计算机网络复习提纲

第一章 引言

- 按照网络规模的分类
- 接口、协议、服务
- 理解面向连接和无连接的服务
- ISO 的 OSI 与 TCP/IP

第二章 物理层

- 各种传输介质的特点和比较
- 数字调制与多路复用
- 基带传输与通带传输的概念
- 基带传输中的几种编码方式（图 2-20）
- 4B/5B 编码的作用和代价
- 通带传输中的三种调制方法
- 频分复用、时分复用、码分复用
- CDMA（图 2-28）
- 电路交换与包交换

第三章 数据链路层

- 4 种成帧方法
- 纠错码与检错码
- CRC 的计算

第四章 介质访问控制子层

- ALOHA：纯的、分槽的
- CSMA：坚持的、非坚持的、p 坚持的、带冲突检测的
- 无冲突协议：位图、令牌传递、二进制倒计数
- 暴露终端、隐藏终端
- 以太网帧格式，关于长度
- 以太网：二进制指数后退的 CSMA/CD
- 无线局域网：CSMA/CA
- 802.11 的帧间间隔：图 4-28
- 停等式交换与直通式交换（虫洞路由）
- VLAN

第五章 网络层

- 虚电路与数据报网络的比较，图 5-4
- 泛洪算法、距离矢量路由、链路状态路由
- 图 5-13
- 层次路由
- 三角路由
- 拥塞控制的途径及其反应速度
- 显示拥塞通知及逐跳后压
- 负载脱落中的 wine 和 milk
- 漏洞和令牌桶
- 加权公平队列的数据包完成时间（图 5-31）
- 数据包分段：透明、非透明
- 路径 MTU 发现
- IPv4 地址分类、子网划分、子网掩码

第六章 传输层

- UDP、TCP
- AIMD
- TCP 段头格式
- TCP 计时器：重传、持续、保活
- TCP 的两个窗口：拥塞窗口、流量窗口
- 图 6-46、图 6-47
- 选择确认

第一章 绪论

按照网络规模分类：个域网 PAN，局域网 LAN，城域网 MAN，广域网 WAN

OSI 的核心概念：

接口：每一对相邻层次之间是接口
协议：通信双方就如何通信的一种约定
服务：服务定义了该层是做什么的，而不是上层如何访问这一层。

面向连接的服务：像一个管道。 有时需要 发送方、接收方、子网一起协商。
无连接服务： 如发送邮件。

有确认的数据报服务：像挂号信一样。

ISO 的 OSI：开放系统互联 open systems interconnection

七层的基本原则如下：

1) 需要不同抽象体的地方创建一个
2) 每层应该执行一个明确定义的功能。
3) 每一层功能选择，应该向定义国际标准化的目标看齐。
4) 层与层边界的选择应该是跨越接口的信息流最小。
5) 层数应该适中。

物理层 ： 原始比特 初始连接如何建立，及撤销连接。
数据链路层： 传**数据帧**，变成一条没有漏检错误的线路，还要接受 **确认帧**
（**有一个子层——介质访问控制子层，处理共享信道的访问**）
网络层：解决路径确定， 拥塞控制， 服务质量（延迟，抖动，传输时间） 以及网络协议不一样的问题。
传输层：真正的端到端 而上面那三个是链式连接的。
会话层：提供一些服务，
表示层：解决编码 管理抽象的数据结构，转换成高层的数据结构
应用层：提供各种各样的协议。

TCP/IP
链路层：（小心前面没有数据） 描述了链路必须完成什么功能才能满足无连接的互联网络层。不是真正意义上的一个层，是主机与传输线路之间的一个接口。
互联网层：互联网络，可对应于网络层
传输层：
应用层： 把是哪个都包括了

注：大写大写(MB)^n 大写小写(Mbps) 为 10^n

第二章 物理层

各种传输介质的特点和比较：

书上另有 磁介质,电力线（利用早期铺成的电话线）

双绞线：

l）最常用的传输介质

2）由规则螺旋结构排列的 2 根、4 根或 8 根绝缘导线组成

3）传输距离为 100m

4）局域网中所使用的双绞线分为二类：屏蔽双绞线（STP ）与非屏蔽双绞线（UTP）；根据传输特性可分为三类线、五类线等

STP 就是加了一个屏蔽层，使得很笨重。

同轴电缆：

l ）由内导体、绝缘层、外屏蔽层及外部保护层组成

2 ）根据同轴电缆的带宽不同可分为：基带同轴电缆和宽带同轴电缆

3 ）安装复杂，成本低

光纤：

1 ）传输介质中性能最好、应用前途最广泛的一种

2 ）光纤传输的类型可分为单模和多模两种

3 ）低损耗、宽频带、高数据传输速率、低误码率、安全保密性好

数字调制与多路复用 （后面的概念基本上是它的子类）

1.数字调制：发送比特要先用模拟信号表示，比特 u 代表它们的信号之间的转换过程称为数字调制。

1.1 基带传输：有线介质使用，信号的传输占据了介质的所有频率。

1.1.1 NRZ 至少用 B/2 HZ 的带宽才能获得 B bps 比特率，2B 次采样

1.1.2 曼切斯特 两倍于 NRZ 的带宽

1.1.3 NRZI 使发送连续的 1 不会导致接收器难以区分， 至于 0 就要使用 4B/5B 编码避开连续三个 0。 增加了 25%的带宽

1.1.4 平衡信号 信号均值为 0 双极编码

1.2 通带传输：以载波信号为中心的一段频带。 无线和光纤通信用。

1.2.1 **调制方法**： 幅移，频移，相移

1.2.2 频分复用：FDM （multiplexing 多路复用）其实频率间也有重复 对于正交频分复用（OFDM）内积为零 802.11 用。

1.2.3 时分复用：TDM 分时间片轮着用。 不过对于统计时分复用，不用就不给，如同包交换。

1.2.4 码分复用：CDM （CDMA 码分多址 Code division multiplexing access）

就是每个比特时间分成更小的时间间隔（称为码片 chip），可以按照站的数目来划分。 每个站有自己的码向量，两两正交。

设计码片 S 的原则：1）不同的码片正交 与别人的内积为 0

2）自己和自己的为 1 （感觉是必然）

3）与自己相反的为-1

使用原则： 1)当有自己发送时，为 1 则发 S，为 0 则发-s（s 加入到运算中）.

2) 与其余的相加。

解码：实现要知道对应的码片，相乘总体的得到的结果就是 自己对应的那个比特。

（当然要除以 向量的模） 结果为 0 则没参入

2．多路复用：信道通常被多个信号共享，这种共享形式称为多路复用。

交换：

电路交换：物理连接，发送数据之前需要建立一条端到端的路径。

包交换：1）不需事先建立一个专门线路。

2）路径的选择取决于发送时的网络状况。

3）存储-转发传输技术

区别 10 种

项目	电路交换	包交换
呼叫建立	需要	不需要
专用物理路径	是	不是
每个包遵循相同的路由	是	不是
包按序到达	是	不是
交换机崩溃是否致命	是	不是
可用带宽	固定	动态
可能拥塞的时间	在建立时	在每个包
潜在浪费带宽	是	不是
存储-转发传输	不是	是
收费	按分钟计	按包计

图 2-44　电路交换和数据包交换网络的比较

第三章 数据链路层

四种成帧的方法：

1 字节计数法　　---每个帧自己确定一个帧长

2 字节填充标志字节法　用特殊的字节而作为开始和结束，然后就要考虑转义了，还有转义的转义。

3. 比特填充的标志比特法

USB 所用， 发送方出现 5 个连续的 1 时就填充一个 0，但是接收方会去掉 0，再存储。

4. 物理层编码违禁法

比如 4B/5B 用保留的信号来指示帧的开始结束。

纠错码与检错码

d 个错误 需要用 d+1 个码来检测 2d+1 来纠错。

海明码纠错 2 的幂次方位是校验位，其余位填充。要查看 K 位置上的校验位则改成 2 的幂次之和，如果是偶校验则结果应该为 0，否则就出错。纠错就是取反。

检错：简单的**奇偶校验**， 就是加起来是偶数就在后面补个 0，否则补个 1

或者是先把数据发了，最后跟个校验和。、

校验和：与信息相关的一组校验位。 奇偶校验也是其中之一。

循环冗余校验(CRC，cyclic redundancy check) ，多项式编码(polynomial code)：

1) 双方预定一个多项式。最高位和最低位的系数必须为 1　G(x)

2) 假设一帧有 m 位，对应多项式 M(x)，为计算其 CRC 则需比 G(X)长，所以要补 0

0 的个数为 G(X)的阶数。

3）做除法异或求得余数。再继续除法

4）得到余数后与添加了 0 的多项式异或，然后发出去。

第四章 介质访问控制子层

1.ALOHA

纯的：共享信道，帧被破坏了就需要随机等待一个时间重传

分槽的 ALOHA：每个时间对应一帧，要求用户遵守统一的时间槽边界。

2.CSMA：

载波检测多路访问。 监听是否存在载波（是否有传输），然后传送。

1-坚持 就是检测到没有载波就传送

非坚持（nonopersistence） 不贪婪，如果信道当时正在使用，那他不持续地监听，以便立即抓住机会传输。 而是过一段随机的时间，重复上面的过程。

P-坚持 空闲按照概率 p 来发送数据，以概率 q=1-p 推迟到下一个时间槽。

带冲突检测的（CSMA/CD collision detection）：空闲时检测冲突，超过 2t（将信号传到最远的站所用的时间）的时间如果发生冲突则过一个**随机的时间**重传。如果没有那么传完这个帧，下面的时间则用来传剩余部分。

3.无冲突协议

位图协议：在竞争期声明自己有传输的意愿，然后大家都遵守，按序来传。传完后就有下一个竞争期。

令牌传递：接收到令牌就传，然后再传递令牌到下一个站。

二进制倒计数： 相传则先广播自己的地址，从高序的位开始。线路会异或，然后每个站监听，如果发现自己的高位的某个 0 被改为 0 则放弃竞争。利用率为

//

暴露终端：检测到有站发送信息就不敢给某个发了，其实根本就没事

隐藏终端：由于不在一个终端的范围内还以为自己要发送的数据不会影响正在发送的数据，但实际上却会影响。

以太网帧格式（p218）：关于长度的问题，（如果对于以太网 DIX 为 类型 ，至于怎么判断通过前导码 8 字节中最后一个字节的后两位来判断，11 为 802.3 10 为以太网）

长度在 64KB-1500KB 之间 达不到则填充，下限是由于防止出现冲突，而无法挽回，上限是随便想出来的。

以太网：二进制指数后退的 CSMA/CD

之前是说明其如何实现冲突检测的，现在是说如果出现冲突，随机等待的时间怎么选。

规则：当冲突在 1-10 次之间则等待的时间间隔（槽）为 0-2^n-1 10-16 次一直为 1023

16 次则放弃，交给高层协议处理。

优点：1.当少量发生冲突的时候延迟较少

2.许多站发生冲突的时候，可保证相对合理的时间间隔内。

无线网

AP:接入点

以前的冲突检测，根本不起作用，因为总是半双工的

CSMA/CA （avoidance） 带有冲突避免的。

当两个都就绪的时候，都执行后退。（没有收到确认帧的时候也要执行后退，因为推测到冲突发生了）后退过程中

一个又开始发了则停止后退，等那个数据发完再继续后退剩下的时间。 后退也要向以太网那样指数后退，直到成功发送帧或达到重传的最大次数。

与以太网相比的区别：

1.采用早期后退

2.利用确认来判断是否发生冲突，因为冲突无法被测

上面那种操作模式称为 分布式协调功能（DCF distributed coordination function）

802.11 的帧间间隔： 为提高服务质量，对不同类型的帧确定不同的时间间隔

五类： 时间排序 SIFS(short interframe spacing 短帧间间隔) <AIFS1（仲裁帧间间隔）<

DIFS (DCF…… 常规的帧) <AFIS4 <EFIS(扩展的 仅用于存储位置或损坏的帧)

直通式交换：

它在输入端口检测到一个数据包时，检查该包的包头，获取包的目的地址，启动内部的动态查找表转换成相应的输出端口，在输入与输出交叉处接通，把数据包直通到相应的端口，实现交换功能。由于它只检查数据包的包头（通常只检查 14 个字节），不需要存储，所以切入方式具有延迟小，交换速度快的优点

它的缺点主要有三个方面：一是因为数据包内容并没有被以太网交换机保存下来，所以无法检查所传送的数据包是否有误，不能提供错误检测能力；第二，由于没有缓存，不能将具有不同速率的输入/输出端口直接接通，而且容易丢包。如果要连到高速网络上，如提供快速以太网（100BASE－T）、FDDI 或 ATM 连接，就不能简单地将输入/输出端口“接通”，因为输入/输出端口间有速度上的差异，必须提供缓存；第三，当以太网交换机的端口增加时，交换矩阵变得越来越复杂，实现起来就越困难。

VLAN 虚拟局域网

直接的局限：1.超越了企业的组织结构

2.负载，有些地方负载大会影响整个网络 LAN

3.广播流量，特别是当借口崩溃或配置错误的时候，会导致广播风暴。

使用：

网桥必须建立配置表，指明通过哪些端口可以访问哪些 VLAN。

802.1Q 帧格式

加了一对 2 字节的字段

第一个两字节

VLAN 协议的 ID 大于 1500 为 0x8100 这样其他的以太网卡会把它认为是类型，而不是长度则不会转发给传统网卡。

第二个两字节

后 12 位 为 **VLAN 标识符**，这样到达一个 **VLAN 感知交换机**，会利用其 VLAN 标识符作为索引。 （哪些端口输入那个 vlan）

第五章 网络层

虚电路与数据报网络的比较 p278

问题	数据报网络	虚电路网络
电路建立	不需要	需要
寻址	每个包包含全部的源和目标地址	每个包包含简短的VC号
状态信息	路由器不保留连接状态	针对每个连接，每条VC 都需要路由器保存其状态
路由方式	每个数据包被单独路由	建立VC 时选择路由，所有包都遵循该路由
路由器失效的影响	没影响，除了那些路由器崩溃期间丢失的包	穿过故障路由器的所有VC都将中断
服务质量	困难	容易，如果在预先建立每条VC 时有足够的资源可分配
拥塞控制	困难	容易，如果在预先建立每条VC 时有足够的资源可分配

图 5-4　数据报网络和虚电路网络的比较

泛洪算法： 总能选出最短路径，且延迟短

首先要产生大量重复的数据包，所以要给每个包上有一个计数器。

抑制包泛滥需要在接收到主机的数据包时填上一个序号，然后每个路由器为每个源路由器准备一张表，记录来自源路由器的序号。如果入境路由器在这张表里面，就不需要泛洪了。

为防止无限膨胀，要比较要用个计数器 K 进行比较，比 K 小的就不要了。

距离矢量算法：

路由表有两项 一个是记录 到目标路由器的首选出境线路 第二个是到达该目标路由器的距离估计值。

如果距离用时间度量则要发送一个特殊的 **ECHO 数据包**给邻居，邻居收到后盖上时间戳，然后尽快发过来。记住时间要除以 2

但是由于互相没联系，则可能出现无穷计数的问题。

链路状态路由算法(LSR)：

每一个路由器必须完成以下几个事情：

1） 发现他的邻居节点，并了解其网络地址

2） 设置到每个邻居节点的而距离或者成本度量值。

3） 构造一个包含所有刚刚获知的链路信息包。

4） 将这个包发送给其他的路由器，并接受来自其他所有路由器的信息包。

5） 计算出到每个其他路径的最短距离。

那个序号其实可以表示接受到的数据的新旧。序号随每一个新数据包的发出而逐一递减。为了防止序号破坏造成影响则用时间 age。

特点（与矢量路由算法的比较）：

收到一个链路状态数据包（LSP）后链路状态路由协议便**立即**将该 LSP 从除接收该 LSP 的接口以外的所有接口泛洪出去。使用距离矢量路由协议的路由器**需要处理每个路由更新**，并且在更新完路由表后才能将更新从路由器接口泛洪出去，即使对触发更新也是如此。因此链路状态路由协议可更快达到收敛状态。

在初始 LSP 泛洪之后，链路状态路由协议仅**在拓扑发生改变时才发出 LSP**。该 LSP 仅包含受影响链路的信息。与某些距离矢量路由协议不同的是，链路状态路由协议**不会定期发送更新**。

层次路由：

为了防止路由太多而导致路由表太长，所以需要分层，这样就成为独立的区域。

但是不一定能够得到最短的路径。 包含 N 个路由器，最优秀的层数是 lnN 层。每个路由器所需要的表项是 elnN

个。

三角路由 （其实就是**移动主机路由**的路由过程）

电话公司及 Internet 几乎都是这么干的

步骤：1.移动主机先把转移地址 告诉家乡代理。

2. 发送者发送的信息。

3.被家乡代理拦截。然后将那个数据包 用新的头**封装，**再发给转交地址。这种机制交封装

4 移动主机提取出真正的包然后直接应答发送者。

5．发送者借鉴转交地址 通过隧道发送转交地址，绕过家乡位置。

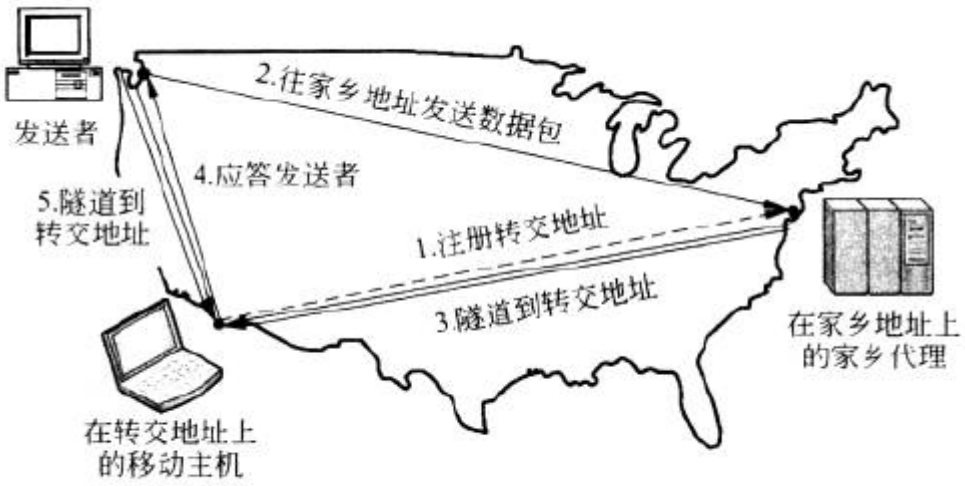

图 5-19 移动主机的数据包路由过程

拥塞控制的途径及其反应速度

网络供给>**流量感知路由**>准入控制>**流量限制**>负载脱落

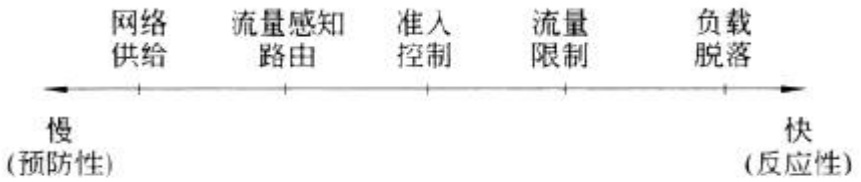

图 5-22 拥塞控制方法的时间尺度

流量调节

抑制包，告诉源主机减少给制定目标的流量

显示拥塞通知（ECN explicit congestion notification）

就是如果自己拥塞了就在他发送的数据包上打上标志（设置包头上的一个标志位） **但是直到到了主机才通知拥塞。**

逐跳后压:

让抑制包在沿途的每一跳都发挥作用。

上游要有更多的缓存空间。

负载脱落（load shedding）中的 wine 和 milk

就是先扔掉什么的问题 最好程序标记一下那些重要。

随机早期检测（RED）

在局面变得毫无希望之前让路由器提前丢包，这里就是讲怎么确定这个时间点。

一般是当平均队列超过某个阀值时。 丢掉的包起到了抑制包的作用，而不是 ECN 那样有个拥塞信号。

服务质量

漏洞和令牌桶

主要讲令牌桶

书上的那个图 是说明 令牌桶有流量整形的作用。 仔细看令牌的初始容量 B 就可以看出图的区别。 注意下面的曲线代表有令牌存起来了。

B+RS=MS S:突发的长度/时间 M 最大速度的突发长度。

加权公平队列

分为两部分 **公平队列+加权**。

公平队列只是假想着“字节接字节发送” **不能抢占正在传输的数据包，因为数据包传送是个整体的行为。**

Fi= max(Ai,Fi-1)+Li/W

Fi :第 i 个包的发送结束时间 Ai 为开始时间 LI 为长度 W 为所在队列的权值。

数据包分段：透明、非透明 （P333）

解决大数据包过最大数据包太小的网络。

法 1 设法使这种事情不会发生 最大路径单元 MTU（Path Maximum Transmission Unit） 不发送这么大的。

法 2 拆分数据包。

透明分段：是指 入口路由器分段出口路由器组合 **问题：** 不知什么时候接受了全部的段。 必须在同一个出口路由器进行性重组。

非透明分段：重组只在目标主机上进行。

IP 则使用这种思想，头分为三个部分 **数据包编号**（同一个数据包则一模一样）

偏移位置：就是指这个包的开头与原来的开头的距离（相减）比如一开始是 0

是否为结束：则不是 1 则是 一开始为 1

路径 MTU 发现

就是打算重新使用上面的第一种方法

IP 有个标志位告诉是否允许分段。如果不允许则路由器就丢弃这个包，并把错误信息报告给源端，这样源端就会知道要发送多长的数据包了。（一个一个地尝试直到符合）

Internet 的网络层

IPv4 地址分类：

从 A-D 网络位开头每个多 1 且最后为 0 ，且总体上是由那划分的三段来划分的而 E 只不过是把 D 的剩余部分要了。 **小心 D 是个组播地址**

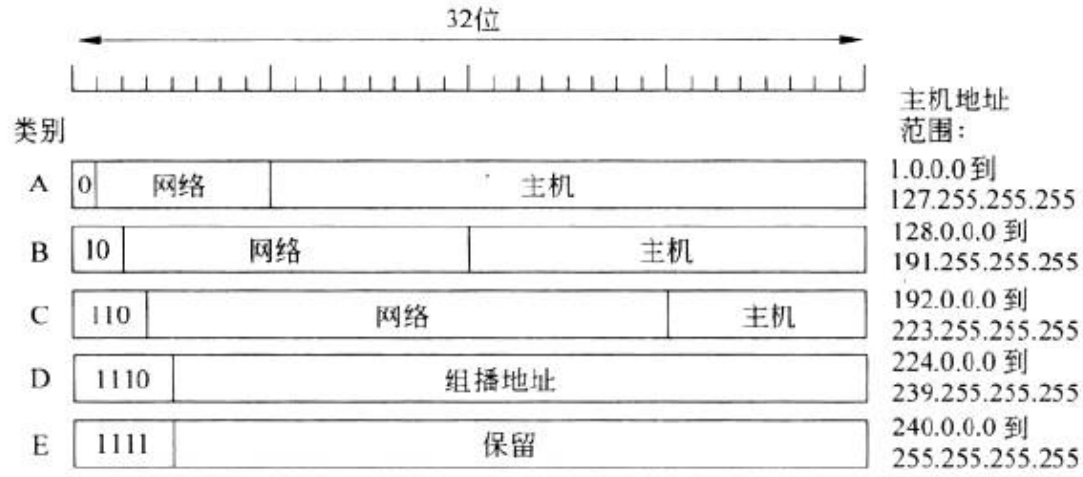

图 5-53　IP 地址格式

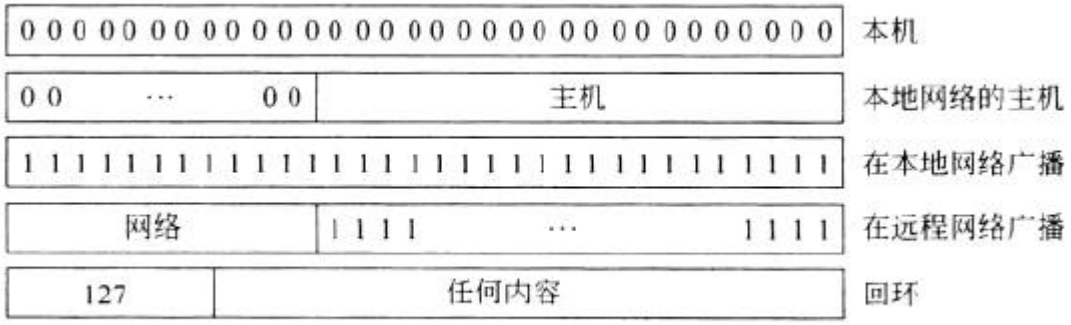

图 5-54　特殊 IP 地址

子网划分：

将内部一个网络块分成几个部分供多个内部网络使用，但对外部世界仍然像等那个网络一样。

方法：数据包到达时，把数据包的目标地址与每个子网的掩码进行 **AND 操作**，看结果**是否对应某个前缀**。　而且可以随意改变内部的子网掩码。

第六章 传输层

总括：　网络层+传输层 为 **网络协议层次的核心。**扩展到两个计算机进程之间的端到端联系。

且其可靠性独立于当前的网络。

其之间可以理解为用 段 来传输。

虽然和网络层很像 但是用户没有对其的控制权。　当然此中需要调用库程序实现。

AIMD (Additive Increase Multiplicative Decrease　) 解决拥塞控制的

TCP/IP 模型中，属于传输层，为了解决拥塞控制的一个方法，即：加性增，乘性减，或者叫做“和式增加，积式减少”。

当 TCP 发送方感受到端到端路径无拥塞时就线性的增加其发送速度，当察觉到路径拥塞时就乘性减小其发送速度。

TCP 拥塞控制协议的线性增长阶段被称为避免拥塞。

当 TCP 发送端收到 ACK，并且没有检测到丢包事件时，拥塞窗口加 1；当 TCP 发送端检测到丢包事件后，拥塞窗口除以 2。

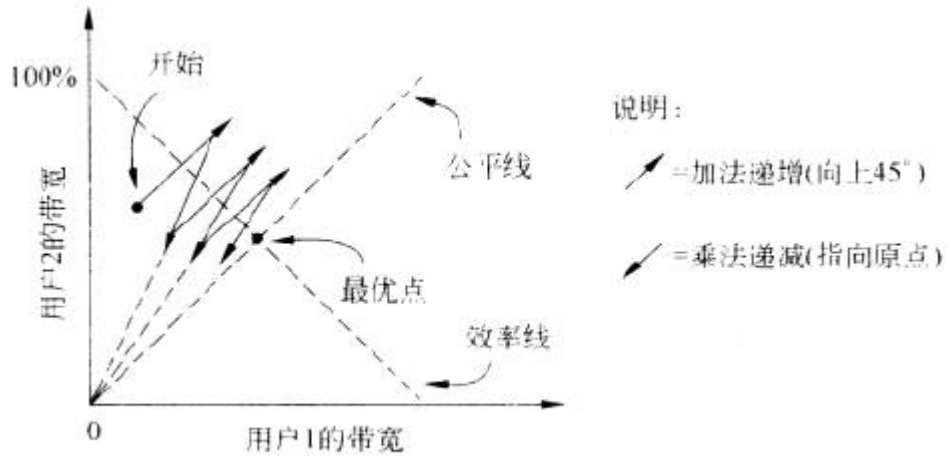

图 6-25　加法递增乘法递减（AIMD）控制法则

UDP（User datagram protocol）：用户数据报协议

八个字节的头

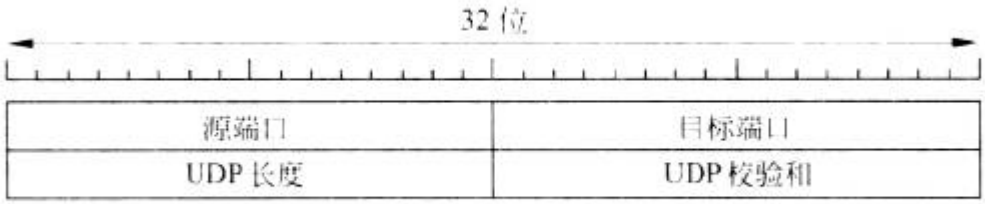

图 6-27　UDP 头格式

UDP 校验和包括了 IPV4 伪头。

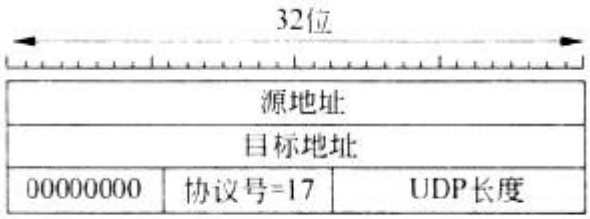

图 6-28　UDP 校验和包括了 IPv4 伪头

RPC （remote procedure call 远程过程调用）

其实就像调用函数一样，通过一个存根，客户过程按照普通过程调用的方式来调用客户存根。

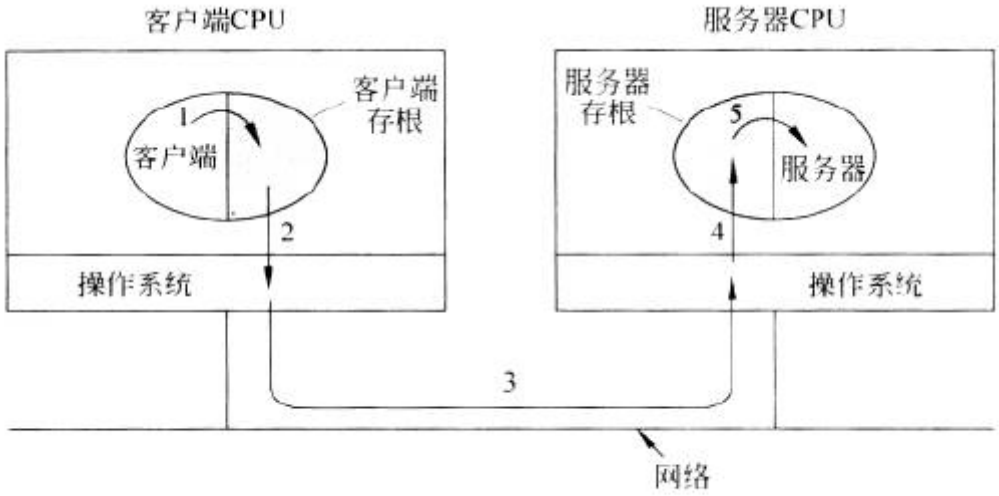

图 6-29　远程过程调用的步骤（阴影部分表示存根）

RTP （real-time transport protocol ） 实时传输协议。

专门对多媒体制定的通用的协议。

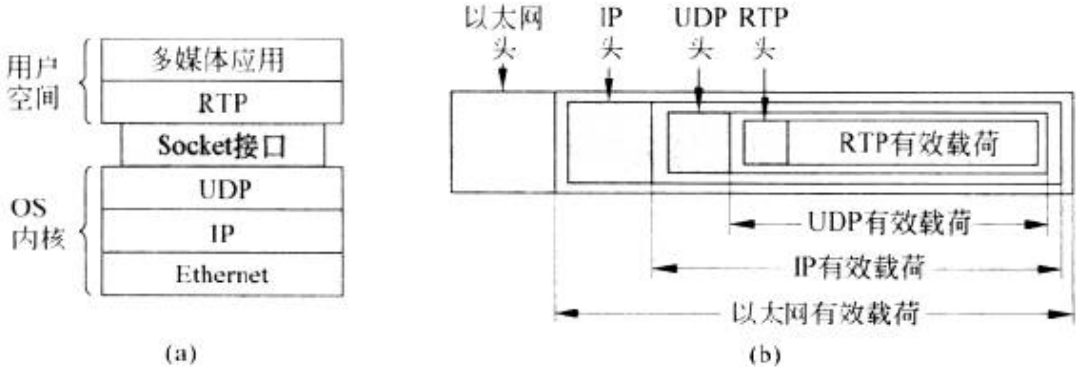

图　6-30

（a）RTP 在协议栈中的位置；（b）数据包的嵌套

RTCP： 实时传输控制协议 ：

不传输任何媒体样值，能处理反馈，同步和用户接口的信息

（上面几乎是建立在 UDP 之间的）

TCP：传输控制协议 为了建立在不可靠的互联网上提出的。

支持 TCP 的机器都有 **TCP 传输实体**（可以是一个库过程，一个用户进程或内核的一部分）管理 TCP 流，和 IP 层之间的接口。其接受本地的数据流并分割成 64kB(去掉 IP 及 TCP 的头不超过 1460 数据字节。)

TCP 服务由发送端和接收端创建一种**套接字**的端点来获得。

TCP 有个 push 标志，标记后立即发送不缓存。

****TCP 在内的每个段要适合 IP 的有效载荷（65535KB），然而还要适合 MTU（最大传输单元），这是由以太网限制的 通常是 1500KB。

TCP 段的头格式：

65536KB-20KB　固定的头也是 20KB （一行 4B）

图 6-36　TCP 头格式.

确认号是期望的下一个序列。

ACK 为 1 表明确认号字段有效。，为 0 则不包含确认信息

ECE：给发送端发送一个 ECN-echo 信号 让其放慢速率

CWR:发送端发送这个信号就表明知道了，这样接收端就不用发 ECE 了

URG：紧急指针，发送端用最少的方式发送数据。

PSH：立即发送

RST：重置混乱连接，收到就表明你的主机有问题了。

SYN=1 ACK=0 连接请求

SYN=1 ACK=1 连接确认

FIN 释放一个连接。

选项里面的

时间戳->

SACK ：选择确认，之后，发送端可以明显地感知到接收端已经有什么数据。

TCP 计时器（三种 分别是 重传 持续 保活 计时器）

重传计时器 RTO（Retransmission TimeOut） 最重要。

发送数据时，启动一个计数器，如何停止之前没有收到确认则重传。 至于时间用一个动态算法。如下：

TCP 维护一个变量 SRTT：Smooth Round-Trip-Time 平滑往返时间。

SRTT=a SRTT + (1-a) R　典型 a=7/8　R 为某次的时间

这样就得到了 最佳计时器的时间。但是对于重传超时仍然不好。

往返时间变化 RTTVAR=p RTTVAR + (1-p)|SRTT-R|　　p=3/4

(RTTVAR 并不确切地等于标准方差**)**

重传超时值　RTO=SRTT+4*RTTVAR　(4 几乎可以认为是随意选的，但也有道理**)**

持续计时器：

接收端告诉发送端满了不要传了（告诉其窗口大小为 0），那么双方就等待，但是 发送方等不及了（持续计数器到了）就去询问，然后接收端告诉结果。这样发送端就决定是重置计数器还是开始传。

保活计数器：有的实现了，也就是长时间连接空闲，则询问，没反应就停止。

还有一个计时器是用于连接停止的时候用的。

TCP 拥塞控制 关键功能

拥塞窗口

把丢包当做信号。 窗口的大小为发送端可以往网络发送的字节数，响应速率则为窗口大小除以连接往返的大小。也是根据 AIMD 来调整窗口的大小。

慢速启动： 为了防止其增长过快，有个慢速启动阀值。发生超时后，就将阀值设置为拥塞窗口的一半。

TCP Tahoe 慢速启动过程

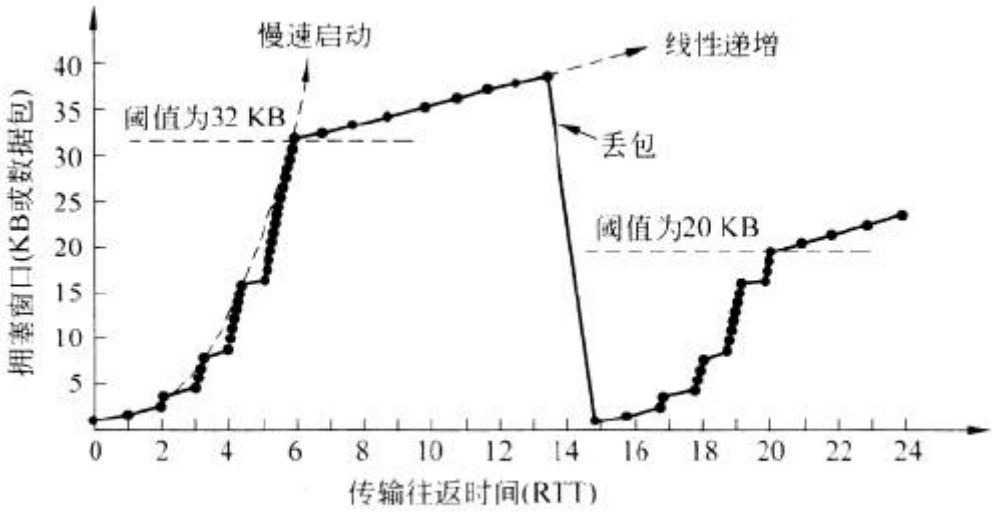

图 6-46 TCP Tahoe 的慢速启动后面接着线性递增

改进基本达到了 AIMD

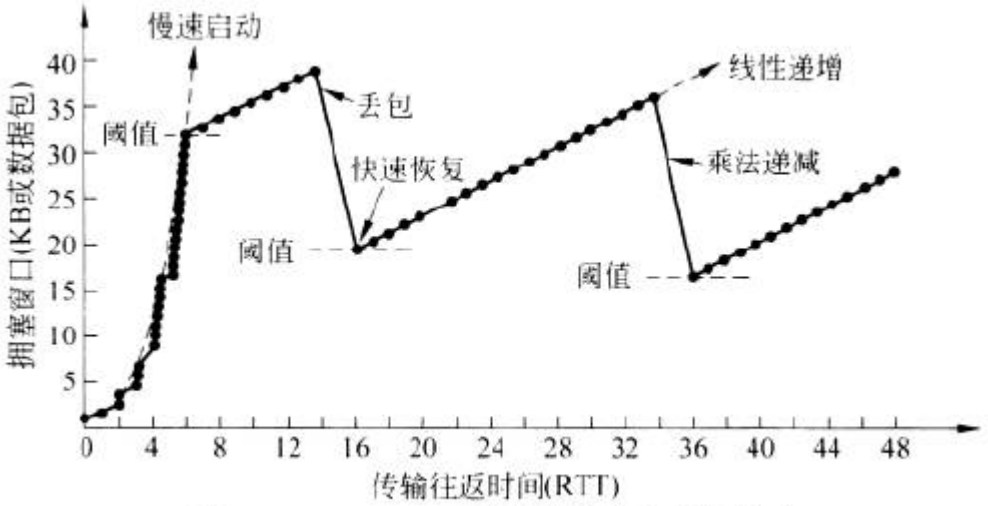

图 6-47 TCP Reno 的快速恢复和锯齿模式

重复确认：丢包后，估计接收端会把后面的序号改成一样的，这样接收端就明白了（自己的理解）

SACK（Selective ACKnowledgement 选择确认 ）：

从一个重复流中推断出 已经到达饱和 和已经丢失的数据包。

起因：TCP 重传时会把原先已经正确传送的包夜重复传送。

工作过程：

1. 建立连接的时候就要发送允许 SACK，这样才能启用 SACK。（有 SYN 标志的前两个包）
2. 正常情况下使用 TCP 的确认号字段。
3. 触发是由接收方引起，里面尽可能告诉有哪些范围被收到。这样发送发就只用发送没有收到的那个包。 （几段范围）

除了丢包走位拥塞信号外，也可以用 ECN（本是 IP 的机制用来通知主机的，因为有 ECE,CWR 标志 ）如果使用 ECN 每个携带 TCP 段的数据包在 IP 头上打标记，以表明可以携带 ECN 信号。

附 课外知识

以太网:局域网.

互联网:广域网

还有一种叫城域网:介与以上两种网络之间的网络.常用于城市间的网络.

以太网：就是物理连接起来的局域网，通过线吧各个主机连在一起。

以太网一般使用同轴电缆和特种双绞线。最通常的以太网系统是 10BASE-T，它的传输速率可达 10 Mbps。

802.3：

连接在电缆上的设备争用线路、冲突采用 CSMA/CD 协议控制。以太网是当今现有局域网采用的最通用的通信协议标准。该标准定义了在局域网（LAN）中采用的电缆类型和信号处理方法。

Internet(互联网)：

是一个网络之上的网络。它具有这样的能力：将各种各样的网络联接起来，而不论其规模、数量、地理位置。同时，把网络互联起来，也就把网络上的资源组合了起来，这当然比独个网络的价值要高出许多。**因此，Internet 的实质是物理网络和信息资源相结合形成的一个信息网络实体。**

TCP/IP 是多台相同或不同类型计算机进行信息交换的一套通信协议。

internet 协议族 TCP/IP 还包含了与这两个协议有关的其它协议及网络应用，如用户数据报协议（UDP）、地址转化协议（ARP）和互连网控制报文协议（ICMP）。由于 TCP/IP 是 internet 采用的协议组，所以将 TCP/IP 体系结构称作 internet 体系结构。

TCP/IP 是世界上最大的 Internet 采用的协议组，而 TCP/IP 底层物理网络多数使用以太网协议，因此，以太网+TCP/IP 成为 IT 行业中应用最普遍的技术。

实际上 TCP/IP 技术支持各种局域网络协议，包括：令牌总线、令牌环、FDDI（光纤分布式数据接口）、SLIP（串行线路 IP）、PPP（点到点协议）、X2.5 数据网等。

IP：网络之间互连的协议（IP）是 Internet Protocol

NAT:解决私有网络访问公邮网络。 宿舍联网问题。

词汇缩写

ARP

地址解析协议（Address Resolution Protocol），是根据 IP 地址获取物理地址的一个 TCP/IP 协议。

UTP

非屏蔽双绞线（UTP)和屏蔽双绞线(STP)两大类

CSMA/CD

（Carrier Sense Multiple Access with Collision Detection）即带冲突检测的载波监听多路访问技术。