Ch-07 应用层

网络应用层

应用层体系结构：

- C/S : client-sever：客户端-服务器
- P2P : peer-to-peer：主机之间直接通信

应用层业务需求

- 可靠传输：文件传输需要可靠数据传输
- 吞吐量
- 实时性：网络电话要求低延迟
- 安全性

HTTP (HyperText Transfer Protocol)：超文本传输协议

- 客户机/服务器模式
- “无状态的”

HTTP 非持续连接和持续连接

- 非持续连接
    - 下载多个对象时需要多个 TCP 连接
- 持续连接
    - 可以在一个 TCP 连接上传输多个对象

cookie

- 用户与服务器的交互

- 记录用户会话状态

电子邮件

- 三大组件：用户代理、邮件服务器、SMTP
- SMTP (Simple Mail Transfer Protocol)：简单邮件传输协议

socket 编程

- 采用 UDP，无连接，不可靠
- 采用 TCP，连接，可靠

多媒体业务与传输协议

流媒体服务

- 存储的流媒体：下载文件后再播放
    - 等待时间长
- 直播的流媒体：边下载边播放
    - 用户端不保存内容
- 交互式流媒体：如 IP 电话、视频会议等
    - 对延迟有较高要求

流媒体传输协议：

RTP (Real-time Transport Protocol)：实时传输协议

- 为实时应用提供端到端的传输服务
- 多媒体数据经 RTP 封装后，交给 UDP 接口

RTCP (RTP Control Protocol)：RTP 控制协议

RTSP (Real-Time Streaming Protocol)：实时流媒体协议

- 媒体播放器与媒体服务器之间的控制协议
- 控制功能在媒体播放器、媒体服务器等专用软件中实现

SIP (Session Initiation Protocol)：会话发起协议

- 用于 IP 电话的信令和服务质量

媒体播放器：

- 提供用户界面
- 提供交互功能，支持 RTSP
- 解压缩
- 消除错误
- 缓存数据，消除抖动

QoS 及其技术

Qos (Quality of Service)：服务质量

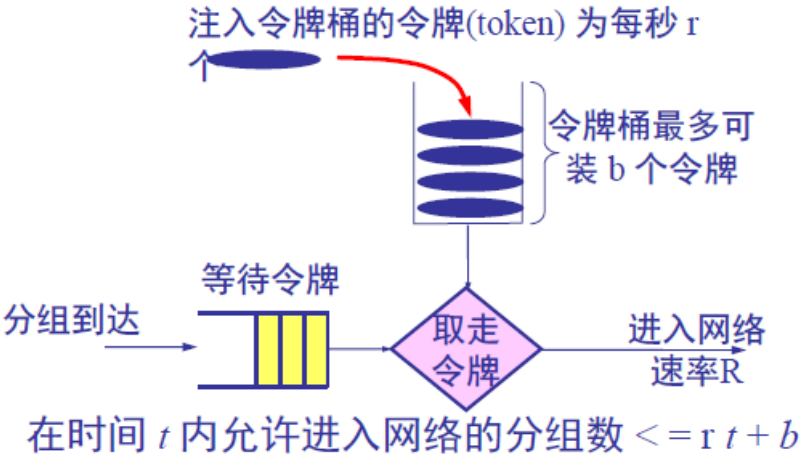
流量整形 (Traffic Shaping)

- 平均速率、峰值速率、突发长度

令牌桶 (Token bucket)

流量整形方法：令牌桶(Token bucket)

流量整形：调节进入网络数据流的发送速率，使之不超过突发长度及平均速率



MPLS (MultiProtocol Label Switching)：多协议标记交换

- 用面向连接的方式代替 IP 的无连接分组交换，利用更快捷的查找算法，而不用最长前缀匹配的方法查找路由表

网络安全

数据加密模型：$D_K(Y = E_K(X)) = X$

常规密码体制

- 加密密钥与解密密钥相同，又称为**对称密钥系统**
  - 置换密码
  - 替代密码
  - DES (Data Encryption Standard)：数据加密标准

公钥密码体制

- 加密密钥与解密密钥不同，又称为**非对称密码系统**

- 只需对解密密钥保密，如 RSA 算法

数字签名

中间人攻击

IPsec：在 IP 数据报中的数据都是加密的

- AH (Authentication Header)：认证首部
    - 使接收结点根据 AH 认证源节点并检查数据完整性，但不提供数据保密性
- ESP (Encapsulation Security Payload)：封装安全有效载荷
    - 使接收结点认证源点，检查数据完整性，并提供数据保密性

SSL (Secure Socket Layer)：安全套接层