**计算机基础知识整理**

目录

[第一章 5](#_Toc144379004)

[1.1计算机的发展 5](#_Toc144379005)

[1.1.1计算机的诞生 5](#_Toc144379006)

[1.1.2计算机技术的发展 7](#_Toc144379007)

[1.1.3计算机技术知名企业 8](#_Toc144379008)

[1.1.4计算机技术的发展方向 14](#_Toc144379009)

[1.1.5现代计算机的新技术以及计算机专业术语 14](#_Toc144379010)

[1.2计算机的特点、分类及应用领域 16](#_Toc144379011)

[1.2.1计算机的特点 16](#_Toc144379012)

[1.2.2计算机的分类 17](#_Toc144379013)

[1.2.3计算机的应用领域 18](#_Toc144379014)

[第二章 19](#_Toc144379015)

[2.1数据与信息的基本术语 19](#_Toc144379016)

[2.2计算机中的数制 20](#_Toc144379017)

[2.3计算机中不同数制间的转换 22](#_Toc144379018)

[2.4信息的存储单位与换算 23](#_Toc144379019)

[2.5计算机中数据的表示 24](#_Toc144379020)

[第三章 29](#_Toc144379021)

[3.1计算机工作原理 30](#_Toc144379022)

[3.1.1计算机的设计思想及工作原理 30](#_Toc144379023)

[3.1.2计算机系统的组成 32](#_Toc144379024)

[3.2计算机硬件及相关设备 33](#_Toc144379025)

[3.2.1主板 33](#_Toc144379026)

[3.2.2总线 34](#_Toc144379027)

[3.2.3处理器 34](#_Toc144379028)

[3.2.4内存储器 36](#_Toc144379029)

[3.2.5外存储器 37](#_Toc144379030)

[3.2.6输入设备 39](#_Toc144379031)

[3.2.7输出设备 40](#_Toc144379032)

[3.2.8声卡，网卡，显卡 42](#_Toc144379033)

[3.3计算机软件基本知识 43](#_Toc144379034)

[3.3.1软件及分类 43](#_Toc144379035)

[3.3.2程序设计的基础知识 45](#_Toc144379036)

[3.4计算机日常使用中的维护 48](#_Toc144379037)

[3.4.1计算机的工作环境 48](#_Toc144379038)

[3.4.2计算机各部件的日常维护 50](#_Toc144379039)

[第四章 53](#_Toc144379040)

[4.1多媒体技术概述 53](#_Toc144379041)

[4.1.1多媒体技术的概念 53](#_Toc144379042)

[4.1.2多媒体技术的特点 55](#_Toc144379043)

[4.2多媒体计算机系统的组成 56](#_Toc144379044)

[4.2.1多媒体计算机硬件系统 56](#_Toc144379045)

[4.2.2多媒体计算机软件系统 57](#_Toc144379046)

[4.3多媒体处理技术 59](#_Toc144379047)

[4.3.1图像处理 59](#_Toc144379048)

[4.3.2音频处理 60](#_Toc144379049)

[4.3.3视频处理 62](#_Toc144379050)

[4.4平面设计基础知识 64](#_Toc144379051)

[4.4.1平面设计概述 64](#_Toc144379052)

[4.4.2位图处理软件 Adobe Photoshop 64](#_Toc144379053)

[第五章 66](#_Toc144379054)

[5.1操作系统概述 66](#_Toc144379055)

[5.1.1操作系统的功能 66](#_Toc144379056)

[5.1.2操作系统的基本特征 67](#_Toc144379057)

[5.1.3操作系统的分类 68](#_Toc144379058)

[5.1.4常用计算机操作系统 70](#_Toc144379059)

[5.1.5常用手机操作系统 72](#_Toc144379060)

[5.2文件及文件夹 74](#_Toc144379061)

[第六章 76](#_Toc144379062)

[6.1通信的基础概念 78](#_Toc144379063)

[6.1.1数据通信三要素 78](#_Toc144379064)

[6.1.2通信信号 78](#_Toc144379065)

[6.1.3数据传输方式 79](#_Toc144379066)

[6.1.4数据交换方式 82](#_Toc144379067)

[6.1.5差错控制技术 83](#_Toc144379068)

[6.1.6数据通信的主要技术参数 85](#_Toc144379069)

[6.2计算机网络概述 86](#_Toc144379070)

[6.2.1计算机网络的产生与发展 86](#_Toc144379071)

[6.2.2计算机网络的概念与功能 87](#_Toc144379072)

[6.2.3计算机网络的分类 88](#_Toc144379073)

[6.2.4网络通信的三种模式 89](#_Toc144379074)

[6.3计算机网络系统结构 90](#_Toc144379075)

[6.3.1计算机网络系统组成 90](#_Toc144379076)

[6.3.2计算机网络逻辑结构 90](#_Toc144379077)

[6.3.3计算机网络拓扑结构 91](#_Toc144379078)

[6.3.4常用网络命令 93](#_Toc144379079)

[6.3.5网络协议 94](#_Toc144379080)

[6.3.6开放网络互连参考模型（OSI - RM） 95](#_Toc144379081)

[6.4TCP/IP体系结构 97](#_Toc144379082)

[6.4.1TCP/IP参考模型 97](#_Toc144379083)

[6.4.2IP地址 98](#_Toc144379084)

[6.4.3端口 103](#_Toc144379085)

[6.5计算机网络设备 104](#_Toc144379086)

[6.5.1网络互连 104](#_Toc144379087)

[6.5.2网络传输介质 105](#_Toc144379088)

[6.5.3网卡 106](#_Toc144379089)

[6.5.4中继转发设备 107](#_Toc144379090)

[6.5.5网桥 108](#_Toc144379091)

[6.5.6网络交换设备 109](#_Toc144379092)

[6.5.7调制解调器 111](#_Toc144379093)

[6.6局域网与广域网技术 111](#_Toc144379094)

[6.6.1局域网技术 111](#_Toc144379095)

[6.6.2典型局域网类型 114](#_Toc144379096)

[6.6.3广域网技术 114](#_Toc144379097)

[6.7Internet 115](#_Toc144379098)

[6.7.1Internet的起源与发展 115](#_Toc144379099)

[6.7.2域名系统DNS 116](#_Toc144379100)

[6.7.3信息浏览服务（WWW） 116](#_Toc144379101)

[6.7.4FTP服务 117](#_Toc144379102)

[6.7.5电子邮件服务（E-mail） 118](#_Toc144379103)

[6.7.6远程登陆服务与查询服务 119](#_Toc144379104)

[6.7.7即时通信 120](#_Toc144379105)

[6.7.8Internet上的新型服务 121](#_Toc144379106)

[6.7.9物联网 122](#_Toc144379107)

[第七章 123](#_Toc144379108)

[7.1信息安全基础知识 124](#_Toc144379109)

[7.1.1信息安全的概念 124](#_Toc144379110)

[7.1.2信息安全级别 127](#_Toc144379111)

[7.1.3信息安全面临的威胁与破坏信息系统的方式 128](#_Toc144379112)

[7.1.4数据加密技术 129](#_Toc144379113)

[7.1.5身份认证技术 132](#_Toc144379114)

[7.1.6访问控制技术 134](#_Toc144379115)

[7.1.7信息隐藏技术 136](#_Toc144379116)

[7.2 网络安全基础知识 137](#_Toc144379117)

[7.2.1 网络安全目标与特征 137](#_Toc144379118)

[7.2.2 局域网攻击 139](#_Toc144379119)

[7.2.3 广域网攻击 141](#_Toc144379120)

[7.2.4 防火墙技术 142](#_Toc144379121)

[7.2.5虚拟专用网络（VPN） 144](#_Toc144379122)

[7.2.6黑客 145](#_Toc144379123)

[7.2.7预防黑客攻击 146](#_Toc144379124)

[7.2.8木马 147](#_Toc144379125)

[7.3 计算机病毒 151](#_Toc144379126)

[7.3.1 计算机病毒的定义与特点 151](#_Toc144379127)

[7.3.2计算机病毒的分类 153](#_Toc144379128)

[7.3.3计算机病毒的传播途径与预防 155](#_Toc144379129)

[7.3.4常见的计算机病毒 157](#_Toc144379130)

[7.3.5计算机病毒的检测与清除 159](#_Toc144379131)

[7.4网络道德 161](#_Toc144379132)

[7.4.1网络道德的定义和原则 161](#_Toc144379133)

[7.4.2网络犯罪 163](#_Toc144379134)

[7.5知识产权与计算机软件产权 163](#_Toc144379135)

[7.5.1知识产权 163](#_Toc144379136)

[7.5.2计算机软件产权 165](#_Toc144379137)

# 第一章

第一章

1.1计算机的发展

1.1.1计算机的诞生

1.1.2计算机技术的发展

1.1.3计算机技术知名企业

1.1.4计算机技术的发展方向

1.1.5现代计算机的新技术以及计算机专业术语

1.2计算机的特点、分类及应用领域

1.2.1计算机的特点

1.2.2计算机的分类

1.2.3计算机的应用领域

## **1.1计算机的发展**

### 1.1.1计算机的诞生

1. 1642年 - 帕斯卡计算器

- 年份：1642年

- 人物：布莱兹·帕斯卡（Blaise Pascal）

- 发明产物：帕斯卡计算器

- 说明：帕斯卡计算器是一种机械装置，用于进行基本的加法和减法运算。

2. 1671年 - 利布尼茨计算器

- 年份：1671年

- 人物：高特弗里德·威廉·利布尼茨（Gottfried Wilhelm Leibniz）

- 发明产物：利布尼茨计算器

- 说明：利布尼茨计算器是一种机械计算设备，能够进行四则运算。

3. 1801年 - 雅卡尔·拉卢斯打孔卡片制表机

- 年份：1801年

- 人物：雅克·拉卢斯（Jacquard）

- 发明产物：雅卡尔·拉卢斯打孔卡片制表机

- 说明：这是一种使用打孔卡片控制纺织机运行的机械设备，为计算机历史中的自动化设备之一。

4. 1822年 - 巴贝奇分析机

- 年份：1822年

- 人物：查尔斯·巴贝奇（Charles Babbage）

- 发明产物：巴贝奇分析机

- 说明：巴贝奇分析机被认为是世界上第一台可以被称为计算机的真正机器，它使用穿孔卡片作为编程指令。

5. 1833年 - 巴贝奇通用机

- 年份：1833年

- 人物：查尔斯·巴贝奇（Charles Babbage）

- 发明产物：巴贝奇通用机

- 说明：巴贝奇通用机是对巴贝奇分析机的改进版本，具备了数字计算和存储的概念，并且包含了控制流程的能力。

6. 1936年 - 图灵机

- 年份：1936年

- 人物：阿兰·图灵（Alan Turing）

- 发明产物：图灵机

- 说明：图灵机是一种理论模型，通过无限长的纸带和有限状态机来模拟计算过程，被视为计算机科学的基础之一。

7. 1941年 - ENIAC

- 年份：1941年至1946年

- 人物：约翰·W·梅奇（John W. Mauchly）和J·普里斯伯格·埃克特（J. Presper Eckert）

- 发明产物：ENIAC（Electronic Numerical Integrator and Computer）

- 说明：ENIAC是世界上第一台通用电子计算机，利用了大量的真空管进行高速计算，被广泛用于科学和工程计算。

8. 1945年 - EDVAC

- 年份：1945年

- 人物：约翰·W·冯·诺伊曼（John W. von Neumann）和其他合作者

- 发明产物：EDVAC（Electronic Discrete Variable Automatic Computer）

- 说明：EDVAC是一台使用存储程序概念的计算机，将程序和数据存储在同一存储器中，这种结构成为现代计算机的基础。

9. 1949年 - EDSAC

- 年份：1949年

- 人物：毕奇·韦利（Maurice Wilkes）和其他合作者

- 发明产物：EDSAC（Electronic Delay Storage Automatic Calculator）

- 说明：EDSAC是世界上第一个实际运行的存储程序计算机，采用了二进制系统和存储器中的延迟线来存储程序和数据。

10. 1951年 - 第一台商业计算机

- 年份：1951年

- 人物：埃克特-马奇计算机公司（Eckert-Mauchly Computer Corporation）

- 发明产物：UNIVAC I（Universal Automatic Computer I）

- 说明：UNIVAC I是世界上第一台商业化的电子计算机，被应用于美国人口普查和其他数据处理任务。

### 1.1.2计算机技术的发展

1. 第一代计算机（1946至1958）

- 主要元器件：真空管、电子管

- 主要存储器和外部存储器：磁鼓、磁带

- 软件及编程语言：机器语言、汇编语言

- 主要应用领域：科学计算、军事应用

2. 第二代计算机（1958至1964）

- 主要元器件：晶体管

- 主要存储器和外部存储器：磁芯存储器、磁带、磁盘

- 软件及编程语言：汇编语言、FORTRAN、COBOL

- 主要应用领域：商业数据处理、科学计算、军事应用

3. 第三代计算机（1964至1971）

- 主要元器件：集成电路（IC）

- 主要存储器和外部存储器：半导体存储器、磁带、磁盘

- 软件及编程语言：高级语言（如ALGOL、BASIC、C、Pascal）

- 主要应用领域：商业数据处理、科学计算、国防和航空航天应用

4. 第四代计算机（1971至现在）

- 主要元器件：微处理器、超大规模集成电路（VLSI）

- 主要存储器和外部存储器：固态硬盘（SSD）、光盘、闪存

- 软件及编程语言：面向对象的语言（如C++、Java）、数据库系统

- 主要应用领域：个人计算机、互联网、嵌入式系统、人工智能、移动应用等

5. 第五代计算机（现在及未来）

- 主要元器件：量子位、光子芯片

- 主要存储器和外部存储器：量子存储器、DNA存储器

- 软件及编程语言：复杂软件系统、人工智能、机器学习

- 主要应用领域：量子计算、大数据处理、人机交互、生物技术、智能物联网等

### 1.1.3计算机技术知名企业

软件

1. 微软（Microsoft）

- 创立时间：1975年

- 企业创始人：比尔·盖茨和保罗·艾伦

- 企业规模：全球有超过14万名员工

- 企业介绍：微软是世界上最大的软件公司之一，总部位于美国华盛顿州的雷德蒙德。微软提供各种软件产品和服务，包括操作系统（如Windows）、办公软件（如Office套件）和开发工具（如Visual Studio）等。

- 主要产品：Windows操作系统、Microsoft Office套件、Azure云平台、Xbox游戏平台等。

2. 谷歌（Google）

- 创立时间：1998年

- 企业创始人：拉里·佩奇和谢尔盖·布林

- 企业规模：全球有超过13万名员工

- 企业介绍：谷歌是全球最大的互联网搜索引擎公司之一，总部位于美国加利福尼亚州的山景城。谷歌提供了许多互联网相关的产品和服务，如搜索引擎、云计算、在线广告等。

- 主要产品：谷歌搜索引擎、Google Chrome浏览器、Android操作系统、Google Cloud云服务等。

3. 苹果（Apple）

- 创立时间：1976年

- 企业创始人：史蒂夫·乔布斯、史蒂夫·沃兹尼亚克和罗恩·韦恩

- 企业规模：全球有超过13万名员工

- 企业介绍：苹果是一家以设计、开发和销售消费电子产品为主的公司，总部位于美国加利福尼亚州的库比蒂诺。苹果以其创新的产品和优质的用户体验而闻名，如iPhone智能手机、iPad平板电脑、Mac电脑和苹果音乐平台等。

- 主要产品：iPhone、iPad、Mac电脑、Apple Watch、苹果音乐等。

4. 亚马逊（Amazon）

- 创立时间：1994年

- 企业创始人：杰夫·贝索斯

- 企业规模：全球有超过140万名员工

- 企业介绍：亚马逊是全球最大的电子商务和云计算公司之一，总部位于美国华盛顿州的西雅图。亚马逊以其广泛的产品种类、快速的物流服务和领先的云计算平台（亚马逊AWS）而闻名。

- 主要产品：亚马逊电商平台、亚马逊Prime会员服务、Kindle电子阅读器、亚马逊AWS云服务等。

5. 甲骨文（Oracle）

- 创立时间：1977年

- 企业创始人：拉里·埃里森、鲍勃·明托夫、埃德·奥茨和布鲁斯·斯科特

- 企业规模：全球有超过13万名员工

- 企业介绍：甲骨文是一家专注于开发和提供企业级软件和云服务的公司，总部位于美国加利福尼亚州的奥克兰。甲骨文以其数据库管理系统（Oracle Database）和企业级应用软件（如Oracle ERP和Oracle SCM）而闻名。

- 主要产品：Oracle Database、Oracle ERP、Oracle SCM等。

6. IBM（International Business Machines）

- 创立时间：1911年

- 企业创始人：查尔斯·费奥尔德、托马斯·沃森

- 企业规模：全球有超过30万名员工

- 企业介绍：IBM是世界上最大的科技和咨询服务公司之一，总部位于美国纽约州的阿蒙克。IBM致力于提供各种技术解决方案和服务，包括硬件设备、软件产品、云计算和人工智能等领域。

- 主要产品：IBM计算机硬件、IBM Watson人工智能平台、IBM云服务、IBM Watson Health医疗解决方案等。

7. 百度（Baidu）

- 创立时间：2000年

- 企业创始人：李彦宏、徐勇、王海峰

- 企业规模：全球有超过5万名员工

- 企业介绍：百度是中国最大的互联网搜索引擎公司，总部位于中国北京。百度提供各种互联网相关的产品和服务，包括搜索引擎、在线广告、人工智能和自动驾驶技术等。

- 主要产品：百度搜索引擎、百度地图、百度文库、百度AI开放平台等。

8. 腾讯（Tencent）

- 创立时间：1998年

- 企业创始人：马化腾、张志东、许晨晔、陈一丹、刘炽平

- 企业规模：全球有超过7万名员工

- 企业介绍：腾讯是中国最大的互联网科技公司之一，总部位于中国广东省深圳市。腾讯提供各种在线服务和产品，包括社交媒体、在线游戏、支付服务和云计算等。

- 主要产品：微信、QQ、腾讯游戏、腾讯云、腾讯支付等。

9. 网易（NetEase）

- 创立时间：1997年

- 企业创始人：丁磊

- 企业规模：全球有超过4万名员工

- 企业介绍：网易是中国领先的互联网公司之一，总部位于中国福建省厦门市。网易提供多种互联网服务，包括在线游戏、电子邮件、娱乐内容和电子商务等。

- 主要产品：《魔兽世界》、《梦幻西游》、《倩女幽魂》、网易邮箱、网易云音乐等。

10. 金山（Kingsoft）

- 创立时间：1988年

- 企业创始人：周鸿祎

- 企业规模：全球有超过3万名员工

- 企业介绍：金山是中国领先的软件开发和互联网服务公司之一，总部位于中国北京。金山提供各种办公软件、安全软件和互联网服务，涵盖了多个领域。

- 主要产品：WPS办公套件、金山毒霸安全软件、金山浏览器、金山云存储等。

11. 阿里巴巴（Alibaba）

- 创立时间：1999年

- 企业创始人：马云

- 企业规模：全球有超过13万名员工

- 企业介绍：阿里巴巴是中国最大的电子商务和互联网科技企业，总部位于中国浙江省杭州市。阿里巴巴提供各种在线市场、支付服务、云计算和物流等解决方案。

- 主要产品：淘宝网、天猫、支付宝、阿里云、菜鸟网络等。

12. 华为（Huawei）

- 创立时间：1987年

- 企业创始人：任正非

- 企业规模：全球有超过19万名员工

- 企业介绍：华为是全球领先的信息和通信技术解决方案供应商，总部位于中国广东省深圳市。华为提供各种通信设备、消费者电子产品和企业解决方案，包括手机、网络设备、云服务等。

- 主要产品：华为手机（Mate系列、P系列）、华为网络设备、华为云、华为企业解决方案等。

13. 米哈游（miHoYo）

- 创立时间：2012年

- 企业创始人：董明晓

- 企业规模：全球有约6,000名员工

- 企业介绍：米哈游是一家以开发和发行游戏为主的公司，总部位于中国上海市。米哈游的游戏作品以动作冒险和角色扮演为主，其作品《原神》在全球范围内拥有广泛的玩家基础。

- 主要产品：《原神》、《崩坏》系列、《崩坏学园》、《崩坏3》等。

14. 360

- 创立时间：2005年

- 企业创始人：周鸿祎

- 企业规模：全球有超过1万名员工

- 企业介绍：360是中国知名的互联网安全公司，致力于为用户提供网络安全解决方案和产品。360以其杀毒软件、网页安全、移动安全等产品而著名，公司还涉及搜索引擎、浏览器和移动应用等领域的开发。

- 主要产品：360安全卫士、360杀毒软件、360免费WiFi、360浏览器等。

硬件

1. 三星（Samsung）

- 创立时间：1938年

- 企业创始人：李秉喆

- 企业规模：全球有超过30万名员工

- 企业介绍：三星是韩国最大的综合性企业集团之一，业务涵盖电子、金融、化学和重工业等领域。在电子领域，三星是全球领先的芯片制造商和消费电子产品供应商。

- 主要产品：智能手机（Galaxy系列）、电视、显示器、芯片等。

2. 英特尔（Intel）

- 创立时间：1968年

- 企业创始人：罗伯特·诺伊斯、戈登·摩尔

- 企业规模：全球有超过11万名员工

- 企业介绍：英特尔是全球最大的半导体芯片制造商之一，总部位于美国加利福尼亚州圣克拉拉。英特尔开发和制造各种处理器和芯片组，广泛应用于计算机、服务器和物联网设备。

- 主要产品：酷睿处理器、至强处理器、芯片组等。

3. 惠普（HP）

- 创立时间：1939年

- 企业创始人：比尔·休利特、戴夫·帕卡德

- 企业规模：全球有超过5万名员工

- 企业介绍：惠普是全球最大的IT技术公司之一，总部位于美国加利福尼亚州帕洛阿尔托。惠普提供各种硬件设备、软件解决方案和服务，包括个人电脑、打印机、企业服务器和存储设备等。

- 主要产品：惠普笔记本电脑、惠普台式电脑、打印机、服务器等。

4. 英伟达（NVIDIA）

- 创立时间：1993年

- 企业创始人：杰克·杜兰特、克里斯·马克罗斯、柯达利·珀森

- 企业规模：全球有超过2.5万名员工

- 企业介绍：英伟达是全球领先的图形处理器（GPU）制造商，总部位于美国加利福尼亚州圣克拉拉。英伟达的GPU广泛应用于游戏、人工智能、数据中心和自动驾驶等领域。

- 主要产品：GeForce系列显卡、数据中心加速器（Tesla系列）、人工智能平台（NVIDIA AI）等。

5. AMD（Advanced Micro Devices）

- 创立时间：1969年

- 企业创始人：杰里·桑德斯、埃德·斯皮基

- 企业规模：全球有超过1.1万名员工

- 企业介绍：AMD是全球知名的半导体公司，总部位于美国加利福尼亚州圣塔克拉拉。AMD设计和制造处理器、图形处理器和嵌入式解决方案，广泛应用于个人电脑、游戏主机和数据中心等领域。

- 主要产品：AMD Ryzen处理器、AMD Radeon显卡、EPYC服务器处理器等。

6. 联想（Lenovo）

- 创立时间：1984年

- 企业创始人：刘军

- 企业规模：全球有超过7万名员工

- 企业介绍：联想集团是全球领先的科技企业，总部位于中国北京。联想设计、制造和销售各类计算机硬件设备，包括个人电脑、服务器、工作站、笔记本电脑、平板电脑和智能手机等。

- 主要产品：ThinkPad系列笔记本电脑、ThinkCentre系列台式电脑、ThinkStation系列工作站等。

7. 华硕（ASUS）

- 创立时间：1989年

- 企业创始人：施崇棠、陈启宏、施崇信、唐骏元

- 企业规模：全球有超过2万名员工

- 企业介绍：华硕是一家台湾知名的电脑硬件和电子产品制造商，总部位于台湾台北。华硕提供各类电脑硬件设备，包括主板、显卡、笔记本电脑、手机、服务器和网络设备等。

- 主要产品：ROG游戏系列产品、ASUS商务笔记本电脑、主板、显卡、无线网络设备等。

8. 技嘉（GIGABYTE）

- 创立时间：1986年

- 企业创始人：彭博硕

- 企业规模：全球有超过4千名员工

- 企业介绍：技嘉是一家台湾硬件制造商，专注于主板和显卡等电脑硬件产品的设计与制造。技嘉的产品以高性能、可靠性和创新性而闻名。

- 主要产品：主板、显卡、笔记本电脑、服务器、工作站等。

9. 微星（MSI）

- 创立时间：1986年

- 企业创始人：姜哲明

- 企业规模：全球有超过6千名员工

- 企业介绍：微星是一家台湾电脑硬件制造商，专注于主板、显卡、笔记本电脑和游戏设备的研发和制造。微星以其高品质的产品和创新的设计而著名。

- 主要产品：主板、显卡、游戏笔记本电脑、工作站等。

10. 七彩虹（Colorful）

- 创立时间：1995年

- 企业创始人：何新

- 企业规模：全球有超过1千名员工

- 企业介绍：七彩虹是中国知名的硬件制造商，专注于图形卡、主板、存储设备和电源等计算机硬件产品的研发和生产。七彩虹以其多样化的产品线和卓越的性能而著名。

- 主要产品：显卡（Colorful iGame系列）、主板（Battle Axe系列）、存储设备（SSD和内存条）等。

11. 小米（Xiaomi）

- 创立时间：2010年

- 企业创始人：雷军、林斌、周兴祖、李德伟、黎万强、黄江吉

- 企业规模：全球有超过2万名员工

- 企业介绍：小米是中国的科技公司，旨在为消费者提供智能硬件、移动应用和互联网服务。小米以其高性价比的智能手机和物联网产品而闻名，是全球最大的智能手机制造商之一。

- 主要产品：智能手机（Mi系列、Redmi系列）、智能家居设备（米家）、笔记本电脑、电视等。

12. oppo（OPPO）

- 创立时间：2004年

- 企业创始人：陈明永

- 企业规模：全球有超过4万名员工

- 企业介绍：OPPO是一家中国电子科技公司，专注于智能手机、耳机、智能穿戴设备和移动通信相关产品的设计、制造和销售。OPPO致力于为用户带来前沿科技和优质的摄影体验。

- 主要产品：智能手机（Find系列、Reno系列、A系列）、耳机（Enco系列）等。

13. vivo（VIVO）

- 创立时间：2009年

- 企业创始人：沈义人

- 企业规模：全球有超过2万名员工

- 企业介绍：VIVO是中国的一家智能手机制造商，专注于提供优质的手机摄影体验和先进的移动通信技术。VIVO注重技术创新和用户体验，不断推出具有创新功能和设计的智能手机产品。

- 主要产品：智能手机（X系列、Y系列、S系列）、耳机（TWS Earphone系列）等。

### 1.1.4计算机技术的发展方向

1. 发展趋势

a) 巨型化：计算机系统的规模不断扩大，从巨型主机到大规模计算机集群，提供更高的处理能力和存储能力。巨型化计算机在科学计算、大数据分析等领域具有重要作用。

b) 微型化：计算机系统的体积不断减小，从传统的台式机和笔记本电脑到智能手机和可穿戴设备。微型化计算机的发展使得计算能力可以随时随地得到满足，并推动了移动计算和便携性的发展。

c) 网络化：计算机系统之间的连接和通信越来越重要，形成了广泛的计算机网络。互联网的兴起和发展使得全球范围内的信息共享和协作成为可能，推动了云计算、大数据和物联网的发展。

d) 智能化：人工智能（AI）和机器学习（ML）的发展推动计算机系统的智能化。计算机不仅能够处理和分析数据，还能模仿人类的认知和决策过程，应用于图像识别、语音识别、自动驾驶等领域。

2. 新型计算机发展趋势

a) 量子计算机：量子计算机利用量子力学的特性进行计算，具有在某些特定问题上比传统计算机快速算法的潜力。量子计算机的研发目标是解决复杂问题，如优化、模拟和密码破解。

b) 生物计算机：生物计算机利用生物分子进行信息存储和计算。通过利用DNA、蛋白质和细胞等生物分子的特性，生物计算机在生物医学、生物信息学和生物工程领域具有潜在的应用前景。

c) 光计算机：光计算机利用光子来进行信息处理和传输，具有高速、低能耗和抗干扰等优势。光计算机的研究致力于开发基于光子的芯片、通信和存储技术，以提高计算机系统的速度和效率。

### 1.1.5现代计算机的新技术以及计算机专业术语

1. 新技术

a) 大数据（Big Data）：指处理规模庞大、复杂多样、快速增长的数据集的技术。大数据技术包括数据收集、存储、处理、分析和可视化等方面，广泛应用于商业智能、市场趋势分析、医疗健康等领域。

b) 脑机接口（Brain-Computer Interface，BCI）：是一种将人脑信号与计算机交互的技术。通过先进的传感器技术和信号处理算法，脑机接口使得人们可以通过思维控制计算机和外部设备，为特殊需求群体提供更多的交互方式。

c) 物联网（Internet of Things，IoT）：是指将各种传感器、设备和物体连接到互联网上，形成智能化网络的技术。物联网技术使得各种设备和物体能够相互交流和共享数据，应用于智能家居、智慧城市、工业自动化等领域。

d) IPv6（Internet Protocol version 6）：是一种网络协议，用于为互联网上的设备分配和识别唯一的IP地址。IPv6取代了传统的IPv4协议，提供了更多的地址空间、更好的安全性和更高的性能。

e) 电子商务（E-commerce）：指通过互联网进行商业活动的模式和方法。电子商务涵盖了网上购物、在线支付、电子供应链管理等各种商务活动，极大地改变了传统商业模式。

f) 云计算（Cloud Computing）：是一种通过网络提供计算、存储和应用服务的技术。云计算允许用户根据需要访问共享的计算资源，提供灵活、可扩展和经济高效的解决方案。

g) 互联网+（Internet Plus）：是中国提出的概念，意味着将互联网与传统产业深度融合。互联网+将互联网技术应用于各个领域，推动传统行业的转型升级，促进经济发展和创新。

h) 人工智能（Artificial Intelligence，AI）：指通过模拟和延伸人类智能的理论、方法、技术，使机器能够模拟、延伸和扩展人类的某些智能行为和认知能力的技术。人工智能包括机器学习、深度学习、自然语言处理等领域。

i) VR（Virtual Reality）：虚拟现实技术是一种利用计算机生成的图像和声音，创造出一种与真实世界类似但实际上是虚构的环境的技术。用户可以通过佩戴VR设备来进行沉浸式的交互体验。

j) AR（Augmented Reality）：增强现实技术是一种通过计算机生成的图像和声音来增强现实世界的技。AR技术可以将虚拟对象叠加在真实世界中，用户可以通过AR设备进行实时的信息交互。

k) MR（Mixed Reality）：混合现实技术是一种将虚拟世界和真实世界相互融合的技术。MR技术将虚拟对象与真实环境进行交互，使用户能够在现实世界和虚拟世界之间自由切换。

l) 5G（Fifth Generation）：第五代移动通信技术，是当前移动通信领域的新一代技术标准。5G技术具有更高的速度、更低的延迟和更大的连接密度，将推动物联网、智能城市等领域的发展。

2. 计算机专业术语

a) CAD（Computer-Aided Design）：计算机辅助设计技术，通过计算机和相关软件来辅助进行产品和工程的设计过程。

b) CAM（Computer-Aided Manufacturing）：计算机辅助制造技术，通过计算机和相关软件来辅助制造过程的控制和管理，提高生产效率和质量。

c) CAI（Computer-Assisted Instruction）：计算机辅助教学技术，利用计算机和相关软件来辅助教学活动，提供个性化和互动式的教学体验。

d)CAE（Computer-Aided Engineering）是一种利用计算机软件和硬件工具辅助进行工程分析和设计的技术。CAE在工程领域中起到关键的作用，用于模拟和优化产品的性能、工艺和制造过程。

e) CIMS（Computer-Integrated Manufacturing System）：计算机集成制造系统，将计算机技术应用于整个制造过程的集成管理系统，实现生产过程的高效自动化和优化管理。

f) 3C技术（Communication, Computer, Control）：3C技术指通信技术、计算机技术和控制技术的结合与发展。它们相互依存、相互促进，共同推动了信息技术的发展和应用。

g)AIGC（AI Generated Content）是指通过人工智能技术生成的内容。这种技术利用深度学习和自然语言处理等算法，从大量的数据中学习并生成新的内容，如文章、音乐、图像等。

## 1.2计算机的特点、分类及应用领域

### 1.2.1计算机的特点

计算机是一种现代化的工具，具有以下特点：

1. 速度：计算机能够在极短的时间内进行大量的数据处理和运算。其内部的芯片和电路设计以及高速传输的总线和存储器使得计算机能够以毫秒级或更快的速度进行操作。

2. 精确性：计算机是以数字的形式进行操作的，它能够提供高度精确的计算结果。在正确的输入和程序操作下，计算机能够以毫无误差的方式执行各种计算和操作。

3. 存储能力：计算机具有大容量的数据存储能力，可以存储和检索大量的信息。硬盘、固态硬盘、内存和其他存储介质提供了不同规模和速度的存储选项，以适应各种应用需求。

4. 可编程性：计算机可以根据用户的需求和程序设计进行自动化操作。用户可以使用编程语言和软件开发工具将任务转化为可执行的程序，从而实现自动化和批量处理。

5. 可靠性：计算机的硬件和软件经过精心设计和测试，以确保其可靠性和稳定性。此外，备份系统和故障恢复机制可用于保护数据和处理中断。

6. 通用性：计算机具有广泛的适用性和灵活性，在各个领域都有应用。它可以处理不同类型的数据和任务，包括文字处理、图形处理、数据分析、娱乐等。

7. 自动化：计算机能够执行不同的任务，并通过预设的算法和规则来自动执行各种操作。它可以自动完成重复性任务和复杂的计算，提高工作效率。

8. 可联网性：现代计算机能够通过网络连接到其他计算机和设备，实现数据交流和资源共享。这种连接性使得计算机能够在全球范围内进行信息交流和协同工作。

### 1.2.2计算机的分类

1. 按规模分类：

a) 超级计算机（Supercomputers）：超级计算机是最强大和最高性能的计算机系统。它们用于处理大规模、复杂的科学计算、天气预报、核能模拟等需要极高处理能力的任务。

b) 微型计算机（Microcomputers）：微型计算机通常是个人计算机的别称，是指基于微处理器的小型计算机系统，如台式机、笔记本电脑、平板电脑等。

c) 工作站（Workstations）：工作站是一种高性能的个人计算机，通常用于科学计算、CAD/CAM设计、媒体制作等需要高性能的专业应用。

d) 服务器（Servers）：服务器是为客户端提供服务并共享资源的计算机系统。它们用于存储和处理大量的数据，提供服务和支持网络应用。

e) 嵌入式计算机（Embedded Computers）：嵌入式计算机是嵌入到其他设备或系统中的特定用途的计算机系统，如无人机、智能家居、汽车控制系统等。

f) 大型计算机（Mainframe Computers）：大型计算机是高性能、高可用性的计算机系统，用于大规模的数据处理和信息管理。

g) 小型计算机（Mini Computers）：小型计算机通常是多用户系统，能够支持多个用户同时进行任务。

h) 无服务器计算（Serverless Computing）：无服务器计算是一种云计算模型，用户无需管理服务器和计算资源，而是依靠云供应商提供的无服务器平台进行计算。

2. 按用途分类：

a) 通用计算机（General-purpose Computers）：通用计算机是可以执行各种任务的计算机系统，包括个人计算机、工作站等。

b) 专用计算机（Special-purpose Computers）：专用计算机是为特定的任务或应用领域而设计的计算机系统，如超级计算机、嵌入式计算机等。

3. 按数据处理形式分类：

a) 数字计算机（Digital Computers）：数字计算机是基于二进制数字的计算机系统，能够处理数字数据和进行数值计算。

b) 模拟计算机（Analog Computers）：模拟计算机是基于连续信号的计算机系统，能够模拟和处理连续变化的物理量。

c) 混合计算机（Hybrid Computers）：混合计算机结合了数字计算机和模拟计算机的特点，既可以处理数字数据又可以进行模拟计算。

这些是常见的计算机分类方式，按规模、用途和数据处理形式进行了分类。

### 1.2.3计算机的应用领域

计算机在各个领域都有广泛的应用，以下是一些常见的计算机应用领域：

1. 科学计算（Scientific Computing）：计算机用于模拟和解析复杂的科学问题，例如天气预测、气候模拟、宇宙演化等。它们可以处理大量数据，进行数值计算和建模。

2. 数据处理（Data Processing）：计算机在数据处理领域起到关键作用，用于存储、管理和分析大规模数据集，支持数据挖掘、统计分析、机器学习等任务。

3. 过程控制（Process Control）：计算机在工业和制造业中用于监测和控制生产过程。它们可以实时采集数据、分析反馈信息，并控制设备的运行。

4. 计算机辅助技术（Computer-aided Technology）：计算机辅助技术包括计算机辅助设计（CAD）、计算机辅助制造（CAM）和计算机辅助工程（CAE），用于支持产品设计、制造和工程分析。

5. 人工智能（Artificial Intelligence）：计算机在人工智能领域应用广泛，包括机器学习、自然语言处理、计算机视觉、专家系统等，以实现自主决策、智能推理和模式识别。

6. 多媒体应用（Multimedia Applications）：计算机用于多媒体应用，例如图像处理、音频处理、视频编辑和虚拟现实等，提供丰富的媒体体验和交互性。

7. 网络与通信（Networking and Communication）：计算机网络和通信技术使得信息传输更加快速和便捷。它们支持互联网、电子邮件、即时通讯、远程访问和云计算等。

这些是计算机的一些常见应用领域，每个领域都有自己独特的需求和挑战。

# **第二章**

第二章

2.1数据与信息的基本术语

2.2计算机中的数制

2.3计算机中不同数制间的转换

2.4信息的存储单位与换算

2.5计算机中数据的表示

## 2.1数据与信息的基本术语

1. 数据（Data）：数据是未经加工和解释的原始事实和观测结果，通常以数字、文字、图像等形式表示存在。

2. 信息（Information）：信息是经过处理和组织的数据，赋予了特定的意义和价值，能够为人们提供有用的知识和理解。

区别与联系：

- 数据是未经加工的原始事实，而信息是经过处理和解释的数据。

- 数据本身可能没有明确的含义，而信息对于特定的目标和应用具有明确的含义和价值。

- 数据是信息的基础，信息是从数据中提取和推导出来的有意义的内容。

信息的特点：

- 客观性（Objectivity）：信息应基于客观事实和准确数据，不带有主观偏见和个人观点。

- 时效性（Timeliness）：信息应及时提供，以满足用户的需求和决策的时效性要求。

- 普遍性（Universality）：信息应具有适用性和普遍性，能够被广泛理解和应用。

- 可传递性（Transmissibility）：信息应能够以合适的形式和方式传递给他人或系统。

- 可处理性（Processability）：信息应具备可处理、分析和应用的特性，可转化为决策和行动。

- 真伪性（Authenticity）：信息应真实、可靠，并且能够被验证和核实。

- 共享性（Sharability）：信息应能够被多个用户共享和访问，支持协作和知识共享。

- 依附性（Dependency）：信息与特定的上下文和用户需求相关联，对特定目标和决策起作用。

信息技术的发展历程：

- 第一次信息革命：语言的使用和传播。

- 第二次信息革命：文字的出现和使用。

- 第三次信息革命：印刷术的发明与使用。

- 第四次信息革命：电话、电报、广播、电视等的使用。

- 第五次信息革命：计算机与互联网的使用。

信息技术（Information Technology，简称IT）：信息技术是指用于处理、存储、传输和应用信息的硬件、软件及相关设备和系统。它涉及计算机科学、通信技术和软件工程等领域。

信息社会（Information Society）：信息社会是在信息技术高度发达的基础上，信息资源成为经济和社会发展的重要生产要素，对社会各个方面产生显著影响的社会现象。在信息社会中，信息的获取、传播和应用起到关键的作用。

信息产业（Information Industry）：信息产业是依托于信息技术进行信息的生产、加工、传输和应用的经济部门和产业。它包括计算机硬件和软件产业、通信和网络产业、媒体和出版产业等相关行业。

## 2.2计算机中的数制

1. 数制（Numeral System）：数制是一种表示和计数数字的方法，它定义了数字字符的基数和位权的规则。

2. 进位计数制（Positional Notation）：进位计数制是一种表示数字的方法，其中每个数字的值取决于其位置（位权）和基数。

- 基数（Radix/Base）：进位计数制的基数是指表示数字的字符集的大小。常见的基数有2（二进制）、8（八进制）、10（十进制）和16（十六进制）。

例子：二进制（基数为2）使用的数位有0和1，八进制（基数为8）使用的数位有0-7。

- 位权（Place Value）：进位计数制中，每个数字的位置决定了其对应的位权值。位权是基数的幂，从右到左依次递增。

例子：对于二进制数1101，从右到左位权分别是2^0、2^1、2^2和2^3。

- 数位（Digit）：数位是表示数字的每个字符。

例子：八进制数47中的4和7就是数位。

3. 二进制（Binary）：二进制是一种基数为2的进位计数制，使用0和1来表示每个数位的值。在计算机中，所有数据都以二进制形式存储和处理。

例子：二进制数1011表示了十进制的数11。

4. 二进制运算：二进制运算是对二进制数进行的各种数学运算，包括加法、减法、乘法、除法、非、与、或、异或和同或。

- 加法（Binary Addition）：将两个二进制数位相加，可能产生进位。

例子：1011 + 0101 = 10000

- 减法（Binary Subtraction）：将两个二进制数位相减，可能需要借位。

例子：1011 - 0101 = 0100

- 乘法（Binary Multiplication）：将两个二进制数相乘，得到一个二进制结果。

例子：1011 \* 0101 = 1101

- 除法（Binary Division）：将一个二进制数除以另一个二进制数，得到商和余数。

例子：1011 / 0101 = 10（商）...01（余数）

- 非（Bitwise NOT）：对二进制数的每个位取反，0变为1，1变为0。

例子：NOT 1011 = 0100

- 与（Bitwise AND）：对两个二进制数的相同位置进行与运算，只有当两个位都为1时，结果位才为1。

例子：1011 AND 0101 = 0001

- 或（Bitwise OR）：对两个二进制数的相同位置进行或运算，只要有一个位为1，结果位就为1。

例子：1011 OR 0101 = 1111

- 异或（Bitwise XOR）：对两个二进制数的相同位置进行异或运算，只有一个位为1时，结果位才为1。

例子：1011 XOR 0101 = 1110

- 同或（Bitwise XNOR，也称为同或运算）：对两个二进制数的相同位置进行同或运算，结果与异或运算的结果相反。

例子：1011 XNOR 0101 = 0001

5. 八进制（Octal）：八进制是一种基数为8的进位计数制，使用0-7的数字来表示每个数位的值。

例子：八进制数47表示十进制的数39。

6. 十进制（Decimal）：十进制是一种基数为10的进位计数制，使用0-9的数字来表示每个数位的值。

例子：十进制数158表示了其本身的值。

7. 十六进制（Hexadecimal）：十六进制是一种基数为16的进位计数制，使用0-9和A-F的数字/字母来表示每个数位的值，其中A-F分别表示十进制的10-15。

例子：十六进制数2F表示十进制的数47。

8. 十进制与不同进制的对照表：

|  |  |  |  |
| --- | --- | --- | --- |
| 十进制 | 二进制 | 八进制 | 十六进制 |
| 0 | 0000 | 0 | 0 |
| 1 | 0001 | 1 | 1 |
| 2 | 0010 | 2 | 2 |
| 3 | 0011 | 3 | 3 |
| 4 | 0100 | 4 | 4 |
| 5 | 0101 | 5 | 5 |
| 6 | 0110 | 6 | 6 |
| 7 | 0111 | 7 | 7 |
| 8 | 1000 | 10 | 8 |
| 9 | 1001 | 11 | 9 |
| 10 | 1010 | 12 | A |
| 11 | 1011 | 13 | B |
| 12 | 1100 | 14 | C |
| 13 | 1101 | 15 | D |
| 14 | 1110 | 16 | E |
| 15 | 1111 | 17 | F |

## 2.3计算机中不同数制间的转换

1. 十进制转换成非十进制数：

- 转换方法：将十进制数逐位除以目标进制的基数，并记录下余数，最后将余数按倒序排列即得到结果。

例子：将十进制数125转换成二进制：

125 ÷ 2 = 62...余数1

62 ÷ 2 = 31...余数0

31 ÷ 2 = 15...余数1

15 ÷ 2 = 7...余数1

7 ÷ 2 = 3...余数1

3 ÷ 2 = 1...余数1

1 ÷ 2 = 0...余数1

结果：二进制数为1111101

2. 非十进制转换成十进制数：

- 转换方法：将非十进制数的每一位与对应进制的幂相乘，再将结果相加即可得到十进制数。

例子：将二进制数1101转换成十进制：

1 \* 2^3 + 1 \* 2^2 + 0 \* 2^1 + 1 \* 2^0 = 13

结果：十进制数为13

3. 二进制转换成八进制：

- 转换方法：将二进制数的每三位分组，然后将每个三位二进制数转换成对应的八进制数。

例子：将二进制数110110转换成八进制：

11 011 0

结果：八进制数为 32

4. 二进制转换成十六进制：

- 转换方法：将二进制数的每四位分组，然后将每个四位二进制数转换成对应的十六进制数。

例子：将二进制数110110转换成十六进制：

1101 10

结果：十六进制数为 DA

## 2.4信息的存储单位与换算

在计算机中，信息的存储容量通常使用以下单位表示：

1. 字节（Byte，简写为B）：字节是计算机中最基本的存储单位，它代表着8个比特（bit）的信息。

2. 千字节（Kilobyte，简写为KB）：1KB等于1024字节。

3. 兆字节（Megabyte，简写为MB）：1MB等于1024KB。

4. 吉字节（Gigabyte，简写为GB）：1GB等于1024MB。

5. 太字节（Terabyte，简写为TB）：1TB等于1024GB。

6. 拍字节（Petabyte，简写为PB）：1PB等于1024TB。

7. 艾字节（Exabyte，简写为EB）：1EB等于1024PB。

8. 泽字节（Zettabyte，简写为ZB）：1ZB等于1024EB。

9. 尧字节（Yottabyte，简写为YB）：1YB等于1024ZB。

10. 结善字节（Brontobyte，简写为BB）：1BB等于1024YB。

结善字节是一个非常庞大的存储单位，目前还没有达到这样的存储规模。但随着科技的发展，未来可能会有需要达到结善字节级别的存储容量。

换算关系如下：

1 字节 = 8 位

1 KB = 1024 字节

1 MB = 1024 KB

1 GB = 1024 MB

1 TB = 1024 GB

1 PB = 1024 TB

1 EB = 1024 PB

1 ZB = 1024 EB

1 YB = 1024 ZB

1 BB = 1024 YB

例如：

1. 如果一个文件的大小为4 MB，我们可以进行如下换算：

4 MB = 4 \* 1024 KB = 4 \* 1024 \* 1024 字节 = 4 \* 1024 \* 1024 \* 8 位

2. 如果一台计算机的硬盘容量为2 PB，我们可以进行如下换算：

2 PB = 2 \* 1024 TB = 2 \* 1024 \* 1024 GB = 2 \* 1024 \* 1024 \* 1024 MB = 2 \* 1024 \* 1024 \* 1024 \* 1024 KB = 2 \* 1024 \* 1024 \* 1024 \* 1024 \* 8 字节

3. 在网络传输中，通常会使用传输速率来衡量数据传输速度。常见的单位有Mbps（兆比特每秒），意味着每秒传输兆比特的数据量。注意这里是比特，而不是字节。如果要换算成字节，需要除以8。例如，如果一个网络连接的速度为100 Mbps，实际的传输速率为100 / 8 = 12.5 MB/s。

## 2.5计算机中数据的表示

1. 机器数与真值：

- 机器数是计算机中表示数字的方法，通常使用二进制形式。真值是机器数所代表的实际数值。

例子：

- 8位无符号整数：00101011表示的机器数为43，真值也为43。

- 8位有符号整数：11001111表示的机器数为-49，真值为-49。

- 16位无符号整数：0000111101010101表示的机器数为40421，真值也为40421。

2. 机器数的表示方法：

- 原码：用第1位表示符号位（0表示正数，1表示负数），其余位表示数值的大小。

例子：

- +5的原码是00000101。

- -5的原码是10000101。

- 反码：正数的反码与原码相同，负数的反码是符号位不变，其他位取反。

例子：

- +5的反码是00000101。

- -5的反码是11111010。

- 补码：正数的补码与原码相同，负数的补码是其反码加1。

例子：

- +5的补码是00000101。

- -5的补码是11111011。

- 移码：在原码基础上，将符号位取反。

例子：

- +5的移码是00000101。

- -5的移码是11111010。

3. 浮点数：

- 阶码：用于表示浮点数的指数部分。通常使用偏移值表示实际的指数。

例子：

- 单精度浮点数32位中的阶码范围通常是-126到127。

- 5.25的阶码为2。

- 尾数：用于表示浮点数的小数部分和部分整数部分。

例子：

- 单精度浮点数32位中的尾数通常由23位组成。

- 5.25的尾数为0.3125。

4. BDC编码

BCD（Binary Coded Decimal）编码是一种数字编码方式，它将十进制数字的每一位分别用4位二进制数表示。BCD编码主要用于将十进制数字转换为二进制表示，以便在数字系统（如计算机）中进行处理。

例子：

假设我们有一个十进制数字：256。下面是它的BCD编码示例：

- 数字2的BCD编码：0010

- 数字5的BCD编码：0101

- 数字6的BCD编码：0110

因此，BCD编码中的十进制数字256可以表示为：0010 0101 0110。

5. 英文字符编码（ASCII码）：

1. ASCII编码（American Standard Code for Information Interchange）：

- ASCII编码是一种最常用的字符编码标准，用于将字符转换为计算机可识别的数字形式。

- ASCII编码最初是为英语和西欧语言设计的，使用7位二进制数字来表示128个不同的字符。

2. ASCII码表格：

- ASCII码表列出了128个字符以及对应的ASCII码值。

- ASCII码表包括控制字符（如回车、换行等）和可打印字符（包括英文字母、数字、标点符号等）。

- ASCII码采用7位表示，将字符映射到十进制数值。

以下是完整的ASCII码表格：

| ASCII码值 | 字符 | ASCII码值 | 字符 | ASCII码值 | 字符 | ASCII码值 | 字符 |
| --- | --- | --- | --- | --- | --- | --- | --- |
| 0 | NUL | 32 | SP | 64 | @ | 96 | ` |
| 1 | SOH | 33 | ! | 65 | A | 97 | a |
| 2 | STX | 34 | " | 66 | B | 98 | b |
| 3 | ETX | 35 | # | 67 | C | 99 | c |
| 4 | EOT | 36 | $ | 68 | D | 100 | d |
| 5 | ENQ | 37 | % | 69 | E | 101 | e |
| 6 | ACK | 38 | & | 70 | F | 102 | f |
| 7 | BEL | 39 | ' | 71 | G | 103 | g |
| 8 | BS | 40 | ( | 72 | H | 104 | h |
| 9 | HT | 41 | ) | 73 | I | 105 | i |
| 10 | LF | 42 | \* | 74 | J | 106 | j |
| 11 | VT | 43 | + | 75 | K | 107 | k |
| 12 | FF | 44 | , | 76 | L | 108 | l |
| 13 | CR | 45 | - | 77 | M | 109 | m |
| 14 | SO | 46 | . | 78 | N | 110 | n |
| 15 | SI | 47 | / | 79 | O | 111 | o |
| 16 | DLE | 48 | 0 | 80 | P | 112 | p |
| 17 | DC1 | 49 | 1 | 81 | Q | 113 | q |
| 18 | DC2 | 50 | 2 | 82 | R | 114 | r |
| 19 | DC3 | 51 | 3 | 83 | S | 115 | s |
| 20 | DC4 | 52 | 4 | 84 | T | 116 | t |
| 21 | NAK | 53 | 5 | 85 | U | 117 | u |
| 22 | SYN | 54 | 6 | 86 | V | 118 | v |
| 23 | ETB | 55 | 7 | 87 | W | 119 | w |
| 24 | CAN | 56 | 8 | 88 | X | 120 | x |
| 25 | EM | 57 | 9 | 89 | Y | 121 | y |
| 26 | SUB | 58 | : | 90 | Z | 122 | z |
| 27 | ESC | 59 | ; | 91 | [ | 123 | { |
| 28 | FS | 60 | < | 92 | \ | 124 | | |
| 29 | GS | 61 | = | 93 | ] | 125 | } |
| 30 | RS | 62 | > | 94 | ^ | 126 | ~ |
| 31 | US | 63 | ? | 95 | \_ | 127 | DEL |

这是一个完整的ASCII码表格，包含了128个字符及其对应的ASCII码值。

6. 汉字编码：

- 汉字编码用于表示汉字的字符编码方式，包括汉字外部码、汉字内部码、汉字交换码和汉字字形码等。

- GB2312编码是中国国家标准规定的汉字编码方案，使用两个字节表示一个汉字。

- 汉字外部码指汉字在计算机系统中的标准化扩展形式，如GB2312、GBK和GB18030。

- 汉字内部码是为了提高处理效率而采用的内部编码形式，如汉字的区位码。

- 汉字交换码是指针对汉字处理而规定的一套数据交换码。

- 汉字字形码是按照笔画和字形进行编码的方式，如五笔字形码。

- GB2312组成结构

第一区（B0A1 - F7FE）：这个区域包含了6763个常用汉字和其他特殊字符。

第二区（A1A1 - A9FE）：这个区域包含了一些符号、数字和日文假名。

1. 一级汉字与二级汉字：

- GB2312将汉字分为一级汉字和二级汉字。

- 一级汉字是常用汉字,按拼音排列，共包括3755个字符。

- 二级汉字是部分不常用的汉字，按部首次序排列，共包括3008个字符。

2. 国标码（国家标准码）：

- GB2312编码通过国标码来表示汉字，也称为字符的编号。

- 国标码由两个十六进制数表示，范围从A1到FE。

3. 区位码：

- 区位码表示汉字在GB2312字符集中的位置，由区号和位号组成。

- 区号范围是A1到F7，对应于编码表的行数。

- 位号范围是A1到FE，对应于编码表的列数。

4. 机内码（内码或机内字符码）：

- 机内码是指计算机内部使用的二进制码。

- GB2312的机内码采用两个字节表示，每个字节都是一个八位的二进制数。

5. GB2312编码的转换公式：

- 国标码，区位码，机内码的转换，可以通过以下公式转换

国标码=区位码+2020（H）

机内码=国标码+8080（H）

机内码=区位码+A0A0（H）

6. 示例：

1. "你"的国标码、区位码和机内码计算：

- 国标码：区位码 + 2020(H) = 2032 + 2020 = 4052(H)

- 区位码：国标码 - 2020(H) = 4052 - 2020 = 2032(H)

- 机内码：区位码 + A0A0(H) = 2032 + A0A0 = C0D2(H)

2. "好"的国标码、区位码和机内码计算：

- 国标码：区位码 + 2020(H) = 3342 + 2020 = 5362(H)

- 区位码：国标码 - 2020(H) = 5362 - 2020 = 3342(H)

- 机内码：区位码 + A0A0(H) = 3342 + A0A0 = D3E2(H)

3. "世"的国标码、区位码和机内码计算：

- 国标码：区位码 + 2020(H) = 3450 + 2020 = 5470(H)

- 区位码：国标码 - 2020(H) = 5470 - 2020 = 3450(H)

- 机内码：区位码 + A0A0(H) = 3450 + A0A0 = D8F0(H)

4. "界"的国标码、区位码和机内码计算：

- 国标码：区位码 + 2020(H) = 297B + 2020 = 499B(H)

- 区位码：国标码 - 2020(H) = 499B - 2020 = 297B(H)

- 机内码：区位码 + A0A0(H) = 297B + A0A0 = 6A1B(H)

7. 汉字存储容量：

- 汉字在计算机中通常使用两个字节表示，即16位。

- 根据GB2312标准，汉字字符集共有6763个字符（一级汉字和二级汉字）。

- 在存储容量计算中，一个汉字占用2个字节或16位。

8. 英文存储容量：

- 英文字符通常使用一个字节表示，即8位。

- 根据ASCII编码，包含128个字符。

9. 全角字符存储容量：

- 全角字符是指占用两个半角字符位置的字符，如全角汉字、全角标点等。

- 全角字符通常使用两个字节表示，即16位。

- 在存储容量计算中，一个全角字符占用2个字节或16位。

示例：

- 100个汉字的存储容量：100 \* 2 = 200字节或1600位。

- 100个英文字符的存储容量：100 \* 1 = 100字节或800位。

- 100个全角字符的存储容量：100 \* 2 = 200字节或1600位。

7. 通用编码（UTF编码、UTF-8和UTF-16）：

1. UTF编码（UCS Transformation Format）：

- UTF编码是一种用于表示Unicode字符的字符编码标准。

- Unicode旨在为全球范围内的所有字符提供唯一的标识码，涵盖了几乎所有已知语言的字符。

- UTF编码为每个Unicode字符指定了一个唯一的数字值，以便在计算机系统中进行处理和存储。

2. UTF-8编码：

- UTF-8是一种可变长度的Unicode编码方案，可以用来表示Unicode字符集中的任何字符。

- UTF-8使用1到4个字节来表示一个字符，根据字符所属的Unicode范围和数值大小进行变长编码。

- ASCII字符与UTF-8编码是兼容的，ASCII字符使用单字节表示。

3. UTF-16编码：

- UTF-16是一种固定长度的Unicode编码方案，使用2个或4个字节表示一个字符。

- UTF-16编码将字符集中的字符划分为基本多语言平面（BMP）字符和辅助平面字符。

- BMP字符的编码使用2个字节，辅助平面字符的编码使用4个字节。

- UTF-16支持所有Unicode字符，并提供了更高的编码范围。

# **第三章**

第三章

3.1计算机工作原理

3.1.1计算机的设计思想及工作原理

3.1.2计算机系统的组成

3.2计算机硬件及相关设备

3.2.1主板

3.2.2总线

3.2.3处理器

3.2.4内存储器

3.2.5外存储器

3.2.6输入设备

3.2.7输出设备

3.2.8声卡，网卡，显卡

3.3计算机软件基本知识

3.3.1软件及分类

3.3.2程序设计的基础知识

3.4计算机日常使用中的维护

3.4.1计算机的工作环境

3.4.2计算机各部件的日常维护

## 3.1计算机工作原理

### 3.1.1计算机的设计思想及工作原理

1. 计算机的设计思想 - 冯·诺依曼体系结构三大思想：

a. 存储程序的原因和好处：

- 存储程序的思想是指把指令和数据存储在计算机的存储器中，并通过控制器按照存储器中指令的顺序进行执行。

- 原因：存储程序的引入消除了传统计算设备需要重新连接和调整硬件的繁琐过程，使得计算机具有更高的灵活性和可编程性。

- 好处：

- 可以方便地编写和修改程序，无需对计算机的硬件进行改造。

- 程序和数据可以同等对待，提高了计算机的通用性和可重用性。

b. 采用二进制数的原因和好处：

- 二进制数作为冯·诺依曼体系结构的计算和存储基础，主要有以下原因和好处：

- 原因：

- 计算机内部电子器件的工作原理适合处理二进制信号，可以简化电路设计和操作。

- 二进制数具有稳定可靠的信号传输和存储特性。

- 好处：

- 二进制数系统只有两个数码（0和1），操作较简单，容易实现和理解。

- 计算机能够通过逻辑门进行基本的逻辑运算和算术运算，从而实现复杂的计算和处理任务。

c. 五大部件（冯·诺依曼体系结构的基本组成）：

冯·诺依曼体系结构的五大部件是计算机设计中的基本组成部分，包括：

- 存储器（Memory）：

- 用于存储程序和数据。

- 可根据需要进行读取和写入操作。

- 运算器（Arithmetic Logic Unit，简称ALU）：

- 用于进行算术和逻辑运算。

- 能够执行加、减、乘、除等运算操作。

- 控制器（Control Unit）：

- 负责控制计算机的操作流程和执行指令。

- 根据存储器中的指令，控制指令的获取、解码和执行。

- 输入设备（Input Device）：

- 用于将外部数据输入到计算机中进行处理。

- 常见的输入设备包括键盘、鼠标和扫描仪等。

- 输出设备（Output Device）：

- 用于将计算机处理后的结果输出给用户或其他设备。

- 常见的输出设备包括显示器、打印机和音频设备等。

2. 冯·诺依曼工作原理：

冯·诺依曼工作原理是指计算机按照一定的步骤进行指令获取、解码和执行的过程，主要包括以下内容：

- 获取指令（Fetch）：控制器从存储器中获取指令。

- 解码指令（Decode）：控制器解析指令，并确定需要执行的操作。

- 执行指令（Execute）：运算器执行指令中的操作，包括算术运算和逻辑判断等。

- 存储结果（Store）：将处理后的数据结果存储到存储器中或输出到外部设备。

3. 数据流草图：

数据流草图是描述计算机中数据流动和处理过程的图形化表示，用于展示计算机内部数据的流动和处理方式。

数据流草图使用箭头表示数据在不同部件之间的流动，用方框表示数据的存储和处理单元，以直观地展示数据的传输和处理路径。

以下是一个示例的数据流草图：

+-------+ +--------+ +-------+

+---->| 输入设备 |----->| 存储器 |----->| 运算器 |

| +-------+ +--------+ +-------+

| | | |

| | | |

| v v |

| +-------+ +--------+ +-------+

+-----| 控制器 |<----->| 输出设备 |<-----| 控制器 |

+-------+ +--------+ +-------+

4. 控制流草图：

控制流草图是描述计算机中指令和控制流程的图形化表示，用于展示指令的获取和执行流程。

控制流草图使用箭头表示指令的流向，用方框表示控制单元以及指令的解码和执行操作，以直观地展示指令的执行路径和控制流程。

以下是一个示例的控制流草图：

+-------------+

+---->| 指令获取器 |

| +-------------+

| |

| |

v |

+-------------+

| 指令解码器 |

+-------------+

| |

| |

v |

+-------------+

| 指令执行器 |

+-------------+

### 3.1.2计算机系统的组成

1. 计算机系统的组成：

a. 硬件系统：

- 硬件系统是计算机的物理组成部分，包括各种实体设备和元件。

- 主要组成部分有：

- CPU（Central Processing Unit，中央处理器）：

- 运算器（Arithmetic Logic Unit，ALU）：执行算术和逻辑运算。

- 控制器（Control Unit，CU）：控制指令的执行和数据的传输。

- 存储器（Memory）：

- 内存储器（Main Memory）：

- 随机存储器（Random Access Memory，RAM）：用于临时存储运行中的程序和数据。

- 只读存储器（Read-Only Memory，ROM）：用于存储固定的指令和数据。

- 外存储器（Secondary Storage）：用于长期存储数据和程序，如硬盘、光盘等。

- 输入设备：接受用户输入的设备，如键盘、鼠标、触摸屏等。

- 输出设备：向用户显示计算机处理结果的设备，如显示器、打印机、音响等。

- 总线系统（Bus）：用于各个硬件组件之间的数据传输。

b. 软件系统：

- 软件系统是计算机的非物理部分，包括各类程序和数据。

- 主要组成部分有：

- 操作系统（Operating System）：管理和控制计算机硬件资源的软件。

- 应用软件（Application Software）：为满足特定任务或应用需求而开发的软件。

## 3.2计算机硬件及相关设备

### 3.2.1主板

1. 主板概述：

主板是计算机系统中的核心组件，它提供电力和数据连接，并将各个硬件组件整合在一起。主板还负责协调各个组件的工作，因此是计算机硬件的主要枢纽。以下是有关主板的重要信息：

2. 主板工作原理：

主板将各个硬件组件连接在一起，并搭建计算机系统的基础结构。它通过提供电源插口、插槽、接口和电路来实现这一功能。主板上的芯片组（Chipset）起着关键的作用，负责控制数据传输和信号处理。主板也包含了BIOS（基本输入输出系统）芯片，它负责启动计算机并初始化各个硬件组件。

3. 主板部件：

a. CPU插座：

- 用于插入和固定中央处理器（CPU）。

- CPU插座会根据不同的CPU规格和架构而有所不同。

b. 芯片组：

- 由北桥和南桥芯片组组成。

- 北桥负责处理高速组件（如主内存和显卡），南桥负责处理低速组件（如硬盘和USB接口）。

c. 内存插槽：

- 用于插入内存模块（RAM）。

- 内存插槽也会根据不同的内存类型和规格而有所不同。

d. 扩展插槽：

- 用于插入扩展卡，如显卡、声卡和网卡。

- 扩展插槽包括PCI、PCIe和AGP插槽等，它们具有不同的数据传输速率和规格。

e. BIOS RAM芯片：

- 包含计算机系统的基本输入输出系统（BIOS）。

- BIOS负责启动计算机、初始化各个硬件设备并加载操作系统。

f. Cache：

- 高速缓存存储器，用于临时存储CPU常用的指令和数据，以提高处理速度。

- Cache与CPU之间通过特定的接口进行连接。

g. 接口：

- 主板上还包含各种接口，用于连接外部设备。

- 常见的接口包括SATA、USB、Ethernet、显示接口（如HDMI、VGA）等。

请注意，这只是一个简要的主板部件和接口的概述，实际主板的设计和配置可能会因不同的制造商和型号而有所不同。

### 3.2.2总线

当涉及计算机硬件之间的数据传输时，总线起着非常重要的作用。总线可以被看作是一组电子线路或电路板，用于在计算机系统的各个部件之间传输数据、地址和控制信号。总线分为三种类型：数据总线、地址总线和控制总线。

1. 数据总线（Data Bus）：

数据总线用于传输数据和指令。它可以是一个单独的线路，也可以是一组并行线路。数据总线的宽度决定了系统中可以同时传输的位数。例如，一个16位数据总线可以同时传输16位（2字节）的数据。数据总线的宽度通常与计算机的字长（Word size）相关，字长指的是一次能处理的二进制数据位数。

2. 地址总线（Address Bus）：

地址总线用于传输指令或数据在内存中的位置。它确定了计算机系统可以寻址的内存空间大小。例如，一个16位地址总线可以寻址的内存空间大小为2的16次方（64KB）。地址总线的宽度也影响处理器能够访问的外部设备的数量。

3. 控制总线（Control Bus）：

控制总线用于传输控制信号，控制和协调系统中各个部件的操作。它包含一组不同的电子线路，用于传输诸如读取、写入、中断请求、时钟信号等控制信息。控制总线也负责发送和接收中央处理单元（CPU）与其他硬件组件之间的同步信号。

### 3.2.3处理器

摩尔定律：

摩尔定律是由英特尔创始人之一戈登·摩尔于1965年提出的观察和预测。根据摩尔定律，集成电路上可容纳的晶体管数量每隔约18个月翻倍，同时成本也将下降。这意味着在相同的芯片面积上，晶体管数量将会增加，从而提高计算机性能。

中央处理器（CPU）组成：

中央处理器是计算机系统中的核心组件，主要由两个部分组成：运算器（Arithmetic Logic Unit，ALU）和控制器（Control Unit，CU）。运算器负责执行算术和逻辑操作，而控制器则负责协调和控制指令的执行。

中央处理器的品牌：

目前市场上有多个中央处理器品牌，其中最为知名的是英特尔（Intel）和AMD（Advanced Micro Devices）。

中央处理器发展史：

1. 第一代4位CPU：在20世纪70年代初，出现了第一代4位CPU，如Intel 4004。这些处理器能够执行简单的指令和运算。

2. 第二代8位CPU：在70年代晚期，8位CPU开始出现，如Intel 8080和Motorola 6800。这些处理器提供了更大的数据宽度和更强的功能。

3. 第三代16位CPU：进入80年代，16位CPU的出现如Intel 8086和Motorola 68000，提供了更高的性能和处理能力。

4. 第四代32位CPU：在80年代末至90年代初，32位CPU如Intel 80386和Motorola 68040开始流行。它们具有更大的寄存器和地址空间，提供了更高的处理能力。

5. 第五代奔腾系列：到了90年代中期，Intel推出了奔腾系列处理器，如Pentium系列。奔腾系列处理器引入了超标量架构，流水线技术以及更高的主频，大大提高了计算性能。

6. 第六代酷睿系列：从2000年起，Intel推出了酷睿系列处理器，如Core i3、i5和i7。酷睿系列处理器采用了多核心设计、更高的主频、更大的缓存容量以及先进的节能技术，进一步提升了性能。

CPU的性能参数：

- 主频（Clock Speed）：主频指的是CPU每秒钟执行的时钟周期数，通常以GHz为单位。较高的主频意味着CPU能够更快地执行指令。

- 外频（Front Side Bus）：外频是CPU与主板之间数据传输的速度，以MHz为单位。较高的外频可以提高数据传输速率。

- 前端总线频率（Front Side Bus Frequency）：前端总线频率用于连接CPU与系统内存之间的数据传输，以MHz为单位。较高的前端总线频率可以提高内存读写速度。

- 倍频系数（Multiplier）：倍频系数是CPU主频和外频之间的比值，用于计算CPU最终的主频。通过调整倍频系数，可以间接影响CPU的性能。

- 超频（Overclocking）：超频是指将CPU的工作频率设置在高于出厂默认值的状态，以获取更高的性能。超频可能会提高性能，但也会增加功耗和散热要求。

- 锁频（Locking）：锁频是指通过设置将CPU的工作频率固定在特定的值，不允许超频。这常用于稳定性要求较高的环境，如服务器。

- 缓存（Cache）：缓存是CPU内部的高速存储器，用于暂存频繁使用的数据和指令，减少对主存的访问时间。CPU通常包含多级缓存，如L1、L2和L3，容量越大、速度越快的缓存可以提高性能。

- CPU指令集（Instruction Set）：CPU指令集指的是CPU能够理解和执行的指令的集合。常见的指令集有精简指令集(RISC)和复杂指令集(CISC)。RISC指令集以精简、高效为特点，而CISC指令集提供了更多复杂的指令，能够在较少的指令下完成更多的操作。

- CPU内核和I/O工作电压：CPU内核和I/O工作电压是指CPU正常运行所需的电压。不同的处理器在工作电压方面有不同的要求。例如，内核电压用于供应内核部分的电源，而I/O电压用于供应I/O部分的电源。

- 制造工艺（Manufacturing Process）：制造工艺指的是CPU芯片制造过程中所采用的技术和工艺。制造工艺的进步可以使芯片更小、更快、更节能。常见的制造工艺单位是纳米（nm）。

- 字长（Word Length）：字长是指CPU一次能够处理的二进制数据位数。例如，32位CPU可以一次处理32位（4字节）的数据。

### 3.2.4内存储器

内存储器（Memory）是计算机系统中用于存储数据和指令的关键组件。下面是关于内存储器的一些重要信息，以及ROM和RAM之间的区别。

内存储器组成：

内存储器由一系列存储单元组成，每个存储单元可以存储一个位（0或1）。最常见的内存储器类型包括：

- 随机存储器（RAM）：可以读取和写入数据的内存储器，如静态随机存储器（SRAM）和动态随机存储器（DRAM）。

- 只读存储器（ROM）：只能读取数据而无法写入的内存储器，如只读存储器（ROM）、可编程只读存储器（PROM）、可擦除可编程只读存储器（EPROM）和闪存存储器。

内存储器的工作原理：

内存储器使用地址和数据总线来读取和写入数据。CPU根据指令中的地址信息发出读取或写入请求，内存控制器将数据从指定地址读取到CPU或从CPU写入到指定地址。

内存储器的性能指标：

1. 内存容量（Memory Capacity）：内存容量指的是内存储器可以存储的数据量，通常以字节或比特为单位。较大的内存容量可支持存储更多的数据。例如，8GB内存模块具有8亿字节（64亿比特）的内存容量。

2. 内存频率（Memory Frequency）：内存频率指的是内存模块的工作频率，通常以MHz或GHz为单位。较高的内存频率可提高数据传输的速度。例如，DDR4内存模块的频率常见为2666MHz或3200MHz。

3. 存取时间（Access Time）：存取时间指的是CPU发出存取请求到获得数据之间的时间延迟，通常以纳秒（ns）为单位。较低的存取时间表示更快的数据获取速度。例如，CL16的内存模块具有16纳秒的存取时间。

4. 数据带宽（Data Bandwidth）：数据带宽指的是内存模块在单位时间内能够传输的数据量，通常以字节或比特每秒为单位。较高的数据带宽表示更高的传输速度。例如，DDR4-3200内存模块具有每秒可传输3200兆字节（25.6吉比特）的数据带宽。

5. 接口类型（Interface Type）：内存模块与主板之间的接口类型，例如DDR4、DDR3等。不同接口类型支持不同的频率、带宽和传输速率。例如，DDR4接口可支持较高的频率和带宽。

下面是关于ROM和RAM之间的主要区别的表格：

|  |  |  |
| --- | --- | --- |
| 特性 | ROM（只读存储器） | RAM（随机存储器） |
| 性质 | 只读，无法修改 | 读写，可以随时修改 |
| 存储数据 | 不易更改的固定数据 | 运行中的数据和程序代码 |
| 读取速度 | 快 | 快 |
| 容量 | 通常较大 | 通常较小，但可扩展 |
| 持久性 | 长期保存数据，通常不会丢失 | 断电后数据丢失，需定期保存到辅助存储器 |
| 使用示例 | BIOS固件、程序代码等 | 运行中的应用程序、操作系统等 |

### 3.2.5外存储器

1.机械硬盘（HDD）

外部结构

- 接口：机械硬盘与计算机主板之间的物理连接方式。常见接口有SATA、SAS等。

- 控制电路板：位于硬盘底部，负责控制和管理硬盘的操作和数据传输。

- 固定面板：硬盘内部平行叠放的磁性盘片，用于存储数据。

内部结构

- 磁头：位于每个盘片的两侧，用于读取和写入数据。

- 磁道：盘片上的圆形区域，由同心圆组成，用于存储数据。

- 扇区：每个磁道划分的等大小存储区域，用于存储数据。

- 柱面：多个盘片上相同位置的磁道构成的一个圆柱体。

容量

- 容量表示机械硬盘可以存储的数据量，通常以字节为单位。例如，1TB硬盘可以存储约1兆字节的数据。

转速

- 转速表示机械硬盘的盘片旋转速度，通常以每分钟转数（RPM）为单位。较高的转速可提高数据读写速度，如常见的7200 RPM硬盘。

平均访问时间

- 评价访问时间：硬盘持续工作的平均时间，通常以小时为单位。

- 平均寻道时间：磁头从一个磁道寻道到另一个磁道的平均时间。

- 等待时间：等待所需数据旋转到磁头位置的平均时间。

- 传输速率：

- 传输数率：数据在磁道上的传输速率，通常以每秒传输的字节数（MB/s或GB/s）衡量。

- 内部传输率：硬盘内部数据传输的速率。

- 外部传输率：硬盘与计算机之间数据传输的速率。

缓存

- 硬盘上的缓存用于临时存储磁盘访问的数据，以加速读写速度。缓存越大，读写性能越好。

制造厂商

- 常见的机械硬盘制造商有西部数据（WD）、希捷（Seagate）、东芝（Toshiba）、日立（Hitachi）等。

2.固态硬盘（SSD）

概述

- 固态硬盘使用闪存存储技术而非机械部件，具有较高的读写速度和抗震性。

优点

- 快速启动和加载速度。

- 低能耗和噪音。

- 较高的数据可靠性和耐用性。

制造厂商

- 常见的固态硬盘制造商有三星（Samsung）、英特尔（Intel）、东芝（Toshiba）等。

3.移动硬盘

- 移动硬盘是便携式的外部存储设备，具有较大的容量。通常用于数据备份和传输。

4.U盘

- U盘是一种小型、可移动、即插即用的闪存驱动器，用于数据存储和传输。常用于个人文件备份和数据共享。

5.光盘

- 光盘使用光学存储技术，用于存储和传输数据。常见的类型包括CD、DVD和蓝光（Blu-ray）光盘。

6.存储卡

- 存储卡是一种小型的可移动存储介质，广泛用于移动设备（如手机、相机）和其他电子设备中。

下面是各种外存储器的对比表格:

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| 特性 | 机械硬盘 | 固态硬盘 | 移动硬盘 | U盘 | 光盘 | 存储卡 |
| 存储技术 | 磁性存储 | 闪存存储 | 磁性存储 | 闪存存储 | 光学存储 | 闪存存储 |
| 访问速度 | 较慢 | 较快 | 较慢 | 较快 | 较慢 | 较快 |
| 容量 | 较大 | 大 | 较大 | 较小 | 较小 | 较小 |
| 重量 | 较重 | 轻 | 较重 | 轻 | 轻 | 轻 |
| 震动和震动影响 | 对机械部件敏感 | 对机械部件不敏感 | 对机械部件敏感 | 无 | 有 | 无 |
| 平均寿命 | 一般较长 | 较短 | 一般较长 | 一般较长 | 一般较长 | 一般较长 |

### 3.2.6输入设备

1.键盘

概述：

键盘是一种常见的人机交互设备，用于输入文字、命令和其他功能键操作。它是计算机用户最常接触和使用的输入设备之一。

键位布局：

键盘通常采用QWERTY键位布局，其中字母和大多数符号键位按照字母表顺序排列。它还包括数字键、功能键（F1至F12）、控制键（Ctrl、Alt、Shift等）以及专用键（如回车键、空格键等）。

键盘类型：

- 传统键盘：标准的键盘布局，具有嵌入式键盘、机械键盘和薄膜键盘等不同类型。

- 笔记本键盘：用于笔记本电脑和便携式设备的键盘，通常较小且紧凑。

- 游戏键盘：专为游戏玩家设计的键盘，带有额外的宏按键、背光和其他游戏特定功能。

2.鼠标

概述：

鼠标是一种用于控制光标位置和执行操作的手持式指针设备。通过鼠标在平面上的移动和按钮的点击，用户可以与计算机进行交互。

鼠标类型：

- 机械鼠标：采用机械传感器和滚轮，需要在平面上滑动以控制光标位置。

- 光学鼠标：使用LED或激光传感器来检测平面上的移动，它通常更精确和灵敏。

- 滚轮鼠标：具有额外的滚轮，可用于在窗口和文档之间进行滚动。

- 触摸鼠标：支持多指触控，用户可以通过手指手势进行各种操作。

3.扫描仪

概述：

扫描仪用于将印刷文档、照片和其他纸质媒体转换为数字格式。它可以将纸质信息输入到计算机中，方便存储、编辑和共享。

扫描仪类型：

- 平板式扫描仪：用户将要扫描的文档放置在扫描仪的平板上，然后通过扫描仪的传感器进行扫描。

- 自动进纸式扫描仪：可以自动进纸并连续扫描多页文档，提高工作效率。

- 手持式扫描仪：便携式设备，用户手持扫描仪在纸质文档上滑动以进行扫描。

4.其他输入设备

除了键盘、鼠标和扫描仪外，还有许多其他输入设备可供选择，以满足不同的个人和专业需求。

一些常见的其他输入设备包括：

- 数位板：用于绘图和设计的设备，用户可以通过使用触控笔在数位板上绘图。

- 触摸屏：可通过手指或触控笔直接与屏幕交互，广泛应用于移动设备和公共信息显示屏。

- 音频输入设备：如麦克风、音频录音设备，用于录制声音和语音输入。

- 视频输入设备：如摄像头、摄像机，用于捕捉静态图片或动态视频。

- 生物识别设备：如指纹扫描仪、虹膜扫描仪，用于身份认证和安全访问。

### 3.2.7输出设备

显示器

概述：

显示器是计算机输出设备的一种，用于显示图像、文字和视频。它是将计算机处理的信息可视化的主要方式。

主要技术指标：

屏幕尺寸：

屏幕尺寸指的是显示器对角线的长度，通常以英寸（inch）为单位。较大的屏幕尺寸可以提供更广阔的视野和更丰富的视觉体验。

示例：21.5英寸、27英寸、32英寸等。

点距：

点距（Pixel Pitch）是指屏幕上相邻像素之间的距离。较小的点距可以提供更高的像素密度和更细腻的图像显示。

示例：0.28毫米、0.25毫米、0.23毫米等。

分辨率：

分辨率指的是显示器可以显示的像素数量，一般以水平像素数乘以垂直像素数来表示。较高的分辨率可以呈现更清晰和更详细的图像。

示例：1920x1080（Full HD）、2560x1440（QHD）、3840x2160（4K Ultra HD）等。

灰度级：

灰度级（Grayscale）指的是显示器能够显示的不同灰度或亮度级别的数量。较高的灰度级可以提供更丰富的色彩深度和细节展现。

示例：8位灰度、10位灰度、12位灰度等。

刷新频率：

刷新频率（Refresh Rate）指的是显示器每秒钟更新图像的次数，以赫兹（Hz）为单位。较高的刷新频率可以提供更流畅的图像和更少的画面闪烁。

示例：60Hz、120Hz、144Hz等。

打印机

概述：

打印机是一种计算机外部设备，用于将电子文档转换为实际的纸质输出。常见的打印机类型包括针式打印机、喷墨打印机和激光打印机。

针式打印机：

针式打印机使用一排针脚（针）来敲击墨带，将墨带上的墨水转移到纸上，形成字符或图像。

喷墨打印机：

喷墨打印机通过喷射墨水微滴到纸上来生成图像。喷墨打印机分为热喷墨和冷喷墨两种类型。

激光打印机：

激光打印机使用激光束和静电技术将墨粉粘附到纸上，形成图像或文字。

音箱：

音箱是输出音频信号的设备，用于增强计算机产生的声音。它可以提供更好的音质和更高的音量。

绘图仪：

绘图仪是一种输出设备，用于将计算机生成的图形信息转化为实际的绘图或绘制。绘图仪通常用于设计、工程和制图领域，以创建精确的图像和图纸。

### 3.2.8声卡，网卡，显卡

声卡

概述：

声卡是计算机中的一种重要组件，用于处理和输出音频信号。它将数字音频信号转换为模拟信号，通过扬声器或耳机播放出来。

功能：

声卡具有以下主要功能：

- 音频输入：接受外部音频信号，例如麦克风、音乐播放器等。

- 音频处理：将音频信号转换为数字格式，并对其进行处理和调整。

- 音频输出：将经过处理的音频信号转换为模拟信号，并通过扬声器或耳机播放出来。

类型：

- 集成声卡：集成在主板上，适用于普通音频需求。

- 独立声卡：可提供更高音质和更多音频输入输出选项，适用于专业音频编辑和高端音乐制作。

声卡示例：

- Creative Sound Blaster Z：一款独立声卡，提供高保真音频和多通道音频输出，适用于音乐制作和游戏体验。

- ASUS Xonar Essence STX II：一款高端独立声卡，采用高品质的数字模拟转换器和放大器技术，提供出色的音频质量和低噪声水平。

网卡

概述：

网卡（网络适配器）是计算机与计算机网络之间进行数据传输的关键设备。它使计算机能够接入局域网或互联网。

功能：

网卡具有以下主要功能：

- 网络连接：通过以太网、Wi-Fi或其他网络技术，将计算机连接到网络。

- 数据传输：将计算机中的数据转换为网络可识别的格式，并通过网络发送和接收数据。

- 网络协议支持：支持不同的网络协议（如TCP/IP），以确保数据在网络中的正确传输和接收。

类型：

- 有线网卡：使用以太网（Ethernet）接口与电脑连接，通过以太网线进行数据传输。

- 无线网卡：支持Wi-Fi技术，通过无线信号进行数据传输，提供无线上网能力。

网卡示例：

- Intel Ethernet Converged Network Adapter X540-T2：一款高性能有线网卡，支持高速以太网连接，适用于数据中心和企业级网络。

- TP-Link Archer T6E：一款双频无线网卡，支持802.11ac Wi-Fi技术，提供快速的无线网络连接，适用于家庭和办公环境。

显卡

概述：

显卡（显卡处理器或图形处理器）是计算机中用于处理和输出图形图像的关键组件。它负责计算和渲染图像，并将其显示在显示器上。

功能：

显卡具有以下主要功能：

- 图像处理：负责计算和处理图形数据，如三维渲染、图像编辑和视频解码。

- 显示控制：将处理后的图像信号转换为显示器可以识别的格式，并输出到显示器上显示。

- 显存管理：管理显卡的专用显存，用于存储和访问图像数据。

类型：

- 集成显卡：集成在主板上，适用于基本图形需求，如办公和网页浏览。

- 独立显卡：也被称为独立图形卡或显卡，是一种插入式设备，适用于游戏、图形设计和视频编辑等需求，提供更高的图形处理能力。

显卡示例：

- NVIDIA GeForce RTX 3080：一款高性能独立显卡，采用先进的图形处理架构和光线追踪技术，适用于游戏和图形设计。

- AMD Radeon Pro WX 9100：一款专业级独立显卡，为专业图形和视频工作提供出色的性能和精准的颜色表现。

## 3.3计算机软件基本知识

### 3.3.1软件及分类

1. 系统软件

1.1 操作系统（Operating System）：操作系统是系统软件的核心，它管理和控制计算机的硬件和软件资源，为应用软件提供运行环境。操作系统的主要功能包括进程管理、内存管理、文件系统管理和设备管理等。常见的操作系统包括：

- Windows操作系统：如Windows 10、Windows Server等。

- macOS：苹果公司开发的操作系统，用于苹果电脑和Mac设备。

- Linux：开源的操作系统，有多个不同的发行版，如Ubuntu、Red Hat、Fedora等。

- Unix：多用户、多任务的操作系统家族，包括GNU/Linux、FreeBSD等。

1.2 计算机语言及语言处理系统：计算机语言是一种用于编写计算机程序的标记系统。根据级别和抽象程度的不同，计算机语言可以分为以下几类：

- 机器语言：机器语言是计算机可直接执行的二进制指令集，使用二进制代码表示指令和数据。每种计算机体系结构都有自己的机器语言，例如x86机器语言用于英特尔和AMD处理器。

- 汇编语言：汇编语言通过使用助记符（mnemonics）来代表机器语言指令和操作数。它使用符号名称代替二进制代码，更易理解和编写。例如，x86汇编语言用于编写与英特尔和AMD处理器兼容的程序。

- 高级语言：高级语言是更接近自然语言的计算机语言。它们使用更抽象的语法和结构，开发者可以用更简洁和可读的代码编写程序。常见的高级语言有Java、Python、C++、C#、JavaScript等。

1.3 数据库管理系统（Database Management System，DBMS）：数据库管理系统是一种软件工具，用于创建、管理和操作数据库。它提供了对数据库的访问、查询和维护功能。常见的数据库管理系统包括：

- Oracle Database：一个功能强大的关系型数据库管理系统。

- MySQL：一个开源的关系型数据库管理系统。

- Microsoft SQL Server：微软开发的关系型数据库管理系统，用于Windows操作系统环境。

2. 应用软件

2.1 概念：应用软件是根据用户需求开发的具体应用程序，用于完成特定的任务和解决特定的问题。它通常建立在操作系统和系统软件的基础上，提供给用户友好的界面和功能。应用软件可以满足各种需求，包括办公、图形设计、视频制作、音频处理、数据分析等。

2.2 例子：常见的应用软件包括：

- 办公套件：例如Microsoft Office（包括Word、Excel、PowerPoint等）、LibreOffice（开源办公套件）等，用于文档处理、电子表格、演示文稿等办公任务。

- 图形图像处理软件：例如Adobe Photoshop、CorelDRAW、GIMP（开源图像处理软件）等，用于图形设计、图像编辑和图形处理。

- 视频编辑软件：例如Adobe Premiere Pro、Final Cut Pro、DaVinci Resolve等，用于视频剪辑、特效处理和视频制作。

- 音频处理软件：例如Adobe Audition、Audacity（开源音频处理软件）等，用于音频录制、编辑、混音等。

- 数据分析软件：例如Microsoft Excel、RStudio、SAS等，用于数据处理、统计分析和建模。

- 网页浏览器：例如Google Chrome、Mozilla Firefox、Microsoft Edge等，用于浏览互联网上的网页内容。

3. 用户程序

3.1 概念：用户程序是由计算机用户自行编写或使用的软件程序，用于满足个人需求或自定义特定功能。

3.2 例子：用户程序可以是各种不同类型的应用软件，例如自行编写的小工具、个人网站的代码、特定领域的模拟程序等。用户程序的具体例子因用户需求的多样性而各异。

4. 应用软件包

4.1 概念：应用软件包是针对特定行业或专业领域开发的软件组合，提供全面的解决方案。

4.2 例子：常见的应用软件包包括医疗信息系统、企业资源计划（ERP）软件、供应链管理软件等。例如，医疗信息系统软件可以集成患者管理、医生排班、病历记录、药物管理等功能，用于医院和医疗机构的管理和运营。

### 3.3.2程序设计的基础知识

1. 程序设计的基本概念

1.1 源程序：源程序是程序员使用编程语言编写的原始代码，它是用来实现特定功能的程序。源程序一般以文本文件的形式存储，例如使用C语言编写的源文件以.c为扩展名。

1.2 编译程序：编译程序是将源程序翻译为目标程序的工具。编译程序将源程序作为输入，进行词法分析、语法分析、语义分析、代码优化等步骤，最终生成可执行的目标程序。常见的编译程序有GCC、Microsoft Visual C++等。

1.3 汇编程序：汇编程序是将汇编语言源程序转换为机器指令的工具。汇编程序将汇编源程序进行词法分析和语法分析，并将汇编指令转换为对应的机器指令。常见的汇编程序有NASM、MASM等。

1.4 目标程序：目标程序是编译或汇编后生成的二进制代码，它是可执行程序的中间形式。目标程序不能直接运行，需要通过连接程序进行最终的链接才能生成可执行程序。

1.5 连接程序：连接程序将目标程序与所需的库文件进行链接，生成最终的可执行程序。链接的过程包括地址分配、符号解析、重定位等。连接程序可以静态链接或动态链接，以生成可执行程序。

1.6 可执行程序：可执行程序是经过编译、汇编和链接后生成的可以直接运行的程序。它包含了机器指令、数据和其他必要的资源。用户可以通过执行可执行程序来实现程序设计中所需的功能。

2. 算法及其表示方法

2.1 算法：算法是解决特定问题的一系列步骤或操作的描述。它描述了问题的输入、如何处理输入数据以及得到正确输出的过程。算法必须具备有穷性、确定性、可行性等特征。例如，冒泡排序算法可以对一组数字进行升序排序。

2.2 算法的时间复杂度与空间复杂度：算法的时间复杂度和空间复杂度度量了算法运行时间和所需内存空间的增长率。

- 时间复杂度：时间复杂度表示了算法运行所需时间与问题规模之间的关系。常见的时间复杂度有O(1)、O(log n)、O(n)、O(n^2)等。例如，一种求解数组中最大值的算法的时间复杂度可以表示为O(n)。

- 空间复杂度：空间复杂度表示了算法运行所需内存空间与问题规模之间的关系。常见的空间复杂度有O(1)、O(n)、O(n^2)等。例如，一种创建二维数组的算法的空间复杂度可以表示为O(n^2)。

2.3 算法的特征

- 有穷性：算法必须在有限步骤内结束，不会无限循环或运行。

- 确定性：算法中的每个步骤都必须明确定义，不会存在二义性。

- 可行性：算法应该能够实际运行，并能够解决给定问题的实例。

- 输入：算法需要从外部接收输入数据，用于问题解决的计算过程。

- 输出：算法产生的结果或解答，用以解决给定问题。

2.4 算法的表示方法

- 流程图：流程图是用图形符号表示算法步骤和流程的图形化工具。它使用不同形状的框和箭头表示不同的操作和控制流程。例如，矩形框表示操作步骤，菱形框表示判断条件，箭头表示控制流程。

- 伪码：伪码是一种类似自然语言的描述性语言，用于表示算法的操作步骤和控制流程。伪码与具体编程语言无关，更便于算法设计和理解。例如，使用伪码可以描述条件判断、循环和基本操作等。

1. 结构化程序设计

1.1 概念：结构化程序设计是一种基于顺序、选择和循环等基本控制结构的编程方法。它强调程序的结构化组织和模块化，将复杂的问题分解为小的可管理的部分，使用顺序、选择和循环等控制结构来实现程序流程控制。结构化程序设计使得程序具有清晰、易于理解和维护的特点。

1.2 例子：一个结构化程序设计的示例是计算一个数列的和。程序使用循环结构控制计算，逐个累加数列中的元素，直到达到指定的终止条件。

1.3 优点：结构化程序设计的优点包括可读性强、易于理解和维护、模块化设计，以及容易进行代码复用等。结构化程序设计方法使得程序结构清晰可见，有助于减少错误和提高代码质量。

2. 面向对象程序设计

2.1 概念：面向对象程序设计（Object-Oriented Programming，简称OOP）是一种以对象为基本单位的编程范式。它通过封装、继承和多态等机制，使得程序以对象的形式进行组织和表达。面向对象的编程方法强调对象之间的交互和消息传递，更加注重数据和行为的关联。

2.2 例子：一个面向对象程序设计的示例是实现一个图书管理系统。系统中的图书、借阅者和管理员等角色被抽象为对象，每个对象具有特定的属性和行为。例如，图书对象可以有属性如书名、作者和出版社，行为如借阅和归还。

3. 面向对象的基本概念

- 对象：对象是类的一个实例，具有类定义的属性和行为。每个对象可以具有独特的状态，但共享类定义的行为。例如，一个名为Person的类可以定义属性如姓名和年龄，并定义行为如打招呼和工作。

- 类：类是对象的模板或蓝图，定义了对象共同的属性和行为。它是面向对象程序设计中的基本构建单元。例如，一个名为Car的类可以定义属性如品牌和颜色，并定义行为如启动和停止。

- 消息和方法：对象之间通过发送消息进行交互。消息是对对象执行特定方法的请求。方法是对象中定义的函数或过程，用于响应消息的请求并完成相应的操作。例如，一个名为run的方法可以被调用来启动Car对象。

4. 面向对象的主要特征

- 封装性：封装是将数据和对数据的操作封装在一个单元中的机制。它使得对象的内部细节对外部不可见，只能通过公共接口进行访问。例如，一个名为BankAccount的类可以封装账户余额，并提供公共方法如存款和取款来访问和更新余额。

- 继承性：继承是一种定义新类的机制，通过继承可以获得已有类的属性和行为，并允许新类添加、修改或覆盖部分属性和行为。它提供了代码的重用和扩展的能力。例如，一个名为CheckingAccount的类可以继承BankAccount类的属性和方法，并添加新的属性和方法。

- 多态性：多态是指同一个消息可以被不同的对象接收和理解，并产生不同的行为。它通过方法的重写和重载实现，增强了代码的灵活性和扩展性。例如，一个名为Animal的类可以定义一个名为makeSound的方法，不同的子类如Dog和Cat可以重写makeSound方法以产生独特的动物声音。

5. 面向对象的要素

- 抽象：抽象是将对象的共同特征提取出来，形成类的过程。它简化了实现的复杂性，提供了更高层次的概念和模型。例如，一个名为Shape的抽象类可以定义共同属性和方法，而具体的子类如Circle和Rectangle可以实现具体的形状。

- 共享性：共享性是指对象之间可以共享相同的属性和行为。这减少了重复代码的出现，提高了代码的复用性和可维护性。例如，多个BankAccount对象可以共享相同的存款和取款方法。

6. 面向对象程序设计的优点包括更好的模块化和组织性、代码复用、可维护性和扩展性，以及更容易理解和调试。面向对象的设计和开发有助于构建更高质量、灵活和可维护的软件系统。

7. 高内聚与低耦合

- 高内聚：高内聚是指一个模块内部的功能元素之间联系紧密的程度。在面向对象的设计中，高内聚意味着类内部的属性和方法彼此关联度高，共同完成某个特定任务。例如，一个名为Calculator的类实现了多个计算功能，它的内部方法彼此紧密联系，共同构成计算器功能。

- 低耦合：低耦合是指模块间的相互依赖关系的松散程度。在面向对象的设计中，低耦合意味着类与类之间的相互影响较小，修改一个类不会对其他类产生太大的影响。例如，一个名为Printer的类可以与多个不同的打印任务类进行交互，而这些打印任务类并不直接依赖于Printer类的具体实现细节。

## 3.4计算机日常使用中的维护

### 3.4.1计算机的工作环境

1. 温度条件

- 概念：计算机需要在适宜的温度范围内工作。过高或过低的温度都可能对计算机的性能和可靠性产生不利影响。

- 推荐条件：一般来说，计算机的温度应该控制在15°C到25°C的范围内。高于或低于这个范围都可能导致设备过热或过冷，影响计算机的正常工作。

2. 湿度条件

- 概念：湿度是指空气中水分的含量。过高或过低的湿度都可能对计算机的性能和可靠性产生不利影响。

- 推荐条件：计算机的工作环境应该保持适度的湿度。一般来说，湿度应该控制在40%到60%的范围内。过高的湿度可能导致电器元件腐蚀和电路短路，而过低的湿度可能导致静电放电和电子元件故障。

3. 电源要求

- 概念：计算机需要稳定的电源供应来确保正常工作。不稳定的电源可能导致计算机崩溃、数据丢失或硬件损坏。

- 要求：计算机通常需要使用交流电源，电压应保持稳定在所需的电压范围内，一般为220伏特（根据地区和设备而有所不同）。此外，应使用电压稳定器、UPS（不间断电源）等设备来保护计算机免受电压波动和停电的影响。

4. 防尘

- 原因：尘埃和颗粒物会堆积在计算机及其组件上，导致散热不畅、损坏电子元件和影响性能。

- 方法：为了保护计算机免受尘埃的影响，可以采取以下措施：

- 定期清洁：定期对计算机和其周围的区域进行清洁，包括键盘、鼠标、机箱和通风孔口。使用吹气罐或柔软的刷子将尘埃清除。

- 过滤器：安装过滤器来阻挡空气中的尘埃和颗粒物。

- 电脑机箱：选择具有良好通风和防尘设计的机箱，以减少尘埃的积累。

5. 防静电

- 原因：静电可以损坏计算机中的电子元件，导致设备故障或数据丢失。

- 方法：为了防止静电影响计算机，可以采取以下措施：

- 接地：确保计算机和周围设备与地面接触良好，以释放静电。使用接地插头和接地线来连接电源插座和计算机。

- 防静电设备：在处理计算机组件之前，使用防静电手环或脚垫来将身体与地面连接，释放静电。

6. 防磁场

- 原因：磁场可以对计算机的磁性存储设备（如硬盘驱动器）产生影响，导致数据损坏或丢失。

- 方法：为了防止磁场对计算机的影响，可以采取以下措施：

- 存放位置：确保计算机远离磁性设备（如大功率扬声器、电视机等）和强磁场区域。

- 屏蔽：使用屏蔽材料或磁屏蔽罩来保护计算机免受外部磁场的干扰。

7. 防震动与噪声

- 原因：震动和噪声可能对计算机中的移动部件（如硬盘驱动器）产生影响，导致设备损坏或性能下降。

- 方法：为了防止震动和噪声对计算机造成影响，可以采取以下措施：

- 放置位置：将计算机放置在稳固的表面上，避免外部冲击和震动。

- 隔离：使用防震垫和隔音垫来减少震动和噪声对计算机的传递。

- 设备选择：选择低噪声和抗震动的设备，如固态硬盘驱动器和无风扇散热器。

### 3.4.2计算机各部件的日常维护

1. 主板

- 检查方法：

- 检查主板上的插头和插槽是否牢固连接。

- 检查主板上的指示灯和显示器输出是否正常。

- 维护方法：

- 定期清洁主板上的灰尘和污垢，使用吹气罐或柔软的刷子小心地清除。

- 确保主板和周围环境的通风良好，并避免灰尘和污垢的积累。

- 常见故障及处理方法：

- 电源问题：检查电源供应是否正常，确保电源线连接良好。

- 内存问题：重新插拔内存条，确保它们得到正确的连接。

- 插槽问题：检查主板插槽是否损坏或过时，必要时更换。

- 注意事项：

- 尽量避免主板与静电敏感的物体接触，以防止静电放电对主板造成损害。

- 注意使用正确的安装和升级方法，避免损坏主板。

2. CPU

- 检查方法：

- 检查CPU温度是否正常，可以使用软件工具来监测CPU温度。

- 检查CPU风扇是否正常运转，确保散热系统的正常工作。

- 维护方法：

- 定期清洁CPU散热器和风扇上的灰尘和污垢，并确保它们的良好安装。

- 定期更换散热膏以提供更好的散热效果。

- 常见故障及处理方法：

- 过热问题：清洁散热器和风扇，确保散热系统的正常工作。

- 电源问题：检查电源连接是否正确。

- 注意事项：

- 处理CPU时要小心，避免损坏CPU芯片或引脚。

- 在升级或更换CPU时，注意选择适用于主板的兼容性。

3. 内存条

- 检查方法：

- 检查内存条是否插入插槽正确，查看系统中的可用内存是否正确识别。

- 维护方法：

- 定期清洁内存条和插槽上的灰尘和污垢。

- 确保内存条插入插槽时牢固连接。

- 常见故障及处理方法：

- 连接问题：重新插拔内存条，确保插入正确的插槽。

- 注意事项：

- 对于使用多个内存条的系统，确保内存条的型号、容量和速度相匹配，以提供最佳的性能和兼容性。

- 避免在带电的环境下触摸内存条，以防止静电放电对其造成损坏。

4. 显示器

- 检查方法：

- 检查显示器连接是否牢固，观察显示屏幕是否正常显示。

- 维护方法：

- 使用液晶显示器清洁剂和柔软的纤维布清洁显示器屏幕。

- 避免长时间显示相同的静态图像，以防止屏幕烧结。

- 常见故障及处理方法：

- 显示问题：检查显示器连接和信号源，确保正确选择显示输入。

- 屏幕损坏：避免长时间显示相同的静态图像，以防止屏幕烧结。

- 注意事项：

- 避免使用过大的亮度和对比度设置，以延长显示器的使用寿命。

- 在移动或搬运显示器时，小心处理，避免碰撞和摔落。

5. 显卡

- 检查方法：

- 检查显卡是否插入插槽正确，查看显卡驱动程序是否正常安装。

- 维护方法：

- 定期清洁显卡上的灰尘和污垢。

- 更新显卡驱动程序以获得更好的兼容性和性能。

- 常见故障及处理方法：

- 显示问题：检查连接和显示设置，确保正确选择显示器输入。

- 注意事项：

- 在安装或拆卸显卡时，小心操作，避免损坏显卡或主板的插槽。

- 当进行显卡升级时，确保电源供应能够满足新显卡的功耗要求。

6. 声卡

- 检查方法：

- 检查声卡是否正常识别和配置，查看声音设置是否正确。

- 维护方法：

- 定期更新声卡驱动程序以获得更好的兼容性和性能。

- 常见故障及处理方法：

- 声音问题：检查连接和声音设置，确保扬声器和耳机正常工作。

- 注意事项：

- 在安装或拆卸声卡时，小心操作，避免损坏声卡或主板的插槽。

- 注意音量的适当调节，以防止过大的音量对耳朵造成损伤。

7. 鼠标

- 检查方法：

- 检查鼠标连接是否牢固，检查鼠标按钮和滚轮是否正常响应。

- 维护方法：

- 定期清洁鼠标表面和按钮，使用纸巾或棉签轻轻擦拭。

- 检查鼠标上的光学或激光传感器是否干净，避免灰尘和污垢的积累。

- 常见故障及处理方法：

- 鼠标运动问题：清洁鼠标表面和底部的传感器，确保没有灰尘或污垢阻碍。

- 注意事项：

- 避免用力敲击或摔落鼠标，以防止损坏内部部件。

- 避免长时间使用鼠标造成手部疲劳，注意适当休息。

8. 键盘

- 检查方法：

- 检查键盘连接是否牢固，检查键盘按键是否正常弹起和回弹。

- 维护方法：

- 定期清洁键盘表面和按键，使用适当的键盘清洁剂和柔软的布料。

- 倒置键盘，轻轻敲击背面以帮助清除落入键盘中的灰尘和污垢。

- 常见故障及处理方法：

- 按键不响应：检查键盘连接和键盘设置，确保键盘正常工作。

- 注意事项：

- 避免键盘接触水和液体，以防止损坏电路和按键的机械部件。

- 避免暴力操作键盘，以防止按键损坏。

# 第四章

第四章

4.1多媒体技术概述

4.1.1多媒体技术的概念

4.1.2多媒体技术的特点

4.2多媒体计算机系统的组成

4.2.1多媒体计算机硬件系统

4.2.2多媒体计算机软件系统

4.3多媒体处理技术

4.3.1图像处理

4.3.2音频处理

4.3.3视频处理

4.4平面设计基础知识

4.4.1平面设计概述

4.4.2位图处理软件 Adobe Photoshop

## 4.1多媒体技术概述

### 4.1.1多媒体技术的概念

1. 多媒体的概念

- 媒体：

- 概念：媒体是指在人与计算机之间传递信息的载体，可以是文字、图像、音频、视频或其他形式的表现方式。

- 例子：报纸、电视、广播、网络、电影等都是媒体的例子。

- 感觉媒体：

- 概念：感觉媒体是通过人类感官器官来传达信息和表达体验的媒体形式，包括视觉媒体、听觉媒体和触觉媒体等。

- 例子：影像、音乐、绘画等都属于感觉媒体的例子。

- 表示媒体：

- 概念：表示媒体是用于表达想法、观点和事实的媒体形式，主要通过符号、文字、图形等来传递信息。

- 例子：书籍、报纸、杂志、网站等都是表示媒体的例子。

- 显示媒体：

- 概念：显示媒体是用于呈现各种媒体内容的设备或载体，它可以是显示器、投影仪、电视等。

- 例子：计算机显示器、电视屏幕、投影幕布等都是显示媒体的例子。

- 存储媒体：

- 概念：存储媒体是用来记录和存储各种媒体内容的物质介质，例如硬盘、光盘、闪存等。

- 例子：硬盘驱动器、CD、DVD、闪存卡等都是存储媒体的例子。

- 传输媒体：

- 概念：传输媒体是用于传递媒体内容的通信信道，包括以太网、无线网络、卫星链路等。

- 例子：以太网、Wi-Fi、蓝牙、卫星传输等都是传输媒体的例子。

2. 媒体元素

- 概念：媒体元素是构成多媒体内容的基本组成部分，包括文本、图像、音频、视频等。

- 例子：

- 文本：电子书、文章、网页内容等。

- 图像：照片、绘画、图标、图表等。

- 音频：音乐、声音效果、语音等。

- 视频：电影、电视节目、动画等。

3. 多媒体与多媒体技术

- 多媒体的概念：

- 概念：多媒体是指在计算机技术的支持下，将不同类型的媒体元素（如文本、图像、音频、视频等）结合起来，以丰富多样的方式呈现和传递信息的形式。

- 例子：多媒体应用程序、电子游戏、互动教育软件等。

- 多媒体技术的概念：

- 概念：多媒体技术是指利用计算机和相关技术手段，对多媒体内容进行创作、处理、存储、传输和展示等方面的技术方法和工具。

- 例子：图像处理技术、音频编解码技术、视频压缩技术等都是多媒体技术的例子。

- 注意事项：

- 多媒体技术的应用涵盖了广泛的领域，包括娱乐、教育、传媒、广告等。

- 在实际应用中，需要根据具体需求选择合适的媒体元素和技术手段，并注重创意、用户体验以及技术的可行性和效果。

### 4.1.2多媒体技术的特点

多媒体技术具有以下特点，它们是多样性、集成性、交互性和实时性。

1. 多样性

- 概念：多媒体技术能够处理和呈现多种形式的媒体，包括文本、图像、音频、视频等，使得信息传递更加丰富、生动和多样化。

- 例子：

- 文本：字体、颜色、样式等的多样性。

- 图像：静态图像、动态图像（连续帧动画、动画 GIF、Flash等）。

- 音频：不同类型的音乐、声音效果、语音等。

- 视频：不同类型的电影、电视节目、动画等。

2. 集成性

- 概念：多媒体技术能够将不同类型的媒体元素有机地融合在一起，通过结合文字、图像、音频和视频等，创建出统一、完整的多媒体内容。

- 例子：

- 讲义设计：将文本、图像、动画和音频结合在一起，制作具有教育内容的讲义。

- 广告制作：将文字、图像、音频和视频相互配合，制作具有吸引力的广告内容。

- 电子图书：将文字、图像和音频以及相应的交互功能融合在一起，打造互动性强的电子图书。

3. 交互性

- 概念：多媒体技术能够实现用户与系统之间的双向交流和互动，用户可以对多媒体内容进行操作、控制和反馈，增加了用户参与度和体验感。

- 例子：

- 互动教育软件：通过点击、拖动、输入等方式，让学习者与教育软件进行互动交流。

- 视频游戏：玩家通过操纵手柄、键盘或触摸屏幕等设备与游戏互动。

- 虚拟现实体验：利用设备提供的交互功能，让用户身临其境地参与虚拟世界的体验。

4. 实时性

- 概念：多媒体技术能够在用户与系统之间实现实时的交互和响应，快速处理和呈现多媒体内容，使用户能够及时感知和反馈信息。

- 例子：

- 视频会议：在线实时传输视频和音频数据，实现远程的面对面沟通和交流。

- 实时多媒体播放：通过流媒体技术将音频和视频内容实时传输和播放，实现实时的娱乐和信息获取。

- 互动娱乐应用：根据用户的实时操作和反馈，动态调整和呈现多媒体内容，提供更加个性化的娱乐体验。

## 4.2多媒体计算机系统的组成

### 4.2.1多媒体计算机硬件系统

1. 多媒体计算机的基本部件

- 概念：多媒体计算机是指专门用于处理和呈现多媒体内容的计算机系统。它包括以下基本部件：

- 处理器：负责计算和控制计算机的核心部件，例如Intel Core i7或AMD Ryzen处理器。

- 内存：用于临时存储计算机正在处理的数据和程序。多媒体内容的处理通常需要较大容量的内存，例如8GB或16GB RAM。

- 存储设备：用于永久存储数据和多媒体文件的设备，例如硬盘驱动器、固态硬盘（SSD）或光盘驱动器。

- 显示器：用于显示多媒体内容的输出设备，可以是液晶显示器、LED显示器或投影仪。

- 键盘和鼠标：用于输入和控制多媒体计算机的输入设备。

- 声音输出设备：用于播放音频内容的设备，例如耳机、扬声器或音箱。

- 网络连接设备：用于与其他设备和网络进行数据交互的设备，例如网卡、无线网卡。

2. 多媒体板卡

- 显卡：

- 概念：显卡是负责计算机图形处理和显示的重要组件，它将计算机数据转换为可供显示器输出的图像信号。

- 例子：NVIDIA GeForce RTX 3080、AMD Radeon RX 6900 XT等显卡。

- 声卡：

- 概念：声卡是负责处理音频数据并产生声音的设备，它可以提供高质量的音频输出，并支持音频输入功能。

- 例子：Creative Sound Blaster AE-9、ASUS Xonar Essence STX II等声卡。

- 视频采集卡：

- 概念：视频采集卡是用于将外部视频信号输入计算机，以便处理、编辑和录制视频内容的设备。

- 例子：Elgato Game Capture HD60 Pro、Blackmagic Design Intensity Pro 4K等视频采集卡。

3. 多媒体设备

- 概念：多媒体设备是用于录制、播放、处理和展示多媒体内容的外部设备。

- 例子：

- 数码相机：用于拍摄照片和视频的设备，例如尼康D850、佳能EOS 5D Mark IV等。

- 摄像机：用于录制高质量视频的设备，例如索尼FS7、佳能XC15等。

- 麦克风：用于录制声音的设备，例如蓝雪球麦克风、森海塞尔EW 112P G4无线麦克风等。

- 扬声器和音箱：用于放大和播放音频内容的设备，例如BOSE Companion 2 Series III、JBL Charge 4等。

- MIDI键盘：用于音乐创作和演奏的设备，例如M-Audio Oxygen 49、Novation Launchkey MK3等。

### 4.2.2多媒体计算机软件系统

1. 多媒体系统软件

- 概念：多媒体系统软件是为多媒体技术提供支持和管理的软件集合，用于控制和调度多媒体内容的创建、处理、存储和传输等功能。

- 例子：

- 操作系统：如Windows、macOS和Linux等操作系统，提供了多媒体设备的驱动程序和基本功能，以及管理和调度系统资源的能力。

- 多媒体框架：如DirectX和OpenGL等多媒体框架，提供了处理图形、音频和视频等多媒体数据的接口和函数库。

- 流媒体服务器：如Adobe Media Server、Wowza Streaming Engine等服务器软件，用于流媒体传输和分发多媒体内容。

2. 多媒体编辑软件

- 概念：多媒体编辑软件用于对多媒体内容进行编辑、处理和合成，使之符合需求并提供更好的视听体验。

- 例子：

- 视频编辑软件：如Adobe Premiere Pro、Final Cut Pro等，用于处理、剪辑和合成视频内容。

- 音频编辑软件：如Ableton Live、Pro Tools等，用于录制、编辑和处理音频内容。

- 图像编辑软件：如Adobe Photoshop、GIMP等，用于处理和编辑图像内容。

- 3D建模软件：如Autodesk Maya、Blender等，用于创建和编辑三维模型和动画。

3. 多媒体创作软件

- 概念：多媒体创作软件是用于创作和设计多媒体内容的工具，通过与用户的交互，提供丰富的创作功能和效果。

- 例子：

- 图形设计软件：如Adobe Illustrator、CorelDRAW等，用于创作和编辑图形和矢量图。

- 动画制作软件：如Adobe Animate、Toon Boom Harmony等，用于制作二维和三维动画。

- 交互式媒体创作软件：如Adobe Flash、Unity等，用于开发交互式媒体应用和游戏。

- 图像处理软件：如Adobe Photoshop、Affinity Photo等，用于对图像进行处理和加工。

4. 多媒体应用软件

- 概念：多媒体应用软件是用于呈现和交互多媒体内容的应用程序，提供丰富的媒体体验和功能。

- 例子：

- 视频播放器：如VLC媒体播放器、Windows媒体中心等，用于播放各种视频格式的文件。

- 音乐播放器：如Winamp、iTunes等，用于播放音频文件和管理音乐库。

- 图片浏览器：如Windows照片查看器、IrfanView等，用于显示、浏览和管理图像文件。

- 3D游戏引擎：如Unity、Unreal Engine等，用于开发和呈现基于三维图形的游戏和应用程序。

## 4.3多媒体处理技术

### 4.3.1图像处理

1. 图形和图像的基本概念及技术指标

- 图形：

- 概念：图形是由点、线、曲线等基本几何元素构成的二维图形，通过点的连接和填充形成具有特定意义的可视化信息。

- 图像：

- 概念：图像是对视觉信息的数字表示，它由一系列像素点构成，每个像素点包含图像中一个位置的颜色和亮度信息。

- 分辨率：

- 概念：分辨率是图像中像素点的密度和细腻程度，通常以水平像素数和垂直像素数表示，如800x600或1920x1080。

- 影响：较高的分辨率可以提供更多的细节和清晰度，而较低的分辨率可能导致图像粗糙或失真。

- 色彩：

- 概念：色彩是图像中呈现的颜色信息，由红、绿、蓝三个基本颜色通道的亮度组合而成。

- 表示：通常使用颜色表示模型，如RGB模型（红、绿、蓝）或CMYK模型（青、洋红、黄、黑）。

- 灰度：

- 概念：灰度是图像中的亮度值，表示像素的黑白程度，通常介于0（黑色）和255（白色）之间。

- 表示：灰度图像由单一的亮度通道组成，适用于只需表达图像亮度信息而不需要彩色的情况。

2. 图像数字化：

- 概念：图像数字化是将连续的图像数据转换为离散的数字表示的过程。它涉及采样、量化和编码等步骤。

- 特点：数字图像由像素组成，每个像素包含颜色信息。图像数字化可以以不同的分辨率进行，即像素的数量和图像的细节级别。

- 图像大小的计算例子：假设一张图像的分辨率为1920×1080（宽度×高度），颜色深度为24位（每个像素用24位来表示颜色，即8位红色、8位绿色和8位蓝色），则图像大小的计算公式为：图像大小（字节） = 宽度（像素） × 高度（像素） × 颜色深度（位） / 8

- 例如，一张1920×1080分辨率、颜色深度为24位的图像大小计算为：1920 × 1080 × 24 / 8 = 6,220,800字节 = 6.22 MB。

3. 图像压缩标准

- 静止图像压缩标准：

- 概念：静止图像压缩标准用于将静止的图像文件压缩为更小的文件大小，同时保持图像质量。

- 示例：

- JPEG（Joint Photographic Experts Group）：广泛使用的有损压缩格式，适用于照片和复杂图像。

- JPEG-2000：基于波尔多瓦波小波变换的新一代图像压缩标准，提供更好的图像质量和高压缩效率。

- 动态图像压缩标准：

- 概念：动态图像压缩标准用于将动态的图像或视频文件压缩为更小的文件大小，同时保持动画和视频质量。

- 示例：

- MPEG-1：适用于低比特率视频和CD视频的有损压缩标准。

- MPEG-2：适用于广播电视、DVD和数字电视的有损压缩标准。

- MPEG-4：适用于流媒体、互联网视频和移动视频的有损压缩标准。

- MPEG-7：用于描述和检索多媒体内容的标准，提供了图像和视频检索的丰富功能。

4. 图像的文件格式

- 概念：图像的文件格式是指保存和存储图像数据的特定文件类型，它规定了图像数据的组织方式、压缩方式和元数据等信息。

- 示例：

- JPEG（.jpg、.jpeg）：用于存储照片和复杂图像的有损压缩格式。

- PNG（.png）：用于存储图标、线条图形和透明图像的无损压缩格式。

- GIF（.gif）：用于存储简单动画和图标的无损压缩格式。

- TIFF（.tiff、.tif）：适用于存储高质量图像的无损压缩或无压缩格式。

5. 图像处理软件

- 概念：图像处理软件是用于编辑、处理和转换图像的计算机程序，它提供了丰富的图像处理功能和工具。

- 示例：

- Adobe Photoshop：功能强大的图像编辑和处理软件，广泛用于图像修复、合成和特效处理等。

- GIMP（GNU Image Manipulation Program）：免费开源的图像编辑和处理软件，类似于Photoshop的许多功能。

- Adobe Lightroom：专业的图像处理和调整软件，用于数字摄影后期处理和效果优化。

### 4.3.2音频处理

1. 声音的基本概念

- 振幅：

- 概念：振幅指声音信号的幅度或振动大小，表示声音的音量或强度。

- 例子：较大的振幅表示较大的音量，而较小的振幅表示较小的音量。

- 周期：

- 概念：周期是声音信号中一次完整振动所需的时间，表示声音信号的频率。

- 例子：例如，440赫兹（Hz）的周期是1/440秒，因此声音每0.00227秒重复一次振动。

- 频率：

- 概念：频率是声音信号中振动的次数，用赫兹（Hz）表示，表示声音的音调。

- 例子：440赫兹的音调为A4，这是钢琴键盘上的标准调音。

2. 数字化音频

- 采样：

- 概念：采样是将连续的模拟音频信号转换为离散的数字音频信号的过程，通过在特定时间间隔内测量声音信号的幅度来实现。

- 例子：采样率为44100赫兹的声音信号意味着每秒进行44100次采样。

- 量化：

- 概念：量化是将采样得到的连续幅度值转换为离散的数字幅度值的过程，表示数字音频的精度。

- 例子：16位量化表示音频幅度的范围分为65,536个离散级别。

- 编码：

- 概念：编码是使用特定的算法将量化后的数字幅度值转换为存储或传输所需的二进制数据的过程。

- 例子：常见的音频编码格式包括MP3（MPEG Audio Layer-3）和AAC（Advanced Audio Coding）。

3. 声音数据传输率计算

- 概念：声音数据传输率是指在一定时间内传送或传输的音频数据量，通常以每秒的比特数（bps）表示。

- 例子：

- 对于16位深度、2声道（立体声）和采样率为44100赫兹的CD质量音频，计算公式为：

数据传输率 = 采样率 × 位深度 × 声道数

= 44100 × 16 × 2

= 1411200 bps

因此，在这种情况下，每秒传输的音频数据量为1411200比特。

4. 声音数据量计算

- 概念：声音数据量是指存储或传输所需的音频数据总量，通常以字节（Byte）或千字节（KB）表示。

- 例子：

- 对于5分钟的CD质量音频，采样率为44100赫兹，16位深度和2声道（立体声）：

数据传输率 = 采样率 × 位深度 × 声道数

= 44100 × 16 × 2

= 1411200 bps

音频数据量 = 数据传输率 × 时间

= 1411200 bps × 300秒

= 423360000比特

= 52.92 MB

因此，在这种情况下，音频数据量为52.92兆字节（MB）。

5. 音频文件格式

- 概念：音频文件格式是指用于存储音频数据的特定文件类型，它规定了音频数据的组织方式、压缩方式和元数据等信息。

- 示例：

- WAV（.wav）：无压缩的音频文件格式，支持多种采样率、位深度和声道数。

- MP3（.mp3）：有损压缩的音频文件格式，具有较小的文件大小和广泛的兼容性。

- FLAC（.flac）：无损压缩的音频文件格式，保留原始音频质量。

- AAC（.aac）：有损压缩的音频文件格式，常用于网络流媒体和移动设备。

音频处理软件

- 概念：音频处理软件是用于编辑、处理和转换音频的计算机程序，提供各种功能和工具，以满足不同的音频处理需求。

- 示例：

- Adobe Audition：功能强大的专业音频编辑和处理软件，支持多轨音频编辑、降噪和音频修复等。

- Audacity：免费开源的音频编辑和处理软件，具有基本的音频编辑和效果处理功能。

- Avid Pro Tools：专业的音频编辑和音乐制作软件，广泛用于录音室和音频后期制作。

- Steinberg Cubase：音乐制作和录音工作站软件，提供丰富的音频处理和音乐创作功能。

### 4.3.3视频处理

1. 视频的概念及特点

- 视频：

- 概念：视频是指由连续的图像帧以一定的帧率播放而成的影像流，通过时间轴展示连续的图像，形成动态效果。

- 特点：视频是以时间为基础的媒体形式，可以同时包含图像、音频和其他多媒体元素。

2. 视频数字化：

- 概念：视频数字化是将连续的视频信号转换为数字格式的过程。它涉及采样、量化、编码和压缩等步骤。

- 特点：视频是由一系列连续帧组成的，每帧都是一个静止图像。帧率表示每秒显示的帧数，通常以帧/秒（fps）为单位。

- 视频大小的计算例子：假设一个视频的分辨率为1280×720，帧率为30fps，颜色深度为24位，则视频大小的计算公式为：视频大小（字节） = 宽度（像素） × 高度（像素） × 颜色深度（位） / 8 × 帧率（fps）

- 例如，一个1280×720分辨率、帧率为30fps、颜色深度为24位的视频大小计算为：1280 × 720 × 24 / 8 × 30 = 66,048,000字节 = 66.05 MB。

3. 视频的分类

- 按产生方式分类：

- 实时视频：即时传输的视频流，如视频会议和直播。

- 非实时视频：预先录制并存储的视频，如电影和电视节目。

- 按编码方式分类：

- 有损压缩视频：通过牺牲一定的图像质量来减小文件大小，常见的有损压缩格式包括MPEG-2（DVD）、MPEG-4（H.264）和AVC（Advanced Video Coding）等。

- 无损压缩视频：保持图像质量的同时减小文件大小，常见的无损压缩格式包括Apple ProRes和Avid DNxHD。

- 按分辨率分类：

- 标清视频：分辨率为720x480或720x576，适用于老式电视和低分辨率显示设备。

- 高清视频：常见的高清分辨率包括1280x720和1920x1080，提供更好的图像清晰度。

- 4K视频：分辨率为3840x2160或4096x2160，提供更高的图像细节和清晰度。

4. 数字视频与模拟视频

- 数字视频：

- 概念：数字视频是以数字形式表示的视频信号，通过将连续的模拟视频信号进行采样、量化和编码转换而成。

- 优点：数字视频具有较高的质量和稳定性，可以进行精确的编辑和处理，易于存储和传输。

- 模拟视频：

- 概念：模拟视频是以连续的模拟信号形式表示的视频信号，采用模拟电压的变化来表示图像和色彩信息。

- 特点：模拟视频使用模拟信号传输，对干扰敏感，质量受到信号品质和传输距离的限制。

5. 视频的文件格式

- 概念：视频的文件格式是指用于存储视频数据的特定文件类型，它规定了视频数据的组织方式、压缩方式和元数据等信息。

- 示例：

- AVI（Audio Video Interleave）：由微软开发的多媒体容器格式，支持多种视频编码和音频编码。

- MP4（MPEG-4 Part 14）：广泛使用的多媒体容器格式，支持流行的视频编码和音频编码，如H.264和AAC。

- MOV（QuickTime）：由苹果开发的多媒体容器格式，广泛支持各种视频和音频编码。

- MKV（Matroska）：开源的多媒体容器格式，支持多种视频和音频编码。

6. 视频处理软件

- 概念：视频处理软件是用于编辑、转码和处理视频的计算机程序，提供各种功能和工具，以满足不同的视频处理需求。

- 示例：

- Adobe Premiere Pro：功能强大的专业视频编辑软件，支持多轨视频编辑、特效和调色等。

- Final Cut Pro：苹果公司的专业视频编辑软件，提供高级剪辑工具和专业特效。

- DaVinci Resolve：全功能的视频后期制作软件，具有强大的调色和视觉效果处理能力。

- HandBrake：开源的视频转码软件，支持多种输入和输出格式的转换。

- FFmpeg：强大的多媒体处理工具集，可用于视频转码、格式转换和处理等。

## 4.4平面设计基础知识

### 4.4.1平面设计概述

1. 平面设计的基础概念

- 概念：平面设计是以视觉表达为基础的艺术和设计领域，通过使用图像、文字和其他元素来传达特定的信息或达到特定的目标。

- 目的：创造有吸引力、有影响力的视觉作品，用于广告、品牌推广、产品设计、插图等领域。

2. 基本要素

- 创意：

- 概念：创意是指从独特的视觉角度和创造性的思维中产生的新颖、有趣的想法和设计概念。

- 重要性：创意是平面设计的核心，能够吸引目标受众并传达清晰的信息。

- 构图：

- 概念：构图是指在设计中组织和安排图像、文本和其他元素的过程，以创建视觉上的平衡、重点和流动性。

- 原则：常用的构图原则包括对称、平衡、比例、重复、对比和节奏等。

- 色彩：

- 概念：色彩是平面设计中用于创造氛围、表达情感和引起注意的重要元素。

- 色彩理论：色彩理论包括色轮、色彩对比和色彩心理学等，了解色彩搭配、互补和调和有助于创造有效的设计。

### 4.4.2位图处理软件 Adobe Photoshop

1. 基本概念

- 像素：

- 概念：像素是表示图像最小单元的图像元素，具有特定的颜色和位置信息。

- 例子：对于一幅800x600像素的图像，总共有480,000个像素，每个像素都存储了其颜色和位置信息。

- 图像分辨率：

- 概念：图像分辨率是指图像中每英寸（或每厘米）包含的像素数量，表示图像的清晰度。

- 例子：常见的图像分辨率包括300dpi（印刷质量）、72dpi（屏幕质量）等。

- 位图：

- 概念：位图是由像素网格组成的图像，每个像素都包含颜色信息。

- 例子：JPEG、PNG和BMP等常见的图像文件格式都是位图格式。

- 矢量图：

- 概念：矢量图使用数学公式来表示图像，以线、曲线和形状等为基础，可以无损放大和缩小而不失真。

- 例子：SVG（可缩放矢量图形）是常见的矢量图格式。

- 设备分辨率：

- 概念：设备分辨率是指显示器、打印机或其他输出设备上能够显示的像素密度。

- 例子：常见的设备分辨率包括屏幕分辨率（如1920x1080）和打印机分辨率（如300dpi）等。

- 位分辨率：

- 概念：位分辨率是指图像中每个像素使用的位数，决定了图像的颜色深度和颜色范围。

- 例子：常见的位分辨率包括8位（256色）、24位（真彩色）和32位（带透明通道）等。

- 颜色模式：

- RGB模式：基于红、绿、蓝三原色混合来创建图像，适用于屏幕显示。

- CMYK模式：基于青、洋红、黄、黑四色油墨混合来创建图像，适用于打印。

- LAB模式：基于亮度（L）和颜色（A和B）通道来创建图像，用于精确的色彩调整。

- HSB模式：基于色调、饱和度和亮度三个通道来创建图像，用于色彩调整和特殊效果。

- 位图模式：每个像素只有两种颜色（黑和白），用于单色图像和图标等。

- 灰度模式：每个像素只有一种灰度值，用于黑白图像和灰度图。

- 多通道模式：使用多个独立的颜色通道来创建图像，可用于分离处理和专色打印。

- 索引颜色模式：使用有限的颜色表来表示图像，适用于网络图像和小尺寸图标。

2. Adobe Photoshop文件格式

- PSD（Photoshop Document）：Adobe Photoshop的原生文件格式，支持图层、滤镜和其他高级特性。

- JPEG（Joint Photographic Experts Group）：一种有损压缩的位图格式，用于在图像质量和文件大小之间进行平衡。

- PNG（Portable Network Graphics）：一种无损压缩的位图格式，支持透明通道和更高的图像质量。

- GIF（Graphics Interchange Format）：一种支持动画和索引颜色的位图格式，常用于简单的图形和动画。

- TIFF（Tagged Image File Format）：一种支持无损压缩和多通道图像的位图格式，适用于专业的印刷和图形设计。

# **第五章**

第五章

5.1操作系统概述

5.1.1操作系统的功能

5.1.2操作系统的基本特征

5.1.3操作系统的分类

5.1.4常用计算机操作系统

5.1.5常用手机操作系统

5.2文件及文件夹

## 5.1操作系统概述

### 5.1.1操作系统的功能

操作系统是计算机系统中的核心软件，负责管理和协调系统资源，提供用户与计算机硬件之间的接口。操作系统具有以下主要功能：

1. 作业管理

- 概念：作业管理涉及对在计算机系统中同时运行的多个作业（任务）进行有效的调度、控制和协调。

- 功能：

- 进程调度：决定哪个进程在某个时间段内占用处理器资源。

- 进程同步：管理并发进程之间的协调和互斥访问共享资源。

- 进程通信：实现进程之间的信息交流和数据传输。

- 资源分配：分配内存、处理器时间和其他计算机资源给作业。

2. 文件管理

- 概念：文件管理涉及对计算机系统中的文件和目录进行组织、存储和访问的管理。

- 功能：

- 文件存储：将文件存储在磁盘或其他存储介质上，并维护文件的物理位置和关联信息。

- 文件访问：通过文件系统提供对文件的读取、写入和删除等操作。

- 文件共享：支持多个用户或进程共享访问同一文件。

- 文件保护：控制文件的权限和访问方式，以确保文件的安全性和完整性。

3. 存储管理

- 概念：存储管理涉及对计算机系统中的主存储器和辅助存储器（如硬盘）进行管理和分配。

- 功能：

- 内存分配：分配和回收主存储器中的物理空间给进程。

- 虚拟内存：通过将部分进程数据存储在磁盘上来扩展可用的内存空间。

- 页面置换：根据需要将主存储器中的页面从磁盘中调入或调出。

- 内存保护：保护进程之间的内存空间，防止相互干扰和破坏。

4. 设备管理

- 概念：设备管理涉及对计算机系统中的输入/输出设备进行控制、分配和协调。

- 功能：

- 设备驱动程序：提供与不同设备通信的软件接口。

- 设备分配：对设备进行分配和调度，以满足进程的输入/输出需求。

- 设备独占：控制设备的独占性，避免多个进程同时访问同一设备。

- 设备错误处理：检测和处理设备出现的错误和异常情况。

5. 处理器管理

- 概念：处理器管理涉及对计算机系统中的处理器资源进行分配、调度和协调。

- 功能：

- 进程调度：决定哪个进程在某个时间段内占用处理器资源。

- 进程同步：管理并发进程之间的协调和互斥访问共享资源。

- 进程通信：实现进程之间的信息交流和数据传输。

- 线程管理：管理线程的创建、销毁和切换。

### 5.1.2操作系统的基本特征

1. 并发性

- 概念：并发性指的是在同一时间内存在多个独立的活动（进程或线程），这些活动可以在重叠的时间段内执行。

- 例子：

- 多任务操作系统：在同一时间内同时运行多个进程或线程，如Windows和Linux操作系统。

- 并行计算：使用多个处理器或处理器核心同时执行多个任务，如分布式计算集群或超级计算机。

2. 共享性

- 概念：共享性指的是多个用户或进程之间共享计算机系统的资源，如文件、内存和设备等。

- 例子：

- 文件共享：多个用户可以同时访问和编辑同一文件，如云存储服务和局域网。

- 内存共享：多个进程可以共享同一块内存空间，以实现数据共享和通信。

3. 虚拟性

- 概念：虚拟性指的是通过使用虚拟化技术，将物理资源抽象为更高级别的逻辑实体来提供更高的灵活性和效率。

- 例子：

- 虚拟内存：将磁盘空间扩展为主存的虚拟空间，以便能够处理比物理内存更大的数据量。

- 虚拟机：在一台物理计算机上创建多个虚拟计算机，每个虚拟计算机都具有独立的操作系统和应用程序。

4. 异步性

- 概念：异步性指的是多个进程或线程以独立的速度和顺序执行，不需要依赖时钟或其他同步机制。

- 例子：

- 事件驱动编程：程序在等待外部事件发生时继续执行，如用户操作、网络请求和硬件事件。

- 异步编程：在处理I/O操作或长时间运行的任务时，允许其他任务继续执行，而不需要等待结果。

### 5.1.3操作系统的分类

操作系统是计算机系统中的核心软件，根据其功能和应用领域的不同，可以进行如下分类：

1. 多用户多任务操作系统

- 概念：多用户多任务操作系统可以同时支持多个用户，并且能够在同一时间内并发执行多个任务。

- 例子：

- Linux：一个开源的多用户多任务操作系统，广泛应用于服务器和个人计算机。

- UNIX：一个多用户多任务操作系统，用于大型或多用户环境，如服务器和超级计算机。

2. 分时操作系统

- 概念：分时操作系统按时间片轮转的方式，将处理器时间分配给多个用户或任务。

- 例子：

- Windows：一个具有分时操作系统特性的个人计算机操作系统，支持多任务和多用户。

- UNIX（包括Linux）：多用户分时操作系统的典型例子。

3. 实时操作系统

- 概念：实时操作系统在特定时间范围内对任务的响应时间有严格要求，可以分为硬实时和软实时两种类型。

- 例子：

- 嵌入式实时操作系统（RTOS）：针对嵌入式系统设计的实时操作系统，如VxWorks和FreeRTOS。

- 实时操作系统（RTOS）：用于对时间敏感应用，如飞行控制系统和工业自动化系统。

4. 网络操作系统

- 概念：网络操作系统是专为网络环境设计的操作系统，在分布式网络中提供资源共享和协作的功能。

- 例子：

- Windows Server：一种针对服务器环境的网络操作系统，用于提供网络服务和资源共享。

- Linux服务器发行版：如Ubuntu Server、Red Hat Enterprise Linux等，支持网络操作系统功能。

5. 分布式操作系统

- 概念：分布式操作系统是用于管理由多个独立计算机组成的分布式系统的操作系统。

- 例子：

- Google的分布式操作系统：Google File System（GFS）和MapReduce实现了大规模数据处理的分布式计算模型。

- Apache Hadoop：一个开源的分布式计算系统，基于Hadoop分布式文件系统（HDFS）实现。

6. 嵌入式操作系统

- 概念：嵌入式操作系统是为嵌入式设备设计的轻量级操作系统，具有实时性和小尺寸的特点。

- 例子：

- Android：一种基于Linux内核的开源嵌入式操作系统，广泛用于智能手机、平板电脑和其他嵌入式设备。

- Windows Embedded：微软提供的适用于嵌入式系统的操作系统，如Windows Embedded Compact和Windows IoT。

7. 桌面操作系统

- 概念：桌面操作系统是安装在个人计算机上的操作系统，提供用户与计算机硬件和软件的交互界面。

- 例子：

- Windows：微软公司开发的桌面操作系统，如Windows 11、Windows 10等。

- macOS：苹果公司开发的桌面操作系统，用于苹果Mac电脑。

8. 服务器操作系统

- 概念：服务器操作系统是用于管理服务器和提供网络服务的操作系统。

- 例子：

- Windows Server：微软公司开发的服务器操作系统，用于搭建和管理服务器环境。

- Linux服务器发行版：如Ubuntu Server、Red Hat Enterprise Linux等，广泛用于服务器环境。

### 5.1.4常用计算机操作系统

计算机操作系统是计算机系统中的核心软件，具有多个常用版本和相应的特点，如下所述：

1. Windows操作系统

- 版本：

- Windows 11：最新版本的Windows操作系统，提供全新的用户界面和改进的性能。

- Windows 10：一种广泛应用的Windows操作系统，具有稳定性和广泛的软件支持。

- Windows 7：一种广泛使用的Windows操作系统，以稳定性和易用性著称。

- 特点：

- 用户友好：Windows操作系统提供直观的用户界面和易于操作的功能。

- 软件兼容性：Windows操作系统支持广泛的第三方软件和应用程序。

- 多任务处理：支持多任务处理和多用户环境。

- 强大的硬件兼容性：适用于各种计算机硬件设备。

2. Linux操作系统

- 版本：

- Ubuntu：最受欢迎的Linux发行版之一，注重易用性和用户友好性。

- CentOS：以稳定性和安全性著称的企业级Linux发行版。

- Debian：一种通用的Linux发行版，重点在稳定性和开源社区合作。

- 特点：

- 开源：基于开源软件，可以自由获取和修改。

- 稳定性和安全性：对系统稳定性和安全性有强调。

- 自定义和灵活性：允许用户自定义操作系统的配置和外观。

- 服务器和嵌入式设备支持：广泛应用于服务器和嵌入式设备领域。

3. UNIX操作系统

- 版本：

- Solaris：由Oracle公司开发的UNIX操作系统版本，用于商业环境。

- FreeBSD：一种开源的UNIX操作系统版本，注重性能和安全性。

- AIX：由IBM公司开发的UNIX操作系统版本，用于IBM硬件平台。

- 特点：

- 多用户和多任务：支持多用户和多任务环境。

- 稳定性和可靠性：具有良好的系统稳定性和可靠性。

- 强大的网络能力：提供强大的网络支持和协议堆栈。

4. macOS操作系统

- 版本：

- macOS Monterey：最新版本的macOS操作系统，为苹果设备提供全新的功能和改进。

- macOS Catalina：面向苹果设备的macOS操作系统，具有增强的隐私和安全功能。

- macOS High Sierra：一种稳定性较高的macOS操作系统版本。

- 特点：

- 设计精美：提供优雅和直观的用户界面设计。

- 性能稳定：具有稳定性和可靠性，适用于苹果硬件设备。

- 创意工具：内置了各种创意工具和专业级应用程序。

- 紧密集成：与其他苹果设备和生态系统的紧密集成。

5. DOS操作系统

- 版本：

- MS-DOS：微软公司开发的第一代DOS操作系统，用于早期个人计算机。

- PC-DOS：由IBM公司授权并修改的DOS操作系统版本。

- 特点：

- 单用户和单任务：仅支持单用户和单任务操作环境。

- 命令行界面：以命令行界面为主要交互方式。

- 适用于早期个人计算机：主要用于早期个人计算机系统。

### 5.1.5常用手机操作系统

手机操作系统是移动设备中的核心软件，具有多个常用版本和相应的特点，如下所述：

1. Android操作系统

- 版本：

- Android 12：最新版本的Android操作系统，提供了更流畅的用户体验和增强的隐私保护。

- Android 11：一种广泛使用的Android操作系统，引入了更多的隐私和安全功能。

- Android 10：稳定性高、性能优化的Android操作系统版本。

- 特点：

- 开放性：基于开源Linux内核，提供广泛的自定义和开发能力。

- 多样化：支持不同品牌和型号的手机设备。

- 大量应用程序：具有丰富的应用程序生态系统，支持多种应用程序的下载和安装。

- Google服务集成：预装了Google服务和应用程序。

2. iOS操作系统

- 版本：

- iOS 15：最新版本的iOS操作系统，带来了全新的功能和改进，如Widgets、App库等。

- iOS 14：一种稳定且成熟的iOS操作系统版本，引入了小组件和应用程序库功能。

- iOS 13：具有更好性能和更多功能的iOS操作系统版本。

- 特点：

- 封闭性：iOS操作系统具有严格的安全性和应用程序审核机制。

- 用户体验：提供流畅的用户界面和直观的操作方式。

- 硬件和软件的紧密结合：与苹果设备和生态系统的紧密结合，提供无缝的使用体验。

- 高质量应用程序：App Store提供高质量的应用程序和游戏。

3. MIUI操作系统

- 版本：

- MIUI 12：最新版本的MIUI操作系统，提供了全新的设计语言和增强的功能。

- MIUI 11：一种稳定和功能丰富的MIUI操作系统版本。

- 特点：

- 平滑的用户界面：提供流畅且可自定义的用户界面。

- 多功能体验：具有丰富的功能和个性化选项。

- 小米生态系统整合：紧密集成小米设备和生态系统的各种功能和服务。

4. 鸿蒙操作系统

- 版本：

- HarmonyOS 2：最新版本的鸿蒙操作系统，适用于各种设备，包括手机、平板电脑等。

- 特点：

- 分布式架构：提供分布式应用能力，让多个设备无缝协同工作。

- 统一开发平台：开发者可以使用统一的开发工具和框架进行应用程序开发。

- 高性能：具有出色的性能和资源管理能力。

5. Flyme操作系统

- 版本：

- Flyme 9：最新版本的Flyme操作系统，提供了全新的设计和功能。

- 特点：

- 简洁的用户界面：提供简洁、直观且个性化的用户界面。

- 高效的性能：具有良好的性能优化和电池管理能力。

- 内置特色功能：提供多种特色功能，如One Mind智能引擎和One Mind音频。

6. One UI操作系统

- 版本：

- One UI 3：最新版本的One UI操作系统，提供更好的用户体验和可访问性。

- One UI 2：一种稳定且具有现代化设计语言的One UI操作系统版本。

- One UI 1：首个One UI操作系统版本。

- 特点：

- 用户友好性：提供直观和易用的用户界面，注重单手操作。

- 分屏和多任务处理：支持分屏和多任务处理功能。

- 具有个性化选项：提供丰富的个性化选项，如夜间模式和主题选项。

7. ColorOS操作系统

- 版本：

- ColorOS 11：最新版本的ColorOS操作系统，提供了更优化的用户体验和创意功能。

- ColorOS 7：一种稳定性高且功能丰富的ColorOS操作系统版本。

- 特点：

- 光滑的用户界面：提供流畅、自然的用户界面。

- 出色的摄影功能：集成了丰富的摄影功能和特效。

- 智能助手和优化：提供智能化的助手和系统优化功能。

8. OriginOS操作系统

- 版本：

- OriginOS：一款创新性的操作系统，注重个性化和性能优化。

- 特点：

- 独特的桌面布局：提供全新的桌面布局和个性化的使用体验。

- 优化的性能：具有出色的性能和响应速度。

- 灵活的主题和壁纸：提供丰富的主题和壁纸选项。

## 5.2文件及文件夹

文件和文件夹是计算机中用于组织和存储数据的基本单位。它们在操作系统中起着重要的作用，如下所述：

1. 文件

- 定义：文件是存储在计算机上的命名数据的集合。它可以包含文本、图像、音频、视频和其他形式的数据。

- 特点：

- 文件类型：文件可以是各种类型，如文本文件（.txt）、图像文件（.jpg、.png）、音频文件（.mp3）等。

常用文件类型表：

| 扩展名 | 类别 | 介绍 |
| --- | --- | --- |
| .jpg或.jpeg | 位图图像 | 有损压缩图像，存储空间小，静态图像专家组推出 |
| .bmp | 位图图像 | windows标准图像，没有压缩，存储空间较大 |
| .gif | 位图图像 | 无损压缩，可存储多张图片，组成简单动画 |
| .png | 位图图像 | 无损压缩，常用于网络或程序 |
| .tif | 位图图像 | 无损压缩，专业领域，打印机常用 |
| .psd | Adobe专用 | Adobe专用位图文件 |
| .ai | Adobe专用 | Adobe专用矢量图文件 |
| .cdr | Adobe专用 | Adobe专用矢量图文件 |
| .au | Adobe专用 | Adobe专用声音文件 |
| .wav | 声音 | windows标准声音,存储空间大 |
| .mp3 | 声音 | 有损压缩，存储空间小 |
| .wma | 声音 | 有损或无损压缩，微软推出 |
| .mid | 声音 | midi音乐格式，记录声音的信息，电子音乐常用 |
| .avi | 视频 | 有损压缩，微软推出，常用于光盘 |
| .mpg或mp4 | 视频 | 有损压缩，存储空间较小，动态图像专家组推出 |
| .mov | 视频 | 无损压缩，Apple公司推出 |
| .wmv | 视频 | 有损压缩，微软推出 |
| .docx | 文档 | 前身为**.doc**，WPS或Microsoft office打开 |
| .xlsx | 文档 | 前身为**.xls**，WPS或Microsoft office打开 |
| .pptx | 文档 | 前身为**.ppt**，WPS或Microsoft office打开 |
| .pdf | 文档 | 常用于已经编辑完成的word,ppt文件，打印时页面元素不变 |
| .txt | 文本 | 微软推出，windows附带 |
| .rtf | 文本 | 微软推出，跨平台 |
| .exe | 程序 | windows系统可执行程序 |
| .bak | 程序 | 备份格式，编程，设计软件常用 |
| .cmd或.bat | 程序 | windows的dos命令脚本，每一行就是一条指令，可直接执行 |
| .ico | 程序 | 程序图标文件格式 |
| .cs | 程序 | C#源文件 |
| .cpp | 程序 | C++源文件 |
| .c | 程序 | C源文件 |
| .h | 程序 | C，C++头文件 |
| .py | 程序 | Python源文件 |
| .java | 程序 | java源文件 |
| .vbs | 程序 | VBS源文件，可直接运行 |
| .vb | 程序 | VB源文件 |
| .md | 程序 | markdown源文件 |
| .dll | 程序 | 动态库文件，包含程序所要用到的数据，函数 |
| .lib | 程序 | 静态库文件，包含程序所要用到的数据，函数 |
| .dgml | 程序 | 微软推出，定向图形标记语言DGML源文件 |
| .iso | 压缩 | 光盘常用 |
| .zip | 压缩 | 常用压缩格式，私人开发，跨平台 |
| .rar | 压缩 | 常用压缩格式，私人开发 |
| .7z | 压缩 | 开源压缩格式，压缩比大，支持最大16EB文件压缩 |
| .swf | 动画 | flash软件设计的动画文件，用flash播放器打开，可用于制作游戏 |
| .html或.htm | 网页 | 超文本标记语言，定义了网页的内容与结构 |
| .css | 网页 | 层叠样式表，定义了网页的样式，布局 |
| .js | 网页 | js源文件，常用于网页的脚本语言 |
| .xml | 网页 | XML源文件，web应用程序中常用来传输数据 |
| .epaper | 题库 | 常用题库文件格式 |
| .sql | 数据库 | SQL脚本文件 |
| .accdb | 数据库 | access数据库格式 |

- 文件大小：文件的大小可以根据其中存储的数据量来变化。

- 文件属性：文件具有一些属性，如文件名称、创建日期、修改日期、文件类型和文件权限等。

- 文件格式：文件可以采用不同的格式，如可执行文件、压缩文件、数据文件等。

- 操作：

- 创建文件：可以通过应用程序创建新文件，或从其他位置复制文件到计算机中。

- 打开文件：可以使用适当的应用程序打开文件来访问其中的数据。

- 编辑文件：可以使用适当的应用程序对文件进行编辑操作，如添加、删除、修改内容。

- 保存文件：对编辑后的文件进行保存，以便将更改持久化在存储介质中。

- 关闭文件：在文件使用完毕后，应该关闭文件以释放系统资源。

2. 文件夹（目录）

- 定义：文件夹是用于组织和存储文件的容器。它可以包含文件和其他文件夹，形成层次结构。

- 特点：

- 文件夹名称：每个文件夹都有一个唯一的名称，用于标识和访问文件夹。

- 文件夹层次结构：文件夹可以根据需要进行层次化组织，以便更好地管理文件。

- 文件夹路径：文件夹路径是指文件夹在文件系统中的位置，可以根据路径来访问文件夹。

- 操作：

- 创建文件夹：可以通过文件管理器或命令行界面创建新文件夹。

- 打开文件夹：可以通过文件管理器来打开文件夹，以便访问其中的文件。

- 复制或移动文件夹：可以将文件夹复制到其他位置，或将文件夹移动到不同的目录中。

- 重命名文件夹：可以对文件夹进行重命名操作，以改变其名称。

- 删除文件夹：可以删除不再需要的文件夹，但需要注意其中的文件会一同删除。

# 第六章

第六章

6.1通信的基础概念

6.1.1数据通信三要素

6.1.2通信信号

6.1.3数据传输方式

6.1.4数据交换方式

6.1.5差错控制技术

6.1.6数据通信的主要技术参数

6.2计算机网络概述

6.2.1计算机网络的产生与发展

6.2.2计算机网络的概念与功能

6.2.3计算机网络的分类

6.2.4网络通信的三种模式

6.3计算机网络系统结构

6.3.1计算机网络系统组成

6.3.2计算机网络逻辑结构

6.3.3计算机网络拓扑结构

6.3.4常用网络命令

6.3.5网络协议

6.3.6开放网络互连参考模型（OSI - RM）

6.4TCP/IP体系结构

6.4.1TCP/IP参考模型

6.4.2IP地址

6.4.3端口

6.5计算机网络设备

6.5.1网络互连

6.5.2网络传输介质

6.5.3网卡

6.5.4中继转发设备

6.5.5网桥

6.5.6网络交换设备

6.5.7调制解调器

6.6局域网与广域网技术

6.6.1局域网技术

6.6.2典型局域网类型

6.6.3广域网技术

6.7Internet

6.7.1Internet的起源与发展

6.7.2域名系统DNS

6.7.3信息浏览服务（WWW）

6.7.4FTP服务

6.7.5电子邮件服务（E-mail）

6.7.6远程登陆服务与查询服务

6.7.7即时通信

6.7.8Internet上的新型服务

6.7.9物联网

## 6.1通信的基础概念

### 6.1.1数据通信三要素

在数据通信中，有三个重要的要素，分别是信源（source）、信道（channel）和信宿（destination）。这些要素在数据传输过程中起到不同的作用。

1. 信源（source）：

信源指的是数据的产生源头，它可以是一个信息源、设备或系统，负责生成要传输的数据。信源可以是各种类型的数据，如文本、图像、音频和视频等。例如，一个摄像头或麦克风可以作为信源，产生图像或音频数据。

2. 信道（channel）：

信道指的是用于传输数据的媒介或路径。它可以是物理媒介（如电缆、光纤、无线信道）或逻辑通道（如计算机网络中的虚拟通道）。数据通过信道从信源传输到信宿。在信道中，数据可能会受到噪声、干扰或损耗影响。例如，互联网或局域网是常见的信道，用于通过计算机网络传输数据。

3. 信宿（destination）：

信宿指的是数据的目标或接收方，它是传输过程中的终点。信宿接收来自信源通过信道传输的数据，并进行相关处理或使用。例如，计算机、手机或电视等设备可以作为信宿，接收并显示或处理从信源传输过来的数据。

这三个要素共同构成了数据通信的基本框架。信源负责产生数据，信道用于传输数据，信宿接收并处理数据。数据通信的目的是确保从信源到信宿的可靠数据传输，并保证传输的数据在目标处得到正确还原或处理。

### 6.1.2通信信号

1. 信号的频率：

信号的频率是指信号中周期性变化的频率，通常以赫兹（Hz）为单位表示。频率决定了信号的周期性，它越高表示信号变化的速率越快。例如，音频信号中，20Hz以下的频率表示低音，而20kHz以上的频率表示高音。

2. 信号的频带：

信号的频带是指信号中包含信息的频率范围。它表示信号能够有效传输的频率范围。例如，对于音频信号，人耳能够感知的频率范围大约在20Hz到20kHz之间。

3. 模拟信号：

模拟信号是连续变化的信号，其数值在时间上可以任意取值。模拟信号可以是连续的时间信号和连续的幅度信号，可以用无限数量的值来表示。例如，声音的波形是模拟信号，它可以在任意时刻取任意幅度。

4. 数字信号：

数字信号是离散化的信号，其数值在时间和幅度上都是离散的。数字信号只能取有限数量的值，并以离散的时间间隔表示。例如，计算机中处理的数据和网络传输的数据都是数字信号。

5. 模拟信号的数字化处理：

模拟信号的数字化处理是将模拟信号通过采样和量化过程转换为数字信号的过程。采样将连续时间信号转换为离散时间信号，而量化将连续幅度信号转换为离散幅度信号。这样处理后的信号可以进行数字处理、存储和传输。

6. 模拟信号的数字化的优点：

- 降低传输误差：数字信号对噪声和干扰更具抗干扰性，可以通过纠错码和差错控制技术来保证数据传输的准确性。

- 实现数字处理：数字信号可以进行更复杂的信号处理，如滤波、压缩、加密等，提高了信号处理的灵活性和效率。

- 方便存储和传输：数字信号可以通过数字存储介质（如硬盘、闪存）和数字通信网络进行高效的存储和传输，便于备份和共享。

### **6.1.3数据传输方式**

1. 基带传输（Baseband Transmission）：

概念：基带传输是指将原始数字数据直接通过信道进行传输，没有经过调制过程。它使用单一的频率范围传输数据信号。

例子：以太网（Ethernet）是一种常见的基带传输技术，它将数字数据以二进制形式直接发送到物理媒介（如双绞线）。

特点：

- 适用于短距离通信，如局域网（LAN）。

- 传输速率相对较高，可以达到几百兆位每秒。

- 相对简单、成本较低。

缺点：

- 传输距离有限，常规情况下不超过几百米。

- 不适用于长距离通信。

- 信号容易受到干扰和衰减。

2. 频带传输（Passband Transmission）：

概念：频带传输是将数字数据转换为模拟信号，再进行调制并传输。它使用多个频率范围传输数据信号。

例子：调幅（AM）广播是一种常见的频带传输技术，数字音频信号经过调制后在广播频带中进行传输。

特点：

- 适用于广播和远距离通信。

- 支持较长的传输距离。

- 可以支持较低的传输速率。

缺点：

- 传输速率相对较低，不适合高速数据传输需求。

- 受到噪声和干扰的影响。

3. 宽带传输（Broadband Transmission）：

概念：宽带传输是指将数据分成不同的频率带宽，使用多路复用技术在不同的频率带宽上同时传输多个信号。

例子：同轴电缆和光纤通信是常见的宽带传输技术，它们能够同时传输多个信号，如电话、电视和互联网数据。

特点：

- 提供高速、高容量的数据传输。

- 支持大范围、长距离通信。

- 可以同时传输多种类型的数据。

缺点：

- 成本较高，需要专门的设备和基础设施。

- 对于短距离通信需求，可能过于复杂和昂贵。

1. 并行传输（Parallel Transmission）：

概念：

并行传输是指同时发送多个比特（位）的数据，一次可以传送一个字符，并且每个比特使用独立的传输线路。在并行传输中，每个比特的传输分别在不同的传输线上进行。

传输数据的类型：

并行传输可用于传输任何类型的数据，包括数字数据和模拟数据。

例子：

传统的打印机连接方式中，使用并行传输将数据同时发送到打印机的每个字符位置。

特点：

- 传输速度快，因为多个比特同时传输。

- 较低的传输延迟。

- 适合短距离和高带宽需求。

缺点：

- 需要较多的传输线路，成本较高。

- 受到线路长度和噪声的限制。

- 可能会出现位移或抖动问题。

2. 串行传输（Serial Transmission）：

概念：

串行传输是指逐位（或逐字节）地传输数据，每次传输只使用单个传输线路。在串行传输中，数据依次发送和接收。

传输数据的类型：

串行传输可用于传输任何类型的数据，包括数字数据和模拟数据。

例子：

通常情况下，计算机与外设（如鼠标、键盘）之间的数据传输是通过串行传输进行的。

特点：

- 相对较低的传输速度，因为每个比特需要单独传输，但是传输效率高。

- 传输距离可以较长。

- 更少的传输线路需要，较低的成本。

- 更容易与其他设备进行连接。

缺点：

- 传输速度较慢。

- 受到噪声和干扰的影响。

- 需要额外的协议和控制机制。

串行传输的工作模式（单工，半双工，全双工）：

1. 单工传输（Simplex Transmission）：

概念：

单工传输是指数据只能在一个方向上进行传输，即只能由发送方向接收方传输数据。发送方只能发送数据，接收方只能接收数据，二者不能同时进行传输。

例子：

广播电台是单向传输的例子。电台可以发送信号给听众，但听众无法直接向电台发送信号。

特点：

- 数据只能在一个方向上传输。

- 发送方和接收方的角色固定，不可更改。

缺点：

- 不具备双向通信能力，无法实现双向数据传输。

- 传输效率相对较低。

2. 半双工传输（Half-duplex Transmission）：

概念：

半双工传输是指数据可以在两个方向上传输，但每次只能在一个方向上传输。发送方和接收方可以交替地发送和接收数据，但不能同时进行。

例子：

对讲机是半双工传输的例子。对讲机允许一方发送语音消息，然后切换到接收模式，以接收另一方发送的语音消息。

特点：

- 数据可以在两个方向上传输。

- 发送方和接收方在时间上交替进行数据传输。

缺点：

- 同一时间只能进行发送或接收，传输效率相对较低。

3. 全双工传输（Full-duplex Transmission）：

概念：

全双工传输是指数据可以同时双向传输，发送方和接收方可以同时进行发送和接收操作，实现即时的双向通信。

例子：

电话通信是全双工传输的例子。双方可以同时进行语音交流，即时地在两个方向上传输数据。

特点：

- 数据可以同时在两个方向上传输。

- 发送方和接收方可以同时进行发送和接收操作。

缺点：

- 需要独立的传输通道或频率资源，以支持同时的双向通信。

- 对通信设备的要求较高。

这些传输模式各有优缺点，并根据实际需求选择合适的传输模式。 单工传输只能在一个方向上传输数据，半双工传输可以在两个方向上传输但不能同时进行，而全双工传输可以同时双向传输数据，实现即时的双向通信。根据实际需求和资源限制，选择适合的传输模式可以提高数据传输的效率和可靠性。

非常抱歉，由于技术限制，我无法提供以Word格式优化排版的回答。以下是关于数据传输方式（同步传输，异步传输）的详细解释：

1. 同步传输（Synchronous Transmission）：

概念：

同步传输是一种数据传输方式，其中发送方和接收方在开始传输之前先进行时钟同步，然后按照时钟信号进行数据传输。

传输数据的单位：

面向比特传输，同步传输按照帧或数据块进行传输。

例子：

在计算机网络中，使用同步传输协议（如Synchronous Transmission Control Protocol）进行数据传输。

特点：

- 数据传输有时钟同步，数据流连续，传输速率相对较高。

- 实时传输，用于需要连续数据流的应用程序，如音频和视频流传输。

- 传输过程中有流量控制和差错检测机制，提高数据的准确性和可靠性。

缺点：

- 需要时钟同步机制，增加了传输的复杂性。

- 传输距离可能受到限制。

- 由于同步要求，传输过程中的错误可能会导致数据丢失。

2. 异步传输（Asynchronous Transmission）：

概念：

异步传输是一种数据传输方式，其中每个数据字符或数据帧之间没有直接的时钟同步，每个字符或帧都包含有关数据的时钟同步信息。

传输数据的单位：

面向字符传输，异步传输按照字符或字节进行传输。

例子：

串行通信中，使用异步传输发送数据字符的起始位和停止位进行时钟同步。

特点：

- 传输相对灵活，易于实现。

- 可用于低速数据传输，并且适用于间歇性数据传输。

- 传输过程中有流控制和差错检测机制，提高数据的可靠性。

缺点：

- 传输速率相对较低。

- 由于需要发送起始位和停止位，实际传输的数据量较大。

- 需要额外的控制位，增加了传输开销。

1. 频分复用（Frequency Division Multiplexing，FDM）：

概念：

频分复用是一种数据传输技术，它将不同的信号分配到不同的频率带宽上进行传输。每个信号占据一段特定的频率范围，它们可以同时进行传输而不互相干扰。

工作原理：

FDM通过将不同的信号调制到不同的子载波上，然后将这些子载波合并成一个复合载波进行传输。

例子：

传统的调幅广播就是通过FDM进行信号传输的一个例子。不同广播电台使用不同的频率段进行广播传输。

特点：

- 支持多个信号同时传输，提高传输效率。

- 不同信号彼此之间能独立传输，互不干扰。

- 适用于宽带信号传输，如电视广播和有线电视。

缺点：

- 需要复杂的调制和解调设备。

- 资源利用率低，会有部分带宽浪费。

2. 时分复用（Time Division Multiplexing，TDM）：

概念：

时分复用是一种数据传输技术，它将不同的信号分配到不同的时间片段上进行传输。每个信号占据一个特定的时间段，通过轮流分配时间片段来实现多个信号的同时传输。

工作原理：

TDM通过周期性地轮流划分时间片段，每个信号在各自的时间段内进行传输。

例子：

电话网络中的数字传输使用TDM。不同电话通话通过轮流占用时间片段的方式进行传输。

特点：

- 支持多个信号同时传输，提高传输效率。

- 不同信号在时间上交替进行传输。

- 适用于窄带信号传输，如电话和数据传输。

缺点：

- 对同步要求较高，需要严格的时钟同步。

- 时延较大，因为每个信号只能在特定的时间段内进行传输。

3. 波分复用（Wavelength Division Multiplexing，WDM）：

概念：

波分复用是一种数据传输技术，它将不同信号使用不同的光波长进行传输。每个信号使用独立的波长进行光传输，它们可以同时进行传输而不互相干扰。

工作原理：

WDM通过将不同信号使用不同的光波长进行光传输，然后将光信号合并成一个复合光信号进行传输。

例子：

光纤传输网络中的光通信使用WDM进行信号传输。不同的数据流使用不同的波长进行光传输。

特点：

- 支持多个信号同时传输，提高传输效率。

- 不同信号彼此之间能独立传输，互不干扰。

- 适用于高速宽带信号传输，如光纤通信和光网络。

缺点：

- 需要复杂的光传输和分离设备。

- 波长资源有限，需要进行精确的波长规划。

4. 码分复用（Code Division Multiplexing，CDM）：

概念：

码分复用是一种多路复用技术，它将不同的信号按照不同的编码序列进行传输。每个信号都使用独特的码片序列进行编码和解码，使得信号能够同时传输并在接收端进行分离。

工作原理：

CDM通过将不同信号与对应的码片序列进行乘法运算，然后将结果叠加在一起进行传输。在接收端，通过将接收到的信号与相应的码片序列进行乘法运算，分离出原始信号。

例子：

一种常见的应用是CDMA（Code Division Multiple Access）无线通信系统，如CDMA2000和WCDMA。在CDMA系统中，不同用户的信号使用不同的码片序列进行编码和解码，以实现多用户同时传输和接收。

特点：

- 支持多个信号同时传输，提高系统容量和频谱效率。

- 不同信号使用不同的码片序列进行编码，彼此之间互不干扰。

- 具有抗多径干扰和噪声的能力，提高传输质量。

缺点：

- 比较复杂的调制和解调过程，需要高效的编码和解码算法。

- 对于大规模用户和多径信道环境，需要处理较大的干扰和复杂的信号处理。

1. 通信频段：

概念：

通信频段是指用于移动通信的无线电频率范围。不同的频段有着不同的特性和应用。

单位：

通信频段通常使用赫兹（Hz）作为单位，也可以使用千赫兹（kHz）、兆赫兹（MHz）或吉赫兹（GHz）。

低频（长波）：

低频通信频段通常指300赫兹（Hz）至3兆赫兹（MHz）之间的频率范围。长波信号在传播过程中衰减较少，具有较远的传输距离。

中频（中波）：

中频通信频段通常指300赫兹（Hz）至3兆赫兹（MHz）之间的频率范围。中波信号具有较好的地面覆盖和穿透能力。

高频（短波）：

高频通信频段通常指3兆赫兹（MHz）至30兆赫兹（MHz）之间的频率范围。短波信号具有较强的穿透和反射能力，适合远距离传播和抗干扰能力强。

2. 移动通信技术：

概念：

移动通信技术指的是用于无线移动通信的各种通信系统和标准。

1. 1G（第一代移动通信）：

- 概念：1G是第一代移动通信技术，主要以模拟信号传输为基础，提供基本的语音通信功能。

- 频段范围：800兆赫兹（MHz）至900兆赫兹（MHz）。

- 传输速度：最高传输速率为2.4千比特/秒。

- 技术体系：使用模拟调制和频分多路复用（FDMA）进行信号传输。

- 例子：AMPS（Advanced Mobile Phone System）是一种1G移动通信系统。

- 特点：低速率，主要支持语音通信，信号覆盖范围较小。

- 缺点：容量有限，不适用于大规模数据传输。

2. 2G（第二代移动通信）：

- 概念：2G是第二代移动通信技术，采用数字信号传输，提供语音和基本的数据传输功能。

- 频段范围：900兆赫兹（MHz）至1.9兆赫兹（GHz）。

- 传输速度：最高传输速率为236千比特/秒。

- 技术体系：采用数字调制和时分多址（TDMA）或码分多址（CDMA）进行信号传输。

- 例子：GSM（Global System for Mobile Communications）是一种2G移动通信系统。

- 特点：提供了数字化的语音通信和基本的数据传输，更好的信号覆盖和通话质量。

- 缺点：相对较低的数据传输速率，不支持高速互联网访问。

3. 3G（第三代移动通信）：

- 概念：3G是第三代移动通信技术，引入了宽带无线接入，提供更高的数据传输速率和多媒体服务。

- 频段范围：1.9兆赫兹（GHz）至2.2兆赫兹（GHz）。

- 传输速度：最高传输速率为2兆比特/秒。

- 技术体系：采用宽带码分多址（WCDMA）或CDMA2000进行信号传输。

- 例子：UMTS（Universal Mobile Telecommunications System）是一种3G移动通信系统。

- 特点：提供较高的数据传输速率，支持多媒体服务，如音频、视频和互联网访问。

- 缺点：信号覆盖范围相对较小，建设成本较高。

4. 4G（第四代移动通信）：

- 概念：4G是第四代移动通信技术，采用全IP（Internet Protocol）网络，提供更高的数据速率和更好的用户体验。

- 频段范围：2兆赫兹（GHz）至38兆赫兹（GHz）。

- 传输速度：最高传输速率为100兆比特/秒。

- 技术体系：采用LTE（Long-Term Evolution）技术进行信号传输。

- 例子：LTE是一种4G移动通信系统。

- 特点：更高的数据传输速率，低延迟，支持高质量的音频、视频和互联网服务。

- 缺点：信号覆盖范围相对较小，建设和频段规划成本较高。

5. 5G（第五代移动通信）：

- 概念：5G是第五代移动通信技术，旨在提供更高的数据传输速率、更低的延迟和更好的网络容量，以支持大规模互联和物联网应用。

- 频段范围：24兆赫兹（GHz）至100兆赫兹（GHz）。

- 传输速度：5G的预期传输速率为10-20 Gbps（下行）和1-10 Gbps（上行）。

- 技术体系：5G采用了多项技术和标准，包括毫米波、大规模天线阵列、高密度调制和调度、网络切片、软件定义网络（SDN）和网络功能虚拟化（NFV）等。

- 例子：一些5G标准和技术包括3GPP Release 15和Release 16，以及5G New Radio（NR）。

- 特点：5G具有高速率、低延迟、大容量、多连接和网络切片等特点，可支持大规模物联网设备、智能城市、自动驾驶车辆等应用。

- 缺点：由于采用了更高频段的信号传输，5G的信号覆盖范围较窄，需要部署更密集的基站和设备。此外，部署和维护成本也较高。

1. GSM（全球移动通信系统）：

- 概念：GSM是一种数字移动通信系统，用于语音和数据传输，是2G移动通信的一种标准。

- 例子：GSM网络由诸如Vodafone、AT&T、T-Mobile等运营商提供。

- 特点：GSM提供全球漫游能力、高质量的语音通话、短信和基本数据传输功能。

- 缺点：传输速率较低，不适用于高速互联网访问和大规模数据传输。

2. GPS（全球定位系统）：

- 概念：GPS是一种卫星导航系统，用于确定地理位置和导航。

- 例子：GPS系统由美国航空航天局（NASA）维护，并广泛应用于导航仪器、智能手机和车辆导航系统等设备。

- 特点：GPS通过接收地面上的多个卫星信号，可以提供准确的位置信息和导航功能。

- 缺点：在某些环境下，如高层建筑群、森林覆盖等地方，会影响GPS信号的接收和定位精度。

3. WCDMA（宽带码分多址）：

- 概念：WCDMA是一种3G移动通信技术，采用宽带码分多址进行信号传输。

- 例子：UMTS（通用移动通信系统）是一种采用WCDMA技术的3G移动通信系统。

- 特点：WCDMA提供高速数据传输、多媒体和互联网访问功能，支持语音和视频通话。

- 缺点：信号覆盖范围相对较小，建设成本较高。

### **6.1.4数据交换方式**

1. 电路交换：

- 概念：电路交换是一种数据交换方式，其中在通信会话期间，为通信双方建立专用的物理连接（电路）来进行数据传输。

- 例子：传统的电话通信是一种电路交换的例子，通话期间使用独占的物理电路进行数据传输。

- 优点：实时连接，传输稳定，适用于持续通信的应用。

- 缺点：资源占用较高，不适用于短时间且不连续通信的应用。

2. 报文交换：

- 概念：报文交换是一种数据交换方式，其中消息作为完整的报文单元进行传输，不需要建立和维护持续的物理连接。

- 例子：电子邮件（Email）系统是一种报文交换的例子，整个邮件以一个报文的形式传输。

- 优点：无需建立持续的物理连接，适用于非实时通信和不连续通信的应用。

- 缺点：传输效率低，报文长度不确定可能导致资源浪费。

3. 报文分组交换：

- 概念：报文分组交换是一种数据交换方式，通过将报文拆分为较小的报文分组，以分组的形式进行传输。

- 例子：因特网（Internet）是一种报文分组交换的例子，其中数据以IP数据报的形式分组传输。

- 优点：支持灵活的路由和多路径传输，适用于不同速率和网络连接的数据传输。

- 缺点：分组到达的顺序不保证，可能会引入传输延迟和重组开销。

4. 分组交换中的数据报：

- 概念：数据报是一种分组交换中使用的报文单元，它包含了完整的源和目的地址。

- 例子：IPv4和IPv6协议中的数据报是分组交换的数据单元。

- 优点：每个数据报独立编址，具有灵活的路由选择和多路径传输能力。

- 缺点：报文长度不确定，可能导致传输效率低下。

5. 分组交换中的虚电路：

- 概念：虚电路是一种分组交换中使用的逻辑连接，类似于电路交换中的物理连接，但是不需要独占的物理路径。

- 例子：X.25和ATM网络中的虚电路是分组交换的一种形式。

- 优点：提供了可靠的有序传输和错误控制，比无连接的分组传输具有更好的效率。

- 缺点：虚电路需要建立和维护连接状态，占用一定的网络资源。

### **6.1.5差错控制技术**

1. 随机热噪声：

- 概念：随机热噪声是通信信道中由于温度引起的不可预测的信号失真。

- 例子：在无线通信中，由于大气、电子器件的热噪声等因素，信道中会存在随机的信号失真。这可能导致接收到的数据中出现误差或错误。

2. 随机差错：

- 概念：随机差错指的是在通信过程中出现的不可预测的单个位或多个位的错误。

- 例子：在数字通信中，由于噪声或干扰的存在，接收到的数据可能与发送的数据不一致，发生随机的位错误。例如，在无线电通信中，信号穿越大气和其他电子干扰源时可能发生随机差错。

3. 冲击噪声：

- 概念：冲击噪声是通信信道中突然出现的强烈干扰信号。

- 例子：在通信中，比如雷击、电力线干扰等突发性噪声，可能会导致数据传输过程中的冲击噪声，进而引起数据传输错误。

4. 突发差错：

- 概念：突发差错是在通信过程中出现的连续的错误，通常是由于信道中的连续干扰导致的。

- 例子：在数据传输中，突发差错可能源自传输介质上的连续干扰，如电力线上的冲击干扰或其他电磁源引起的干扰，导致接收到的连续数据位出现错误。

5. 奇校验：

- 概念：奇校验是一种差错控制技术，通过在数据位中添加一个奇数个校验位来检测传输过程中的错误。

- 例子：例如，假设要传输数据10110，使用奇校验时，加入奇校验位变为101100，校验位的值由发送方设定为使整个数据中包含奇数个1的值。在接收端，如果接收到的数据位中的1的个数为偶数，说明数据发生了错误。

6. 偶校验：

- 概念：偶校验是一种差错控制技术，通过在数据位中添加一个偶数个校验位来检测传输过程中的错误。

- 例子：例如，假设要传输数据10110，使用偶校验时，加入偶校验位变为101101，校验位的值由发送方设定为使整个数据中包含偶数个1的值。在接收端，如果接收到的数据位中的1的个数为奇数，说明数据发生了错误。

7. 循环冗余校验（CRC）：

- 概念：循环冗余校验是一种基于多项式计算的差错控制技术，通过添加生成多项式的余数作为校验码来检测传输过程中的错误。

- 例子：例如，在以太网通信中使用的CRC校验算法，发送方利用生成多项式对待发送的数据进行计算，生成冗余校验码（CRC）。接收方接收到数据后，再进行一次CRC计算，并与接收到的CRC校验码进行比较，如果结果不一致，则说明数据传输过程中发生了差错。

8.CRC算法

1. 生成多项式：选择一个生成多项式作为CRC算法的基础，通常通过一个二进制数表示。生成多项式对应着CRC校验码的特征，不同的生成多项式能提供不同的校验能力。

2. 数据位扩展：将发送的数据位按照约定的规则进行位扩展，例如在数据末尾添加若干个0，扩展成数据位+附加检验位的形式。

3. 除法运算：使用生成多项式进行多项式除法运算。将扩展后的数据位与生成多项式进行逐位按位异或运算（即模2除法），直到运算到最后一位得到余数。

4. 附加校验位：将得到的余数作为附加校验位，附加到原始数据位之后。

5. 发送数据：将原始数据位和附加校验位一起发送。

6. 接收数据：接收端接收到数据后，对接收到的数据位执行与发送端相同的除法运算，得到余数。

7. 校验结果：如果接收到的余数为0，则说明数据没有发生错误；如果余数不为0，则表示数据发生了错误。

以下是一个CRC校验算法的例子：

假设有要发送的数据位为1011001，生成多项式为1101。

1. 数据位扩展：在数据位末尾添加三个零，扩展成1011001000。

2. 除法运算：执行多项式除法运算，按位进行异或（模2除法）。

1011001000

⊕ 1101

----------

1111 -- 第一次异或结果

⊕ 1101

----------

1011 -- 第二次异或结果

⊕ 1101

----------

111 -- 第三次异或结果

⊕ 1101

----------

10 -- 最终余数，即CRC校验码

3. 附加校验位：将最终余数 10 作为附加校验位，附加到原始数据位之后，得到完整的发送数据为：101100110。

当接收端收到数据101100110后，使用相同的生成多项式进行除法运算，得到最终余数。如果最终余数为0，则说明数据传输过程中没有发生错误。

### **6.1.6数据通信的主要技术参数**

1. 数据传输速率：

- 概念：数据传输速率是指单位时间内传输的数据量，通常以比特每秒（bps）表示。

- 例子：以太网的数据传输速率常见的有10 Mbps、100 Mbps、1 Gbps等。

2. 信道带宽：

- 概念：信道带宽是指该信道中可传输数据的频率范围。

- 例子：在无线电通信中，一个频率带宽为20 kHz的信道可以传输20,000 Hz的频率范围内的信号。

3. 误码率：

- 概念：误码率是指在数据传输过程中出现误码（错误比特）的概率。

- 例子：一个系统的误码率为0.01%，意味着在每传输10,000个比特中，平均有1个比特是错误的。

4. 比特率：

- 概念：比特率是指每秒钟传输的比特数，也称为数据传输速率。它与调制方式和信道带宽有关。

- 例子：调制方式为64-QAM，信道带宽为1 MHz，那么比特率可以达到64 Mbps。

5. 波特率：

- 概念：波特率是指单位时间内变化的信号波形数量，通常与无线电频率相关。

- 例子：一个调制方式的波特率为10,000 baud，意味着每秒可以变化10,000个信号波形。

6. 信道容量：

- 概念：信道容量是指信道能传输的最大数据速率，受到信道带宽和信噪比的影响。

- 例子：一个信道带宽为10 MHz，信噪比为30 dB的信道容量可以达到20 Mbps。

7. 信噪比：

- 概念：信噪比是指信号与噪声之间的相对强度比较，用于衡量信号强度与背景噪声的关系。

- 例子：一个信号强度为100 dBm，背景噪声强度为-90 dBm，那么信噪比为190 dB。

## **6.2计算机网络概述**

### 6.2.1计算机网络的产生与发展

1. 第一代计算机网络：

- 概念：第一代计算机网络起源于20世纪60年代末，是为满足科学和军事研究的需要而建立的。这些网络使用分组交换方式进行数据传输，具有较低的传输速率和局限的覆盖范围。

- 例子：美国的ARPANET是第一个广泛部署的计算机网络，建立于1969年。它连接了多个研究机构，为科学家们提供了分布式的资源共享和通信能力。

2. 第二代计算机网络：

- 概念：第二代计算机网络兴起于20世纪80年代，注重建立多种异构网络之间的互联，以实现更大范围的资源共享和信息传输。

- 例子：局域网（LAN）和广域网（WAN）是第二代计算机网络的代表。以太网是最早的局域网技术之一，而X.25和Frame Relay等技术则用于建立广域网连接。

3. 第三代计算机网络：

- 概念：第三代计算机网络开始于20世纪90年代，主要目标是提供更高的传输速率、更稳定的连接和多媒体传输能力。

- 例子：第三代计算机网络采用了光纤通信和宽带接入技术（如ADSL和光纤到户），从而实现了更高的传输速率。同时，基于IP协议的互联网架构在这一阶段得到了广泛应用。

4. 第四代计算机网络：

- 概念：第四代计算机网络起源于21世纪初，主要关注于推动无线通信和移动互联网的发展，提供更高的移动性和连接性。

- 例子：LTE（长期演进）和WiMAX（全球互通的微波接入）等无线通信技术是第四代计算机网络的代表。这些技术提供了更高的无线数据传输速率和更广阔的覆盖范围。

5. 计算机网络在中国的发展：

- 概述：中国在计算机网络的发展中发挥了重要作用，经历了快速的增长和覆盖范围的扩大。

- 发展过程：中国的计算机网络起步较晚，但通过不断努力，在20世纪80年代末和90年代初实现了基于IP协议的互联网接入。随后，在21世纪初迅速推动了移动互联网的发展，成为全球最大的互联网用户国家。

- 应用广泛：如今，中国拥有庞大的互联网用户群体，涵盖了各个领域的应用，包括电子商务、社交媒体、在线支付、云计算等。

8.中国基于Internet的公用网络

- 中国公用计算机互联网（CHINANET）：

- 概述：中国公用计算机互联网是指中国国内的公用互联网，为中国的个人用户和企业组织提供广泛的网络接入和互联互通服务。

- 发展历程：中国公用计算机互联网的发展始于20世纪90年代，通过各级互联网服务提供商（ISP）的建设和发展，构建了大规模的网络基础设施。

- 特点：中国公用计算机互联网具有庞大的用户群体、高速的网络连接、多样化的网络应用和丰富的数字内容。

-. 中国金桥信息网（CHINAGBN）：

- 概述：中国金桥信息网是中国领先的内容分发网络（CDN）和云服务提供商，致力于提供高速、稳定的内容分发和加速服务。

- 服务内容：金桥信息网提供静态和动态内容分发、云计算基础设施和边缘计算服务等。通过全球分布式的加速节点，加快用户对内容的访问速度。

- 应用领域：金桥信息网的服务广泛应用于电子商务、媒体和娱乐、在线教育、游戏和移动应用等领域。

- 中国教育和科研计算机网（CERNET）：

- 概述：中国教育和科研计算机网是为中国高校和科研机构之间提供网络连接和资源共享的专用计算机网。

- 发展历程：CERNET于1987年建立，最初是为了满足高校和科研机构之间的数据传输和合作研究需求。随着互联网的发展，CERNET逐渐与全球互联网接入互通。

- 特点：CERNET在网络连接速度、网络服务质量和安全性等方面进行了优化，为高校和科研机构提供了高效可靠的网络环境。

- 中国科学技术网（CSTNET）：

- 概述：中国科学技术网是中国科学技术人员之间提供网络连接和信息交流的专用计算机网。

- 发展历程：CSTNET成立于1994年，旨在促进科学技术领域的合作研究和学术交流。作为中国科学院下属的网路与信息中心负责运营和维护。

- 特点：CSTNET提供高速、稳定的网络连接和专业的服务，为科学研究机构、科学家和学术团体提供了良好的网络环境和资源支持。

### 6.2.2计算机网络的概念与功能

1. 计算机网络的概念：

- 概念：计算机网络是由一组计算机和网络设备组成的系统，通过通信链路和协议进行连接，从而形成一个共享资源和通信交流的虚拟空间。

- 例子：互联网是最典型的计算机网络，它将全球范围内的数十亿计算机和设备连接到一起，以实现信息交流和资源共享。

2. 计算机网络的功能：

1) 信息传递：计算机网络使得不同地点的计算机和设备能够相互通信和传输数据，实现信息的快速传递和交流。例如，电子邮件、即时通讯和文件传输协议（FTP）等都是计算机网络中常用的信息传递方式。

2) 资源共享：计算机网络提供了分布式的资源共享能力，使得多台计算机可以共享硬件设备（如打印机、扫描仪）、软件应用程序和存储空间等资源。例如，在局域网中，多台计算机可以共享同一台打印机，提高了资源的利用效率。

3) 提高系统可靠性：计算机网络可以通过冗余和备份机制来提高系统的可靠性和容错性。当一个节点或链路发生故障时，数据可以通过其他路径传输，从而保障通信的连续性。例如，在企业的计算机网络中，通过建立冗余的网络设备和链路，以防止单点故障。

4) 分布式处理：计算机网络可以将任务分配给不同的计算节点进行并行处理，从而提高计算效率和系统的性能。分布式计算范围从集群服务器到全球范围的云计算平台。例如，分布式系统可以将大规模的数据处理任务分发给多台计算机进行并行计算和协同处理。

### 6.2.3计算机网络的分类

1. 按照覆盖范围分类：

- 局域网（LAN）：局域网是在一个相对较小的地理范围内建立的计算机网络，例如办公楼、学校或家庭。它们通常使用高速的本地连接技术，例如以太网（Ethernet）。局域网允许在局域网内的计算机之间进行资源共享和通信。

- 城域网（MAN）：城域网是覆盖一个城市或地理范围较大的区域的计算机网络。它们通常由多个局域网通过广域网连接而成，提供了更广泛的资源共享和协作能力。典型的城域网技术包括光纤分布式数据接口（FDDI）和无线电传输器。

- 广域网（WAN）：广域网覆盖范围更广，可以跨越大片区域，甚至跨越国家和大洲。广域网使用广域连接技术，例如电话线、光纤和卫星链路，将远距离地理位置的计算机和网络设备连接起来。互联网就是最大的广域网，连接了全球的计算机和网络。

2. 按照有线/无线分类：

- 有线网：有线网络使用物理连接线（如以太网电缆、光纤电缆或同轴电缆）将计算机和网络设备连接在一起。有线网络可以提供较高的传输速率和较低的延迟，且较不受干扰。例如，以太网是常见的有线局域网技术。

- 无线网：无线网络通过无线信号传输（如Wi-Fi或蓝牙）实现计算机和网络设备之间的通信和连接。无线网络提供了更大的灵活性和移动性，使用户可以从任何位置访问网络。无线局域网（WLAN）是常见的无线网络类型。

3. 按照传输带宽分类：

- 基带网：基带网是指使用基带信号传输的网络，只能在一个频率上发送信号。基带网络通常用于传输数字信号，具有较低的传输带宽和短距离的限制。典型的基带网包括以太网。

- 宽带网：宽带网通过调制调试技术将多个信道的信号合并在一起，实现并行传输，提供了更高的传输速率。宽带网络可以传输更大容量的数据，并支持多种数据类型，如音频、视频和图像。常见的宽带网络包括数字用户线路（DSL）、电缆网络和光纤网络。

4. 按照使用范围分类：

- 公用网：公用网络是指面向公众、广泛开放的网络，在其中人们可以访问互联网和各种在线服务。最明显的例子就是Internet，它是全球公用的网络基础设施，连接了各种公共和私人网络。

- 专用网：专用网络通常是为特定组织、行业或个人定制的私有网络。它们提供了专门的资源和服务，被用于满足特定的通信和安全需求。例如，公司内部的企业网、研究机构的科研网络、政府部门的政府网络等都属于专用网络。

### 6.2.4网络通信的三种模式

1. 单播（Unicast）：

单播是一种点对点的通信模式，其中一个发送方向一个接收方发送数据。在单播模式下，数据包被发送到特定的目标地址，只有该地址上的设备能够接收和处理数据。

例子：

当您在浏览器中输入网址并访问网站时，您发送的请求被单播到远程服务器，然后服务器响应数据包返回给您的计算机。

2. 广播（Broadcast）：

广播是一种一对多的通信模式，其中一个发送方向所有连接到网络的设备发送数据。在广播模式下，数据包被发送到特定的广播地址，网络上的所有设备都能接收和处理数据。

例子：

当局域网中的某个设备发送ARP（地址解析协议）请求时，它将ARP请求包作为广播发送到所有的设备。所有收到广播包的设备都会检查请求中的目标IP地址，并向发送方提供自己的MAC地址。

3. 组播（Multicast）：

组播是一种一对多的通信模式，其中一个发送方向一组设备发送数据。在组播模式下，数据包被发送到特定的组播地址，只有加入了该组播组的设备才能接收和处理数据。

例子：

在视频会议中，当主持人发送音频/视频流时，数据通过组播地址发送给所有参与者。只有加入了该组播组的参与者才能接收和播放流媒体数据。

## 6.3计算机网络系统结构

### 6.3.1计算机网络系统组成

1. 网络硬件：

1.1 网络服务器：

网络服务器是一台高性能的计算机，用于存储和处理网络中的数据和资源。它提供服务，例如文件共享、打印服务、数据库管理等。

1.2 工作站：

工作站是计算机网络中的客户端设备，用于执行特定的计算任务。工作站可以是桌面计算机、笔记本电脑或其他终端设备。

1.3 网络设备：

网络设备用于连接和管理计算机网络中的各个节点。常见的网络设备包括路由器、交换机、网桥和集线器等。

1.4 传输介质：

传输介质是网络中用于传输数据的物理媒介。常见的传输介质包括以太网电缆（如光纤、双绞线）、无线信号（如Wi-Fi）和卫星链接等。

2. 网络软件：

2.1 网络操作系统：

网络操作系统是安装在网络服务器上的软件，它提供网络管理、配置、安全和资源共享等功能。常见的网络操作系统包括Windows Server、Linux和Unix。

2.2 网络通信协议：

网络通信协议是计算机网络中用于在不同设备之间传输和交换数据的规则和标准。常见的网络通信协议包括TCP/IP、HTTP、FTP、SMTP等。

2.3 网络应用软件：

网络应用软件是在计算机网络中运行的应用程序，用于完成特定的任务和提供服务。常见的网络应用软件包括Web浏览器、电子邮件客户端、远程桌面软件等。

### 6.3.2计算机网络逻辑结构

1. 通信子网：

通信子网是计算机网络中负责数据传输和通信的部分。它提供了将数据从一个节点传输到另一个节点的通信通道，具有传输数据的功能。

例子：

在一个企业内部的计算机网络中，局域网（LAN）被视为通信子网。设备通过交换机或无线接入点连接到局域网，可以通过局域网进行数据传输和通信。

2. 资源子网：

资源子网是计算机网络中负责提供共享资源和服务的部分。它承载了网络中的各种资源，例如文件、打印机、数据库等，供其他设备访问和使用。

例子：

在一个大型公司的计算机网络中，文件服务器和打印服务器可以被视为资源子网。这些服务器提供了共享的文件存储和打印服务，其他设备可以通过网络访问并使用这些资源。

### 6.3.3计算机网络拓扑结构

概念：计算机网络拓扑结构指的是不同设备在计算机网络中的连接方式和布局关系。常见的计算机网络拓扑结构包括总线型、环型、星型、树型、网状和蜂窝。

1. 总线型拓扑结构：

概念：总线型拓扑结构将所有设备连接到同一条共享传输介质上，每个设备可以直接发送或接收数据。

例子：以太网是最常见的总线型拓扑结构的例子，所有计算机通过一根共享的以太网电缆连接。

优点：

- 易于实施和维护。

- 成本相对较低。

缺点：

- 传输线带宽可能成为瓶颈。

- 故障节点可能导致整个网络中断。

2. 环型拓扑结构：

概念：环型拓扑结构将所有设备连接成一个环，每个设备通过令牌来顺序传递数据。

例子：Token Ring网络是环型拓扑结构的一个例子，其中数据通过令牌在环上传输。

优点：

- 具有良好的性能和高可靠性。

- 数据传输无冲突。

缺点：

- 扩展性较差，添加或删除设备相对困难。

- 故障节点可能导致整个环中断。

3. 星型拓扑结构：

概念：星型拓扑结构将所有设备连接到一个中心节点，所有数据都通过中心节点进行通信。

例子：以太网通过集线器或交换机实现星型拓扑结构。

优点：

- 易于管理和维护。

- 故障设备不会影响其他设备运行。

缺点：

- 中心节点的故障会导致整个网络中断。

- 网络性能受到中心节点的限制。

4. 树型拓扑结构：

概念：树型拓扑结构通过将多个星型网络连接起来，形成树状结构，具有层级关系。

例子：大规模企业网络通常采用树型拓扑结构，不同办公室通过路由器连接形成树型网络。

优点：

- 提供更好的可扩展性和容错性。

- 网络分段可以独立管理。

缺点：

- 需要额外的硬件设备（如路由器）来管理网络。

- 整个网络的性能受到根节点和路由器的限制。

5. 网状拓扑结构：

概念：网状拓扑结构中，所有设备直接连接到其他设备，形成多对多的连接关系。

例子：互联网就是一个网状拓扑结构的典型例子，不同网络之间相互连接。

优点：

- 高度可靠的冗余路径。

- 数据传输效率高。

缺点：

- 硬件和软件配置复杂。

- 维护成本较高。

6. 蜂窝拓扑结构：

概念：蜂窝拓扑结构模仿蜂窝的布局，将网络划分为许多小的基本单元，每个单元都有自己的连接。

例子：移动通信网络中的无线蜂窝网络就采用蜂窝拓扑结构。

优点：

- 具有高度可靠性和冗余路径。

- 提供较强的扩展性。

缺点：

- 需要大量的基站和信号覆盖。

- 部署和维护成本高。

### 6.3.4常用网络命令

1. ping命令：

用法：ping [目标主机或IP地址]

作用：测试本地主机与目标主机之间的网络连接状态。

示例：ping www.google.com

2. traceroute命令：

用法：traceroute [目标主机或IP地址]

作用：显示数据包从本地主机到目标主机之间经过的路由器路径。

示例：traceroute www.google.com

3. netstat命令：

用法：netstat [-options]

作用：显示当前计算机网络连接和端口的统计信息。

示例：

- 显示所有活动的网络连接：

netstat -a

- 只显示TCP连接：

netstat -t

- 显示监听中的端口：

netstat -l

4. ipconfig命令：

用法：ipconfig [-options]

作用：显示当前计算机的IP配置信息。

示例：

- 显示当前IP配置：

ipconfig

- 显示详细的网络适配器信息：

ipconfig /all

- 刷新IP配置（释放和续约DHCP租约）：

ipconfig /renew

### 6.3.5网络协议

概念：网络协议是计算机网络中通信参与方之间约定的规则和标准，用于指导数据在网络中的传输和处理。网络协议定义了通信的语义、语法和时序等方面的规定。

1. 语义：

- 语义指定了通信参与方之间交换的信息的含义和解释。

- 语义规定了如何理解数据包中的字段、消息的状态转换以及各种操作的含义。

- 语义是网络协议中最核心的部分，确保了参与方之间的有效通信。

示例：HTTP协议规定了客户端与服务器之间的数据交互方式，包括请求和响应的格式，以及状态码的含义。

2. 语法：

- 语法规定了通信数据的格式和结构。

- 语法定义了数据包中各个字段的编码方式以及它们在数据流中的位置。

- 语法确保了参与方能够正确解析和构建通信数据。

示例：TCP/IP协议中的IP头部定义了数据包传输的源地址、目标地址和其他相关信息的格式。

3. 时序：

- 时序规定了通信参与方之间消息的顺序和处理的时机。

- 时序确保了消息的有序交付和正确处理。

示例：TCP协议通过序列号和确认机制来确保数据包的有序传输和可靠性。

网络协议的设计和实现通常需要综合考虑语义、语法和时序等方面。通过制定统一的规则和标准，网络协议使得不同设备和系统能够在网络中相互通信和交换数据。

### 6.3.6开放网络互连参考模型（OSI - RM）

概念：

开放网络互连参考模型，也称为OSI参考模型，是一个分层的网络架构，旨在描述计算机网络中的通信和连接。它将网络通信过程划分为七个不同的层次，每个层次具有特定的功能和责任，并通过标准化的接口实现层与层之间的协作。

以下是OSI参考模型的七个层次，包括它们的概念、功能、数据单位、典型协议和设备，以及五个详细的例子：

7. 应用层（Application Layer）：

- 概念：提供网络应用服务的接口，允许用户访问网络资源。

- 功能：处理特定的应用程序通信需求。

- 数据单位：消息、命令。

- 典型协议：HTTP、FTP、SMTP。

- 设备：Web服务器、电子邮件服务器。

- 例子:

- 使用HTTP协议进行网页浏览。

- 使用FTP协议进行文件传输。

- 使用SMTP协议发送电子邮件。

6. 表示层（Presentation Layer）：

- 概念：处理数据格式转换和数据加密解密等，确保应用程序之间的语义问题。

- 功能：实现数据的格式转换和加密解密。

- 数据单位：数据块、报文。

- 典型协议：JPEG、ASCII、TLS。

- 设备：加密器、解密器。

- 例子:

- JPEG协议用于压缩和解压缩图像文件。

- ASCII编码用于表示文本数据。

- TLS协议对传输数据进行加密。

5. 会话层（Session Layer）：

- 概念：管理不同应用程序之间的会话和连接。

- 功能：建立、维护和终止应用程序之间的会话。

- 数据单位：会话数据。

- 典型协议：NetBIOS、RPC。

- 设备：会话管理器。

- 例子:

- 使用NetBIOS协议在网络上建立会话。

- 使用RPC协议进行远程过程调用。

4. 传输层（Transport Layer）：

- 概念：提供端到端的可靠数据传输，确保数据分组的完整性和顺序。

- 功能：处理数据的分段、流量控制和错误检测。

- 数据单位：报文段或数据包。

- 典型协议：TCP、UDP。

- 设备：网关、防火墙。

- 例子:

- 使用TCP协议进行可靠的数据传输。

- 使用UDP协议进行无连接的数据传输。

3. 网络层（Network Layer）：

- 概念：处理分组转发和路由选择，实现不同网络之间的数据传输。

- 功能：将数据包从源节点传输到目标节点。

- 数据单位：数据包、IP数据报。

- 典型协议：IP、ICMP。

- 设备：路由器、三层交换机。

- 例子:

- 使用IP协议将数据包从源地址路由到目标地址。

- 使用ICMP协议进行网络连接和错误检测。

2. 数据链路层（Data Link Layer）：

- 概念：提供可靠的点对点数据传输，通过物理地址（MAC地址）将数据分组封装为帧。

- 功能：处理帧的传输和错误检测。

- 数据单位：帧、比特。

- 典型协议：Ethernet、PPP。

- 设备：交换机、网卡。

- 例子:

- 使用以太网协议在局域网上传输数据。

- 使用PPP协议在拨号连接中传输数据。

1. 物理层（Physical Layer）：

- 概念：负责传输比特流，处理物理介质和电信号传输。

- 功能：对比特流进行编码、传输和接收。

- 数据单位：比特。

- 典型协议：RS-232、Ethernet物理标准。

- 设备：网线、双绞线。

- 例子:

- 使用RS-232协议进行串行通信。

- 使用以太网标准定义的物理介质进行数据传输。

OSI参考模型提供了一种通用框架，用于理解和设计计算机网络中的通信和连接。通过这个模型，不同设备和系统之间可以实现互操作性和兼容性。

## 6.4TCP/IP体系结构

### 6.4.1TCP/IP参考模型

概念：

TCP/IP参考模型是一个基于分层的网络架构，用于描述计算机网络中的通信和连接。它由四个层次组成：应用层、传输层、网际层和网络接口层。每个层次具有特定的功能和责任，并通过协议和接口进行协作。

以下是TCP/IP参考模型的四个层次：

4. 应用层（Application Layer）：

- 概念：为用户提供网络服务和应用程序之间的接口。

- 功能：处理特定的应用程序通信需求。

- 数据单位：报文。

- 典型协议：HTTP、FTP、SMTP。

- 设备：Web服务器、电子邮件服务器。

- 例子：

- 使用HTTP协议进行网页浏览。

- 使用FTP协议进行文件传输。

- 使用SMTP协议发送电子邮件。

3. 传输层（Transport Layer）：

- 概念：提供端到端的可靠数据传输。

- 功能：处理数据的分段、流量控制和错误检测。

- 数据单位：报文段或数据包。

- 典型协议：TCP、UDP。

- 设备：网关、防火墙。

- 例子：

- 使用TCP协议进行可靠的数据传输。

- 使用UDP协议进行无连接的数据传输。

2. 网际层（Internet Layer）：

- 概念：网际层负责在不同网络之间进行数据传输。

- 功能：提供逻辑地址分配、路由选择和分片重组。

- 数据单位：包（Packet）。

- 协议：常见的网际层协议有IP（网际协议）、ICMP（Internet控制消息协议）和ARP（地址解析协议）。

- 设备：路由器、三层交换机等。

- 例子：

- IPv4（网际协议版本4）：提供逻辑地址分配和路由选择，广泛用于互联网通信。

- IPv6（网际协议版本6）：为了解决IPv4地址不足的问题而引入的下一代网际协议。

1. 网络接口层（Network Interface Layer）：

- 概念：处理网络接口和物理介质之间的通信。

- 功能：将数据帧从一个网络节点传输到另一个网络节点。

- 数据单位：帧、比特。

- 典型协议：Ethernet、ARP。

- 设备：交换机、网卡。

- 例子：

- 使用以太网协议在局域网上传输数据。

- 使用ARP协议解析IP地址和MAC地址之间的映射。

TCP/IP参考模型是互联网通信的基础，它定义了不同层次的功能和责任，确保网络的正常运行和互操作性。

### 6.4.2IP地址

IP地址是互联网协议（IP）中用于标识和定位设备的数字地址。它分为IPv4和IPv6两个版本。

IPv4（Internet Protocol version 4）：

IPv4是目前广泛使用的IP协议版本，它由32位二进制组成，通常用点分十进制表示。

IPv4地址分类（A类，B类，C类，D类，E类）：

1. A类地址：

- 概念：A类地址用于大型网络，网络部分占8个比特。

- 主机数：A类地址总共有2^24-2个可用主机。

- 例子：10.0.0.1、10.10.10.10

2. B类地址：

- 概念：B类地址用于中等规模的网络，网络部分占16个比特。

- 主机数：B类地址总共有2^16-2个可用主机。

- 例子：172.16.0.1、172.31.255.255

3. C类地址：

- 概念：C类地址用于小型网络，网络部分占24个比特。

- 主机数：C类地址总共有2^8-2个可用主机。

- 例子：192.168.0.1、192.168.255.255

4. D类地址：

- 概念：D类地址用于多播通信，不用于标识单个设备。

- 例子：224.0.0.1、239.255.255.255

5. E类地址：

- 概念：E类地址为保留地址，留作将来使用。

- 例子：240.0.0.0、255.255.255.255

IPv4地址结构（A类，B类，C类，D类，E类）：

1. A类地址：

- 概念：A类地址的网络部分占8个比特，主机部分占24个比特。

- 例子：10.0.0.1、10.10.10.10

2. B类地址：

- 概念：B类地址的网络部分占16个比特，主机部分占16个比特。

- 例子：172.16.0.1、172.31.255.255

3. C类地址：

- 概念：C类地址的网络部分占24个比特，主机部分占8个比特。

- 例子：192.168.0.1、192.168.255.255

4. D类地址：

- 概念：D类地址用于多播通信，没有固定的网络和主机部分。

- 例子：224.0.0.1、239.255.255.255

5. E类地址：

- 概念：E类地址为保留地址，没有固定的网络和主机部分。

- 例子：240.0.0.0、255.255.255.255

IPv4子网掩码：

IPv4子网掩码用于划分IP地址中的网络部分和主机部分。它们具有32位，与IPv4地址的每一位相对应，用来指示对应位是网络部分还是主机部分。

各类IPv4地址子网掩码（A类，B类，C类，D类，E类）：

A类地址子网掩码：255.0.0.0

B类地址子网掩码：255.255.0.0

C类地址子网掩码：255.255.255.0

D类地址子网掩码：无子网掩码（D类地址用于多播通信，没有固定的子网掩码）

E类地址子网掩码：无子网掩码（E类地址保留作其他用途）

IPv4动态地址：

概念：IPv4动态地址是指由DHCP（Dynamic Host Configuration Protocol，动态主机配置协议）服务器动态分配给主机的IP地址，主机每次连接网络时可能会获得不同的IP地址。

例子：当计算机通过DHCP服务器连接到局域网或互联网时，DHCP服务器会分配一个可用的IPv4动态地址给该计算机。例如，一个计算机可能在一次连接后获得了192.168.0.100作为动态地址，而下一次连接时可能获得192.168.0.200作为动态地址。

IPv4静态地址：

概念：IPv4静态地址是指手动配置给主机的固定IP地址，不会随着连接的变化而改变。

例子：管理员可以手动为主机分配静态IP地址，以确保主机的网络连接稳定。例如，一个服务器可能被分配了静态IP地址192.168.0.10，无论何时它连接到网络，它都会保持相同的IP地址。

IPv4地址网络部分的计算：

概念：IPv4地址的网络部分用于标识网络，网络部分的长度由子网掩码来确定。

详细方法：将IP地址和子网掩码进行逻辑与（AND）运算即可得到网络部分。

IPv4地址网络部分的计算示例：

1. IP地址：192.168.0.1，子网掩码：255.255.255.0

- 运算：192.168.0.1 AND 255.255.255.0 = 192.168.0.0

- 结果：网络部分为192.168.0.0

2. IP地址：172.16.42.128，子网掩码：255.255.0.0

- 运算：172.16.42.128 AND 255.255.0.0 = 172.16.0.0

- 结果：网络部分为172.16.0.0

3. IP地址：10.0.0.50，子网掩码：255.0.0.0

- 运算：10.0.0.50 AND 255.0.0.0 = 10.0.0.0

- 结果：网络部分为10.0.0.0

IPv4主机部分的计算：

概念：IPv4地址的主机部分用于标识主机或设备，主机部分的长度由子网掩码来确定。

详细方法：将子网掩码取反，然后与IP地址进行逻辑与（AND）运算，即可得到主机部分。

IPv4主机部分的计算示例：

1. IP地址：192.168.0.1，子网掩码：255.255.255.0

- 运算：192.168.0.1 AND 0.0.0.255 = 0.0.0.1

- 结果：主机部分为0.0.0.1

2. IP地址：172.16.42.128，子网掩码：255.255.0.0

- 运算：172.16.42.128 AND 0.0.255.255 = 0.0.42.128

- 结果：主机部分为0.0.42.128

3. IP地址：10.0.0.50，子网掩码：255.0.0.0

- 运算：10.0.0.50 AND 0.255.255.255 = 0.0.0.50

- 结果：主机部分为0.0.0.50

IPv4不可用地址：

概念：IPv4地址空间中存在一些特殊的地址，不能被分配给主机使用，通常用于保留或特定目的。

原因：这些不可用地址是为了避免冲突、保留特定功能或用于特殊用途。

IPv4不可用地址的例子：

1. 网络地址（Network Address）：用于表示整个网络的地址，即网络的第一个地址。

例如，192.168.0.0是一个网络地址。

2. 广播地址（Broadcast Address）：用于向网络中的所有主机广播数据的特殊地址，表示所有主机。

例如，192.168.0.255是一个广播地址。

3. 回环地址（Loopback Address）：用于本地主机内部的测试和通信，表示主机自身。

例如，127.0.0.1是IPv4中的回环地址。

4. 零地址（Zero Address）：在路由中表示默认路由或未知地址，不能用作主机地址。

例如，0.0.0.0是IPv4中的零地址。

5. 非法地址（Illegal Address）：保留用于特定目的，如地址分配测试、保留未分配地址等。

例如，240.0.0.0/4是保留的多播地址范围。

6. 特定用途地址（Special Purpose Address）：用于特定用途的地址。

例如，169.254.0.0/16是自动配置IP地址（APIPA），用于主机自动获取IP地址时未找到DHCP服务器。

7. 私有地址（Private Address）：用于局域网内部，不在公共网络中路由的地址范围。

例如，10.0.0.0/8、172.16.0.0/12和192.168.0.0/16都是私有地址范围。

这些不可用地址的存在和使用有助于保证IP地址的有效分配和网络通信的正常运作。

IPv4根据自定义子网掩码确定主机数的计算示例：

1. 子网掩码：255.255.255.0

- 主机数量：254

在子网掩码的最后一个字节中，有8个主机位可用，所以可以表示2^8-2=254个主机。

2. 子网掩码：255.255.252.0

- 主机数量：1022

在子网掩码的最后一个字节中的2个主机位和倒数第二个字节中的6个主机位可用，所以可以表示2^6\*2^2-2=1022个主机。

3. 子网掩码：255.255.128.0

- 主机数量：32766

在子网掩码的最后一个字节中的7个主机位和倒数第二个字节中的1个主机位可用，所以可以表示2^7\*2^1-2=32766个主机。

IPv4根据主机数确定自定义子网掩码的计算：

概念：根据给定的主机数量，确定合适的自定义子网掩码。

详细方法：根据主机数量，计算所需的主机位数，并生成对应的自定义子网掩码。

IPv4根据主机数确定自定义子网掩码的计算示例：

1. 主机数量：50

- 子网掩码：255.255.255.192

需要6位主机位可用，即在子网掩码的最后一个字节中有6个连续的位为主机位，所以使用子网掩码255.255.255.192。

2. 主机数量：1000

- 子网掩码：255.255.252.0

需要10位主机位可用，即在子网掩码的倒数第二个字节中有10个连续的位为主机位，所以使用子网掩码255.255.252.0。

3. 主机数量：5000

- 子网掩码：255.255.224.0

需要13位主机位可用，即在子网掩码的倒数第二个字节中有13个连续的位为主机位，所以使用子网掩码255.255.224.0。

IPv6：

概念：IPv6是下一代互联网协议，用于取代IPv4。它采用128位地址空间，相较于IPv4的32位地址空间，具有更大的地址容量和更好的路由性能等优势。

IPv6的例子：

1. 2001:0db8:85a3:0000:0000:8a2e:0370:7334

2. 2001:db8:0:0:0:ff00:42:8329

3. 2001:0:5ef5:79fd:4c5e:b274:46e3:ae9c

4. 2001:468:abcd:1111:2222:3333:4444:5555

5. fe80::1

IPv6地址结构：

概念：IPv6地址由8个16位的字段构成，使用冒号分隔，每个字段采用十六进制表示。

IPv6地址结构包括前缀、全球路由前缀、子网标识、接口标识等部分。

IPv6地址结构的例子：

1. 2001:0db8:85a3::/48

- 前缀：2001:0db8:85a3

- 全球路由前缀：2001

- 子网标识：0db8

- 接口标识：85a3

2. 2001:db8::/32

- 前缀：2001:db8

- 全球路由前缀：2001

- 子网标识：db8

- 接口标识：（省略）

3. fe80::/10

- 前缀：fe80

- 全球路由前缀：（省略）

- 子网标识：（省略）

- 接口标识：（省略）

4. 2001:468:abcd:1111::/64

- 前缀：2001:468:abcd:1111

- 全球路由前缀：2001

- 子网标识：468

- 接口标识：abcd:1111

5. ::1/128

- 前缀：（省略）

- 全球路由前缀：（省略）

- 子网标识：（省略）

- 接口标识：1

### 6.4.3端口

端口的概念：

在计算机网络中，端口是用于标识应用程序或网络服务的逻辑门户。它允许多个应用程序在同一台设备上同时进行网络通信。每个端口都有一个唯一的数字，称为端口号，用于识别发送方和接收方之间的数据流。

众所周知的端口：

众所周知的端口是一些被标准化的端口号，用于特定的网络协议或应用程序。这些端口号在计算机网络中得到广泛使用，以便不同的设备可以互相识别和通信。

以下是一些常见的众所周知的端口及其对应的协议或应用程序：

- 21端口：用于FTP协议，用于文件传输。

- 23端口：用于Telnet协议，用于远程登录。

- 25端口：用于SMTP协议，用于发送电子邮件。

- 53端口：用于DNS协议，用于域名解析。

- 80端口：用于HTTP协议，用于Web服务器和浏览器之间的通信。

- 135端口：用于RPC（Remote Procedure Call，远程过程调用）协议，用于远程执行操作。

- 443端口：用于HTTPS协议，提供加密的Web通信。

动态端口：

除了众所周知的端口外，还有一些被称为动态端口的端口号范围。动态端口允许临时分配给应用程序或服务，以便它们可以在需要时与其他设备进行通信。

动态端口的范围通常是49152至65535（或在早期的一些操作系统中是1024至65535）。当应用程序或服务需要与其他设备进行通信时，操作系统会自动分配一个可用的动态端口。

动态端口提供了更大的灵活性和可扩展性，使得多个应用程序可以同时进行网络通信，而不会发生端口冲突。在网络通信结束后，动态端口会被释放并可以重新使用。

## 6.5计算机网络设备

### 6.5.1网络互连

网络互连的概念：

网络互连指的是将多个计算机网络连接在一起，并实现彼此之间的通信和数据交换。通过网络互连，不同的网络可以共享资源、提供服务和实现信息传输。

物理层互连：

物理层互连是指在网络中连接设备的物理连接。它涉及到使用传输媒体（如电缆）和连接器将计算机、路由器、交换机等设备相连。

例子：

- 使用以太网电缆连接两台计算机，以实现直接的点对点通信。

- 使用跨楼层的光纤电缆将两个交换机连接起来，以扩展局域网的范围。

数据链路层互连：

数据链路层互连是指在网络中将不同网络和设备连接在一起的操作。它基于物理层提供的物理连接，并负责确保数据在连接的设备之间可靠地传输。

例子：

- 使用交换机将多台计算机连接到局域网，交换机提供透明的数据传输和设备间的交换功能。

- 使用有线或无线连接将多个局域网连接起来，形成更大规模的网络。

网络层互连：

网络层互连涉及到将不同的网络通过路由器或三层交换机连接在一起，以实现不同网络之间的通信。它使用IP（Internet Protocol，因特网协议）进行数据交换和路由选择。

例子：

- 使用路由器将多个局域网连接成一个广域网（WAN），实现不同局域网之间的跨网段通信。

- 使用三层交换机将具有不同子网的多个局域网连接在一起，实现内部路由和分组转发。

互连设备网关：

互连设备网关是用于连接不同类型网络的设备，例如将局域网与因特网连接起来的设备。它可以实现不同网络之间的协议转换和数据交换。

### 6.5.2网络传输介质

有线传输介质：

有线传输介质指的是利用物理电缆或光纤等有线连接来传输数据的介质。

1. 屏蔽双绞线（STP）

- 概念：屏蔽双绞线由一对一对的导线组成，每对导线之间都有屏蔽层进行保护，以降低电磁干扰。

- 优点：提供良好的抗干扰性能，适用于长距离传输和高频率传输。

- 缺点：相对较高的成本和相对复杂的安装过程。

- 传输速率：最高可达10 Gbps。

- 使用场景：广泛应用于以太网和电话线路等数据和语音通信。

2. 非屏蔽双绞线（UTP）

- 概念：非屏蔽双绞线由一对一对的导线组成，每对导线之间没有屏蔽层。

- 优点：成本较低，安装简单方便。

- 缺点：较差的抗干扰性能，适用于较短距离的数据传输。

- 传输速率：根据等级不同，最高可达10 Gbps。

- 使用场景：广泛应用于家庭、办公场所的以太网和电话线路等短距离数据和语音通信。

3. 同轴电缆

- 概念：同轴电缆由中心导体、绝缘层、金属网屏蔽层和外部覆盖层组成。

- 优点：提供较高的传输速率和抗干扰性能，适用于长距离传输。

- 缺点：较大且笨重，安装和维护成本较高。

- 传输速率：最高可达10 Gbps。

- 使用场景：常用于电视有线信号、封闭电路监视等应用。

4. 光纤

- 概念：光纤是由光导纤维组成的细长柔性线缆，利用光信号传输数据。

- 优点：具备高带宽和远距离传输能力，抗干扰性强且安全性高。

- 缺点：相对较高的成本和对安装和维护技术的要求较高。

- 传输速率：可达数百 Gbps，甚至更高。

- 使用场景：广泛应用于长距离高速数据传输、通讯网络和数据中心等。

无线传输介质：

无线传输介质指的是利用无线电波、微波或红外线等无线信号来传输数据的介质。

1. 无线电波

- 概念：无线电波是一种无线传输介质，利用无线信号在空气中传输数据。

- 优点：无线覆盖范围广，适用于移动通信和广播电视等应用。

- 缺点：易受干扰和信号衰减，带宽有限。

- 传输速率：取决于使用的无线技术，一般可达几Mbps至几十Mbps。

- 使用场景：无线局域网（WLAN）、蓝牙、移动通信等。

2. 微波

- 概念：微波是指在高频段使用的无线传输介质，能够实现高速数据传输。

- 优点：传输速率高，抗干扰能力强，适用于长距离通信。

- 缺点：对天气条件敏感，需要建设传输设备和基站。

- 传输速率：可达数百Mbps至数Gbps。

- 使用场景：卫星通信、移动通信等。

3. 红外线

- 概念：红外线是一种电磁辐射，能够实现短距离的无线数据传输。

- 优点：安全性高，不容易受到外界干扰。

- 缺点：传输距离较短，需要视线传输。

- 传输速率：一般较低，通常在数百kbps至几Mbps之间。

- 使用场景：红外遥控、红外数据传输等。

### 6.5.3网卡

网卡的功能：

网卡，也被称为网络接口卡或网络适配器，是计算机与网络之间进行数据通信的关键组件。它使计算机能够发送和接收数据包，并与其他计算机或网络设备进行通信。网卡提供了计算机与网络之间的物理接口，将数据转换为适合在网络上传输的格式。

网卡的分类：

按传输速率分：

1. 万兆以太网卡（10 Gigabit Ethernet Card）：支持传输速率为10 Gbps的以太网。

2. 千兆以太网卡（Gigabit Ethernet Card）：支持传输速率为1 Gbps的以太网。

3. 快速以太网卡（Fast Ethernet Card）：支持传输速率为100 Mbps的以太网。

4. 以太网卡（Ethernet Card）：支持传输速率为10 Mbps的以太网。

按传输介质分：

1. 有线网卡：使用物理电缆（如双绞线、同轴电缆或光纤）进行数据传输。

2. 无线网卡：使用无线电波或红外线进行无线数据传输。

网卡的MAC地址：

每个网卡都有一个唯一的标识符，称为MAC地址（Media Access Control Address），它是一个由6组十六进制数字组成的48位地址。MAC地址用于在局域网中唯一标识网卡，并确保每个网卡具有独特的标识。

网卡的MAC地址结构及示例：

MAC地址由6组十六进制数字（0-9，A-F）组成，各组之间用冒号或短横线分隔。例如，00:0A:95:9D:68:16 或 00-0A-95-9D-68-16。

MAC地址的前三组（称为前缀部分）标识了网卡的制造商，而后三组（称为唯一识别部分）是由制造商分配的唯一标识。

示例：

前缀部分：00:0A:95

唯一识别部分：9D:68:16

通过MAC地址，网络设备可以确定数据包应该发送到哪个接收者，确保数据在局域网中准确传输。

以下是几个主流网卡的示例，这些网卡是在当前常见和流行的计算机和网络设备中广泛使用的：

1. 以太网卡示例：

- Intel Ethernet Server Adapter X710-DA2：支持10 Gbps的双口以太网卡，适用于服务器环境。

- Realtek PCIe Gigabit Ethernet Network Card：支持1 Gbps的PCIe接口千兆以太网卡，适用于桌面和小型企业网络。

2. 无线网卡示例：

- TP-Link Archer T9E AC1900 Wireless Dual Band PCI Express Adapter: 支持双频段（2.4 GHz和5 GHz）的无线网卡，提供高速无线连接。

- Intel Dual Band Wireless-AC 8265: 支持最新Wi-Fi标准，提供高速无线连接和较大的网络覆盖范围。

### 6.5.4中继转发设备

中继转发设备是一种用于扩展局域网（LAN）范围的网络设备。它的作用是接收来自一个网络段的数据包，并将其转发到另一个网络段中。中继转发设备可以工作在OSI模型的物理层或数据链路层。在物理层中，中继转发设备被称为中继器（repeater），它负责将信号放大并传输到远端。在数据链路层，中继转发设备可以是集线器（Hub）、网桥（bridge）或交换机（switch），它们通过学习和过滤数据帧来实现转发。

集线器（Hub）：

集线器是一种简单的局域网设备，用于连接多台计算机或其他网络设备，使它们可以共享数据。集线器工作在物理层，它会接收来自一个端口的数据包，并将其复制到所有其他端口上，实现广播的数据传输。然而，集线器无法区分转发和管理网络流量，因此在现代网络中已经被更先进的交换机所取代。集线器通常用于较小或简单的网络环境。

主流集线器示例：

1. TP-Link TL-SF1008D Fast Ethernet Switch：

- 描述：这是一款8端口的快速以太网集线器，支持10/100 Mbps的数据传输速率。

- 特点：简单的插拔式安装、自动MDI/MDIX功能、IEEE 802.3x流控制。

- 适用场景：小型办公室、家庭网络等简单网络环境。

2. NETGEAR GS108 8-Port Gigabit Ethernet Unmanaged Switch：

- 描述：这是一款8端口的千兆以太网集线器，支持10/100/1000 Mbps的数据传输速率。

- 特点：简单的即插即用安装、自动协商网络速度和数据流控制、全双工模式。

- 适用场景：小型企业、中小型办公室或家庭网络等需要高速连接的环境。

### 6.5.5网桥

网桥是一种用于连接多个网络段的设备，它工作在OSI模型的数据链路层。网桥通过学习和过滤数据帧的目的MAC地址，将数据帧从一个网络段转发到另一个网络段，实现不同网络段之间的互连。网桥能够在不同网络段之间实现流量控制和隔离，提高网络性能和可靠性。

网桥的功能：

1. 桥接（Bridging）：网桥能够连接两个或多个不同的局域网（LAN），并通过学习和过滤数据帧的MAC地址来转发数据。

2. 学习（Learning）：网桥会学习网络中不同主机的MAC地址，并将这些地址存储在转发表中。随着数据帧的传输，网桥会根据目的MAC地址在转发表中查找相应的端口并进行转发。

3. 过滤（Filtering）：网桥根据转发表中的信息过滤数据帧，只将数据帧转发到目标网络段的端口，并避免在不必要的网络段上广播。

4. 转发（Forwarding）：网桥能够实现数据帧从一个端口到另一个端口的转发，连接不同网络段。

主流网桥示例：

1. Cisco Catalyst 2960 Series Switches：这是思科公司生产的一系列企业级以太网交换机，支持网桥功能和多种网络协议。它们具有高性能、可靠性和可扩展性，适用于中大型企业网络。

2. HPE Aruba 2530 Series Switches：这是惠普企业（HPE）旗下的一系列网络交换机，支持网桥功能和灵活的网络管理。它们提供安全的企业级功能和可靠的性能，适用于中小型企业网络。

### 6.5.6网络交换设备

路由器：

路由器是一种网络设备，用于在广域网（WAN）或局域网（LAN）中实现数据包的转发和路由功能。它工作在网络层（第三层），能够根据目标IP地址选择最佳路径，并将数据包传递到正确的目标地址。路由器通过学习和更新路由表来确定数据包的转发策略，并支持各种网络协议。

路由器的功能：

1. 数据转发：根据路由表中的信息，将数据包从一个网络接口转发到另一个网络接口，以实现不同网络之间的互联。

2. 路由选择：通过路由协议，学习和交换路由信息，建立网络拓扑，并选择最佳路径来传递数据。

3. 网络隔离：将不同网络段划分为单独的子网，实现网络隔离和安全保护。

4. 流量控制：监控和控制网络流量，包括拥塞控制、流量优先级和负载平衡，以提高网络性能和稳定性。

主流路由器示例：

1. Cisco ISR 4000系列路由器：适用于大中型企业网络的集成服务路由器，提供高性能路由和多种连接方式，支持丰富的服务集成和高级安全功能。

2. Juniper Networks MX系列路由器：适用于大型企业和服务提供商，提供高度可扩展的路由和服务功能，并具备卓越的性能和安全性能。

交换机：

交换机是一种网络设备，用于在局域网（LAN）内实现数据帧的转发和交换。它工作在数据链路层（第二层），通过学习和转发数据帧的MAC地址，将数据包交付到目标设备。交换机能够提供高速、可靠和灵活的局域网连接。

交换机的功能：

1. 学习：学习并记录与每个接口关联的MAC地址，构建转发表以实现准确的数据帧转发。

2. 过滤：根据转发表中的信息，只将数据帧转发到目标MAC地址所在的接口，避免不必要的广播。

3. 转发：将数据帧通过交换机的端口迅速转发到目标设备，实现点对点的直接通信。

4. 虚拟局域网（VLAN）划分：支持VLAN的划分，将不同的设备分组到不同的虚拟网络中，实现流量隔离和安全性提升。

主流交换机示例：

1. Cisco Catalyst 9000系列交换机：适用于大中型企业网络的企业级以太网交换机，提供高性能、可扩展的局域网连接和先进的安全功能。

2. HPE Aruba 5400R zl2系列交换机：适用于中大型企业和服务提供商，提供高度可靠的网络连接和灵活的管理功能，支持高密度数据流量。

网关：

网关是将一个网络与另一个网络连接的设备，用于实现不同网络之间的互联通信。它可以是硬件设备（如路由器），也可以是软件程序。网关工作在不同的网络层和协议上，负责数据的路由和转换。

网关的功能：

1. 网络互连：连接不同类型的网络，如将局域网与互联网连接起来，实现不同网络之间的通信。

2. 协议转换：将一个协议的数据包转换为另一个协议的数据包，使不同网络之间能够互相通信。

3. 安全过滤：实施防火墙、VPN等安全策略，对数据进行过滤和保护，提高网络的安全性。

4. 地址转换：使用网络地址转换（NAT）技术，将私有IP地址转换为公有IP地址，实现内部网络与外部网络的通信。

主流网关示例：

1. Cisco ASR 1000系列路由器：集成了丰富的网关功能、高性能的路由功能和高级安全特性，适用于中大型企业网络。

2. Juniper Networks SRX系列网关：具备高度灵活和可扩展的网关功能，提供先进的安全特性和高性能的路由功能，适用于大型企业和服务提供商的网络环境。

### 6.5.7调制解调器

调制解调器：

调制解调器（Modem，调解器或简称为调制器）是一种用于将数字信号转换为模拟信号或将模拟信号转换为数字信号的设备。它在计算机和通信系统中起到重要的作用，用于在数字通信中传输数据。

调制解调器的功能：

1. 调制（Modulation）：调制器将数字数据转换为模拟信号的过程，将数字信号调制到载波信号上，以便在传输媒介（如电话线或电缆）上进行传输。

2. 解调（Demodulation）：解调器将模拟信号转换为数字信号的过程，将模拟信号还原为原始的数字数据。

3. 数模转换（Digital-to-Analog Conversion）：调制器将数字信号转换为模拟信号，以便在传输中传送。

4. 模数转换（Analog-to-Digital Conversion）：解调器将接收到的模拟信号转换为数字信号，以供计算机或其他数字设备处理。

主流调制解调器示例：

1. ADSL Modem：ADSL（Asymmetric Digital Subscriber Line）调制解调器是一种常见的家庭和办公室宽带接入设备，用于通过电话线进行高速上网。它将数字信号转换为模拟信号，并在电话线上进行传输。

2. Cable Modem：有线调制解调器是用于有线网络的调制解调器，通常与有线电视系统配合使用。它将数字信号转换为模拟信号，并将其发送到有线电视网络进行传输。

3. Dial-up Modem：拨号调制解调器是一种传统的调制解调器，通过电话线与拨号接入服务器连接。它将数字信号转换为模拟信号，并通过普通电话线进行数据传输。

## 6.6局域网与广域网技术

### 6.6.1局域网技术

IEEE 802标准局域网参考模型：

IEEE 802标准局域网参考模型包括三个主要层次：

3. 逻辑链路控制层（LLC，Logical Link Control）：提供透明的数据传输服务，负责错误检测和恢复，位于数据链路层之上。

2. 介质访问控制层（MAC，Media Access Control）：定义了访问共享介质的规则，决定了在共享介质上传输的顺序。

1. 物理层（Physical Layer）：负责将数据转换为物理信号，并传输到局域网的物理介质上。

IEEE 802标准局域网参考模型与OSI-RM的对应关系：

IEEE 802标准局域网参考模型与OSI-RM（开放系统互连参考模型）对应如下：

- 物理层（Physical Layer）对应于OSI-RM的物理层。

- 逻辑链路控制层（LLC）和介质访问控制层（MAC）对应于OSI-RM的数据链路层。

局域网的主要特点：

1. 局限性：局域网的覆盖范围通常仅限于一个建筑物或一个有限的地区。

2. 高带宽：局域网提供高速的数据传输，通常以千兆位/秒（Gbps）为单位。

3. 低延迟：局域网的延迟时间较低，因为数据传输距离相对较短。

4. 高效性：局域网使用专用的局域网技术和协议，提供高效的网络通信。

决定局域网特性的主要因素：

局域网的特性受以下主要因素的影响：

1. 传输介质：局域网可以使用不同的传输介质，如双绞线、同轴电缆、光纤等。传输介质的选择直接影响到局域网的带宽和传输速度。

2. 网络拓扑结构：局域网的拓扑结构决定了节点之间的连接方式。常见的拓扑结构有总线型、星型、环型和网状型等。

3. 介质访问控制方法：局域网使用不同的介质访问控制方法来管理多个节点对共享介质的访问。常见的方法包括CSMA/CD（载波监听多路访问/碰撞检测）、Token Passing（令牌传递）和Token Bus（令牌总线）等。

局域网的传输介质：

局域网可以使用多种传输介质，其中常见的包括：

- 双绞线：常用于以太网，可以分为未屏蔽双绞线（UTP）和屏蔽双绞线（STP）。

- 同轴电缆：常用于早期的10BASE2和10BASE5以太网。

- 光纤：提供更高的带宽和抗干扰能力，适用于高速以太网和光纤通信。

局域网的网络拓扑结构：

局域网可以采用多种网络拓扑结构，常见的有：

- 总线型拓扑：所有节点共享同一根传输线，如以太网的10BASE2和10BASE5。

- 星型拓扑：所有节点连接到一个中心节点（如交换机或集线器）。

- 环型拓扑：节点通过连接在一起的链路形成一个环，如令牌环网。

- 网状拓扑：每个节点都与其他节点直接连接，形成一个网状结构，如无线局域网。

局域网的介质访问控制方法（IEEE802.3，IEEE802.4，IEEE802.5）：

- IEEE 802.3：Ethernet标准，使用CSMA/CD（载波监听多路访问/碰撞检测）方法进行介质访问控制。

- IEEE 802.4：Token Bus标准，使用令牌传递（Token Passing）方法进行介质访问控制。

- IEEE 802.5：Token Ring标准，使用令牌传递（Token Passing）方法进行介质访问控制。

局域网的网络协议：

局域网使用各种网络协议来管理和控制数据的传输，常见的局域网协议有：

- Ethernet（以太网）：基于IEEE 802.3标准的局域网协议。

- Wi-Fi（无线局域网）：基于IEEE 802.11系列标准的无线局域网协议。

- Token Ring（令牌环网）：基于IEEE 802.5标准的局域网协议。

局域网的网络操作系统：

局域网使用各种网络操作系统来管理和控制网络中的计算机和设备，常见的局域网网络操作系统有：

- Windows Server：由微软开发的网络服务器操作系统，支持局域网管理和服务。

- Linux：开源操作系统，提供多种局域网管理工具和服务。

- macOS Server：由苹果公司开发的服务器操作系统，适用于苹果产品的局域网环境。

### 6.6.2典型局域网类型

1. 以太网（Ethernet）：

- 概念：以太网是一种最常见和广泛应用的局域网技术，采用CSMA/CD（载波监听多路访问/碰撞检测）介质访问控制方法。

- 传输介质：以太网使用不同的传输介质，包括双绞线、同轴电缆、光纤等。

- 100BASE-TX：采用双绞线（UTP或STP）作为传输介质，其中“100”表示传输速率为100 Mbps，“BASE”表示基带传输，“T”表示采用双绞线，“X“表示全双工工作方式。

- 100BASE-FX：采用光纤作为传输介质，其中“100”表示传输速率为100 Mbps，“BASE”表示基带传输，“F”表示光纤，“X“表示全双工工作方式。

- 100BASE-T4：采用4根双绞线（UTP或STP）作为传输介质，其中“100”表示传输速率为100 Mbps，“BASE”表示基带传输，“T”表示双绞线，“4“表示最大传输距离不超过400m。

2. 令牌环网（Token Ring）：

- 概念：令牌环网是一种基于令牌传递的局域网技术，节点通过传递令牌来访问共享介质。

- 传输介质：令牌环网使用光纤或双绞线作为传输介质。

- FDDI网（光纤分布式数据接口）：

- 概念：FDDI网是一种基于光纤的局域网技术，提供高带宽和高可靠性的数据传输。

- 传输介质：FDDI网使用光纤作为传输介质，支持双向传输。

### 6.6.3广域网技术

广域网（Wide Area Network，简称WAN）是一种连接远距离地理位置的计算机网络，可覆盖大片区域，常用于连接城市、国家或跨国的网络，涉及物理层，数据链路层，网络层。下面是典型广域网技术的介绍：

1. 公共电话网（Public Switched Telephone Network，简称PSTN）：公共电话网是一种传统的电话通信系统，用于连接电话用户并提供音频通信服务。这种网络使用传统的电话线路进行连接，通过交换机完成呼叫路由和电话号码转换等功能。

2. 综合业务数字网（Integrated Services Digital Network，简称ISDN）：综合业务数字网是一种数字通信网络技术，可以在单个传输线路上同时传输语音、数据和视频等不同类型的信息。ISDN提供了多种通信服务，包括电话、传真和数据传输等。

3. 非对称数字用户线路（Asymmetric Digital Subscriber Line，简称ADSL）：非对称数字用户线路是一种常用于家庭和小型企业的宽带接入技术。它通过普通的电话线路传输数据，提供了高速的下载速度和相对较低的上传速度。ADSL适用于对下载速度要求较高的应用，如视频流媒体和大文件下载。

4. 数字数据线（Digital Data Service，简称DDS）：数字数据线是一种提供低速数字数据传输的广域网连接服务。它使用专用的数字传输设备和电缆，通常用于连接远程办公地点、自动柜员机和数据采集设备等。

5. 帧中继（Frame Relay）：帧中继是一种广域网传输技术，涉及OSI模型数据链路层，用于在高速数字线路上传输数据。它将数据分割为较小的帧进行传输，并通过网络交换机进行路由和转发。帧中继提供了高效的传输和连接管理功能，可用于连接远程办公地点和分支机构等。

## 6.7Internet

### 6.7.1Internet的起源与发展

Internet是当今世界上最大的计算机网络，它的起源可以追溯到1969年的美国。下面是关于Internet的起源与发展的专业回答：

Internet起源：

Internet的起源可以追溯到美国国防部高级研究计划局（ARPA）在20世纪60年代末的一项研究计划，即ARPANET。ARPANET的初衷是为科学家和研究机构之间提供一种分布式的通信方式，以便共享计算资源和研究成果。1969年，ARPANET在美国加州的四个大学之间建立了第一个分组交换网络，这被认为是Internet的雏形。

Internet发展：

随着时间的推移，ARPANET逐渐发展为一个更大、更复杂的网络系统，吸引了更多的研究机构和大学加入。1980年代初，TCP/IP（Transmission Control Protocol/Internet Protocol）协议成为连接ARPANET和其他网络的标准。这一协议的设计使得不同类型的计算机网络得以相互连接，形成一个更大的网络，即Internet。

随着时间的推移，Internet经历了快速的发展和扩张。1990年代初，万维网（World Wide Web）的出现使得Internet变得更加普及和易用。万维网是一种基于超文本传输协议（HTTP）的信息系统，通过统一资源定位符（URL）和超文本标记语言（HTML）等技术，将各种信息资源连接在一起，形成了一张全球性的信息网络。

1990年代中期以后，商业互联网服务提供商的兴起进一步推动了Internet的普及和商业化。人们开始使用Internet进行电子邮件、网上购物、社交媒体等各种在线活动。

到了21世纪，移动互联网的快速发展使得通过移动设备访问Internet成为现实。无线网络技术的进步以及智能手机和平板电脑的普及，使得人们可以随时随地与Internet连接，并享受丰富的在线服务和应用。

总结：

Internet作为全球性的计算机网络，起源于1969年的ARPANET项目，并经过多年的发展和演变。它的普及得益于TCP/IP协议的标准化、万维网的出现以及商业互联网服务的兴起。如今，Internet已经成为连接世界各地的人们、组织和设备的重要基础设施，为各种在线活动和信息交流提供支持。

### 6.7.2域名系统DNS

域名系统（Domain Name System，简称DNS）是互联网中用于将域名（例如www.example.com）转换为IP地址（例如192.0.2.1）的分布式命名系统。下面是对DNS的专业解释：

DNS的作用：

DNS的主要作用是将易于记忆的域名转换为计算机可识别的IP地址。在互联网上，每个设备都需要一个唯一的IP地址来进行通信，而IP地址是由一串数字组成的，对人们来说很不直观和难以记忆。因此，通过DNS，我们可以使用例如www.example.com这样的域名来访问网站，而不需要记住对应的IP地址。

DNS的分层结构：

DNS采用了分层的结构，由多个DNS服务器组成。它分为多个层级，最顶层是根域名服务器，接下来是一些顶级域名服务器（例如.com、.org等），然后是二级域名服务器，以此类推，直到最底层的本地域名服务器。

DNS查询过程：

当用户在浏览器中输入一个域名时，DNS会完成域名解析的过程，将域名转换为对应的IP地址。这个过程通常包括以下步骤：

1. 本地域名服务器查询：首先，浏览器会向本地域名服务器发送一个域名查询请求。

2. 递归查询：如果本地域名服务器不知道域名对应的IP地址，那么它会向根域名服务器发起递归查询，询问顶级域名服务器的IP地址。

3. 迭代查询：根域名服务器会返回顶级域名服务器的IP地址给本地域名服务器，然后本地域名服务器再向顶级域名服务器发起迭代查询，询问二级域名服务器的IP地址。

4. 迭代查询的过程会一直往下进行，直到找到负责该域名的域名服务器，返回对应的IP地址给本地域名服务器。

5. 本地域名服务器将IP地址返回给浏览器，浏览器可以根据该IP地址发起网络请求，并与目标服务器进行通信。

DNS缓存：

为了加快DNS查询的速度，DNS还采用了缓存机制。当本地域名服务器解析完一个域名后，会将得到的IP地址保存在缓存中一段时间，下次再查询同样的域名时可以直接使用缓存中的IP地址，避免重复的查询过程。

### 6.7.3信息浏览服务（WWW）

WWW（World Wide Web）是互联网上的一个信息浏览服务，它基于超文本和互联网技术，使得用户可以通过浏览器访问和浏览各种信息资源。下面是对WWW中相关术语的专业解释：

超文本（Hypertext）：

超文本是一种通过文本之间的链接实现非线性连接的信息展示方式。它允许文本中包含指向其他文档或资源的链接，用户可以通过点击链接跳转到其他相关内容。超文本一般使用超链接（Hyperlink）来实现文本之间的关联。

主页（Homepage）：

主页是一个网站的起始页面，也是网站的入口。它通常包含网站的导航菜单、重要内容的简介、搜索框、最新动态等信息，可以帮助用户快速了解并访问网站的其他页面和资源。

超文本传输协议（HTTP）：

超文本传输协议是WWW中用于在客户端和服务器之间传输超文本数据的一种协议。它基于请求-响应模式，客户端通过发送HTTP请求向服务器请求某个资源，服务器则通过发送HTTP响应返回请求的资源。HTTP通过使用URL来指定资源的位置，并支持各种请求方法（如GET、POST等）和状态码来进行交互。

统一资源定位器（URL）：

统一资源定位器是在WWW中用于标识和定位资源的一种标准化格式。URL由多个部分组成，包括协议（如HTTP、HTTPS）、主机名、端口号（可选）、路径、查询字符串和片段标识等。它提供了一种统一的方式来表示网站、页面和其他资源的地址。

通过WWW，用户可以使用浏览器访问和浏览各种网站、页面和文档。超文本技术使得用户可以方便地跳转和浏览相关内容，HTTP协议负责实现客户端和服务器之间的数据传输，URL则用于标识和定位资源的位置。

### 6.7.4FTP服务

FTP（File Transfer Protocol，文件传输协议）是一种用于在计算机网络上进行文件传输的标准协议。下面是对FTP服务的专业解释：

FTP的作用：

FTP旨在简化和加速文件的传输，允许用户在客户端和服务器之间进行文件的上传和下载。通过FTP，用户可以通过网络将文件从一个计算机传输到另一个计算机，无论这两台计算机处于同一局域网内还是位于远程地理位置。

FTP的工作原理：

FTP使用客户端-服务器模型进行文件传输。客户端是发送或接收文件的一方，服务器是存储和提供文件的一方。

FTP连接：

客户端和服务器之间的FTP连接是通过TCP/IP协议建立的。客户端使用标准的FTP客户端软件（如FileZilla、WinSCP等）与FTP服务器建立连接，然后进行文件传输操作。

FTP命令和响应：

在FTP连接的过程中，客户端可以向服务器发送各种FTP命令，包括登录认证、浏览目录、上传文件、下载文件等。服务器则根据收到的命令作出响应，返回相应的状态码和消息。

FTP模式：

FTP支持两种传输模式：主动模式和被动模式。在主动模式中，客户端建立数据连接，并告知服务器它将会使用的端口号。在被动模式中，服务器主动打开一个监听端口，等待客户端的连接请求。主动模式在服务器防火墙后更易于配置，而被动模式在客户端防火墙后更易于配置。

FTP安全性：

由于FTP使用明文传输数据，所以存在安全性的风险。为了增加安全性，可以使用安全的FTP协议，例如FTPS（基于SSL/TLS加密）或SFTP（基于SSH加密）来进行文件传输。

FTP广泛应用于各种场景，包括网站维护、文件共享、软件更新等。通过FTP，用户可以方便地将文件上传到服务器或从服务器下载文件，实现快速和可靠的文件传输

### 6.7.5电子邮件服务（E-mail）

电子邮件（E-mail）是一种通过计算机网络进行电子信息传输的服务。下面是对电子邮件服务相关概念和协议的专业解释：

电子邮件的概念：

电子邮件是一种通过互联网传输和交换电子信件的方式，它允许用户在全球范围内快速、便捷地发送和接收邮件。电子邮件可以包含文本、图片、附件等多种形式的信息内容。

简单邮件传输协议（SMTP）：

SMTP是用于发送电子邮件的主要协议。它定义了邮件的传输方式、邮件的编码格式以及与邮件服务器之间的通信方式。SMTP客户端向SMTP服务器发送邮件，SMTP服务器负责将邮件传递给目标服务器或收件人。

邮局协议（POP）：

POP是一种接收邮件的协议，它定义了客户端和邮件服务器之间的通信方式。POP允许用户通过POP客户端从邮件服务器上下载邮件到本地设备，然后在本地设备上进行查看和管理。

因特网信息访问协议（IMAP）：

IMAP也是一种接收邮件的协议，它与POP类似，但提供更多的功能。IMAP允许用户在邮件服务器上管理邮件，包括查看、搜索、标记、删除等操作。IMAP客户端通常保留邮件服务器上的副本，使得用户可以从不同的设备上访问和管理同一份邮件。

多用途网际邮件扩展协议（MIME）：

MIME是一种扩展协议，用于支持在电子邮件中传输不同类型的数据和文件附件。MIME允许邮件中嵌入图片、音频、视频等多媒体内容，并通过Base64编码进行传输。

电子邮件的地址：

电子邮件地址通常由两个部分组成：用户名和域名。用户名是邮件地址的唯一标识符，域名指定了邮件服务器的地址。例如，"username@example.com"是一个典型的电子邮件地址。

电子邮件的地址格式：

标准的电子邮件地址格式通常为"user@domain.com"。@前为用户部分，用户部分可以包含字母、数字以及一些特殊字符，@后为域名部分，域名部分则指定了邮件服务器的地址。

电子邮件的信息格式：

电子邮件的主体部分通常由邮件头和邮件体组成。邮件头包含了邮件的一些元信息，例如发件人、收件人、主题、日期等；邮件体则是邮件的主要内容，可以包含文本、HTML格式的内容、附件等。

主流电子邮件软件：

目前，有许多主流的电子邮件软件供用户选择，包括Microsoft Outlook、Gmail、Mozilla Thunderbird、Apple Mail等。这些软件提供了丰富的功能，支持电子邮件的发送、接收、管理、搜索等操作。

通过电子邮件服务，用户可以方便地进行电子邮件的发送和接收，快速地与他人进行沟通和信息交流。

### 6.7.6远程登陆服务与查询服务

远程登录服务：

远程登录服务允许用户通过网络从本地计算机访问和控制远程计算机。用户可以使用远程登录协议（如SSH、RDP、VNC等）建立与远程计算机的连接，并获得类似于直接操作远程计算机的体验。

远程登录服务的作用：

远程登录服务的主要作用是提供远程访问和管理远程计算机的能力。通过远程登录，用户可以在不同的地理位置使用远程计算机，无论是远程办公、远程教学，还是远程维护，都可以借助远程登录服务进行操作和控制。

常见的远程登录服务协议：

- SSH（Secure Shell）：SSH是一种加密的远程登录协议，用于安全地远程访问和操作命令行界面的远程计算机。

- RDP（Remote Desktop Protocol）：RDP是微软开发的远程桌面协议，用于远程访问和控制具有图形界面的远程Windows计算机。

- VNC（Virtual Network Computing）：VNC是一种远程视窗协议，允许用户显示和操作远程计算机上的图形界面。

查询服务：

查询服务提供了一种查询机制，用户可以向目标服务发送查询请求，获得特定域的相关信息。查询服务常用于域名查询、IP地址查询、DNS查询等。

常见的查询服务协议和应用：

- DNS（Domain Name System）：DNS是一种查询服务协议，用户可以通过DNS解析域名，获取对应的IP地址和其他与域名相关的信息。

- WHOIS：WHOIS是一种查询服务协议，用于查询域名的注册信息，包括域名所有者、注册商、联系信息等。

- IP地址查询：用户可以使用IP地址查询服务，通过输入IP地址获取与之相关的信息，如IP地址的地理位置、运营商等。

网页快照：

网页快照是指对网页内容进行截图或快照拍摄，以便在后续时间进行查看或备份。网页快照可以记录网页在某一时刻的实际呈现效果，并保存网页的内容和布局。

对于查询服务，有一种特殊的查询服务称为网页快照服务或网页存档服务。这种服务会定期抓取和存储网页的快照，以便用户在未来可以访问和查看已存储的网页快照，即使原始网页已经变动或无法访问。常用的网页快照服务包括互联网档案馆（Internet Archive）和Wayback Machine。

通过远程登录服务，用户可以方便地远程访问和操作远程计算机。查询服务则提供了一种查询机制，使得用户可以获取特定域的相关信息，如域名的IP地址、注册信息等。而网页快照服务允许用户在任何时间点查看保存的网页快照，以便进行历史记录和备份。

### 6.7.7即时通信

即时通信的概念：

即时通信是一种通过计算机网络实现实时交流的服务。它允许用户通过文本、语音、图像或视频等多种形式进行即时交流，无论对方与自己在同一地理位置还是远隔千里。

网上聊天室：

网上聊天室是一种提供多人实时聊天功能的网络平台。用户可以通过加入不同的聊天室与其他用户进行群聊或私聊，实现实时文本交流。

网上寻呼：

网上寻呼是一种类似于传呼机的服务，用户可以通过网络发送文字消息给其他用户，并通过弹窗、推送等形式进行即时提醒。

IP电话：

IP电话是一种基于互联网协议（IP）进行语音通话的技术。与传统的电话系统不同，IP电话将语音数据转换为数字信号，并通过互联网进行传输。

电子公告牌：

电子公告牌是一种在线交流平台，用户可以在其中发布文本、图片、链接等信息，并与其他用户进行交流和讨论。电子公告牌通常以论坛的形式存在，提供了特定主题或领域的讨论区。

微博：

微博是一种社交媒体平台，用户可以在其中发布短文本消息，分享观点、新闻、图片等内容。微博用户可以关注其他用户，以便获取其发布的消息和动态。

QQ：

QQ是一个即时通信软件平台，提供了实时聊天、语音通话、视频通话、文件传输等功能。用户可以通过QQ建立联系，进行一对一或多人聊天，并通过QQ空间发布动态、分享照片等。

微信：

微信是一款移动端即时通信软件，提供了文本、语音、视频、图片等多种交流形式。用户可以通过微信与其他用户进行聊天、打电话、发红包等，并可以关注公众号、加入微信群等拓展社交关系。

以上即时通信服务为用户提供了快速、方便和互动性强的沟通方式，使人们能够实时交流、分享信息和建立社交网络。

### 6.7.8Internet上的新型服务

Internet上出现了许多新型服务，以下是有关云计算、大数据、数据挖掘、区块链和数字支付的专业解释：

云计算：

云计算是一种基于互联网的服务模式，通过虚拟化技术将计算资源、存储资源和应用程序提供给用户。云计算服务提供了按需获取和管理计算资源的能力，用户可以根据需求灵活使用资源并实现按需付费。

大数据：

大数据是指规模庞大、类型多样、高速增长的数据集合。大数据服务通过应用相关技术和工具，处理、存储、分析和可视化大数据，从中获得有价值的洞察和决策支持。

数据挖掘：

数据挖掘是从大数据中发现隐藏模式、关联和趋势的过程。它包括数据清洗、特征选择、模型构建、模型评估等技术和流程，以提取有用的知识和信息。

数据挖掘的功能：

- 分类：通过构建模型，将数据分为不同的类别或标签。

- 预测：基于历史数据，使用模型预测未来事件或趋势。

- 关联分析：寻找数据中的相关关系，如购物篮分析、协同过滤等。

- 聚类分析：将数据分成多个群组，每个群组内的数据相似。

数据挖掘的技术：

- 机器学习：使用算法和模型自动发现数据中的模式。

- 自然语言处理：分析和处理自然语言文本，抽取有用的信息。

- 图像处理：处理和分析图像数据，例如物体识别、图像分类等。

数据挖掘的流程：

- 数据准备：收集、清洗和集成数据，以便进行后续分析。

- 特征选择：选择对建模有意义的特征。

- 模型构建：选择合适的算法和模型，建立预测模型。

- 模型评估：评估模型的准确性和可靠性。

- 结果解释：解释模型的结果并提取有用的知识。

区块链：

区块链是一种去中心化的分布式账本技术，通过加密算法确保数据的安全性和可信度。区块链服务提供了可靠的数据存储和交易机制，被广泛应用于加密货币、合同管理、供应链追溯等领域。

数字支付：

数字支付是基于互联网的电子支付系统，用户可以使用电子钱包、移动支付应用等进行在线支付和电子货币交易。数字支付服务提供了快速、安全和便捷的支付和转账功能。

以上是关于云计算、大数据、数据挖掘、区块链和数字支付的专业解释。这些新型服务推动了互联网的发展，为用户和企业创造了更多的便利和创新机会。

### 6.7.9物联网

概念：

物联网是由各种传感器、设备和对象组成的网络，它们通过互联网进行通信和数据交换，实现智能化、自动化和互操作性。物联网将现实世界中的物理对象与数字系统相连接，实现对物体、环境和人的感知、交互和控制。

特点：

1. 异构性：物联网中的设备和对象多样性，涵盖了各种不同类型和技术的传感器、执行器和通信设备。

2. 互连性：物联网通过互联网连接设备，实现设备之间的相互通信和数据交换。

3. 自组织性：物联网中的设备可以自动组网和配置，实现自动发现和自动适应环境的能力。

4. 实时性：物联网需要实时处理和传输数据，以支持实时监测、反馈和决策。

5. 安全性：物联网中的设备和数据需要保护，以防止未经授权的访问和数据泄露。

分层：

物联网通常可以划分为三个主要层级：

3. 应用层：应用层是物联网的上层，包括数据分析、决策支持、应用开发和用户界面等功能。

2. 网络层：网络层负责将感知层中的设备连接到互联网，并提供通信和数据传输的功能。

1. 感知层：感知层包括各种传感器、执行器和物理设备，用于收集环境、物体和人的数据。

关键领域：

物联网在许多领域都有广泛应用，包括但不限于以下领域：

1. 工业领域：工业物联网可以实现智能制造、设备监控、远程维护等，提高生产效率和运营效率。

2. 城市领域：智慧城市利用物联网技术，实现智能交通、智能能源管理、环境监测、公共安全等。

3. 农业领域：农业物联网应用于农作物监测、智能灌溉、畜牧管理等，提高农业生产效益和资源利用率。

4. 医疗健康领域：医疗物联网实现了远程监护、智能医疗设备、健康管理等，提供了更好的医疗服务和健康管理手段。

实际应用：

实际应用包括但不限于以下方面：

1. 智能家居：物联网技术使得家庭设备和家居环境智能化，如智能家电、智能安防、智能照明等。

2. 智能交通：应用物联网实现智能交通管理、智能车辆和选路导航等，提高交通效果和安全性。

3. 智能能源：物联网应用于能源监测、节能管理和可再生能源集成，实现智能能源系统。

4. 智慧零售：物联网技术在零售业中应用，实现智能货架、智能支付、智能价格调整等。

以上是对物联网的概念、特点、分层、关键领域和实际应用的专业解释。物联网作为一种新兴技术，为各个行业带来了创新和改变，并有着广阔的发展前景。

# 第七章

第七章

7.1信息安全基础知识

7.1.1信息安全的概念

7.1.2信息安全级别

7.1.3信息安全面临的威胁与破坏信息系统的方式

7.1.4数据加密技术

7.1.5身份认证技术

7.1.6访问控制技术

7.1.7信息隐藏技术

7.2 网络安全基础知识

7.2.1 网络安全目标与特征

7.2.2 局域网攻击

7.2.3 广域网攻击

7.2.4 防火墙技术

7.2.5虚拟专用网络（VPN）

7.2.6黑客

7.2.7 预防黑客攻击

7.2.8木马

7.3 计算机病毒

7.3.1 计算机病毒的定义与特点

7.3.2计算机病毒的分类

7.3.3计算机病毒的传播途径与预防

7.3.4常见的计算机病毒

7.3.5计算机病毒的检测与清除

7.4网络道德

7.4.1网络道德的定义和原则

7.4.2网络犯罪

7.5知识产权与计算机软件产权

7.5.1知识产权

7.5.2计算机软件产权

## **7.1信息安全基础知识**

### **7.1.1信息安全的概念**

信息安全是指保护信息系统和其中的数据免受未经授权的访问、使用、披露、破坏、干扰或篡改的措施。以下是信息安全中的一些概念和例子：

1. 实体安全

- 概念：实体安全是指保护物理资源和设施免受未经授权的访问、损坏或破坏。

- 例子：安全门禁系统、视频监控系统、生物识别技术（如指纹、面部识别）等。

2. 软件安全

- 概念：软件安全是指保护计算机软件免受未经授权的访问、恶意代码和漏洞利用等威胁的措施。

- 例子：防病毒软件、防火墙、加密软件、漏洞扫描工具等。

3. 数据安全

- 概念：数据安全是指保护数据免受未经授权的访问、泄露、修改、损坏或销毁。

- 例子：数据加密技术、访问控制机制、数据备份和恢复方案等。

信息安全的四大要素

1. 技术：

- 概念：技术是信息安全的基础，包括硬件和软件的安全措施和防护机制。

- 示例：防火墙、入侵检测系统（IDS）、加密技术、访问控制、安全审计等。

- 作用：技术层面的安全措施能够帮助保护系统和数据免受攻击和恶意行为。

2. 制度：

- 概念：制度是指组织内部建立的一系列规章制度和信息安全政策。

- 示例：信息安全政策、用户权限管理、风险评估和管理、安全培训等。

- 作用：通过制度的规范和约束，确保组织内部的信息安全得以实施和遵守。

3. 流程：

- 概念：流程是指一系列标准化的操作活动和管理流程，有助于保障信息的安全。

- 示例：安全审计程序、事件响应计划、备份和恢复流程、变更管理等。

- 作用：流程的规范化和执行确保了信息安全控制按照一定的步骤和流程进行。

4. 人：

- 概念：人作为信息安全的最重要要素，指的是组织内部的员工、用户和相关人员。

- 示例：员工的安全意识培训、授权和身份验证、安全责任和意识教育等。

- 作用：人的因素在信息安全中起着决定性的作用，他们的行为和决策能够直接影响信息资产的安全性。

这四大要素相互关联，共同构成了一个综合的信息安全体系。技术、制度和流程为信息安全提供了技术和管理上的支持，而人的因素则是信息安全实施的重中之重，他们作为实际操作者和最终用户，需具备一定的安全意识和责任。通过综合考虑和综合使用这四大要素，组织可以建立强大的信息安全能力，并保护其重要资产和机密信息免受威胁。

信息安全特征

信息安全的特征描述了保护信息系统和数据所需的属性和功能。以下是信息安全的特征和对应的概念和例子：

1. 可靠性（Reliability）：

- 概念：信息系统能够提供正确和一致的结果，并在需要时持续可用。

- 示例：一个可靠的系统能够防止数据丢失、硬件故障或其他错误导致的中断或损坏。

- 破坏特征的行为：恶意软件、硬件故障、数据损坏或传输错误等可能破坏系统的可靠性。

2. 可用性（Availability）：

- 概念：信息系统在需要时可用并能够正常工作。

- 示例：用户能够在任何时间和任何地点访问所需的信息资源。

- 破坏特征的行为：拒绝服务攻击、系统故障、网络中断或不可预料的事件可能会降低系统的可用性。

3. 保密性（Confidentiality）：

- 概念：信息只能被授权的个体访问和阅读，对未经授权者保持秘密。

- 示例：敏感数据仅限于被授权的人员访问，例如加密通信、访问控制和身份验证。

- 破坏特征的行为：未经授权的访问、信息泄露或窃取、监听或侵入可能破坏保密性。

4. 可控制性（Integrity）：

- 概念：保护信息免受未经授权的修改、删除或篡改。

- 示例：确保数据在传输、存储和处理过程中保持完整性，通过校验和、加密、数字签名等方式实现。

- 破坏特征的行为：数据篡改、未经授权的数据修改、恶意软件感染等可能破坏可控制性。

5. 可审查性（Accountability）：

- 概念：能够追溯和验证操作行为，确定事件的发生及相关责任。

- 示例：记录和监控系统中发生的事件和操作，并提供审计日志和审计功能。

- 破坏特征的行为：未经授权的访问、篡改审计记录或日志、隐蔽行为等可能破坏可审查性。

6. 不可抵赖性（Non-repudiation）：

- 概念：确保参与方不能否认已完成的操作或交易。

- 示例：使用数字签名或时间戳等技术来确保交易的不可抵赖性，以防止参与方否认其行为。

- 破坏特征的行为：伪造数字签名、否认参与交易、篡改时间戳等可能破坏不可抵赖性。

7. 完整性（Authenticity）：

- 概念：确保所传输或存储的信息在传输过程中没有被篡改或损坏。

- 示例：使用加密技术、消息摘要或数字签名来验证数据的完整性。

- 破坏特征的行为：未经授权的数据修改、数据损坏、篡改数字签名等可能破坏完整性。

信息安全的工作目的

1. 访问控制机制（进不来）：

- 概念：访问控制是一种保护系统资源免受未经授权访问的安全机制。

- 示例：使用密码、用户身份验证、访问许可和权限控制等技术和方法，限制只有授权用户可以进入系统或访问特定资源。

- 作用：确保只有授权的用户可以进入系统或访问特定资源，防止未经授权的访问和恶意行为。

2. 授权机制（拿不走）：

- 概念：授权是指授予用户或实体特定的权限和访问权限。

- 示例：管理员可以授权用户访问特定的文件夹或执行特定的操作，如读取、写入或修改数据。

- 作用：通过授权机制，确保只有获得授权的用户可以执行特定的操作或访问特定的资源。

3. 加密机制（看不懂）：

- 概念：加密是将明文转换为密文的过程，以防止未经授权的人可读取内容。

- 示例：使用加密算法和密钥将数据加密，只有正确的密钥才能解密并还原为可读的明文。

- 作用：通过加密机制，确保敏感数据的机密性，使其对未经授权的人员保持不可读状态。

4. 数据完整性鉴别机制（改不了）：

- 概念：数据完整性鉴别是通过校验和、数字签名等方法，保证数据在传输或存储过程中没有被篡改或损坏。

- 示例：使用哈希函数生成数据的校验和，在传输或存储过程中重新计算校验和来验证数据的完整性。

- 作用：通过数据完整性鉴别机制，确保数据在传输和存储过程中不被篡改，防止数据的不完整性和损坏。

5. 审计、监控和防抵赖（走不脱）：

- 概念：审计、监控和防抵赖是指跟踪和记录系统的操作活动，并提供可追溯性和证据的能力。

- 示例：记录用户登录日志、操作日志、审计操作，并使用数字签名和时间戳来确保操作的不可抵赖。

- 作用：通过审计、监控和防抵赖，可以追踪和监控系统的操作活动，形成可靠的证据，并防止操作的否认和抵赖。

以上工作目的的措施是信息安全的重要组成部分，通过合理的设计和实施，可以提供综合的保护措施，确保系统和数据的安全性。这些措施相互关联，共同作用，以保障信息安全的完整性、保密性、可用性和可靠性。

### 7.1.2信息安全级别

1. 文件保护级别：

- 概念：文件保护级别是根据信息的重要性和敏感性对文件进行分类和标记，以决定其安全保护措施和访问控制权限。

- 示例：以下是常见的文件保护级别：

- 绝密（Top Secret）：包含国家安全和最高机密信息，只能被授权人员访问。例如，政府军事计划文件。

- 机密（Confidential）：涉及重要的保密信息，只能被特定授权人员访问。例如，商业机密合同文件。

- 秘密（Secret）：包含敏感但不太重要的信息，仅限授权人员访问。例如，内部研究报告。

- 非密但敏感（Sensitive Unclassified）：不被明确定义为机密级别，但包含敏感信息，需要限制访问。例如，员工薪资表。

- 无密（Unclassified）：非敏感信息，没有特定访问限制。例如，公司公开发布的新闻稿。

2. 安全保护级别：

- 概念：安全保护级别是根据对信息系统的保护需求，划分不同层次的安全控制要求和技术规范。

- 示例：以下是常见的安全保护级别：

- 自主保护级（最低级）：用户自行选择和实施安全控制措施，缺乏集中的管理和监控。例如，个人电脑上的基本防火墙和密码保护。

- 指导保护级：提供基本的安全控制指导和建议，但实施由用户自行决定。例如，企业提供的安全最佳实践指南。

- 监督保护级：通过集中的监控和管理，确保安全控制的合规性和有效性。例如，企业内部的安全运维团队负责监控和响应安全事件。

- 强制保护级：强制执行固定的安全控制措施和规则，无法被绕过。例如，军事系统中的强制访问控制机制。

- 专控保护级（最高级）：最高级别的安全保护，需要高度专业化的设备和控制手段，严格限制访问和操作。例如，核能研究设施。

以上是信息安全级别中文件保护和安全保护级别的概念和示例。不同级别的文件保护和安全保护要求根据组织需求和信息的重要性来确定，以确保信息的机密性、完整性和可用性。

### **7.1.3信息安全面临的威胁与破坏信息系统的方式**

被动攻击：

被动攻击是指攻击者在不干扰正常通信的情况下，以获取目标系统或数据的敏感信息为目的。

1. 信息截获（Information Interception）：攻击者截获通信数据的一部分或全部，以获取敏感信息。例如，黑客通过中间人攻击截获用户的登录凭证，从而窃取账户信息。破坏了保密性。

2. 窃听（Eavesdropping）：攻击者监听和记录通信内容，以获取敏感信息。例如，黑客监听无线网络上的数据流量，窃取用户发送的敏感数据。破坏了保密性。

3. 监听（Interception）：攻击者拦截和复制数据流，以获取敏感信息。例如，黑客拦截网络传输的数据包，获取包含敏感信息的文件。破坏了保密性。

4. 嗅探（Packet Sniffing）：攻击者截获数据包并分析其中的信息，以获取敏感信息。例如，黑客使用嗅探软件截获网络数据包，获取用户的个人信息。破坏了保密性。

5. 信息收集（Information Gathering）：攻击者收集目标系统或个人的信息，以便进一步攻击。例如，黑客收集社交媒体上的个人信息，用于社会工程攻击。破坏了保密性。

6. 流量分析（Traffic Analysis）：攻击者分析网络通信模式和流量，以得出敏感信息。例如，黑客分析用户的网络流量模式，推断出用户的在线行为习惯。破坏了保密性。

主动攻击：

主动攻击是指攻击者主动干扰目标系统或通信，目的是破坏、篡改或非法获取信息。

1. 拒绝服务（Denial of Service，DoS）：攻击者通过发送大量请求或占用系统资源，使目标系统无法提供正常的服务。例如，黑客发动DDoS攻击，使目标网站无法响应合法用户的请求。破坏了可用性。

2. 分布式拒绝服务（Distributed Denial of Service，DDoS）：攻击者通过多个来源同时发动拒绝服务攻击，增加攻击力度和难以阻止。例如，黑客控制大量僵尸计算机（Botnet），一起发动对目标系统的拒绝服务攻击。破坏了可用性。

3. 信息篡改（Information Tampering）：攻击者对传输的数据进行修改，以改变信息的内容或影响其可信度。例如，黑客篡改数据包中的订单信息，导致错误的商品邮寄或付款。破坏了完整性。

4. 信息重放（Information Replay）：攻击者复制和重播已捕获的通信数据，以达到欺骗或非法访问的目的。例如，黑客重放一段网络通信，以获取认证凭证或执行未经授权的操作。破坏了完整性。

5. 信息伪造（Information Forgery）：攻击者制造虚假信息，以冒充合法用户或欺骗系统。例如，黑客伪造电子邮件发送者的身份信息，以获得目标用户的信任并获取敏感信息。

6. 信息中断（Information Interruption）：攻击者中断或破坏网络通信，使目标系统无法正常运行。例如，黑客通过破坏关键网络设备或网站服务器，使其无法提供服务。破坏了可用性。

7. 旁路控制（Side-channel Attacks）：攻击者利用系统实现上的弱点，如电磁辐射、功耗分析等，窃取敏感信息。例如，黑客通过分析设备的电源消耗来推断出密码。破坏了可审查性。

8. 抵赖（Repudiation）：攻击者在完成某个操作后否认其参与或行为，以逃避责任。例如，黑客篡改数据库中的日志记录，以否认他们的非法访问。破坏了不可抵赖性。

9. 假冒（Spoofing）：攻击者伪造或篡改网络数据的来源，以冒充合法用户或系统。例如，黑客使用IP地址欺骗技术伪装成合法网站，骗取用户的登录凭证。破坏了保密性。

10. 网络钓鱼（Phishing）：攻击者通过伪装成合法实体（如银行、社交媒体平台）的方式，诱使用户输入敏感信息。例如，黑客发送虚假电子邮件或链接，引导用户进入伪造的网站并泄露账户信息。破坏了保密性。

技术因素：

1. 后门程序（Backdoor）：在系统中植入的秘密通道或代码，用于绕过正常的认证和安全控制。例如，某些恶意软件会在受感染的系统上安装后门程序，使攻击者可以在后续访问和控制该系统。破坏了可控制性。

2. BUG（漏洞）：软件或系统中存在的错误或缺陷，可能被攻击者利用。例如，软件程序中的缓冲区溢出漏洞可以导致远程代码执行，从而使攻击者能够控制受影响的系统。

请注意，这只是信息安全面临的威胁的一小部分，还有其他威胁和技术存在。同时，防范这些威胁需要多种安全措施和实践，如使用强密码、更新和修补软件漏洞、使用防火墙和入侵检测系统等。这些安全措施应该根据具体情况和需求进行定制和实施。

### 7.1.4数据加密技术

信息安全技术主要有数据加密技术、身份认证技术、访问控制技术、安全审计技术、反病毒技术、防火墙技术，其中数据加密技术是信息安全系统的核心技术。

数据加密技术是一种保护数据安全性的方法，它使用加密算法将明文（未加密的原始数据）转换为密文（经过加密算法处理的不可读数据），需要使用密钥来进行加密和解密操作。

- 明文（plaintext）：指未经过加密的原始数据，易于阅读和理解。例如，将文本消息“Hello World!”作为明文。

- 密文（ciphertext）：指通过加密算法处理后的数据，具有很高的安全性，只有拥有正确密钥的人才能解密并还原为明文。例如，应用AES加密算法和密钥将明文“Hello World!”加密得到的密文可能是“FJ9sWznz2jaIj7UDdN/KHA==”。

- 密钥（key）：是一个或一组参数，它用于在加密和解密过程中转换明文和密文。密钥可以是秘密的（单钥加密算法）或公开的（双钥加密算法）。例如，使用密钥“mysecretkey”来加密和解密数据。

- 加密（encryption）：是将明文转换为密文的过程，通过应用加密算法和相应的密钥来实现。例如，应用AES加密算法和密钥将明文“Hello World!”加密为相应的密文。

- 解密（decryption）：是将密文转换回明文的过程，通过应用解密算法和相应的密钥来实现。例如，使用正确的密钥和解密算法将密文解密为原始的明文数据。

- 加密算法（encryption algorithm）：是指用于执行加密过程的数学函数或计算机程序。加密算法决定了加密和解密的方式。例如，常见的对称加密算法包括AES（高级加密标准）和DES（数据加密标准）；常见的非对称加密算法包括RSA和ECC等。

- 解密算法（decryption algorithm）：是指用于执行解密过程的数学函数或计算机程序。解密算法与加密算法相对应，用于将密文转换回明文。

- 单钥加密（symmetric encryption）：也称为对称加密，使用相同的密钥进行加密和解密操作。密钥在传输和存储过程中需要保持安全。例如，AES和DES都是对称加密算法的例子。

- 双钥加密（asymmetric encryption）：也称为公钥加密，使用两个相关但不同的密钥进行加密和解密操作。其中一个密钥是公开的（公钥），用于加密数据；另一个密钥是私密的（私钥），用于解密数据。例如，RSA和ECC是常见的双钥加密算法的例子。

对称密钥加密（Symmetric Key Encryption）：使用相同的密钥进行加密和解密操作的加密方式。加密和解密使用相同的密钥，因此需要通过安全手段来保护密钥的传输和存储。例如，AES算法是一种常用的对称密钥加密算法。

TDEA算法（Triple Data Encryption Algorithm）：也称为3DES算法，是对称密钥加密算法的一种。它通过对数据进行三次DES加密来提高安全性。

Blowfish算法：是一种对称密钥加密算法，广泛应用于加密通信和文件存储等领域。Blowfish具有较高的安全性和加密效率。

RC5算法：是对称密钥加密算法中的一种，其特点是可调节的密钥长度和分块长度。RC5算法适用于多种应用的数据加密需求。

IDEA算法（International Data Encryption Algorithm）：是一种对称密钥加密算法，被广泛应用于加密通信和安全传输等领域。IDEA算法以其安全性和效率而闻名。

DES算法（Data Encryption Standard）：是一种对称密钥加密算法，过去被广泛应用于加密应用中。DES使用56位的密钥对数据进行加密和解密。

非对称密钥加密（Asymmetric Key Encryption）：使用两个相关但不同的密钥进行加密和解密操作的加密方式。其中一个是公开的密钥（公钥），用于加密数据，而另一个是私密的密钥（私钥），用于解密数据。

公钥（Public Key）：在非对称密钥加密中，公钥是公开的，可供任何人使用。用公钥加密的数据只能通过相应的私钥进行解密。

私钥（Private Key）：在非对称密钥加密中，私钥是保密的，只有密钥的所有者可以使用它进行解密操作。

DSA系统（Digital Signature Algorithm）：是一种基于非对称密钥加密的数字签名算法。其主要用于验证数字签名的合法性和完整性。

ECC系统（Elliptic Curve Cryptography）：是一种基于椭圆曲线理论的非对称密钥加密系统。ECC系统具有较高的安全性和效率。

RSA系统：是一种非对称密钥加密算法，广泛应用于数字加密和数字签名等领域。RSA算法基于大素数的数论问题，其安全性依赖于因数分解的困难性。

单向散列函数加密：也称为哈希函数加密，是一种将任意长度的输入数据映射为固定长度散列值的算法。常见的单向散列函数包括MD4、MD5和SHA系列算法。

HASH值：也称为散列值或摘要，是通过单向散列函数对输入数据计算得到的唯一的固定长度的值。

MD4算法：是一种单向散列函数，但由于其安全性的不足，已经被更安全的算法所取代。

MD5算法：是一种广泛使用的单向散列函数，但由于其存在碰撞攻击的漏洞，已经不适用于安全性要求较高的场景。

SHA算法（Secure Hash Algorithm）：是一组由国家标准与技术研究院（NIST）发布的单向散列函数算法。其中，SHA-1已经被认为不再安全，而SHA-2和SHA-3系列算法具有更高的安全性。

序列号保护：序列号保护是一种软件保护机制，通过使用唯一的序列号来限制对软件的访问和使用。每个用户或设备都被分配一个唯一的序列号，该序列号需要在软件激活或注册时进行验证，以确保合法的使用。

注册文件保护：注册文件保护是一种软件保护方法，通过加密和验证注册文件来保护软件免受未经授权的访问和使用。注册文件通常包含用户的许可证信息和授权信息，通过加密和签名技术可以确保注册文件的完整性和真实性。

加密狗：加密狗是一种硬件设备，用于提供额外的安全保护，以防止未经授权的访问和使用。加密狗通常包含加密芯片和存储器，用于存储许可证信息和加密密钥。软件需要与加密狗进行通信和验证，以确保只有授权的加密狗才能使用软件。

### 7.1.5身份认证技术

身份认证是一种用于验证用户或实体身份的过程，确保只有合法的用户可以访问系统或资源。它是计算机安全领域中的重要概念，用于保护系统免受未经授权的访问。

身份认证的目的与作用：

身份认证的目的是确保系统只被授权用户所使用，防止未经授权的访问和数据泄露。它有助于确保用户身份的真实性和可靠性，并提供一种可信的方式来控制用户对资源的访问权限。

认证的概念和例子：

认证是验证用户或实体身份的过程。常见的认证方式包括：

1. 用户名和密码：用户通过提供正确的用户名和密码来验证身份。

2. 双因素认证：结合多个验证因素，例如密码和手机验证码，以增加身份验证的安全性。

3. 生物识别认证：使用指纹、虹膜、人脸识别等生物特征来验证身份。

4. USB Key认证：使用存储在USB Key中的安全证书来进行身份验证。

5. 动态口令认证：通过生成动态口令，如使用令牌生成的一次性密码，来验证身份。

授权的概念和例子：

授权是给予经过认证的用户访问资源和执行特定操作的权限。授权控制用户可以访问哪些资源、在何种程度上进行操作。例如，给予用户读取文件的权限或允许用户在系统中创建新文件。

审计的概念和例子：

审计是记录和监控用户活动以及系统资源使用的过程。审计可以追踪和识别安全事件，提供审计日志以供后续分析和调查。例如，记录用户登录时间、访问的文件和操作等信息。

静态密码的概念和例子：

静态密码是指在身份认证过程中使用固定不变的密码进行验证。例如，在登录系统时，用户需要提供预先设定的密码来验证身份。

动态口令认证的概念和例子：

动态口令认证使用一次性密码或基于时间的口令来增强身份认证的安全性。这些口令在每次验证过程中都会发生变化，提供额外的身份验证层级。例如，通过令牌生成的一次性密码或从移动设备接收的时间限制口令。

USB Key认证的概念和例子：

USB Key认证使用存储在USB Key中的安全证书进行身份验证。用户插入USB Key，系统通过读取其中的证书来验证用户的身份。这种方式可以提供更高的安全性，因为证书存储在物理设备中，难以被复制或篡改。

生物识别技术的概念和例子：

生物识别技术使用人体的生物特征来进行身份认证。常见的例子包括指纹识别、虹膜扫描和人脸识别。通过比对用户提供的生物特征和预先存储的模板，系统可以验证用户的身份。

CA认证的概念和例子：

CA认证是由受信任的认证机构（CA）发行的数字证书，用于验证用户或实体的身份。CA会对申请者进行身份验证，并签发包含其身份信息的数字证书。数字证书用于加密通信、验证签名以及建立安全连接。

数字签名是使用私钥对数据进行加密的过程，以证明数据的来源和完整性。发送者使用私钥对数据进行签名，接收者使用对应的公钥进行验证。常见的数字签名算法包括RSA（Rivest-Shamir-Adleman）和DSA（Digital Signature Algorithm）。

例如，Alice想要向Bob发送加密的消息，Alice先用自己的私钥对消息进行数字签名，生成数字签名后，将签名和公钥附在消息上一起发送给Bob。Bob收到消息后，使用Alice的公钥来验证数字签名的有效性和消息的完整性，以确定消息的来源和完整性。

数字签名的功能：

数字签名具有以下功能：

1. 数据完整性验证：接收者可以使用发送者的公钥验证数字签名，以确保数据在传输过程中没有被篡改或损坏。

2. 身份验证：数字签名可以验证数据的来源，可以确定发送者的身份，因为只有私钥的持有者才能够正确地生成数字签名。

3. 抗抵赖性：发送者无法否认自己所签名的数据，因为数字签名是基于私钥生成的，私钥只有发送者知道。

签名算法的概念和例子：

签名算法是生成数字签名的数学算法。常见的签名算法包括：

1. RSA（Rivest-Shamir-Adleman）：基于大数分解的公钥密码算法，广泛用于数字签名和加密通信。

2. DSA（Digital Signature Algorithm）：用于数字签名的公钥密码算法，主要用于数字证书和安全协议中。

验证算法的概念和例子：

验证算法用于验证数字签名的有效性和数据的完整性。在验证过程中，接收者使用发送者的公钥来验证数字签名。常见的验证算法包括：

1. RSA验证算法：使用发送者的公钥和数字签名对数据进行验证，并比较计算出的哈希值与原始数据的哈希值，以确定数据的完整性和来源。

2. DSA验证算法：使用发送者的公钥、签名和原始数据，使用一系列数学运算来验证签名的有效性。

数字证书的概念和例子：

数字证书是由受信任的认证机构（CA）签发的电子文件，用于验证个人或实体的身份信息。数字证书中包含了公钥以及与该公钥相关联的身份信息，并由CA对其中的信息进行数字签名。常见的数字证书标准是X.509，其中包括了证书的各种属性和扩展字段。

### 7.1.6访问控制技术

访问控制是指控制用户或实体对系统、资源或信息的访问权限的过程和技术。它的目标是限制未经授权的访问并确保合法用户只能访问其授权的资源。

访问控制的目的与作用：

访问控制的主要目的和作用是：

1. 保护系统与资源：限制未经授权的访问，防止非法或恶意用户获取敏感信息或篡改资源。

2. 维护数据完整性和机密性：确保只有授权用户能够读取或修改数据，以保持数据的完整性和保密性。

3. 实施合规性要求：确保系统和资源遵守相关法规、标准和政策，例如数据隐私法和行业规范。

访问控制的手段：

访问控制通过以下手段来实现：

1. 身份认证：验证用户或实体的身份，确认其是否有权访问系统或资源。

2. 授权管理：根据用户的身份和角色分配访问权限，确保用户只能访问其授权的资源。

3. 审计和监控：记录和跟踪用户的访问活动，并监控异常行为或安全事件。

重要过程（鉴别和授权）：

访问控制涉及两个重要的过程：

1. 鉴别（Identification）：用户或实体提供身份信息进行验证，以确认其身份。

2. 授权（Authorization）：根据用户身份和角色，授予适当的访问权限，决定其可以访问的资源和操作。

自主访问控制（Discretionary Access Control）的概念和例子：

自主访问控制是一种基于主体的访问控制模型，其中用户被授予对资源的控制权，用户可以独立决定对资源的访问权限。例如，文件系统中的访问控制列表（ACL）允许文件的所有者在文件级别上设置访问权限。

强制访问控制（Mandatory Access Control）的概念和例子：

强制访问控制是一种基于安全策略和标签的访问控制模型，其中访问权限由系统定义和强制执行，而不是由用户决定。例如，多级安全（MLS）系统根据安全级别和访问标签限制用户对资源的访问。

基于角色的访问控制（Rule – Based Role – Based Access Coniiol，RB - RBAC）的概念和例子：

基于角色的访问控制（RBAC）是一种访问控制模型，其中用户被分配到角色，而不是直接授予访问权限。角色具有特定的权限和功能，用户根据其角色的权限来访问系统和资源。例如，网络管理员、数据库管理员和普通用户可以分别被分配不同的角色，访问不同级别的功能和资源。

访问控制原则是在访问控制技术中非常重要的指导原则，它们有助于确保系统和资源的安全性、完整性和保密性。以下是这些原则的详细解释：

1. 最小特权原则（Principle of Least Privilege）：根据这一原则，用户、程序或实体应当被授予执行其工作所需的最低权限级别，而不是具有无限制的权限。这个原则的目的是限制每个主体的访问权限，以减少潜在攻击面，防止用户或程序滥用权限以及减轻可能的损害。通过最小特权原则，用户或程序只能访问、修改或处理必须的资源和数据，这有助于减少安全漏洞和意外错误的风险。

2. 最小泄露原则（Principle of Least Disclosure）：这一原则要求用户、程序或实体仅能够访问他们需要了解的关键信息，防止敏感信息的泄露。例如，不同层次的用户或不同角色的员工可能只能查看与其职责相关的数据，而无权访问其他部门或用户的敏感信息。最小泄露原则确保将信息的可视性和可获得性限制在必要的水平上，以减少信息泄露和滥用的风险。

3. 多级安全策略（Multilevel Security Policies）：多级安全策略适用于特定场景，其中信息根据其保密性等级进行分类，并为不同级别的主体或用户提供访问控制措施。在这种环境中，信息具有不同的标签或类别，用户只能够查看或访问与其授权级别相匹配的信息。这种安全策略确保信息在不同的保密性级别之间保持隔离，并防止未经授权者访问高级别的敏感信息。多级安全策略通常在军事、情报和政府机构中应用广泛。

这些访问控制原则是安全设计和实施中的关键要素，可以帮助保护系统、资源和信息免受未经授权的访问和滥用。

### 7.1.7信息隐藏技术

信息隐藏技术是一种通过在数据中隐藏附加信息而不影响原始数据完整性的技术。这些技术可以在多媒体文件（如图像、音频和视频）、文本文档或通信通道中嵌入隐藏的数据。隐藏的数据可以是文本、图像、音频、视频或其他形式的信息。

信息隐藏技术目的与作用：信息隐藏技术的主要目的是隐蔽地传输信息或保护数据的完整性和版权。它们可以用于隐秘通信、数字版权保护、内容认证和数字取证等领域。

实际应用：信息隐藏技术在许多领域都有实际应用，包括数字版权保护、医学图像处理、视频监控、网络安全和取证分析等。

鲁棒性：信息隐藏技术的鲁棒性是指隐藏的信息在经历攻击、压缩、加噪声或其他变换之后仍能被正确提取出来。它能够保持对隐藏信息的可靠性和准确性。例如，图像隐写中的一种鲁棒性技术是使用可纠错码来确保隐藏信息的可靠提取。

不可检测性：不可检测性是指隐藏的信息在外观上不可察觉，无法被人或机器直观地感知到。例如，图像隐写中的一种方法是将信息嵌入到像素值的最低有效位（LSB）中，这样人眼无法察觉到嵌入的变化。

透明性：透明性是指信息隐藏技术对原始数据的影响尽可能小，使得人无法察觉到嵌入过隐藏信息。透明性是信息隐藏技术的一个重要指标，尤其在图像、音频和视频等媒体数据中的应用较为重要。

安全性：信息隐藏技术通常需要与安全性相结合，以保护隐藏的信息不被未经授权的访问者获取和破解。安全性涉及加密和认证等技术，以确保隐藏信息的机密性和完整性。例如，加密的数字水印技术可用于保护嵌入在数字媒体中的信息。

自恢复性：自恢复性是指隐藏信息在经过一定程度的攻击或扭曲后，仍然可以被恢复出来。这种技术通常利用冗余信息和错误纠正码来实现。例如，在音频数字水印中，通过分布在整个音频中的冗余信息，可以在一定程度上提高隐藏信息的恢复性。

隐写术（Steganography）：隐写术是一种信息隐藏技术，通过将隐藏信息嵌入到无关文件或载体中，使得外部观察者无法察觉到隐藏信息的存在。隐写术的目标是确保隐藏信息的保密性。一种常见的隐写术示例是将文本信息嵌入图像的像素值中。

数字水印（Digital Watermarking）：数字水印是一种保护数字媒体内容安全性和版权的技术。它是通过在数字媒体中嵌入特定的标识信息来实现的，这个标识信息通常是不可察觉的。数字水印可以应用于图像、音频、视频和文档等多种类型的媒体。一个常见的数字水印示例是在数字图像中嵌入一些不可见的标识信息，以证明图像的所有权和完整性。

数字指纹（Digital Fingerprinting）：数字指纹是一种用于识别和追踪数字媒体的技术。它通过在数字媒体中嵌入唯一的标识信息或参数，对媒体内容进行标记和跟踪。数字指纹技术可以应用于音频、视频和图像等媒体。一个常见的数字指纹示例是在音频文件中嵌入一个独特的指纹，以便对音频进行版权追踪。

叠像术（Data Hiding in Image）：叠像术是一种将隐藏信息嵌入到图像中，使得嵌入的信息在外观上不可察觉的技术。叠像术可以通过修改图像的像素值、调整图像中的频域信息或利用图像的局部特征来实现隐藏。一个常见的叠像术示例是在图像的最低有效位（LSB）中嵌入隐藏信息。

潜信道（Covert Channel）：潜信道是一种通过利用系统的正常通信机制来传递隐藏信息的技术。它可以利用系统资源或通信渠道中的若干特性，将隐藏信息传递给其他实体。潜信道一般用于绕过安全策略或进行隐蔽通信。一个常见的潜信道示例是利用网络协议头部的保留字段来传递隐藏信息。

## **7.2 网络安全基础知识**

### 7.2.1 网络安全目标与特征

网络安全是保护计算机网络系统免受未经授权的访问、攻击和恶意活动的一系列措施和技术。以下是网络安全的目标与特征：

1. 机密性

- 目标：机密性是保护数据和信息资源免受未经授权的披露的目标。

- 特征：通过加密和访问控制等技术手段，确保只有授权的用户或系统能够访问和获取敏感信息。

- 例子：使用SSL/TLS协议对网站进行加密通信，确保用户的个人信息在传输过程中不被窃取。

2. 完整性

- 目标：完整性是确保数据和信息在传输、存储和处理过程中保持完整和未被篡改的目标。

- 特征：通过数字签名、消息认证码和访问权限控制等技术手段，防止数据被篡改或恶意修改。

- 例子：使用数字签名技术确保软件在下载和安装过程中未被篡改。

3. 可用性

- 目标：可用性是确保网络和系统能够按需提供服务和资源的目标。

- 特征：通过备份和灾难恢复机制、负载均衡、容错和容灾技术等，确保网络和系统持续可用。

- 例子：使用冗余服务器和负载均衡技术确保网站在并发访问高峰时仍能正常运行。

4. 可控性

- 目标：可控性是确保有授权的实体能够有效地管理和控制网络和系统的目标。

- 特征：通过访问控制策略、权限管理和用户身份验证等技术手段，实现对系统资源和功能的控制。

- 例子：使用访问控制列表（ACL）限制特定用户对文件和文件夹的访问权限。

5. 可审查性

- 目标：可审查性是确保对系统和网络活动进行审计和监控的目标。

- 特征：通过日志记录、事件和行为分析等技术手段，追踪和检测恶意活动，并对安全事件进行调查和分析。

- 例子：使用入侵检测系统（IDS）监测网络中的异常活动，并生成详细的事件日志供审计使用。

实现网络安全的层次

实现网络安全需要考虑多个层次和方面。以下是实现网络安全的层次：

1. 物理安全

- 概念：物理安全是保护物理设施和网络基础设施免受未经授权的访问、破坏和损害的措施。

- 例子：保护数据中心和服务器房间的门禁、视频监控和入侵报警系统等。

2. 安全控制

- 概念：安全控制是通过访问控制和权限管理等手段，限制和控制对系统和数据的访问和使用。

- 例子：身份验证、用户权限管理和访问策略的实施和执行。

3. 安全服务

- 概念：安全服务是通过提供安全管理和监控的服务，确保网络和系统的安全性。

- 例子：安全事件和威胁管理、漏洞扫描和漏洞修复、安全策略执行等。

4. 安全机制

- 概念：安全机制是通过加密、认证和防御技术，保护数据和通信免受威胁和攻击。

- 例子：数据加密、防火墙、入侵检测和防御系统等。

### 7.2.2 局域网攻击

局域网攻击是指针对局域网内部的设备和通信进行的恶意行为。其中，ARP欺骗和ARP洪水是两种常见的局域网攻击技术：

1. ARP欺骗

- 概念：ARP欺骗（Address Resolution Protocol Spoofing）是指攻击者通过发送虚假的ARP响应，伪装成合法设备的MAC地址，从而欺骗其他设备将网络流量发送给攻击者或中间人。

- 原理：ARP协议用于将IP地址解析为MAC地址，攻击者发送伪造的ARP响应告诉其他设备自己拥有目标IP地址对应的MAC地址，以此达到截获网络流量或进行中间人攻击的目的。

- 影响：ARP欺骗攻击可以导致数据被窃听、篡改或中断，还可能导致网络拥塞和服务不可用。

- 例子1：中间人攻击

攻击者在局域网上伪造自己的MAC地址，并发送虚假的ARP响应，欺骗其他设备将网络流量发送给自己。攻击者可以在通信过程中窃听、截取、篡改或重放数据，并将数据转发给目标设备，使得通信双方都不知道其间存在攻击者。

- 例子2：ARP缓存中毒

攻击者发送大量的虚假ARP响应，欺骗局域网内其他设备将其自身的MAC地址与某个合法设备的IP地址相绑定。当设备试图与目标设备通信时，会将数据发送给错误的MAC地址，导致通信失败或传输到错误的设备。

2. ARP洪水

- 概念：ARP洪水（ARP Flooding）是指攻击者发送大量的虚假ARP请求，使局域网内设备的ARP缓存表被填满，造成网络拥塞或瘫痪。

- 原理：攻击者发送大量的ARP请求，每个请求都包含不同的源MAC地址和相同的目标IP地址，以此迷惑目标设备的ARP缓存表，导致其无法正确解析IP地址和MAC地址的对应关系。

- 影响：ARP洪水攻击会导致网络拥塞，正常通信受阻，网络性能下降，甚至可能导致服务不可用。

防御措施：

1. 使用静态ARP表：将局域网内的设备和MAC地址手动绑定，减少ARP欺骗的可能性。

2. 限制ARP请求和响应：通过配置网络设备，限制ARP请求和响应的频率和数量，防止ARP洪水攻击。

3. 使用网络入侵检测系统（NIDS）：监测和识别异常的ARP行为，及时发现和阻止潜在的ARP欺骗和洪水攻击。

4. 加密通信：使用加密协议（如SSL/TLS）保护敏感数据在局域网内的传输过程中避免被窃听和中间人攻击。

- 例子1：网络拒绝服务（DoS）

攻击者发送大量的虚假ARP请求，每个请求都包含不同的源MAC地址和相同的目标IP地址。这将导致局域网内的设备的ARP缓存表被填满，无法正确解析IP地址和MAC地址的对应关系，导致网络拥塞或瘫痪。

- 例子2：网络性能下降

攻击者发送大量的虚假ARP请求，不断刷新局域网内设备的ARP缓存表。这将消耗设备的处理能力和网络带宽，导致网络性能下降，使正常通信和服务受到影响。

### 7.2.3 广域网攻击

1. 分布式拒绝-of-Service (DDoS) 攻击：

- 概念：DDoS攻击通过利用大量已感染的计算机或僵尸网络发送大量流量，超过目标网络的处理能力，导致网络服务不可用。

- 例子：2016年的Mirai僵尸网络攻击，攻击者利用感染了数十万个物联网设备的僵尸网络，对目标网络进行了大规模的DDoS攻击。

- 防范方法：使用防火墙和入侵检测系统来监测和过滤潜在的DDoS流量，配置流量限制和过滤规则以限制异常的流量，使用DDoS防护服务来缓解攻击。

2. 源地址欺骗 (IP Spoofing)：

- 概念：源地址欺骗是指攻击者伪造IP数据包的源IP地址，以隐藏自己的真实身份或绕过网络的认证和访问控制机制。

- 例子：攻击者使用源地址欺骗发起的TCP SYN洪水攻击，通过伪造大量的源IP地址发送SYN请求，造成目标服务器资源枯竭。

- 防范方法：在网络边界设备上实施反源地址欺骗（RFC 2827）的过滤和验证机制，使用网络流量分析工具检测和识别伪造的IP数据包。

3. 广域网钓鱼 (WAN Phishing)：

- 概念：广域网钓鱼是指攻击者冒充合法机构或个人，通过伪造的电子邮件、网站或通信方式诱骗用户透露敏感信息，以达到欺骗和非法获取信息的目的。

- 例子：攻击者向用户发送伪装成银行官方网站的电子邮件，要求用户输入银行账号和密码，从而盗取用户的银行登录凭据。

- 防范方法：加强用户教育和意识培训，认识并警惕钓鱼攻击，使用安全浏览器和反钓鱼工具，检查URL的真实性，避免点击可疑链接和提供个人信息。

4. 远程访问攻击：

- 概念：远程访问攻击是指攻击者通过利用广域网上的弱点和漏洞，未经授权地远程访问目标网络或系统。

- 例子：攻击者通过猜解或盗取管理员密码，远程登录到企业的远程桌面服务，获取敏感信息或操纵系统。

- 防范方法：强化远程访问的安全设置，使用强密码或多因素身份验证，限制远程访问的IP范围，定期更新和修补系统和应用程序的漏洞。

5. VPN 破解攻击：

- 概念：VPN破解攻击是指攻击者试图突破虚拟专用网络（VPN）的加密机制，以获取传输中的敏感数据。

- 例子：攻击者通过中间人攻击或拦截VPN流量，并进行解密和分析，以窃取敏感信息。

- 防范方法：使用强大的加密算法和协议，如IPsec或TLS/SSL，及时更新和修补VPN设备的漏洞，限制和监控对VPN的访问，实施访问控制和身份验证机制。

6. 嗅探和窃听：

- 概念：嗅探和窃听攻击是指攻击者通过在广域网上部署嗅探工具，拦截、监听和窃取流经网络的数据信息。

- 例子：攻击者使用网络嗅探工具对无线网络进行被动监听，获取用户的敏感信息（如登录凭据、信用卡号等）。

- 防范方法：使用加密的通信协议（如HTTPS），避免使用不安全的传输协议（如HTTP），部署入侵检测系统（IDS）和入侵防御系统（IPS）来监控和阻止异常的数据流量，定期审计和更新网络设备的配置。

7. 路由器攻击：

- 概念：路由器攻击是指攻击者利用广域网上路由器的弱点或漏洞，进行篡改、拒绝服务或网络干扰等恶意行为。

- 例子：攻击者通过访问未授权的管理接口，修改路由器的路由表，导致网络流量被重定向到恶意服务器。

- 防范方法：及时更新和修补路由器的固件和操作系统，加强路由器的访问控制，禁用未使用的服务和接口，实施安全配置策略，定期审计和监测路由器的活动日志。

### 7.2.4 防火墙技术

防火墙的概念：防火墙是一种网络安全设备或软件，用于监控和过滤网络流量，以保护内部网络免受未经授权的访问和恶意活动的攻击。它主要用于控制网络流量的进出，根据预先设置的策略允许或阻止特定类型的流量通过。

防火墙的目的与作用：防火墙的主要目的是保护网络和系统免受恶意入侵、未经授权的访问和网络攻击。它实现了网络安全的目标，包括访问控制、信息保密性、完整性和可用性。

防火墙的基本功能

访问控制：防火墙基于预定义的规则和策略，控制网络流量的进出，仅允许授权的流量通过，阻止未经授权的访问。

网络地址转换（NAT）：防火墙可以执行网络地址转换，将内部网络的私有IP地址转换为公共IP地址，以保护内部网络的隐私和安全。

状态跟踪：防火墙可以跟踪网络连接的状态和信息，以便对连接行为进行检查和控制，防止潜在的攻击和异常连接。

日志记录和报告：防火墙可以记录网络流量和安全事件的日志，并生成报告，用于安全审计、事件分析和安全决策。

防火墙的弱点：尽管防火墙可以提供重要的网络安全保护，但它们仍然存在一些弱点。一些常见的防火墙弱点包括配置错误、软件漏洞、传输层协议的漏洞以及对高级攻击和新型威胁的适应性不足。

基本型防火墙：基本型防火墙也称为网络层防火墙，它基于网络层（OSI模型的第三层）对网络流量进行过滤和控制。它通过检查数据包的源IP地址、目标IP地址和端口号来决定是否允许通过。常见的基本型防火墙示例包括Cisco ASA和HPE TippingPoint。

基本型防火墙的特点和缺点：

- 特点：基本型防火墙具有简单、高效的数据包过滤功能，可以快速处理大量的网络流量，并提供了基本的访问控制。

- 缺点：基本型防火墙缺乏应用层（OSI模型的第七层）的深度检查和控制能力，容易被绕过和攻击。它无法识别应用层协议中潜在的安全漏洞。

包过滤防火墙：包过滤防火墙是一种基于数据包头信息的网络安全设备，它根据预先设置的规则对数据包进行过滤和控制。它可以根据源IP地址、目标IP地址、端口号和协议类型等进行过滤。常见的包过滤防火墙示例包括iptables和Windows防火墙（Windows Firewall）。

包过滤防火墙的特点和缺点：

- 特点：包过滤防火墙具有良好的性能和灵活的配置选项。它可以快速处理大量的数据包，并提供了对网络流量的基本控制和过滤。

- 缺点：包过滤防火墙缺乏应用层的深度检查和控制能力。它主要依赖于数据包头信息，无法处理对应用层协议的高级攻击。

应用型防火墙：

- 概念：应用型防火墙是一种工作在应用层的网络安全设备，它能够对网络流量进行深度检查和过滤，甚至可以理解和解析特定应用层协议的数据。

- 例子：常见的应用型防火墙包括Palo Alto Networks的Next-Generation Firewall（NGFW）和Check Point的Application Firewall（AppFW）。

- 特点：应用型防火墙具有深度的应用层检测能力，可以对应用行为进行识别和控制，提供细粒度的访问控制和安全策略。

- 缺点：应用型防火墙的配置和管理相对复杂，对硬件性能有一定要求，可能会对网络性能产生一定的影响。

复合型防火墙：

- 概念：复合型防火墙是一种综合多种防火墙技术的集成型安全设备，结合了不同层次和功能的防火墙技术，以提供全面的防御和保护机制。

- 例子：典型的复合型防火墙包括Cisco的Adaptive Security Appliance（ASA）和Fortinet的FortiGate。

- 特点：复合型防火墙具备多层次的安全防护能力，可以根据实际需求配置多种防火墙策略，提供细粒度的访问控制和威胁防御。

- 缺点：复合型防火墙的配置和管理相对复杂，对设备性能要求较高，需要具备一定的专业知识和经验。

主机屏蔽防火墙：

- 概念：主机屏蔽防火墙是一种部署在主机上的软件或服务，用于保护主机免受网络攻击和未经授权的访问。它在主机上实施访问控制和策略，并监控和过滤网络流量。

- 例子：常见的主机屏蔽防火墙包括Windows操作系统自带的防火墙和Linux系统上的iptables。

- 特点：主机屏蔽防火墙可以提供个体化的主机保护，根据主机特性和需求进行定制配置，对入站和出站流量进行控制和审计。

- 缺点：主机屏蔽防火墙只能保护所部署的主机，对于网络层面的攻击无能为力，配置和管理相对复杂，可能会对主机性能产生一定的影响。

子网屏蔽防火墙：

- 概念：子网屏蔽防火墙是一种位于子网级别的网络安全设备或服务，用于保护子网内的主机和资源免受网络攻击和威胁。它工作在网络层，监控并控制进出子网的流量。

- 例子：Juniper Networks的SRX系列防火墙和Cisco的ASA系列防火墙是常见的子网屏蔽防火墙。

- 特点：子网屏蔽防火墙具有如下特点：

- 提供对整个子网的统一访问控制和安全策略，能够限制流入和流出子网的流量，保护子网内的主机和资源。

- 对子网内的数据流进行监控和过滤，检测和阻止恶意流量和网络攻击。可以使用各种技术如数据包过滤、状态检测和安全协议加密等。

- 可以与其他网络安全设备集成，如入侵检测系统（IDS）和虚拟专用网络（VPN）等，提供更全面的保护和安全功能。

- 缺点：子网屏蔽防火墙也存在一些缺点：

- 配置和管理相对复杂，对网络管理员需要一定的专业知识和经验来正确配置和维护。

- 由于位于子网边界，可能会成为性能瓶颈，并对网络吞吐能力产生一定的影响。

- 不能提供对网络层之外的攻击的防护，如应用层攻击等，需要结合其他安全机制来提供全面的保护。

### 7.2.5虚拟专用网络（VPN）

虚拟专用网络（VPN）是一种通过公共网络（如互联网）建立安全连接的技术。它允许远程用户或不同地理位置的网络之间建立加密通信，提供私密性和安全性。

功能：

- 远程访问：远程用户可以通过VPN安全地访问内部网络资源，如文件、打印机等。

- 数据加密：VPN使用加密协议对数据进行加密，防止被未经授权的人员截获和查看。

- 身份验证：VPN可以要求用户进行身份验证，确保只有授权用户可以访问网络资源。

- 匿名性：VPN可以隐藏用户的真实IP地址，提供匿名性和隐私保护。

按协议分类：

- PPTP（点对点隧道协议）：一种基于客户端/服务器模型的VPN协议，常用于Windows系统。由于安全性较低，现已不推荐使用。

- L2TP（第2层隧道协议）：结合了PPTP和Cisco的L2F协议，提供更高的安全性。常用于跨平台的客户端连接。

- IPSec（网际协议安全性）：一种通过加密和验证确保IP数据包安全传输的协议。可用于建立站点到站点或远程访问VPN。

按应用分类：

- 远程接入VPN：远程用户通过互联网连接到公司内部网络，以访问公司资源。例如，远程员工使用VPN远程连接公司网络。

- 内联网VPN：通过VPN将不同地理位置的内部网络连接在一起。用于实现分支机构、办公室和数据中心之间的安全通信。

- 外联网VPN：连接公司内部网络与外部合作伙伴、供应商或云服务提供商的网络。用于安全共享资源和数据。

按设备类型分类：

- 路由器VPN：通过在路由器上部署VPN功能，实现点对点或多点到点的VPN连接。例如，在分支机构使用路由器建立VPN连接到总部网络。

- 交换机式VPN：基于二层交换机的VPN，通过VLAN隔离和传输VLAN跨越不同的物理地理位置。常用于构建企业内部的VPN。

- 防火墙式VPN：利用防火墙设备建立VPN连接，提供访问控制和数据包过滤等安全功能。例如，通过防火墙建立VPN隧道连接不同的网络。

### 7.2.6黑客

黑客：

- 概念：黑客是指具备计算机技术能力的人，通过研究和理解计算机系统的内部工作原理，以获取未授权的访问权限或执行其他恶意行为。

- 例子：黑客可以利用漏洞入侵目标系统，窃取、篡改或删除数据，或者对系统进行拒绝服务攻击等。

白客：

- 概念：白客，也被称为"良性黑客"或"道德黑客"，是指受雇于组织或企业，以授权的方式测试和评估系统安全性的安全专家。

- 例子：白客通过模拟攻击和漏洞扫描等手段，帮助组织发现和修复安全漏洞，提高系统的安全性。

红客：

- 概念：红客是指受组织聘请，对其进行实际攻击和渗透测试的安全专家。他们模拟真实黑客行为，以评估组织的防御能力。

- 例子：红客可能使用各种攻击手段，如社会工程、网络渗透、应用程序漏洞利用等，以暴露组织的弱点并提供改进建议。

骇客：

- 概念：骇客是黑客的俚语术语，与黑客具有相同的含义，但有时带有更贬义的意味，强调其不道德的行为。

- 例子：骇客可能窃取个人信息、发起网络攻击、传播恶意软件等，用于非法牟利或破坏目的。

极客：

- 概念：极客是指对计算机技术和相关领域具有极大热情和专业知识的人。他们追求技术深度和创新。

- 例子：极客可能擅长编程、网络安全、系统管理等领域，通过参与开源项目、创造新技术或提供技术解决方案来展示其技术能力。

黑客常用攻击手段：

- 社会工程：通过欺骗、虚假信息或人际关系来获取目标系统的访问权限。

- 拒绝服务攻击：通过向目标系统发送大量请求，耗尽其资源或导致服务不可用。

- 漏洞利用：利用操作系统、应用程序或网络设备中的漏洞，获取非授权的访问权限。

- 木马程序：通过在目标系统上安装潜在恶意软件，实现远程控制或数据窃取。

- 礼品卡欺诈：利用礼品卡、优惠券或积分系统的漏洞，实施欺诈行为。

### 7.2.7预防黑客攻击

黑客攻击是指非法入侵计算机系统或网络以获取未经授权的访问、窃取敏感信息或进行破坏等恶意活动。了解黑客攻击的策略和采取预防措施对于保护计算机系统和网络的安全至关重要。以下是有关黑客攻击的策略和预防措施的详细信息：

1. 黑客攻击的策略

- 伪装：黑客常常使用伪装的方式获取未经授权的访问。他们可能冒充合法用户、设备或系统，以获取登录凭据或其他敏感信息，进而入侵目标系统。

- 发现漏洞：黑客利用各种手段来发现系统或应用程序中的漏洞。他们可能使用扫描工具、漏洞利用技术或社会工程等手段来发现系统中可能存在的弱点。

- 利用后门：黑客攻击者可能通过在系统中留下后门程序或恶意软件来维持对系统的持久访问权限。他们可以利用后门来窃取敏感信息、操纵系统或进行其他恶意活动。

2. 预防措施

- 更新和维护：及时更新和维护操作系统、应用程序和网络设备，以修复已知漏洞和安全弱点。确保使用最新版本的软件，并及时应用安全补丁。

- 强化身份验证：采用强化的身份验证机制，如使用二步验证、多因素认证等，以提高系统的安全性，防止黑客使用伪造的身份进行访问。

- 加密通信：使用加密协议（如SSL/TLS）保护敏感数据在传输过程中的安全性，确保数据在传输过程中不被黑客窃听或篡改。

- 访问控制：限制和管理对系统和网络资源的访问权限。使用最小权限原则，确保只有授权的用户能够访问特定的资源，并定期审查和更新访问控制策略。

- 安全意识培训：及时培训用户和员工有关网络安全的最佳实践，教育他们识别和防范黑客攻击，提高组织整体的安全意识。

- 实施网络防火墙：配置和管理网络防火墙，以监控和控制网络流量，防止未经授权的访问和恶意活动。选择适合组织需求的防火墙类型，并根据最佳实践进行配置。

### 7.2.8木马

木马的起源、概念和功能：

- 起源：木马（Trojan Horse）一词来源于希腊神话中的特洛伊木马，意指伪装成正常程序但实际上带有恶意功能的恶意软件。

- 概念：木马是一种具有隐藏性质的恶意软件，冒充合法或有用的程序或文件，但却在用户运行时暗中进行恶意活动。

- 功能：木马的功能各不相同，但通常包括远程控制、数据窃取、系统破坏、恶意广告弹窗、密码记录等。

破坏型木马：

- 概念：破坏型木马是一种具有系统破坏性质的木马，旨在对目标系统进行破坏、损坏或删除数据等。

- 例子：Stuxnet是一种有名的破坏性木马，旨在攻击工业控制系统，破坏伊朗核设施。

密码发送型木马：

- 概念：密码发送型木马是一种通过窃取用户在受感染计算机上输入的密码和敏感信息的木马。

- 例子：ZeuS是一种著名的密码发送型木马，用于窃取银行账户和登录凭证等敏感信息。

远程访问型木马：

- 概念：远程访问型木马是一种允许攻击者远程控制受感染计算机的木马。

- 例子：DarkComet是一种远程访问型木马，可用于远程监视和控制受感染系统。

键盘记录型木马：

- 概念：键盘记录型木马是一种通过记录用户在受感染计算机上的按键活动，以窃取密码和敏感信息的木马。

- 例子：KeyRaider是一种针对iOS设备的键盘记录型木马，用于窃取Apple ID和密码。

DOS攻击型木马：

- 概念：DOS攻击型木马（Denial of Service Trojan）是一种旨在通过发送大量请求使目标系统过载或不可用的木马。

- 例子：Low Orbit Ion Cannon（LOIC）是一种被广泛用于网络攻击的DOS攻击型木马。

代理型木马：

- 概念：代理型木马是一种通过受感染计算机作为代理服务器来隐藏攻击者的真实身份和活动的木马。

- 例子：NetBus是一种早期的代理型木马，用于远程控制受感染计算机。

FTP型木马：

- 概念：FTP型木马是一种通过FTP（文件传输协议）将恶意文件上传到受感染计算机的木马。

- 例子：SubSeven是一种著名的FTP型木马，常用于远程控制和文件传输。

木马的结构：

木马通常由服务端和客户端两个主要组成部分构成。

服务端（Server）：

- 概念：服务端是木马的主要组件，负责接收来自客户端的连接，并执行指令或传输数据。

- 例子：DarkComet RAT（远程访问工具）是一个常见的木马服务端示例。

客户端（Client）：

- 概念：客户端是与服务端通信的组件，通常由攻击者使用。它提供与服务端建立连接并发送指令的接口。

- 例子：程序员自定义的木马客户端。

木马软件的组成部分：

木马软件通常由三个主要组成部分构成：木马配置程序、控制端程序和被控端程序。

木马配置程序：

- 概念：木马配置程序用于设置木马的特定行为和参数，例如监听端口、远程控制设置和隐藏功能等。

- 例子：ZeuS Config是用于配置Zeus木马的工具。

控制端程序（C&C）：

- 概念：控制端程序允许攻击者与木马服务端进行交互，发送指令和接收数据。

- 例子：Phoenix Exploit Kit的控制端。

被控端程序（Agent）：

- 概念：被控端程序是在受感染计算机上执行的木马组件，负责执行指令、收集信息、传输数据等。

- 例子：Zbot（或称为Zeus）是一种常见的被控端程序。

木马的植入方式：

木马可以利用多种途径进行植入，包括以下几种常见方式：

1. 网页脚本（Web Scripting）：

概念：攻击者可以通过在恶意网站上插入木马脚本，利用浏览器的安全漏洞将木马植入到用户的计算机中。

例子：Blackhole Exploit Kit是一种经常用于通过网页脚本植入木马的工具。

2. 电子邮件（Email）：

概念：木马可以伪装为正常的电子邮件附件或链接，诱使用户打开或点击以导致木马的植入。

例子：ILOVEYOU（爱你木马）是一个著名的通过电子邮件传播的木马，它伪装成一个爱情信件附件。

3. 操作系统漏洞Operating System Vulnerabilities）：

概念：木马可以利用操作系统或软件的已知漏洞来进行植入，因此操作系统和软件补丁的及时更新至关重要。

例子：EternalBlue是一种利用Windows操作系统漏洞的木马传播工具，被用于传播WannaCry勒索软件。

4. U盘（USB Drives）：

概念：攻击者可以在U盘中植入木马，一旦用户将U盘连接到受感染的计算机，木马将自动运行。

例子：Stuxnet是一种通过感染U盘来传播的恶意软件，它被用于攻击伊朗的核设施。

5. 程序绑定（Software Bundling）：

概念：木马可以被绑定到其他合法软件的安装程序中，当用户安装该软件时，木马也随之植入。

例子：Superfish是一种常见的预装软件（bloatware），它在某些品牌的个人电脑上绑定了广告插件和恶意软件。

木马的危害：

木马的危害可以多种多样，取决于其功能和攻击者的意图，以下是一些常见的危害：

- 数据窃取：木马可以通过监视用户活动、窃取密码、截取敏感信息等方式获取用户的个人和机密数据。

- 远程控制：木马可以让攻击者远程控制被感染计算机，执行恶意操作、下载其他恶意软件等。

- 系统破坏：某些木马可以对操作系统进行损坏、文件删除、重要数据破坏等，导致计算机无法正常运行。

- 传播恶意软件：木马可以被用作传播其他恶意软件（如勒索软件、僵尸网络等）的入口，进一步危害其他系统和网络。

- 违反用户隐私：木马可以悄悄地监视用户活动、拍摄截屏、记录敏感信息，严重侵犯用户的隐私权。

木马的入侵过程：

木马的入侵过程通常包括以下几个阶段：

1. 配置木马（Configuration）：

概念：攻击者在木马服务端进行配置，设置木马的特定行为和参数，如监听端口、远程控制设置和隐藏功能等。

例子：DarkComet RAT（远程访问工具）是一个常见的木马服务端，攻击者可以使用它来配置木马的各项参数。

2. 传播木马（Propagation）：

概念：木马通过各种手段进行传播，如利用漏洞、发送恶意邮件、植入恶意网站等方式，使用户的计算机感染木马。

例子：Emotet是一种通过垃圾邮件传播的木马，攻击者使用Emotet来发送含有恶意附件或链接的电子邮件以传播木马。

3. 运行木马（Execution）：

概念：一旦木马被用户的计算机感染，木马开始在受感染系统上运行，并执行攻击者设定的指令和功能。

例子：Zeus（或称为Zbot）是一种常见的木马，一旦感染计算机，它可以执行各种指令，如窃取用户信息、拦截网络通信等。

4. 信息泄露（Information Leakage）：

概念：木马可以利用各种技术手段，如键盘记录器、屏幕截图等，窃取用户的敏感信息并将其发送给攻击者。

例子：KeyLogger是一种常见的木马功能，它记录用户的键入操作，以便攻击者获取密码和其他敏感信息。

5. 建立连接（Establishing Connection）：

概念：木马与控制端建立连接，以便攻击者远程操控被感染的计算机，并向其发送指令和获取数据。

例子：NetWire是一种常见的木马，它可以与控制端建立加密连接，使攻击者能够远程控制受感染的计算机。

6. 远程控制（Remote Control）：

概念：一旦与控制端建立连接，攻击者可以通过木马远程控制受感染计算机，并执行各种恶意操作。

例子：Magecart是一个恶意软件家族，攻击者使用它来在受感染网站上注入恶意代码，以窃取用户的支付信息。

防范木马的措施：

以下是一些防范木马的常见措施：

1. 及时更新操作系统和软件：定期安装最新的安全补丁和更新，以修复已知漏洞，减少被利用的机会。

2. 使用可信赖的安全软件：安装有效的防病毒软件和防火墙，及时更新病毒定义文件，对电脑进行实时防护。

3. 警惕电子邮件和附件：不打开来自不熟悉或可疑来源的电子邮件，尤其是包含附件或链接的邮件。可以使用反垃圾邮件功能进行过滤。

4. 定期备份重要数据：将重要文件和数据定期备份到安全的存储介质，以防数据丢失或受到勒索。

5. 使用强密码和多因素认证：使用复杂、独特的密码来保护账户和系统，同时启用多因素认证提供额外的安全层。

6. 不随意下载和安装软件：只从官方或可信赖的来源下载软件，并对下载文件进行安全扫描，避免从非正规渠道获取软件。

7. 谨慎点击网页链接：避免点击可疑或不可信的网页链接，尤其是来自社交媒体、在线广告等渠道。

8. 定期进行系统安全扫描：使用安全软件进行系统全面扫描，及时发现和清除潜在的威胁。

9. 尽量避免使用未授权的插件和应用程序：只安装来自可信赖来源的插件和应用程序，并删除不再使用的插件。

10. 加强员工教育和网络安全意识：通过安全培训和教育，提高员工对网络威胁的认识和警觉性，避免误操作。

11. 使用安全的网络连接：避免使用不安全的公共Wi-Fi网络，尽量使用VPN来加密网络连接。

12. 监测异常行为：定期检查系统日志和网络流量，注意异常活动和不寻常的文件或进程。

## **7.3 计算机病毒**

### 7.3.1 计算机病毒的定义与特点

计算机病毒是一种具有恶意行为的程序或代码，能够自我复制并在计算机系统中传播，对系统和数据造成破坏或干扰。计算机病毒具有以下特点：

1. 寄生性：计算机病毒会依附于合法的程序、文件或系统资源，并将其感染，以便在目标计算机系统中传播和执行。

2. 传染性：计算机病毒可以通过多种方式传播，例如通过网络、可移动存储介质（如USB驱动器）或电子邮件等途径传播到其他计算机系统。

3. 潜伏性：计算机病毒会尽可能地隐藏自己的存在，以避免被发现和清除。它们可以在感染主机上潜伏一段时间，等待触发时机或条件。

4. 隐蔽性：计算机病毒通常会采用一些技术手段来隐藏自身的存在，如加密、压缩、修改文件大小等，以逃避防护软件的检测和移除。

5. 可触发性：计算机病毒可以在特定的条件下触发其恶意行为，如特定日期、用户操作或特定文件的存在等。触发后，病毒可能进行数据破坏、系统崩溃或其他恶意活动。

6. 破坏性：计算机病毒的目标是破坏计算机系统和文件，导致丢失、损坏或不可用的数据或功能。

7. 主动攻击性：某些计算机病毒具有主动攻击性，可以尝试传播、感染和破坏其他计算机系统，并通过蠕虫、僵尸网络或分布式拒绝服务攻击等方式来进行攻击。

计算机病毒的生命周期

计算机病毒通常会经历以下生命周期阶段：

1. 传播阶段：病毒在此阶段尝试传播到其他计算机系统。它可以利用网络漏洞、可移动存储介质、恶意下载程序或社交工程等方式进行传播。

2. 感染阶段：一旦成功传播到目标计算机系统，病毒会将自己插入或修改合法程序或文件，以便在系统中的其他位置进行感染。

3. 潜伏阶段：在此阶段，病毒隐藏并潜伏在感染的系统中，等待触发时机、条件或特定的触发事件。

4. 触发阶段：当病毒接收到触发条件（如特定日期、用户操作）时，它会激活并执行其恶意行为，可能导致数据损坏、系统崩溃等。

5. 传播更新阶段：部分病毒会尝试通过更新自身代码或利用新的漏洞来绕过防护措施，并进行新一轮的传播和感染。

计算机病毒的结构

计算机病毒通常由以下四个主要组成部分构成：

1. 引导模块：引导模块位于病毒代码的开头部分，负责在感染过程中加载和执行病毒代码。

2. 感染模块：感染模块是病毒的核心组件，负责寻找目标文件或程序，并将病毒代码插入或修改目标文件，以实现感染目标的目的。

3. 破坏模块：破坏模块是病毒的恶意行为部分，负责破坏文件、系统或数据，可能包括删除文件、破坏数据或破坏系统功能等。

4. 触发模块：触发模块用于触发病毒的恶意行为，可以根据特定的条件或事件来触发。触发后，病毒可能会执行破坏性操作或继续传播。

### 7.3.2计算机病毒的分类

计算机病毒的分类（按媒体、传染方式、入侵途径和破坏能力）

1. 按病毒存在的媒体分

网络病毒：

- 概念：网络病毒通过网络传播，感染连接在网络上的计算机系统。它们可以利用网络漏洞、恶意下载或通过电子邮件等途径传播。

- 例子：Code Red和SQL Slammer是著名的网络病毒，前者通过IIS服务器漏洞进行传播，后者利用Microsoft SQL Server的漏洞进行传播。

文件病毒：

- 概念：文件病毒通过感染文件或程序来传播。它们会依附于合法的文件上，并在被执行或打开时将自身复制到其他文件中。

- 例子：Melissa和ILOVEYOU是著名的文件病毒，前者通过感染Microsoft Word文档传播，后者通过电子邮件附件传播。

引导型病毒：

- 概念：引导型病毒感染计算机的引导扇区或主引导记录，它们在计算机启动时被加载，并在系统启动过程中传播到其他存储介质。

- 例子：Stoned和Michelangelo是著名的引导型病毒，前者感染计算机的硬盘引导扇区，在系统启动时被加载。

2. 按传染方式分

引导型病毒：

- 概念：引导型病毒专门感染计算机的引导扇区或主引导记录，以在系统启动时传播。

- 例子：Form和Polyboot是著名的引导型病毒，前者感染计算机的引导记录，传播到其他存储介质。

文件型病毒：

- 概念：文件型病毒通过感染文件来传播。它们会将病毒代码嵌入到合法文件的程序段中，并在文件执行时将其加载到内存中。

- 例子：Sality和Conficker是著名的文件型病毒，前者通过感染可执行文件和DLL文件传播，后者通过利用Windows漏洞进行传播。

混合型病毒：

- 概念：混合型病毒结合了引导型病毒和文件型病毒的特点，可以通过引导扇区和文件的感染来传播。

- 例子：Hokum和Stream是著名的混合型病毒，它们可以同时感染引导扇区和文件。

宏病毒：

- 概念：宏病毒是利用应用软件中的宏语言的功能来感染和传播的病毒。它们通常隐藏在文档文件（如Word或Excel）的宏代码中。

- 例子：Melissa和Macro/W97M是著名的宏病毒，它们利用Microsoft Office中的宏功能进行传播。

3. 按入侵途径分

源码病毒：

- 概念：源码病毒通过感染软件的源代码来传播，以在编译过程中将病毒代码注入到最终的可执行文件中。

- 例子：Morris和Stuxnet是著名的源码病毒，前者感染了UNIX系统上的源代码文件，后者利用USB设备传播并感染了工业控制系统。

入侵型病毒：

- 概念：入侵型病毒通过攻击系统的弱点、漏洞或通过网络服务进入计算机系统。

- 例子：Nimda和Blaster是著名的入侵型病毒，前者通过利用多个漏洞进行传播，后者通过攻击Windows操作系统进行传播。

操作系统病毒：

- 概念：操作系统病毒直接感染计算机操作系统的关键组件和文件，以在系统内传播和执行恶意行为。

- 例子：CIH和Sasser是著名的操作系统病毒，前者感染Windows操作系统的可执行文件和BIOS芯片，后者可以利用Windows漏洞进行传播。

外壳病毒：

- 概念：外壳病毒通过感染可执行文件的执行代码部分来传播，以便在文件执行时将病毒加载到系统中。

- 例子：W32/Virut和W95/CIH是著名的外壳病毒，它们感染可执行文件并传播到其他文件。

4. 按病毒破坏的能力分

无害型病毒：

- 概念：无害型病毒不会对系统和数据造成明显破坏，主要用于展示病毒本身的存在和传播。

- 例子：Cookie和NYB是无害型的计算机病毒，它们主要用于演示和传播病毒。

无危险型病毒：

- 概念：无危险型病毒不会对系统和数据造成严重破坏，但可能会导致计算机系统的不稳定。

- 例子：Cascade和Stoned是无危险型病毒，它们可能导致系统速度变慢或不稳定。

危险型病毒：

- 概念：危险型病毒可以对系统和数据造成破坏，可能导致文件损坏、数据丢失或系统崩溃。

- 例子：Melissa和CIH是危险型病毒，前者通过感染Word文档传播，后者可以破坏硬盘数据。

非常危险型病毒：

- 概念：非常危险型病毒对系统和数据具有特别严重的破坏能力，可以导致系统无法恢复，数据无法恢复或计算机彻底瘫痪。

- 例子：W32/Mydoom和Code Red是非常危险型病毒，前者可以瘫痪计算机网络，后者可以导致网站无法访问。

### 7.3.3计算机病毒的传播途径与预防

1. 计算机病毒的传播途径

计算机病毒可以通过以下途径进行传播：

- 电子邮件附件：恶意软件或病毒常常通过电子邮件附件传播。用户打开或下载附件时，病毒就有可能感染计算机。

- 受感染的网站：某些网站可能被黑客植入恶意代码，当用户访问这些网站时，他们的计算机就可能被感染。

- 可移动存储介质：通过USB闪存驱动器、移动硬盘、光盘等可移动存储介质传输的文件可能带有病毒。当用户连接这些介质或打开其中的文件时，病毒就可能感染计算机。

- 恶意下载：下载来路不明的文件、软件或媒体文件时，很可能会下载到带有病毒的文件。

- P2P文件共享：通过P2P（点对点）文件共享软件下载文件时，用户可能同时下载到病毒。

2. 计算机病毒的最新趋势

计算机病毒的最新趋势包括以下几点：

- 社交工程攻击：病毒制作者通过利用社交工程技巧，例如欺骗性链接、诱饵内容等，来诱使用户点击恶意链接或下载恶意文件。

- 针对移动设备：随着移动设备的普及，病毒制作者也将目光转向了移动平台。移动设备上的病毒会通过应用下载、恶意链接和可移动存储介质等途径传播。

- 加密勒索软件：加密勒索软件通过加密用户的文件，并勒索赎金以解密文件。这种恶意软件变得越来越普遍，病毒制作者通过不断改进勒索软件的技术来获取利益。

- 远程访问工具（RAT）：远程访问工具是一种恶意软件，可能被黑客用于远程控制被感染计算机。黑客可以通过RAT窃取敏感信息、监视操作、进行远程攻击等。

3. 计算机病毒的防治措施

为了防止计算机病毒的感染，可以采取以下防治措施：

- 安装可靠的防病毒软件：选择一款受信任的、经过认证的防病毒软件，并将其及时更新到最新版本。

- 更新系统和应用程序：及时安装操作系统和应用程序的安全更新和补丁，以修复已知漏洞，减少被攻击的风险。

- 注意电子邮件和下载的内容：不打开来路不明的电子邮件附件，避免下载未经认证的软件、文件或媒体内容。

- 小心通过可移动存储介质传输的文件：使用可靠的防病毒软件扫描可移动存储介质上的文件，确保它们没有感染。

- 避免点击可疑链接：不要点击来路不明的链接，尤其是通过社交媒体、电子邮件或即时消息发送的链接。

- 备份数据：定期备份系统和重要数据，以防止数据丢失。

4. 计算机感染病毒后常见的症状

计算机感染病毒后，可能出现以下常见症状：

- 性能下降：计算机变得缓慢，常常出现无故卡顿、延迟或响应不良。

- 弹窗广告：频繁弹出广告窗口，即使在未打开浏览器的情况下也会出现。

- 文件损坏或丢失：重要文件损坏、丢失或无法访问。

- 网络问题：无法连接到互联网、无法访问特定网站，或者发现网络流量异常。

- 新增或修改的文件：出现未知的文件、程序或桌面快捷方式。

5. 计算机感染病毒后的防治措施

如果计算机感染了病毒，可以采取以下措施来防治：

- 隔离受感染的计算机：将受感染的计算机从网络中隔离，以避免病毒进一步传播。

- 扫描和清除病毒：使用可靠的防病毒软件对计算机进行全面扫描，并按照软件指示清除病毒。

- 更新系统和应用程序：确保操作系统和应用程序已更新到最新版本，以修复漏洞。

- 修改密码：如果计算机上保存着重要账户的登录信息，更改这些账户的密码，以防黑客窃取敏感信息。

- 恢复数据：如果数据被加密或损坏，可以尝试从备份中恢复数据。

### 7.3.4常见的计算机病毒

常见的计算机病毒和木马程序

计算机病毒的命名格式

计算机病毒的命名通常遵循前缀、病毒名和后缀的格式。下面是一些常见的命名格式：

前缀：前缀通常由字母或数字组成，用于标识病毒的类型或特征。例如：W32、Trojan、Win32等。

病毒名：病毒名描述了病毒的特定名称或别名。例如：Mydoom、Conficker、Sasser等。

后缀：后缀指示了病毒感染的文件类型或特征。例如：.exe、.doc、.bat等。

以下是一些常见的计算机病毒的例子：

- W32.Sobig.F@mm：这是一种以W32作为前缀，Sobig为病毒名，.F为病毒的特征后缀，通过电子邮件附件进行传播，利用受感染计算机的邮件系统发送自身副本。

- Trojan.Ransom.WannaCry：这是一种以Trojan为前缀，Ransom为病毒名，WannaCry为特定名称的病毒，通过利用Windows操作系统的漏洞进行传播，加密用户的文件并勒索赎金。

常见病毒的概念和例子

木马病毒（Trojan）：木马病毒是一种伪装成合法程序的恶意软件，通过欺骗用户获取其信任，进而实施恶意行为。例如：Back Orifice是一种远程控制木马程序，允许黑客远程访问被感染计算机并执行恶意操作。

黑客病毒：黑客病毒是由黑客创建的恶意软件，通常用于攻击其他计算机系统或网络。例如：Stuxnet是一种针对工业控制系统的恶意软件，针对伊朗的核设施进行攻击。

脚本病毒：脚本病毒是一种利用脚本语言编写的恶意代码，可以通过运行脚本文件感染计算机。例如：LoveLetter是一种脚本病毒，通过电子邮件传播，感染用户的计算机并破坏文件。

系统病毒：系统病毒是一种感染计算机操作系统的恶意软件，它会修改或破坏操作系统的核心组件，导致系统功能异常或崩溃。例如：Code Red是一种利用微软IIS服务器漏洞进行传播的系统病毒。

宏病毒：宏病毒是一种嵌入在文档或电子表格中的恶意宏代码，会在用户打开文件时触发执行，并可能感染计算机或执行恶意操作。例如：Melissa是一种宏病毒，通过电子邮件附件传播，感染用户的计算机。

蠕虫病毒：蠕虫病毒是一种自我复制的恶意软件，可以通过网络传播到其他计算机，导致网络拥塞和系统性能下降。例如：ILOVEYOU是一种蠕虫病毒，通过电子邮件附件传播，并严重影响计算机和网络系统。

影响力较大的病毒表格：

| 病毒名称 | 年份 | 发明人物 | 感染数量 | 感染症状 | 影响 |
| --- | --- | --- | --- | --- | --- |
| Elk Cloner | 1982 | Richard Skrenta | 较少 | 无 | Elk Cloner是第一个在个人电脑上感染Apple II系统的病毒，虽然感染数量较少，但引起了广泛关注。 |
| Melissa | 1999 | David L. Smith | 数十万 | 电子邮件滥用、系统崩溃、网络拥塞 | Melissa是通过感染微软Office文档中的宏而传播的病毒，迅速在互联网上传播并造成大规模破坏。 |
| Love Bug | 2000 | Onel de Guzman | 数百万 | 密切关注邮件、系统崩溃、破坏文件 | Love Bug是一种电子邮件蠕虫，通过欺骗性邮件附件传播，对个人和组织的电子邮件系统造成了严重影响。 |
| 求职信病毒 | 2004 | Farid Essebar | 几千 | 个人信息泄露、系统崩溃 | 求职信病毒通过即时通讯软件传播，通过发送伪造的求职信来欺骗用户，造成一些用户信息泄露。 |
| 红色代码病毒 | 2001 | 红色代码团队 | 数百万 | 网页重定向、网络瘫痪 | 红色代码病毒通过植入恶意网页脚本，在互联网上造成大规模网站断线和网络瘫痪。 |
| 尼姆达病毒 | 2001 | 尼古拉斯·费拉瓦 | 数百万 | 系统崩溃、网络拥塞 | 尼姆达病毒通过利用各种漏洞进行传播，感染了数百万计算机，对网络和系统造成了严重干扰。 |
| 灰鸽子病毒 | 2002 | 未知 | 数百万 | 计算机性能下降、网络拥塞 | 灰鸽子病毒利用Windows漏洞传播，在数百万计算机上感染并造成网络拥塞和系统性能下降。 |
| 震荡波病毒 | 2003 | Slammer病毒的作者 | 数百万 | 网络瘫痪、数据库服务中断 | 震荡波病毒通过利用SQL Server漏洞传播，在互联网上造成数百万服务器网络瘫痪和服务中断。 |
| 熊猫烧香病毒 | 2006 | 李俊 | 数以百万计 | 网络拥塞、计算机性能下降 | 熊猫烧香病毒是一种蠕虫病毒，感染数以百万计的计算机，严重影响了网络和计算机的正常运行。 |
| AV终结者病毒 | 2012 | 未知 | 数百万 | 禁用安全软件、系统崩溃 | AV终结者病毒是一种自我保护的恶意软件，通过禁用计算机上的安全软件对计算机造成严重威胁。 |
| 永恒之蓝病毒 | 2017 | NSA（美国国家安全局） | 数十万至数百万 | 系统崩溃、勒索行为、网络传播 | 永恒之蓝病毒利用Windows操作系统漏洞进行传播，导致数十万至数百万计算机遭受攻击和感染。 |
| 骷髅病毒 | 1996 | 谢益辉（Ghost） | 几千 | 系统崩溃、删除系统文件 | 骷髅病毒是最早出现的Windows系统文件传送工具，在感染计算机后会导致系统崩溃和文件丢失。 |
| QQ尾巴 | 2007 | 未知 | 数百万 | 个人信息泄露、系统崩溃 | QQ尾巴是通过QQ聊天软件进行传播的木马程序，感染了数百万计算机，对用户的信息安全构成威胁。 |
| 彩虹猫病毒 | 2011 | 未知 | 数千至数百万 | 个人信息泄露、系统崩溃 | 彩虹猫病毒是一种文件攻击病毒，主要通过游戏下载来源传播，对计算机系统和用户信息造成威胁。 |
| horror病毒 | 1990 | Mark Washburn | 几百 | 系统崩溃、文件删除 | horror病毒是最早在互联网上传播的病毒之一，对感染计算机进行破坏并删除文件。 |
| 勒索病毒 | 2012 | 未知 | 数十万至数百万 | 文件加密、勒索行为 | 勒索病毒通过加密用户文件并要求赎金来勒索用户，感染了数十万至数百万计算机，造成了严重的经济损失和数据丢失。 |

### 7.3.5计算机病毒的检测与清除

计算机病毒的检测与清除方法包括以下几种常见的技术：

1. 特征代码法（Signature-based Detection）：

概念：特征代码法通过识别计算机病毒已知的唯一特征代码来进行检测。这些特征代码通常是病毒的特定模式、签名或独特行为。

例子：防病毒软件会使用病毒特征数据库，其中包含各种已知病毒的特征代码。当系统进行扫描时，软件会与数据库中的特征代码进行比对，以找出可能的病毒。

2. 行为监测法（Behavior-based Detection）：

概念：行为监测法通过观察计算机系统的行为活动，检测异常或恶意行为来判断是否存在病毒感染。它关注病毒的活动模式、文件操作、注册表修改等行为特征。

例子：某些防病毒软件会监视系统进程、文件系统、注册表等，当发现可疑的行为模式时，会发出警报或采取相应的防护措施。

3. 比较法（Heuristic-based Detection）：

概念：比较法通过与已知病毒行为模式进行比较，检测系统中的非常规或可疑活动。它不仅依赖于特征代码，还关注病毒的行为特征和模式。

例子：一些防病毒软件使用启发式算法来识别新型病毒。它们分析文件的操作行为、代码的执行方式等，以判断是否存在病毒或恶意软件。

4. 软件模拟法（Emulation-based Detection）：

概念：软件模拟法是通过在虚拟环境中模拟执行可疑文件，监测其行为和活动，以确定是否存在病毒感染。它可以检测未知的病毒或变种。

例子：一些防病毒软件使用虚拟机技术，运行可疑文件并监测其行为。如果文件表现出病毒行为，软件会将其标记为恶意并采取相应的措施。

防病毒软件：

防病毒软件是用于预防和检测计算机病毒的软件。它们可以提供实时保护、自动更新病毒定义文件、进行系统扫描等功能。常见的防病毒软件包括 Norton Antivirus、McAfee、Kaspersky、360安全卫士、金山毒霸等。

计算机病毒的检测与清除通常包括以下几个阶段：

1. 检测病毒存在：使用防病毒软件对计算机进行全面扫描，以发现潜在的病毒感染。一般包括对文件、内存、注册表和启动项等的扫描。

2. 确认病毒类型：通过病毒特征码、行为分析和比对算法等，确认病毒的类型、变种和级别。这有助于选择合适的清除策略。

3. 隔离受感染的文件：将受感染的文件从系统中隔离出来，以防止病毒进一步传播和对系统造成更多危害。

4. 清除病毒：根据病毒类型和感染程度，采取相应的清除措施。常见的清除方法包括删除感染的文件、修复受损的文件、恢复受感染的系统状态等。

计算机病毒的清除措施：

以下是一些常见的计算机病毒清除措施：

1. 使用实时防病毒软件：安装并保持最新的防病毒软件，确保其具备实时保护和自动病毒库更新功能。

2. 进行全面系统扫描：定期对整个系统进行全面扫描，包括硬盘、内存、注册表和启动项等，以检测和清除潜在的病毒。

3. 删除受感染的文件：将被检测到的病毒文件移至隔离区，并在确认不会对系统造成危害后，彻底删除这些受感染的文件。

4. 修复受损的文件：对部分病毒感染造成的文件损坏进行修复，恢复文件的原始状态。

5. 恢复系统配置：对受感染的系统配置文件进行修复或还原，确保系统正常运行并消除潜在的漏洞。

6. 更新操作系统和应用程序：定期安装最新的操作系统和应用程序补丁，以修复已知的漏洞，减少病毒入侵机会。

7. 启用防火墙：配置防火墙以阻止未经授权的访问和网络通信，提供额外的安全层面。

8. 定期备份数据：定期备份重要文件和数据，以防止数据丢失或受到勒索软件等攻击。

9. 加强员工教育和网络安全意识：通过培训和教育提高员工对计算机病毒的认识和警觉性，减少误操作和不慎下载感染病毒的风险。

## **7.4网络道德**

### 7.4.1网络道德的定义和原则

网络道德的定义和原则

网络道德的定义：

网络道德是在计算机和互联网使用过程中遵循的伦理和道德准则。它关注个人和群体在网络空间中承担道德责任，并遵守公认的道德原则和价值观。

网络道德的基本原则：

1. 全民原则：

- 平等原则：每个网络用户都应该受到平等对待，无论其身份或背景如何。

例子：不进行网络歧视、不侵犯他人的隐私和权益。

- 公正原则：网络用户应该遵循公正的行为准则，对待他人和解决纠纷。

例子：尊重他人的知识产权，遵守版权法和其他法律法规。

2. 兼容原则：

- 概念：网络用户应该遵守共同的规则和标准，以确保网络的稳定和安全。

- 例子：遵守网络协议和标准，不故意干扰网络的正常运行。

3. 互惠原则：

- 概念：网络用户应该相互尊重、互相支持，并遵守公平的行为准则。

- 例子：尊重他人的观点和意见，不进行网络欺凌或恶意中伤。

网络道德的特点：

1. 自主性：

- 概念：网络道德要求个体在使用计算机和互联网时具有独立思考和自主选择的能力。

- 例子：个体需要在发布内容时自行判断是否合适，是否存在侵权或违法行为。

2. 开放性：

- 概念：网络道德强调信息的共享和开放，促进信息的自由流通。

- 例子：支持公开讨论和言论自由，尊重他人的知识产权和信息隐私。

3. 多元性：

- 概念：网络道德承认和尊重不同文化、价值观和观点的存在，鼓励多元性。

- 例子：尊重网络中的多元文化现象，不歧视或攻击他人的种族、宗教或性别。

网络道德的规范：

美国计算机伦理协会的计算机理论十诫表格：

|  |
| --- |
| 计算机理论十诫 |
| 1. 不干扰他人计算机的正常操作 |
| 2. 不侵犯其他人的计算机隐私 |
| 3. 不侵犯软件版权和知识产权 |
| 4. 尊重他人的计算机资源和个人观点 |
| 5. 使用计算机技术服务于人类社会，避免对人类社会造成伤害 |
| 6. 不滥用计算机进行破坏、偷窃或欺骗 |
| 7. 遵纪守法，遵守计算机伦理准则和法律规定 |
| 8. 不使用计算机技术侵害他人权益 |
| 9. 尊重计算机系统的安全和隐私 |
| 10. 履行计算机专业人士的职业责任 |

网络用户的职业道德：

网络从业人员应遵守职业道德，包括保护用户的隐私和信息安全，不滥用职权等。

文明上网行为的例子：

- 遵守网络礼仪，尊重他人的言论自由。

- 尊重他人的隐私，不散布谣言或攻击性内容。

不文明行为的例子：

- 进行网络欺凌、网络诈骗等违法行为。

- 侵犯他人隐私，散布虚假信息或恶意中伤他人。

### 7.4.2网络犯罪

网络犯罪的概念：

网络犯罪是指利用计算机和互联网技术进行犯罪活动的行为。它涉及通过网络攻击、网络欺诈、网络盗窃等手段进行非法操作或获取利益的行为。

网络犯罪的特点：

1. 匿名性：网络犯罪往往通过隐藏身份或使用匿名技术，使得犯罪者很难被追踪和辨认。

2. 国际性：互联网无国界的特点使得网络犯罪往往跨越国家边界，难以处理和追责。

3. 技术性：网络犯罪利用复杂的计算机和互联网技术进行实施，对受害者造成极大的伤害和损失。

常见的网络犯罪形式：

1. 黑客攻击：入侵他人计算机系统，窃取个人信息、盗取财产或破坏网络安全。

2. 网络诈骗：通过欺诈手段获取他人财产，如钓鱼网站、虚假购物网站、电信诈骗等。

3. 网络盗窃：盗窃他人的电子数据、软件、版权作品或知识产权。

4. 赌博和非法赌博：通过互联网进行各种赌博活动，包括网络赌球、网络扑克等。

5. 色情和色情暴力信息传播：通过互联网传播非法的色情信息或暴力内容。

预防网络犯罪：

1. 更新和加强安全措施：包括安装安全更新、使用防火墙、设置强大的密码等。

2. 提高网络安全意识：加强对网络安全的培训和教育，提醒用户避免点击可疑链接或下载不明文件。

3. 加强法律法规和执法力度：制定和完善与网络犯罪相关的法律法规，建立健全执法机构。

4. 开展国际合作：加强跨国合作，共同打击跨国网络犯罪活动。

5. 加强技术研发和创新：不断提高网络安全技术水平，及时应对新型网络犯罪手段。

## **7.5知识产权与计算机软件产权**

### **7.5.1知识产权**

知识产权的概念：

知识产权是指对于知识、创作和创新的产权保护。它包括对于发明、原创作品、商标和商业秘密等的法定权利。知识产权的保护旨在鼓励创新和创作，促进知识的传播和经济发展。

知识产权的特点：

1. 无形财产：知识产权所保护的是无形的思想、创意和创新成果，不同于有形财产的物品。

2. 双重性：

- 概念：知识产权既是对个人创作成果的保护，也是对社会共同利益和文化遗产的保护。

- 例子：专利保护既鼓励发明者的创新，也促进了技术的进步。

3. 专有性：

- 概念：知识产权赋予权利人独有的权利，以限制他人在未经许可的情况下使用和复制其创作成果。

- 例子：商标所有人拥有对商标的专有权，在特定范围内可以拒绝他人对商标的使用。

4. 时间性：

- 概念：知识产权的有效期有限，根据不同类型的知识产权，保护时间不同。

- 例子：专利权一般有效期为20年，商标可连续更新和维持，版权在作者终身加上70年有效。

5. 地域性：

- 概念：知识产权的保护范围通常限定在国家或地区边界之内。

- 例子：在美国获得的知识产权通常只在美国境内有效，需要在其他国家或地区分别申请和获得保护。

自然人和法人

自然人：

自然人是指具备法律能力的个体，有权享受和承担法律权益和义务。

特点：

1. 生物学身份：自然人是指具有生物学身份的个人，拥有特定的生物属性。

2. 个体身份：自然人是单个个体，在法律上具有特定的权利和义务。

3. 民事权利能力：自然人具有通过民事行为来获得权利和履行义务的能力。

4. 民事行为能力：自然人具备独立行使民事权利和履行民事义务的能力。

法人：

法人是指根据法律设立并具有法律地位的组织或机构，可以拥有和行使权利，并承担责任。法人可以是企业、非营利组织、政府机构等。

特点：

1. 法律地位：法人依法成立并登记注册，具有独立法律地位和法人资格。

2. 组织实体：法人是一个组织实体，可以拥有和行使权利，承担法律责任。

3. 法人责任：法人可以独立承担债务、侵权责任等法律责任。

4. 经济实体：法人可以进行经济活动，拥有财产和经济利益。

知识产权的保护时间：

1. 发明专利：

- 概念：对新的技术发明的保护，使发明者在特定时间内独享权利。

- 例子：比如一种新型机械装置的构造，可以通过发明专利得到保护。发明专利的保护期限为申请日起的20年。

2. 实用新型和外观设计专利：

- 概念：实用新型专利保护对于物品的新的形状、结构或组合的保护；外观设计专利保护对于物品的新的外观设计的保护。

- 例子：一种新型手机的机身形状可以通过实用新型专利进行保护，而手机外观的外观设计则可以通过外观设计专利进行保护，保护期为10年。

3. 注册商标：

- 概念：商标是用于标识特定商品或服务来源的标志，通过注册商标进行保护。

- 例子：著名品牌如阿里巴巴的商标"Alibaba"和华为的商标"Huawei"都可以通过注册商标获得保护。商标的保护期限为10年，可以连续续展。

4. 作品：

- 概念：版权保护对于原创作品的保护，如文学、艺术、音乐、电影等作品的权益。

- 例子：一本小说、一幅画作、一首歌曲等都可以通过版权获得保护。自然人作品的版权保护期限为作者终身加上50年，法人或非法人单位的作品的版权保护期限为首次发表后50年，但作品创作完成后50年内未发表，不受著作权法保护。

知识产权的相关法律：

知识产权保护法律主要包括：

- 专利法：用于保护发明、实用新型和外观设计专利。

- 商标法：用于保护商标权和商标的独占使用权。

- 著作权法：用于保护著作权，包括文学、艺术、音乐、电影等作品的权益。

- 反不正当竞争法：用于保护市场秩序，保护商业秘密等。

这些法律体系为知识产权的持有者提供了法律保护和救济途径，以维护创作成果和创新的权益。

### 7.5.2计算机软件产权

计算机软件知识产权：

计算机软件知识产权是指对计算机软件的法律保护，包括软件著作权和其他相关权利。它是保护软件开发者的权益和鼓励创新的重要手段。

软件著作权：

软件著作权是指对计算机软件的创作权，由软件作者拥有。

- 人身权：

概念：软件作者享有将自己的名字标识在所创作的软件中的权利。

例子：在软件的“关于”页面或版权声明中标明软件作者的姓名或名称。

- 财产权：

概念：软件作者对软件的经济权益和控制权，包括复制权、发行权等。

例子：软件作者可以决定是否允许他人复制、分发以及销售其软件。

- 发表权：

概念：软件作者有权决定何时公开发布其软件。

例子：软件作者可以决定何时发布软件的正式版本，并决定发布的渠道和方式。

- 使用权：

概念：软件作者对软件的使用进行限制和授权。

例子：软件作者可以制定软件使用许可证，明确软件的使用条件和限制。

- 开发者身份权：

概念：软件作者对于软件的署名、声明和维护等权利。

例子：软件作者可以在软件中声明自己的身份，保留对软件的开发者身份的权利。

- 使用许可证和获得报酬权：

概念：软件作者可以决定以何种限制和条件向他人授权使用软件，并获得相应的报酬。

例子：授予他人有限的使用权或者提供授权许可证，以及收取相应的授权费用或使用费用等。

- 转让权：

概念：软件作者可以将软件著作权出售或转让给他人。

例子：软件作者可以将自己开发的软件著作权出售给其他公司，转让所有权和控制权。

软件著作权人：

软件著作权人是指拥有对软件著作权的权利人。根据软件的开发方式不同，软件著作权人可以是合作开发方或委托开发方。

- 合作开发：

概念：多个实体共同参与软件开发，共享软件著作权。

例子：多个开发者、公司或组织共同开发一款软件，并达成共享著作权的协议。

- 委托开发：

概念：委托开发方将软件开发任务交给第三方开发，并依法享有著作权。

例子：一家公司委托一家软件开发公司开发软件，委托开发方成为著作权人。

软件知识产权的特征：

1. 移动性：软件可被复制、传输、分发，使其易于在不同的设备和平台上部署和使用。

2. 增值性：软件可通过不断的更新和升级进行功能改进和性能优化，具有较高的增值潜力。

3. 非排他性：一个软件可以被多个用户在不同设备上同时使用，而不会相互干扰。

4. 技术创新性：软件开发可以通过技术创新推动行业发展和进步。

软件知识产权保护的意义：

1. 保护软件创作者的权益，鼓励创新和创造。

2. 促进软件产业的发展和壮大，提高软件的质量和可靠性。

3. 维护市场秩序，遏制盗版和侵权行为，保护合法软件市场的健康发展。

软件著作权的保护期：

根据著作权法，软件著作权的保护期为25年，可以续展，但保护期最长不超过50年，软件开发者的开发者身份权不受限制。

软件著作权的保护级别：

- 开源软件：

概念：允许用户自由查看、使用、修改和分发源代码的软件。

例子：Linux操作系统、Apache服务器等。

- 闭源软件：

概念：不公开源代码，而且限制使用和修改的软件。

例子：Microsoft Office、Adobe Photoshop等。

- 共享软件：

概念：在符合特定授权协议的前提下，允许用户免费获取和使用软件。

例子：MySQL数据库、VirtualBox虚拟机等。

- 免费软件：

概念：可以免费获取和使用的软件，但不一定开源。

例子：Mozilla Firefox、VLC media player等。

- 自由软件：

概念：允许用户自由获取、使用、修改和分发的软件，且开源。

例子：GNU项目下的软件，如GNU Emacs、GNU GCC等。

这些保护级别根据软件作者对软件的使用、修改和分发的限制程度不同，给用户提供了不同的权利和使用方式。

软件著作权的使用许可：

软件著作权的使用许可是指软件著作权人授予他人对其拥有的软件著作权进行一定程度的使用的权利。

- 使用许可：

概念：软件著作权人向他人授予使用其软件的特定权限和条件。

例子：一个软件公司授予一家企业使用其开发的专有软件，并规定了具体的使用范围和限制。

使用许可的种类：

1. 独占使用许可：

概念：被授权者在特定的范围和时间内独享使用软件的权利，其他人不能使用同样权利的许可。

例子：一个企业获得了一款软件的独占使用许可，其他竞争对手不能使用该软件。

2. 排他使用许可：

概念：被授权者在特定的范围和时间内独享使用软件的权利，但软件著作权人自身也可以使用同样权利的许可。

例子：一个企业获得了一款软件的排他使用许可，其他竞争对手也可以使用该软件，但需经过软件著作权人的授权。

3. 普通使用许可：

概念：被授权者获得基本的使用权，但其他人也可以获得同样权利的许可。

例子：一家公司购买了一款商业软件的普通使用许可，其他公司也可以购买相同的许可并使用该软件。

使用许可的特点：

- 被许可人：

概念：获得软件使用许可的人或组织。

例子：一个公司、组织或个人获得了软件著作权人授予的使用许可。

- 被保护对象：

概念：软件著作权人对其软件享有著作权的范围和内容。

例子：软件著作权人对其开发的软件享有使用、复制、修改、分发等权利，这些权利在许可中可能被授予给被许可人。

软件著作权的限制：

- 合理使用：

概念：指在合理范围内对软件进行使用和利用，符合法律规定的合理使用原则。

例子：在符合法律规定的前提下，使用软件进行学习、研究、个人备份等属于合理使用范围。

- 法定许可：

概念：软件著作权法规定的特殊许可情况下，可以在未获得软件著作权人许可的情况下使用软件。

例子：法律可能规定一些情况下可以在特定条件下使用软件，如备份软件、安全测试等。

软件使用者的权利：

概念：根据软件著作权法或许可协议，软件使用者可以合理使用软件的一些权利和特定权限。

例子：使用者可能会被授权在特定设备上安装软件、进行必要的备份、进行性能优化调整等。

Github是一个基于Web的代码托管平台，提供了版本控制、协作和代码管理的功能。开发者可以使用Github创建、存储和共享代码仓库，并与其他开发者合作开发项目。

Github许可证表格是指在Github上托管项目时，开发者可以选择一种适合自己项目的开源许可证，并在项目的根目录中创建一个LICENSE文件来说明项目所采用的许可证类型及相关信息。

以下是Github许可证表格：

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 许可证 | 商用性 | 闭源性 | 版权说明 | 描述 |
| MIT License | 允许 | 允许 | 版权归属于原作者 | 简洁、宽松的许可证 |
| GNU GPL v3 | 允许 | 要求 | 版权归属于原作者 | 强调保护开源软件自由 |
| Apache License 2.0 | 允许 | 允许 | 版权归属于原作者 | 广泛使用的业界许可证 |
| BSD 3-Clause | 允许 | 允许 | 版权归属于原作者 | 简洁、灵活的许可证 |
| Mozilla Public License 2.0 | 允许 | 允许 | 版权归属于原作者 | 强调保护用户权利 |
| GNU AGPL v3 | 允许 | 要求 | 版权归属于原作者 | 强调网络应用的开源协议 |
| Unlicense | 允许 | 允许 | 无版权归属 | 放弃所有权利的许可证 |
| GNU LGPL v3 | 允许 | 要求 | 版权归属于原作者 | 对于程序库使用的开源协议 |
| Creative Commons Zero v1.0 Universal | 允许 | 允许 | 无版权归属 | 公有领域中的免费文化协议 |
| Eclipse Public License 2.0 | 允许 | 允许 | 版权归属于原作者 | 企业开发的开源协议 |
| GNU FDL v1.3 | 允许 | 要求 | 版权归属于原作者 | 强调文档的开源协议 |
| ISC License | 允许 | 允许 | 版权归属于原作者 | 简洁、宽松的许可证 |
| Microsoft Public License | 允许 | 要求 | 版权归属于原作者 | 适用于微软开源项目 |