2020年7月29日 13:41

《计算机网络》

一、概述

ISP 互联网服务供应商

IXP 互联网交换点

C/S 方式 Client Server

P2P方式 Peer-to-Peer

电路交换 报文交换 分组交换

速率

带宽 最高数据率 bit/s

吞吐量 实际数据量

时延 delay/latency

发送时延 数据发送时间

$$发送时延 = \frac{数据帧长度\ (bit)}{发送速率\ (bit/s)}$$

传播时延 数据传播时间

$$传播时延 = \frac{信道长度(m)}{电磁波在信道上的传播速率(m/s)}$$

处理时延

排队时延

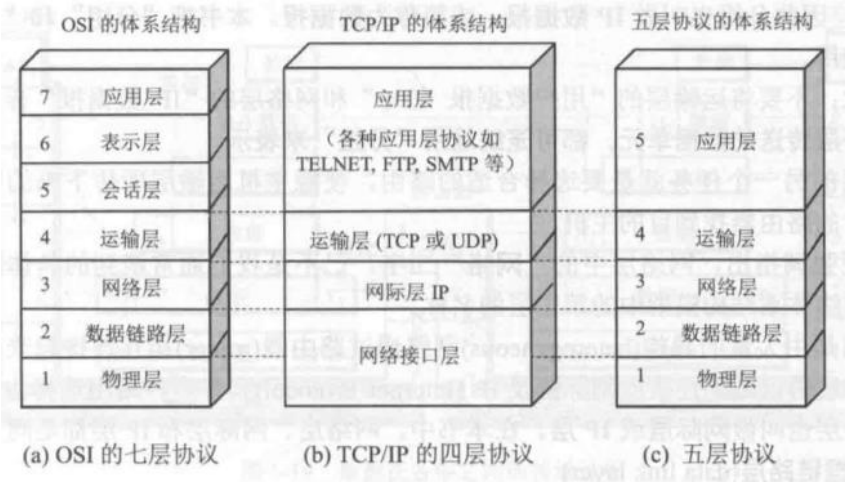
加起来就是总时延

时延带宽积 以bit为单位我的链路长度

往返时间 RTT

利用率

1. 协议体系结构



应用层 应用进程间通信和交互的规则 DNS HTTP SMTP 报文message

运输层 提供数据传输服务 UDP TCP

网络层 不同主机间通信服务 IP

链路层 组装成帧 控制信息（同步信息，地址信息，差错控制）

物理层 比特 01

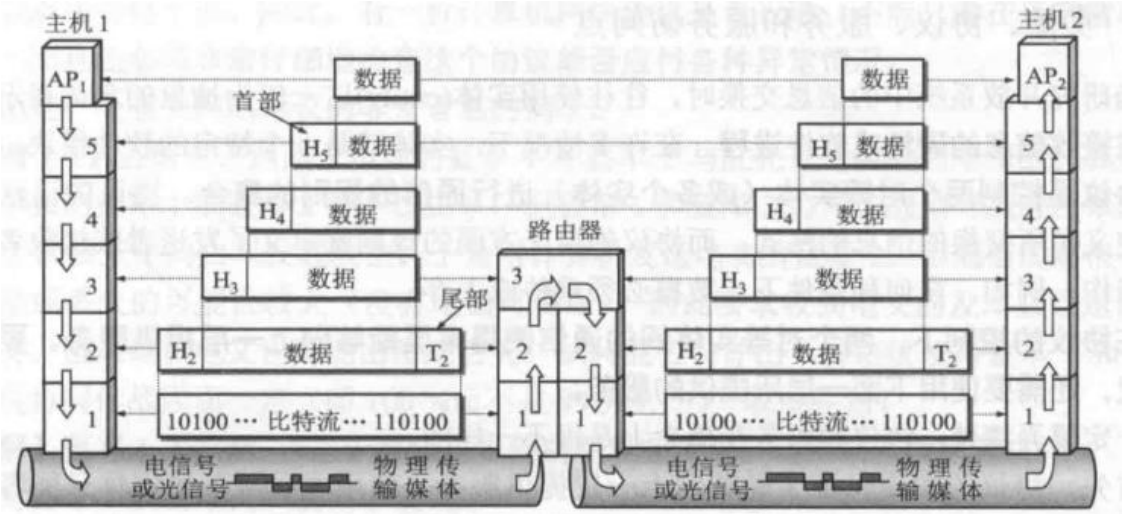


图 1-19 数据在各层之间的传递过程

协议水平，服务竖直

二、物理层

1. 物理层协议 物理层规程procedure

   串行传输

2. 数据通信系统

   源系统/发送端 传输系统 目的系统/接收方

   源系统： 源点 发送器 接收器 终点

3. 单向通信/单工通道 双向交替通信/半双工通道 双向同时通信/全双工通道

   基带信号 调制 基带调制 编码

   载波 带通信号 带通调制

4. 编码方式

   不归零制 归零制 曼彻斯特编码（自同步能力） 差分曼彻斯特编码

5. 奈奎斯特准则，信道传输频率上限

   $f_s > 2 * f_N$

   信噪比

   $$\text{信噪比(dB)} = 10 \log_{10}(S/N) \text{ (dB)}$$

   香农公式

   在 1948 年，信息论的创始人香农(Shannon)推导出了著名的**香农公式**。香农公式指出：**信道的极限信息传输速率** C 是

   $$C = W \log_2(1+S/N) \text{ (bit/s)} \quad (2\text{-}2)$$

   式中，W 为信道的带宽（以 Hz 为单位）；S 为信道内所传信号的平均功率；N 为信道内部的高斯噪声功率。香农公式的推导可在通信原理教科书中找到。这里只给出其结果。

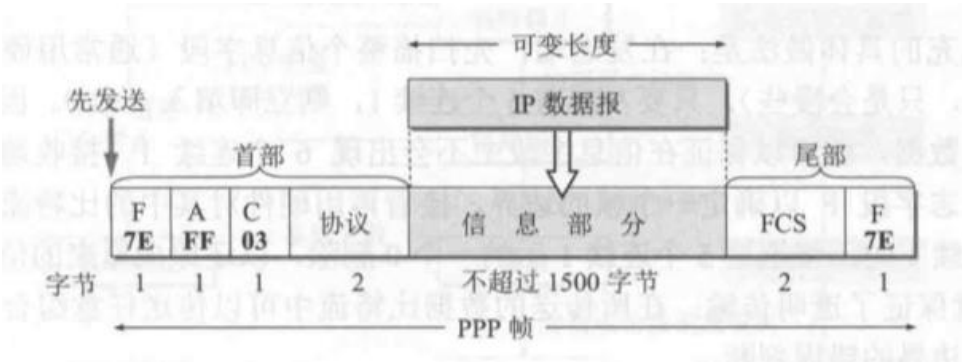
   信道的带宽或者信噪比越大，信息的极限传输速率就越高

6. 传输媒介 双绞线 同轴电缆 光缆

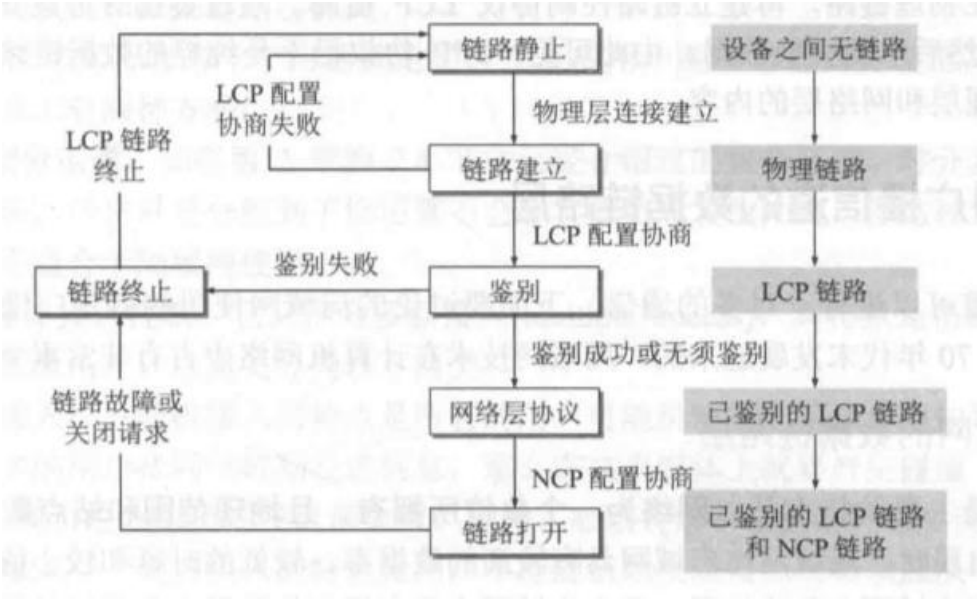
7. 信道复用技术
   频分复用 FDM
   时分复用 TDM 等时信号
   统计时分复用 STDM 异步时分复用
   波分复用 光的频分复用
   码分复用 CDM 码分多址 CDMA 码片序列正交 伪随机码序列

三、链路层

1. 点对点信道
   广播信道
2. 帧 网络层交下来的数据构成帧
   封装成帧 framing 最大传送单元MTU 控制字符 SOH EOT
   透明传输 传输帧中 SOH EOT 进行转义操作
   差错检测 误码率 Bit Error Rate 循环冗余检验 CRC 帧检测序列FCS Frame Check Sequence
   无差错接收！=可靠传输
   帧丢失 帧重复 帧失序 通过上层，例如运输层的TCP协议完成
3. 点对点协议 PPP



   F 标志位 进制
   A 规定为0xFF
   C 规定为0x03
   第四个 两个字节的协议字段
   尾部的第一个字段（2字节）是使用CRC的FCS
   字节填充 转义字符 信息字段修改出现的标志字段 异步传输
   零比特填充 五个连续的1就加个0 转义
4. PPP协议状态图



鉴别 Authenticate

口令鉴别协议 PAP

口令握手鉴别协议 CHAP

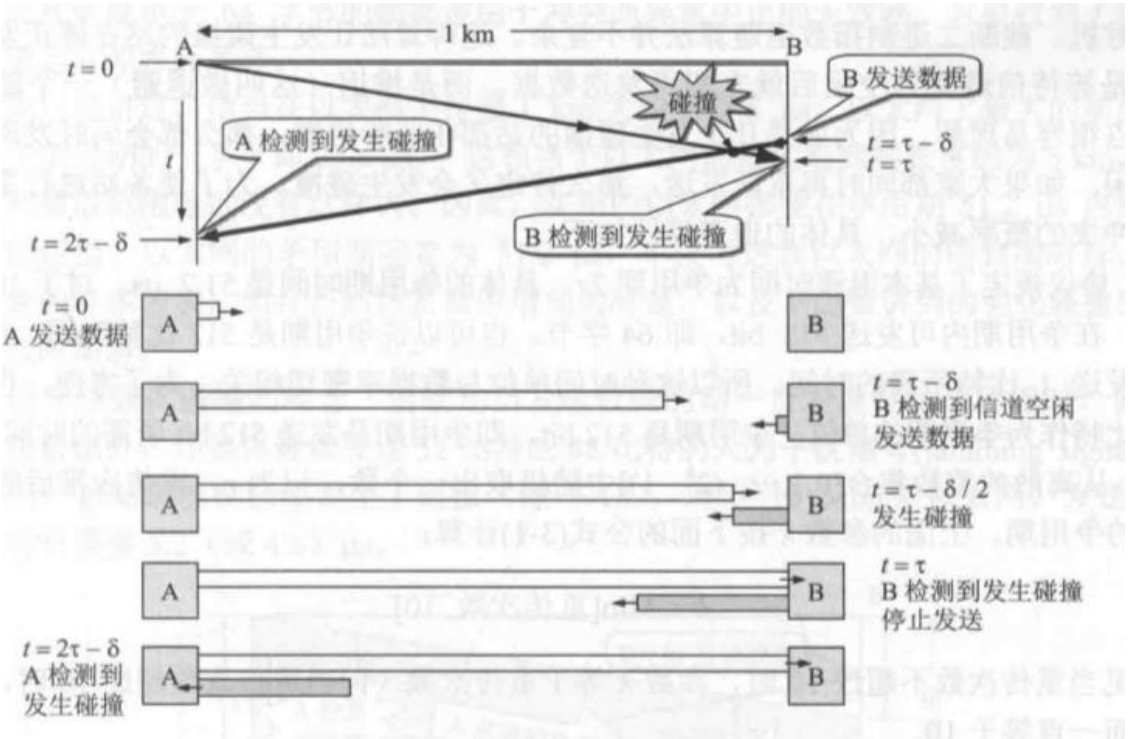
5. 广播信道的链路层

CSMA/CD协议 载波监听多点接入/碰撞检测

多点接入 总线型网络

载波监听 发送前发送中都在检测信道

碰撞检测 边发送边监听



不能同时发送或者接收，双向交替通信/半双工通信

截断而二进制指数退避

争用期为512bit

$$k = \text{Min}[\text{重传次数}, 10] \tag{3-1}$$

可见当重传次数不超过 10 时，参数 k 等于重传次数；但当重传次数超过 10 时，k 就不再增大而一直等于 10。

(3) 当重传达 16 次仍不能成功时（这表明同时打算发送数据的站太多，以致连续发生冲突），则丢弃该帧，并向高层报告。

使重传需要推迟的平均时间随着重传次数而增大 动态退避

人为干扰信号

根据以上所讨论的，可以把 CSMA/CD 协议的要点归纳如下：

(1) 准备发送：适配器从网络层获得一个分组，加上以太网的首部和尾部（见后面的 3.4.3 节），组成以太网帧，放入适配器的缓存中。但在发送之前，必须**先检测信道**。

(2) 检测信道：若检测到信道忙，则应不停地检测，一直等待信道转为空闲。若检测到信道空闲，并在 96 比特时间内信道保持空闲（保证了帧间最小间隔），就发送这个帧。

(3) 在发送过程中仍不停地检测信道，即网络适配器要**边发送边监听**。这里只有两种可能性：

①发送成功：在争用期内一直未检测到碰撞。这个帧肯定能够发送成功。发送完毕后，其他什么也不做。然后回到(1)。

②发送失败：在争用期内检测到碰撞。这时立即停止发送数据，并按规定发送人为干扰信号。适配器接着就执行指数退避算法，等待 r 倍 512 比特时间后，返回到步骤(2)，继续检测信道。但若重传达 16 次仍不能成功，则停止重传而向上报错。

以太网每发送完一帧，一定要把已发送的帧暂时保留一下。如果在争用期内检测出发生了碰撞，那么还要在推迟一段时间后再把这个暂时保留的帧重传一次。

6. 集线器工作在物理层

从图 3-21 可看出，要提高以太网的信道利用率，就必须减小 τ 与 T_0 之比。在以太网中定义了参数 a，它是以太网**单程端到端时延** τ 与**帧的发送时间** T_0 之比：

$$a = \frac{\tau}{T_0} \tag{3-2}$$

7.

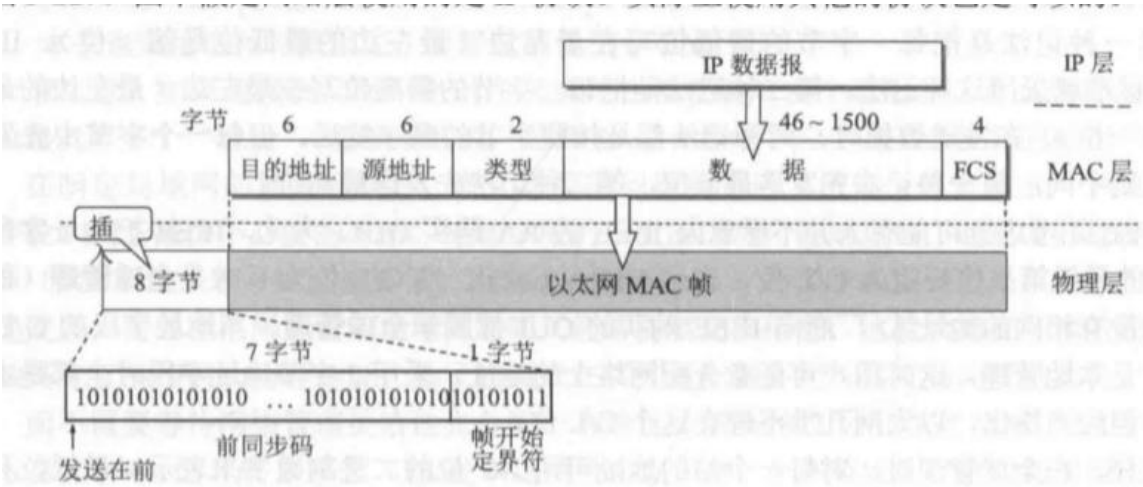
当 $a \to 0$ 时，表示只要一发生碰撞，就立即可以检测出来，并立即停止发送，因而信道资源被浪费的时间非常非常少。反之，参数 a 越大，表明争用期所占的比例越大，这就使得每发生一次碰撞就浪费了不少的信道资源，使得信道利用率明显降低。因此，以太网的**参数**

使得单程传播时间尽可能的短

极限信道利用率

$$S_{\max} = \frac{T_0}{T_0 + \tau} = \frac{1}{1 + a}$$

8. MAC层 硬件地址/物理地址



无效MAC帧

IEEE 802.3 标准规定凡出现下列情况之一的即为无效的 MAC 帧：

(1) 帧的长度不是整数个字节；

(2) 用收到的帧检验序列 FCS 查出有差错；

(3) 收到的帧的 MAC 客户数据字段的长度不在 46 ~ 1500 字节之间。考虑到 MAC 帧首部和尾部的长度共有 18 字节，可以得出有效的 MAC 帧长度为 64 ~ 1518 字节之间。

对于检查出的无效 MAC 帧就简单地丢弃。以太网不负责重传丢弃的帧。

9. 交换机工作在链路层

   交换表 生成树协议 STP 记录MAC地址和端口

10. VLAN 虚拟局域网 利用VLAN标记 增加了四个字节

四、网络层

1. 网络层不提供服务质量的承诺

   网际协议IP

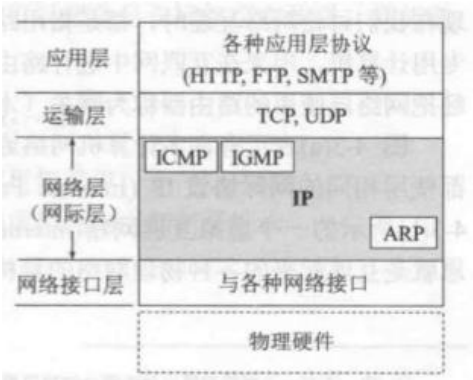


图 4-2 网际协议 IP 及其配套协议

- **地址解析协议 ARP** (Address Resolution Protocol)
- **网际控制报文协议 ICMP** (Internet Control Message Protocol)
- **网际组管理协议 IGMP** (Internet Group Management Protocol)

2. 中间设备

(1) 物理层使用的中间设备叫做**转发器**(repeater)。

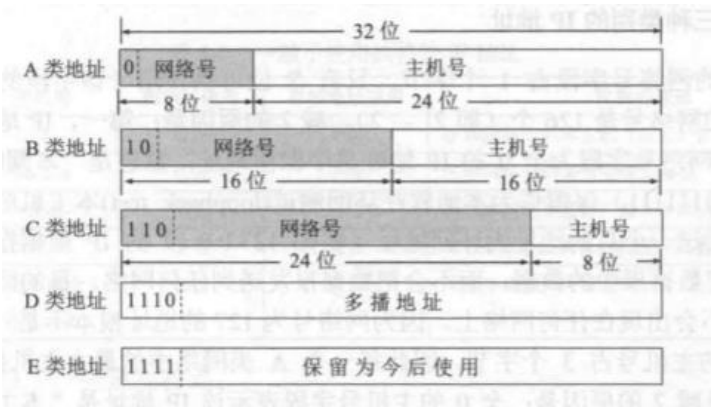
(2) 数据链路层使用的中间设备叫做**网桥**或**桥接器**(bridge)。

(3) 网络层使用的中间设备叫做**路由器**(router)[①]。

(4) 在网络层以上使用的中间设备叫做**网关**(gateway)。用网关连接两个不兼容的系统需要在高层进行协议的转换。

互联网可以由多种异构网络互联而成

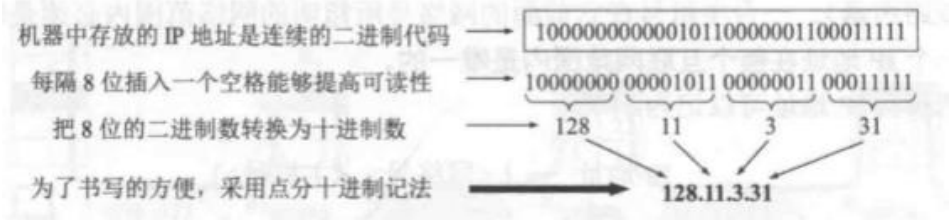
3. IP地址



A、B、C都为单播地址

D类地址用于多播

点分十进制记法



4. 常用网络IP

A类网络 7位： 126个

全0 this 本网络

127 环回测试

B类中 128.0.0.0不使用

C类中 192.0.0.0不使用

网络类别	最大可指派的网络数	第一个可指派的网络号	最后一个可指派的网络号	每个网络中的最大主机数
A	126 (2^7-2)	1	126	16777214
B	16383 ($2^{14}-1$)	128.1	191.255	65534
C	2097151 ($2^{21}-1$)	192.0.1	223.255.255	254

不使用网络

网络号	主机号	源地址使用	目的地址使用	代表的意思
0	0	可以	不可	在本网络上的本主机（见 6.6 节 DHCP 协议）
0	host-id	可以	不可	在本网络上的某台主机 host-id
全 1	全 1	不可	可以	只在本网络上进行广播（各路由器均不转发）
net-id	全 1	不可	可以	对 net-id 上的所有主机进行广播
127	非全 0 或全 1 的任何数	可以	可以	用于本地软件环回测试

5. IP地址和MAC地址区别

IP层上只能看到IP数据报

路由器只根据目的站的IP地址的网络号进行路由选择

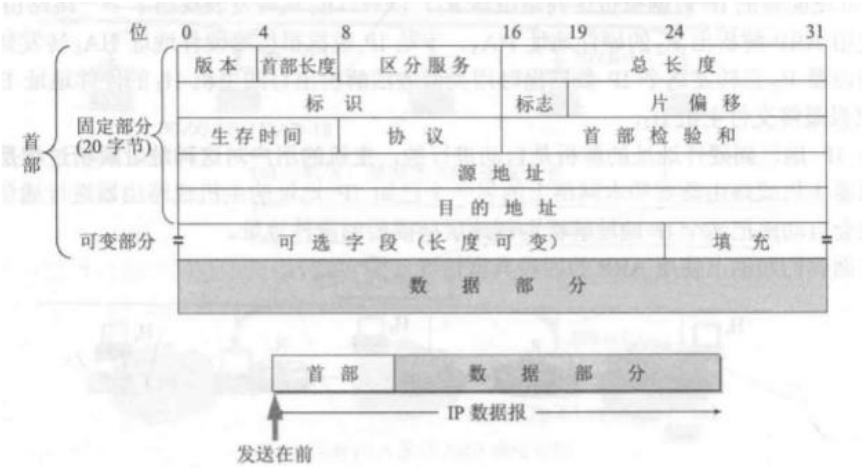
局域网的链路层，只能看见MAC帧

6. ARP协议 地址解析协议

构建IP到硬件地址的映射

（因为硬件地址多种多样，所以进行IP编址简化

7. IP数据报



版本 4位

首部长度 4位

区分服务 8位

总长度 16位 最大长度为2^16-1 字节

MTU 最大传送单元 以太网规定MTU为1500字节 分片处理

总长度为 分片后每个分片首部长度与该分片数据长度的总和

标识 16位 每产生一个数据报 计数器+1

标志 3位 后两位有意义

最低位MF MF=1 表示后面还有分片 MF=0表示是最后一个

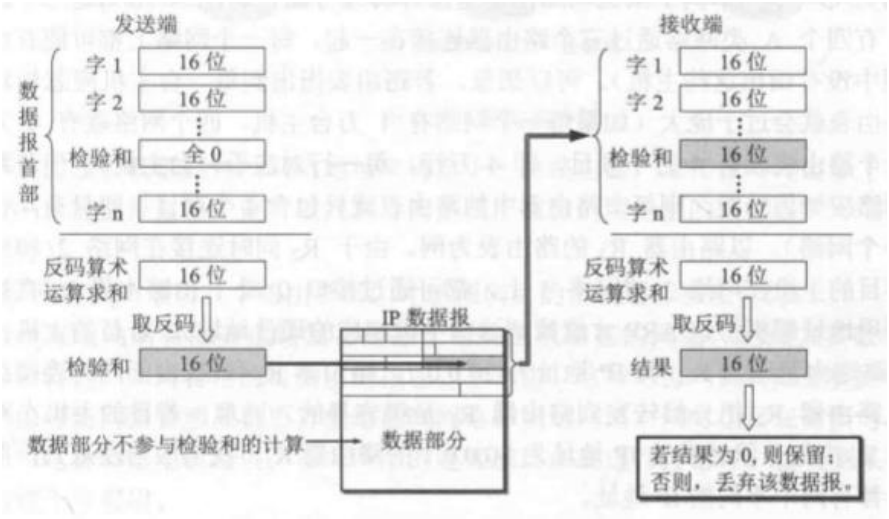
中间位DF DF=1 不能分片 反之亦然

片位移 13位 分片后某片的相对位置 8个字节为偏移单位 所以分片长度一定是8字节整数倍

生存时间 8位 TTL 转发一次就是一跳 跳数限制 最大255

协议 8位

首部检验和 16位 只检验数据报首部 不包括数据部分 每路过一个路由器重新计算



源地址 32位

目的地址 32位

可变部分 1-40字节 增加功能 在IPv6中首部长度固定

8. 分组转发流程

路由器表：（目的网络地址，下一跳地址）

特定主机路由

默认路由（只要是其他网络就发送）

分组转发算法

(1) 从数据报的首部提取目的主机的 IP 地址 D，得出目的网络地址为 N。

(2) 若 N 就是与此路由器直接相连的某个网络地址，则进行**直接交付**，不需要再经过其他的路由器，直接把数据报交付目的主机（这里包括把目的主机地址 D 转换为具体的硬件地址，把数据报封装为 MAC 帧，再发送此帧）；否则就是间接交付，执行(3)。

(3) 若路由表中有目的地址为 D 的特定主机路由，则把数据报传送给路由表中所指明的下一跳路由器；否则，执行(4)。

(4) 若路由表中有到达网络 N 的路由，则把数据报传送给路由表中所指明的下一跳路由器；否则，执行(5)。

(5) 若路由表中有一个默认路由，则把数据报传送给路由表中所指明的默认路由器；否则，执行(6)。

(6) 报告转发分组出错。

9. 子网划分

{<网络号>,<子网号>,<主机号>}

子网掩码 逐位与 AND

子网分组转发

目的网络地址、子网掩码、下一跳地址

(1) 从收到的数据报的首部提取目的 IP 地址 D。

(2) 先判断是否为直接交付。对路由器直接相连的网络逐个进行检查：用各网络的子网掩码和 D 逐位相“与”（AND 操作），看结果是否和相应的网络地址匹配。若匹配，则把分组进行直接交付（当然还需要把 D 转换成物理地址，把数据报封装成帧发送出去），转发任务结束。否则就是间接交付，执行(3)。

(3) 若路由表中有目的地址为 D 的特定主机路由，则把数据报传送给路由表中所指明的下一跳路由器；否则，执行(4)。

(4) 对路由表中的每一行（目的网络地址，子网掩码，下一跳地址），用其中的子网掩码和 D 逐位相“与”（AND 操作），其结果为 N。若 N 与该行的目的网络地址匹配，则把数据报传送给该行指明的下一跳路由器；否则，执行(5)。

(5) 若路由表中有一个默认路由，则把数据报传送给路由表中所指明的默认路由器；否则，执行(6)。

(6) 报告转发分组出错。

10. 无分类编址CIDR

消除ABC类地址和划分子网的概念 使用网络前缀 无分类两级编址

{<网络前缀>,<主机号>}

斜线记法

128.14.35.7/20 = **10000000 00001110 0010**0011 00000111

网络前缀相同的最为CIDR地址块

32位地址掩码

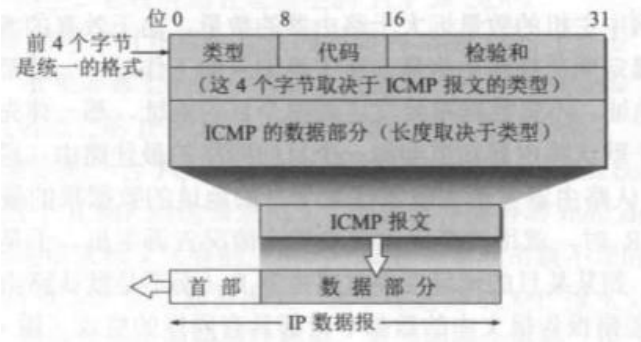
路由聚合 构成超网

最长前缀匹配 在路由匹配中选择具有最长网络前缀的路由

11. 路由表查找

二叉线索 先找出唯一前缀

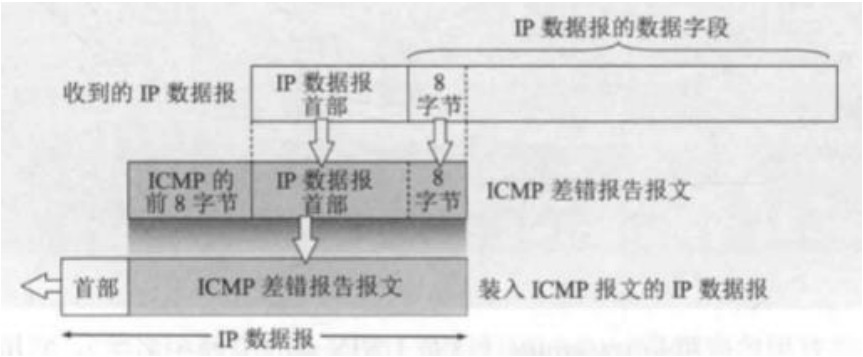
12. ICMP 网际控制报文协议



报文种类

ICMP 报文种类	类型的值	ICMP 报文的类型
差错报告报文	3	终点不可达
	11	时间超过
	12	参数问题
	5	改变路由(Redirect)
询问报文	8 或 0	回送(Echo)请求或回答
	13 或 14	时间戳(Timestamp)请求或回答

差错报文格式



不应该发送ICMP差错报文的情况

- 对 ICMP 差错报告报文，不再发送 ICMP 差错报告报文。
- 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。
- 对具有多播地址的数据报，都不发送 ICMP 差错报告报文。
- 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。

13. ICMP应用

分组网间监测PING 没有通过运输层TCP或UDP

Traceroute/Tracert 追踪路径

经过路由器数量 —— 花费时间 有关但是不绝对 因为拥塞程度随时变化

14. **路由算法选择**

静态路由选择策略 非自适应路由选择

动态路由选择策略 自适应路由选择

自治系统 AS

路由选择协议

内部网关协议IGP RIP和OSPF协议

外部网关协议EGP BGP-4 边界网关协议

域间路由选择 自治系统之间的路由选择

域内路由选择 自治系统内部的路由选择

15. 内部网关协议 RIP 实现简单 开销小

基于距离向量的路由选择协议 适用于小型互联网

距离： 跳数

1）仅和相邻路由器交换信息

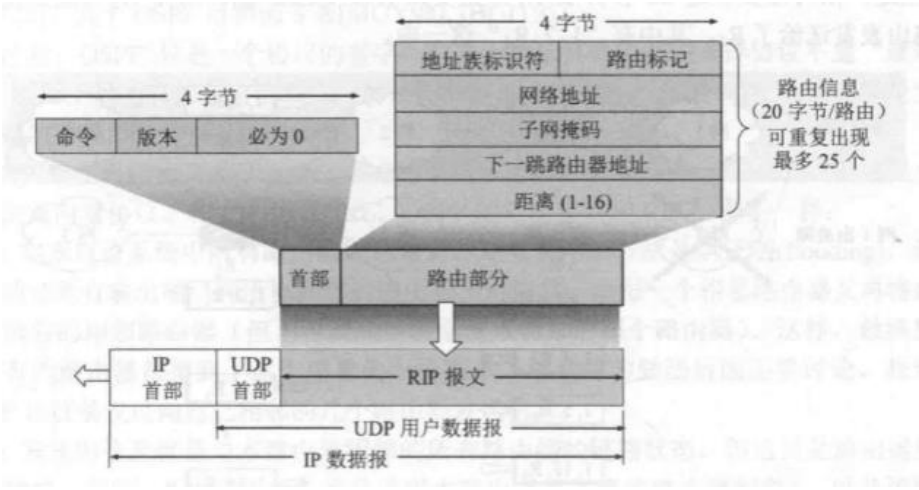
2）交换路由表 即为本路由器知道的所有信息

3）按固定时间间隔交换路由信息

距离向量算法：弗洛伊德算法

超过3min没有收到相邻路由器更新 记为不可达 距离16

报文格式



运输层 使用UDP 端口520

路由信息需要20字节

一个RIP报文最多包括25个路由

RIP最大长度为4+20*25=504字节

问题：网络出现故障 传递信息过慢

好消息传的快 坏消息传的慢

16. OSPF协议

开放最短路径优先 dijkstra

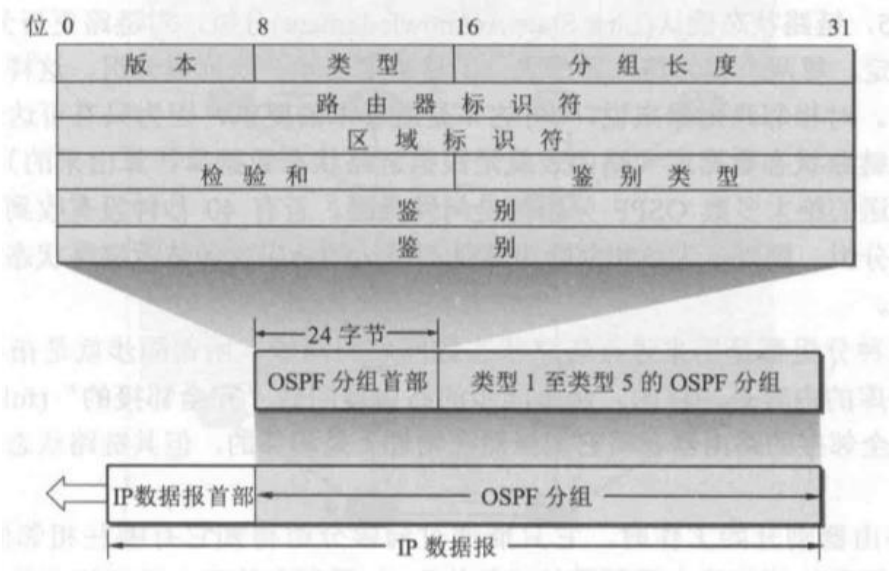
向本自治系统中所有路由器发送消息 洪泛法 flooding

发送内容就是本路由器相邻所有路由器的链路状态 度量metric

只有链路状态变化，才向所有路由器发送此消息

链路状态数据库 全网拓扑结构图 全网范围内一致（链路状态数据库的同步）

直接使用IP数据报通信



其他特点：

对于不同类型的业务可计算出不同的路由

多路径间的负载平衡

所有交换分组都存在鉴别功能

支持可变长度的子网划分和无分类编制CIDR

每条链路状态上带一个32位序号

OSPF五种分组类型：

1）问候hello分组

2）数据库描述

3）链路状态请求

4）链路状态更新

5）链路状态确认

17. 外部网关协议BGP

需要找一条比较好的路由，而不是最佳路由

路径向量路由选择协议

四种报文

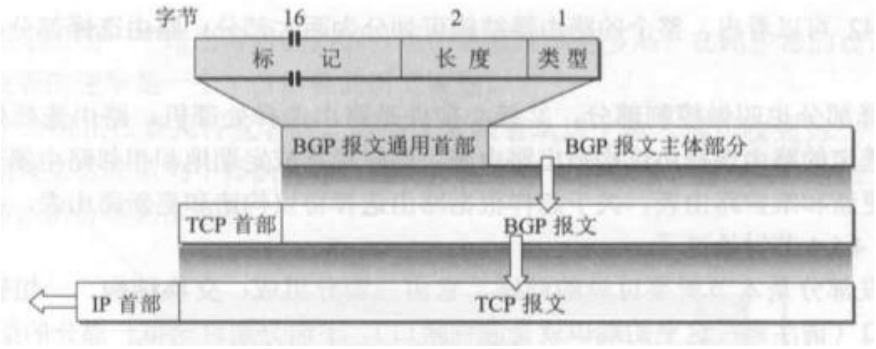
（1）OPEN（打开）报文，用来与相邻的另一个 BGP 发言人建立关系，使通信初始化。

（2）UPDATE（更新）报文，用来通告某一路由的信息，以及列出要撤销的多条路由。

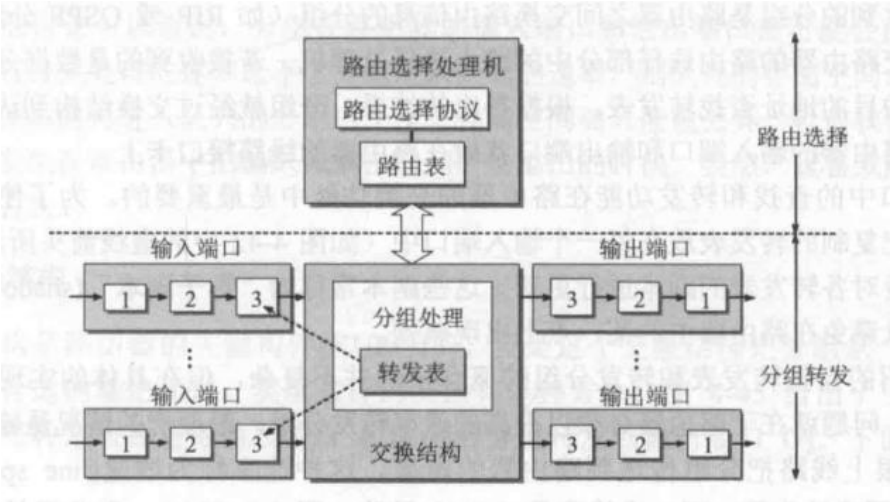
（3）KEEPALIVE（保活）报文，用来周期性地证实邻站的连通性。

（4）NOTIFICATION（通知）报文，用来发送检测到的差错。

报文格式

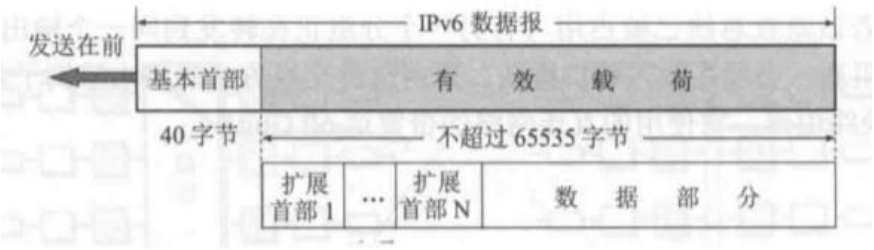


18. 路由器构成



交换结构 输入端口 输出端口

19. IPv6



相比IPv4更改

- 取消了首部长度字段，因为它的首部长度是固定的（40 字节）。
- 取消了服务类型字段，因为优先级和流标号字段实现了服务类型字段的功能。
- 取消了总长度字段，改用有效载荷长度字段。
- 取消了标识、标志和片偏移字段，因为这些功能已包含在分片扩展首部中。
- 把 TTL 字段改称为跳数限制字段，但作用是一样的（名称与作用更加一致）。
- 取消了协议字段，改用下一个首部字段。
- 取消了检验和字段，这样就加快了路由器处理数据报的速度。我们知道，在数据链路层对检测出有差错的帧就丢弃。在运输层，当使用 UDP 时，若检测出有差错的用户数据报就丢弃。当使用 TCP 时，对检测出有差错的报文段就重传，直到正确传送到目的进程为止。因此在网络层的差错检测可以精简掉。
- 取消了选项字段，而用扩展首部来实现选项功能。

数据报结构

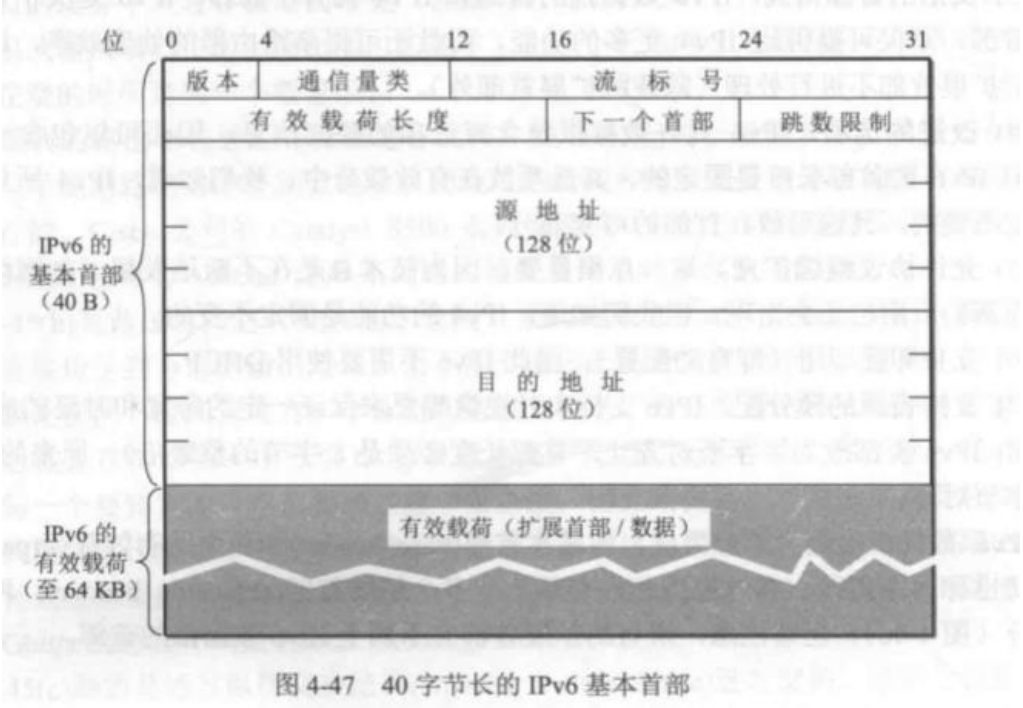


图 4-47　40 字节长的 IPv6 基本首部

版本 4位

通信量类 8位

流标号 20位

有效载荷长度 16位

下一个首部 8位

跳数限制 8位

源地址 128位

目的地址 128位

IPv6数据报目的地址：单播 多播 任播

冒号十六进制记法 零压缩

地址类型	二进制前缀
未指明地址	00…0（128 位），可记为::/128。
环回地址	00…1（128 位），可记为::1/128。
多播地址	11111111（8 位），可记为 FF00::/8。
本地链路单播地址	1111111010（10 位），可记为 FE80::/10。
全球单播地址	（除上述四种外，所有其他的二进制前缀）

本地链路单播地址 没有连接到互联网上 使用本地地址通信

全球单播地址

IPv6与IPv4的兼容: 双协议栈 隧道技术

ICMPv6

20. IP多播（略）
21. 虚拟专用网VPN

网络地址转换NAT多协议标记交换 MPLS

五、运输层

端到端应用进程间的通信

1. 用户数据报协议 UDP 无需建立连接

传输控制协议 TCP 面向连接的服务

应用	应用层协议	运输层协议
名字转换	DNS（域名系统）	UDP
文件传送	TFTP（简单文件传送协议）	UDP
路由选择协议	RIP（路由信息协议）	UDP
IP 地址配置	DHCP（动态主机配置协议）	UDP
网络管理	SNMP（简单网络管理协议）	UDP
远程文件服务器	NFS（网络文件系统）	UDP
IP 电话	专用协议	UDP
流式多媒体通信	专用协议	UDP
多播	IGMP（网际组管理协议）	UDP
电子邮件	SMTP（简单邮件传送协议）	TCP
远程终端接入	TELNET（远程终端协议）	TCP
万维网	HTTP（超文本传送协议）	TCP
文件传送	FTP（文件传送协议）	TCP

2. 端口

复用 所有应用进程都可以通过运输层再传到IP层

分用 IP层收到数据后，必须分别交付指明各应用进程

协议端口 port

在协议栈层间的抽象协议端口是软件端口 是应用层的各种协议进程与运输实体进行层间交互的一种地址

服务器使用的端口号：0~1023

表 5-2 常用的熟知端口号

应用程序	FTP	TELNET	SMTP	DNS	TFTP	HTTP	SNMP	SNMP (trap)	HTTPS
熟知端口号	21	23	25	53	69	80	161	162	443

登记端口号 1024~49151

客户端端口号 49152~65535

3. UDP

无连接

尽最大努力交付

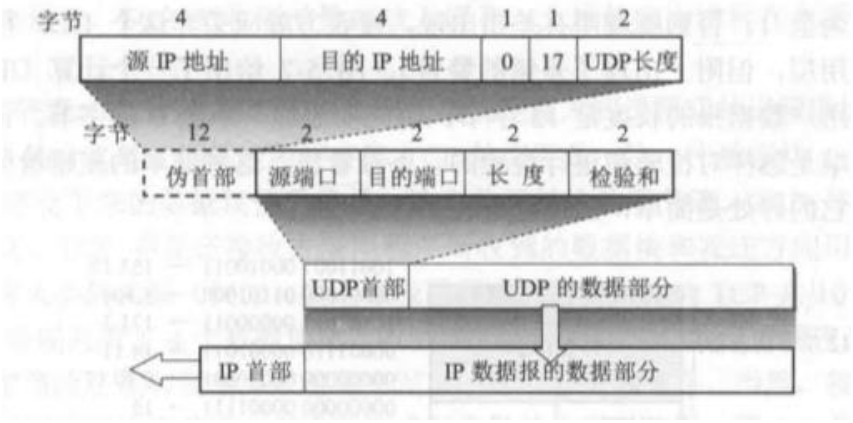
面向报文 不合并也不拆分

没有拥塞控制

支持一对一，一对多，多对多交互通信

UDP首部开销小

(1) 源端口	源端口号。在需要对方回信时选用。不需要时可用全 0。
(2) 目的端口	目的端口号。这在终点交付报文时必须使用。
(3) 长度	UDP 用户数据报的长度，其最小值是 8（仅有首部）。
(4) 检验和	检测 UDP 用户数据报在传输中是否有错。有错就丢弃。



伪首部用于计算检验和 不进行传送

将首部和数据部分一起检验

4. TCP协议

面向连接的运输层协议

每个TCP只能有两个端点

TCP提供可交付的服务 无差错 不丢失 不重复 按序到达

TCP提供全双工通信

面向字节流 TCP将应用程序交下来的数据仅仅看成一连串的无结构的字节流

套接字socket

5. **停止等待协议**

无差错情况

发送一个就停止，等待确认，得到确认后再发下一个

出现差错 超时重传 超时计时器

暂时保留已发送的分组的副本

分组和确认分组都必须进行编号

重传时间比数据在分组传输的平均往返时间更长一些

确认丢失和确认迟到

丢弃这个重复分组

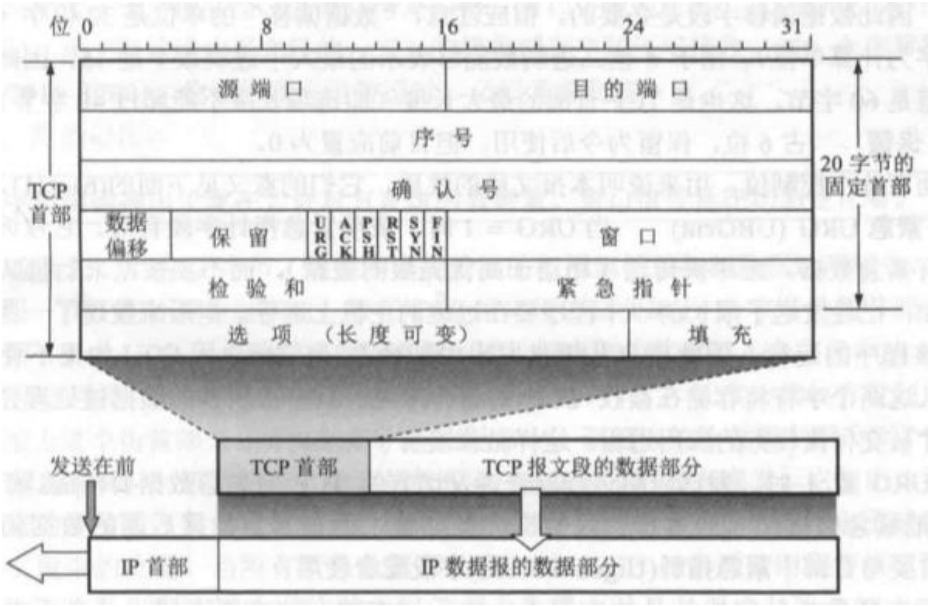
向A发送确认

连续ARQ协议

滑动窗口 每收到一个确认就往前滑动一个分组

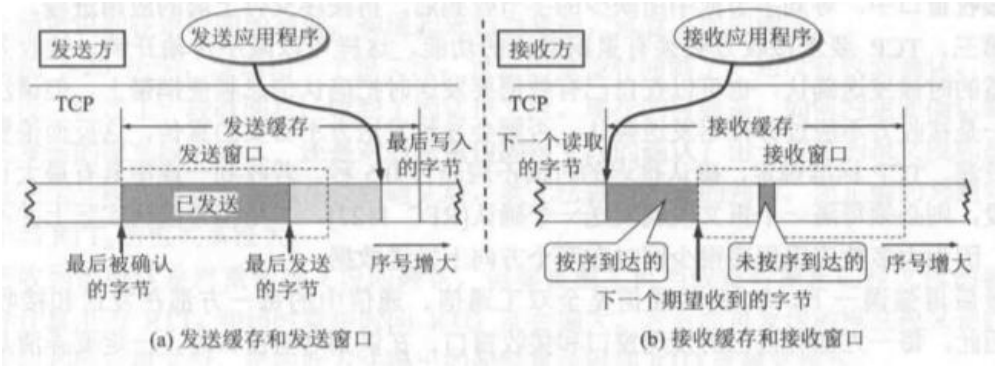
累计确认 对按序到达的最后一个分组发送确认 Go-back-N

TCP报文格式



6. 可靠传输实现

发送缓存和发送窗口 接收缓存和接收窗口



缓存空间和序号空间有限 循环利用

报文往返时间RTT α推荐为1/8

$$\text{新的 RTT}_S = (1 - \alpha) \times (\text{旧的 RTT}_S) + \alpha \times (\text{新的 RTT 样本})$$

超时重传时间 RTO

$$\text{RTO} = \text{RTT}_S + 4 \times \text{RTT}_D$$

β推荐为1/4

$$\text{新的 RTT}_D = (1 - \beta) \times (\text{旧的 RTT}_D) + \beta \times |\text{RTT}_S - \text{新的 RTT 样本}|$$

7. 流量控制 让发送方数据不要太快 点对点通信量控制

拥塞控制 降低网络负荷 端对端控制

TCP拥塞控制 慢开始 拥塞避免 快重传 快恢复

慢开始和拥塞避免

发送窗口等于拥塞窗口 由小到大逐渐增大发送/拥塞窗口

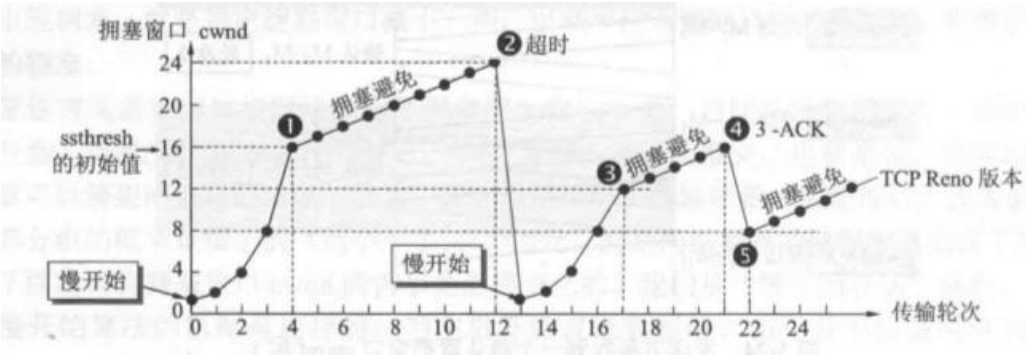
最大报文段 SMSS

在每收到一个对新的报文段的确认后，可以把拥塞窗口增加最多一个SMSS的数值

$$\text{拥塞窗口 cwnd 每次的增加量} = \min(N, \text{SMSS})$$

慢开始门限 拥塞避免算法 加法增大

一旦超时 ssthresh=cwnd/2



快重传 发送方收到连续3个重复确认 立即进行重传

快恢复 只是丢失个别报文段 不以慢启动开始 使用快恢复 拥塞避免算法

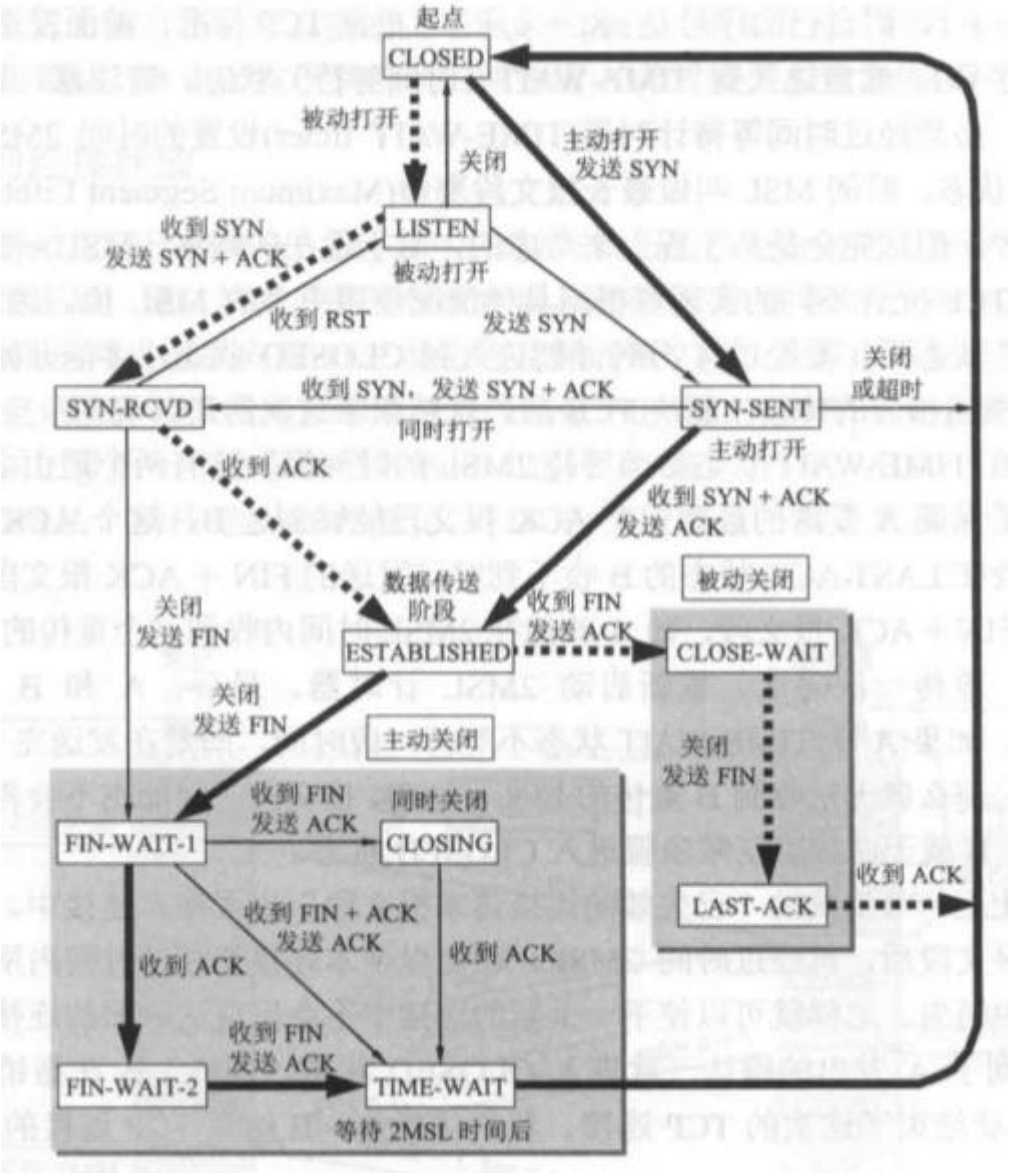
接收方窗口/通知窗口 发送窗口一定不能超过对方给出的接收方窗口值rwnd

8. 主动队列管理 AQM （略）
9. TCP的连接管理

   连接建立 三报文握手

   连接释放 四次挥手 时间等待计时器TIME-WAIT timer 等待2MSL 最长报文段寿命

   有限状态机：



六、应用层

1. DNS域名解析

   国家顶级域名 通用顶级域名 基础结构域名

   域名服务器

2. FTP协议

   两个并行的TCP连接 控制连接 数据连接

3. 简单文件传送协议 TFTP

   可用于UDP环境 所占内存小

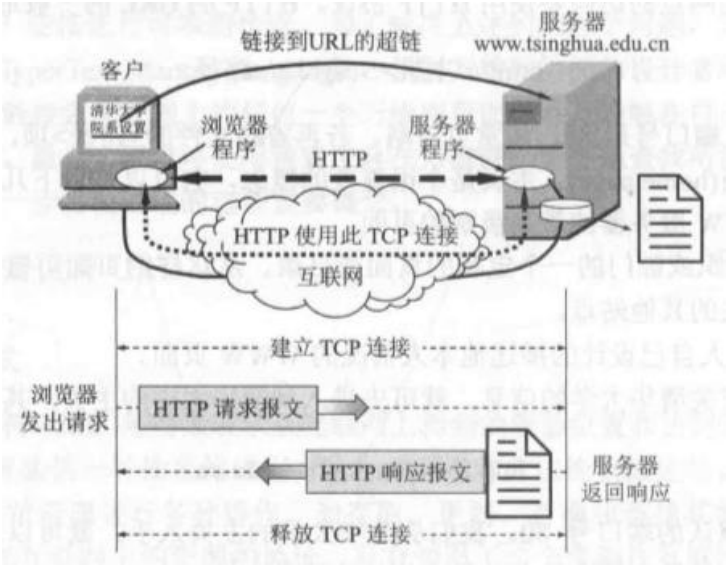
4. 远程终端协议 TELNET

5. 超文本传送协议HTTP

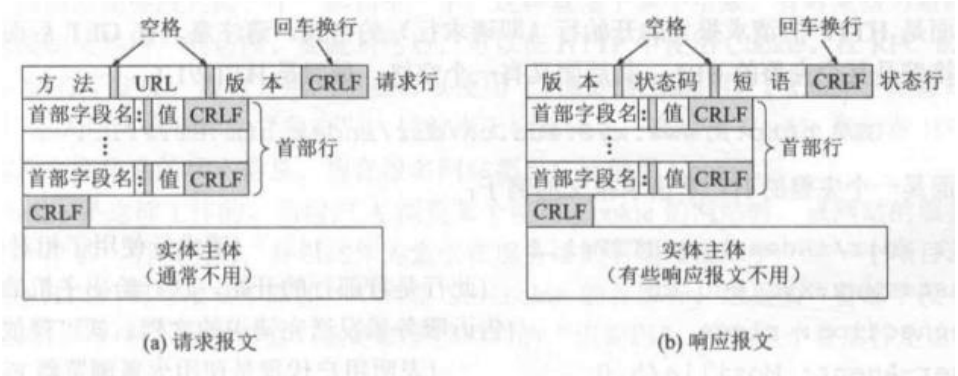
   统一资源定位符 URL

   http://<主机>:<端口>/<路径>

   操作过程



   报文结构 请求报文 响应报文



   请求报文的一些方法

表 6-1 HTTP 请求报文的一些方法

方法（操作）	意义
OPTION	请求一些选项的信息
GET	请求读取由 URL 所标志的信息
HEAD	请求读取由 URL 所标志的信息的首部
POST	给服务器添加信息（例如，注释）
PUT	在指明的 URL 下存储一个文档
DELETE	删除指明的 URL 所标志的资源
TRACE	用来进行环回测试的请求报文
CONNECT	用于代理服务器

状态码

1xx 表示通知信息，如请求收到了或正在进行处理。
2xx 表示成功，如接受或知道了。
3xx 表示重定向，如要完成请求还必须采取进一步的行动。
4xx 表示客户的差错，如请求中有错误的语法或不能完成。
5xx 表示服务器的差错，如服务器失效无法完成请求。

部分常用状态码

200 OK：请求已正常处理。

204 No Content：请求处理成功，但没有任何资源可以返回给客户端，一般在只需要从客户端往服务器发送信息，而对客户端不需要发送新信息内容的情况下使用。

206 Partial Content：是对资源某一部分的请求，该状态码表示客户端进行了范围请求，而服务器成功执行了这部分的GET请求。响应报文中包含由Content-Range指定范围的实体内容。

301 Moved Permanently：资源的uri已更新，你也更新下你的书签引用吧。永久性重定向，请求的资源已经被分配了新的URI，以后应使用资源现在所指的URI。

302 Found：资源的URI已临时定位到其他位置了，姑且算你已经知道了这个情况了。临时性重定向。和301相似，但302代表的资源不是永久性移动，只是临时性性质的。换句话说，已移动的资源对应的URI将来还有可能发生改变。

303 See Other：资源的URI已更新，你是否能临时按新的URI访问。该状态码表示由于请求对应的资源存在着另一个URL，应使用GET方法定向获取请求的资源。303状态码和302状态码有着相同的功能，但303状态码明确表示客户端应当采用GET方法获取资源，这点与302状态码有区别。

当301,302,303响应状态码返回时，几乎所有的浏览器都会把POST改成GET，并删除请求报文内的主体，之后请求会自动再次发送。

304 Not Modified：资源已找到，但未符合条件请求。该状态码表示客户端发送附带条件的请求时（采用GET方法的请求报文中包含If-Match，If-Modified-Since，If-None-Match，If-Range，If-Unmodified-Since中任一首部）服务端允许请求访问资源，但因发生请求未满足条件的情况后，直接返回304.。

307 Temporary Redirect：临时重定向。与302有相同的含义。

400 Bad Request：服务器端无法理解客户端发送的请求，请求报文中可能存在语法错误。

401 Unauthorized：该状态码表示发送的请求需要有通过HTTP认证（BASIC认证，DIGEST认证）的认证信息。

403 Forbidden：不允许访问那个资源。该状态码表明对请求资源的访问被服务器拒绝了。（权限，未授权IP等）

404 Not Found：服务器上没有请求的资源。路径错误等。

500 Internal Server Error：貌似内部资源出故障了。该状态码表明服务器端在执行请求时发生了错误。也有可能是web应用存在bug或某些临时故障。

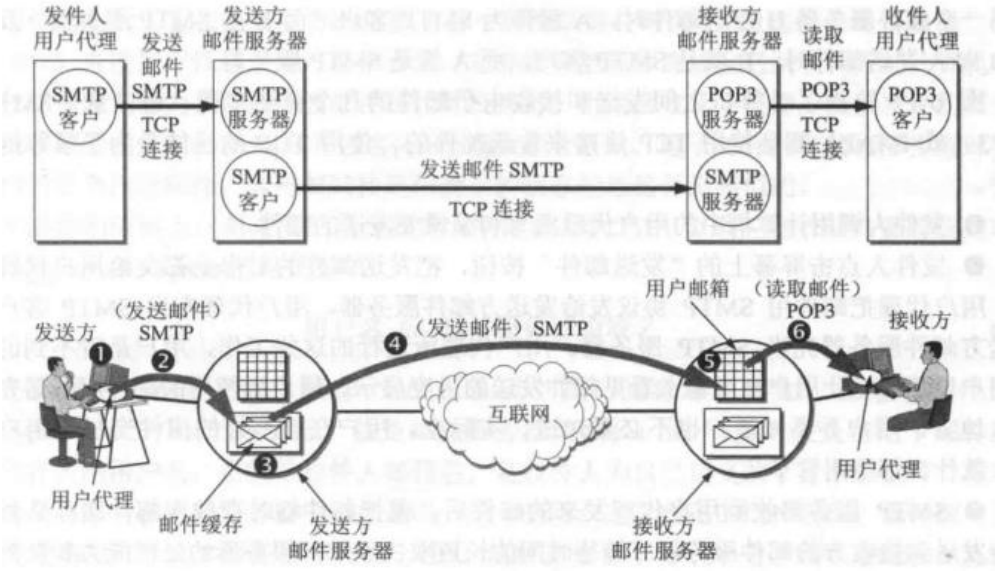
503 Service Unavailable：抱歉，我现在正在忙着。该状态码表明服务器暂时处于超负载或正在停机维护，现在无法处理请求。

6. 电子邮件

简单邮件传送协议 SMTP 邮件发送协议

邮局协议 POP3 邮件读取协议

网际报文存取协议 IMAP 邮件读取协议



几个协议对比

操作位置	操作内容	IMAP	POP3
收件箱	阅读、标记、移动、删除邮件等	客户端与邮箱更新同步	仅在客户端内
发件箱	保存到已发送	客户端与邮箱更新同步	仅在客户端内
创建文件夹	新建自定义的文件夹	客户端与邮箱更新同步	仅在客户端内
草稿	保存草稿	客户端与邮箱更新同步	仅在客户端内
垃圾文件夹	接收并移入垃圾文件夹的邮件	支持	不支持
广告邮件	接收并移入广告邮件夹的邮件	支持	不支持

7. 动态主机配置协议 DHCP
8. 简单网络管理协议 SNMP
9. P2P应用

BT 最稀有优先 将最稀有的文件块收集到

分布式散列表DHT索引和查找

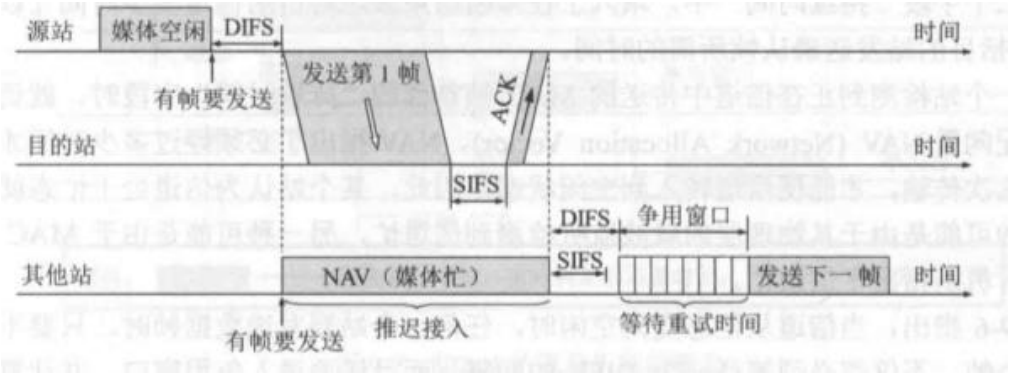
第七章 网络安全（略）

第八章 音频视频服务（略）

第九章 无线网络和移动网络

802.11局域网

1. CSMA/CA协议 碰撞避免



虚拟载波监听

后续略

如有面经出现或需要作为后续补充知识点

1.