第四章 计算机网络

4.1 计算机网络概述

4.1.1 计算机网络的定义

- 计算机网络：利用通信线路和通信设备，将地理位置不同的、具有独立功能的多台计算机及其外部设备连接起来，在网络操作系统、网络管理软件及网络通信协议的管理和协调下，实现资源共享和信息传递的计算机系统。
- 计算机网络的发展经历了四个阶段：
  - 第一阶段：面向终端的计算机网络
  - 第二阶段：计算机-计算机网络
  - 第三阶段：开放式标准化网络
  - 第四阶段：因特网广泛应用与高速网络技术发展阶段

4.1.2 计算机网络的功能

- 资源共享
- 数据通信
- 分布处理
- 提高计算机的可靠性和可用性
- 负载均衡

4.1.3 计算机网络的组成

- 从组成部分上看，一个计算机网络由硬件、软件、协议三个主要部分组成。
- 从逻辑功能上看，计算机网络可以分为资源子网和通信子网两个部分。
- 资源子网：负责信息处理，为网络用户提供网络资源及网络服务。
- 通信子网：负责数据通信，为资源子网提供传输服务。

4.1.4 计算机网络的分类

- 按覆盖范围分类：
  - 局域网（LAN）：覆盖范围一般在几千米以内，如一个办公室、一栋楼、一个校园。
  - 城域网（MAN）：覆盖范围一般在几十千米以内，如一个城市。
  - 广域网（WAN）：覆盖范围一般在几千千米以内，如一个国家、一个洲。
- 按传输介质分类：
  - 有线网：双绞线、同轴电缆、光纤
  - 无线网：微波、红外线、蓝牙、Wi-Fi
- 按拓扑结构分类：
  - 总线型
  - 星型
  - 环型
  - 树型
  - 网状型

4.1.5 计算机网络的拓扑结构

- 拓扑结构：网络中各个节点相互连接的形式，反映网络中各实体间的结构关系。
- 总线型拓扑：
  - 优点：结构简单，易于扩展，可靠性较高
  - 缺点：同一时刻只能有一个节点发送数据，其他节点必须等待
- 星型拓扑：
  - 优点：结构简单，易于管理，故障诊断和隔离容易
  - 缺点：中心节点负担重，一旦中心节点故障，整个网络瘫痪
- 环型拓扑：
  - 优点：结构简单，传输速率较高
  - 缺点：一个节点故障，整个网络瘫痪
- 树型拓扑：
  - 优点：结构简单，易于扩展，故障隔离容易
  - 缺点：对根节点依赖性大
- 网状型拓扑：
  - 优点：可靠性高，资源共享能力强
  - 缺点：结构复杂，成本高

4.1.6 计算机网络的性能指标

- 速率：数据传输速率，单位为bps（比特/秒）
- 带宽：网络通信线路所能传送数据的最大速率
- 吞吐量：单位时间内通过某个网络的数据量
- 时延：数据从网络的一端传送到另一端所需的时间
- 时延带宽积：传播时延×带宽
- 往返时间（RTT）：从发送方发送数据开始，到发送方收到来自接收方的确认，总共经历的时间
- 利用率：网络的利用率越高，网络的时延越大
- 丢包率：在一定的时间范围内，传输过程中丢失的数据包数量与总数据包数量的比率

4.2 计算机网络体系结构

4.2.1 网络协议

- 网络协议：为进行网络中的数据交换而建立的规则、标准或约定。
- 网络协议的三要素：
  - 语法：数据与控制信息的结构或格式
  - 语义：需要发出何种控制信息，完成何种动作以及做出何种响应
  - 时序：事件实现顺序的详细说明

4.2.2 OSI参考模型

- OSI参考模型：开放系统互连参考模型，是国际标准化组织（ISO）提出的一个网络体系结构模型。
- OSI参考模型分为七层：
  - 物理层：传输比特流
  - 数据链路层：传输帧
  - 网络层：传输分组
  - 传输层：传输报文
  - 会话层：建立、管理和终止会话
  - 表示层：数据的表示、压缩和加密
  - 应用层：为用户提供网络服务

4.2.3 TCP/IP参考模型

- TCP/IP参考模型：是因特网的体系结构模型，分为四层：
  - 网络接口层：对应OSI参考模型的物理层和数据链路层
  - 网际层：对应OSI参考模型的网络层
  - 传输层：对应OSI参考模型的传输层
  - 应用层：对应OSI参考模型的会话层、表示层和应用层
- TCP/IP参考模型与OSI参考模型的比较：
  - 相同点：都采用分层结构，都有传输层和网络层
  - 不同点：TCP/IP参考模型是实际应用的标准，OSI参考模型是理论模型；TCP/IP参考模型的网络接口层对应OSI参考模型的物理层和数据链路层

4.2.4 五层参考模型

- 五层参考模型：综合OSI参考模型和TCP/IP参考模型的优点，分为五层：
  - 物理层
  - 数据链路层
  - 网络层
  - 传输层
  - 应用层

4.3 物理层

4.3.1 物理层的基本概念

- 物理层：OSI参考模型的第一层，负责在物理介质上传输比特流。
- 物理层的主要任务：确定与传输介质的接口有关的一些特性，即机械特性、电气特性、功能特性和过程特性。

4.3.2 数据通信的基本概念

- 数据：传递信息的实体。
- 信号：数据的电气或电磁表现。
- 模拟信号：连续变化的信号。
- 数字信号：离散的信号。
- 码元：承载信息量的基本信号单位。
- 单工通信：只有一个方向的通信，如广播、电视。
- 半双工通信：两个方向都可以通信，但不能同时进行，如对讲机。
- 全双工通信：两个方向可以同时通信，如电话。

4.3.3 物理层下面的传输介质

- 导向型传输介质：
  - 双绞线：两根绝缘铜线按一定规则绞合在一起，减少干扰。
  - 同轴电缆：由内导体、绝缘层、外导体和保护层组成。
  - 光纤：利用光的全反射原理传输光信号，分为单模光纤和多模光纤。
- 非导向型传输介质：
  - 无线电波
  - 微波
  - 红外线
  - 激光

4.3.4 信道的极限容量

- 奈奎斯特定理：在无噪声的情况下，信道的最大传输速率为 $C = 2W \log_2 V$，其中W为信道带宽，V为码元的离散电平数。
- 香农定理：在有噪声的情况下，信道的最大传输速率为 $C = W \log_2 (1 + S/N)$，其中S为信号功率，N为噪声功率，S/N为信噪比。

4.3.5 信道复用技术

- 频分复用（FDM）：将信道的带宽分成若干个互不重叠的频段，每个频段传输一路信号。
- 时分复用（TDM）：将信道的时间分成若干个互不重叠的时间片，每个时间片传输一路信号。
- 统计时分复用（STDM）：根据用户的实际需要动态分配时间片。
- 波分复用（WDM）：在光纤上传输多个不同波长的光信号。
- 码分复用（CDM）：每个用户使用不同的码序列，在同一频段上传输。

4.3.6 数字传输系统

- 数字传输系统：利用数字信号进行传输的系统。
- 脉冲编码调制（PCM）：将模拟信号转换为数字信号的过程，包括采样、量化和编码三个步骤。

4.3.7 宽带接入技术

- 宽带接入技术：用户接入因特网的带宽较高的技术。
- 常见的宽带接入技术：
  - ADSL：非对称数字用户线，利用电话线传输数据。
  - 光纤接入：利用光纤传输数据。
  - 光纤同轴混合（HFC）：利用光纤和同轴电缆传输数据。
  - 无线接入：利用无线电波传输数据。

4.4 数据链路层

4.4.1 数据链路层的基本概念

- 数据链路层：OSI参考模型的第二层，负责在相邻节点之间传输帧。
- 数据链路层的主要任务：
  - 封装成帧
  - 透明传输
  - 差错检测
  - 可靠传输
  - 流量控制
  - 介质访问控制

4.4.2 封装成帧

- 封装成帧：将网络层的分组加上帧头和帧尾，构成帧。
- 帧头：包含源地址、目的地址、帧类型等信息。
- 帧尾：包含校验和等信息。

4.4.3 透明传输

- 透明传输：数据链路层对上层协议来说，看不见任何特殊的控制字符。
- 字节填充：在数据中出现与帧定界符相同的字节时，在其前面插入一个转义字节。
- 零比特填充：在数据中出现连续5个1时，在其后面插入一个0。

4.4.4 差错检测

- 差错检测：检测数据在传输过程中是否发生了错误。
- 奇偶校验：在数据后面添加一个校验位，使得数据中1的个数为奇数或偶数。
- 循环冗余校验（CRC）：利用多项式除法进行校验，检错能力强。

4.4.5 可靠传输

- 可靠传输：保证数据正确、无丢失、无重复、按序到达。
- 停止等待协议：发送方每发送一个帧，就停止发送，等待接收方的确认。
- 连续ARQ协议：发送方连续发送多个帧，接收方对每个帧进行确认。
- 滑动窗口协议：发送方和接收方各维护一个窗口，窗口内的帧可以连续发送。

4.4.6 流量控制

- 流量控制：控制发送方的发送速率，使接收方来得及接收。
- 滑动窗口协议：通过调整窗口大小来实现流量控制。

4.4.7 介质访问控制

- 介质访问控制：控制多个节点对共享介质的访问。
- 静态划分信道：
  - 频分复用
  - 时分复用
  - 波分复用
  - 码分复用
- 动态分配信道：
  - 轮询访问
  - 令牌传递
  - 随机访问

4.4.8 局域网

- 局域网：覆盖范围一般在几千米以内，如一个办公室、一栋楼、一个校园。
- 局域网的特点：
  - 覆盖范围小
  - 传输速率高
  - 误码率低
  - 拓扑结构简单
  - 多采用广播式通信

4.4.9 以太网

- 以太网：最常见的局域网，采用CSMA/CD协议。
- CSMA/CD协议：载波监听多点接入/碰撞检测协议。
- 以太网的帧格式：
  - 前导码：7个字节的10101010和1个字节的10101011
  - 目的地址：6个字节
  - 源地址：6个字节
  - 类型：2个字节
  - 数据：46～1500个字节
  - 校验和：4个字节

4.4.10 高速以太网

- 高速以太网：传输速率在100Mbps以上的以太网。
- 常见的高速以太网：
  - 100BASE-T：100Mbps以太网
  - 1000BASE-T：1Gbps以太网
  - 10GBASE-T：10Gbps以太网

4.4.11 无线局域网

- 无线局域网：利用无线电波传输数据的局域网。
- 无线局域网的特点：
  - 移动性好
  - 安装方便
  - 易于扩展
  - 成本低
  - 传输速率低
  - 误码率高
  - 安全性差

4.4.12 局域网设备

- 网卡：连接计算机和网络的设备。
- 集线器：工作在物理层，对信号进行放大和转发。
- 交换机：工作在数据链路层，根据MAC地址转发帧。
- 路由器：工作在网络层，根据IP地址转发分组。

4.5 网络层

4.5.1 网络层的基本概念

- 网络层：OSI参考模型的第三层，负责在不同网络之间传输分组。
- 网络层的主要任务：
  - 路由选择
  - 分组转发
  - 拥塞控制
  - 网络互连

4.5.2 IP协议

- IP协议：网际协议，是TCP/IP参考模型的网际层的核心协议。
- IP协议的特点：
  - 无连接
  - 不可靠
  - 尽力而为
- IP数据报的格式：
  - 版本：4位
  - 首部长度：4位
  - 区分服务：8位
  - 总长度：16位
  - 标识：16位
  - 标志：3位
  - 片偏移：13位
  - 生存时间：8位
  - 协议：8位
  - 首部校验和：16位
  - 源IP地址：32位
  - 目的IP地址：32位
  - 可选字段：长度可变
  - 填充：长度可变

4.5.3 IP地址

- IP地址：因特网上每台主机的唯一标识。
- IP地址的分类：
  - A类：0开头，网络号8位，主机号24位
  - B类：10开头，网络号16位，主机号16位
  - C类：110开头，网络号24位，主机号8位
  - D类：1110开头，多播地址
  - E类：1111开头，保留地址
- 子网掩码：用于区分网络号和主机号。
- 子网划分：将一个网络划分为若干个子网。
- 超网：将多个网络合并为一个网络。

4.5.4 ARP协议

- ARP协议：地址解析协议，将IP地址转换为MAC地址。
- ARP协议的工作过程：
  - 主机A广播ARP请求，询问主机B的MAC地址
  - 主机B收到ARP请求，发送ARP响应，告知主机A其MAC地址
  - 主机A收到ARP响应，将主机B的IP地址和MAC地址存入ARP缓存

4.5.5 ICMP协议

- ICMP协议：因特网控制报文协议，用于在IP主机、路由器之间传递控制消息。
- ICMP报文的类型：
  - 差错报告报文：目的不可达、源抑制、时间超过、参数问题
  - 询问报文：回送请求/回答、时间戳请求/回答、掩码地址请求/回答

4.5.6 路由选择协议

- 路由选择协议：用于路由器之间交换路由信息，建立和维护路由表。
- 内部网关协议（IGP）：在一个自治系统内部使用的路由选择协议。
  - RIP：路由信息协议，基于距离向量算法
  - OSPF：开放最短路径优先，基于链路状态算法
- 外部网关协议（EGP）：在不同自治系统之间使用的路由选择协议。
  - BGP：边界网关协议

4.5.7 IPv6

- IPv6：下一代IP协议，地址长度为128位。
- IPv6的特点：
  - 地址空间大
  - 简化首部格式
  - 支持即插即用
  - 支持安全性
  - 支持移动性
- IPv6的地址表示：
  - 冒号十六进制表示法
  - 零压缩表示法
  - 内嵌IPv4地址表示法

4.5.8 IP多播

- IP多播：一对多的通信方式，将数据发送给一组接收者。
- 多播地址：D类地址，224.0.0.0～239.255.255.255。
- 多播路由选择协议：
  - DVMRP：距离向量多播路由选择协议
  - MOSPF：多播开放最短路径优先
  - PIM：协议无关多播

4.5.9 虚拟专用网

- 虚拟专用网（VPN）：利用公用网络建立的专用网络。
- VPN的特点：
  - 安全性
  - 经济性
  - 灵活性
- VPN的实现技术：
  - 隧道技术
  - 加密技术
  - 身份认证技术

4.5.10 网络地址转换

- 网络地址转换（NAT）：将内部网络的私有IP地址转换为公有IP地址。
- NAT的类型：
  - 静态NAT：一对一转换
  - 动态NAT：从地址池中动态分配公有IP地址
  - 端口NAT：多对一转换，利用端口号区分不同的内部主机

4.6 传输层

4.6.1 传输层的基本概念

- 传输层：OSI参考模型的第四层，负责在端到端之间传输报文。
- 传输层的主要任务：
  - 端口寻址
  - 建立连接
  - 可靠传输
  - 流量控制
  - 拥塞控制

4.6.2 UDP协议

- UDP协议：用户数据报协议，是一种无连接的传输层协议。
- UDP协议的特点：
  - 无连接
  - 不可靠
  - 尽力而为
  - 面向报文
  - 开销小
- UDP数据报的格式：
  - 源端口：16位
  - 目的端口：16位
  - 长度：16位
  - 校验和：16位
  - 数据：长度可变

4.6.3 TCP协议

- TCP协议：传输控制协议，是一种面向连接的传输层协议。
- TCP协议的特点：
  - 面向连接
  - 可靠传输
  - 流量控制
  - 拥塞控制
  - 全双工通信
  - 面向字节流
- TCP报文段的格式：
  - 源端口：16位
  - 目的端口：16位
  - 序号：32位
  - 确认号：32位
  - 首部长度：4位
  - 保留：6位
  - 紧急URG：1位
  - 确认ACK：1位
  - 推送PSH：1位
  - 复位RST：1位
  - 同步SYN：1位
  - 终止FIN：1位
  - 窗口：16位
  - 校验和：16位
  - 紧急指针：16位
  - 选项：长度可变
  - 填充：长度可变

4.6.4 TCP连接管理

- TCP连接管理：建立连接、维护连接、释放连接。
- 三次握手：建立连接的过程。
  - 第一次握手：客户端发送SYN报文段，请求建立连接
  - 第二次握手：服务器发送SYN+ACK报文段，确认客户端的请求，并请求建立连接
  - 第三次握手：客户端发送ACK报文段，确认服务器的请求
- 四次挥手：释放连接的过程。
  - 第一次挥手：客户端发送FIN报文段，请求释放连接
  - 第二次挥手：服务器发送ACK报文段，确认客户端的请求
  - 第三次挥手：服务器发送FIN报文段，请求释放连接
  - 第四次挥手：客户端发送ACK报文段，确认服务器的请求

4.6.5 TCP可靠传输

- TCP可靠传输：保证数据正确、无丢失、无重复、按序到达。
- 超时重传：发送方在规定时间内没有收到确认，就重传数据。
- 冗余ACK：接收方收到乱序的报文段，就发送冗余ACK，提醒发送方重传。
- 选择确认（SACK）：接收方告诉发送方已经收到的报文段，发送方只重传未收到的报文段。

4.6.6 TCP流量控制

- TCP流量控制：控制发送方的发送速率，使接收方来得及接收。
- 滑动窗口协议：通过调整窗口大小来实现流量控制。

4.6.7 TCP拥塞控制

- TCP拥塞控制：防止网络中出现过多的数据包，导致网络性能下降。
- 慢开始：发送方开始时发送少量数据，然后逐渐增加发送量。
- 拥塞避免：当发送量达到一定阈值时，发送量增加变慢。
- 快重传：发送方收到三个冗余ACK，就立即重传数据。
- 快恢复：发送方收到三个冗余ACK，就将发送量减半，然后进入拥塞避免阶段。

4.6.8 TCP性能

- TCP性能：TCP协议的效率和可靠性。
- 影响TCP性能的因素：
  - 网络带宽
  - 网络时延
  - 丢包率
  - 拥塞控制算法

4.7 应用层

4.7.1 应用层的基本概念

- 应用层：OSI参考模型的第五层，为用户提供网络服务。
- 应用层的主要任务：
  - 网络应用
  - 用户接口
  - 网络服务

4.7.2 域名系统

- 域名系统（DNS）：将域名转换为IP地址的系统。
- 域名的结构：
  - 根域：.
  - 顶级域：.com、.net、.org、.edu、.gov、.mil、.cn、.jp、.uk等
  - 二级域：.baidu、.sina、.163、.qq等
  - 三级域：www、mail、ftp等
- DNS的工作过程：
  - 客户端向本地DNS服务器发送查询请求
  - 本地DNS服务器向根DNS服务器发送查询请求
  - 根DNS服务器向顶级DNS服务器发送查询请求
  - 顶级DNS服务器向二级DNS服务器发送查询请求
  - 二级DNS服务器向三级DNS服务器发送查询请求
  - 三级DNS服务器向本地DNS服务器发送查询结果
  - 本地DNS服务器向客户端发送查询结果

4.7.3 文件传输协议

- 文件传输协议（FTP）：用于在网络上传输文件的协议。
- FTP的特点：
  - 可靠传输
  - 支持匿名访问
  - 支持断点续传
- FTP的工作过程：
  - 客户端向服务器发送连接请求
  - 服务器向客户端发送连接确认
  - 客户端向服务器发送用户名和密码
  - 服务器向客户端发送登录确认
  - 客户端向服务器发送文件传输请求
  - 服务器向客户端发送文件传输确认
  - 客户端和服务器进行文件传输
  - 客户端向服务器发送连接释放请求
  - 服务器向客户端发送连接释放确认

4.7.4 远程终端协议

- 远程终端协议（TELNET）：用于远程登录的协议。
- TELNET的特点：
  - 可靠传输
  - 支持远程登录
  - 支持远程命令执行
- TELNET的工作过程：
  - 客户端向服务器发送连接请求
  - 服务器向客户端发送连接确认
  - 客户端向服务器发送用户名和密码
  - 服务器向客户端发送登录确认
  - 客户端向服务器发送远程命令
  - 服务器向客户端发送远程命令执行结果
  - 客户端向服务器发送连接释放请求
  - 服务器向客户端发送连接释放确认

4.7.5 电子邮件

- 电子邮件：利用网络传输信息的服务。
- 电子邮件的组成：
  - 邮件头：包含发件人、收件人、主题、日期等信息
  - 邮件体：包含邮件的正文
  - 附件：包含邮件的附件
- 电子邮件的协议：
  - SMTP：简单邮件传输协议，用于发送邮件
  - POP3：邮局协议第3版，用于接收邮件
  - IMAP：因特网邮件访问协议，用于接收邮件
- 电子邮件的工作过程：
  - 发件人使用邮件客户端软件撰写邮件
  - 发件人使用SMTP协议将邮件发送到发件人邮件服务器
  - 发件人邮件服务器使用SMTP协议将邮件发送到收件人邮件服务器
  - 收件人使用POP3或IMAP协议从收件人邮件服务器接收邮件

4.7.6 万维网

- 万维网（WWW）：利用超文本标记语言（HTML）和超文本传输协议（HTTP）在因特网上传输信息的服务。
- WWW的组成：
  - 统一资源定位符（URL）：用于标识因特网上的资源
  - 超文本传输协议（HTTP）：用于传输超文本
  - 超文本标记语言（HTML）：用于编写超文本
- URL的格式：协议://主机名:端口号/路径/文件名
- HTTP的特点：
  - 无连接
  - 无状态
  - 简单快速
  - 灵活
- HTTP的工作过程：
  - 客户端向服务器发送HTTP请求
  - 服务器向客户端发送HTTP响应
  - 客户端和服务器进行数据传输
  - 客户端向服务器发送连接释放请求
  - 服务器向客户端发送连接释放确认

4.7.7 动态主机配置协议

- 动态主机配置协议（DHCP）：用于自动分配IP地址的协议。
- DHCP的特点：
  - 自动分配IP地址
  - 减少手工配置的工作量
  - 减少IP地址冲突的可能性
- DHCP的工作过程：
  - 客户端向DHCP服务器发送DHCP发现报文
  - DHCP服务器向客户端发送DHCP提供报文
  - 客户端向DHCP服务器发送DHCP请求报文
  - DHCP服务器向客户端发送DHCP确认报文

4.7.8 简单网络管理协议

- 简单网络管理协议（SNMP）：用于网络管理的协议。
- SNMP的组成：
  - 管理站：负责网络管理的计算机
  - 代理：运行在被管理设备上的软件
  - 管理信息库（MIB）：被管理设备的信息集合
- SNMP的工作过程：
  - 管理站向代理发送SNMP请求
  - 代理向管理站发送SNMP响应
  - 管理站和代理进行数据传输
  - 管理站向代理发送SNMP请求
  - 代理向管理站发送SNMP响应

4.7.9 流媒体

- 流媒体：利用网络传输音频、视频等多媒体信息的技术。
- 流媒体的特点：
  - 实时性
  - 连续性
  - 交互性
- 流媒体的传输协议：
  - RTP：实时传输协议
  - RTCP：实时传输控制协议
  - RTSP：实时流协议

4.7.10 内容分发网络

- 内容分发网络（CDN）：利用网络将内容分发到离用户最近的节点，提高访问速度。
- CDN的组成：
  - 源站：存储原始内容的服务器
  - 边缘节点：存储内容副本的服务器
  - 调度系统：负责将用户请求调度到最近的边缘节点
- CDN的工作过程：
  - 用户向调度系统发送请求
  - 调度系统将请求调度到最近的边缘节点
  - 边缘节点向用户发送内容
  - 如果边缘节点没有内容，则向源站请求内容
  - 源站向边缘节点发送内容
  - 边缘节点向用户发送内容

4.8 网络安全

4.8.1 网络安全的基本概念

- 网络安全：保护网络系统中的硬件、软件、数据不受偶然或恶意的破坏、更改、泄露，保证网络系统连续可靠正常地运行。
- 网络安全的主要威胁：
  - 窃听
  - 篡改
  - 伪造
  - 拒绝服务
  - 病毒
  - 木马
  - 蠕虫
  - 黑客

4.8.2 密码学

- 密码学：研究信息加密和解密的科学。
- 加密：将明文转换为密文的过程。
- 解密：将密文转换为明文的过程。
- 密钥：加密和解密所使用的参数。
- 对称加密：加密和解密使用相同的密钥。
  - DES：数据加密标准
  - AES：高级加密标准
- 非对称加密：加密和解密使用不同的密钥。
  - RSA：Rivest-Shamir-Adleman
  - ECC：椭圆曲线密码
- 哈希函数：将任意长度的输入转换为固定长度的输出。
  - MD5：消息摘要算法第5版
  - SHA-1：安全哈希算法第1版
  - SHA-256：安全哈希算法第256版

4.8.3 数字签名

- 数字签名：利用非对称加密技术对数字信息进行签名，以确认信息的来源和完整性。
- 数字签名的过程：
  - 发送方使用哈希函数对信息进行哈希运算，得到信息摘要
  - 发送方使用自己的私钥对信息摘要进行加密，得到数字签名
  - 发送方将信息和数字签名一起发送给接收方
  - 接收方使用发送方的公钥对数字签名进行解密，得到信息摘要
  - 接收方使用哈希函数对信息进行哈希运算，得到信息摘要
  - 接收方比较两个信息摘要，如果相同，则信息来源和完整性得到确认

4.8.4 数字证书

- 数字证书：由证书颁发机构（CA）颁发的，用于证明公钥所有者身份的电子文件。
- 数字证书的内容：
  - 公钥
  - 公钥所有者的身份信息
  - 证书颁发机构的身份信息
  - 证书的有效期
  - 证书的序列号
  - 证书颁发机构的数字签名
- 数字证书的作用：
  - 证明公钥所有者的身份
  - 防止公钥被篡改
  - 防止公钥被伪造

4.8.5 防火墙

- 防火墙：在网络之间执行访问控制策略的计算机系统。
- 防火墙的类型：
  - 包过滤防火墙：根据IP地址、端口号等信息过滤数据包
  - 应用网关防火墙：根据应用层协议过滤数据包
  - 状态检测防火墙：根据连接状态过滤数据包
- 防火墙的作用：
  - 保护内部网络免受外部网络的攻击
  - 控制内部网络对外部网络的访问
  - 记录网络访问日志

4.8.6 入侵检测系统

- 入侵检测系统（IDS）：检测网络或系统中的入侵行为的系统。
- 入侵检测系统的类型：
  - 基于主机的入侵检测系统：检测主机上的入侵行为
  - 基于网络的入侵检测系统：检测网络上的入侵行为
- 入侵检测系统的作用：
  - 检测入侵行为
  - 记录入侵日志
  - 报警

4.8.7 入侵防御系统

- 入侵防御系统（IPS）：检测并阻止网络或系统中的入侵行为的系统。
- 入侵防御系统的类型：
  - 基于主机的入侵防御系统：检测并阻止主机上的入侵行为
  - 基于网络的入侵防御系统：检测并阻止网络上的入侵行为
- 入侵防御系统的作用：
  - 检测入侵行为
  - 阻止入侵行为
  - 记录入侵日志
  - 报警

4.8.8 虚拟专用网

- 虚拟专用网（VPN）：利用公用网络建立的专用网络。
- VPN的特点：
  - 安全性
  - 经济性
  - 灵活性
- VPN的实现技术：
  - 隧道技术
  - 加密技术
  - 身份认证技术

4.8.9 网络地址转换

- 网络地址转换（NAT）：将内部网络的私有IP地址转换为公有IP地址。
- NAT的类型：
  - 静态NAT：一对一转换
  - 动态NAT：从地址池中动态分配公有IP地址
  - 端口NAT：多对一转换，利用端口号区分不同的内部主机

4.8.10 网络安全协议

- 网络安全协议：保护网络通信安全的协议。
- 网络安全协议的类型：
  - SSL：安全套接层协议
  - TLS：传输层安全协议
  - IPSec：IP安全协议
  - SSH：安全外壳协议
- SSL/TLS的特点：
  - 保密性
  - 完整性
  - 身份认证
- SSL/TLS的工作过程：
  - 客户端向服务器发送SSL/TLS请求
  - 服务器向客户端发送SSL/TLS响应
  - 客户端和服务器进行密钥协商
  - 客户端和服务器进行数据传输
  - 客户端向服务器发送连接释放请求
  - 服务器向客户端发送连接释放确认

4.9 无线网络

4.9.1 无线网络的基本概念

- 无线网络：利用无线电波传输数据的网络。
- 无线网络的特点：
  - 移动性好
  - 安装方便
  - 易于扩展
  - 成本低
  - 传输速率低
  - 误码率高
  - 安全性差

4.9.2 无线局域网

- 无线局域网：利用无线电波传输数据的局域网。
- 无线局域网的特点：
  - 移动性好
  - 安装方便
  - 易于扩展
  - 成本低
  - 传输速率低
  - 误码率高
  - 安全性差
- 无线局域网的标准：
  - IEEE 802.11a：5GHz频段，54Mbps
  - IEEE 802.11b：2.4GHz频段，11Mbps
  - IEEE 802.11g：2.4GHz频段，54Mbps
  - IEEE 802.11n：2.4GHz/5GHz频段，600Mbps
  - IEEE 802.11ac：5GHz频段，1Gbps
  - IEEE 802.11ax：2.4GHz/5GHz频段，10Gbps

4.9.3 无线局域网设备

- 无线网卡：连接计算机和无线网络的设备。
- 无线接入点（AP）：连接无线网络和有线网络的设备。
- 无线路由器：集成了无线接入点和路由器功能的设备。

4.9.4 无线局域网的安全

- 无线局域网的安全威胁：
  - 窃听
  - 篡改
  - 伪造
  - 拒绝服务
  - 病毒
  - 木马
  - 蠕虫
  - 黑客
- 无线局域网的安全措施：
  - WEP：有线等效保密协议
  - WPA：Wi-Fi保护访问
  - WPA2：Wi-Fi保护访问第2版
  - WPA3：Wi-Fi保护访问第3版

4.9.5 蓝牙

- 蓝牙：利用无线电波传输数据的短距离无线通信技术。
- 蓝牙的特点：
  - 短距离
  - 低功耗
  - 低成本
  - 传输速率低
- 蓝牙的协议栈：
  - 物理层
  - 链路管理层
  - 逻辑链路控制和适配协议层
  - 应用层

4.9.6 红外线

- 红外线：利用红外线传输数据的短距离无线通信技术。
- 红外线的特点：
  - 短距离
  - 低功耗
  - 低成本
  - 传输速率低
  - 视线传输

4.9.7 移动通信

- 移动通信：利用无线电波传输数据的移动通信技术。
- 移动通信的特点：
  - 移动性好
  - 覆盖范围广
  - 传输速率低
  - 误码率高
  - 安全性差
- 移动通信的标准：
  - 1G：模拟移动通信
  - 2G：数字移动通信
  - 3G：宽带移动通信
  - 4G：高速移动通信
  - 5G：超高速移动通信

4.9.8 卫星通信

- 卫星通信：利用卫星传输数据的通信技术。
- 卫星通信的特点：
  - 覆盖范围广
  - 传输速率高
  - 误码率低
  - 时延大
  - 成本高

4.9.9 无线传感器网络

- 无线传感器网络：由大量传感器节点组成的无线网络。
- 无线传感器网络的特点：
  - 节点数量多
  - 节点分布密集
  - 节点能量有限
  - 节点计算能力有限
  - 节点存储能力有限
  - 节点通信能力有限
- 无线传感器网络的应用：
  - 环境监测
  - 智能家居
  - 智能交通
  - 智能医疗
  - 智能农业

4.9.10 无线网络的安全

- 无线网络的安全威胁：
  - 窃听
  - 篡改
  - 伪造
  - 拒绝服务
  - 病毒
  - 木马
  - 蠕虫
  - 黑客
- 无线网络的安全措施：
  - WEP：有线等效保密协议
  - WPA：Wi-Fi保护访问
  - WPA2：Wi-Fi保护访问第2版
  - WPA3：Wi-Fi保护访问第3版
  - 蓝牙安全
  - 红外线安全
  - 移动通信安全
  - 卫星通信安全
  - 无线传感器网络安全

4.10 网络管理

4.10.1 网络管理的基本概念

- 网络管理：对网络进行监视、控制、维护和优化的过程。
- 网络管理的主要任务：
  - 故障管理
  - 配置管理
  - 计费管理
  - 性能管理
  - 安全管理

4.10.2 简单网络管理协议

- 简单网络管理协议（SNMP）：用于网络管理的协议。
- SNMP的组成：
  - 管理站：负责网络管理的计算机
  - 代理：运行在被管理设备上的软件
  - 管理信息库（MIB）：被管理设备的信息集合
- SNMP的工作过程：
  - 管理站向代理发送SNMP请求
  - 代理向管理站发送SNMP响应
  - 管理站和代理进行数据传输
  - 管理站向代理发送SNMP请求
  - 代理向管理站发送SNMP响应

4.10.3 远程网络监视

- 远程网络监视（RMON）：用于远程监视网络的协议。
- RMON的组成：
  - 探针：运行在被监视设备上的软件
  - 管理站：负责网络管理的计算机
- RMON的工作过程：
  - 探针收集网络数据
  - 探针将网络数据发送给管理站
  - 管理站对网络数据进行分析
  - 管理站向探针发送控制命令
  - 探针执行控制命令

4.10.4 网络管理的安全

- 网络管理的安全威胁：
  - 窃听
  - 篡改
  - 伪造
  - 拒绝服务
  - 病毒
  - 木马
  - 蠕虫
  - 黑客
- 网络管理的安全措施：
  - SNMPv3：简单网络管理协议第3版
  - RMON2：远程网络监视第2版
  - 网络管理的安全协议

4.10.5 网络管理的工具

- 网络管理的工具：
  - 网络监视工具：Wireshark、Tcpdump、Ethereal
  - 网络扫描工具：Nmap、Nessus、OpenVAS
  - 网络性能测试工具：Iperf、Netperf、Ping
  - 网络配置工具：Cisco IOS、Juniper JUNOS、Huawei VRP
  - 网络管理平台：HP OpenView、IBM Tivoli、Cisco Prime

4.10.6 网络管理的标准

- 网络管理的标准：
  - ISO/IEC 7498-4：开放系统互连参考模型第4部分：管理框架
  - ISO/IEC 10040：开放系统互连系统管理概述
  - ISO/IEC 10164：开放系统互连系统管理
  - ITU-T M.3010：电信管理网络
  - ITU-T M.3400：电信管理网络的管理功能
  - ITU-T M.3600：电信管理网络的管理信息模型
  - ITU-T M.3700：电信管理网络的管理信息库

4.10.7 网络管理的发展趋势

- 网络管理的发展趋势：
  - 智能化
  - 自动化
  - 集成化
  - 开放化
  - 标准化
  - 安全化
  - 移动化
  - 云化
  - 虚拟化
  - 软件定义网络（SDN）
  - 网络功能虚拟化（NFV）

4.10.8 网络管理的挑战

- 网络管理的挑战：
  - 网络规模越来越大
  - 网络结构越来越复杂
  - 网络应用越来越多样
  - 网络安全越来越重要
  - 网络管理越来越困难
  - 网络管理的成本越来越高
  - 网络管理的人才越来越缺乏
  - 网络管理的技术越来越新
  - 网络管理的标准越来越多
  - 网络管理的工具越来越多

4.10.9 网络管理的解决方案

- 网络管理的解决方案：
  - 采用智能化的网络管理系统
  - 采用自动化的网络管理工具
  - 采用集成化的网络管理平台
  - 采用开放化的网络管理协议
  - 采用标准化的网络管理接口
  - 采用安全化的网络管理机制
  - 采用移动化的网络管理终端
  - 采用云化的网络管理服务
  - 采用虚拟化的网络管理资源
  - 采用软件定义网络（SDN）
  - 采用网络功能虚拟化（NFV）

4.10.10 网络管理的未来

- 网络管理的未来：
  - 网络管理将更加智能化
  - 网络管理将更加自动化
  - 网络管理将更加集成化
  - 网络管理将更加开放化
  - 网络管理将更加标准化
  - 网络管理将更加安全化
  - 网络管理将更加移动化
  - 网络管理将更加云化
  - 网络管理将更加虚拟化
  - 网络管理将更加软件定义网络（SDN）
  - 网络管理将更加网络功能虚拟化（NFV）

4.11 新一代网络技术

4.11.1 软件定义网络

- 软件定义网络（SDN）：将网络的控制平面和数据平面分离，通过软件来控制网络的技术。
- SDN的特点：
  - 控制平面和数据平面分离
  - 集中控制
  - 开放接口
  - 可编程
- SDN的架构：
  - 应用层：运行网络应用程序
  - 控制层：运行网络控制软件
  - 基础设施层：运行网络设备
- SDN的协议：
  - OpenFlow：开放流协议
  - NETCONF：网络配置协议
  - YANG：数据建模语言

4.11.2 网络功能虚拟化

- 网络功能虚拟化（NFV）：将网络功能从专用硬件设备中分离出来，通过软件来实现的技术。
- NFV的特点：
  - 网络功能软件化
  - 网络功能虚拟化
  - 网络功能集中化
  - 网络功能自动化
- NFV的架构：
  - 网络功能虚拟化基础设施（NFVI）：运行网络功能软件的硬件设备
  - 虚拟网络功能（VNF）：运行在NFVI上的网络功能软件
  - 网络功能虚拟化管理和编排（MANO）：管理和编排VNF的软件
- NFV的协议：
  - ETSI NFV：欧洲电信标准协会网络功能虚拟化
  - OpenStack：开源云计算平台
  - Kubernetes：开源容器编排平台

4.11.3 云计算

- 云计算：通过网络提供计算资源、存储资源、网络资源、软件资源的服务。
- 云计算的特点：
  - 按需自助服务
  - 广泛网络访问
  - 资源池化
  - 快速弹性
  - 可计量服务
- 云计算的服务模式：
  - 基础设施即服务（IaaS）：提供计算资源、存储资源、网络资源
  - 平台即服务（PaaS）：提供开发平台、运行平台
  - 软件即服务（SaaS）：提供软件应用
- 云计算的部署模式：
  - 公有云：面向公众提供服务
  - 私有云：面向企业内部提供服务
  - 混合云：公有云和私有云的组合
  - 社区云：面向特定社区提供服务

4.11.4 大数据

- 大数据：数据量大、数据类型多、数据处理