网络通信与信息安全

WANGLUO TONGXIN YU XINXI ANQUAN

何　鲲◇著

合肥工業大學出版社
HEFEI UNIVERSITY OF TECHNOLOGY PRESS

网络通信与信息安全

何　鲲　著

合肥工业大学出版社

图书在版编目(CIP)数据

网络通信与信息安全/何鲲著. —合肥:合肥工业大学出版社,2012.7
ISBN 978-7-5650-0813-9

Ⅰ.①网… Ⅱ.①何… Ⅲ.①计算机通信网—安全技术 Ⅳ.①TN915.08

中国版本图书馆 CIP 数据核字(2012)第 158242 号

网络通信与信息安全

何 鲲 著　　责任编辑 吴毅明

出 版	合肥工业大学出版社	版 次	2013 年 2 月第 1 版
地 址	合肥市屯溪路 193 号	印 次	2013 年 2 月第 1 次印刷
邮 编	230009	开 本	710 毫米×1000 毫米 1/16
电 话	总 编 室:0551—62903038	印 张	12.5
	市场营销部:0551—62903198	字 数	238 千字
网 址	www.hfutpress.com.cn	印 刷	合肥现代印务有限公司
E-mail	hfutpress@163.com	发 行	全国新华书店

ISBN 978-7-5650-0813-9　　定价:28.00 元

前　言

20世纪90年代以来，Internet在世界各国都得到了飞速发展和广泛应用，成为全球范围内传播科研、教育、商业和社会信息的主要渠道。网络的方便、快捷及其储存在各服务站点中的大量信息，无可置疑地使其成为人们获取信息的重要途径。

计算机网络是计算机技术与通信技术相结合的产物，具有交叉学科的特点。其主要内容包括数据通信、计算机网络体系结构、网络软件、网络协议、网络设备、组网的方法、网络互联、网络安全、网络管理、计算机网络的应用等。本书研讨了网络数据通信的基本原理和最新技术，以计算机网络的五层体系结构为主线，详细说明了每一层的工作原理与实现的功能。第1章主要阐释本书的主体结构及计算机网络的一些最基本概念；第2章至第6章为计算机网络从物理层至应用层的各层功能、协议、工作原理的分析研究；第7章阐述了无线网络的主要协议标准和关键技术及应用范围；第8章探讨了网络安全的几种常见问题，并以比较的方式提出了解决方案。

本书使用通俗易懂的语言进行阐述，翔实研讨了计算机网络的组成结构以及信息安全的基本原理，并列举了大量实例进行说明。计算机网络的理论、知识、技术更新很快，为使读者了解计算机网络的前沿发展动态，作者参考了国内外大量的最新出版物和网上及时的电子资料，力求使读者理解、掌握计算机网络技术最前沿的知识。在此向各文献的作者表示衷心的感谢。

作者于2009年获安徽省“信息管理与信息系统”省级专业带头人称号，一直致力于信息系统安全方面的研究，该著也是研究成果之一；同时本著的

撰写也是对2008年安徽省教育厅自然科学基金课题“安徽省汽车制造企业质量管理体系建立与完善的研究”的延续研究成果，主要是着力于企业信息安全防控的研究。

由于作者的能力和水平有限，错误与不妥之处在所难免，希望广大读者和专家进行批评指正。

作　者

2012年4月

目　录

第 1 章　计算机网络的基本概念阐释

现代计算机网络的飞速发展和广泛应用，使人类社会信息的存储、传递、交流和利用都发生了革命性的变化。网络已经成为全球范围内传播与共享科研、教育、商业和社会信息的主要渠道，网络信息资源也成为人们日常工作和生活中不可缺少的资源。

那究竟什么是计算机网络呢？一般而言，我们将采用通信线路将分散在不同地点的具有独立自主的计算机系统相互联结，并按照网络协议进行数据通信和实现资源共享的计算机集合，称为计算机网络，而在各种不同的网络中，发展最快、覆盖面积最广的，就是 Internet。

1.1　Internet 概述

Internet 是世界上覆盖面最广、规模最大、信息资源最丰富的计算机网络。Internet 是 Inter Network 的缩写，即国际互联网，也就是“网络中的网络”。Internet 是由世界各地的计算机和计算机网络所组成的一个巨大的松散的联合体。

从通信的角度来看，Internet 是一个以 TCP/IP 协议作为统一标准，将世界范围内各个国家的部门和机构的计算机网络联接而成的数据通信网；从资源的角度来看，Internet 是一个集各部门、各领域、各学科的信息资源为一体的数据资源网。

1.1.1　Internet 的起源与发展

Internet 的发展经历了实验研究、学术性网络、商业化网络等阶段。

1. 实验研究阶段(1969—1985 年)

Internet 最初起源于美国国防部高级研究项目署(Advanced Research Project Agency,简称 ARPA)为军事目的于 1969 年建立的一个实验型网络 ARPANET。该网络将美国多所大学和研究机构中从事国防研究项目的计算机联接在一起。1981 年,ARPA 建立了以 ARPA 为主干的 Internet 网。1983 年,TCP/IP 协议开发成功并得到了全面应用,Internet 开始由一个实验型网络转变为一个实用型网络。

2. 学术性网络阶段(1986—1995 年)

1986 年,美国国家科学基金会(NSF)建立了以 ARPANET 为基础的学术性网络,即 NSFNET。NSFNET 将美国的五个超级计算机中心联接起来,使用 TCP/IP 协议与 Internet 联接。NSFNET 建成后,Internet 得到了快速的发展。1988 年,NSFNET 最终取代了 ARPANET,成为 Internet 的主干网。1992 年,专门为 NSFNET 建立高速通信线路的公司 ANS(Advanced Networks and Services)建立了一个传输速率为 NSFNET 的 30 倍的商业化 Internet 骨干通道——ANSNET,并逐步取代了 NSFNET,成为 Internet 的主干网。1995 年,ANSNET 正式停止运营,Internet 也从学术性网络转化为商业化网络。

3. 商业化网络阶段(1996 年至今)

ANSNET 停止运营以后,出现了许多专门为个人或单位提供 Internet 接入服务的公司,即 Internet 服务提供商(Internet Service Provider,简称 ISP)。Internet 服务提供商之间的高速链路逐步成为 Internet 的骨干网。

近年来,Internet 逐渐发展到各个国家的各个行业,并呈现了公众化的发展趋势。其应用范围日益广泛:从国防军事、教育科研到金融贸易,从远程教育到远程医疗,从政府办公到日常生活,可以说,Internet 使世界成为一个数字地球。

1.1.2 Internet 的主要特点

1. 全球信息浏览

Internet 将世界范围内各个国家和地区的计算机网络联接在一起,网络用户可以方便地与本地、异地的其他网络用户进行信息通信。通过 Internet

网络，人们能够及时地获取世界各地的政治、经济、教育、文化、科学、技术、生活、娱乐等各方面的最新信息。

2. 信息查询方便快捷

Internet 的用户界面独立于网络，用户在使用 Internet 时无需了解网络底层结构以及网络互联的情况。用户可以通过各种网络工具，方便快捷地查询、获取和传递网络信息。

3. 接入方式灵活多样

Internet 是基于 TCP/IP 通信协议的网络，不同网络、不同类型的计算机只要采用 TCP/IP 协议，就可实现与 Internet 的联接。Internet 提供了各种不同的接入方式，包括终端仿真方式、拨号接入方式、宽带接入方式等，用户可以根据自身需要灵活地进行选绎。

4. 费用低廉

各国政府都注重“信息高速公路”的建设，通过多种政策和措施来推动 Internet 的发展。Internet 的服务收费较低，并且随着网络通信技术的发展呈现继续下降的趋势。

1.2　计算机网络的软件和硬件

介绍完 Internet 后，我们来看一看以 Internet 为代表的计算机网络究竟是如何工作的。要想实现网络通信功能，则软件和硬件两部分的协调工作是最基本的前提。

1. 网络软件

网络软件是挖掘网络潜力的工具，为了协调网络系统资源，系统需要通过软件工具对网络资源进行全面管理、调度和分配，并采取一系列的安全保密措施，防止用户对数据和信息的不合理访问，避免数据和信息被破坏和丢失。网络软件研究的重点不是网络中互联的各个独立的计算机本身的功能，而是如何实现网络特有的功能。网络软件通常包括以下几种：

(1)网络协议和协议软件：主要是通过协议程序实现网络协议的功能，如 TCP/IP。

(2)网络通信软件:实现网络中各种设备之间进行通信的软件。

(3)网络操作系统:用以实现资源共享、管理用户等不同资源访问的应用程序。

(4)网络管理及网络应用软件:网络管理软件是用来对网络资源进行管理和对网络进行维护的软件;网络应用软件是为网络用户提供服务并为网络用户解决实际问题的软件。

2. 网络硬件

网络硬件的选择对网络起着决定性的作用,它们是计算机网络系统的物质基础。要构建一个计算机网络,首先要将计算机及其附属硬件设备与网络中的其他计算机系统联接起来。随着计算机技术和网络技术的发展,网络硬件也日渐多样化,功能更加强大。计算机网络硬件组成主要包括主体设备、联接设备及通信信道等。

(1)终端主体设备(Host):一般又可分为工作站(客户机)和中心站(服务器)两类,工作站一般对设备的指标参数和配置要求不是很高,多采用 PC 及携带相应的外部设备;中心站则要选择高档次的机型,对其工作速度、硬盘和内容容量和携带的外部设备要求也相对较高。

(2)联接设备:网络的联接设备有很多种类型,不同规模、不同类型的网络所采用的联接设备也是有区别的。一般而言,用于网络的联接设备主要有网络适配器(网卡)、集线器、复用器、中继器、网桥、交换机、路由器和网关等。

(3)通信信道:计算机网络使用的信道,可分为有线信道和无线信道两种。有线信道包括电缆、双绞线、光纤等;无线信道包括红外线、微波等。

1.3 计算机网络的分类

1. 按网络的交换功能分类

(1)电路交换网:以电话系统为模式。在使用面向联接的服务时,必须经过三个步骤:即建立联接、数据通信和释放联接。当使用电路交换来传送计算机数据时,传输效率往往很低,线路上真正用于传送数据的时间往往不

到 10%，甚至不到 1%。

(2)分组交换网：目前 Internet 所采用的类型，它的主要特点是在发送方将长的数据报分成小片，各自加上首部控制信息(例如源地址、目的地址等)，然后每片独立地查找路由发送出去。这样做的好处在于发送方可以非常及时地将数据送入网络中，并且一旦网络出现故障，不至于整个用户数据全部损毁，从而提高了生存性。但这种方式也带来了一些问题，例如增加了首部开销，以及因为小片分组的丢失而造成在接收端无法将整个报文正确地拼接。

2. 按地理范围分类

(1)局域网(Local Area Network，LAN)：约 0.1km；

(2)校园网(Campus Area Network，CAN)：约 1km；

(3)城域网(Metropolitan Area Network，MAN)：约 10km；

(4)广域网(wide Area Network，WAN)：100～1000km；

(5)全球网(Global Area Network，GAN)：大于 1000km。

3. 按照网络拓扑结构分类

(1)星形网：星形拓扑是以中央节点为中心与其他各节点联接组成的，各节点与中央节点通过点到点的方式联接，如图 1-1(a)所示。中心采用集中式通信控制策略，任何两个节点要进行通信都必须经过中央节点控制。

(2)环形网：环形拓扑是由节点和联接节点的链路组成的一个闭合环，每个节点的接口设备是有源的。任何节点均可以请求发送信息，请求一旦被批准，便可以相环路发送信息，如图 1-1(b)所示。环形网络中的数据传输主要是单向的，也可以是双向传输。由于环线是公用的，因此一个节点发出的信息必须穿越环中所有的环路接口。当信息流中的目的地址与环上某节点地址相符时，信息被该节点的环路接口所接收，然后，信息继续流向下一环路接口，一直流回到发送该信息的环路接口节点位置。

(3)总线网：总线拓扑采用总线电缆作为公用信道，所有节点都通过相应的硬件接口直接联接到总线上，如图 1-1(c)所示。在总线型拓扑结构中，任何一个节点的信息都可以沿着总线向两个方向传输扩散，并且能被总线上任何一个节点接收。由于其信息向两个方向传播，很适用于广播发送，所以也被称为广播式网络。总线上传输信息通常以基带形式串行传递，每

个节点上的网络接口板硬件均具有收发功能。接收器负责接收总线上的串行信息并将其转换成并行信息送到计算机工作站；发送器是将并行信息转换成串行信息广播并发送到总线上。当总线上发送信息的目的地址与某个节点的接口地址相符合时，该节点的接收器便接受信息。

(4)树形网：树型拓扑的形状像一棵倒置的树，顶端是树根，以下是分支节点，如图 1－1(d)所示。各节点按层次进行联接，信息交换主要在上、下节点之间进行，相邻及同层节点之间一般不进行数据交换或数据交换量比较少。树型网是一种分层网，一般一个分支和节点的故障不影响另一分支和节点的工作，任何一个节点送出的信息都可以传遍整个网络站点，是一种广播式网络。一般树型网上的链路相对具有一定的专用性，无需对原网做任何改动就可以扩充工作站。

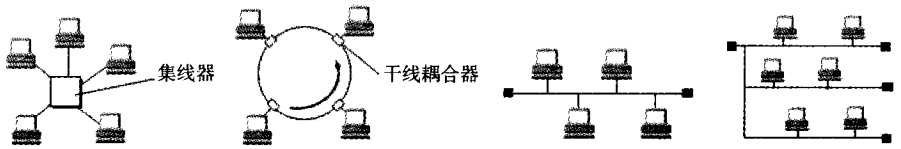

图 1－1　网络拓扑结构

1.4　计算机网络体系结构

计算机网络的体系结构(architecture)是计算机网络的各层及其协议的集合。为什么要分层来完成网络通信呢？这是因为相互通信的两个计算机系统必须高度协调工作才能实现相互通信，然而这种“协调”是相当复杂的，需要解决的问题很多，而且一旦出现故障，则很难排查。分层可将庞大而复杂的问题，转化为若干较小的局部问题，而这些较小的局部问题就比较易于研究和处理。那么究竟将整个网络体系分成几层才合适呢？

国际标准化组织将网络体系分成七层，如图 1－2(a)所示。七层体系虽然概念清楚，理论也较完善，但它过于复杂，导致网络的铺设成本大大提高，

而且其中某些层划分的也不尽合理，相邻层之间也有一定的重复，所以目前并没有得到广泛地推广。TCP/IP 体系结构正好相反，它抛弃了所以有不必要的元素，结构简单、实用、成本低廉，所以得到了广泛的应用，成为实际上的 Internet 标准。TCP/IP 是一个四层的体系结构，如图 1－2(b)所示，它包含应用层、运输层、网际层和网络接口层。

本书综合了 OSI 体系结构和 TCP/IP 体系结构的优点，采用一种五层协议的体系结构，即应用层、运输层、网络层、数据链路层和物理层，如图 1－2(c)所示。

(a) OSI模型　　(b) TCP/IP模型　　(c) 五层协议模

图 1－2　三种不同的协议体系结构

下面分别对五层协议做简单的说明：

(1)应用层：应用层是体系结构中的最高层。应用层直接为用户的应用进程服务。在因特网中，应用层的协议是最多的，因为要为不同的应用软件服务，例如 HTTP，SMTP，FTP 等。

(2)运输层：也叫传输层，它的主要任务就是负责向终端主机对等进程的通信提供服务。由于一个主机可同时运行多个进程，因此运输层有复用和分用的功能。复用就是多个应用层进程可同时使用下面运输层的服务，分用则是运输层把收到的信息分别交付给上面应用层中的相应的进程。

(3)网络层：网络层负责为分组交换网上的不同主机提供通信服务。在发送数据时，网络层把运输层产生的报文段或用户数据报封装成分组(packet)进行传送。网络层的另一个重要功能就是要选择合适的路由，通过网络中的路由器找到目的主机。

(4)数据链路层：通常简称为链路层。数据链路层的作用是解决在两个

相邻节点之间(主机和路由器之间或两个路由器之间)进行点对点的传输数据时,帧的封装、定界以及透明的传输和接收比特流数据等功能。

(5)物理层:物理层的主要任务是确定与传输媒体的接口的一些特性,包括:

- 机械特性。指明接口所用接线器的形状和尺寸、引线数目和排列、固定和锁定装置等等。
- 电气特性。指明在接口电缆的各条线上出现的电压的范围。
- 功能特性。指明某条线上出现的某一电平的电压表示何种意义。
- 规程特性。指明对于不同功能的各种可能事件的出现顺序。

第2章 关于物理层的研讨

2.1 物理层的基本概念辨析

物理层位于OSI参考模型的最底层，它是直接面向实际承担数据传输的物理媒体。物理层是指在物理媒体之上为数据链路层提供一个原始比特流的物理联接。现有的计算机网络中的物理设备和传输媒体的种类繁多，而通信手段也有多种不同方式，物理层的作用正是要尽可能地屏蔽掉这些差异，使物理层上面的数据链路层感觉不到这些差异，这样可使数据链路层只需要考虑如何完成本层的协议和服务，而不必考虑网络具体的传输媒体是什么。这里，用于物理层的协议通常称为物理层规程。

2.1.1 数据通信的基本概念

在数据通信系统中，信道是传送信号的通路。信号分为模拟信号和数字信号，模拟信号即连续的信号，如话音信号和目前的广播电视信号；数字信号即离散的信号，如计算机通信所用的二进制代码1和0组成的信号。

从通信的双方信息交互的方式来看，可以有以下三个基本方式。

(1)单向通信：又称单工通信，即只能有一个方向的通信，而没有反方向的交互。无线电广播、有线电广播以及电视广播就属于这种类型。

(2)双向交替通信：又称半双工通信，即通信的双方都可以发送信息，但不能双方同时发送(或同时接收)，这种通信方式往往是一方发送另一方接收，一般用于计算机网络的非主干线路中。

(3)双向同时通信：又称全双工通信，即通信双方可以同时发送和接收

信息。如现代电话通信提供了全双工传送。这种通信方式主要用于计算机与计算机之间的通信。

信道的传输能力是有一定限制的，某个信道传输数据的速率有一个上限，叫做信道的最大传输速率，即信道容量。信道的最大传输速率是与信道带宽有直接联系的。信道上传输的是电磁波信号，某个信道能够传送电磁波的有效频率范围就是该信道的带宽。数据通信系统的信道传输的是电磁波（包括无线电、微波、光波等），带宽就是它所能传输电磁波的最大有效频率与最小有效频率之差。信道上传送的信号还可以分为以下两个基本方式。

（1）基带信号：基带是一种传输形式，其中，数字信号通过直流脉冲被发送，这种直流形式需要独占电线的容量。因此，基带系统一次仅能传输一个信号。基带系统中的每个设备都共享相同的信道。当基带系统上一个节点在传输数据，网络中所有的其他节点在发送数据前必须等待前面的传输结束。

（2）宽带信号：将基带信号进行调制后形成的频分复用模拟信号，基带信号进行调制后，其频谱被搬移到较高的频率处，由于每一路基带信号的频谱被搬移到不同的频段，因此合在一起后并不会互相干扰。

2.1.2 数据通信系统模型

数据通信是依照通信协议，利用数据传输技术在两个功能单元之间传递数据信息。它可以实现计算机与计算机、计算机与终端以及终端与终端间的数据信息传递。

数据通信是计算机与通信相结合而产生的一种通信方式和通信业务，其基本作用是完成两个实体间的数据交换。图 2-1 是通信系统的一个实例，工作站可以通过公共电话网与另一端的服务器通信，也可以在公共电话网间交换声音信号。

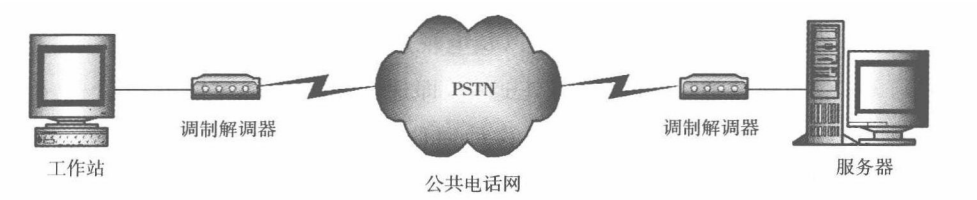

图 2-1 通信系统实例