计算机网络安全理论与实践

李冠楠◎著

吉林大学出版社

佛山市产学研专项资金项目及顺德职业技术学院资助项目《基于人脸识别的企业考勤系统》，项目编号：2012HC100303；省级培育中心、顺德职业技术学院创新强校专项项目《智能制造协同创新中心》，项目编号：2015－KJZX054、2015－KJZX055；广东省自然科学基金项目《定制家具智造系统的设计与开发》

计算机网络安全理论与实践

李冠楠　著

吉林大学出版社

图书在版编目(CIP)数据

计算机网络安全理论与实践 / 李冠楠著. — 长春 : 吉林大学出版社, 2017.3
ISBN 978-7-5677-8970-8

Ⅰ. ①计… Ⅱ. ①李… Ⅲ. ①计算机网络-网络安全-研究 Ⅳ. ①TP393.08

中国版本图书馆 CIP 数据核字(2017)第 044808 号

书　　名　计算机网络安全理论与实践
JISUANJI WANGLUO ANQUAN LILUN YU SHIJIAN

作　　者　李冠楠　著
策划编辑　朱　进
责任编辑　朱　进
责任校对　王文涛　何　静
装帧设计　美印图文
出版发行　吉林大学出版社
社　　址　长春市朝阳区明德路 501 号
邮政编码　130021
发行电话　0431-89580028/29/21
网　　址　http://www.jlup.com.cn
电子邮箱　jlup@mail.jlu.edu.cn
印　　刷　北京市媛明印刷厂
开　　本　787×1092　1/16
印　　张　12
字　　数　200 千字
版　　次　2017 年 4 月第 1 版
印　　次　2017 年 4 月第 1 次
书　　号　ISBN 978-7-5677-8970-8
定　　价　36.00 元

目　录

第一章 计算机网络

第一节 计算机网络的定义和功能

一、计算机网络的定义

计算机网络在不同的发展阶段或从不同的观点看有不同的定义。

ARPA 网建成后，把计算机网络定义为："以相互共享（硬件、软件和数据）资源方式而联结起来，且各自具有独立功能的计算机系统之集合。"这个定义着重于应用目的，而未指出物理结构。当联机终端网络发展到计算机—计算机网时，为了区分前者和后者，从物理结构看，计算机网络被定义为："在网络协议控制下，由多台功能独立的主计算机、若干台终端、数据传输设备以及计算机与计算机间、终端与计算机进行通信的设备所组成的计算机复合系统。"这个定义强调联网的计算机必须具有数据处理能力且功能独立。

目前，一般较公认的计算机网络的定义如下："计算机网络就是利用通信设备和线路将地理位置不同的、功能独立的多个计算机系统互联起来，以功能完善的网络软件实现软件、硬件资源共享和信息传递的系统。"

这里强调了计算机网络是通信技术和计算机技术结合的产物，强调计算机网络是将处在不同地理位置的计算机进行互联，强调互联的计算机主机是具有功能独立的数据处理能力的计算机，强调互联的目的是为了实现信息传输和资源共享。

二、计算机网络的功能

计算机网络的主要目的是为用户提供一个网络环境，使用户能通过计算机网络实现资源共享和信息传递。

(一)资源共享

计算机在广大的地域范围联网后,资源子网中各主机的资源原则上都可共享。计算机网络的共享资源有硬件、软件、数据等。

硬件资源有超大型存储器、特殊的外部设备以及大型、巨型机的 CPU 处理能力等,共享硬件资源是共享其他资源的物质基础。软件资源有各种语言处理程序、服务程序和各种应用程序等。数据资源有各种数据文件、各种数据库等,共享数据资源是计算机网络最重要的目的。

在网络中,资源共享的最典型的例子就是数据中心存储系统、高性能计算中心的计算系统和云计算。数据中心存储系统由具有近百 T 的存储容量,实现企事业单位的数据集中存储、集中管理,各种应用系统的数据都以共享数据中心存储空间的方式存储在数据中心存储系统中。

高性能计算中心由具有每秒上万亿次计算能力的计算系统和相关计算业务软件构成,用户通过网络远程提交计算作业,由计算中心计算系统处理后,将计算结果输出到用户终端。所有需要计算资源的用户都可以通过网络共享高性能计算中心的计算资源。

云计算通过共享的软硬件资源和信息资源实现按用户需求提供服务,是计算机网络资源共享最令人向往的理想实现。

(二)信息传递

计算机网络的另一主要目的是信息传递。通过计算机网络可以实现文件传输、电子邮件和声音、数据、图形和图像等多媒体信息的上传和下载。

计算机网络除了以上两个主要功能外,还有以下一些功能:

1. 提高可靠性

计算机网络一般都属于分布控制方式,如果有单个部件或少量计算机发生故障,可以利用网络上的其他计算机来完成它们要完成的任务。由于相同的资源可分布在不同地方的计算机上,这样,网络可通过不同路由来访问这些资源。计算机网络中的通信双方存在多条路径可达对方,当一条通信链路故障时,从其他路径仍然可达对方,从而大大提高了通信的可靠性。

2. 分布式处理

由于计算机价格下降的速度快,在计算机网络内计算机和通信装置的价格比发生了显著的变化,这使得在计算机网络内部可以充分利用计算机资源,在计算机网络上设置一些专用服务器,专门进行某种业务的处理,把所需的各种处理功能分散到各个计算机网络上,提高处理能力和效率。

3. 改善工作环境条件

电子邮件、QQ 等通信应用使用户可以得到快捷的通信，实现全球快捷的电子通信，使世界范围的通信过程缩短到几分钟的电子过程。利用即时通网络业务，可以轻松实现网上对话、视频聊天、文件传输，获取资讯等网络业务。

利用视频会议系统，可以实现可视电话、网络会议，使远隔千里的人们只要坐在自己办公室的计算机旁就可以和其他网络上的用户进行会议讨论、相互交谈和协商。

利用计算机网络可以实现信息查询，联在网上的每一个信息库，只要是开放的，你都可以通过计算机网络去访问、去查询你所需要的信息。网络的查询使得使用计算机网络可以查询世界任何与 Internet 网相连的计算机上的信息，使世界变成一个全球性的电子图书馆。

尽管以上我们提出了一些计算机网络的功能，事实上，目前的互联网还远远不是我们经常说到的“信息高速公路”。这不仅因为目前互联网的传输速度仍不够快，而且更重要的是互联网还没有定型，还一直在发展、变化。因此，任何对互联网的技术定义也只能是当下的、现时的。与此同时，在越来越多的人加入到互联网中、越来越多地使用互联网的过程中，也会不断地从社会、文化的角度对互联网的意义、价值和本质提出新的理解。

第二节　计算机网络的组成

计算机网络的组成是计算机、计算机外部设备通过由通信设备及线路组成的通信网络进行互联，所以计算机网络可分为由计算机及计算机外部设备组成的资源子网和由通信设备及线路组成的通信子网构成。资源子网负责网络中的数据处理任务，通信子网负责网络中的数据传输任务。

在实际网络中，资源子网由个人终端计算机、PC 服务器、小型机等主机组成，通信子网由调制解调器、数据网接入设备、交换机、路由器等网络设备组成，传输链路由电话线、同轴电缆、无线电线路、卫星线路、微波中继线路、光缆、铜缆等传输介质组成。

如果把资源子网中的计算机、外部设备和通信子网中的通信控制处理机抽象成节点，将通信子网中的传输线路抽象成链路，则计算机网络就是由节点和链路两种元素组成的，即网络节点和通信链路。

网络节点又分为端节点和转接节点。端节点指通信的源节点和目的节点，源节点是传输数据的出发源点，目的节点是传输数据的最终接收点，源节点和目的节点都是由用用户主机等主机设备构成，又称为数据终端设备DTE。转接节点指网络通信过程中起控制和转发信息作用的节点，如程控交换机、集中器、接口信息处理机等，又称为数据通信设备 DCE。通信链路是指传输信息的信道，可以是电话线、同轴电缆、无线电线路、卫星线路、微波中继线路、光纤缆线等传输介质。

计算机网络在逻辑功能上可以划分为两个部分：一部分的主要工作是对数据信息的收集和处理；另一部分则专门负责信息的传输。ARPANET 把前者称为资源子网，后者称为通信子网。

一、计算机资源子网

（一）资源子网的组成

资源子网由拥有资源的主计算机、请求资源的用户终端、终端控制器、联网的外设、各种软件资源及信息资源等组成。

1. 主计算机

主计算机系统简称为主机，它可以是大型机、中型机、小型机、工作站或微机。

主机是资源子网的主要组成单元，它通过高速通信线路与通信子网的通信控制处理机相连接。普通用户终端通过主机连入网内。主要为本地用户访问网络上其他主机设备与资源提供服务，同时要为网中远程用户共享本地资源提供服务。它可以作为主机的一种类型，直接通过通信控制处理机连入网内，也可以通过联网的大、中、小型计算机系统间接连入网内。

2. 终端

终端是用户访问网络的界面。终端一般是指没有存储与处理信息能力的简单输入、输出设备。也可以是带有微处理机的智能终端。智能终端除具有输入、输出信息的功能外，本身还具有存储与处理信息的能力。

3. 网络中的共享设备

网络共享设备一般是指计算机的外部设备。

（二）资源子网的基本功能

资源子网负责全网的数据处理业务，并向网络用户提供各种网络资源和网络服务。

二、通信子网

通信子网主要负责计算机网络内部信息流的传递、交换和控制，以及信号的变换和通信中的相关处理工作，间接地服务于用户。它主要包括网络节点、通信链路、交换机和信号变换设备等软硬件设施。

（一）网络节点

网络节点的作用：

1. 作为通信子网与资源子网的接口，负责管理和收发本地主机和网络所交换的信息，相当于通信控制处理机 CCP；

2. 作为发送信息、接收信息、交换信息和转发信息的通信设备，负责接收其他网络节点传送来的信息并选择一条合适的链路发送出去，完成信息的交换和转发功能。网络节点可以分为交换节点和访问节点两种。

（1）交换节点主要包括交换机、网络互联时用的路由器以及负责网络中信息交换的设备等。

（2）访问节点主要包括连接用户计算机和终端设备的接收器、收发器等通信设备。

（二）通信链路

通信链路是两个节点之间的一条通信信道。链路的传输媒体包括双绞线、同轴电缆、光导纤维、无线电、微波通信、卫星通信等。

（三）信号变换设备

信号变换设备的功能是对信号进行变换以适应不同传输媒体的要求。这些设备一般有将计算机输出的数字信号变换为电话线上传送的模拟信号的调制解调器、无线通信接收和发送器、用于光纤通信的编码解码器等。

三、网络硬件系统和软件系统

与计算机系统相似，计算机网络也是由硬件系统和软件系统两大部分构成的。

（一）网络硬件系统

计算机网络的硬件主要包括主计算机、终端、通信控制处理机、调制解调器、多路复用器、集线器和通信线路等。

1. 主计算机。主计算机负责网络中的数据处理、执行网络协议、进行网络控制和管理等工作，也包括供用户共享访问的数据库的管理，它与其他主

计算机系统联网后构成网络中的主要资源，它既可以是单机系统，也可以是多机系统。

2. 终端。终端是用户访问网络的设备，一般具有键盘和显示及打印功能，也可以是汉字输入/输出终端、智能终端、虚拟终端等。终端的主要作用是把用户输入的信息转变为适合传送的信息传送到网络上，或把网络上其他节点输出的经过通信线路的信息转变为用户所能识别的信息。

3. 通信控制处理机。通信控制处理机也称为通信控制器，在某些网络中也称为前端处理机、接口信息处理机等，它是一种在数据通信系统或计算机网络系统中执行通信控制与处理功能的专用计算机，通常由小型机或微型机组成，大型网络采用专用通信设备，其主要作用就是承担通信控制和管理工作，减轻主机负担。

4. 调制解调器。调制解调器是把数据终端设备与模拟通信线路连接起来的一种接口设备。调制解调器的种类很多，有基带的、宽带的，无线的、有线的，音频的、数字的，低速的、高速的，同步的、异步的等，一般常用的就是利用电话线作为传输介质的音频调制解调器。

5. 多路复用器。采用多路复用技术可使多个信号共用一个通道，这样就能使信道容量尽可能地被充分利用。利用多路复用器可实现多路信号的同时传输，提高信道利用率。

6. 通信线路。通信线路是传输信息的载波媒体。通信线路也称为通信信道或通信链路。计算机网络中的通信线路有有线线路和无线线路。

7. 网络互联设备。现在大多数网络都是由一种或多种网络互联设备将两个或两个以上的网络连接起来，构成一个更大的互联网络系统。常用的网络互联设备有网桥、路由器、交换机和网关等。

（二）计算机网络软件

利用计算机网络进行通信时，需要控制信息传送的协议以及其他相应的网络软件。计算机网络软件是实现计算机网络功能所不可或缺的软环境。这是因为仅仅使用硬件进行通信就好像用 0 和 1 进行 M 进制编程那样难以实现。

1. 网络操作系统

网络操作系统是网络的心脏和灵魂，是向网络中的计算机提供数据通信和资源共享功能的操作系统。网络操作系统运行在网络硬件之上，为网络用户提供共享资源管理服务、基本通信服务、网络系统安全服务及其他网

络服务。

网络操作系统与运行在工作站上的单用户操作系统或多用户操作系统因提供的服务类型不同而有所差别。一般情况下,计算机操作系统,如 DOS 和 OS/2 等,目的是让用户与系统及在此操作系统上运行的各种应用之间的交互作用最佳。而网络操作系统以使网络相关特性最佳为目的,如共享数据文件、应用软件以及共享硬盘、打印机、调制解调器、扫描仪和传真机等。

目前,有三大主流计算机网络操作系统:Windows NT、Linux 和 UNIX 等,另外,还有 Netware 类。

(1)Windows NT 类。微软公司的 Windows 系统不仅在个人操作系统中占有绝对优势,在网络操作系统中也具有非常强劲的力量。这类操作系统配置局域网时最为常见,但由于对服务器的硬件要求较高,且稳定性能不是很高,所以微软的网络操作系统一般只用在中低档服务器中,高端服务器通常采用 UNIX,Linux 或 Solaris 等非 Windows 操作系统。在局域网中,微软的网络操作系统主要有 Windows NT 4.0 Server、Windows 2000 Server/Advanced Server,以及 Windows 2003 Server/Advanced Server,包括个人操作系统 Windows 9x/ME/XP 等。这些操作系统可运行在微型机和工作站上,支持客户—服务器结构。

(2)Linux。Linux 是一种新型的网络操作系统,最大的特点是源代码开放,可以免费得到许多应用程序。目前也有中文版本的 Linux,如 Redhat、红旗 Linux 等。在安全性和稳定性方面,Linux 得到了用户的充分肯定。

(3)UNIX 系统。UNIX 网络操作系统历史悠久,拥有丰富的应用软件支持,功能强大,其良好的网络管理功能已为广大网络用户所接受。UNIX 采用一种集中式分时多用户体系结构,稳定和安全性能非常好。由于它是针对小型机主机环境开发的操作系统,多数以命令方式进行操作,不容易掌握,特别是初级用户。因此,UNIX 一般用于大型网站或大型企、事业单位的局域网,小型局域网基本不使用。

(4)Netware 类。在局域网中,Netware 操作系统早年曾雄霸一方,现在气势虽然已经失去,但仍以对网络硬件的要求较低而受到一些用户的青睐。常用版本有 Netware3.11、Netware3.12 和 Netware4.10、Netware4.11、Netware5.0 等中英文版本。由于 Netware 服务器对无盘工作站和游戏的支持较好,常用于教学网和游戏厅。

总的来说,对特定计算机环境的支持使得每一个网络操作系统都有适

合于自己的工作场合，这就是系统对特定计算机环境的支持。

2. 网络协议通信软件

为了在各网络单元之间进行数据通信，通信的双方必须遵守一套能够彼此理解、全网一致遵守的网络协议，而网络协议靠具体网络协议软件的运行支持才能工作，因此，凡是连入计算机网络的服务器和工作站都必须运行相应的网络协议通信软件。

综上所述，我们可以进一步加深对计算机网络的认识：计算机网络是运行在传输主干网之上，由用户资源子网和通信传输子网组成的一类业务网，它承载着数据交换和资源共享的任务，是国家信息基础设施中重要的组成部分。

第三节　计算机网络的分类

计算机网络可以按地域范围、拓扑结构、交换技术、有线、无线等进行分类。

一、按地域范围分类

按地域范围分类，计算机网络可以分为局域网、城域网、广域网。

局域网的地域范围仅在几十米到几千米，主要是一个工作室、一栋大楼、一个园区范围内的网络。

城域网的地域范围仅在一个城市内的距离，100 公里以内。主要是一个城市的专门机构的网络。如每个城市的大学网络、中学网络以及政府有关管理机构的专用网络等。

广域网的地域范围是互联网络的概念，指各个城市、各个省乃至各个国家互联的网络。广域网一般要借助电信覆盖全国、全省的网络实现各个城市、各个局域网之间的互联，所以广域网主要是电信运营商的网络。

二、按拓扑结构分类

网络中的连接模式叫作网络的拓扑结构。为了方便研究网络的拓扑结构，将网络中的主机、外部设备和通信控制处理机用抽象的节点来表示，将通信线路抽象成链路线段来表示。在网络中负责信息处理的计算机、服务器等统称为数据终端设备 DTE，负责通信控制的交换机、路由器等统称为数据通信设备 DCE。

在拓扑结构表示中，将 DTE、DCE 都抽象成节点，将所有的传输介质都抽象成线段。这样一来计算机网络被抽象成点和线的连接，这种点线连接构成的网络结构图称为网络拓扑结构图。按照拓扑结构表示，图 1-1 的网络将被表示成图 1-2 所示。

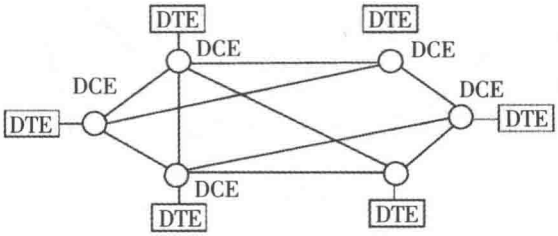

图 1-1　计算机网络结构

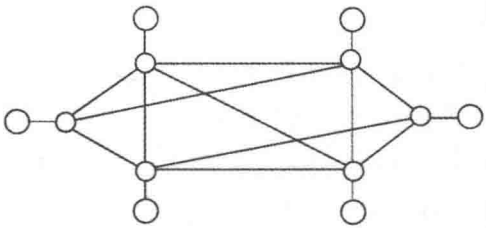

图 1-2　按拓扑结构表示的计算机网络结构

在计算机网络中，计算机互联采用全连接型构成点到点的通信是最理想的，即每一对节点之间都存在一条线路直接连接。这样使得传输速度最快，如图 1-3 所示。在全连接方式中，系统需要的链路数是节点数的平方倍，需要大量的传输线路，使得通信线路费用过高，所以在实际网络中采用全连接实际上是不现实的。

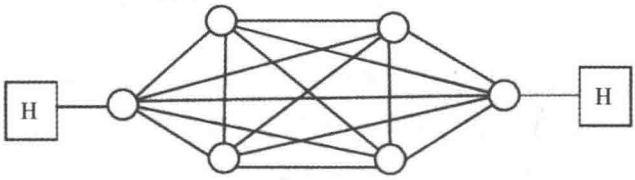

图 1-3　全连接

在实际网络中不采取全连接方式，而是采取中间转接方式。在图 1-4 所示采用中间转接方式的网络中，Ha 主机要与 Hb 通信时，传输的数据可以从 Ha 主机出发，经 a 到 b 到 d 再到 f 的转接，仍然可以达到 Hb 主机；同样从 Ha 主机出发，还可以经 a 到 b 到 e 再到 f 的转接，也可以达到 Hb 主机。尽

管需要通信的两台主机之间没有直接的连接，但是通过中间的转结，仍然能实现数据的传输。中间转接方式需要的线路大大减少，节省了大量的通信费用，计算机网络中一般都采用中间转接方式。在局域网、城域网及广域网的拓扑结构中，中间转接方式一般多用于广域网。

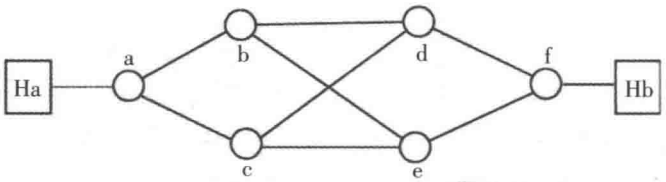

图 1-4　中间转接

按照网络拓扑分类，计算机网络拓扑有网形拓扑、树形拓扑、混合形拓扑，总线拓扑、星形拓扑和环形拓扑。广域网的拓扑结构一般为：网形拓扑、树形拓扑、混合形拓扑。

网形拓扑由于节点之间有许多条路径相连，可以为数据分组的传输选择适当的路由，当网络某部分出故障或数据流量过大时，数据分组可以绕过失效的部件或过忙的节点，大大提高网络的传输可靠性。网形拓扑结构的网络协议复杂，但由于它的可靠性高，被广泛使用在广域网中。

树形拓扑像一棵倒置的树，顶端是树根，树根以下带若干分支，每个分支还可以再带子分支。这种拓扑的站发送时，根接收该信号，然后重新广播到全网。树型网容易扩充，新的节点和分支很容易加入到网中。容易进行故障隔离，某一分支或节点出故障，很容易将故障分支或节点与整个网络系统隔离开来。其缺点是对根的依赖较大，根若出故障，全网则不能正常工作。

混合形拓扑一般是将两种不同的网络拓扑结构混合起来，具有各自的优缺点。

总线形拓扑是属于共享信道的广播式网络，所有站点通过相应的接口直接连接到这一公共信道上。任何一个站发送的信息都沿着公共信道传输，而且能被所有的其他站接收。当一对站进行数据传输时，靠目的地址实现识别接收站。因为所有站共享一条公共信道，所以一个时刻只能有一个站发送信号。要发送信息的站通过某种仲裁协议（介质访问控制方法）获得使用信道的权力。网上的所有站分时地使用信道进行数据传输。

总线形拓扑的优点为：结构简单、容易扩充；连接采用无源部件，有较高的可靠性。