思维导图

【金山文档】 第1章 概述（思维导图）
https://kdocs.cn/l/cqzI95zH7t6v

【金山文档】 第3章 数据链路层（思维导图）-1
https://kdocs.cn/l/cgV0rfS0qZEA

【金山文档】 第3章 数据链路层（思维导图）-2
https://kdocs.cn/l/ciOEeLV6ffuJ

【金山文档】 第3章 数据链路层（思维导图）-3
https://kdocs.cn/l/cnRBS8NFgTll

【金山文档】 第4章 网络层（思维导图）-1
https://kdocs.cn/l/ceLxGZ0br8Gy

【金山文档】 第4章 网络层（思维导图）-2
https://kdocs.cn/l/cu2tek1gzIPq

【金山文档】 第4章 网络层（思维导图）-3
https://kdocs.cn/l/cjXVALCjxr0X

【金山文档】 第4章 网络层（思维导图）-4
https://kdocs.cn/l/cbSlBNdR8CSr

【金山文档】 第5章 运输层（思维导图）-1
https://kdocs.cn/l/cgoja6Lpohhj

【金山文档】 第5章 运输层（思维导图）-2
https://kdocs.cn/l/chkSS9vn9Zgd

【金山文档】 第6章 应用层（思维导图）-1
https://kdocs.cn/l/cle5dxMBHZIH

【金山文档】 第6章 应用层（思维导图）-2
https://kdocs.cn/l/cabHsokbKiNO

GBN与SR异同

GBN（Go-Back-N）和SR（Selective Repeat）是两种数据链路层的协议，都是基于停等协议的改进，用于解决数据传输中的可靠性和流量控制问题。它们的共同点和不同点如下：

共同点：

1. GBN和SR都使用滑动窗口协议，通过在发送方和接收方之间建立窗口来控制数据包的流量。
2. 两种协议都支持可靠数据传输，即发送方发送的数据会等待接收方确认收到，直到收到确认消息后再发送下一个数据包。
3. 两种协议都可以在不丢失数据的情况下，对传输速率进行控制，以避免网络拥塞。

不同点：

1. GBN协议在发送方发送了一个窗口内的数据包后，只等待接收方对窗口中的第一个数据包进行确认，一旦接收方确认了第一个数据包，发送方会向前滑动窗口，并继续发送下一个窗口的数据包。而SR协议允许接收方对窗口中的任何数据包进行确认，只要它们按顺序到达。
2. GBN协议不支持乱序数据包的接收。如果接收方收到了一个失序的数据包，它将忽略该数据包，直到收到正确的数据包为止。而SR协议支持乱序数据包的接收，接收方可以缓存失序的数据包，并在接收到缺失的数据包时发送选择性重传请求。
3. GBN协议中，每个数据包只能被发送一次，如果发送方发送的数据包在一个超时时间内没有得到接收方的确认，发送方将重传整个窗口内的数据包。而SR协议中，如果接收方收到了一个数据包，但发送方没有收到确认消息，发送方只需要重新发送这个数据包，而不需要重传整个窗口。

总之，GBN协议和SR协议都是可靠的数据传输协议，但它们在窗口管理、数据包丢失处理和重传机制方面存在一些不同。具体应该根据不同的实际应用场景，选择适合的协议。

表 5-2　3 种可靠数据传输协议发送窗口和接收窗口值的比较

可靠数据传输协议	发送窗口值 W_T	接收窗口值 W_R
停-等协议	$W_T=1$	$W_R=1$
回退 N 协议	大于 1，$W_T \leqslant 2^K-1$	1
选择重传协议	大于 1，$W_T \leqslant 2^K/2$，$W_T \leqslant 2^K-W_R$	大于 1，$W_R \leqslant 2^K/2$，$W_R \leqslant 2^K-W_T$

DNS解析过程

域名系统（DNS）是一个分布式的、层次化的系统，包括根域名、顶级域名、权限/权威

当用户在浏览器中输入 www.hdu.edu.cn，以下是域名解析的一般过程：

1. 用户的计算机向本地DNS服务器（也称递归DNS服务器）发出DNS查询请求。本地DNS服务器通常由互联网服务提供商（ISP）提供，并由用户计算机的网络设置自动配置。
2. 如果本地DNS服务器的缓存中已经有了该域名的DNS记录，它将直接返回IP地址，并跳过后续的查询流程。否则，本地DNS服务器将向根域名服务器发送一个DNS查询请求，询问哪个顶级域名服务器负责管理 .cn 域名。
3. 根域名服务器返回响应，提供一个 .cn 顶级域名服务器的IP地址。
4. 本地DNS服务器向 .cn 顶级域名服务器发出DNS查询请求，询问哪个权威域名服务器负责管理 hdu.edu.cn 域名。
5. .cn 顶级域名服务器返回响应，提供 hdu.edu.cn 域名的权威域名服务器的IP地址。
6. 本地DNS服务器向 hdu.edu.cn 的权威域名服务器发出DNS查询请求，询问 www.hdu.edu.cn 的IP地址。
7. hdu.edu.cn 的权威域名服务器返回响应，提供 www.hdu.edu.cn 的IP地址。
8. 本地DNS服务器将 www.hdu.edu.cn 的IP地址返回给用户的计算机，并将该DNS记录存储在缓存中，以备下次查询使用。
9. 用户的计算机使用该IP地址建立到 www.hdu.edu.cn 网站的连接，以加载网页。

TCP拥塞控制

慢开始： **CongWin** < **Threshold**, **CongWin** 指数增长.

拥塞避免：**CongWin** > **Threshold**, **CongWin** 线性增长.

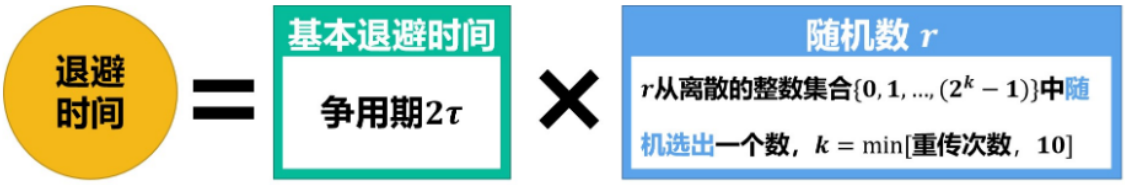
快重传：3个冗余ACK，立即重传

快恢复：3个冗余ACK, **Threshold** 设为**CongWin/2**，**CongWin**设为**Threshold+3MSS**.

超时处理： timeout事件, **Threshold**设为**CongWin/2**, **CongWin**设为1MMS大小.

退避算法

- 在使用CSMA/CD协议的共享总线以太网中，正在发送帧的站点一边发送帧一边检测碰撞，当检测到碰撞时就立即停止发送，退避一段随机时间后再重新发送。
- 共享总线以太网中的各站点采用截断二进制指数退避（Truncated Binary Exponential Backoff）算法来选择退避的随机时间。



重传次数	k	离散的整数集合$\{0, 1, ..., (2^k-1)\}$	可能的退避时间
1	1	$\{0，1\}$	$0\times2\tau$，$1\times2\tau$
2	2	$\{0，1，2，3\}$	$0\times2\tau$，$1\times2\tau$，$2\times2\tau$，$3\times2\tau$
12	10	$\{0，1，2，3，4，5，\ldots，1023\}$	$0\times2\tau$，$1\times2\tau$，$2\times2\tau$，$\ldots$，$1023\times2\tau$

- 如果连续多次发送碰撞，就表明可能有较多的站点参与竞争信道。但使用上述退避算法可使重传需要推迟的平均时间随重传次数而增大（即动态退避），因而减小产生碰撞的概率。
- 当重传达16次仍不能成功时，就表明同时打算发送帧的站点太多，以至于连续产生碰撞，此时应放弃重传并向高层报告。

常见端口号

1. HTTP (HyperText Transfer Protocol)：80
2. HTTPS (HTTP Secure)：443
3. FTP (File Transfer Protocol)：20 (数据)、21 (控制)
4. SMTP (Simple Mail Transfer Protocol)：25
5. DNS (Domain Name System)：53
6. DHCP (Dynamic Host Configuration Protocol)：67 (服务器)、68 (客户端)
7. POP3 (Post Office Protocol version 3)：110
8. RIP (Routing Information Protocol)：520
9. BGP (Border Gateway Protocol)：179
10. IMAP (Internet Message Access Protocol)：143

UDP复用（IP协议字段17）：DNS、DHCP、RIP

TCP复用（IP协议字段6）：HTTPS、HTTP、FTP、SMTP、BGP

OSPF直接封装为IP数据报，协议为89