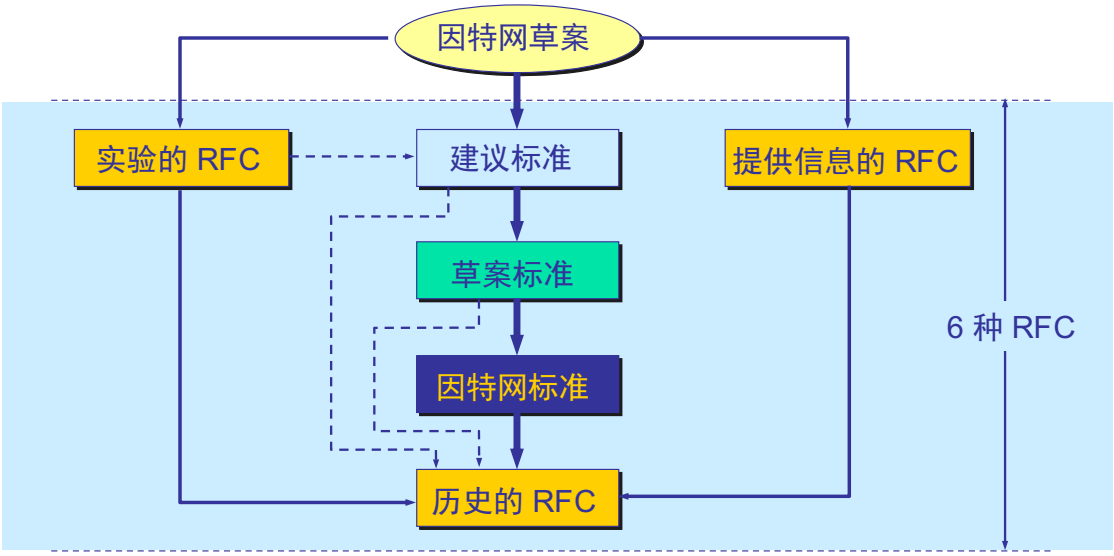
1. 互联网有关协议、标准开发的机构、过程、文档形式及文档命名规则

机构：因特网协会 ISOC - 因特网体系结构研究委员会 IAB

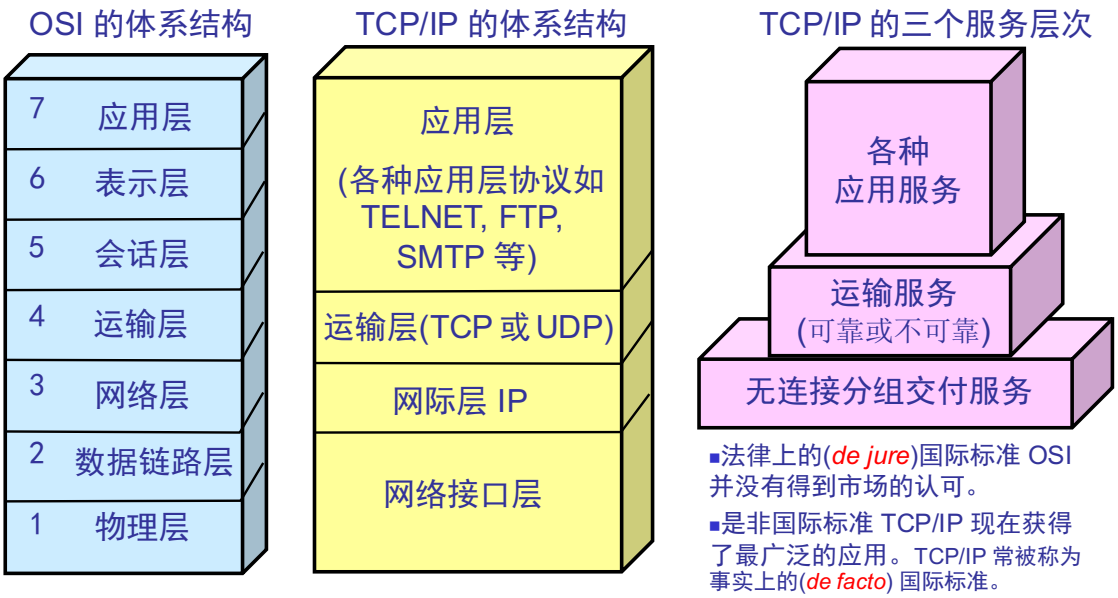
过程：

- 因特网草案(Internet Draft)　*在这个阶段还不是 RFC 文档。*
- 建议标准(Proposed Standard)　*从这个阶段开始就成为RFC 文档。*(RFC xxxx)
- 草案标准(Draft Standard)
- 因特网标准(Internet Standard)　STDxx

文档形式：RFC 请求评论



2. TCP/IP 模型与 OSI 模型各层的名称、对应关系、实现的功能、各层的主要协议及其作用，以及在主机和网络节点中的区别，分层设计的优点



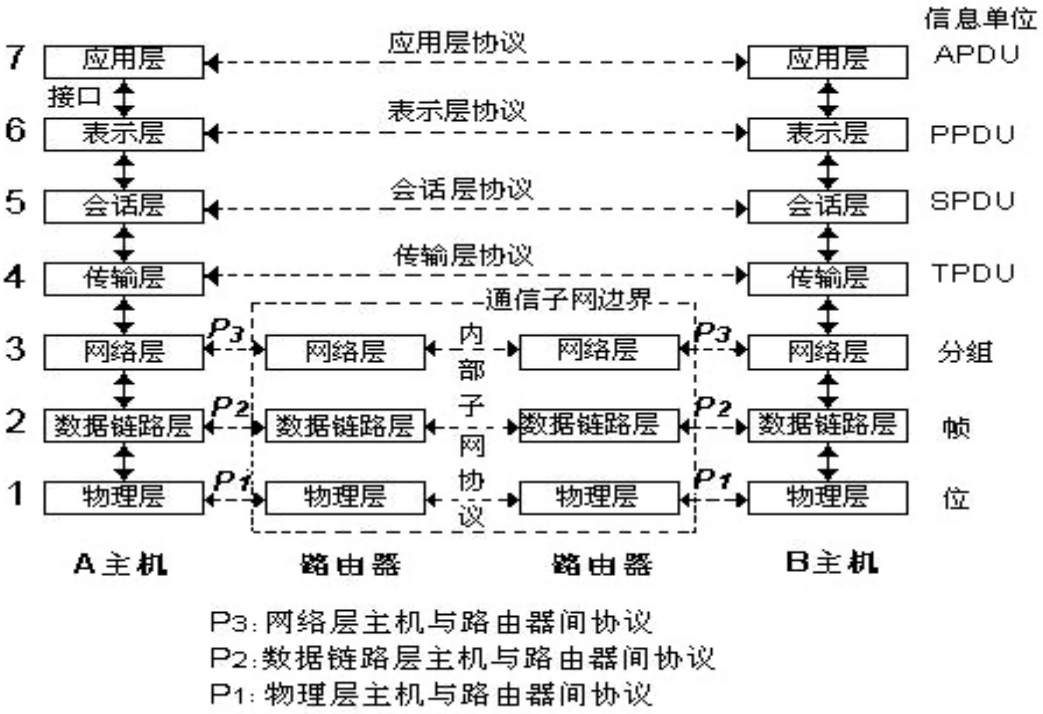
TCP/IP 协议：

- **应用层：**为用户提供访问 Internet 的一组高层协议 (如 FTP、TELNET、SMTP 等)
- **传输层：**为源和目的主机的应用程序间提供端-端的数据传输服务 (如 TCP、UDP)
- **网络互联层（网际层）：**把分组独立地从信源传送到信宿。解决路由选择、

拥塞控制和网络互联等问题 (如 IP)

- **网络接口层**：负责将 IP 分组封装成适合在物理网络上传输的帧格式并传输，或将从物理网络接收到的帧解封，取出 IP 分组交给网络互联层 (如 Ethernet、PPP)

OSI 协议：



- **物理层**：在物理媒体上传输原始的数据比特流。
- **数据链路层**：在相邻节点间无差错地传输一帧数据。
  内容：封装成帧；透明传输；差错监测。
- **网络层**：将分组穿过通信子网从信源传输到信宿。
  内容：路由选择；拥塞控制（实际上是传输层在做）；数据分片和组装；网络互联。
- **传输层**：提供端到端的数据传输服务
  内容：连接管理；报文分割和装配；端到端的差错控制与流量控制；分流和多路复用。
- **会话层**：在两个互相通信的进程之间建立、组织和同步会话、会话活动管理、对话控制。
  内容：会话管理；同步；活动管理
- **表示层**：提供数据或信息语法的表示变换，以确保不同表示方法的计算机能互相通信。
  内容：各机器内部的数据表示与网络传输的抽象数据表示之间的变换；数据的压缩/解压缩；数据的加密/解密
- **应用层**：直接面向用户的一层。它为应用进程提供访问 OSI 环境的手段，同时为应用进程提供服务。对于一些普遍需要的网络应用（如文件传输、电子邮件、域名服务等）制定了一系列标准。

分层设计的优点：

- 各层之间**独立**：只管调用接口，不管下层如何实现。
- **灵活**性好：任何一层变化时，只要接口不变，不影响其它层。

- 结构上是**可分割的**：各个层都可以用最合适的技术来实现
- **易于实现和维护**
- 能**促进标准化**工作：使得每层的服务都有精确说明。

3. 计算机网络面临的主动攻击和被动攻击的定义、类型、DoS/DDoS 攻击的定义、特点

被动攻击（截获）：攻击者从网络上**窃听**他人的通信内容。

攻击者只是观察和分析某一个协议数据单元 PDU，以便了解所交换的数据的某种性质，但不干扰信息流。又称为流量分析。

主动攻击 类型：

- **篡改**：故意篡改网络上传送的报文。也称为更改报文流。
- **恶意程序**：种类繁多，主要包括：计算机病毒、计算机蠕虫、特洛伊木马、逻辑炸弹、后门入侵、流氓软件等。
- **拒绝服务** DoS (Denial of Service)：指攻击者向互联网上的某个服务器不停地发送大量分组，使该服务器无法提供正常服务，甚至完全瘫痪。

分布式拒绝服务 DDoS（网络带宽攻击或连通性攻击）：从互联网上的成百上千的网站集中攻击一个网站。

4. 每个层次数据传输单元的名称、最大值、最小值

层	协议数据单元(PDU)	最小值（字节）	最大值（字节）
物理层	比特	/	/
数据链路层	帧	64	1500+6+6+2+4=1518
网络层	IP 数据报（分组）	20（只有首部）	65535（MTU 限制）
运输层	用户数据报 UDP	8（只有首部）	65535
	TCP 数据段	20（只有首部）	65535（MSS 限制）
应用层	数据	/	/

5. 域名、邮件地址、URL 的区别，以及各自命名或者取值的限制条件

- **域名**：任何一个连接在因特网上的主机或路由器，都有一个**惟一**的层次结构的名字，即**域名**。域名的结构由若干个分量组成，各分量之间用点隔开，各分量分别代表不同级别的域名。

  ….三级域名.二级域名.顶级域名

- **电子邮件**地址的格式：

  用户名@邮箱所在主机的域名

  用户名在**该域名的范围内**是惟一的；邮箱所在的**主机的域名**在**全世界**必须是惟一的。

- **统一资源定位符 URL**：对可以从因特网上得到的资源的位置和访问方法的一种简洁的表示。URL 给资源的位置提供一种抽象的识别方法，并用这种方法给资源定位。

  <URL 访问方式>://<主机>:<端口>/<路径>

  访问方式有：ftp http https mailto 等

  主机：IP 地址或域名

  端口：0~65535（缺省为 80）

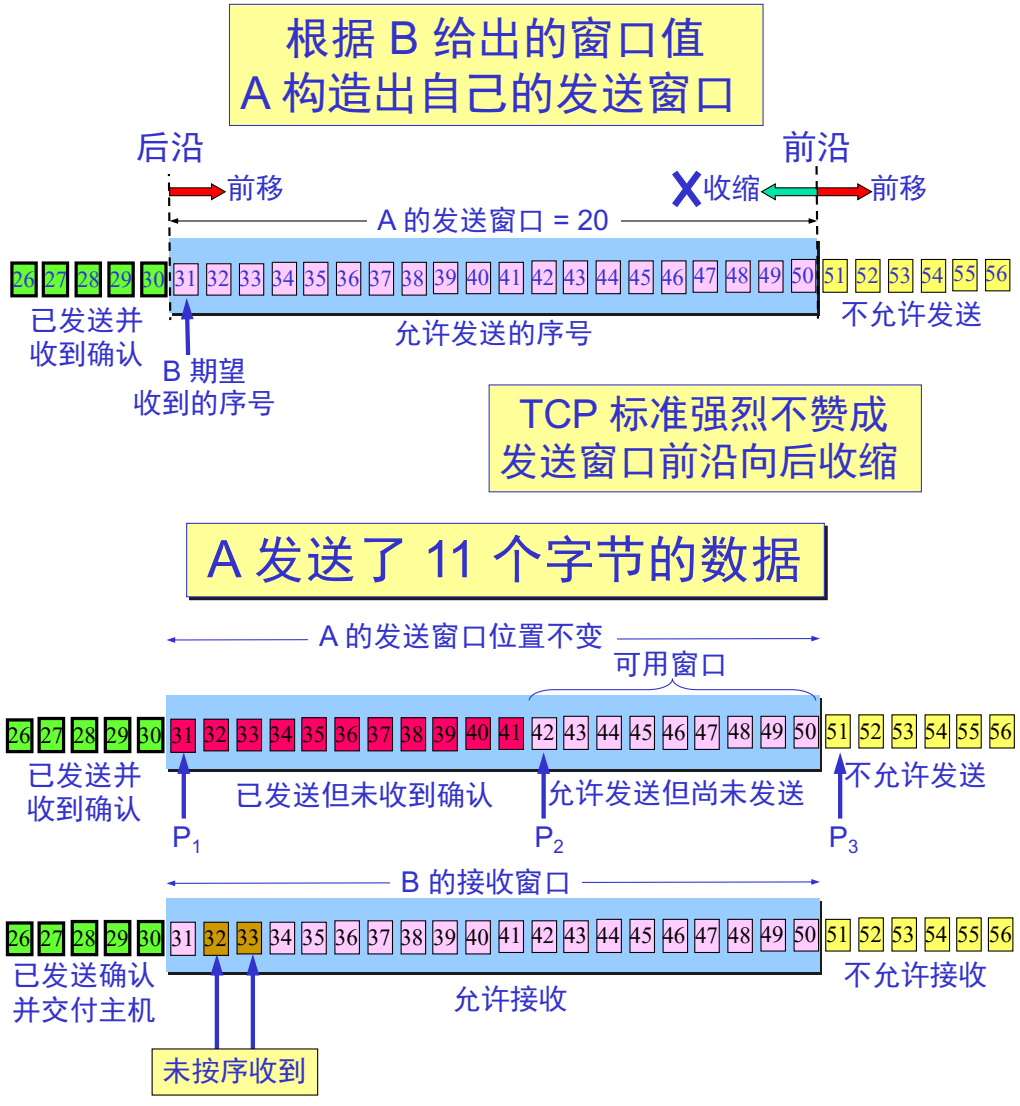
  0~1023 是熟知端口号，1024~69151 为登记端口号，这两类是服务器使用的；其余为短暂端口号，客户端使用。

6. 滑动窗口、ARQ 的定义、原理、特点

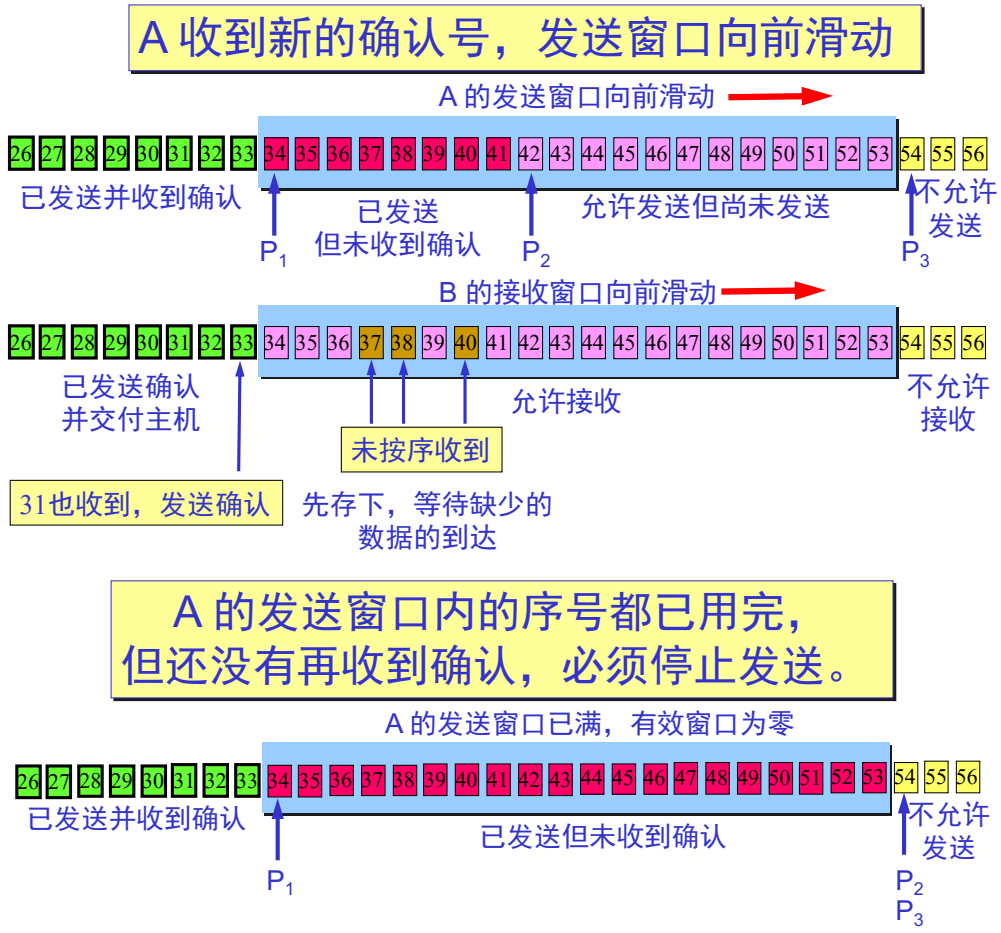
自动重发请求 ARQ：发送方使用检错码，接收方对收到的数据进行检错。接收

方使用应答向发送方进行信息反馈：肯定应答——数据已被正确接收；否定应答——传输有错，重发直至正确接收。为防止帧丢失导致发送方收不到应答，发送方发完一帧后，会启动一个**超时定时器**，定时到仍未收到应答便进行重发。**滑动窗口**：发送方和接收方各自维持着**发送窗口**和**接受窗口**，发送方**每收到一个确认**，就把发送窗口向前滑动一个分组的位置。接收方一般采用**累计确认**方式，即接收方不必对收到的分组逐个发送确认，而是可以在收到几个分组后，对**按序到达**的最后一个分组发送确认，这样就表示：到这个分组位置的所有分组都已经正确收到了。

- TCP 采用**大小可变**的滑动窗口进行流量控制。窗口大小的单位是**字节**。
- 在 TCP 报文段首部窗口字段写入的数值就是当前给对方设置的**发送窗口**数值的**上限**。
- 发送窗口在连接建立时由双方商定。



$P_3 - P_1$ = A 的发送窗口（又称为通知窗口）
$P_2 - P_1$ = 已发送但尚未收到确认的字节数
$P_3 - P_2$ = 允许发送但尚未发送的字节数（又称为可用窗口）



举例：

发送端的主机在确定发送报文段的速率时，既要根据接收端的**接收能力**，又要从全局考虑**不要使网络发生拥塞**。因此，每一个 TCP 连接需要有以下两个状态变量：

- **接收端窗口 rwnd** (receiver window) 又称**通知窗口：接收端**根据其目前的接收缓存大小所许诺的最新的窗口值，是来自**接收端的流量控制**。接收端

将此窗口值放在 TCP 报文的首部中的**窗口字段**，传送给发送端。

- **拥塞窗口 cwnd**：**发送端**根据自己估计的**网络拥塞程度**而设置的窗口值，是来自**发送端的流量控制**。

发送窗口的上限值 = Min [rwnd, cwnd]

- 当 rwnd < cwnd 时，是接收端的接收能力限制发送窗口的最大值。
- 当 cwnd < rwnd 时，则是网络的拥塞限制发送窗口的最大值。

7. 流量控制和拥塞控制的本质、相同点、不同点、实现的方法

流量控制：一种利用软件或硬件方式来实现对网络流量的控制。用于控制调制解调器与计算机之间的数据流，具有防止因为计算机和调制解调器之间通信处理速度的不匹配而引起的数据丢失。

拥塞控制：到达通信子网中某一部分的分组数量过多，使得该部分网络来不及处理，以致引起这部分乃至整个网络性能下降的现象，严重时甚至会导致网络通信业务陷入停顿，即出现死锁现象。

相同点都是为了提高网络性能。

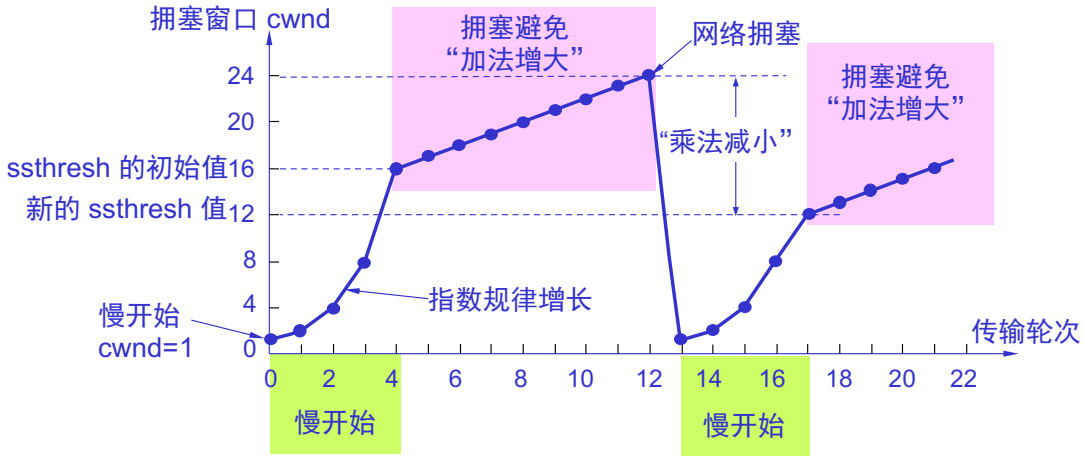
不同点：

- **拥塞控制**所要做的都有一个前提，就是**网络能够承受现有的网络负荷**。拥塞控制是一个**全局性的过程**，涉及到所有的主机、所有的路由器，以及与降低网络传输性能有关的所有因素。
- **流量控制**往往指在给定的**发送端和接收端之间**的**点对点通信量的控制**。流量控制所要做的就是**抑制发送端发送数据的速率**，以便使**接收端来得及接收**。

TCP 流量控制实现方法：基于**滑动窗口**协议的流量控制机制。*（见上题）*

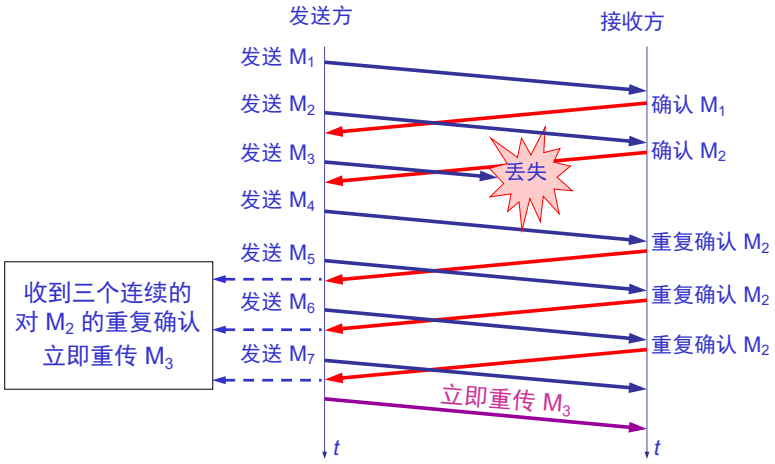
TCP 拥塞控制实现方法：

1）慢开始和拥塞避免：

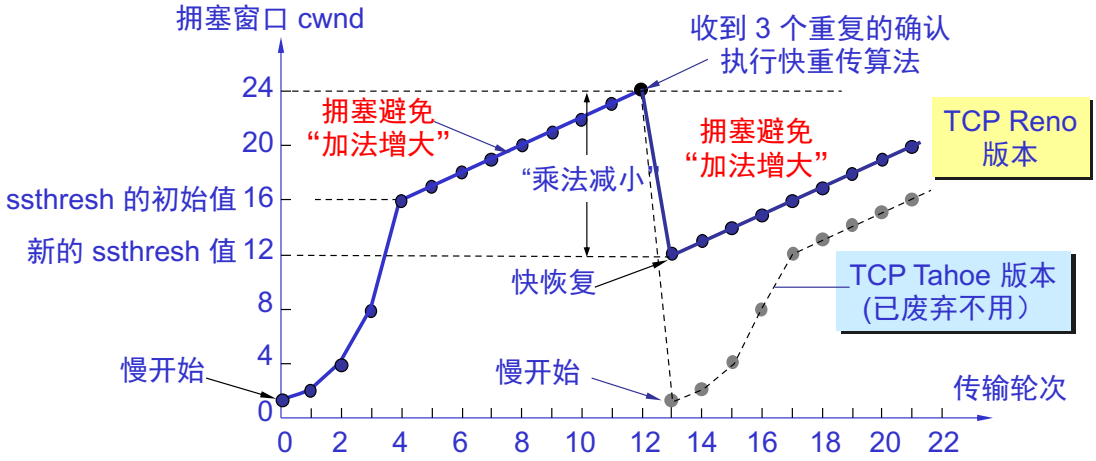


注：若 2cwnd>ssthresh，则下一轮 cwnd=ssthresh，即 cwnd 不能越过 ssthresh

2）快重传：快重传算法首先要求**接收方**每收到一个**失序**的报文段后就立即**发出重复确认**。发送方只要一连收到**三个重复确认**就应当**立即重传**对方尚未收到的报文段。这样做可以让发送方及早知道有报文段没有到达接收方。

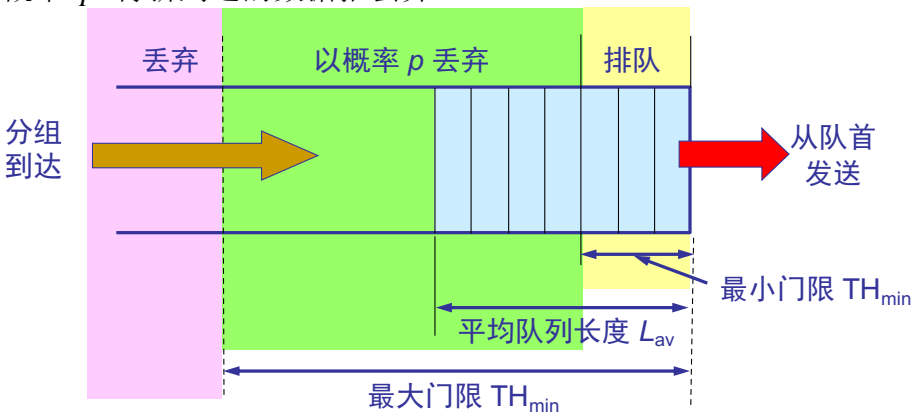


快恢复：当发送端收到连续三个重复的确认时，就执行“乘法减小”算法，把慢开始门限 ssthresh 减半，而不是执行慢开始算法。拥塞窗口 cwnd 现在不设置为 1，而是**设置为慢开始门限 ssthresh 减半后的数值**。



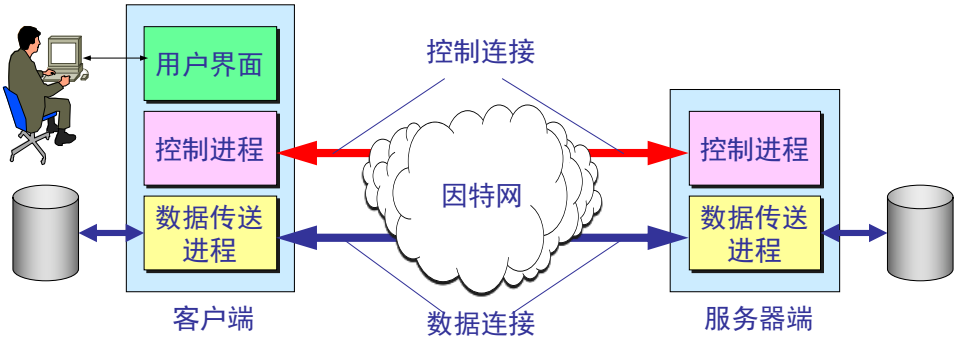
3）随机早期检测 RED

- 使路由器的队列维持两个参数：队列长度最小门限 TH_{min} 和最大门限 TH_{max}。
- RED 对每一个到达的数据报都先计算平均队列长度 L_{AV}。
  - 若平均队列长度小于最小门限 TH_{min}，则将新到达的数据报放入队列进行排队。（p=0）
  - 若平均队列长度超过最大门限 TH_{max}，则将新到达的数据报丢弃。（p=1）
  - 若平均队列长度在最小门限 TH_{min} 和最大门限 TH_{max} 之间，则按照某一概率 p 将新到达的数据报丢弃。



8. 默认的 FTP、DNS、SMTP、POP3、HTTP 等协议服务的应用场景、端口号、版本号

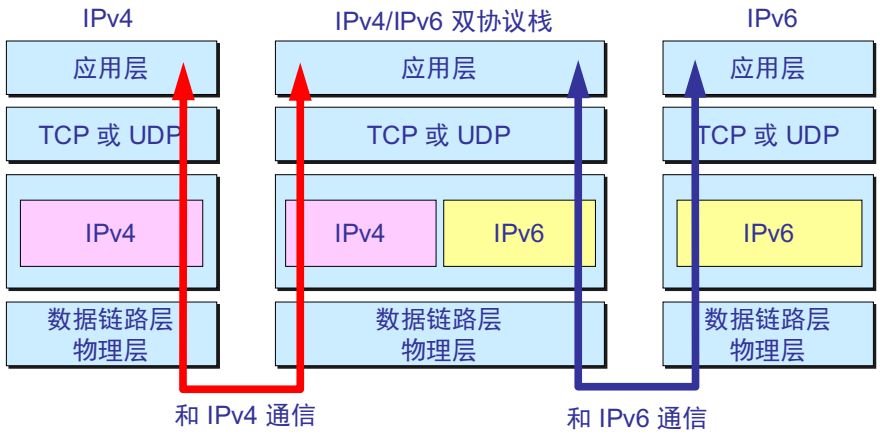
- **文件传送协议 FTP**：提供文件传送的一些基本的服务，使用 TCP 可靠的运输服务，C/S 工作方式。



  - **21** 端口：用于控制连接
  - **20** 端口：用于传输数据
- **域名系统 DNS**：把互联网上的主机名字（域名）转换为 IP 地址。
  辅域名服务器会定时向主域名服务器进行查询以便了解数据是否有变动，如有变动，则会执行一次区域传送，进行数据同步。
  区域传送将使用 TCP；客户端向 DNS 服务器查询域名，使用 UDP。
  使用 **53** 端口。
  查询方式：递归查询、迭代查询。
- **简单邮件传送协议 SMTP**：（发送邮件）使用了可靠的 TCP 连接将邮件从发送者的邮件服务器传输到接收者的邮件服务器中。端口 **25**。
- **邮局协议 POP3**：（读取邮件）负责将邮件从邮箱中取出后传输到接收者的主机上。使用 TCP 可靠的运输服务，C/S 工作方式，端口 **110**。
- 超文本传输协议 HTTP：定义了浏览器想万维网服务器请求万维网文档，以及服务器如何把文档传送给浏览器的方法。使用 80 端口。
  HTTP 是面向事务的、无状态的、无连接的。
- **HTTPS**：以安全为目标的 HTTP 通道，在 HTTP 的基础上通过传输加密和身份认证保证了传输过程的安全性，使用 443 端口。

9. IPv4 和 IPv6 的过渡技术

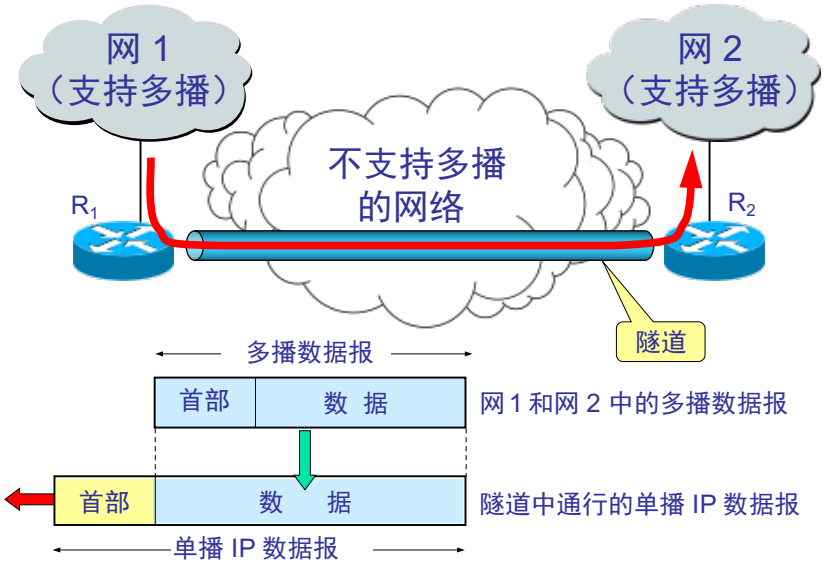
1) **双协议栈**：使一部分主机（或路由器）装有两个协议栈，一个 IPv4 和一个 IPv6。



2) **隧道技术**：将整个 IPv6 数据报封装到 IPv4 数据报的数据部分。

隧道技术的其他应用

在不支持多播的网络中转发多播数据报：路由器对多播数据报进行再次封装，使之成为单播数据报。

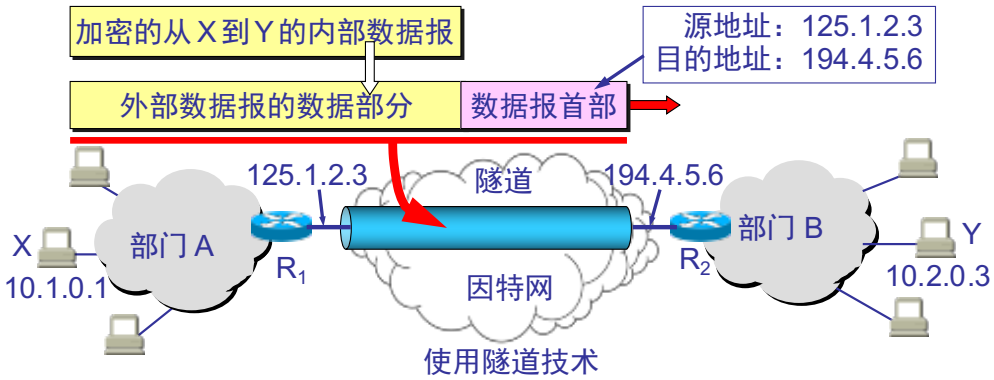


虚拟专用网 VPN：

- 本地地址：仅在机构内部使用的 IP 地址，可以由本机构自行分配，而不需要向因特网的管理机构申请。

  专用地址：只能用于一个机构内部通信，而不能用于和因特网上主机通信
  - 10.0.0.0/8，即 10.0.0.0 到 10.255.255.255
  - 172.16.0.0/12，即 172.16.0.0 到 172.31.255.255
  - 192.168.0.0/16，即 192.168.0.0 到 192.168.255.255
- 全球地址：全球惟一的 IP 地址，必须向因特网的管理机构申请。

每个网络至少有一个路由器和互联网的接口具有合法的全有 IP 地址，内部数据报到达路由器后，将数据报加密后重新加上首部，封装为在互联网上发送的外部数据报发往另一部门。



10. CIDR 表示法

CIDR：无分类域间路由选择

IP 地址 ::= {<网络前缀>, <主机号>}

斜线记法：在 IP 地址后加斜线“/”，后跟网络前缀位数（即子网掩码 1 的个数）

特点：

- 消除了传统的**分类地址**以及**划分子网**的概念，可以更加有效地分配 IPv4 的地址空间。

- 把网络前缀都相同的**连续的** IP 地址组成“CIDR 地址块”

11. TCP 序号、确认号的关系，IP 分片的偏移、标志位如何设置和计算

IP 分片

数据部分长度为 *m* 字节，给定 MTU（默认 1500）

- *n* 个分片的标志位均与原分片相同；
- 第 *i* 个分片的片偏移为 *(i-1)**MTU/*8* ；
- 第 0…n-1 个分片 MF=1，DF=0；第 n 个分片 MF=0，DF=0 。

TCP 报文

建立连接：三次握手

1、C->S: SYN=1, **seq=x**

2、S->C: SYN=1, ACK=1, **ack=x+1**, seq=y

3、C->S: ACK=1, ack=y+1, **seq=x+1**

释放连接：四次挥手

1、C->S: FIN=1, **seq=u**

2、S->C: ACK=1, **ack=u+1**, seq=v

3、S->C: FIN=1, ACK=1, **ack=u+1**, seq=w

4、C->S: ACK=1, ack=w+1, **seq=u+1**

12. 防火墙，入侵监测的定义及采用的技术

- **防火墙**：一种访问控制技术，通过严格控制进出网络边界的分组，**禁止**任何不必要的通信，从而减少潜在入侵的发生，尽可能降低这类安全威胁所带来的安全风险。

  技术：
  - **分组过滤路由器**：根据过滤规则对进出内部网络的分组进行过滤（转发或者丢弃）；
  - **应用网关**：对报文进行中继，实现基于应用层数据的过滤和高层用户鉴别。
- **入侵检测系统** IDS：能够在入侵已经开始，但还没有造成危害或在造成更大危害前，及时检测到入侵，以便尽快阻止入侵，把危害降低到最小。

  技术：基于异常的 IDS，基于特征的 IDS

13. 内部网关和外部网关协议各自采用的路由算法

内部网关协议 IGP

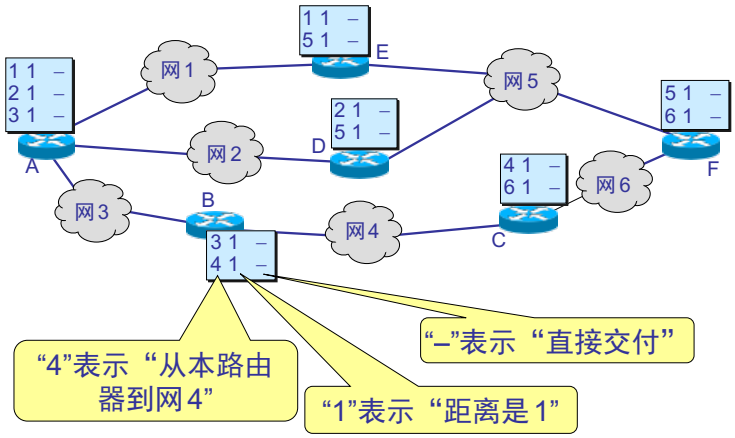
1) 路由信息协议 RIP

- 采用**距离矢量算法 DVA**(Distance Vector Algorithm)
- 仅和**相邻**路由器交换信息；
- 交换的信息是当前本路由器所知道的**全部信息**，即自己的路由表；
- 按**固定的时间间隔**交换路由信息，例如，每隔 30 秒。

距离：从**一个路由器**到**直接连接**的网络的距离定义为 1；从**一个路由器**到**非直接连接**的网络的距离定义为所**经过的路由器数加 1**。

DVA 算法：

一开始，各路由表只有到相邻路由器的信息

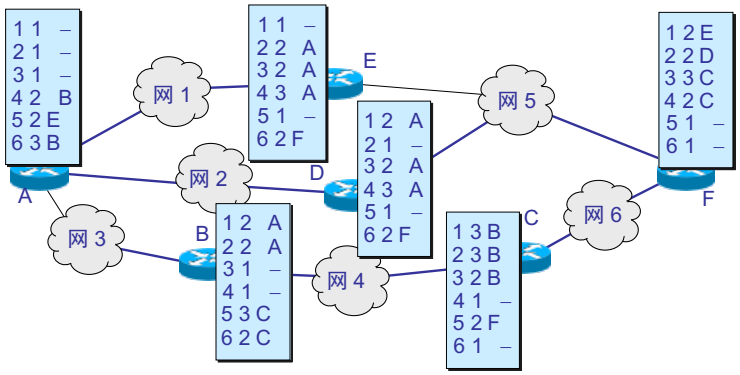


路由器 B 收到相邻路由器 A 和 C 的路由表，更新后为：

1	2	A
2	2	A
3	1	–
4	1	–
6	2	C

（若超时没收到相邻路由器更新的路由表，则记为不可达 16）

最终所有的路由器的路由表都更新了



优点：实现简单，开销较小。

缺点：

- 收敛慢：**好消息传播得快，而坏消息传播得慢**；
- RIP 限制了网络的规模，它能使用的最大距离为 **15**（16 表示不可达）；
- 路由器之间交换的路由信息是路由器中的完整路由表，因而随着网络规模的扩大，开销也就增加。

2) 开放最短路径优先协议 OSPF

- **更新发送**：只有当**链路状态**发生变化时，路由器才用**洪泛法**向所有路由器发送此信息
- **洪泛法**：向本自治系统中**所有路由器**发送信息，这里使用的方法是**洪泛法**。
- **链路状态**：发送的信息就是与本路由器相邻的所有路由器的链路状态
  即说明本路由器都和哪些路由器相邻，以及该链路的"度量"(metric)。

步骤：

1、构造包含发现信息的 L-S 报文(LSP)向全网广播

2、根据收集的 LSP 建立拓扑数据库 LSDB

4、启动 SPF 算法（Dijkstra）以 C 为源点计算 SPF 树

5、建立到达所有信宿的路由表（端口和代价）

OSPF 分区域管理：同一个区域内路由器才会建立邻居关系，交换 LSA，收敛后，同一个区域内所有设备具有相同的 LSDB，这个 LSDB 反映了区域内的链路状态，再计算区域内的路由。不同区域之间，由区域边界路由器 ABR 直接转发路由。

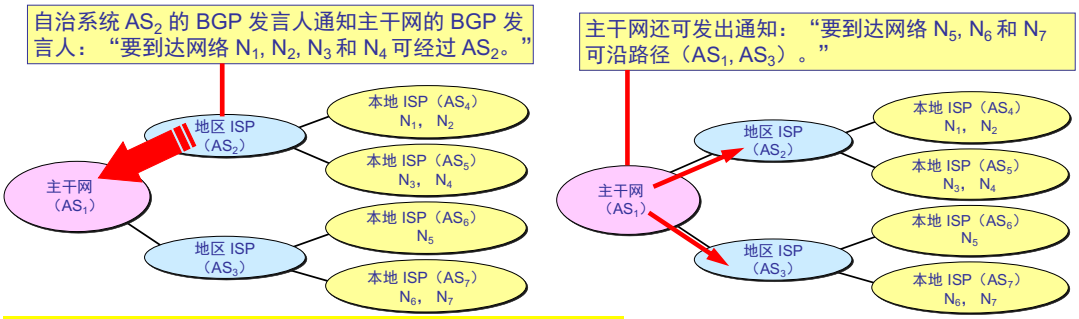
特点：

- **定时刷新**：OSPF 还规定每隔一段时间，如 30 分钟，要刷新一次数据库中的链路状态。
- **通信量少**：由于一个路由器的链路状态只涉及到与相邻路由器的连通状态，因而与整个互联网的规模并无直接关系。
- **收敛快**：OSPF 没有“坏消息传播得慢”的问题，据统计，其响应网络变化的时间小于 100 ms。
- **计算复杂**：构造 LSDB，计算 SPF 树。

外部网关协议 EGP：边界网关协议 BGP

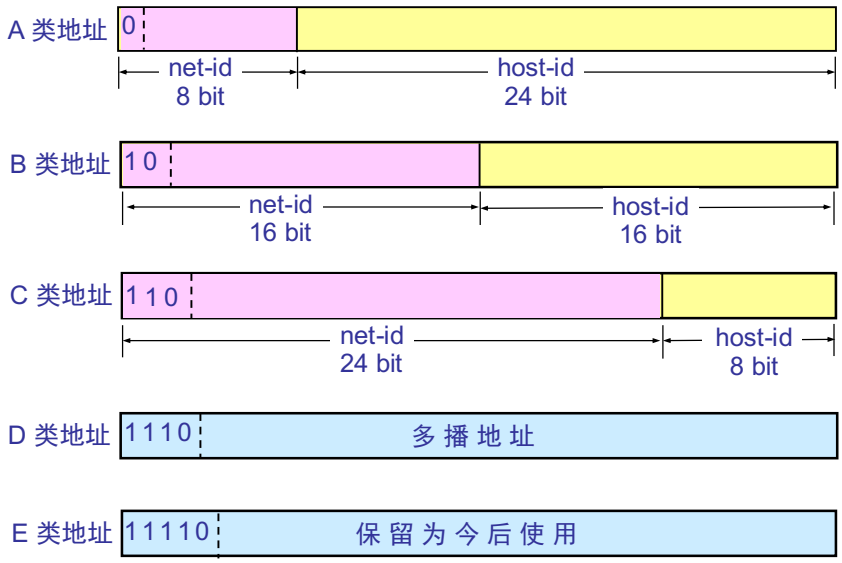
力求寻找一条能够到达目的网络且比较好的路由（不能兜圈子），而并非要寻找一条最佳路由。

工作原理：每个自治系统的管理员要选择至少一个路由器（可以有多个）作为该自治系统的**“BGP 发言人”**。一个 BGP 发言人与其他自治系统中的 BGP 发言人要交换路由信息，就要先建立 **TCP 连接**（BGP 报文是 TCP 报文的数据部分），然后在此连接上交换 BGP 报文以建立 **BGP 会话**，再利用 **BGP 会话**交换**路由信息**。当所有 BGP 发言人都相互交换网络**可达性的信息**后，各 BGP 发言人就可找出**到达各个自治系统的较好路由**。每个 BGP 发言人除必须运行 BGP 外，还必须运行该 AS 所用的内部网关协议。



14. ABCDE 类地址的定义、特点及判别方法

类别	网络号位数	最大网络数	可指派网络号起止	最大主机数	地址掩码
A	8	2^7-2	1-126	2^{24}-2	255.0.0.0
B	16	2^{14}-1	128.1-191.255	2^{16}-2	255.255.0.0
C	24	2^{21}-1	192.0.1-223.255.255	2^8-2	255.255.255.0
D	多播地址				
E	保留				



特殊的 IP 地址：

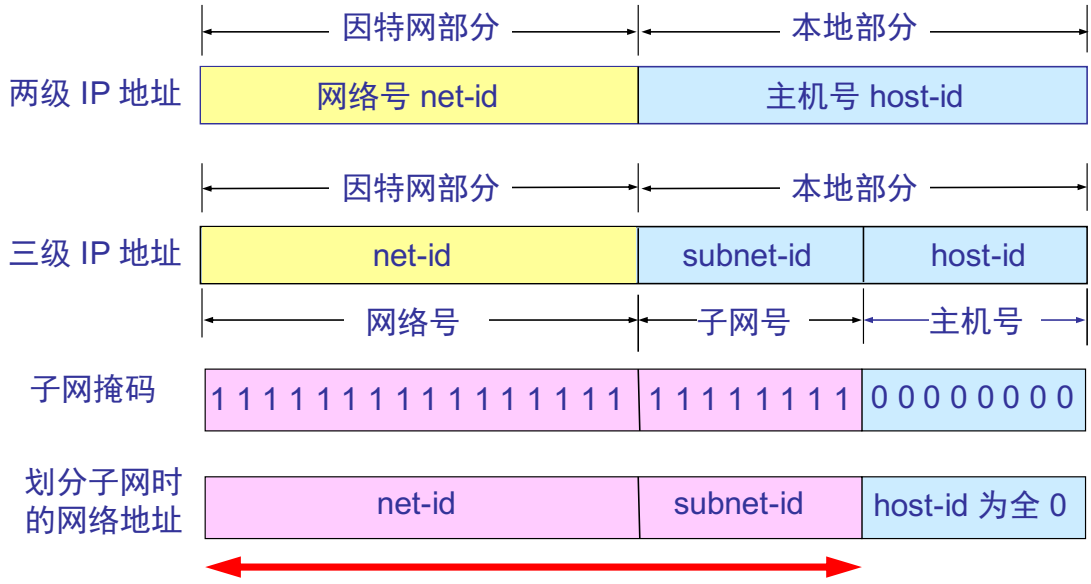
- 0.0.0.0：本主机（默认路由）。只可用作源地址
- 网络号为 0，主机号为 X：主机地址，主机号为 X 的主机。只可作源地址
- 255.255.255.255：广播地址（有限广播），只可用作目的地址
- 网络号为 Y，主机号全 1：对网络号为 Y 广播（直接广播），只可用作目的地址
- 127.0.0.1-127.255.255.254：本地环回测试

15. IP 地址的合法性、子网掩码的作用，子网号、主机号的区别，网络地址、主机地址、广播地址的区别。

IP 地址：网络号+主机号，点分十进制

子网掩码的作用：将某个 IP 地址划分成网络地址和主机地址两部分。

从主机号（前面）借用若干位作为子网号，而主机号也就相应减少了若干位。



子网掩码和 IP 地址**按位与**运算得到**网络地址**；

子网掩码的**反码**和 IP 地址**按位与**运算得到**主机地址**；

IP 地址=主机地址+网络地址；

广播地址=主机地址+子网掩码的**反码**。

16. 三种交换方式、两种服务方式、两种通信方式的概念、名称、本质和区别

三种交换方式：

- **电路交换**：以电路连接为目的的交换方式。面向连接的，适合于语音通信，数据具有突发性，线路的利用率低
- **报文交换**：基于存储转发原理，时延较长
- **分组交换**：把较长的报文划分成较短的、固定长度的数据段，加上首部构成分组；高效、灵活、迅速、可靠

两种服务方式：

- **面向连接的服务**：面向连接服务具有连接建立、数据传输和连接释放这三个阶段。
- **无连接的服务**：两个实体之间的通信不需要先建立好连接，是一种不可靠的服务“尽最大努力交付”

两种通信方式：

- **串行通信**：在数据通道上每次传输一个位元数据。节省传输线，适用于长距离的通信，但数据的传送效率低。
- **并行通信**：一次同时传输若干位元数据。效率高，速度快，适用于短距离进行大量、实时的数据交换，但成本较高，抗干扰能力差。

17. 计算机网络性能指标的名称、定义、计算方法

带宽：原指信号具有的频带宽度（Hz），现指数字信道所能传送的“**最高数据率**”。

速率（数据传输率、比特率）：在数字信道上传送数据的速率。

最高数据传输速率称为**带宽**。

排队时延：数据进入路由器后再输入队列中排队等待处理，确定转发端口后在输出队列等待转发花费的时间。

处理时延：数据在交换节点为存储转发而进行的一系列必要处理花费的时间。

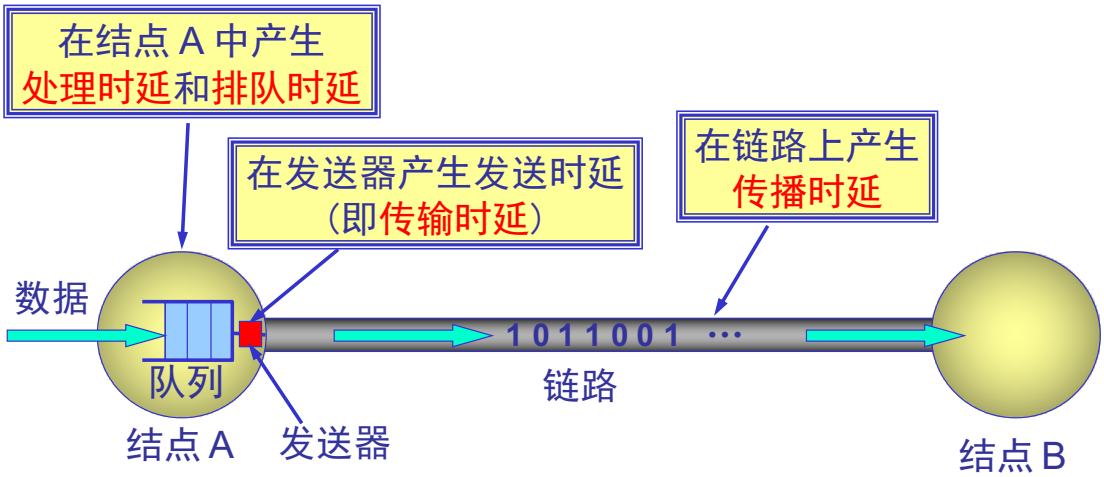
发送时延（传输时延）：发送数据时，数据块从结点进入到传输媒体所需要的时间。发送时延=数据块长度/信道带宽(传输速率、发送速率)

传播时延：电磁波在信道中需要传播一定的距离而花费的时间。

传播时延=信道长度/信号在信道上的传播速率

真空光速：$3*10^5$ km/s；铜缆中的电信号：$2.3*10^5$ km/s；光纤：$2*10^5$ km/s

总时延=发送时延+传播时延+处理时延+等待时延



往返时延 RTT：从发送端发送数据开始，到发送端收到来自接收端的确认（接收端收到数据后立即发送确认），总共经历的时延。

时延带宽积：以比特为单位的链路长度。时延带宽积=传播时延*带宽
吞吐量：单位时间内通过某个网络（或信道、接口）的数据量。
信道利用率：某信道有百分之几的时间是被利用的（有数据通过）。
信道利用率=有数据通过时间/(有+无)数据通过时间
网络利用率：全网络的信道利用率的加权平均值。

18. 时延的组成及其各自的区别和计算方法

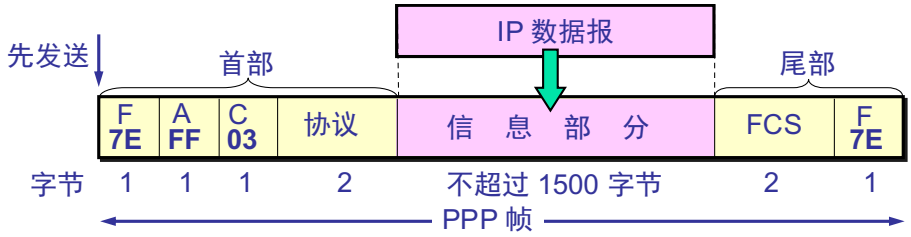
见上一题

19. 复用技术的特点、实现方法、本质、应用领域

- 频分复用 FDM：多个信号调制在不同的频率上。用于模拟信号传输。
- 时分复用 TDM：将信道分为若干时间片，轮换给多路信号使用。用于数字信号传输。
- 波分复用 WDM：不同信源的信号占用不同波长的光波。用于光纤信道。
- 码分利用 CDM：不同信源的信号使用不同的编码。

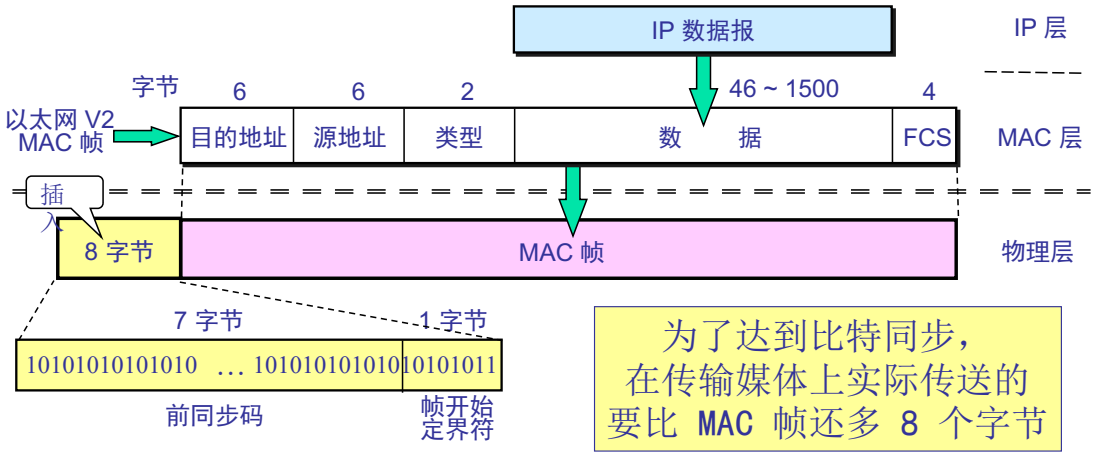
20. 以太网帧、802.1Q 帧、IP、UDP、TCP 首部格式及每个字段的定义、计算规则和约束条件

PPP 协议的帧格式



标志字段 F：7E（01111110）
地址字段 A：FF（全 1，广播地址）
控制字段 C：03
协议字段：0x0021：IP 数据报；0xC021：LCP 数据；0x8021：NCP 数据。
链路控制协议 LCP；网络控制协议 NCP
帧校验序列 FCS：CRC 计算检错码，不校验 F 字段。

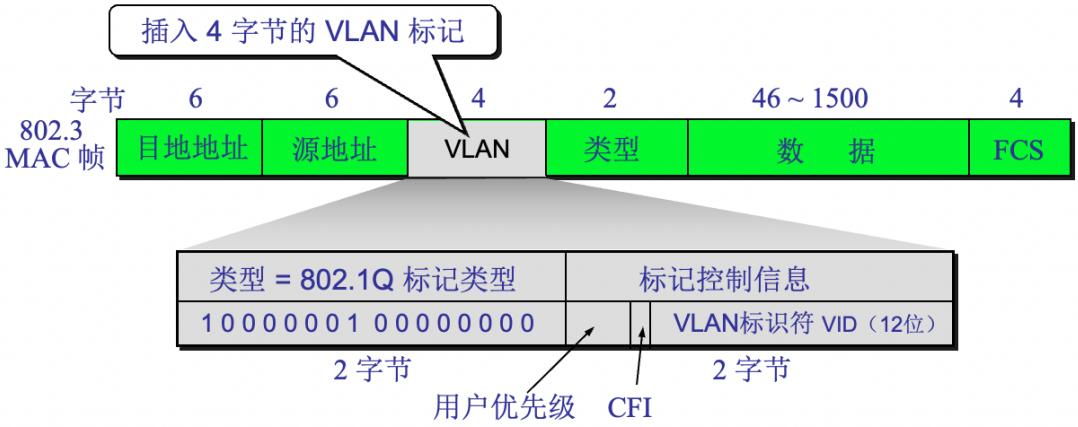
以太网 V2 的 MAC 帧格式



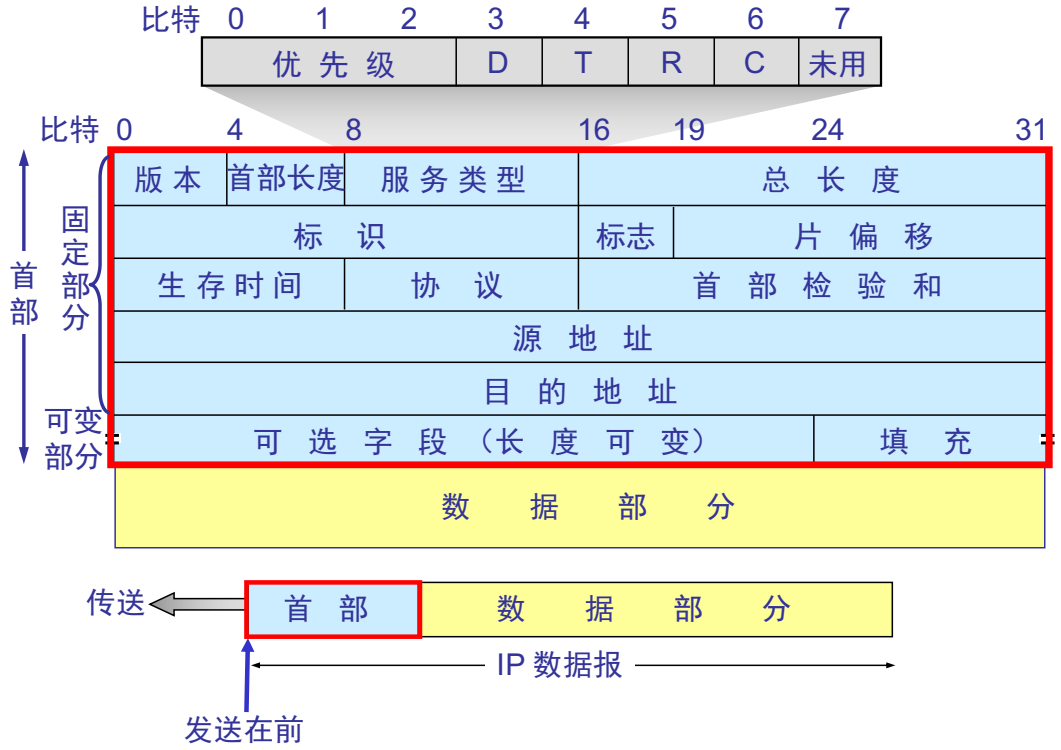
目的地址和源地址：6 字节
类型字段：使用上一层的协议
数据字段：46（最小 64-6-6-2-4=46）~1500（MTU）
帧校验序列 FCS：CRC 检验

802.1Q 帧

虚拟局域网 VLAN 是由一些局域网网段构成的与物理位置无关的逻辑组。这些网段具有某些共同的需求。在以太网的帧格式中插入一个 4 字节的标识符，称为 **VLAN 标记(tag)**，用来指明发送该帧的工作站属于哪一个虚拟局域网。



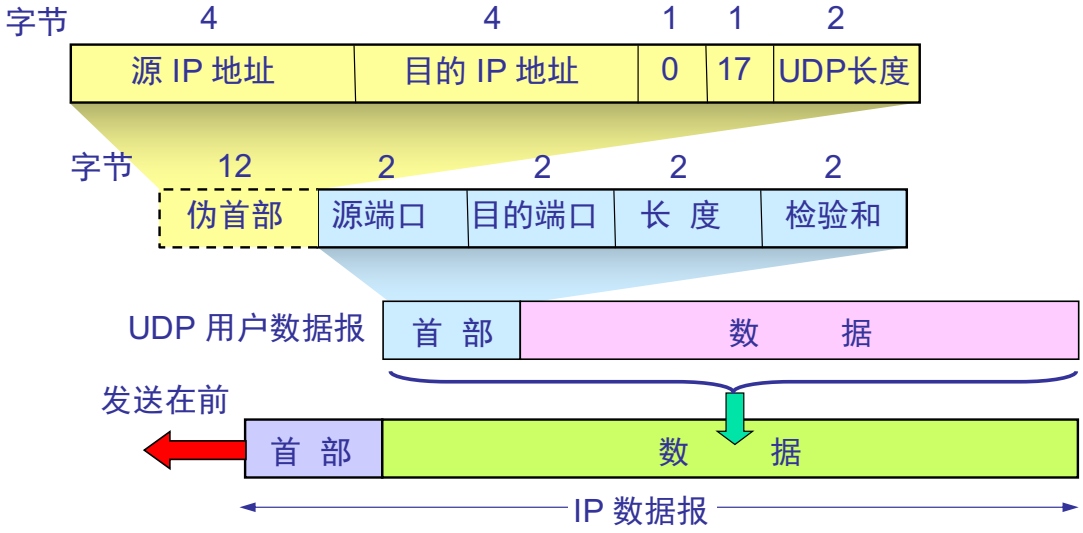
IP 数据报首部



- **版本**：占 4 bit，指 IP 协议的版本，4 或 6，双方的版本必须一致。
- **首部长度**：占 4 bit，首部的最大数值（**4 字节**整数倍），5~15。
- **服务类型**：占 8 bit，弃用。
- **总长度**：占 16 bit，指首部和数据之和的长度，单位为**字节**，因此数据报的最大长度为 65535 字节。数据的总长度必须不超过最大传送单元 MTU。
- **标识**：16 bit，相同标识的分片会重新组装成原来的数据报。
- **标志**：3 bit，只有 2 位有意义，MF=1 还有分片，DF=1 不能分片。
- **片偏移**：13 bit，某片在原分组中的相对位置（**8 字节**整数倍）。
- **生存时间**(8 bit)：记为 TTL，**跳数限制**，路由器每转发一次 TTL-1，为 0 则丢弃，1（只在本局域网内传播）~255。

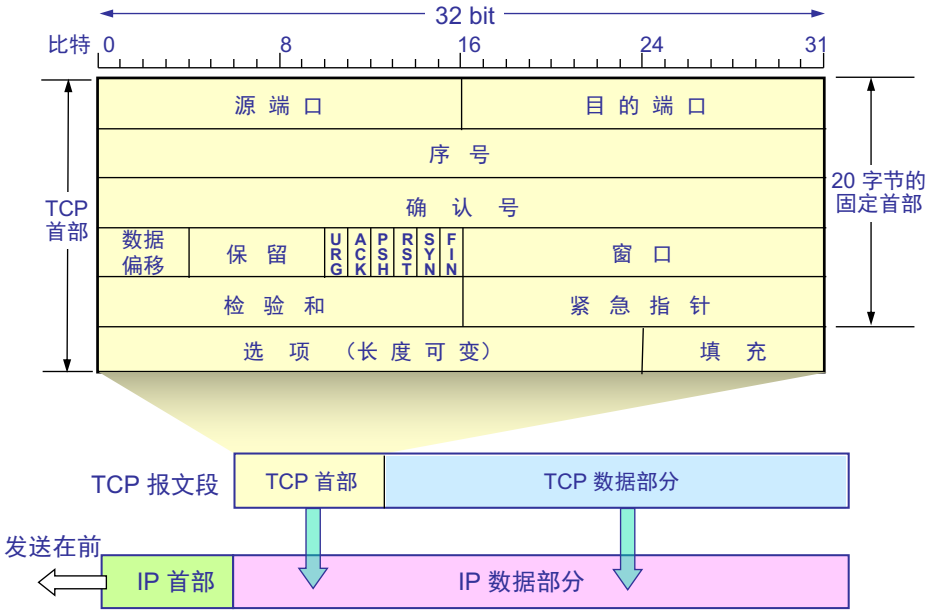
- **协议**(8 bit)：字段指出此数据报携带的数据使用何种协议。
  ICMP=1, IGMP=2, IP=4, TCP=6, UDP=17
- **首部检验和**(16 bit)：只检验数据报的首部
  发送：字段置 0，首部划分为 16 位字的序列，反码算数求和，**取反**写入；
  接收：再次反码算数求和，取反为 0 则保留。
  注意：进行反码运算求和时，最高位有进位应当加到最低位。
- **源地址**和**目的地址**：各占 4 字节

UDP 用户数据报



- **源端口**和**目的端口**：2 字节（16 位）
- **长度**：2 字节（16 位），首部+数据，单位**字节**，最小值为 8（仅有首部）
- **校验和**：2 字节（16 位），可选，不计算填 0；但计算之前要添加 12 字节的**伪首部**，**且检查首部和数据部分**，若数据部分不是偶数字节，则填充一个**全零字节**（但不发送），使用反码运算求和，结果**取反**写入校验和字段，接收方同样反码运算求和，结果**取反**后为全 0 则无差错。

TCP 数据段



- **源端口**和**目的端口**：各占 2 字节（16 位）。端口是运输层与应用层的服务

接口。运输层的复用和分用功能都要通过端口才能实现。

- **序号 seq**：占 4 字节。本报文段所发送的数据的**第一个字节的序号**。TCP 连接中传送的数据流中的**每一个字节都编上一个序号**。
- **确认号 ack**：占 4 字节，是期望收到对方的**下一个报文段**的**数据的第一个字节的序号**。
- **数据偏移（首部长度）**：占 4 位，它指出 TCP 报文段的数据起始处距离 TCP 报文段的起始处有多远。单位是 **32 位字（4 字节）**。
- **保留字段**：占 6 位，保留为今后使用，但目前应置为 **0**。
- **紧急 URG**：为 1 时，表明**紧急指针**字段**有效**。它告诉系统此报文段中有**紧急数据**，应尽快传送(相当于**高优先级**的数据)。
- **确认 ACK**：为 1 确认号有效，为 0 确认号无效。
- **推送 PSH**：为 1 **尽快地交付**接收应用进程，而不再等到整个缓存都填满了后再向上交付。
- **复位 RST**：为 1 表明连接中出现**严重差错**（如由于主机崩溃或其他原因），必须释放连接，然后再重新建立运输连接。
- **同步 SYN**：为 1 表示这是一个**连接请求**或**连接接受**报文。
- **终止 FIN**：用来**释放**一个连接。为 1 表明此报文段的发送端的数据已发送完毕，并要求释放运输连接。
- **窗口**：占 2 字节，用来让对方设置**发送窗口**的依据，单位为**字节**。
- **检验和**：占 2 字节。检验和字段检验的范围**包括首部和数据**这两部分。在计算检验和时，要在报文段的前面加上 12 字节的**伪首部**。
- **紧急指针**：占 16 位，指出在本报文段中**紧急数据共有多少个字节**（紧急数据放在本报文段数据的最前面）。
- **选项**：长度可变。*最初只规定了一种* **最大报文段长度 MSS** (数据字段的最大长度，以太网 MSS=1500-20-20=1460)
- **填充**：使整个首部长度是 **4 字节**的整数倍。

---

21. PPP 字符填充和比特填充的方式、特殊情况处理

- 当 PPP 用在**同步传输链路**时，协议规定采用**硬件**来完成**比特填充**。
  连续出现 5 个 1 时，立刻填入一个 0。
- 当 PPP 用在**异步传输**时，就使用一种特殊的**字符填充法**。
  标志字段为 0x7E，转义字符定义为 **0x7D**；
  若信息部分出现 **0x7E**，替换为 0x7D **0x5E**（与 0x20 异或，前面插入 0x7D）；
  若信息部分出现 ASCII 码控制字符（小于 0x20 的字符），**与 0x20 异或后**，前面插入 **0x7D**。

22. 数据、信号、信息、编码方式等通信基本概念

- **数据**：运送信息的实体。
- **信号**：数据的电气的或电磁的表现，是数据在传输过程中的具体存在形式
- **信息**：信息是用来消除随机不确定性的东西
- **数据编码**（调制）：将数据转换为适合于在信道上传输的某种电信号形式(模拟或数字信号)。

编码方式：

- **不归零码**在一个码元的全部时间内，电平保持恒定。低电平 0，高电平 1，或相反。
- **归零码**在一个码元结束时电平总是回到零(低电平)。

- **曼彻斯特编码**：每位中间有一个电平跳变，从高到低的跳变表示“1”，从低到高的跳变表示“0”，或者相反。**以太网使用的就是曼彻斯特编码。**
- **差分曼彻斯特编码**：曼彻斯特编码的一种变形。在这种编码方式中，每位的中间跳变只用于作为同步时钟信号，而用位的起始处有无跳变来区分“0”和“1”，若有跳变表示“0”，无跳变表示“1”。

23. 路由聚合、子网划分

划分子网：

- 划分子网纯属一个单位内部的事情。这个单位对外仍然表现为没有划分子网的网络。*划分子网只是对主机号进行划分，不改变原有的网络号。*
- 从主机号借用若干个比特作为子网号，而主机号也就相应减少了若干个比特，形成三级 IP 地址：{<网络号>, <子网号>, <主机号>}

原因：

- IP 地址空间的利用率有时很低。
- 给每一个物理网络分配一个网络号会使路由表变得太大而使网络性能变坏。
- 两级的 IP 地址不够灵活。

路由聚合（构成超网）：

- 将网络前缀都相同的**连续的** IP 地址组成“CIDR 地址块”。一个 CIDR 地址块可以表示很多地址。
- 可以使得路由表中的一个项目可以表示多个原来传统分类地址的路由，有利于减少路由器之间的路由选择信息的交换，从而提高网络性能。

24. 网络协议三要素

1) **语义**：涉及需要发出何种控制信息，完成何种动作与做出何种响应。
2) **语法**：涉及数据与控制信息的结构与格式。
3) **定时**：涉及速度匹配与事件顺序。

25. 光纤的类型

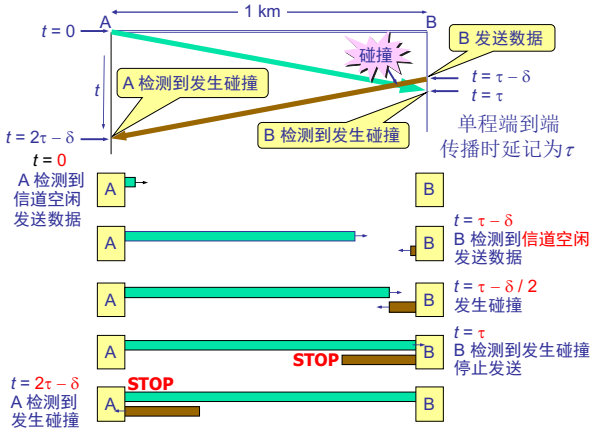
多模光纤：从不同角度入射的多条光纤在一根光纤中传输。只适合近距离传输。
单模光纤：直径只有一个光的波长。衰减小，适合远距离传输，但成本高。

26. 10M/100M/1000M 以太网的争用期定义及计算方法

争用期：以太网的端到端**传播时延** 2τ 称为争用期，或碰撞窗口。

长度为 x 的 CSMA/CD 网络的数据率为 m Mbps，信号在网络上的传播速率为 $2*10^8$m/s，则能使用该协议的最短帧长：

- 首先计算传播时延τ=距离/传播速率=x/$2*10^8$ (μs)
- 在 2τ内要发送的数据量为 2τ*m Mb 即为最短帧长



最迟要经过 2τ才能知道是否发生了碰撞。

CSMA/CD 的必要条件：

- 帧的传输时间>=2τ
- 以太网规定**争用期长度**为 51.2 μs。
- 对于 10 M 以太网，在争用期内可以发送 512 bit，即**最短帧长**为 64 字节。

CSMA/CD：载波监听多点接入/碰撞检测

- 载波监听：每一个站点在发送数据之前以及发送的过程中都检测总线上是否有计算机在发送数据。
- 多点接入：是总线型网络。
- 碰撞检测（冲突检测）：边发送边监听（半双工通信）

27. CRC 计算方法和过程

生成多项式 G(x)的阶为 r，在帧的末尾加上 r 个 0；

利用模 2 除法用 G(x)对应的数据串去除数据得到的余数就是 CRC。

模 2 除法：被除数最高位为 1 即可相除，商 1，加减使用异或。

28. 网络测试的常用命令

- ping：测试两台主机的连通性。
- traceroute（MS-DOS 中为 tracert）：跟踪一个分组从源点到终点的路径。
- ipconfig（UNIX 为 ifconfig）：显示当前的 TCP/IP 配置的设置值。
- netstat：了解网络的整体使用情况，正在活动的网络连接的详细信息。

29. 奈氏准则、香农公式的定义、计算过程。

码元：时间轴上的一个信号编码单元

波特率 B：每秒钟发送的码元数，或者说每秒钟信号（比如电压）变化的次数，单位为波特。

奈氏准则：理想低通信道的**最高码元传输速率** = 2W Baud

W 是理想低通信道的带宽，单位为赫(Hz)

比特率 S：每秒钟能传送的二进制位数，单位为比特/秒（bps）。

$S=B\cdot\log_2 N$, N 为码元状态数

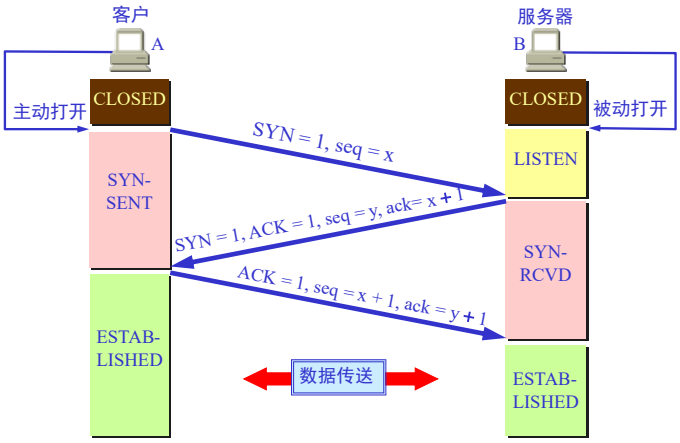
香农公式：信道的**极限信息传输速率** $C = W\log_2(1+S/N)$ bps，S/N 为信噪比

30. internet 与 Internet 的区别

- **Internet**，因特网，专有名词，全球最大的、开放的、由众多网络相互连接而成的特定计算机网络，它采用 TCP/IP 协议族作为通信的规则，且其前身是美国的 ARPANET
- **internet**，互联网，通用名词，它泛指由多个计算机网络互连而成的网络。

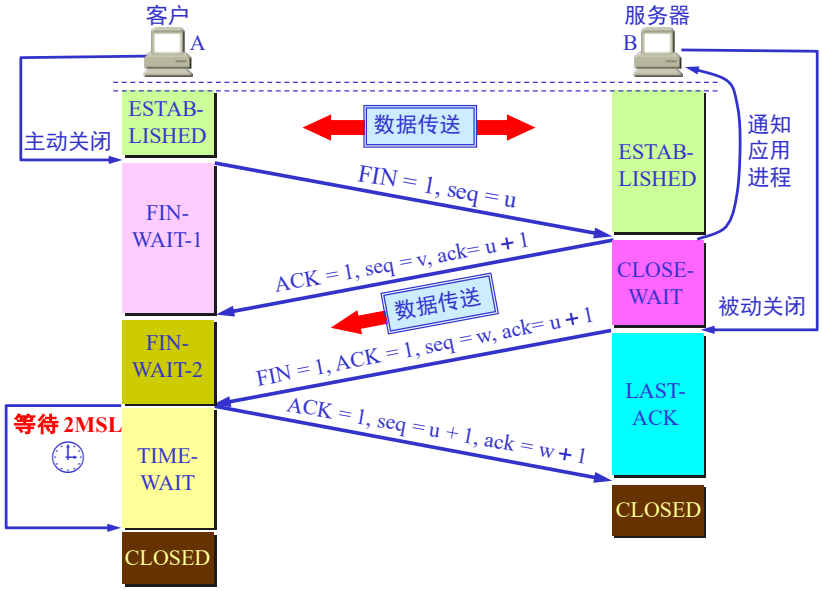
31. TCP 连接的建立和拆除过程，及其简化、拆分、修改方法

TCP 连接的建立：三次握手



1、客户 A 向服务器 B 发出 TCP **连接请求报文段**，首部同部位 SYN=1，同时选择一个初始序号 seq=x。规定 SYN 报文段（SYN=1 的报文段）不能携带数据，但要消耗掉一个序号。TCP 客户进程进入 SYN-SENT（同步已发送状态）。
2、服务器 B 收到报文后向客户 A 发送**确认报文段**，SYN=1，ACK=1，确认号是 ack=x+1。同时也选一个初始序号 seq=y。同理，确认报文段不能携带数据，但要消耗掉一个序号。同时，为 TCP 连接分配缓存和变量，进入 SYN-RCVD（同步收到）状态。
3、客户 A 的 TCP 客户进程在收到服务器的确认后，还要向服务器进程给出确认。**确认报文段** ACK=1，确认号 ack=y+1，而自己的序号 seq = x + 1。这个报文段可以携带数据，也可以不携带数据，如果不携带数据，下一个数据报文段的序号仍是 seq = x + 1。这时，TCP 连接已经建立，客户进入 ESTABLISHED（已建立连接）状态。服务器收到客户的确认后，也进入 ESTABLISHED 状态。

TCP 连接的释放：四次挥手



1、客户 A 先发出**释放连接报文段**，并停止发送数据，主动关闭 TCP 连接。首部 FIN=1，其序号为 seq=u。这时 A 进入 FIN-WAIT-1（终止等待 1）状态。
2、服务器 B 收到**连接释放报文段**后立即发出确认，ACK=1，确认号为 ack=u+1，自己的序号为 seq=v。然后 B 就进入 CLOSE-WAIT（关闭等待）状态。此时从客户端到服务器这一方向的连接断开，TCP 连接处于半关闭状态，即 A 已经没有数据要发送了，但 B 若发送数据，A 仍接收。
3、客户 A 收到来自服务器 B 的确认后，就进入 FIN-WAIT-2（终止等待 2）状态，等待 B 发出的**连接释放报文段**。若服务器没有要发送的数据了，通知 TCP 释放连接，发出的**连接释放报文段**，FIN=1，ACK=1，重复上次已发送过的确认号 ack=u+1，自己的序号 seq=w。这时 B 就进入了 LAST-ACK（最后确认）状态，等待 A 的确认。
4、客户 A 收到了的连接释放报文段后，必须对此发出**确认**。ACK=1，确认号为 ack=w+1，而自己的序号为 seq=u+1。此时，TCP 连接还没有释放掉，进入到 TIME-WAIT（时间等待）状态。必须经过**时间等待计时器**设置的时间 **2MSL**（最长报文段寿命）后，A 才进入到 CLOSED 状态。服务器 B 只要收到客户 A 发出的确认，就进入 CLOSED 状态。
32. 习题 1-29，1-30，1-31，3-09，3-10，3-20，4-22，4-41，4-48，