国家教材委员会专家委员会审核通过
2020

普通高中教科书

信息技术

选择性必修 2 网络基础

华东师范大学出版社

普通高中教科书

信息技术

选择性必修 2

网络基础

华东师范大学出版社
· 上海 ·

总　主　编：李晓明

副 总 主 编：赵　健

本 册 主 编：沈富可

本册副主编：袁文铮

编 写 人 员(按姓氏笔画排序)：

王婷婷　毛杰文　刘　欢　沈富可　张　俍　袁文铮

责 任 编 辑：王　健　竺　笑

美 术 设 计：储　平

普通高中教科书　信息技术　选择性必修 2　网络基础

上海市中小学(幼儿园)课程改革委员会组织编写

出版发行　华东师范大学出版社(上海市中山北路 3663 号)

印　　刷　上海昌鑫龙印务有限公司

版　　次　2021 年 3 月第 1 版

印　　次　2021 年 3 月第 1 次

开　　本　890 毫米×1240 毫米　1/16

印　　张　8.25

字　　数　146 千字

书　　号　ISBN 978-7-5760-0550-9

定　　价　10.40 元

本册教材图片提供信息：

本册教材中的部分图片由全景网、视觉中国等图片网站提供。

致同学们

亲爱的同学们：

当今，信息技术发展日新月异，物联网、大数据、人工智能等新技术、新工具扑面而来，显著地改变着人们的生活、学习和工作模式。我们每一个人都不可避免地会接触信息技术，应用信息技术，甚至去创造新的信息技术。在具备了基本信息技术应用能力的基础上，高中阶段我们要进一步学习信息技术的知识与技能，利用信息技术负责任地解决生活与学习中的问题，全面提升信息素养，迎接信息社会的挑战。

本书是普通高中信息技术课程中的选择性必修课程之一。为了增强学习的趣味性，我们预设自己是中国科考队中的网络工程师，需要在一个遥远的星球上建立起计算机网络。同学们将跟随本书循序渐进地了解和掌握网络基础知识，并通过各种项目任务、项目活动丰富知识和提升技能。

全书共分为六章。第一章“初识计算机网络”介绍了计算机网络的发展历史、网络类型，以及协议和分层结构等基础网络知识；第二章“走近真实网络”介绍了网络传输介质、网络设备与拓扑结构、路由原理等知识；第三章“网络传输与资源共享”介绍了网络数据传输和网络资源共享等知识；第四章“网络中的安全问题”介绍了网络安全意识和各类基础网络安全技术；第五章“网络故障排查与修复”介绍了网络软硬件故障及其基本处理方法；第六章“物联网世界”介绍了物联网的发展历史、技术应用及创新服务。

通过对本书的学习，希望同学们能够了解计算机网络的核心概念与发展历程，了解常用网络设备的功能，能通过网络命令查询网络及设备的工作状态、发现联网故障，认识到物联网对社会发展的影响，能使用典型的网络服务解决生活与学习中的问题，能利用信息技术分享网络资源，同时能具备基本的网络应用安全意识。

编　者

目　录

第一章

初识计算机网络

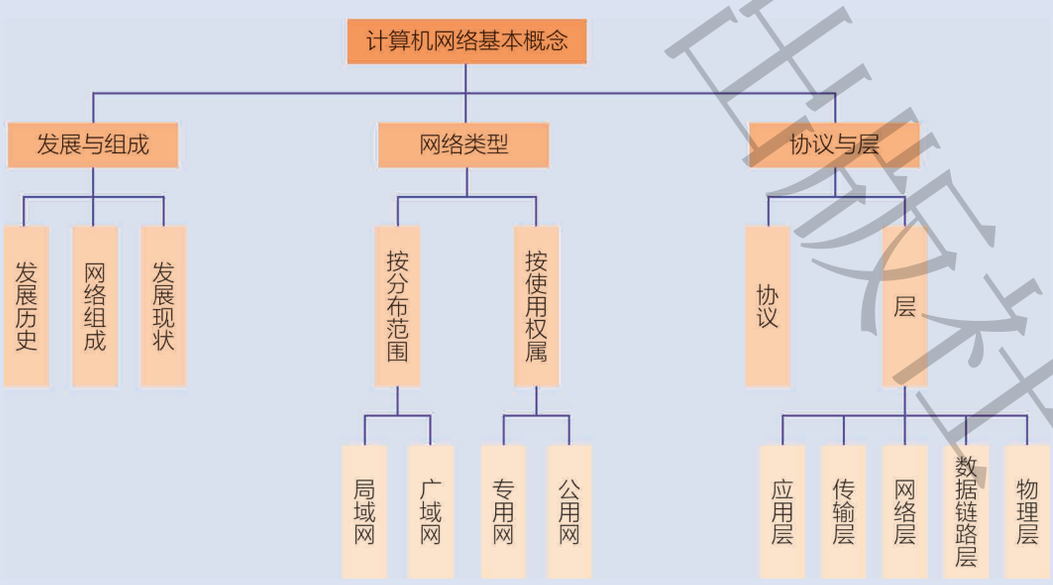
本章学习目标

- 描述计算机网络的定义，列举计算机网络的主要组成元素，举例说明计算机网络对于人们生活的价值和意义。
- 描述计算机网络的发展历史和发展趋势。
- 区分计算机网络的不同类型。
- 描述计算机网络中协议和“层”模型的概念，解释分层体系结构的意义。

计算机网络正在深刻地改变着人们的生活。过去，处于相隔较远的两地的人们主要靠电话或信件进行交流，而如今即便在偏远的乡村，智能手机也逐渐普及，人们可以随时随地通过手机上网，和亲人以语音、视频等方式互通消息；在过去，人们大多通过电视或报纸来获得最新的消息，而现在，只需要打开网页或是各种应用程序，人们就可以便捷地了解到世界各地发生的事情；过去，来到一个陌生的城市，人们大多依赖于纸质地图或者找人问路来确定通往目的地的路径，而现在，许多人更习惯于打开手机上的地图应用程序进行导航。在当今社会，人们正不断与计算机网络建立起更加深入、广泛的连接关系。

作为 21世纪的高中生，我们有必要学习与探究计算机网络背后的科学原理。计算机网络究竟是什么样的事物，它是怎么组成的，它的运行原理是怎样的？接下来，就让我们带着这些问题出发，一起去探究计算机网络这个神奇的世界吧。

本章知识结构



项目主题

认识计算机网络

项·目·情·境

未来某一天，中国科考队肩负星际探索的使命，抵达了一个遥远的星球，开始建设适宜人类居住的环境。科考队成员们来自各行各业，包括医生、建筑师、网络工程师、农业专家等。假设你就是科考队中的一名网络工程师，你的任务是与团队成员一起努力，在这个星球上建立起计算机网络，让这个星球上的各个科考团队之间能够实现快速的信息交流。

当然，计算机网络的建设不是一蹴而就的。在探索这个星球的过程中，不得不借助一些传统的通信手段，并且需要使用一些口头的约定来传达信息。但不同团队之间有不同的通信约定，反而导致了通信的混乱。为此，你需要有一种统一的约定来保证不同团队之间都能够顺畅地传输信息。作为网络工程师，你会如何思考这个问题呢？

项·目·任·务

任务 1

通过查阅资料等方式，梳理出：计算机网络出现之前，人类使用的传统通信方式；计算机网络自身的发展历程；其中我国的成就与贡献。用思维导图的方式呈现以上内容。

任务 2

根据科考队所面临的不同任务和条件，给出在该任务和条件下应该使用的网络类型。

任务 3

在没有依赖电力的电话、计算机网络等通信手段的情况下，设计一种能够保证两个科考团队顺畅通信的方法，并以此解释“协议”与“层”的概念。

第一节　计算机网络发展和组成

本节首先回顾人类通信的发展历史，认识计算机网络对通信的革命性影响，了解计算机网络发展进程中的标志性事件，并初步认识计算机网络的软硬件组成。

体　验　思　考

从古到今，人类的生活都与通信息息相关。通信的发展也极大地促进了人类生产力的发展，推动了社会的进步。在当今的信息社会，每位中学生都需要认识和理解以计算机网络为代表的通信技术发展对人类社会所产生的重要影响。

思考：在人类通信技术及计算机网络技术发展历程中，有哪些标志性事件？

一、通信技术与计算机网络的发展历史

1. 从烽火狼烟到计算机网络

数千年前的一天黄昏，一位戍守边关的士兵，焦急地在烽火台上燃起烟火，向十里之外的另一个烽火台传递着敌情信息。

战场瞬息万变，谁掌握了最新的信息，谁就获得了制胜的砝码。很显然，上面这位士兵所做的，就是要将信息以最快的方式发送出去。然而，几千年来，人们发送信息的方式也在不断地发生着变化，继烽火狼烟之后，又发明了飞鸽传书、电报、电话等种种通信的方法。

随着经济社会的发展，以烽火和信鸽为主要通信手段的时代已经一去不复返，电报也早已退出了历史舞台。电话虽然还是人们生活中的一部分，但或许已并非人们相互沟通的最主要渠道了。时间来到了今天——信息时代，人们通信的方式又发生了重要的变化。以军事战场为例，前线的士兵通过佩戴的联网电子设备拍摄下战场动态，与此同时，千里之外的指挥部大屏幕上，就能够实时显示来自前线的实况影像，使指挥官能够迅速做出战略判断。

从烽火、信鸽，到电报、电话，再到计算机网络，人与人之间传递信

息的速度越来越快，所传递的信息量也越来越大（如图 1.1 所示）。计算机网络，这个诞生于 20 世纪下半叶的新兴事物，正在快速改变着人类所处的世界。

图 1.1　从烽火狼烟到计算机网络

2. 计算机网络的诞生

20 世纪 60 年代，出于军事方面的需要，人们开始尝试将若干台计算机相互连接起来，使这些计算机能够相互传输数据。阿帕网（ARPAnet）由此诞生，成为互联网的前身。阿帕网最开始只有 4 个节点（如图 1.2 所示），网络传输能力只有 50 Kbps（Kbps 是一种网络传输速度的单位，表示每秒传送多少千比特），按现在的标准来看这是“极慢”的网速。1972 年，阿帕网发展到大约 15 个节点。到了 20 世纪 70 年代末，大约有 200 台主机连接到了阿帕网。

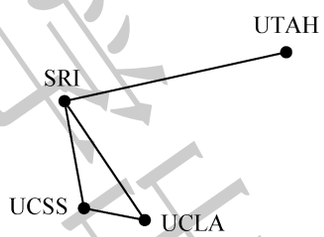


图 1.2　阿帕网（ARPAnet）

从 20 世纪 70 年代早期至中期，除阿帕网之外的其他网络也应运而生，其中包括了 ALOHAnet、Telenet、Tymnet、Transpac 等，网络数量开始增长。计算机网络开始发挥更多的作用。

1973 年，罗伯特·梅特卡夫（Robert Metcalfe）提出了一种被称为“以太网”（Ethernet）的通信原理及技术，这一技术后来导致了局域网（LAN）的爆发性增长，也使得以太网的技术快速更新（详见本书第二章）。此时，开发一种将所有网络连接在一起的全面架构的时机已经悄悄成熟了。计算机网络即将步入快速发展的时期。

1974年，文顿·瑟夫（Vinton Cerf）和罗伯特·卡恩（Robert Kahn）设计了一种“开放的网络架构”，可以使不同环境中的计算机相互联系，形成一个“网际网”。这个“网际网”就是现在的互联网（Internet，又称因特网）。

互联网在其诞生后迎来了快速发展。20世纪80年代，连接到互联网的主机数量不断增长，但此时使用互联网的技术操作较为复杂，主要用户群体还是科研人员。1989年，蒂姆·伯纳斯-李（Tim Berners-Lee）设计了万维网（world wide web，简称WWW），它极大地降低了在网络上获取信息的技术门槛，将互联网带入了每一个人的生活中（详见本书第三章）。自此以后，互联网开始真正地走入了千家万户。

在万维网的发展历程中，出现了各种各样划时代的科技产品。1994年，网景公司推出了Netscape浏览器，人们开始使用浏览器来访问网页，获取各种信息和服务。同是1994年，杨致远（Jerry Yang）和大卫·费罗（David Filo）创立了雅虎，开始面向大众提供搜索引擎、电邮、新闻等服务。各种各样的公司也开始通过互联网进行商业交易，1995年，杰夫·贝佐斯（Jeff Bezos）创办了亚马逊公司，开始通过网络销售商品。近年来，我国的互联网产业也发展迅猛，阿里巴巴、腾讯、百度是其中有代表性的公司。

从阿帕网到局域网，再到互联网，计算机网络已成为了日渐影响人类生产生活的重要工具。

二、走近计算机网络

1. 计算机网络组成

在了解了计算机网络的发展历史后，接下来要回答的问题是：什么是计算机网络？今天的计算机网络都包含了哪些基本的组件呢？

（1）网络硬件

首先，计算机网络离不开“计算机”这个最为重要的组成单元。我们最为熟悉的计算机网络实例之一就是校园中的机房。在机房里，一台台计算机通过网线连接在一起形成网络。同学们可以通过网络将作业提交给老师，老师也可以通过网络将教师机的显示内容播放到学生机的屏幕上。

现代社会中很多人都拥有智能手机和平板电脑，可以随时随地

图 1.3　可以连接到网络上的计算设备

浏览网页、收发邮件、在线聊天等，这些可以上网的设备也同样处于计算机网络之中。从这一角度出发，计算机网络中的“计算机”并不只限于传统意义上的台式电脑，而是一切可以连接到网络上的计算设备。比如，日常生活中使用的笔记本电脑、智能手机、平板电脑、智能手表、智能摄像头、智能电视、智能扫地机器人等等，都属于这一范畴。

计算机与计算机的连接需要通过物理介质，这就是通信线路。例如，在我们生活中常常可以见到网线，它就是最常见的通信介质之一。

现在，许多人的家里都安装了无线路由器。当人们连接到互联网时，连接计算机网络的并非只有网线，路由器也是其中的一个部分。事实上，一条网线最多只能将两台电脑连到一起，这还算不上典型的“网”。而只有在具备了路由器、交换机这样的“枢纽”条件下，这些设备才能够通过网线连接到一起，变得像是一张真正的“网”。（路由器、交换机详见本书第二章）

由此可知，在计算机网络中，除计算机外，还包括各种各样的传输介质和设备（如网线、交换机、路由器等），它们共同协作，在通信过程中发挥了各自的功能，与计算机一起并称为“网络硬件”。因此，在计算机网络中，硬件是计算机、网络设备和传输介质等物理装置的总称。

（2）网络软件

计算机与计算机的连接还需要一些功能程序，即“软件”。许多同学都有过在电脑或者手机上使用聊天软件，向朋友发送文字、图片或视频的切身体验，这些软件工具也是计算机网络中的一个组成部分。通过软件，人们才能更好地利用计算机网络。

软件不仅包含人们经常使用的各种网络上的应用软件，还包括了网络通信协议、网络管理软件、网络操作系统等。其中，网络操作系统（network operation system，简称 NOS）是一种重要的网络软件，它提供了基础的平台和环境，使得人们能够更加方便地使用网络上的各种功能应用。网络操作系统支持网络文件管理、网络安全管理、网络可靠性措施、多种网络协议、网络资源管理和网络服务管理等特性。早期的操作系统被称为单机操作系统，如 MS-DOS、Windows 3. x 等并不支持上述功能。现在人们常用的操作系统，如 Windows、Linux、iOS、安卓等都支持上述网络功能，因此它们都属于网络操作系统。

综上所述，计算机网络就是将不同的计算机，通过通信线路（如网线等）和通信设备（如交换机、路由器等）连接起来，在软件（各种应用软件、通信协议等）的作用下，实现信息传递的一种系统。

2. 计算机网络对现代社会的意义

（1） 计算机网络与人们的生活

计算机网络所带来的技术变革，在较短的时间内极大地提升了社会生产力，改变了人们工作、生活的方式。计算机网络最重要的特征是连通性和共享。

如今，小到一条短信，大到一套图书、一系列视频，都可以通过网络快速便捷地传递。计算机网络促进了信息资源的共享。足不出户而知天下事，在今天成为了现实。通过网络，我们不仅可以分享文字、图片、音频、视频等，还可以分享计算机软件，甚至计算机的硬件也可以通过网络共享。获取资源和分享资源也成为了现代人们工作和生活中的必备技能。

计算机网络实现了生产效率的提升。如今，人们可以通过网络便捷地查询、购买商品，商家也可以通过网络向大众推广自己的产品，这极大地促进了社会商品的流动，改变了传统的零售商业模式。在生产的各个环节，网络也在控制、协调、任务处理等方面发挥着巨大的作用。

同时，计算机网络还改变着人们的学习方式。通过网络，每一位同学都能够方便地查找到海量的学习资料，极大地拓展个人的视野。随着移动网络、智能设备等技术的不断发展，方便高效的个性化学习已成为了现实。

（2） 计算机网络的创新发展——“互联网+”

以互联网为代表的计算机网络已经成为人们生活中不可或缺的一部分，而随着技术的不断发展，互联网开始颠覆各种传统行业，不断超越着人们的想象。

以出租车行业为例，当移动互联网和定位技术逐步成熟后，新的技术和应用环境逐步解决了传统出租车行业中存在的弊端，手机打车软件以其便利和优越的服务迅速征服了用户。互联网与出租车行业的融合形成了新的商业模

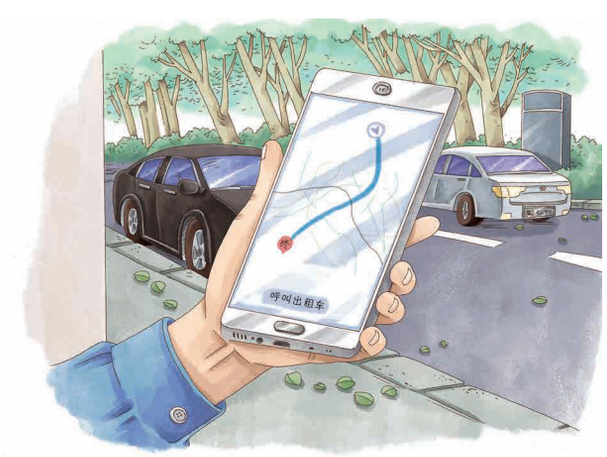


图 1.4　使用手机打车软件

式，这样的创新模式如今有了专门的称谓——“互联网＋”。

近年来，“互联网＋”这一话题的热度不断提升，各行各业开始重新审视其在与互联网的互联交融中实现价值增值的种种可能性。我国制定了“互联网＋”战略行动计划，推动移动互联网、云计算、大数据、物联网等新兴技术与现代制造业结合，促进电子商务、工业互联网和互联网金融等业态的健康发展。总体而言，“互联网＋”代表了一种新的经济形态，即充分发挥互联网在生产要素配置中的优化和集成作用，将互联网的创新成果深度融合于经济社会各领域之中。

知 识 延 伸　　关于“互联网＋”中的加号

“互联网＋”聚焦于利用互联网技术对传统行业形成渗透和改变。“互联网＋”所要“加”的，就是传统的各行各业。例如，互联网“加”到传统媒体行业之后，产生了网络媒体，对报纸、电视、户外广告等传统媒体业态造成了巨大冲击；互联网“加”到娱乐行业之后，各种智能硬件设备都开始具备了和娱乐内容结合的能力，并由此产生了在线阅读、网络游戏、网络直播等新的娱乐业态；互联网“加”到传统零售行业之后，产生了电子商务和新零售等新的业态，并促进了快递物流、移动支付等行业的蓬勃发展，使人们的生活变得更加便利。可以说，每一个传统行业都孕育着“互联网＋”的机会。

（3） 计算机网络与网络安全

互联网为人们带来便利的同时，也带来了一定的信息安全隐患。网络上不时爆发的各种隐蔽、怪异的病毒，时刻觊觎着人们的网络设备，从网络上接收的一些来路不明的图片、邮件或文件，有可能让人们的计算机系统顷刻瘫痪。在网络时代，信息的传递速度越来越快，信息传播成本与获取门槛越来越低，而这也促成了虚假、错误信息的泛滥。在当今这个信息时代，如果不对网络安全加以重视，计算机网络就可能变利为弊，给个人和社会带来灾难性的后果。

2016 年，我国颁布了《网络安全法》，明确了个人和企事业单位在网络空间安全事业中的责任，保障网络安全，维护网络空间主权和国家安全、社会公共利益，使得我国经济社会信息化健康发展有法可依。

影响网络安全的因素很多，其中人为的因素危害较大。要抵御这些人为的网络攻击，大家需要具备基本的个人信息保护意识，养成良好、正确的网络使用习惯。此外，大家还应了解一些基本的网络安全技术，其中包括网络加密技术、防火墙技术等（详见本书第四章）。

作业练习

回顾通信技术与计算机网络的发展历史，思考计算机网络对现代社会的重要影响，尝试将各个标志性事件及其意义与价值绘制成思维导图。

通信和计算机网络发展史思维导图

第二节　网络类型

计算机网络是一个复杂的体系，有着各种各样的类型。例如，按照分布范围，网络可分为局域网和广域网；而按照使用权属，网络又可分为公用网和专用网。

体　验　思　考

在生活中经常会遇到互联网、局域网、校园网等带有“网”字的词汇，其中，大部分的“网”都指代了某种网络。要正确区分不同的“网”，我们就需要对网络的主要类型加以了解。

思考：计算机网络有哪些主要的网络类型？各种类型的网络分别具有什么特征？

一、局域网与广域网

按照网络的分布范围，网络可以被主要划分为局域网和广域网。

1. 局域网

局域网（local area network，简称 LAN）是在较小范围内组建的网络，比较适合家庭、学校、企业、政府机构等单位和组织构建内部互联互通的计算机网络。例如，许多学校的校园网就是一种局域网，企业内部搭建的企业网也是一种局域网（如图 1.5 所示）。

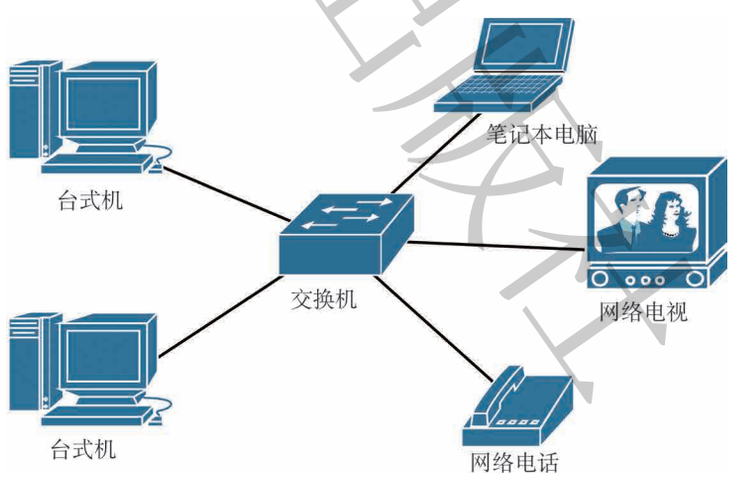


图 1.5　局域网模式图

2. 广域网

广域网(wide area network,简称 WAN)的覆盖范围从几十公里到几千公里,可能覆盖一个省,一个国家,几大洲甚至全球(如图 1.6 所示)。互联网就是一种广域网。广域网本身也可能是由另一些局域网或广域网组成的多级网络。

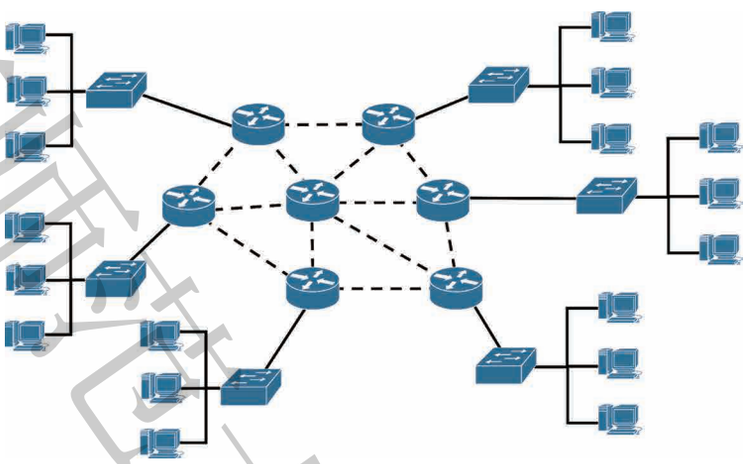


图 1.6 广域网模式图

知 识 延 伸　　城域网

此外,有些文献中也会把城域网(metropolitan area network,简称 MAN)作为一种独立的网络类型来分类。城域网的覆盖范围大于局域网,它能够覆盖一座大城市的地理范围。城域网可以将位于同一城市内不同地点的计算机设备,以及多个局域网互相连接起来。城域网的传输媒介主要为光纤,其传输速率通常在 100 Mbps(兆比特/秒)以上。

二、公用网和专用网

按网络的使用权属,网络可以被划分为公用网和专用网。

1. 公用网

公用网又被称为公共数据网,顾名思义,是为大众所用,向所有人提供服务的网络。例如,人们在家中较常使用的中国电信网络

ChinaNet，就是一种公用网。

2. 专用网

与公用网相对应的是专用网。专用网可以被理解为某些特定群体内部使用的网络，也可以被通俗地称为“内部网”。例如，某个学校的校园网就是一种专用网，因为通常学校之外的人群是无法访问这一网络的。实际上，大部分局域网都可以被视为专用网。而一些军事、运输、金融等领域的网络由于覆盖范围较大，同时有着较强的保密和内部使用属性，虽然其为广域网，但也同样是专用网。

项 目 实 践

科考队员们四散在星球各处，建设了许多居住点。有的居住点相距很近，聚集到了一起，形成小型的社区。而有的居住点则相距遥远。此外，医生、建筑师、农业专家等各行业人员还对网络的专用性提出了一定要求。网络工程师面对这种复杂的情况该如何应对呢？如果你是一名网络工程师，面对以下情境，你会如何选择对应的网络类型呢？请将答案填写在表 1.1中。

表 1.1 根据情境选择网络类型

情境描述	你所选择的网络类型
在一平方公里的范围内有一些居住点，其中的科考队员们希望通过网络共享资料	
相隔数千公里的居住点中的科考队员们希望能够通过网络视频互相联系	
科考队中的医生们希望共享病人数据，但不希望这些信息公开给其他人	
科考队中的记者希望将新闻及时发布到网络上，使得所有人都能及时了解星球上发生的最新事件	

第三节　计算机网络中的协议与分层结构

在本节中，我们将学习和了解计算机网络中的一些关键性的专有名词，如协议、层等。本节的学习将为我们在后续章节深入了解计算机网络世界打下基础。

体　验　思　考

网络中随时随地在传输大量的数据，如果把这些数据看作现实生活中的“货物”的话，这绝对是一件匪夷所思的奇迹——在庞大的传输体系下，所有的传输过程看上去都井井有条。这是怎么实现的呢？在这里，网络中的协议和层都起到了重要的作用。

思考：你知道计算机网络的结构分为哪几层吗？为什么人们需要将计算机网络划分为不同的层？生活中又有哪些与计算机网络中的分层结构类似的事物？

一、计算机网络中的协议

在计算机网络与信息通信领域里，最常见的一个词可能就是“协议”。网际协议（internet protocol，简称 IP）、传输控制协议（transmission control protocol，简称 TCP）、超文本传输协议（hypertext transfer protocol，简称 HTTP）等都是互联网中常用的、具有代表性的协议。那么，在计算机网络的世界里，协议的意义和作用是什么？为什么计算机网络需要协议呢？

1. 生活中的协议

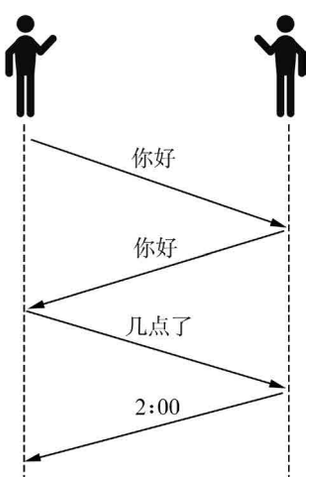


图 1.7　人与人交流的“协议”

在现实生活中，若你想要向他人询问时间，你会怎样做呢？

按照人与人沟通的“协议”，询问的一方应该首先问候对方“你好”（如图 1.7 所示），从而有礼貌地开始对话（在计算机网络中，这样的信息被称为一条“报文”）。如果被询问者也回答一个“你好”，这就表示对话可以继续进行下去，发话者能够继续询问时间了（在计算机网络中，我们将前一个“你好”视为“发送报文”，后一个“你好”视为“应答报文”）。而如果被询问者回答的是“我现在正忙”，或是“I can't speak Chinese”，那么按照人与人沟通的“协议”，发话者就不能继续询问时间了。此外，问候的结果也可能是根本得不到任何回答，此时，发话者

通常会放弃向对方继续询问。在这个例子中，发送和应答的报文，以及相关事件出现时所采取的动作（例如在某个给定的时间内对方没有回答），都在人与人的沟通中起到了核心作用。

如果人们使用不同的“协议”，例如，一个人说汉语，而另一人说英语，或一个人明白“时间”这个概念，而另一人却不知道，那么双方很可能就无法有效交流，因而不能实现“询问时间”这样的目标。

2. 计算机网络中的协议

在网络中，这个道理同样成立。为了完成一次通信，两个（或多个）通信实体都要使用相同的协议。这里的“通信实体”指的是网络中的硬件设备或软件组件，可以是计算机，也可以是交换机、路由器等用于网络通信的设备，还可以是运行在这些设备上的程序或软件。

在互联网中，凡是涉及两个或多个远程通信实体的所有活动都受到协议的制约。协议就是计算机与计算机之间通过网络实现通信时事先达成的一种“约定”。这种“约定”使那些由不同厂商生产的设备及不同的操作系统组成的计算机之间，只要遵循相同的协议就能够实现通信。反之，如果所使用的协议不同，就无法实现通信。这就好比两个人使用两种不同的语言交流，就无法相互理解一样。

以一个最常见的浏览网页行为为例。当你在网页浏览器中键入一个网址，并按下回车键时，你的计算机就会向一台远程计算机（被称为“服务器”，详见第三章）发出浏览网页的请求。首先，你的计算机向该服务器发送一条连接请求报文，并等待回答，这类似于人与人之间问候“你好”。该服务器接收到连接请求报文，并返回一条连接响应报文，表明自己愿意和你的计算机通信。接收到连接响应报文后，你的计算机会再发送一条请求报文来请求网页。最后，服务器向计算机返回网页内容（如图 1.8 所示）。

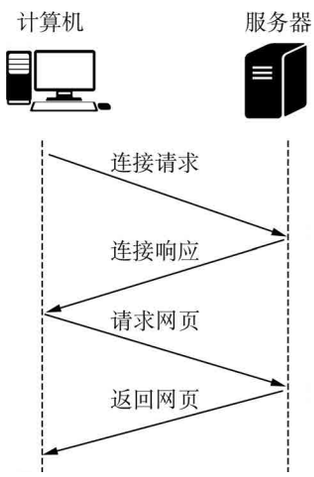


图 1.8　计算机网络协议

通过以上例子可以发现，一个协议包含了在两个或多个通信实体之间交换的报文格式、次序，以及处理报文时所采取的动作。互联网广泛地使用了各类协议，不同的协议用于完成不同的通信任务。本书在后续章节中将进一步讨论各种协议。

二、计算机网络中的分层结构

计算机网络是一个非常复杂的系统，在这一庞大的系统中，不同类型的计算机之间要相互连接，还要运行不同的应用程序和协议，要

能够高效、准确地传输数据，并不是那么容易的事情。试想，在亚马逊丛林里居住的土著人，和在太平洋的海岛上悠闲度假的游客，无论是在地理位置、语言上，还是对世界的理解方式上，都存在着巨大的差异，他们之间的沟通无疑具有巨大的鸿沟。那么，如何才能使这样一种异常复杂的系统高效通信、有效运行呢？

1. 层次化的网络协议体系

模型是现实世界中人们对事物、规律的合理简化。计算机网络的设计者采用了分层结构的方法来组织网络中各种协议，以及运行这些协议所必需的网络硬件和软件。在实际应用中，我们通常将计算机网络体系自上而下地分为五个层，分别是应用层、传输层、网络层、数据链路层和物理层。它们有机结合，共同构成了一种有序的网络传输体系。每个层的主要作用如下：

- 应用层：主要负责通过应用进程（详见第三章）间的交互来完成特定网络应用。应用层交互的数据单元称为报文（message）。
- 传输层：主要为应用进程之间提供端到端的逻辑通信。传输层提供通用的数据传输服务来传送应用层的报文。在该层中数据传输单位有两种，分别是报文段（segment）和用户数据报（user datagram）。
- 网络层：主要负责确定数据最佳的传输路径。在发送数据时，网络层把传输层产生的报文段或用户数据报封装成分组或包（packet）进行传送。网络层中传送的数据单元可被称为 IP 数据报，或简称数据报（对于网络层传送的数据单元，也有些书中笼统地用“分组”来表示）。
- 数据链路层：主要负责相邻结点之间的通信传输。数据链路层将网络层的数据封装成帧（frame），并在两个相邻结点间的链路上传送帧。
- 物理层：主要负责比特流的传送。包括规定用多大的电压代表“1”或“0”，以及接收方如何识别发送方所发送的比特，连接电缆的接头应该有多少根引脚，各引脚应如何连接等。

分层体系结构中的数据的传输过程可以采用如图 1.9 所示的理想化场景描述。假定小林和小明这两位同学的电脑是通过网线直接相连的，当小林通过聊天软件向小明发送一段消息时，小林电脑上的聊天软件通过应用层在该数据之前加上必要的控制信息 H5（首部）形成应用层报文，再将该报文交给传输层。传输层加上本层的控制信息（H4）后，再交给网络层。网络层加上本层的控制信息（H3），再交给数据链路层。数据链路层的控制信息被分成两部分，分别加到数据单元的首部（H2）和尾部（T2）。物理层则以比特流的方式，从数据链路

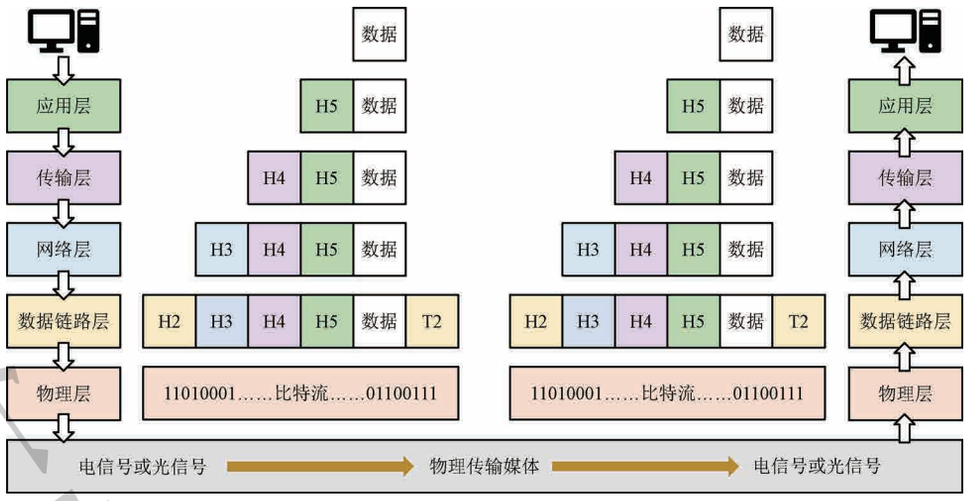


图 1.9　数据在各层之间的传输过程

层首部开始传送以上的数据单元。当这一比特流到达小明的电脑时，再从物理层依次向上传递，每一层均根据本层的控制信息进行必要的操作，然后将控制信息剥去，将该层剩下的数据单元上交给更高层。最后，小明电脑中的聊天软件解析应用层报文中的数据，并呈现在计算机屏幕上，小明就能够看到小林发送过来的消息了。

知　识　延　伸　　**协议数据单元**

计算机网络中有很多看起来很相似的表述，如报文、包、帧、数据包、数据报、数据段、消息等。为了明确这些概念，本书中它们的定义如下：我们用“数据包”（同义词为包或分组，源自英文 packet）表示通过网络传输的格式化数据单位。在 TCP/IP 协议中，每个数据包在不同的层之间传输的时候，会按照各层的协议数据单元格式进行封装。自上而下，数据通过“报文”（message）在应用层之间传输，而当“报文”通过 TCP 传输时，它被封装为传输层“段”（segment），当通过 UDP 传输时，“报文”被封装为传输层“用户数据报”（user datagram）。传输层的“段”或“用户数据报”进一步被封装为“数据报”（datagram）通过网络层传输，在数据链路层，数据报封装为“帧”（frame），继而通过物理层转化为比特流，传输到网络中的下一个节点。

这些名词和概念，我们在后续章节中还能看到很多次。

2. 分层体系结构的作用和优点

计算机网络的分层体系结构是一个有效的协作体系，每个层都接受由它下一层所提供的特定服务，并且负责为自己的上一层提供特定的服务。分层体系结构中还存在“接口（interface）”和“协议（protocol）”这两个术语，前者是指上下层之间进行交互时所遵循的约定，后者是指同一层的对等通信实体之间的交互所遵循的约定。前文

“烽火狼烟”中提到的烽火台之间的信号就是一种“协议”。

在通信过程中，数据从发送方到达接收方的过程也就是各个层共同协作的过程。当发送方发送数据的时候，从应用层开始，每一层对数据进行该层的相应处理，然后转交给下一层，直到物理层进行数据传输，然后，当接收方接收数据的时候，则从下往上对每一层进行数据处理，这样就能获取发送方的原始内容。

计算机网络中的通信需要首先确保数据传输的可靠性，这就像生活中给朋友写信，我们要确保信件经过千山万水、长途跋涉后，能够顺利到达朋友手中，而不是半路丢失或去了陌生人手里。而层模型则通过数据链路层和网络层的“点到点”和传输层的“端到端”保证了数据传输的可靠性。其中，“端到端”通信指的是在数据传输前，在数据的发送端到接收端之间建立起一条连接，而忽略掉跨越其间的各种各样的交换设备。一旦这样的连接建立后，发送端就可以开始发送数据，直至数据发送完毕，接收端确认接收成功。“点到点”通信指的是发送端把数据传给与它直接相连的设备，这台设备在合适的时候又把数据传给与之直接相连的下一台设备，通过一台一台直接相连的设备，把数据传到接收端。

使用分层体系结构的优点在于可以最大限度地减少网络传输的复杂性。各种协议应用在不同的层，分别担负起不同的职能，界定了各个分层的具体责任和义务。各层可以灵活地实现自己的功能，只要满足上层对下层的要求即可。各个分层也是独立的，对一个层的改动不会影响其他的层。这样，就构建起了一个兼具扩展性和灵活性的系统。

项 目 实 践

在星球建设初期，通信网络还没有完全建设好，科考队员们在工作中达成了一些关于交流的约定。例如，当一位队员要向前方的另一位队员询问前方的情况时，他会用手电筒快速闪烁两次，表示“你好”。当前方的队员也回以两次快速闪烁时，表示可以继续通信。通信发起者可以再以手电筒“三长一短”的方式闪烁，表示“前方安全吗？”如果前方队员回以一次快速闪烁，表明“前方安全”，但若是回以两次快速闪烁，则表示“前方有危险”。试设想一种科考队员的沟通场景，尝试一次角色扮演活动，小组成员各自选取角色，演示使用一种协议完成通信的过程，填入表 1.2中。

表 1.2 科考队员之间的协议过程

扮演的角色	角色行为	达成的协议
同学 1：_____		
同学 2：_____		

第二章

走近真实网络

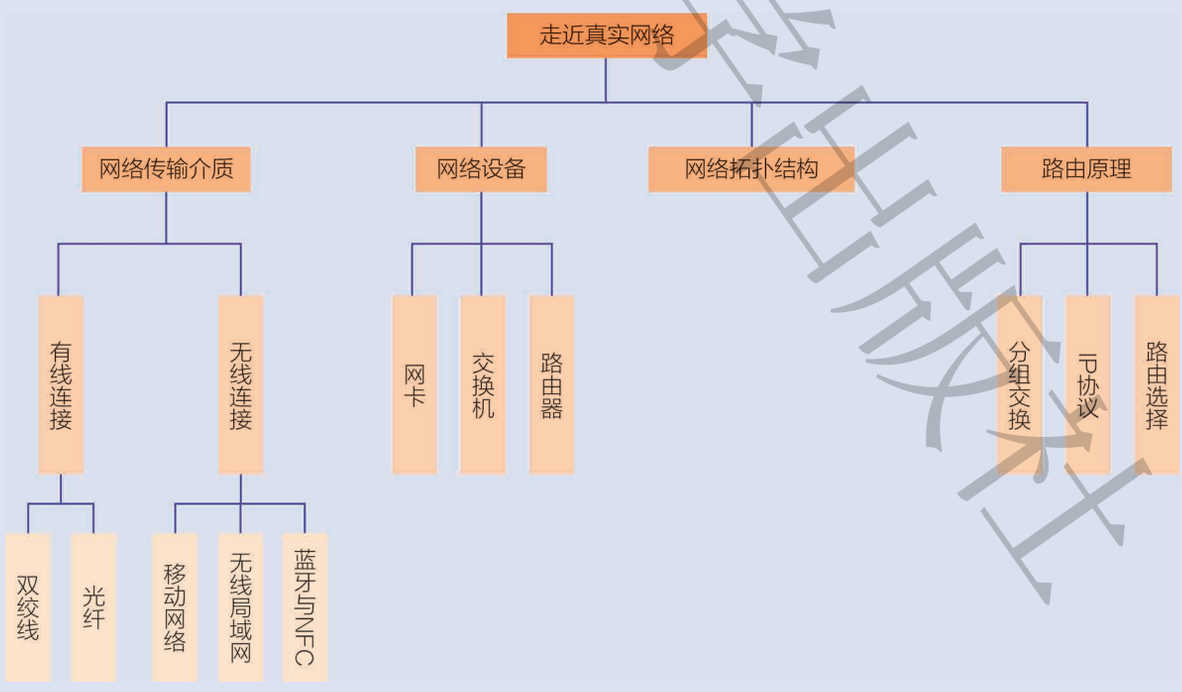
本章学习目标

- 描述双绞线、光纤、同轴电缆等传输介质的特点，识别不同的无线连接方式，描述影响网络传输质量的主要物理因素。
- 描述网卡的功能，描述交换机、路由器的功能和它们的区别。分析现有的网络拓扑图，并根据需求绘制网络拓扑图。能描述交换机学习转发过程。
- 识别 IP 地址的类型，使用 ICMP 协议及相关网络命令检查网络节点的连通性。区分 IPv4地址和 IPv6地址。
- 解释路由选择原理，根据需求识别报文的转发路径。

如今，互联网已经发展成为覆盖全球的计算机网络。在互联网中，有数以亿计的计算机、平板电脑和智能手机终端，通过大量网络节点和连接这些网络节点的链路互联在一起，彼此交换信息和分享资源。在这样一种复杂的体系中，都有着哪些关键的传输介质和网络设备？它们如何有效协作，各自在网络中发挥了哪些作用？真实世界中的网络通信，是如何通过这些介质和设备实现的？

让我们带着这些问题，走近真实的计算机网络世界，认识各种不同的传输介质，了解交换机、路由器、防火墙等网络设备，学习网络通信的真实过程，并探究 IP 协议的原理和路由过程。

本章知识结构



项目主题

组建小型网络

项·目·情·境

为了实现在新的星球上建立计算机网络的目标，你所在的网络工程师团队成立了网络实验室。你和同伴们打算先从小规模网络开始搭建，以验证各种网络设备和通信协议。除此之外，你还要负责向其他的科考团队说明网络组件的功能和作用。

项·目·任·务

任务 1

学会区分网络实验室中的各种设备，阐述它们的名称、原理和作用。

任务 2

使用网络实验室中的设备或虚拟组网软件组建一个小型的网络，并思考如何简洁而准确地表示你所组建的网络。

任务 3

采用流程图、表格等方式，解释说明计算机网络中的两台计算机是如何相互传输数据的。

第一节　网络传输介质

要实现两台计算机之间的相互通信，必须使用相应的传输介质。这些介质可以是有形的“线”，也可以是无形的“电磁波”。我们从常见的网络传输介质开始认识网络，并了解影响网络传输质量的物理因素。

体　验　思　考

从 1997年起，中国互联网络信息中心（CNNIC）每半年发布一次《中国互联网络发展状况统计报告》。图 2.1显示了 2010年～ 2018年中国每年的手机上网用户数量和占网民整体数量的比例。可以看到，手机用户数量由 2010年的 2.33亿人迅速增长到 2018年的 8.17亿人，且手机上网用户数量占整体网民数量的比例也从 2010 年的 60%增长到 2018 年的 98%。而台式机、笔记本电脑上网用户的增长率在逐年走低。手机上网成为了多数网民的首选方法。据估算，随着 5G 网络的商用化，采用手机上网的网民数量和所占比例将会迎来新一轮的迅猛增长。

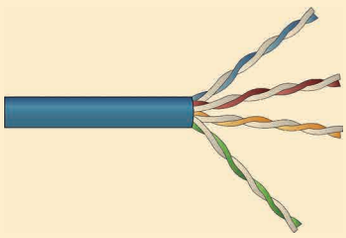
图 2.1　2010~2018年手机上网用户数量和占整体网民比例

思考：你觉得将来无线网络会完全取代有线网络吗？“网线”会从人们的生活中消失吗？

一、有线连接

我们已经在必修二《信息系统与社会》中学习了两种常见的有线网络传输介质：双绞线和光纤。表 2.1 对此做了回顾和总结。有线连接的优点是信号传输质量比较稳定，但是如果采用有线方式接入网络，主机往往是固定在某一个地方，如果要使主机能够随时随地接入网络，有线连接方式就无能为力了。因此，近年来无线连接方式越来越流行，后面将重点阐述无线网络的种类和特性。

表 2.1　常见有线网络传输介质总结

名称	双绞线	光纤
外观		
主要物理特性	1　传输电信号。 2　有效传输距离　100米左右。 3　主要用于构建局域网。 4　成本较低，加工较方便。	1　传输光信号。 2　传输距离较长，为数公里至数百公里。 3　可用于构建城市主干网等广域网。 4　成本较高，加工难度较大。

知　识　延　伸　　**光纤之父**

光纤是一项非常重要的发明，它极大地改变了人类的通信方式，推进了人类的科学进程。但你知道是谁发明了它吗？

光纤的发明者实际上是一位华裔物理学家——高锟。高锟出生在上海，1954年赴英国攻读电机工程。此前，通信的传输主要通过铜丝来完成，然而这一传输过程也是信号不断衰减的过程，传输损耗较大。1966年，高锟发表了一篇题为《光频率介质纤维表面波导》的重要论文，开创性地提出了用玻璃代替铜线的设想——利用玻璃清澈、透明的性质，使用光来传送信号。在不断探索下，高锟最终发明了石英玻璃，制造出了世界上第一根光导纤维。与此前的传输方式相比，光纤传输具有传输容量大、损耗低、重量轻、抗干扰能力强、保真度高、工作性能可靠、性价比高等优点。

图 2.2　高锟

1996年，中科院紫金山天文台将编号为“3463”的小行星命名为“高锟星”，以表彰“世界光纤之父”高锟在科学上的杰出贡献。2009年，高锟因在“有关光在纤维中的传输以用于光学通信方面”的突破性成就，获得诺贝尔物理学奖。

二、无线连接

近年来，随着移动设备的发展和繁荣，人们又将互联网时代划分为了两类，一类是过去的“传统互联网时代”，而另一类则是现在已到来的“移动互联网时代”。

在移动互联网时代，上网设备不再需要笨重的、长长的网线，而是

以更加直接、轻便的方式进行连接，这就是无线网络连接。这种无形的“线”大大拓展了计算机网络在社会生活中的应用场景，使每一个人随时随地与网络连接到一起成为可能。

1. 移动通信网络

对于手机等移动设备而言，最常见的无线网络连接方式就是移动通信网络。在使用移动通信网络的过程中，数字信号从基站发出，通过特定频率的电磁波传输给接收端。移动通信网络在这十几年间经历了从 1G、2G、3G、4G 到 5G 的技术发展。其中，G 是英文“代”(generation)的首字母，5G 即代表第五代移动通信网络技术。

4G 移动通信网络目前已经得到了广泛应用，它的上传和下载速率分别能达到 50Mbps(每秒传送 50 兆比特)和 100Mbps(每秒传送 100 兆比特)，这意味着它可以快速传输包括高质量音视频在内的各种数据。在我们使用智能手机时，可以通过屏幕上显示的通信标识来确定自己连接的网络类型。目前，我国采用的 4G 移动通信频率为 1.8GHz～2.6GHz，而到了 5G 时代，5G 网络的通信频率将会达到 24GHz 以上，这就会使数字信号的传输速度更快。同时，5G 还采用了多天线技术，这意味着将具有更加密集的天线和更强的信号处理能力。因此，5G 网络的速度将会更快(达到 10Gbps，即每秒传送 10G 比特)，延迟更短(1 毫秒以下)，覆盖率更高。本书将在第三章对 4G 技术和 5G 技术进行更详细的解读。

2. 无线局域网

和安装了移动通信模块的手机不同，对于平板电脑等移动设备而言，它们最常见的无线网络连接方式是无线局域网。

无线局域网又常被简称为 WLAN(wireless local area networks)。WLAN 利用射频技术，使用电磁波在空中进行通信连接，使得用户手中的设备能够无线接入到局域网，继而通过局域网实现与互联网的连接。

在 WLAN 的各种技术产品中，Wi-Fi(wireless-fidelity)是最为大众熟知的一种技术，它的传输速度较高(约 450 Mbps)，有效距离也较长(有效覆盖面积可达 80 平方米)，因此在办公室、家庭、公共设施等场所中被广泛使用。目前，几乎所有智能手机、平板电脑和笔记本电脑都安装了 Wi-Fi 模块，支持通过 Wi-Fi 连接到网络。

提供 WLAN 上网的信号发射点常常又被称为“热点”。目前，一些国内城市的重要公共区域已具备了热点覆盖，为公众用户提供免费上网服务，其中较具代表性的有上海的 i-Shanghai 等。

3. 其他无线网络连接方式

除了移动通信网络和无线局域网外，移动设备还常常采用如下两种方式实现无线网络连接。

（1）蓝牙：英文名为 Bluetooth，是一种无线技术标准，目前的有效距离一般在 10 米以内。具有蓝牙的设备之间可以相互匹配，并进行无线通信。和 Wi-Fi 一样，目前大多数移动设备均配备了蓝牙模块。此外，常见的蓝牙设备还包括蓝牙耳机、蓝牙音箱、蓝牙鼠标、蓝牙键盘等。

（2）NFC（near field communication）：近场通信技术。NFC 技术由非接触式射频识别（radio frequency identification，简称 RFID）演变而来，该技术在单一芯片上结合感应式读卡器、感应式卡片和点对点的功能，能在短距离内与兼容设备进行识别和数据交换。NFC 目前主要被用于移动支付、身份验证等。

本书第六章中，我们将对蓝牙和 NFC 做更详细的介绍。

知 识 延 伸　量子通信

目前还有一种新型的无线通信方式——量子通信。量子通信是指利用量子纠缠效应进行信息传递的一种新型的通信方式。量子通信是近二十多年发展起来的新型交叉学科，是量子论和信息论相结合的新的研究领域。量子通信主要基于量子纠缠态的理论，使用量子隐形传态（传输）的方式实现信息传递。根据实验验证，具有纠缠态的两个粒子无论相距多远，只要一个发生变化，另外一个也会瞬间发生变化，利用这个特性，就可能实现量子通信。量子通信主要涉及量子密码通信、量子远程传态和量子密集编码等。由于高效安全的信息传输日益受到人们的关注，近来这门学科已逐步从理论走向实验，并向实用化发展。

三、影响网络传输质量的主要物理因素

数据通过电信号形式在传输介质中传输，必然会受到传输介质本身的物理因素影响。影响网络传输质量的物理因素中，最主要的是噪声和衰减。

1. 噪声

数据是以电信号的形式在传输介质中传输的，而电信号的本质是大量正弦波的叠加。在信号的传输过程中，很容易受到外界的干扰而引入一些随机的信号（如随机产生的电磁波），这就是外部噪声；电磁波在传输介质中传播时也可能会产生干涉，从而相互叠加或相互抵消，这就是内部噪声。噪声会影响网络传输的稳定性。例如，在一个具有强磁场的环境附近使用无线网络连接，由于无线路由器产生的电磁波被强磁场干扰，引入了大量的噪声，会严重影响无线网络的信号强度和网络传输速度（如图 2.3 所示）。

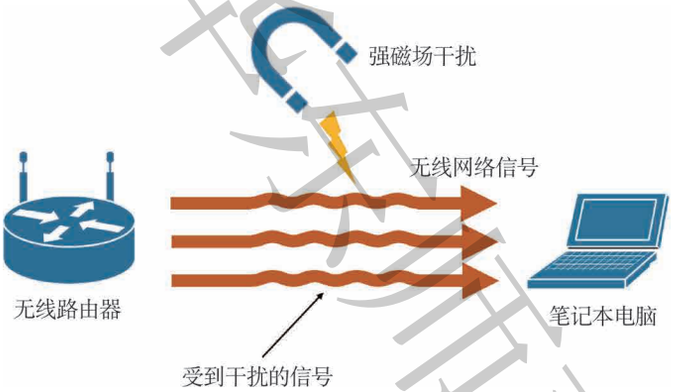


图 2.3　强磁场干扰无线网络信号

2. 衰减

电信号在传输介质中传输时会随着距离增加而不断减弱，这就是衰减现象。由于衰减现象的存在，人们在设计网络时必须考虑网络传输介质的长度或主机与网络设备间的距离。在无线网络中，信号的频率越高，其最大传输距离越短。例如，双绞线的长度不能超过 100 米，否则网络信号就会迅速衰减；移动网络中，4G 信号的传输距离在 1 千米左右，而 5G 信号由于提高了频率，其传输距离只有 200 米左右。相比双绞线，光纤在信号衰减的距离上要长得多，因此人们往往选择光纤作为长距离信号传输的介质（如海底光缆）。

第二节　网络设备与拓扑结构

网卡、交换机、路由器是构成计算机网络的基本设备。虽然随着技术的发展，一些新型设备已经将交换机、路由器的功能集为一体，但无论是独立设备或是集成设备，其包含的基本原理是一致的。本节将对几种主要设备的功能和原理进行介绍，为同学们理解网络拓扑结构和实践组网打下基础。

体　验　思　考

如果我们走进学校的机房（如图 2.4所示），能看到机柜上摆放着一台台“黑盒子”，这些“黑盒子”上插着各种线缆，LED指示灯不停闪烁，意味着数据正通过这些“黑盒子”如滔滔大河般奔流不息。这些“黑盒子”支撑着我们平时的校园网络，如果缺了它们，校园网络就无法建立，我们也无法通过校园网络完成各项工作。

思考：这些“黑盒子”分别由哪些设备组成？你能分清它们的区别吗？

图 2.4　一个校园网中心机房

一、网卡

网卡的全称是网络接口卡（network interface card），有时又被称为网络适配器（network adapter），是计算机接入网络时进行数据通信所必需的硬件设备。

每个网卡都拥有独一无二的标识符，这是由国际电气和电子工程师协会（Institute of Electrical and Electronics Engineers，简称 IEEE）分配给网卡制造商的，这就是 MAC 地址（media access control address，媒体访问控制地址），往往也被称为物理地址（physical address）。如果一台计算机设备含有多个网卡，则每个网卡都有且只有一个唯一的 MAC 地址。

网卡的一个重要功能是进行数据串行传输和并行传输的转换。网卡与网络之间的通信采用数据串行传输，而网卡与计算机之间的通信是并行传输。由于网络上的数据传输速率与计算机总线上的数据传输速率并不相同，因此网卡还必须具备对数据进行缓存的存储芯片。

二、交换机

在计算机网络发展的早期，人们采用集线器(hub)连接计算机，但集线器存在安全性差(传输的数据容易被他人获取)、通信效率低(多台计算机同时传输数据时容易发生冲突)、拓展性差(集线器使人们扩展局域网变得很困难)等缺点。为了解决这些问题，人们发明了网桥(bridge)。顾名思义，网桥就像是连接两个局域网的桥梁。网桥工作在数据链路层，能够通过检查数据链路层的 MAC 地址来转发数据帧。为了连接更多的局域网，人们又对网桥进行了扩展，发明了交换机(switch)，图 2.5 所示是一种常见的交换机。

图 2.5　常见交换机

一般来说，只要开启交换机的电源，然后将每台计算机的网线插入交换机的端口，工作就完成了，一个小型的局域网就诞生了！但是，在看似简单的局域网组网过程背后，交换机做了大量工作。

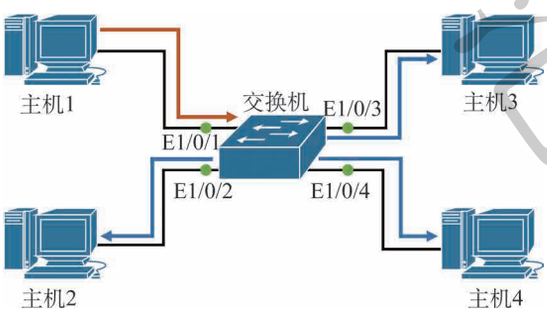


图 2.6　交换机通过泛洪方式转发数据帧

假设四台主机连接到一台交换机(如图 2.6 所示)，编号依次为主机 1～主机 4。主机 1 向主机 4 发出一个数据帧，交换机收到这个数据帧的时候，会把主机 1 的源 MAC 地址(MAC1)与收到这个帧的端口(E1/0/1 端口)关联起来，记录到 MAC 地址表里(见表 2.2)，这被称为学习(learning)。

表 2.2　交换机的 MAC 地址表

MAC 地址表	
MAC 地址	网络接口号
MAC1	E1/0/1

刚开始的时候，交换机还不知道目的地址在哪个端口，于是它把该数据帧转发至除 E1/0/1 以外的所有端口。在图 2.6 中，蓝色的箭头表示这个数据帧被转发到除主机 1 以外的所有计算机中。这被称

为泛洪(flooding)。

接下来,主机 4 收到了该数据帧,并发现这是发给自己的数据,于是它向主机 1 发出确认帧(其他主机发现主机 1 发来的数据帧不是发给自己的,就丢弃该数据帧)。交换机收到确认帧后,在 MAC 地址表中记录下主机 4 相关联的端口号。其他端口的 MAC 地址映射也以此方式学习获得。最终交换机就得到了完整的 MAC 地址表,如表 2.3 所示。

表 2.3 学习了局域网中所有主机和对应接口的 MAC 地址表

MAC 地址表	
MAC 地址	网络接口号
MAC1	E1/0/1
MAC2	E1/0/2
MAC3	E1/0/3
MAC4	E1/0/4

在交换机构建了完整的 MAC 地址表以后,当主机之间再发送数据帧时,交换机只需要通过查询 MAC 地址表就可以将发送到某台主机的数据帧直接通过该接口转发出去,不会再进行泛洪。如图 2.7 所示。

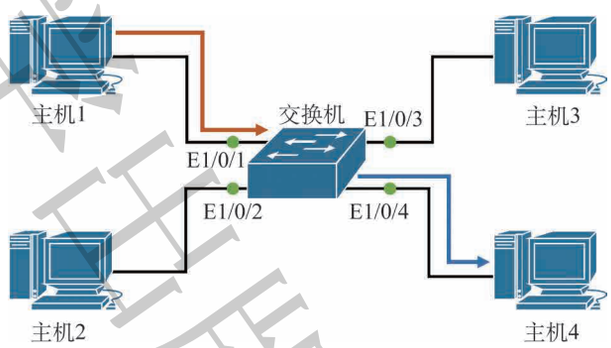


图 2.7 建立了完整 MAC 地址表后,交换机直接转发数据帧

知 识 延 伸 交换机的种类

工作在数据链路层的交换机也称为二层交换机。当然,交换机不仅可以工作在数据链路层,还可以工作在网络层,对应的称之为三层交换机。此外,交换机按照不同的以太网传输速率可分为以太网交换机(10Mbps传输速率)、快速以太网交换机(100Mbps传输速率)、千兆以太网交换机(1000Mbps传输速率)、10千兆以太网交换机(10000Mbps传输速率)、100千兆以太网交换机(100000Mbps传输速率)等。

三、路由器

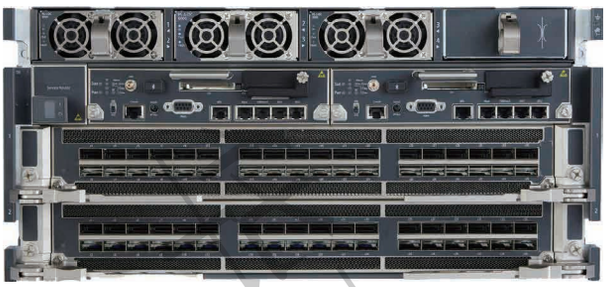


图 2.8　常见商用路由器

路由器是实现网络之间互联互通的设备，一般分为商用路由器和家用路由器。商用路由器的外观如图 2.8 所示，它们一般安装在机房的机架上。常见的家用路由器如图 2.9 所示。家用路由器通过标注为“WAN”（广域网）的接口接入公共网络，通过标注为“LAN”（局域网）的接口连接家庭中的台式机、网络电视等设备。同时，家用路由器还可以通过天线发送无线信号，可以使手机、平板电脑等设备接入无线局域网。另外，在不使用 WAN 接口，只使用 LAN 接口的情况下，家用无线路由器也可以当作交换机使用。

图 2.9　常见家用无线路由器

路由器工作在网络层，负责将源端数据包送到接收方。路由器具有两种重要的网络层功能：转发和路由选择。转发是指由路由器输入端进入路由器的数据包被移动到适当的路由器输出端；路由选择是指网络层决定数据包从源端送到目的端所需经过路径的过程。本章第三节将对路由器的路由功能展开详细介绍。

分　析　评　价

一天，科考队中的一名网络工程师要求搬运工去仓库为他找一台路由器，但搬运工送来了两台外观相似的设备（如表 2.4中第一行所示），搬运工说他无法分清这两个设备中哪个是网络工程师需要的。现在，请你帮助搬运工区分这两台设备，将它们的对应名称填入表 2.4中，并写出你区分它们的理由。

表 2.4　交换机与路由器的区分

完整图		
局部放大图		
名称		
理由		

知 识 延 伸　　交换机和路由器的比较

交换机和路由器都被称为“分组交换机”，但它们的本质是不同的。首先，交换机工作在数据链路层，根据 MAC 地址转发数据帧；而路由器工作在网络层，根据网络地址转发数据包。

交换机的特点在于“即插即用”，在绝大多数情况下，只要将计算机接入交换机即可实现通信。交换机还具有相对高的数据包过滤和转发效率。但交换机的缺点在于，为了防止广播风暴（即报文在网络中不断循环导致交换机的系统资源被迅速耗尽），交换机网络的活跃拓扑限制为一棵生成树。当网络越大，交换机中的 MAC 转发表也会越大，因为交换机需要学习每一个新 MAC 地址的转发规则，这对交换机的存储容量是一个挑战。

路由器的特点在于没有生成树限制，所以它们允许以丰富的拓扑结构建构大型网络。路由器还可以使用源地址和目的地址构建一条最佳路径。但路由器不能“即插即用”，需要人为配置每个接口的网络地址。另外，路由器在处理数据包的时间上要比交换机长。

综上所述，在配置小型局域网时，采用交换机就足够满足要求了。而当需要跨网络传递数据时，应该使用路由器连接到其他网络。

四、网络拓扑结构

计算机网络是一个复杂的系统，各种各样的设备有自己的特点，在实际部署一个网络的过程中，不仅要考虑网络设备在建筑物内的位置，还要考虑设备之间错综复杂的连接关系与线缆的各种排布方式。如果在研究网络的过程中过于关注这些细节，将严重地影响人们对计算机网络本质的认识。因此，我们需要一种更简洁的方式来表示一个网络和它内部设备之间的连接方式。

拓扑指的是一种不考虑物体的大小、形状等物理属性，而仅仅使用点和线描述多个物体实际位置与关系的抽象表示方法。拓扑不关心事物的细节，也不在乎相互的比例关系，而只是以图的形式表示一定范围内多个物体之间的相互关系。

当采用拓扑图来表示一个网络时，就不需要关心这些计算机和设备实际的位置、内部的功能、接口具体的位置等细节，而只是简单地表示哪些设备之间有互联关系。这样做的好处是可以使研究该网络的人员更好地关注网络传输的本质。图 2.6 所示就是一个网络拓扑图，通过它可以研究连接到交换机的主机是如何建立联系的，网络又是如何通过路由器实现相互连通的。采用拓扑图，可以有效地简化问题，从而使人们更好地解决问题。

为了进一步提高抽象性，在绘制网络拓扑图时，一般都会采用一

些通用的符号(详见附录)。本书已经使用了这些符号来绘制拓扑图。在阅读其他技术手册、文档中的网络拓扑图时,可以通过这些符号识别出设备的具体类型。

项 目 实 践

网络工程师们在网络实验室中搭建了一个小型网络。主机 1、主机 2、主机 3、主机 4连接在一台交换机上。请动手构建该网络,并绘制出网络拓扑图。已知四台主机的 MAC 地址分别为 MAC1、MAC2、MAC3、MAC4。主机 1分别向主机 2和主机 3发送了一次数据帧。请写出交换机的学习过程,将其填入表 2.5中。最后写出此时交换机的 MAC 地址表(表 2.6)。

表 2.5 交换机 MAC 地址学习过程

①	主机 1向主机 2发送数据帧
②	交换机_____
③	主机 2_____
④	交换机_____
⑤	主机 1向主机 3发送数据帧
⑥	_____
⑦	_____
⑧	_____

表 2.6 交换机的 MAC 地址表

MAC 地址	网络接口号

第三节　路由原理

在了解了各种网络设备、传输介质和拓扑结构的基础上，我们将进一步了解数据是怎么在这些设备中传输的，即网络路由的原理。在网络中要实现数据的传输，首先需要了解网络层地址——IP 地址，以及相对应的一种重要的网络协议——IP 协议。

体　验　思　考

假设高中生小张居住在一个十分和谐的小区，其中的居民可以经常相互串门，只要步行就可以到其他人的家中。但是小张的外祖母居住在距离本小区数公里远的另一个小区，小张显然不可能用步行的方式去外祖母家玩。他必须要选择一条从本小区到外祖母所在小区的路线。考虑到交通便利程度、路况等种种因素，这条路线可能不是最短的，但一定是最适合的。小张启动他手机上的导航软件，寻找到一条到他外祖母家的合适路径（如图 2.10所示）。

如果把两个小区分别比作两个网络，那么一个报文从一个网络出发，选取合适的路径到达另一个网络的过程就是路由。但是，报文可没有导航软件为它指路，它必须通过一个又一个路由器，通过路由器为它指路，它才能最终到达目的地。

思考：路由器是如何知道报文要到哪个网络去的？又是如何为报文“指路”的？

图 2.10　通过导航软件寻找路径

一、分组交换

在计算机网络设计之初，网络应提供有连接的服务还是无连接的服务曾引起了长期的争论。有人提出应效仿电话网络，即在主机与主机之间建立连接后进行通信，这称为“电路交换”。双方要传输数据，要经过“建立连接——传输数据——释放连接”的过程。在数据传输过程中，双方始终占用着一条完整的通信信道，当双方处于空闲状态但仍保持连接时，这是非常浪费通信资源的。此外，计算机和电话不同，具有更强的数据恢复和差错处理能力。为了提高通信信道的利用率，也为了使数据传输更加灵活，人们采用了如下的策略：网络层只提供简单灵活的、无连接的、不可靠的分组交换策略。也就是说，网络中的两台计算机在相互发送数据时不需要先建立连接，而是将要发送的

报文分成一个一个更小的数据分组，每一个分组独立发送；路由器采取“存储转发”的策略，对到达路由器的分组，路由器将其暂存，查找路由表后将其转发出去；网络本身不保证通信的可靠性，可靠性要依靠主机（或端系统）自身实现。这就使网络设计大为简化，但运行方式更加灵活。正是因为有了这样的设计，才使得网络层既能够适应下层不同的物理网络，也能够适应上层不同的应用。

图 2.11 所示为电路交换模式和分组交换模式的对比图。为了实现分组交换的灵活性，我们需要一个重要的协议来完成分组交换的功能。这就是大名鼎鼎的网际协议（IP）。

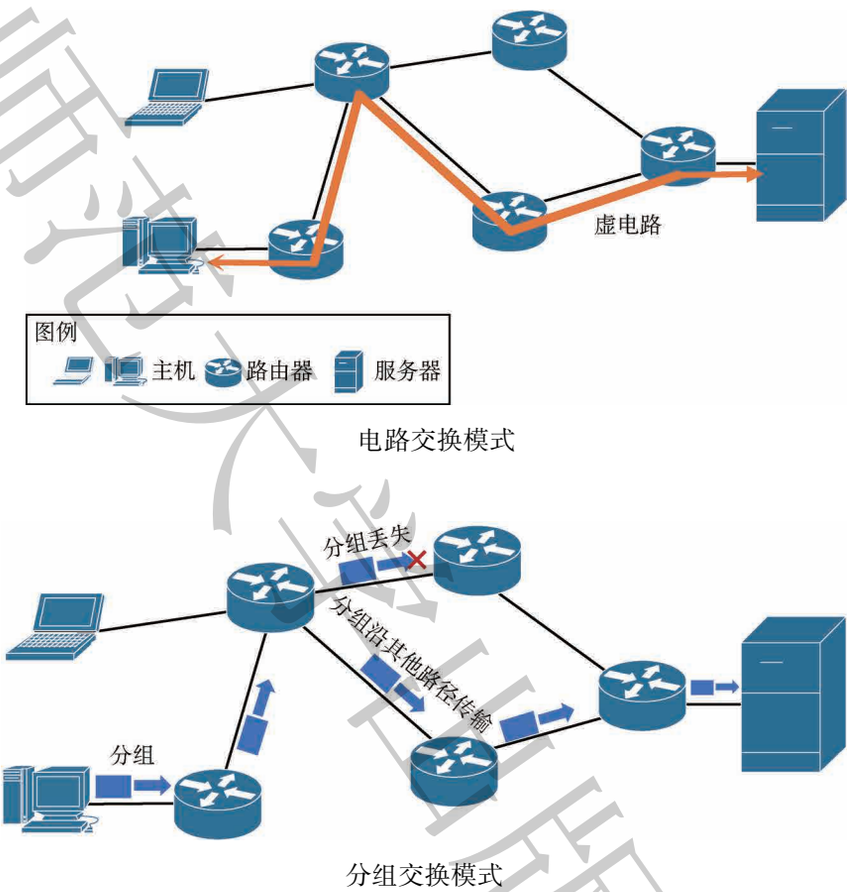


图 2.11 电路交换与分组交换模式对比

二、IP 协议

IP 协议是 TCP/IP 体系结构中最重要的协议之一。如果要把全世界的网络都互连起来，并且使它们能够相互通信，会遇到各种复杂的问题。比如不同的网络有不同的物理地址、不同的接入机制、不同的管理与控制方式，等等。为了让这些网络能够相互连接，在网络层

上我们采用统一的 IP 协议将这些不同的网络连接起来，这样形成的一个网络称为“虚拟互联网络”。这样，人们就不需要过多关注这些互联网络的内部细节，很多问题都可以得到简化。也就是说，采用 IP 协议，可以将这些不完全相同的网络连接在一起，从而更有效地扩展网络。

接下来，我们将从 IP 地址这一重要概念开始，学习 IP 协议的基本原理，从而了解主机或其他网络设备寻找对方并传输数据的方式。

1. IP 地址

IP 地址是网络层上每个网络接口的标识符。一般来说，一台主机只有一个网络接口，因此只有一个 IP 地址；而一台路由器至少有两个网络接口，因此它有多个 IP 地址。

如今我们常用的 IP 协议为 IPv4 协议，其 IP 地址（IPv4 地址）是由 32 位二进制正整数来表示的。在网络通信中，IP 地址被分配给每一个参与通信的主机。IP 地址在计算机内部以二进制方式被处理。然而，由于日常生活中二进制并不是常用的计数方法，因此我们将 32 位的 IP 地址以每 8 位为一组，分成 4 组，每组以“.”隔开，再将每组数转换为十进制数。这就是 IP 地址的点分十进制表示法。采用这种表示法主要是使人容易识别并分析 IP 地址。例如：二进制 IP 地址 10101100000101000000000100000001 转换为点分十进制 IP 地址为 172.20.1.1。

如果 32 位全部为 1，即可以得到 IP 地址的最大不同取值数：

$$2^{32} = 4,294,967,296$$

从这个计算结果可知，互联网中最多只可以允许约 43 亿台主机连接到网络。但是，这 43 亿台主机不全是计算机，因为路由器的每一个接口也会有自己的 IP 地址。另外，随着目前网络的不断发展，需要接入网络的主机数远远超过 43 亿，IPv4 地址已经不能满足需要。我们将在后面介绍 IPv6 协议。

2. IP 地址的划分

IP 地址是具有层次性的，每个 IP 地址由网络号和主机号两个部分组成。例如在一个局域网中，每台主机的 IP 地址的网络号是相同的。网络号必须是 IP 地址最高位的前 L 个二进制位，主机号则是

32－L 位，如图 2.12 所示。

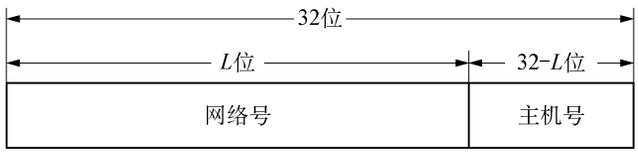


图 2.12　IP 地址的网络号和主机号

过去，人们按照网络号前几位的不同模式将 IP 地址简单划分为 A、B、C、D、E 五类。但随着网络的发展，主机数量不断增长，原有的分类方法已经不再适用了。现在 IP 地址采用构造子网的方法灵活地设置网络的大小。

由于从 IP 地址本身无法推断出网络号的长度，因此当路由器转发分组时，还需要把网络号的长度考虑在内。这个长度通过一串同样为 32 位的编码表示，称为子网掩码。其特点是：和网络号一致的部分全为二进制“1”，而和主机号一致的部分全为二进制“0”。路由器会把收到的每个数据包的目标地址与子网掩码进行“逻辑与”操作，这样路由器就知道将要把数据包送往哪个网络，从而有效减少了路由器中路由表的条目数量，提高了路由器的工作效率。

下面举一个 IP 地址通过子网掩码划分网络号和主机号的例子。如表 2.7 所示，假设 IP 地址“210. 133. 51. 2”的网络号长度为 24 位，主机号长度为 8 位，那么其子网掩码写成点分十进制表示法为“255. 255. 255. 0”，其网络号为“210. 133. 51. 0”，该网络共可容纳 $2^8-2=254$ 台主机。这里需要减 2 是因为主机号如果全为二进制“0”，表示的是以网络号为标识符的网络。主机号全为二进制“1”，表示该网络的广播地址。因此这两个地址不能用于标识实际的主机。

表 2.7　IP 地址和子网掩码

IP 地址(十进制)	210	133	51	2
IP 地址(二进制)	11010010	10000101	00110011	00000010
子网掩码(二进制)	11111111	11111111	11111111	00000000
子网掩码(十进制)	255	255	255	0

有时为了记录的简便，网络号的长度也可以通过在 IP 地址后加上“/”来表示。如“210. 133. 51. 2/24”就表示该 IP 地址的网络号长度为 24 二进制位。

网络号的长度可以根据需要改变。例如一个网络中只有 20 台主机连接，并且增加主机数量的可能性很小，那么即使分配 24 位的网络号也会造成很大的浪费。此时可以进一步扩展网络号的长度，减小主机号分配的空间。但要注意主机号的数量必须是 2 的整数次幂。仍以上面的 IP 地址为例，可以将网络号拓展至 27 位，即网络号变成“210.133.51.0/27”，主机号数量变为 $2^5-2=30$，在保证该网络能容纳 20 台主机的同时，可以将更多的 IP 地址分配给其他主机。

作业练习

1 试一试将下列二进制形式表示的 IP 地址转换为点分十进制表示形式，填入表 2.8 中。

表 2.8 二进制 IP 地址与点分十进制 IP 地址的转换

二进制 IP 地址	点分十进制 IP 地址
10101100000101110000010111011111	
01100100001101110000001011000011	
00101000111110111010001100001010	

2 已知一个 IP 地址是 180.10.35.24/20。这个网络中的最大地址是_____，最小地址是_____。子网掩码（采用点分十进制）是_____。该网络中总共有_____个地址。

知 识 延 伸　环回地址、广播地址、内部地址和保留地址

IPv4地址总数虽有将近 43亿个，但并不能全部用于标识每一个网络接口。有一些特殊的地址有其自己特殊的用途。

1 环回地址

网络号高 8位为 127（01111111）的 IP 地址称为“环回地址”，用于测试本主机自身的进程之间的通信。最常见的环回地址是 127.0.0.1。若主机发送一个目的地址为环回地址的分组，则该主机自身的协议软件会对该分组进行处理，不会将其发送到网络上去。目的地址为环回地址的分组永远不会在网络上出现。

2 广播地址

主机号为全“1”的 IP 地址称为广播地址。它表示以该地址为目的地址的 IP 分组会被转发到该网络内

所有的主机。另外有一种特殊的广播地址为“255.255.255.255”，即整个32位IP地址全为“1”。但它并不表示互联网上的所有主机，而是在主机采用动态主机配置协议（DHCP）获取IP地址时才会采用的目的地址。

3 私有地址

由于IPv4地址已经耗尽，但网络规模仍在不断扩大，为了保证在IPv4到IPv6过渡的阶段仍可以扩展网络规模，人们规定以下三段网络地址为私有地址：10.0.0.0/8、172.16.0.0/16、192.168.0.0/24。这三段私有地址只能在局域网内部使用，如果要通过这些主机与互联网上其他主机进行通信，必须进行网络地址转换（network address translation，简称NAT），将私有地址转换为公共地址才能实现主机间的正常通信。源地址或目的地址为私有地址的分组永远不应该在公共网络上出现。

4 保留地址

网络号高4位为1110（即高8位介于224与240之间）的地址为组播地址（即五类地址划分中的D类地址），用于IP组播技术。网络号高4位为1111的网络地址为保留地址（即五类地址划分中的E类地址），暂不使用。虽然现在已经取消了五类地址的划分，但目前习惯上仍不采用网络号高8位大于240的地址。

3. 自动获取IP地址：动态主机配置协议（DHCP）

手动配置一台主机的IP地址是一件费时费力的事情，很多情况下我们希望主机接入网络即可获取IP地址在网络上通信。动态主机配置协议（dynamic host configuration protocol，简称DHCP）就是为了这一目的而设计的协议。

要使用DHCP，网络中首先需要有一台DHCP服务器（现在的家用路由器已经集成了这一功能）。它维护一个IP地址池，规定了接入该网络的主机能获得的IP地址的范围（如IP地址池为192.168.0.100～192.168.0.199，表示该网络中能获得IP地址的主机个数为100个）。当一台主机接入该网络时，它还没有配置IP地址，因此它会采用广播的方式，向局域网内所有其他主机发送一个源地址为0.0.0.0，目标地址为255.255.255.255的报文（DHCP请求）。当DHCP服务器收到该请求时，会将分配的IP地址作为其响应报文的内容，主机收到该响应后，就可以根据该响应配置自己的IP地址。该过程如图2.13所示。DHCP极大地降低了网络配置的复杂程度，使得接入网络的主机可以实现“即插即用”。

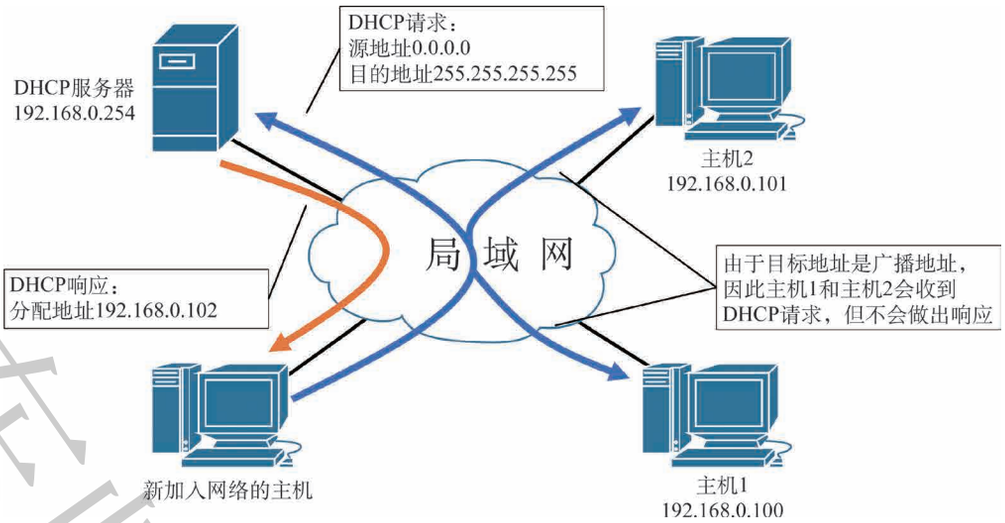


图 2.13　新加入网络的主机使用 DHCP 协议自动获得 IP 地址

4. 检查网络状态：ICMP 协议

在架构网络时，我们需要时常关注两个情况：网络是否正常工作；遇到异常时如何进行问题诊断。为此我们需要一个可以完成网络问题诊断等工作的协议。ICMP（Internet control message protocol）即互联网控制报文协议，它也是 TCP/IP 协议族的一员，用于在主机、路由器之间传递控制消息。

ICMP 的主要功能包括：确认 IP 包是否成功送达目标地址，通知在发送过程当中 IP 包被丢弃的具体原因，改善网络设置等。有了这些功能以后，就可以获得网络是否正常、设置是否有误以及设备有何异常等信息，从而便于进行网络上的问题诊断。

ICMP 协议的重要应用就是操作系统中的 ping 命令（packet Internet groper），用来测试两台主机间的连通性。

ping 命令的格式是：

```
ping [参数] hostname
```

hostname 是要测试网络连通性的目标主机，可以是目标主机的 IP 地址，也可以是域名（见第三章）。参数为可选项，我们可以通过不同的参数来改变 ping 的方式。例如：-t 参数可以连续不断地向目标主机发送 ICMP 请求，直到手动停止；-n（后面跟数字）可以指定发送请求的次数；-l（后面跟数字）可以指定发送请求报文的大小，等等。

图 2.14 是一个运行 ping 命令的例子。在命令行提示符中输入“ping 202.120.88.2”，表示我们要测试本机到这个 IP 地址的连通性。ping 命令会发送 ICMP 请求报文到目标主机以检测与目标主机之间

的连通性，并根据 ICMP 响应报文的类别和内容在屏幕上返回相应的结果。

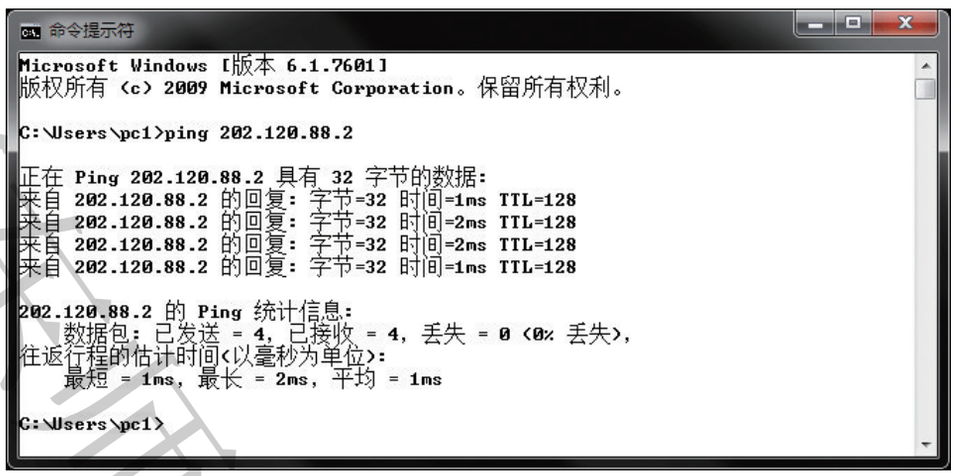


图 2.14　运行 ping 命令的一个例子

5. 下一代 IP：IPv6

随着互联网规模的飞速扩大，IPv4 协议已无法应对当前互联网对 IP 地址总量的需求，于是人们提出了下一代 IP 协议，即 IPv6（IPversion 6）。

IPv6 是为了解决 IPv4 地址耗尽的问题而被提出的网际协议。我们已经知道 IPv4 的地址长度为 4 个 8 位组，即 32 比特。而 IPv6 的地址长度则是 IPv4 的 4 倍，即 128 比特，能表示的 IP 地址数量高达 $2^{128} \approx 3.40 \times 10^{38}$ 个，是 IPv4 地址总数的 2^{96} 倍。这可谓是天文数字，足以为地球上每一粒沙子分配一个地址。

IPv6 和 IPv4 在标记方法上亦有所区分，IPv4 采用的是“点分十进制表示法”，而 128 比特的 IPv6 地址以每 16 比特为一组，每组用冒号（“:”）隔开，采用十六进制数进行标记。如果出现连续的 0 时还可以将这些 0 省略，并用两个冒号（“::”）隔开。但是，一个 IPv6 地址中只允许出现一次两个连续的冒号。

IPv6 地址具体的表示方法如下所示：

（1）IPv6的 IP地址的基本表示法

- 用二进制数表示

1111111011011100：1011101010011000：0111011001010100：0011001000010000：
1111111011011100：1011101010011000：0111011001010100：0011001000010000

■ 用十六进制数表示

FEDC：BA98：7654：3210：FEDC：BA98：7654：3210

（2） IPv6的 IP地址省略表示法

■ 用二进制数表示

0001000010000000：0000000000000000：0000000000000000：0000000000000000：
0000000000001000：0000100000000000：0010000000001100：0100000101111010

■ 用十六进制数表示

1080：0：0：0：8：800：200C：417A

■ 用十六进制数省略表示

1080：：8：800：200C：417A

IPv6 不仅仅能解决 IPv4 地址耗尽的问题，同时还修改了一部分 IPv4 中存在的性能缺陷。然而，从 IPv4 切换到 IPv6 极其耗时，需要将网络中所有主机和路由器的 IP 地址进行重新设置。在互联网已经广泛普及的当下，替换所有 IP 地址会是更为艰巨的任务。

三、路由选择

假设存在一个网络，其拓扑如图 2.15 所示。每一个路由器都连接了三个网络，而每一个网络都可能包含上万台主机（可以从其子网掩码计算得到）。如果路由表要给出到每一台主机的转发路径，则这个路由表会非常庞大。而如果路由表只指出到某个网络应如何转发，则路由表条目数量就能得到极大简化。因此，我们能够得到一个重要

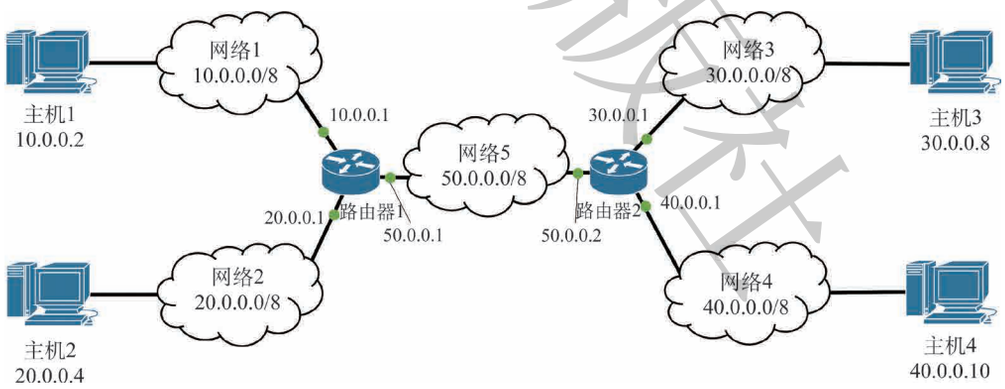


图 2.15 实验网络拓扑图

的概念：互联网所有的分组转发都是基于目的主机所在的网络的。在路由表中，对每一条路由来说最主要的是以下两个信息：目的网络地址和下一跳地址。分组在互联网上转发时，是从一个路由器转发到下一个路由器（称为“一跳”），只有当路由器直接连接目标网络时，才考虑直接交付给目标主机。

以路由器 1 为例。路由器 1 中的路由表如表 2.9 所示，可以看到网络 1、网络 2 和网络 5 由于直接连接路由器 1，因此发到这些网络的报文可以直接交付。而网络 3 和网络 4 不和路由器 1 直接连接，因此路由器 1 收到目标网络为网络 3 或网络 4 的报文时，要通过下一跳路由器（即路由器 2）转发，该报文会被转发到路由器 2，再由路由器 2 决定如何进一步转发。

表 2.9　路由器 1的路由表

目的主机所在网络	下一跳地址
10.0.0.0/8	直接交付，从端口 0转发
20.0.0.0/8	直接交付，从端口 1转发
50.0.0.0/8	直接交付，从端口 2转发
30.0.0.0/8	50.0.0.2
40.0.0.0/8	50.0.0.2

互联网是由许许多多的小网络构成的，一个路由器不可能知道互联网上每一个小网络的网络地址，那么这样的路由器将如何转发分组呢？答案是采用默认路由。默认路由是路由表中多个表项合并的结果。考虑图 2.16 所示的情况，R1 直接连接到网络 1，通过 R2 连接到网络 2，通过 R3 连接到互联网。那么 R1 这台路由器可以将除网络 1 和网络 2 以外的目标网络的下一跳地址全部指定为默认路由。在路

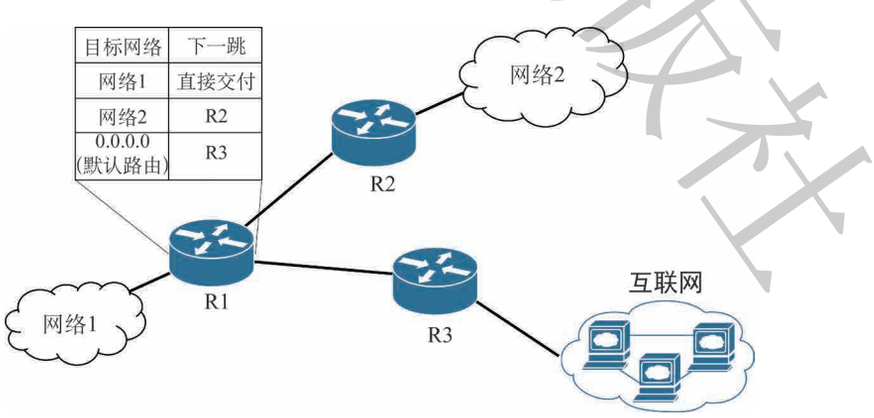


图 2.16　默认路由

由表中，我们使用 0.0.0.0 这一个特殊的 IP 地址表示默认路由的目标网络地址。

在某些情况下，也可以指定转发到某个特定主机时路由器的下一跳地址，这称为特定主机路由。其原理和一般路由基本一致，但实际上很少使用。

知 识 延 伸　静态路由和动态路由

本书在前文所述的路由配置方法属于静态路由。在小型局域网中，选择路由相对比较容易，因为这些路由器之间往往只存在一条路径，我们可以通过手工配置所有的路由表来满足需求，当网络拓扑发生变化时，我们就需要手工更改路由表以满足新的变化。

但是，在一些规模比较大的网络中，路由器之间可能有多条链路相互连接，有一些网络的拓扑也可能经常发生变化。在这种情形下，静态路由就很难适应网络的变化。为了解决这个问题，人们发明了动态路由协议，通过路由器之间交换的路由信息自动地更新每一张路由表。相比人工配置静态路由，动态路由的响应时间很短，且出错率比人工配置要低。因此，动态路由得以广泛地应用，现在主流的骨干网络均采用动态路由的方式进行配置和管理。

分 析 评 价

使用流程图方式绘制出路由器转发分组时的算法。图 2.17中已经给出了一个算法流程图框架，表 2.10和表 2.11中分别给出了所需的条件和满足条件时的行动。请在流程图中合适的地方填入相应的内容。

表 2.10　转发条件

C1：目标网络和路由器直接相连
C2：路由表中有默认路由
C3：路由表中有到目标网络的路由

表 2.11　满足条件后的行动

A1：交付给默认路由
A2：交付给下一跳
A3：直接交付

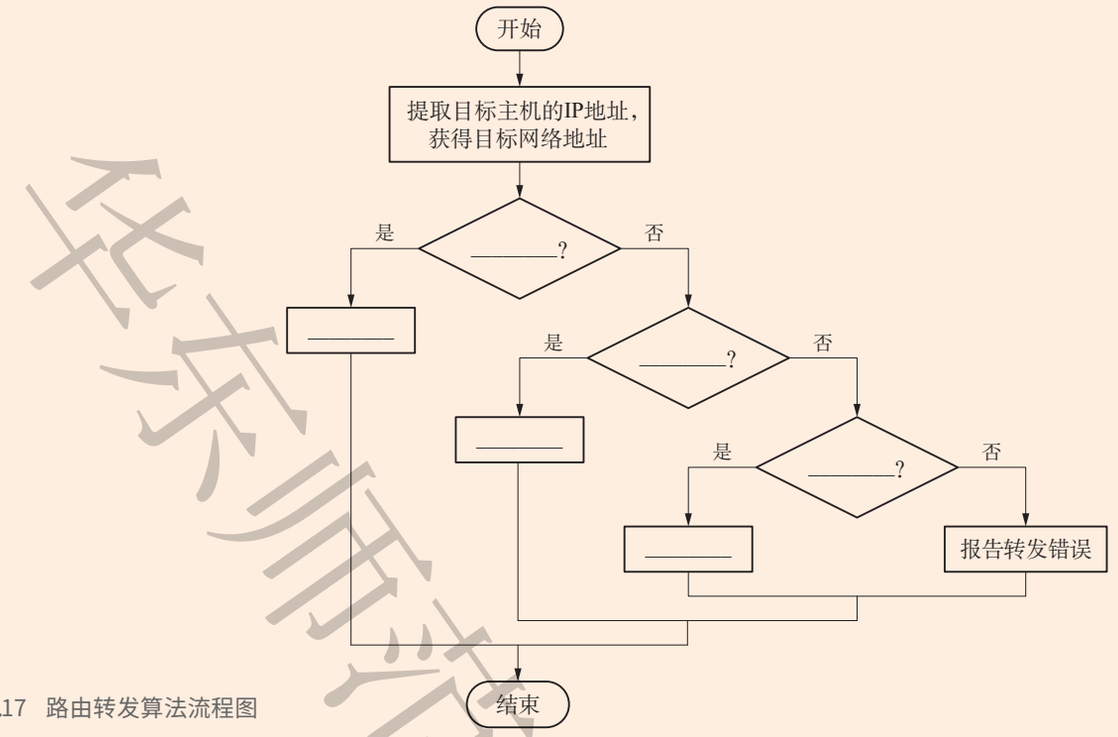


图 2.17　路由转发算法流程图

作业练习

科考队的网络工程师在实验室中建立了如图 2.18所示的网络，路由器 A、B、C、D 相互连接，网络 1和网络 2连接在路由器 A上，网络 3连接在路由器 D上。请将路由器 A的路由表填写完整（表 2.12），并保证目的地为网络 3的所有报文都通过路由器 B转发。

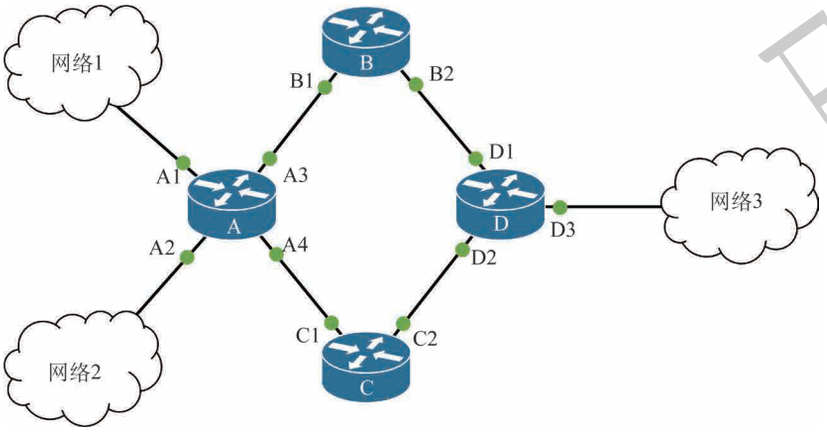
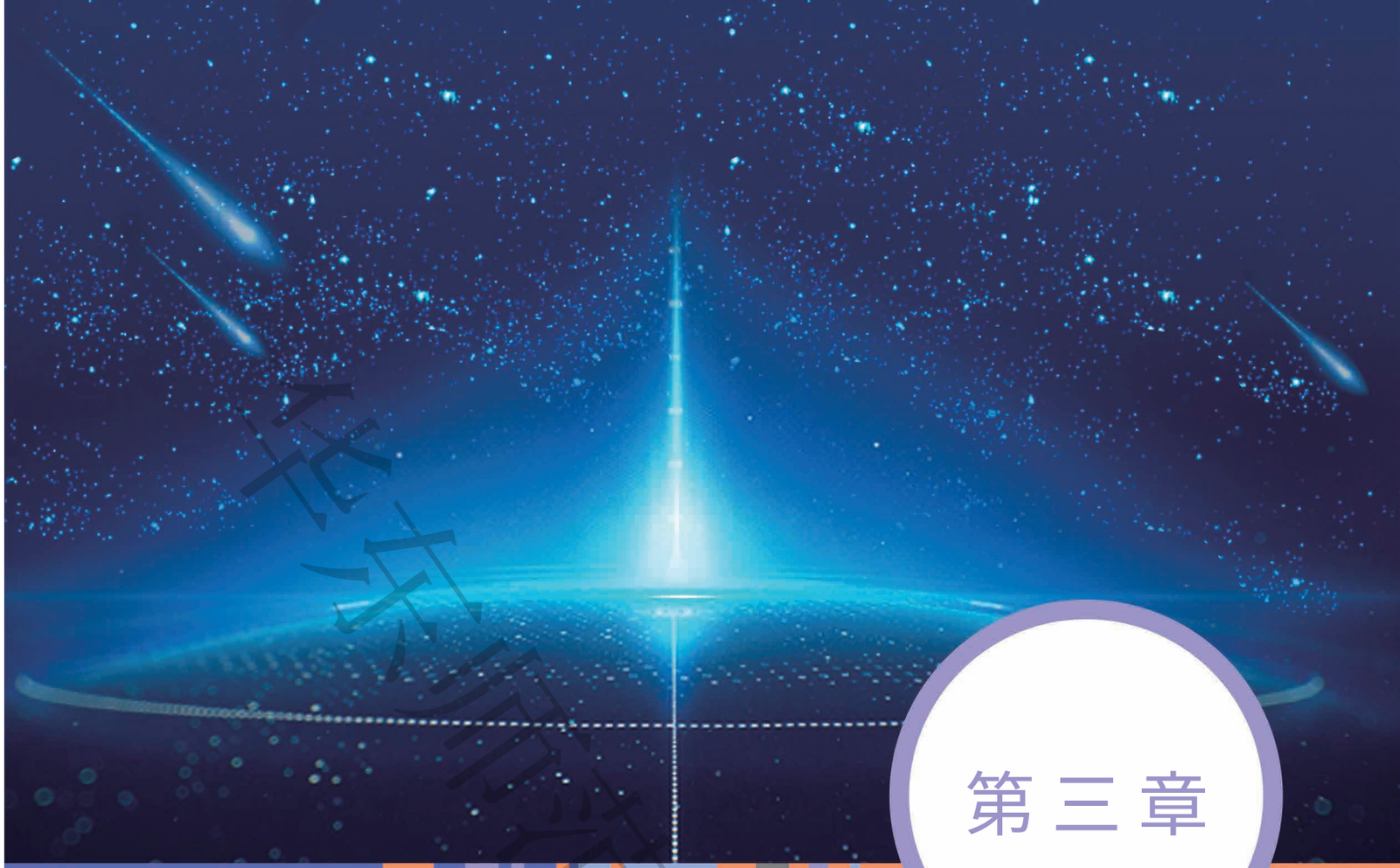


图 2.18　路由器形成的网络

表 2.12　路由器 A的路由表

目的主机所在网络	下一跳地址
网络 1	直接交付，从A1转发
网络 2	
网络 3	



第三章

网络传输与资源共享

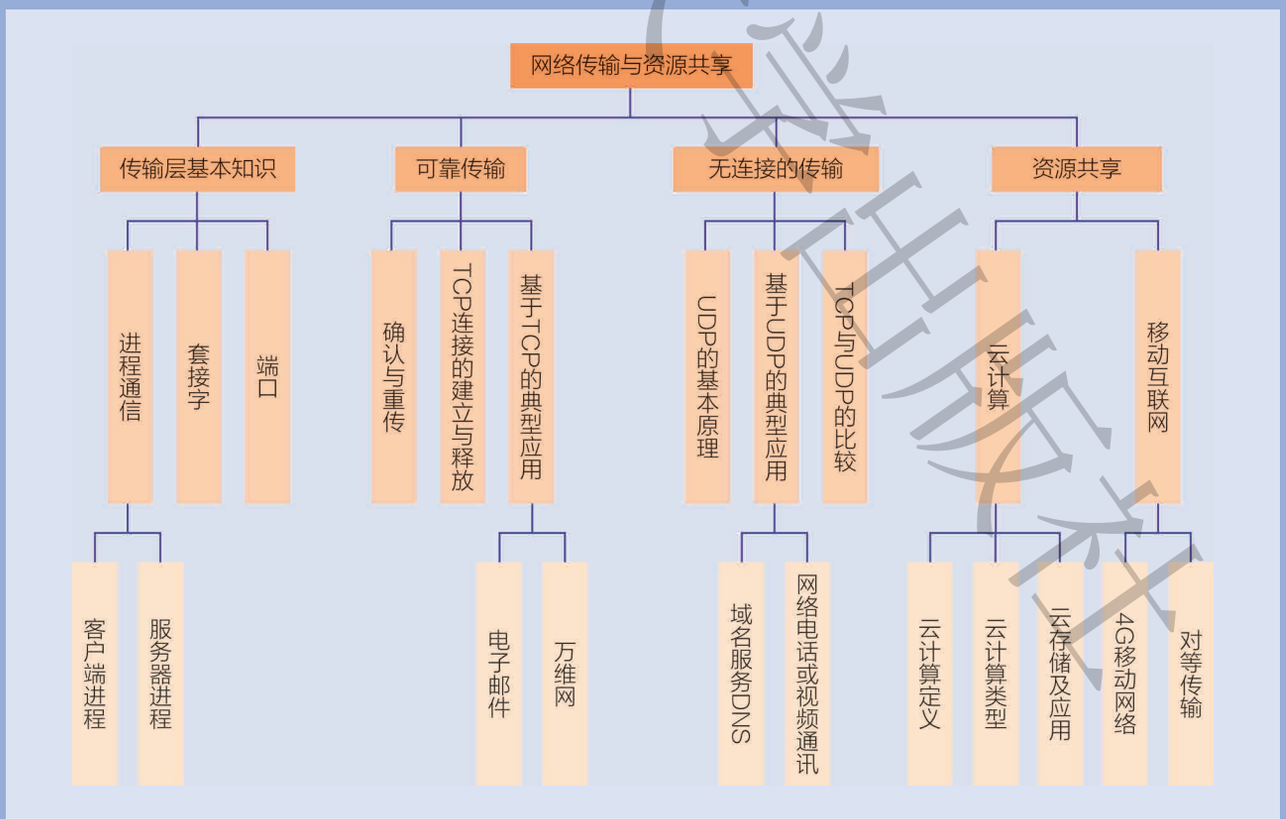
本章学习目标

- 区分基础网络服务中的客户端与服务端。描述套接字概念。
- 描述 TCP 中连接建立和释放的原理。描述万维网浏览过程中网络资源的传输过程。描述使用电子邮件传输网络资源的详细过程及原理。区分各种与电子邮件相关的协议。
- 描述 UDP 和 TCP 的区别，列举 UDP 和 TCP 在不同场合中的应用。
- 描述云计算的概念。区分不同云计算服务模式。使用云存储服务共享与同步文件。
- 能描述 4G 与 5G 移动网络原理。区分对等传输模式与“客户端—服务端”模式。使用移动互联网应用生成并分享网络资源。

从远古时代开始，人类就在长期的生产实践中不断地运用和共享信息。互联网的诞生让信息的共享变得更加方便快捷。文本、图像、音频、视频等都能在互联网上被分享，成为网络上的资源。那么，网络资源该如何生成，我们又该如何利用网络硬件设备和通信协议实现网络资源的共享呢？

万维网、电子邮件和即时通信是当前常用的网络服务，人们已经广泛地使用它们来分享网络资源。为了更好地理解网络服务的本质，我们不仅要学习它们自身的工作原理，更要理解以它们为代表的网络应用是如何将数据通过网络传输到世界各地的。与此同时，我们还将学习云计算和移动互联网等新兴的资源共享方式，感受网络技术发展给人们生活带来的便利。

本章知识结构



项目主题

探究数据传输过程

项·目·情·境

你所在的网络工程师团队经过一段时间的努力，在新的星球上构建了一个能够连接科考队每位成员通信终端的网络。而科考队中的其他专家团队又有着不同的通信需求。你现在面临的问题是：针对不同的通信需求采用或建立不同的通信协议，使每个团队都能够完成他们的任务。

项·目·任·务

任务 1

考虑在这个星球上所有可能存在的专家团队的通信需求以及针对这些通信需求可能的实现方式。通过表格方式整理出他们需要的通信协议。

任务 2

假设气象专家经过了一段时间的监测，获得了这个星球上大量的温度、湿度、风力、降水等数据，他们希望找出其中的规律以预测未来天气的变化。在他们的计算机性能有限，并且无法添加新计算机的情况下，为他们设计一个解决方案，使他们能够完成有限条件下大数据分析的工作。

第一节　传输层基本知识

体　验　思　考

根据 2018年度《中国互联网络发展状况统计报告》，截至 2018年 5月，我国应用市场上监测到的移动应用程序为 415万款。而使用网上购物、网络音视频应用程序的网民比例也分别占到 71.0%和 74.1%。这些应用程序在网络上产生了大量的数据，这些数据会经过若干网络和若干路由器，从源主机到达目标主机，完成用户之间的交互。

思考：应用程序应该如何将自己的数据通过网络设备进行传输？当目的主机收到数据以后，又如何将数据转化为应用能够识别的形式？不同应用程序之间的数据又将如何区分？

一、进程通信

我们此前已学习了两台主机之间如何通过网络进行通信。但真正参与通信的并不是主机本身，而是运行在主机上的进程。进程是一个执行中的程序，在网络通信过程中，两个相互通信的进程成为一对对等实体。一台主机中往往同时有多个应用进程和另一台主机上的多个进程进行通信。例如，我们一边浏览网页，一边使用电子邮件软件收发邮件。这时主机中就同时运行着浏览器进程和电子邮件软件的进程。进程之间的通信称为“端到端通信”，从逻辑上来看，就好像两台主机上的进程直接与对方进行通信。

要完成两个应用进程之间的通信，进程需要保持运行状态。例如一个万维网网站，承载该网站的进程会一直运行，以随时接受来自世界各地的访问者。那些长期运行的，随时准备接受其他进程连接的进程被称为服务端进程（server，或简称服务端）。相对地，那些按需运行的，主动连接服务端进程的进程被称为客户端进程（client，或简称客户端）。大多数的网络应用都采用这样的体系架构，即“客户端—服务端”架构（client/server，简称 C/S）。而另一些应用采取了通信双方可以同时作为客户端和服务端的体系架构，这称为“对等连接”架构（peer-to-peer，简称 P2P）。

二、套接字与端口

在端对端通信中，客户端进程与服务端进程在逻辑上是直接相互

通信的，但实际上，它们还要将数据交给网络层，才能通过实际网络完成通信。那么，进程产生的数据是如何进入下层网络中的呢？

进程通过被称为套接字（socket）的软件接口向网络发送数据和从网络接收数据。如果把进程比喻成一座房子，套接字就可以类比为它的门。在两个进程相互通信的过程中，源主机上的一个进程产生数据并通过套接字将它们发送到网络上（出门），当数据到达目的主机时，通过另一个套接字进入另一个进程（进门）。因此，每一个进程都通过套接字和传输层产生联系，发送方将数据通过套接字送入传输层，传输层就会自动地将数据通过下层协议发送出去；接收方的传输层收到数据后，就会将数据通过套接字传递给上层应用，使上层应用可以处理这些数据。图 3.1 描述了这一过程。

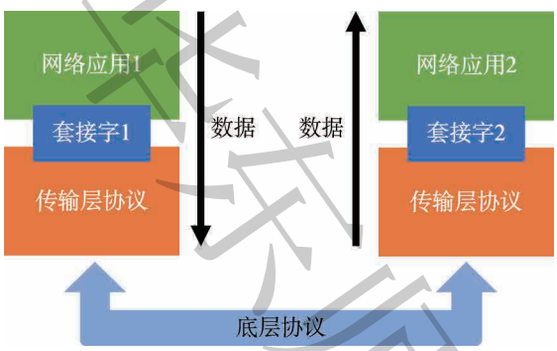


图 3.1　进程之间使用套接字通过底层协议传输数据

计算机运行着各种不同的应用程序进程，如果所有的进程都通过同一个套接字发送或接收数据，就好比一个房间只有一扇小门，人员进出势必会受到不小的阻碍。在计算机系统中，不同的应用必须使用不同的套接字才能正常传输数据。那么，该如何区分不同的套接字呢？不同的套接字可以通过传输层协议中的端口号来区分。所谓的端口号就是应用程序设计者或操作系统给每个套接字指定的一个编号。计算机中可以有 65535 个端口号，其中，1～1023 被称为熟知端口号，通常用于一些广泛使用的网络服务，如万维网服务端一般用 80 作为其端口号，电子邮件发送服务端一般采用 25 号端口，等等。1024～49151 被保留用于其他应用程序的服务端使用。49152～65535 用于客户端与服务端建立连接时采用，客户端要与服务端通信时，会从这些端口号中随机选择一个未使用的作为其端口号，当服务端收到客户端发来的报文时，就知道了客户端的端口号，从而能够使服务端将数据发给客户端。当通信结束时，该端口号即被释放，可被其他进程再次使用。

我们可以通过 netstat 命令来查看目前计算机中有哪些进程正在连接网络。在命令提示符中输入“netstat”，屏幕上会出现一个表格，展示出目前计算机上连接了哪些 IP 地址的哪些端口、本地地址及端口、所用的协议和连接状态，如图 3.2 所示。和 ping 命令一样，netstat 也可以带上各种参数以获得更详细的信息，可以输入“netstat －help”来查看这些参数。

图 3.2 netstat命令输出结果示例

项 目 实 践

1 请在命令提示符中输入“netstat”，查看自己的计算机上连接到了哪些 IP地址的哪些端口，并将结果的前 5行填入表 3.1中。

2 请在命令提示符中输入“netstat -help”，了解 netstat命令的各种参数及它们的作用。并回答问题：如果要知道目前有哪些进程正在连接网络，需要输入什么命令？实际输入该命令并查看结果。

表 3.1 netstat命令的输出（前 5行）

协议	本地地址及端口	远程地址及端口	连接状态

第二节　可靠的数据传输

IP 协议无法保证数据在传输过程中不丢失，不出错。因此，还需要有保证数据可靠传输的手段。在传输层中，传输控制协议（transmission control protocol，简称 TCP）就是用来实现可靠的数据传输的协议。

体　验　思　考

假设有红蓝两军举行军事演习（如图 3.3所示）。红军分别占据两个山头，准备向山下的蓝军发起进攻。这两支红军部队没有能直接通信的方法，唯一的方法是派出传令兵到对面的山头传递约定信息。但传令兵有可能被蓝军抓住。只有两个山头上的红军达成一致协议，同时向蓝军发起进攻才能获胜，否则红军就无法获胜。

思考：能否设计一个协议，使得红军一定能够获得胜利？

图 3.3　两军问题

一、传输控制协议

TCP 是为了在不可靠的网络上提供可靠的数据传输服务而专门设计的传输层协议。它既要负责足够快地发送数据报，又要避免引起网络阻塞，还要负责将到达的数据报按照正确的顺序重新组装。因此，TCP 是一个很复杂的协议。

1. 基于 TCP 的可靠传输

当两个人打电话时，由于双方看不见对方的表情，不知道对方是否还在认真听自己说话，因此打电话的人会经常发出“嗯，嗯”的声音，来让对方知道自己还“在线”。这就是对对方说话的一种确认。TCP 正是基于确认机制来实现可靠传输的。

如图 3.4(a)所示，主机 A 通过 TCP 向主机 B 发送数据时，主机 B 会根据每个从主机 A 发来的报文段向主机 A 回发一个确认，意思就是“你发来的数据我收到了”。而主机 A 收到来自主机 B 的确认以

后，知道自己的上一段数据已经成功发送，因此会继续发送剩余的数据，直到数据全部发送完毕。

如果网络传输质量不好，主机 A 发送的报文段没有被主机 B 收到，如图 3.4(b)所示，主机 B 则不会发出任何确认。一段时间后（称为超时时间），A 没有收到来自 B 的确认，A 就认为自己这次发送没有成功，它会重新发送刚才的报文段，直到收到来自 B 的确认为止。通过这种方法，A 就能保证它发送的每一个报文段都能够被 B 收到。

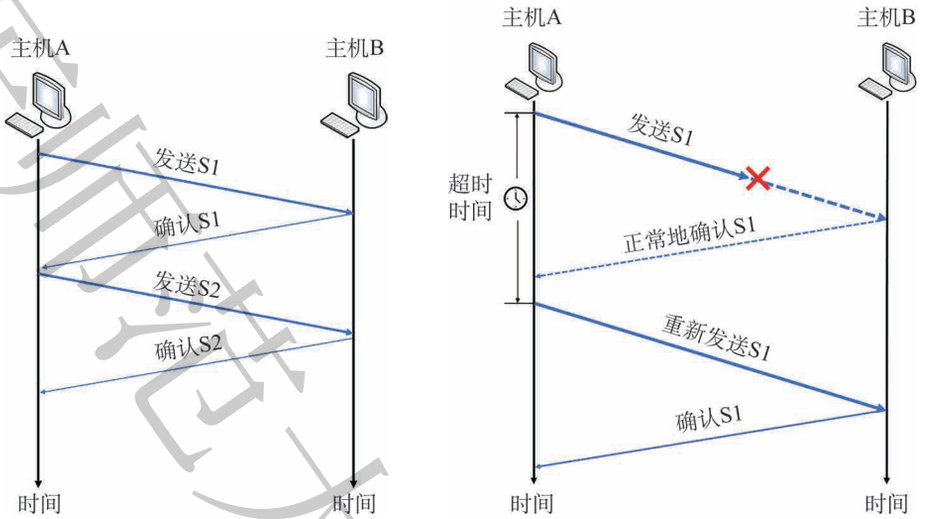


图 3.4　确认机制和重传机制

(a) 接收方（主机 B）对发送方（主机 A）发来的报文段进行确认

(b) 主机 A 发送的报文段丢失，经过超时时间后主机 A 重传报文段

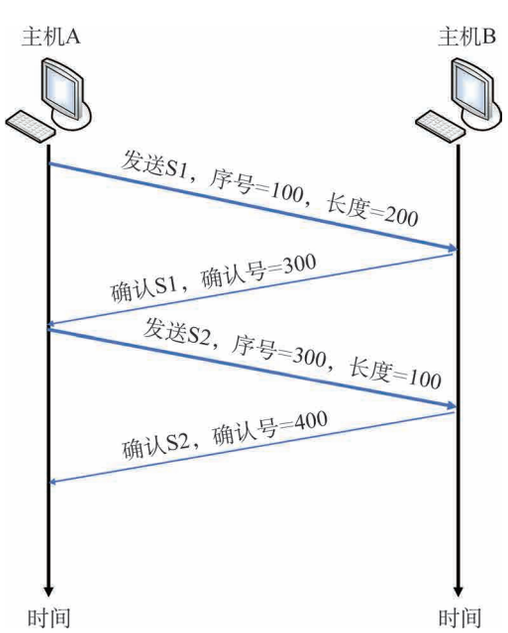


图 3.5　TCP 的序号和确认号机制

前面说过，TCP 要保证报文段有序地到达目标主机。因此，TCP 对每个报文段都有两个编号。一个称为序号，它表示该 TCP 报文段的顺序。需要注意的是，这个顺序表示的是本报文段所发送的第一个字节的序号。例如在图 3.5 中，A 发给 B 的第一个报文段的起始序号是 100，而该报文段有 200 个字节，那么下一个报文段的序号应从 300 开始。第二个编号称为确认号，它表示期望收到对方下一个报文段的第一个字节的序号。图 3.5 中 B 收到了来自 A 的序号为 100 的报文段，且该报文段有 200 字节的数据，这就表明 B 正确地收到了 A 发送的到序号 299 为止的数据。因此，B 期望收到的下一个数据序号是 300，于是 B 在发送给 A 的确认报文中，将确认号设置为 300。也就是说，如果确认号为 n，那么意味着到序号 $n-1$ 为止的数据已经全部正确收到。这样，TCP 就能做到按序接收对方发来的报文段。

分 析 评 价

如图 3.6所示，A发送 TCP报文给 B，B也收到了该 TCP报文并做出了确认，但在途中这个确认报文丢失了，A将_____。在 A做出相应处理以后，B又将_____（假设此后的所有报文不会途中丢失）。并在图 3.6上绘制出相应过程。

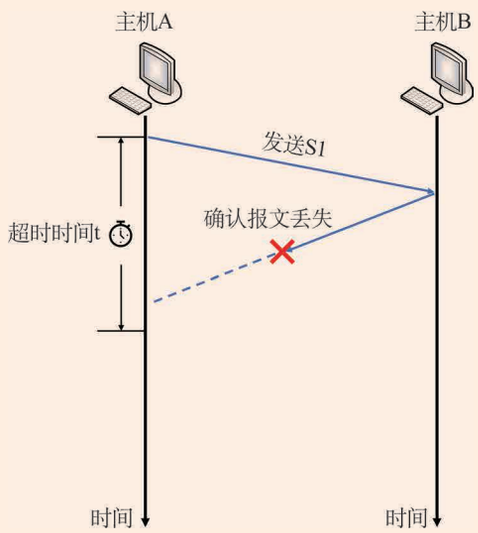


图 3.6 确认报文丢失的情况

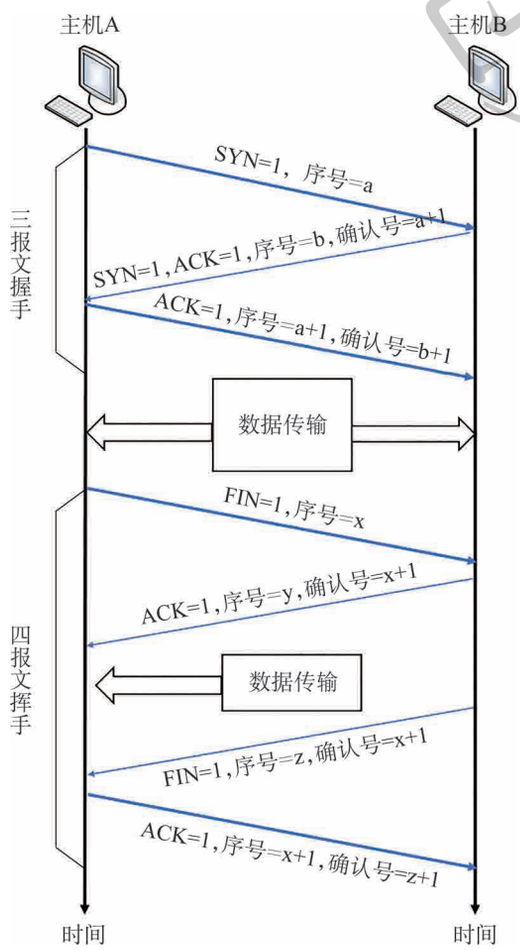


图 3.7 TCP的“三报文握手”和“四报文挥手”

2. 连接的建立与释放

TCP是面向连接的协议。如果两台主机通过TCP传输数据，那么它们之间必须先建立连接才能开始数据的传输。而在数据传输完成后，它们也要释放这条连接。那么，TCP如何建立和释放连接呢？

（1） TCP建立连接

建立一个TCP连接需要双方先后共发送三个报文，这个过程称为“三报文握手”。如图 3.7 所示，主机A要通过TCP向主机B发送数据，A会先发送一个带有SYN(synchronize)标记的报文作为建立连接的请求，并等待确认应答。如果B同意建立连接，就发来一个带有ACK(acknowledgement)标记的SYN报文，A收到该确认后再发送对该确认的确认，此时双方的连接就建立完成了，接下来可以进行数据传输。

（2） TCP释放连接

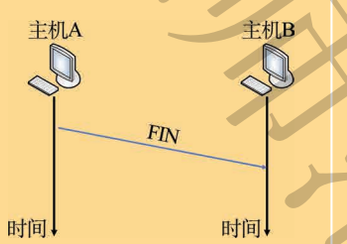
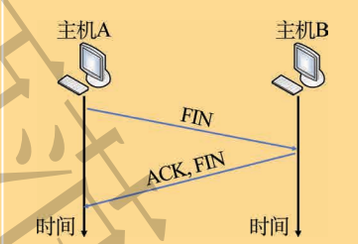
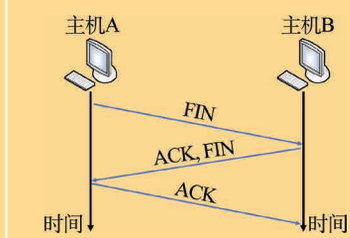
TCP释放连接过程相对复杂一些。在图 3.7 中，假设A要主动断开和B的连接，那么A首先发送一条带有FIN(finish)标记的报文给B，B收到该报文后发送相应的确认给A，此时A、B之间并不能马上断开连接，因为B还可能有数据要发给A。当B发送完毕以

后，它也发送一个带 FIN 标记的报文给 A，A 收到该报文后发送相应的确认，双方才能真正地断开连接。可以看到双方一共发送了四个报文断开连接，因此这一过程被称为“四报文挥手”。

探 究 活 动

科考队中有一名见习网络工程师认为，TCP 断开连接不一定要“四报文挥手”。为此他绘制了表 3.2，分别展示了 TCP 断开连接使用 1个报文、2个报文和 3个报文的情况。请帮助他思考一下，如果采用少于四个报文断开连接会有什么现象发生？填入表 3.2中。

表 3.2 断开连接少于四个报文时可能产生的现象

情形	 (a)一个报文断开连接	 (b)两个报文断开连接	 (c)三个报文断开连接
可能产生的现象			

二、基于 TCP 的典型应用

由于 TCP 为不可靠的下层网络提供了可靠传输的保证，因此得到了十分广泛的应用。其中，电子邮件和万维网都是经典的基于 TCP 的应用。我们通过对它们的探究来学习网络服务与网络应用的基本原理。

1. 电子邮件

当我们写好了一封信，还需要将邮件“寄出去”这一动作，收信人才可能收到信件。同样地，电子邮件协议中不仅包含邮件所需的“信封”和“信件内容”，还包含了一系列动作，使得我们可以成功地发送和接收电子邮件。

首先来看一下电子邮件系统的整体情况。假设某人 A（邮箱地址

为 userA@mailA. com)要发送一封电子邮件给他的好朋友 B(邮箱地址为 userB@mailB. com),那么 A 首先需要登录自己的邮件代理程序。邮件代理程序也叫邮件客户端,允许用户阅读、回复、转发、保存和撰写邮件。A 撰写好邮件以后,通过简单邮件传输协议(simple mail transfer protocol,简称 SMTP)将电子邮件发送到 mailB. com 的邮件服务器上。当 B 想要接收邮件时,他也只需要登录自己的邮件代理程序,程序会通过邮局协议(post office protocol version 3,简称 POP3)或因特网邮件访问协议(Internet mail access protocol,简称 IMAP)从 mailB. com 的邮件服务器上收取所有的未读邮件。整个过程如图 3. 8 所示。

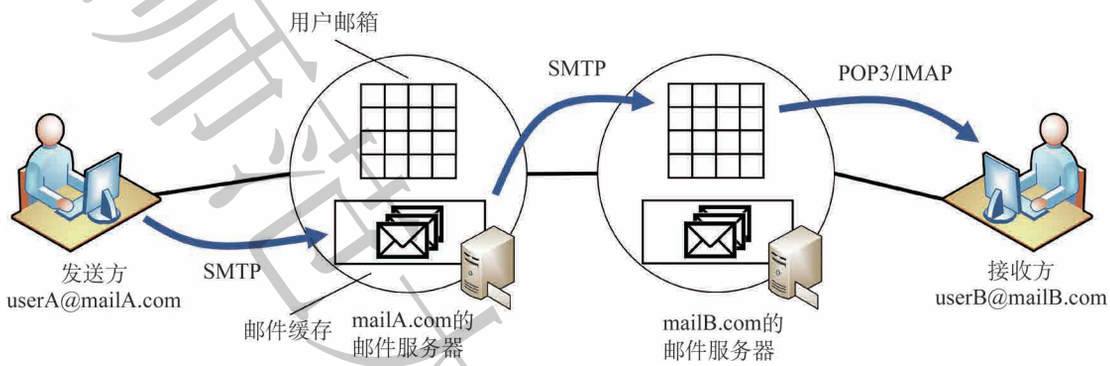


图 3.8 电子邮件发送—接收过程

1	S:220 mailB. com
2	C:**HELO** mailA. com
3	S:250 Hello mailA. com, pleased to meet you
4	C:**MAIL FROM**:<userA@mailA. com>
5	S:250 userA@mailA. com ... sender ok
6	C:**RCPT TO**:<userB@mailB. com>
7	S:250 userB@mailB. com ... recipient ok
8	C:**DATA**
9	S:354 Enter mail, end with "." on a line by itself
10	C:From:userA@mailA. com
11	C:To:userB@mailB. com
12	C:Subject:A question about the lesson
13	C:Hello, this is A from Shanghai.
14	C:I have some questions about the lesson last week ...
15	C:.
16	S:250 Message accepted for delivery
17	C:**QUIT**
18	S:221 mailB. com closing connection

图 3.9 电子邮件发送过程

(1) 使用 SMTP 发送邮件

A 发送一封邮件的过程如下:A 的邮件代理程序为客户端(C),它登录 A 的邮件服务器 mailA. com 与 mailB. com 的邮件服务器(S)产生交互。图 3.9 描述了这一通信过程,其中加粗的部分为客户端向服务器发送的命令。

客户端通过连接服务器的 TCP 25 号端口开始 SMTP 的交互过程。第 1 行服务器返回的信息表示客户端已经和服务器建立连接。第 2 行的 HELO 命令(是 HELLO 的缩略)是客户端向服务器发起的问候,表明客户端希望和服务器进行通信。第 4 行和第 6 行分别发送发件人和收件人的邮箱地址,以便邮箱服务器识别通信双方。第 8 行,客户端发送一行 DATA 命令表示后面

的内容都是邮件本身的数据。第 10～12 行，客户端发送包含发件人、收件人和主题等字段的数据内容，这些数据内容并不被邮件服务器识别，而是被邮件代理程序识别。第 15 行，客户端发送只包含一个句点的消息来结束报文的构成并将报文传输出去。此时客户端如果还有下一封邮件需要发送，则重复第 4 行到第 15 行的过程。如果没有，那么就发送 QUIT 指令结束和邮件服务器的交互。

（2） 电子邮件接收协议：POP3和 MAP

1	S：+ OK POP3 Server Ready
2	C：**USER** userB
3	S：+ OK
4	C：**PASS** * * * * * *
5	S：+ OK user successfully logged on
6	C：**LIST**
7	S：1 498
8	S：2 128
9	S：.
10	C：**RETR** 1
11	S：(mail content . . .)
12	S：.
13	C：**DELE** 1
14	C：**QUIT**
15	S：+ OK POP3 server signing off

图 3.10　POP3邮件接收过程

当邮局将信件送到收信人家时，一般不会当面交到收信人手中，而是将信件放在收信人的信箱里，等收信人主动去打开信箱接收信件。电子邮件也是如此。SMTP 协议以及邮件服务端软件将邮件推送到收件人的邮箱中，还需要一个协议使收件人可以收取发给他的邮件。

和 SMTP 类似，POP3 通过一些命令获取并下载邮件。现在 userB 打开了他的邮箱客户端，邮箱客户端连接上 mailB. com 服务器的 TCP 110 号端口，并通过执行 POP3 协议规定的命令来获取并下载邮件。整个交互过程如图 3. 10 所示。

第 6 行，在客户端发出 LIST 命令后，可以看到服务器会返回目前邮箱中存在的邮件的编号和它们的大小。第 10 行中客户端发出 RETR(return)命令收取编号为 1 的邮件，同样地，服务器也通过只含一个句点的行来表示传输的结束。在一些 POP3 协议实现中，客户端会在收取完邮件后通过 DELE(delete)命令要求服务器删除该邮件(当然也可以设置客户端不要删除邮件)。

POP3 一般是将邮件下载到客户端本地，使得用户可以建立自己的邮件文件夹并将邮件保存在里面。如果一个邮箱使用的时间比较长，那么必然会积累大量的邮件，如果使用 POP3，这些邮件会全部被完整地保存到用户本地的计算机中。这对于存储容量不够大，网络流量也有限的移动终端是不现实的。同时，POP3 也没有管理远程邮箱文件夹的能力。为了解决这些问题，IMAP 应运而生。和 POP3 一样，IMAP 也通过一些指令来收取或管理邮件，但它的指令集更多也更复杂。IMAP 运行在 TCP 的 145 号端口上。

IMAP 可以提供用户创建并管理远程文件夹的功能，使得用户可以远程管理自己的邮件而不必把它们全部下载到本地。IMAP 也允许邮件代理程序只获取邮件的某些部分，比如只读取首部，这样可以

避免在网络连接状况较差的时候消耗大量带宽下载邮件的内容，特别是含有附件的邮件。

探 究 活 动

从教学资源网站上获取“电子邮件工具”，参照图 3.9和图 3.10所示，使用命令完成一封邮件的发送和接收。在此过程中，可以启动流量抓取软件，抓取邮件收发过程中传输的报文，将电子邮件发送过程（图 3.11）填写完整。

1	S：220 _____
2	C：HELO _____
3	S：250 Hello _____，pleased to meet you.
4	C：MAIL FROM：_____
5	S：sender ok
6	C：RCPT TO：_____
7	S：recipient ok
8	C：DATA
9	S：354 Enter mail，end with “.” on a line by itself
10	C：From：_____
11	C：To：_____
12	C：Subject：_____
13	C：_____（此处填写你自己邮件的正文内容）
14	C：.
15	S：250 Message accepted for delivery
16	C：QUIT
17	S：221 _____ closing connection

图 3.11 电子邮件传输过程

2. 万维网

“上网”已经成为人们生活中一件常见的事情。人们几乎每天都会打开浏览器，在各类网站中搜寻着自己感兴趣的信息。同时，越来越多的人开始在个人网站上撰写文章，上传自己喜欢的照片或视频，开始将各种有趣的信息放在互联网上共享。如今，社交网络依托互联网的快速发展已经融入每个人的生活。

网页中不仅含有文本，还含有图像、链接等多种内容，因此网页又被称为“超文本”。浏览器和 Web 服务器之间的通信协议就是“超文本传输协议”。HTTP 协议通常建立在 TCP 协议的 80 号端口上（也

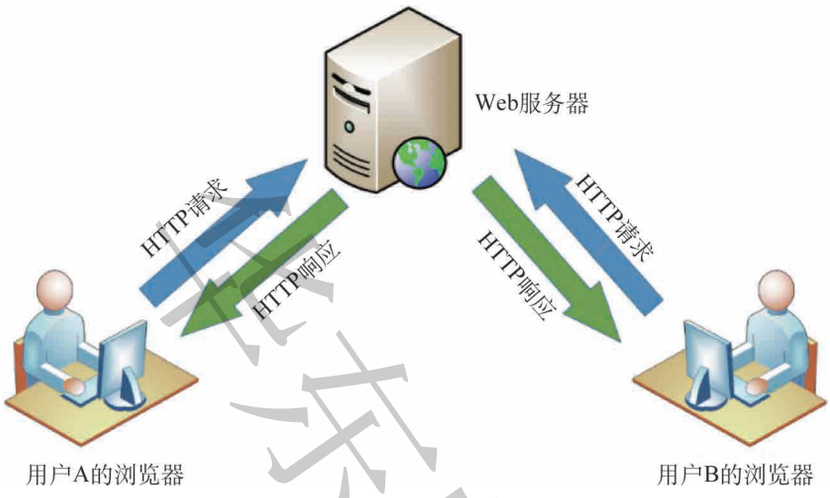


图 3.12　HTTP 的请求与响应

可以建立在其他端口上)。HTTP 可以理解为浏览器和 Web 服务器之间的对话。当一个网页被打开时,浏览器向服务器发起 HTTP 请求,服务器收到浏览器发来的 HTTP 请求时,根据请求的内容给出相应的 HTTP 响应。虽然不同用户的浏览器可能是不同的,但它们都遵循统一的 HTTP 协议。无论使用怎样的浏览器,只要请求的是同一个页面,那么在浏览器中呈现出来的内容基本上是一样的(如图 3.12 所示)。

当人们上网时,人们会在浏览器的地址栏里输入资源的地址(URL)。例如,我们想通过网上购票方式参观上海科技馆,这个页面位于 http://www.□□□□.org.cn/buytickets,我们就要输入这个网址。此时浏览器先去查找 www.□□□□.org.cn 所在的服务器,找到服务器以后,浏览器对服务器说:“我要请求 buytickets 这个页面。”服务器找到这个页面以后回答浏览器:“页面 buytickets 已经找到,内容是……”。如果这个页面不存在,服务器也会回答浏览器:“页面 buytickets 找不到!”此时浏览器也会向用户返回“该页面找不到”的信息。

知　识　延　伸　　**统一资源定位符**

统一资源定位符(uniform resource locator,简称 URL)是对可以从互联网上得到的资源的位置和访问方法的一种简洁的表示,是互联网上标准资源的地址。互联网上的每个文件都有一个唯一的 URL,它包含的信息指出了文件的位置以及浏览器应该怎么处理它。它的标准格式如下:

协议 ://服务器地址 资源路径 文件名

例如上面的网址中,http表示该资源通过 HTTP 协议获取,服务器地址是 www.□□□□.org.cn,资源路径和文件名是 /buytickets。

这样,通过 URL,人们就可以获取万维网上的各种资源。

用来描述网页的语言就是超文本标记语言。HTML 描述如何格式化页面,通过各种各样的标签对不同的内容做出标记,浏览器在读

取到这个文件的时候，就会根据里面的标签呈现不同格式的内容。在Web发展的早期，人们一般将内容通过静态HTML页面呈现给浏览者。但随着网络应用的不断发展，传统的静态网站已经无法满足人们对个性化服务的需求。因此人们开始使用动态网站提高交互性和个性化。我们已经在“信息系统与社会”模块中学习过如何开发一个网络应用软件，其中采用了Flask框架，这就是一种动态网站框架。该框架读取浏览者对网站发出的请求，根据请求从数据库中获取相应的数据，动态地生成HTML并通过前端渲染最终呈现在浏览者眼前。整个过程如图3.13所示。

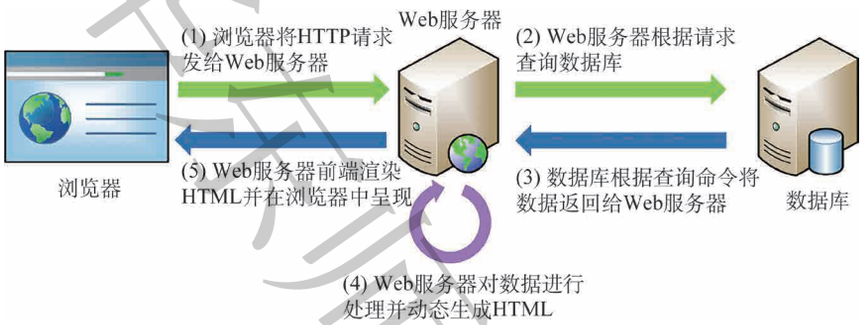


图 3.13　动态网站运行过程

探　究　活　动　探究网页浏览过程中传输的数据

使用浏览器浏览教学资源平台首页，同时开启流量抓取工具，抓取浏览过程中传输的报文。当网页全部加载完毕后，查看抓取的报文，并填写网页浏览过程中传输的数据（表3.3）。根据抓取的报文，结合查阅的资料，回答下列问题。

表 3.3　网页浏览过程中传输的数据

客户端(浏览器)		服务端	
IP地址		IP地址	
端口		端口	
HTTP方法		HTTP版本号	
HTTP版本号		状态码	
请求 URL		服务端类型	
客户端类型		传输的文件类型	

1.本次HTTP传输过程中共发起了_____次请求，得到了_____次响应。

2.本次HTTP传输过程中一共有_____种状态码，分别是_____，它们分别代表_____。

3.你抓取的报文中有完整的TCP握手建立连接和挥手断开连接的过程吗？如果有，请参考图3.7绘制握手和挥手过程的时序图。如果没有，请思考可能的原因。

第三节　无连接的传输

TCP 协议虽然保证了两台主机之间通信的可靠性，但其反复的确认和重传机制增加了通信开销，也降低了双方通信的效率。在某些情况下，可以通过无连接的传输，以牺牲可靠性的代价换取通信效率的提升。因此传输层中还存在另一个重要协议——用户数据报协议（user datagram protocol，简称 UDP）。

体　验　思　考

在本书第一章，我们回顾了不少曾经出现在人类历史上的通信方式。这其中，有些方式需要通信双方建立连接，例如，在打电话的过程中，通信双方建立了一条连接以相互通话。但也有很多方式并不需要双方建立连接。比如写信，通信双方并不需要事先建立好一个通信连接。

思考：在计算机网络中，为什么在存在有连接通信协议的情况下，还会存在无连接的通信协议？

一、用户数据报协议

UDP 是一种无连接的协议，发送数据之前，通信双方不需要像 TCP 那样进行“握手”。因此，主机不需要通过复杂的参数维持连接状态，这使得 UDP 的首部比 TCP 简单得多。UDP 也没有拥塞控制机制，因此网络出现的拥塞不会使源主机降低发送速率，这对于一些实时性要求更高的应用（如后面内容中将提到的网络电话或视频聊天）更加适合。这些应用允许部分丢失数据，但数据传输的时延和开销较小。

要注意的是，UDP 和 IP 都是无连接的协议，但它们之间是有区别的。首先，UDP 和 IP 分别位于传输层和网络层，因此它们的功能不一样。IP 的基本传输单元称为数据报或分组，而 UDP 的基本传输单元被称为用户数据报。UDP 负责将应用数据封装成用户数据报或从接收到的用户数据报中取得应用数据，而 IP 负责将分组传输到目标主机。UDP 和 IP 的另一大不同是 UDP 既校验用户数据报的首部，又校验整个数据部分，而 IP 只校验首部的信息。因此，和 IP 相比，UDP 能够进一步保证数据传输的正确性。

二、基于 UDP 的典型应用

大部分应用层协议虽然是基于 TCP 的，但也有不少应用采用

UDP 的传输方式，这些应用的特点有：(1)报文传输量小，即带宽要求较低；(2)对实时性要求高而对可靠性要求较低，能容忍部分报文的丢失。下面介绍基于 UDP 的两个典型应用：域名系统(domain name system，简称 DNS)和网络电话或视频通信。

1. 域名系统

本章第二节已经介绍了电子邮件和万维网的相关知识。人们在收发电子邮件和浏览 Web 网站时，通常不会采用 IP 地址去和服务器通信，而是通过一串由字母、数字组成，通过点号“.”来分隔的域名访问服务器。DNS 正是将域名转换为对应 IP 地址的系统。由于域名通常由有意义的单词、数字等构成，比单纯的 IP 地址更容易记忆。例如：上海市政府官方网站的域名“www. shanghai. gov. cn”明显要比目前其对应的 IP 地址“117. 184. 226. 77”好记得多。

假设某人要访问一个网站，他会在浏览器里输入网站的域名，浏览器首先会向网络中发送一个 DNS 查询报文，该报文会通过 UDP 发往服务器的 53 号端口。随后该报文到达 DNS 服务器，DNS 服务器将包含该域名对应 IP 地址的 DNS 响应报文发回给源主机，源主机就知道了目标主机的 IP 地址，就能够开始建立和网站的连接了。

2. 网络电话或视频通信

如今，人们经常会使用各种即时通信工具进行语音或视频通信。从用户的角度看，这和传统的电话服务几乎没有区别。使用 IP 技术实现的语音通信通常也被称为“IP 语音”(voice-over-IP，简称 VoIP)。

VoIP 服务报文通常被封装在 UDP 中。UDP 提供的是无连接的不可靠传输服务，如果网络发生拥塞或传输路径上出现了问题，该报文有可能会丢失。如果采用 TCP，虽然可以避免报文的丢失，但会带来较大的时延，这对于实时性要求更高的 VoIP 服务是不可容忍的。对于 VoIP 服务来说，分组丢失并不一定意味着传输质量的下降，一些网络电话或视频应用会采用编码的方式恢复一些丢失的数据，或是通过软件运算补帧等方式做到语音或视频“看起来比较流畅”。总体上，对 IP 语音服务来说，10%左右的丢包率还是可以容忍的。但是，如果网络情况很糟糕，丢包率达到 20%甚至更多，那么无论采取哪种措施都无法保证通信的质量。因此，VoIP 服务采用 UDP 具有一定局限性，但在一般情况下，仍是比 TCP 更好的选择。

三、TCP与 UDP的使用场合

作为一个软件开发者，当我们创建一个新的网络应用时，选择何种传输协议承载应用是非常关键的。如前所述，TCP 和 UDP 分别具有不同的特性，因此适用于不同场合和用途的网络应用。

1. 基于 TCP 的网络服务

TCP 主要用于可靠的数据传输服务。如果要开发的网络应用本身是不能容忍差错和数据丢失的，那么应该采用 TCP 作为传输层的协议。TCP 还具有拥塞控制机制，使每个进程能够比较公平地共享网络带宽。另外，建立在 TCP 之上的一系列的网络安全协议能够保障数据在传输时是安全的。但是，使用 TCP 进行数据传输，其传输时延会长一些，对一些实时性要求更高的服务来说，TCP 就不一定是最好的选择。

2. 基于 UDP 的网络服务

UDP 是一种轻量级传输层协议，它是一个无连接的协议，网络两端的两个进程在传送数据时不需要反复地确认或重传。因此我们说 UDP 是不可靠的。但 UDP 实现相对简单。在对通信质量要求不高，但实时性和传输速度要求更高时，可以选择 UDP 作为传输层协议。

表 3.4 总结了几种常见的网络应用场景及它们可以采用的传输层协议。

表 3.4　常用的网络服务场景和可采用的传输层协议

网络服务场景	对可靠性的要求			可采用的传输层协议
	容忍丢失	带宽要求	实时性	
文件传输	不能丢失	弹性	弱	TCP
电子邮件	不能丢失	弹性	弱	TCP
网页浏览	不能丢失	弹性	弱	TCP
网络电话 视频	容忍丢失	高	强	UDP
网络游戏	容忍丢失	中等	强	UDP或 TCP
移动即时通信	不能丢失	弹性	强	UDP或 TCP

探　究　活　动

建筑工程师、气象专家、农业专家等不同的科考团队有不同的通信需求，请为他们选择合适的应用程序，并向他们介绍该应用程序的连接特性，填入表 3.5中。

其中，农业专家在决定使用哪类传输协议时产生了争论，争论的主要焦点在于“为什么要采用 UDP作为传输层协议，如果采用 TCP会出现什么问题”。请模拟农业专家讨论的情境并记录讨论结果。

表 3.5　不同科考团队的通信需求、所需的应用程序和它们的连接特性

科考团队及其通信需求	应用程序	连接特性
建筑工程师：需要实时地交流工程建设情况	即时通信软件	可靠传输
气象专家：需要将采集到的气象数据及时公布给大众		
农业专家：需要通过视频监视农作物的生长情况		
医疗团队：需要_____		

讨论结果记录

第四节　网络资源共享

网络资源主要是指借助于网络环境可以利用的各种信息资源的总和。网络资源又称网络信息资源。也就是说，我们日常接触的文本、图像、音频、视频等文件，一旦在互联网上传播，就成为了网络资源。除此之外，这些文件中蕴含的信息本身也是可以利用的网络资源。正当地、正确地使用网络资源也是每一位高中生都要做到的基本要求。

体　验　思　考

常见的文本、图像、音频、视频等都是以文件形式保存的。我们已经学习了通过电子邮件或万维网将这些文件共享给其他人。但是，网络资源往往并不以单个文件存在。比如说，一个很复杂的软件（如文字处理软件、图像处理软件等），它需要很多文件来支撑自己的运行，而这些文件并不一定全部都在这个软件的安装路径下。

思考：如果要将一个很复杂的软件通过网络共享给别人，能否通过简单文件共享的方式来处理？另外，能否将计算机的硬件，如网络打印机、硬盘、显卡等，也作为网络资源共享给其他人？

一、云计算

随着网络规模的不断扩大和互联网技术的不断发展，“云计算”这种新型网络服务模式发展迅速。那么，究竟什么是“云计算”？它和网络资源共享又存在什么关系呢？

1. 云计算概念

假设三个不同地区的科研小组的科学家们要共同解决一个科学问题，其中科研小组 A 提供大量的数据，科研小组 B 提供计算和存储的资源，科研小组 C 提供易于识别的输出形式。通过互联网，这些科学家们可以将这些资源全部连接起来，从而实现输入输出、计算、存储等功能在不同的计算机上运行。同样通过互联网，三个小组的科学家也可以共享输出的结果。如图 3.14 所示，数据是如何传输的，经过什么路线传输的，对于这些科学家们并不关心，在绘制网络拓扑图的时

候，人们往往就用一朵云来代替复杂的网络结构。因此，人们开始采用“云计算”一词来描述这种输入/输出设备、存储设备、计算设备相分离的计算机资源服务模式。

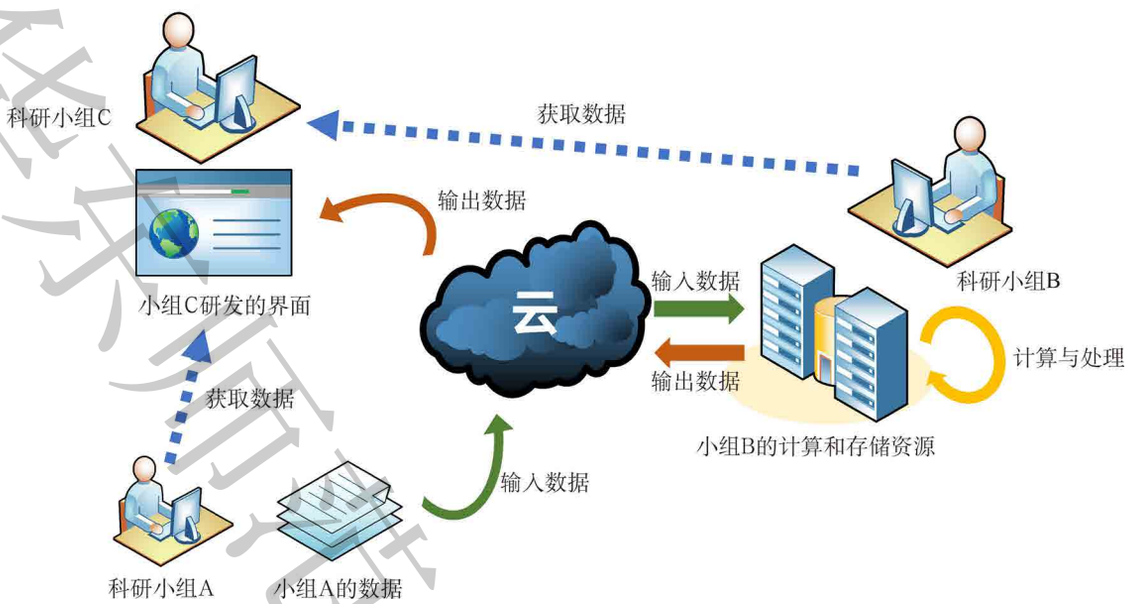


图 3.14　云计算实例

云计算定义如下：云计算是一种基于互联网的计算机资源服务模式，通过这种方式，共享的软硬件资源和信息可以按需提供给计算机和各种终端设备。

用户不需要了解“云”中基础设施的细节，不需要拥有专业知识，也无需进行直接控制。用户通过浏览器、桌面应用程序或是移动应用程序来访问云服务。“云”的主要优势在于动态性、易扩展。也就是说，云计算服务可以动态地调整资源来满足用户的不同需要。

2. 云计算分类

(1) 按运行层次分类

云计算按照运行层次可分为三种主要服务模式，如图 3.15 所示。这三种主要服务模式分别是：

- 软件即服务(software as a service，简称 SaaS)：用户使用由云计算服务商提供的软件进行日常的工作，这些软件并不运行在用户自己的计算机上，而是通过互联网运行在云上。比较常见的例子就是无盘办公系统。
- 平台即服务(platform as a service，简称 PaaS)：用户使用主机

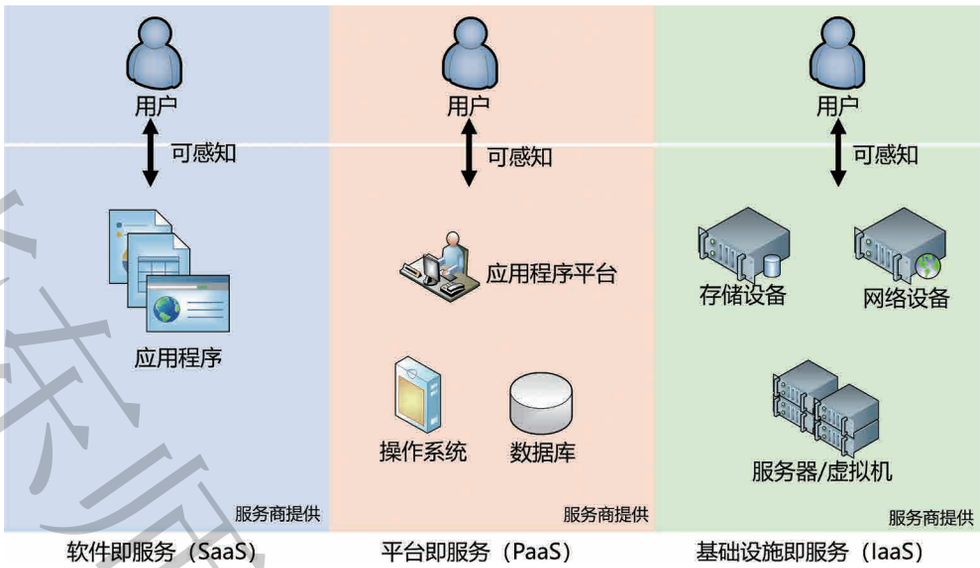


图 3.15　云计算的三种主要服务模式

操作应用程序，并掌控运作应用程序的环境。比如，用户可以将符合一定规范的应用程序部署并运行在云端平台上，可以通过该平台对程序进行管理，但不能直接操作云端的操作系统。

- 基础设施即服务（infrastructure as a service，简称 IaaS）：用户使用“基础计算资源”，如处理能力、存储空间、网络组件等等。通常 IaaS 以虚拟机的形式提供给用户，用户在虚拟机上部署操作系统和应用程序，但看不到云基础设施的架构。现在，大部分企业都采用这种方式部署云端的服务器。

（2）按使用权属分类

云计算可能有不同的权属，按照不同的权属也可以分为三类：

- 私有云：是指由终端用户自己出资建设云端，用户自己对云端有完全的访问权和控制权。根据使用环境不同又可进一步分为家庭私有云和企业机构私有云。
- 公有云：一般由云计算公司建立并运营，向用户以有偿租用的方式提供服务。很多云计算公司运营的都是这种公有云。
- 混合云：是指由几个企业或机构联合出资组建的云计算服务，能够满足各个机构的用户需要。对这些企业或机构来说是公有云，可以实现信息的共享；对外界公众来说是私有云，保证了这些企业或机构的数据和信息的安全。

知 识 延 伸　　在线教育平台

随着社会的不断发展，近年来，人们对知识的需求越来越大，终身学习已经成为一种新时尚。但是，人们往往有自己的工作，不能再像学生时代一样集中在一个固定的课堂里听课。互联网和云计算的发展让人们有更充分的机会利用碎片化的时间进行学习。

图 3.16展示了一个基于云计算的在线教育平台。云服务器提供了运行该平台所必需的软硬件环境；云存储为管理人员存储用户数据，为教师存储其上传的讲座视频，也为学生存储其提交的作业或试卷；应用平台提供各种应用软件运行的环境；用户可直接通过运行在云上的应用软件完成教学视频上传或直播、用户数据管理、在线学习、生成学习报告等等。这些设备通过计算机网络形成了有机整体。用户完全不需要知道其内部运行的细节。这样的在线教育平台，通过云计算技术把自己的软硬件资源共享给每位学习者，给他们提供了个性化的学习体验。

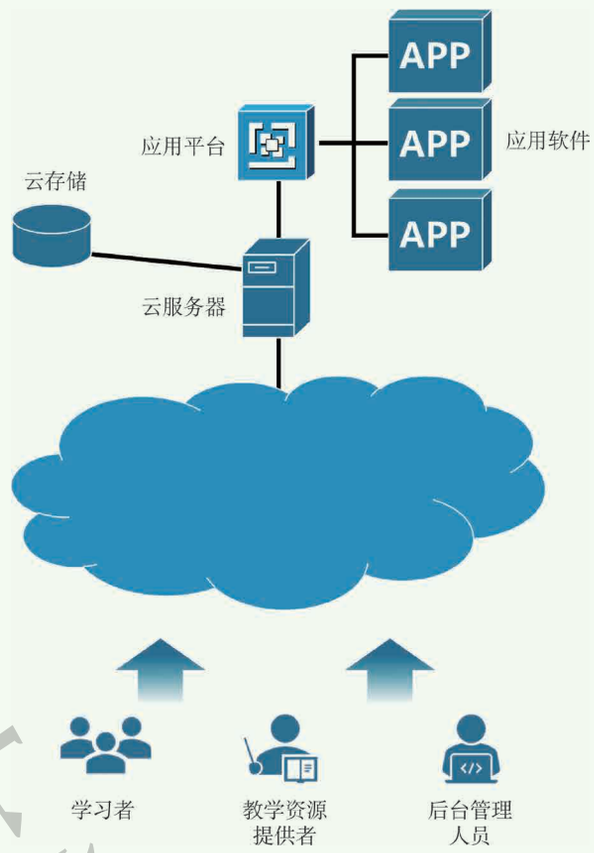


图 3.16　某在线教育平台架构图

3. 云存储服务

云存储服务是 IaaS 的一个特例。云存储是指通过集群应用、网格技术或分布式文件系统等功能，将网络中大量各种不同类型的存储设备通过应用软件集合起来协同工作，共同对外提供数据存储和业务访问功能的一个系统，以保证数据的安全性，并节约存储空间。简单来说，云存储就是将储存资源放到云上供人存取的一种新兴方案。使用者可以在任何时间、任何地方，通过任何可联网的装置连接到云上方便地存取数据。

云存储的重要应用是文件同步和文件共享。

文件同步是云存储的一项重要应用。在过去没有云存储的时代，人们在计算机上编辑各种文件，并用可移动存储设备将它们随身携带。这样就造成一个问题：如果同一份文件在不同的计算机上被编辑

了不同的地方，那么当它们最终要合并的时候，很可能造成文件修改的冲突，从而给人们的工作带来不便。而使用云存储服务存储文件时，由于文件一直保存在云端，编辑者可以像在本地编辑一样直接打开并编辑云端的文件。无论编辑者做了哪些修改，这些修改都会被及时地自动保存下来，从而避免了同一文件的不同修改造成的同步冲突问题。不少云存储产品还提供版本历史回溯功能，用户可以轻易地将文件还原成某个过去的版本。云存储还使得不同用户协同编辑文件成为可能，例如，通过云存储技术和文件同步，两位作者可以分别在两地撰写同一篇文章，作者 A 甚至可以在家中的电脑屏幕上看到位于另一个城市的作者 B 是如何修改文章的，云存储技术给人们的工作方式带来了巨大的便利。

云存储技术给人们生活带来的另一项巨大改变，就是使文件共享变得更加容易。首先，云存储服务中，文件的存储是一种链接式存储，只要用户上传的文件和云端已存在的文件存在一样的特征值（这个特征值会被事先计算好），那么用户所看到的“文件”只是指向同一份文件的链接，如图 3.17 所示。当用户需要将这份文件共享出去时，云存储服务会自动生成一个指向该文件的链接，其他用户就可以通过这个链接获得被分享的文件。此外，云存储服务还支持断点续传或对等传输功能，用户可以随时中断或恢复传输。如今，运用云存储服务上传、共享文件也已经成为了广大互联网用户乐于接受的文件传输方式。

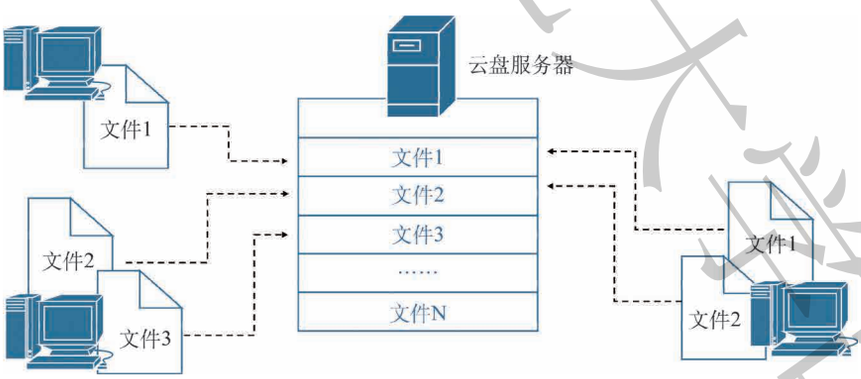


图 3.17　云盘的链接式存储

二、移动互联网

手机从 20 世纪 80 年代的“大哥大”到现在的小巧玲珑，从仅仅只能打电话的“手提电话”到拥有各种移动应用、能智能感知用户网络生活、给用户带来巨大便利的移动设备，这其中的进步是巨大的。2012 年智能手机开始呈现井喷式发展，智能手机上的各种应用也越来越丰富，人们开始真正拥抱移动互联网时代。那么，在现在这个移动互联网主导的时代，我们又应当如何共享资源？这其中又包含了哪些关键技术呢？

1. 4G 移动网络

首先要指出的是，“无线网络”和“移动网络”并不是“孪生兄弟”。一台采用无线方式（如 Wi-Fi）接入互联网的计算机可能并不能移动，而一台可移动的主机也未必采用无线方式接入互联网。

本书讲的“移动网络”，主要讲的是以蜂窝网作为支撑的移动通信系统。自 20 世纪 90 年代以来，全球移动通信系统（global system for mobile communication，简称 GSM）已经成长为移动电话领域的庞然大物。蜂窝（cellular）是指这样一种无线通信网络：信号覆盖区域被分为许多“小区”，这些小区一般呈正六边形，与现实中的蜂窝相似（如图 3.18 所示）。图中每个小区包含一个收发基站，负责向位于其小区内的移动站点发送或接收信号。

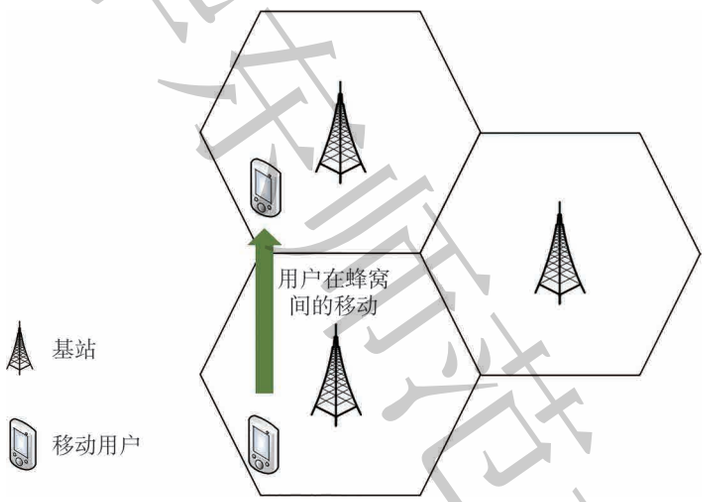


图 3.18　蜂窝网示意图

现在的智能手机已经支持完整的 TCP/IP 协议族，并能够经过蜂窝网接入互联网。

移动网络的发展经过了 3G、4G 到今天的 5G，从早期的移动电话开始，移动通信技术已经经历了四代，如今已经发展到第五代。3G 网络采用了语音网络和数据网络分立的体系结构，如图 3.19 所示，语音信息通过移动交换网进入公共电话网，而非语音的数据信息通过通用分组无线服务核心网（general packet radio service，GPRS）在互联网上传输。

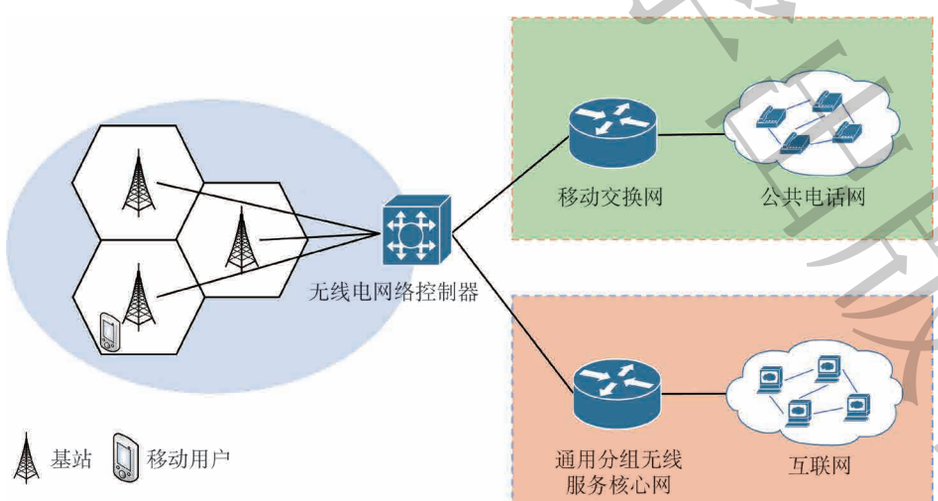


图 3.19　3G 移动网络架构图

3G 网络只能算一

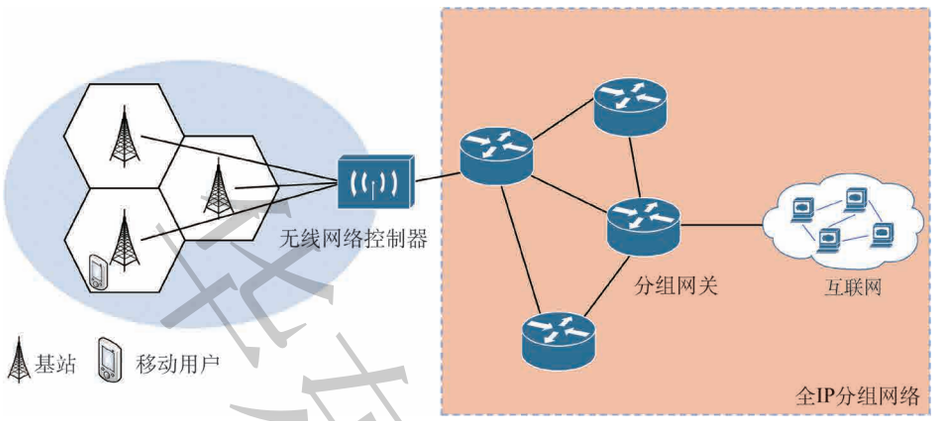


图 3.20　4G 网络拓扑示意图

种权宜之计，提高数据传输效率的根本解决方法是将数据网络和语音网络融合。因此，4G 长期演进互联网(long term evolution，简称 LTE)网络采用了完全不同的体系结构，它是一种统一的、全 IP 网络的体系结构，其拓扑图如图 3.20 所示。4G 网络的特点是：语音和数据都承载在 IP 报文中。到了 4G 时代，原来的电话网络的痕迹已经荡然无存，全部让位给统一的 IP 服务了。

图 3.20 展示了 4G 网络拓扑的示意图，以 4G 无线网络控制器为界，无线电接入网与全 IP 核心网之间实现了清晰的分离。无论是语音还是数据，都将通过 4G IP 网络通往互联网。在 IP 核心网内，数据像在有线网络中一样，通过不同的移动通信路由器进入互联网。同时，这些移动通信路由器还具有账单处理、流量分析与拦截、移动性管理、鉴别用户数据来源等一系列功能。

但是，4G 网络也存在一些弱点。4G LTE 的核心网络是一个扁平化的 IP 网络，比起 3G 网络，一般 IP 网络中可能存在的攻击，也更容易存在于 4G 网络中。

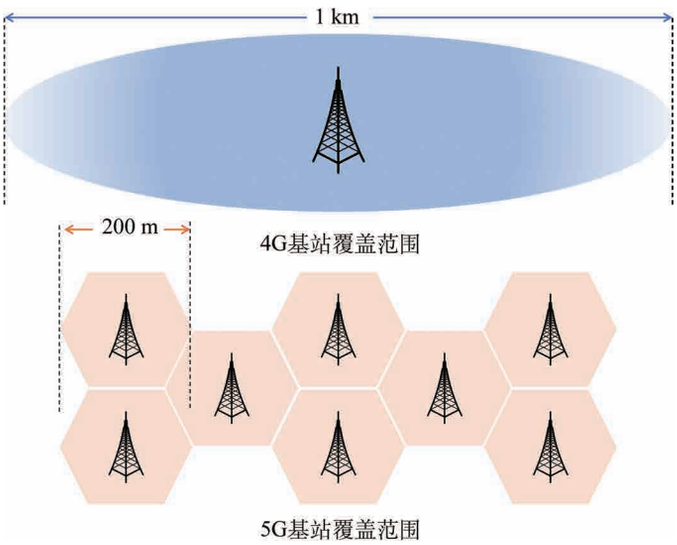


图 3.21　4G 基站和 5G 基站覆盖范围对比

2. 演进到 5G 网络

5G 移动通信网络将开始商用。这一全球瞩目的通信技术革新和 4G 相比具有哪些优势？又可以为我们的生活带来哪些进步呢？

(1) 5G 和 4G 的比较

表 3.6 展现了 5G 和 4G 的部分技术指标的对比。可以看到，虽然 5G 比 4G 拥有更高的通信频率和平均带宽(这也就意味着单位时间携带数据量的提升)，但随着通信频率的提升，5G 信号的传播范围比 4G 更小了(如图 3.21 所示)。同时，5G 尚

未解决网络连接的可靠性问题，在一些对时延要求特别严格的场合可能不能体现 5G 的优势。

表 3.6　4G 网络与 5G 网络的部分技术指标对比

技术指标	4G 网络	5G 网络
通信频率	1.8 GHz~ 2.6 GHz	24 GHz, 28 GHz, 65 GHz
平均带宽	约 100 Mbps	约 10 Gbps
传播范围	约 1 km	约 200 m
平均时延	10 ms~ 100 ms	1 ms以下
天线阵列	2× 2或 4× 4	64× 64以上
穿透性	较好	较弱

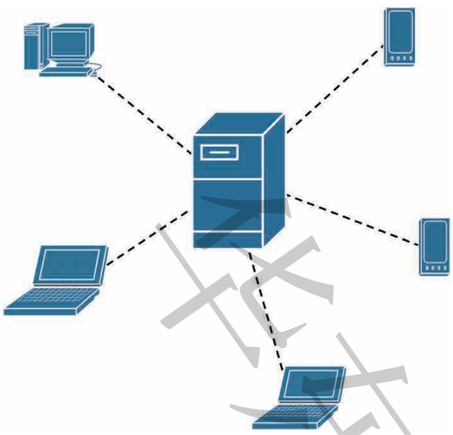
（2）5G 应用场景

3G、4G 网络的出现标志着移动互联网的诞生，能够覆盖占地球表面积约 30％的人类活动。但随着物物相连的物联网时代到来（将在第六章详细阐述），人们开始追求计算机网络更广阔的覆盖面积。同时，人们对物联网和智能设备的需求越来越多，追求更高的带宽、更低的时延和更高的可靠性。因此，5G 网络正是为了解决这些问题而诞生的。

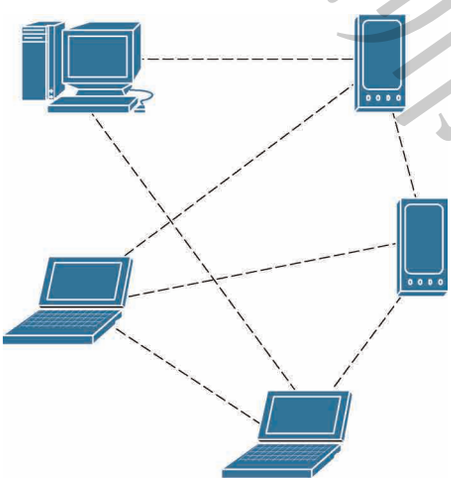
5G 应用场景一：工业物联网。工业化大规模生产意味着可能有成百上千个物联网设备要同时连接到网络。因此，5G 带来的高带宽能够使它容纳下更多的设备同时连接，且每个设备都具有自己的通信路径。这就类似于一条具有成百上千根车道的“高速公路”，数据包就是行驶在这样的“高速公路”上的“汽车”，由于很少发生抢占“车道”的现象，每个数据包都能够获得最大的传输效率。

5G 应用场景二：无人驾驶汽车和无人机。无人驾驶汽车在行驶过程中会持续将数据通过网络上传至数据中心，以使用数据中心的计算资源分析复杂路况，并及时获得分析结果以便汽车遇到突发状况时快速做出响应。这就要求汽车连接到的网络应是低时延的。5G 网络将带来更低的时延，无人汽车能够在极短的时间内，完成“获取道路图像”——“上传图像等待处理”——“获得处理结果”——“做出响应”等一系列动作，从而避免交通事故的发生。

5G 应用场景三：影音娱乐。如前文所述，5G 网络会带来更高的带宽，单位时间内能够传输更多的数据。实验证明，一部 4K 高清电影也能够在几秒钟内下载完毕，在线观看视频更没有卡顿等现象。5G



（a）C/S 架构



（b）P2P 架构

图 3.22　C/S 体系架构和 P2P 体系架构的比较

时代的到来会提升人们的日常娱乐体验。

3. 移动网络中的资源共享

前面几节描述的网络服务都是采用 C/S 架构运行的，它们极大地依赖于服务器，一旦服务器出现问题，那么整个网络服务的运作都会受到影响。在如今的移动互联网和物联网的时代，如果所有的网络通信都需要依赖于服务器，不仅极大地占用了网络带宽，更可能因为服务器的故障导致该移动互联网应用或物联网络崩溃。对等传输（P2P）可以解决这一问题。使用 P2P 体系结构，主机可以尽最大可能减少对中心服务器的依赖，称为对等方的成对主机可以直接进行通信。C/S 架构和 P2P 架构的对比如图 3.22(a)和图 3.22(b)所示。图中设备之间的虚线表示这些设备之间建立了通信关系。需要强调的是，这两种通信架构各有优缺点，各有不同的应用场景，并不能说哪种架构比另一种更优秀。

本节我们重点关注两款典型的 P2P 应用：文件分发和即时通信，它们在现代网络应用中占据了很大的比重。特别是近年来随着即时通信软件的发展，它们也同时具备文件分发和共享的功能，这两类软件之间的区别也越来越小。

（1）P2P 文件分发

传统的文件共享场景是这样的：用户 A 希望将他的文件 F 分享给他人，于是将该文件上传至一个中心服务器上，当用户 B 希望下载该文件时，他将从服务器上下载该文件的一个完整的副本。同理，当用户 C、D 希望下载该文件时，都会从同一服务器上获取该文件的副本。在这种场景下，当有大量用户同时下载或上传文件时，服务器将会承受巨大的负担，并且会占用大量网络带宽。而到了 P2P 的文件分发场景中，每个对等方能够直接向任何其他对等方发送该文件的一部分，同时也能够向任何其他对等方获取自己还缺少的部分。

当一台新的主机加入该 P2P 文件分发网络中时，它能够获取一个目前网络中存在用户的列表，同时尝试与每一个用户建立 TCP 连接。当成功建立 TCP 连接后，该连接的双方就被称为“邻接对等方”，从而能够实现文件块的传输。而一个用户的邻接对等方数量会随时间波动变化，因为可能不断有新的用户加入该网络，同样也会有用户离开

该网络。理论上，当加入的对等节点越多，文件下载或上传速度将会越快，这和传统的“客户端—服务器”模式下载文件有本质的区别，也是用户喜欢 P2P 下载的重要原因之一。

（2） 即时通信技术

随着移动互联网和智能手机的发展，用户使用即时通信的需求日益增长，如果采用“客户端—服务器”架构的通信方式，服务器的负担也是十分巨大的，因此现在的即时通信软件也采用 P2P 技术使用户相互通信。但和 P2P 文件分发不同，即时通信技术并不是严格的 P2P 架构，而是有服务器参与其中的混合型架构。该架构可以用图 3.23 来描述。

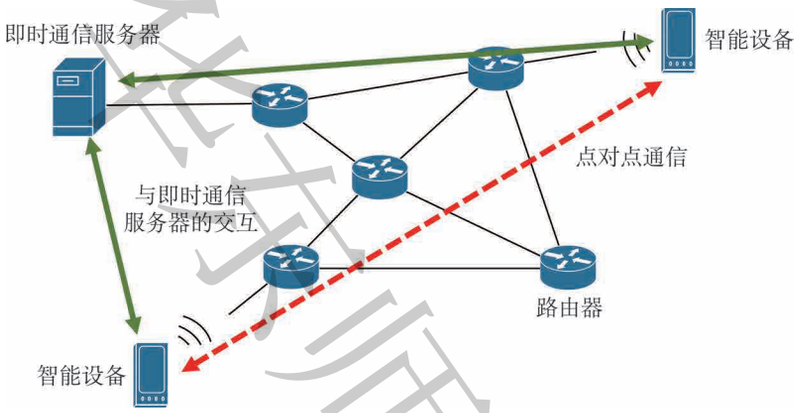


图 3.23　即时通信网络传输过程

从图 3.23 中可以看到，用户到用户的即时通信消息在用户主机之间直接发送，而无需通过服务器。但网络中仍存在即时通信服务器，它并不负责交换即时通信的内容，只是负责跟踪用户的 IP 地址，维护目前在线的好友列表等功能。需要注意的是，虽然图 3.22(b)用直线表示移动设备之间，以及移动设备和服务器之间的交互，但实际上它们的通信仍需要经过路由器等网络设备。

探　究　活　动

气象专家们需要对自己监测、采集到的各种气象数据进行分析和预测。但是他们手上的计算机资源有限，为此，他们将目光投向了互联网，希望能够找到一个能满足他们需求的平台并完成计算任务。假设你是一名网络工程师，请为他们完成一份“针对气象数据分析和预测的云计算方案”。

实施步骤：

1　通过网上查阅资料，列举两三例常用云计算平台。并选择其中一例，进一步搜索其在大数据处理方面有哪些解决方案。

2　基于上述整理的解决方案，完成“针对气象数据分析和预测的云计算方案”任务单。

3　将你的研究内容与解决方案形成电子文档或演示文稿，通过云存储共享给全班同学。

任务单

针对气象数据分析和预测的云计算方案

1 目前，我国主要采用的云计算平台有：

（1）_____

（2）_____

（3）_____

2 我所选择的云计算平台是：_____

该平台对大数据处理的解决方案有：（择要记录）_____

_____

_____

_____

3 根据上述选择，我设计的气象大数据云计算方案是：

（可绘制需要的组件和它们相互连接的情况，可仿照网站上的内容进行描述）

（1）需求分析

（2）可行性分析

（3）解决方案

（4）预期成果

第四章

网络中的安全问题

本章学习目标

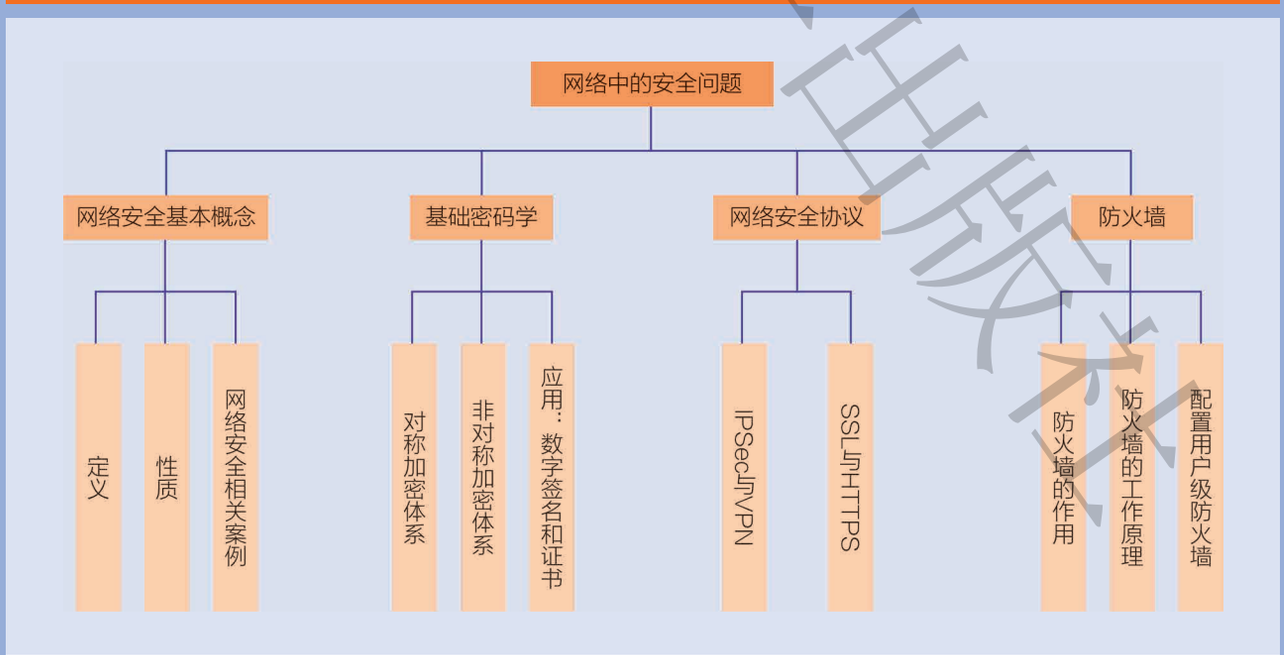
- 通过分析实际案例，总结在网络使用过程中的安全原则。
- 区分对称加密体系和非对称加密体系，描述数字签名和证书的工作原理。
- 描述网络安全协议（IPSec和 SSL）的工作原理，解释密码学在网络安全协议中的作用。
- 描述防火墙的作用和工作原理，尝试配置用户级防火墙。

计算机网络已经渗透到人们生活的方方面面。然而，网络上有不少不怀好意的人利用网络设计上的一些缺陷，试图对人们所处的网络环境进行破坏或是窥探他人的隐私数据。这些“坏家伙”让人们意识到网络是不安全的。

网络安全和信息化是“一体之两翼、驱动之双轮”。“没有网络安全就没有国家安全，没有信息化就没有现代化。”我国拥有大量网民，其中许多人受到过不同程度的网络安全问题的困扰。提高大众的网络安全意识已成为我国网络安全工作的重要环节。

在本章的学习中，我们将共同直面计算机网络中的安全问题，首先我们要了解网络安全和隐私保护的重要性，增强隐私保护意识，从常见的情境入手，学习网络安全的基础知识，并尝试构建安全的网络环境。这样，我们就不会再饱受安全问题和故障问题的困扰，从而享受信息时代本该拥有的乐趣。

本章知识结构



项目主题

阻止“窃听者”

项·目·情·境

在这个新的星球上，除了来自地球的科考队员，还有来自其他星球的“外星人”。大多数“外星人”是友好的，但也有少部分不怀好意。图 4.1所示的是在这个星球上的某个网络拓扑，其中五个科考队的网络通过几个路由器相互连接。

一天，你接到来自两个科考团队的报告，称他们之间相互发送的数据遭到了篡改。你检查了网络，发现一群不怀好意的“窃听者”已经占据了网络 5。这是其他四个科考团队之间发送数据的必经之路，一旦被“窃听者”占据，科考团队之间汇报的科考数据就会被窃取甚至修改，有可能影响到科考团队的人生安全！而且，“窃听者”们还可以进一步入侵其他网络，造成更大的破坏。阻止“窃听者”，势在必行！

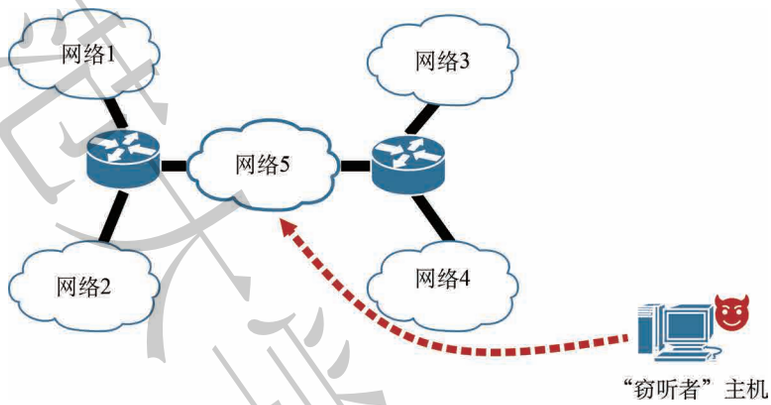


图 4.1　网络环境拓扑图

项·目·任·务

任务 1

分析判断“窃听者”是如何入侵网络 5 的，并探究在使用网络时需要注意的地方。

任务 2

针对可能的攻击手段，尽可能多地找出阻止“窃听者”进一步入侵其他网络的方法。

第一节　网络安全意识

我国互联网的规模仍在不断扩大，互联网正潜移默化地影响着人们生活的方方面面。对信息和数据的保护成了人们关注的热点问题。

体　验　思　考

在各种新闻媒体上，“黑客”一词时常出现在大众的视野里。以 2018年为例 就多次出现了“黑客”窃取用户数据并公开在互联网上售卖的案例，如中国 H酒店集团、Y快递公司等都遭遇过黑客的入侵与信息的泄露。据不完全统计，被窃取信息的用户数量已经超过 1亿人次，给用户和互联网公司造成了巨大的经济损失和隐私泄露问题。

思考：为什么这些大企业都会遭受黑客的威胁？为什么黑客对普通用户的个人信息如此感兴趣？我们在平时使用网络的过程中又有哪些方法可以防止自己的个人隐私数据遭到泄露？

一、网络安全概述

在日常生活中，大家经常能看到“安全”一词。例如，“住宅安全”意味着我们的住宅免受非法入侵；“金融安全”意味着我们的资金不被他人非法挪用；“交通安全”意味着我们出行时不发生交通事故。在特定的环境中，“安全”一词都有它特定的内涵和外延。那么，“网络安全”的内涵和外延又是什么呢？

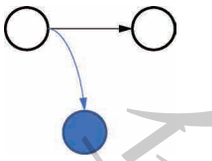
1. 网络安全性质

如果一个计算机网络是“安全”的，那么该网络具有以下性质：

机密性：机密性意味着网络中的任意双方在通信时，它们之间传输的信息是保密的，不会被第三方读取。

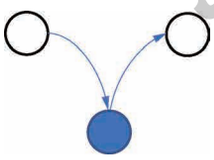
完整性：完整性意味着网络中的任意双方在通信时，它们之间传输的信息是完整的，没有遭到第三方的破坏或篡改。

可用性：可用性意味着网络中的资源需要被使用时，可以由合法的用户不受阻碍地使用，同时未经授权的访问者不能随意使用该资源。

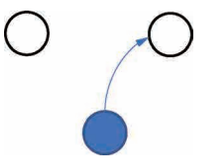


（a）截获

（b）中断



（c）篡改



（d）伪造

图 4.2　安全威胁的类型

2. 网络安全威胁

相对应地，试图破坏这些安全性质的行为就成为计算机网络中的威胁。主要有以下几种类型：

截获：攻击者从网络上窃听到他人的通信内容。这破坏了通信的机密性。

中断：攻击者有意拦截他人在网络上的通信。这破坏了通信的完整性和可用性。

篡改：攻击者篡改了在网上传输的内容。这也破坏了通信的完整性和可用性。

伪造：攻击者伪造信息在网络上传送。这破坏了通信的机密性和可用性。

这些威胁可以用图 4.2 形象地表示，白色的圆圈表示网络中正常的发送方和接收方，蓝色的圆圈表示攻击者，黑色的箭头代表正常的数据发送路径，而蓝色的箭头表示攻击发生的路径。

如果再进一步地分类，又可以将这几种威胁分为被动攻击和主动攻击。其中，“截获”可认为是一种被动攻击，攻击者只是观察和分析某一段网络上传输的数据而不干扰信息的传输。而被动攻击还可细分为直接嗅探和边信道攻击。直接嗅探指的是攻击者直接获取数据的内容并尝试分析这些内容的行为。而边信道攻击指的是攻击者不直接获取数据的内容，而是从网络运行的状态（如流向服务器或网络设备的电流/电压变化、网络设备的 CPU 运转情况，甚至是机房的温度变化）探测出目前该网络的状态，以便开展进一步的攻击。

另外三种威胁则属于主动攻击的范畴。主动攻击是指攻击者对网络上传输的数据进行各种处理，如更改、删除、增加信息的内容。这些攻击往往通过伪造的或修改过的数据引起目标系统的特殊反应，比如返回一段关键信息，或是直接造成目标系统的崩溃等等。主动攻击的危害性要比被动攻击大得多。

二、网络安全案例分析

计算机网络的发展，给人们的生活带来了极大的便利。但是，如果在使用网络时缺少了安全意识，就很有可能造成严重的后果。下面通过几个案例来详细了解一下。

1. 网络安全的相关案例

案例一：某人 A 为了方便地记忆密码，将他所有的网站登录密码全部设置为简单的“123456”。某天，A 最常去的一个视频网站的数据库遭到了黑客的攻击，攻击者看到了或者猜中了 A 的注册邮箱和这个简单的密码。于是黑客开始尝试利用这个信息成功登录了 A 的邮箱，不仅如此，黑客还看到了 A 的银行卡账单，获取了他的银行账户。又经过一次试探，黑客惊讶地发现 A 的银行登录密码也是“123456”，于是，黑客登录了 A 的银行账户并转走了他所有的存款。

图 4.3　弱密码的危害

分析：本案例是典型的由于使用弱密码而导致的安全风险。弱密码是指含有明显规律，容易被人猜到的密码。据统计，“123456”和“password”长期位于“使用得最多的弱密码”排行榜的前两位。由于这些密码很容易被猜测到，如果一个系统采用这样的弱密码，将大幅提升该系统被攻击的概率。因此，在平时设置密码时，不应采用这类过于简单的密码，应采用数字、大小写字母和符号混合且具有一定长度的密码。

案例二：某大四学生 B 下载并安装了一个所谓的“破解版”软件。然而，B 为了图方便省事没有安装任何杀毒软件，也没有开启防火墙，还关闭了操作系统的应用权限控制功能。终于有一天，他看到自己的电脑桌面上弹出一个窗口，要求他将巨额财产转账至某个账户。此时正面临毕业论文终稿答辩的关键时刻，B 却发现自己电脑上的所有文件都被加密且无法打开。

分析：很多“破解版”软件由于会修改系统文件，很容易让病毒、木马藏匿其中。本例中 B 既没有安装杀毒软件，也没有开启防火墙和应用权限控制功能，从而导致病毒、木马长驱直入，对系统数据造成了极大的破坏。

案例三：某人 C 收到一个似乎是来自某著名手机厂商的邮件，邮件中说 C 被抽中获得了该公司最新款的手机，并附上一个确认链接。C 打开这个链接后发现浏览器提示“该网站的安全证书有问题”，C 贪奖心切，点击了“继续访问”，并填写了自己的手机账户名和密码。但之后网站页面无法打开，他试了几次以后就放弃了。过了几天，C 发

现自己的手机被远程锁定，无法使用。虽然经过申诉，手机恢复了使用，但手机内的数据也丢失了，给 C 的生活带来了巨大的不便。

分析：本例是典型的钓鱼网站攻击。钓鱼网站会精心伪造成一些大企业的网站，吸引用户填入自己的账户和密码从而窃取数据。一旦攻击者认为该用户是有价值的，就可以通过他的账户密码展开进一步的攻击活动。预防这种攻击的方法是在上网浏览时注意网站的域名，如果和官方网站不同，或没有安全证书，就必须多留一个心眼了。

知 识 延 伸　　病毒和木马

计算机病毒是一种会“感染”其他程序的恶意程序，这种“感染”是通过修改其他程序，把自身或自身的变种复制进去而完成的。早期的病毒由于会明显改变文件大小，因此容易被识别出来。如今的病毒程序体积很小，可能只有几个字节，但会常驻在操作系统的系统文件区域。病毒会在特定日期或时间发作，会造成计算机系统卡顿、停止运行、出现奇怪的窗口，甚至硬盘上的全部文件被删除等。现在的病毒大多属于“蠕虫”，通过网络进行传播，其传播能力更强，破坏性也很大。

木马，即“特洛伊木马”，其名来源于古希腊传说故事，也是一种恶意程序。和纯粹为了破坏的计算机病毒不同，木马很少对系统造成明显的破坏，但会在系统中开启一个特定的端口称为“后门”。入侵者会通过该端口连接到中了木马的计算机，能轻而易举获取并提升用户权限，从而窃取计算机上的重要数据。

2. 隐私保护的相关案例

上面三个案例分别从密码安全、系统安全和传输安全三个角度体现了加强信息安全意识的重要性。除此之外，在使用网络的过程中，我们也要注意对自己隐私的保护。请看下面三个案例：

案例四：某学校 D 为了公示新生奖学金的名单，将含有姓名、学号、身份证号、手机号等信息的电子表格直接上传到学校的官网上。不久以后，该学校的学生 E 接到了来自“学校”的电话，对方准确地报出了 E 的身份证号、手机号等信息，并要求 E 以“入学保证金”的名义向某个账户汇款才能领取新生奖学金，E 照做以后不久就接到来自真正的学校发送的警示邮件，这才发现自己上当受骗，痛悔不已。

分析：本例中学校 D 违反了隐私保护的基本原则，将含有重要敏感隐私数据的文件上传至互联网，导致数据能够被任何人查看，从而使别有用心的人能够获取并利用这些数据。在平时使用互联网的过程中，也要注意不能把含有重要敏感数据的文档随意上传至互联网上，而应采用加密传输或对文件本身加密等方式以保护数据。

案例五：某企业 F 的中央服务器安装了全世界最强的防火墙，号称“任何来自外部的攻击都无法攻破它”。然而黑客截获了企业 F 的网络管理员给老板发的邮件，其中提到了系统管理员的账户和密码。于是黑客利用这些信息，不费吹灰之力就登录了 F 企业的中央服务器，窃取了重要的数据资料。

分析：本例中虽然企业 F 安装了最强的防火墙，但由于员工的疏忽使得系统管理员的账户和密码在互联网上公开流传。和上一个例子一样，本例中的系统管理员也应采用加密传输方法发送数据。

案例六：喜爱旅游的某同学 G 是个社交网络“达人”，经常在社交网络上“晒”自己的旅行经历和照片。一天，她接到一个自称“公安局”打来的电话，对方不仅准确地报出 G 的姓名，更精准地说出了她最近一个月的行程，并声称 G 涉嫌一起涉外犯罪，要求她向某个“安全账户”汇入巨款。虽然 G 没有上当，但是她也对自己的隐私泄露感到了害怕，从此停止了在社交网络上分享自己旅行经历的行为。

图 4.4　使用社交媒体不当造成隐私泄露

分析：本例是由于使用社交媒体不当造成的隐私泄露。目前社交媒体仍是广大网民使用最广泛的网络应用之一，但其公开性和强烈的个人属性很容易导致用户“引火烧身”。为此，在使用社交媒体时要注意保护自己的隐私，不要把自己的生活完全公开在社交媒体上。

从以上几个例子可以看出，如果不注重自己的隐私保护，可能会造成严重的后果，如金钱的损失、资料的破坏等等。我们要从这些案例中吸取教训，在使用网络时要不断告诫自己绷紧网络安全这根“弦”，不要让类似的事件在自己身上上演。

分　析　评　价

请根据上述案例和分析，讨论并总结出在使用计算机网络过程中要注意的安全事项。

第二节　网络安全技术

我们在生活中经常使用密码，例如电子邮箱账户的密码、网上银行的密码等。那么密码的本质是什么？它又是如何保护我们的数据不被其他人窥探的呢？密码在网络传输过程中又起到什么作用？

体　验　思　考

人类社会从古代开始就已经有了信息安全的意识。例如，早在春秋战国时期，各诸侯国为了防止将领私自调兵，会采用“虎符”作为调兵凭证。“虎符”由中央政府发给掌兵大将，其背面刻有铭文，分为两半，右半存于朝廷，左半发给统兵将帅或地方长官，调兵时需要两半合对铭文才能生效（如图 4.5所示）。到了近代，人们为了安全地传递军情，发明了能够生成密码的密码机，用于保护重要军事情报。1941年，著名计算机科学家图灵破译了当时德军的密码机“恩尼格玛”（Enigma）（如图 4.6所示），为盟军最后的胜利提供了有力保障。

图 4.5　虎符

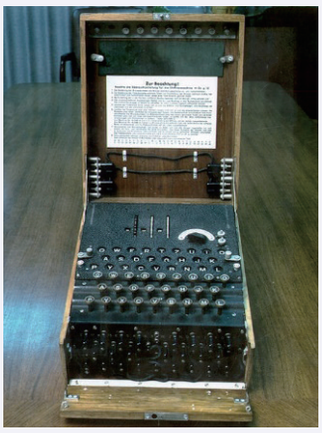


图 4.6　恩尼格玛密码机

思考：“虎符”为什么能够保障调兵命令的准确传达？它符合信息安全的哪些特征？它又和我们今天的哪些安全技术相类似？

一、基础密码学及其应用

在数据传输的过程中需要有安全的传输手段。很容易想到的一种方法是将我们要传输的内容进行某种变换，使得第三方即使截获了在网络上传输的信息，也无法解读出信息的内容，这样就能起到保护信息的作用。其中，要传输的信息的本来面目称为明文，变换后的信息称为密文。将明文变换为密文的过程称为加密，反之称为解密。明文和密文之间的转换根据加密算法来进行，加密算法中会使用密钥作为参数，作用于明文或密文来实现加密或解密。

加密算法主要可以分为两大类。在加密和解密时如果采用相同的密钥，那么这种加密算法就称为对称加密算法，如果采用不同的密

钥，称为非对称加密算法。本节主要讨论这两种体系的基本原理，同时还会介绍密码学的重要应用——数字签名和证书，它们共同构成网络安全协议的基础。

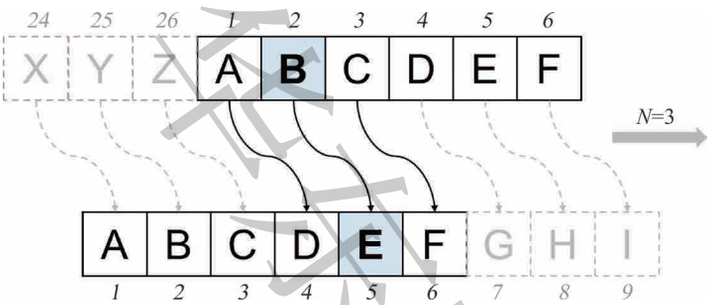


图 4.7　恺撒密码中当 N = 3时的移位变化

1. 对称加密体系

一种最简单的对称加密方法如图 4.7 所示。以英文字母的加密为例，将每一个英文字母分别标上 1 至 26 的编号，将每个字符向后循环移动 N 位，得到新的字符。如图 4.7 中所示，当 N = 3 时，A 向后移动 3 位变为 D，B 向后移动 3 位变为 E，X 向后移动 3 位重新循环到 A，等等。通过这种方法就能将明文变换成密文。这里的 N 就是密钥。接收方收到密文后，只要知道密钥 N，就可以反向解密出明文。这就是移位加密法，相传这种方法是古罗马的恺撒发明的，所以又称为“恺撒密码”。例如：明文“GOODLUCK”用密钥 N = 3 加密得到的密文为“JRRGOXFN”，又如密文“WKDQNBRX”用密钥 N = 3 解密得到的明文是“THANKYOU”。

除了这种最简单的移位替换密码外，还有随机替换密码（即不是按字母顺序移动替换，而是随机打乱顺序替换）、栅栏密码（将原文按一定长度打乱顺序重新排列）、词典密码（使用词典内若干单词对某个字母循环加密）等等。另外，为了进一步提高安全性，在实际的加密场景中，人们可能不止采用一次加密，而是几种加密方法的混合。这样，可有效避免密钥被第三方猜测出来从而破解密码。AES（高级加密系统）就采用了这样的做法。它的复杂性足够大，以至于在短时间内无法破解密钥，在一定程度上足以保证系统或数据的安全。

作业练习

根据恺撒密码原理，解密如下密文：

密文：XAXZTCTILDGZHTRJGXN　　明文：_____

提示：密钥 N 请通过观察字母规律自行寻找。句子中只包含大写字母。注意原句中不含空格，请解密后在句子的适当地方加上空格，使之成为一句完整的句子。

2. 非对称加密体系

对称加密虽然形式简单，但如何传递密钥成了最大的问题。如果密钥不幸被第三方截获，那么通信双方之间的一切秘密就荡然无存了。此外，一个有 n 个用户的系统需要$n(n-1)/2$ 个密钥，用户数量越多，需要管理的密钥就越多，管理密钥的难度会越来越大。为了解决上述问题，计算机科学家们提出了非对称加密方法。在非对称密码中，通过某种算法能产生一对不同的密钥，一把称为公钥（记作 K^+），大家都能使用它对数据加密；一把称为私钥（记作 K^-），只有合法的接收方拥有。加密方使用公钥对传输的信息进行加密，只有合法的接收方才能使用自己的私钥进行解密，该过程如图 4.8 所示。采用这种密码技术，即使公开了加密方法也不会造成泄密。这在一定程度上解决了密钥被截获造成的通信安全问题，同时也有效减少了通信所需密钥的数量。因此，非对称加密体系也被许多网络安全技术使用。

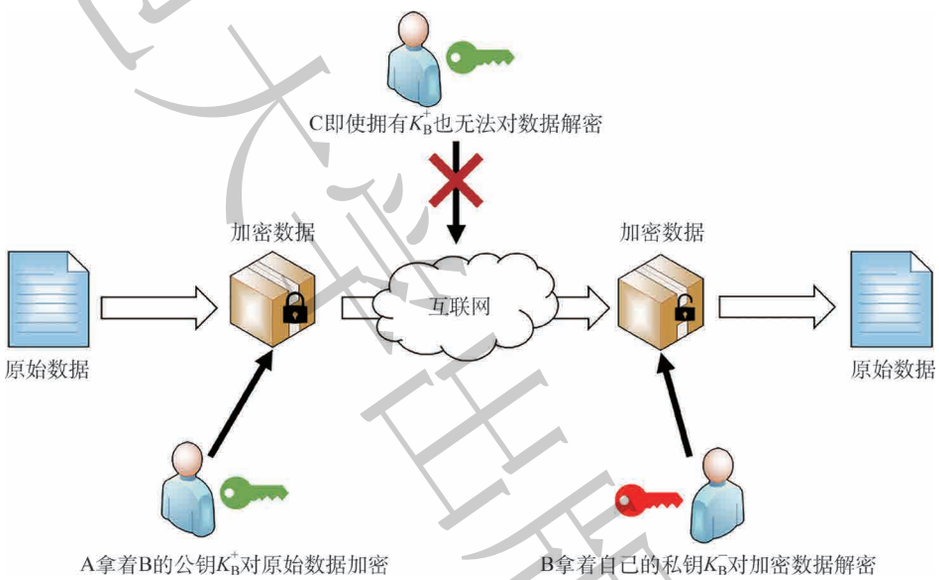


图 4.8　非对称加密

项　目　实　践

非对称密码中的公钥和私钥设计是一个数学问题。其中，RSA算法（由提出该算法的三名科学家的名字命名）是一种典型的非对称密码体系，它依赖的是大整数的质因数分解十分困难，从而利用这两个质因数产生密钥，实现对数据的加密。

RSA算法原理如下：

(1) 选择一对不同的，足够大的质数 p 和 q.

(2) 计算 $n=pq$.

(3) 计算 $f(n)=(p-1)(q-1)$.

(4) 找一个与 $f(n)$ 为互质数的整数 e，且满足 $1<e<f(n)$.

(5) 计算整数 d，使 $d \equiv (e-1) \pmod{f(n)}$.

(6) 获得公钥 $K^{+}=(e, n)$，私钥 $K^{-}=(d, n)$.

(7) 将明文变换至 0 到 $n-1$ 的一个整数 N，可对明文进行分块处理.

(8) 加密过程为：$C \equiv N^{e} \pmod{n}$.

(9) 解密过程为：$N \equiv C^{d} \pmod{n}$.

其中 mod表示求余数的运算。第(5)步、第(8)步和第(9)步中的表达式表示同余运算，即两个数除以同一个数的余数相等。

请根据这一原理，选取一对质数生成公钥和私钥，对明文“SECRET”加密，并对加密后的密文解密，看看是否能还原出明文。为了便于计算，可以选择较小的质数。你也可以使用程序来实现这个算法。

3. 密码学应用：数字签名与证书

现实生活中我们免不了要经常在合同、收据、文件上签名。签名是证明一个人自己（而不是其他人）承认或同意这些文件的内容的手段。在计算机网络安全领域中，我们也经常要证明自己是某个文件的拥有者，或者承认某个文件的内容。数字签名就是密码学在这一领域的应用。

和手写签名一样，数字签名也应该是可以认证的，并且是不可伪造的。换句话说，首先能够证明某个人的数字签名是他本人签署的（可认证性），同时只有他能够签署（不可伪造性）。

数字签名是通过非对称加密方法实现的，但和数据的加密解密过程恰好相反。某人想对他的文件进行数字签名，就用生成的一对密钥（K^{+}，K^{-}）中的私钥 K^{-} 对附加了特征值（由散列算法生成）的文件进行加密，别人需要验证这份签名是否有效，只需要用公钥 K^{+} 进行解密，如果生成的文件与原文件一致，那么这份签名就是有效的。

但是这又带来一个问题：怎么证明这一对密钥（K^{+}，K^{-}）的确是属于这个人的呢？这就需要一个公证机构来证明密钥持有人的合法性。因此证书应运而生。证书是用来证明一个人（或一个网络实体）的真实身份的。一旦证书证明了某个实体的身份，就把该身份和所对

应的公钥绑定起来了。在验证签名的过程中，由于公钥和身份通过证书绑定，就能验证公钥持有人的身份，从而避免了盗用公钥的危险。

整个数字签名和证书的运行过程如图 4.9 所示。

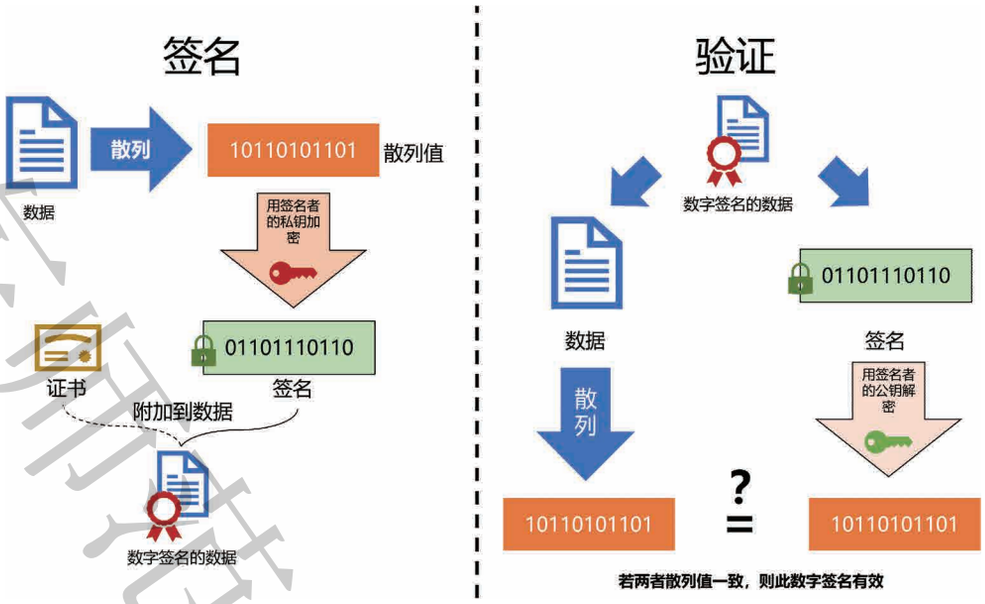


图 4.9　数字签名的生成与验证

知　识　延　伸　区块链技术

狭义来讲，区块链是一种按照时间顺序将数据区块以顺序相连的方式组合成的一种链式数据结构，并以密码学方式保证的不可篡改和不可伪造的分布式账本。广义来讲，区块链技术是利用块链式数据结构来验证与存储数据、利用分布式节点共识算法来生成和更新数据、利用密码学的方式保证数据传输和访问的安全、利用由自动化脚本代码组成的智能合约来编程和操作数据的一种全新的分布式基础架构与计算方式。区块链技术示意图如图 4.10所示。

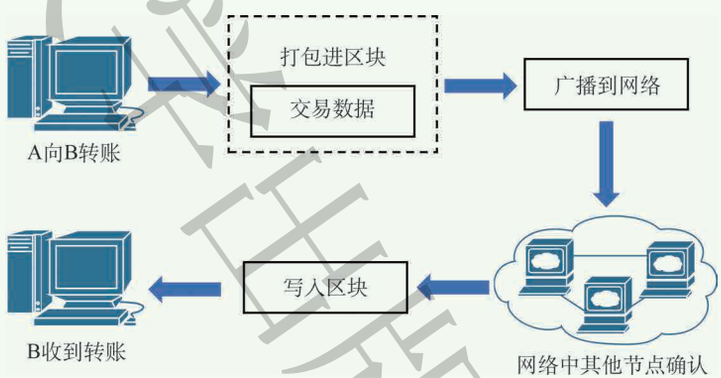


图 4.10　区块链技术示意图

区块链主要解决的是交易的信任和安全问题，因此它针对这个问题提出了四个技术创新：分布式账本、非对称加密和授权技术、共识机制和智能合约。

区块链具有下列特征：去中心化、开放性、自治性、信息不可篡改性、匿名性。

区块链最早是用于维护电子货币账目的方法。将来，除金融领域外，区块链将在数字资产、智能合约、物联网技术等方向发挥作用。

二、网络安全相关协议

在网络通信过程中，如果要考虑到安全的因素，只有加密算法是不够的，因为还需要在两个节点之间建立一致的安全通信协议才可以完成安全的通信。本节将分别介绍网络层和传输层中最常用的安全协议和它们的应用。

1. 网络层安全协议：IPSec 和虚拟专用网

随着经济的全球化发展，很多公司和组织在全球各地都有分公司或办事处。如果某跨国企业的两个位于不同地点的分公司要通过网络进行通信，而通信的内容不希望被其他人看到，应该制定怎样的通信方式呢？

一种容易想到的方法是通过电信企业租用一条专线，但这样的专线造价高昂，而且当通信流量不大时，专线实际上是很浪费的。如果改为通过互联网通信，虽然可以获得较高的链路利用率，但是有通信内容被截取的危险。

为了解决这个问题，虚拟专用网（virtual private network，简称 VPN）应运而生。它虽然建立在互联网上，共享访问互联网的线路出口，但是从用户的角度看来相当于一条专线，所以称为“虚拟”专用网。

VPN 的实现方法有很多种，最常见的一种设计是在每个分公司或办事处之间设立一条网络“隧道”，使数据通过这条“隧道”直接到达目标分公司的网络。那么如何保证这条“隧道”是这个公司“专用”的而不会被其他流量占用呢？“安全的 IP 传输”（IPSec）是一种解决方案。IPSec 不是单一的协议而是一套协议，它通过在网络层的加密传输，提供用户身份的认证。

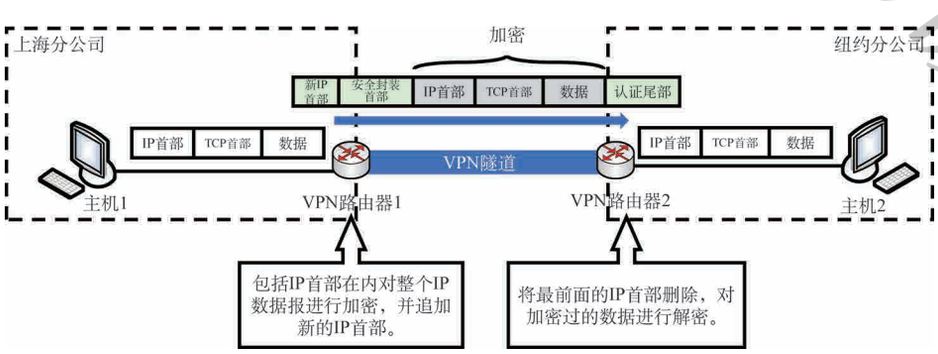
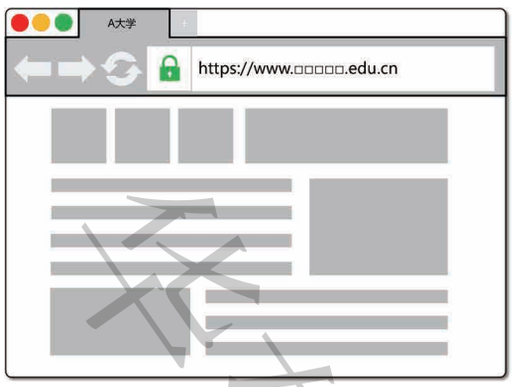
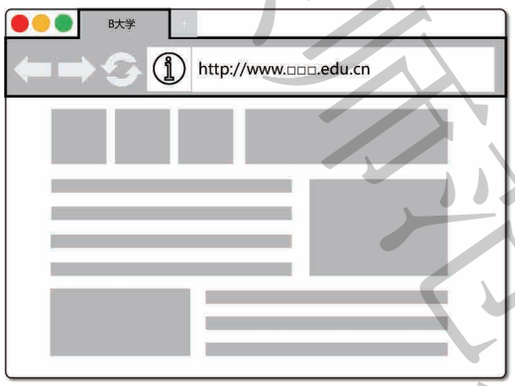


图 4.11　使用 IPSec隧道技术实现 VPN 通信

VPN 中的“隧道”可以类比到现实生活中的高速公路。在这个隧道的两端，各有一个网络安全设备负责检查通信流量的身份信息，就好像是现实中高速公路的收费站一样。如图 4.11 所示，



(a) 使用了安全证书的 HTTPS 站点



(b) 未使用安全证书的 HTTP 站点

图 4.12　不同网站的地址栏

如果某跨国企业的上海分公司要通过 VPN 与纽约总公司通信，那么在隧道的上海端，出口网络设备（可能是路由器或防火墙）对通信流量进行加密并加上认证信息，通过 IPSec 传输到纽约总公司的出口设备，该设备接收到数据以后检查数据，发现认证信息符合该公司事先约定好的格式（比如特定的用户名和密码，或者特殊的数据格式），就对数据解密并发送到要接收数据的目标计算机上，完成一次通信。

2. 传输层安全协议：安全套接字层

使用浏览器浏览网页，可能是人们使用网络时最常进行的操作之一。例如，高中生小李要查找他准备报考的两所大学的信息，A 大学官方网站的域名是 www. □□□□□. edu. cn，B 大学官方网站的域名是 www. □□□. edu. cn。图 4.12 中的图(a)、(b)分别展示了访问两所大学官方网站时，浏览器的地址栏，小李注意到这两个地址栏有一处不同。

不难发现，浏览 A 大学官网时，地址栏左侧出现了一个绿色的锁型标记，同时，访问 A 大学网站 URL 所采用的协议不再是 http，而是 https。这个“s”指的就是安全（security）。比起 HTTP 协议，通过 HTTPS 协议传输的网页更加安全。

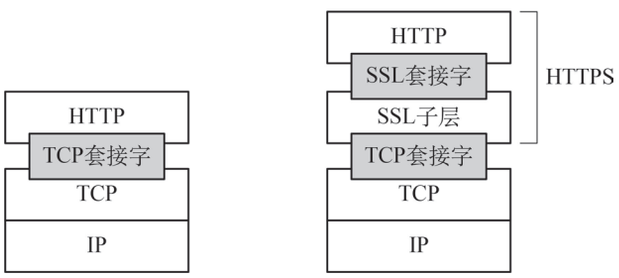


图 4.13　TCP 套接字和加入 SSL 的套接字

第三章介绍过套接字的概念。在传统的 HTTP 中，网页是通过 TCP 套接字进行传输的。当网页采用 HTTPS 协议传输时，HTTP 协议的数据首先通过 SSL（security socket layer，安全套接字层）套接字加密，再将加密后的数据通过 TCP 套接字在互联网上传输，如图 4.13 所示。也就是说，原本的 HTTP 协议报文经过了 SSL 子层的加密，网络上的其他主机就看不到传输的内容，也就保证了传输的安全性。

如果服务器的证书没有经过验证，或是根本就是个伪造的证书，浏览器一般都会给出如图 4.14 的提示，提醒用户此网站的安全证书

有问题，希望用户不要继续访问该网站。如果对网站的内容不确定，则请务必点击“关闭网页”离开该站点。

图 4.14　网站的安全证书有问题时，浏览器发出的提示

很多“钓鱼网站”的界面可能和正规网站极为相似，但缺少相应的证书。例如，假设 sample.net 是正规网站，拥有合法的 SSL 证书，而 samp1e.net（注意是数字 1 而不是字母 l）是钓鱼网站，它就没有也不可能有合法的证书。这个时候图 4.14 所示的提示就会出现了。此时应仔细检查网站的域名，确认是否是自己将要访问的网站，避免被“钓鱼”。

项　目　实　践

1　在计算机上启动“本地安全策略”工具（一般位于“控制面板”中的“管理工具”下），找到“ IP安全审核策略”，学习如何配置 IPSec协议。使用 IPSec协议和组内其他计算机通信，并使用流量抓取软件查看抓取的通信流量，说一说它们和未加密通信的区别。

2　访问一个 HTTPS网站，在浏览器的地址栏左侧（或右侧）找到安全证书，查看它的详细信息。并填写在表 4.1中。

表 4.1　安全证书的信息

表项	内　容
证书的目的	
颁发给	
颁发者	
有效期	
签名算法	

三、防火墙

加密算法或网络安全协议能够有效防止网络上的两台主机之间

传输的数据被第三方“窃听”，但它不能阻止主动攻击。例如，一台被植入“木马”的主机相当于给攻击者留下一个后门，即使在通信时采用了加密手段，也无法阻止恶意主机通过该后门入侵受害主机。那么，我们又可以采取哪些手段防止这样的入侵呢？

早在古代，人们就发现石砖砌成的墙壁能够有效阻止火势在木质建筑物之间的蔓延，“防火墙”一词就此诞生。在计算机网络中，人们借用“防火墙”这一名词来描述一种网络设备：它是一种特殊的网络设备，通过严格检查和控制进出网络边界的分组，禁止任何不符合既定规则的通信，从而减少潜在入侵的发生，尽可能降低这类安全威胁带来的安全风险。

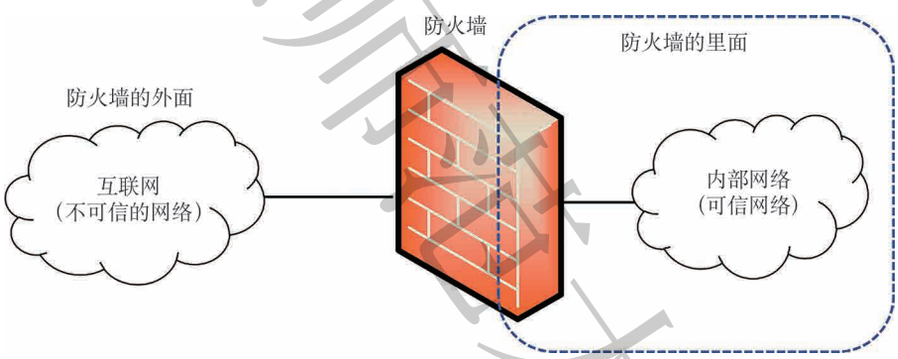


图 4.15　防火墙在网络中的位置

防火墙通常位于互联网和内部网络之间，一般都把防火墙内部的网络称为“可信网络”，而防火墙外的网络称为“不可信网络”，如图 4.15 所示。

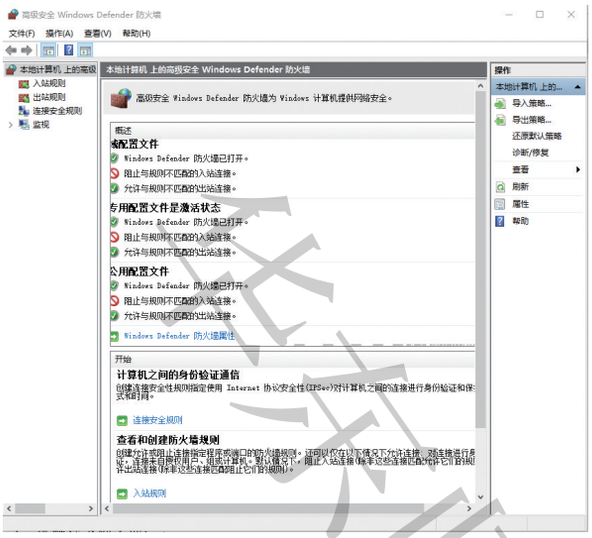
防火墙主要有两种类型：

一种是分组过滤路由器。它是一种具有分组过滤功能的路由器，它根据预先设置的过滤规则对进出内部网络的分组执行转发或丢弃的动作。过滤规则一般基于分组的网络层或传输层首部的信息，例如：源/目的 IP 地址、源/目的端口、协议类型（如 TCP、UDP）等等。

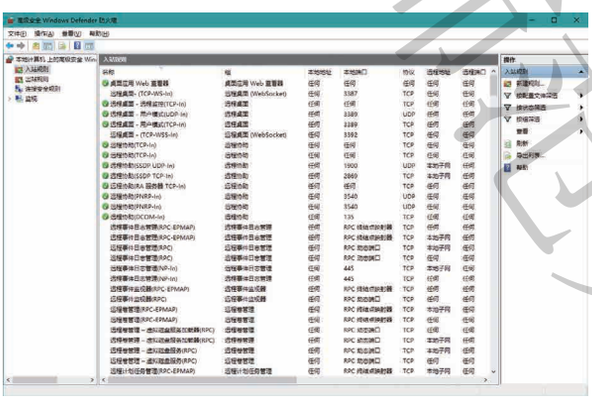
假设某公司拥有一台服务器，运行 Web 网站服务程序和数据库应用程序。其中 Web 服务程序位于 TCP 80 端口上，数据库应用程序运行在 TCP 3306 端口上。为了防止互联网上的用户直接访问数据库，但又不影响访问 Web 服务，那么就可以将防火墙设置为如表 4.2 所示的规则。

表 4.2　防火墙设置示例

源地址	目的地址	源端口	目的端口	协议	动作
任意	（网站服务器的 IP 地址）	任意	80	TCP	允许
任意	（网站服务器的 IP 地址）	任意	3306	TCP	阻止



（a）Windows 防火墙首页



（b）“入站规则”配置界面

图 4.16　Windows系统中内置的用户防火墙

另一种是应用网关。它在应用层中扮演报文检查和转发的角色。一种网络应用就需要一个应用网关。所有进出网络的应用程序报文都必须通过应用网关，应用网关检查该报文是否符合要求（如特定的用户 ID、特定的内容等），如果报文符合要求则放行，不符合要求则丢弃报文。

应用网关也有一些缺点。由于每种应用都需要一个不同的应用网关，应用程序的处理负担较重，且需要在应用程序开发的时候配置应用网关地址。

随着用户对网络安全的需求越来越大，操作系统的设计者也开始在操作系统内部预装了用户级防火墙。用户级防火墙结合了分组过滤防火墙和应用网关的特点，可以根据分组特征和应用报文内容实施动态的分组过滤。但这个防火墙只对本地计算机有效，而不是针对整个网络进行防护。例如 Windows 系统中就内置了用户级防火墙，如图 4.16（a）和图 4.16（b）所示。可以在该防火墙中设置“入站规则”和“出站规则”，对进出该主机的网络流量进行控制。

项　目　实　践

启动 Windows中的防火墙，研究其中的各项功能，设置该防火墙使“窃听者”无法访问受保护的主机。

第五章

网络故障排查与修复

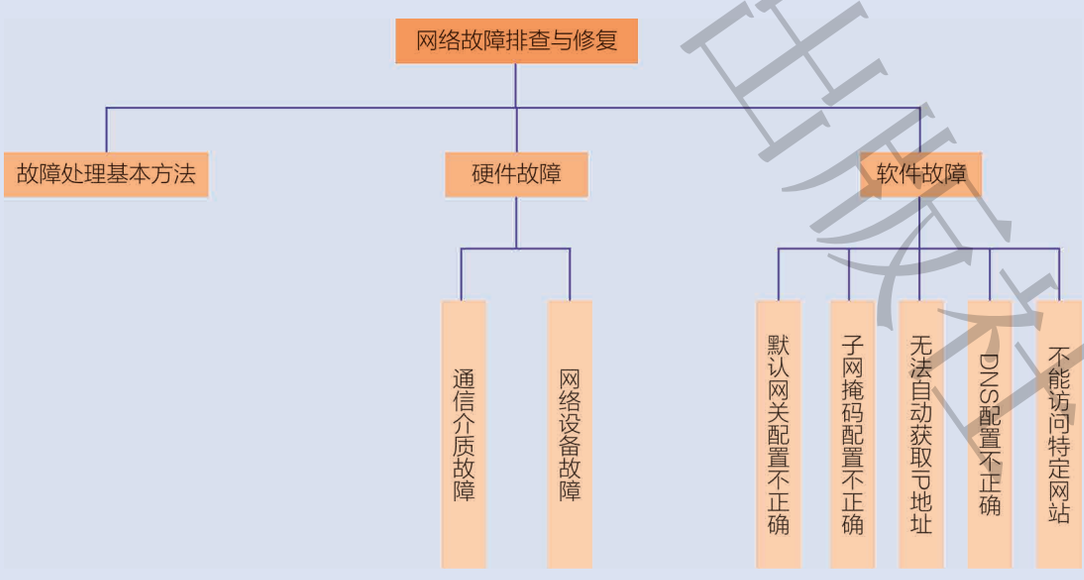
本章学习目标

- 列举故障处理的基本方法、常见策略与常见故障的原因。
- 列举常见的计算机网络硬件故障，尝试定位故障点，修复常见的硬件故障。
- 列举常见的网络软件或协议配置问题，尝试定位故障点并能修复这类常见故障。

人们的生活已越来越离不开网络，一旦网络出现故障，将会对我们的学习、工作与生活产生很大的影响。这些故障可能来自硬件，也可能来自软件或协议配置不当的问题。作为高中阶段学生，同学们应能够掌握故障处理的基本方法和常见策略，认真分析故障原因，查找故障点，并最终采取措施解决故障。

本章从故障排查的基本方法开始，逐步介绍常见的硬件、软件或协议故障及其排除方法，帮助同学们初步建立一个“修复工具箱”。今后遇到其他网络问题时，可以本章学习内容为起点，结合互联网上众多的故障修复相关资料，解决这些网络问题，为我们的网上漫游“保驾护航”。

本章知识结构



项目主题

网络故障排查与修复

项·目·情·境

科考队员们已经在新的星球上建立了庞大的互联网。各个科考团队之间通过互联网展开了良好的合作，极大地提高了工作效率。然而有一天，某科考团队向你的网络工程师团队发来报告，说他们的计算机无法连接到互联网，他们需要发送的考察数据无法传输到另一个科考团队的计算机，也无法通过任何远程计算机下载。如果不能尽快修复，将影响到其他科考团队对该数据的利用，也无法继续完成其他的科考任务。

你经过现场分析判断，排除了网络攻击的因素。于是你将目光放在了网络设备本身的问题上。这个科考团队的局部网络拓扑如图 5.1所示。请你尽快帮助他们恢复通信。

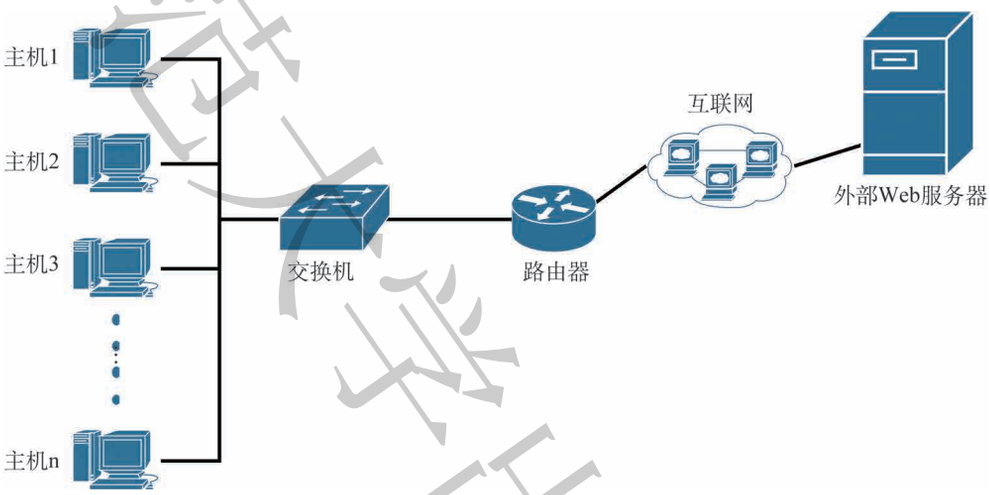


图 5.1 某科考团队局部网络拓扑

项·目·任·务

任务 1

根据故障现象，制订一个初步的排错计划。

任务 2

检查网络实验室中各主机的硬件和连接情况，找出可能存在问题的地方并修复。

任务 3

检查网络实验室中各主机的网络协议与配置，找出可能存在问题的地方并修复。

第一节　故障处理基本方法

体　验　思　考

“不能上网了”是每一个普通网民在使用网络时都很容易出现的问题。而这五个字背后可能有着千奇百怪的故障原因。

思考：如果你的同学或家人对你说“不能上网了”，你会采用什么样的方法来查找并排除网络故障？

在介绍具体的故障现象及解决手段之前，我们先了解一下常用的故障诊断和排除策略。

一、分层故障排除法

TCP/IP 协议分层结构的概念指出，只有当下层工作正常时，它的上层才能正常工作。例如，在局域网中，由于物理层的设备不稳定，导致网络连接一直反复断开，但从表象上看，会表现为到达远端的路由反复中断，如果仅看表象，就会以为是路由协议出了问题，从而忽视了真正的错误原因。如果采用分层故障排除法，自底向上地分析、查找，就能快速定位故障点并顺利解决故障。

二、分块故障排除法

分块故障排除法类似于分层故障排除法，也是将一个大的系统分为若干部分，分步解决问题。所不同的是，分层故障排除法用于还不清楚网络故障出现在哪一层的时候，而分块故障排除法用于已经确定了故障所在的层次，但不清楚故障点的具体位置时。例如，如果已经确定是网络层的故障，那么就可以将网络层分为若干块，如路由管理、端口、协议、策略、接入等，同样采取逐步分析、接近的方法来解决故障。

三、分段故障排除法

前面所说的分层法和分块法可认为是纵向的，在横向上还可以采用分段排除法。例如从自己家里到网络服务商可以分成几段，主机本身的故障、主机到路由器的链路故障、路由器本身的故障、路由器到大楼网络出口的链路故障、网关本身的故障、网关到最近网络服务商节点的链路故障，等等。

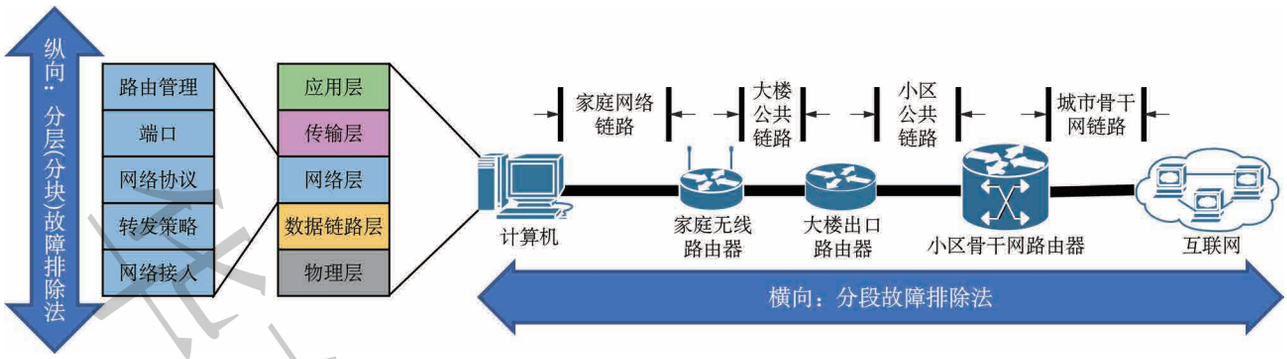


图 5.2　分层、分块和分段故障排除法示意图

四、替换法

替换法是排查网络硬件故障时最常用、最实用的方法。例如，当怀疑是网线问题导致网络故障时，只要更换一根确定是正常的网线再试一次即可；当怀疑是交换机或路由器故障时，只要更换一个工作正常的交换机或路由器尝试一下。操作既方便，效果又显著。

当然，上述四种方法不是孤立的，而是要在排查错误的过程中综合运用，使复杂的问题简单化，从而提高故障处理的效率。

分　析　评　价

请根据图 5.1的项目情境，制订出排查故障的计划，即从什么地方入手，预期的现象是什么，拟采用哪些解决问题的手段。

图 5.1中，网络工程师经过仔细排查，找出了故障主机和具体的故障现象，请将可能存在的故障点及你的初步排错计划填入表 5.1中。

表 5.1　故障现象及其初步解决方案

故障现象	可能的故障点	初步的排错计划
主机 1可以连接局域网内其他主机，但无法连接互联网		
主机 2可以连接互联网，但无法连接局域网内的其他主机		
主机 3无法连接到网络，且网卡指示灯不亮		
主机 4无法访问 Web网页，但可以使用即时通信工具		
局域网内无线路由器处于开启状态，但所有主机都无法连接无线网络		

第二节　计算机网络的硬件故障

我们已经学习过各种类型的网络线缆、网卡、交换机、路由器和无线网络设备。它们是构成网络的基石，是网络正常运行必不可少的。如果它们出了故障，那么我们就不能正常使用网络完成工作。当确定硬件出故障时，应按照“由近及远、先易后难”的顺序，逐步定位故障点，查明故障出现的原因，并最终修复硬件的故障。

体　验　思　考

我们已经学习过，网络硬件包括线缆、网卡（包括有线网卡和无线网卡）、交换机、路由器（包括无线路由器）。这些网络硬件设备在使用的过程中可能会由于设备老化、配置不当等原因发生故障，从而导致网络通信异常或中断。

思考：你在生活中遇到过哪些计算机网络硬件故障？如何确定故障确实是由于硬件故障引起的？

一、通信介质故障

通信介质主要是指双绞线、光纤或其他线路系统构成。如果把数据包比喻为装满了货物的卡车，那么通信介质就是道路。毫无疑问，道路如果出现损坏或阻塞，势必会影响货物的运输速度，同理，通信介质如果出现问题，一定会影响通信质量。

图 5.3　网线检测仪

1. 双绞线的故障和解决方法

首先应检查线缆状态，确认线缆已确实与计算机连接。一般情况下，如果线缆没有与计算机连接（或无线网络没有连接），操作系统会有相应提示。如果确定线缆已经插好却仍无法连通网络，则考虑是否是网线本身的问题（如断路、接口损坏），此时应采用替换法，替换一根网线再做尝试。同时，可以使用网线检测仪对网线进行检测。将网线两端分别插入网线检测仪的主机和副机中，并打开开关。若主机和副机分别闪烁“1”“2”“3”“6”四个指示灯，说明网线正常，否则说明这根网线有故障。

2. 光纤的故障和解决方法

光纤是借助光信号传输网络数据的介质，当光纤出现问题时，光信号就无法正常被发送到其他设备从而导致网络连接出现中断。一种检验光纤是否有问题的方法是用激光笔或明亮的手电筒对准光纤的一头照射，如果另一头有光线射出，表明光纤本身传导光的能力正常，否则说明光纤损坏。如果光纤完好但线路无法传输网络数据，那也有可能是光纤接口的损坏，需要替换新的光纤接口。

3. 无线网络的故障和解决方法

无线网络经常出现的一种故障是上网设备无法接收到无线路由器发出的信号。要解决这种故障，一是可以改变无线路由器的位置，二是可以增加一些无线 AP 作为中继器，这样既可以保证无线网络信号保持在一定强度，又可以保证在该房间内的若干台主机都处于同一个局域网中。

二、网络设备故障

1. 网卡故障

网卡作为计算机与网络的接口，其重要性不言而喻。如果网卡损坏，则计算机将彻底失去与网络的连接。一般检测网卡是否损坏，可以通过操作系统中的提示，以及命令行工具中的 ping 命令来检测。具体方法是：在命令行提示符中输入“ping 127.0.0.1”（不含引号，下同）。127.0.0.1 是一个特殊的 IP 地址，被称为“回环地址”。ping 命令是用于测试网络连通性的命令，使用该命令可测试计算机网卡和网络协议是否安装正确。图 5.4 所示是正常情况下“ping 127.0.0.1”的运行结果，如果出现“连接超时”或者数据包丢失的情况，说明网卡损坏或 TCP/IP 协议安装不正确，需要进一步排查。如果网卡损坏，则需要更换网卡。如果是协议安装不正确，则需要重新安装网卡的驱动程序。

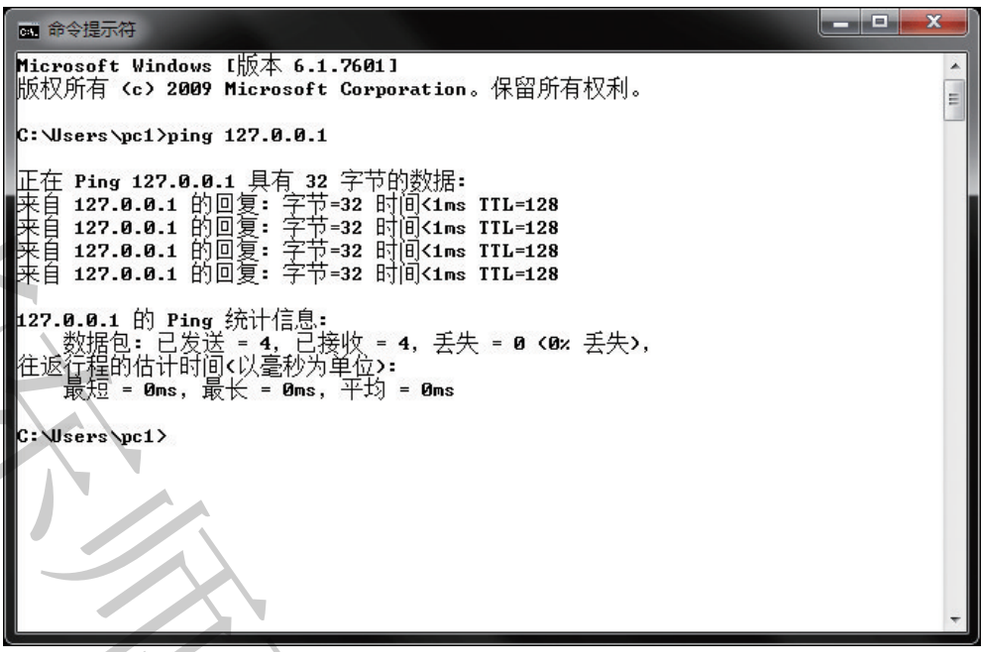


图 5.4 正常情况下“ping 127.0.0.1”的输出信息

2. 交换机或路由器的故障

交换机和路由器是网络传输路径上的重要设备，如果它们损坏，会导致计算机与局域网、局域网与广域网的连接中断。

一般检测交换机或路由器故障的过程是：检查交换机或路由器上的指示灯，如果发现已经接入线缆的指示灯不闪烁或不亮，且已经排除了线缆本身的故障，那么可能是交换机或路由器的这个接口损坏，可以尝试将线缆接入另一个接口。如果交换机或路由器上的指示灯没有异常，但仍无法上网，则需要考虑是不是交换机或路由器本身的损坏，可以尝试更换交换机或路由器。

3. 无线网络设备的故障

大多数情况下无线网络设备（通常是无线路由器）的故障和有线网络很相似。因此这里只列举一些无线网络设备特有的故障。

（1）搜索不到 SSID

SSID（service set identification，服务集标识）是无线网络的标识。在连接无线网络时，我们需要知道要连接的网络的 SSID。如果安装好了无线路由器，但计算机搜索不到无线路由器的 SSID，这可能是由于无线路由器中没有开启 SSID 广播。登录进无线路由器的设置界面，找到“开启 SSID 广播”选项，如果这个选项是关闭的，则将其打开，

一般都能够在终端设备上找到无线路由器对应的 SSID。当然，有时为了提高无线网络的安全性，也可以主动关闭 SSID 广播。

（2） 无线网络信号很差

如果终端设备距离无线网络设备很近，但无线网络信号依然很差。则可能是无线网络设备的天线损坏或周围有强烈干扰。此时应检查无线网络设备周围是否存在大功率、高辐射电器（如微波炉、电磁炉等），如果有，请让这些电器远离路由器。另外，无线设备的天线损坏也会导致这些情况，如果是这样，可尝试更换天线或更换整个无线设备。

（3） 无线网络被人“蹭网”

由于无线网络的便捷性，不少人会通过“蹭网”的方式未经授权接入无线网络，轻则影响正常用户无线网络连接的速率，重则影响正常用户的数据安全。通常这种现象是因为没有设置无线设备的密码，或密码由于过于简单而被破解引起的，因此需要给无线网络设置密码。登录进入无线网络设置界面，修改无线网络密码，注意请选用大小写字母、数字、特殊符号混合的复杂密码，以降低无线网络密码被破解的风险。另外，还有一些控制访问的手段，如通过设置 MAC 访问控制列表来允许某些指定的设备访问无线网络，或是通过设置禁用 DHCP 来防止未经授权用户获取 IP 地址。

项 目 实 践

请检查网络实验室中各主机的硬件和连接情况，找出故障点并修复故障，将过程记录在表 5.2中。

表 5.2 硬件故障及其修复方法

主机名	故障点	修复方法
主机 1		
主机 2		
主机 3		
主机 4		

第三节　计算机网络的软件或协议故障

计算机软件和安装的网络协议配置不当也可能导致无法连接到网络。因此要学会使用网络命令来检查并发现网络故障的原因。我们之前已经学习了 ping 命令的使用，本节还将学习更多的网络命令。

体　验　思　考

网络协议是各种网络硬件能够正常工作，能够协同处理数据报文的有力保障。但在网络协议配置或网络软件安装过程中，由于使用者缺乏相关知识或经验，可能导致各种协议配置问题。

思考：你在生活中遇到过哪些由于软件或协议配置问题而引发的故障？这些配置分别属于网络协议层次体系结构中的哪些层？

一、默认网关配置不正确

有时我们会发现无法连接至互联网，却可以连通局域网内的其他主机。此时就要怀疑是否是默认网关的问题。默认网关是一个局域网内的 IP 地址，它一般是计算机连接到互联网的出口，如果它出现问题，那么计算机就无法接入互联网。此时应检查默认网关的设置。

假设如下场景：计算机采用有线方式连接到网络，其 IP 地址是 192.168.1.2，出现可以连通局域网其他主机却不能连接到互联网的情况。如图 5.5 所示。

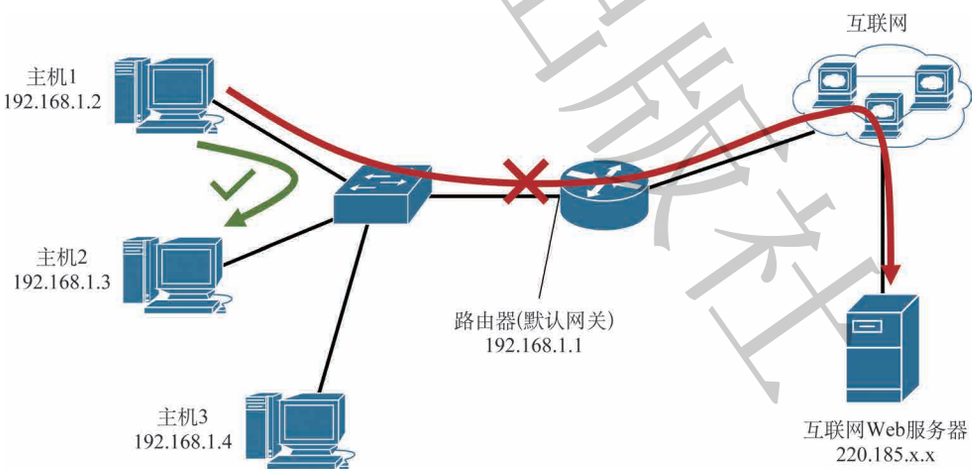


图 5.5　可连通局域网其他主机但无法访问互联网

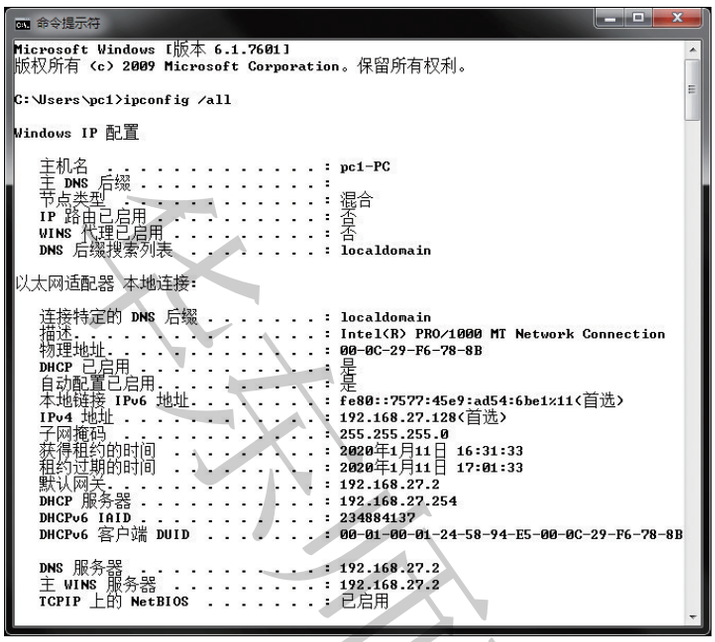


图 5.6　ipconfig命令的输出结果示例

首先要检查一下网卡配置。在命令行提示符中输入 ipconfig 命令，这是一个检查网卡配置状态的命令，它返回目前计算机中所有的网卡以及它们的 IP 地址等信息。并且，它还可以带有/all 选项来返回更加详细的信息。如图 5.6 所示。

为了简化问题，图中略去了一些无关信息。图 5.6 中，ipconfig 命令返回的信息显示该计算机的默认网关是 192.168.27.2。为了检查是否是默认网关的问题，可以采用 ping 命令测试计算机与默认网关的连通性。如果 ping 命令显示“无法访问目标主机”，说明默认网关配置错误，需要进入“网络适配器属性”中对默认网关进行修改。如果 ping 命令显示“连接超时”，则说明可能是计算机到默认网关的链路出现了问题，需要进一步排查这条链路或网关设备（一般为路由器）本身。

二、子网掩码配置不正确

子网掩码的作用是进一步划分子网。当某台主机的子网掩码不正确时，可能无法和局域网内其他主机通信。

如图 5.7 所示，该网络中有三台主机，主机 2 无法和主机 1、主机 3 通信，但可以访问远程服务器。经检查，三台主机的子网掩码如表 5.3 所示。由于主机 2 的子网掩码设置不正确，虽然从 IP 地址来看三台

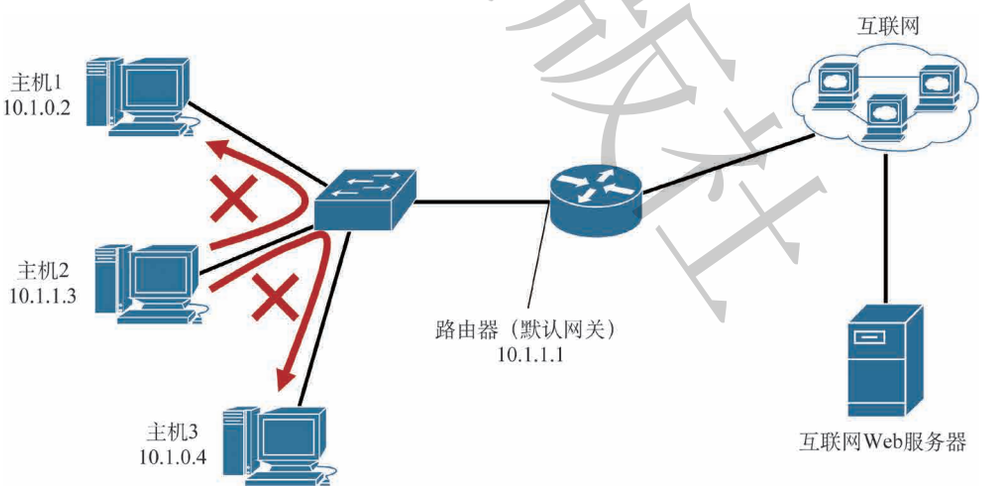


图 5.7　子网掩码设置不正确会导致主机无法访问局域网内其他主机

主机似乎是处于同一个网段，但实际上并不处于同一子网。因此它们是无法通信的。而主机 2 和路由器虽然子网掩码不同，但它们属于同一网段。因此主机 2 可以与路由器通信，当然也可以访问远程服务器了。

表 5.3　该拓扑中各主机（网络接口）的 IP 地址和子网掩码

主机名	IP 地址	子网掩码
主机 1	10.1.0.2	255.255.0.0
主机 2	10.1.1.3	255.255.255.0
主机 3	10.1.0.4	255.255.0.0
路由器（默认网关）	10.1.1.1	255.255.0.0

针对这类问题，我们也可以进入“网络适配器属性”中对计算机的子网掩码进行修改。本例中，将主机 2 的子网掩码改为 255. 255. 0. 0 后，主机 2 就可以访问局域网中的其他主机了。

三、无法自动获取 IP 地址

计算机无法访问网络，查看操作系统提示，出现“网络受限制或无连接”。此时应使用 ipconfig 命令检查本机 IP 地址。如果发现本机 IP 地址为 169. 254. ×. ×，那么可以判断是由于计算机无法从 DHCP 服务器处获取正确的 IP 地址，169. 254. ×. × 是一个保留地址段，如果计算机试图采用 DHCP 协议获得自动分配的 IP 地址，但没有成功的话，就会被分配到这样的 IP 地址（这称为“故障转移机制”）。

产生这种现象的可能原因如下：（1）计算机和 DHCP 服务器的连接中断了，此时应判断计算机和 DHCP 服务器的连接状态。（2）IP 地址租约到期但没有及时续租，此时可以通过依次运行“ipconfig /release”和“ipconfig /renew”这两个命令重新获取 IP 地址。（3）网络中主机太多，DHCP 服务器中的地址池已经耗尽。这种情况很容易出现在访问公共 Wi-Fi 的时候。在这种情况下，只能等待网络中的其他主机离开该网络。如果 DHCP 服务器是由网络运营商管理的，那么需要通过联系运营商解决。

四、DNS 配置不正确

有时我们会发现计算机不能访问 Web 网站，但可以使用一些例

图 5.8 使用 nslookup命令查询域名对应的 IP地址

如即时通信软件，网络文件共享系统等非 Web 应用。此时应将目光聚焦到 DNS 服务器上，DNS 负责域名和其对应的 IP 地址的转换，如果这一部分出了问题，那么计算机就无法通过域名方式访问 Web 网站。

要检查 DNS 解析的状况，可以通过命令行中的 nslookup 工具。图 5.8 显示的是使用该命令获取上海市政府网站域名(www.shanghai.gov.cn)对应 IP 地址的情况。如果使用该命令检测一个常见网站时，出现“DNS request time out”字样，则说明计算机和 DNS 服务器之间的连接不正常。解决方法是在“网络适配器属性”中将 DNS 服务器改为“自动获取”或采用一个有效的 DNS 地址，如果仍有问题，则问题可能出现在网络运营商处，需要联系运营商解决。

五、不能访问特定网站

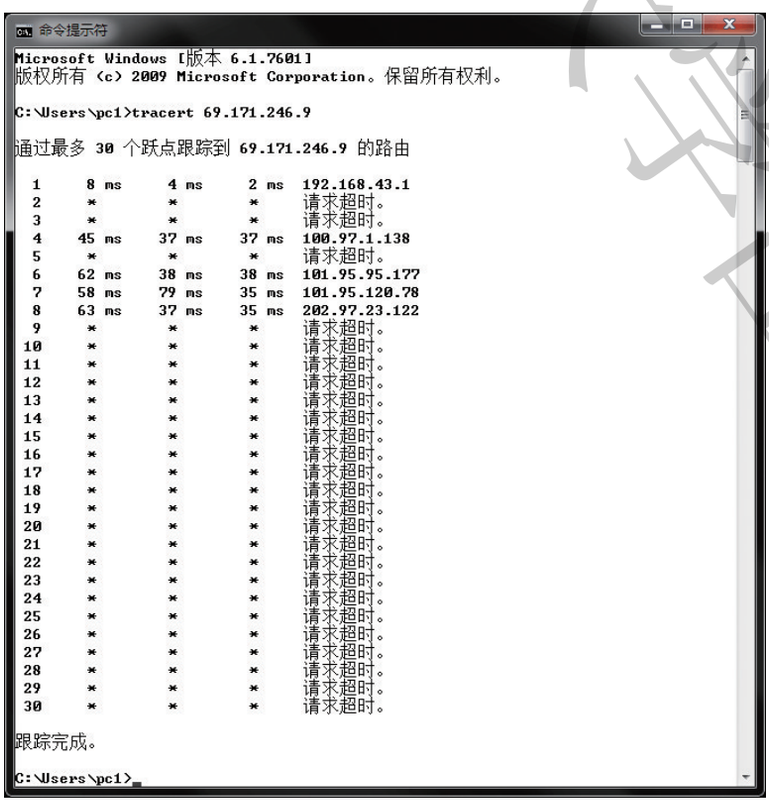


图 5.9 tracert命令输出结果示例

如果是不能访问特定网站，可能有两种故障原因：(1) 网站本身出现问题，这种情况下只能等待网站管理员将问题修复后再访问。(2) 路由问题。此时可以使用命令 tracert（有的操作系统中是 traceroute 命令），在默认情况下，该命令经过最多 30 个路由器来检测到达目标的路径是否出现问题。一个可能的命令输出结果如图 5.9 所示。如果在检测过程中出现三个连续的“*”号，说明通过这个路由器无法到达目标站点，可能是传输路径出现了问题。

这种情况下，可采用前文所述的“分段故障排查方法”，由近及远地分段找出是哪段路径的问题。如

果问题在近端，那么可以使用替换法，替换掉出故障的线路或设备。如果问题在远端，那么只能联系网络运营商解决。

项 目 实 践

请检查网络实验室中的各主机，找出它们软件或协议配置不当之处并修复问题。填入表 5.4中。

表 5.4 软件或协议故障及修复方法

主机名	故障点	修复方法
主机 1		
主机 2		
主机 3		
主机 4		

第六章

物联网世界

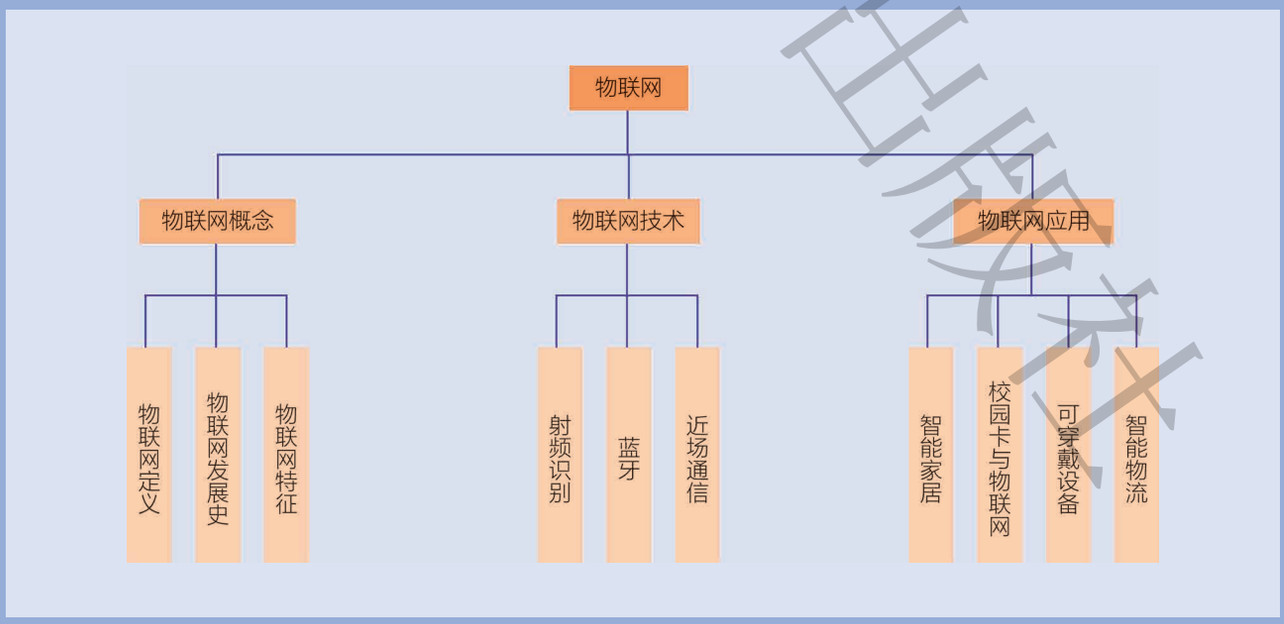
本章学习目标

- 描述物联网发展的历程，描述物联网的定义和特征。
- 描述物联网常用技术的基本原理和应用场景。
- 描述常见物联网应用的原理，举例说明创新网络服务对人们生活、学习、工作的影响。

随着人们对网络应用需求的不断扩大、网络硬件设备的不断发展，人们开始希望网络进一步扩展，能够让全世界的物体都连接成网络。在这样的需求下，物联网应运而生，标志着人类开始向“智能时代”迈出坚实的步伐。在物联网中，物体可以通过传感器感知内外环境，可以通过各种无线通信方式共享数据，也可以通过软件对工作状态进行智能判断并对数据进行智能化处理。计算机网络是物联网的基础，物联网是计算机网络的重要应用。物联网的应用将进一步提高社会的生产力水平，推动人们生产方式和生活方式的重大变革。

本章将分别介绍物联网的发展历史、定义与特征、核心技术和创新应用，向同学们展示一个丰富多彩的物联网世界。

本章知识结构



项目主题

探究物联网系统及其应用

项·目·情·境

随着人类在新的星球上的不断探索和建设，这个星球展现出了如同地球一般的勃勃生机。人们已经可以利用计算机网络便捷地开展交流。

为了更好地生产和生活，在这个星球上出现了很多需要大规模、自动化监控的场景。例如农业、交通、医疗、消防等，然而，监测设备部署量大，分布广，造成了维护成本高，管理难度大的情况。你作为网络工程师，需要提出一种新形态的网络，能够“物物相连”，实现自动化的信息采集、上传和连续监测。人们也可以远程操控这些物品，并实现可视化管理。

项·目·任·务

任务 1

探究物品连接到网络或物品相互连接的各种场景。探究为了连接到网络，物品需要增加哪些部件。

任务 2

探究自动驾驶系统运作的方式，探究其中存在的技术原理和安全问题，并提出相应的解决方法。

第一节　物联网概述

你能想象吗？有一天人们身边的万事万物都可以通过网络连接在一起，通过网络共享数据，帮助人们更好地学习、工作与生活。这是和不断发展的物联网技术分不开的。那么，到底什么是物联网，它的发展历程是怎样的，我们身边又有哪些事物与物联网有关呢？

物联网（Internet of things，简称 IoT）是指这样一种网络：它通过各种信息传感设备，按照约定的协议，把物体与互联网连接起来，进行通信和信息交换，以实现智能化识别、定位、跟踪、监控和管理等功能。

通俗地说，安装在物体上的传感器、电子标签和全球定位系统等设备将赋予物体“感知”的能力，计算机网络将赋予物体“对话”的能力，既可以实现人与物之间的沟通，也可以实现物与物之间的对话。

“物联网”和“互联网”虽只有一字之差，但其本质有很大不同。互联网是以人为核心，而物联网是以物为核心，大到房子、汽车，小到台灯、茶杯，都可以是物联网中的一个实体。物联网的规模要远大于互联网，复杂程度也比互联网高许多。互联网是物联网的基础，物联网是互联网的延伸，两者又同时具有紧密的联系。

体　验　思　考

传统温度计主要利用的原理是：液体的热胀冷缩改变液柱表面在玻璃管中的位置从而指示温度。由于传统温度计中的材料（主要是水银或煤油）存在一定危险性，20世纪末人们发明了电子温度计，采用温度传感器与电子显示屏来指示温度。但这些温度数据仍需要人去观测记录。在地球上有一些特殊的地区，如寒冷的极地和炎热的沙漠，人类无法长时间停留在其中观测与记录温度。为此，人们通过物联网的方式使温度传感器获得的温度数据通过网络传输到科研基地，这样，人们就能够在不深入这些危险地区的前提下获得当地准确的温度数据。

思考：从传统温度计，到电子温度计，再到如今的物联网温度计，这其中蕴含了怎样的技术进步？你还能举出更多的例子吗？

一、物联网发展历史

1991 年，剑桥大学的几名科学家在一个咖啡壶旁安装了一台摄像机，用图像捕捉技术将咖啡壶的实况图像传输到计算机上，以便这些科学家们可以知道咖啡壶的状态。这一次实验的模式上已经具有

传感、传输、共享等特点，已经十分接近后来的物联网。

1999 年，美国的麻省理工大学自动识别中心首次提出了“物联网”概念。而同一时期，中国也提出“传感网”的概念，虽然名称不同，但实质是一样的，都是将物体传感设备与互联网连接起来，实现智能化识别与管理。与其他国家相比，我国的技术研发水平已处于世界前列，具有同发优势和重大影响力。

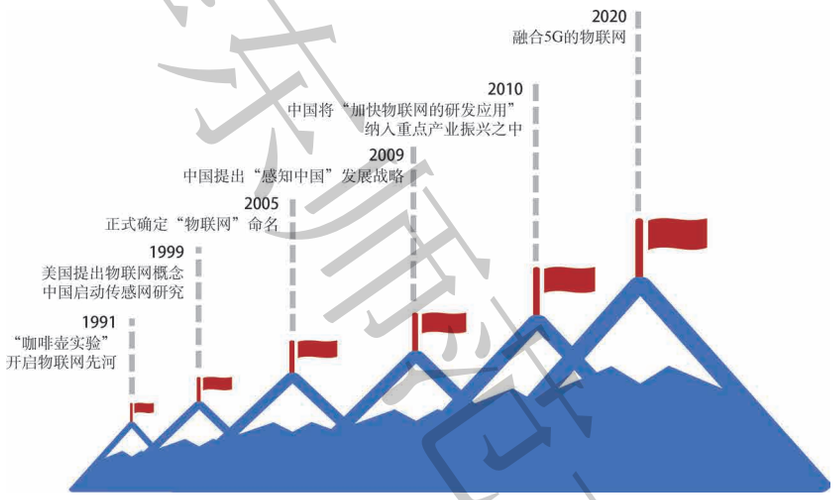


图 6.1　物联网发展史

2005 年，在突尼斯举办的信息社会世界峰会上，国际电信联盟发布了《ITU 互联网报告 2005：物联网》，正式确定了“物联网”这一命名，介绍了物联网的特征、相关的技术、面临的挑战和未来的市场机遇。

2009 年，我国提出了“感知中国”发展战略。这标志着中国正式搭上了“物联网”的快车。2010 年，我国将“加快物联网的研发应用”明确纳入重点产业振兴规划之中。各有关部门都在研究制定促进物联网产业发展的扶持政策，推动了我国物联网建设从概念推广、政策制定、配套建设到技术研发的快速发展。2011 年，我国又发布了《物联网十二五发展规划》，将物联网纳入“十二五”国家战略性新兴产业发展规划。2020 年，随着 5G 技术正式开始商用，物联网的性能得到了进一步巨大提升，与 5G 技术相结合的物联网应用也得到了进一步推广和发展。

二、物联网特征

物联网的基本特征包含全面感知、可靠传输和智能处理三点。

（1）全面感知

物联网的全面感知指的是通过各种技术手段，能做到随时随地对物体进行信息的采集和获取。

（2）可靠传输

物联网的可靠传输指的是通过各种通信网络与互联网有机结合，将物体感知的信息送入网络，使人与物、物与物之间随时随地进行可靠的信息交互和共享。

（3）智能处理

物联网的智能处理指的是通过云计算、数据挖掘、模式识别等新的智能计算技术，对海量数据进行分析和处理。

分 析 评 价

在网络工程师的努力下，科考队员们建立起了各种使用物联网的生产生活设施，请讨论其中分别包含了哪些物联网应用，并填入表 6.1中。

场景一：智能农场大大提升了工作效率。农场职工已经不用整天下地干活。农场的智能化设备会做好大棚内温湿度的控制，并自动给农作物供给养料和水分，农场职工只会在有必要的时候才到大棚内检查设施状况。到了收获时节，农场职工只要在控制室里轻点鼠标，就能控制机器人采摘农作物并通过无人机运输到仓库或加工厂中。

场景二：乘客能预知等公交车的时间了。许多公交车已经装备了 GPS，这样就能够实时地判断公交车目前所处的位置，并根据交通状况预估到达下一站的时间，再通过网络及时地更新车站电子显示屏上的班次和到达信息，提高了乘客的知晓度和乘车体验。

场景三：图书馆中的书会“说话”了。读者在图书馆内的智能终端上输入书名或书号，书本中植入的智能芯片就会自动向读者的手机上（当然，要事先绑定好）发送此书目前所在的位置。这一发明大大提高了读者查找图书的效率。

场景四：智能家居给人们的生活带来了更多便利。现在只要拥有一台智能手机，就可以控制家里的灯光、空调、电饭煲、洗衣机等家居产品。而这些家居产品也会把自身的工作状态通过网络传输给主人的手机，主人即使出门在外也能随时知道家里的电器正在做什么。

表 6.1 生活场景对应的物联网应用

场景	物联网应用
场景一	1 _____ 2 _____ 3 _____
场景二	1 _____ 2 _____
场景三	1 _____ 2 _____
场景四	1 _____ 2 _____

第二节　常用的物联网传输技术

本节将学习射频识别(radio frequency identification，简称RFID)、蓝牙(Bluetooth)和近场通信(near field communication，简称NFC)的原理，这些都是物联网中常用的传输技术。

体　验　思　考

图 6.2所示是一种常见的温度传感器。它的主要组成部分是利用特殊材料制成的热敏电阻。当温度发生变化时，传感器的电阻会发生改变，通过这种材料的电阻与温度的关系式就能计算出某个电阻值对应的温度值。但是，仅仅采用温度传感器只能获取到温度数据，要将这些数据传输出去，还需要其他设备帮忙。

思考：如果让你设计一个物联网温度计，你会在温度传感器的基础上加上哪些设备？这些设备分别起到哪些作用？

进一步思考：这些设备哪些是必需的，哪些还可以精简？

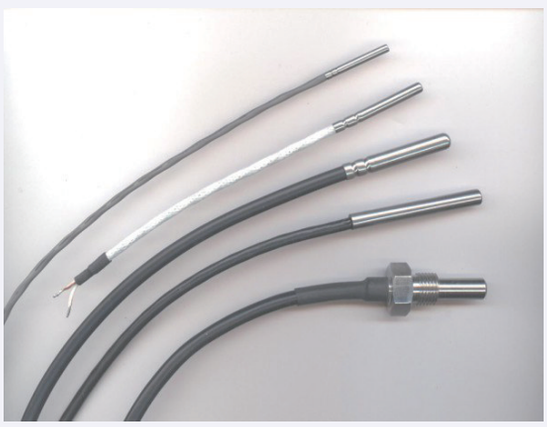


图 6.2　温度传感器

一、射频识别

20 世纪初发明的条形码在当时掀起了一场技术革命。然而到了今天，条形码已经无法满足人们对于大量信息存储的需求。20 世纪末人们发明了二维码，在一定程度上改进了条形码的缺点，但仍具有存储能力小、适应性不强、容错能力低以及不能写入等问题。射频识别技术的发明带来了一场更大更广泛的技术革命。特别是 RFID 技术与互联网的融合，一定程度上满足了人们对于大量信息存储和传输的需求。

我们通过读者小王在智能图书馆的借书过程来理解 RFID 的原理。

小王在图书馆查询到了自己想要的书籍名称。当她单击“检索”按钮的时候，图书馆的智能书架通过自己的天线发出一段电磁波，该图书内部的 RFID 标签接收到这段电磁波后，将自己的定位数据发送给智能书架，智能书架又通过网络将图书所在位置传输到了小王所使用的查询终端。这一过程如图 6.3 所示。这样，小王就能精准地找到自己要借阅图书的位置。

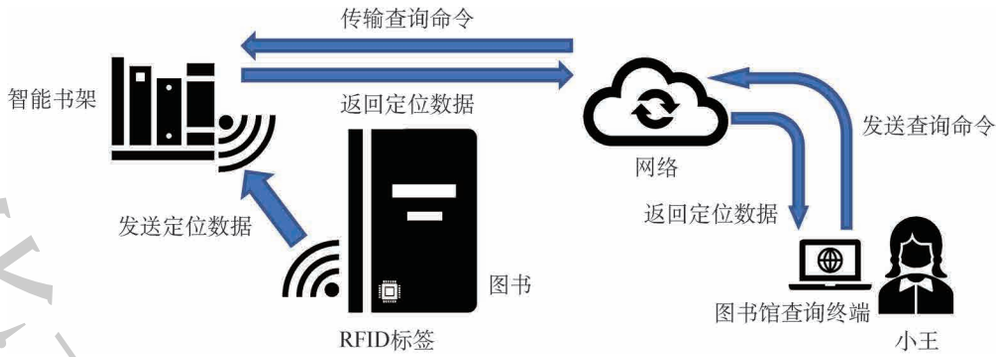


图 6.3 使用 RFID 技术的图书馆借书过程

RFID 标签有许多优点。首先，RFID 标签体积小且形状多样，在读取上不受尺寸和形状限制。RFID 对环境的适应能力很强，不容易受水、油等物质的污染，并且 RFID 还能在黑暗的环境中读取。RFID 标签不仅可以让阅读器读取数据，还可以通过阅读器写入数据，因此可以重复利用。RFID 在短距离内（数十厘米）可以进行穿透性通信，因此可以对 RFID 设备进行一定保护。最后，标签内的数据含有校验码，可以保证数据发送的正确性。

二、蓝牙

1998 年，出现了一个特别兴趣组（special interest group，SIG），打算开发一个无线标准，可以将计算设备、通信设备或其他附件通过短距离、低功耗和低成本的无线电连接起来。这个项目被命名为蓝牙。后来，这个特别兴趣组改组为蓝牙技术联盟，负责维护蓝牙的技术标准。

现在蓝牙已经被广泛应用于电子设备中。无论是在手机、笔记本电脑，还是耳机、打印机、鼠标、键盘、音乐播放器等设备中，蓝牙功能都是非常常见的。蓝牙协议使这些设备能够互相发现并连接，从而安全地传输数据。这种相互发现并相互确认连接的行为称为配对。两台蓝牙设备之间只有先进行配对才能相互传输数据。其中，发起连接的设备称为主设备，接受连接的设备称为从设备。

在日常生活中，当人们使用无线耳机时，需要与手机等设备连接后才能够收听音乐，这就是一种蓝牙连接过程。其中，手机是主设备，耳机是从设备。连接时，手机先发起呼叫，搜索周围处于可被查找状态的蓝牙设备。当搜索到耳机后，开始进行配对（有的设备在配对环节会要求输入相应的密码）。配对完成后，耳机会记录手机的信任信息，此时手机与耳机就完成了蓝牙连接。实际上，手机和耳机在这一

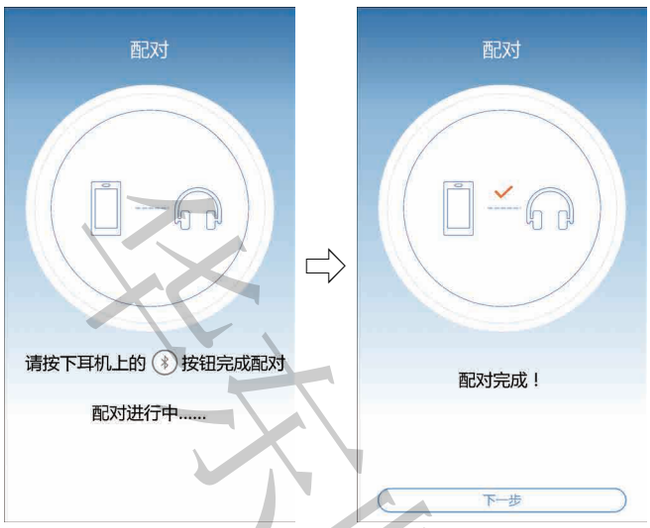


图 6.4　某型号手机与蓝牙耳机配对过程

连接过程中建立起了一个名叫微微网的临时网络，双方通过无线电波进行连接，这种网络可同时容纳二至八台设备。一旦手机和耳机配对成功，下次就可以直接连接，不再需要重新配对了。图 6.4 展示了某型号手机和蓝牙耳机的配对过程。

三、近场通信

近场通信是一种工作频率在 13.56 MHz，通信距离只有 0～20 cm 的近距离无线通信技术。具有 NFC 功能的电子设备通过相互靠近的方式就可以完成信息交换与服务访问。

我们通过一个故事来说明 NFC 的几种工作模式。

“五一”劳动节，小李坐地铁去看望奶奶。小李来到地铁闸机前，打开手机上的“虚拟交通卡”程序，将手机靠近地铁闸机上的读卡器。读卡器发出一段电磁波，激活了小李手机上的 NFC 模块。此时，手机上的 NFC 模块“变”成了一张交通卡，它将模拟的交通卡数据发送给读卡器，读卡器迅速完成扣费操作，小李得以成功进站。

到了奶奶家，奶奶让小李到地铁站帮她为交通卡充值，小李说：“不用这么麻烦，手机就可以充值啦！”小李将手机贴近交通卡，此时手机上的 NFC 模块“变”成了读卡器，它读取了交通卡的 ID 信息并显示“余额 0.80 元”。小李在应用程序上执行充值操作，往卡里充入 100 元。

图 6.5　NFC 应用领域举例

小李带给奶奶一个礼物——电子相框。和奶奶合影后，小李将自己的手机靠近了具有 NFC 功能的电子相框，通过 NFC 的点对点传输功能将手机中存储的照片传输到了电子相框中。电子相框显示出了小李与奶奶的合影。

这就是 NFC 的三种主要工作模式：卡模拟模式、读卡器模式和点对点传输模式。

基于以上三种工作模式，NFC 设备可以广泛地应用在门禁卡、公交车、手机支付、智能海报、数据传输等领域，如图 6.5 所示。

NFC 起源于 RFID，但与 RFID 有很多区别。它们的主要区别如表 6.2 所示：

表 6.2　NFC与 RFID的比较

性能指标	NFC	RFID
工作频率	13.56 MHz	多个频段，分为低频、高频和超高频
工作距离	0~ 20厘米	数厘米至数米
工作模式	可同时支持读卡器模式和卡模拟模式	读卡器模式和标签分离
点对点通信	支持	不支持
应用领域	模拟各类卡片、支付、短距离数据传输等	工业、物流等
兼容性	低频领域兼容 RFID	不兼容 NFC

NFC有主动通信和被动通信两种通信模式。在NFC主动通信模式中，双方设备交替产生射频场，当一方产生射频场发送数据时，另一方进入侦听模式接收数据。而被动通信模式中只有一方持续开启射频场，另一方持续处于侦听模式，从对方的射频场中获得能量，并使用负载调制等技术以和发送方相同的速率进行数据应答。图6.6中两台手机正在通过NFC，以“背靠背”的方式传输数据。无论采用主动还是被动模式传输，在同一时刻只能有一方发送，另一方接收。

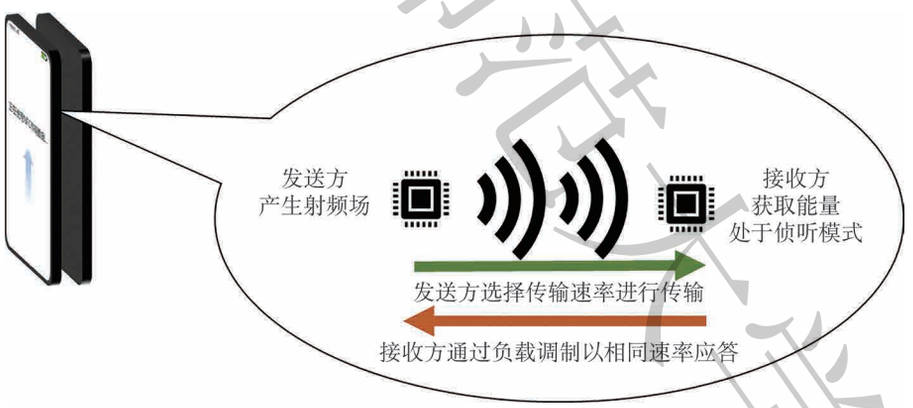


图 6.6　NFC传输原理和传输过程

知　识　延　伸　窄带物联网（NB-IoT）

窄带物联网（narrowband Internet of things，简称NB-IoT）是一种专门为万物互联打造的蜂窝网络技术。“窄带”一词体现在其通信频率上，只有180kHz，并且它能够与现有的3G、4G网络共存，实现对网络的复用，降低了网络的部署成本。

NB-IoT具有如下特点：

（1）广覆盖：NB-IoT由于频率低，因此其覆盖范围更广，一般能达到几百千米。它能够进入一般手机网络无法进入的地下，因此如果要在深层地下进行网络连接，NB-IoT将会是不错的选择。

（2）大连接：NB-IoT可以支持更多的连接数，最大可支持50000个连接。这一特性为物联网提供了更有力的支持。

（3）低功耗：采用NB-IoT技术的终端在99%的时间内处于休眠态，待机时间最长可达10年，已远超

出一台设备的使用寿命。

（4）低成本：NB-IoT设备的软硬件环境都可以按需简化，降低了设备的成本。一个单独的通信模块价格不超过 5美元。

当然，NB-IoT虽然具有上述优势，但也存在低速率、低移动性的缺点。因此对高速通信需求不能使用NB-IoT设备。

NB-IoT设备目前已经商用。如智能停车能实现预定、转租停车位等功能，低功耗和高穿透力使这个方案更具可行性；共享单车的智能锁也采用了 NB-IoT技术；智能井盖借助 NB-IoT技术能实现自动定位与跟踪等。

分 析 评 价

如图 6.7所示的一间智能房间内，有不少智能设备，请判断它们使用了 Wi-Fi、蓝牙、NFC、RFID中的哪些连接方式，填入表 6.3中。

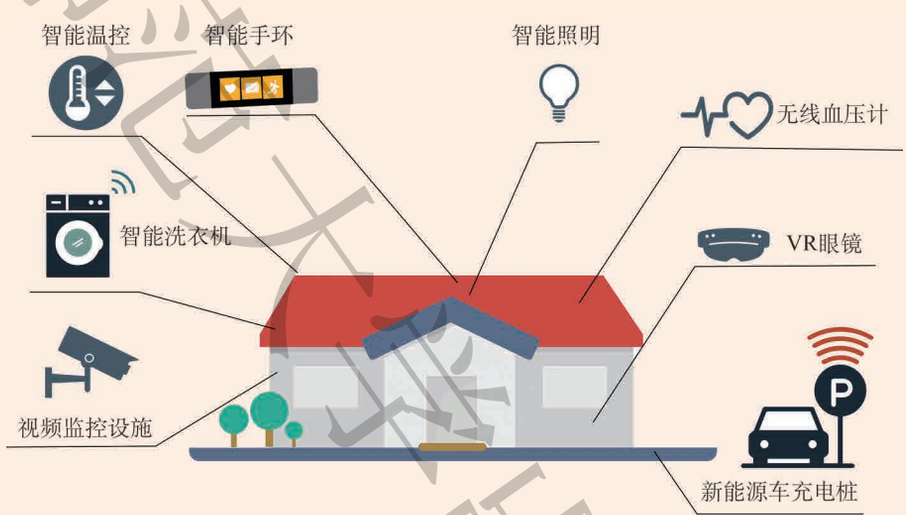


图 6.7 智能房间内的智能设备

表 6.3 智能设备可能的连接方式

设备	可能的连接方式
智能温控	
智能洗衣机	
视频监控设施	
智能手环	
智能照明	
无线血压计	
VR眼镜	
新能源车充电桩	

第三节　物联网应用实例与创新网络服务

现在，物联网已经悄然进入了我们的日常生活。随着无线网络的发展和传感器的广泛分布，物联网可以随时感知我们的生活状态，通过互联网传输数据，通过软件处理数据，做出智能的分析判断或者执行特定的动作。本节通过若干实例，展示物联网是如何引领创新网络服务的。

体　验　思　考

小林同学是一名出生在普通双职工家庭的高中学生。他回忆起自己小时候，由于父母下班的时间和自己放学的时间几乎是一样的，父母下班后还需要去买菜做晚饭，等吃上晚饭要过很久。家里虽然有空调，但如果没人在家是不能控制空调的，在炎热的夏天或是寒冷的冬天，从开启空调到完全制冷制热也要等上相当长的一段时间。小林同学家里也养了几盆植物，但由于父母忙于工作，自己忙于学习，常常忘记给植物浇水施肥。窗外的晾衣杆也需要人手动推拉，一旦遇到突变的天气，衣服也无法及时收回……

如今，小林的家里添置了不少智能家居设备。例如，自动料理机和空调都可以通过手机自动开启，不必等小林和父母回到家，一顿可口美味的饭菜就可以做好，家里也早已调整到合适的温度。智能花盆可以监控土壤的水分和肥料，并将这些数据发送到主人的手机上，提醒主人为植物浇水施肥。窗外的晾衣杆也会在感应到雨水时自动收回，有效地防止了衣服被雨水打湿的现象。通过这些智能家居设备，小林和他父母的生活得到了极大改善，小林可以在学校安心学习，父母也可以在单位安心地工作啦。

思考：除了上述的智能家居设备，你还在哪些地方看到过基于物联网的智能设备？它们给人们的生活带来了哪些改变？

一、智能家居

过去，家庭中的家用电器处于“各自为政”的运行模式。人们将大量的时间用于不同设备的开关和状态监视过程，不仅使人们失去了自己的空闲时间，也造成了能源的浪费。随着计算机网络技术的发展，特别是物联网技术的兴起，“互联网 + 家庭”的概念被提出，“智能家居”开始逐步普及到普通家庭中。

在一个典型的智能家居场景中，各设备都至少具有以下两个功能：①能通过手机或平板电脑的应用程序识别、监视与控制；②能自动感知本身的工作状态并将这些状态发送到网络上。智能家居基本原理图如图 6.8 所示。各智能家居设备都通过无线网络与位于互联网上的物联网服务器相连接。物联网服务器负责对设备和用户进行认证，确保用户操控的是自己所拥有的设备，而不会将用户的控制指令错误地发送

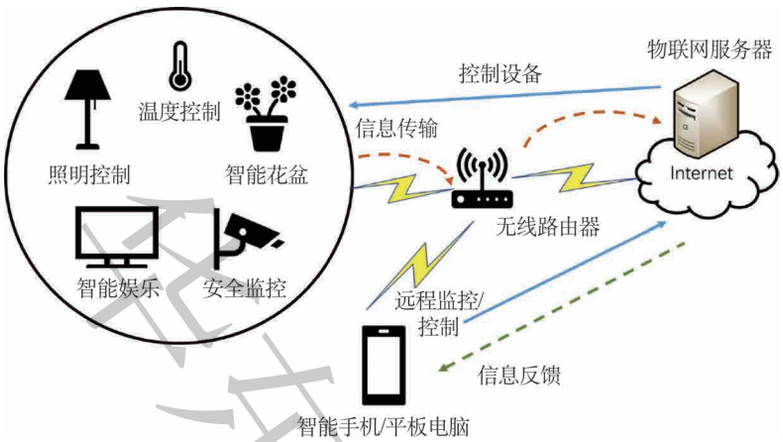


图 6.8　智能家居工作原理

到其他人的智能设备上。物联网设备通过互联网连接将自己的状态信息等传输给服务器，服务器也通过互联网将物联网设备的信息经过处理以后推送给用户的智能手机或平板电脑，使用户知道设备目前的状态。当然，物联网服务器也可以通过人工智能的方式自动做出一些决策。而用户如果需要远程控制设备，也需要通过物联网服务器将控制信息发送给设备。

二、校园卡与物联网

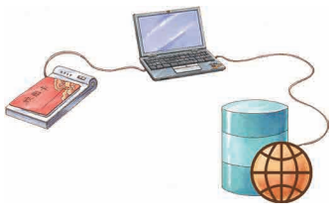


图 6.9　校园卡刷卡过程

现在，不少学校采用的校园卡的主要实现方式就是 RFID 技术。学号作为学生的唯一 ID 被存储在校园卡的 RFID 标签内。如图 6.9 所示，当学生用校园卡刷卡时，刷卡机读取 RFID 标签内的 ID，并迅速与数据库比对，从而调出该同学的各项数据按需进行读取或写入。未来，校园将与物联网紧密融合，形成更加智能化的“智慧校园”，能够自动感知同学们在校学习生活的各种状态，给我们提供各种便利措施，让我们感受到在校园中学习的快乐。

三、可穿戴设备

图 6.10　可穿戴设备

可穿戴设备即直接穿在身上，或是整合到用户的衣服或配件的一种便携式设备。可穿戴设备不仅仅是一种硬件设备，还可以通过软件和互联网交换数据，实现强大的功能。可穿戴设备将会给人们的生活、感知带来很大的转变。

可穿戴设备多以具备部分计算功能、可连接手机及各类终端的便携式配件形式存在，目前，主流的产品形态包括智能手表、智能手环，智能眼镜等。图 6.10 展示了一个典型的可穿戴设备场景。

可穿戴设备往往通过蓝牙和智能手机相连接，这就形成了个人区域网（personal area network，简称 PAN）。这些设备可以具有监测、感知、录音录像等功能，并通过智能手机将它们收集的数据经过处理以后展示给用户。由于使用方便，且数据和自身身体状况相匹配，可穿戴设备正得到越来越多人的关注和喜爱。

四、智能物流

现在，网络购物已经越来越受到人们的喜爱。顾客在网上下单付款后，物流服务都能准确地将商品送到顾客指定的收货地址。那么，物联网技术在其中又扮演了怎样的角色呢？

随着物联网理念的逐步引入、技术的不断提升、相关政策的扶持，物联网将引发物流产业革命性的变化。

通常，一些规模较大的企业都会有自己的仓库。而商品从仓库到运输再到目的地的全过程中就有物联网的参与。每件商品移动一次，都要用终端扫描器扫描一次 RFID 电子标签，将其最新状态告知系统。每件商品也都拥有能被射频系统识别的“姓名”，这个“姓名”就是商品外包装上的条形码或二维码，并且可被全球识别。图 6.11 展示了这一过程。目前一些先进的无人仓库中，遍布整个仓库的 RFID 设备会周期性地自动收集当前仓库内保存的货品信息。当货品需要运输时，货运机器人会通过物联网自动地找到货品位置并开始搬运货品。通过我们看不见的电波，基于物联网的智能物流系统正在有条不紊地运行着。

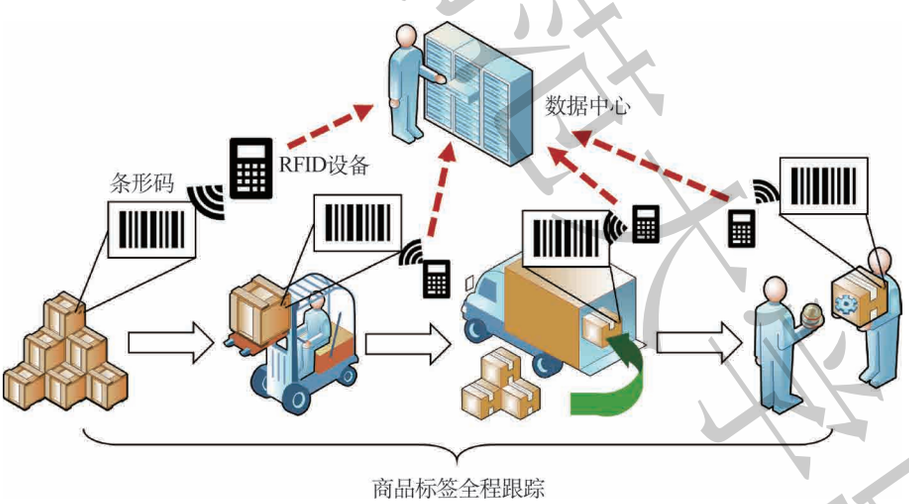


图 6.11　智能物流

探　究　活　动　　**探究课题：无人驾驶中的信息安全**

随着物联网技术的发展，无人驾驶技术逐步从实验室走向实际应用，不少企业推出了自己的无人驾驶汽车。但无人驾驶汽车也面临着一系列网络安全问题，这些问题中有些是在物联网环境下产生的新问题。

请同学们 3～4人一组，跟着下列活动步骤开展调查研究，并形成《无人驾驶中的信息安全》调研报告。

1　目前，无人驾驶技术是如何实现的？其中涉及到哪些物联网技术？

2　现在无人驾驶汽车在数据的采集、通信过程中，遇到过哪些网络安全问题？

3　针对这些安全问题，选择其中一个，探究目前存在哪些解决手段。

4　针对上述解决手段，选择其中一个，探究是否存在更好的改进措施。

附录　常见网络拓扑符号及其含义

符　号	含　义
	线缆(双绞线)
	线缆(光纤)
	计算机(主机)
	计算机(笔记本电脑)
	交换机
	路由器
	无线路由器
	数据库
	移动设备 (智能手机、平板电脑等)

后　记

本册教科书依据教育部《普通高中信息技术课程标准（2017 年版 2020 年修订）》编写，并经国家教材委员会专家委员会审核通过。全体编写人员认真领会国家基础教育改革精神，精心研究当代信息社会的人才培养要求，广泛调研上海及各地高中信息技术教育的现状和挑战，深入了解高中学生的学习需求，并汲取了上海市《普通高中信息科技（试用本）》的编写经验。

编写过程中，上海市中小学（幼儿园）课程改革委员会专家工作委员会，上海市教育委员会教学研究室，上海市课程方案教育教学研究基地、上海市心理教育教学研究基地、上海市基础教育教材建设研究基地、上海市信息科技教育教学研究基地（上海高校“立德树人”人文社会科学重点研究基地）及基地所在单位华东师范大学等单位给予了大力支持，在此表示感谢！

本册教科书出版之前，我们已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，我们衷心地表示感谢！恳请尚未联系到的作者与我们联系，以便出版社及时支付相关稿酬。

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。

编　者