



高级计算机网络

闭卷考试

题型：

- 填空
- 四个名词解释
- 四个论述题

复习重点：

- ☒ 全部PPT
- ☒ 第七章第一小节和第九章第一小节的概述

第七章 无线网络和移动网络

第一小节概述

1. 无线网络的要素
 - 无线接入点
 - 无线主机
 - 运动中的无线主机
 - 覆盖区域
 - [!Pasted image 20230216222542.png](#)
2. 无线主机：如同在有线网络中一样，主机是运行在应用重的端系统设备。**无线主机**可以是便携机、掌上机、智能机或者桌面计算机。主机本身可能移动，也可能不移动。
3. 无线链路：主机通过无线通信链路连接到一个基站或者另一台无线主机。
 - 部分无线网络标准的链路特性![Pasted image 20230216222830.png](#)
4. 基站：基站是无线网络基础设施的一个关键部分。与无线主机和无线链路不同，基站在有线网络中没有明确的对应部分。它负责向与之关联的无线主机发送多个无线主机的传输。当我们说一台无线主机与某基站相关联时，则是指：
 1. 该主机位于该基站的无线覆盖范围内。

2. 该主机使用该基站中继它（该主机）和更大网络之间的数据。
 3. 蜂窝网络中的蜂窝塔和802.11无线LAN中的接入点都是基站的例子。
5. 网络基础设施：这是无线主机希望与之进行通信的更大网络。

在最高层次，我们能够根据两个准则对无线网络分类。

1. 在该无线网络中的分组是否跨越了一个无线或多个无线跳。
2. 网络中是否有诸如基站这样的基础设施。

- 单跳，基于基础设施。这些网络具有与较大有线网络连接的基站。此外，该基站与无线主机之间的所有通信都经过一个无线跳。（802.11、4G LTE）

- 单跳，无基础设施。在这些网络中，不存在与无线网络相连的基站。（蓝牙）

- 多跳，基于基础设施。在这些网络中，一个基站表现为以有线方式与较大网络相连。（无线网状网络）

- 多跳，无基础设施。在这些网络中没有基站，并且节点为了达到目的地可能必须在几个其他无线节点之间中继报文。

第九章 多媒体网络应用

多媒体应用：

1. 流式存储音频/视频
2. 会话式IP音频/视频
3. 流式实况音频/视频

第一小节概述

我们将多媒体网络应用定义为任何应用音频或视频的网络应用。

视频的性质

- 视频最显著的特点：高比特率
- 视频的另一重要特点是：可以被压缩
- 空间冗余
- 时间冗余
- 视频的多重版本

音频的性质

- 模拟音频转换为数字信号再转换为模拟音频
1. 采样

2. 量化

3. 解码

- MP3 : MPEG 1 第三层
- AAC : Advanced Audio Coding
- 对音频的小失误对比视频的小失误更为敏感

多媒体网络应用的类型

1. 流式存储音频/视频

- 流：它避免了在开始播放之前必须下载整个视频
- 相互作用：用户可以对多媒体内容进行暂停、重新配置前进、重新配置倒退、快进等操作
- 连续播放：一旦视频开始播放，它应该根据初始记录的时序进行。
- 流视频最重要的性能测度时平均吞吐量。

概述

分组交换的优点：

- 高效
- 灵活
- 迅速
- 可靠

按照网络的作用范围进行分类

- 广域网 (WAN)
- 城域网 (MAN)
- 局域网 (LAN)
- 个人区域网 (PAN)

按照网络的使用者进行分类

- 公用网
- 专用网

体系结构

开放系统互连参考模型OSI/RM

TCP/IP

分层的好处与缺点

好处：

1. 各层之间独立
2. 灵活性好
3. 结构可分割开
4. 易于实现和维护
5. 能促进标准化工作

缺点：

1. 降低效率
2. 有些功能会在不同的层次中重复出现，因而产生了额外开销

OSI：物链网输会示用

TCP/IP：

1. 应用层
2. 运输层
3. 网际IP
4. 网络接口层

五层协议：

1. 应用层
2. 运输层
3. 网络层
4. 数据链路层
5. 物理层

物理层

- 机械特性
- 电气特性
- 功能特性
- 过程特性

数据链路层

三个基本问题

1. 封装成帧——帧定界

2. 透明传输
3. 差错控制——CRC、FCS

CSMA/CD协议 (Carrier Sense Multiple Access with Collision Detection)

载波监听多点接入/碰撞检测

特性：

- 智能进行双向交替通信（半双工通信）
- 每站在发送数据之后的一小段时间内，存在彩玉碰撞的可能性
- 发送的不确定性使整个以太网平均通信量远小于以太网的最高数据率

争用期：两倍的端到端往返时延

- 10Mbit/s以太网：51.2us
- 以太网在发送数据时，若前64字节没有发生冲突，则后续的数据就不会发生冲突
- 最短有效帧长：64字节

二进制指数类型退避算法

要点：

1. 准备发送。在发送之前，必须先检测信道
2. 检测信道。若检测到信道忙，则应不停地检测，一直等待信道转为空闲。若检测到信道空闲，并在 96 比特时间内信道保持空闲（保证了帧间最小间隔），就发送这个帧。
3. 检测碰撞：在发送过程中仍不停地检测信道，即网络适配器要边发送边监听。这里只有两种可能性：
 1. 发送成功：在争用期内一直未检测到碰撞。这个帧肯定能够发送成功。发送完毕后，其他什么也不做。然后回到(1)。
 2. 发送失败：在争用期内检测到碰撞。这时立即停止发送数据，并按规定发送人为干扰信号。适配器接着就执行指数退避算法，等待 r 倍 512 比特时间后，返回到步骤 (2)，继续检测信道。但若重传达 16 次仍不能成功，则停止重传而向上报错

网络层

网际协议 IP

- 网际协议IP是TCP/IP体系结构中两个最主要的协议之一
- 与IP协议配套使用的还有三个协议
 - 地址解析协议 ARP (Address Resolution Protocol)
 - 网际控制报文协议 ICMP
 - 网际组管理协议 IGMP

常用的三种类别的IP地址

!Pasted image 20230217114434.png

一般不使用的特殊的IP地址

!Pasted image 20230217114503.png

内部网关协议

- RIP
 - 仅和相邻路由器交换信息
 - 交换本路由器全部信息
 - 按固定时间间隔交换路由信息
- OSPF
 - 向本自治系统中所有路由器使用洪泛法发送信息
 - 发送本路由器相邻的所有路由器的链路状态，部分信息
 - 只有当链路状态发生变化时，才向所有路由器发送此信息

外部网关协议

运输层

- 进程间的端到端通信
- 复用
- 分用
- 面向连接的TCP，无连接的UDP

UDP

主要特点：

1. 无连接
2. 最大努力交付
3. 面向报文
4. 没有拥塞控制
5. 支持一对一、一对多、多对一和多对多
6. 首部开销小，只有8个字节

TCP

- 面向连接
- 只提供一对一服务
- 可靠交付
- 全双工通信
- 面向字节流

可靠传输

- 停止等待
 - 优点：简单；缺点：效率低
 - 信道利用率： $U = \frac{T_D}{T_D + RTT + T_A}$
- 连续ARQ协议
 - 累计确认
 - 优点：容易实现
 - 缺点：不能向发送方反映出接收方已经正确收到的所有分组的信息
- TCP拥塞控制算法
 - 慢开始
 - 拥塞避免
 - 快重传
 - 快恢复

应用层

- DNS
- FTP
- WWW
 - URL：统一资源定位符
 - HTTP：超文本传送协议
 - HTML：超文本标记语言
- Email
- DHCP

网络安全

消息被称为明文。用某种方法伪装消息以隐藏它的内容的过程称为加密（Encrypt），加了密的消息称为密文，而把密文转变为明文的过程称为解密（Decrypt）。

分组密码的操作模式

1. 电子密码本（ECB）
对于长报文，ECB模式可能并不安全。
2. 密码分组链接模式（CBC）
3. 计数器模式（CTR）
4. 输出反馈模式（OFB）
5. 密码反馈（CFB）

加密技术

1. 对称密钥密码体系
 1. 密钥K的可能值的范围叫做密钥空间
 2. 加密函数表示为：
 - $E_k(M) = C$
 - $D_K(C) = M$
 - $D_K(E_K(M)) = M$
2. 非对称密钥密码体系
 - $E_{K1}(M) = C$
 - $D_{K2}(C) = M$
 - $D_{K2}(E_{K1}(M)) = C$

!Pasted image 20230217154510.png
3. 对称加密算法：
优点：
 - 加密速度快，适合大量数据的加密
 - 极强的安全性，可以用增加密钥长度增加密文的安全缺点：
 - 用户难以安全地分享密钥
 - 扩展性差
 - 密钥更新困难

- 不能用以数字签名，也不能用以身份认证

4. 公钥加密算法：

优点：

- 参与方不用共享密钥
- 扩展性好
- 熟悉数字签名

缺点：

- 加密速度很慢，不适合大量数据地加解密

5. 数字水印

◦ 特征：

- 隐蔽性
- 强壮性
- 安全性

6. 防火墙

1. 服务控制
2. 方向控制
3. 用户控制
4. 行为控制

计算机病毒

计算机病毒是一种人为编制能够对计算机正常程序的执行或数据文件造成破坏，并且能够自我复制的一组指令程序代码。

特点：

1. 复制性
2. 感染性
3. 潜伏性
4. 触发性
5. 破坏性

计算机病毒进入系统的途径主要有三种：

1. 通过计算机网络进行传播
2. 通过移动存储设备来进行传播
3. 通过通信系统进行传播

IPv6

- 为什么要引用IPv6

IPv4取得了巨大的成功；IPv4地址资源的紧张限制了Internet的进一步发展；NAT、CIDR、VLSM等技术仅仅暂时缓解IPv4地址紧张，但不是根本解决办法，所以新技术的出现对IP协议提出了更多的要求。

- 特点：

- 近乎无限的地址空间
- 更简洁的报文头部
- 内置的安全性
- 更好的QoS支持
- 更好的移动性
- 编址层次等级

- IPv6地址的压缩表示

一个IPv6的地址使用冒号十六进制表示方法：128位的地址每16位分成一段，每个16位的段用十六进制表示并用冒号分隔开，例如一个普通公网IPv6地址：

2001:0D12:0000:0000:02AA:0987:FE29:9871

IPv6地址支持压缩前导零的表示方法，例如上面的地址可以压缩表示为：

2001:12:0:0:2AA:987:FE29:9871

为了进一步精简IPv6地址，当冒号十六进制格式中出现连续几段数值0的位段时，这些段可以压缩为双冒号的表示，例如上面的地址还可以进一步精简表示为：

2001:12::2AA:987:FE29:9871

又例如IPv6的地址FF80:0:0:0:FF:3BA:891:67C2可以进一步精简表示为：

FE80::FF:3BA:891:67C2

这里值得注意的是：双冒号只能出现一次。

- IPv6扩展报头优势

- IPv4选项缺点
 - IPv4选项对路由器转发性能产生负面影响
 - 很少使用
- IPv6扩展报头的优势
 - 扩展报头在IPv6报头的外部
 - 路由器可以不考虑这些选项（逐跳选项除外）
 - 对路由器转发性能无负面影响
 - 易于通过新的扩展报头进行功能扩展

- 动态路由协议：
 - RIPng
 - 距离矢量路由协议，利用UDP传输机制
 - 用跳数度量路由，16跳为不可达
 - 利用水平分割技术来减少环路发生的可能性
 - IS-IS
 - 属于内部网关协议
 - 链路状态协议
 - 最短路径优先
 - MBGP
 - OSPFv3
- IPv6过渡技术
 - 多个IPv6网络之间互通
 - 手工隧道
 - GRE隧道
 - IPv6 in IPv4隧道
 - 自动隧道
 - 6 to 4 隧道
 - ISATAp
 - 其他
 - IPv6网络和IPv4网络互通
 - 双栈网络
 - NAT-PT
 - 其他技术

多播技术

- 多播地址就是D类IP地址，即224.0.0.0~239.255.255.255
- 三个基本要求：
 1. 需要有唯一一个标识多播组的机制，IP网络中通过多播编制技术来实
 2. 需要有多播组成员加入或退出多播组的机制。IGMP用来实现对多播组成员的管理
 3. 在IP网络上高效传送多播分组到各个组成员的多播路由协议
- 两种组地址：
 1. 永久组地址

2. 临时组地址

- IP多播组地址到以太网多播地址的映射：将D类IP地址的低23位放到专用的以太网多播地址的低23位，01-00-5E
- 以太网多播地址对应的多播组是不唯一的
- IP多播分组在网络上的传送
 - 单个物理网络的多播较简单：
 - 发送方的多播进程使用多播目的地址，设备驱动程序将它转换成相应的以太网多播地址，然后发送出去
 - 接收方的进程将主机想接收的多播数据报报告给IP层，并且设备驱动程序必须能够接收这些多播帧
 - 当一个主机收到多播数据报时，它必须向属于哪个多播组的每个进程均传送一个副本
 - 多个物理网络的多播
 - 当把多播扩展到单个物理网络意外，需要通过路由器转发多播数据时，复杂性就增加了，需要有一个协议让多播路由器了解网络中属于某个多播组的任何一个主机。这个协议就是因特网组管理协议（IGMP）
- 多播组内的成员关系是动态的，进程可以随时离开一个组
- IGMP
 - IGMPv1实现简单，但是离开延迟过大，选举查询路由器需要依赖多播路由协议。
 - IGMPv2对此进行了改进，增加了离开组保留选举查询路由器机制
 - IGMPv3协议的主要目的是支持源特定多播，并进一步对IGMPv2进行完善