

计算机网络与安全

第一节 计算机网络基础知识

一、计算机网络的定义

（一）计算机网络的诞生

1969 年美国国防部创建第一个分组交换网 ARPANET。我国在 1994 年接入因特网。

（二）计算机网络的定义

计算机网络是指将分布在不同地理位置具有独立功能的多个计算机系统，通过通信设备和通信线路连接起来，在网络软件的管理下实现数据通信和资源共享的系统。

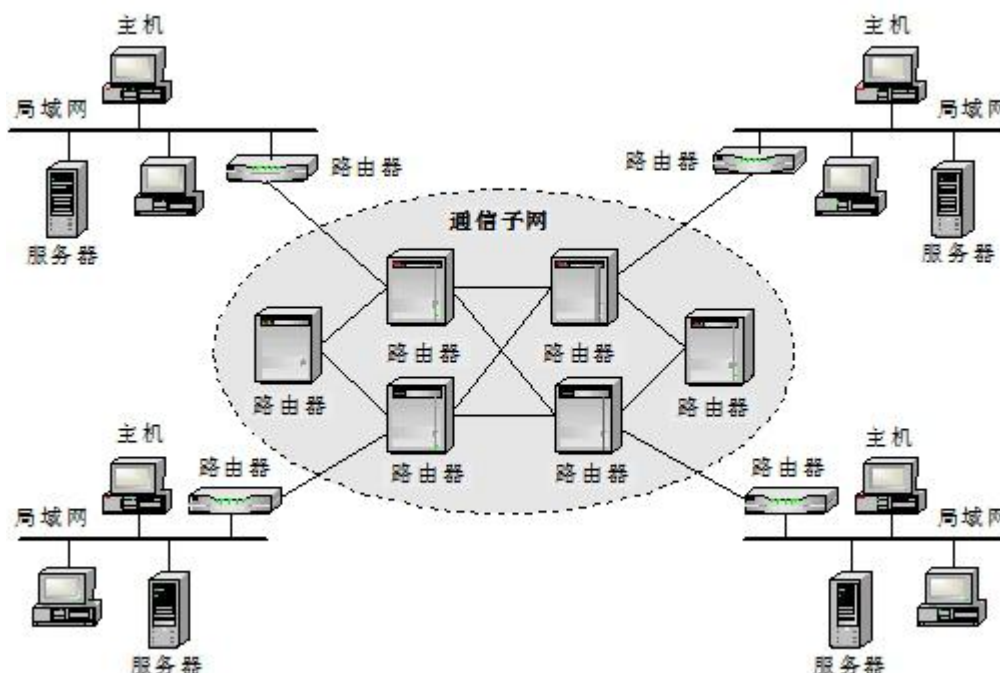
二、计算机网络的组成与结构

（一）计算机网络的功能

不管什么类型的网络，都有三大功能：数据通信、资源共享与分布处理。

（二）计算机网络的组成

计算机网络=资源子网+通信子网



（三）各部分的功能

资源子网：即我们所用的终端或服务器，负责数据的处理。

通信子网：由网络连接设备（网卡、路由器等）和通信线路（光纤、双绞线等）组成，负责数据传输。

三、计算机网络的硬件和软件

（一）网络硬件

1.网络接口卡（网卡）

每块网卡都有唯一的一个固定的硬件编号，称为 MAC 地址。

2.传输介质

网络的物理通道，分有线介质和无线介质两种。

无线介质：无线电波、红外线、微波、激光等。

有线介质：双绞线、同轴电缆、光缆等。

类型	传输介质	特点	连接距离	适用范围
有线介质	双绞线	价格便宜且易于安装和维护，但它容易受到外部高频电磁波的干扰，线路本身也会产生一定的噪声，误码率较高。	100m 以内	作建筑物内部的局部网通信介质
	同轴电缆	同轴电缆频带宽，损耗小，具有比双绞线更强的抗干扰能力和更好的传输性	500 米以内	很少用
	光缆	电磁绝缘性能好，信号衰变小，频带较宽，传输距离较大，传输误码率很低	100km 以上	传输距离较长及主干网的连接
无线介质	无线电波	其传输是全方向，要使用天线，通信质量较差	全球	手机、电视等
	蓝牙	无线电波的一种，体积小，功率低，可以集成到任何数字设备中频段全球通用，跳频抗干扰，采用 ATM 交换技术	10 米以内 可扩充至 100 米	无线鼠标，键盘； 相机、手机等
	微波	在空间主要是直线传播，主要有地面微波接力通信和卫星通信		
	红外线通信	红外线广泛应用于很短距离的通信，不需要天线。有方向性，也不能在室外应用	室内短距离	
	激光	传输距离可以很远，但激光束不能被遮挡，也不能穿透植物		

3.连接设备

连接设备	工作原理	特点
集线器	它工作于 OSI 参考模型的物理层，对接收到的信号进行整形放大，然后转发到所有端口，以扩大网络的传输距离	共享带宽、半双工、易产生广播风暴
交换机	MAC 地址学习、一次广播，多次单播	独占带宽、可以单工，也可双工
路由器	工作在网络层，将不同网络、网段或 VLAN 之间的数据信息进行“翻译”，以使它们能够相互“读”懂对方的数据，从而构成一个更大的网络	连接不同子网、选择路径、流量控制
中继器	工作在物理层，信号整形放大重发，扩大信号传输距离	信号放大、不能控制流量

4.工作站和服务

网络中的计算机按其功能的不同有工作站(Workstation)与服务器(Server)之分，工作站也称客户机(Client)。

服务器：是网络上一种为客户机提供各种服务的高性能的计算机，它能够提供网络管理、运行应用程序、处理各网络工作站成员的信息请示等服务。

工作站：享受服务器所提供的服务的那些计算机，我们称之为工作站。

（二）网络软件

网络操作系统：Windows NT、Windows 2000、Novell.Netware、Unix 和 Linux 等。

网络应用软件：解压缩工具、文件下载工具、文件上传工具、网络媒体播放器等。

网络通信软件：是执行各种网络通信协议和通信功能的程序。

1.网络应用软件结构 B/S，C/S

B/S 结构：浏览器/服务器（Browser/Server）使用该结构，可以直接在浏览器中操作。

C/S 结构：客户机/服务器（Client/Server）结构，使用该结构，需要安装客户端软件，如 CuteFTP 等。

FTP 服务采用的就是 C/S 结构，安装了 FTP 服务的计算机就是服务器端，安装了 CuteFTP 等软件的计算机就是客户端。使用 Outlook Express 等软件收发电子邮件，采用的是 C/S 结构。

2.B/S 和 C/S 的比较

比较内容	C/S 结构	B/S 结构
客户端安装与维护	需要安装客户端软件，维护、升级时服务器和每台客户端都要操作，工作量较大	不需要安装客户端软件，只要使用浏览器上网就行，维护、升级只要在服务器上操作就行
对客户端、服务器的要求	客户端和服务端都能够处理任务，对客户机要求较高，服务器压力较小	客户端只能完成简单功能，绝大部分工作由服务器承担，服务器的负担较重
客户端响应速度	客户端响应快	页面动态刷新、响应速度明显降低
对客户端、操作系统的要求	对客户端的操作系统有要求	对客户端的操作系统没有要求
适合场合	更适合于局域网	更适合于广域网

四、计算机网络分类

分类方法	分类结果
按覆盖范围	局域网（LAN）、广域网（WAN）、城域网（MAN）
按交换方式	电路交换网络、报文交换网络、分组交换网络
按网络拓扑结构	星型网络、树型网络、总线型网络、环型网络和网状网络
按传输介质	有线网、无线网
按网络通信方式	点对点网络、广播网络

按网络控制方式	集中式网络、分散式网络、分布式网络
按网络组件功能	对等网络、客户机/服务器网络、混合网络

五、网络性能指标

指标项	指标描述
连通性	网络组件间的互连通性
吞吐量	单位时间内传送通过网络中给定点的数据量
带宽	单位时间内所能传送的比特数
传输延时	数据分组在网络传输中的延时时间

六、计算机网络拓扑结构

（一）网络拓扑结构含义

拓扑学是一种研究与大小距离无关的几何图形的方法。网络拓扑结构是指网络连接线路所构成的几何图形。

（二）网络拓扑结构分类

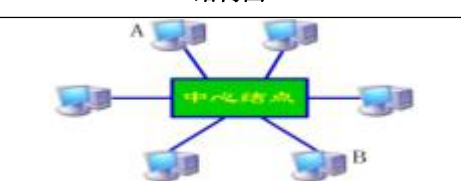
1.总线型网络拓扑结构

特点	结构图
1.各计算机地位平等 2.无中心控制节点 3.易于扩展、安装 4.费用低 5.局部节点出故障不影响整体	

2.环型网络拓扑结构

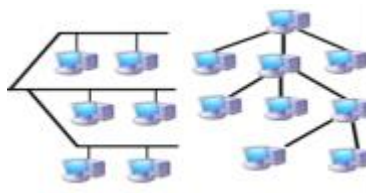
特点	结构图
1.实时性好 2.可扩充性差 3.可靠性差，局部节点故障可导致全网瘫痪，故障检测困难	

3.星型网络拓扑结构

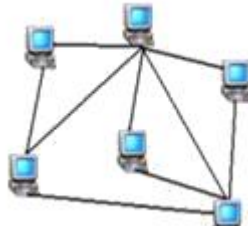
特点	结构图
1.结构简单、易维护、扩充 2.电缆成本高 3.中心节点出故障，导致全网瘫痪	

4.树型网络拓扑结构

特点	结构图
----	-----

1.易于扩展，故障易于隔离、可靠性高 2.电缆成本高 3.对根节点依赖大	
--	--

5.网型网络拓扑结构

特点	结构图
1.可靠性高 2.不易维护，线路成本高 3.性能好，路径选择复杂	

七、多路复用技术

（一）什么是复用技术

一般来说，正在通信的两个站点不会完全用尽数据链路的全部带宽。“复用”就是使一条数据链路能同时传输多路信号的一组技术。复用技术最常用在使用大容量光纤、同轴电缆或微波链路的长途通信方面，以及广域网的主干连接。

（二）多路复用技术分类

多路复用技术可以分为：频分多路复用技术 FDM（Frequency Division Multiplexing）、时分多路复用技术 TDM（Time Division Multiplexing）、波分多路复用技术 WDM（Wavelength Division Multiplexing）、码分多路复用技术 CDMA（Code Division Multiple Access）、空分多路复用技术 SDM（Space Division Multiplexing）。

（三）频分复用

1.频分复用的概念

频分复用是一种模拟多路复用技术，用于将多路模拟信号合成为一路复合信号。用于链路带宽大于要传输的几路信号带宽之和的情况。每路信号都被调制到一个不同的载波频率上，然后组合成一个复合信号。各载波频率之间应有一定间隔（防护频带），保证各路信号不会重叠。

2.频分复用应用实例

ADSL(非对称数字用户线路)，利用现有电话线(实际带宽 1.1MHz)实现宽带网络连接。非对称(Asymmetric)的含义：下行速率大于上行。采用频分复用技术，分配两个频带(上行和下行)，实现上网和打电话同时进行，传输距离可达 5.5 千米。

（四）波分复用

1.波分复用概念

不同频率的多路光线在同一光纤上传输，即在一根光纤上采用频分复用技术，承载若干不同频率的光信号。每一种颜色（波长）的光承载一个数据信道。

波分复用简称 WDM（Wavelength Division Multiplexing）技术非常复杂，原理却非常简单：光源的

组成与分离由棱镜完成。

一般认为，信道间距大于 1nm 且信道总数低于 8 以下，称之为 WDM 系统,反之，若波道间距小于 1 nm 且波道总数大于 8，即称之为密集波分复用 DWDM 系统。采用 DWDM 以后单根光纤可以传输的数据流量达到 400 Gbps 以上。

2.波分复用应用实例

铁通公司已利用 DWDM 等技术建成了先进的京沪穗环、东北环、西北环、西南环、东南环等五个高速传输网。

Cernet 2 和中国下一代互联网示范工程 CNGI 也采用 DWDM 构建高速主干网。

（五）同步时分复用

1.同步时分复用概念

同步时分复用（Time Division Multiplexing，简称 TDM）是一种数字复用技术，用于将多个低速通道组合成为一个高速通道。将信道用于传输的时间划分为若干个时间片；每个用户分得一个时间片；在每个用户占有的时间片内，用户使用通信信道的全部带宽。

如果源端发送的是模拟信号，复用前要先转换为数字信号。

2.同步时分复用

复用器将不同的输入交替组合成帧，然后送入传输链路。

传输链路的容量必须能容纳所有的输入。如果上图中每路输入的带宽是 9.6kbps，传输链路所需总带宽至少要 48kbps。

因为将每个时隙分配给特定的输入线路，如果这些输入线路没有全部进入工作状态，就会出现空闲的时隙。

（六）统计时分复用

使用统计时分复用时，时隙并未预先分配给特定的数据源，而是按需进行动态分配。用户数据先进入缓存，然后被尽快地通过可用的时隙传送出去。对统计复用器而言，存在 n 条输入线路，但 TDM 帧中只有 k ($k < n$) 个时隙可用。所以复用线路上的数据率小于各输入线路数据率的总和。

在输入端，复用器扫描输入缓存区，搜集数据，直到一个帧被填满，然后发送这个帧。在输出端，复用器接收一个帧，然后将各时隙中的数据分发给相应的输出缓存区。

第二节 计算机网络体系结构与网络协议

一、网络体系结构概念

（一）体系结构的概念

计算机网络的各层及其协议的集合称为网络的体系结构。

（二）网络协议的概念

网络中数据交换的规则、标准或约定称为网络协议，类似于交通规则。网络协议由语法、语义和同步三要素构成。

（三）网络协议三要素

语法：确定通信双方“如何讲”，定义了数据格式、编码和信号电平等。

语义：确定通信双方“讲什么”，定义了用于协调同步和差错处理等控制信息。

同步：确定通信双方“讲话的次序”，定义了速度匹配和排序等。

二、网络体系结构参考模型

（一）OSI 参考模型

1.OSI 参考模型简介

OSI 含义	开放系统互联
OSI 提出的目的	使不同厂家的网络产品实现互联和通信
OSI 的特点	开放性
谁提出的 OSI	ISO 国际标准化组织

2.OSI 参考模型的 7 个层次

物理层——数据链路层——网络层——传输层——会话层——表示层——应用层。

3.各层功能

（1）物理层(Physical Layer)

物理层是 OSI 参考模型的最低层，它利用传输介质为数据链路层提供物理连接。它主要关心的是通过物理链路从一个节点向另一个节点传送比特流，物理链路可能是铜线、卫星、微波或其他通讯媒介。

（2）数据链路层(Data Link Layer)

数据链路层是为网络层提供服务的，解决两个相邻节点之间的通信问题，传送的协议数据单元称为数据帧。

数据帧中包含物理地址（又称 MAC 地址）、控制码、数据及校验码等信息。该层的主要作用是通过校验、确认和反馈重发等手段，将不可靠的物理链路转换成对网络层来说无差错的数据链路。

此外，数据链路层还要协调收发双方的数据传输速率，即进行流量控制，以防止接收方因来不及处理发送方来的高速数据而导致缓冲器溢出及线路阻塞。

（3）网络层(Network Layer)

网络层是为传输层提供服务的，传送的协议数据单元称为数据包或分组。该层的主要作用是解决如何使数据包通过各节点传送的问题，即通过路径选择算法（路由）将数据包送到目的地。另外，为避免

通信子网中出现过多的数据包而造成网络阻塞，需要对流入的数据包数量进行控制（拥塞控制）。当数据包要跨越多个通信子网才能到达目的地时，还要解决网际互连的问题。

(4) 传输层(Transport Layer)

传输层的作用是为上层协议提供端到端的可靠和透明的数据传输服务，包括处理差错控制和流量控制等问题。该层向高层屏蔽了下层数据通信的细节，使高层用户看到的只是在两个传输实体间的一条主机到主机的、可由用户控制和设定的、可靠的数据通路。

传输层传送的协议数据单元称为段或报文。

(5) 会话层(Session Layer)

会话层主要功能是管理和协调不同主机上各种进程之间的通信（对话），即负责建立、管理和终止应用程序之间的会话。会话层得名的原因是它很类似于两个实体间的会话概念。例如，一个交互的用户会话以登录到计算机开始，以注销结束。

(6) 表示层(Presentation Layer)

表示层处理流经节点的数据编码的表示方式问题，以保证一个系统应用层发出的信息可被另一系统的应用层读出。如果必要，该层可提供一种标准表示形式，用于将计算机内部的多种数据表示格式转换成网络通信中采用的标准表示形式。数据压缩和加密也是表示层可提供的转换功能之一。

(7) 应用层(Application Layer)

应用层是 OSI 参考模型的最高层，是用户与网络的接口。该层通过应用程序来完成网络用户的应用需求，如文件传输、收发电子邮件等。

(二) TCP/IP 参考模型

1.TCP/IP 参考模型简介

TCP/IP 含义	传输控制协议/网际协议
为什么叫 TCP/IP 参考模型	这个模型中包含了很多协议，但 TCP 协议和 IP 协议是最重要的协议，所以叫 TCP/IP 模型
谁提出的 TCP/IP 参考模型	美国国防部赞助的 ARPANET

TCP/IP 参考模型：大致可分成四层，是一个协议集合，TCP 协议和 IP 协议是最重要的核心协议。IP 协议的工作是把数据包从一个地方传递到另一个地方。TCP 协议的工作是对数据包进行管理 with 校核，保证数据包的正确性。TCP/IP 协议是组建局域网的首选协议也是因特网的主要协议。

2.TCP/IP 参考模型各层的功能

层	功能
应用层	向用户提供一组常用的应用程序，比如电子邮件、文件传输访问、远程登录。
传输层	提供应用程序间的通信。其功能包括：格式化信息流；提供可靠传输。
网络层	负责相邻计算机之间的通信，处理数据报、路径、流量控制、拥塞。
网络接口层	定义物理介质的各种特性，处理数据帧。

3.TCP/IP 协议组

协议	功能	特点
网际协议—IP	1.对数据包进行寻址和路由	是一个无连

	2.分割和重编在传输层被分割的数据包	接协议
网际控制报文协议— ICMP	为 IP 协议提供差错报告	
网际主机组管理协议— IGMP	负责点到多点的数据包传输	
传输控制协议—TCP	1.数据分段和重组 2.流量控制和差错报告	面向连接的 协议
用户数据报协议—UDP	一对多和多对多数据传输，短信传输	无连接协议
地址解析协议（ARP） 反向地址解析协议 （RARP）	将源主机和目的主机的 IP 地址与它们物理地址（MAC）相匹配	

4.TCP/IP 参考模型和 OSI 模型对比

OSI 参考模型	设备	TCP/IP 参考模型	协议
应用层		应用层	HTTP、FTP、Telnet、SMTP、POP3、DNS
表示层			
会话层			
传输层		传输层	TCP、UDP
网络层	路由器	网络层	IP、ARP、RARP、ICMP
数据链路层	交换机、网桥	网络接口层	
物理层	中继器、集线器		

5.TCP 与 UDP

TCP（Transmission Control Protocol，传输控制协议）是一种面向连接的、可靠的、基于字节流的传输层通信协议。在简化的计算机网络 OSI 模型中，它完成第四层传输层所指定的功能，用户数据报协议（UDP）是同一层内另一个重要的传输协议。在因特网协议族（Internet protocol suite）中，TCP 层是位于 IP 层之上，应用层之下的中间层。不同主机的应用层之间经常需要可靠的、像管道一样的连接，但是 IP 层不提供这样的流机制，而是提供不可靠的包交换。TCP 提供一种面向连接的、可靠的字节流服务。面向连接意味着两个使用 TCP 的应用（通常是一个客户和一个服务器）在彼此交换数据包之前必须先建立一个 TCP 连接。

UDP 是 User Datagram Protocol 的简称，中文名是用户数据报协议，是 OSI（Open System Interconnection，开放式系统互联）参考模型中一种无连接的传输层协议，提供面向事务的简单不可靠信息传送服务，在网络中它与 TCP 协议一样用于处理数据包，是一种无连接的协议。在 OSI 模型中，在第四层——传输层，处于 IP 协议的上一层。UDP 有不提供数据包分组、组装和不能对数据包进行排序的缺点，也就是说，当报文发送之后，是无法得知其是否安全完整到达的。UDP 用来支持那些需要在计算机之间传输数据的网络应用，包括网络视频、会议系统在内的众多客户/服务器模式的网络应用都需要使用 UDP 协议。

与所熟知的 TCP（传输控制协议）协议一样，UDP 协议直接位于 IP（网际协议）协议的顶层。根据 OSI（开放系统互连）参考模型，UDP 和 TCP 都属于传输层协议。UDP 协议的主要作用是将网络数据流量压缩成数据包的形式。一个典型的数据包就是一个二进制数据的传输单位。每一个数据包的前 8 个字节用来包含报头信息，剩余字节则用来包含具体的传输数据。

UDP 报文没有可靠性保证、顺序保证和流量控制字段等，可靠性较差。但是正因为 UDP 协议的控制选项较少，在数据传输过程中延迟小、数据传输效率高，适合对可靠性要求不高的应用程序，或者可以保障可靠性的应用程序，如 DNS、TFTP、SNMP 等。

第三节 网络通信基础

一、通信系统简介

通信系统是用以完成信息传输过程的技术系统的总称。现代通信系统主要借助电磁波在自由空间的传播或在导引媒体中的传输机理来实现，前者称为无线通信系统，后者称为有线通信系统。一般由信源（发端设备）、信宿（收端设备）和信道（传输媒介）等组成，被称为通信的三要素。

二、数据通信分类

（一）按信息分类

按照信息可以分为：电话通信系统、数据通信系统、有线电视系统。

（二）按调制分类

按照调制可以分为：基带传输、调制传输。

（三）按传输信号特征分类

按照传输信号可以分为：模拟通信系统、数字通信系统。

三、数据通信方式

异步传输：以字节为单位独立传输，传输间隔任意。

同步传输：以数据块为单位整体传输。

四、数据传输方向

（一）单工通信

指传送的数据始终是一个方向，而不能进行与此相反方向的传送，好像单行线一样。

（二）半双工通信

指传送的数据可以在两个方向传送，但不是同时传送。就像单线铁路一样，某时允许 A 站发出列车到 B 站，另一时刻允许 B 站发出列车到 A 站，火车往返运行要由调度控制。

（三）双工通信

指传送的数据可以同时两个方向传送，就像宽马路中间划一条黄线，只要司机开车不越黄线逆行，就不会发生碰撞。

五、数据通信的主要技术指标

（一）带宽（车道）

所能传输的电磁波的频率范围。

（二）数据传输率（车速）

每秒传输的比特数。

六、数据传输类型

（一）基带传输

数字信号被称为数字基带信号，在信道中直接传输这种基带信号就称为基带传输。在基带传输中，

整个信道只传输一种信号，通信信道利用率低。

由于在近距离范围内，基带信号的功率衰减不大，从而信道容量不会发生变化，因此，在局域网中通常使用基带传输技术。

在基带传输中，需要对数字信号进行编码来表示数据。

（二）频带传输

频带传输就是先将基带信号变换（调制）成便于在模拟信道中传输的、具有较高频率范围的模拟信号（称为频带信号），再将这种频带信号在模拟信道中传输。

计算机网络的远距离通信通常采用的是频带传输。

基带信号与频带信号的转换是由调制解调技术完成的。

（三）宽带传输

带宽划分，分别传输数字、音频、视频信号。

七、数据交换技术的分类

在一个通信网络系统中，通常采用的数据交换技术有：电路交换、报文交换和分组交换。

交换技术	工作原理	特点	使用范围
电路交换	建立连接→通信→释放连接	面向连接，独占信道； 线路利用率低； 不同类型用户不能通信。	传统电话
报文交换	存储→选择空闲线路→转发	无连接，信道利用率高； 不同类型用户可通信； 可多地址转发； 有时延，不适合实时通信。	电报电子信箱
分组交换	报文划分成分组→给分组加“首部”→存储→转发→报文重组。 采用“虚电路”和“数据报”两种交换技术。	无连接，线路利用率高； 传输质量好，可靠性高； 经济性好； 排队制，支持优先级； 时延不固定。	计算机网络；IP 电话。

第四节 IP 地址

一、IP 地址的格式

（一）IP 地址

网络之间实现计算机的相互通信，必须有相应的地址标识，这个地址标识称为 IP 地址。IP 地址是唯一标识出主机所在的网络及其网络中位置的编号。

（二）IP 地址的组成概述

IP 地址是由 32 个二进制位 (bit) 组成。常用“点分十进制”方式来表示。即将 IP 地址分为 4 个字节，每个字节以十进制数 (0~255) 来表示，各个数之间以英文圆点来分隔。

每个 IP 地址有两部分组成，网络标识 NET-ID 和主机标识 HOST-ID。网络标识确定了该主机所在的物理网络，主机标识确定了在某一物理地址上的一台主机。

	192.	168.	0.	3
	第1字节	第2字节	第3字节	第4字节
	0	NET-ID	HOST-ID	
A	1 0	NET-ID	HOST-ID	
B	1 1 0	NET-ID	HOST-ID	
C	1 1 1 0	NET-ID	HOST-ID	

由 IP 地址确定网络地址的方法是，将网络号不变，主机号全变成 0。

（三）IP 地址的分类

将 IP 地址空间划分为 A、B、C 三种基本类型，每类有不同长度的网络标识和主机标识。还有 D 类用于组播，E 类用于试验和保留。

IP 地址	地址范围	可支持的网络数目	每个网络支持的主机数
A 类	1.x.y.z~126.x.y.z	126	1,677,214
B 类	128.x.y.z~191.x.y.z	16,384	65,534
C 类	192.x.y.z~223.x.y.z	2,097,152	254

判断 IP 地址对应的网络类型，主要是依据左边第一段来判断，第一段小于 128 是 A 类，第一段大于等于 128 小于 192 是 B 类，大于等于 192 是 C 类。

（四）特殊 IP 地址

地址	说明
全 0 主机号 (host-id)	是网络地址 如 C 类地址：192.168.2.1，其网络地址为 192.168.2.0
全 1 主机号 (host-id)	广播地址 如：192.168.2.1 它的广播地址 192.168.2.255

127.X.Y.Z	主机对自身进行测试的回送地址 常用的 127.0.0.1
-----------	---------------------------------

二、网络掩码

（一）网络掩码的含义

将 IP 地址的 net-id 用全 1 表示，host-id 用全 0 表示，就是网络掩码。

A 类 IP 地址的网络掩码：255.0.0.0。

B 类 IP 地址的网络掩码：255.255.0.0。

C 类 IP 地址的网络掩码：255.255.255.0。

（二）网络掩码的功能

1.切割网络，增加网络数

为了便于管理,可将 A、B、C 三类网络划分为更小的网络。

2.判断主机位置

当两台主机通信时，可根据网络掩码判断他们是否在同一网络内。若在，信息就在网内传，若不在，信息就通过路由传递。

（三）网络掩码如何划分子网

将主机号划出一定位数，做子网号。注意:从左边开始划，拿出的几位一定是连续的。

C 类网络掩码为：

11111111.11111111.11111111.00000000 即 255.255.255.0。

若将主机号的 2 位拿出作子网号，则子网掩码为：

11111111.11111111.11111111.11000000 即 255.255.255.192。

划分了 $2^2=4$ 个子网。

三、IP 地址的管理

IP 地址按照分级的方式管理。

IANA，负责全球 IP 地址与域名的管理。

CNNIC（中国互联网络信息中心），负责中国 IP 地址与域名的管理。

四、IPv6

绝大多数 IP 地址已被美国所占有，使原本有限的 IP 地址资源出现分配严重不均衡的局面。中国，世界上人口最多的国家，所分得的大多是 C 类地址，A 类和 B 类地址几乎没有。

IPv4 由 32 个二进制位(bit)组成，IPv6 由 128 个二进制位(bit)组成。

IPv6 地址数量非常多，安全机制也增强了。

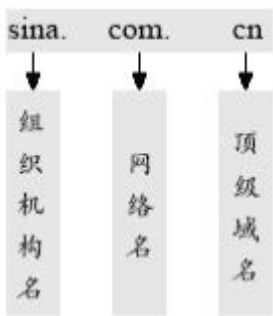
第五节 DNS 域名系统

一、什么是域名

域名 (Domain Name) 是因特网上一个服务器或一个网络系统的名字，网络间通过域名进行相互访问，在全世界没有重复的域名。

二、域名解析

因特网上的计算机之间是通过 IP 地址来进行通信的，域名必须转换成 IP 地址才能实现对网站的访问，这项工作由域名解析系统（DNS）来完成。这一过程称为域名解析。



三、域名的基本结构

一个完整的域名由两个或两个以上部分组成，各部分之间用英文的句号“.”来分隔，例如下列域名：yahoo.com，yahoo.ca.us，yahoo.co.uk。其中第一个域名由二部分组成，第二个域名和第三个域名由三部分组成。

在一个完整的域名中，最后一个“.”的右边部分称为顶级域名或一级域名（TLD），在上面的域名例子中，com.us 和 uk 是顶级域名。最后一个“.”的左边部分称为二级域名（SLD），例如，域名 yahoo.com 中 yahoo 是二级域名，域名 yahoo.ca.us 中 ca 是二级域名，而域名 yahoo.co.uk 中 co 是二级域名。二级域名的左边部分称为三级域名，三级域名的左边部分称为四级域名，以此类推。例如，域名 yahoo.ca.us 和 yahoo.co.uk 中 yahoo 是三级域名。

顶级域名	意义
COM	商业组织
EDU	教育机构
GOV	政府部门
MIL	军事部门
NET	主要网络支持机构
ORG	非赢利组织
INT	国际组织

四、域名命名的一般规则

（一）域名中包含的字符

1.26 个英文字母

2.10 个阿拉伯数字

3. “-” (英文中的连字符)

（二）域名中字符的组合规则

在域名中，不区分英文字母的大小写。

对于一个域名的长度是有一定限制的。例如，注册 CN 下域名，三级域名的长度不能超过 20 个字符。

五、域名的管理

全球域名的管理职责由“因特网域名与地址管理机构(ICANN)”来承担，该组织是一个非盈利性组织。

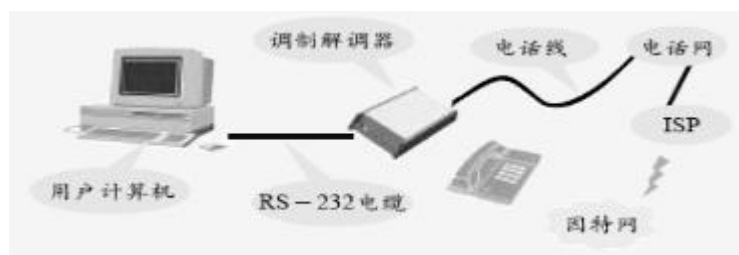
我国的域名管理职责由“中国互联网络信息中心(CNNIC)”承担。

第六节 因特网服务

一、接入因特网

拨号上网，通过电话线与因特网建立连接，也可以通过局域网接入因特网，但一般要通过代理服务器。

（一）拨号上网



拨号上网指客户拥有上网终端（通常是计算机）使用调制解调器（Modem）通过电话线以拨号的方式进行上网。调制解调器是调制器（Modulator）与解调器（Demodulator）的简称。所谓调制，就是把数字信号转换成电话线上传输的模拟信号；解调，即把模拟信号转换成数字信号。合称调制解调器。

（二）局域网接入



（三）代理服务器

1. 代理服务器的作用

充当局域网与外部网络连接的出口，同时将内部网络结构的状态对外屏蔽起来，使外部用户不能直接访问内部网络。从这一点上说，代理服务器就充当了网关。

临时存储大量的网上信息资源。

对局域网内用户访问外网的权限进行一定限制。

2. 在浏览器中设置代理服务器

在 IE 图标上右击→属性（或在 IE 窗口中选“工具”中的“Internet 选项”），打开“Internet 选项”窗口，再选“连接”→“局域网设置”→“代理服务器”，在其中作相应的设置。

二、因特网服务组织

名称	说明
ISP	因特网服务提供商
ICP	因特网内容提供商
ASP	因特网应用服务提供商

三、服务

（一）WWW 服务

1.WWW 含义

万维网：Word Wide Web（WWW），世界范围的网。万维网采用 B/S 工作模式。万维网的网页是一种“超文本文件”，是用超文本标记语言（HTML）编写的。

2.URL 的含义及功能

统一资源定位符（URL），表明某网页在网络中的位置。

URL 格式：协议名称://主机名/目录名/文件名

例 1：http://www.ntzx.net.cn/webfile/index.htm

例 2：ftp://ftp.ntzx.cn/downfile/student.rar

HTTP：超文本传输协议，是 TCP/IP 协议中的一种，使用 TCP 协议。

（二）FTP 服务

1.FTP 简介

文件传输协议（FTP）也是因特网上重要服务之一。FTP 也是 TCP/IP 协议中的一种，使用 TCP 协议。FTP 一般采用 C/S 工作模式。

2.如何进行 FTP

三种途径可以进行 FTP:

（1）使用 Windows 自带的 ftp 命令

（2）使用 IE 浏览器

在 IE 地址栏中输入如下格式的 URL 地址：

ftp://[用户名：口令@]FTP 服务器域名

（3）安装并运行专门的 FTP 客户程序

例如 LeapFTP、CuteFTP、WSFTP 等，它们都是专门用来连接 FTP 服务器的应用程序，提供了图形化的用户界面。

（三）Telnet 服务

是指本地计算机通过 Internet 访问远程计算机上的硬件资源、软件资源和信息资源的过程。对于限制公开访问的远程主机，登录时要输入用户名和密码。远程登录（Telnet）也是 TCP/IP 协议中的一种，采用 C/S 工作模式。随着 www 的普及，Telnet 已少有使用。

（四）E-mail 服务

1.协议

POP3 即邮局协议版本 3，用来接收电子邮件。

SMTP 即简单邮件传输协议，用来发送电子邮件。

2.格式

E-mail 地址的统一格式是：用户名@域名，“用户名”是用户申请的账号，“域名”是 E-mail 服务器的域名，例如：apple@163.com。

第七节 局域网技术

一、局域网标准 IEEE802

（一）IEEE802 标准列表

标准	说明
IEEE802	是一个局域网标准系列
IEEE802.2	逻辑链路控制 (LLC)
IEEE802.3	CSMA/CD 访问控制方法与物理层规范
IEEE802.4	Token-Bus 访问控制方法与物理层规范
IEEE802.5	Token-Ring 访问控制方法
IEEE802.6	城域网访问控制方法与物理层规范
IEEE802.7	宽带局域网访问控制方法与物理层规范
IEEE802.8	FDDI 访问控制方法与物理层规范
IEEE802.9	综合数据话音网络
IEEE802.10	网络安全与保密
IEEE802.11	无线局域网访问控制方法与物理层规范，当前主流技术 WIFI
IEEE 802.15	无线个人网技术标准，其代表技术是 zigbee，蓝牙

（二）蓝牙、WIFI、ZigBee 比较

类型	标准	速度	通信距离	频段	安全性	主要应用
ZigBee	IEEE802.15.4	100K	0-20 米	2.4GHz	中	无线传感器，医疗等自动控制和远程控制。
WIFI	IEEE802.11	11-54M	0-200 米	2.4GHz	低	无线上网
蓝牙	IEEE802.15.1	1M	0-100 米	2.4GHz	高	移动设备互联

二、组建小型局域网的过程

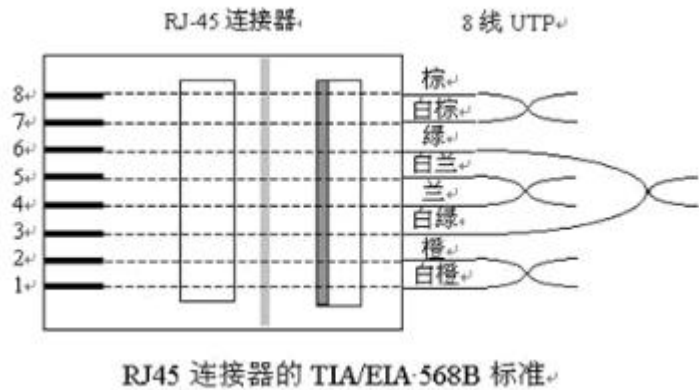
- （一）通过需求分析确定网络规模
- （二）选择局域网技术
- （三）确定网络拓扑结构
- （四）选择硬件
- （五）选择网络协议
- （六）选择软件
- （七）配置参数，测试运行

三、网线制作方法

直通线：线两头的排序标准一样，比如都是 568B，不同的设备相连用直通线，比如计算机和交换机。

交叉线：线两头的排序标准一样，一头是 568A，一头是 568B，相同的设备相连用交叉线，比如计算机和计算机相连，即常说的 1--3、2--6 交接法。

标准	排线规律
568A	绿白、绿、橙白、蓝、蓝白、橙、棕白、棕
568B	橙白、橙、绿白、蓝、蓝白、绿、棕白、棕



四、局域网 IP 配置

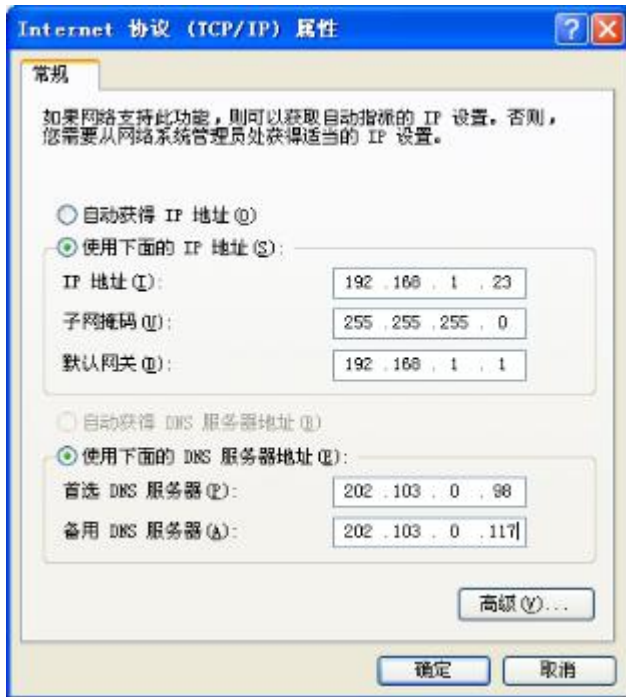
（一）静态 IP 分配和动态 IP 分配

静态 IP 分配：给每台计算机分配一个固定的地址。优点：易于管理；缺点：浪费 IP 地址资源。

动态 IP 分配：把 IP 地址暂时分配给用户使用，不使用时由服务器收回。优点：实现了 IP 地址的动态分配，节约了 IP 地址资源，缺点安全性较差。

（二）设置静态 IP 地址和网关、子网掩码、DNS

右键点击“网上邻居”，选择“属性”，查看设置组件“TCP/IP 协议”的属性。



（三）查看本机 IP 地址

在“开始”——“运行”里输入：cmd，再输入：ipconfig。

右键点击“网上邻居”，选择“属性”，查看组件“TCP/IP 协议”的属性。

五、常用网络测试命令

命令	功能	举例
NET	它可以轻松的管理本地或者远程计算机的网络环境，以及各种服务程序的运行和配置。	NET SHARE 查阅本地计算机上共享文件。
Ping	PING (Packet Internet Groper)，因特网包探索器，用于测试网络连接量的程序。Ping 发送一个 ICMP(Internet Control Messages Protocol)即因特网信报控制协议；回声请求消息给目的地并报告是否收到所希望的 ICMP echo（ICMP 回声应答）。它是用来检查网络是否通畅或者网络连接速度的命令。	Ping www.baidu.com 检测本节和百度之间是否连通。
Netstat	检测计算机与网络之间详细的连接情况,可以得到以太网的统计信息并显示所有协议（TCP 协议、UDP 协议以及 IP 协议等）的使用状态。	Netstat -a 所有的有效连接信息列表。
IPConfig	显示网卡的 IP 地址、子网掩码和缺省网关值。	IPconfig
ARP	用于查看或指定对应 IP 地址的网卡物理地址。	arp -a
Tracert	显示数据包到达目的主机所经过的路径。	Tracert www.sohu.com
Route	查看路由表或编辑路由表。	route print 显示路由表中的内容。
Nslookup	IP 地址和主机名称的互相查询。	Nslookup www.sina.com.cn

第八节 网络新技术

一、Web 2.0 技术

Web2.0 已成为实际意义上的标准互联网运用模式。以博客(Blogging)、内容聚合(RSS)、百科全书(WiKi)、社会网络(SNS)和对等网络(P2P)为代表的 Web 2.0 应用已被用户广泛地接受和使用。

与 Web 1.0 时代相比，Web 2.0 时代满足 7 大原则：

- (一) 互联网作为平台；
- (二) 利用集体智慧；
- (三) 数据是核心；
- (四) 软件发布周期的终结；
- (五) 轻量型编程模型；
- (六) 软件超越单一设备；
- (七) 丰富的用户体验。

二、云计算

Web 2.0 为云计算的出现提出了内在需求。云计算的出现使得人们可以通过互联网获取各种服务，并且可以实现按需支付的要求，随着电信和互联网网络的融合发展，云计算将成为跨越电信和互联网的通用技术。直观而言，云计算（Cloud Computing）是指由几十万甚至上百万台廉价的服务器所组成的网络，为用户提供需要的计算机服务，用户只需要一个能够上网的设备，比如一台笔记本或者手机，就可以获得自己需要的一切计算机服务。作为一种基于互联网的新兴应用模式，云计算通过网络把多个成本相对较低的计算实体整合成一个具有强大计算能力的完美系统，并借助 SaaS、PaaS、IaaS、MSP 等先进的商业模式把这强大的计算能力分布到终端用户手中，其核心理念就是通过不断提高自身处理能力，进而减少用户终端的处理负担，最终使用户终端简化成一个单纯的输入输出设备，并能按需享受“云”的强大计算处理能力，从而更好地提高资源利用效率并节约成本。通过云计算所提供的应用，用户将不再依赖某一特定的计算机来访问、处理自己的数据，只要可以通过网络连接至自己的数据，就能随时检索自己的文件、继续处理上次未完成的工作并完成保存。事实上，人们已开始享受着“云”所带来的好处。以谷歌(Google)用户为例，免费申请一个账号，就可以利用 GoogleDoc、Gmail 和 Picasa 服务来保存私有资源。

云计算具有以下特点：

- (一) 超大规模；
- (二) 高可扩展性；
- (三) 高可靠性；
- (四) 虚拟化；
- (五) 按需服务；
- (六) 极其廉价；
- (七) 通用性强。

Web 2.0 提供了云计算的接入模式，也为云计算培养了用户习惯。随着云计算平台的建立，将使运营商移动互联网应用开发和运营的成本大大降低。

三、云存储

云存储是一个以数据存储和管理为核心的云计算系统。它是指通过集群应用、网格技术或分布式文件系统等功能，将网络中大量各种不同类型的存储设备通过应用软件集合起来协同工作，共同对外提供数据存储和业务访问功能的一个系统。

在常见的局域网系统中，我们为了能更好的使用局域网，一般来讲，使用者需要非常清楚地知道网络中每一个软硬件的型号和配置，比如采用什么型号交换机，有多少个端口，采用了什么路由器和防火墙，又是如何配置的。当我们使用广域网时，我们只知道用户名和密码就可以使用，至于广域网中到底有多少个路由器、交换机等，使用者是不需要知道的。这样来看广域网对于具体的使用者来说是完全透明的。云存储就类似于广域网，云存储对使用者来说不是一个具体的设备，而是一个由许多的存储设备和服务器所构成的集合体。使用者使用云存储并不是使用一个具体的设备，而是使用整个云存储系统带来的一种数据访问服务。

四、物联网

物联网是新一代信息技术的重要组成部分，也是“信息化”时代的重要发展阶段。其英文名称是：“Internet of things (IoT)”。顾名思义，物联网就是物物相连的互联网。这有两层意思：其一，物联网的核心和基础仍然是互联网，是在互联网基础上的延伸和扩展的网络；其二，其用户端延伸和扩展到了任何物品与物品之间，进行信息交换和通信，也就是物物相息。物联网通过智能感知、识别技术与普适计算等通信感知技术，广泛应用于网络的融合中，也因此被称为继计算机、互联网之后世界信息产业发展的第三次浪潮。物联网是互联网的应用拓展，与其说物联网是网络，不如说物联网是业务和应用。因此，应用创新是物联网发展的核心，以用户体验为核心的创新 2.0 是物联网发展的灵魂。

五、3D 打印技术

3D 打印，即快速成型技术的一种，它是一种以数字模型文件为基础，运用粉末状金属或塑料等可黏合材料，通过逐层打印的方式来构造物体的技术。3D 打印通常是采用数字技术材料打印机来实现的。常在模具制造、工业设计等领域被用于制造模型，后逐渐用于一些产品的直接制造，已经有使用这种技术打印而成的零部件。该技术在珠宝、鞋类、工业设计、建筑、工程和施工（AEC）、汽车，航空航天、牙科和医疗产业、教育、地理信息系统、土木工程、枪支以及其他领域都有所应用。

六、可穿戴技术

可穿戴技术是 20 世纪 60 年代，美国麻省理工学院媒体实验室提出的创新技术，利用该技术可以把多媒体、传感器和无线通信等技术嵌入人们的衣着中，可支持手势和眼动操作等多种交互方式。

通过“内在连通性”实现快速的数据获取、通过超快的分享内容能力高效地保持社交联系。摆脱传统的手持设备而获得无缝的网络访问体验。

可穿戴健康设备是随着可穿戴设备的产生发展而逐渐衍生出来的可穿戴设备的又一支。1960 年代以来，可穿戴式设备逐渐兴起。到了 70 年代，发明家 Alan Lewis 打造的配有数码相机功能的可穿戴式

计算机能预测赌场轮盘的结果。1977 年，Smith-Kettlewell 研究所视觉科学院的 C.C.Colin 为盲人做了一款背心，它把头戴式摄像头获得的图像通过背心上的网格转换成触觉意象，让盲人也能“看”得见，从广义上来讲，这可以算是世界上第一款可穿戴健康设备。

比较有代表性的产品有：Google Glass，苹果 Iwatch，Pebble Time。

第九节 计算机病毒与网络安全

一、计算机病毒概述

（一）计算机病毒的定义

计算机病毒是编制者在计算机程序中插入的破坏计算机功能或者数据的代码，能影响计算机使用，能自我复制的一组计算机指令或者程序代码。

（二）计算机病毒的特点

计算机病毒是一组程序代码，具有寄生性、传染性、潜伏性、隐蔽性、可触发性、破坏性、不可预见性等特点。

寄生性：计算机病毒寄生在其他程序之中，当执行这个程序时，病毒就起破坏作用，而在未启动这个程序之前，它是不易被人发觉的。

传染性：计算机病毒不但本身具有破坏性，更有害的是具有传染性，一旦病毒被复制或产生变种，其速度之快令人难以预防。计算机病毒是一段人为编制的计算机程序代码，这段程序代码一旦进入计算机并得以执行，它就会搜寻其他符合其传染条件的程序或存储介质，确定目标后再将自身代码插入其中，达到自我繁殖的目的。

潜伏性：一个编制精巧的计算机病毒程序，进入系统之后一般不会马上发作，可以在几周或者几个月内甚至几年内隐藏在合法文件中，对其他系统进行传染，而不被人发现，潜伏性愈好，其在系统中的存在时间就会愈长，病毒的传染范围就会愈大。

隐蔽性：计算机病毒具有很强的隐蔽性，有的可以通过病毒软件检查出来，有的根本就查不出来，有的时隐时现、变化无常，这类病毒处理起来通常很困难。

可触发性：病毒因某个事件或数值的出现，诱使病毒实施感染或进行攻击的特性称为可触发性。病毒具有预定的触发条件，这些条件可能是时间、日期、文件类型或某些特定数据等。病毒运行时，触发机制检查预定条件是否满足，如果满足，启动感染或破坏动作，使病毒进行感染或攻击；如果不满足，使病毒继续潜伏。

破坏性：计算机中毒后，可能会导致正常的程序无法运行，把计算机内的文件删除或受到不同程度的损坏。通常表现为：增、删、改、移。

不可预见性：不同类型的病毒，它们的代码千差万别，反病毒软件对病毒永远是滞后的。

（三）计算机病毒的分类

1.按照传播媒介分类

单机病毒：单机病毒的载体是磁盘，常见的是病毒从软盘传入硬盘，感染系统，然后再传染其他软盘，软盘又传染其他系统。

网络病毒：网络病毒的传播媒介不再是移动式载体，而是网络通道，这种病毒的传染能力更强，破坏力更大。

2.按照寄生方式和传染途径分类

引导型病毒：会去改写（即一般所说的“感染”）磁盘上的引导扇区（BOOT SECTOR）的内容，软盘或硬盘都有可能感染病毒。再不然就是改写硬盘上的分区表（FAT）。如果用已感染病毒的软盘来启动

的话，则会感染硬盘。引导型病毒几乎清一色都会常驻在内存中，差别只在于内存中的位置。

文件型病毒：主要以感染文件扩展名为.com、.exe 和.ovl 等可执行程序为主。它的安装必须借助于病毒的载体程序，即要运行病毒的载体程序，方能把文件型病毒引入内存，大多数文件型病毒都是常驻在内存中的。

混合型病毒：其综合了引导型和文件型病毒的特性，它的“性情”也就比引导型和文件型病毒更为“凶残”。这种病毒透过这两种方式来感染，更增加了病毒的传染性以及存活率。

宏病毒：是一种寄存于文档或模板的宏中的计算机病毒。一旦打开这样的文档，宏病毒就会被激活，转移到计算机上，并驻留在 Normal 模板上。从此以后，所有自动保存在文档都会“感染”上这种宏病毒，而且如果其他用户打开了感染病毒的文档，宏病毒又会转移到他的计算机上。

3.按照计算机病毒的破坏情况分类

良性计算机病毒：是指其不包含有立即对计算机系统产生直接破坏作用的代码。这类病毒为了表现其存在，只是不停地进行扩散，从一台计算机传染到另一台，并不破坏计算机内的数据。良性病毒取得系统控制权后，会导致整个系统和应用程序争抢 CPU 的控制权，时时导致整个系统死锁，给正常操作带来麻烦。有时系统内还会出现几种病毒交叉感染的现象，一个文件不停地反复被几种病毒所感染。

恶性计算机病毒：是指在其代码中包含有损伤和破坏计算机系统的操作，在其传染或发作时会对系统产生直接的破坏作用。这类病毒是很多的，如米开朗基罗病毒。

4.按照计算机病毒激活的时间分类

按照计算机病毒激活时间可分为：定时的和随机的，定时病毒仅在某一特定时间才发作，而随机病毒一般不是由时钟来激活的。

（四）蠕虫病毒

蠕虫病毒是一种常见的计算机病毒。它是利用网络进行复制和传播，传染途径是通过网络和电子邮件。最初的蠕虫病毒定义是因为在 DOS 环境下，病毒发作时会在屏幕上出现一条类似虫子的东西，胡乱吞吃屏幕上的字母并将其改形。蠕虫病毒是自包含的程序（或是一套程序），它能传播自身功能的拷贝或自身的某些部分到其他的计算机系统中（通常是经过网络连接）。比如近几年危害很大的“尼姆亚”病毒就是蠕虫病毒的一种，2007 年 1 月流行的“熊猫烧香”以及其变种也是蠕虫病毒。

（五）木马

木马，是指通过特定的程序（木马程序）来控制另一台计算机。木马通常有两个可执行程序：一个是控制端，另一个是被控制端。“木马”程序是目前比较流行的病毒文件，与一般的病毒不同，它不会自我繁殖，也并不“刻意”地去感染其他文件，它通过将自身伪装吸引用户下载执行，向施种木马者提供打开被种主机的门户，使施种者可以任意毁坏、窃取被种者的文件，甚至远程操控被种主机。

（六）黑客

黑客是利用不正当手段窃取计算机网络系统的口令和密码，非法进入计算机网络的人；黑客常用的攻击手段包括后门程序、信息炸弹、拒绝服务攻击和网络监听等。有一些别有用心之徒侵入他人系统后，会破坏文件或修改数据、盗窃内部信息，对国家安全、社会安全、公共秩序、个人合法权益造成极大的危害。因此我们需要采取一些方法预防黑客的入侵比如：安装必要的安全软件和防黑软件、杀毒软件和防火墙、关闭不必要的端口、不要回陌生人的邮件、隐藏 IP 地址等。

二、计算机病毒的传播途径

（一）移动设备

（二）网络

三、计算机病毒的检测预防与网络安全

（一）计算机病毒的检测

一般用户可以根据下列情况来判断系统是否感染病毒：

- 1.计算机的启动速度较慢且无故自动重启；工作中机器出现无故死机现象；
- 2.桌面上的图标发生了变化；
- 3.桌面上出现了异常现象：奇怪的提示信息，特殊的字符等；
- 4.在运行某一正常的应用软件时，系统经常报告内存不足；
- 5.文件中的数据被篡改或丢失；
- 6.音箱无故发生奇怪声音；
- 7.系统不能识别存在的硬盘；
- 8.当你的朋友向你抱怨你总是给他发出一些奇怪的信息，或你的邮箱中发现了大量的不明来历的邮件；
- 9.打印机的速度变慢或者打印出一系列奇怪的字符等。

（二）计算机病毒的预防

1.隔离来源

2.杀毒软件

杀毒软件的任务是扫描磁盘，查杀病毒。大部分杀毒软件还具有防火墙功能，可实时监控系统。一旦发现病毒，就会及时报警并拒绝打开染毒文件。由于新的病毒在不断地产生，所以必须及时更新杀毒软件。

常用杀毒软件：**360 杀毒软件、金山毒霸、百度杀毒、卡巴斯基、小红伞等。**

3.防火墙

防火墙是一个或一组网络设备，架在两个或两个以上的网络之间，用来加强访问控制，免得一个网络受到来自另一个网络的攻击。防火墙从实现方式上分成：硬件防火墙和软件防火墙两类。

4.加密解密技术

使用计算机加密所使用的算法有对称密钥加密算法和公开密钥加密算法。

对称密钥加密算法是使用同一密钥进行加密和解密的，又称会话密钥加密算法。

公开密钥加密算法是使用不同的密钥进行加密和解密的，又称非对称密钥加密算法。

5.安全防范措施

- （1）安装杀毒软件并经常升级。
- （2）选用合适的防火墙系统。
- （3）设置电脑和网络口令。
- （4）用安全类软件打补丁、更新漏洞。

- (5) 移动设备使用前先杀毒。
- (6) 不要打开来历不明的邮件、文件、连接和弹窗。
- (7) 备份文件。
- (8) 输入账号和密码时使用软键盘。

第十节 信息安全

一、信息安全的定义

信息安全主要包括以下五方面的内容，即需保证信息的保密性、真实性、完整性、未授权拷贝和所寄生系统的安全性。信息安全本身包括的范围很大，其中包括如何防范商业企业机密泄露、防范青少年对不良信息的浏览、个人信息的泄露等。

二、信息安全防范的基本方法

信息安全防范的基本方法包含物理防范和逻辑防范。

（一）物理防范

1.物理防范可以从**环境维护、防盗、防火、防静电、防雷击、防电磁泄露**几个方面着手。

（1）环境维护

实体设备的位置应远离噪声源、振动源；保持设备运行所需的温度、湿度、洁净度；远离火源和易被水淹没的地方；尽量避开强电磁场源；保持系统电源的稳定及可靠性

（2）防盗

应采取严格的防范措施。对于重要的计算机系统及外部设备，可安装防盗报警装置及制定安全保护措施

（3）防火

应经常检查重要部门的各种电路的安全性做好各种防火措施

（4）防静电

配备良好的接地系统，避免静电积储。此外，将容易产生静电的物体分开存放。防止由于静电放电损坏电路板。计算机显示器也会产生静电，注意不要将容易产生一静电的物体靠近它。

（5）防雷击

应根据被保护设备的特点和雷电侵入的不同途径，采用相应的防护措施，分类分级保护

（6）防电磁泄漏

一是抑制电磁发射，二是屏蔽隔离，三是相关干扰，采取各种措施使信息相关电磁发射泄漏即使被收到也无法识别。

2.物理安全的范畴

除了上述介绍的外，基于物理环境的容灾技术和物理隔离技术也属于物理安全的范畴。

（二）逻辑防范

逻辑防范可以从访问控制和信息加密方面着手。

1.访问控制

通过用户身份的识别和认证，一是可以鉴别合法用户和非法用户，阻止非法用户的访问。二是通过访问权限控制，即对用户访问哪些资源，对资源的使用权限等加以控制。

2.信息加密

常用的方法有数据加密和数字签名。

三、信息安全技术

（一）防火墙

1. 防火墙的概念

在网络中，所谓“防火墙”，是指一种将内部网和公众访问网（如 Internet）分开的方法，它实际上是一种隔离技术。防火墙是在两个网络通讯时执行的一种访问控制尺度，它能允许你“同意”的人和数据进入你的网络，同时将你“不同意”的人和数据拒之门外，最大限度地阻止网络中的黑客来访问你的网络。换句话说，如果不通过防火墙，公司内部的人就无法访问 Internet，Internet 上的人也无法和公司内部的人进行通信。

2. 防火墙的基本功能作用

- （1）网络安全的屏障。
- （2）强化网络安全策略。
- （3）对网络存取和访问进行监控审计。
- （4）防止内部信息的外泄。

（二）数字签名技术

数字签名在 ISO7498—2 标准中定义为：“附加在数据单元上的一些数据，或是对数据单元所作的密码变换，这种数据和变换允许数据单元的接收者用以确认数据单元来源和数据单元的完整性，并保护数据，防止被人（例如接收者）进行伪造”。

数字签名要实现的功能是我们平常的手写签名要实现功能的扩展。平常在书面文件上签名的主要作用有两点，一是因为对自己的签名本人难以否认，从而确定了文件已被自己签署这一事实；二是因为自己的签名不易被别人模仿，从而确定了文件是真的这一事实。

（三）加密技术

1. 对称加密

需要对加密和解密使用相同密钥的加密算法。由于其速度快，对称性加密通常在消息发送方需要加密大量数据时使用。对称性加密也称为密钥加密。

所谓对称，就是采用这种加密方法的双方使用方式用同样的密钥进行加密和解密。密钥是控制加密及解密过程的指令。算法是一组规则，规定如何进行加密和解密。

因此加密的安全性不仅取决于加密算法本身，密钥管理的安全性更是重要。因为加密和解密都使用同一个密钥，如何把密钥安全地传递到解密者手上就成了必须要解决的问题。

2. 非对称加密

非对称加密技术又被称为公用/私有密钥，与单独密钥不同，它使用的是一对相互关联的密钥，一个是公用密钥，任何人都可以知道，另一个私有密钥，只有拥有该对密钥的人知道。如果有人发信给一个人，他会用公用密钥对信件进行加密，把信发出去，只有持有私有密钥的人可以解密。这样的话，密钥只有一个人持有，更容易保密，因为不需要在网络上传送私人密钥，也就不担心密钥会被其他的人给窃取。

（四）数字认证技术

它是以数字证书为核心的加密技术可以对网络上传输的信息进行加密和解密、数字签名和签名验证，

确保网上传递信息的安全性、完整性。使用了数字证书，即使您发送的信息在网上被他人截获，甚至您丢失了个人的账户、密码等信息，仍可以保证您的账户、资金安全。简单来说就是保障在网上交易的安全。