JISUANJI WANGLUO
JIQI XINXI ANQUAN GUANLI YANJIU

计算机网络及其信息安全管理研究

董建刚　著

吉林科学技术出版社

计算机网络及其信息安全管理研究

董建刚　著

吉林科学技术出版社

图书在版编目(CIP)数据

计算机网络及其信息安全管理研究 / 董建刚著. —
长春：吉林科学技术出版社，2019.5
ISBN 978-7-5578-5496-6

Ⅰ. ①计… Ⅱ. ①董… Ⅲ. ①计算机网络—信息安全
—研究 Ⅳ. ①TP393.08

中国版本图书馆 CIP 数据核字(2019)第 106178 号

JISUANJI WANGLUO JIQI XINXI ANQUAN GUANLI YANJIU

计算机网络及其信息安全管理研究

著　董建刚
出 版 人　李　梁
责任编辑　李思言
封面设计　马静静
制　版　北京亚吉飞数码科技有限公司
开　本　710mm×1000mm　1/16
字　数　233 千字
印　张　18
印　数　1—5 000 册
版　次　2020 年 3 月第 1 版
印　次　2020 年 3 月第 1 次印刷

出　版　吉林科学技术出版社
发　行　吉林科学技术出版社
地　址　长春市人民大街 4646 号
邮　编　130021
发行部传真/电话　0431—85635176　85651759　85635177
85651628　85652585
储运部电话　0431—86059116
编辑部电话　0431—85635186
网　址　www.jlsycbs.net
印　刷　三河市铭浩彩色印装有限公司

书　号　ISBN 978-7-5578-5496-6
定　价　70.00 元

前　言

随着 Internet 在全球的普及和发展，计算机网络成为信息的主要载体之一。计算机网络的全球互联趋势越来越明显，其应用范围日渐普及和广泛，应用层次逐步深入。国家发展、社会运转以及人类的各项活动对计算机网络的依赖性越来越强。计算机网络已经成为人类社会生活不可缺少的组成部分。

与此同时，随着网络规模的不断扩大和网络应用的逐步普及，网络安全问题也越发突出，受到越来越广泛的关注。计算机和网络系统不断受到侵害，侵害形式日益多样化，侵害手段和技术日趋先进和复杂化，已经严重威胁到网络和信息的安全。一方面，计算机网络提供了丰富的资源以便用户共享；另一方面，资源共享度的提高也增加了网络受威胁和攻击的可能性。事实上，资源共享和网络安全是一对矛盾，随着资源共享的加强，网络安全问题也日益突出。计算机网络的安全已成为当今信息化建设的核心问题之一。

本书的特点是将网络安全理论、网络安全协议和主流网络安全技术有机集成在一起。既能让读者掌握完整、系统的网络安全理论，又能让读者具备运用网络安全协议和主流网络安全技术解决实际网络安全问题的能力。理论阐述严谨、透彻，技术讨论翔实、细致。在撰写过程中，融入学科方法论，倡导科学的思维方法，通过大量的图表，形象直观地讲解了知识概念。

本书以网络面临的常见安全问题以及相应的检测和防护为主线，系统地介绍了网络安全的基本概念、理论基础、安全技术及其应用。全书共分 8 章，第 1 章为计算机网络概述，第 2 章为计

算机网络体系基础，第 3 章为计算机局域网，第 4 章为计算机网络安全，第 5 章为数据加密技术，第 6 章为防火墙技术，第 7 章为计算机病毒与防治，第 8 章为网络攻击与入侵检测。

本书的撰写凝聚了作者的智慧、经验和心血，在撰写过程中参考并引用了大量的书籍和文献，在此向这些专家、编辑及文献原作者表示衷心的感谢。由于作者水平所限以及时间仓促，书中难免存在一些不足和疏漏之处，敬请广大读者和专家给予批评指正。

作　者

2018 年 3 月

目　录

第 1 章　计算机网络概述

计算机网络是利用通信线路把地理位置上分散的计算机和通信设备连接起来，在系统软件和协议的支持下，以实现数据通信和资源共享为目的的复杂计算机系统。网络的基本资源包括硬件资源、软件资源和数据资源等。网络的广泛应用，使得网络与人们的生活、工作密切相关，网络已经成为维系社会正常运作的支柱。网络中的信息事关企业甚至国家的发展，因此，网络和网络信息的安全已经事关个人、企业，甚至国家的安危。

1.1　计算机网络的形成与发展

1.1.1　通信网络的形成与发展

通信网络的形成与发展可以追溯到 20 世纪 50 年代。这个阶段的特点与标志性成果主要表现在：

①数据通信技术日趋成熟，为计算机网络的研究奠定了技术基础。

②分组交换概念的提出为计算机网络的形成奠定了理论基础。

③ARPANET 的成功运行证明了分组交换理论的正确性。

④TCP/IP 协议的广泛应用为更大规模的网络互联奠定了坚实的基础。

1.1.2 互联网的形成与发展

互联网的形成与发展可以追溯到20世纪90年代初期。这个阶段的特点与标志性成果主要表现在：

①E-mail、FTP、TELNET、DNS等应用展现出计算机网络广阔的应用前景。

②NSFNET允许商业应用，加快了Internet形成的速度。

③Web技术的出现促进了电子商务、电子政务、远程医疗与远程教育应用的发展。

④全球信息高速公路的建设与大规模的用户接入使互联网进入高速发展阶段。

1.1.3 移动互联网的形成与发展

移动互联网的形成与发展可以追溯到20世纪90年代末。这个阶段的特点与标志性成果主要表现在：

①移动IP技术与无线通信技术的研究为移动互联网的发展奠定了技术基础。

②移动通信网与互联网业务的融合为移动互联网开辟了广阔的发展空间。

③智能手机、平板计算机与可穿戴计算设备的应用促进了移动网络应用的快速发展。

④移动互联网应用成为信息产业新的增长点。

1.1.4 物联网的形成与发展

物联网的形成与发展开始于2010年前后，这个阶段的特点与标志性成果主要表现在：

①物理世界与网络世界融合的需求促进了物联网概念的形成与研究的发展。

②感知技术、智能技术的发展与应用为物联网的发展奠定了坚实的基础。

③物联网被列为我国优先发展的战略性新兴产业之一。

④物联网的发展为计算机网络技术的研究提供了更大的发展空间。

综上所述，我们可以清晰地得出以下两点结论：

第一，计算机网络正在沿着“互联网-移动互联网-物联网”的轨迹，“由小到大”地发展、壮大，“由表及里”地渗透到社会的各个角落，遵循“互联网＋”的模式，在与各行各业的跨界融合中，推动着我国社会和国民经济的发展。

第二，如果说互联网的作用是扩大了信息社会人与人之间信息共享的广度，移动互联网的作用是扩大了信息共享的深度与灵活性，那么物联网则是利用传感器、无线传感器网络与射频标签(RFID)等感知技术，将人与人的互联扩大到人与物、物与物的互联，使人类对外部世界具有“更全面的感知能力、更广泛的互联互通能力、更智慧的处理能力”。

1.2　计算机网络定义与分类

1.2.1　计算机网络定义

1. 计算机网络的定义要点

人们根据计算机网络发展的不同阶段或者从不同的角度对计算机网络提出了不同的定义，这些定义反映了当时的计算机网络技术发展水平以及人们对网络的认知程度。其中资源共享的观点能够比较准确地描述计算机网络的特征，被广泛地接受和使用，从资源共享的观点将计算机网络定义为“以能够相互共享资

源的方式互联起来的自治计算机系统的集合”，但是这个定义侧重应用，没有指出网络的结构，因此不够全面。本书采用以下定义：“将地理位置不同的两台以上的具有独立功能的计算机通过通信设备和通信介质连接起来，以功能完善的网络软件实现资源共享的计算机系统。”

这个定义从四个方面描述了计算机网络：

①网络中必须有两台以上的计算机，地理位置不限，机型不限。所谓独立功能是指这个计算机自己可以独立工作，有数据处理能力，不是一定依赖于网络才能工作。这一点很关键，现代计算机网络强调的是功能独立的计算机之间的互联，按照这样的观点，早期的主机-终端型的网络以及无盘工作站连接而成的网络不属于现代计算机网络。

②联网计算机系统是相互独立的自治系统。网络中每台计算机的硬件、软件与数据资源可以在各自操作系统的控制下离线独立工作。联网计算机在操作系统的内核中增加实现网络通信协议的软件（如 Ethernet 网卡驱动程序与 TCP/IP 协议软件）构成网络操作系统。联网计算机之间通过网络操作系统之间的进程通信，来实现互联计算机系统之间的协同工作。

③计算机之间要通过通信介质和通信设备互连。通信介质包括双绞线、光纤、同轴电缆、无线介质等，通信设备包括路由器、交换机、网桥、集线器等。只有互连才能够将一台计算机上的信号传输到另一台计算机上。

④网络中要有网络软件。网络软件主要有三类，第一类是网络协议软件，联网的计算机以及通信设备必须遵守相同的协议；第二类是网络操作系统，通过网络操作系统对网络进行管理和控制，实现各种服务功能；第三类是网络应用软件，帮助用户访问网络，为用户使用网络服务功能提供便利。

⑤联网的目的是实现资源共享，计算机网络中的资源包括硬件资源和软件资源，联网后，用户可以通过自己的计算机使用网络上其他计算机上的硬件和软件资源。

2. Computer Network、internet、Internet 与 Intranet 的区别与联系

在讨论计算机网络基本概念时，需要注意术语 Computer Network、internet、Internet 与 Intranet 的区别与联系。

①计算机网络(Computer Network)表示的是用通信技术将大量独立的计算机系统互联起来的集合。计算机网络有各种类型，如广域网、城域网、局域网或个人区域网。

②网络互联(internet，internetworking)表示的是将多个计算机网络互联成大型的网络系统。

③Internet 或因特网、互联网是专用名词，专指目前广泛应用、覆盖了全世界的大型网络系统。因此 Internet 不是一个单一的广域网、城域网或局域网，而是由很多种网络互联起来的网际网。

④随着 Internet 的广泛应用，一些大型企业、管理机构也采用了 Internet 的组网方法，采用 TCP/IP 与 Web 的系统设计方法，将分布在不同地理位置的部门局域网互联成企业内部的专用网络系统，供内部员工办公使用，不连接或不直接连接到 Internet，这种内部的专用网络系统称为 Intranet。

1.2.2　计算机网络的分类

按网络覆盖的范围划分，可将网络分为广域网(Wide Area Network，WAN)、城域网(Metropolitan Area Network，MAN)、局域网(Local Area Network，LAN)。

1. 广域网

(1)广域网的基本概念

广域网(WAN)又称为远程网，所覆盖的地理范围从几十千米到几千千米，它可以将分布在不同地区的计算机系统连接起

来，达到资源共享的目的。广域网一般是公用网络，采用网状拓扑结构，用户以租用专线的方法来使用。

初期广域网的设计目标是将分布在很大地理范围内的若干台大型机、中型机或小型机互联起来，用户通过连接在主机上的终端访问本地主机或远程主机的计算与存储资源。随着 Internet 应用的发展，广域网作为核心主干网的地位日益清晰，广域网的设计目标逐步转移到将分布在不同地区的城域网、局域网互联起来，构成大型互联网络系统。

(2)广域网的主要技术特征

早期的广域网主要用于大型计算机系统与中小型计算机系统的互联。大型或中小型计算机的用户终端接入到本地计算机系统，本地计算机系统再接入到广域网中。用户通过终端登录到本地计算机系统之后，才能实现对异地联网的其他计算机系统中的硬件、软件或数据资源进行访问和共享。针对这样一种工作方式，人们提出了“资源子网”与“通信子网”的概念。随着互联网应用的发展，广域网更多的是作为覆盖地区、国家、洲际地理区域的核心交换网络平台。

目前，大量的用户计算机通过局域网或其他接入技术接入到城域网，城域网接入到连接不同城市的广域网，大量的广域网互联形成了 Internet 的宽带核心交换平台，从而构成了具有层次结构的大型互联网络。因此，用描述单个广域网的通信子网与资源子网的两级结构概念，已不能准确地描述当前互联网网络结构。

随着网络互联技术的发展，广域网作为互联网的宽带核心交换平台，其研究的重点已经从开始阶段的“如何接入不同类型的异构计算机系统”，转变为“如何提供能够保证服务质量(Quality of Service，QoS)的宽带核心交换服务”。因此，广域网研究的重点是“保证 Qos 的宽带核心交换”技术。

2. 城域网

20 世纪 80 年代后期，IEEE 802 委员会提出了城域网的概

念：以光纤为传输介质，能够提供 45～150 Mbps 高传输速率，支持数据、语音与视频综合业务的数据传输，可以覆盖 50～100 km 的城市范围，实现高速数据传输。

宽带城域网是以 IP 为基础，通过计算机网络、广播电视网、电信网的三网融合，形成覆盖城市区域的网络通信平台，为语音、数据、图像、视频传输与大规模的用户接入提供高速与保证质量的服务。

如果说广域网设计的重点是保证大量用户共享主干通信链路的容量，那么城域网设计的重点是交换节点的性能与容量。城域网的每个交换节点都要保证大量接入用户的服务质量。当然，城域网连接每个交换节点的通信链路带宽也必须得到保证。因此，不能简单地认为城域网是广域网的缩微，也不能简单地认为城域网是局域网的自然延伸。宽带城域网应该是一个在城市区域内，为大量用户提供接入和各种信息服务的高速通信网络。

宽带城域网的结构特点需要从功能结构与网络层次结构两个方面来认识。宽带城域网的功能结构由“三个平台与一个出口”构成，即管理平台、业务平台、网络平台，以及城市宽带出口。图 1-1 给出了宽带城域网的功能结构示意图。

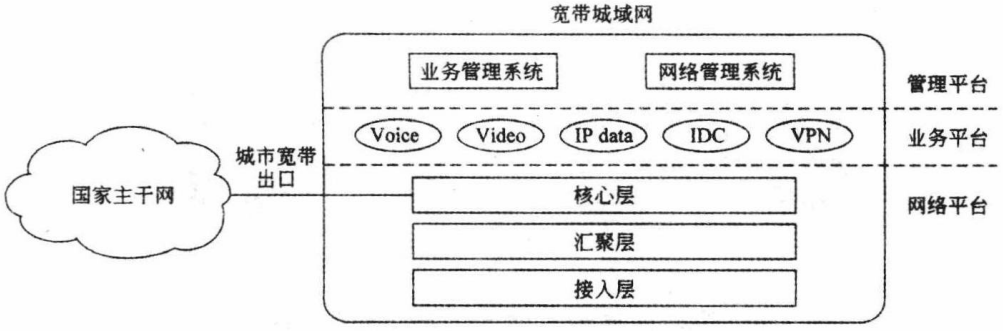

图 1-1　宽带城域网的功能结构①

①管理平台。组建的宽带城域网一定是可管理的。作为一个实际运营的宽带城域网，需要有足够的网络管理能力。管理平

① 吴功宜，吴英．计算机网络[M]．4 版．北京：清华大学出版社，2017.

台的作用主要表现在用户认证与接入管理、业务管理、网络安全、计费能力、IP 地址分配与 QoS 保证等方面。

②业务平台。组建的宽带城域网一定是可赢利的。宽带城域网的业务平台可以为用户提供 Internet 接入业务、虚拟专网业务、话音业务、视频与多媒体业务、内容提供业务等。

③网络平台。宽带城域网的网络平台结构是由核心交换层、边缘汇聚层与用户接入层组成。

④城市宽带出口。组建城域网一个重要的目的是满足一个城市地区范围内各类用户接入 Internet 的需求，城市宽带出口是连接城域网与地区级或国家级主干网，进而接入 Internet 的重要通道。

图 1-2 给出了典型的宽带城域网的网络层次结构示意图。采用层次结构的优点是结构清晰，各层功能实体之间的定位明确，接口开放，标准规范，便于组建和管理。

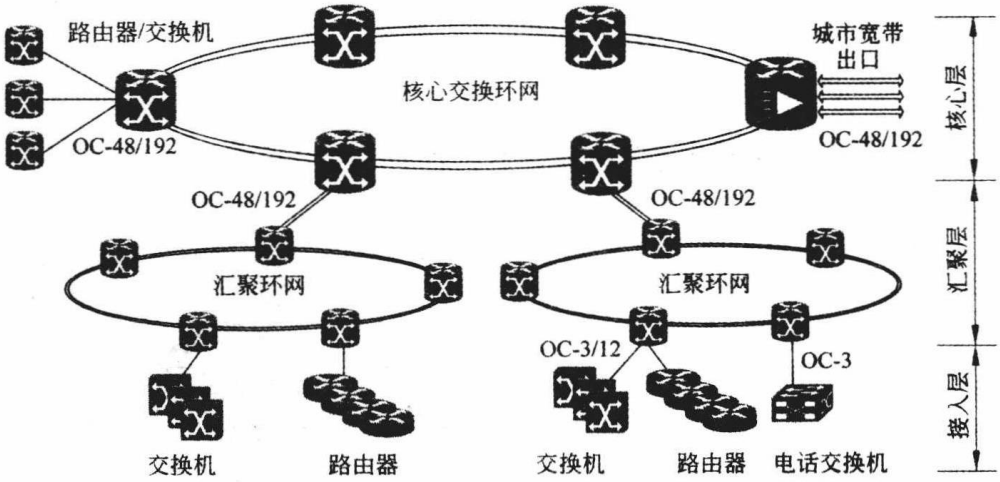

图 1-2　典型的宽带城域网的网络层次结构示意图

3. 局域网

局域网用于将有限范围内(如一个办公室、一幢大楼、一个校园、一个企业园区)的各种计算机、终端及外部设备连接成网络，彼此高效地共享资源，例如共享文件和打印机。

局域网有以下技术特点：

①覆盖范围有限，一般覆盖几公里。

②结构简单，容易实现。

③速度快，其数据传输速率可以达到 10～10 000 Mbps。

④私有性，局域网都是由企业或学校自己出资建设，供单位内部使用。

当然，局域网与广域网不仅仅在覆盖范围上不同，更重要的是二者使用的网络技术也是完全不同的，广域网主要采用分组交换技术，而局域网则采用广播或帧交换技术。

1.3　计算机网络的组成与结构

1.3.1　现代计算机网络结构

早期的计算机网络的资源子网由主机、终端、信息资源组成，通信子网主要由通信控制处理机和通信线路组成。早期的计算机主要是指大型计算机、中型计算机或小型计算机，用户通过连接在主机上的终端去访问本地主机与远程主机。联网主机主要有两个基本的功能：一是为本地的终端用户提供服务；二是通过通信线路与路由器连接，完成计算机之间的数据交互功能。随着微型机的普及和局域网的大量使用，现在的计算机网络资源子网以局域网、微型机以及信息资源为主，主机-终端型的用户在不断减少，通信子网则由路由器、交换机和通信线路组成。

由于现在的计算机几乎都要连入网络，企业、学校、政府等机构的计算机要先连成局域网，然后再接入因特网，个人家庭的计算机也要通过某种专线接入因特网，因此从宏观上看，全世界的计算机都通过因特网连在一起，组成一个覆盖全球的“大网”，其基本结构如图 1-3 所示。

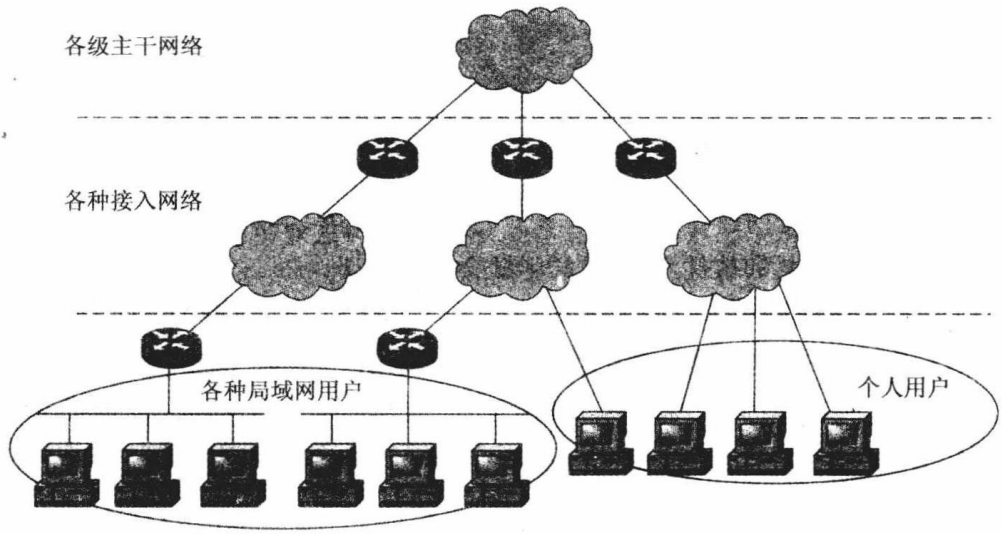

图 1-3　现代计算机网络结构

1.3.2　ISP 的层次结构

1. ISP 的基本概念

Internet 是由分布在世界各地的广域网、城域网、局域网通过路由器互联而成的。从网络结构角度看，Internet 是一个结构复杂并且在不断变化的网际网。同时，Internet 并不是由任何一个国家组织或国际组织来运营，而是由一些私营公司分别运营各自的部分。用户接入与使用的各种网络服务都需要经过 Internet 服务提供者(Internet Service Provider，ISP)提供。ISP 运营商向 Internet 管理机构申请了大量的 IP 地址，铺设了大量的通信线路，购置了高性能路由器与服务器，组建了 ISP 网络，提供接入服务。

ISP 一般是根据流量向用户收取费用。只要家庭用户或企业用户向 ISP 提出申请并交纳一定的费用，ISP 就会为用户提供接入服务，并以动态或静态的方式提供 IP 地址。小的 ISP 运营商可以向电信运营商租用通信线路来提供接入服务。随着 Internet 应用的发展，出现了 Internet 内容提供商(Internet Content Provider，