计算机网络概论——期末复习

陈小康 1500012741

$Chapter\ 5-1$ 网络层概述

1、网络层

网络层主要功能：发送主机和接收主机之间传输报文。

路由器对经过的数据分组并检查头部信息。

--------主要功能：路由(决定源主机到目的主机的路径) && 转发(将分组由输入端口移动到适当的输出端口)

--------OSI网络层提供的服务

- 面向连接：虚电路
  - 发送请求，建立连接，然后传输，再拆除连接
  - 每个路由器维护源主机到目的主机的连接状态
  - 分组带有VC标志。不同的链路，需要有不同的VC标志
- 无连接：数据报
  - 每个分组头含有目的地址，选路是独立的。但是开销增大。
  - 可能出现先发后到的现象
  - 生存时间的限制

--------路由器

多个输入端口 && 多个输出端口

- 路由选择：按照分布式算法，根据相邻路由器得到的网络拓扑变化情况，动态改变选择的路由器
- 输入端口的排队：**HOL阻塞**，线路前部阻塞。排队的分组必须等待通过交换结构。
  - 解决HOL阻塞：虚拟输出队列 VOQ。在输入端，对不同的CELL建立FIFO。到达的cell被分配到不同队列。在每个时隙开始时，中心调度算法检测每个队列，找到不冲突的输入输出端口进行匹配。
  - 阵列结构。线卡到中心交换机为端到端连接。传输的数据在到达分组背板之前被分割为固定长度的cell。到达输出线路之前再合并成可变长度的分组。
  - 缓冲区长度设计：平均换存量 $B = RTT * C_{(链路容量)}$

$Chapter\ 5-2$ 路由算法

1、路由算法

--------网络中的路由选择

- 数据报：每个分组在途径的节点单独选路
- 虚电路方式：建立电路时选路

--------Flooding

源节点将分组转发给相邻节点。节点接收到分组后，在除接收链路以外的所有链路上转发。最终会有多个备份到达目的节点，但根据分组序号去重。

--------路由选择分类

集中式：路由器有全部的拓扑及链路代价的完整信息

分布式：路由器只知道其邻居节点，以及到邻居节点的代价。通过与邻居节点交换信息，迭代获得最小代价路径。

Dijkstra算法

每次加入一个距离源点最近的点，并利用这个点更新源点到其他点的距离

```
# 初始化
N = {u}
for all nodes v:
    if v is neighbour of u:
        D(v) = c(u, v)
    else:
        D(v) = ∞
# loop
find w that (w is not in N) && (D(w) is minest of all):
    N.append(w)
for v in w.neighbours():
    D(v) = min(D(v), D(w)+c(w,v))
```

距离-矢量算法

$D_x(y)$为 x 到 y 的最小代价路径的代价。遍历 x 的所有邻居节点 v，得到 v 到 y 的最小代价。

$D_x(y) = min_v(c(x,v) + d_v(y))$

对每个邻居v，X需要维护一个表：$D_v = [D_v(y) : y \in N]$

并且每个节点v周期地向邻居节点发送D_v

2、路由协议

--------RIP(Routing Information Protocol)

基于距离矢量(DV)的分布式路由协议。

每个路由器维护到目的网络的距离记录。

距离的定义：跳数。

一条路径最多包含15个路由器，否则表示不可达。

仅与相邻路由器交换路由表信息。$路由表信息：目的，跳数，下一跳路由器$

无穷计算问题

——无穷大的路由器跳数设置为15+1

——禁止向邻居返回一个从邻居得到的最佳路径(循环更新)

--------OSPF (open shortest path first 开放最短路径优先3

步骤

- 主动测试相邻节点的状态。(hello 信息)
- 将与其相邻节点的状态信息传送给所有节点
- 每个节点拥有完整的网络拓扑信息，利用$Dijkstra$算法计算到每个节点的最佳路径。

性能分析：一个路由器的链路状态只涉及与相邻路由器的联通状态，与互联网的规模没有直接关系。所以效率比RIP高很多。

--------练习题 P19

$Chapter\ 5-3$ IP互联协议

1、因特网的网络层协议

ARP(Address Resolution Protocol)：地址解析协议

RARP(Reverse Address Resolution Protocol)：反向地址解析协议

ICMP(Internet Control Message Protocol)：因特网报文控制协议

IGMP(Internet Group Management Protocol)：因特网组管理协议

2、IP地址

IP地址是连接在因特网上的主机的唯一标志。IPV4 32位，IPV6 128位。

--------IP地址编址方法

- 分类IP地址
- 子网划分
- 构成超网

--------分类IP地址

IP地址分为ABCDE五类。每类地址由$\{<网络号><主机号>\}$组成

- A 类地址：8+24，0开头
- B 类地址：16+16，10开头
- C 类地址：24+8，110开头
- D 类地址：1110开头，多播地址
- E类地址：1111开头，暂时没用到

网络类别	最大网络数	可用网络范围	最大主机数
A	$2^7-2=126$	$[1,126]$	$2^{24}-2$
B	$2^{14}-1$	$[128.1,191.255]$	$2^{16}-2$
C	$2^{21}-1$	[192.0.1]	2^8-2

同一网络上的主机或路由器，其IP地址的网络号必须相同。主机号由网络所属单位分配。

路由器具有两个或两个以上IP地址。不同接口的IP地址一般不同

3、分组传送

主机A向主机B交送分组。先检查主机B是否与主机A在同一网络。如果是，就直接交付。否则简介交付，将分组发送给本网络上某个路由器，由路由器负责转发。

4、ARP

链路层传输需要使用硬件地址。就需要建立网络地址与硬件地址的映射关系。

--------ARP的功能：建立同一局域网上主机的IP地址到网卡硬件地址（MAC地址）的映射。根据IP找MAC

--------例题1

主机A向主机B发送IP分组，途中经过了4个路由器，那么，在IP分组的发送和转发过程中，共使用ARP协议的次数是( )。

答：5次。每次主机(/路由器)需要根据目的地址，找到下一跳的硬件地址。比如转发到本网路的主机，就寻找本网络主机的目的地址。转发到另一个网络的主机，就寻找本网路一个路由器的地址。一个主机加上4个路由器，一共使用5次ARP协议。

--------例题2

IP分组在转发时，源和目的IP地址都不会改变。因为这两个代表了IP数据报的源和目的地址。而源/目的Mac地址可能改变。(经过转发路由器)

5、子网划分

需求：AB类地址主机地址过多=>广播风暴。将主机地址部分比特作为子网地址

--------子网掩码：为1的部分表示子网地址。为0的部分表示主机地址

例子：162.105.75.1 255.255.255.0 前24位是子网地址，后8位是主机地址。

子网掩码的分组转发过程

```
1.提取接收分组的首部IP地址D
2.用各网络的子网掩码与D“与”，看是否与相应的网络地址匹配。若匹配则直接交付。
3.路由表中若有目的地址为D的特定路由，传送给指明的下一跳
4.否则是对路由表中每一项的子网掩码和D相"与"，若结果与网络地址匹配，传送给下一跳
5.若路由表中有默认路由，将分组传送给路由表中指明的默认路由器。不然的话报错。
```

6、无分类编址CIDR(Classless Inetr-Domain Routing)

没有ABCDE类地址、子网的概念，用网络前缀代替网络号和子网号。

--------斜线记法

162.105.75.1/16，后面的数字表示这个组中 前面16位相同。

把网络前缀相同的连续IP地址组成“CIDR地址块”，这种地址的聚合称作**路由聚合**。也称**超网。**

————练习题 P37

Chapter 5 — 4 控制协议

1、DHCP(Dynamic Host Configuration Protocol)

- 允许计算机加入新的网络并自动获取IP地址。主机启动时向DHCP服务器广播报文DISCOVER，DHCP服务器响应OFFER。
- DHCP服务器在数据库中查找计算机配置信息。若找到，返回信息。若找不到，从IP地址缓存区去一个地址分配给计算机。

2、专用地址与虚拟专网VPN

- 专用地址只能用于内部通信。路由器不会转发目的地址是专用地址的分组。
- VPN与外网的通信，需要通过**NAT**路由器与因特网连接

3、网络地址转换NAT(Network Address Translation)

- 将专用地址转换成全球地址IP_G
- 网络地址转换过程

```
1.主机用IPx和主机Y通信。数据报经过NAT转发。
2.NAT将IPx转化为IPg，利用IPx和TCP端口得到NAT表的索引。用IPg作为源地址发送给Y
3.NAT路由器收到Y发来的数据报。将目的地址IPg转化为IPx，再转发给内部的主机IPx
```

4、隧道技术

--------概念：把一种网络层协议封装到另一个协议中，以跨过网络传送到另一个路由器的处理过程 。

实质：对一种网络协议进行封装使其得以在网络上正常传播给另一路由器。

--------**应用场景**：实现IPV6子网互联、实现VPN

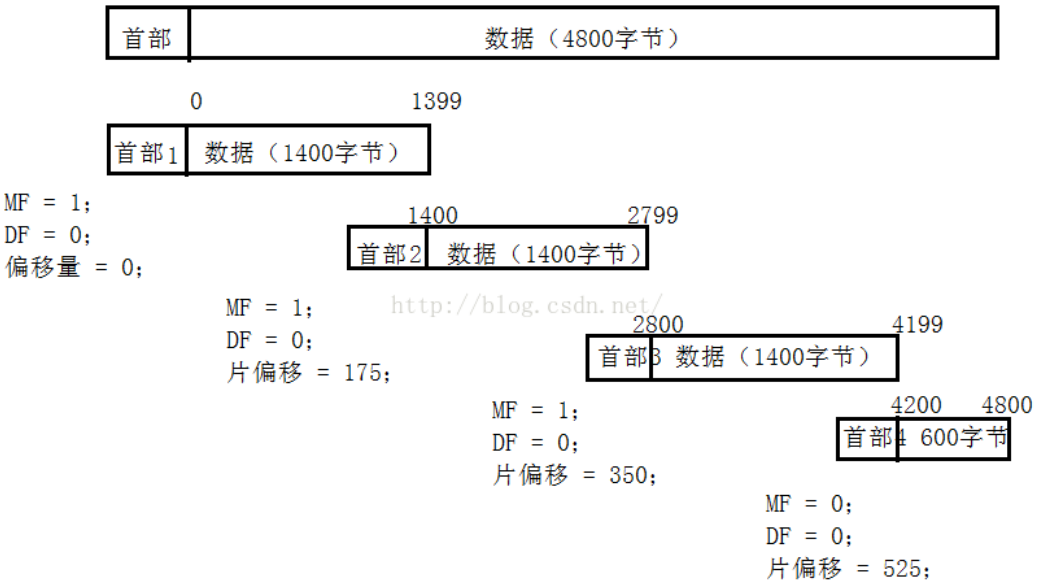
5、分组

--------分组分段

- 透明分段：路由器负责分段与重组。路由器开销比较大。
- 非透明分段：路由器对传输超过MTU的分组分段，目的主机负责重组。增加了传输的分组数，传输时间边长。

————分组分段的例子

片偏移以8字节为单位。



6、网络拥塞控制

--------流量调节方法

- 向源主机发送抑制报文(沿数据流反向传送到源节点)
- 逐跳后压(在拥塞沿路传输抑制报文，路由器减缓发送速率。消耗路由器缓存区空间)

7、ICMP因特网报文控制协议

--------报文分类

- ICMP差错报告报文
  - 目的地不可达、生存时间为0、源站抑制
- ICMP询问报文
  - 检查一台机器是否工作、时间戳请求和应答。

8、移动IP

--------问题背景

改变IP地址，会有“通信中断——再连接”的问题

--------**Mobile IP**

1.移动节点根据HA/FA代理**通告**，获得当前位置。

2.节点改变网络连接点时，获得CoA

移动节点向HA**注册**，建立$(CoA, MNIP)$的绑定关系

3、建立**隧道**，开始传送

$Chapter\ 5-5$ IP组播、移动主机和自组织网络

1、IP组播及路由

--------**IP组播的特点**

- 使用组播地址：D类地址支持组播(只可以用作目的地址)
- 永久组地址(由IANA分配)
- 使用硬件进行组播
  - D类地址的后28位参与组成以太网硬件地址

--------**IGMP**

IGMP：使路由器获得组播组的成员信息

```
1.主机加入或离开组播组
----主机加入组播组，向组播组对应的某一D类地址发送IGMP成员报告报文，
本地组播组路由器收到IGMP报文之后，将组成员关系转发给其他组播路由器
----主机离开组播组，发送IGMP成员离开报文。
2.组播路由器维护成员信息，周期性发送探寻报文
如果一个在几次探寻之后仍然没有一个主机响应，就不在向其他组播路由器转发成员信息
```

--------**组播路由选择协议**

组播路由选择协议：使组播路由器之间协同工作，用最小代价将组播数据报传送给所有的组成员

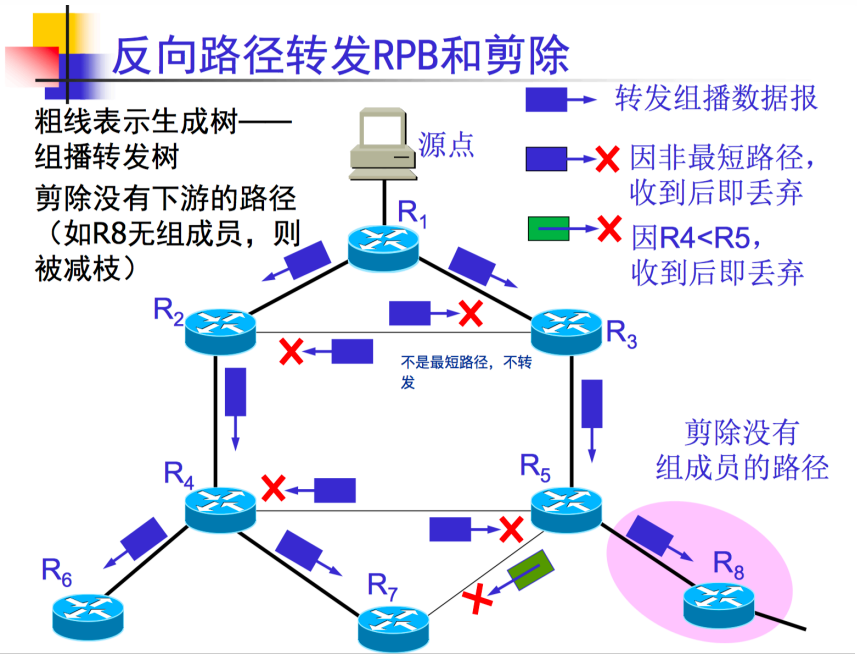
目的：找出以**源主机**为**根节点**的组播转发树。

转发组播数据报的方法

- 基于生成树

  路由器转发组播数据包使用$flooding$。使用 **RPF**(Reverse Path Forwarding反向路径转发)避免循环

  RPF：路由器收到组播数据报时，检查是否是从源点经过最短路转发来的。若是，继续转发；否则丢弃。如果存在几条最短路径，则只选择IP地址最小的路由器。



- 基于核心树

  全部路由器同意以某一路由器作为核心。成员先向核心发送组播分组，然后核心发送组播分组给组内各成员。

几种组播路由选择协议

- 距离向量组播路由协议$DVMRP$
- 组播$MOSPF$
- 协议独立组播PIM
- 基于核心的转发树CBT

--------练习题 P20

2、移动主机路由(同上)

3、自组织网络路由(Ad Hoc)

网络中所有节点均可移动

--------AODV路由协议

全称：Ad Hoc On-Demand Distance Vector

过程：

```
1.节点S发送分组给节点D，但没有到节点D的路径，启动路由发现过程。
2.节点S泛洪RREQ(Route Request)分组
3.其他节点收到RREQ后广播，同时建立到源节点的反向路径
4.目的节点D收到RREQ，发送RREP作为相应。
5.RREP沿着RREQ转发过程建立的路径的相反方向转发
```

Chapter 6 — 1 传输层概述-UDP与DNS

1、传输层的功能及服务

--------寻址：应用程序接收不同端口上的消息

--------多路复用：多个应用使用同一主机地址

> 服务器如何为多个用户提供服务?
> 1.服务器在固定端口监听，不同端口提供不同的服务
> 2.端口映射器。用户与端口映射器连接，得到指定服务器的TSAP，再连接。类似查号台。
>
> 传输层负责进程间通信。端口在进程间通信的作用：标志进程

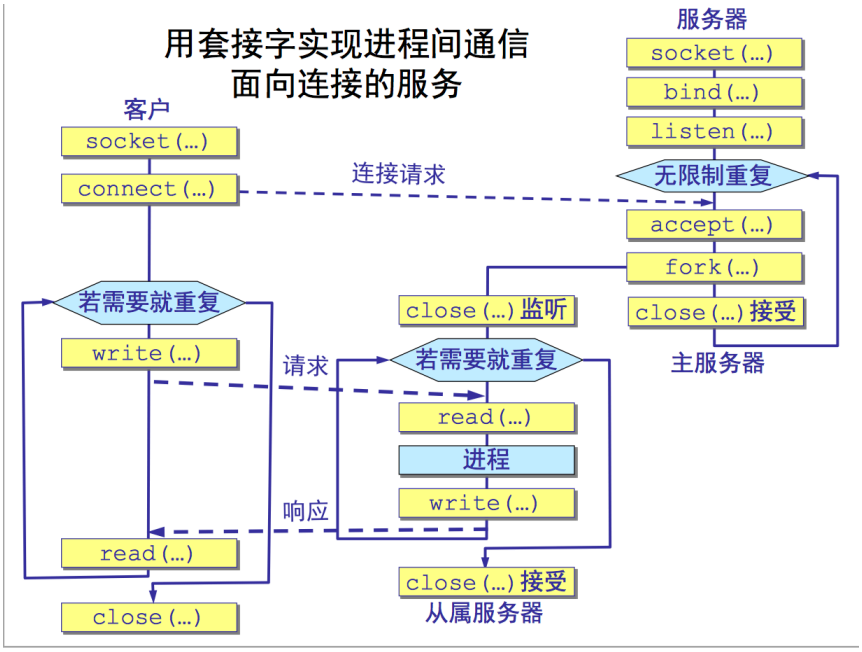
--------提供可靠和不可靠的逻辑信道

TCP && UDP

——端口：端口号占16bit

——套接字 socket = (IP address : port)

——使用套接字实现进程间通信(有连接) listen到一个连接请求，fork一个子进程出来处理相关服务。



2、DNS系统

概念：(Domain Name System)域名系统

全球13个root服务器

ISP：互联网服务提供商

--------DNS工作步骤

本地DNS若无法对域名进行解析，就先求助于根域名服务器。根域名服务器使用迭代查询，把下一步要找的顶级域名服务器的IP地址告诉本地DNS。

--------域名解析过程

```
********递归查询********
本地DNS代替主机处理域名解析工作，直到返回完整的答案。
主机向本地DNS一般递归查询。若本地无法解析域名，就以DNS客户的身份，向根DNS继续发出查询请求报文。
********迭代查询********
本地DNS向根DNS的查询通常是迭代查询。根DNS收到本地DNS的迭代查询请求报文时，给出IP地址或下一步要查询的域名服务器。
```

--------DNS缓存

每个域名服务器维护一个高速缓存，存放最近用过的名字，以及从何处获得名字映射信息的记录。

可以减少根域名服务器的负载。

--------习题 P47

$Chapter\ 6-2$ TCP与可靠传输

1、连接建立过程

发送端发送连接请求CR，等待确认ACK。由于网络拥塞会导致数据重复接收。

解决方案：源端设置段序号作为段标记，基于主机时钟设置初始序号，序号递增。

在T秒内序号不能重用。序号空间要足够大，这样在序号回绕时，旧序号的段已经消失。

禁用区的概念。

--------练习题 P8

--------发送方如何知道接收方的序号

三次握手

```
1.主机1发送CR，初始序号为X
2.主机2发送ACK，确认主机1的序号X，并告诉主机1它的序号为Y(seq = Y, ack = X)
3.主机1向主机2发送data，确认主机2的序号，并声明自己的序号X
```

网络层面向连接需要2次握手，非连接需要3次握手。

2、连接释放

正常需要三次握手。DR=>DR=>ACK。

若ACK丢失，主机2会启动定时器。定时器时间到，释放连接。

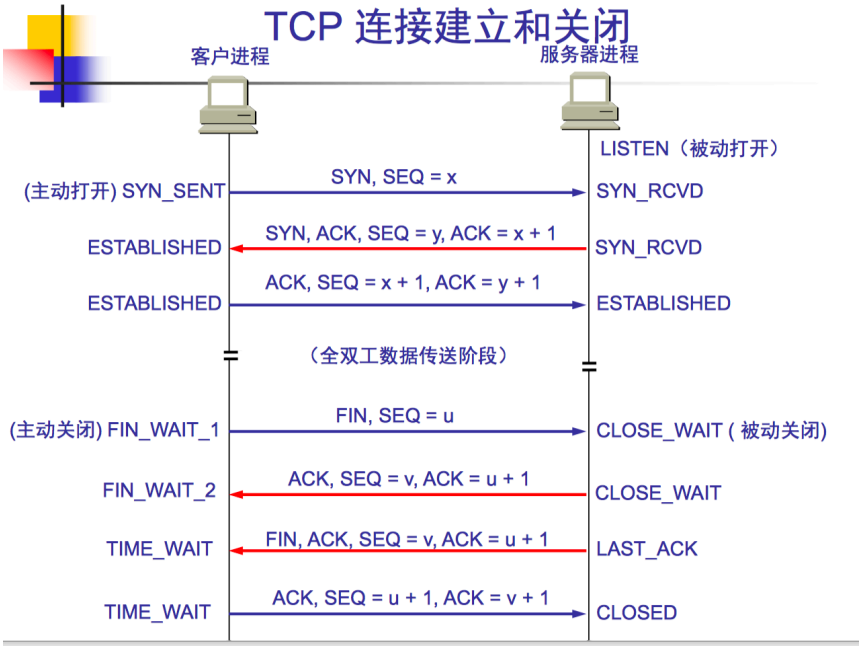
响应丢失=>杀死半连接

3、TCP

--------TCP连接的三个阶段：连接建立、数据传送、连接释放

--------TCP连接建立

3次握手，保证收发双方序号同步。和数据报的3次握手很像。



--------TCP滑动窗口

提高效率：发端不发送太小的报文段，收端不通告太小的接收窗口。

————练习题 最后一页

Chapter 6 — 3 TCP协议与拥塞控制

1、流量控制与拥塞控制

--------流量控制

TCP提供流量控制，防止数据在接收缓存中溢出。

--------拥塞控制原因

源主机数太多，向网络发送数据速率过高。协调多个发送端。

--------最大-最小公平性：分配一个流的带宽时，若不减少另一个流的带宽，就无法增加该流的带宽。

--------最大-最小公平算法

```
形式化定义：
    资源按需求递增顺序分配。
    不存在用户得到的资源超过其需求。
    未得到满足的用户等价分享资源
tot_money = c
tot_people = n
x[] = 每个人分到的资源量
need[] = 每个人实际需求量

x = [c/n for i in range(1, n+1)]         # 初始平均分
for i in range(1, n+1):
    if need[i]-x[i]>0:
        for j in range(i+1, n+1):        # 多余的量，让剩下(n-i)个人平均分
            x[j] += (need[i]-x[i]) / (n-i)
            x[i] = need[i]       # 它只要满足自己需求就行了
            else:   # 已经无法再分配，算法结束
                break
```

--------拥塞控制具体操作

发送端维护流量控制窗口 $rwnd$ 和拥塞窗口 $cwnd$

发送窗口 $swnd = min(rwnd, cwnd)$

TCP Tahoe（Jacobson）

- 慢启动(指数增加)
  - 若cwnd ssthresh (慢启动门限)，则为慢启动阶段
  - 每收到一个ACK，增加一个报文长度(成倍增长)
- 拥塞避免(线性增加)
- 发生拥塞时，拥塞门限减半(乘性减少)
  - 定时器超时，$ssthresh = cwnd/2$
- 若数据发送成功，增加拥塞窗口

TCP Reno (1990)

继承了Jacobson 算法，增加快重传及快恢复

- 快重传：3次重复ACK代表报文段丢失
- 快恢复（直接从减半之后的慢启动门限开始继续）
- 收到n个重复ACK时，慢启动门限ssthresh = cwnd / 2, cwnd = ssthresh + n * MSS(最大报文长度)

--------TCP定时器管理

根据往返时延来定。超时重发机制。

指数加权移动平均(EWMA)

$RTT = \alpha * RTT + (1 - \alpha) * M$：aplha越接近1，新的往返时延对RTT影响越小。

超时重传时间 RTO

$RTO = \beta * RTT$，一般beta设置为2

另一种算法

```
延迟变化为 RTT-M
平均延迟的变化D为
D = alpha * D + (1-alpha)*(|RTT-M|)
RTO = RTT + 4 * D
```

--------练习题 P65

Chapter 7 — 1 应用层

1、流媒体应用与协议

--------流媒体：音频/视频数据

--------三类服务

- 存储的流媒体
  - 媒体存在信源端，传递给客户
  - 早期的电台和电视
- 实况的流媒体
  - 弱交互
  - 录音机录像机
  - 可以暂停回放快进
- 交互式流媒体
  - 交互式
  - IP电话，视频会议

2、传输协议

实施传输协议 RTP(Real-time Transport Protocol)：为实时应用提供端到端的服务

RTCP：RTP控制协议：服务质量检测与反馈、媒体流之间的同步、多播组的成员标识

实时流媒体协议RTSP(Real-time Streaming Protocol)：播放器控制多媒体流的传送

SIP协议(Session Initiation Protocol)

- VOIP 信令协议，支持移动性。比如因特网电话呼叫，视频会议

多媒体播放器的功能

- 用户界面、解压缩、消除错误、缓存播放

————练习题P 60

$Chapter\ 7-2$ QoS概述

1、QoS

概念：$Quality\ of\ Service$

————带宽，延迟，抖动(网络时延变化导致分组到达速率变化=>语音忽快忽慢)，丢帧率

--------IntServ

综合服务与资源预留

- 资源预留：路由器知道为某一会话预留多少资源
- 呼叫建立：需要服务质量保证的会话必须首先在源到目的的路径上的每个路由器预留足够的资源。

RSVP：资源预留协议(Resource Reservation Protocol)

--------DiffSer 区分服务

- 路由器中增加区分服务的功能，对服务类型划分等级
- 将网络划分为许多DS域
    - 边界路由器功能复杂，域内路由器功能尽可能简单
- 边界路由器：分类，标记，整形，测量
- 聚合：根据流的DS值将若干个流聚合成更少的流

--------调度机制

概念：选择链路上需要发送的下一个分组

调度算法

- FIFO
- 优先级调度　分类器：根据分组头部信息进行标记，比如 ip 源/目的地址，端口号
- 循环调度
    - 按类别归队
    - 循环扫描各个类别的队列，每个队列服务一次
- 加权公平调度
    - 为每个类别的队列分配一个服务权重

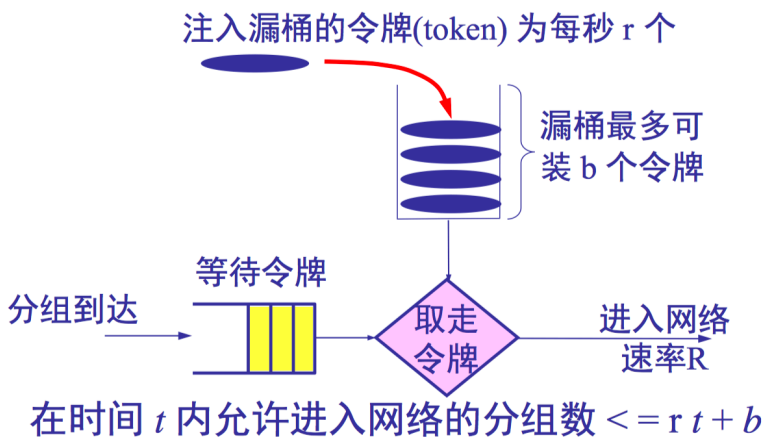
--------流量整形

目的：将输入流的速率控制在有效带宽之内，以避免拥塞和分组延迟

几个概念

- 平均速率：控制1个数据流的平均速率
- 峰值速率：限制数据流在非常短的时间内的流量
- 突发长度：限制在非常短的时间内连续注入到网络中的分组数

令牌桶



突发时间 $rt+b=tR,\ t=b/(R-r)$

突发数据长度$Rt=Rb/(R-r)$

长期速率由r限制，短期突发长度由b限制

```
令牌桶 B>0 ：限制平均速率，也允许某种程度的突发
令牌桶 B=0：又叫漏桶，强行限制数据速率，不允许突发
```

--------内容分发网络CDN

目的：避开网络上可能影响数据传输速率和稳定性的瓶颈，在各部分设置节点，可以根据用户的请求将请求导到最近的节点服务器上。可以解决internet拥挤。

--------多协议标记交换MPLS

概念：用面向连接的方式代替IP的无连接分组交换。用更快捷的查找算法替代最长前缀匹配方法来查找路由表。

每个分组携带一个标记，交换机读取分组标记，用标记值检索转发表

--------习题 P66

$Chapter\ 7-3$ 网络安全概述

1、信息传输安全的概念（***必考***）

- 机密性：保证信息为授权者使用
- 认证性：接收敏感信息时，确认对方是谁
- 完整性：信息传递中不会被第三方修改添加删除

- 不可否认性：不可否认已发送的信息

2、信息传输面临的问题

- 窃取
- 中断
- 篡改
- 伪造

3、数据加密模型

加密函数 E，密钥 K。

解密函数 D，密钥 K

算法公开，密钥保密

--------密码体制

- 常规密码体制——对称密钥系统
  - 加密密钥解密密钥相同
  - 置换密码、替代密码、DES（数据加密标准）
  - ```
    加密：
        对明文分组，每组64位。
        对每个64位加密，产生一组64位的报文。连接后得到密文
    解密：
        密钥64位(56位密钥 + 8位奇偶校验)
        经过16次迭代运算得到L16,R16。行逆置换
    ```
  -
- 公钥密码体制
  - 两个密钥不同
  - ```
    RSA算法
    1.选两个素数
    2.n = p*q, z = (p-1)*(q-1)
    3.选一个和z互素的数d
    4.找到e使得e*d = 1 mod (z)
    明文加密：  C = p^e mod (n)
    解密C：P = C^d mod (n)
    ```
  -

4、数字签名

--------产生背景

- 接收者能核实发送者身份

- 发送者事后不能抵赖
- 接收者不能伪造报文

--------数字签名的方法

- 对称密钥签名
- 公开密钥签名
- 报文摘要

举例：A 给 B 发东西，用B 的**公钥**加密，用A的**私钥**加数字签名。

报文摘要：方便接收方验证报文的真伪。减少计算量

```
A对报文X用密码散列算法得到报文摘要H。
用私钥对H进行数字签名，得到签名的报文摘要D(H)。
将其追加在报文X后面发送给B。

B如何验证?
    收到报文x，先将签名和报文分离。用A的公钥对D(H)作E运算得到H。
    然后对报文X进行报文摘要得到H'。
    比较H是否等于H'
```

5、认证

--------概念：验证通信对端是期望的实体而不是伪造者。

--------重放：第三方截取A到B的报文并重新发送。

--------认证方法

- 基于共享密钥
- 基于公开密钥
- 基于密钥分发中心
- **一种认证方法**：用KDC分配对称密钥

-------认证中心与证书

认证中心CA：将实体的公钥与实体进行绑定。

每个都有CA发送的证书，含有公钥以及拥有者的标志。证书被CA加上了**数字签名**

验证时，用户从可信任的地方获得CA的公钥，验证某个公钥是否是某个实体的。

6、DNSsec

DNS安全扩展：DNS发送信息用私钥签名

7、网络层安全协议

-------IPsec

网络协议安全性：在IP数据包中的数据都是加密的，包括

- 认证首部AH：接收点根据AH认证源节点并检查数据完整性，不保密
- 封装安全有效载荷ESP：接收点认证源节点，检查数据完整性，提供数据保密性

————安全关联SA(Security Association)

使用AH或ESP之前，从源主机到目的主机建立一条安全关联SA，有一个共享密钥。

8、传输层安全协议

--------安全 套接层SSL

全称：secure socket Layer

作用

- 对web客户与服务器之间传送的数据进行加密和认证
- 连接建立阶段协商将要使用的加密算法和密钥。以及客户与服务器之间的认证。

SSL三次握手

```
不会考，略
```

8、IEEE 802.11 (无线网)安全性

--------WEP（有线等效保密）

可以数据加密和认证。

认证

```
无线主机通过AP请求认证
AP回应一个128字节的不重数
无线主机用一个与AP共享密钥加密该不重数
AP解密该不重数
不重数与发出去的相同 => 通过认证
```

--------EAP（可扩展认证协议）

端到端客户到认证服务器的协议

————练习题 P71

名词解释

路由 && 转发

路由表 VS 转发表：转发表描述了主机方面的信息，在主机内部将一个数据包从一个端口导向另一端口，而路由表描述网络信息，将数据包从一个机器导向另一机器

HOL

Flooding

RIP

OSPF

因特网四大协议：ARP, RARP, ICMP, IGMP

子网掩码

CIDR

路由聚合/超网

DHCP

VPN

NAT

隧道技术

组播路由选择协议

RPF

Ad Hoc

AODV路由协议

DNS

递归查询与迭代查询

序号回绕

RTP

RTSP

RSVP

CDN

MPLS

DES

数字签名

报文摘要

重放

中间人攻击(过程比较复杂，应该不会考)

CA，证书

DNSsec

SSL

WEP

EAP

ADSL：非对称用户数字电路。上行下载带宽不对称