存储空间，分享打印机等硬件设备，还可以分享计算机的计算资源，也就是利用网络，使用别的计算机的计算能力来完成计算任务。下面将要介绍如何用Python中的dispy库来组建和使用分布式计算系统。

项目实施

组建分布式计算系统

1. 每一位同学查看自己所用计算机的IP地址，并记录下来。

2. 进入安装Python的目录，然后执行“python Scripts\dispynode -c 1 -i [IP地址] --clean ”命令，窗口显示类似图3.2.7。

```
d:\CODE\python>python.exe Scripts\dispynode.py -c 1 -i 10.50.16.99 --clean

Reading standard input disabled, as multiprocessing does not seem to workwith reading input under Windows
2018-07-19 16:06:11 dispynode - dispynode version: 4.8.7, PID: 26572
2018-07-19 16:06:11 pycos - version 4.7.5 with IOCP I/O notifier
2018-07-19 16:06:12 dispynode - "pepxxjs-cll" serving 1 cpus
```

图3.2.7　执行命令

运行命令后，所用的计算机就会提供一个CPU充当运算资源。大家都这样做，就可以组成含有多个运算资源的分布式计算系统，系统中的每一台计算机就是一个计算节点。接下来，学习如何使用这个计算网络进行计算。

项目实施

寻找素数

1. 打开名为disp_c.py的文件，观察并熟悉其中各段代码的功能。

```
# 编程库
import dispy,socket

# 求指定范围内的素数
def compute(min_n,max_n):
    import socket,math
    host = socket.gethostname()      # 获取节点计算机的名称
    num=[];
    if (min_n<2):min_n=2
    for i in range(min_n, max_n):    # 查找素数
        for j in range(2,i):
            if(i%j==0):break
        else:
            num.append(i)
    return (host,num)                # 返回计算结果
```


微信公众号：电子课本大全

```
# 显示计算结果
def status(status, node, job):
    if status == dispy.DispyJob.Finished:
        print(' 素数 %s: %s' % (job.id, job.result))
    elif status == dispy.DispyJob.Terminated:
        print('sha1sum for %s failed: %s' % (job.id, job.exception))

# 获取本机 IP
ip = socket.gethostbyname(socket.gethostname())
# 组织参与计算的计算机
cluster = dispy.JobCluster(compute,ip_addr=ip,cluster_status=status)
# 查看系统中的计算节点
cluster.print_status()

# 把计算 60000 以内的素数这一任务，分为 10 段进行分配
for i in range(0,10):
    cluster.submit(i*10000,(i+1)*10000)

# 关闭集群
cluster.close()
```

2. 运行程序，观察屏幕上的显示。

```
                     Node|   CPUs|   Jobs|      Sec/Job|      Node Time Sec
-----------------------------------------------------------------------------
10.50.16.21 (class1-21)   |     1 |     0 |       0.000 |              0.000
10.50.16.24 (class1-24)   |     1 |     0 |       0.000 |              0.000
10.50.16.10 (class1-10)   |     1 |     0 |       0.000 |              0.000
10.50.16.15 (class1-15)   |     1 |     0 |       0.000 |              0.000
10.50.16.30 (class1-30)   |     1 |     0 |       0.000 |              0.000
10.50.16.08 (class1-08)   |     1 |     0 |       0.000 |              0.000
10.50.16.16 (class1-16)   |     1 |     0 |       0.000 |              0.000
......
素数 None: ('class1-16', [2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43,
47, 53, 59, 61, 67, 71, 73, 79, 83, 89, 97, 101, 103, 107, 109, 113, 127,
131, 137, 139, 149, 151, 157, 163, 167, 173, 179, 181……
素数 None: ('class1-08', [10007, 10009, 10037, 10039, 10061, 10067, 10069,
10079, 10091, 10093, 10099, 10103, 10111, 10133, 10139, 10141, 10151, 10159,
10163, 10169, 10177, 10181, 10193, 10211, 10223, 10243, 10247……
......
```

3. 看看系统中都有哪些计算节点，又有哪些计算节点参与了自己提交的寻找素数的计算任务。

在上面的运算过程中，默认把系统中的所有计算节点都用来计算素数，从而形成了一个寻找素数的计算网络。实际运算时，寻找素数的过程被分成了10段，并被自动分配到计算网络的空闲节点上。

也就是说，在同一时间，这个分布式计算系统的不同计算节点，会在不同段落中寻找素数。通过这种方式，可以有效减少复杂计算所需的时间。

微信公众号：电子课本大全

实际使用时，可以把计算网络中的计算节点组织起来，用来完成不同的计算任务。

项目实施

继续计算其他数学问题

1. 参照下列代码，再创建几个计算函数。

```
# 寻找指定范围内的完全数（一个数等于自身以外的因数之和，如 6=1+2+3）
def compute2(min_n,max_n):
    import socket
    host = socket.gethostname()    # 获取节点计算机的名称
    num=[];
    if (min_n<1):min_n=1
    for i in range(min_n,max_n):
        s=0
        for k in range(1,i):
            if i%k==0:s=s+k
        if (i==s):num.append(i)
    return (host,num)

# 求取指定范围内的平方回文数（一个数是回文数，同时还是其他数的平方，如 121=11×11）
def compute3(min_n,max_n):
    import time,socket,math
    time.sleep(1)
    host = socket.gethostname()
    num=[]
    if (min_n<1):min_n=1
    for n in range (min_n,max_n):
        a = int(math.sqrt(n))      # 获取平方根并取整
        if a*a!=n:continue;        # 判断是否为平方数
        sq = str(n)                # 数字转换成字符串形式
        if (sq == sq[::-1]):       # 正序字符串与倒序字符串相比较，相同则为回文数
            num.append(n)
    return (host,num)
```

2. 参照下列代码，修改程序，把不同的计算节点组织起来完成不同的计算任务。

```
# 指定计算网络中的一些计算节点
nodes=['10.50.16.99','10.50.16.204']
# 用指定的多个节点进行计算
cluster = dispy.JobCluster(compute2,nodes=nodes,ip_addr=ip,cluster_
status=status)
```

3. 修改完毕后，同学们同时运行不同程序，用各自指定的计算节点完成不同的计算任务，体会分布式计算系统的好处。

思考活动

总结分布式计算的特点

通过前面的项目活动，你觉得分布式计算有哪些特点？通过分享计算资源，能完成什么类型的任务？

微信公众号：电子课本大全

在现实操作中，研究人员利用分享计算资源的原理，创建了很多用于科学研究的分布式计算项目。简单地说，分布式计算就是把大的计算任务分割成小的任务单元，并通过网络分发给各节点进行计算，各节点完成计算后，再通过网络把各自的计算结果反馈给服务器。

BOINC（Berkeley Open Infrastructure for Network Computing，伯克利开放式网络计算平台）是目前主流的分布式计算平台之一。下面以这个平台为例，介绍当前正在利用分享计算资源进行的科学研究。

如果利用软件，把网络中不同设备的存储空间组合起来，就可以形成分布式存储系统，这是一种分享存储资源的方式。

项目实施

参与分布式科学研究项目

1. 启动软件BOINC Manager。

2. 增加一个项目，如计算素数的项目PrimeGrid，然后根据软件的提示，进行登录或账号注册等操作。操作后，软件就会自动把所用的计算机变成计算网络中的一个节点，并自动为项目提供必要的运算资源（图3.2.8）。



图3.2.8　参与科学运算

3. 再浏览几个计算平台中的项目，如寻找外星人的项目SETI@home、模拟宇宙运行的项目Universe@Home、研究蛋白质的项目Protein Folding等，并适当加入一两个感兴趣的项目。

不难发现，一个真实可用的分布式系统，要做的工作比前面的项目活动实验复杂得多，通常还要包括项目选择、用户身份认证等操作。

微信公众号：电子课本大全

思考活动

网络分享二三事

1. 以“分布式计算的安全性”为关键词进行搜索，分别从普通参与者和项目组织者的角度，了解采用分布式计算这种方式时，各自可能面临的风险是什么，又该分别采取哪些应对措施。

2. 下列说法对吗？为什么？

（1）共享上网是一种网络资源分享过程，这个时候大家分享的是带宽。

（2）DHCP（dynamic host configuration protocol，动态主机配置协议）服务是一种网络资源分享服务，分享的是IP地址资源。

3. 你还知道哪些分享网络资源的服务？它们分享了什么资源？

项目实施

网络资源分享总结报告

完成项目报告，检查自己这个阶段的学习情况。

报告人：_____　　时间：_____

主题：认识网络分享。

1. 总结网络资源的分类方式和具体的类型。

按_____分类，包括：_____

按_____分类，包括：_____

按_____分类，包括：_____

2. 总结分享文件的方法，以及这些方法的优缺点。

☐ 局域网共享，优缺点：_____

☐ _____，优缺点：_____

☐ _____，优缺点：_____

☐ _____，优缺点：_____

☐ _____，优缺点：_____

3. 总结二维码的作用，以及二维码分享的应用场景。

_____

_____

4. 总结数字摘要、加密等安全技术在网络资源分享过程中的作用。

_____

_____

微信公众号：电子课本大全

练习提升

1. 王红的爸爸想跟大家分享他的研究成果，但又担心这些研究成果会被人篡改，误导他人。对此，你有什么办法吗？

2. 赵明只想和朋友分享、交流自己的学习计划，他应该采用哪种方式分享资源？为什么？

□ 微博 □ 微信朋友圈 □ QQ群 □ 博客 其他：_____

3. 下面的说法，你认为哪个对？为什么？

（1）二维码中可能隐藏病毒或木马程序，所以不能随意扫描。

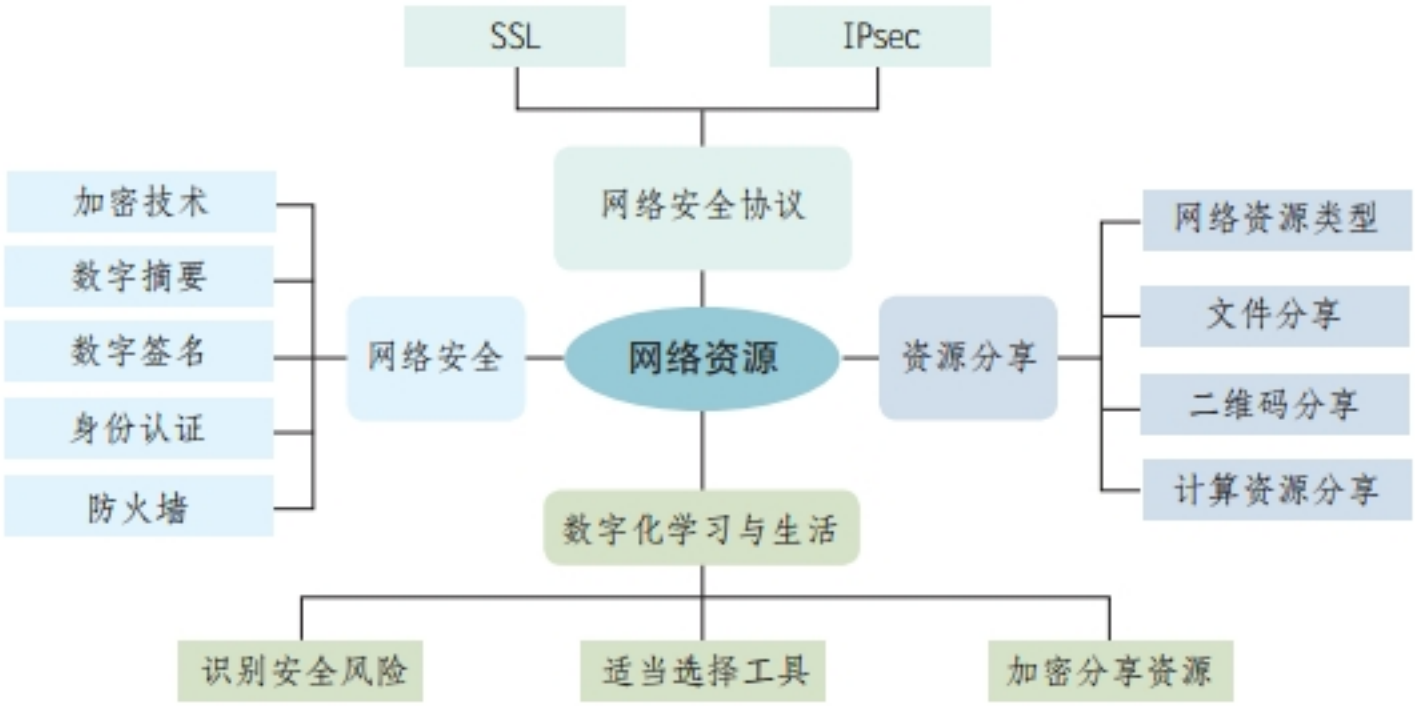
（2）二维码中可能隐藏病毒或木马程序的超链接，诱导人在不经意间下载安装，所以不能轻易扫描。

4. 云存储服务可以帮助大家方便地存储和分享资源，同时也很容易成为侵犯知识产权的重灾区。请根据你的使用体会，谈一谈这个说法是否有道理。

微信公众号：电子课本大全

总结评价

1. 下图展示了本章的核心概念与关键能力，请同学们对照图中的内容进行总结。



2. 根据自己的掌握情况填写下表。

学习内容	掌握程度		
网络资源的类型	□ 不了解	□ 了解	□ 理解
网络分享的方式	□ 不了解	□ 了解	□ 理解
利用适当的工具生成和分享网络资源	□ 不会	□ 会	□ 熟练
常用网络安全协议的作用	□ 不了解	□ 了解	□ 理解
设置及使用简易防火墙	□ 不会	□ 会	□ 熟练
加密技术	□ 不了解	□ 了解	□ 理解
数字摘要技术	□ 不了解	□ 了解	□ 理解
使用适当的工具对数据和终端进行加密	□ 不会	□ 会	□ 熟练

3. 回答以下问题，完成活动反思。

（1）“网络的美妙之处在于你能连接任何人；网络的可怕之处在于任何人都能与你连接。”谈一谈你对这句话的看法。

（2）有人说“人们通过网络分享资源的活动越频繁，其面临的安全风险也就越大，所以要尽可能避免网络分享行为。”对于这个观点，你怎么看？

微信公众号：电子课本大全



第 4 章

物联网与创新网络服务

以物联网和“互联网 +”为特征的信息网络服务正在广泛流行。一方面，智能手机、网络电视、智能冰箱……越来越多的设备开始接入网络；另一方面，工业、农业、商业、教育、交通等传统行业也纷纷开始“互联网化”。可以说，随着信息化的进程，网络已经渗透到社会的各行各业，产生了网络购物、线上支付等一系列创新网络服务，对人们的生活、工作和学习产生了重大的影响。

微信公众号：电子课本大全

4 主题学习项目：创新网络与社会

项目目标

以“物联网”为代表的创新网络服务正在影响着人们的生活、工作与学习，因而受到了人们前所未有的重视。本章以“创新网络与社会”为项目主题，力求探讨物联网等的工作原理，以及它们对社会的推动作用和可能引发的安全问题。

1. 围绕项目进行调研，收集资料，完成作品。
2. 掌握物联网的发展历程，感受物联网的社会应用。
3. 领悟创新网络服务给社会生活带来的改变。

项目准备

为了完成项目，需要做以下准备。

- 依据项目目标和自己承担的任务，各自查询、收集所需资料，这一过程中既要积极完成自己的任务，也要兼顾组员的进展，在协作中共同学习与实践。
- 准备多部具备蓝牙和近场通信功能的智能手机，至少一台能够进行蓝牙通信的计算机，以及展示用的传感器等设备。
- 本章的项目活动，需要使用智能手机、传感器等硬件设备，使用前要熟悉使用规范，使用时应严格遵守规范，以免造成自身危险或设备损害。

项目过程

为了保证顺利完成本章的学习活动，在不同学习阶段，小组长要注意检查组员项目学习的进度，并做好协调互助工作。

1 收集信息

收集介绍物联网的资料，体验蓝牙、近场通信等无线传输技术。 P110

2 归纳总结

整理各种资料，并结合实际的心得体会，总结自己对物联网的认识。 P115

3 交流探讨

交流、探讨网络创新网络服务对社会的影响，归纳保护个人隐私的途径。 P120

4 制作作品

汇总资料和心得体会，制作主题为“创新网络与社会”的电子作品。 P123

项目总结

学完本章后，及时分析活动时遇到的问题，归纳总结解决问题的方法。通过项目学习活动，掌握物联网的概念及其发展历程，了解与物联网相关的设备及其功能，并能描述其工作原理，体验物联网、“互联网+”以及其他相关网络在日常生活、学习中的应用，探讨创新网络服务对人们未来生活、工作与学习的影响。

微信公众号：电子课本大全

4.1 物联网简介

学习目标 ▶▶▶

- 掌握物联网的概念及其发展历程。
- 了解与物联网相关的设备及其功能。
- 能描述物联网设备的工作原理。

体验探索

回顾对物联网的认识

当前，网络不仅广泛用于即时通信、网络视频等信息技术相关产业，还在农业、工业等传统行业中频繁展现身影；网络不仅连接着计算机，还连接着智能手机、平板计算机、汽车、网络电视等多种智能设备（图4.1.1）。

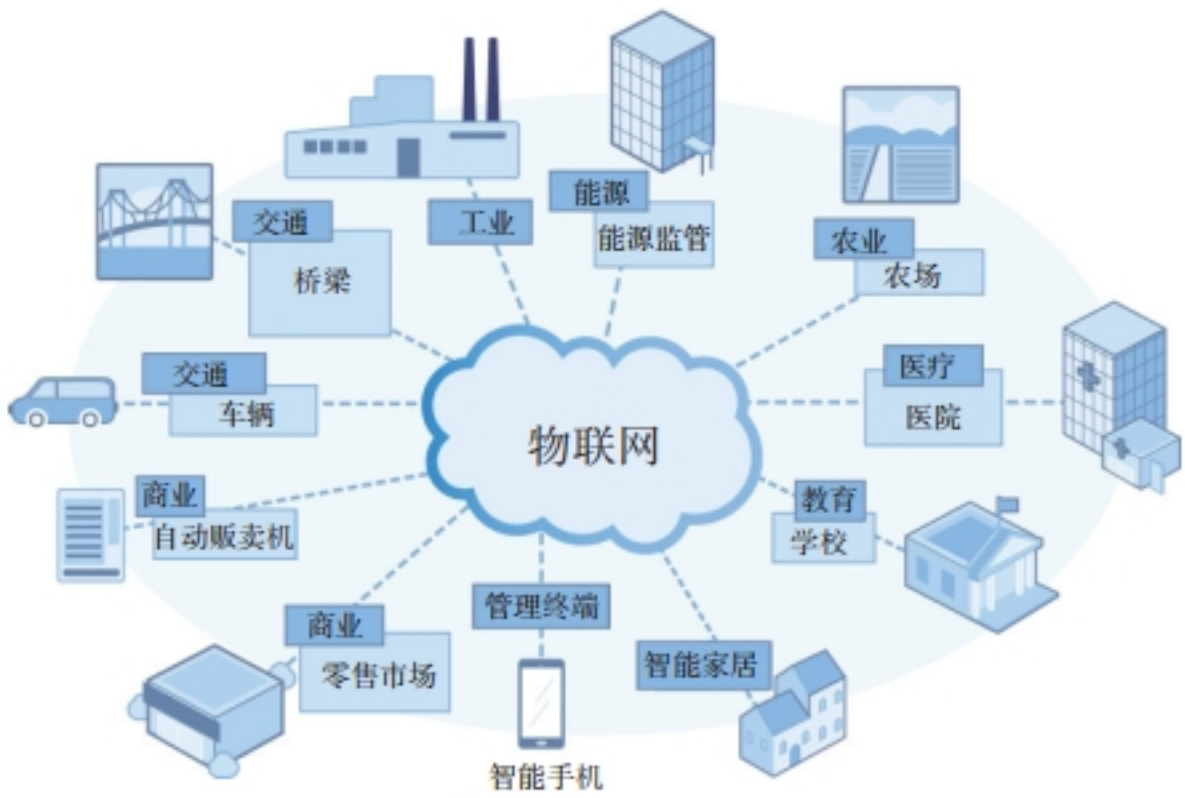


图4.1.1 物联网示意图

参照图4.1.1，谈一下你对物联网的认识。

微信公众号：电子课本大全

4.1.1 认识物联网

物联网指通过各种信息传感设备，实时采集需要监控、连接、互动的物体的信息，与互联网结合形成的一个巨大网络。其目的是实现物与物、物与人之间的连接，以便识别、管理和控制。

从硬件设备上看，物联网主要有三个构成要素：终端设备、网关和服务器（图4.1.2）。



图4.1.2　物联网的硬件结构

从工作逻辑上，则可以分为应用层、网络层和感知层（图4.1.3）。

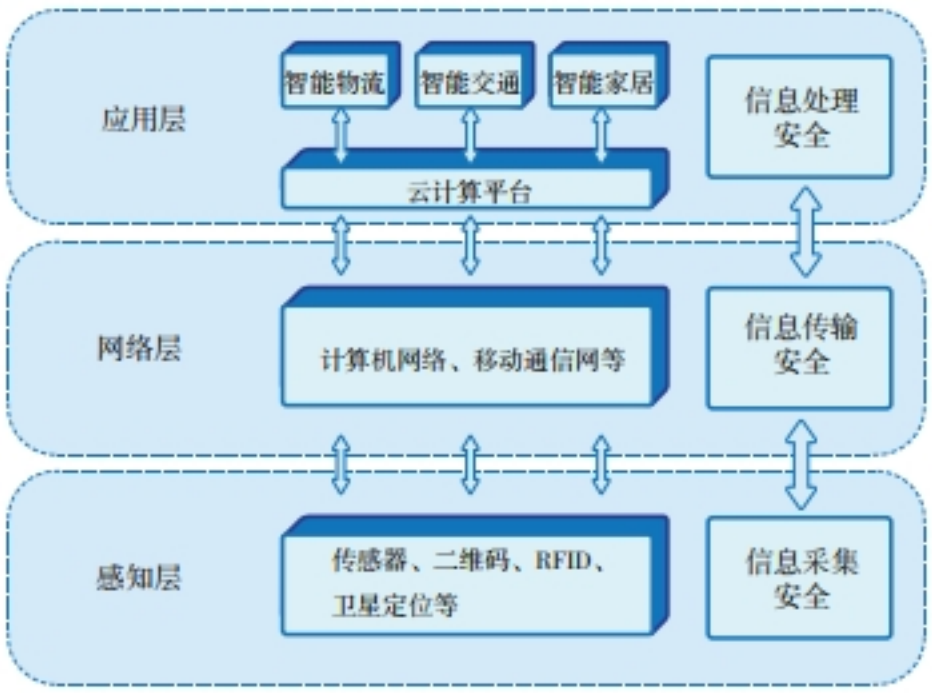


图4.1.3　物联网的逻辑结构

微信公众号：电子课本大全

4.1.2 物联网的发展历程

物联网的理念最早出现在1995年出版的《未来之路》一书中，书中提到了物物互联，但受当时技术条件的限制，并未引起重视。一般认为，物联网这一概念是1999年出现的，当时的科研工作者提出“万物皆可通过网络互联”，阐明了物联网的基本含义。

从计算机网络到物联网，大体经过了三个阶段（图4.1.4）。在最开始，网络发展注重的是把计算机和服务器连接起来，形成了以“万维网”为代表的关注信息的网络；随着“普适计算”等思想的普及，人在网络中的作用受到了重视，通过智能手机、平板计算机等设备，使得人“随时随地”连接网络成为可能，从而形成了关注人的网络；随着网络连接的普及，以及芯片技术、传感技术等技术的发展，汽车、眼镜、手表等物品也开始连入网络，从而形成了关注物的网络，也就是物联网。

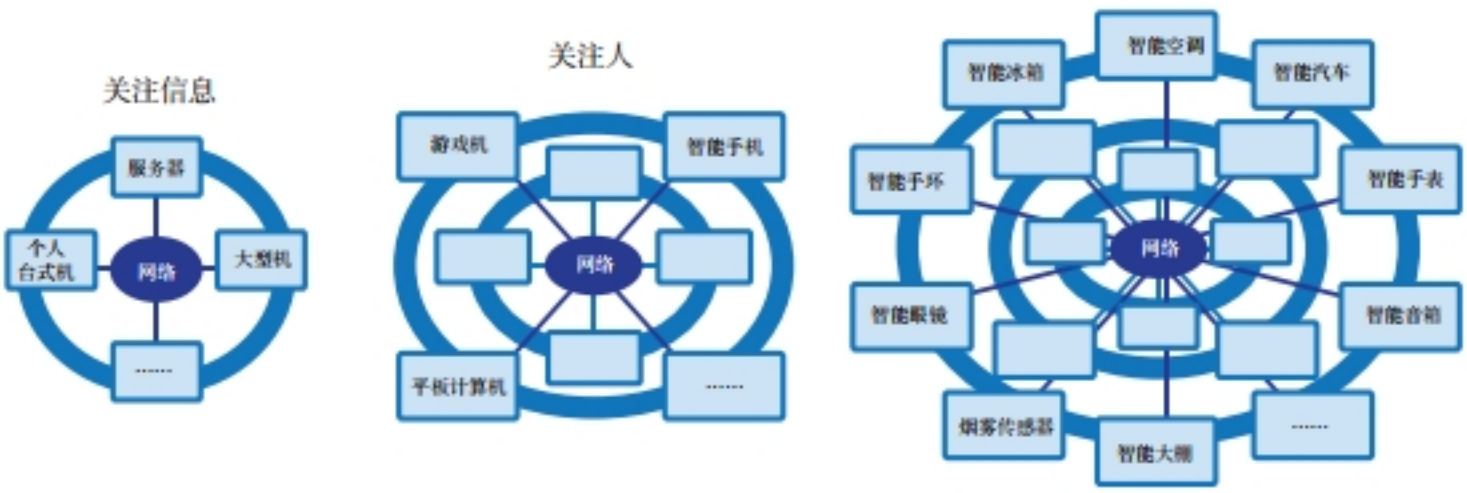


图4.1.4 物联网的发展历程

尽管物联网的基本思想在20世纪90年代就提出来了，但近年来才引起人们的关注。进入21世纪后，物联网受到了世界各国前所未有的重视，被认为是下一个推动世界高速发展的“重要生产力”。

思考活动

了解我国物联网建设成果

说一说你接触过的物联网应用，然后搜索并阅读相关资料，了解我国物联网的建设成果。

微信公众号：电子课本大全

4.1.3 相关设备

前面已经介绍过，物联网的相关设备主要分为终端设备、网关和服务器三种。

终端设备

物联网中的终端设备，主要指物，除了平板计算机、智能手机外，电视、手表、眼镜……任何一件物品，都有可能成为终端设备。这些终端设备主要发挥着两大类作用：感测和反馈。

对于物联网来说，感测是从现实世界获取信息的过程，可用于感测的设备被称为输入设备（图4.1.5和图4.1.6）。

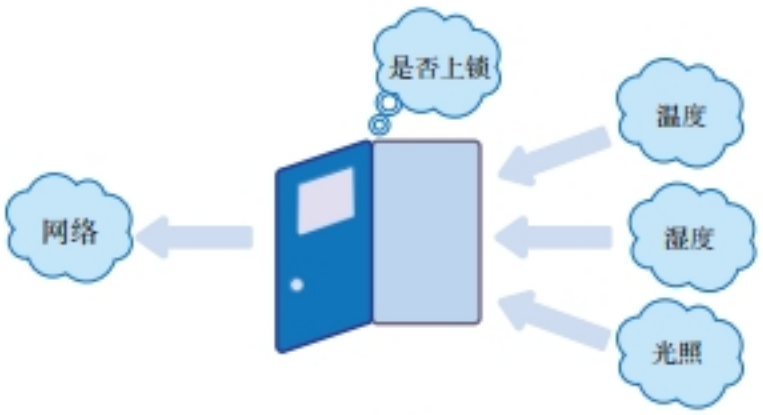


图4.1.5 感测



图4.1.6 输入设备

物联网系统收到上传的信息后，就要决定该如何应对，并把应对方式传给相应的终端设备。对于物联网来说，反馈就是针对现实世界采取行动的过程，可用于反馈的设备被称为输出设备（图4.1.7和图4.1.8）。



图4.1.7 反馈



图4.1.8 输出设备

微信公众号：电子课本大全

也有很多终端设备不能进行这样简单的划分，它们不仅具有输入、输出功能，还能进行比较复杂的信息处理，如智能手机、平板计算机等。日常生活中，常把这些终端设备称为智能终端。

网关

与计算机网络不同的是，物联网中的终端设备类型多种多样，有很多设备自身很难具备独立连入网络的能力，这时，就需要网关的帮助。

在感测过程中，网关主要用于连接设备和收发数据；在反馈过程中，网关主要用于向终端设备传达来自服务器的指令（图4.1.9）。



图4.1.9　网关的作用

服务器

物联网系统的服务器，跟普通服务器的功能类似，通常也具备收发数据、处理数据和存储数据三大功能（图4.1.10）。

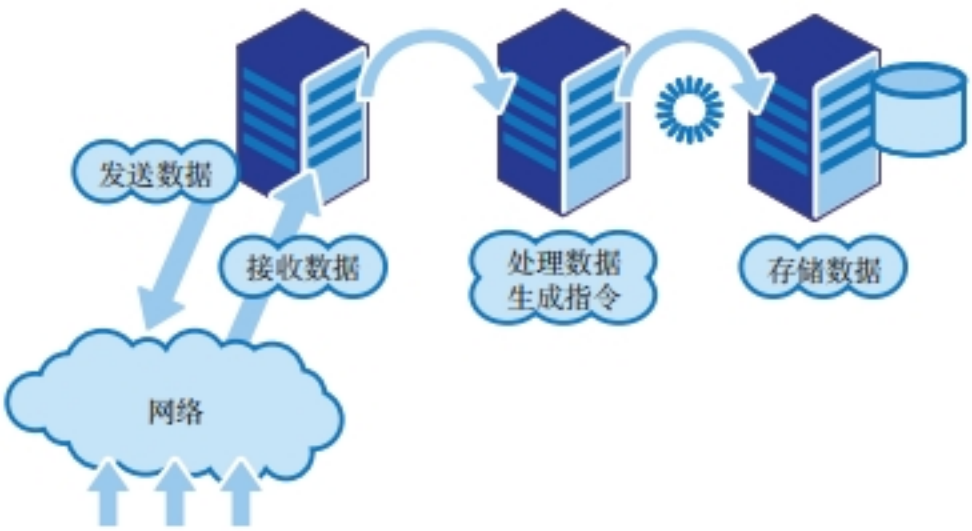


图4.1.10　服务器的功能

微信公众号：电子课本大全

不同的是，物联网服务器收发的数据，其格式或类型通常更复杂（图4.1.11），数据量也更大，因而数据的处理和存储可能会用到大数据技术。



图4.1.11　数据处理的示意图

服务器处理数据主要有批处理和流处理两种方式。采用批处理方式时，会先保存数据，等待一定的时间后，一次性集中处理这段时间保存的数据（图4.1.12）；采用流处理方式时，则会在收到数据后立刻进行处理，并进行保存（图4.1.13）。



图4.1.12　批处理



图4.1.13　流处理

思考活动

总结物联网相关设备的功能

你还知道哪些物联网相关设备？它们具备怎样的功能？

微信公众号：电子课本大全

4.1.4 感测技术简介

物联网的一大任务是感测现实世界。目前，感测现实世界主要有以下关键技术。

传感器技术

一般认为，传感器技术与通信技术、计算机技术构成了信息技术的三大支柱。传感器技术的典型产品是种类各异的传感器。

情境 1：

慢慢接近中午了，天越来越热，空气也越来越干燥。突然，王红叔叔家的智能大棚自动开始喷水了。喷洒了一会之后，又自动结束了。

在这个过程中，可能用到了哪些传感器，这些传感器起了什么作用？

传感器是一种能够将某一被测物理量（如速度、温度、声、光等）转换成便于传输和处理的另一物理量（通常为电量）的器件或装置。传感器是物联网感知物理世界的重要依托，物联网系统根据传感获知的情况来开启或停止相应的操作。

射频识别技术

射频识别（radio frequency identification，RFID）技术主要用于解决物体识别问题，如识别交通卡、托运的行李、饲养的动物等。

你知道哪些使用了射频识别技术的产品？这些产品分别用于识别哪些物体？

图 4.1.14 展示了一个典型的 RFID 系统。这个系统由标签、阅读器和天线三部分构成。使用时，先在标签上写入关于物体的信息，并放入物体中，此后，阅读器无需接触标签，就可以读取标签，从而获取相关的信息。

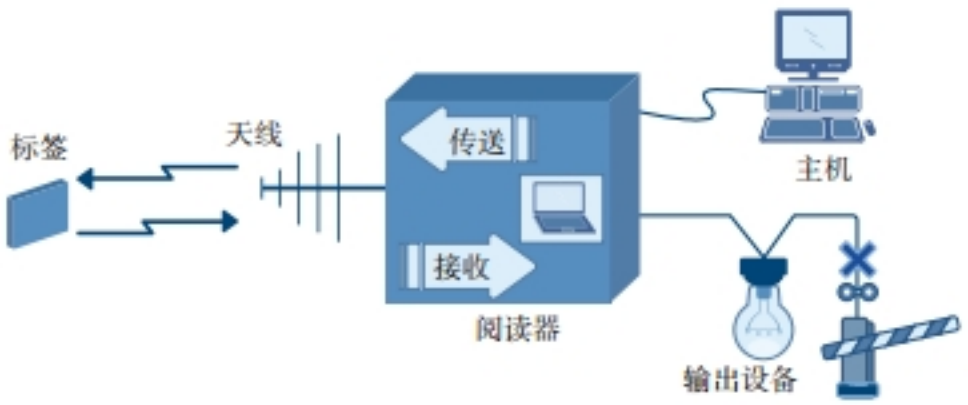


图 4.1.14　典型 RFID 系统示意图

微信公众号：电子课本大全

二维码技术

二维码具有信息容量大、成本低、准确性高等特点。那些不适合嵌入电子标签的物体，可以通过张贴二维码来解决识别问题（图4.1.15）。



图4.1.15　二维码的应用

定位技术

感测物体所处的位置，也是物联网感测客观世界的一个重要任务。从应用场景上看，定位技术可以分为两大类：室外定位和室内定位（图4.1.16）。

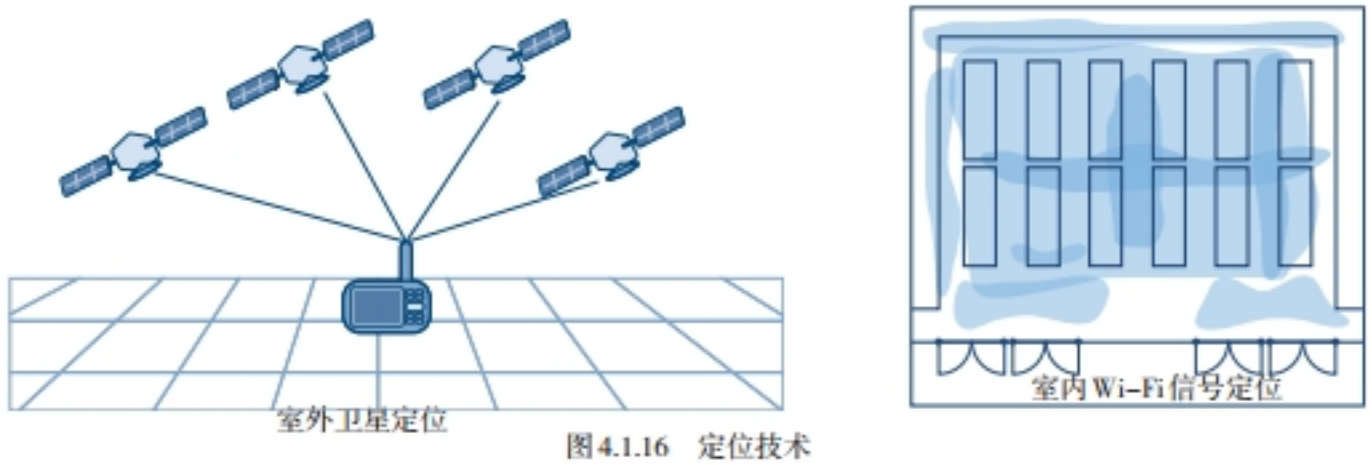


图4.1.16　定位技术

室外定位相对成熟，利用卫星、手机基站等，都可以较好地实现相关功能，精度也比较高。室内精确定位一直是个难题，现在一般借助各种无线信号来完成，比如把屋内Wi-Fi信号的特征分布记录下来，然后根据特征确定联网设备所处的位置。

思考活动

讨论定位功能在网络服务中的应用

你知道哪些基于定位功能的网络服务？它们为什么要利用定位功能？这些服务如何获取和利用位置信息？

微信公众号：电子课本大全

4.1.5 联网技术简介

从功能上看，物联网中的网络可以分为两种：一种是用于连接服务器的网络；一种是把设备连接到其他设备的网络（图4.1.17）。

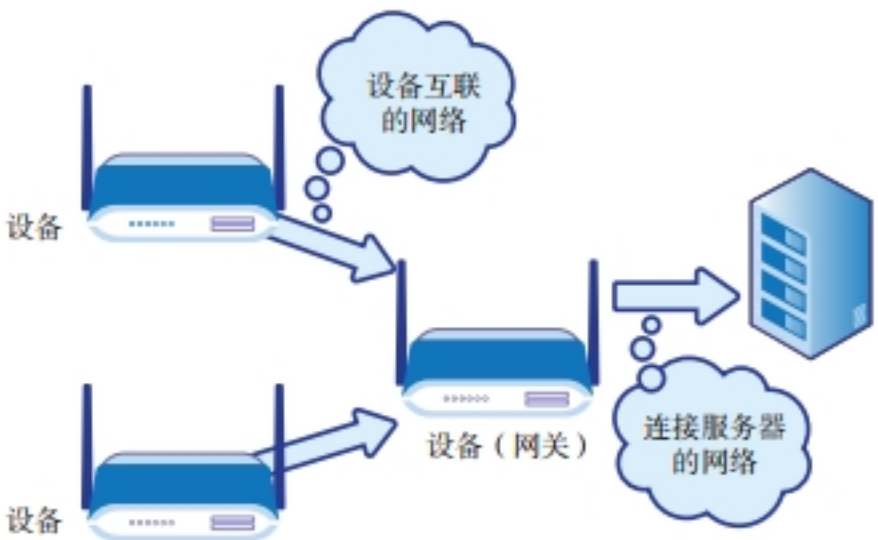


图4.1.17 物联网中的网络

用于连接服务器的网络比较好理解，前面介绍的互联网、移动互联网等都属于这类网络；用于实现物联网设备互联（如传感器和网关互联）的网络，则是物联网特有的。

从传输介质上看，把“万物”接入物联网，也可以分为有线网和无线网两种。有线连接包括网线连接、USB连接等（图4.1.18）。

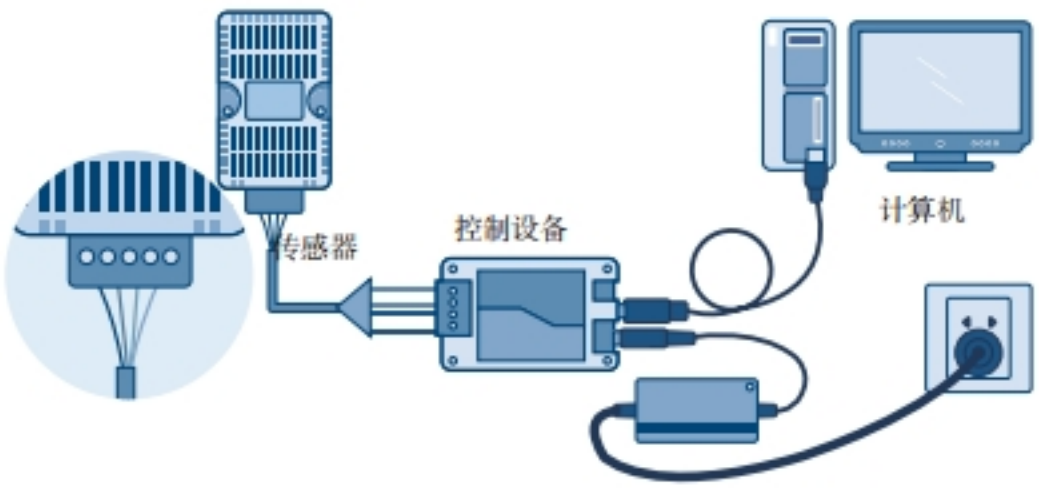


图4.1.18 有线连接传感器

无线连接包括Wi-Fi、移动通信网、蓝牙（bluetooth）、近场通信（near field communication，NFC）、ZigBee等。下面对蓝牙、近场通信等进行介绍。

微信公众号：电子课本大全

蓝牙

蓝牙是一种近距离无线通信技术，多数智能手机和笔记本计算机都具有蓝牙通信功能。蓝牙可用于设备连接，同时也可以用来传输数据。

项目实施

试用蓝牙技术通信

1. 准备一台具备蓝牙功能的计算机和两部具有蓝牙功能的智能手机。
2. 让计算机搜索蓝牙设备，并参照手机屏幕中的提示，完成配对操作（图4.1.19）。

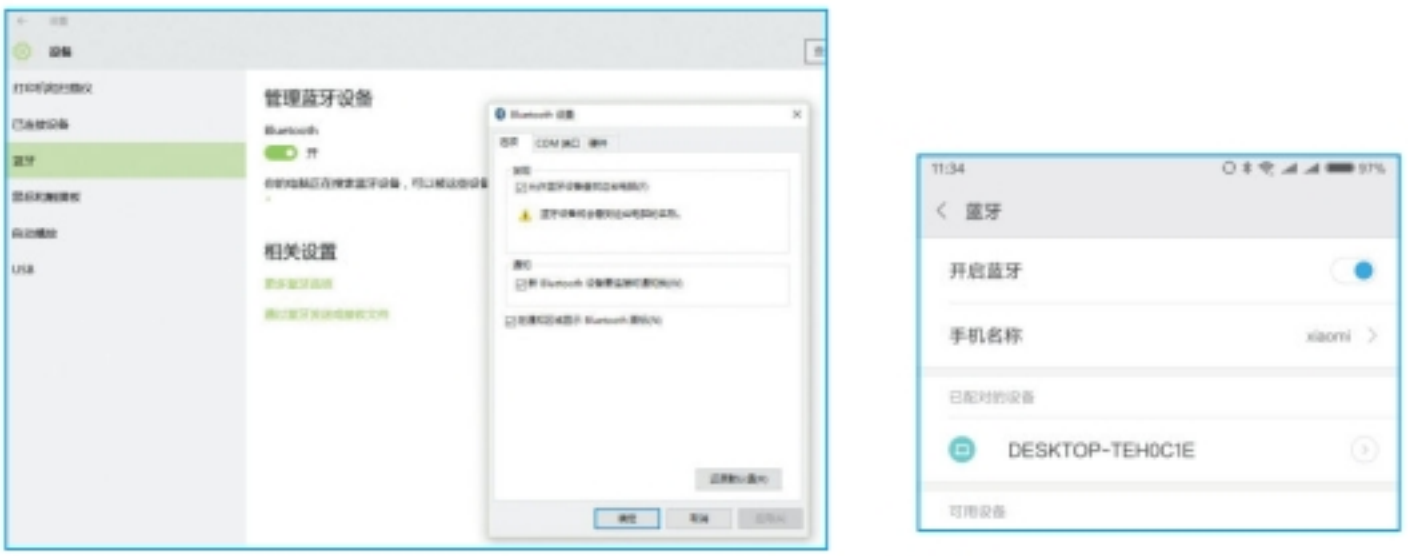


图4.1.19　蓝牙配对

3. 在计算机中打开蓝牙管理界面，并启用接收文件功能。
4. 在手机上打开一张照片，然后利用蓝牙功能发送这张照片（图4.1.20）。



图4.1.20　用蓝牙发送文件

5. 传输完毕后，用计算机打开接收到的照片。
6. 用手机搜索附近的蓝牙设备，让这两部手机进行蓝牙配对。
7. 尝试用一部手机向另一部手机发送照片。

微信公众号：电子课本大全

情境2：

很多人肯定有这样的经历：上下公共汽车或出入地铁站时，大家只要把交通卡在刷卡设备上“嘀”一下，相关的计费或付费工作就完成了（图4.1.21）。这个“刷”卡行为的背后，依靠的是什么技术原理呢？

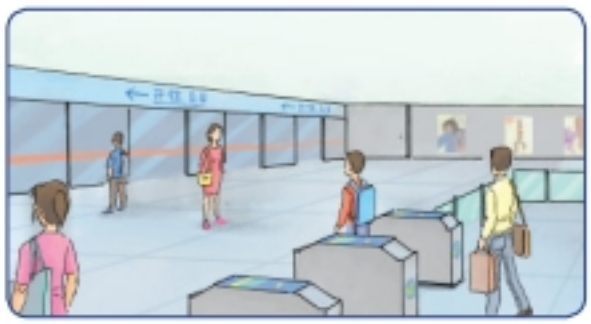


图4.1.21　刷交通“一卡通”进站

项目实施

试用手机读取交通卡中的信息

1. 准备一部具备NFC功能的手机和一张交通卡。

2. 把交通卡放到手机NFC模块的位置处，听到“嘀”的一声后，手机的屏幕上就会显示通过NFC发现的物体。

3. 选择相关的程序，查看交通卡信息（图4.1.22）。



图4.1.22　用NFC功能查看交通卡

不难想象，如果是一个具有修改功能的设备，就可以增加或减少交通卡中的金额，从而完成充值或付费任务。

微信公众号：电子课本大全

近场通信技术不仅可以用来读取各种设备，也能用来传输文件。

项目实施

试用NFC功能传输文件

1. 准备两部支持NFC功能的手机，了解它们的NFC模块所在位置。

2. 在一部手机上打开一张图像，然后让两部手机的NFC模块互相靠近。几乎要互相贴着时，会听到“嘀”的一声，表示两部手机已经建立了NFC连接。

3. 查看已经打开图像的手机，然后按屏幕的提示点击一下，手机就会自动把图像发送到另一部手机中（图4.1.23）。



图4.1.23　用NFC功能传送文件

提示：发送过程中，两部手机不能相隔太远。

4. 用另一部手机翻看刚刚获取的图像文件。

思考活动

总结蓝牙技术和近场通信技术的异同

根据前面的实践活动并查阅相关资料，然后参照下面的问题，总结蓝牙技术和近场通信技术的异同。

- 互联设备是否都要有供电装置？
- 通信前是否需要进行手工配对？
- 哪种技术支持的传输距离长？
- 哪种技术的传输速度快？

微信公众号：电子课本大全

除了上面介绍的技术外，物联网中使用的无线通信技术还有ZigBee、Li-Fi等。

ZigBee具有网络容量大、安全可靠等特点，ZigBee网中的设备之间可以自动形成一个网状拓扑。Li-Fi利用可见光波（如灯泡发出的光）进行数据传输，理论上，人们甚至可以利用街边的路灯传输信息。

思考活动

讨论无线通信技术的特点

图4.1.24是一位同学总结的物联网常用无线通信技术的特点。请查阅相关资料，说一说这张图对不对，并说明你认为理想型的无线通信技术应该是怎样的。

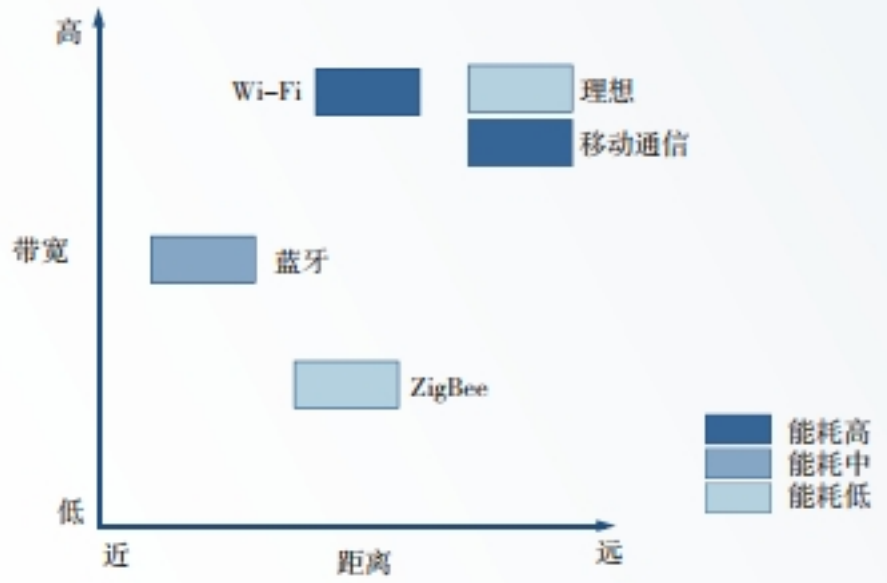


图4.1.24　一位同学总结的技术对比图

4.1.6　服务器端技术简介

感测技术获得的大量信息，通过各种网络传输汇聚到服务器后，还需要在服务器上进行有效地整合分析。相关的技术非常多，其中大数据和云计算目前在服务器端的应用非常广泛。

大数据

大数据是用来形容数据爆炸性增长的术语，其显著特征是“数据量大”，但直到今日，研究者仍无法给出一个科学的定义。一般来说，大数据指大小超出了常规数据工具处理能力的数据集。

通常认为，大数据具有巨量性、多样性、迅变性等特征，物联网中传输的数据恰好与这些特征相吻合。

微信公众号：电子课本大全

云计算

云计算可以视为一种全新的，方便人们使用各种资源（包括中央处理器、内存、硬盘、软件等）的计算模式。计算资源所在的地方称为云端；使用这些资源，负责输入和输出的设备称为云终端（图4.1.25）。

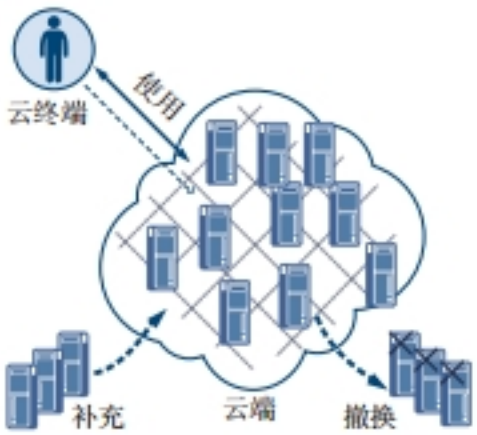


图4.1.25　云端和云终端

使用时，云终端通过网络向云端发送请求，云端处理后返回结果。具体来说，包括3种服务模式（图4.1.26）：

基础设施即服务。云端提供中央处理器、内存、存储器等资源，用户像使用一台普通计算机那样，根据自己的需要安装系统和应用软件。

平台即服务。云端提供已经配好的各种开发、应用平台，用户根据需要开发、安装各种应用软件。

软件即服务。云端提供用户需要的应用软件，用户只要关心如何使用就可以了。

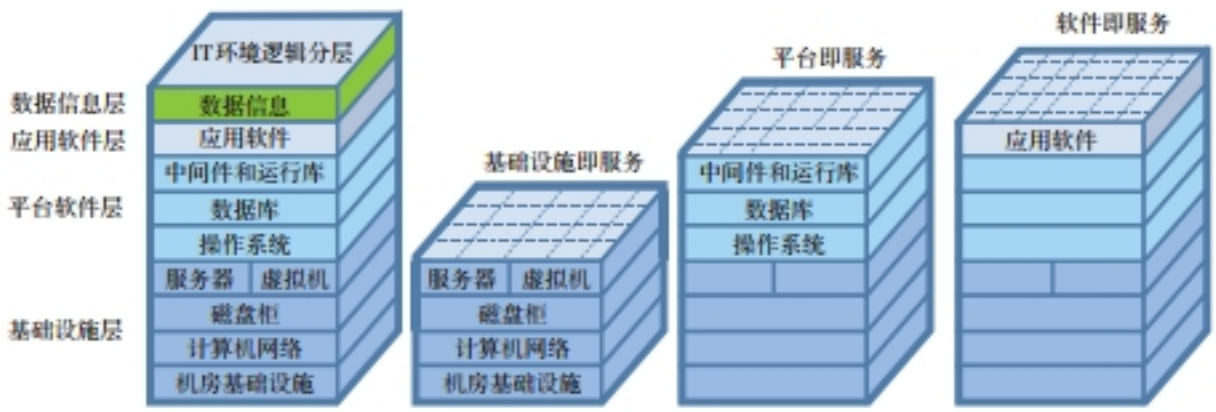


图4.1.26　云计算的三种服务模式

可以这样认为，物联网产生了大数据，大数据的处理需要借助云计算，而云计算则支持了物联网的发展。三者的关系可见图4.1.27。

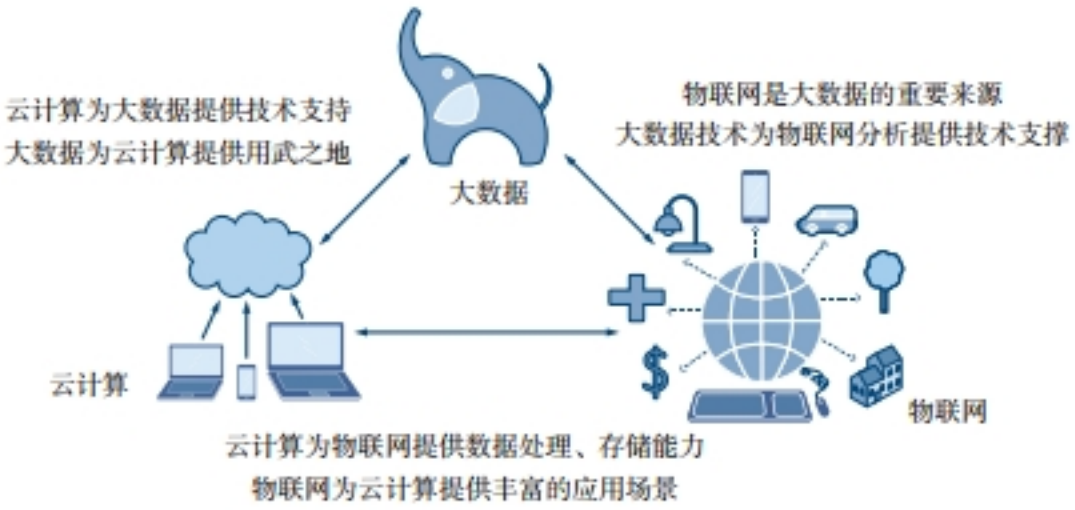


图4.1.27　物联网、大数据与云计算

微信公众号：电子课本大全

项目实施

总结自己对物联网的认识

在了解物联网的概念和发展历程、物联网设备及其功能，以及它的社会影响的基础上，结合自己的使用感受，总结自己对物联网的认识。

提示：

1. 可以宏观地、全方位地介绍对物联网的认识，也可以选择一个切入点，就某一具体的问题进行阐述；

2. 观点鲜明，内容严谨；

3. 语言精练，便于理解。

练习提升

1. 物联网的结构体系可以分为几层，分别是什么？

2. 尝试在没有Wi-Fi的情况下，让两个智能设备实现文件分享。

3. 不同的物联网设备是如何跟物联网信息系统相连接的？

4. 物联网的终端设备，主要承担着哪两大功能？

5. 物联网中，网关设备和服务器的主要功能是什么？

6. 有哪些常见的感测技术？它们的特点是什么？

7. 物联网中常用的联网技术有哪些？

8. 物联网中，在服务器端经常使用的技术有哪些？

微信公众号：电子课本大全

4.2
创新网络服务与隐私保护

学习目标 ▶▶▶

- 体验物联网、“互联网+”以及其他网络在日常生活、学习中的应用。
- 探讨创新网络服务对人们未来生活、工作与学习的影响。
- 了解个人隐私保护相关政策，提高保护个人隐私的意识和能力。

体验探索

回顾、总结创新网络服务

近年来出现的移动支付、网络购物和共享单车等网络服务，展示了我国在物联网和“互联网+”等领域的建设成果。这些新的应用改变着中国人的生活方式，也刷新了世界对中国的认识（图4.2.1）。



图4.2.1　网络应用

结合自己的知识和使用心得，回答以下问题。

1. 在图4.2.1展示的网络服务中，你接触最多的是哪一种？你觉得它给你的生活带来了哪些改变？

2. 你觉得这些服务与网络技术有什么关系？你认为这些服务的哪些环节体现了网络技术的作用？

微信公众号：电子课本大全

4.2.1 网络服务新案例

物联网和“互联网+”已经广泛用于交通、环境保护、公共安全、家居等诸多领域。下面一起来简单认识几种近年来出现的网络服务。

移动支付

移动支付俗称手机支付，就是允许用户使用其移动设备（通常是手机）对所消费的商品或服务进行账务支付的一种服务方式。

移动支付可以分为两大类：近场支付和远程支付。以手机刷卡的方式坐车、买东西等，都可算作近场支付；用手机转账、发红包等，可以算作远程支付（图4.2.2）。移动支付简捷方便，使用越来越广，与此同时，人们携带和使用现金的需求在不断下降。可以说，“无现金”趋势是移动支付给我们的生活带来的最直接的影响。



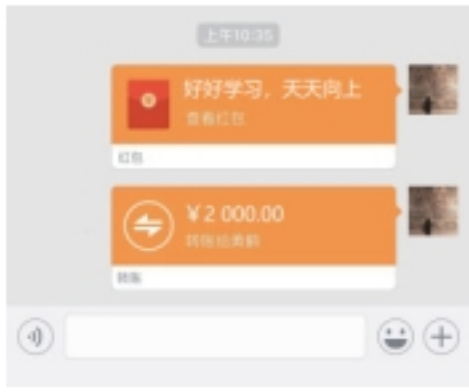


图4.2.2　移动支付

网络购物

近年来，网络购物成为互联网在商业领域最典型的应用，网络购物与手机等移动设备的进一步融合，更使其得到了长足的发展。

借助智能物流的发展，网络购物的对象范围正在不断扩大，已经从图书、衣服等日用商品，扩展到新鲜的瓜果、热腾腾的饭菜等商品上。可以说，小到一根针，大到一架飞机，都可以通过网络购买（图4.2.3、图4.2.4和图4.2.5）。

网络购物的流行，使得人们的购物习惯发生了巨大的变化，现在“足不出户”就可以货比三家，买到自己心仪的产品。

微信公众号：电子课本大全



图4.2.3　网络下单



图4.2.4　智能分拣



图4.2.5　机器人配送

共享单车

共享单车指在校园、地铁站点、公交站点、居民区、商业区、公共服务区等提供的自行车共享服务。

共享单车属于分时租赁模式，也就是把一天中自行车的使用时间，分别租给不同的人，从而实现自行车的共享。共享单车被视为物联网的典型应用，是一种环保的、符合低碳出行理念的共享经济模式（图4.2.6）。

共享单车出现后，购买自行车的人在显著减少，愿意骑车出行的人在逐渐增多。现在甚至出现了共享电动汽车等类似的服务。

不过，共享单车在实际应用中，也存在很多问题。比如，很多人随意停放，使得原本便于通行的共享单车，反而成了导致交通拥堵的原因（图4.2.7）。同时，还出现了不爱护共享单车，甚至刻意损坏共享单车的现象。



图4.2.6　有序使用共享单车



图4.2.7　共享单车出现的问题

思考活动

创新网络服务新思考

- 你还接触过哪些新的网络服务？这些网络服务给你的生活带来了哪些改变？
- 你希望未来还会出现什么样的网络服务？

微信公众号：电子课本大全

4.2.2 信息社会中的个人隐私保护

思考活动

思考漫画的含义

观察下面两张漫画（图4.2.8），思考一下，你能明白它们的寓意吗？

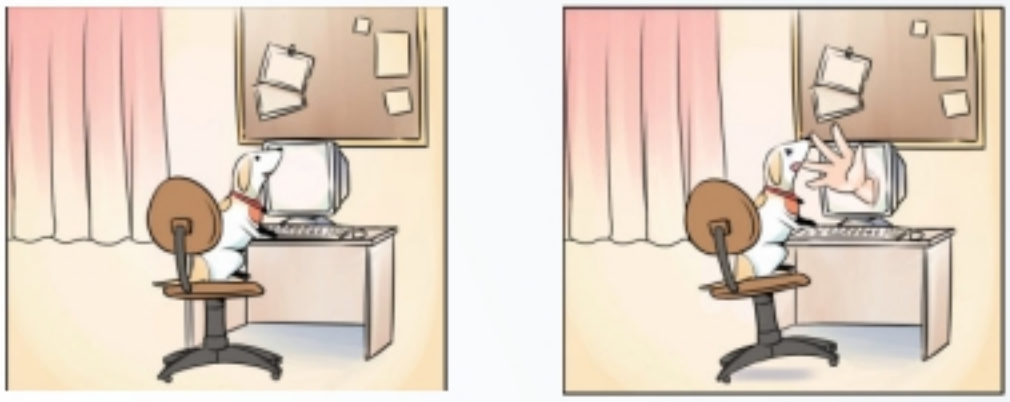


图4.2.8 漫画两则

有一句话曾经在互联网上非常流行，那就是：“在互联网上，没有人知道你是一条狗。”但随着“互联网+”、大数据、物联网等为代表的信息技术在生活中的进一步普及，个人隐私问题变得越发严重，于是一些人提出了相反的观点：“别以为我不知道你是一条狗。”

在实际生活中，人们经常会发现自己的个人信息莫名其妙地泄露了（图4.2.9）。比如，刚刚办完购置新房的手续，很多装修公司就会主动找上门来；刚刚做完体检，就有推销人员来推销各种药品、补品……这些素未谋面的“熟人”不仅知道你的姓名、电话号码、车辆情况、身体状况，甚至还能知道你的银行账号、家庭成员等信息。



图4.2.9 受困扰的社会公民

微信公众号：电子课本大全





图4.2.10　手环传送睡眠信息

哪些途径有可能泄露个人信息呢？除了因信息设备保管不善、信息系统被攻击等技术因素造成的个人信息泄露外，生活中很多不起眼的行为也会泄露个人信息。比如，填写会员注册单、网络购物单、递送单时，都需要留下姓名、电话号码、住址等个人信息。

除此以外，网站可以通过长时间记录用户的浏览情况，从而分析出他的兴趣爱好；智能手机可以时时记录用户的位置，从而分析出他的主要活动范围；即便是在睡觉，佩戴的智能手环也可能正不断地把心跳、睡眠情况等信息传送给服务器（图4.2.10）……

如果把这些信息收集起来并进行相应的整理，就有可能获得关于用户的各方面信息。

项目实施

分析物联网数据与隐私泄露的关系

1. 图4.2.11展示了一个家庭组建的物联网获取的关于用电量的数据。你能利用这些数据分析出这个家庭什么时候家里没人吗？

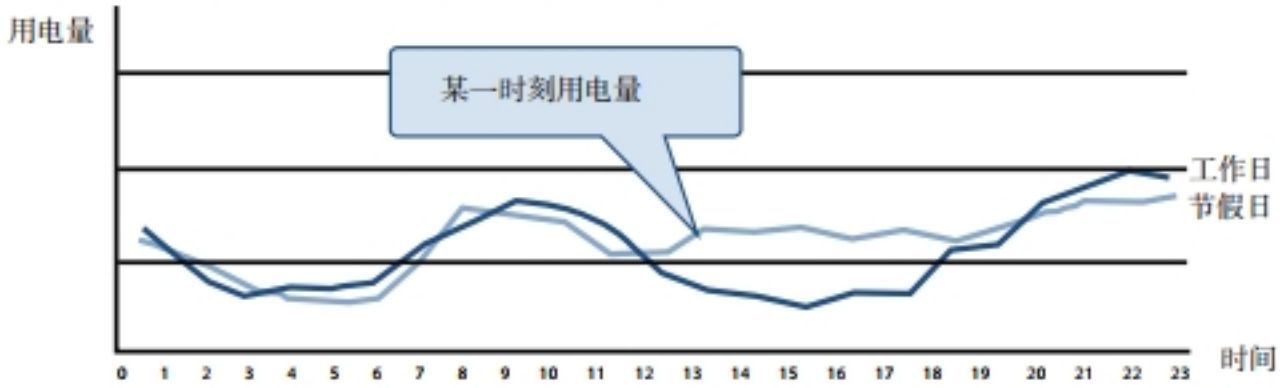


图4.2.11　用电情况

2. 图4.2.12是根据定位功能所描绘的某个人在工作日的主要活动轨迹。从这张图中，你能知道哪些信息？这些信息泄露后，有可能带来什么危害？



图4.2.12　行动轨迹

微信公众号：电子课本大全

可以发现，很多看似没多大作用的信息，经过整理后，就会泄露住址、工作单位、出行时间等隐私信息，从而可能带来各种危害。

但矛盾的是，在现代社会中，人们为了享受某些服务，通常不得不公开一些个人信息。如果不填写电话号码、地址等信息，就无法享用便捷的网络购物服务（图4.2.13）；如果完全不允许网站采集个人浏览记录，那它就无法智能地推送用户感兴趣的新闻、商品；如果不允许智能手机获取用户的位置信息，手机软件就无法提供地图导航等服务；如果不允许智能手环等传送心跳、睡眠情况等信息，就可能无法及时获得相应的健康分析报告和健康服务……

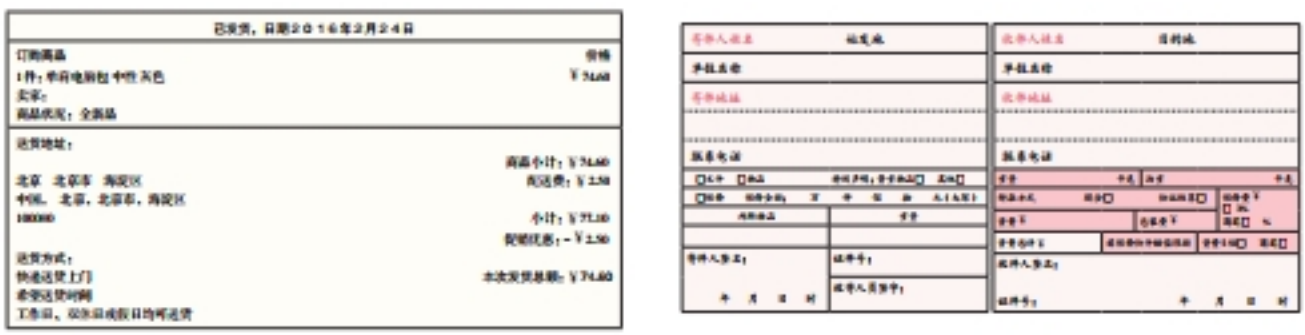


图4.2.13　快递单

虽然人们为了享受某些服务而愿意公开一些个人信息，但这并不意味着他人可以随意使用、传播这些信息，更不能未经同意就非法窃取他人的个人信息，否则就有可能触犯刑法（图4.2.14）。

国家制定了相关的法律法规，用来保护人们的个人隐私。《中华人民共和国刑法》中就规定：

违反国家有关规定，向他人出售或者提供公民个人信息，情节严重的，处三年以下有期徒刑或者拘役，并处或者单处罚金；情节特别严重的，处三年以上七年以下有期徒刑，并处罚金。

违反国家有关规定，将在履行职责或者提供服务过程中获得的公民个人信息，出售或者提供给他人的，依照前款的规定从重处罚。

窃取或者以其他方法非法获取公民个人信息的，依照第一款的规定处罚。

单位犯前三款罪的，对单位判处罚金，并对其直接负责的主管人员和其他直接责任人员，依照各该款的规定处罚。



图4.2.14　擅自出售个人信息违法

微信公众号：电子课本大全

据研究，个人信息泄露之所以屡禁不止，主要有以下三大原因：一、信息泄露已形成成熟的地下产业链，巨大的利益诱使某些人铤而走险；二、相关法律法规存在不健全、难执行等问题，而且威慑力仍显不足；三、一些网络服务商不重视，不作为。

那么，该如何应对个人隐私泄露问题呢？

首先，应该加大制度约束，制定更加有针对性的、更加具体可行的法律法规。比如，更具体地限定网络服务平台能够获取的个人信息种类，以及保管责任等。

其次，相关企业应该在保护个人隐私的相关技术上加大投入，降低因技术因素泄露个人隐私的可能性，还要加强教育，加强企业对个人隐私的尊重。

最后，对于个人来说，以下几点措施可供参考。

1. 在不影响正常使用的情况下，可以有意使用“假”信息来保护个人隐私，比如，在网上只填写自己的网名。

2. 尽量使用规模大、信用好的网络平台。在使用网络服务前，要仔细阅读网站的个人信息保护规定，然后再决定是否填写个人信息。

3. 安装、使用安全软件，防止恶意程序窃取个人信息。

4. 合理设置并妥善保管自己的密码。密码是保护个人信息的关键，如果密码没管理好，电子邮件、即时通信记录等个人信息就容易被人非法窃取（图4.2.15）。



图4.2.15　密码泄露

5. 密码应有特定的使用范围，即在某几个网站或软件中使用；密码应有特定的使用时间，即在一段时间后应更换密码。

6. 给智能手机、平板计算机等安装软件时要注意权限说明。对读取通信录、获取位置等容易造成个人信息泄露的权限，要谨慎对待，确有必要再进行授权。

7. 不要轻易使用免费Wi-Fi，并尽可能使用网络安全协议，以防数据在传输过程中发生泄露。

思考活动

探讨个人隐私泄露问题

你听说或者遇到过个人隐私泄露事件吗？这些事件给当事人带来了哪些烦恼或损害？你知道哪些应对个人隐私泄露的方法？

微信公众号：电子课本大全

项目实施

制作演示作品

在了解创新网络服务对社会的影响，以及个人隐私保护策略的基础上，结合自己的心得体会，制作主题为“创新网络与社会”的演示作品。

制作要求：

1. 可以宏观地、全方位地介绍对创新网络服务的认识，也可以选择一个切入点，就某一具体的问题进行阐述，如畅想未来的网络服务；

2. 必须关注新型网络服务可能带来的泄露个人隐私的风险；

3. 观点鲜明，内容严谨，语言精练。

练习提升

1. 问问老师或家长，他们像你们这么大时，用网络做过哪些事情；再对比现在，说一说网络应用发生了哪些变化。

2. 你听说过“智慧城市”“智能家居”“智慧校园”吗？以这些词为关键词，上网搜索有关的资料，了解它们的特点。

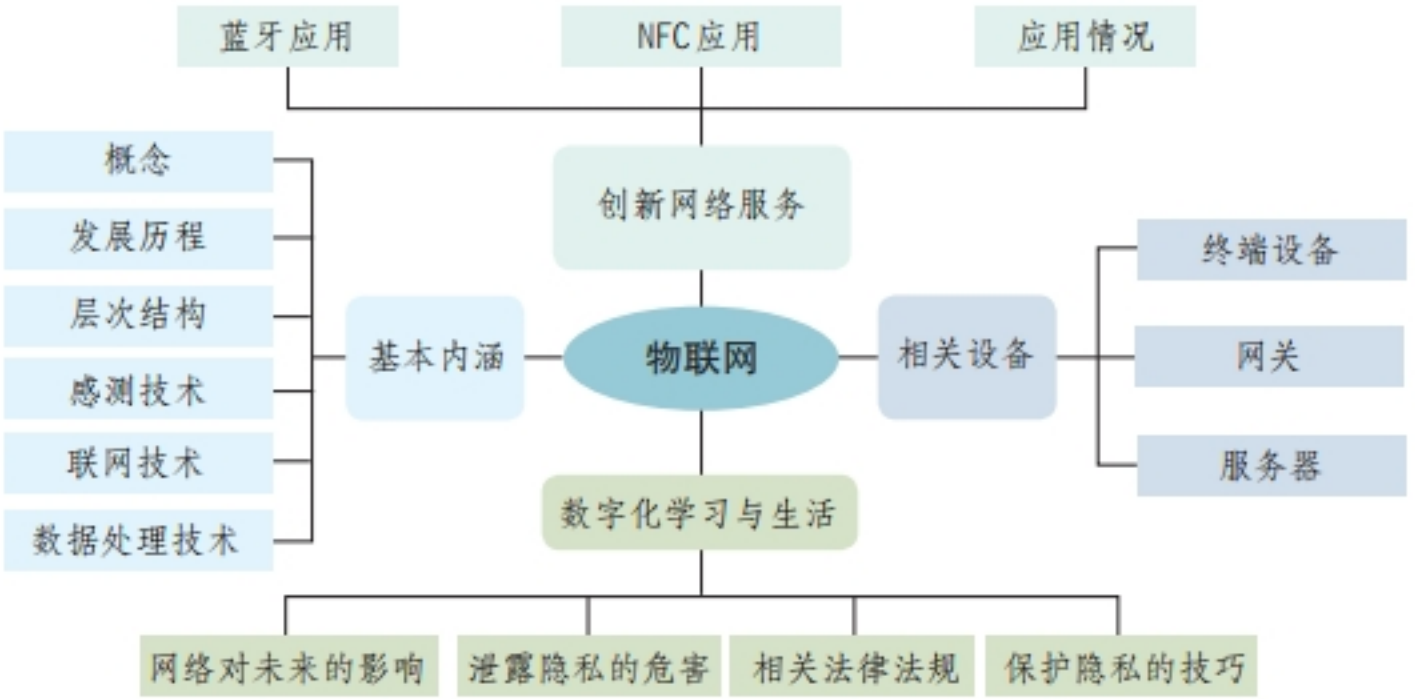
3. 有同学说：“有了网络，自己不用动脑筋了，什么问题都可以在网上找到答案。”对于这个说法，你怎么看？你觉得在学习中该如何合理地使用网络？

4. 如何看待信息社会中的个人隐私保护问题？罗列几条你用来保护自己个人隐私的措施。

微信公众号：电子课本大全

总结评价

1. 下图展示了本章的核心概念与关键能力，请同学们对照图中的内容进行总结。



2. 根据自己的掌握情况填写下表。

学习内容	掌握程度
物联网的概念	□ 不了解 □ 了解 □ 理解
物联网的发展历程	□ 不了解 □ 了解 □ 理解
物联网相关设备的功能	□ 不了解 □ 了解 □ 理解
物联网相关设备的工作原理	□ 不了解 □ 了解 □ 理解
物联网在日常生活、学习中的应用	□ 不了解 □ 了解 □ 理解
保护个人隐私的技巧	□ 不了解 □ 了解 □ 理解
创新网络服务对人类社会的影响	□ 不了解 □ 了解 □ 理解

3. 回答以下问题，完成活动反思。

（1）“以前是数字世界虚拟物理世界，以后是物理世界响应数字世界。”谈谈你对这句话的看法。

（2）“物联网的定位技术使得个人活动等信息可能被连入网络，从而造成隐私泄露。为此，应该禁用定位服务。”对于这个观点，你怎么看？

微信公众号：电子课本大全

项目评价

在完成项目活动后，请各组对项目完成情况进行评价。评价实施围绕项目主题、实施过程、分工合作、项目成果和展示交流五方面进行。根据项目评价中的评分参考，结合项目实际完成情况，确定各项评分结果，给出评分理由。同时，对项目活动进行全面梳理，指出需要进一步改进的地方。将评价内容如实填写到项目评价表中。

评价项	评分参考	评分（1 ~ 5分）	评分理由	待改进之处
项目主题	项目主题能反映出学科核心素养的要求（信息意识、计算思维、数字化学习与创新、信息社会责任）；主题任务与学习目标保持一致			
实施过程	项目研究计划详细，准备充分；实施过程完整，过程记录翔实，资料丰富；研究数据来源渠道多，出处明确，收集方式多样，质量高；研究方法得当，技术手段适宜			
分工合作	小组成员分工明确，态度积极，参与度高；善于提出问题，分析问题，解决问题能力强；踊跃分享观点，交流充分；能在完成自己任务的前提下，乐意帮助他组完成任务			
项目成果	项目活动成果丰富，内容具体，符合项目目标要求；研究结论清晰准确，有价值，有创新，具有指导及建设意义；项目报告或作品内容完整，论述充分，表述清楚，整齐美观			
展示交流	项目展示形式新颖，综合运用多种技术呈现成果，表现力高；语言表达清晰准确，逻辑性好			
项目总分				

微信公众号：电子课本大全

后　记

本册教科书是中国地图出版社与人民教育出版社依据教育部《普通高中信息技术课程标准（2017 年版）》，由双方共同组织团队联合编写的，经国家教材委员会 2019 年审查通过。

本册教科书的编写，集中反映了我国十余年来普通高中课程改革的成果，吸取了 2004 年版《普通高中课程标准实验教科书 信息技术》的编写经验，凝聚了参与课改实验的教育专家、学科专家、教材编写专家、教研人员和一线教师，以及教材设计装帧专家的集体智慧。本册教科书的编写人员还有王璐、聂璐。为本册教科书进行装帧设计的有吕旻、李媛，绘制插图的有北京大方四象、李筱甜。

我们感谢所有对教科书的编写、出版、试教等提供过帮助与支持的同仁和社会各界朋友。同时，我们还要感谢 2004 年版《普通高中课程标准实验教科书 信息技术》的编写人员。

本册教科书出版之前，我们通过多种渠道与教科书选用作品（包括照片、画作）的作者进行了联系，得到了他们的大力支持。对此，我们表示衷心的感谢！恳请未联系到的作者与我们联系，以便及时支付稿酬。

我们真诚地希望广大教师、学生及家长在使用本册教科书的过程中提出宝贵意见。我们将集思广益，不断修订，使教科书趋于完善。

联系方式

电　　话：010–83543863　　010–58758866

电子邮箱：sinomaps@yeah.net　　jcfk@pep.com.cn

中国地图出版社教材出版分社

人民教育出版社课程教材研究所信息技术课程教材研究开发中心

2019 年 4 月

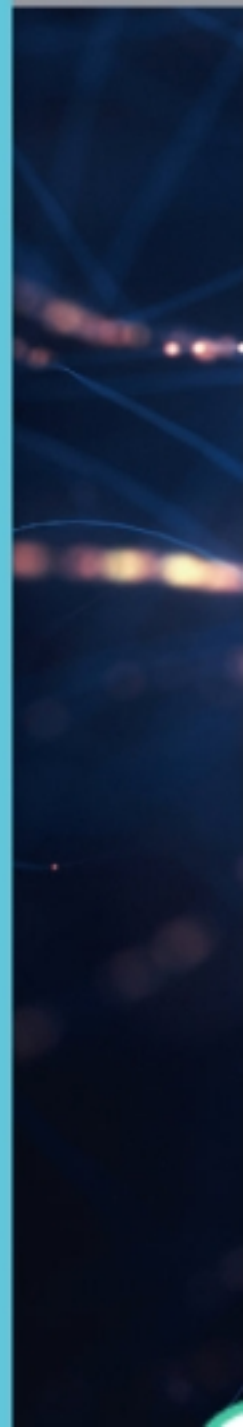
微信公众号：电子课本大全



微信公众号：电子课本大全

PUTONG GAOZHONG JIAOKESHU

XINXI JISHU



微信公众号：电子课本大全