

- 注意计算题

## 试题

---

- [计算机网络试题及答案（史上最全）](#)

## 名词解释

---

## 简答

---

### 请简述以太网的工作原理和数据传输过程

以太网是总线型局域网，任何节点都没有可预约的发送时间，它们的发送是随机的，网络中不存在集中控制节点。以太网的节点发送数据是通过“广播”方式将数据送往共享介质，概括为“[先听后发，边听边发，冲突停止，延时重发](#)”。

### 试从多个方面比较共享式以太网和交换式以太网

共享式以太网：组建简单、便宜、但覆盖地理范围有限，网络总带宽固定，随着节点数的增加，冲突碰撞加大，浪费加大，不支持多速。

交换式以太网：增加了交换机，以分段方式将一个大型以太网分割成多个小型以太网，段与段之间通过交换设备沟通，由于分成小型网，节点数减少，冲突碰撞浪费减少，各段可按需要选择自己的网络速率。

## 计算

---

Z4-15

[问答题，简答题]一个3200位长的TCP报文传到IP层，加上160位的首部后成为数据报。下面的互联网由两个局域网通过路由器连接起来。但第二个局域网所能传送的最长数据帧中的数据部分只有1200位。因此数据报在路由器必须进行分片。试问第二个局域网向其上层要传送多少比特的数据（这里的“数据”当然指的是局域网看见的数据）？

## 解答

第二个局域网所能传送的最长数据帧中的数据部分只有1200bit，即每个IP数据片的数据部分 $<1200-160$  (bit)，由于片偏移是以8字节即64bit为单位的，所以IP数据片的数据部分最大不超过1024bit，这样3200bit的报文要分4个数据片，所以第二个局域网向上传送的比特数等于 $(3200 \div 4 \times 160)$ ，共3840bit。

# 第1章 概述

---

## 互联网的组成

---

### 1.5 计算机网络的类别

---

#### 1.5.2 几种不同类别的网络

##### 按网络的作用范围进行分类

- **广域网 WAN (Wide Area Network)**: 作用范围通常为几十到几千公里。
- **城域网 MAN (Metropolitan Area Network)**: 作用距离约为 5 ~ 50 公里。
- **局域网 LAN (Local Area Network)** : 局限在较小的范围（如 1 公里左右）。
- **个人区域网 PAN (Personal Area Network)** : 范围很小，大约在 10 米左右。

若中央处理机之间的距离非常近（如仅1米的数量级甚至更小些），则一般就称之为**多处理机系统**，而不称它为计算机网络。

## 1.6 计算机网络的性能

### 1.6.1 计算机网络的性能指标

**速率**

**带宽**

$$\left\{ \begin{array}{l} \text{数字} \rightarrow \text{最大传输能力 } (bit/s) \\ \text{模拟} \rightarrow \text{传输频率 } (Hz) \end{array} \right.$$

在计算机网络中，带宽用来表示网络中某通道传送数据的能力。表示在单位时间内网络中的某信道所能通过的“**最高数据率**”。单位是 bit/s，即“比特每秒”

**吞吐量**

**时延**

总时延 = 发送时延 + 传播时延 + 处理时延 + 排队时延

**注意** 容易产生的错误概念

- 对于高速网络链路，我们提高的仅仅是数据的发送速率而不是比特在链路上的传播速率。
- 提高链路带宽减小了数据的发送时延。

以下说法是错误的：

“在高速链路（或高带宽链路）上，比特会传送得更快些”。  
传播时延由传播介质决定

## 组成

- 发送时延（也称传输时延）
  - 发送数据时，数据帧从结点进入到传输媒体所需要的时间。
  - 也就是从发送数据帧的第一个比特算起，到该帧的最后一个比特发送完毕所需的时间。

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

- 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。
  - 发送时延与传播时延有本质上的不同。
  - 信号发送速率和信号在信道上的传播速率是完全不同的概念。

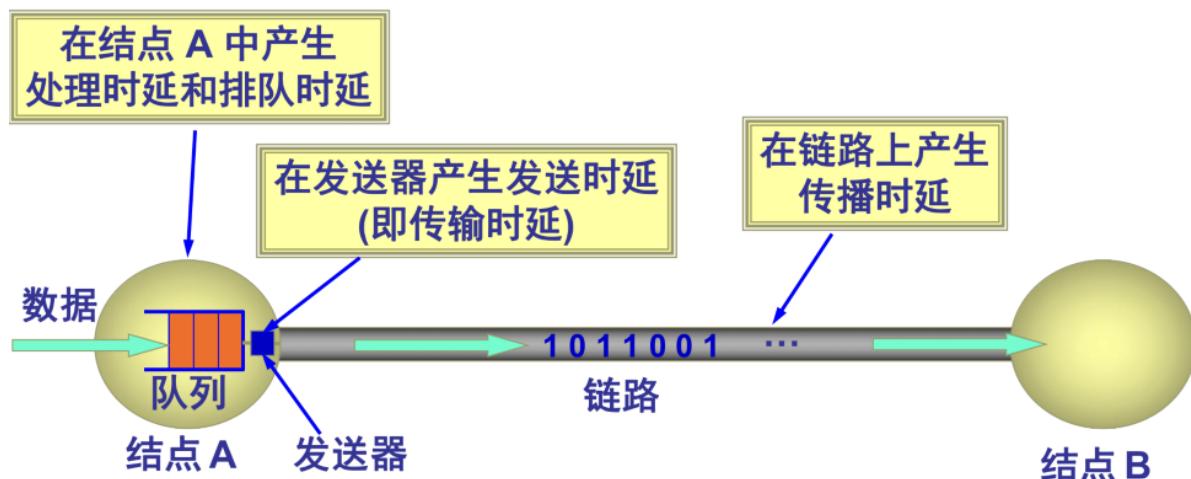
$$\text{传播时延} = \frac{\text{信道长度 (米)}}{\text{信号在信道上的传播速率 (米/秒)}}$$

- 处理时延
  - 主机或路由器在收到分组时，为处理分组（例如分析首部、提取数据、差错检验或查找路由）所花费的时间。
- 排队时延

- 分组在路由器输入输出队列中排队等待处理所经历的时延。
- 排队时延的长短往往取决于网络中当时的通信量。

时延的产生地

假设从结点 A 向结点 B 发送数据



几种时延产生的地方不一样

时延带宽积

往返时间RTT

利用率

## 1.7 计算机网络的体系结构

### 1.7.3 具有五层协议的体系结构 P139



- 应用层 (application layer)
- 运输层 (transport layer)
- 网络层 (network layer)
- 数据链路层 (data link layer)
- 物理层 (physical layer)

# 第2章 物理层

## 物理层的基本概念

### 2.2 数据通信的基础知识

#### 2.2.1 数据通信系统的模型

#### 2.2.2 有关信道的几个基本概念

##### 调制 P13

- 基带调制
- 带通调制

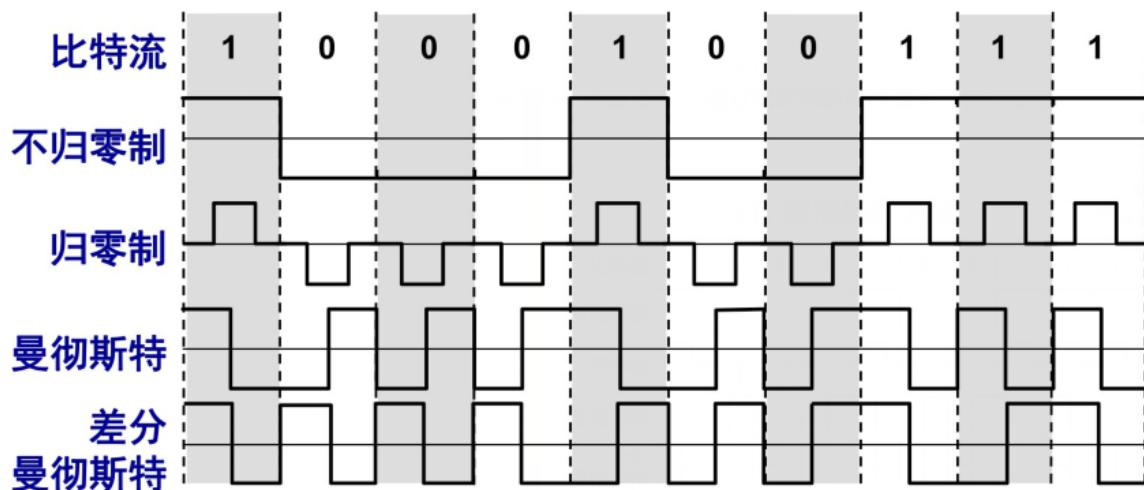
**调制分为两大类：** 调制 { 编码  
载波调制

- **基带调制：**仅对基带信号的波形进行变换，使它能够与信道特性相适应。**变换后的信号仍然是基带信号（数字信号）** 把这种过程称为**编码 (coding)**。
- **带通调制：**使用**载波 (carrier)**进行调制，把基带信号的频率范围搬移到较高的频段，并**转换为模拟信号**，这样就能够更好地在模拟信道中传输（即仅在一段频率范围内能够通过信道）。
- **带通信号：** 经过载波调制后的信号（**模拟信号**）

##### 曼彻斯特编码 P14

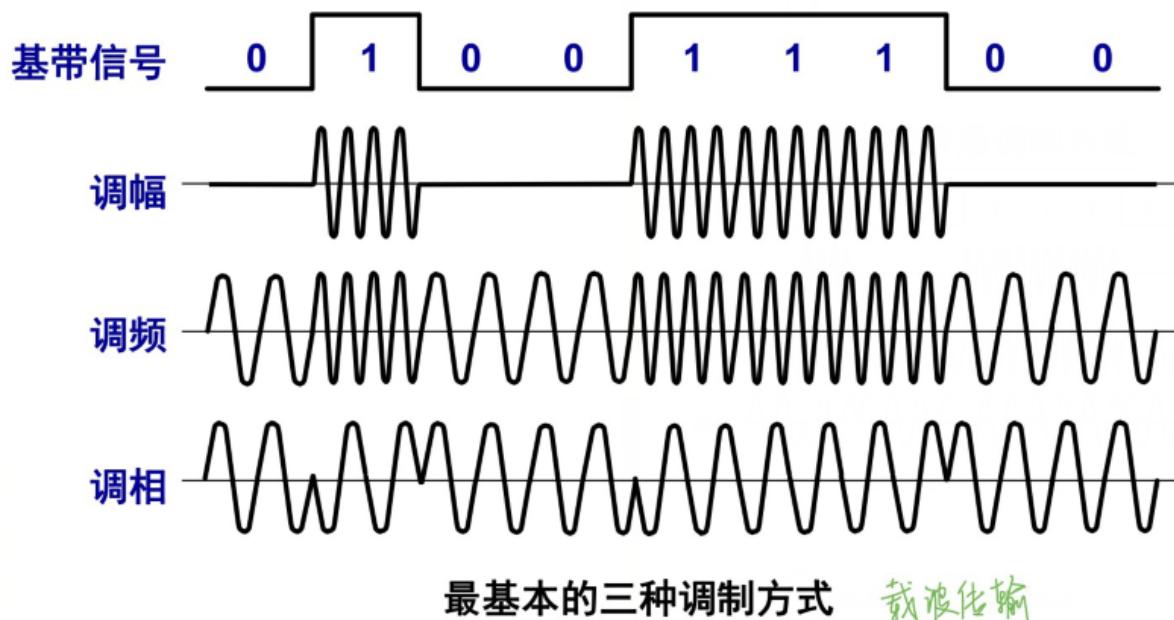
位中心**向上跳变**代表0，**向下跳变**代表1：

## (1) 常用编码方式



## 基本的带通调制方法

- 调幅
- 调频
- 调相



## 2.2.3 信道的极限容量

### 信噪比

信噪比 = 信号的平均功率 / 噪声的平均功率，记为  $S/N$ ，用分贝作为度量单位 ( $dB$ )：

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

## 香农公式 P28

带宽受限且有高斯白噪声干扰的信道的极限、无差错的信息传输速率：

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

### 说明

- 信道的带宽或信噪比越大，则信道的**极限传输速率**越高
- 只要信息传输速率低于信道的极限信息传输速率，就一定可以以某种方法实现无差错的传输
- 若信道带宽 $W$ 或信道信噪比 $S/N$ 无上限，则信道的极限传输速率无上限（实际信道不可能这样）

**注意** 在信道带宽已确定、信噪比和码元传输速率无法再提高的情况下，如何提高信息的传输速率：用编码的方法让每一个码元携带更多比特的信息量

## 2.3 物理层下面的传输媒体

### 2.3.1 导引型传输媒体 P32

- 双绞线
- 同轴电缆

### 光缆

多模光纤与单模光纤

#### ■ 多模光纤

可能存在**多条不同角度入射**的光线在一条光纤中传输。  
这种光纤就称为**多模光纤**。

#### ■ 单模光纤

若**光纤的直径减小到只有一个光的波长**，则光纤就像一根波导那样，它可使光线一直向前传播，而不会产生多次反射。这样的光纤称为**单模光纤**。

1. 通信容量非常大
2. 传输损耗小，中继距离长
3. 抗电磁干扰性能好
4. 无串音干扰，保密性好
5. 体积小，重量轻

## 2.4 信道复用技术

### 2.4.1 频分复用、时分复用和统计时分复用

- 频分复用：在同样的时间里占用不同的带宽资源
- 时分复用：在不同的时间占用相同的频带宽度

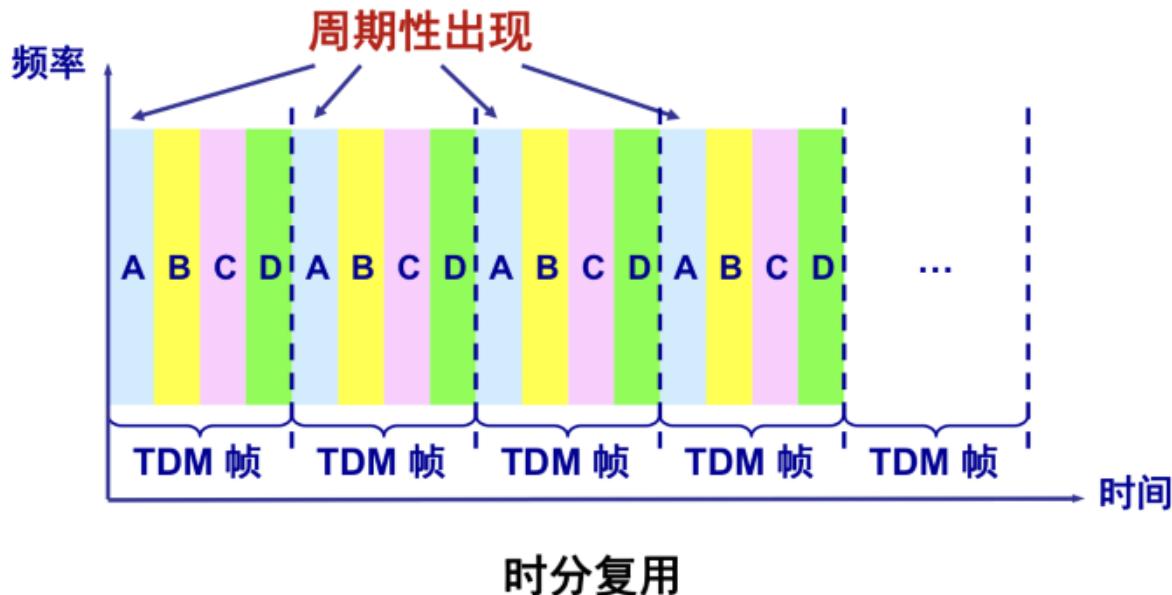
#### 频分复用

- 将整个带宽分为多份，用户在分配到一定的频带后，在通信过程中自始至终都占用这个频带。
- 频分复用的所有用户在同样的时间占用不同的带宽资源（请注意，这里的“带宽”是频率带宽而不是数据的发送速率）。



#### 时分复用

- 时分复用则是将时间划分为一段段等长的时分复用帧（TDM 帧）。每一个时分复用的用户在每一个 TDM 帧中占用固定序号的时隙。
- 每一个用户所占用的时隙是周期性地出现（其周期就是 TDM 帧的长度）。
- TDM 信号也称为等时(isochronous)信号。
- 时分复用的所有用户是在不同的时间占用同样的频带宽度。



## 2.4.2 波分复用

## 2.4.3 码分复用

- 常用的名词是**码分多址 CDMA**  
(Code Division Multiple Access)。
- 每一个用户**在同样的时间使用同样的频带**，各用户使用经过特殊挑选的**不同码型**，因此彼此不会造成干扰。
- 这种系统发送的信号有很强的抗干扰能力，其频谱类似于白噪声，不易被敌人发现。

# 宽带接入技术

# 第3章 数据链路层

## 3.1 使用点对点信道的数据链路层

### 3.1.2 三个基本问题 P11

- 封装成帧
- 透明传输
- 差错控制

## 封装成帧

在一段数据的前后分别添加首部和尾部，构成一个帧。

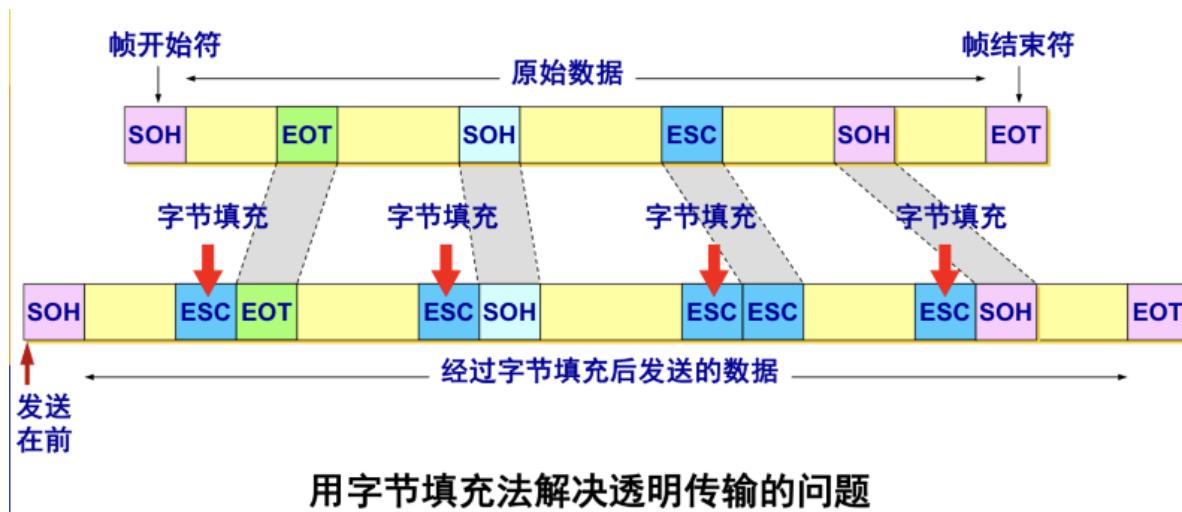
## 透明传输

如果数据中的某个字节的二进制代码恰好和SOH(Start Of Header)或EOT(End Of Transmission)一样，数据链路层就会错误地“找到帧的边界”。

- 解决透明传输问题

字节填充或字符填充：

- 解决方法：字节填充 (byte stuffing) 或字符填充 (character stuffing)。
- 发送端的数据链路层在数据中出现控制字符“SOH”或“EOT”的前面插入一个转义字符“ESC”(其十六进制编码是1B)。
- 接收端的数据链路层在将数据送往网络层之前删除插入的转义字符。
- 如果转义字符也出现在数据当中，那么应在转义字符前面插入一个转义字符 ESC。当接收端收到连续的两个转义字符时，就删除其中前面的一个。



## 差错控制

## 循环冗余检验CRC (计算)

假设待传送的一组数据  $M$ , 含  $k$  个比特, 在  $M$  的后面添加供差错检测用的  $n$  位冗余码一起发送。

- 冗余码的计算

模2减法 (按位异或) :

$$0 - 0 = 1 - 1 = 0$$

$$0 - 1 = 1 - 0 = 1$$

模2除法 (二进制除法 + 模2减法), 示例:

$$\begin{array}{r} \overline{1011} \\ 1101 \overline{)1111000} \\ \underline{1101} \\ 001000 \\ \underline{001101} \\ 01010 \\ \underline{1101} \\ 0111 \end{array}$$

冗余码的计算步骤:

- 
- 数据
- 1、用二进制的模 2 运算进行  $2^n$  乘  $M$  的运算, 这相当于在  $M$  后面添加  $n$  个 0。
  - 2、得到的  $(k + n)$  位的数除以事先选定好的长度为  $(n + 1)$  位的除数  $P$ , 得出商是  $Q$  而余数是  $R$ , 余数  $R$  比除数  $P$  少 1 位, 即  $R$  是  $n$  位。
  - 3、将余数  $R$  作为冗余码拼接在数据  $M$  后面发送出去。

示例:

- 现在  $k = 6$ ,  $M = 101001$ 。
- 设  $n = 3$ , 除数  $P = 1101$ ,
- 1、被除数是  $2^n M = 101001000$ 。
- 2、模 2 运算的结果是: 商  $Q = 110101$ ,  
余数  $R = 001$ 。
- 3、把余数  $R$  作为冗余码添加在数据  $M$  的后面发送出去。发送的数据是:  $2^n M + R$   
即:  $101001001$ , 共  $(k + n)$  位。

检验方式：把收到的每一帧除以同样的除数P，检查得到的余数R：

### 接收端对收到的每一帧进行 CRC 检验

- (1) 若得出的余数  $R = 0$ ，则判定这个帧没有差错，就接受 (accept)。
- (2) 若余数  $R \neq 0$ ，则判定这个帧有差错，就丢弃。
- 但这种检测方法并不能确定究竟是哪一个或哪几个比特出现了差错。
- 只要经过严格的挑选，并使用位数足够多的除数  $P$ ，那么出现检测不到的差错的概率就很小很小。

#### 注意

- 仅用循环冗余检验CRC差错检测技术只能做到无差错接受
- 无差错接受：凡是接受的帧（不包括丢弃的帧），都能以非常接近1的概率认为这些帧在传输过程中没有产生差错。
- 要做到“可靠传输”（即发送什么就收到什么），必须加上确认和重传机制。

#### 帧检验序列FCS

在数据后面添加上的冗余码称为帧检验序列FCS

**注** 循环冗余检验CRC是一种常用的检错方法，帧检验序列FCS是添加在数据后面的冗余码。

## 3.2 使用广播信道的数据链路层

### 3.3.2 CSMA/CD协议 P37

载波监听多点接入/碰撞检测 (Carrier Sense Multiple Access with Collision Detection)

- 多点接入：许多计算机以多点接入的方式连接在一根总线上
- 载波监听：每个站在发送数据之前先检测总线上是否有其他计算机在发送数据，若有则暂时不要发送数据，以免发生碰撞
- 碰撞检测：计算机边发送数据边检测信道上的信号电压大小
- 争用期

# 争用期



- 最先发送数据帧的站，在发送数据帧后至多经过时间  $2\tau$ （两倍的端到端往返时延）就可知道发送的数据帧是否遭受了碰撞。
- 以太网的端到端往返时延  $2\tau$  称为**争用期**，或**碰撞窗口**。
- 经过争用期这段时间还没有检测到碰撞，才能肯定这次发送不会发生碰撞。

## CSMA/CD协议的要点

- (1) 准备发送。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(9.6us)内信道保持空闲（保证了帧间最小间隔），就发送这个帧。空闲时间
- (3) 检查碰撞。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(51.2us)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。

### 3.3.3 使用集线器的星形拓扑

#### 集线器 P60

集线器的一些特点：

- (1) 集线器是使用电子器件来模拟实际电缆线的工作，因此整个系统仍然像一个传统的以太网那样运行。  
相当于将总线缩成一个点
- (2) 使用集线器的以太网在逻辑上仍是一个总线网，各工作站使用的还是 CSMA/CD 协议，并共享逻辑上的总线。
- (3) 集线器很像一个多接口的转发器，**工作在物理层**。
- (4) 集线器采用了专门的芯片，进行自适应串音回波抵消，减少了近端串音。
- 目前已经基本退出市场

### 3.3.5 以太网的MAC层

#### MAC层的硬件地址 P62

在局域网中，硬件地址又称为物理地址，或MAC地址。

48位的MAC地址：

- IEEE 802 标准规定 MAC 地址字段可采用 **6 字节 (48位)** 或 **2 字节 (16位)** 这两种中的一种。
- IEEE 的注册管理机构 RA 负责向厂家分配地址字段 6 个字节中的前三个字节 (即**高位 24 位**)，称为**组织唯一标识符**。
- 地址字段 6 个字节中的后三个字节 (即**低位 24 位**) 由厂家自行指派，称为**扩展唯一标识符**，必须保证生产出的适配器没有**重复地址**。



### 3.4 扩展的以太网

#### 3.4.2 在数据链路层扩展以太网

#### 以太网交换机 P80

## 以太网交换机的特点

- 以太网交换机实质上就是一个**多接口的网桥**。
  - 通常都有十几个或更多的接口。
- 每个接口都**直接与一个单台主机或另一个以太网交换机相连**，并且一般都**工作在全双工方式**。
- 以太网交换机具有**并行性**。
  - 能同时连通多对接口，使**多对主机能同时通信**。
- 相互通信的主机都是**独占传输媒体**，**无碰撞地传输数据**。
- 以太网交换机的**接口有存储器**，能在输出端口繁忙时把到来的帧进行缓存。
- 以太网交换机是一种**即插即用**设备，其内部的**帧交换表**（又称为**地址表**）是通过**自学习算法**自动地逐渐建立起来的。
- 以太网交换机使用了**专用的交换结构芯片**，用硬件转发，其转发速率要比使用软件转发的网桥快很多。

## 以太网交换机的优点

- **用户独享带宽，增加了总容量。**
  - 对于普通 10 Mbit/s 的**共享式以太网**，若共有  $N$  个用户，则每个用户占有的平均带宽只有总带宽 (10 Mbit/s) 的  $N$  分之一。
  - 使用**以太网交换机**时，每一个用户在通信时是**独占 10 Mbit/s**。
- **即插即用**——从共享总线以太网转到交换式以太网时，所有接入设备的软件和硬件、适配器等都不需要做任何改动。
- **速率自适应**——以太网交换机一般都具有多种速率的接口，方便了各种不同情况的用户。

## 以太网交换机的交换方式

- **存储转发方式**
  - 把整个数据帧先缓存后再进行处理。
- **直通 (cut-through) 方式**
  - 接收数据帧的同时就**立即按数据帧的目的 MAC 地址**决定该帧的转发接口，因而提高了帧的转发速度。
  - **缺点**是它不检查差错就直接将帧转发出去，因此有可能也将一些无效帧转发给其他的站。

### 3.4.3 虚拟局域网 P87

虚拟局域网VLAN (Virtual LAN)

- 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。每一个VLAN的帧都有一个明确的标识符，指明发送这个帧的计算机是属于哪一个VLAN
- 虚拟局域网是局域网给用户提供的一种服务，并不是一种新型局域网

## 第4章 网络层 重点

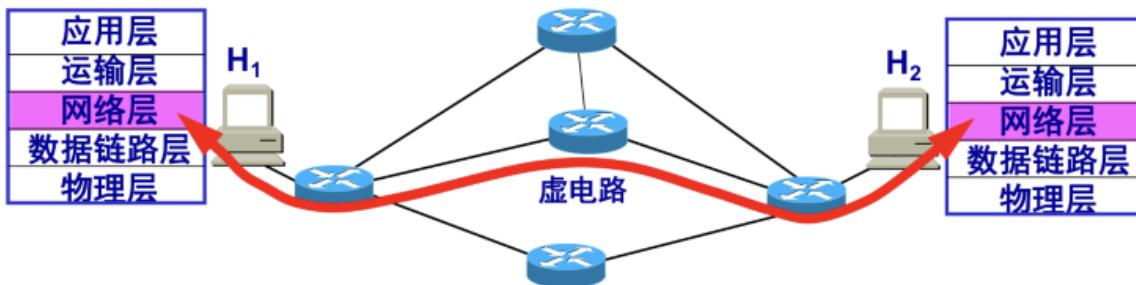
### 4.1 网络层提供的两种服务

- 虚电路服务
- 数据报服务

对比的方面	虚电路服务	数据报服务
思路	可靠通信应当由网络来保证	可靠通信应当由用户主机来保证
连接的建立	必须有	不需要
终点地址	仅在连接建立阶段使用，每个分组使用短的虚电路号	每个分组都有终点的完整地址
分组的转发	属于同一条虚电路的分组均按照同一路由进行转发	每个分组独立选择路由进行转发
当结点出故障时	所有通过出故障的结点的虚电路均不能工作	出故障的结点可能会丢失分组，一些路由可能会发生变化
分组的顺序	总是按发送顺序到达终点	到达终点时不一定按发送顺序
端到端的差错处理和流量控制	可以由网络负责，也可以由用户主机负责	由用户主机负责

### 虚电路服务

虚电路服务：面向连接



H<sub>1</sub> 发送给 H<sub>2</sub> 的所有分组都沿着同一条虚电路传送

- 虚电路表示这是一条逻辑上的连接，分组都沿着这条逻辑连接按照存储转发方式传送，而并不是真正建立了一条物理连接。
- 请注意，电路交换的电话通信是先建立了一条真正的连接。
- 因此分组交换的虚连接和电路交换的连接只是类似，但并不完全一样。

## 数据报服务 P6

无连接的、尽最大努力交付的数据报服务

- 网络层向上只提供简单灵活的、无连接的、尽最大努力交付的数据报服务。
- 网络在发送分组时不需要先建立连接。每一个分组（即 IP 数据报）独立发送，与其前后的分组无关（不进行编号）。
- 网络层不提供服务质量的承诺。即所传送的分组可能出错、丢失、重复和失序（不按序到达终点），当然也不保证分组传送的时限。

### 尽最大努力交付

- 传输网络不提供端到端的可靠传输服务
- 若需要可靠通信，则由主机中的运输层负责可靠交付（包括差错处理、流量控制等）

## 4.2 网际协议IP (Internet Protocol)

注：IP是网际协议的名字，与IP协议配套使用的还有三个协议：

- 地址解析协议ARP

- 网际控制报文协议ICMP
- 网际组管理协议IGMP (不涉及)

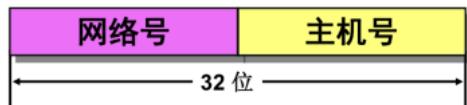
## 虚拟互连网络

### 4.2.2 分类的IP地址

#### IP地址及其表示方法

- IP 地址就是给每个连接在互联网上的主机（或路由器）分配一个在全世界范围是唯一的 32 位的标识符。

两级IP地址结构：



- 这种两级的 IP 地址可以记为：

IP 地址 ::= { <网络号>, <主机号>} (4-1)

::= 代表“定义为”

#### 常用的三种类别的IP地址

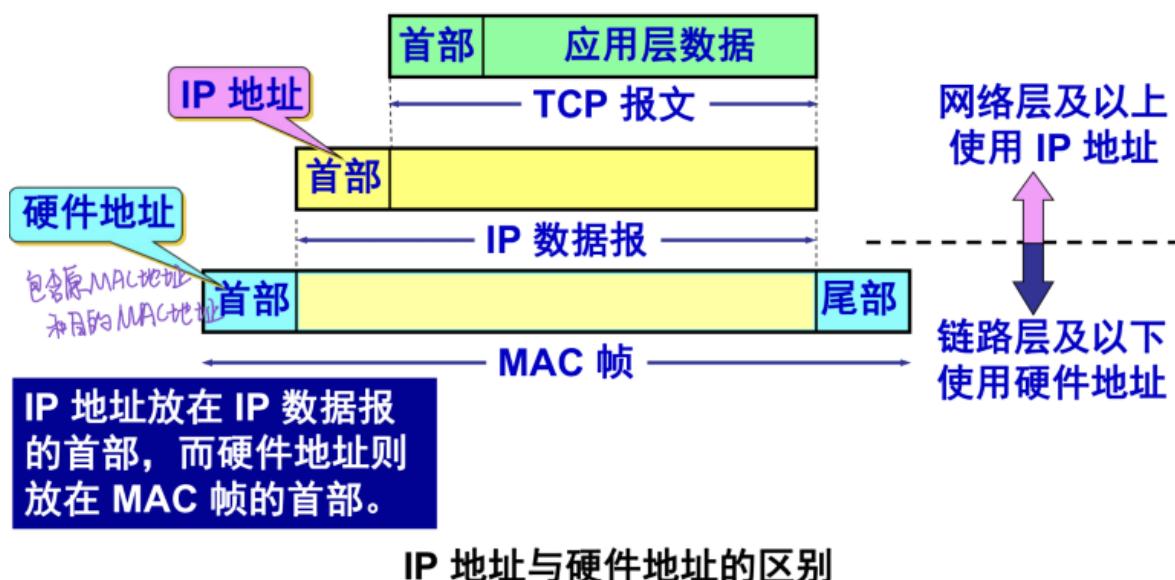
网络类别	最大可指派的网络数	第一个可指派的网络号	最后一个可指派的网络号	每个网络中最大主机数
A	$126 (2^7 - 2)$	1	126	16777214
B	$16383 (2^{14} - 1)$	128.1	191.255	65534
C	$2097151 (2^{21} - 1)$	192.0.1	223.255.255	254

#### 互联网中的IP地址 (图, 理解) P40

- 在同一个局域网上的主机或路由器的IP地址中的网络号必须相同
- 路由器总是具有两个或以上的IP地址，每一个接口都有一个不同网络号的IP地址

### 4.2.3 IP地址与硬件地址

- IP 地址与硬件地址是不同的地址。
- 从层次的角度看，
  - 硬件地址（或物理地址）是数据链路层和物理层使用的地址。
  - IP 地址是网络层和以上各层使用的地址，是一种逻辑地址（称 IP 地址是逻辑地址是因为 IP 地址是用软件实现的）。



IP 地址与硬件地址的区别

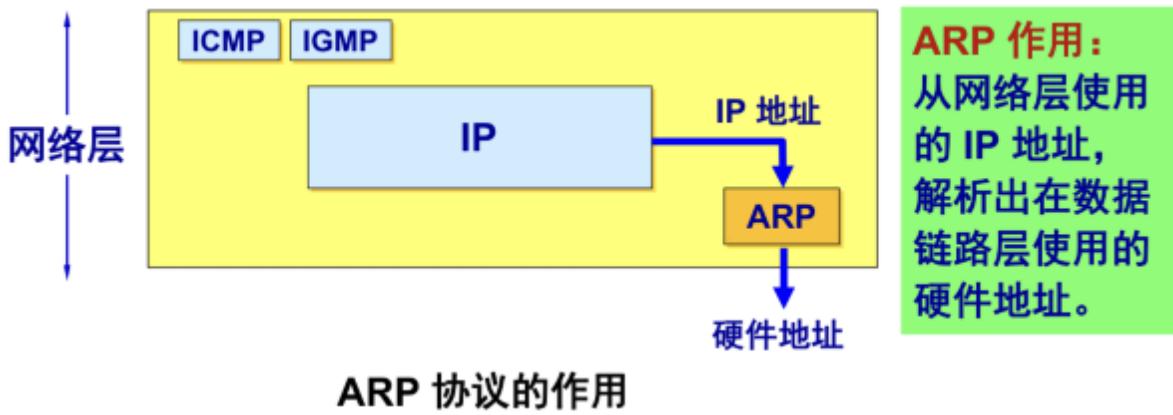
图：从协议栈的层次上看数据的流动（理解） P53

### 4.2.4 地址解析协议ARP 重要 P61

地址解析协议ARP (Address Resolution Protocol)

- IP地址--网络层地址 (可变)
- MAC地址--数据链路层地址 (不可变)

地址解析协议ARP的作用：由主机或路由器的IP地址，找出其相应的硬件MAC地址



## 地址解析协议ARP要点

- 不管网络层使用的是什么协议，在实际网络的链路上传送数据帧时，最终还是必须使用硬件地址。
- 每一个主机都设有一个 **ARP 高速缓存 (ARP cache)**，**里面有所在的局域网上的各主机和路由器的 IP 地址到硬件地址的映射表**。
- 当主机 A 欲向本局域网上的某个主机 B 发送 IP 数据报时，就先在其 ARP 高速缓存中查看有无主机 B 的 IP 地址。
  - **如有**，就可查出其对应的**硬件地址**，再将此硬件地址写入 **MAC 帧**，然后通过局域网将该 MAC 帧发往此硬件地址。
  - **如没有**，ARP 进程在本局域网上**广播发送一个 ARP 请求分组**。收到 **ARP 响应分组**后，将得到的 IP 地址到硬件地址的映射写入 ARP 高速缓存。
- ARP高速缓存的作用

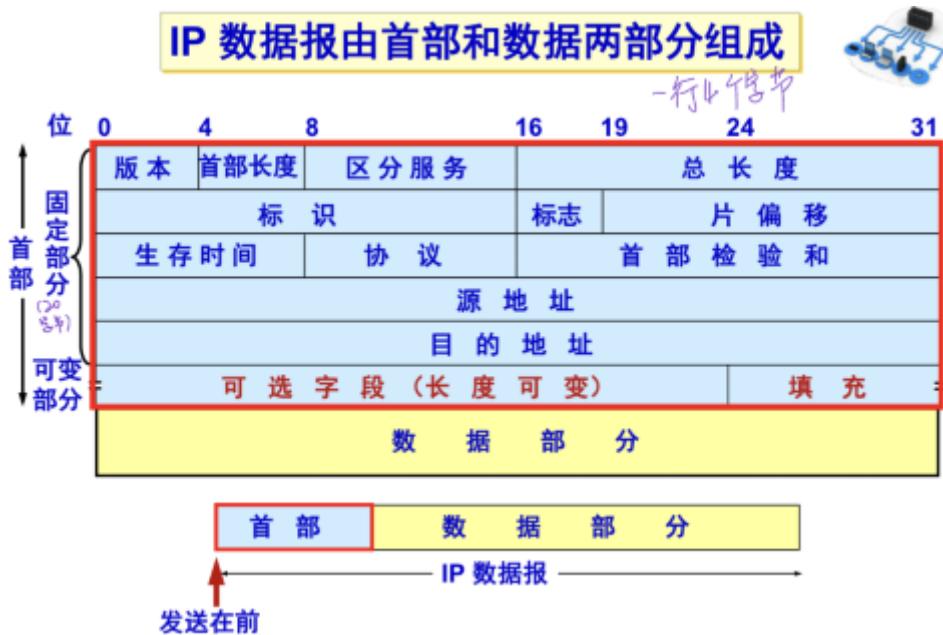
存放最近获得的IP地址到MAC地址的绑定，以减少ARP广播的数量。

## 使用ARP的四种典型情况

- 发送方是主机，要把 IP 数据报发送到本网络上的另一个主机。这时用 ARP 找到目的主机的硬件地址。
- 发送方是主机，要把 IP 数据报发送到另一个网络上的一个主机。这时用 ARP 找到本网络上的一个路由器的硬件地址。剩下的工作由这个路由器来完成。
- 发送方是路由器，要把 IP 数据报转发到本网络上的一个主机。这时用 ARP 找到目的主机的硬件地址。
- 发送方是路由器，要把 IP 数据报转发到另一个网络上的一个主机。这时用 ARP 找到本网络上另一个路由器的硬件地址。剩下的工作由这个路由器来完成。

#### 4.2.5 IP数据报的格式 P74

- 首部的前一部分是固定长度，共20字节，是所有IP数据报必须具有的。
  - 一个 IP 数据报由首部和数据两部分组成。
  - 首部的前一部分是固定长度，共 20 字节，是所有 IP 数据报必须具有的。
  - 在首部的固定部分的后面是一些可选字段，其长度是可变的。



## 4.2.6 IP层转发分组的流程 P95

路由表的结构：目的网络地址 + 下一跳地址



查找路由表：由目的网络地址可以确定下一跳路由器

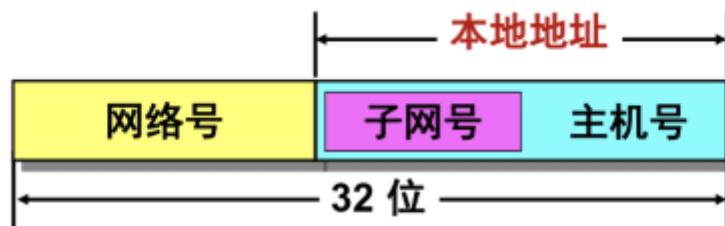
- 通过多次**间接交付**最终可以找到目的主机所在目的网络上的路由器
- 到达最后一个路由器时，向目的主机进行**直接交付**

**注** 路由表没有给出到某个网络的完整路径，而是指出应当先到哪个下一跳路由器。

## 4.3 划分子网

### 4.3.1 划分子网

三级IP地址



IP地址 ::= {<网络号>, <子网号>, <主机号>} (4-2)

- 当没有划分子网时，IP 地址是两级结构。
- 划分子网后 IP 地址就变成了三级结构。
- 划分子网只是把 IP 地址的主机号 host-id 这部分进行再划分，而不改变 IP 地址原来的网络号 net-id。

划分子网所用的字段属于原IP地址的[主机号部分](#)。

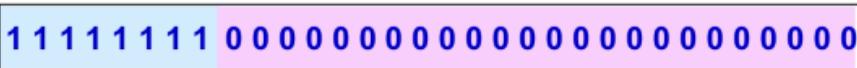
## 子网掩码（计算） P109

网络地址 = IP地址 AND 与 子网掩码

**规则：**

- 子网掩码长度 = 32 位
- 某位 = 1：IP地址中的对应位为网络号和子网号
- 某位 = 0：IP地址中的对应位为主机号

默认子网掩码

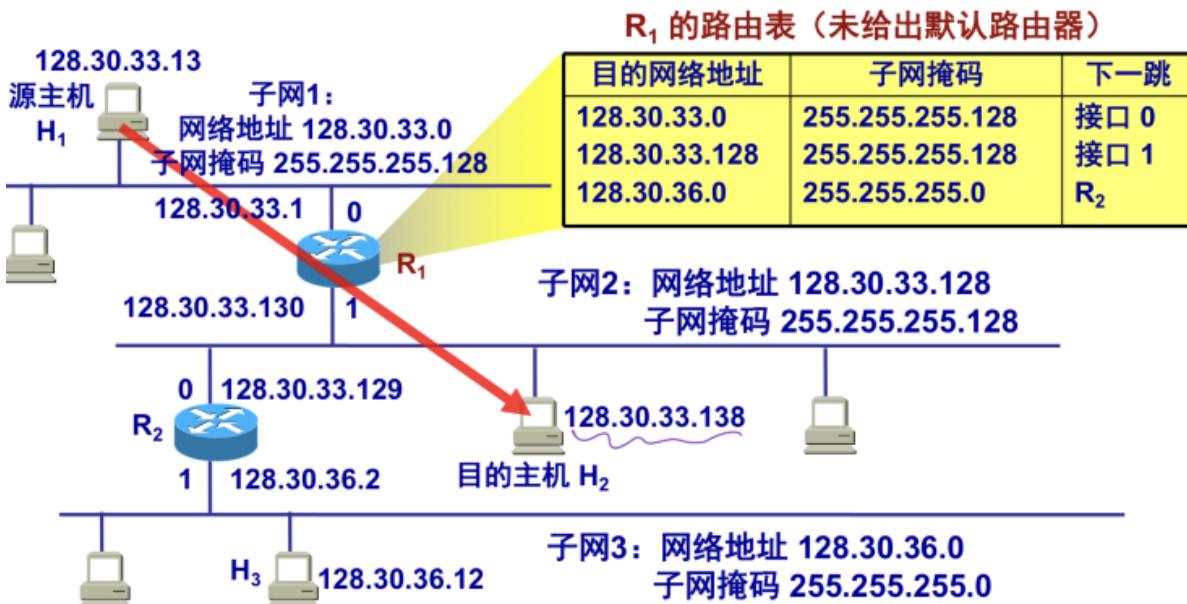
<b>A类地址</b>	网络地址	网络号	主机号为全 0
	默认子网掩码 255.0.0.0		
<b>B类地址</b>	网络地址	网络号	主机号为全 0
	默认子网掩码 255.255.0.0		
<b>C类地址</b>	网络地址	网络号	主机号为全 0
	默认子网掩码 255.255.255.0		

**注意** 一般情况下，[子网号不能为全0或全1](#)

### 4.3.2 使用子网时分组的转发

## 例4-4 P122

【例4-4】已知互联网和路由器 R<sub>1</sub> 中的路由表。  
主机 H<sub>1</sub> 向 H<sub>2</sub> 发送分组。  
试讨论 R<sub>1</sub> 收到 H<sub>1</sub> 向 H<sub>2</sub> 发送的分组后查找路由表的过程。



## 在划分子网情况下路由器转发分组的算法

- (1) 从收到的分组的首部提取**目的 IP 地址 D**。
- (2) 先用各网络的**子网掩码**和 D 逐位相“与”，看是否和相应的网络地址匹配。若匹配，则将分组直接**交付**。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**，则将分组传送给指明的下一跳路由器；否则，执行 (4)。
- (4) 对路由表中的每一行，将**子网掩码**和 D 逐位相“与”。若结果与该行的目的网络地址匹配，则将分组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**，则将分组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。

## 4.4 网际控制报文协议ICMP P128

- 网际控制报文协议ICMP (Internet Control Message Protocol)，为IP层的协议。
- ICMP允许主机或路由器报告差错情况和提供有关异常情况的报告。

## 4.4.1 ICMP报文的种类

- ICMP差错报告报文

差错报告报文共有4种：

1. 终点不可达
2. 时间超过
3. 参数问题
4. 改变路由（重定向）

- ICMP询问报文

询问报文共两种：

1. 回送请求和回答报文
2. 时间戳请求和回答报文

## 4.4.2 ICMP的应用举例

### PING (Packet InterNet Groper)

- 用来测试两个主机之间的连通性
- 使用ICMP回送请求与回送回答报文
- PING是应用层直接使用网络层ICMP的例子，没有通过运输层的TCP或UDP

## 4.5 互联网的路由选择协议

### 有关路由选择协议的几个基本概念

#### 理想的路由算法

- 关于“最佳路由”

#### 分层次的路由选择协议

## 自治系统AS

- **自治系统 AS 的定义：**在单一的技术管理下的一组路由器，而这些路由器使用一种 **AS 内部的路由选择协议** 和共同的度量以确定分组在该 AS 内的路由，同时还使用一种 **AS 之间的路由选择协议** 用以确定分组在 AS 之间的路由。
- 现在对自治系统 AS 的定义是强调下面的事实：尽管一个 AS 使用了多种内部路由选择协议和度量，但**重要的是一个 AS 对其他 AS 表现出的是一个单一的和一致的路由选择策略。**

## 路由选择协议

- **内部网关协议 IGP (Interior Gateway Protocol)**
  - 在一个自治系统**内部使用**的路由选择协议。
  - 目前这类路由选择协议使用得最多，如 **RIP 和 OSPF 协议**。
- **外部网关协议 EGP (External Gateway Protocol)**
  - 若源站和目的站处在不同的自治系统中，当数据报传到一个自治系统的边界时，就需要使用一种协议**将路由选择信息传递到另一个自治系统中**。这样的协议就是外部网关协议 EGP。
  - 在外部网关协议中目前使用最多的是 **BGP-4**。

### 4.5.2 内部网关协议RIP (掌握) P148

路由信息协议RIP (Routing Information Protocol)

- RIP 是一种**分布式的、基于距离向量的路由选择协议**。
- RIP 协议要求网络中的每一个路由器都要维护从它自己到其他每一个目的网络的**距离记录**

## RIP协议的三个特点

- (1) 仅和**相邻路由器**交换信息。
- (2) 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**。
- (3) 按固定的时间间隔**交换路由信息**，例如，**每隔 30 秒**。当网络拓扑发生变化时，路由器也及时向相邻路由器通告拓扑变化后的路由信息。

- RIP协议特点之一：好消息传播得快，坏消息传播得慢
- RIP存在的一个问题：当网络出现故障时，要经过比较长的时间（数分钟）才能将此信息传送到所有的路由器

## RIP协议的优缺点

### ■ 优点：

- 实现简单，开销较小。

### ■ 缺点：

- 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。
- “坏消息传播得慢”，使更新过程的收敛时间过长。

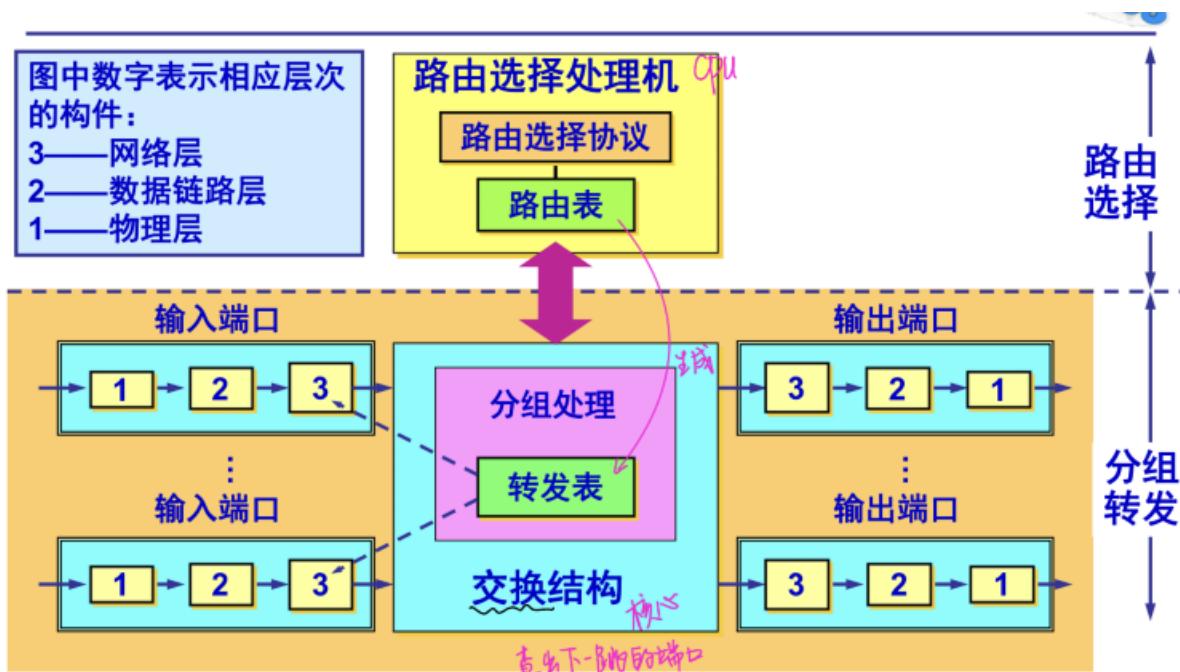
## 4.5.5 路由器的构成 P164

路由器的主要作用：

- 连通不同的网络
- 选择信息传送的线路

## 路由器的结构

典型路由器的结构：



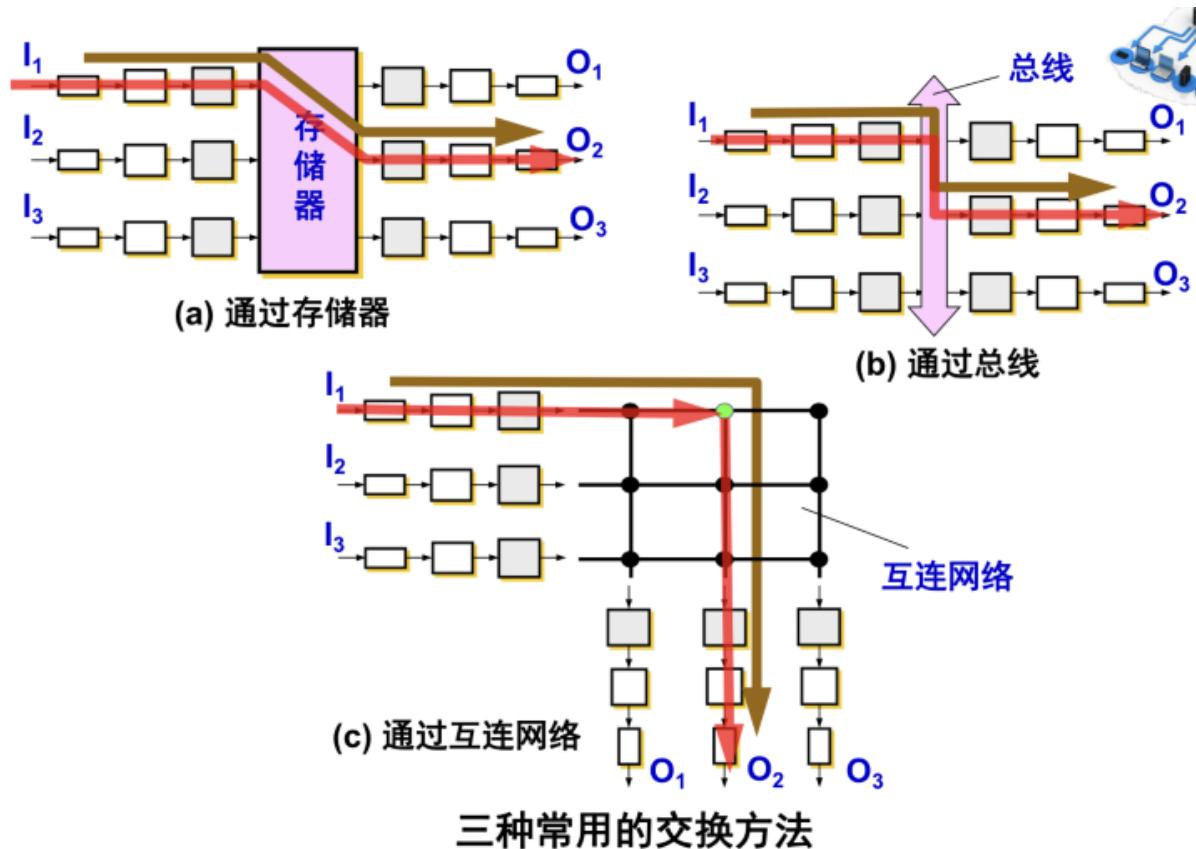
路由器的两大组成部分：

- **路由选择部分**：也叫做控制部分，其核心构件是路由选择处理机，其任务是：根据选定的路由选择协议构造路由表，同时经常或定期地和相邻路由器交换路由信息，不断更新和维护路由表
- **分组转发部分**：由**输入端口**、**输出端口**和**交换结构**三部分组成；交换结构又称交换组织，作用是根据转发表对分组进行处理

## 交换结构：路由器的关键构件

常用的交换方法：

- 通过存储器
- 通过总线
- 通过纵横交换结构



## 4.8 虚拟专用网VPN和网络地址转换NAT

P180

## 4.8.1 虚拟专用网VPN

### 本地地址与全球地址

- **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，而不需要向互联网的管理机构申请。
- **全球地址**——全球唯一的IP地址，必须向互联网的管理机构申请。
- **问题：**在内部使用的本地地址就有可能和互联网中某个IP地址重合，这样就会出现地址的二义性问题。
- **解决：**RFC 1918指明了一些**专用地址**(private address)。专用地址只能用作**本地地址**而不能用作**全球地址**。在互联网中的所有路由器，对目的地址是**专用地址**的数据报一律不进行转发。

### 专用IP地址

## RFC 1918 指明的专用 IP 地址

三个专用IP地址块：只能在局域网内使用

(1) 10.0.0.0 到 10.255.255.255

A类，或记为10.0.0.0/8，它又称为24位块

(2) 172.16.0.0 到 172.31.255.255

B类，或记为172.16.0.0/12，它又称为20位块

(3) 192.168.0.0 到 192.168.255.255

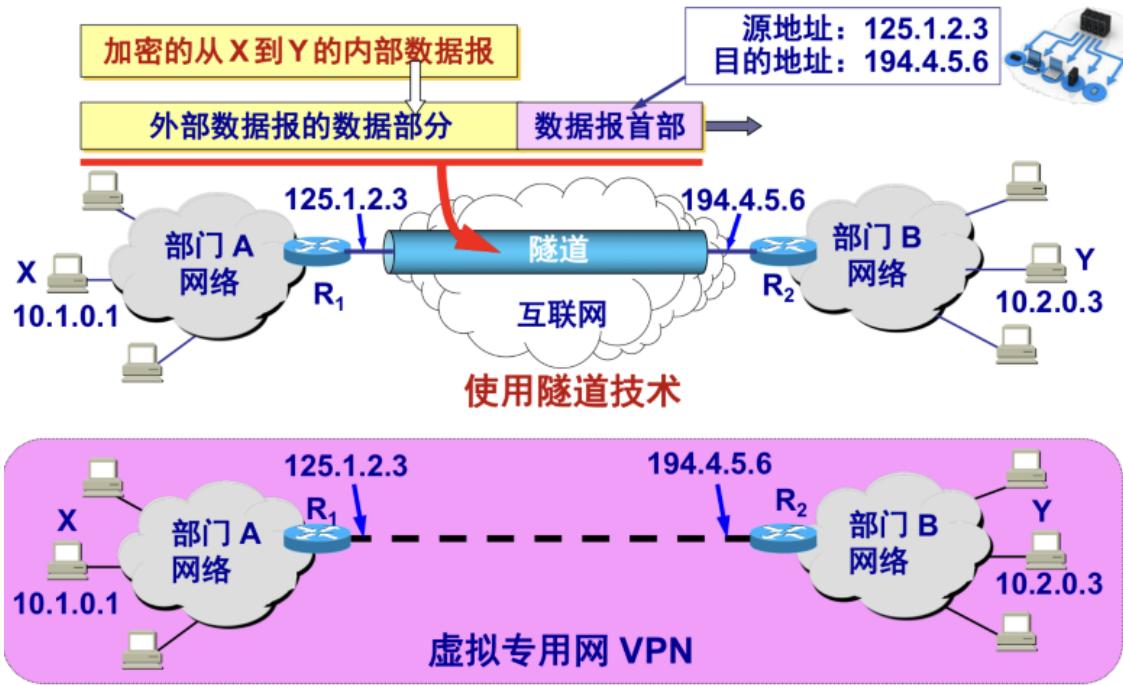
C类，或记为192.168.0.0/16，它又称为16位块

注 专用IP地址只能在局域网内部使用，只能用作本地地址

### 虚拟专用网VPN

利用公用的互联网作为本机构各专用网之间的通信载体，这样的专用网称为**虚拟专用网VPN** (Virtual Private Network)

- 用隧道技术实现虚拟专用网

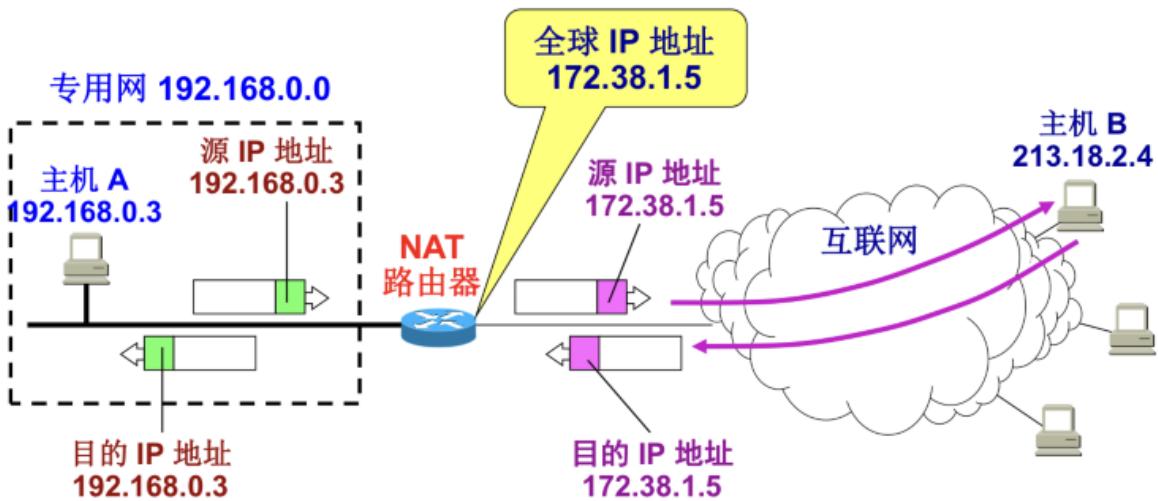


用隧道技术实现虚拟专用网

## 4.8.2 网络地址转换NAT（原理，和NAPT的区别）

网络地址转换NAT（Network Address Translation）：解决在专用网上使用专用地址的主机与互联网上主机的通信问题（无需加密）

- 需要在专用网连接到互联网的路由器上安装 NAT 软件。装有 NAT 软件的路由器叫做 **NAT路由器**，它至少有一个有效的外部 **全球IP地址**。
- 所有使用本地地址的主机在和外界通信时，都要在 NAT 路由器上将其**本地地址转换成全球IP地址**，才能和互联网连接。
- 当 NAT 路由器具有  $n$  个全球 IP 地址时，专用网内**最多可以同时有  $n$  台主机接入到互联网**。这样就可以使专用网内较多数量的主机，轮流使用 NAT 路由器有限数量的全球 IP 地址。
- 通过 NAT 路由器的通信必须由专用网内的主机发起。**专用网内部的主机不能充当服务器用**，因为互联网上的客户无法请求专用网内的服务器提供服务。
- 网络地址转换的过程



NAT 路由器的工作原理

## 网络地址与端口号转换NAPT

使用端口号的NAT称为**网络地址与端口号转换NAPT**（Network Address and Port Translation）

常用的NAT转换表同时利用上了运输层的端口号，可以使多个拥有本地地址的主机，共用一个NAT路由器上的全球IP地址，因而可以同时和互联网上的不同主机进行通信。

# 第5章 传输层

## 5.1 运输层协议概述

运输层的重要功能：复用和分用

两种不同的运输协议：

- 面向连接的TCP
- 无连接的UDP

### 5.1.2 运输层的两个主要协议 P13

- 用户数据包协议UDP (User Datagram Protocol)

- **UDP：一种无连接协议**
  - 提供无连接服务。
  - 在传送数据之前不需要先建立连接。
  - 传送的数据单位协议是 **UDP 报文或用户数据报**。
  - 对方的运输层在收到 UDP 报文后，不需要给出任何确认。
  - 虽然 **UDP 不提供可靠交付**，但在某些情况下 UDP 是一种最有效的工作方式。
- 传输控制协议TCP (Transmission Control Protocol)
  - **TCP：一种面向连接的协议**
    - 提供面向连接的服务。
    - 传送的数据单位协议是 **TCP 报文段 (segment)**。
    - **TCP 不提供广播或多播服务**。
    - **由于 TCP 要提供可靠的、面向连接的运输服务**，因此不可避免地增加了许多的开销。这不仅使协议数据单元的首部增大很多，还要占用许多的处理机资源。

## 用户数据报协议UDP

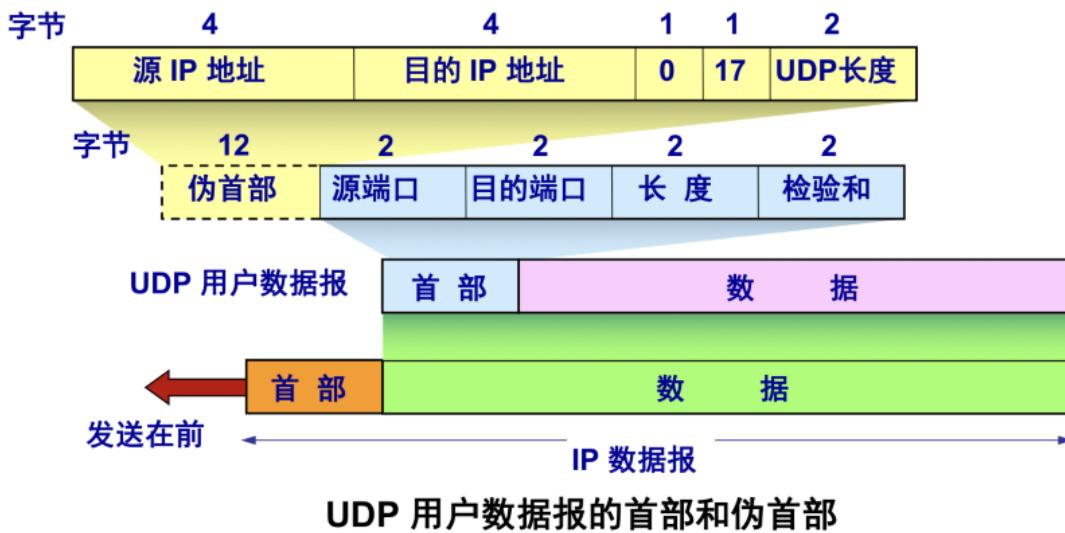
---

### UDP的主要特点

- (1) **UDP 是无连接的**，发送数据之前不需要建立连接，因此减少了开销和发送数据之前的时延。
- (2) **UDP 使用尽最大努力交付**，即不保证可靠交付，因此主机不需要维持复杂的连接状态表。
- (3) **UDP 是面向报文的**。UDP 对应用层交下来的报文，既不合并，也不拆分，而是保留这些报文的边界。UDP 一次交付一个完整的报文。
- (4) **UDP 没有拥塞控制**，因此网络出现的拥塞不会使源主机的发送速率降低。这对某些实时应用是很重要的。**很适合实时多媒体通信的要求**。
- (5) **UDP 支持一对一、一对多、多对一和多对多的交互通信**。
- (6) **UDP 的首部开销小**，只有 8 个字节，比 TCP 的 20 个字节的首部要短。

# UDP的头部格式

用户数据报 UDP 有两个字段：数据字段和首部字段。  
首部字段很简单，只有 8 个字节。



## 5.3 传输控制协议TCP概述

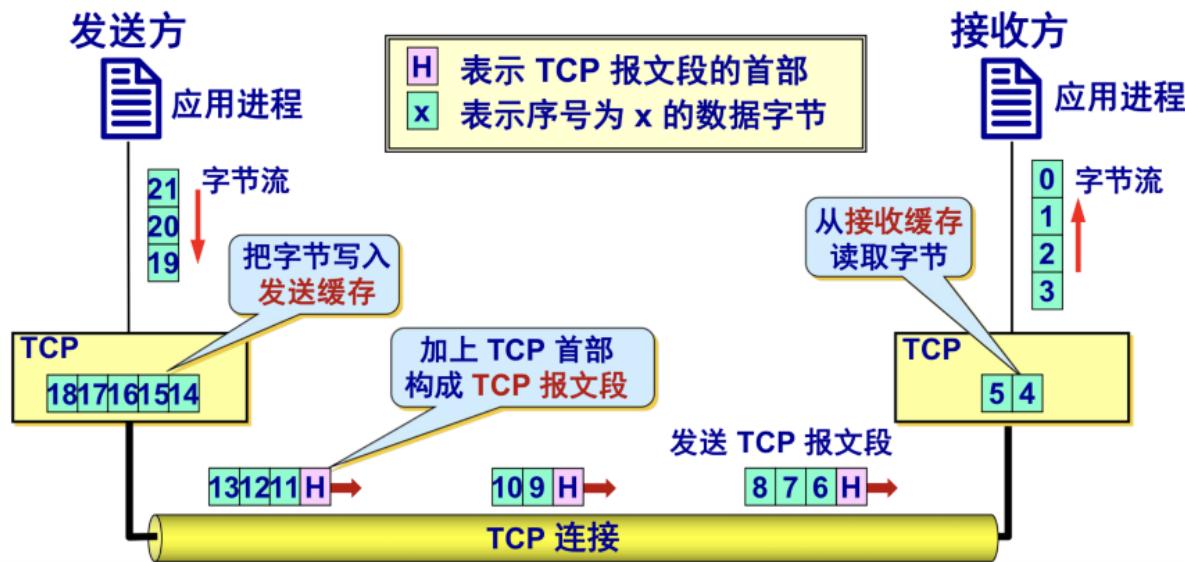
### 5.3.1 TCP最主要的特点

TCP面向流的概念（理解） P39

面向字节流：

- TCP中“流”指的是流入或流出进程的字节序列
- “面向字节流”的含义：虽然应用程序与TCP的交互是一次一个数据块，但TCP把应用程序交下来的数据看成仅仅是一串无结构的字节流

- TCP 不保证接收方应用程序所收到的数据块和发送方应用程序所发出的数据块具有对应大小的关系。
- 但接收方应用程序收到的字节流须和发送方应用程序发出的字节流完全一样。



## 5.4 可靠传输的工作原理 P46

### 5.4.1 停止等待协议

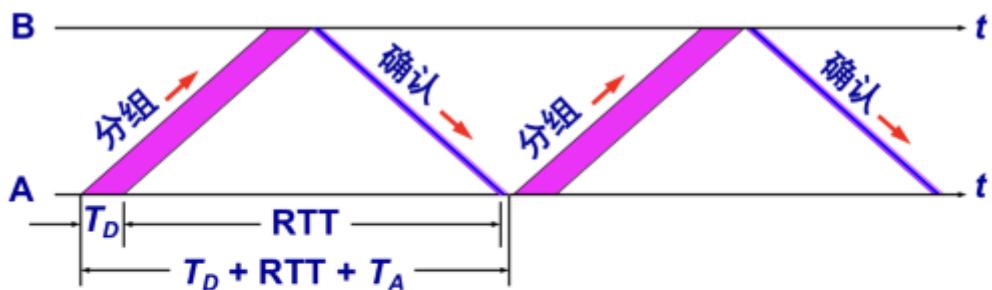
停止等待协议：每发送完一个分组就停止发送，等待对方的确认，在收到确认后再发送下一个分组。

- 无差错情况
- 出现差错

保证接收方正确收到数据：超时重传

- 确认丢失和确认迟到
- 信道利用率

停止等待协议的优点是简单，缺点是信道利用率太低：



停止等待协议的信道利用率太低

$$\text{信道利用率 } U = \frac{T_D}{T_D + \text{RTT} + T_A} \quad (5-3)$$

提高传输效率：流水线传输，发送方可连续发送多个分组，不必每发完一个分组就停顿下来等待对方的确认。

## 5.4.2 连续ARQ协议

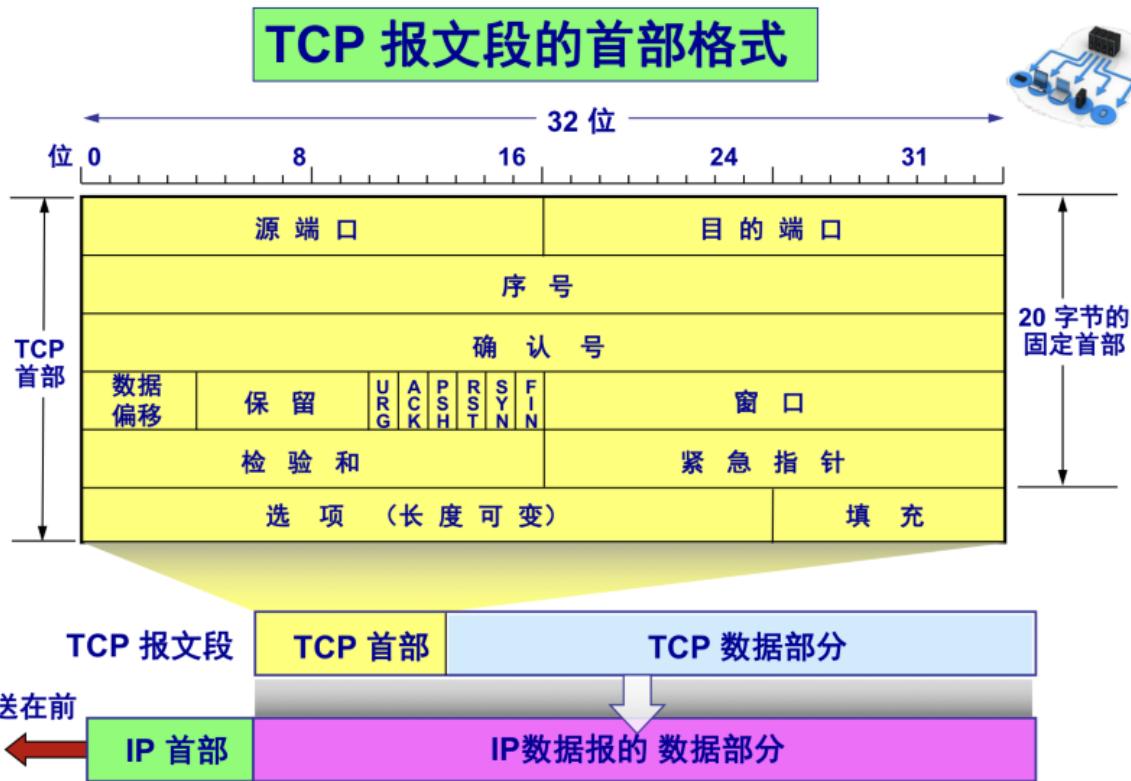
TCP协议的精髓：滑动窗口协议



### 连续 ARQ 协议的工作原理

- 发送方的发送窗口：位于发送窗口内的分组可以连续发送出去，不需要等待对方的确认
- 累积确认：不必对收到的分组逐个发送确认，而是对按序到达的最后一个分组发送确认，表示到这个分组为止的所有分组都已正确收到
- Go-back-N (回退N)

## TCP报文段的头部格式



## 5.6 TCP可靠传输的实现

### 5.6.1 以字节为单位的滑动窗口

### 5.6.2 超时重传时间的选择 P98

TCP超时重传时间的设置：

- 一个报文段发出的时间和收到相应确认的时间，两个时间之差为**报文段的往返时间RTT**
- 加权平均往返时间 $RTT_s$ :  $RTT_s$ 的初值为第一次测量到的 $RTT$ 样本，此后按以下公式迭代要会算：

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

其中 $0 \leq \alpha \leq 1$ ，若 $\alpha$ 接近于0，则RTT值更新慢，反之更新较快。

RFC 2988推荐 $\alpha = 0.125$

- 超时重传时间RTO (Retransmission Time-Out) : 略大于 $RTT_s$

## 5.6.3 选择确认ACK

# TCP的流量控制

---

- 一般来说，我们总是希望数据传输得更快一些。
  - 但如果发送方把数据发送得过快，接收方就可能来不及接收，这就会造成数据的丢失。
- 所谓流量控制（flow control）就是让发送方的发送速率不要太快，要让接收方来得及接收。
- 利用滑动窗口机制可以很方便地在TCP连接上实现对发送方的流量控制。
  - TCP接收方利用自己的接收窗口的大小来限制发送方发送窗口的大小。
  - TCP发送方收到接收方的零窗口通知后，应启动持续计时器。持续计时器超时后，向接收方发送零窗口探测报文。

## 5.8 TCP的拥塞控制 重要 P118

---

### 5.8.1 拥塞控制的一般原理

- 拥塞控制与流量控制的区别
- 开环控制与闭环控制
- **开环控制方法**就是在设计网络时事先将有关发生拥塞的因素考虑周到，力求网络在工作时不产生拥塞。
- **闭环控制方法**是基于反馈环路的概念。属于闭环控制的有以下几种措施：
  - (1) 监测网络系统以便检测到拥塞在何时、何处发生。
  - (2) 将拥塞发生的信息传送到可采取行动的地方。
  - (3) 调整网络系统的运行以解决出现的问题。

### 5.8.2 TCP的拥塞控制方法

- TCP 采用**基于窗口的方法**进行拥塞控制。该方法属于闭环控制方法。
- TCP发送方维持一个**拥塞窗口 CWND (Congestion Window)**
  - 拥塞窗口的大小取决于网络的拥塞程度，并且动态地在变化。
  - 发送端利用**拥塞窗口**根据网络的拥塞情况调整发送的数据量。
  - 所以，发送窗口大小不仅取决于接收方公告的接收窗口，还取决于网络的拥塞状况，所以真正的发送窗口值为：

**真正的发送窗口值 = Min(公告窗口值, 拥塞窗口值)**  
**公告窗口就是前面提到的接收方窗口 RWND**

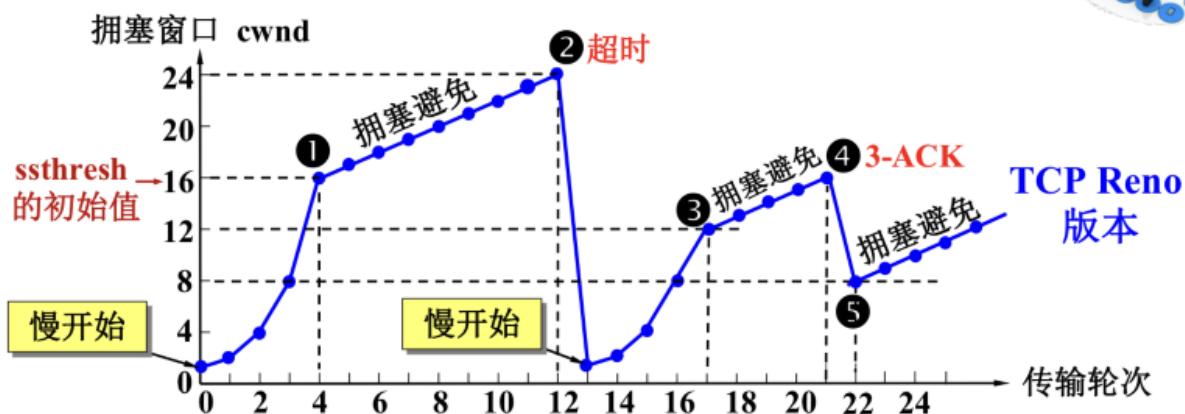
TCP拥塞控制算法（4种）：

- 慢开始
- 拥塞避免
- 快重传
- 快恢复

**图：慢开始和拥塞避免算法的实现举例（重点大题，会画）**

P139

### 慢开始和拥塞避免算法的实现举例



- TCP连接初始化时，拥塞窗口cwnd置为1，慢开始门限ssthresh初始值置为16，此时 $cwnd < ssthresh$ ，执行慢开始算法，拥塞窗口cwnd随传输轮次按指数规律增长
- 点1：当拥塞窗口增长到慢开始门限值ssthresh时，改为执行拥塞避免算法，此时拥塞窗口将按线性规律增长
- 点2：当拥塞窗口 $cwnd = 24$ ，网络出现超时，发送方判断为网络拥塞，调整门限值 $ssthresh = cwnd/2 = 12$ ，设置拥塞窗口

$cwnd = 1$ , 重新进入慢开始阶段

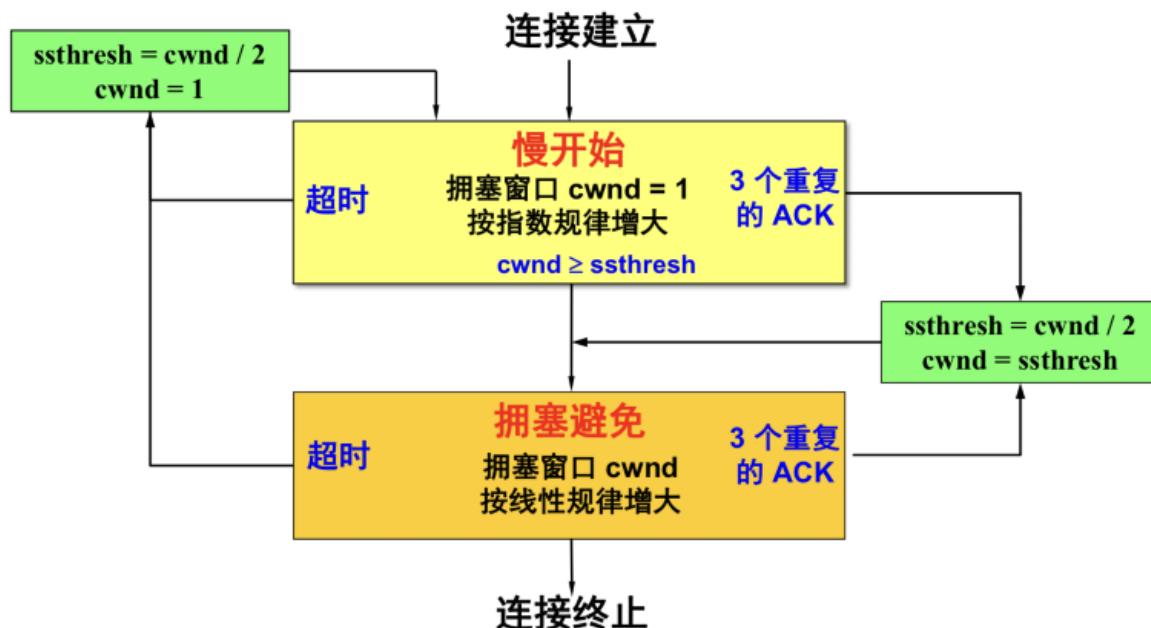
- 点4: 发送方一连收到3个对同一个报文段的重复确认, (3-ACK) , 此时发送方改为执行快重传和快恢复算法, 调整门限值  
 $ssthresh = cwnd/2 = 8$ , 设置拥塞窗口 $cwnd = ssthresh = 8$ , 直接执行拥塞避免算法

快重传算法: 发送方一连收到三个对报文段M的重复确认, 立即重传报文段M

快恢复算法:

- 当发送端收到连续三个重复的确认时, 由于发送方现在认为网络很可能没有发生拥塞, 因此现在不执行慢开始算法, 而是执行快恢复算法 FR (Fast Recovery) 算法:
  - (1) 慢开始门限  $ssthresh =$  当前拥塞窗口  $cwnd / 2$  ;
  - (2) 新拥塞窗口  $cwnd =$  慢开始门限  $ssthresh$  ;
  - (3) 开始执行拥塞避免算法, 使拥塞窗口缓慢地线性增大。

### TCP拥塞控制流程图 (理解) P157



### 5.8.3 主动队列管理AQM

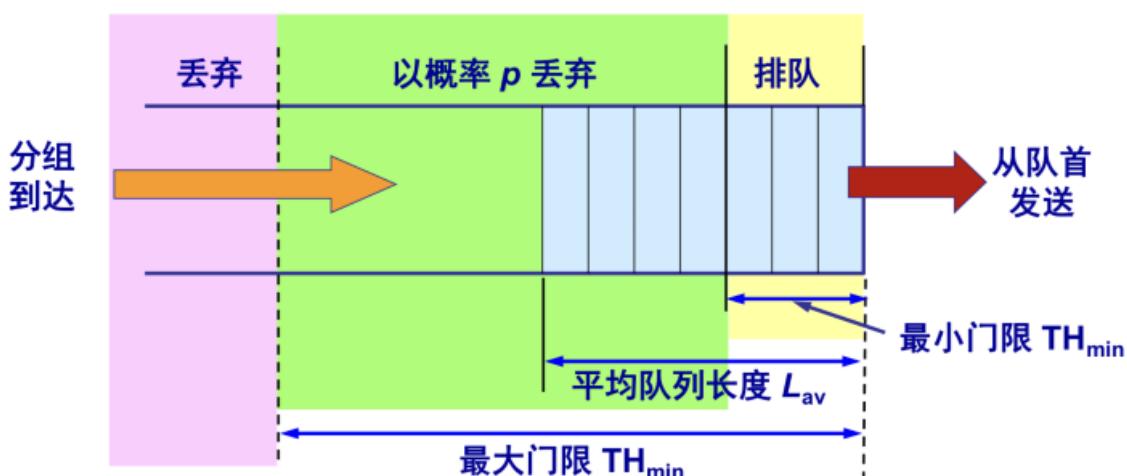
## 全局同步 P161

- 更为严重的是，在网络中通常有很多的 TCP 连接，这些连接中的报文段通常是复用在网络层的 IP 数据报中传送的。
- 在这种情况下，若发生了路由器中的尾部丢弃，就可能会同时影响到很多条 TCP 连接，结果使这许多 TCP 连接在同一时间突然都进入到慢开始状态。这在 TCP 的术语中称为**全局同步** (global synchronization)。
- **全局同步**使得全网的通信量突然下降了很多，而在网络恢复正常后，其通信量又突然增大很多。

## 随机早期检测RED (特点) P164

随机早期检测RED (Random Early Detection)

RED 将路由器的到达队列划分成为三个区域：



## 5.9 TCP的运输连接管理

# 第6章 应用层

## 6.1 域名系统DNS

### 6.1.1 域名系统概述

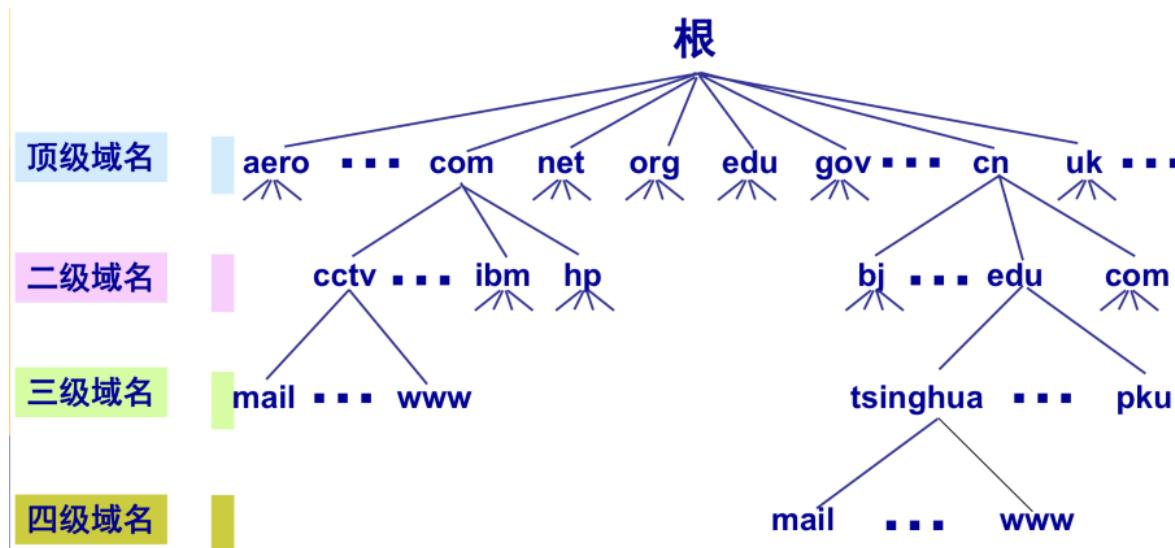
域名系统DNS (Domain Name System)

## 6.1.2 互联网的域名结构

顶级域名TLD (Top Level Domain) :

- 国家顶级域名nTLD
- 通用顶级域名gTLD
- 基础结构域名（又称反向域名，只有一个：arpa）

互联网的域名空间：



## 6.1.3 域名服务器

域名服务器：[域名](#) → [IP地址](#)

域名服务器的四种类型：

1. 根域名服务器
2. 顶级域名服务器
3. 权限域名服务器
4. 本地域名服务器

## 6.2 文件传送协议

文件传送协议FTP (File Transfer Protocol)

## 6.2.1 FTP概述

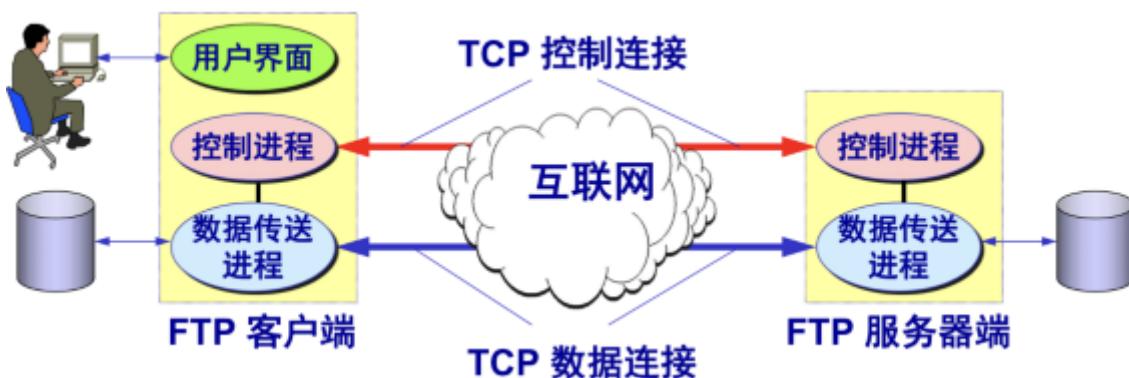
## 6.2.2 FTP的基本工作原理

### FTP特点

- 文件传送协议 FTP 只提供文件传送的一些基本的服务，它使用 TCP 可靠的运输服务。
- FTP 的主要功能是减少或消除在不同操作系统下处理文件的不兼容性。
- FTP 使用**客户服务器方式**。一个 FTP 服务器进程可同时为多个客户进程提供服务。FTP 的服务器进程由两大部分组成：**一个主进程**，负责接受新的请求；另外有**若干个从属进程**，负责处理单个请求。

### FTP使用的两个TCP连接

- **控制连接**在整个会话期间一直保持打开，FTP 客户发出的传送请求通过控制连接发送给服务器端的控制进程，但控制连接不用来传送文件。
- 实际用于传输文件的是“**数据连接**”。服务器端的控制进程在接收到 FTP 客户发送来的文件传输请求后就创建“**数据传送进程**”和“**数据连接**”，用来连接客户端和服务器端的数据传送进程。
- 数据传送进程实际完成文件的传送，在传送完毕后关闭“**数据传送连接**”并结束运行。



## 6.2.3 简单文件传送协议TFTP

# 6.4 万维网WWW

---

## 6.4.1 万维网概述

### 万维网需解决的问题

(1) 怎样标志分布在整个互联网上的万维网文档？

- 使用**统一资源定位符 URL (Uniform Resource Locator)** 来标志万维网上的各种文档。
- 使每一个文档在整个互联网的范围内具有唯一的标识符 URL。

(2) 用何协议实现万维网上各种超链的链接？

- 在万维网客户程序与万维网服务器程序之间进行交互所使用的协议，是**超文本传送协议 HTTP (HyperText Transfer Protocol)**。
- HTTP 是一个应用层协议，它使用 TCP 连接进行可靠的传送。

(3) 怎样使各种万维网文档都能在互联网上的各种计算机上显示出来，同时使用户清楚地知道在什么地方存在着超链？

- **超文本标记语言 HTML (HyperText Markup Language)** 使得万维网页面的设计者可以很方便地用一个超链从本页面的某处链接到互联网上的任何一个万维网页面，并且能够在自己的计算机屏幕上将这些页面显示出来。

(4) 怎样使用户能够很方便地找到所需的信息？

- 为了在万维网上方便地查找信息，用户可使用各种的**搜索工具**（即**搜索引擎**）。

## 6.4.2 统一资源定位符URL

统一资源定位符URL (Uniform Resource Locator)

## 6.4.3 超文本传送协议HTTP

超文本传送协议HTTP (HyperText Transfer Protocol)

## 6.4.4 万维网的文档

### 动态万维网文档 P91

动态万维网文档：由应用程序[动态创建](#)

- **静态文档**是指该文档创作完毕后就存放在万维网服务器中，在被用户浏览的过程中，内容不会改变。
- **动态文档**是指文档的内容是在浏览器访问万维网服务器时才由应用程序动态创建。
- 动态文档和静态文档之间的主要差别体现在**服务器**一端。这主要是文档内容的生成方法不同。而从浏览器的角度看，这两种文档并没有区别。

## 6.4.5 万维网的信息检索系统

- 全文检索搜索引擎
- **全文检索搜索引擎**是一种纯技术型的检索工具。它的工作原理是通过搜索软件到互联网上的各网站收集信息，找到一个网站后可以从这个网站再链接到另一个网站。然后按照一定的规则建立一个很大的在线数据库供用户查询。
- 用户在查询时只要输入关键词，就从已经建立的**索引数据库上进行查询**（并不是实时地在互联网上检索到的信息）。
- 分类目录搜索引擎
- **分类目录搜索引擎**并不采集网站的任何信息，而是利用各网站向**搜索引擎**提交的网站信息时，填写的关键词和网站描述等信息，经过人工审核编辑后，如果认为符合网站登录的条件，则输入到分类目录的数据库中，供网上用户查询。
- 分类目录搜索也叫做**分类网站搜索**。
- 垂直搜索引擎

- **垂直搜索引擎** (Vertical Search Engine) 针对某一特定领域、特定人群或某一特定需求提供搜索服务。
- 垂直搜索也是提供关键字来进行搜索的，但被放到了一个行业知识的上下文中，返回的结果更倾向于信息、消息、条目等。

## 6.5 电子邮件

### 6.5.2 简单邮件传送协议SMTP (Simple Mail Transfer Protocol)

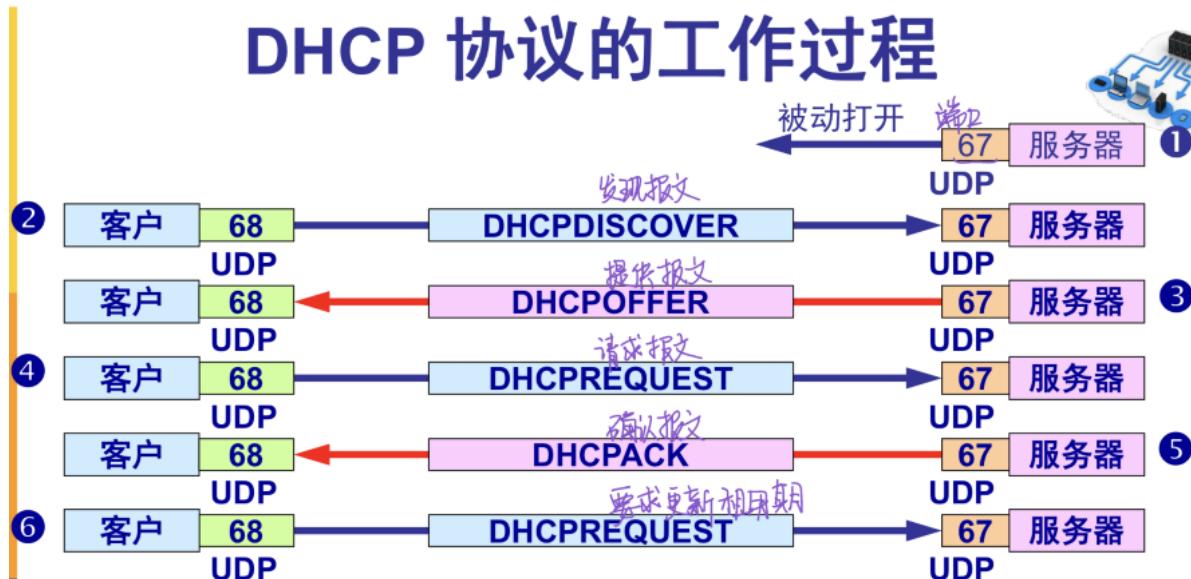
1. **连接建立**: 连接是在发送主机的 SMTP 客户和接收主机的 SMTP 服务器之间建立的。SMTP不使用中间的邮件服务器。
2. **邮件传送**
3. **连接释放**: 邮件发送完毕后，SMTP 应释放 TCP 连接。

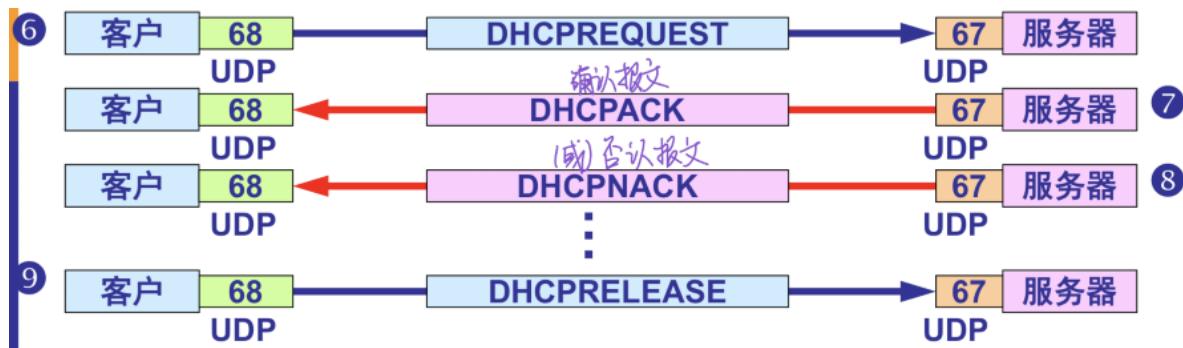
### 6.5.4 邮件读取协议POP3和IMAP

## 6.6 动态主机配置协议DHCP

动态主机配置协议DHCP (Dynamic Host Configuration Protocol)

### DHCP协议的工作过程





# 第9章 无线网络和移动网络

WiFi信号满格为什么网速慢？

1. 无线路由器的[信号频道过于拥挤](#)，导致网络速度下降。这是因为许多设备都默认连接2.4GHz频段，如果该频段上的设备过多，就会导致通信质量下降。
2. 家里的各种电器设备、智能终端和金属制品都可能[对Wi-Fi信号产生干扰](#)，从而影响网络质量。尽管信号强度可能仍然满格，但由于受到干扰，实际的网络速度可能会变慢。
3. [路由器本身的性能问题](#)也可能是导致网速慢的原因。例如，路由器的网络处理能力不足或者配置不当，都可能导致网速降低。

## 9.1 无线局域网WLAN

### 9.1.1 无线局域网的组成

无线局域网WLAN (Wireless Local Area Network) 分为两大类：

- [有固定基础设施的WLAN](#)

有接入点AP (Access Point) 、基站

- [无固定基础设施的WLAN](#)

[注](#) 802.11，俗称wifi

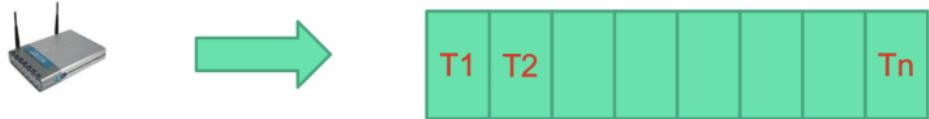
### 9.1.3 802.11局域网的MAC层协议

CSMA/CA (Collision Avoidance, 碰撞避免) 协议是CSMA/CD协议 (载波监听多点接入/碰撞检测) 的改进

### CSMA/CA 协议基本原理



争用窗口



- AP为每一个站点分配**发送时隙**，（又称为每个站点在**争用窗口中**）
- 每个站点在发送前先检查信道**是否空闲**：如果空闲，等待一个帧间间隔时间后直接发送；如果不空闲，执行**二级制指数退避算法**，在T1-Tn个时隙中选择一个；
- 一旦发送就要把一帧发送完，**不能中途停止**
- 任何时刻**只有一个站点**发送数据帧
- 在MAC层进行**差错控制和重传**

#### 二进制指数退避算法

$$\text{时隙}_i = \text{rand}(0, 2^{2+i} - 1)$$

- 第*i*次退避就在 $2^{2+i}$ 个时隙中随机地选择一个，即：  
第*i*次退避是在时隙 $\{0, 1, \dots, 2^{2+i}-1\}$ 中随机地选择一个。
- 第1次退避是在8个时隙（而不是2个）中随机选择一个。
- 第2次退避是在16个时隙（而不是4个）中随机选择一个。
- 当时隙编号达到255时（这对应于第6次退避）就不再增加了。
- 这里决定退避时间的变量*i*称为**退避变量**。

## 9.2 无线个人区域网WPAN

无线个人区域网WPAN (Wireless Personal Area Network)

## **9.3 无线城域网WMAN**

---

无线城域网WMAN (Wireless Metropolitan Area Network)

## **9.4 蜂窝移动通信网**

---

## **9.5 两种不同无线上网**

---

# **第10章 工业控制网络**

---

## **工业自动控制系统简介**

---

### **10.2 传统工业控制网络**

---

三种现场总线 + CAN总线

- Modbus现场总线
- Profibus现场总线：工厂自动化
- DeviceNet现场总线
- CAN总线：汽车工业

#### **10.2.1 传统工业控制网络简介**

现场总线的定义：指安装在制造或过程区域的现场装置与控制室内的自动控制装置之间数字式、串行、多点通信的数据总线。

#### **10.2.2 Modbus现场总线**

#### **10.2.3 Profibus现场总线**

## ■ 2. PROFIBUS的家族成员

- PROFIBUS-PA

应用于过程控制系统

- PROFIBUS-FMS

应用于车间监控级通信

- PROFIBUS-DP

应用于设备级的高速数据传输

### 10.2.4 DeviceNet现场总线

### 10.2.5 CAN总线

## 工业以太网

---

