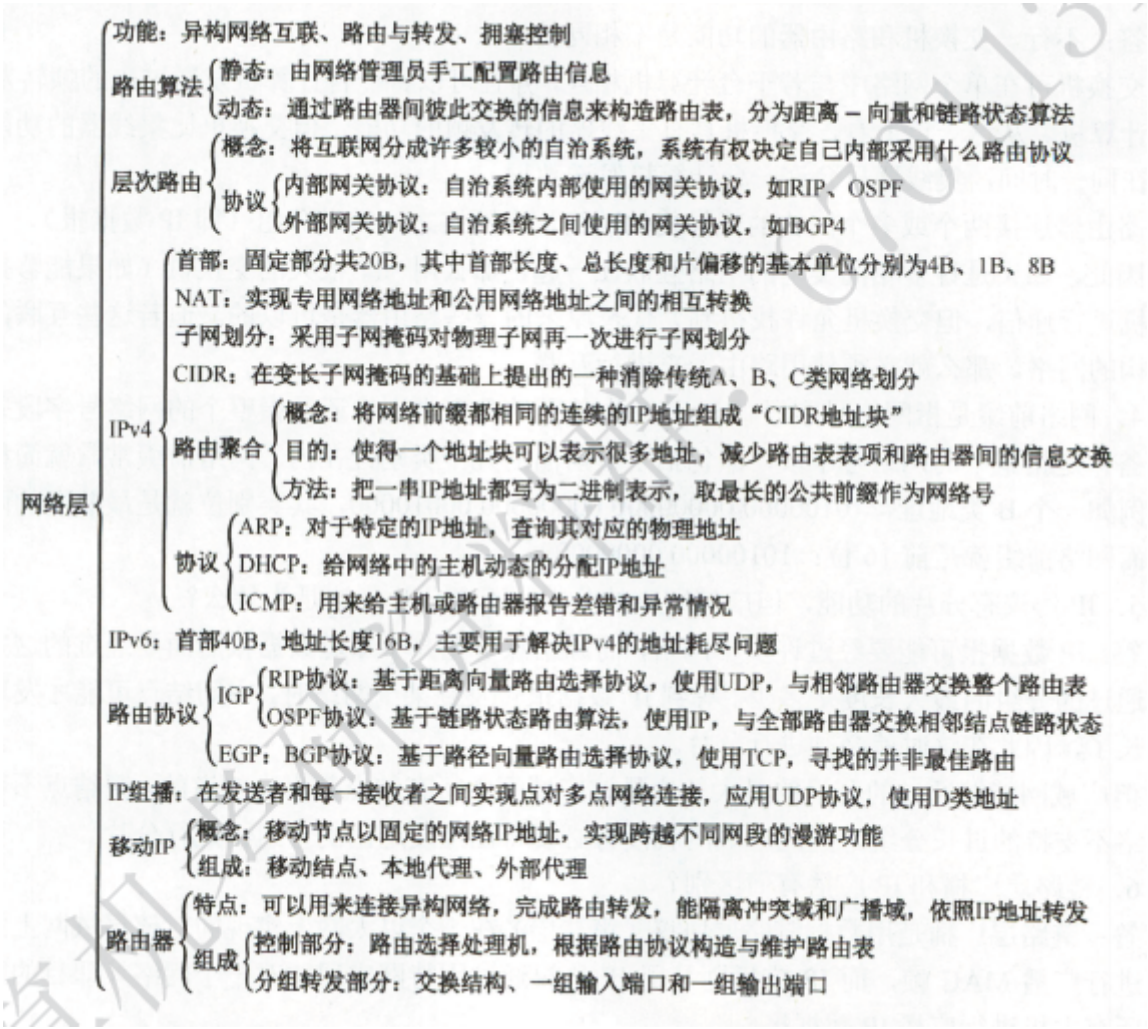
- 物理层
  - 通信基础
    - 信道
      - 单工：只有一个方向的通信，而没有反方向的交互
      - 半双工：通信双方都可以发送、接收信息，但不能同时发送接受
      - 全双工：通信双方可以同时发送、接收信息
    - 定理
      - 奈氏准则：理想低通信道下的极限数据传输率=$2W\log_2 V$
      - 香农定理：信道的极限数据传输速率$W\log_2(1+S/N)$
    - 调制与编码
      - 调制：把数据变换为模拟信号的过程
      - 编码：把数据变换为数字信号的过程
      - 数字数据 → 数字信号：非归零码、曼彻斯特编码、差分曼彻斯特编码等
      - 数字数据 → 模拟信号：幅移键控、频移键控、相移键控、正交振幅调制
      - 模拟数据 → 数字信号：1.抽样2.量化3.编码
      - 模拟数据 → 模拟信号：频分复用技术等
    - 传输方式
      - 电路交换：两结点之间建立一条专用的物理通信路径，传输期间一直独占
      - 报文交换：无需建立专门连接，报文携带有目标地址等信息，采用存储转发方式
      - 分组交换：把报文分割成小的数据块，加上必要的控制信息进行传输
    - 分组交换
      - 数据报：分组之间可能存在不同路径，各个分组分别转发
      - 虚电路：在发送方和接收方建立一条逻辑上相连的虚电路，分组沿着虚电路传输
  - 传输介质
    - 无线：无线电波、微波、红外线和激光
    - 有线：双绞线、同轴电缆、光纤
  - 设备
    - 中继器：将信号整形并放大再转发出去，消除信号的失真和衰减问题，具有5-4-3规则
    - 集线器：实质上是一个大多端口中继器，对信号进行放大后发到其他所有端口

- 数据链路层
  - 功能：为网络层提供服务、链路管理、帧定界、帧同步与透明传输、流量控制和差错控制
  - 组帧
    - 字符计数法：在帧头部使用一个计数字段来标明帧内字符数
    - 首尾定界法
      - 概念：使用特定字符或比特模式定结帧的开始和结束
      - 字符填充：在数据中的特殊字符前面用转义字符填充
      - 比特填充，数据区每遇到连续5个1就填充一个
    - 违规编码法：信号传输过程中采用违规的编码来表示帧的起始和终止
  - 差错控制
    - 检错编码：奇偶校验码、循环冗余码
    - 纠错编码：海明码
  - 可靠传输：数据链路层通常使用确认和超时重传两种机制来保证可靠传输
  - 流量控制
    - 停止等待协议：发送方每发送一帧都要等待接收方的应答信号才能发送下一帧
    - 后退N帧协议：发送方一次可发送N帧，按序接收，重传从最后一个确认开始
    - 选择重传协议：发送方一次可发送N帧，可以不按序接收，重传没有确认的帧
  - 介质访问
    - 信道划分
      - 频分复用：将多路信号调制到不同频率载波上叠加形成一个复合信号
      - 时分复用：将物理信道按时间分为若干时间片，轮流给不同信号使用
      - 波分复用：在一根光纤中传输多种不同波长（频率）的光信号
      - 码分复用：靠不同的编码来区分各路原始信号，例如CDMA技术
    - 随机访问
      - ALOHA协议
        - 纯ALOHA：不检测直接发送，若无确认则等待重发
        - 时隙ALOHA：将时间划分为若干等长时隙，按时发送
      - CSMA协议
        - 1-坚持：闲则发送，忙则继续监听
        - 非坚持：闲则发送，忙则等待一个随机时间再听
        - p-坚持：闲则以概率p发送，1-p等待下一个时隙
忙则等待一个随机时间再听
      - CSMA/CD协议
        - 流程：先听后发，边听边发，冲突停发，随机重发
        - 碰撞解决：采用二进制指数退避算法来解决碰撞问题
      - CSMA/CA协议
        - 避免碰撞：预约信道、ACK帧、RTS/CTS帧
        - 解决碰撞：采用二进制指数退避算法来解决碰撞问题
    - 轮询访问：令牌传递协议，只有得到令牌的机器才能发送数据，其他必须等待
  - 局域网：在一个较小地理范围内，将各种计算机等设备通过双绞线等介质连接
  - 广域网
    - PPP协议：面向字节，采用字节填充方式，只支持全双工链路
    - HDLC协议：面向比特，采用0比特插入法，帧类分为信息帧、监督帧和无编号帧
  - 设备
    - 网桥
      - 特点：把两个或多个以太网通过网桥连接起来变成一个网段
      - 类型
        - 透明网桥：按照自学习算法填写转发表，按转发表转发
        - 源路由网桥：先发送发现帧，按返回结果转发
    - 交换机
      - 特点：实际就是一个多端口网桥
      - 交换方式
        - 直通式：帧在接收后只检查目的地址，几乎能马上就被传出去
        - 存储转发：先将接收到的帧缓存到高速缓存器，检查数据正确性
    - 相同点：按MAC地址转发，都能隔离冲突域，不能隔离广播域



物理层

RS232特性

（1）电气特性

连线长度：小于50ft

电压范围：-15V—+15V

线路编码：负电压表示1，正电压表示0

（2）机械特性

D型插头座，至少有三根针：发送、接收、地

（3）以字符为单位传输，每个字符7个b，另加一个起始位，1或1.5个停止位

奈奎斯特定理和香农定理

奈：硬件带宽和理论最大数据发送速率之间的关系，提高：带宽和电压值

香农：有噪声的传输系统可以达到的最大数据速率，提高：信噪比

复用和解复用

复用是**多个信源**的信息流组合在**一条共享介质**上传输

解复用是将信息流组合分隔回分开的信息流

频分：收音机无线广播，ADSL

波分：光纤

时分：以太网

数据链路层

1、奇偶校验的简单计算

2、Checksum的简单计算

3、CRC的理解

4、交换技术

线路交换（电路交换）：通信之前在通信双方之间建立一条被双方**独占**的**物理通道**：类似电话线

特点：独立信道、实时性高、通信时延小

报文交换：数据交换的单位是报文，报文携带有目标地址、源地址等信息。报文交换在交换节点采用的是**存储转发**的方式

特点：无需建立连接、线路利用率高

由于报文交换**对报文大小没有限制**，要求网络节点需要有较大的缓存空间，现在**被分组交换所取代**

分组交换（**Packet Switching**）：以分组为单位进行传输和交换的存储转发方式。

采用**统计复用（时分）**

特点：异步（无建立时延）、无需建立连接、信道利用率高

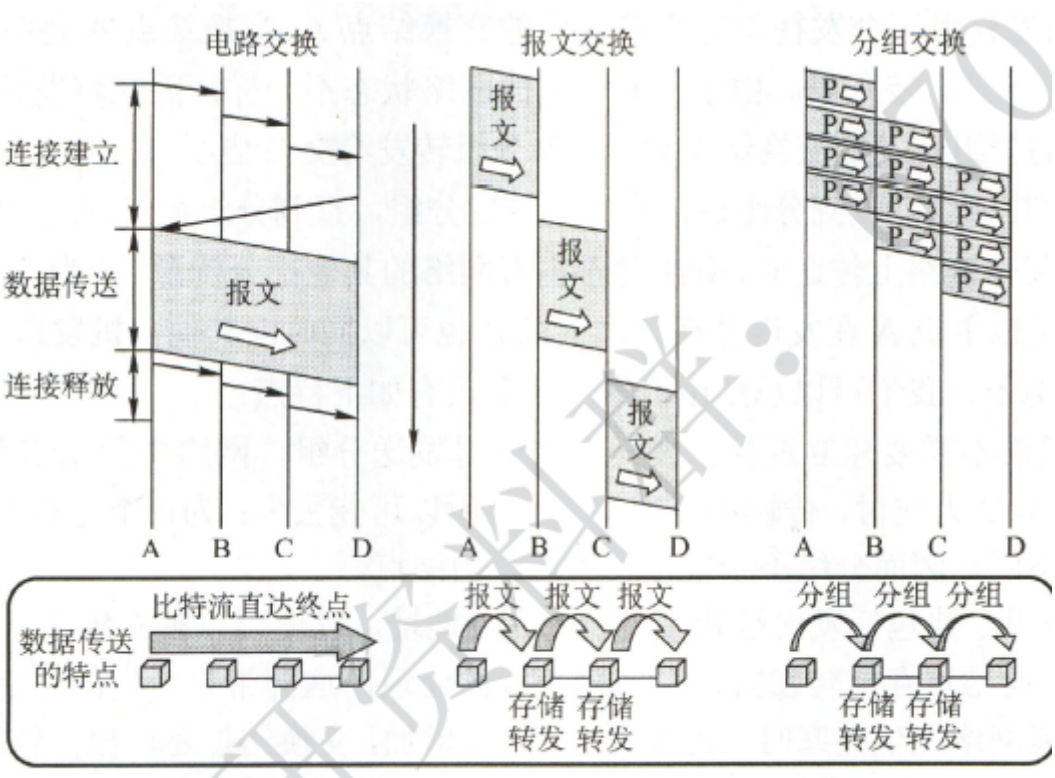


图 2-4　三种数据交换方式的比较

5、网络接口卡（NIC）的作用

网卡：Network Interface Card，是处理计算机进行网络通讯的设备

作用：

（1）处理地址识别

（2）数据的封装与解封：发送时将上一层交下来的数据加上首部和尾部，成为以太网的帧。接收时将以太网的帧剥去首部和尾部，然后送交上一层；

（3）帧的识别和发送/接受

6、MAC地址的构成

MAC（Media Access Control,介质访问控制），也叫硬件地址，长度为48b，由十六进制的数字构成，分为前24位和后24位

前24位叫做组织唯一标识（OUI），通过此区分不同的厂家

后24位是由厂家自己分配的，称为扩展标识符

即：**厂商号+序列号**

MAC地址是计算机的**物理网卡唯一对应的地址**

7、以太网的帧格式

前同步码	帧首定界符	目的地址	源地址	类型	数据	CRC
7B	1B	6B	6B	2B	46-1500B	4B

以太网规定了最短有效帧长为64字节

因为10Mbps以太网在争用期可发送64字节，**若前64字节没有发生冲突，则后续的数据都不会发生冲突**

若检测到冲突立即中止发送，则已发送的数据一定小于64字节

凡长度小于64字节的帧都是无效帧

8、局域网拓扑

星形拓扑：一组计算机通过中心节点实现信息传输

总线型结构：所有站点共享一条数据通道，任何连接到总线上的计算机都可以通过电缆发送信号，接收信号，确保任何时候**只有一台计算机发送信号**，否则会混乱。

特殊点：

对于**双绞线以太网**（**共享型以太网**），在物理上，它采用星型拓扑结构，在逻辑上，它像总线一样工作，称为星形总线

比如10BaseT，布线形成**以集线器（Hub）**为中心的星型拓扑结构，计算机和集线器之间使用带RJ-45连接器的双绞线布线

不同拓扑的优缺点：

星型有交换表，只要不是同一端口就可以并行传输

总线型有冲突域，hub

9、以太网介质访问控制策略（CSMA/CD）

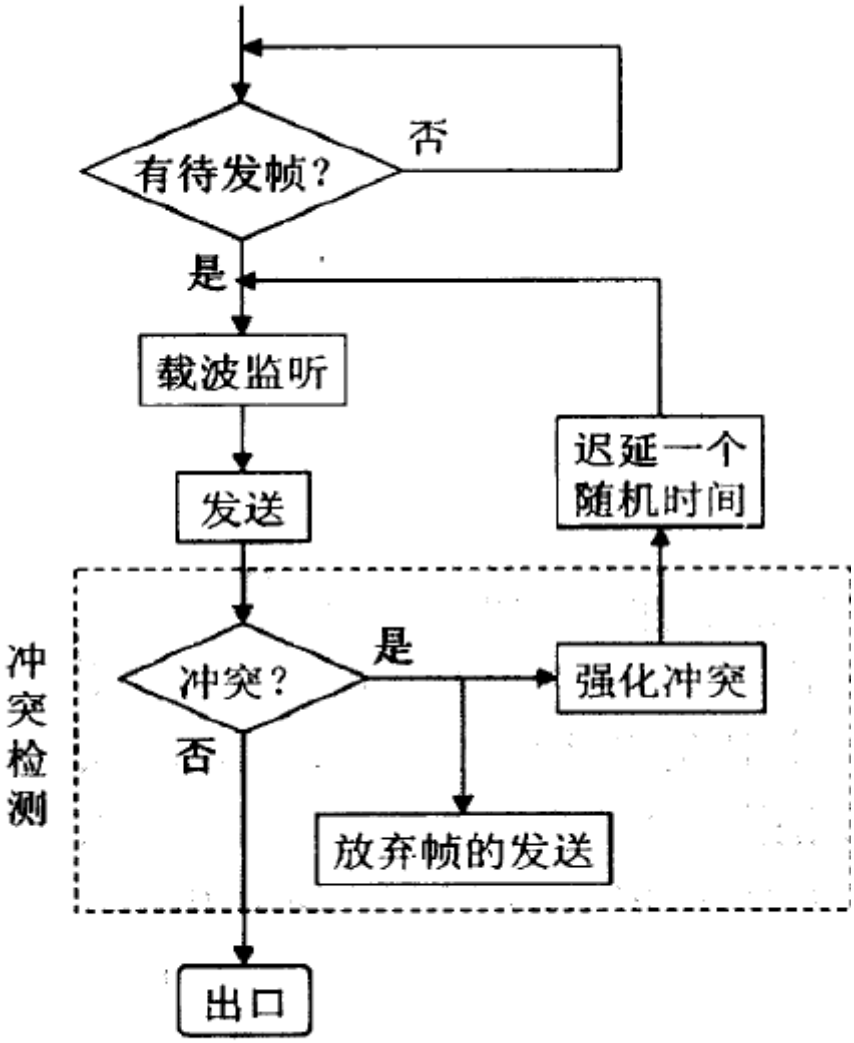


图 5-12　CSMA/CD 的流程图

以太网如何处理介质接入?

（1）载波侦听（先听后发）

以太网要求每个站点监听电缆，检测是否已有一个传输正在处理

（2）冲突检测（边发边听，冲突停发）

每个站点在发送过程中监听电缆，如果电缆信号与本站发送的信号不符即认定为冲突，立即终止发送。

（3）二进制指数规避（随机延迟后重发）

冲突发生后，需要从冲突中恢复

标准规定基本退避时间d，每个检测到冲突的站点随机选一个小于2的整数r，延迟rd时间。

10、高速以太网

以太网从10Mb到100Mb的演进是无缝连接的

11、其他网络

LocalTalk、令牌环、FDDI、

ATM（异步传输模式）：是星型拓扑结构

12、WLAN（无线局域网）的基本概念

蓝牙速率：1Mbps左右

GPS和GPRS的区别：GPS是全球定位系统

而GPRS是通用分组无线服务技术的简称，它是GSM移动电话用户的一种移动数据业务。

WIFI>4G>蓝牙

13、什么是冲突域和广播域

（1）冲突域，是同一时间内只能有**一台设备发送信息的范围**，它属于**物理层**范围，可以由数据链路层的设备隔离冲突域，比如**交换机。**交换机可以缩小冲突域的范围，每一个端口就是一个冲突域。

（2）广播域：如果站点发出一个广播信号，**所有能接收收到这个信号的设备范围**称为一个广播域，它属于**数据链路层**，可以由网络层的设备隔离广播域，比如路由器。路由器的每一个端口就是一个广播域。

	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）	√	√

14、中继器、集线器、网桥

（1）中继器（Repeater）是工作在**物理层**上的连接设备，它**不理解帧格式，也没有物理地址**，它的功能是通过对数据信号的重新发送或者转发，来**扩大网络传输的距离。**

扩展局域网上的计算机不知道中继器是否将它们分开。

中继器**不能隔离域**

（2）集线器工作在**物理层**，它使原来属于不同碰撞域的局域网上的计算机能够进行跨碰撞域的通信，扩大了局域网的覆盖的地理范围

集线器**不能隔离域**

（3）网桥是用于连接两个局域网的互联设备，它工作在**数据链路层**，可以对帧进行过滤转发，对设备的物理地址进行学习，但传播过多广播则会产生网络阻塞，即广播风暴。

网桥**可以隔离冲突域，不能隔离广播域。**

15、交换机（Switch）

局域网交换机，又称**以太网交换机**，工作在数据链路层，保证每个设备在一个独立的网段中，能将网络分成小的冲突域，为每个工作站提供更高的带宽：以太网交换机可以让用户**独占传输媒体的带宽**，而不是共享，**每个接口都是全双工。**

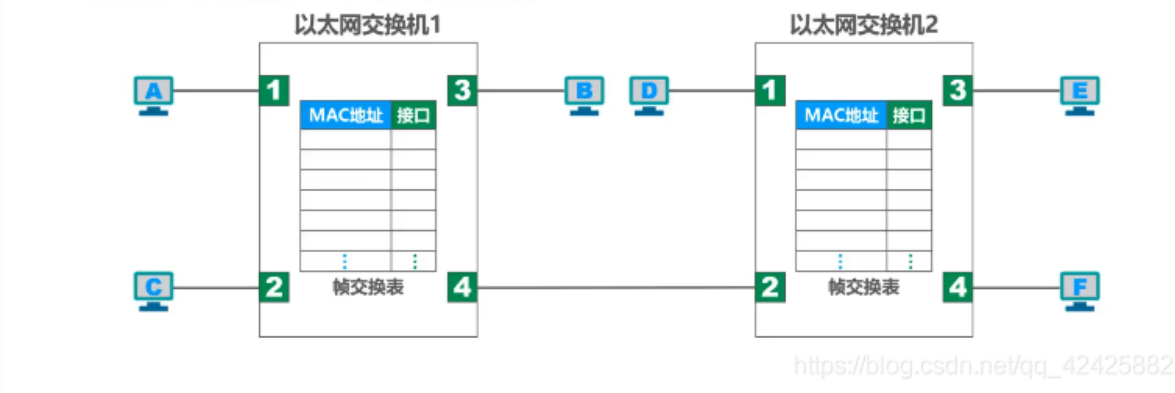
以太网交换机由CPU+RAM+ROM+NIC构成

交换机**可以隔离冲突域，不能隔离广播域。**

交换机在收到帧后，在交换机表中查找目的MAC地址对应的接口好，然后通过该接口转发帧。

交换机的自学习

从下边这个模型分析：交换机表初始为空



当A->B发送帧：

交换机1**首先记录A的MAC地址及对应的接口1**，查找交换机表，无B的MAC，**则除A的接口，其他接口全部转发帧（盲目泛洪）**；
接口4将帧转发到交换机2，交换机2记录A的MAC地址及对应接口号2，查找B的MAC地址，没有，则盲目泛洪，D、E、F主机接收到帧，根据目的MAC判断不是自己的帧，不理会；
交换机1转发的帧到达B主机，B回应帧，在交换机1中记录B的MAC地址及接口号3，查找A的MAC地址，能找到，转发到接口1.

16、上行和下行

多数互联网用户遵循非对称模式：即**接受的数据比发送的多**

上行（upstream），即**用户传输数据**到ISP（互联网服务提供商）

下行（downstream），是指从互联网ISP传取数据到用户

在网络方面，**网络带宽指的是数据速率**

17、ADSL

非对称数字用户线路（ADSL）采用**频分多路复用**

ADSL的特点：**上行和下行带宽是不对称的**

住在同一条街上的两个邻居都用ADSL服务，但下载速率不一样，为什么?

答：ADSL是**自适应的**，启动时，用户线两端测试可用频率、各子信道受干扰情况，并使用质量来选择调制方案。

18、广域网（Wide Area Network）

广域网（WAN），一般范围为国家层面。

由于广域网主机多，需要分层寻址方案，采用**站点号+主机号**的方式

第一部分标识分组交换机，每个分组交换机被分配唯一一个号码

第二部分标识特定计算机

广域网使用**路由器**连接成网络

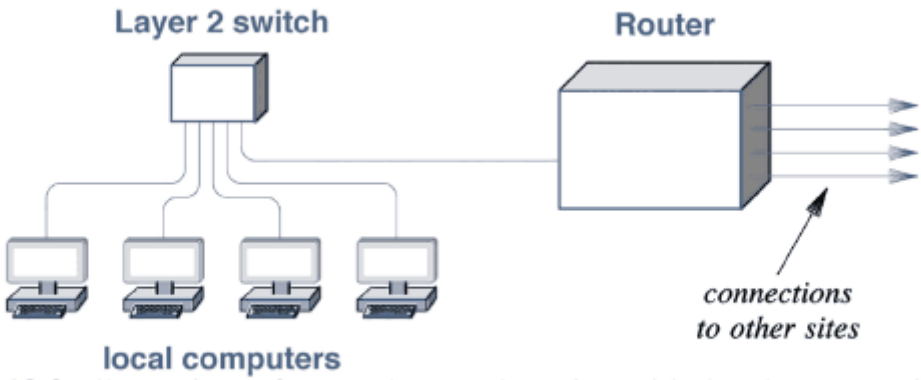


Figure 18.2 Illustration of a modern WAN site with local communication handled by a separate LAN.

其中，第二场交换机主要发挥交换作用，路由器（Router）主要发挥路由功能。

19、路由与转发

将数据包转发到下一跳的过程称为路由

路由器主要完成两个功能：一个是路由选择，另一个是分组转发（当一个分组到达时所采取的动作）

（1）路由选择：根据特定的路由选择协议构造出路由表，同时根据相邻的路由表交换路由信息，不断更新和维护路由表

（2）分组转发：路由器根据转发表将用户的IP数据报从合适的端口转发出去。

路由器和交换机的区别：

每一个路由器与其之下连接的设备，其实构成一个局域网

交换机工作在路由器之下，就是也就是**交换机工作在局域网内**

交换机用于**局域网内网的数据转发**

路由器用于**连接局域网和外网**

路由器可以用来连接不同类型的网络，而交换机不行

20、路由表、默认路由

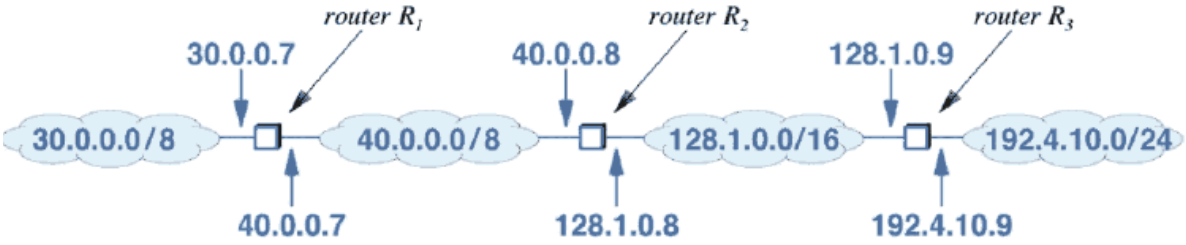
路由器转发分组是通过路由表转发的，而路由表是通过各种算法得到的主要分为两类

（1）静态路由：交换机启动时，计算并安装路由，路由不会改变

（2）动态路由：路由器

对比：静态路由简便、可靠，在负荷稳定、拓扑变化不大的网络中运行效果很好，动态路由算法能改善网络的性能并有助于流量控制。

路由表的组成：目标网络号，子网掩码，下一跳（包括直接传送标志或者**子网IP地址**）



(a)

Destination	Mask	Next Hop
30.0.0.0	255.0.0.0	40.0.0.7
40.0.0.0	255.0.0.0	deliver direct
128.1.0.0	255.255.0.0	deliver direct
192.4.10.0	255.255.255.0	128.1.0.9

该图为R2的路由表

😨21、分层、每一层的作用、传输最小单位等，看表

网络层

1、IPV4编址方案

采用**点分十进制记数法**（Dotted decimal notation）

每8位作为无符号十进制数（0-255）并用点分隔

IP地址是全球唯一的32位数字，组成方式是**网络号+主机号**

其中，网络号标志主机（或路由器）所连接到的网络，全球协调

主机号标识网络上的特定计算机，局域网内协调。

传统分类方式：ABCDE类

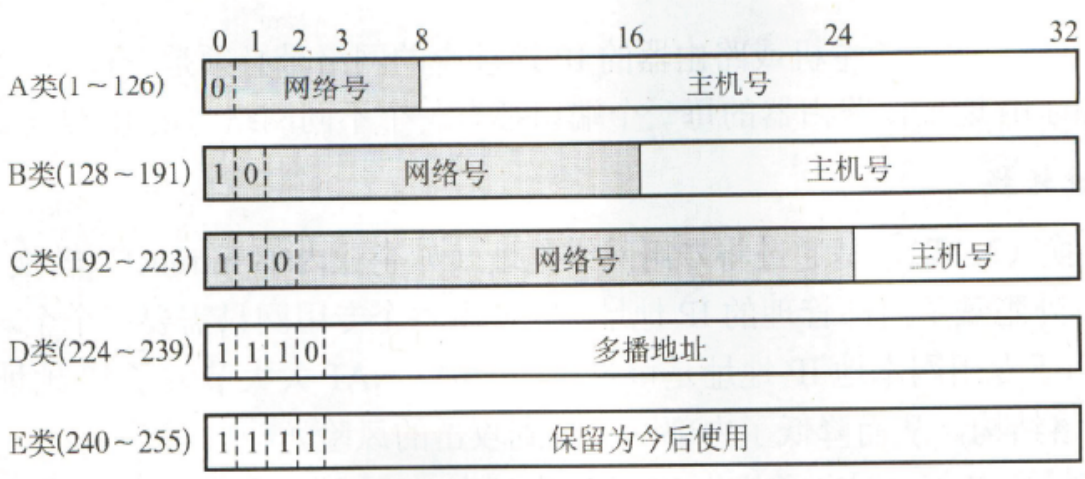


图 4-6 分类的 IP 地址

特点：**根据前几位**来确定该ip地址属于哪一类

A类前8位是网络号，B类前16位是网络号，C类前24位是网络号

特殊的 IP地址，不用做主机IP地址：

①主机号全为0，表示网络本身

②主机号全为1，表示本网络的广播地址

③32位全为0，表示本网络上的主机

④32位全为1，表示受限广播地址，255.255.255.255等效为本网络的广播地址

⑤127.0..0.0/8网络保留为环路自检地址，表示任意主机本身

2、CIDR表示法

无类域间路由，一般形式为**ddd.ddd.ddd.ddd/m**

其中，**d为网络号，m为子网掩码中1的个数（不一定是8的倍数）**

例：

3、子网划分（考综合题）

将网络进一步划分成子网，即：**网络号+子网号+主机号**

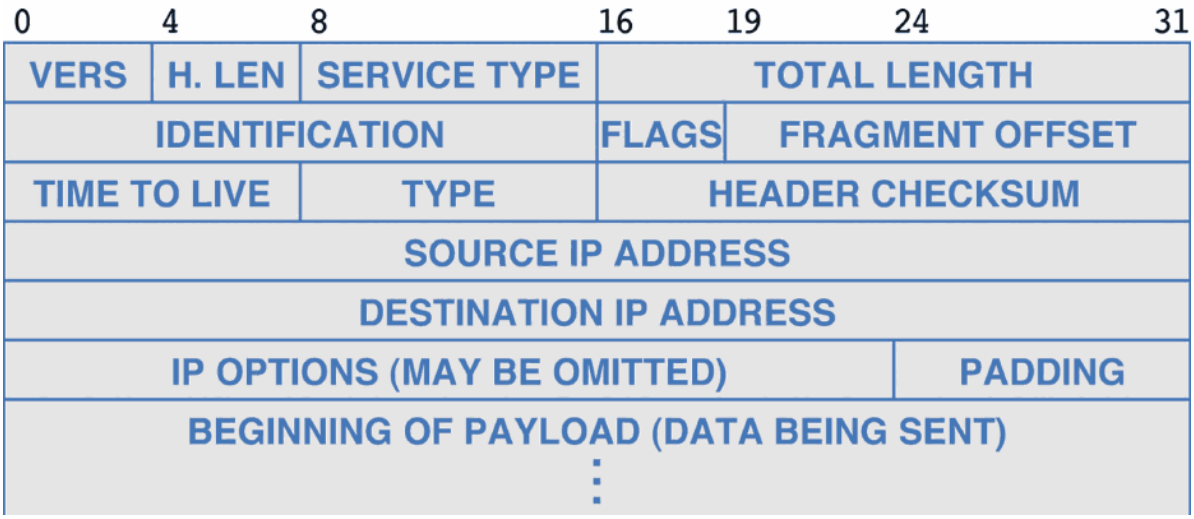
从主机号借若干位作为子网号，主机号相应减少

从其他网络发送给本单位某台主机的IP数据报，**仍根据其目的网络号，找到本单位的路由器**，随后该路由器提取子网号找到目的子网，最后将IP数据报直接交付给目的主机

路由器在和相邻路由器交换路由信息时，必须把自己所在网络（子网）的子网掩码告诉路由器，路由表中的每一个项目，**除了要给出目的网络地址外，还必须给出该网络的子网掩码**

4、IP数据报

TCP/IP协议使用IP Datagram来引用Internet数据分组



IPV4数据报包含20B至64KB

版本：4b

报头长度：4b

服务类型：8b

报文总长度：16b

标识：16b

分片标志：3b

片偏移：13b

生存时间（TTL）：8b

协议类型：8b

报头校验和：16b

源IP地址：32b

目的IP地址：32b

选项内容/

5、最大传输单元MTU

数据链路层帧支持的最大传输字节数

当MTU<IP报文长时，分成较小分片传输，每个分片**依然使用IP数据报格式**，并独立发送

分片原则：

IP头部固有长度（20字节）也在帧的载荷内，且后续片的**偏移量应为8的整数倍**

报文重组：**所有分片重组在目标端进行**，中间路由设备不做分片重组

6、ICMP协议

Internet Control Message Protocol，Internet控制报文协议，为了**提高IP数据报交付成功的机会**，在**网络层**使用其来允许主机或路由器报告差错和异常情况

（1）Ping命令的原理

Ping用ICMP回应请求和回应应答报文来实现。它发送一个包含ICMP回应请求的报文给目的地，如果在等待时间内没用收到应答，则重新传送请求，若重传请求仍没有收到应答（或者收到了ICMP的目的不可达报文），则Ping声称该机器为不可达。

Ping命令**没有通过传输层的TCP或UDP**，它是应用层直接使用网络层ICMP的例子

（2）TraceRoute命令的原理

TraceRoute利用ICMP及IP头部的TTL域得到一连串数据包路径，如果TTL达到0，则路由器丢弃数据报，并将ICMP超时错误发送回源。每次将送出的报文的TTL加1来发现另一个路由器，直到该值足够大到数据报到达其最终目标。

7、地址解析协议（ARP）：使用UDP传输

无论网络层使用什么协议，在实际网络的链路上传送数据帧时，最终必须使用硬件地址，将**ip地址解析为MAC地**址叫做地址解析，这就是Address Resolution Protocol，它工作在**网络层**，每个主机都设有一个ARP高速缓存，存放本局域网上各主机和路由器的IP地址到MAC地址的**映射表，称为ARP表**

注意：ARP解决的是**同一局域网**上的IP和MAC的映射问题，如果所要找的主机和源主机不在同一个局域网上，则要通过ARP协议找到**一个位于本局域网上的路由器**的硬件地址，将分组发给这个路由器，再让这个路由器把**分组转发给下一个网络。**

ARP高速缓存

当主机A向主机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，有的话即可查出其硬件地址，再将此硬件地址写入MAC帧，将MAC帧发往此地址。

8、IPV6

地址空间：**128位**，采用**冒分十六进制数表示法**（兼容CIDR表示法）

即：16位一组，以冒号分隔每个组

注意：前导0压缩和零压缩(两个冒号代替连续出现两个以上的0)

2001:0db8:85a3:0000:0000:8a2e:0370:7334

正确的应为: 2001:db8:85a3::8a2e:370:7334

传输层☆

传输层为运行在不同主机上的**进程**之间提供了逻辑通信（**端对端的通信**）

1、UDP

用户数据报协议（User Datagram Protocol）

作用：不可靠但是**轻快**的传输，允许丢失重复延迟乱序损坏

UDP的主要特点：

（1）无连接：发送数据之前不需要建立连接，，而TCP协议中通信双方保持序列号等变量，确保通信可靠

（2）尽力而为：不保证可靠交付，同时也不使用拥塞控制

（3）轻量级

（4）支持一对一、**一对多**的交互通信

（5）**支持广播通信**

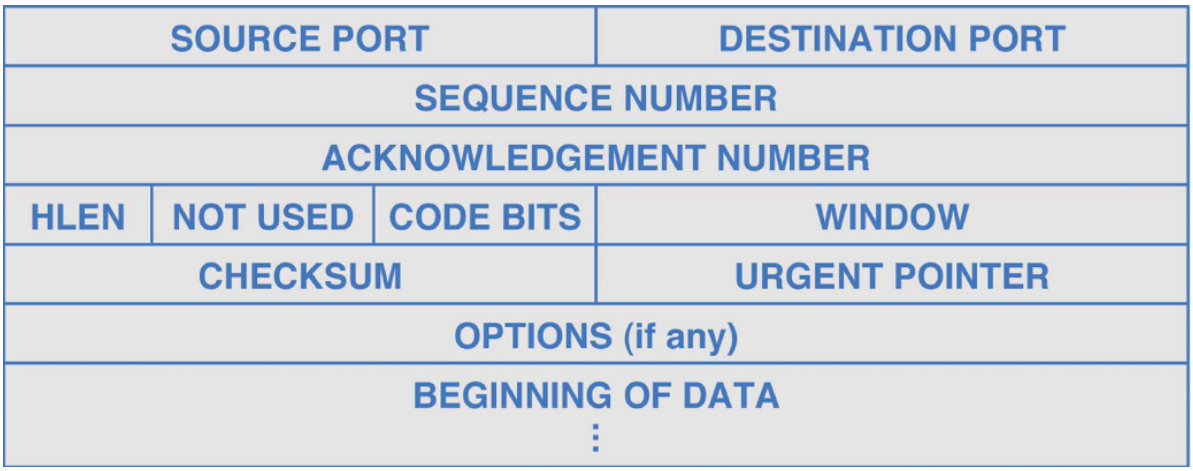
应用场景：常用于**丢包损失不大**，应用层可以控制丢包的场景

比如DNS、DHCP、网络游戏、**广播**

2、TCP

传输控制协议（Transmission Control Protocol）,即TCP，它提供面向连接、**点对点**、流接口、**完整可靠**的**全双工**通信

TCP报文段的格式（基本信息20B）



源端口号：16b 目的端口号：16b

发送数据的序列号（报文段序号）：32b

确认序列号（32b）：**期望收到下一个字节的序号，不是已收到的序号**

报头长度：4b 保留位：4b 标识符：8b 滑动窗口缓冲区大小：16b

校验和：16b 紧急指针16b

数据

TCP的传输是以**字节**为单位，封装在**报文段**中传输

将字节写入发送缓存->加入TCP首部变成报文段->发送->读取缓存并去掉头部

TCP连接是一条**虚连接**，不是真正的物理连接

3、对比

4、停止等待协议

A和B双方建立好tcp连接后就可以相互发送数据了，A为发送方，B为接收方。**“停止等待”就是每发送完一个分组就停止发送，等待对方确认后再发送下一个分组**，即：发送、停止、等待。

协议会设置一个超时计时器，当出现差错时，在计时器结束后仍然没有收到确认，则丢弃之前那份报文，进行”**超时重传**“

优点：简单，缺点：**信道利用率太低**

窗口机制：可以通过发送窗口传递信息

窗口内的分组都连续发送出去，不需要等待确认，每收到一个确认，窗口向前推进一格

5、流量控制：滑动窗口机制

如果发送方把数据发送得过快，接收方可能来不及接收，造成数据的丢失

流量控制的目的就是**使发送方的发送速率让接收方来得及接收**，且不使网络发生拥塞。

TCP窗口单位是字节，不是报文段

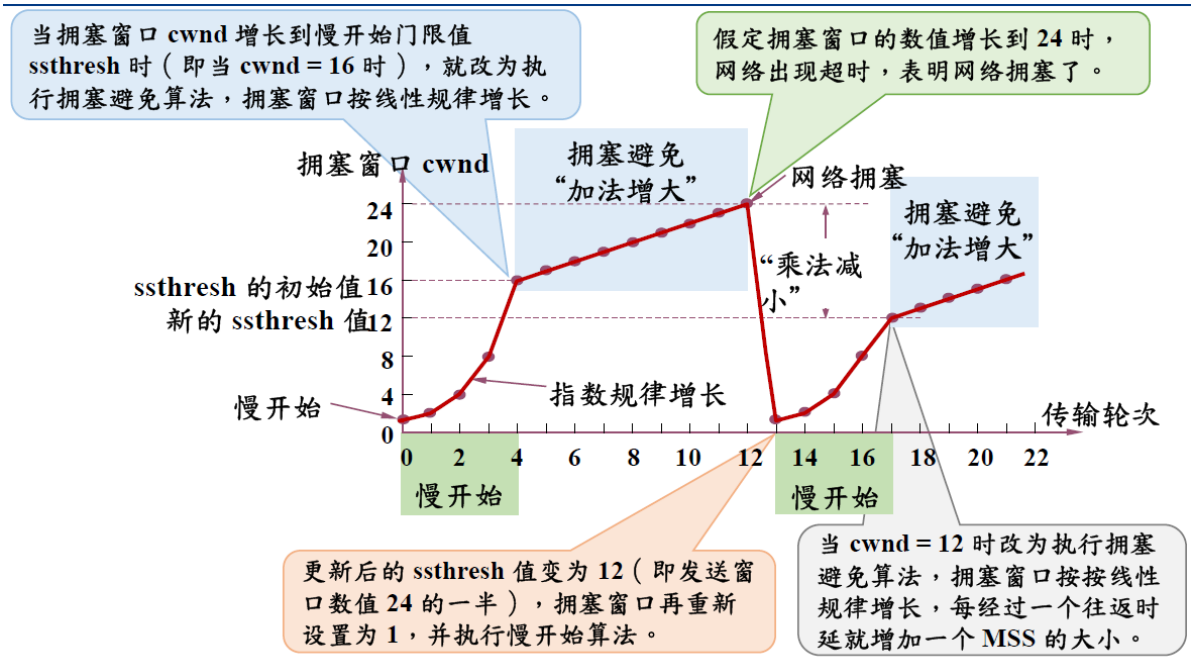
TCP为每一个连接设有一个持续计时器，只要一方收到对方的零窗口通知， 就启动持续计时器。**若计时器时间到期，就发送一个零窗口探测报文段，对方给出现在的窗口值**

6、拥塞控制

在某段时间，若对网络中**某资源的需求超过了该资源所能提供的可用部分**，网络的性能就会变坏，产生拥塞。

条件：对资源需求总和>可用资源

慢开始和拥塞避免



快重传和快恢复:

接收方每收到一个失序的报文段后就立即发出重复确认，让发送方及早知道

发送方只要**一连收到三个重复确认**就应当重传对方尚未收到的报文段

7、流量控制和拥塞控制的区别

二者的控制目的不同。流量控制是指抑制发送端发送数据的速率，以便接收端来得及接收；而拥塞控制是防止过多的数据注入到网络中，使网络中的路由器不至于过载。

8、为什么TCP不能发送广播?

因为TCP建立连接是一对一 的通路，建立流的通路，而流是不能广播的，接受字节很难区分接收方，造成混乱。

☆9、TCP的三次握手建立连接

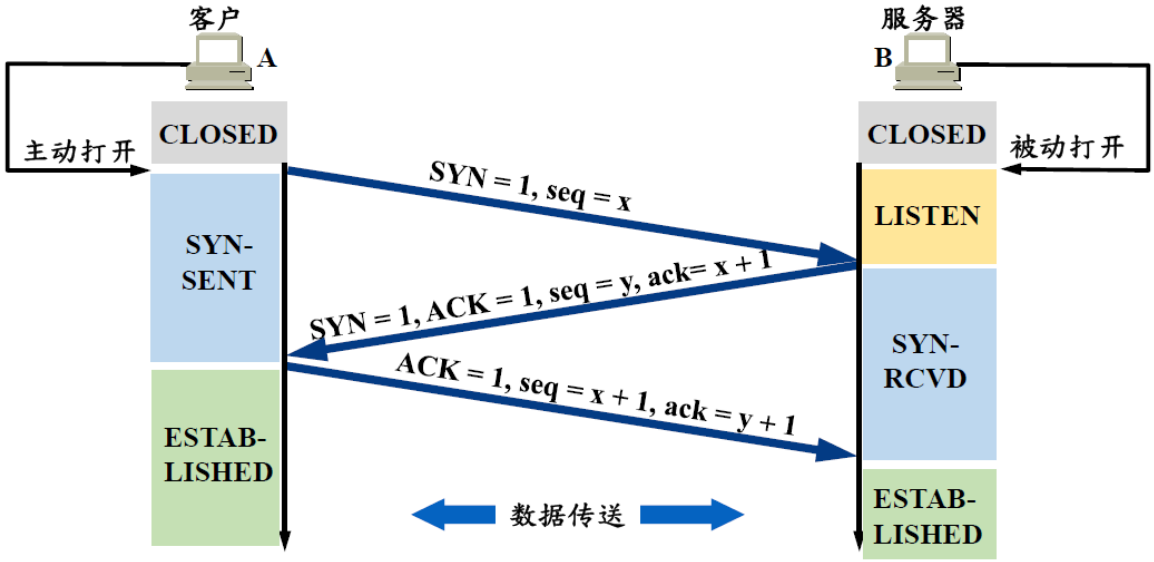
1、A的TCP向B发出**连接请求**报文段，其首部的**同步位SYN=1。**同时**选择序号seq=x**，表明传送数据时的第一个数据字节的序号是x

2、B的TCP在收到连接请求报文段后，如果同意，则发回确认。

在确认报文段中，使**SYN=1**，**ACK=1**，其**确认号ack=x+1**，自己选择的**seq=y。**

3、A在收到确认报文段后，**ACK=1，seq=x+1，ack=y+1**

此时，A的TCP通知应用进程，连接已建立，B收到A确认后，通知上层应用进程连接建立



10、TCP的四次握手建立连接

数据传输结束后，**双方都可以释放连接。**

1、A把连接释放报文段首部的**FIN=1**，**seq=u**，等待B的确认

2、B发出确认，ACK=1，确认号ack=u+1，该报文段序号seq=v

此时，从A到B的这个方向的连接是释放了，但B若发送数据，A仍要接收

3、若B已经没有向A发送的数据，则FIN=1，ACK=1，ack=u+1，seq=w

4、A在收到释放报文段后要发出确认，ACK=1，ack=w+1，seq=u+1

应用层

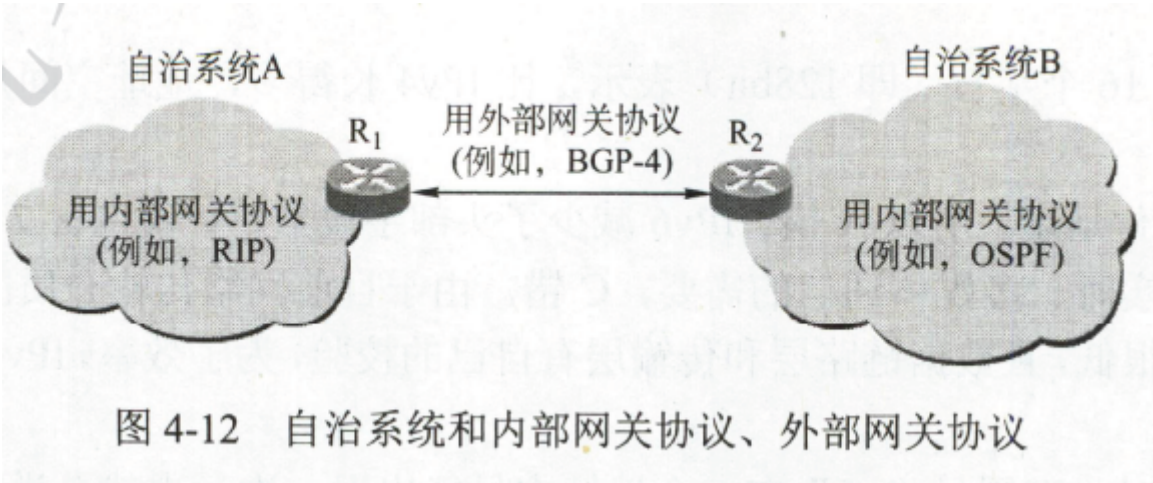


图 4-12　自治系统和内部网关协议、外部网关协议

☆1、内部网关协议（IGP）

（1）路由信息协议（RIP）

RIP是一种分布式的**基于距离向量**的路由选择协议，最大优点是简单

距离也称为跳数，规定从一**路由器到直接连接的网络的跳数为1**，每经过一个路由器，跳数加一。

算法步骤：

①对地址为X的相邻路由器发来的RIP报文，先修改此报文中的所有项目，把下一跳改为X，把所有距离字段的值加1

②对修改后的RIP报文中的项目进行以下步骤

原来路由表没有网络N，添加到路由表中

原来路由表有网络N，且下一跳是X，则替换原来的

原来路由表有N，但下一跳不算X，若收到的距离短，则替换原来的

否则什么都不做。

③如果180s还没有收到相邻路由器的更新路由表，则把相邻的路由器距离置为16（不可达）

缺点：限制了网络的规模，最大距离为15

网络出现故障时需要较长时间才能将信息传送到所有的路由器

（2）开放最短路径优先（**OSPF**）

OSPF向本自治系统中的所有路由器发送信息，**洪泛法**，发送的信息是本路由器相邻的

2、二者比较

（1）RIP协议仅向自己**相邻**的几个路由器发送信息，而OSPF向自治系统中的所有路由器发送信息（**洪泛法，广播**）

（2）RIP发送的信息是**整个路由表**，而OSPF发送的是与本路由器相邻的所有路由器的**链路状态**

（3）RIP协议中，不管网络拓扑是否发生变化，路由器之间都会**定期交换路由表信息**，而OSPF只有**当链路状态发生变化**时才发送信息

（4）RIP会有"**坏消息传得慢**"的情况，而OSPF**更新过程收敛的快。**

（5）RIP是**应用层**协议，它在传输层使用**UDP**协议，而OSPF是**网络层**协议，它使用**IP数据报**进行传送

3、C/S交互模式工作原理

客户和服务器都是指通信中所涉及的两个应用进程，

客户端是访问服务器提供的服务的程序，

服务器是为客户程序或设备提供功能的计算机程序或设备

工作模式：

客户是主动打开的，主动结束的

服务器向被动打开的大门，响应客户端的请求，当请求到达时，它会作出迭代的或同步的响应。

☆4、Socket函数调用流程

bind的作用是什么?

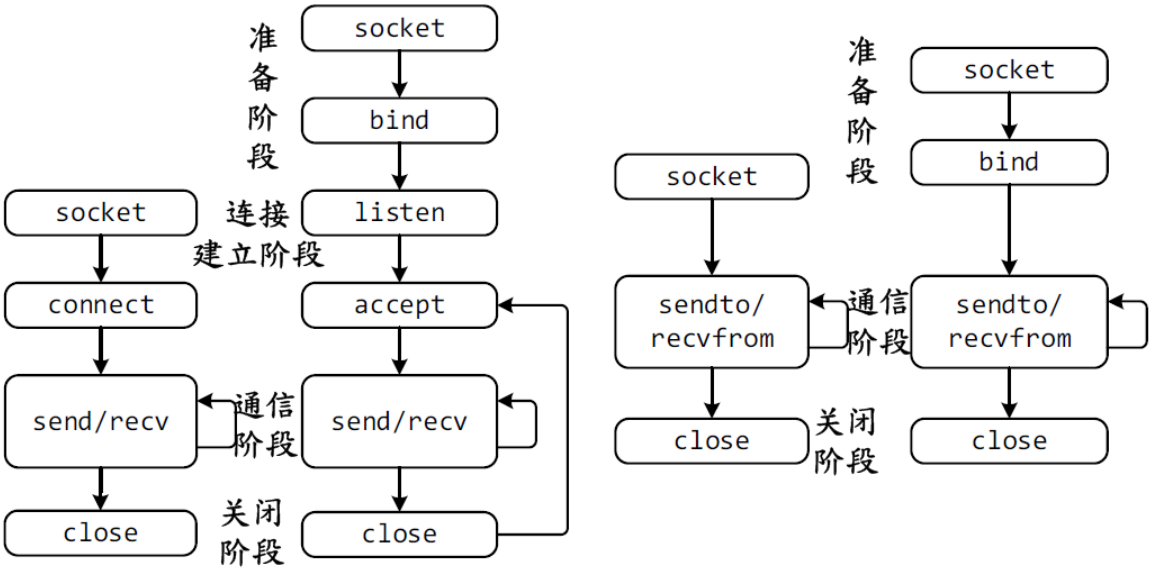
通过调用bind来**把熟知的端口号和本地IP地址填写到已创建的套接字中。**

listen的作用是什么？（TCP）

在调用bind后，服务器还必须调用listen**把套接字设置为被动方式，以便随时接受客户的服务请求**

服务器紧接着就调用accept，用来提取用户发来的连接请求，示例图如下

• TCP面向连接　　UDP无连接

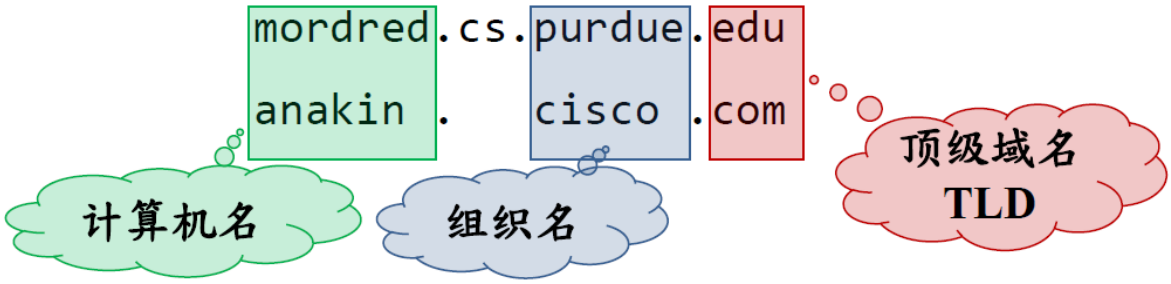


每张图左边的是Client端的连接情况，右边的是Server端的连接情况

5、DNS

域名系统提供了将人类可读符号域名映射到计算机地址的服务

层次树状结构：计算机名+组织名+顶级域名TLD



6、递归查询和迭代查询

7、域名高速缓存

☆8、点击鼠标发生的事件

用户点击鼠标后所发生的事件

- 浏览器分析超链指向页面的 URL。
- 浏览器向DNS请求解析 www.tsinghua.edu.cn 的 IP 地址。
- 域名系统DNS解析出清华大学服务器的 IP 地址。
- 浏览器与服务器建立 TCP 连接
- 浏览器发出取文件命令：GET /chn/yxsz/index.htm。
- 服务器给出响应，把文件 index.htm 发给浏览器。
- TCP 连接释放。
- 浏览器显示院系设置文件 index.htm 中的所有文本。