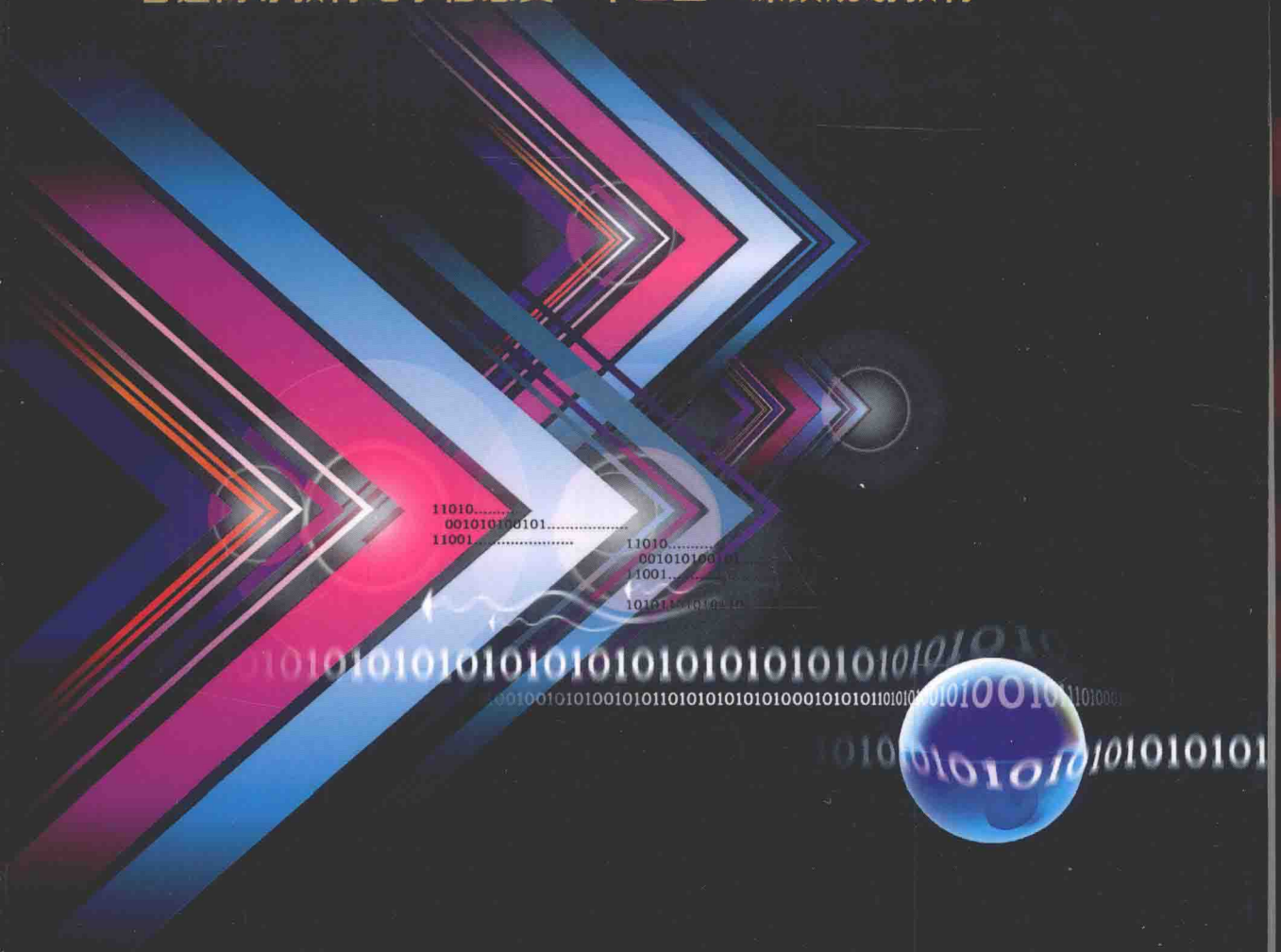
中国电子教育学会高教分会推荐

普通高等教育电子信息类“十三五”课改规划教材



# 信息安全导论

（第二版）

王继林　苏万力　编著

西安电子科技大学出版社
http://www.xduph.com

中国电子教育学会高教分会推荐

普通高等教育电子信息类“十三五”课改规划教材

# 信息安全导论

(第二版)

王继林　苏万力　编著

西安电子科技大学出版社

## 内 容 简 介

本书面向学过计算机基础课的学生，力图通过“一讲一练”的方式让学生掌握信息安全的基础知识。书中没有复杂的公式推导，通过大量图表来简化对问题的理解，并对大家普遍关心的口令认证和网络交易安全进行了重点论述。

全书共 17 章，内容涵盖了攻击方法、防守方法和信息安全管理的理论和实训，每一章章末配备了两个相关实验供不同基础的同学选做。本书内容既体现信息安全理论的博大精深，又不过多纠缠于技术细节，在实践安排上突出对学生编程能力的培养。

本书可作为高等学校及各类培训机构信息安全课程的教材或教学参考书。

**图书在版编目(CIP)数据**

**信息安全导论**/王继林，苏万力编著. —2 版. —西安：西安电子科技大学出版社，2015.8
普通高等教育电子信息类“十三五”课改规划教材
ISBN 978-7-5606-3761-7

Ⅰ. ① 信… Ⅱ. ① 王… ② 苏… Ⅲ. ① 信息安全—高等学校—教材 Ⅳ. ① TP309

**中国版本图书馆 CIP 数据核字(2015)第 198502 号**

策　　划　毛红兵
责任编辑　毛红兵　秦媛媛
出版发行　西安电子科技大学出版社(西安市太白南路 2 号)
电　　话　(029)88242885　88201467　　邮　　编　710071
网　　址　www.xduph.com　　电子邮箱　xdupfxb001@163.com
经　　销　新华书店
印刷单位　虎彩印艺股份有限公司
版　　次　2015 年 8 月第 1 版　　2015 年 8 月第 1 次印刷
开　　本　787 毫米×1092 毫米　1/16　印　张　19
字　　数　450 千字
印　　数　3001～4000 册
定　　价　35.00 元
ISBN 978-7-5606-3761-7/TP

**XDUP 4053002-2**

# 前　言

由于信息安全在人们日常生活中的作用越来越重要，很多非 IT 专业学生开始选修该课程，很多高校也在全校范围内开设了“信息安全”选修课。

作者在讲授有关“信息安全”方面的课程时，接触并使用过很多教材。这些教材往往偏重理论论述，在实验教学和动手能力的培养方面不是很理想，并且大都要求学生有“计算机网络”、“离散数学”和“操作系统”课程的前期知识，而非 IT 专业学生仅学过“计算机基础”课程，部分学生选修过“程序设计”课程，难以满足要求。针对这种现状，作者萌生了编写一本面向理、工、管、法、商等大多数学生的“信息安全”课教材的想法，本书就是作者为此目的编写的。本书是在第一作者所著《信息安全导论》教材的基础上修订完成的。

基于“做中学”的指导思想，本书按一个学期 17 次专题讲授和 17 次实验编写，内容涵盖了信息安全的主要研究领域，在编写过程中突出了“导论”的地位和作用，即不过于纠缠技术细节，力争让学生对信息安全的现状和未来研究动向有个全面了解。本书主要具有以下特点：

(1) 通俗易懂，适用面宽。考虑到学生的基础差异，本书理论部分仅假定学生学过“计算机基础”课程；实验部分分两个层次，每章的第二个实验难度稍大并需要程序设计方面的知识，不同基础的学生仅需在实验内容上进行取舍即可。因而本书适合绝大多数管理、工学和文科专业学生，也适合 IT 专业二年级学生。

(2) 突出实践能力尤其是编程能力训练。为克服理论和实践脱节的现象，本书按“一讲一练”的思路编排，详细设计了相关实验内容，力图突破过去学生反映的“空”和“难”的障碍。本书在实验内容的选取上，之所以突出编程能力的训练，主要是基于学生前期计算机知识和课程衔接方面的考虑。

(3) 结合生活实际，强调实用。本书对口令认证和网络交易安全进行了重点论述和训练；另外，使用本书不需要为实验配置专门硬件，学生只要有台电脑就可学习。

本书可以作为高校和各类培训机构相关课程的教材或教学参考书。建议使用本书的教师按照 34 学时讲授全部理论内容，并根据学生实际情况开设实验：对于没学过“程序设计”课程的学生可仅开设其中的验证性实验，对于计算机和电子商务等专业的学生则需强调其中的设计性实验。与本书有关的电子材料请到浙江财经大学网络课堂“计算机安全与保密”课程中下载。

本书在编写过程中，参考了众多学者的教材、论文和专著，以及很多网上材料，在参

考文献中力求将其一一列出，如有疏漏，恳请谅解并指正。作者要特别感谢西安电子科技大学王育民、王新梅和肖国镇三位导师，是他们把我引入信息安全领域。在本书的编写过程中，作者还得到了美国 UNCC 大学郑玉良教授等很多老师和西安电子科技大学出版社老师的指导、鼓励和帮助，在此也一并致谢。

由于作者水平有限，书中难免出现不妥之处，恳请广大读者不吝赐教。对于本书的任何问题敬请通过下列邮箱与作者联系：wangjilin@msn.com。

编著者

2015 年 5 月 30 日

# 目　录

# 第 1 章　信息技术是一把双刃剑

**内容导读**

从单机模式到云计算，计算技术的不断提升给人们的生活方式带来了巨大改变。未来，人类将以更加精细和动态的方式管理生产和生活，从而使我们的地球更“智慧”，使我们的生活更美好。

现在，网络虚拟空间已经成为人类生存空间的一个有机组成部分。如何更好地保证人们健康、有序、和谐地利用信息资源，如何在信息社会保护自己的隐私和合法权益等问题便构成了信息安全这一学科的研究内容。

本章要求学生重点掌握网络协议、TCP/IP 协议、包交换等有关概念和常用的网络命令，初步理解网络投票系统的安全要求和各参与方的责任。

## 1.1　快速发展的信息技术

### 1.1.1　信息技术令我们的生活丰富多彩

人们普遍认为物质、能量和信息是构成世界的三大要素。信息是事物运动状态和状态变化的方式，是物质和能量的形态、结构、属性和含义的表征，是人类认识客观世界的纽带。由于事物的状态和变化是多姿多彩、变幻无穷的，因此，就出现了不同的信息。

在某种程度上，我们的社会是靠信息组织起来的，一个机构的行为其实就是一系列的信息处理活动。对于一个小单位而言，其信息组织与处理可能相对较为简单；而对一个大单位而言，其信息的处理不但重要，而且繁琐，需要有标准的、一致的处理流程和系统化的收集、存储、共享、销毁等方案。把信息分为保密信息、内部信息和可公开信息三大类以后再对信息进行使用和管理是一般单位通行的做法。

原则上，能够延长或扩展人的信息感知能力的手段和方法都称为信息技术，但计算机和现代通信技术的发展，使得信息的加工和处理产生了质的飞跃。目前谈到信息技术，都离不开计算机和现代通信技术的支持，因此，《新华字典》中把信息技术定义为利用电子计算机和现代通信手段，获取、传递、存储、处理、显示和分配信息并且提供服务的方法，相关内容涵盖了通信、控制、计算机软硬件、电子器件、光和量子技术等领域。

信息技术正在促进经济社会和文化建设的各个领域发生深刻的变革，并成为拉动国民

经济增长、丰富人们精神文化生活、提高人民生活质量、促进社会和谐的重要力量。《第34次中国互联网络发展状况统计报告》显示，截至2014年6月，我国网民规模达6.32亿，其中手机网民达5.27亿。手机网上支付、手机网络购物、手机网上银行和手机旅行预订应用的全年增长率均超15%。

21世纪的重要特征就是信息化、数字化和网络化。信息与通信技术的应用已成为许多国家改善宏观管理、社会管理，提升人民生活质量的重要手段。发展电子信息产业是各主要经济体带动经济增长的首要战略选择。

### 1.1.2　计算模式的每次变革都带来生活方式的巨大改变

信息技术的高速发展推动了计算模式的不断变革，从单机时代的主机/终端模式，文件服务器时代的共享数据模式，客户机/服务器时代的C/S(Client/Server)计算模式，到电子商务时代的B/S(Browse/Server)网络计算模式和正在探讨的基于虚拟化技术的云计算，计算模式已经发生了巨大变化。计算模式每一次的更新都伴随着计算技术的不断提升和人们生活方式的巨大变革。

20世纪90年代，计算技术最引人注目的进展之一就是应用计算环境从集中走向分布，其中，C/S计算技术成为分布式计算的主流技术，并在企业计算环境中得到广泛应用。

通过基于Internet的B/S计算模式，企业能够实现全球化、高效率的协作和个性化的服务，并建立一个能够真正面向未来、面向全球、完全开放的电子商务系统。

随着移动技术、宽带网络和虚拟化技术的发展，今天的个人计算机(PC)将被各种各样简单的终端所取代，而未来终端价格将如同“书本”一样便宜、好用、无所不在，云计算将使超级计算能力和存储能力通过网络自由流通成为可能，人类社会将进入一个大规模“知识生产”的时代，IT令世界的明天更加美好。

### 1.1.3　我国在信息技术领域的成就与不足

我国在信息技术领域取得的成就可用“可上九天揽月，可下五洋捉鳖”来概括。

导航与定位服务对城市规划与管理、公共安全与日常生活都有非常重要的作用，中国北斗区域卫星导航系统的基本系统已建设完成。北斗卫星导航系统是中国自行研制开发的区域性有源三维卫星定位与通信系统(CNSS)，是除美国的全球定位系统(GPS)、俄罗斯的GLONASS之后第三个成熟的卫星导航系统。北斗系统除了能导航、定位，还可传递一定数量的短信，这是其他卫星导航系统所不具备的。

深海载人潜水器是海洋开发的前沿与制高点之一，其水平可以体现一个国家在材料、通信与控制、海洋学等领域的综合科技实力。中国的“蛟龙号”潜水器下潜深度可达7000多米。在中国之前，世界上只有美国、日本、法国和俄罗斯拥有深海载人潜水器。在深海中，无线电无法使用，水声通信是远距离数据传输的唯一方法。陆地上的无线电通信速度是30万千米每秒，但水声通信只有1500米每秒。我国研究人员克服了重重困难才解决了联络问题，使“蛟龙号”具有先进的水声通信能力，可以高速传输图像和语音。

尽管我国在信息技术领域取得了一些重大突破和重要进展，但是从整体来看，我国的科学技术水平与发达国家仍然存在较大差距，自主创新的能力依然较弱。在信息技术领域，高端通用芯片、核心电子器件和大尺寸液晶面板等关键产品几乎全部依赖进口，中国软件

业 70%依赖于国外，某些行业领域曾一度被国外的软件产品所垄断，如办公软件、制图软件、大型数据库软件等。目前，国外公司基本上主导了智能终端操作系统的发展，谷歌、苹果以及微软三家美国公司已占据了先发优势和规模优势。反观国内智能操作平台，尽管中国移动和中国联通在奋力追赶，但国内智能终端的操作系统独立之路还相当漫长。国外巨头的垄断，开发的技术创新，用户习惯的改变，都将是艰难的挑战。

## 1.2　网络就是计算机

将众多的信息资源、计算资源、仪器资源和人力资源汇集起来，充分发挥其综合效能，面向应用提供高效的信息服务支撑和计算服务支撑是人们不懈的追求目标。

19 世纪以前的漫长的历史时期内，人类传递信息主要依靠人力和畜力，也曾使用信鸽或借助烽火等方式来实现。1969 年底出现的 ARPAnet 和后来的 Internet，使得相互之间不兼容的异种计算机在全球范围内实现了互联和通信。随着各类计算机的迅速普及和网络的迅猛发展，20 世纪 90 年代初 SUN 公司提出的“网络就是计算机”的观点正越来越被广大用户所接受。

### 1.2.1　计算机网络与协议

把处于不同地理位置的、独立的、自治的多个计算机系统通过通信设备和线路连接起来，以功能完善的网络软件实现资源共享的系统称为计算机网络系统。计算机网络示意图如图 1-1 所示。

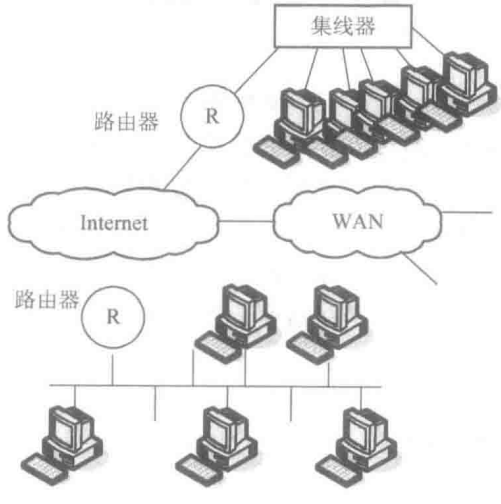



图 1-1　计算机网络示意图

网络中连接收发双方的物理通路和传送信息的载体称为传输介质。网络传输介质包括同轴电缆(BNC/10Base-2、AUI/10Base-5)、双绞线(UTP/10Base-T、100Base-T、1000Base-T)、光缆(Fiber-optic/100Base-FX)、微波(扩频/跳频无线传输)、无线电、卫星通信和红外线。其中使用较广泛的是双绞线、光缆和无线电。

网络根据所覆盖的地理范围可划分为局域网、城域网、广域网和互联网四种。局域网一般来说只覆盖一个较小区域，城域网是不同地区的网络互联。目前流行的局域网组网技术包括共享式以太网、交换式快速以太网(10/100Mbps)、千兆交换以太网、万兆交换以太网和无线网。

局域网按拓扑结构可分为星型网络、环型网络和总线型网络。局域网的三种拓扑结构如图 1-2 所示。

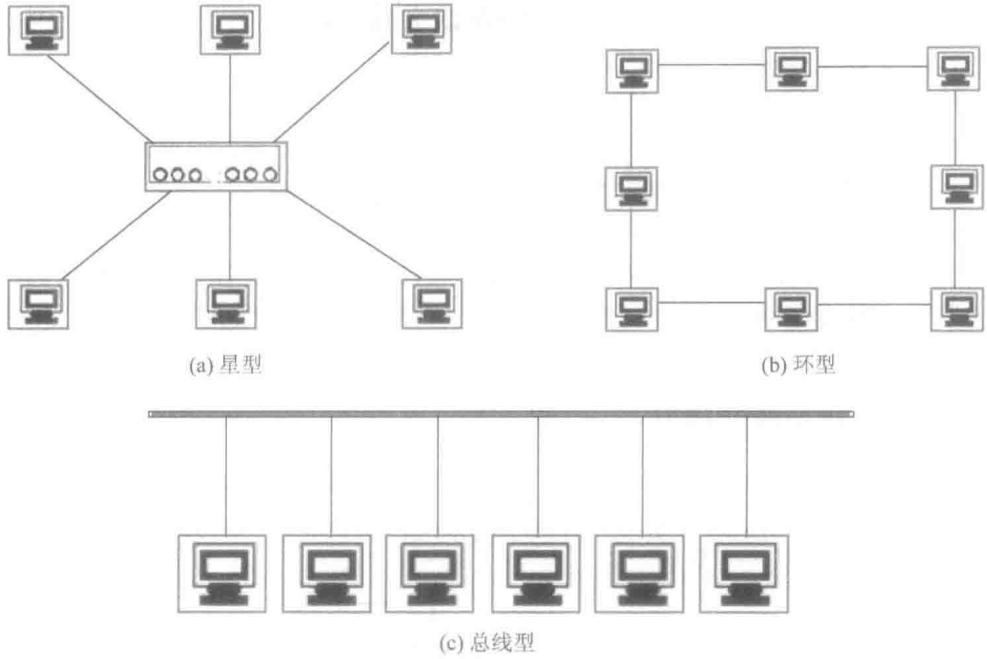



图 1-2　局域网的三种拓扑结构

在星型网络中，各站点通过点到点的链路与中心站相连。在环型网络中，各站点通过通信介质连成一个封闭的环形。环形网容易安装和监控，但容量有限，网络建成后，难以增加新的站点。在总线型网络中，网络中所有的站点共享一条数据通道。总线型网络安装简单方便，需要铺设的电缆最短，成本低，某个站点的故障一般不会影响整个网络，但介质的故障会导致网络瘫痪。总线型网络安全性低，监控比较困难，增加新站点也不如星型网络容易。

网络中的实体只有遵循规则才能实现通信。为进行网络中的数据(信息)交换而建立的规则、标准或约定称为网络协议。网络协议的功能主要有：

(1) 分割与重组。协议的“分割”功能将较大的数据单元分割成较小的数据包，其反过程为“重组”。

(2) 寻址。协议的“寻址”功能使得设备彼此识别，同时可以进行路径选择。

(3) 封装与拆装。协议的“封装”功能是指在数据单元(数据包)的始端或者末端增加控制信息，其相反的过程是“拆装”。

(4) 信息流控制。协议的流量控制功能是指在信息流过大时，为保证正确传送所采取的一系列措施。

(5) 排序、差错控制、同步、干路传输、连接控制等。

网络协议通过语法、语义和规则(时序)来表述。常见的网络协议有 TCP/IP 协议、IPX/SPX 协议等。其中 TCP/IP 协议是 Internet 最基本的协议。

### 1.2.2　IP、UDP 和 TCP 协议

TCP/IP 协议簇分为两类协议：应用层协议和网络与传输层协议。大家比较熟悉应用层协议，例如，经常使用 HTTP 协议浏览网页，使用 FTP 协议传输文件。网络与传输层协议管理着计算机间的数据传输，这些协议用户注意不到，是在系统表层以下工作的。其中网络层协议 IP 主要负责网络间数据的传送，就像通过邮局发信的时候要用一个带有目的地和始发地址的信封把内容封装起来一样，网络层协议也要对要传输的数据添加一个“信封”(IP 头)。

IP 协议只能保证数据到达指定 IP 地址的机器，但一台机器上往往运行着多个程序(进程)，因而还应当指明数据是发送给哪个进程的，这一工作由传输层协议 UDP 或 TCP 负责。TCP 是面向连接的协议，即在收发数据前，必须和对方建立可靠的连接。UDP 是一个非连接的协议，在传输数据之前，源端和终端不建立连接，当它想传送时就简单地去抓取来自应用程序的数据，并尽可能快地把它扔到网络上。在发送端，UDP 传送数据的速度仅仅受应用程序生成数据的速度、计算机的能力和传输带宽的限制；在接收端，UDP 把每个消息段放在队列中，应用程序每次从队列中读一个消息段。相比较而言，基于连接的 TCP 对系统资源的要求较多，但能保证数据的可靠传输，而利用 UDP 的程序结构较简单，但不保证数据的可靠传输。

### 1.2.3　分组交换技术

在使用 TCP/IP 协议传输数据时，发端计算机首先将用户传送的数据划分成一定长度的分组(包)，然后在每个分组的前面加上一个分组头，用以指明该分组发往何地址，最后把相应分组交给交换机。交换机根据每个分组的地址标志将它们转发至目的地。接收端计算机再去掉分组头将各数据字段按顺序重新装配成完整的报文。这一过程称为包交换或分组交换。

分组交换实质上是在“存储—转发”基础上发展起来的。在分组交换方式中，以分组方式进行数据的暂存交换，经交换机处理后，很容易实现不同速率、不同规程的终端间的通信。分组交换的特点主要有：

(1) 线路利用率高。分组交换以虚电路的形式进行信道的多路复用，实现资源共享，可在一条物理线路上提供多条逻辑信道，极大地提高了线路的利用率，使传输费用明显下降。

(2) 不同种类的终端可以相互通信。分组数据以分组为单位在网络内存储转发，使不同速率终端、不同协议的设备利用网络提供的协议变换功能实现互相通信。

(3) 信息传输可靠性高。网络中每个分组进行传输时，在节点交换机之间采用了差错校验与重发的功能，因而使信息传输的误码率大大降低，而且在网内发生故障时，网络中的路由机制会使分组自动地选择一条新的路由避开故障点，不会造成通信中断。

### 1.2.4　最终目的地和下一跳

如图 1-3 所示，节点 A 的数据到底如何才能到达节点 B 呢？A 的数据首先要送到交换机 R1，由 R1 送往 R2，以此类推，最后到达目的地 B。相邻节点的传送称为点到点的一跳。在相邻两跳中，转发节点要做很多工作，其中包括下一跳的节点选择(路由)、原来数据链路层报头数据的去除和新数据链路层报头数据的添加等。相邻节点由于在同一个网络中，因而使用的底层(数据链路层和物理层)协议是相同的，而不相邻的节点可能使用不同的底层协议，这就需要协议转换。

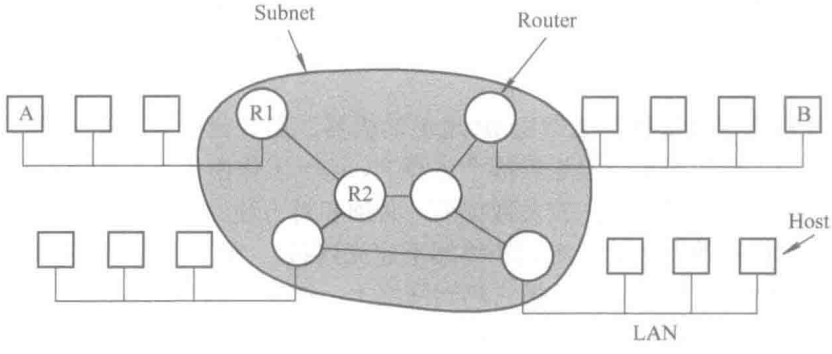



图 1-3　数据在不同网络中的传输

### 1.2.5　网络计算的复杂性和人们的追求目标

不需购买和安装 Office 软件，你只要打开浏览器、输入一个网址，就可以使用 Word 了！这就是云计算带来的方便，各种计算、存储、软件、应用都可以以“服务”的形式提供给客户。

分布、并行和虚拟化技术的发展令云计算环境的建设成为可能。分布式计算是指利用网络把成千上万台计算机连接起来，组成一台虚拟的超级计算机，完成单台计算机无法完成的超大规模的问题求解。

从技术角度来说，分布式系统的底层问题(通信、协调、同步及不确定)主要控制着选举、互斥、一致性、时钟同步等，以及最新的快速互斥算法、对列锁、分布式共享存储器、无等待层级和故障检测器等。例如，在一个分布式数据库系统中，数据和管理软件分布在各个计算点，系统的各个分布点通过某种形式的通信设施互相连接在一起(通信和数据分布的细节对于用户来说是不可见的)。分布式数据库系统需要解决的问题包括数据的分布与冗余、分布式查询处理、分布式并发控制、分布式事务恢复、目录管理和异构数据库的相联等。

新的计算模式可以控制大量的终端用户设备、传感器、作用器，并将它们联系到强大的后台系统上。再辅之以诸如超级计算机的先进计算能力，以及配合“云计算”模式，众多数据得以转换成信息。这些信息又可以被转化为行动，提高系统、流程和基础设施的效率、生产力和反应速度——总而言之，使系统更有智慧。

现在人们谈论网络与信息技术时，更多的是将它们和社会、健康、能源、材料以及数

字地球、物联网等领域联系起来。可以预见，通过超级计算机和计算将物联网整合起来，人类以更加精细和动态的方式管理生产和生活，可以使我们的地球更“智慧”，生活更美好。

## 1.3　信息技术带来的负面影响与挑战

大多数网民在使用互联网过程中遇到过病毒或木马攻击，账号或密码被盗、假冒网站、隐私泄漏、非法监控等事件时有发生，网络安全和信任问题已经成为当今社会快速发展的最大制约因素。

### 1.3.1　有关案例

**案例 1-1**　苹果承认 iPhone 泄露用户隐私。

人民网 2014 年 7 月 28 日报道，一位法国科学家在苹果移动操作系统 ioS 中发现多个未经披露的“后门”。这些后门可以帮助有关机构、美国国家安全局或其他恶意分子绕开 ioS 的加密功能，窃取用户的私人信息。美国苹果公司已经承认 iPhone 确实存在“安全漏洞”，但否认为情报部门服务。

**案例 1-2**　美国政府“棱镜”计划于 2013 年 6 月被曝光。

自 2007 年开始，美国情报机构一直在九家美国互联网公司中进行数据挖掘工作，从音视频、图片、邮件、文档以及连接信息中分析个人的联系方式与行动。监控的类型有 10 类：信息电邮，即时消息，视频，照片，存储数据，语音聊天，文件传输，视频会议，登录时间，社交网络资料的细节。其中包括两个秘密监视项目，一是监视、监听民众电话的通话记录，二是监视民众的网络活动。美国国家安全局与联邦调查局参与了该项目。与政府机构合作的九家互联网公司分别是：微软、雅虎、谷歌、Facebook、PalTalk、美国在线、Skype、YouTube、苹果。这些项目都侵犯了公民基本权利。

**案例 1-3**　网络投票。

从 2010 年 9 月开始，四川省乐山市开始进行杰出人才评选。截至 2010 年 11 月 10 日，20 名候选人中有 16 人得票超过 100 万，7 人得票超过 160 万，然而，乐山市总人口只有 350 多万。

主办方是设置了很复杂的验证码，而且规定一台电脑一个小时内只能投一次票。如何规避这些限制呢？一家名为远道网络科技公司的人员称，其拥有一种特殊的刷票软件，可以既让投票量增长，又不被主办方发现。

这种情况的出现，让主办方和候选者处在了一个尴尬的境地上。规则被破坏，候选者被伤害，社会风气被毒害，公信力被质疑。那么对于网络幕后的灰色交易该如何核实、查处和惩戒？如何通过更严密的技术和制度手段，对网络违法违规行为进行有效的防范？在网络日益发达的今天，这是我们必须要面对和尽快解决的问题。

### 1.3.2　新技术带来的新挑战

全球信息化正在引发当今世界的深刻变革，重塑世界政治、经济、社会、文化和军事发展的新格局，加快信息化发展，已经成为世界各国的共同选择。

信息技术的发展日新月异，促使人们对信息资源的依赖性越来越强。人民群众的社会生活、企业的生产经营、国民经济和社会发展、国防和军队建设等都离不开信息系统。虚拟空间已经成为人类生存空间的一个有机组成部分。

网络和信息技术的快速发展和对人类生活巨大的正、负面影响，迫使世界各国都在思考如何更好地规范网络空间的秩序，如何在信息社会中保证人们健康、有序、和谐地开发、传递和利用信息资源；迫使各个行业、企业和单位考虑如何阻止、防止、检测和纠正有关违反合理使用其信息资源规则的行为和意图；也使得广大基层民众担心在信息社会如何保证自己的隐私和合法权益；甚至在信息化战争中的敌对双方都在思考如何获得信息的优势，达到制胜的目的。所有上述问题的研究，便构成了信息安全这一学科的主要内容。

## 思 考 题

(1) 你平时上网是如何注意保护个人隐私的？
(2) 用户在 AT&T 公司网站注册时密码有什么要求？你的网络密码设置是否安全？
(3) 什么是网络协议？什么是包交换？什么是下一跳？
(4) 假如要你为所在的班级建设一个网站，试描述建设步骤。
(5) 你认为一个网络拍卖系统在技术上应该满足哪些要求？
(6) 什么是云计算？什么是物联网？什么是虚拟化技术？

# 实验 1A　熟悉网络环境

## 一、实验目的

(1) 掌握局域网的特性，熟悉局域网的几种拓扑结构，比较它们各自的特点。
(2) 初步理解 TCP/IP 协议。
(3) 学会使用 TCP/IP 常用命令，能通过使用相关命令进行网络连接测试与故障排除。

## 二、实验准备

### 1. 熟悉局域网的分类

局域网按网络的拓扑结构可分为星型网络、环型网络和总线型网络。各种网络的特点请参看第一章中的相关内容。局域网还可按服务方式分为客户机/服务器(C/S)网络和对等网络。

### 2. 初步理解 TCP/IP 协议

网络中计算机之间进行通信的语言被称为“协议”。只有能够讲，而且可以理解这些“语言”的计算机才能在网络上与其他计算机彼此通信。协议定义了网络上的各种计算机和设备之间相互通信、数据管理、数据交换的整套规则。

因特网(Internet)是使用 TCP/IP 协议栈组成的国际互联网。TCP/IP 协议栈是一个网络通