计网复习

1. ISO 提出的七层 OSI 网络体系结构模型：物理层（比特流）、数据链路层（帧）、网络层（分组）、运输层（TPDU：TCP 用报文段，UDP 用用户数据报）、会话层（SPDU）、表示层（PPDU）、应用层（APDU）
   五层模型将会话层、表示层并入应用层，TCP/IP 模型再将物理层和数据链路层合并为网络接口层

2. 物理层通过频分、时分（可能有浪费）、统计时分、波分（光的频分）、码分复用（码分多址 CDMA 产生伪随机码序列）解决复用问题

3. 数据链路层（可靠/不可靠）
   （1） 分为点对点信道（PPP 帧，有首尾）和广播信道（MAC 帧，有首尾）
   （2） 错误检验：循环冗余检验（CRC），用于 PPP 帧和 MAC 帧的帧检验序列 FCS 中
   （3） 点对点信道的 PPP 协议由封装成 PPP 帧、链路控制协议 LCP、网络控制协议 NCP 构成，全双工通信
   （4） 广播信道由局域网实现，其中 IEEE802.3 的以太网占据了局域网的绝大市场，成为其代名词
      A. 以太网下数据链路层被分为逻辑链路控制层（LLC，已弃用）和媒体接入控制层（MAC）
      B. 以太网下半双工通信通过载波监听多点接入/碰撞检测协议（CSMA/CD）和载波监听多点接入/碰撞避免协议（CSMA/CA，解决站点隐藏）实现，其中碰撞后采用截断二进制指数退避方式确定重传时机
      C. 计算机通过网络适配器（网卡）实现与外界网络的连接
      D. 以太网的扩展：
         物理层：集线器/转发器（不合并碰撞域）
         数据链路层：网桥，细分为透明网桥（生成树算法，常用）、源路由网桥、以太网交换机（多接口网桥，全双工，用于实现虚拟局域网 VLAN，VLAN 间的通信需要通过网络层的路由器实现）
   （5） 可靠性保证：自动重传请求 ARQ
      分为停等 AQR、回退 NAQR、选择重传 ARQ，其中后两者合称连续 ARQ
      A. 停等 ARQ：发送一个分组后等待对方返回的确认，没有则超时重传
      B. 回退 NARQ：发送窗口大小为 N，接收窗口大小为 1，发生错误或乱序重传错误帧及其之后已发送的帧
      C. 选择重传 ARQ：发送接收窗口大小均大于 1，只重传错误或乱序帧

4. 网络层（不可靠，主机间通信）
   （1） 在虚电路服务（面向连接，可靠）和数据报服务（无连接，不可靠）中选择后者
   （2） 由四部分组成：网际协议 IP 及其配套协议、路由选择协议和多播相关协议、VPN 相关
   （3） 网际协议 IP
      A. 核心问题：寻径

B. 配套使用协议：地址解析协议（ARP，被 IP 协议调用）、网际控制报文协议（ICMP，调用 IP 协议）、网际组管理协议（IGMP，调用 IP 协议）
C. IP 数据报：有首无尾，校验和是首部校验和（反码加和检验，路由器负责），最大字节数=65535-60
D. 解决 IP 地址不足：划分子网（子网掩码）、构造超网（CIDR 前缀，如 1.2.3.4/16）、IPV6
E. 地址解析协议（ARP）：从 IP 地址获得硬件地址，若目标主机不在当前网络则获得相应路由器的硬件地址
F. 网际控制报文协议（ICMP）：主机或路由器向高级报告异常，通过 IP 报文传输，分为差错报告报文和询问报文，前者的结构是首部+错误 IP 数据报首部以及前八个字节（为了得到运输层的端口号和发送序号）。如 ping 是应用层直接调用网络层 ICMP 的例子
G. 网际组管理协议（IGMP）：见多播相关协议

（4） 路由选择协议
A. 分类 :内部网关协议 IGP（含 RIP 和 OSPF）和外部网关协议 EGP（含 BGP），均支持 CIDR，仅 RIPv1 不支持。这里 IGP\EGP 仅是分类而不是具体协议
B. 路由信息协议 RIP：分布式且基于距离向量，每隔固定时间通过 UDP 传输和相邻路由器交换全部信息，维持 15 跳，简单开销小，适用于规模小的网络，但坏消息传播得慢（收敛慢），只找最短路径而不考虑流量负载
C. 开放最短路径优先 OSPF：分布式且基于链路状态，链路状态改变时通过 IP 数据报传输和全部路由器交换自己相邻路由器信息，采用洪泛法，复杂，适用于规模大的网络，收敛快，多条最短路径时考虑负载平衡
D. 边界网关协议 BGP：基于路径向量，通过 TCP 传输和相邻边界路由器交换信息（通过什么网络到达什么自治系统）

（5） 多播相关协议
A. 分类：网际组管理协议 IGMP（本地局域网）和多播路由选择协议（局域网间）
B. 网际组管理协议 IGMP：周期性询问本地局域网组成员是否活跃
C. 多播路由选择协议：三种方法：洪泛与减除（较小的多播组）、隧道技术（地理位置分散的多播组）、基于核心的发现技术（大小变化剧烈的多播组）

（6） VPN 相关：
A. 虚拟专用网 VPN：专用/可重用 IP 地址用于构建一个集体的专用 VPN
B. 网络地址转换 NAT：将本机的虚拟专用网 IP 通过 NAT 路由器转换为全球 IP

5. 运输层（TCP 可靠 UDP 不可靠，进程间通信（通过端口））

（1） 用户数据报协议 UDP
A. 无连接，不可靠，面向报文、对下层报文不拆分不合并，没有拥塞控制，首部开销小（8 字节），支持 M 对 N 通信
B. UDP 传输单元：用户数据报，伪首部 12 字节，首部 8 字节，计算校验和（反码求和）时算上伪首部，有错就丢弃
C. 用例：网际组管理协议 IGMP、路由信息协议 RIP、域名系统 DNS、网络文件系统 NFS、简单文件传输协议 TFTP

（2） 传输控制协议 TCP

A. 面向连接（虚连接），可靠，面向（无结构的）字节流，只能是点对点通信（其端点叫做套接字 socket），全双工，根据窗口值和网络拥塞进行传输

B. TCP 传输单元：报文段，首部 20 固定字节，计算校验和（反码求和）时也算上伪首部

C. 用例：简单邮件传送协议 SMTP、超文本传送协议 HTTP、文件传输协议 FTP、远程终端协议 TELENT

D. 相关协议 :可靠保证（确认应答 ACK, 超时重传）、流量控制（滑动窗口）、拥塞控制（慢开始+拥塞避免+快重传+快恢复或随机早期检测 RED）、连接建立与取消（三次握手四次挥手）

E. 确认应答 ACK：TCP 帧里的 ACK 标志位，置为 1 时确认号有效
选择确认 SACK：在可选项中增加 SACK 选项，类似选择重传 ARQ

F. 滑动窗口协议：接收方返回"ACK=1,ack=确认字段值,rwnd=允许再发送的字节数"，其分类与 ARQ 相同

G. 慢开始+拥塞避免+快重传+快恢复

a. 慢开始：发送窗口由 1 个最大报文段 MSS 开始，每经过一个传输轮次大小加倍，呈指数型增长

b. 拥塞避免：发送窗口大小到达慢开始门限后，每经过一个传输轮次大小+1MSS，呈线型增长

c. 快重传：接收方接收到失序报文段后（此时认为网络拥塞），重复发送上一个正常确认的报文段 ACK，令发送方尽早重传失序报文段

d. 快恢复：接收方接收到失序报文段、网络拥塞后，慢开始门限=现在的发送窗口=拥塞时的发送窗口/2，之后执行拥塞避免算法

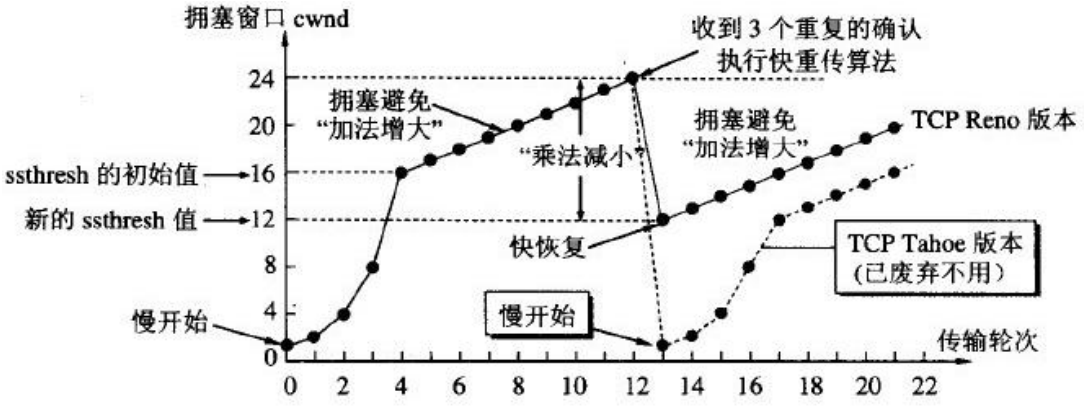


图 5-27 从连续收到三个重复的确认转入拥塞避免

H. 随机早期检测 RED：为避免发生网路中的**全局同步**现象（许多的 TCP 连接在同一时间进入慢开始状态，网络恢复正常之后，其通信量又突然增大很多），RED 维持队列最小门限 min 和最大门限 max，每当一个分组到达的时候根据概率 p 将其丢弃

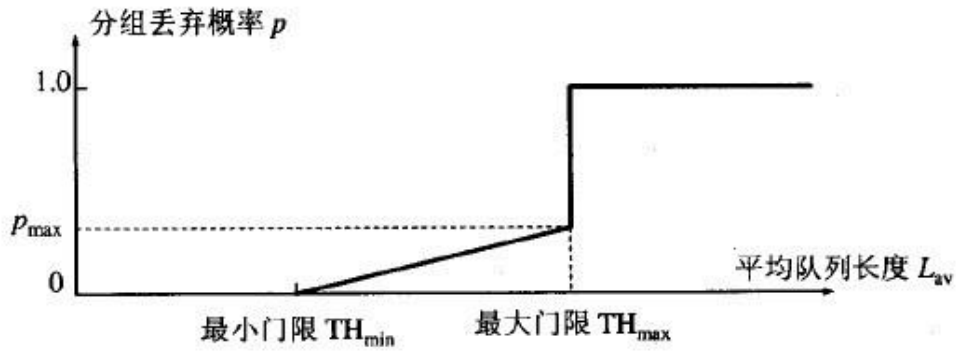
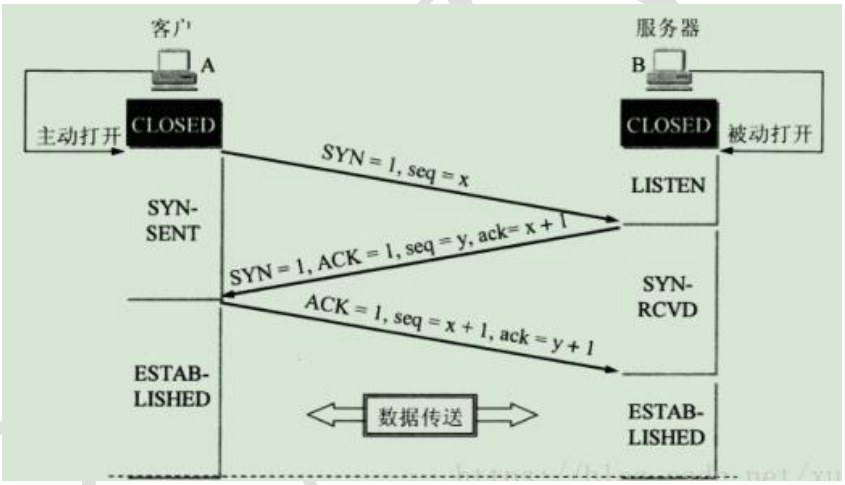
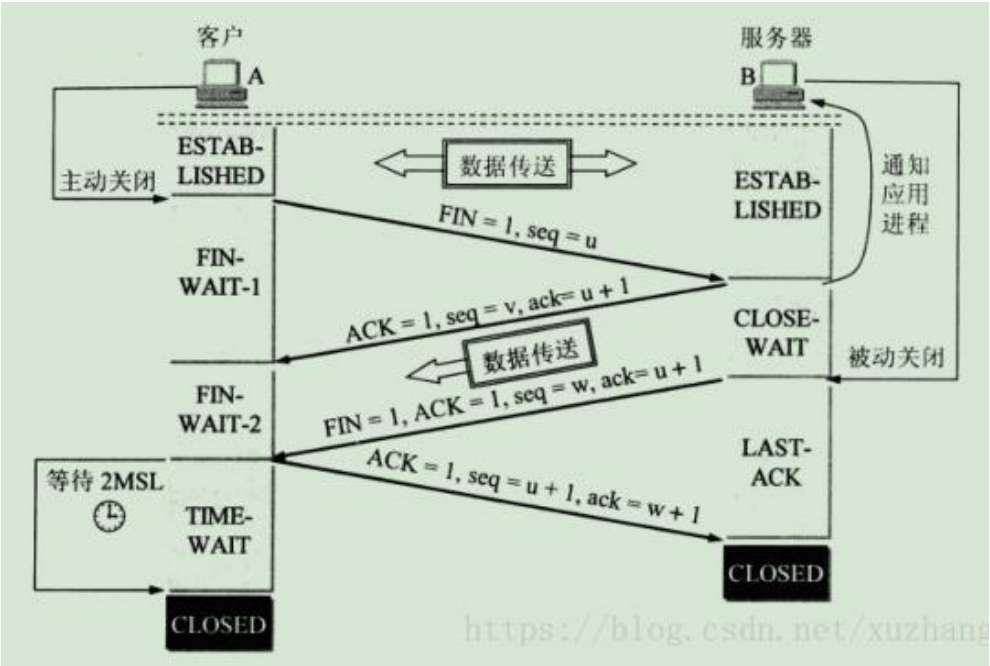


图 5-29　分组丢弃概率 p 与两个门限值 TH_{min} 和 TH_{max} 的关系

I. 三次握手
   a. 三次握手中仅第三次握手能携带数据（SYN=1 的报文段不能携带数据）
   b. 第三次握手的必要性：
      a) 避免已失效的连接请求报文段突然传给服务器
      b) 避免客户只发送一次连接请求报文段后直接关机



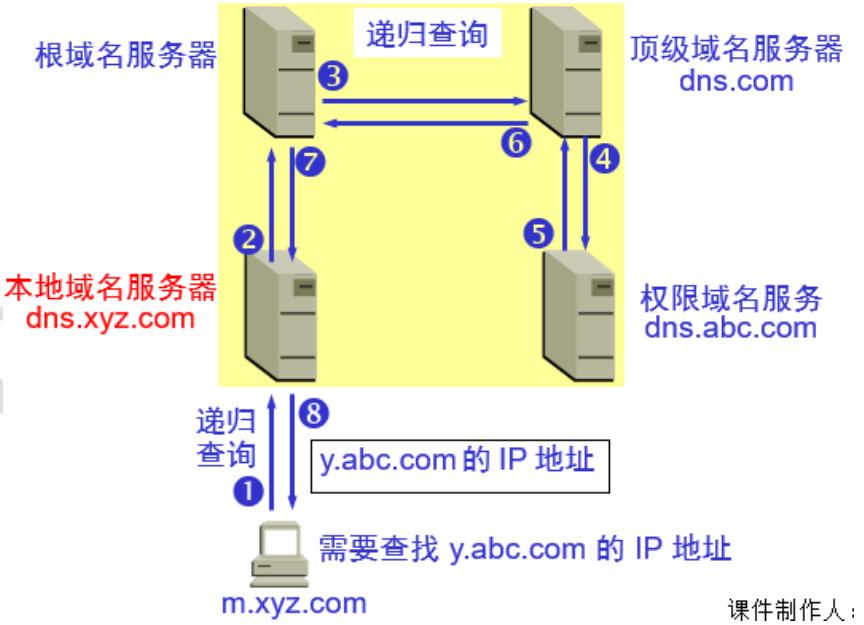
J. 四次挥手
   a. 四次挥手中仅第四次挥手不能携带数据
   b. 等待 2MSL（最长报文段寿命）的必要性：
      a) 若第四次挥手报文段丢失，确保客户能接收到服务器超时重传的 FIN=1 报文段，以便客户重传第四次挥手报文段
      b) 确保此时网络中二者联系的所有报文段失效，方便下次建立连接



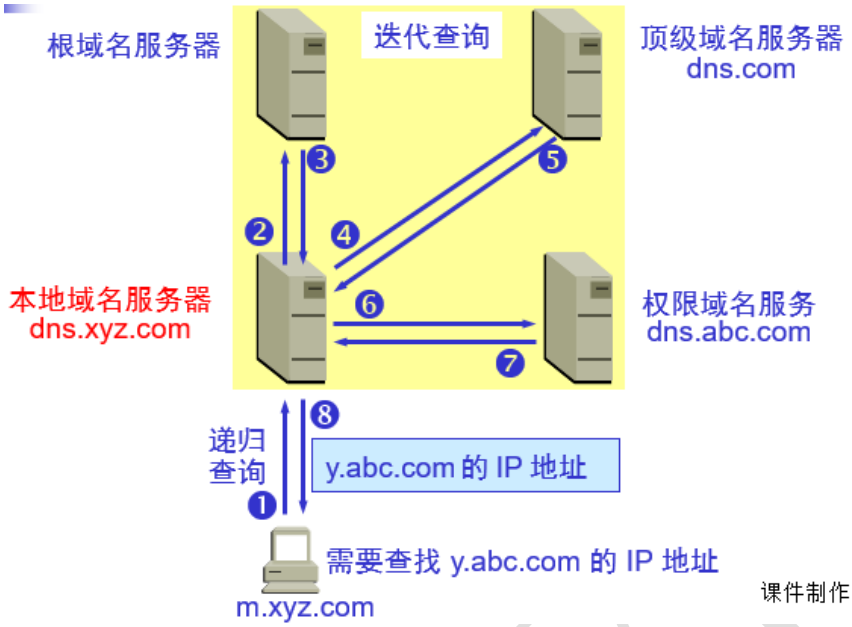
6. 应用层（可靠）

（1） 域名系统 DNS：将域名地址转换为 IP 地址，UDP 传输（减小开销）

A. 递归查询：主机向本地域名服务器查询



B. 迭代查询：本地域名服务器向根域名服务器查询（常用）



(2) 几个文件传送协议

A. 文件传送协议 FTP：TCP 可靠传输，C/S 模式，之间建立两个并行 TCP 连接：控制连接（一直开启）数据连接（传输数据）

B. 网络文件系统 NFS：UDP 传输，C/S 模式，传输少量的修改数据

C. 简单文件传送协议 TFTP：UDP 传输，C/S 模式，内存小易实现，类似停等模式，只传输数据而不交互

(3) 万维网 WWW 相关

A. 分布式超媒体系统，C/S 模式，客户端程序是浏览器

B. 统一资源定位符 URL、超文本传送协议 HTTP（面向事务，TCP 可靠传输，本身无连接、无状态）、超文本标记语言 HTML

C. HTTP 的长连接与短连接

HTTP 的长连接和短连接本质上是 **TCP** 长连接和短连接。

a. 短连接：HTTP/1.0 中默认使用，客户端和服务器每进行一次 HTTP 操作，就建立一次连接，任务结束就中断连接。当客户端浏览器访问的 Web 页中包含有其他的 Web 资源（如 JavaScript 文件、图像文件、CSS 文件等），每遇到这样一个 Web 资源，浏览器就会重新建立一个 HTTP 会话。

优点是管理简单，**常用于 web 网站的 http 服务**

b. 长连接：HTTP/1.1 中默认使用，当一个网页打开完成后，客户端和服务器之间用于传输 HTTP 数据的 TCP 连接在一段可设定的保持时间内不会关闭，客户端再次访问这个服务器时，会继续使用这一条已经建立的连接。

优点是省去较多的 TCP 建立和关闭的操作，减少浪费，节约时间，但客户端过多可能导致服务器崩溃，**常用于操作频繁、点对点且连接数不多通讯**

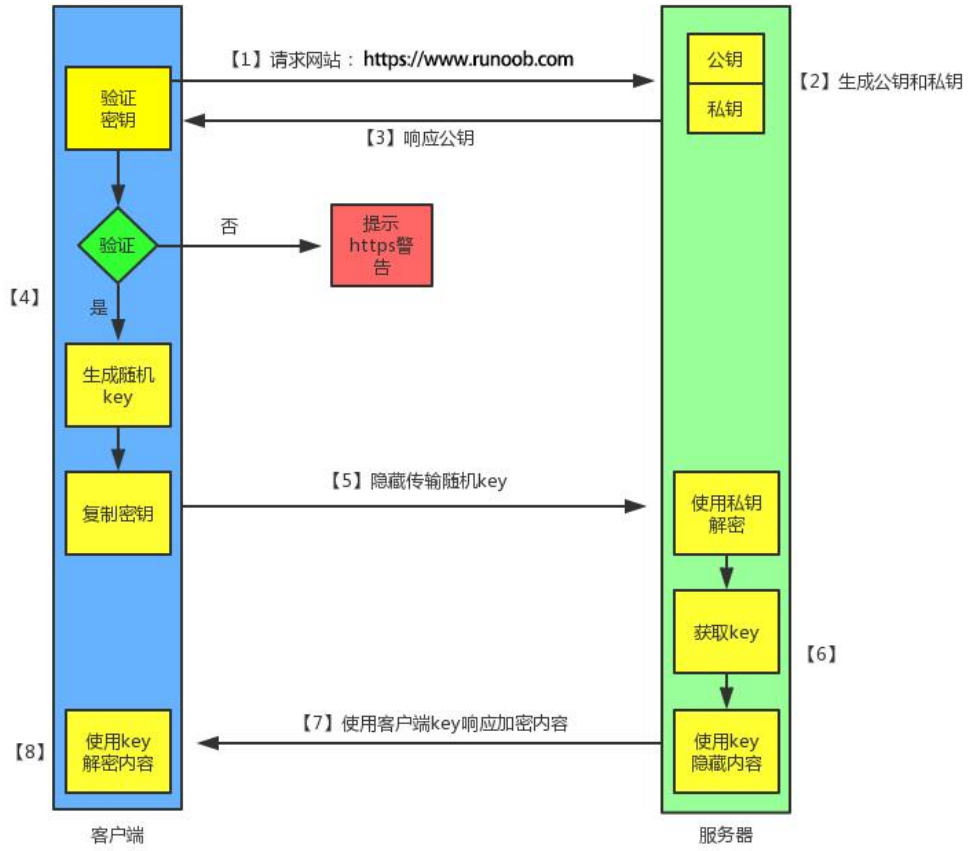
D. HTTP 和 HTTPS 的区别

a. 加密：http 明文传输，不提供任何方式的数据加密，不适合传输一些敏感信息比如银行卡号，https 可以通过 SSL 进行加密传输

b. 端口：http 默认 80 端口，https 默认 443 端口

c. 响应速度：http 较快（主要是 TCP 三次握手的包），https（还要加上 SSL 握手的 9 个包）较慢

d. HTTPS 加密流程：



（4） 电子邮件相关协议（C/S 架构，TCP 传输）

A. 分类 :发送协议（简单邮件传送协议 SMTP、通用因特网邮件扩充 MIME）和接收协议（邮局协议 POP3、网际报文存取协议 IMAP）

B. 简单邮件传送协议 SMTP：只能传输 7 位的 ASCII 码

C. 通用因特网邮件扩充 MIME：SMTP 的扩充，可传输各种文件

D. 邮局协议 POP3：邮件一旦被取走，服务器删除原邮件

E. 网际报文存取协议 IMAP：邮件只存储在服务器上，每次读取邮件需要和服务器建立连接