

计网

考纲能力要求等级

了解：只需要知道有这么个事物，大概的内容就可以了，一般考选择题

理解：知道并且需要知道为什么，之间的关系，怎么形成，一般简答题和辨析

掌握：必考，更高的层次，是自己内化后的东西，一般论述和辨析

熟悉：需要记忆的，一般简答题和选择

计算机网络概述

计算机网络的定义和内涵（掌握）

- 计算机网络的定义

计算机网络主要是由一些通用的、【可编程的硬件】互连而成的，而这些硬件并非专门用来实现某一特定目的。这些可编程的硬件能够用来传递多种不同的数据，并能支持广泛的和日益增长的应用

- 内涵

- a. 上述的“可编程的硬件”表明这种硬件一定包含中央处理机 CPU
- b. 计算机网络所连接的硬件，并不限于一般的计算机，而是包括了智能手机。
- c. 计算机网络并非专门用来传送数据，而是能够支持很多种的应用（包含了今后可能出现的各种应用）

计算机网络的分类（了解）

- 按照网络的作用范围

- WAN（广域网）/远程网
 - 作用范围：几十到几千公里【跨国】
 - 广域网是互联网的核心部分。连接广域网各节点交换机的链路一般都是高速链路
- MAN（城域网）
 - 作用范围：5~50km【城市】
 - 多采用以太网技术
- LAN（局域网）

- 作用范围：如1 km 左右
- 举例：如【校园网、企业网】
- PAN（个人局域网）
 - 作用范围：【10m左右】
 - 在个人工作的地方把属于个人使用的电子设备用无线技术连接起来
- 按照网络的使用者
 - 公用网/公众网：电信公司出资建造的大型网络，【对外提供服务】
 - 专用网：满足本单位的业务工作的网络，【不对外提供服务】
- 接入网/本地接入网/居民接入网
 - 接入网【既不属于互联网的核心部分，也不属于互联网的边缘部分】
 - 接入网是从某个用户端系统到互联网中的第一个路由器之间的一种网络

协议、层次、接口与网络体系结构的基本概念（掌握）

- 协议
 - 网络协议即协议，是为进行网络中的数据交换而建立的规则
 - 构成协议的三要素
 - 语法：即数据与控制信息的结构或格式（信息格式）
 - 语义：即需要发出何种控制信息，完成何种动作，以及做出何种响应（动作）
 - 同步：即事件实现顺序的详细说明
- 层次

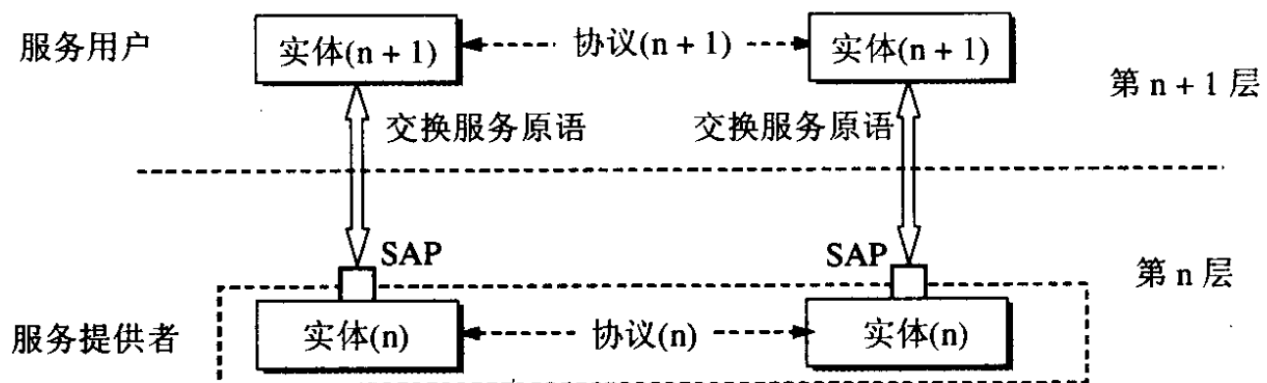


图 1-18 相邻两层之间的关系

- 第 n 层向第 n+1 层提供服务。
- 第 n 层的实体（n）之间使用协议（n）进行通信。第 n+1 层的实体之间使用协议（n+1）进行通信

- **接口**：在同一系统中相邻两层的实体进行交互（即交互信息）的地方，通常称为服务访问点SAP（Service Access Point）。服务访问点实际上就是逻辑接口
- **网络结构体系**：计算机网络的各层及其协议的集合就是网络的体系结构

TCP/IP 参考模型的层次划分、各层的基本服务功能与主要协议（了解）

• 各层基本功能

1. 应用层：通过应用进程间的交互来完成特定网络应用
2. 运输层：负责向两台主机中进程之间的通信提供通用的数据传输服务
3. 网际层
 - a. 为分组交换网上的不同主机提供通信服务
 - b. 选择合适的路由，使源主机运输层所传下来的分组，能够通过网络中的路由器找到目的主机
4. 网络接口层：解决不同网络的互连问题

• 各层的基本服务功能与主要协议

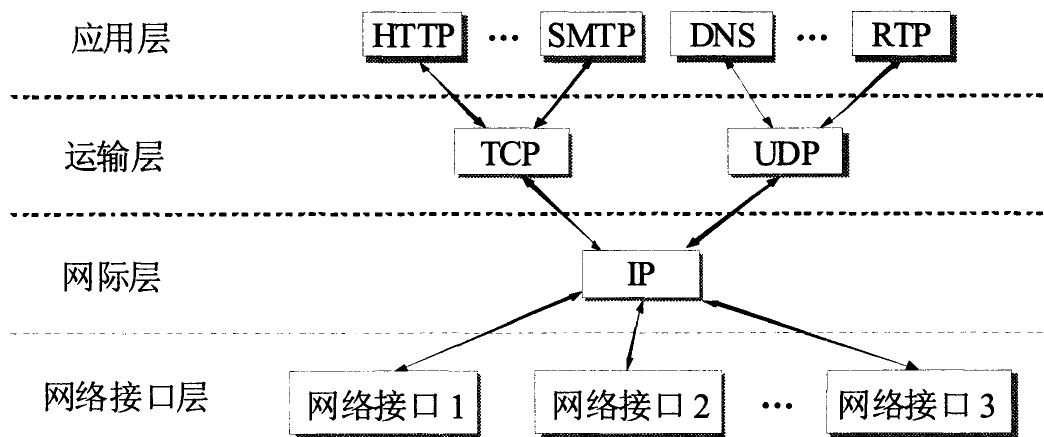


图 1-24 沙漏计时器形状的 TCP/IP 协议族示意

○ 应用层协议：

- 域名协议 DNS
- 文件传输 FTP
- 超文本传输协议 HTTP
- 电子邮件协议 SMTP
- 动态主机配置协议 DHCP

计算机网络体系结构（补充）

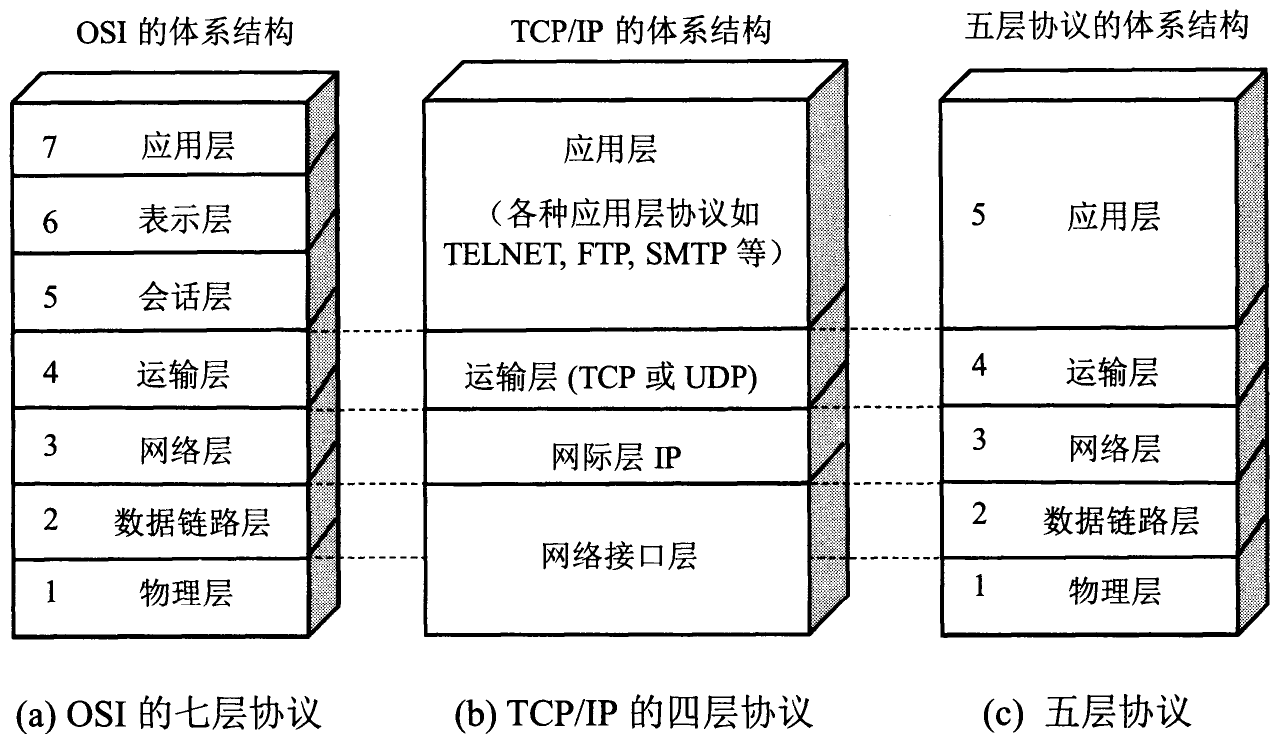


图 1-18 计算机网络体系结构

1. 物理层

数据通信的相关概念和知识，通信技术基本原理、通信模型等（了解）

- 数据通信系统的模型
 - 数据通信系统的三个组成部分

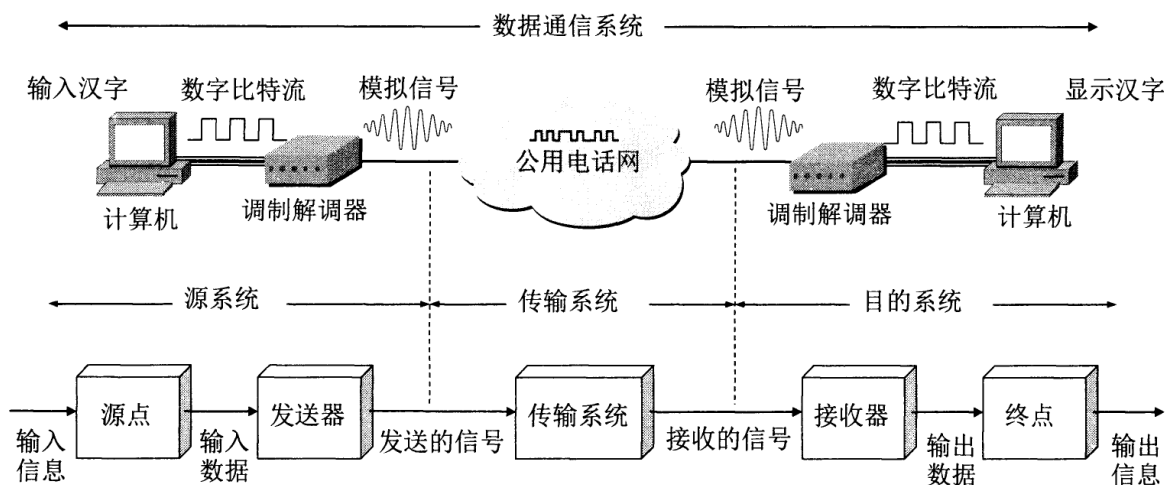


图 2-1 数据通信系统的模型

- 1、源系统（或发送端、发送方）

- 源点（源站、信源）：源点设备产生要传输的数据
 - 发送器：源点的设备经过发送器编码后才能在传输系统中传输
- 2、传输系统（或传输网络）
- 3、目的系统（接收端、接收方）
 - 接收器：接收传输系统传输的信号，并把它转为能被目的设备处理的信息
 - 终点（目的站、信宿）：终点设备从接收器获取传送来的数字比特流，然后把信息输出
- 常用术语
 - 信息：通信的目的是传送信息
 - 数据：数据是运送信息的实体
 - 信号：信号是数据的电气或电磁表现
 - 码元：
 - 在使用时间域的波形表示数字信号时，代表不同离散数值的基本波形被称为码元。
 - 在使用二进制编码时，只有两种不同类型的码元，一种代表状态0，一种代表状态1
- 信号分类
 - 模拟信号（或连续信号）：代表消息的参数的取值是连续的
 - 数字信号（或离散信号）：代表消息的参数取值是离散的
- 有关信道的几个基本概念
 - 从通信双方信息交互的方式来看，通信有三种基本方式
 - 1、单向通信【单工通信】
 - 只能有一个方向的通信而没有反方向的交互
 - 举例：广播、电视
 - 2、双向交替通信【半双工通信】
 - 通信的双方都可以发送信息，但是不能双方同时发送信息
 - 举例：对讲机
 - 3、双向同时通信【全双工通信】
 - 通信的双方可以同时发送和接收信息
 - 举例：手机
 - 基带信号
 - 来自信源的信号就是基带信号
 - 基带信号需要进行调制。因为基带信号往往有很多低频或直流成分，信道不能传输
 - 调制分为两大类

1. 基带调制（编码）

- 仅对基带信号的波形进行变换，使它能与信号特性相适应。变换的信号仍然是基带信号。
- 由于基带调制是把数字信号转为另一种形式的数字信号，所以这种过程也被称为【编码】
- 【常用的编码方式】
 - 不归零制
 - 归零制
 - 曼彻斯特编码
 - 差分曼彻斯特编码

2. 带通调制

- 带通调制需要使用载波进行调制，把基带信号的频率范围搬移到较高的频段，并转为模拟信号。
- 经过载波调制的信号称为带通信号
- 【基本的带通调制方法】
 - 调幅（AM）
 - 调频（FM）
 - 调相（PM）

• 信道的极限容量

- 1、信道能够通过的频率范围
 - 码间串扰：发送信号波形受到干扰，导致接收信号波形失真无法识别
 - 【信道的频带越宽，越能避免码间串扰】
- 2、信噪比
 - 【根据香农公式，信噪比越大，信息极限传输速率就越高】
 - 【根据香农公式，可以让每一个码元携带更多比特的信息量】

各种传输介质的特点（理解）

• 导引型传输介质

a. 双绞线

- 类型：屏蔽双绞线、无屏蔽双绞线
- 特点
 - 越粗信号传的越好，越粗信号传的越远

- 通信距离几到十几公里，传输速率每秒几个兆比特
- 物美价廉，使用广泛
- b. 同轴电缆
 - 抗干扰性好
 - 有线电视在使用
 - 高质量的带宽接近 1 GHz
- c. 光缆
 - 多模光纤
 - 单模光纤。【单模光纤更细更贵更好！】
- 架空明线
 - 方法落后，快要淘汰。老少偏穷地区还在用
- 非导引型传输介质
 - 短波通信
 - 靠电离层的反射。这种通信靠天吃饭，效果差，速率低
 - 微波通信
 - 【地面微波接力通信】
 - 通信距离只有 50 km，需要使用【天线塔】把信号放大
 - 电话、电报等都在用
 - 卫星通信
 - 使用卫星代替天线塔放大信号
 - 较大的传播时延
 - 举例：美国的GPS、中国北斗、马斯克的星链

时分复用，频分复用技术等概念（了解）

- 复用就是共享信道
- 频分复用
 - 【不同的用户分配不同的频带】。这样一来，所有用户在同一的时间占用的是不同的频带宽度。
 - 在使用频分复用时，若每一个用户占用的带宽不变，则当复用的用户增加时，复用后的信道总带宽就变宽。如电话通信时每一个标准话路的带宽是 4kHz，若有 1000 个用户进行频分复用，则复用后的总带宽就是 4MHz
- 时分复用

- 同步时分复用
 - 【不同的用户在不同的时间占用同样的频带宽度。】
 - 使用时分复用时，每一个时分复用帧的长度是不变的，始终是 125 us。若有 1000 个用户进行时分复用，则每一个用户分到的时隙宽度就是 125 us 的千分之一
 - 时分复用可能会造成线路资源的浪费。因为分配给用户信道后，用户没数据传输。等到时间到期了，用户有数据了但是没信道了，只能等到下一次再传送。
- 【异步时分复用】/统计时分复用
 - 统计时分复用是改进版的时分复用，可以提高信道的利用率。
 - 【统计时分复用不是固定分配时隙，而是按需动态分配时隙。】所以又被称为异步时分复用。而普通的时分复用被称为同步时分复用。
- 波分复用
 - 波分复用就是光的频分复用。具体来说，【就是用一根光纤来同时传输多个频率很接近的光载波信号。】
 - 密集波分复用
 - 现在已经能做到在一根光纤上复用十几路的光载波信号
 - 如，每一路的数据率是 40 Gbit/s，使用密集波分复用后，如果在一根光纤上复用 64 路，就能获得 2.56Tbit/s 的数据率
- 码分复用（码分多址）
 - 【各用户使用不同的码型】，所以各用户在同样的时间使用同样的频带进行通信不会造成干扰
 - 抗干扰能力强，用于军事、无线局域网等

2. 数据链路层（重点）

数据链路层的概念和知识（掌握）

- 数据链路层使用的两种信道类型
 - 1、点对点信道：这种信道使用一对一的点对点的通信方式
 - 2、广播信道：这种信道使用一对多的广播通信方式
- 点对点信道的数据链路层进行通信的主要步骤

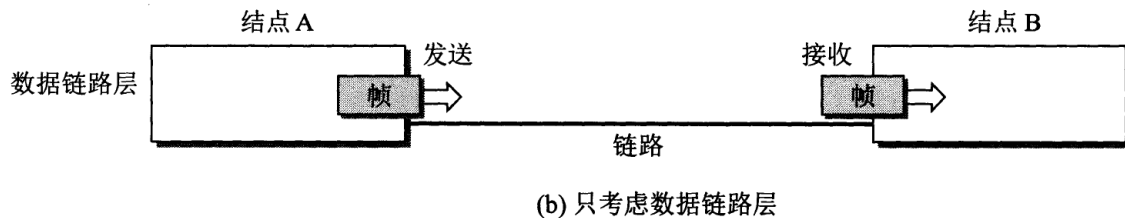


图 3-3 使用点对点信道的数据链路层

○

- 1、结点 A 的数据链路层把网络层交下来的 IP 数据报添加首部和尾部封装成帧。
- 2、结点 A 把封装好的帧发送给结点 B 的数据链路层
- 3、若结点 B 的数据链路层收到的帧无差错，则从收到的帧里提取出 IP 数据报交给上面的网络层；否则丢弃这个帧。

• **【数据链路层的三个基本问题】**

1. 封装成帧

- 封装成帧就是在一段数据的前后分别添加首部和尾部，这样就构成了一个帧。
- 首部和尾部的一个重要作用是帧定界（即确定帧的界限）。
- **【帧是数据链路层的协议数据单元】**
- 数据链路层的帧长=帧首部+帧的数据部分+帧尾部
- **【帧界定符】**
 - 帧定界可以使用特殊的帧定界符
 - 特殊的帧定界符
 - 首部开始符 SOH (Start Of Header)：表示帧开始
 - 尾部结束符 EOT (End Of Transmission)：表示帧结束
 - (SOH 和 EOT 并不是三个字符，而是在 ASCII 表中挑了两个字符代表 SOH 和 EOT。)
 - 接收端通过帧定界符判断收到的帧是否完整。如果是不完整的帧，则丢弃。

2. 透明传输

- 什么是透明？
 - 某个实际存在的事物看起来却像好像不存在一样（举例：玻璃）
 - 透明传输：无论什么样的比特组合的数据，都能按照原样没有差错地通过这个数据链路层。
- 透明传输解决的问题
 - 数据链路层所传输的数据如果有字符 SOH 或 EOT 话，会造成帧定界错误
 - 解决方法：**【字符填充】**

- 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”
- 接收端的数据链路层在把数据送往网络层之前删除这个插入的转义字符。
- 如果转义字符也出现在数据中，解决方法是在转义字符前面插入一个转义字符。因此，当接收端收到连续的两个转义字符时，就删除前面的一个。

3. 差错检测

a. 比特差错

- 现实的通信链路都不理想。比特在传输中可能会出现差错。1 可能会变成 0，0 可能会变成 1。这就叫做比特差错。
- 解决方法：【循环冗余检验 CRC】
- 把收到的每一个帧都除以同样的除数 P（模2运算），然后检查所得到的余数 R。如果传输无差错，则余数为 0

b. 传输差错

- 无比特差错不等于无传输差错。无比特差错只是保证收到的帧是完整的。但是依然可能出现：帧丢失、帧重复、帧失序。帧丢失、帧重复、帧失序都属于传输差错。
- 解决方法
 - 帧编号、确认、重传机制
 - 通信质量良好的有线传输链路，不使用“帧编号、确认、重传机制”。通信质量差的有线传输链路则开启。这样是为了提高传输效率。

CSMA/CD 协议的工作原理（掌握）

- 协议解决的问题
 - 最初以太网是将许多计算机连在一根总线上。采用广播的方式进行通信，即当一台计算机发送数据时，总线上所有的计算机都能检测到这个数据，总线的传输资源就被占用了。所以，使用 CSMA/CD 协议使总线上的计算机能协调工作。
- 【协议要点】
 - **多点接入**：“多点接入”就是说明这是总线型的网络。网络中的主机以多点接入的方式连接在总线上。协议的实质是“载波监听”和“碰撞检测”。
 - **载波监听**：CSMA/CD 协议要求发送端在发送数据前对总线进行监听，若监听到其他计算机在发送数据，则等待一段时间，在总线空闲时才开始发送数据
 - **碰撞检测**：在数据发送过程中保持对总线上信号的监听，根据信号电压的变化幅度即可判断是否发生了碰撞。一旦监听到碰撞就立即停止数据发送，等待一段时间后再次尝试重发，直到发生成功

- 协议特性
 - 使用 CSMA/CD 协议的以太网不能进行全双工通信而只能进行双向交替通信【半双工通信】。
 - 每个站在发送数据之后的一小段时间内，存在着遭遇碰撞的可能性。这种发送的不确定性使整个以太网的平均通信量远小于以太网的最高数据率

网桥的工作原理。网桥的转发过滤机制，以及透明网桥转发表的建立过程（掌握）

- 网桥解决的问题
 - 连接不同的网络，对以太网进行扩展
- 【网桥工作在数据链路层】
- 网桥的工作原理

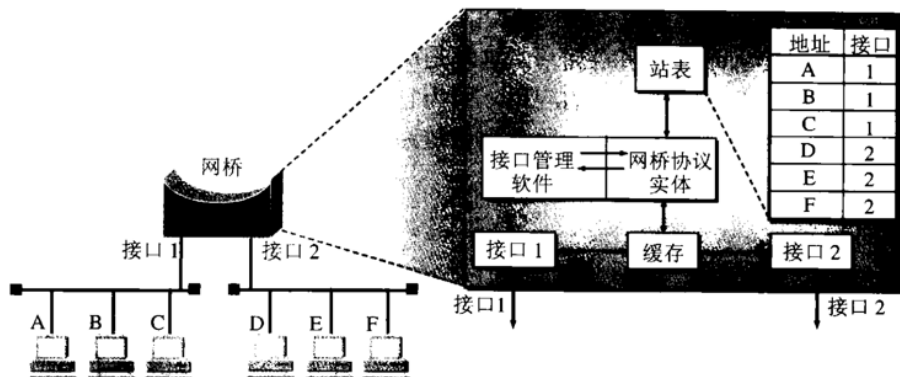


图 3-25 网桥的工作原理

- 若网桥从接口 1 收到 A 发给 E 的帧，则在查找转发表后，把这个帧送到接口 2 转发到另一个网段，使 E 能收到这个帧。
- 若网桥从接口 1 收到 A 发给 B 的帧，就丢弃这个帧，因为转发表指出，转发给 B 的帧应该从接口 1 转发出去，而现在正是从接口 1 收到这个帧，这说明 B 和 A 处于同一个网段上，B 能直接收到这个帧而不需要借助于网桥的转发
- 网桥的转发过滤机制
 - 网桥依靠【转发表】来转发帧。
 - 当网桥收到一个帧时，查找转发表中与收到帧的目的地址有无相匹配的项目。
 - 如果没有，则通过所有其他接口（但进入网桥的接口除外）进行转发。
 - 如有，则按照转发表给出的接口进行转发。
 - 但是，若转发表给出的接口就是该帧进入网桥的接口，则应丢弃这个帧【因为这时不需要经过网桥进行转发】
- 透明网桥转发表的建立过程

- 透明网桥：透明指以太网上的站点不知道所发送的帧经过哪几个网桥，以太网上的站点都看不见以太网上的网桥。
- 转发表的建立过程
 - 当网桥刚刚接入以太网时，其转发表是空的。
 - 网桥收到一帧后先进行【自学习】。查找转发表中与收到帧的源地址有无相匹配的项目。
 - 如没有，就在转发表中增加一个项目（源地址、进入接口和时间）
 - 如有，则把原有的项目进行更新。

虚拟局域网的概念（掌握）

- 定义：虚拟局域网 VLAN（Virtual LAN）是由一些局域网网段构成的与物理位置无关的逻辑组，而这些网段具有某些共同的需求。每一个 VLAN 的帧都具有一个明确的标识符，指明发送这个帧的计算机属于哪一个 VLAN
- 细节
 - 虚拟局域网是局域网给用户提供服务。【虚拟局域网并不是一种新型局域网】
 - 使用交换机可以将计算机分为不同的局域网
 - VLAN 标记
 - 以太网的帧格式中的一个【4 字节的标识符】，称为 VLAN 标记
 - VLAN 标记用来指明发送该帧的计算机属于哪一个虚拟局域网
 - VLAN 标志的前两个字节总是设置为 0x8100，称为 标志类型

习题

- 第五版 3-32

3-32 图 3-35 表示有五个站分别连接在三个局域网，并且用网桥 B_1 和 B_2 连接起来。每一个网桥都有两个接口（1 和 2）。在一开始，两个网桥中的转发表都是空的。以后有以下各站向其他的站发送了数据帧：A 发送给 E，C 发送给 B，D 发送给 C，B 发送给 A。试把有关数据填写在表 3-2 中。

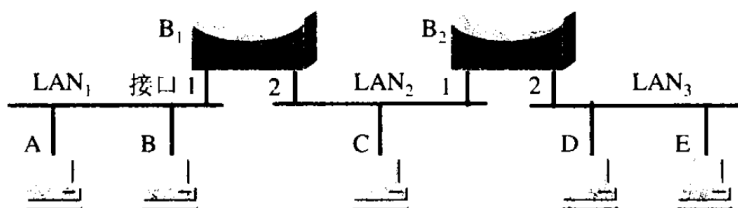


图 3-35 习题 3-32 的图

表 3-2 习题 3-32 的表

发送的帧	B ₁ 的转发表		B ₂ 的转发表		B ₁ 的处理 (转发? 丢弃? 登记?)	B ₂ 的处理 (转发? 丢弃? 登记?)
	地址	接口	地址	接口		
A → E						
C → B						
D → C						
B → A						

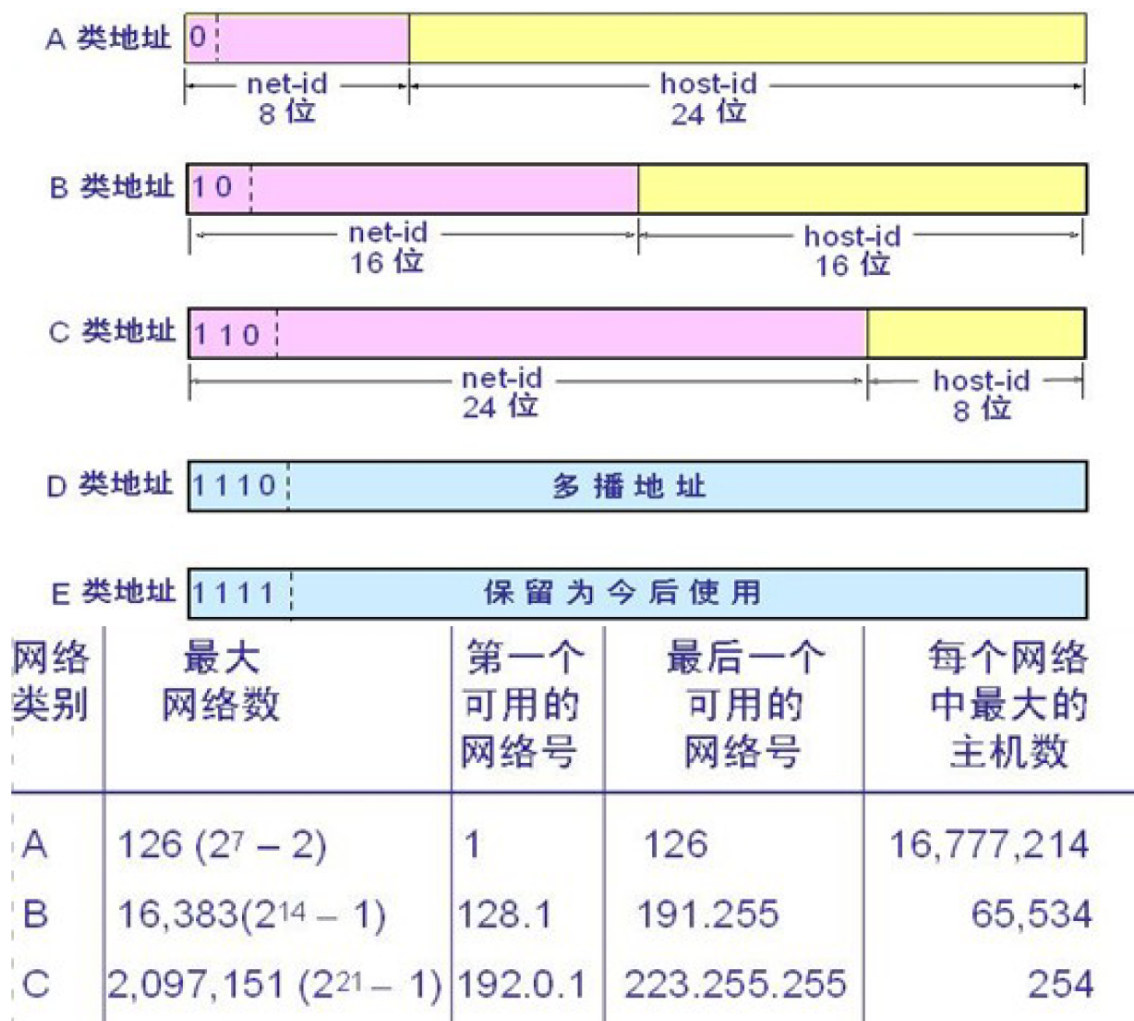
• 第五版 3-33

3-33 网桥中的转发表是用自学习算法建立的。如果有的站点总是不发送数据而仅仅接收数据，那么在转发表中是否就没有与这样的站点相对应的项目？如果要向这个站点发送数据帧，那么网桥能够把数据帧正确转发到目的地址吗？

3. 网络层

分类IP地址的基本概念与分类方法（掌握）

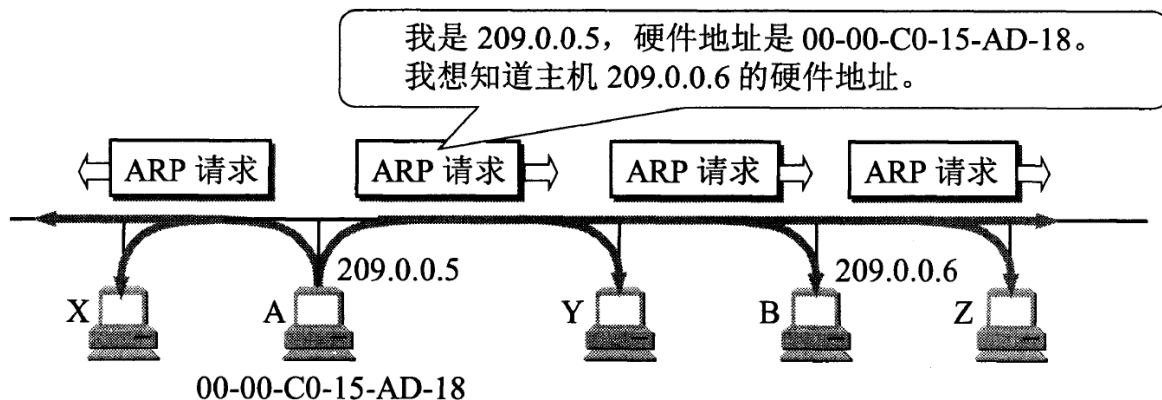
- 概念：IP 地址就是给互联网上每一台主机（或路由器）的每一个接口分配一个在全世界范围内是唯一的 32 位的标识符
- 【IP 地址 ::= {<网络号>,<主机号>}】
- 分类



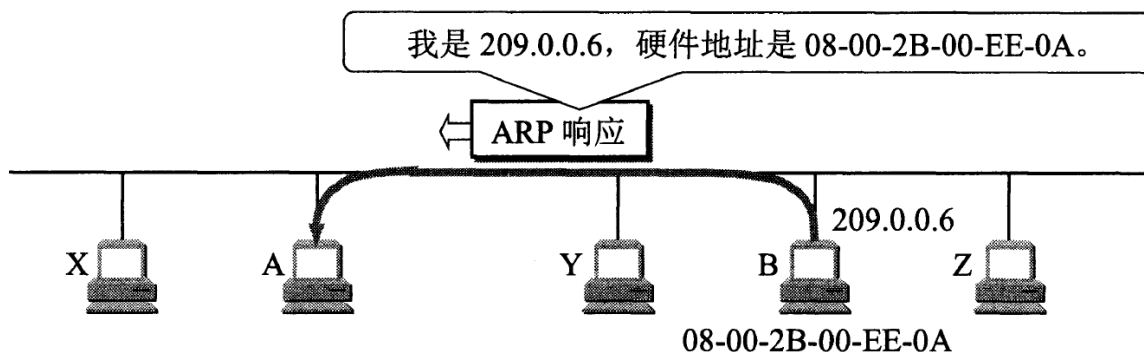
-
- 【A类、B类、C类】
- D类地址：多播地址
- E类地址：保留使用

地址解析协议 ARP（掌握）

- ARP 的作用是从网络层使用的 IP 地址，解析出在数据链路层使用的硬件地址
- 要点
 - ARP 高速缓存
 - 主机 ARP 高速缓存中存放一个从 IP 地址到硬件地址的映射表，并且这个映射表还经常动态更新（新增或动态删除）
 - 生存时间
 - ARP 对保存在高速缓存中的每一个映射地址项目都设置生存时间。凡是超过生存时间的项目就从高速缓存中删除掉
- 具体步骤



(a) 主机 A 广播发送 ARP 请求分组



(b) 主机 B 向 A 发送 ARP 响应分组

图 4-11 地址解析协议 ARP 的工作原理

-
- 当主机 A 要向本局域网上的某台主机 B 发送 IP 数据报时, 先在其 ARP 高速缓存中查看有无主机 B 的 IP 地址。
 - 如有, 就在 ARP 高速缓存中查出对应的硬件地址, 再把这个硬件地址写入 MAC 帧, 然后通过局域网把该 MAC 帧发往此硬件地址
 - 如无
 1. ARP 进程在本局域网发送一个 ARP 请求分组
 2. 本局域网上所有的主机运行 ARP 进程都收到 此 ARP 请求分组
 3. 主机 B 的 IP 地址与 ARP 请求分组中要查询的 IP 地址一致, 就收下这个 ARP 请求分组, 并向主机 A 发送 ARP 响应分组, 其余主机不理睬
 4. 主机 A 收到响应后, 就在其 ARP 高速缓存中写入主机 B 的 IP 地址到硬件地址的映射。

划分子网的概念 (掌握)

- 划分子网的原因 (补充)
 - a. IP 地址空间的利用率有时很低

b. 给每一个物理网络分配一个网络号会使得路由表变得太大，因此使得网络性能变坏

c. 两级 IP 地址不够灵活

- 解决方案

- 在 IP 地址中增加一个“子网号字段”，使两级IP 地址变为三级 IP 地址。这种做法就叫做划分子网

- IP 地址 ::= {网络号，子网号，主机号}

- 基本思路

- 1、划分子网纯属一个单位内部的事情。单位对外仍然表现为没有划分子网的网络，IP 地址的原网络号也没有改变

- 2、从主机号借用若干个位作为子网号 subnet-id，而主机号 host-id 也就相应地减少了若干位。

- 3、从其他网络发送到本单位某个主机的 IP数据报，仍然是根据 IP 数据报的目的网络号 net-id,先找到连接在本单位网络上的路由器。然后此路由器在收到 IP 数据报后，再按目的网络号 net-id 和子网号 subnet-id 找到目的子网

- 子网掩码

- 子网掩码解决的问题

- IP 数据报的首部无法看出源主机或目的主机是否进行了子网划分，那么路由器如何把 IP 数据报转发到对应的子网？

- 子网掩码带来的问题

- 划分子网增加了灵活性，但却减少了能够连接在网络上的主机总数

- 子网掩码结合本地IP地址后，用来确定目标 IP 是否在“逻辑上”与本计算机在同一个网络内。

- 同一个逻辑网，直接发送数据

- 不同逻辑网，将数据报发往默认网关 IP 对应的主机，由其负责路由转发

练习题

【例 4-2】已知 IP 地址是 141.14.72.24，子网掩码是 255.255.192.0。试求网络地址。

【解】子网掩码是 11111111 11111111 11000000 00000000。请注意，掩码的前两个字节都是全 1，因此网络地址的前两个字节可写为 141.14。子网掩码的第四字节是全 0，因此网络地址的第四字节是 0。可见本题仅需对地址中的第三字节进行计算。我们只要把 IP 地址和子网掩码的第三字节用二进制表示，就可以很容易地得出网络地址（图 4-22）。

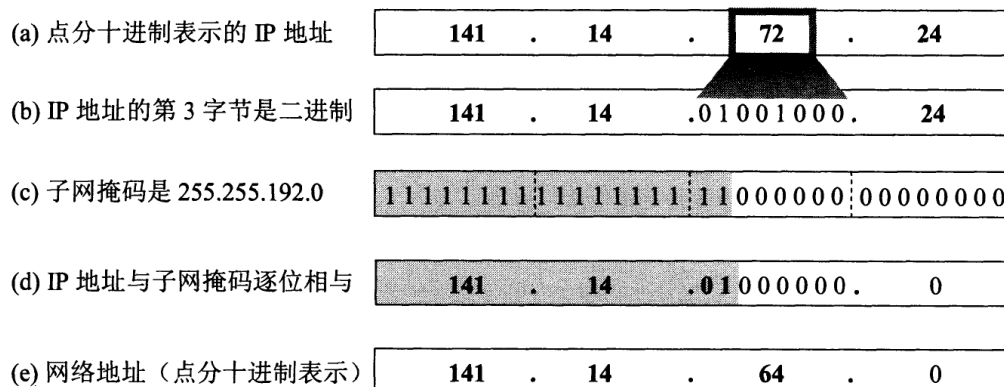


图 4-22 网络地址的计算

内部网关协议 RIP 和 OSPF（了解）

- 内部网关协议 RIP
 - RIP 是一种分布式的【基于距离向量的路由选择协议】
 - 距离：从一路由器到直接连接的网络的距离定义为 1。距离也称为跳数，因为每经过一个路由器，跳数就加 1
 - 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（因此，这是一组距离，即“距离向量”）。
 - 特点
 - i. 仅和【相邻路由器】交换信息
 - ii. 路由器交换的信息是当前本路由器所知道的【全部信息】，即自己现在的路由表
 - iii. 按【固定的时间间隔】交换路由信息
- 内部网关协议 OSPF
 - OSPF 是使用【分布式的链路状态】协议
 - 要点
 - i. 使用【洪泛法】向本自治系统中的【所有路由器】发送信息
 - ii. 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】
 - 链路状态就是说明本路由器都和哪些路由器相邻，以及该链路的“度量”
 - OSPF 将这个“度量”用来标识表示费用、距离、时延、带宽等

iii. 【只有当链路状态发生变化时】，路由器才向所有路由器用洪泛法发送此信息

Internet 控制报文协议与多播管理协议的概念（了解）

- Internet 控制报文协议 ICMP (Internet Control Message Protocol)
 - ICMP 作用：为了更加有效地转发 IP 数据报和提高交付成功的机会
 - ICMP 是 【网络层的协议】，ICMP 报文封装在 IP 层数据报的 【数据部分】
 - ICMP 报文的种类
 - ICMP 报文的前 4 个字节是同一的格式，共有三个字段：类型、代码和检验和。最后面是数据字段，其长度取决于 ICMP 的类型
 - ICMP 差错报告报文的数据字段
 1. 终点不可达
 2. 时间超过
 3. 参数错误
 4. 改变路由（重定向）
 - ICMP 询问报文的数据字段
 1. 回送请求和回答
 2. 时间戳请求和回答
 - 【ICMP 的应用举例】
 - PING：使用了 ICMP 回送请求与回送回答报文
 - Traceroute：使用了 ICMP 终点不可达报文
- 多播管理协议
 - 概念

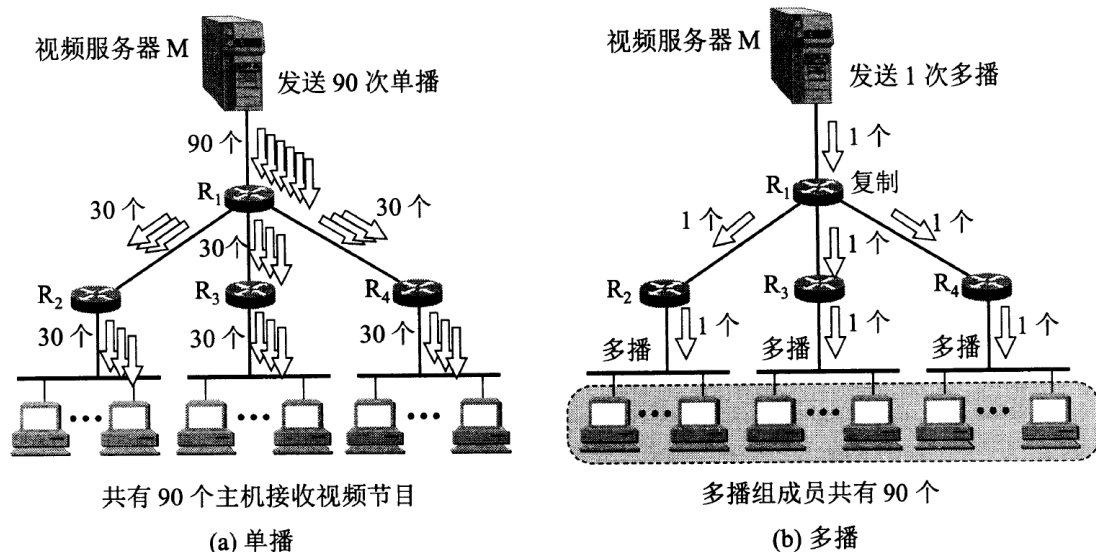


图 4-53 单播与多播的比较

- 服务器只需要发生一次数据报，路由器在转发分组时，把收到的分组复制成多个副本，进行转发
- 多播使用 D 类 IP 地址。IP 地址就像 QQ 群号，只要加入了就能收到信息
- IP 多播需要两种协议
 - 网际组管理协议 IGMP(Internet Group Management Protocol)
 - 为了使路由器知道【多播组成员的信息】，需要利用网际组管理协议 IGMP。类似地 IGMP使用【IP数据传递其报文】（即IGMP报文+IP首部构成一个IP数据报），也向IP提供服务。
 - 多播路由选择协议
 - 连接在局域网上的多播路由器还必须和因特网上的【其他多播路由器协同工作】，以便把多播数据报用【最小代价】传送给所有的组成员。这就需要使用多播路由选择协议。

VPN 和 NAT 的基本概念（了解）

- 【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，这样的专用网又称为“虚拟专用网 VPN”
- 【网络地址转换】 NAT
 - 要解决的问题：专用网络内部的一些主机本来已经分配到了本地 IP 地址，又想和互联网上的主机通信
 - 使用本地地址的主机和外界通信时，都要在 【NAT 路由器上将其本地地址转为全球 IP 地址

址】，才能和互联网连接

4. 传输层

网络环境中进程通信的基本概念（理解）

- 主机进程通信
 - 两台主机进行通信就是两台主机中的【应用进程互相通信】
- 运输层的功能
 - 复用：发送方不同的应用程序都可以使用同一个运输层协议传输数据（当然要加上适当的部首）
 - 分用：接收方的运输层在剥去报文的部首后能把这些数据正确的交付目的应用进程
 - 差错检测
- 运输层协议和网络层协议的主要区别

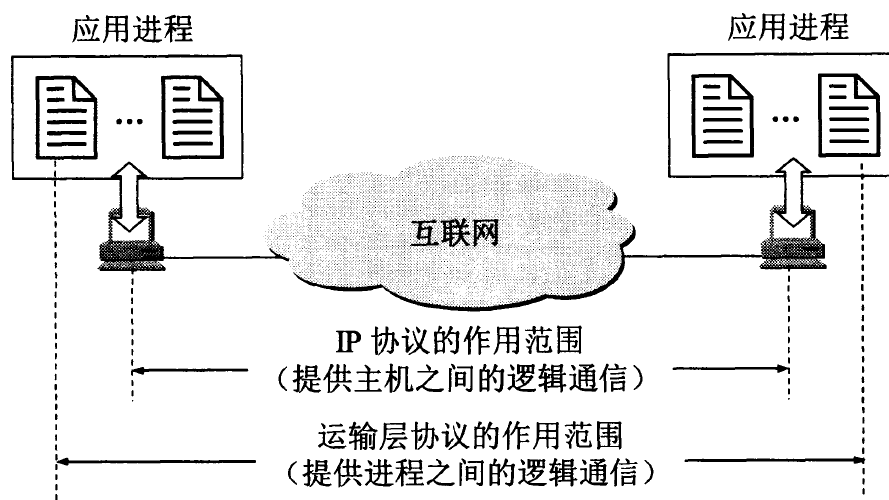


图 5-2 运输层协议和网络层协议的主要区别

-
- 逻辑通信：好像是这样通信，实际上不是这样。逻辑通信是从水平讨论某一层的通信

常见端口（了解）

- 服务器端口号：登记端口号（1024~49151）
- 客户端使用的端口号：49152~65535
- 【熟知端口号（0~1023）】
 - FTP 21

- TELNET 23
- SMTP 25
- DNS 53
- TFTP 69
- HTTP 80
- SNMP 161
- SNMP 162
- HTTPS 443

进程相互作用的客户/服务器模型（掌握）

- TCP 连接的建立采用客户服务器方式
- 主动发起连接建立的应用进程叫做客户（client）
- 被动等待连接建立的应用进程叫做服务器（server）

用户数据报协议 UDP 的基本内容（掌握、重点）

- UDP 特点
 - 1、【UDP 是无连接的】，即发送数据之前不需要建立连接
 - 2、UDP 使用尽最大努力交付：【即不保证可靠交付】
 - 3、【UDP 是面向报文的】
 - 【一次交付一个完整的报文。UDP 对应用层交付的报文，既不合并，也不拆分】
 - 发完整报文带来的问题
 - 报文过长，IP 层在传输时需要拆分，降低 IP 层的效率
 - 报文太短，IP 层数据报的首部相对长度太大，降低了 IP 层效率
 - 4、【UDP 没有拥塞控制】：因此网络即使出现了拥塞也不会使源主机发送速率降低
 - 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 首部格式

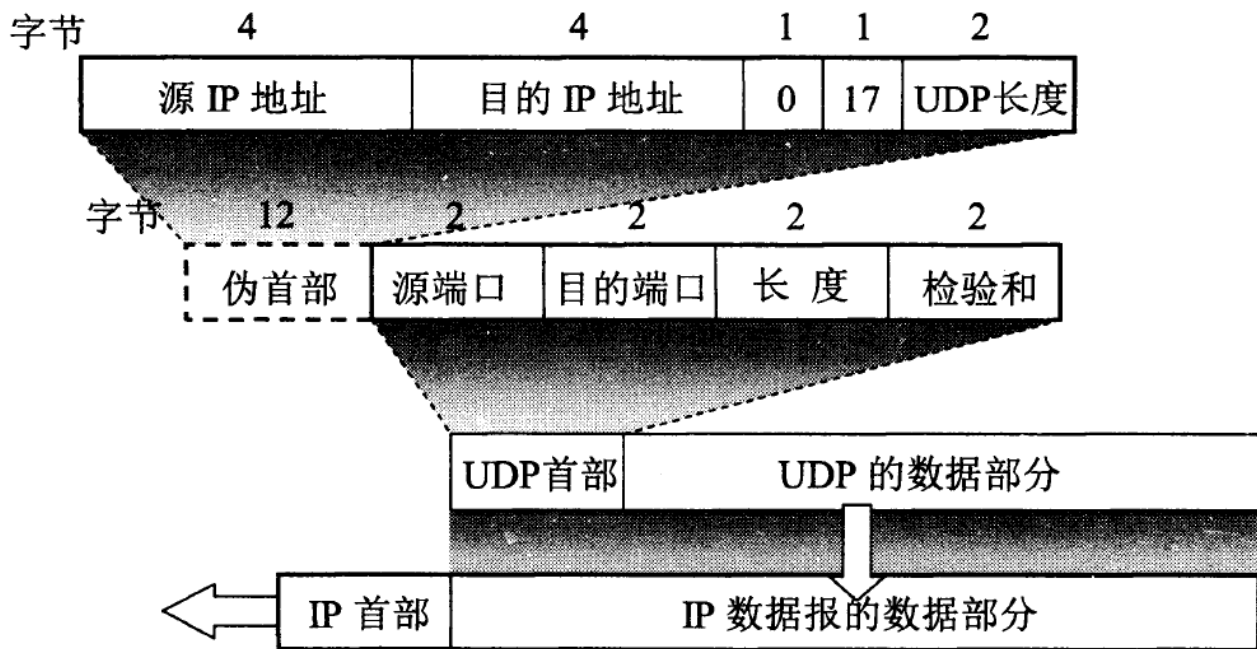


图 5-5 UDP 用户数据报的首部和伪首部

- 伪首部不是 UDP 用户数据报真正的首部。伪首部既不向下传送也不向上递交，只是为了计算检验和
- a. 源端口号：需要对方回信时选用
- b. 目的端口：交付终点报文时必须使用
- c. 长度：UDP 用户数据报的长度，其最小值是 8
- d. 检验和：检验 UDP 用户数据报在传输中是否有错。有错就丢弃。

传输控制协议 TCP 的基本内容（掌握、重点）

- TCP 特点
 - a. TCP 是【面向连接】的运输层协议。就像打电话一样，使用协议前先建立 TCP 链接，数据传输完毕后，要释放连接
 - b. 每一条 TCP 只能有两个端点，【每一条 TCP 连接只能是点对点的】
 - c. 【TCP 提供可靠交付的服务】。通过 TCP 连接传送的数据，无差错、不丢失、不重复，并且按时到达
 - d. TCP 提供【全双工通信】。TCP 连接的两端都设有发送缓存和接收缓存，用来存放双向通信的数据。
 - e. 【面向字节流】：虽然应用程序和 TCP 的交付是一次一个数据块，但 TCP 把应用程序交下来的数据仅仅看成是一连串的无结构的字节流

- 注意点
 - TCP 连接是一条【虚连接】而不是一条真正的物理连接。
 - TCP 对应用进程一次把【多长的报文】发送到 TCP 的缓存中是不关心的。
 - TCP 根据对方给出的【窗口值和当前网络拥塞的程度】来决定一个报文段应包含多少个字节（UDP 发送的报文长度是应用进程给出的）。
 - TCP 可把太长的数据块划分短一些再传送。TCP 也可等待积累有足够多的字节后再构成报文段发送出
- TCP 的连接
 - TCP 连接的端点叫做套接字（socket）或插口
 - 【套接字 socket = (IP 地址：端口号)】

TCP 连接的基本过程（掌握、重点）

- 1、连接建立
 - 握手：TCP建立连接的过程叫握手，握手需要在客户和服务端之间交换三个 TCP 报文段
 - 三报文握手

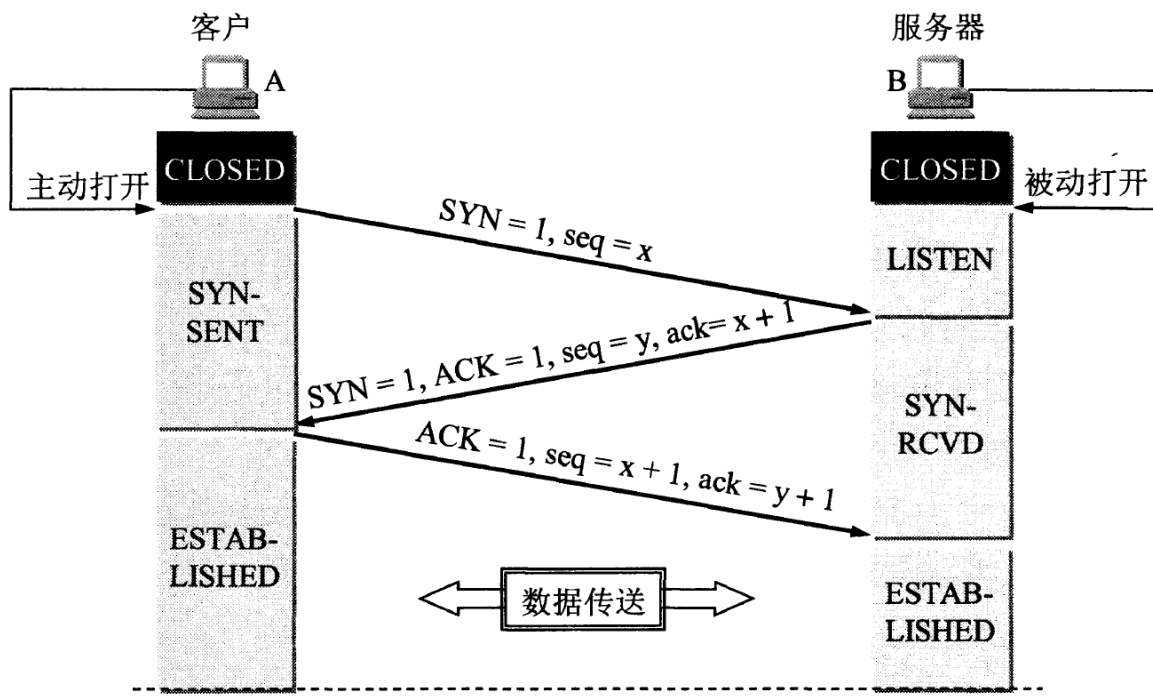


图 5-28 用三报文握手建立 TCP 连接

- 客户端发送的TCP报文中标志位SYN置1，初始序号seq=x（随机选择）。Client进入SYN_SENT状态，等待Server确认。
- 服务器收到数据包后，根据标志位SYN=1知道Client请求建立连接，Server将标志位SYN和ACK

都置为1, $ack=x+1$, 随机产生一个初始序号 $seq=y$, 并将该数据包发送给Client以确认连接请求, Server进入SYN_RCVD状态。

- iii. Client收到确认后, 检查 ack 是否为 $x+1$, ACK是否为1, 如果正确则将标志位ACK置为1, $ack=y+1$, 并将该数据包发送给Server。Server检查 ack 是否为 $y+1$, ACK是否为1, 如果正确则连接建立成功, Client和Server进入ESTABLISHED状态, 完成三次握手, 随后Client与Server之间可以开始传输数据了。

- 2、连接释放
 - 四报文握手

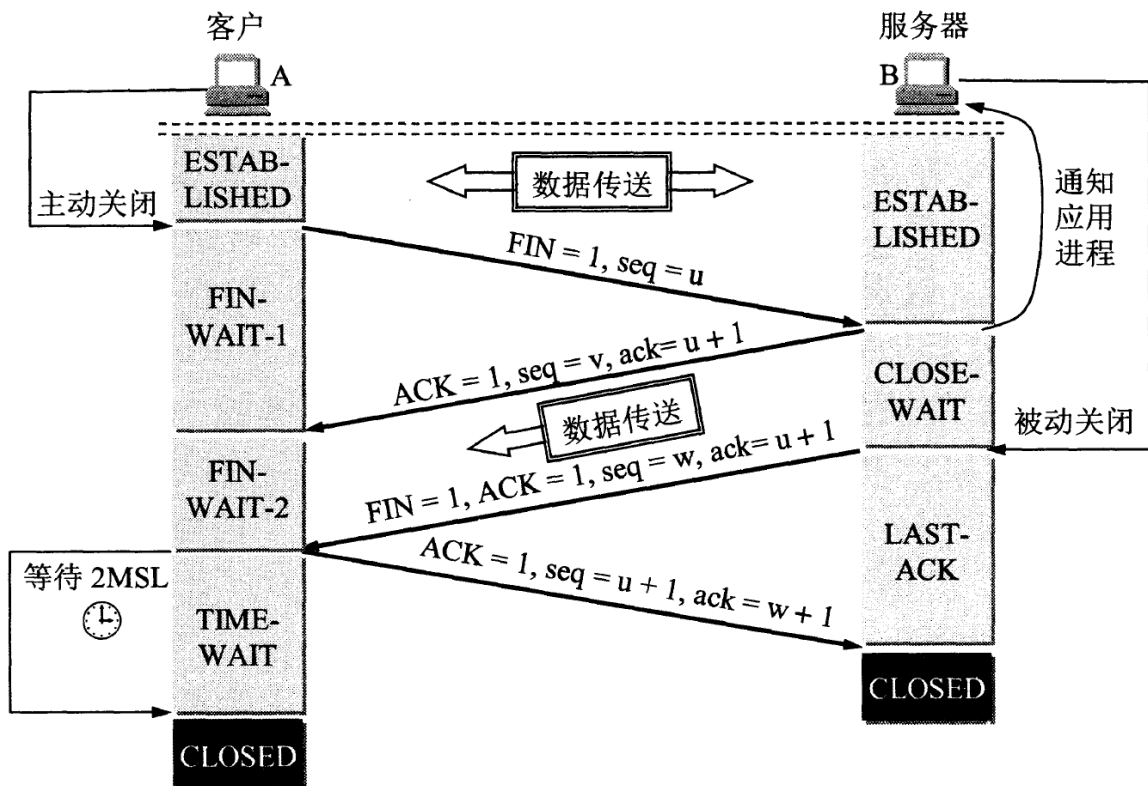


图 5-29 TCP 连接释放的过程

- a. 客户端发送一个 FIN, 用来关闭客户端到服务器的数据传送, 客户端进入 FIN_WAIT_1 状态。
- b. 服务器收到 FIN 后, 发送一个 ACK 给客户端, 确认序号为 $u+1$ (与 SYN 相同, 一个 FIN 占用一个序号), 服务器进入 CLOSE_WAIT 状态。
- c. 客户端收到 ACK, 从 FIN_WAIT_1 变为 FIN_WAIT_2, 等待服务器发生确认断开的包。
- d. 服务器发送一个 FIN, 用来关闭服务器到 Client 的数据传送, 服务器进入 LAST_ACK 状态。
- e. 客户端收到 FIN 后, 客户端进入 TIME_WAIT 状态(主动关闭方才会进入该状态), 接着发送一个 ACK 给服务器, 确认序号为 $w+1$, 服务器进入 CLOSED 状态, 完成四次挥手。

5. 应用层

表 5-1 使用 UDP 和 TCP 协议的各种应用和应用层协议

应用	应用层协议	运输层协议
名字转换	DNS（域名系统）	UDP
<u>文件传送</u>	<u>TFTP（简单文件传送协议）</u>	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
<u>文件传送</u>	<u>FTP（文件传送协议）</u>	TCP

域名系统 DNS 基本过程与工作原理（了解）

- 含义：把互联网上的主机名字转为 IP 地址
- 域名结构：三级域名.二级域名.顶级域名
- 域名解析
 - 当某一个应用进程需要把主机名解析为 IP 地址时，该应用程序就调用解析程序（resolver），并成为 DNS 的一个客户，把待解析的域名放在 DNS 请求报文中，以【UDP 用户数据报】方式发给本地服务器（使用 UDP 是为了减少开销）。本地域名服务器在查找域名后，把对应的 IP 地址放在回答报文中返回。应用进程获得目的主机的 IP 地址后即可进行通信。
 - 若本地域名服务器不能回答该请求，则此域名服务器就暂时成为 DNS 中的另外一个客户，并向其他域名服务器发出查询请求。
- 查询区别
 - 递归查询
 - 主机向本地域名服务器的查询一般是递归查询。即：如果主机所询问的本地域名服务器不

知道被查域名的 IP 地址，那么本地域名服务器就以 DNS 客户的身份，向其他根域名服务重启继续发出查询请求报文，而不是让该主机自己进行下一步的查询

- 迭代查询
 - 本地域名服务器向根域名服务器的查询通常是采用迭代查询。
- 域名解析举例（查询 y.abc.com）
 - a. 主机先向其本地域名服务器 dns.xyz.com 进行递归查询
 - b. 本地域名服务器采用迭代查询。它先向一个根域名服务器查询
 - c. 根域名服务器告诉本地域名服务器，下一次查询应查询的顶级域名服务器的 dns.com 的 IP 地址
 - d. 本地域名服务器向顶级域名服务器 dns.com 进行查询
 - e. 顶级域名服务器 dns.com 告诉本地域名服务器，下一次应查询的权限域名服务器 dns.abc.com 的地址
 - f. 本地域名服务器向权限域名服务器 dns.abc.com 进行查询
 - g. 权限域名服务器 dns.abc.com 告诉本地域名服务器，所查询的主机的 IP 地址
 - h. 本地域名服务器最后把查询结果告诉主机

文件传输协议 FTP 基本过程与工作原理（了解）

- 【基于 TCP 可靠的运输服务】
- FTP 的主要功能是减少或消除在不同的操作系统下处理文件的不兼容性
- FTP 使用客户服务器方式
 - 服务器
 - 一个 FTP 服务器进程可同时为多个客户进程提供服务
 - 服务器进程由 2 个部分组成
 - a. 主进程，负责接收新的请求
 - b. 若干从属进程，负责处理单个请求
 - 服务器主进程的工作步骤
 - a. 打开熟知的端口（端口号 21），使客户进程能够连接上
 - b. 等待客户进程发出连接请求
 - c. 启动从属进程处理客户进程发来的请求。从属进程对客户进程的请求处理完毕后即终止
 - d. 回到等待状态，继续接受其他客户进程发来的请求。
 - 客户端

- 与服务器建立 2 个 TCP 连接
 - a. 控制连接：会话期间一直打开，但不传输文件数据
 - b. 数据连接：用于传输文件

超文本传输协议 HTTP 基本过程与工作原理（了解）

- 统一资源定位符 URL
 - URL 的格式：<协议>://<主机>:<端口>/<路径>
 - 使用 HTTP 的 URL
 - HTTP 协议默认端口 80
 - HTTPS 协议默认端口 443
 - URL 里面的字母不区分大小写
- HTTP 的操作过程
 - HTTP 使用 TCP 作为运输层协议，保证了数据传输的可靠性
 - HTTP 协议是无状态的，即服务器不知道当前客户是否访问过
 - HTTP/1.0 请求花费的时间
 - 文档的传输时间
 - 两倍往返时间 RTT
 - 一个 RTT 用于连接 TCP 连接
 - 另一个 RTT 用于请求和接收文档
 - （TCP 建立连接的三报文握手的第三个报文段中的数据，就是客户对万维网文档的请求报文）
 - HTTP/1.1 的改进：持续连接
 - 优点：HTTP/1.1 使用了持续连接节省了请求时间
 - 含义：持续连接就是万维网服务器在发送响应后仍然在一段时间内保持了这个连接，使同一个客户和该服务器可以继续在这个连接上传输后续的 HTTP 请求报文和响应报文
 - 持续连接的两种工作方式
 - 非流水线方式
 - 特点：客户在收到前一个响应后才能发出下一个响应
 - 花费时间：客户每访问一个对象都要用去一个往返时间的 RTT
 - 流水线方式
 - 特点：客户在收到 HTTP 响应报文之前就能接着发送新的请求报文。于是，一个接一个的请求报文到达服务器后，服务器就可以连续发回响应报文

- 花费时间：客户访问所有的对象只需要花费一个 RTT 时间

- 代理服务器

- 个人理解：CDN 就可以理解为一种代理服务器
- 代理服务器是一种网络实体，它又被称为万维网高速缓存（Web cache）

- HTTP 的报文结构

- 分类

- 请求报文
- 响应报文

- 组成

1. 开始行。开始行的三个字段之间都以空格分开，最后的“CR”和“LF”分别代表“回车”和“换行”

- 分类

- 请求报文：请求行

- 方法
- URL
- 版本

- 响应报文：状态行

- 版本
- 状态码
- 短语

2. 首部行

- 每一个首部都有字段名和它的值
- 每一行结束后都有回车和换行（即 CRLF）
- 整个首部行结束时，还有一空行将首部行和后面的实体主体分开

3. 实体主体

- 请求方法

- OPTION：请求的一些选项的信息
- GET：请求读取由 URL 所标识的信息
- HEAD：请求读取由 URL 所标识的首部的信息
- POST：给服务器添加信息
- PUT：在指明的 URL 下存储一个信息
- DELETE：删除指明的 URL 所标识的信息

- TRACE：用来进行环回测试的请求报文
- CONNECT：用于代理服务器
- 响应状态码
 - 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
 - 3xx：表示重定向
 - 4xx：表示客户端的差错
 - 5xx：表示服务器的差错
- 在服务器上存放用户信息
 - Cookie 是为了解决 HTTP 无状态的问题
 - Cookie 工作原理
 - 用户浏览使用 Cookie 的网站时，该网站的服务器就会为用户产生一个唯一标识码，在给用户 A 的响应报文中添加 Set-cookie 的首部行。
 - 用户浏览器收到这个响应后，会在它管理的特定 Cookie 文件中保存此 Cookie。
 - 用户继续浏览这个网站时，浏览器会自动把这个 Cookie 添加到请求的首部行 Cookie。

简单邮件传输协议 SMTP 基本过程与工作原理（了解）

- 架构：客户服务器方式
- 端口：25
- 基本过程
 - a. 建立连接
 - 发件人的邮件发到发送方邮件服务器的缓存后，SMTP 客户每隔一段时间对邮件进行扫描。
 - 如果发现邮件，就使用 SMTP 熟知的端口号 25 与接收方的服务器的 SMTP 服务器建立【TCP 连接】。
 - SMTP 不使用中间的邮件服务器。即发送服务器与接收方的服务器直接建立 TCP 连接
 - b. 邮件传送
 - MAIL FROM:<发件人地址>
 - RCPT TO:<收件人地址>
 - DATA 后加正文内容
 - c. 连接释放
 - SMTP 客户应当发生 QUIT 命令

动态主机配置协议 DHCP 基本过程与工作原理（了解）

- 功能：DHCP 提供了“即插即用联网”的机制，当运行客户软件的计算机移至一个新的网络时，就可使用 DHCP 获取其配置信息而不需要手动干预
- 【运输层协议是UDP】
- 端口：客户端 68。服务端 67
- 基本过程
 - a. 需要 IP 地址的主机广播发送发现报文（DHCP DISCOVER），数据报源 IP 地址 0.0.0.0，目的 IP 地址 255.255.255.255
 - b. DHCP 服务器对此广播报文应答。DHCP 服务器先在其数据库中查找该计算机的信息。若找到，则返回该信息。若找不到，则从服务器的 IP 地址池中取一个新的地址分配给该计算机。DHCP 服务器的回答报文叫做提供报文（DHCPOFFER）
- 租用期
 - DHCP 服务器分配给 DHCP 客户的 IP 地址是临时的，因此 DHCP 客户只能在一段有效时间内使用这个 IP 地址。DHCP 称这段时间为租用期。