



南京大學

NANJING UNIVERSITY

# 互联网计算期末复习



# 这门课我们学了什么

- 各种协议（自顶向下）
  - 应用层
  - 传输层
  - 网络层
  - 数据链路层
  - 局域网
  - 无线网络
  - 网络安全协议





# 应用层协议

- DNS
  - 名字空间的分级结构、四种名字服务器、名字解析流程
- SMTP c/s TCP 25 只负责发邮件
  - SMTP
- FTP 21 20 TCP
  - 控制连接、数据传输连接 两个并写的TCP连接
- WWW and HTTP TCP 80 无连接 无状态 1.0非持续 1.1持续连接
- CDN<sub>s</sub> DNS





# 传输层协议

- 传输层地址
  - 端口、复用/解复用
  - 流量控制、拥塞控制
- UDP 首部8B，无拥塞控制，不保证可靠交付 UDP不分片
  - 无连接，best effort
  - 校验和计算 + 伪首部12B 以2B为单位+后再反码放入校验和，进位要回卷
- TCP 首部至少20B，是4B的整数倍，累计确认
  - 面向连接，拥塞控制

三次握手：

  - 1.SYN=1，seq=x
  - 2.SYN=1，ACK=1，seq=y，ack=x+1
  - 3.ACK=1，seq=x+1，ack=y+1

4次挥手：

  - 1.FIN=1，seq=u
  - 2.ACK=1，seq=v，ack=u+1
  - 3.FIN=1，ACK=1，seq=w，ack=u+1
  - 4.ACK=1，seq=u+1，ack=w+1





# 传输控制协议——TCP

- 连接的建立和断开
  - 三次握手、四次挥手
- 数据包序号
  - 按序到达、积累确认
  - 接收报文序号与确认序号之间的关系
  - 时序图
- 拥塞控制的基本问题
  - 拥塞检测
  - 速率调整

流量控制：滑动窗口机制，有rwnd限制发送窗口

慢开始、拥塞避免  
快重传、快恢复





# 拥塞检测

- 数据包延时

- 测RTT

$$\begin{aligned} sRTT(k+1) &= (1-a)sRTT(k) + aRTT(k+1) \\ sERR(k+1) &= RTT(k+1) - sRTT(k) \\ sDEV(k+1) &= (1-g)sDEV(k) + g|sERR(k+1)| \\ RTO(k+1) &= sRTT(k+1) + 4sDEV(k+1) \end{aligned}$$

- 路由器功能

- ECN

和丢包一样处理

- 丢包

- 冗余ACK
- 超时
- 不同的拥塞情况对应不同的丢包现象
  - 对应不同的拥塞控制方式





# 速率控制

- 发送窗口调整
  - Slow start vs. congestion avoidance、
    - 门限值threshold
  - 窗口减半 vs. 窗口回退到1
- TCP协议的状态机表示
- TCP协议的公平性





# 网络层协议

- 网络层地址
  - IP中的子网掩码、网络地址、主机地址、广播地址
- 数据平面—数据包从入端口到出端口
  - 路由器中的队列管理
    - HOL blocking
  - 端口转发
    - 最长前缀匹配
  - 路由聚合
    - 网络编址
  - 地址转换NAT

主机数-2

主机号全0

主机号全1







# 控制平面

- 决定数据报文的端到端路径
- 链路状态协议
  - Dijkstra算法
  - 路由震荡问题
- 距离矢量协议
  - Bellman-Ford算法
  - 距离及转发端口更新过程
  - 毒性反转问题
    - 好消息传得快，坏消息传得慢
- IGP、BGP
  - IGP和BGP的作用范围
  - AS选择





# 数据链路层

- MAC地址
  - MAC平面地址 vs IP结构性地址
- 错误检测
  - CRC计算
- 局域网
  - 多址接入协议
  - 信道划分 vs. 随机接入
- 随机接入
  - 冲突检查
  - 冲突恢复
- 地址解析协议ARP
- 数据帧跨越子网时帧头的变化
- 以太网
  - 交换机的地址学习机制
- MPLS协议

到此为止，已经完整给出一套日常生活中，用户接入互联网所需要的协议流程。





# 无线与移动网络

- 无线信道的特征
  - 衰落、多径、噪声、隐藏终端
- CDMA
  - 编码、解码
- CSMA/CA
  - CD vs. CA
- 互联网移动性支撑
  - Direct routing vs. indirect routing

直接路由：效率高，但复杂、不透明      间接路由：效率低，但简单、透明。





# 网络安全

- RSA加密算法
  - 加密、解密，安全性分析
- 不同协议层次中的安全保障方式
  - TLS、IPSec、802.11、4G LTE
- 防火墙
  - 有状态 vs. 无状态





提问

---

Q & A



南京大學  
NANJING UNIVERSITY