目　录

第一章

计算机网络

第一节　计算机网络概述

一、计算机网络的定义

什么是计算机网络？人们对此一直存在争论，迄今为止仍没有一个公认的定义。

从技术门类的角度来看，计算机网络可以认为是计算机技术和通信技术相结合，实现远程信息处理、资源共享的系统。从现代计算机网络的角度出发，可以认为是自主计算机系统的互连集合。“自主”这一概念排除了网络系统中的从属关系，“互连”不仅指计算机间物理上的连通，而且指计算机间的交换信息、资源共享，这就需要通信设备和传输介质的支持，以及网络协议的协调控制。因此，本书给出的计算机网络的定义如下：计算机网络是将若干台具有独立功能的计算机通过通信设备和传输介质相互连接，以网络软件实现通信、资源共享和协同工作的系统。

网络中由传输介质链路连接在一起的设备，称为网络节点（Node Computer，NC），链路称为通信信道（Channels of Communication），常简称为节点和信道。

计算机网络的组成部件主要完成网络通信和资源共享两种功能，从而可将计算机网络看成一个两级网络，即核心部分和边缘部分。其中，NC 为网络节点，与通信介质构成网络核心；H 为主机（Host），T 为终端（Terminal），两者共同构成网络边缘。两级计算机子网是现代计算机网络结构的主要形式。

二、网络边缘

网络边缘实现资源共享功能，包括数据处理、提供网络资源和网络服务。网络边缘主要包括主机、外围设备及其相关软件，如服务器、客户机、智能手机、网络摄像头等。网

络边缘设备之间的通信方式主要有客户机 / 服务器（Client/Server，C/S）方式和对等连接（P2P）方式。

（一）客户机 / 服务器方式

计算机网络中，为网络用户提供共享资源和服务功能的计算机或设备称为服务器。根据服务器所提供的服务，又可以将服务器分为文件服务器、打印服务器、应用服务器和通信服务器等。服务器运行服务器端软件。接受服务或访问服务器上共享资源的计算机称为客户机，客户机运行客户端软件。

随着计算机网络服务功能的改变，这种方式经历了前期的工作站 / 文件服务器方式，以及目前在 internet 上普遍应用的浏览器 / 服务器（Browser/Server，B/S）方式的发展过程。

1. 工作站 / 文件服务器方式

在工作站 / 文件服务器方式的计算机网络中，工作站对文件服务器的文件资源的访问处理过程，是将所需的文件整个下载到工作站上，处理结束后再上传到文件服务器。目前，单纯的工作站 / 文件服务器方式的计算机网络基本上已不再使用了。

2. 客户机 / 服务器方式

在 C/S 方式的计算机网络中，客户机对服务器资源的访问处理，只下载相关部分，处理结束后再上传到服务器。

3. 浏览器 / 服务器方式

B/S 方式的计算机网络与 C/S 方式的计算机网络的主要区别是在客户端运行的浏览器软件。客户不需要了解更多的计算机操作知识，甚至只需会操作鼠标就能够完成相应的操作。

（二）对等连接方式

在对等连接方式中，没有专用的服务器，网络中的所有计算机都是平等的。各台计算机既是服务器又是客户机。每台计算机分别管理自己的资源和用户，同时又可以作为客户机访问其他计算机的资源。

由于每台计算机独自管理自己的资源，因此，很难控制网络中的资源和用户，安全性稍差。

三、网络核心

网络核心主要包括交换机（Switch）、路由器（Router）、入网桥（Bridge）、中继器

（Repeater）、集线器（Hub）、网卡（Network Interface Card，NIC）和缆线等设备和相关软件。网络核心实现网络通信功能，包括数据的加工、传输和交换等通信处理工作，即将位于网络边缘的一台主机的信息传送给另一台主机。其中交换是网络核心部分最重要的功能。

交换又称转接，是在多节点网络中，利用交换机、路由器等转接设备，在节点间建立临时连接，完成通信的一种技术。交换技术按照其原理划分，可分为线路交换（Circuit Switching）和存储转发交换（Store and Forward Switching）两种技术。其中，存储转发交换又可按照转发的信息单位不同，分为报文交换（Message Switching）和分组交换。

（一）线路交换

线路交换就像电话系统一样，在通信期间，发送方和接收方之间一直保持一条专用的物理通路，而通路中间经过了若干节点的转接。

线路交换的通信过程包括建立线路、传输数据和拆除线路三个阶段。线路交换在传输数据之前需建立连接，增加时延。建立连接之后就专用该线路，即使在没有数据传输时，也要占用线路，因此，线路的利用率低。但是，建立连接之后，线路就被用户专用，传输时延短（只存在传播时延），这一特性使线路交换适合实时性强的信号传输，如电话和实况转播等。

（二）报文交换

报文交换是基于存储转发原理的一种交换技术。存储转发的基本原理：数据在传输过程中，要由交换节点将输入数据存入节点的缓冲区内，一旦输出线路空闲，就将数据发送出去。报文交换所传输的信息单位是报文，其中包含收发站地址、检验码等控制信息。在发送站，先将要发送的信息分割成一个个的报文，然后发送到相邻的交换节点，报文在交换节点存储等待。当通往报文接收站的线路空闲时，交换节点就将报文发送到下一个交换节点，直至传送到接收站。

报文交换方式以报文为单位来占用信道，发送站和接收站无须建立专用的通路，可实现多个用户共用一个信道，从而提高信道的利用率。但是，由于报文一般较长，因此，交换节点需配置大容量的存储器，以备存储整个报文。报文交换的传输时延取决于交换节点的存储转发时间，具有不确定性。因此，它适用于高信息容量的数据通信，不适合实时性传输。

（三）分组交换

分组交换又称包交换，最早应用于 ARPANET。分组交换也是基于存储转发原理的一

种技术。与报文交换不同的是，它的信息传输单位是分组(Packet)。分组格式要比报文短，包括分组头部和数据两部分，头部包含收发站地址、分组编号和检验码等控制信息。在源节点，报文被分割成若干分组，分组可按不同的路径传输，其间要在交换节点存储转发，最后在接收端按照分组编号重新装配成报文。分组交换的分组长度小，降低了对交换节点存储容量的要求，同时也缩短了网络时延。但是，在发送端和接收端需对报文进行拆卸和装配，增加了网络软硬件的复杂性和报文处理时间。分组交换适用于大型、高信息容量的数据通信。分组交换有数据报(Datagram) 和虚电路(Virtual Circuit) 两种常用的实现方法。

“虚电路”这一术语是区别于线路交换而言的。线路交换是各交换节点为发送站和接收站建立一条专用的物理通路；而虚电路方式是在交换节点之间建立路由，即在交换节点的路由表内创建一个表项。在交换节点收到一个分组后，检查路由表，按照其匹配项的出口发送分组。因此，虚电路是一条逻辑线路，可以与其他连接共享一条物理线路。

第二节　计算机网络的分类与组成

一、计算机网络的分类

（一）按地理位置分类

按地理位置划分，计算机网络可分为广域网（Wide Area Network，WAN）、城域网（Metropolitan Area Network，MAN）和局域网（Local Area Network，LAN）。

1. 广域网

广域网的作用范围通常为几十千米到几千千米，可以跨越辽阔的地理区域进行长距离的信息传输，所包含的地理范围通常是一个国家或洲。

在广域网内，用于通信的传输装置和介质一般由电信部门提供。网络则由多个部门或国家联合组建，网络规模大，能实现较大范围的资源共享。

2. 城域网

城域网的作用范围介于广域网和局域网之间，是一个城市或地区组建的网络，作用范

围一般为几十千米。城域网及宽带城域网的建设已成为目前网络建设的热点。由于城域网本身没有明显的技术特点，因此，后续章节只讨论广域网和局域网。

3．局域网

局域网是一个单位或部门组建的小型网络，一般局限在一座建筑物或园区内，其作用范围通常为十米至几千米。局域网规模小、速度快，应用非常广泛。

需要指出的是，广域网、城域网和局域网的划分只是一个相对的分界，随着计算机网络技术的发展，三者的界限已经变得模糊。另外，internet 不是广域网，而是广域网、城域网和局域网互连而形成的遍布全球的网络。

（二）按网络拓扑结构分类

计算机网络拓扑结构是引用拓扑学中研究与大小、形状无关的点、线特性的方法，把网络单元定义为节点，两节点间的线路定义为链路，则网络节点和链路的几何位置就是网络拓扑结构。网络拓扑结构的基本类型主要有总线拓扑结构、环状拓扑结构、星状拓扑结构、树状拓扑结构和网状拓扑结构。

1．总线拓扑结构

总线拓扑（Bus Topology）结构是将网络中的所有设备都通过一根公共总线连接，通信时信息沿总线进行广播式传送。

总线拓扑结构简单，增删节点容易。网络中任何节点的故障都不会造成全网瘫痪，可靠性高。但是任何两个节点之间传送数据都要经过总线，总线成为整个网络的瓶颈。当节点数目多时，易发生信息堵塞。

总线拓扑结构投资少、安装布线容易、可靠性较高，是常用的局域网拓扑结构之一。由于网络中的所有设备共用总线这一条传输信道，因此，存在信道争用问题。为了减少信道争用带来的冲突，带有冲突检测的载波监听多路访问（Carrier Sense Multiple Access/Collision Detection，CSMA/CD）协议被用于总线网中。为了防止信号到达总线两端的回声，总线两端都要安装吸收信号的端接器。最著名的总线网是以太网，以太网曾一度成为总线网的代名词。

2．环状拓扑结构

环状拓扑（Ring Topology）结构中，所有设备被连接成环，信息是通过环广播传送的。环状拓扑结构中的每一台设备只能和相邻节点直接通信。与其他节点通信时，信息必须依

次经过二者间的每一个节点。

节点的增加、删除和修改，一般需要将整个网重新配置，扩展性、灵活性差，维护困难。

环状网一般采用令牌（一种特殊格式的帧）来控制数据的传输，只有获得令牌的节点才能发送数据，因此，避免了冲突现象。环状网有单环和双环两种结构。双环结构常用于以光导纤维作为传输介质的环状网中，目的是设置一条备用环路。当光纤环发生故障时，可迅速启用备用环，提高环状网的可靠性。曾被广泛应用的环状网有令牌环（Token Ring）网和光纤分布式数据接口（Fiber Distributed Data Interface，FDDI）。

3. 星状拓扑结构

星状拓扑（Star Topology）结构由一个中央节点和若干从节点组成。中央节点可以与从节点直接通信，而从节点之间的通信必须经过中央节点的转发。

星状拓扑结构简单，建网容易，传输速率高。每个节点独占一条传输线路，消除了数据传送堵塞现象。一台计算机及其接口的故障不会影响到网络，扩展性好，配置灵活，增加、删除和修改一个站点容易实现，网络易管理和维护。网络可靠性依赖于中央节点，中央节点一旦出现故障将导致全网瘫痪。

星状网的中央节点是该网的瓶颈。早期的星状网，中央节点是一台功能强大的计算机，既具有独立的信息处理能力，又具备信息转接能力。目前，星状网的中央节点多采用诸如交换机等网络转接设备。

必须特别注意网络的物理拓扑和逻辑拓扑之间的区别。物理拓扑是指网络布线的连接方式，而逻辑拓扑是指网络的访问控制方式。自 20 世纪 90 年代以来，网络的物理拓扑大多向星状网演化。常见的采用星状物理拓扑的网络有 100 BaseT 以太网、令牌环网和异步传输模式（Asynchronous Transfer Mode，ATM）网等。

4. 树状拓扑结构

树状拓扑（Tree Topology）结构的形状像一棵倒置的树，顶端是树根，树根以下带分支，每个分支还可以再带子分支，但不形成闭合回路。树状拓扑结构是一种层次结构，节点按层次连接，信息交换主要在上、下相邻节点之间进行，同层节点之间不进行数据交换。树根接收各节点发送的数据，然后再广播发送到全网。

树状拓扑结构适用于汇集信息的应用要求，连接简单，维护方便，易于扩展和故障隔

离。其链路具有一定的专用性，无需对原网做任何改动就可以扩充节点。一般一个分支和节点的故障不影响另一分支节点的工作，很容易将故障分支与整个系统隔离开来。树形拓扑结构的缺点是各个节点对根的依赖性太大，如果根发生故障，那么全网不能正常工作。

树状拓扑结构是星状拓扑结构的一种变形，是由多个层次的星状结构纵向连接而成。当局域网的规模比较大，而且网络覆盖的单位存在行政或业务隶属关系时，一般采用树状拓扑结构组网。

5. 网状拓扑结构

网状拓扑（Mesh Topology）结构分为一般网状拓扑结构和全连接网状拓扑结构两种。全连接网状拓扑结构中的每个节点都与其他所有节点相连通。一般网状拓扑结构中每个节点至少与其他两个节点直接相连。

网状拓扑结构的容错能力强，如果网络中一个节点或一段链路发生故障，那么信息可通过其他节点和链路到达目的节点，可靠性高。但其建网费用高，布线困难。

网状网的最大特点是其强大的容错能力，主要用于强调可靠性的网络中，如帧中继（Frame Relay）网、ATM 网等。

在实际组网中，为了符合不同的要求，拓扑结构不一定是单一的，往往都是几种结构的混用。

（三）其他分类

计算机网络还有多种分类方法，如按网络的使用范围、按信息交换方式分类等。

按网络的使用范围分类，计算机网络可分为公用网和专用网两类。公用网（Publie Network）一般是国家邮电部门建造的网络，所有按规定缴纳费用的人都可以使用，如 CHINANET、CERNET 等。专用网（Private Network）是某个部门为其特殊工作的需要而建造的网络，一般只为本单位的人员提供服务，如军队、银行和铁路等系统的专用网。

按信息交换方式划分，计算机网络可分为电路交换网、报文交换网和分组交换网三类。电路交换网的特征是在整个通信过程中，需始终保持两节点间的通信线路连通，即形成一个专用的通信线路，如同电话通信。电路交换网适用于实时通信，但网络利用率低。报文交换网的通信线路是非专用的，利用存储转发原理，将待传输的报文存储在网络节点中，等到信道空闲时再发送出去。报文交换网提高了网络利用率，但由于长报文传输时会带来很多问题，因此，目前已很少使用。分组交换网将报文划分为若干小的传输单位——

分组，并将分组单独传送，能够更好地利用网络，是当今广泛采用的网络形式，如大家熟知的 internet。

二、计算机网络的组成

（一）计算机网络的硬件组成

计算机网络硬件系统是由服务器、客户机、通信处理设备和通信介质组成。服务器和客户机是构成网络边缘的主要设备，通信处理设备和通信介质是构成网络核心的主要设备。

1. 服务器

服务器一般是一台高配置（诸如中央处理器速度快、内存和硬盘的容量高等）的计算机，为客户机提供服务。按照服务器所能提供的资源来区分，可分为文件服务器、打印服务器、应用系统服务器和通信服务器等。在实际应用中，常把几种服务集中在一台服务器上，这样一台服务器就能执行几种服务功能。例如，将文件服务器连接到网络共享打印机，此服务器就能作为文件和打印服务器使用。

文件服务器在网络中起着非常重要的作用。它负责管理用户的文件资源，处理客户机的访问请求，将相应的文件下载到某一客户机。为了保证文件的安全性，常为文件服务器配置磁盘阵列或备份的文件服务器。

打印服务器负责处理网络中用户的打印请求。一台或几台打印机与一台计算机相连，并在计算机中运行打印服务程序，使得各客户机都能共享打印机，这就构成了打印服务器。还有一种网络打印机，内部装有网卡，可以直接与网络的传输介质相连，作为打印服务器。

应用系统服务器运行 CS 应用程序的服务器端软件，该服务器一般保存着大量信息供用户查询。应用系统服务器处理客户端程序的查询请求，只将查询结果返回给客户机。

通信服务器负责处理本网络与其他网络的通信，以及远程用户与本网的通信。

2. 客户机

客户机运行 CS 应用程序的客户端软件，网络用户通过客户机与网络联系。由于网络中的客户机能够共享服务器的资源，因此，一般情况下其配置比服务器低。

3. 网卡

服务器和客户机都需要安装网卡。网卡是计算机和传输介质之间的物理接口，又称网

络适配器。网卡的作用是将计算机内的数据转换成传输信号发送出去，并把传输信号转换成计算机内的数据接收进来。其基本功能是并行数据和串行信号的转换、帧的拆装、网络访问控制和数据缓冲等。内置网卡的总线接口插在计算机的扩展槽中，网络缆线接口与传输介质相连。

4. 通信介质

通信介质又称传输介质，用于连接计算机网络中的网络设备，一般可分为有线传输介质和无线传输介质两大类。常用的有线传输介质是双绞线（Twisted-Pair）、同轴电缆（Coaxial Cable）和光导纤维（Optical Fiber），常用的无线传输介质是微波（Microwave）、激光（Laser）和红外线（Infrared）等。

5. 通信处理设备

通信处理设备主要包括调制解调器（Modem）、中继器、集线器、网桥、交换机、路由器和网关（Gateway）等。

（1）调制解调器

调制解调器是远程计算机通过传输介质（如电话线、光纤）连接网络所需配置的设备。调制是指发送方将数字信号转换为线缆所能传输的模拟信号。解调是指接收方将模拟信号还原为数字信号。由于调制解调器同时具备调制和解调双重功能，因此，它既能发送信号又能接收信号。

（2）中继器和集线器

由于信号在线缆中传输会发生衰减，因此，要扩展网络的传输距离，可以利用中继器使信号不失真地继续传播。

1）中继器可以把接收到的信号物理地再生并传输，即在确保信号可识别的前提下延长了线缆的距离。由于中继器不转换任何信息，因此，和中继器相连接的网络必须使用同样的访问控制方式。

2）集线器是一种特殊的中继器。它除对接收到的信号再生并传输之外，还可为网络布线和集中管理带来方便。集线器一般有 8 ~ 16 个端口，供计算机等网络设备连接使用。

（3）网桥

网桥不仅能再生数据，还能够实现不同类型的局域网互连。网桥能够识别数据的目的地址，如果不属于本网段，就把数据发送到其他网段上。

（4）交换机

应用广泛的交换机是二层交换机和三层交换机。

二层交换机同时具备集线器和网桥的功能。

三层交换机除具有二层交换机的功能之外，还具有路由功能。

（5）路由器

路由器具有数据格式转换功能，可以连接不同类型的网络。路由器能够识别数据的目的地址所在的网络，并可根据内置的路由表从多条通路中选择一条最佳路径发送数据。

（6）网关

网关又称协议转换器，作用是使网络上采用不同高层协议的主机，能够互相通信，进而完成分布式应用。网关是传输设备中最复杂的一个，主要用于连接不同体系结构的网络或局域网与主机的连接。

（二）计算机网络的软件组成

计算机网络的软件系统包括网络操作系统和网络应用服务系统等。网络应用服务系统针对不同的应用有不同的应用软件，下面只介绍网络操作系统。

1. 网络操作系统的功能及组成

网络操作系统除具有常规操作系统所应具有的功能之外，还应具有网络管理功能，如网络通信功能、网络资源管理功能和网络服务功能等。

针对上述功能，网络操作系统可划分为三个组成部分：网卡驱动程序、网络协议软件和应用程序编程接口（Application Program Interface，API）软件。

1）网卡驱动程序完成网卡接收和发送数据的处理。正确地为网卡选择驱动程序及设置参数是建立网络的重要操作。一般网络操作系统包含一些常用网卡的驱动程序，网卡生产商也提供一张网卡驱动程序的光盘。

2）网络协议软件分布在网络的所有层中，直接关系到网络操作系统的性能。

3）应用程序编程接口软件建立本地系统与网络环境的联系。

2. 常用的网络操作系统

应用于计算机网络的操作系统，最常见的有 Windows、UNIX 和 Linux。

（1）Windows

Microsoft Windows 是微软公司制作和研发的桌面操作系统。它问世于 1985 年，从最初运行在磁盘操作系统下的 Windows3.0 到风靡全球的 Windows XP、Windows7 和 Windows10，一直是人们喜爱的操作系统。

Windows Server 版本的持续更新，也是不断融合网络技术的过程。从面向小型企业服务器领域的 Windows Server2003，逐渐发展为 Windows Server2008R2（Windows7 的服务

器版本），提升了虚拟化、系统管理弹性、网络存取方式，以及信息安全等领域的应用。Windows Server2012R2（Windows8.1 的服务器版本）提供企业级数据中心和混合云解决方案。基于 Windows10 的 Windows Server2019 具有四大重点新特性：混合云、安全、应用程序平台和超融合基础架构。

（2）UNIX

UNIX 是一个强大的多用户、多任务分时操作系统，支持多种处理器架构。经过长期的发展和完善，已成长为一种主流的操作系统。UNTX 的系统结构包括操作系统内核、系统调用和应用程序三个部分。UNTX 具有技术成熟、可靠性高、网络和数据库功能强、伸缩性突出和开放性好等特色，可满足各行各业的实际需要，特别能满足企业重要业务的需要，已经成为主要的工作站平台和重要的企业操作平台。

UNIX 与其他商业操作系统的不同之处主要在于其开放性，在系统开始设计时就考虑了各种不同使用者的需要，因此，UNIX 被设计为具备很大可扩展性的系统。由于其源码被分发给大学，因此，在教育界和学术界影响很大，进而影响到商业领域。大学生和研究者为了科研目的或个人兴趣在 UNIX 上进行各种开发，并且不计较经济利益，将这些源码公开，互相共享，这些行为丰富了 UNIX 本身。目前，UNIX 成为 internet 上提供网络服务的最通用的平台，是所有开发的操作系统中可移植性最好的系统之一。

由于 UNIX 的开放性，因此，在发展过程中产生了多个不同的 UNIX 版本，可归纳为符合单一 UNIX 规范的 UNIX 操作系统及类 UNIX（UNIX-like）操作系统。目前应用较为广泛的有 AIX、Solaris、HP-UX、IRIX 和 A/UX 几种 UNIX 版本。

（3）Linux

Linux 是一套免费使用和自由传播的类 UNIX 操作系统，是一个多用户、多任务、支持多线程和多 CPU 的操作系统。Linux 支持 32 位和 64 位硬件，能运行主要的 UNIX 工具软件、应用程序和网络协议。Linux 继承了 UNIX 以网络为核心的设计思想，是一个性能稳定的网络操作系统。

Linux 与其他操作系统相比，具有开放源码、没有版权、技术社区用户多等特点。开放源码使得用户可以自由裁剪，灵活性高，功能强大，成本低。伴随着 internet 的发展，Linux 得到了来自全世界的软件爱好者、组织、公司的支持，市场份额逐步扩大，逐渐成为主流操作系统之一。

Linux 的发行版本目前已超过 300 个，应用普遍的有十几个。这些发行版大体可分为两类：一类是商业公司维护的发行版本；一类是社区组织维护的发行版本。前者以 Redhat 为代表，后者以 Debian 为代表。Redhat 是中国用户使用最多的 Linux 版本。

第三节　计算机网络安全

一、网络安全的基本属性

（一）网络安全的定义

网络安全就是为了保证网络系统的硬件、软件及其系统中的数据资源能够完整、准确、连续运行，相关服务不受到干扰破坏和非授权使用。保护网络的信息安全是网络安全的最终目标和关键。因此，从本质上讲，网络安全就是网络的信息安全，它涉及的领域相当广泛。这是因为在目前的公用通信网络中存在着各种各样的安全漏洞和威胁。

网络安全的通用定义是指网络系统的硬件、软件和系统中的数据受到保护，不因偶然或恶意的攻击而遭到破坏、更改、泄露，系统连续、可靠、正常地运行，网络服务不中断。广义上讲，凡是涉及网络上信息的保密性、完整性、可用性、可控性和不可否认性的相关技术和理论都是网络安全所要研究的领域。

网络安全的具体含义会随着重视“角度”的变化而变化。例如，从用户（个人、企业等）的角度来说，希望涉及个人隐私或商业利益的信息在网络上传输时受到保护，避免其他人或对手利用窃听、冒充、篡改、抵赖等手段侵犯用户的隐私和利益。从网络运行和管理者的角度来说，希望对本地网络信息的访问、读、写等操作受到保护和控制，避免出现后门、病毒、非法存取、拒绝服务、网络资源非法占用和非法控制等威胁，从而制止和防御网络黑客的攻击。从安全保密部门的角度来说，希望对非法、有害或涉及国家机密的信息进行过滤，避免机要信息泄露，避免对社会产生危害、对国家造成巨大损失。从社会教育和意识形态的角度来说，网络上不健康的内容会对社会的稳定和人类的发展造成阻碍，必须对其进行控制。

（二）网络安全的重要性

随着信息科技的迅速发展及计算机网络的普及，计算机网络深入国家的政府、军事、文教、金融、商业等诸多领域，可以说网络无处不在。资源共享和计算机网络安全一直作为一对矛盾体而存在着，随着计算机网络资源共享进一步加强，信息安全问题日益突出。

互联网在我国政治、经济、文化及社会生活中发挥着越来越重要的作用。作为国家关键基础设施和新的生产、生活工具，互联网的发展极大地促进了信息流通和共享，提高了社会生产效率和人民生活水平，促进了经济社会的发展。带来这些便利和发展的同时，上

网数据也遭到了不同程度的攻击和破坏。攻击者不仅可以窃听网络上的信息，窃取用户的口令、数据库的信息，还可以篡改数据库内容，伪造用户身份，否认自己的签名。更有甚者，他们删除数据库内容，摧毁网络节点，释放计算机病毒等，这些都使网络信息的安全性和用户自身的利益受到了严重的威胁。因此，维护网络安全工作的重要性日益突出。

信息安全空间将成为传统的国界、领海、领空的三大国防和基于太空的第四国防之外的第五国防空间，称为 Cyber-Space，是国际战略在军事领域的演进。这对我国网络安全提出了严峻的挑战。我们国家对信息安全的建设也非常重视，正在加快建设我国网络安全保障体系。

无论是有意的攻击，还是无意的误操作，都将会给系统带来不可估量的损失。因此，计算机网络必须有足够强的安全措施。无论是在局域网还是在广域网中，网络安全措施应该能够抵抗各种不同的威胁和脆弱性，这样才能确保网络信息的保密性、完整性和可用性。

1. 保密性

保密性也称机密性，是指网络信息按规定要求不泄露给非授权的个人、实体或过程，或提供其利用的特性，即保护有用信息不泄露给非授权个人或实体，强调有用信息只被授权对象使用的特征。加密是保护存储在系统中的数据的一种有效方法。人们通常用加密方法来保证数据的保密性。解决的问题：防止用户非法获取关键的敏感信息，避免机密信息的泄露。

2. 完整性

完整性是指网络数据在传输、交换、存储和处理过程中保持非修改、非破坏和非丢失的特性，即保持信息原样性，使信息能正确生成、存储、传输，既是最基本的安全特征，也是计算机系统和数据传输的安全目标。完整性包括软件完整性和数据完整性。完整性用于保护计算机系统内的软件和数据不被非法删改。

3. 可用性

可用性是指无论何时，只要用户需要，系统和网络资源必须是可用的，尤其是当计算机及网络系统遭到非法攻击时，它必须仍然能够为用户提供正常的系统功能和服务。为了保证系统和网络的可用性，必须解决网络和系统中存在的各种破坏可用性的问题。网络信息可被授权实体正确访问，并按要求能正常使用或在非正常情况下能恢复使用的特征，即在系统运行时能正确存取所需信息，当系统遭受攻击或破坏时，能迅速恢复并投入使用。可用性是衡量网络信息系统面向用户的一种安全性能，属于网络服务的安全目标。

二、网络安全的概念

（一）信息安全及网络安全的概念

目前，国内外对信息安全尚无统一确切的定义。国际标准化组织（ISO）提出信息安全（information security）的定义如下：为数据处理系统建立和采取的技术及管理保护，保护计算机硬件、软件、数据不因偶然及恶意的原因而遭到破坏、更改和泄露。

《中华人民共和国计算机信息系统安全保护条例》对信息安全的定义如下计算机信息系统的安全保护，应当保障计算机及其相关的配套设备、设施（含网络）的安全，运行环境的安全，保障信息的安全，保障计算机功能的正常发挥，以维护计算机信息系统的安全运行，主要防止信息被非授权泄露、更改、破坏或使信息被非法的系统辨识与控制，确保信息的完整性、保密性、可用性和可控性

（二）网络安全的发展过程

网络安全概念的出现远远早于计算机的诞生，但计算机的出现，尤其是网络出现以后，信息安全变得更加复杂、更加“隐形”了。现代意义上的信息安全区别于传统意义上的信息介质安全，是专指电子信息的安全。

随着信息技术的发展，各种信息的电子化更加便于信息获取、携带与传输。相对于传统的信息安全保障，现代意义上的信息安全需要更加有力的技术保障，不单单是对接触信息的人和信息本身进行管理，介质本身的形态已经从“有形”转变到“无形”。在以计算机网络为支撑的业务系统中，正常业务的处理人员都有可能接触、获取这些信息，信息的流动是隐性的，对业务流程的控制就成了保障涉密信息的重要环节。

从网络安全的发展历程来看，安全保障的理念分为下面几个阶段。

1. 面向信息的安全保障

计算机网络刚刚兴起时，各种信息陆续电子化，各个业务系统相对比较独立，需要交换信息时往往是通过构造特定格式的数据交换区或文件式来实现，这个阶段从计算机诞生一直延续到互联网兴起的 20 世纪 90 年代末期。

面向信息的安全保障体现在对信息的产生、传输、存储、使用过程中的保障，主要的技术是信息加密，即保障信息不外露在“光天化日”之下。因此，信息安全保障设计的理念是以风险分析为前提（如 ISO13335 风险分析模型），找到系统中的漏洞，分析漏洞可能带来的威胁，评估“堵上”漏洞的成本，再“合理”地“堵上”漏洞，威胁也就消失了。

然而，风险的大小、漏洞的危害程度是随着攻击技术的发展而变化的，在大刀长矛

的冷兵器时代，敌人在几十米外你就是安全的；到了大炮、机枪的火器年代，几百米、几十千米都可能成为攻击的对象；而到了激光、导弹的现代，即使你在地球的另一端，也可能随时成为被攻击的对象。因此，面对信息的安全保障，分析漏洞往往是随着攻击技术的发展、入侵技术的进步而变化的，一句话，就是被动地跟着攻击者的步调，建立自己的防御体系，是被动的防护。更为严峻的是，随着攻击技术的发展，你与“敌人”的“安全距离”越来越大，这就需要你具有更强大的监控力，因为监控不到敌人的动向，安全就无从谈起。

在信息安全阶段，安全技术一般采用防护技术加上人员的安全管理，出现得最多的足防火墙、加密机等，但大多边界上的防护技术都属于识别攻击特征的“后升级”防护方式，也就是说，你在攻击者来之前升级了，就可以防止他的入侵。若没有来得及升级，或者没有可升级的“补丁”，则你的系统就危险了。加密技术的暴力破解技术也随着计算机的发展而发展，加密系统的密钥长度也越来越长。

2．面向业务的安全保障

如果说对信息的保护主要还是从传统安全理念到信息化安全理念的转变，那么面向业务的安全保障，就完全是从信息化的角度考虑信息的安全。到 2005 年，互联网已经深入社会的各个角落，网络成了人们工作与生活的“信息神经”，人们发现各种工作已经从传统的管理模式进入了“无纸化”的办公时代，此时计算机的故障、网络的中断已经不再是 IT 管理部门的小事件，而是整个企业的大故障。有些金融、物流、交通等企业，网络的故障完全可以导致企业业务的中断，甚至导致企业的停业。

此时，需要保护的信息不再只是某些文件，或者某些特殊权限目录的管理，而是用户的访问控制、系统服务的提供方式；也不再只是信息，而是整个业务系统，以及业务的 IT 支撑环境。业务本身的安全需求超过了信息的安全需求，安全保障自然也就需要从业务流程的控制角度考虑了，这个阶段我们称为面向业务的安全保障。

系统性的安全保障理念不仅是关注系统的漏洞，而且从业务的生命周期入手，对业务流程进行分析，找出流程中的关键控制点，从安全事件出现的前、中、后三个阶段进行安全保障。具体的保障设计——“花瓶模型”给了我们一个清晰的设计框架，把安全保障分为防护技术、监控手段和审计威慑三个部分，其中防护技术沿用信息安全的防护理念，同时针对“防护总落后于攻击”的现状，全面实施系统监控，对系统内各个角落的情况动态收集并掌握，任何的“风吹草动”都及时察觉，即使有危害也要降到最低程度，攻击没有了“战果”，也就达到了防护的目的。另外，针对网络事件的起因多数是内部人员，采用审计技术是震慑不法分子恶意滋生的“武器”。

面向业务的安全保障不只是建立防护屏障，而是建立一个立体的“陆、海、空”防护体系，通过更多的技术手段把安全管理与技术防护联系起来，不再被动地保护自己，而是主动地防御攻击。也就是说，面向业务的安全保障已经从被动走向主动，安全保障理念从风险承受模式走向安全保镖模式。

3．面向服务的安全保障

随着网络上的业务系统越来越多，各个业务系统的边界逐渐模糊，系统间需要相互融合，数据需要互通交换。若能把多个业务系统的开发与运营统一到一个管理平台上来，则不仅方便新业务的开发，而且可以缓解日益严重的运营维护危机。此时 Web2.0 技术出现了，它不仅继承了客户端维护的 B/S 架构，而且可以以方便、交互的方式促使业务模式的开发，很多软件公司把它作为 SOA（面向服务的架构）的实现基础。

SOA 是一个面向业务用户角度的开发架构，面向服务就是从最终用户的角度看待业务，IT 部门就是提供这种服务来支撑用户的各种业务流程实现。Web2.0 是支撑其实现的一个技术，而 SOA 的真正意图是“生产”出业务实现的各种标准构件——方便的“软件积木”，在实现新业务时，只要利用“积木”重新构造一下就可以了。这不仅可以大大减少了开发的工作量，而且大大提高了开发的效率，提高了企业的敏捷性。

业务中的“流程片段”，或者是流程组件打包，实现软件开发不再是专业软件人员的工作，而是业务使用人员的“自助式组装”，实现软件开发的 DIY（do it yourself）。所以说，SOA 思想是软件业真正把软件推广为“全民化”的梦想。

软件开发的模式改变了，对业务流程的分析方式也就不同了，因为“流程片段”对使用者来说是“组件积木”，也就是只关心其外部功能的“黑箱”，安全保障不仅是组件间的环节控制，对组件本身的安全同样需要。对单个业务的安全保障需求演变为对多个业务交叉系统的综合安全需求，IT 基础设施与业务之间的耦合程度逐渐降低。安全也分解为若干单元，不再面向业务本身，而是面向使用业务的客户，具体地说，就是用户在使用 IT 平台承载业务的时候，涉及该业务安全保障。由此，安全保障也从面向业务发展到面向服务。

面向服务的安全保障还有一层含义，随着业务的增多，IT 支撑平台成为公共的技术设施。安全保障也分为公共网络的基础安全与业务本身的控制安全，而这两种安全需要有机结合，最终都是为了一个目标，就是为客户提供安全、可靠的业务服务。

（三）网络信息安全技术

随着科学技术的发展，网络信息安全技术也进入了高速发展的时期。人们对信息安全

的需求也从单一的通信保密发展到各种各样的信息安全产品、技术手段等多方面。总体来说，网络信息安全技术在发展过程中经历了以下四个阶段。

1. 通信保密

20 世纪 40 年代至 20 世纪 70 年代，通信技术还不发达，电话、电报、传真等信息交换过程中存在的安全问题，如有线通信容易被搭线窃听、无线传播由于电磁波在空间传播易被监听，使得保密成为通信安全阶段的核心安全需求。因此，这一阶段主要是通过密码技术加密通信内容，保证数据的保密性和完整性，对安全理论和技术的研究只侧重于密码学。这一阶段的信息安全可以简单地称为通信安全，即 COMSEC（communication security）。

2. 计算机安全

20 世纪 80 年代后，计算机的性能迅速提高，应用范围不断扩大，计算机和网络技术的应用进入了实用化和规模化阶段。人们利用通信网络把孤立的计算机系统连接起来，并共享资源，信息安全问题也逐渐受到重视。人们对安全的关注已经逐渐扩展为以保密性、完整性和可用性为目标的计算机安全阶段，即 COMPSEC（computer security）。

这个阶段的重点是确保计算机系统中的软、硬件及信息在处理、存储、传输中的保密性、完整性和可用性。安全威胁已经扩展到非法访问、恶意代码、口令攻击等。

3. 信息系统安全

信息系统是由计算机及其相关和配套的设备、设施（含网络）构成的，按照一定的应用目标和规则对信息进行采集、加工、存储、传输、检索等处理的人机系统。20 世纪 90 年代，信息系统安全的威胁发展到网络入侵、病毒破坏、信息对抗的攻击等，重点放在确保信息在存储、处理、传输过程中及信息系统不被破坏，确保合法用户的服务和限制非授权用户的服务，以及必要的防御攻击的措施。人们对安全的关注进入到强调信息的保密性、完整性、可控性、可用性的信息安全阶段，即 ITSEC（information technology security）。

信息系统安全的主要保护措施包括防火墙、防病毒软件、漏洞扫描、入侵检测、公钥基础设施、虚拟专用网络等措施。

4. 网络空间安全

20 世纪 90 年代后期，随着电子商务等的发展，网络安全衍生出了诸如可控性、抗抵赖性、真实性等其他原则和目标。此时对安全性有了新的需求：可控性，即对信息及信息系统实施安全监控管理；不可否认性，即保证行为人不能否认自己的行为。信息系统安全也转化为从整体角度考虑其体系建设的信息保障（information assurance）阶段，也称为网

络信息系统安全阶段。

这一时期，在密码学方面，公开密钥密码技术得到了长足的发展，如著名的 RSA 公开密钥密码算法获得了广泛的应用，对用于完整性校验的散列函数的研究也越来越多。此时主要的保护措施包括防火墙、防病毒软件、漏洞扫描、入侵检测系统、公钥基础设施、虚拟专用网络等。

面对日益严峻的国际网络空间形势，我们应立足国情、创新驱动，解决受制于人的问题。坚持纵深防御，构建牢固的网络安全保障体系。