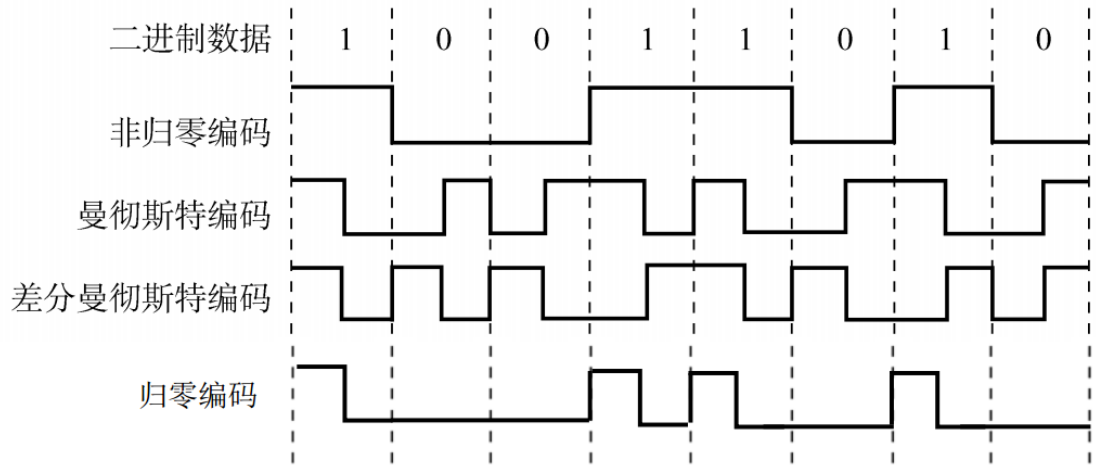
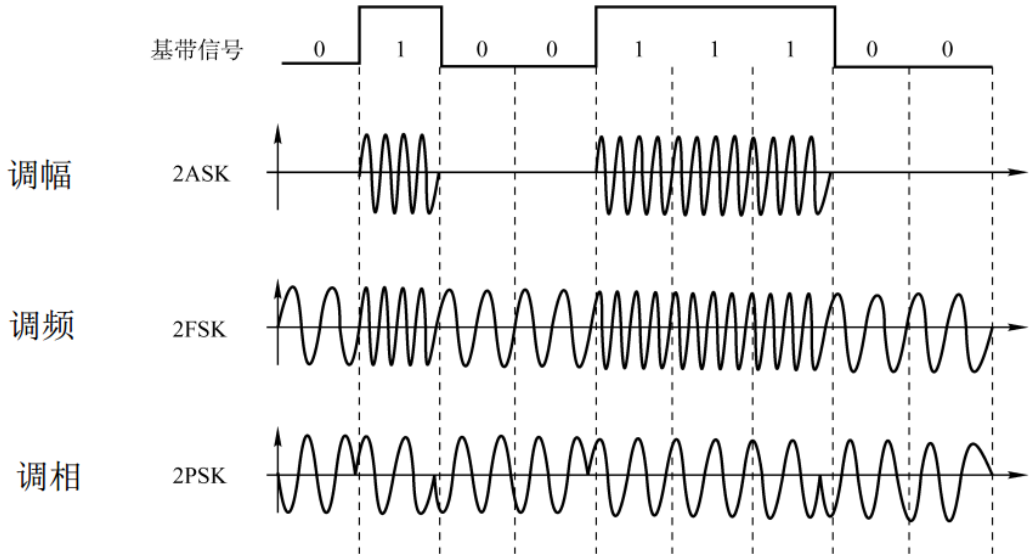




调幅+调相（QAM）　某通信链路的波特率是1200Baud，采用4个相位，每个相位有4种振幅的QAM调制技术，则该链路的信息传输速率是多少？

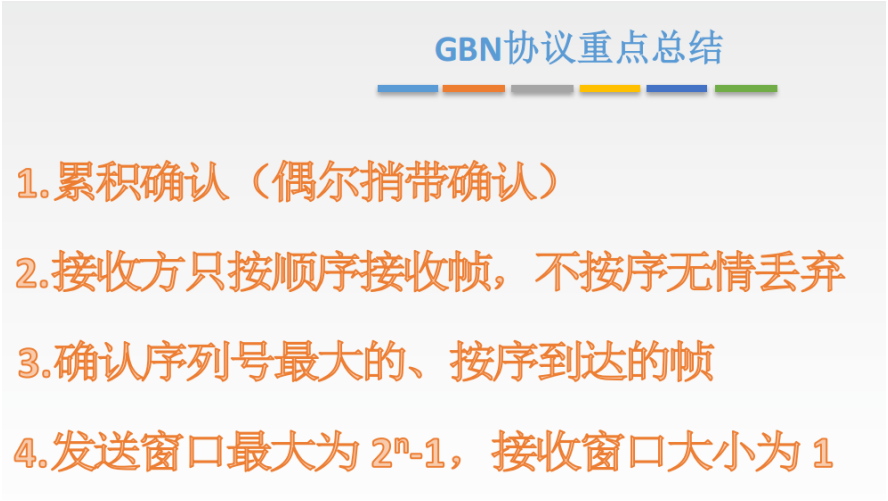
计算机内部处理的是二进制数据，处理的都是**数字音频**，所以需要将模拟音频通过采样、量化转换成有限个数字表示的离散序列（即实现音频数字化）。
最典型的例子就是对音频信号进行编码的脉码调制（**PCM**），在计算机应用中，能够达到**最高保真水平**的就是PCM编码，被广泛用于素材保存及音乐欣赏，CD、DVD以及我们常见的 WAV文件中均有应用。它主要包括三步：抽样、量化、编码。

1.抽样： 对模拟信号周期性扫描，把时间上连续的信号变成时间上离散的信号。
为了使所得的离散信号能无失真地代表被抽样的模拟数据，要使用采样定理进行采样：$f_{采样频率} \geq 2f_{信号最高频率}$

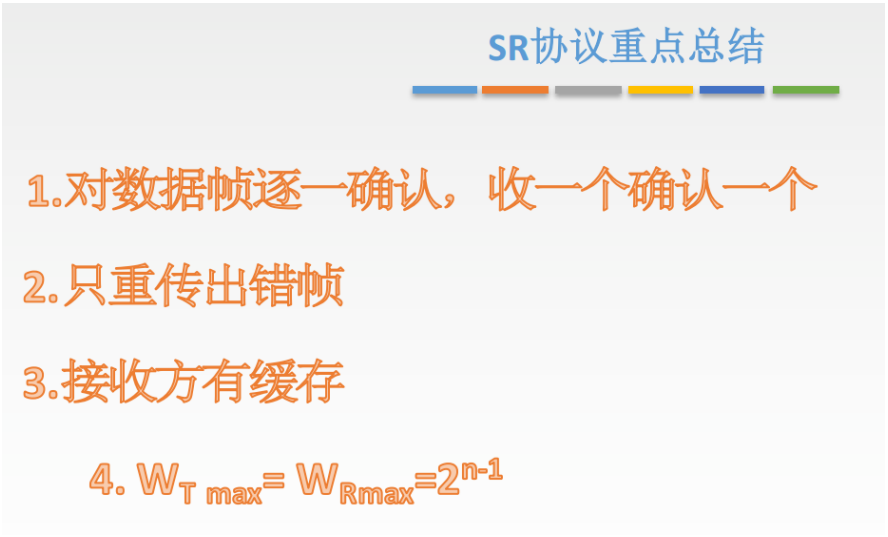
2.量化： 把抽样取得的电平幅值按照一定的分级标度转化为对应的数字值，并取整数，这就把连续的电平幅值转换为离散的数字量。

3.编码： 把量化的结果转换为与之对应的二进制编码。

GBN 协议：



选择重传协议：



ALOHA 协议：

关于ALOHA要知道的事

1.纯ALOHA比时隙ALOHA吞吐量更低，效率更低。

2.纯ALOHA想发就发，时隙ALOHA只有在时间片段开始时才能发。

CSMA 协议：

	1-坚持CSMA	非坚持CSMA	p-坚持CSMA
信道空闲	马上发	马上发	p概率马上发 1-p概率等到下一个时隙再发送
信道忙	继续坚持监听	放弃监听，等一个随机时间再监听	放弃监听，等一个随机时间再监听

超想喝！到我就买，没到我就排队等！

不急喝。到我就买，没到我就一会再来。

随性喝。到我按概率买，没到就一会再来。

截断二进制指数规避算法&最小帧长：

截断二进制指数规避算法

1.确定基本退避（推迟）时间为争用期 2τ。

2.定义参数k，它等于**重传次数**，但k不超过10，即k=min[重传次数，10]。当重传次数不超过10时，k等于重传次数；当重传次数大于10时，k就不再增大而一直等于10。

3.从离散的整数集合**[0, 1, , 2^k-1]**中随机取出一个数r，重传所需要退避的时间就是**r倍的基本退避时间**，即 2r τ 。

4.当重传达16次仍不能成功时，说明网络太拥挤，认为此帧永远无法正确发出，抛弃此帧并向高层报告出错。

帧的传输时延至少要两倍于信号在总线中的传播时延。

$$\frac{\text{帧长（bit）}}{\text{数据传输速率}} \geq 2\tau$$

最小帧长=总线传播时延 x 数据传输速率 x 2

$$2\tau \times \text{数据传输速率}$$

以太网规定最短帧长为64B，凡是长度小于64B的都是由于冲突而异常终止的无效帧。

CSMA/CA:

发送数据前，先检测信道是否空闲。

空闲则发出**RTS（request to send）**，RTS包括发射端的地址、接收端的地址、下一份数据将持续发送的时间等信息；信道忙则等待。

接收端收到RTS后，将响应**CTS（clear to send）**。

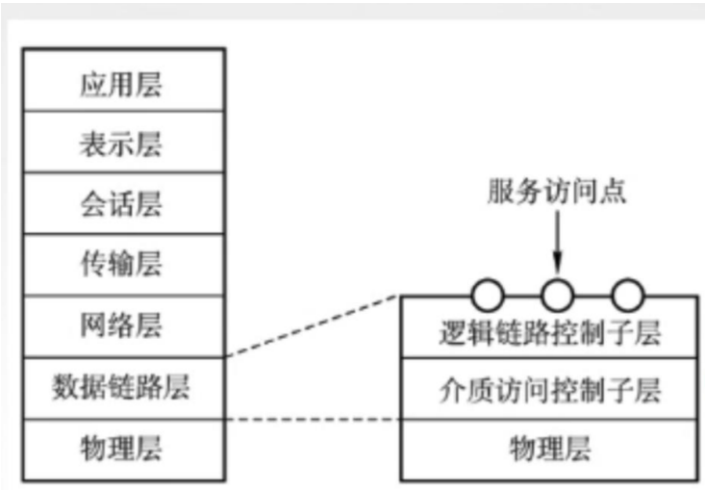
发送端收到CTS后，开始发送数据帧（同时**预约信道**：发送方告知其他站点自己要传多久数据）。

接收端收到数据帧后，将用CRC来检验数据是否正确，正确则响应**ACK帧**。

发送方收到ACK就可以进行下一个数据帧的发送，若没有则一直重传至规定重发次数为止（采用**二进制指数退避算法**来确定随机的推迟时间）。

1.预约信道　　2.ACK帧　　3.RTS/CTS帧（可选）

LLC&MAC:



以太网标准:

以太网两个标准

DIX Ethernet V2：第一个局域网产品（以太网）规约。

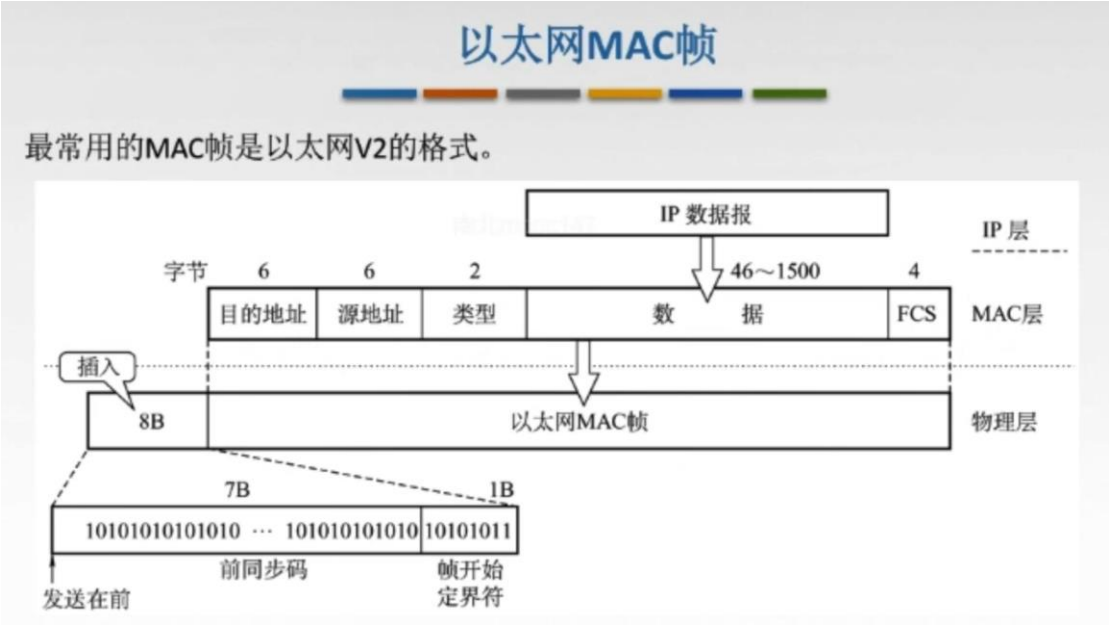
IEEE 802.3：IEEE 802委员会802.3工作组制定的第一个IEEE的以太网标准。

以太网拓扑:

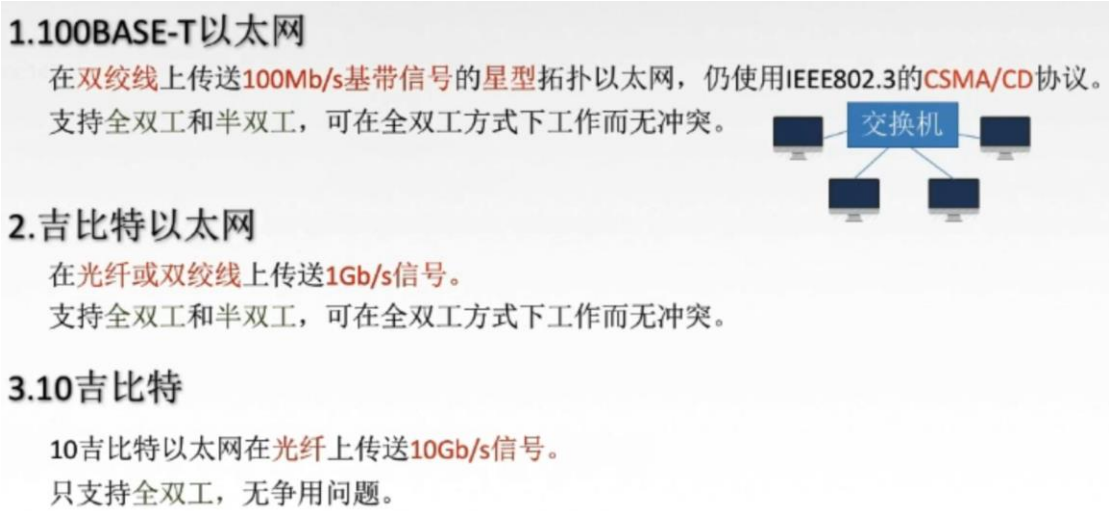
使用集线器的以太网在逻辑上仍是一个总线网，
各站共享逻辑上的总线，使用的还是CSMA/CD协议。

以太网拓扑：逻辑上总线型，物理上星型。

以太网 MAC 帧：



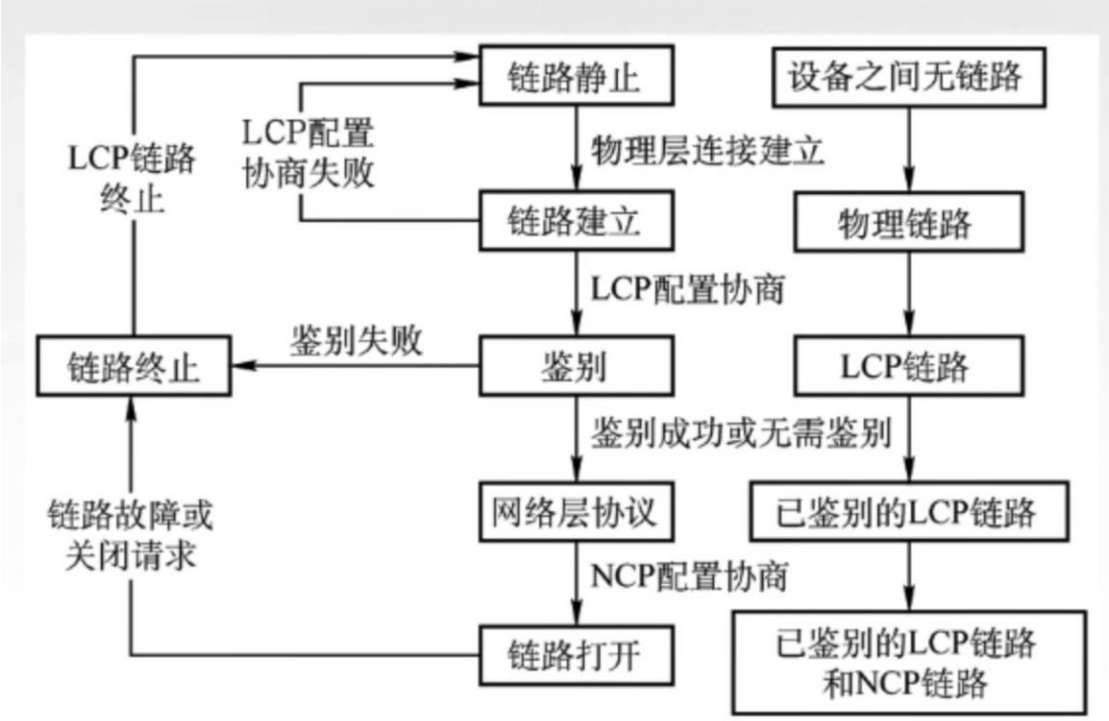
高速以太网：



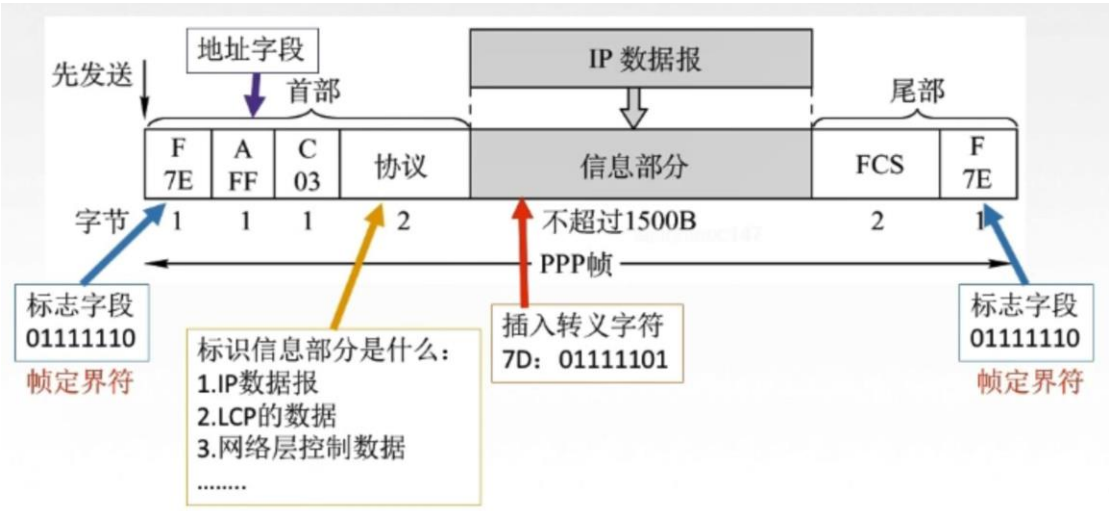
802.11 的 MAC 帧头格式

功能	To DS	From DS	Address1（接收端）	Address2（发送端）	Address3	Address4
IBSS	0	0	DA	SA	BSSID	未使用
To AP（基础结构型）	1	0	BSSID	SA	DA	未使用
From AP（基础结构型）	0	1	DA	BSSID	SA	未使用
WDS（无线分布式系统）	1	1	RA	TA	DA	SA

PPP 协议状态图：



PPP 帧：



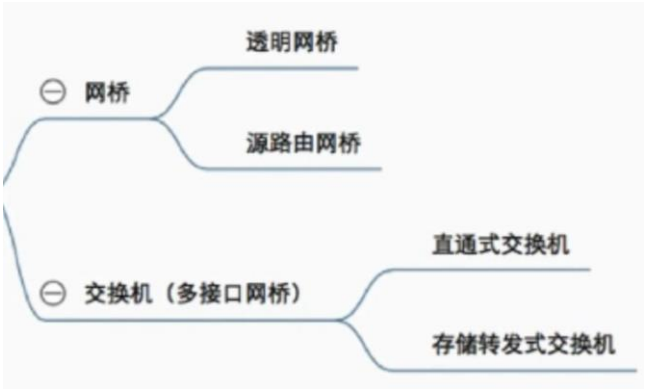
PPP&HDLC：

PPP协议	面向字节	2B协议字段	无序号和确认机制	不可靠
HDLC协议	面向比特	没有	有编号和确认机制	可靠

冲突域与广播域：

	能否隔离冲突域	能否隔离广播域
物理层设备【傻瓜】（中继器、集线器）	×	×
链路层设备【路人】（网桥、交换机）	√	×
网络层设备【大佬】（路由器）	√	√

网桥与交换机：



开环控制系统：系统的输出端和输入端之间不存在反馈回路，输出量对控制作用没有影响。

闭环控制系统：反馈控制系统，输出量对控制作用有直接影响。

IP 数据报：

标识：同一数据报的分片使用同一标识。

标志：只有2位有意义 x __

中间位DF（Don't Fragment）：
DF=1，禁止分片
DF=0，允许分片

最低位MF （More Fragment）：
MF=1，后面“还有分片”
MF=0，代表最后一片/没分片

片偏移：指出较长分组分片后，某片在原分组中的相对位置。
以8B位单位。

IP 地址：

特殊 IP 地址：

NetID 网络号	HostID主机号	作为IP分组源地址	作为IP分组目的地址	用途
全0	全0	可以	不可以	本网范围内表示主机，路由表中用于表示默认路由（表示整个Internet网络）
全0	特定值	不可以	可以	表示本网内某个特定主机
全1	全1	不可以	可以	本网广播地址（路由器不转发）
特定值	全0	不可以	不可以	网络地址，表示一个网络
特定值	全1	不可以	可以	直接广播地址，对特定网络上的所有主机进行广播
127	任何数（非全0/1）	可以	可以	用于本地软件换回测试，称为环回地址

私有 IP 地址：

地址类别	地址范围	网段个数
A类	10.0.0.0~10.255.255.255	1
B类	172.16.0.0~172.31.255.255	16
C类	192.168.0.0~192.168.255.255	256

分类的 IP 地址：

网络类别	最大可用网络数	第一个可用的网络号	最后一个可用的网络号	每个网络中的最大主机数
A	2^7-2	1	126	2^{24}-2
B	2^{14}-1	128.1	191.255	2^{16}-2
C	2^{21}-1	192.0.1	223.255.255	2^8-2

DHCP：

动态主机配置协议DHCP是**应用层**协议，使用**客户/服务器**方式，客户端和服务端通过**广播**方式进行交互，基于**UDP**。

DHCP提供**即插即用**联网的机制，主机可以从服务器动态获取IP地址、子网掩码、默认网关、DNS服务器名称与IP地址，允许**地址重用**，支持**移动用户加入网络**，支持**在用地址续租**。

1.主机广播DHCP**发现**报文　“有没有DHCP服务器呀？”　试图找到网络中的服务器，服务器获得一个IP地址。

2.DHCP服务器广播DHCP**提供**报文　“有！”“有！”“有！”　服务器拟分配给主机一个IP地址及相关配置，先到先得。

3.主机广播DHCP**请求**报文　“我用你给我的IP地址啦？”　主机向服务器请求提供IP地址。

4.DHCP服务器广播DHCP**确认**报文　“用吧！”　正式将IP地址分配给主机。

ICMP 差错报告报文：

1.终点不可达：当路由器或主机不能交付数据报时就向源点发送终点不可达报文。
无法交付

2.[illegible]：当路由器或主机由于拥塞而丢弃数据报时，就向源点发送源点抑制报文，使源点知道应当把数据报的发送速率放慢。拥塞丢数据

3.时间超过：当路由器收到生存时间TTL=0的数据报时，除丢弃该数据报外，还要向源点发送时间超过报文。当终点在预先规定的时间内不能收到一个数据报的全部数据报片时，就把已收到的数据报片都丢弃，并向源点发送时间超过报文。　TTL=0

4.参数问题：当路由器或目的主机收到的数据报的首部中有的字段的值不正确时，就丢弃该数据报，并向源点发送参数问题报文。　首部字段有问题

5.改变路由（重定向）：路由器把改变路由报文发送给主机，让主机知道下次应将数据报发送给另外的路由器（可通过更好的路由）。　值得更好的路由

1.对**ICMP差错报告报文**不再发送ICMP差错报告报文。

2.对第一个分片的数据报片的所有**后续数据报片**都不发送ICMP差错报告报文。

3.对具有**组播地址**的数据报都不发送ICMP差错报告报文。

4.对具有**特殊地址**（如127.0.0.0或0.0.0.0）的数据报不发送ICMP差错报告报文。

IPv6：

1.IPv6将地址从32位（4B）扩大到**128位（16B）**，更大的地址空间。
2.IPv6将IPv4的**校验和字段彻底移除**，以减少每跳的处理时间。
3.IPv6将IPv4的可选字段移出首部，变成了**扩展首部**，成为灵活的首部格式，路由器通常不对扩展首部进行检查，大大提高了路由器的处理效率。
4.IPv6支持**即插即用**（即自动配置），不需要DHCP协议。
5.IPv6首部长度必须是**8B的整数倍**，IPv4首部是4B的整数倍。
6.IPv6**只能在主机处分片**，IPv4可以在路由器和主机处分片。
7.ICMPv6：附加报文类型“分组过大”。
8. IPv6支持资源的预分配， 支持实时视像等要求，保证一定的带宽和时延的应用。
9.IPv6取消了协议字段，改成下一个首部字段。
10.IPv6取消了总长度字段，改用有效载荷长度字段。
11.IPv6取消了服务类型字段。

IPv4 向 IPv6 过渡：

双栈协议　双协议栈技术就是指在一台设备上**同时启用IPv4协议栈和IPv6协议栈**。这样的话，这台设备既能和IPv4网络通信，又能和IPv6网络通信。如果这台设备是一个路由器，那么这台路由器的不同接口上，分别配置了IPv4地址和IPv6地址，并很可能分别连接了IPv4网络和IPv6网络。如果这台设备是一个计算机，那么它将同时拥有IPv4地址和IPv6地址，并具备同时处理这两个协议地址的功能。

隧道技术　通过使用互联网络的基础设施在网络之间传递数据的方式。使用隧道传递的数据（或负载）可以是不同协议的数据帧或包。隧道协议将其它协议的数据帧或包**重新封装**然后通过隧道发送。

BGP 报文：

1.OPEN（打开）报文：用来与相邻的另一个BGP发言人建立关系，并认证发送方。

2.UPDATE（更新）报文：通告新路径或撤销原路径。

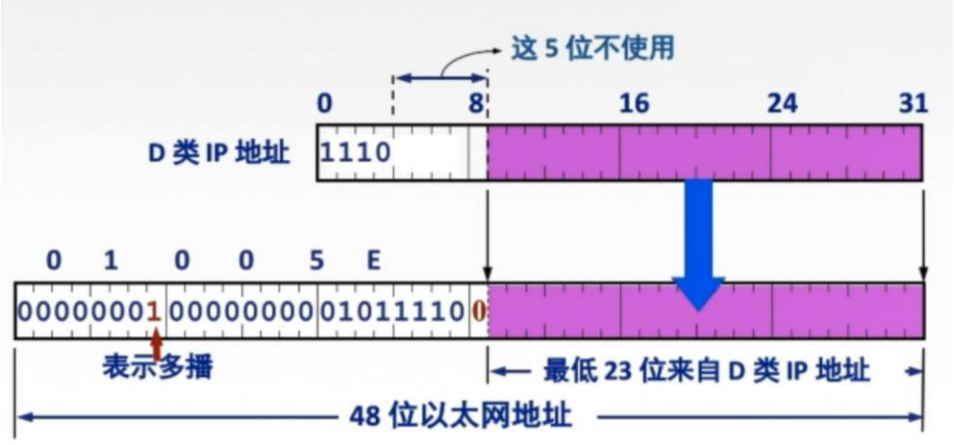
3.KEEPALIVE（保活）报文：在无UPDATE时，周期性证实邻站的连通性；也作为OPEN的确认。

4.NOTIFICATION（通知）报文：报告先前报文的差错；也被用于关闭连接。

三种路由选择协议：

协议	RIP	OSPF	BGP	
类型	内部	内部	外部	
路由算法	距离-向量	链路状态	路径-向量	
传递协议	UDP	IP	TCP	
路径选择	跳数最少	代价最低	较好，非最佳	
交换结点	和本结点相邻的路由器	网络中的所有路由器	和本结点相邻的路由器	
交换内容	当前本路由器知道的全部信息，即自己的路由表	与本路由器相邻的所有路由器的链路状态	首次	整个路由表
			非首次	有变化的部分

多播 MAC 地址：



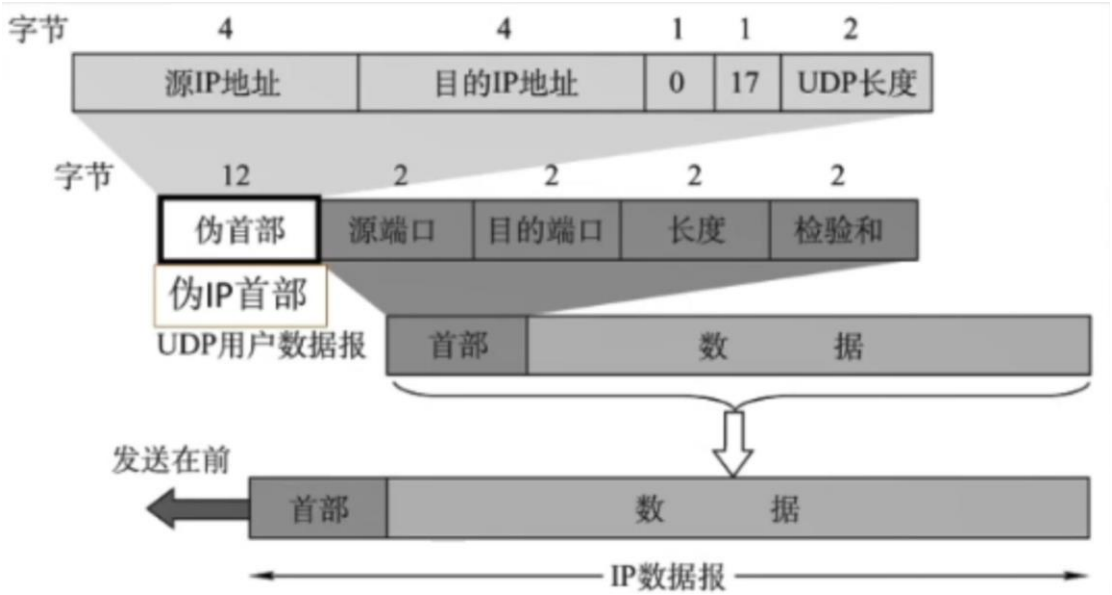
组播路由选择协议：

组播路由协议目的是找出以源主机为根节点的**组播转发树**。

构造树可以避免在路由器之间兜圈子。

对不同的多播组对应于不同的多播转发树；同一个多播组，对不同的源点也会有不同的多播转发树。

UDP：



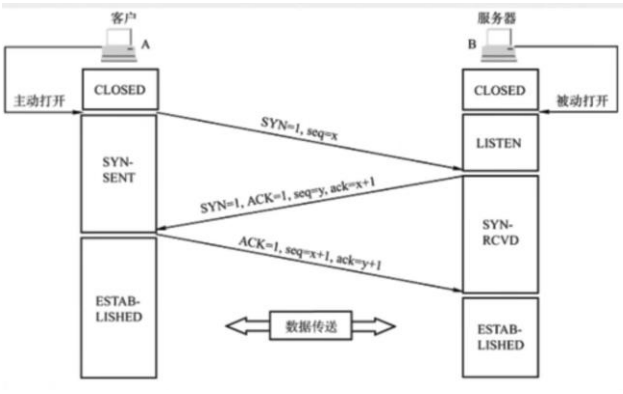
TCP：

序号：在一个TCP连接中传送的字节流中的每一个字节都按顺序编号，本字段表示本报文段所发送数据的**第一个字节的序号**。

确认号：**期望**收到对方下一个报文段的第一个数据字节的序号。若确认号为N，则证明到序号N-1为止的所有数据都已正确收到。

数据偏移（**首部长度**）：TCP报文段的数据起始处距离TCP报文段的起始处有多远，以4B位单位，即1个数值是4B。

TCP 建立连接：



ROUND 1:

客户端发送**连接请求报文段**，无应用层数据。

SYN=1，seq=x(随机)

ROUND 2:

服务器端为该TCP连接**分配缓存和变量**，并向客户端返回**确认报文段**，允许连接，无应用层数据。

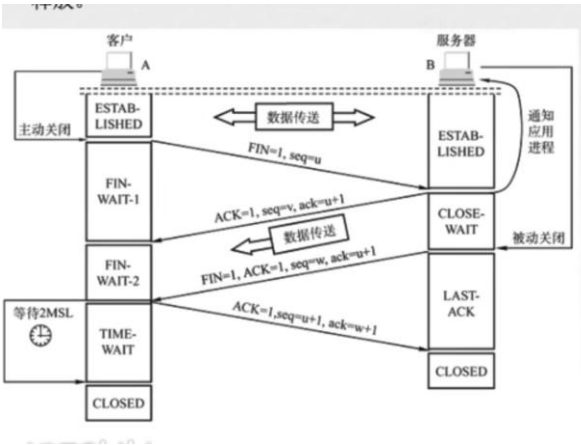
SYN=1，ACK=1，seq=y(随机)，ack=x+1

ROUND 3:

客户端为该TCP连接**分配缓存和变量**，并向服务器端返回确认的确认，可以携带数据。

SYN=0，ACK=1，seq=x+1，ack=y+1

TCP 释放连接：



ROUND 1:

客户端发送**连接释放报文段**，停止发送数据，主动关闭TCP连接。

FIN=1，seq=u

ROUND 2:

服务器端回送一个确认报文段，客户到服务器这个方向的连接就释放了——半关闭状态。

ACK=1，seq=v，ack=u+1

ROUND 3:

服务器端发完数据，就发出连接释放报文段，主动关闭TCP连接。

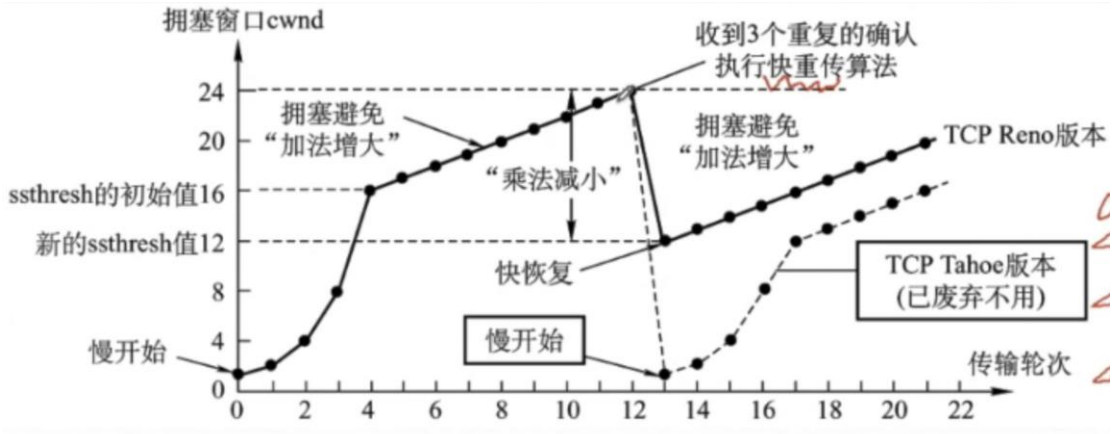
FIN=1，ACK=1，seq=w，ack=u+1

ROUND 4:

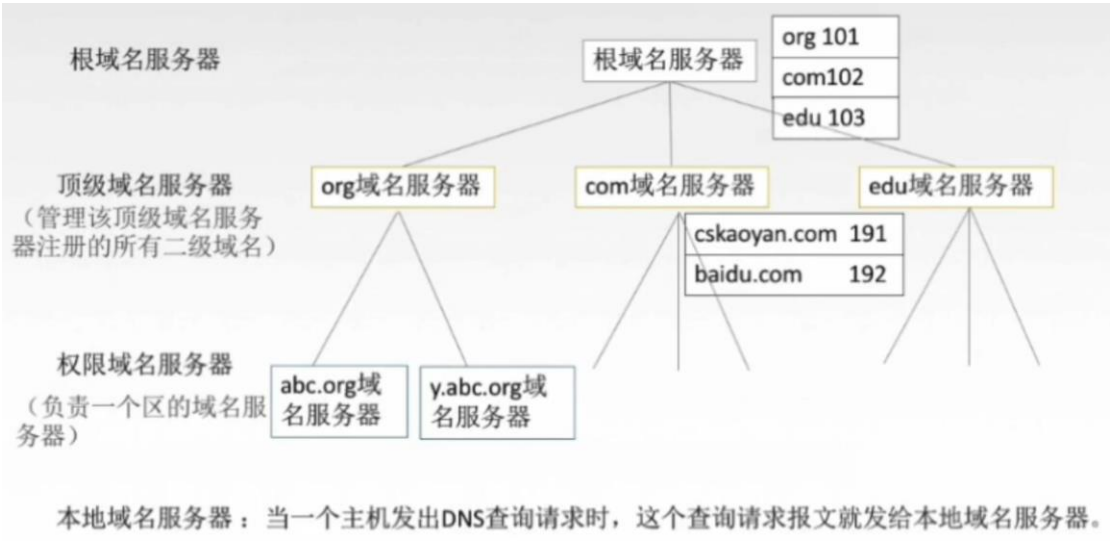
客户端回送一个确认报文段，再等到时间等待计时器设置的2MSL（最长报文段寿命）后，连接彻底关闭。

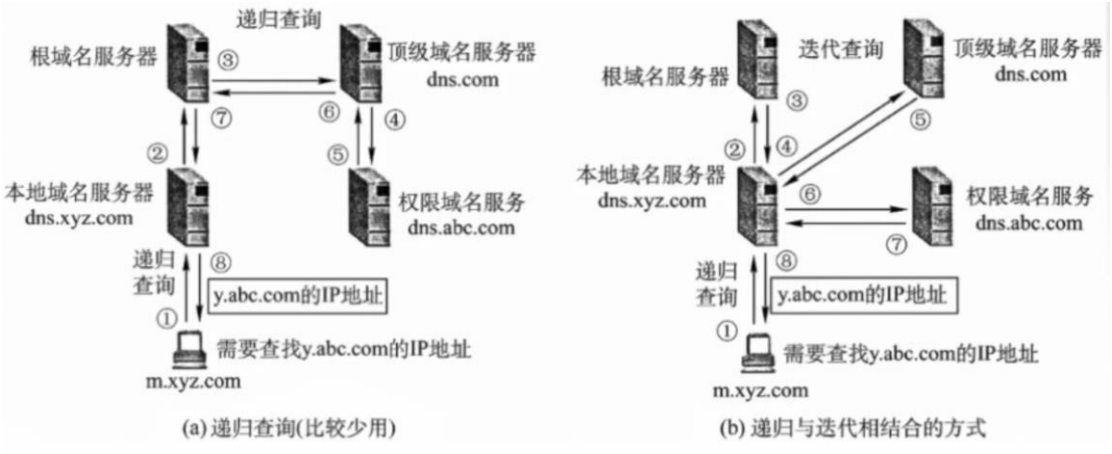
ACK=1，seq=u+1，ack=w+1

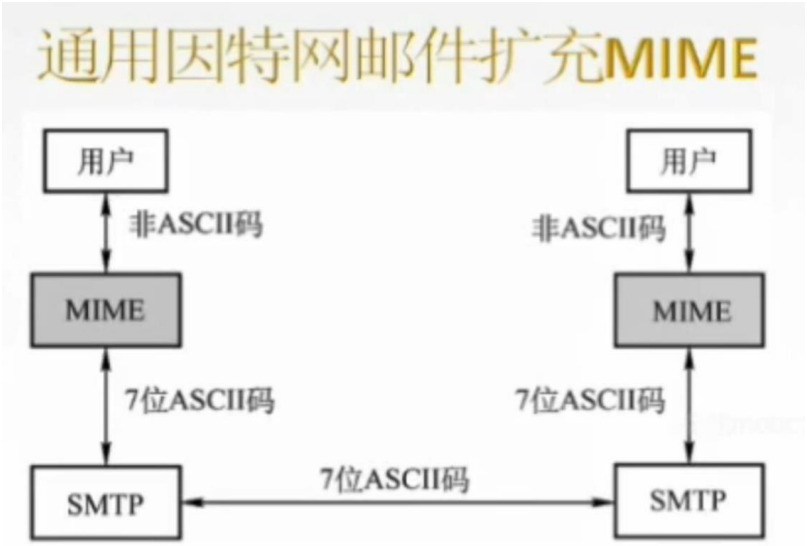
TCP 传输：



域名服务器：


根域名服务器
根域名服务器
org 101
com102
edu 103
顶级域名服务器
（管理该顶级域名服务器注册的所有二级域名）
org域名服务器
com域名服务器
edu域名服务器
cskaoyan.com 191
baidu.com 192
权限域名服务器
（负责一个区的域名服务器）
abc.org域名服务器
y.abc.org域名服务器
本地域名服务器：当一个主机发出DNS查询请求时，这个查询请求报文就发给本地域名服务器。

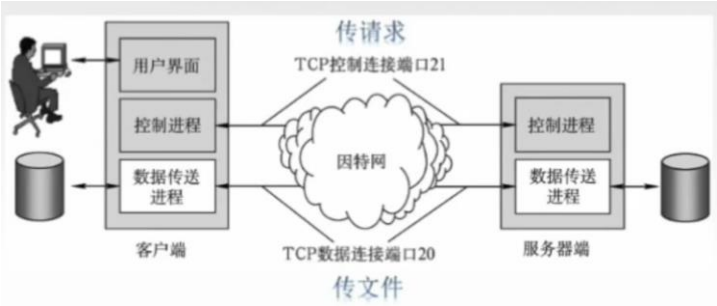

递归查询
根域名服务器
顶级域名服务器
dns.com
本地域名服务器
dns.xyz.com
权限域名服务
dns.abc.com
递归查询
y.abc.com的IP地址
需要查找y.abc.com的IP地址
m.xyz.com
(a) 递归查询(比较少用)
迭代查询
根域名服务器
顶级域名服务器
dns.com
本地域名服务器
dns.xyz.com
权限域名服务
dns.abc.com
递归查询
y.abc.com的IP地址
需要查找y.abc.com的IP地址
m.xyz.com
(b) 递归与迭代相结合的方式


通用因特网邮件扩充MIME
用户
非ASCII码
MIME
7位ASCII码
SMTP
用户
非ASCII码
MIME
7位ASCII码
SMTP
7位ASCII码

IMAP协议比POP协议复杂。当用户Pc上的IMAP客户程序打开IMAP服务器的邮箱时，用户可以看到邮箱的首部，若用户需要打开某个邮件，该邮件才上传到用户的计算机上。

IMAP可以让用户在不同的地方使用不同的计算机随时上网阅读处理邮件，还允许只读取邮件中的某一个部分（先看正文，有WiFi的时候再下载附件）。

HTTP采用**TCP**作为运输层协议，但**HTTP协议本身是无连接**的（通信双方在交换HTTP报文之前不需要先建立HTTP连接）。



控制连接始终保持

数据连接保持一会

是否使用TCP 20端口建立**数据连接**与**传输模式**有关

主动方式使用TCP 20端口

被动方式由服务器和客户端自行协商决定（端口>1024）