1.电路交换与分组交换的区别？优劣对比。

**电路交换：**由于电路交换在通信之前要在通信双方之间建立一条被双方独占的物理通路（由通信双方之间的交换设备和链路逐段连接而成）。因而有以下优缺点。

**优点：**

①由于通信线路为通信双方用户专用，数据直达，所以传输数据的时延非常小。

②通信双方之间的物理通路一旦建立，双方可以随时通信，实时性强。

③双方通信时按发送顺序传送数据，不存在失序问题。

④电路交换既适用于传输模拟信号，也适用于传输数字信号。

⑤电路交换的交换的交换设备控制均较简单。

缺点：

①电路交换的平均连接建立时间对计算机通信来说嫌长。

②电路交换连接建立后，物理通路被通信双方独占，即使通信线路空闲，也不能供其他用户使用，因而信道利用低。

③电路交换时，数据直达，不同类型、不同规格、不同速率的终端很难相互进行通信，也难以在通信过程中进行差错控制。

**分组交换**：分组交换采用存储转发传输方式，但将一个长报文先分割为若干个较短的分组，然后把这些分组（携带源、目的地址和编号信息）逐个地发送出去，因此分组交换除了具有报文的优点外，与报文交换相比有以下优缺点：

优点：

①加速了数据在网络中的传输。因为分组是逐个传输，可以使后一个分组的存储操作与前一个分组的转发操作并行，这种流水线式传输方式减少了报文的传输时间。 此外，传输一个分组所需的缓冲区比传输一份报文所需的缓冲区小得多，这样因缓冲区不足而等待发送的机率及等待的时间也必然少得多。

②简化了存储管理。因为分组的长度固定，相应的缓冲区的大小也固定，在交换结点中存储器的管理通常被简化为对缓冲区的管理，相对比较容易。

③减少了出错机率和重发数据量。因为分组较短，其出错机率必然减少，每次重发的数据量也就大大减少，这样不仅提高了可靠性，也减少了传输时延。

④由于分组短小，更适用于采用优先级策略，便于及时传送一些紧急数据，因此对于计算机之间的突发式的数据通信，分组交换显然更为合适些。

缺点：

①尽管分组交换比报文交换的传输时延少，但仍存在存储转发时延，而且其结点交换机必须具有更强的处理能力。

②分组交换中的每个分组都要加上源、目的地址和分组编号等信息，这将增大传送的信息量，一定程度上降低了通信效率，增加了处理的时间，使控制复杂，时延增加。

③当分组交换采用数据报服务时，可能出现失序、丢失或重复分组，分组到达目的结点时，要对分组按编号进行排序等工作，增加了麻烦。若采用虚电路服务，虽无失序问题，但有呼叫建立、数据传输和虚电路释放三个过程。

2. OSI有哪几层，会画出来，知道主要几层的各自作用。



物理层：提供一个传输原始比特流的物理连接，实现透明的传送比特流。

数据链路层：建立相邻节点间的数据链路，在有差别的物理介质上实现无差错的传输、

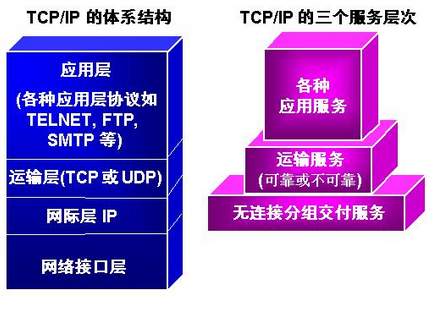
网络层：提供逻辑编址，数据寻址和路由。

传输层：提供端到端的透明传输。

会话层：提供数据同步过程中的会话管理。

表示层：数据格式转换。

应用层：为用户的应用程序提供网络接口。  
3. TCP/IP有哪几层，会画出来，知道所有层数的作用，会列举各层主要的协议名称。



**1、网络接口层**

     物理层定义与传输媒体的接口有关的一些特性，即机械特性、电气特性、功能特性、过程特性，并需要完成并行传输和串行传输之间的转换。

     数据链路层向该层用户提供透明的和可靠的数据传输服务。 透明性是指该层上传输的数据的内容、格式及编码没有限制，也没有必要解释信息结构的意义；可靠性是指在传输过程中将物理层提供的可能出错的物理连接改造成为逻辑上无差错的数据链路，其具体的方法有帧同步、差错控制、流量控制、链路管理。

     物理层中主要的宽带接入技术有xdsl、光纤同轴混合网（HFC）、FTTx技术

     数据链路层中的主要协议有点对点协议PPP，CSMA/CD协议，以太网802.3。

**2、网际层**

     网际层向上值提供简单灵活的、无连接的、尽最大努力交付的数据报服务。网际层不提供服务质量的承诺，即所传输的分组可能出错、丢失、重复和失序，当然也不保证分组交付的时限。

     网际层中主要协议有IP协议，地址解析协议ARP和逆地址解析协议RARP，网际控制报文协议ICMP。

     IP协议是网际层的核心，通过路由选择将下一跳IP封装后交给网络接口层。IP 数据报是无连接服务。

     ICMP是网际层的补充，可以回送报文。用来检测网络是否通畅（使用ping命令）。

     ARP是通过已知IP，寻找对于主机的MAC地址。

     RARP是通过过MAC地址确定IP地址。

**3、运输层**

     运输层为应用进程之间 提供端到端的逻辑通信，并具有复用和分用的功能，即发送方不同的应用进程都可以使用听一个运输层协议传送数据；接收方的运输层在剥去报文的首部后能够把这些数据正确交付到目的应用进程。运输层还将对报文进行差错控制，以提高可靠传输。

     运输层中主要协议有用户数据报协议UDP和传输控制协议TCP

**4、应用层**

应用层为用户提供应用程序。

     应用层中主要协议有域名系统DNS，文件传输协议FTP，远程终端协议TELNET，超文本传输协议HTTP，简单邮件传送协议SMTP，邮件读取协议POP3和IMAP，动态主机配置协议DHCP，简单网络管理协议SNMP。

     DNS：提供域名解析服务，提供域名到IP地址之间的转换，使用端口53

     FTP：在异构网络中任意计算机之间传送文件，使用端口21

     TELNET：提供用户远程登录服务，使用端口23，使用明码传送，保密性差、简单方便

     HTTP：用于实现万维网上的各种链接，即万维网客户程序与万维网服务器之间的连接，使用端口80

     SMTP/POP3、IMAP：提供邮件的传输，用来控制信件的发送、中转/从邮件服务器读取邮件。

     DHCP：为新加入网络的计算机自动分配IP地址。

     SNMP：管理互联网Internet上众多厂家生产的软硬件平台  
4. 硬件(MAC)地址的概念及作用。

概念：MAC地址就是在媒体接入层上使用的地址，也叫物理地址、硬件地址或链路地址，其被固化在适配器的ROM中。可见MAC地址实际上就是适配器地址或适配器标识符。当某台计算机使用某块适配器后，适配器上的标识符就成为该计算机的MAC地址。MAC地址长度为6字节（48比特），由IEEE的注册管理结构RA进行管理分配。

作用：MAC地址是计算机的唯一标识，在数据链路层中，交换机通过识别MAC地址进行数据包的传输。  
5. ARP协议的用途 及算法、在哪一层上会使用arp ？

ARP协议的用途：解决同一个局域网内主机或路由器的IP地址和MAC地址的映射问题。

算法：在主机的ARP高速缓存中应存放一个从IP地址到MAC地址的映射表，并且这个映射表还经常动态更新（新增或超时删除）。

在网络层会使用ARP。  
6. CRC冗余校验算法，反码和检验算法。  
7. 如何实现透明传输。

透明传输的基本概念：

* 数据透明传输就是用户不受协议中的任何限制，可随机的传输任意比特编码的信息
* 用户可以完全不必知道协议中所规定的结束段的比特编码或者其他的控制字符，因而不受限制的进行传输。

数据透明传输技术：

* 转义字符填充法
* 零比特填充法
* 采用特殊的信号与编码法：IEEE802.3(由于使用CSMA/CD协议，没有结束字符段；IEEE802.4（令牌总线，在起始定界符SD/结束定界符ED这两个字段被使用模拟编码，而不是0和1）；IEEE802.5（令牌环，违例的曼切斯特码）
* 确定长度法，固定数据段长度法：各控制字段的长度固定，数据段长度也是固定的，那么在帧格式中就不必设结束符，也不必设数据长度字段。

8. 知道各个层使用的是哪个数据交换设备。（交换机、路由器、网关）

物理层用到的设备是集线器和中继器

数据链路层用到的设备是交换机和网桥

网络层用到的设备是路由器

应用层用到的设备是网关

* 中继器的主要功能是对接收到的信号进行再生整形放大以扩大网络的传输距离。
* 集线器在此基础上将所有的节点集中在以它为中心的节点中，可组成星型拓扑结构。
* 交换机是一种基于MAC识别，能完成封装转发数据包功能的网络设备。它可以“学习”MAC地址，并把其存放在内部地址表中，当一个数据帧的目的地址在MAC地址表中有映射时，它被转发到连接目的节点的端口而不是所有端口。交换机将局域网分为多个冲突域，每个冲突域都是有独立的宽带，因此大大提高了局域网的带宽。
* 网桥是数据链路层互联的设备，在网络互联中可起到数据接收、地址过滤与数据转发的作用，可用来实现多个不同网络系统之间的数据交换。
* 路由器用于连接多个逻辑上分开的网络，具有判断网络地址和选择IP路径的功能，它能在多网络互联环境中，建立灵活的连接，可用完全不同的数据分组和介质访问方法连接各种子网。
* 网关在网络层以上实现网络互连，用于两个高层协议不同的网络互连。与网桥只是简单地传达信息不同，网关对收到的信息要重新打包，以适应目的系统的需求。  
  9. 路由表的内容。
* Network Destination：目标网段
* Netmask：子网掩码，IP地址与子网掩码按位与，可以得出该IP地址的网络号，IP地址与子网掩码取反后按位与，可以得出该IP地址的主机号。
* Interface：达到该目标网段的本地路由器的出口IP。
* Gateway：网关IP，下一跳路由器的入口IP，通常情况下，interface和gateway是同一网段的。
* Metric：跳数，该条路由记录的质量，一般情况下，如果有多条到达相同目的地的路由记录，路由器会采用metric值小的那条路由。

10. 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N

2）若N就是于此路由器直接相连的某个网络地址，则进行直接交付，不需要在经过其他路由器，直接把数据报交付给目的主机（这里      包括把目的地址D转换为具体的MAC地址，把数据报封装成MAC帧，在发送此帧）；否则就是间接交付。

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。

4）若路由表中有达到网络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。

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

6）报告转发分组出错。  
11. IP报文的格式，格式的各个字段的含义要理解。



IP数据包由报头和数据两部分组成。报头的前一部分是固定长度，共20字节。在报头的固定部分的后面是可选部分——IP选项和填充域。

首部各字段的含义如下

1、版本

     占4位，指IP协议的版本。

2、报头长度

     占4位，该字段的单位是32位字（1个32位字长是4字节），因此当IP报头长度为1111时，报头长度就达到最大值60字节。当IP分组的首部长度不是4字节的整数倍是，就需要对填充域加以填充。最常用的报头长度为20位(报头长度值为0101)，这时不使用任何选项。

3、区分服务（服务类型）

     占8位，在一般情况下都不使用这个字段。

4、总长度

     指报头和数据之和的长度，单位是字节。总长度字段为16位，故IP数据报的最大长度为65535。

     每一种数据链路层都有其自己的帧格式，其中包括帧格式中的数据字段的最大长度，这称为最大传送单元MTU。当IP数据报封装成链路层的帧时，此数据报的总长度不能超过对应MTU的值。若数据报长度超过对于MTU的值，就将数据报进行分片处理，此时数据报首部中的“总长度“字段是指分片后的每一个分片的报头长度和数据长度之和。

5、标识

     占16位。IP软件在存储器中维持一个计数器，每产生一个数据报，计数器就加1，并赋给标识字段。当数据报进行分片处理后，每个分片的标识值都与原数据报的标识值相同，则在接收端具有相同标识值的分片就能最终正确的重装成为原来的数据报。

6、标志

     占3位，但目前只有两位有意义。

* 最低位记为MF。MF=1即表示后面”还有分片“的数据包。MF=0表示这已是若干数据包片中的最后一个。
* 中间位记为DF，意思是”不能分片“。只有当DF=0时才允许分片。

7、片偏移

     占13位。表示每个数据报的分片在原数据报中的相对位置。片偏移以8个字节为偏移单位，即每个分片的长度一定是8字节的整数倍。

8、生存时间

     占8位。表示数据报在网络中的寿命。最初以秒为TTL值为单位，现在以跳数为单位，则目前的最大数据为255.

9、协议

     占8位，指出此数据报携带的数据是使用何种协议，以便使目的主机的IP层知道应将数据部分上交给那个处理过程。

     TCP对应协议字段值6；UDP对应协议字段值17

10、首部校验和

     占16位，该字段只校验数据报的报头，但不包括数据部分。

11、源地址

     占32位

12、目的地址

     占32位  
12.MTU的概念，啥叫路径MTU？ MTU发现机制，TraceRoute(了解)。

1、MTU的概念

     MTU即Maximum Transmission Unit 最大传输单元。它是指一种通信协议的某一层上面所能通过的最大数据包大小（以字节为单位）。

**2、路径MTU**

     路径MTU是指一条因特网传输路径中，从源地址到目的地址所经过的“路径”上的所有IP跳的最大传输单元的最小值。或者从另外一个角度来看，就是无需进行分片处理就能穿过这条“路径”的最大传输单元的最大值。

**3、路径MTU的发现方法**

     这是确定两个IP主机之间路径最大传输单元的技术，其目的就是为了避免IP分片。首先源地址将数据报的DF位置位，在逐渐增大发送的数据报的大小——路径上任何需要将分组进行分片的设备都会将这种数据报丢弃并返回“数据报过大“的ICMP响应到源地址——这样源主机就”学习“到了无需分片就能通过这条路径的最大的最大传输单元。

**4、TraceRoute**

Traceroute是用来侦测主机到目的主机之间所经路由情况的重要工具。它的原理如下：它受到目的主机的IP后，首先给目的主机发送一个TTL=1的UDP数据包（每次送出的为3个40字节的包，包括源地址，目的地址和包发出的时间标签），而经过的第一个路由器收到这个数据包以后，就自动把TTL减1，而TTL变为0以后，路由器就把这个包给抛弃了，并同时产生 一个主机不可达的ICMP数据报给主机。主机收到这个数据报以后再发一个TTL=2的UDP数据报给目的主机，然后刺激第二个路由器给主机发ICMP数据报。如此往复直到到达目的主机。这样，traceroute就拿到了所有的路由器ip。

Traceroute提取发送 ICMP TTL到期消息设备的IP地址并作域名解析。每次 ，Traceroute都打印出一系列数据,包括所经过的路由设备的域名及 IP地址,三个包每次来回所花时间。

  
13.RIP协议的概念及算法。

1、RIP协议的概念

     路由信息协议RIP是一种分布式的基于距离向量的路由选择协议属于内部网关协议。RIP协议中的“距离”也称为“跳数”，因为每经过一个路由器，跳数就加1。协议规定同一自治系统(A.S.)中的路由器每 30秒会与相邻的路由器交换子讯息，以动态的建立路由表。当传输数据时，RIP将选择一条具有最少路由器的路由。

2、算法

     对每一个相邻路由器发送过来的RIP报文，进行以下步骤：  
（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”字段中的地址都改为X，并把所有的"距离"字段的值加1.每个项目都有三个关键数据，即：目的网络N，距离是d，下一跳路由器是X。  
（2）对修改后的RIP报文中的每一个项目，进行如下步骤：  
\* 若原来的路由表中没有目的网络N，则把该项目添加到路由表中，  
\* 若下一跳路由器地址是X，则把收到的项目替换原路由表中的项目  
\* 若收到的项目中距离d小于路由表中的距离，则进行更新  
（3）若3分钟还没有收到相邻路由器的更新路由表，则把此相邻路由器记为不可到达的路由器，即把距离设置为16。  
（4）返回  
14.ICMP协议的主要功能。

ICMP的全称是 Internet Control Message Protocol 。从技术角度来说，ICMP就是一个“错误侦测与回报机制”，其目的就是让我们能够检测网路的连线状况﹐也能确保连线的准确性﹐其功能主要有：

* 侦测远端主机是否存在
* 建立及维护路由资料
* 重导数据传送路径
* 数据流量控制

ICMP在沟通之中，主要是通过不同类型的报文让主机或路由器识别不同的链路传输情况。常用的ICMP报文类型如下

  
15.组播和广播的概念，IGMP的用途。(环回地址、广播地址)

**1、组播和广播的概念**

**组播**

主机之间的通讯模式，也就是加入了同一个组的主机可以接收到此组内的所有数据，网络中的交换机和路由器只向有需求者复制并转发其所需数据。主机可以向路由器请求加入或退出某个组，网络中的路由器和交换机有选择的复制并传输数据，即只将组内数据传输给那些加入组的主机。这样既能一次将数据传输给多个有需要（加入组）的主机，又能保证不影响其他不需要（未加入组）的主机的其他通讯

**广播**

是指在IP子网内广播数据包，所有在子网内部的主机都将收到这些数据包。广播意味着网络向子网每一个主机都投递一份数据包，不论这些主机是否乐于接收该数据包。所以广播的使用范围非常小，只在本地子网内有效，通过路由器和网络设备控制广播传输。

组播协议与现在广泛使用的单播协议的不同之处在于，一个主机用单播协议向n个主机发送相同的数据时，发送主机需要分别向n个主机发送，共发送n次。一个主机用组播协议向n个主机发送相同的数据时，只要发送1次，其数据由网络中的路由器和交换机逐级进行复制并发送给各个接收方，这样既节省服务器资源也节省网络主干的带宽资源。

**2、IGMP（Internet Group Management Protocol）的用途**

它用来在ip主机和与其直接相邻的组播路由器之间建立、维护组播组成员关系。组播路由器不需要保存所有主机的成员关系，它只是通过igmp协议了解每个接口连接的网段上是否存在某个组播组的组成员。而主机只需要保存自己加入了哪些组播组。

简而言之，IGMP协议是让连接在本地局域网上的组播路由器知道本局域网上是否有主机上的某个进程参加或退出了某个组播组。

**3、环回地址/广播地址**

环回地址：127.0.0.1，通常被称为本地回环地址(Loop back address)，不属于任何一个有类别地址类。它代表设备的本地虚拟接口，所以默认被看作是永远不会宕掉的接口。

主要作用有两个：一是测试本机的网络配置，能PING通127.0.0.1说明本机的网卡和IP协议安装都没有问题；另一个作用是某些SERVER/CLIENT的应用程序在运行时需调用服务器上的资源，一般要指定SERVER的IP地址，但当该程序要在同一台机器上运行而没有别的SERVER时就可以把SERVER的资源装在本机，SERVER的IP地址设为127.0.0.1同样也可以运行。

广播地址：是专门用于同时向网络中所有工作站进行发送的一个地址。在使用TCP/IP 协议的网络中，主机标识段host ID 为全1 的IP 地址为广播地址，广播的分组传送给host ID段所涉及的所有计算机。

例如，对于10.1.1.0 （255.255.255.0 ）网段，其广播地址为10.1.1.255 （255 即为2 进制的11111111 ），当发出一个目的地址为10.1.1.255 的分组（封包）时，它将被分发给该网段上的所有计算机。  
16.Ping协议的实现原理，ping 命令格式。

Ping（Packet InterNet Groper）分组网间探测是ICMP的一个重要应用，用来测试两个主机之间的连通性。Ping使用了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的一个例子。它没有通过运输层的TCP或UDP。  
     实现原理为向目的主机发送4个32字节长的ICMP回送请求报文，若目的主机正常工作并且响应了该ICMP回送请求报文，就将发回ICMP回送回答报文。最后可得出的统计结果为目的IP地址，发送的，收到的和丢失的分组数，及往返时间的最小值、最大值和平均值。  
     Ping命令格式为 ping hostname 此hostname即为妖测试连通性的主机名或它的IP地址。  
  
17. 子网划分的概念，子网掩码。

1、子网划分的概念

* 一个拥有许多物理网络的单位，可将所属的物理网络划分为若干个子网。划分子网纯属一个单位内部的事情。本单位以外的网络看不见这个网络是由多少子网组成，因为这个单位对外仍然表现一个网络。
* 划分子网的方法是从网络的主机号借用若干位作为子网号subnet-id。于是两级IP地址在本单位内部就变为三级IP地址：网络号，子网号和主机号。
* 凡是从其他网络发送给本单位某个主机的IP数据报，仍然是根据IP数据报的目的网络号找到连接在本单位网络上的路由器。但此路由器在收到IP数据报后，在按目的网络号和子网号找到目的子网，把IP数据报交付给目的主机

**2、子网掩码**

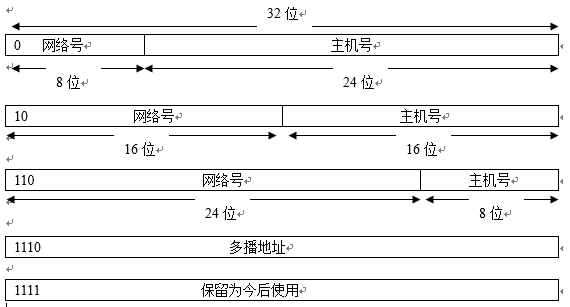
     子网掩码也是32位，由一串1和跟随的一串0组成。子网掩码中的1对应于IP地址中原来的网络号和子网号，而子网掩码中的0对应于现在的主机号。

     故将子网掩码和IP地址进行按位”与“运算（AND），就可得出网络地址。

     划分子网增加了 灵活性，但也减少了能够连接在网络上主机总数。  
18. IP地址的分类，如何划分的，及会计算各类地址支持的主机数。

1、IP地址的分类，划分

以下为A类地址，B类地址，C类地址，D类地址，E类地址



2、IP地址的指派范围

  
19.DNS的概念，用途，DNS查询的实现算法。

1、DNS的概念，用途

     DNS是由解析器以及域名服务器组成的。域名服务器是指保存有该网络中所有主机的域名和对应IP地址，并具有将域名转换为IP地址功能的服务器。DNS使用TCP与UDP端口号都是53，主要使用UDP，服务器之间备份使用TCP。

     域名到IP地址的解析过程的要点如下：当某一个应用进程需要主机名解析为IP地址时，该应用进程就调用解析程序，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域名服务器。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中的另一个客户，并向其他域名服务器发出查询请求。这种过程直至找到能够回答该请求的域名服务器为止。

**2、DNS查询算法**

* 主机向本地域名服务器的查询一般都是采用递归查询，即如果主机所询问的本地域名服务器不知道被查询域名的IP地址，那么本地域名服务器就以DNS客户的身份，向其他根域名服务器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。因此，递归查询返回的查询结果或是所要查询的IP地址，或是报错。
* 本地域名服务器想根服务器的查询通常采用迭代查询，即**当根域名服务器**收到**本地域名服务器**收到本地域名服务器发出的迭代查询请求报文时，要么给出所要查询的IP地址，要么告诉本地域名服务器“下一次应向那个域名服务器进行查询”。然后让本地域名服务器进行后续的查询。**根域名服务器**通常把自己知道的顶级域名服务器的IP地址告诉本地域名服务器，让本地域名服务器再向**顶级域名服务器**查询。顶级域名服务器在收到本地域名服务器的查询请求后，要么给出所要查询的IP地址，要么告诉本地域名服务器下一步应当向哪一个**权限域名服务器**进行查询。本地域名服务器就这样进行迭代查询。

20. TCP与UDP的概念，相互的区别及优劣。

1、TCP（Transmission Control Protocol）的概念

     TCP是一种面向连接的，提供可靠交付服务和全双工通信的，基于字节流的端到端的传输层通信协议。

* TCP在传输数据之前必须先建立连接，数据传输结束后要释放连接。
* 每一条TCP连接只能有2个端点，故TCP不提供广播或多播服务。
* TCP提供可靠交付，通过TCP连接传输的数据，无差错、不丢失、不重复、并且按序到达。
* TCP是面向字节流的。虽然应用进程和TCP的交互是一次一个数据块(大小不等），但TCP把英语程序交下来的数据看成仅仅是一连串的无结构的字节流。TCP并不知道所传输的字节流的含义。

**2、UDP（User Datagram Protocol）的概念**

     UDP是一种无连接的，尽最大努力交付的，基于报文的端到端的传输层通信协议。

* UDP，在发送数据之前不需要建立连接
* UDP不保证可靠交付，主机不需要位置复杂的连接状态
* 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的边界，即应用层交给UDP多长的报文，UDP就照样发送，即一次发送一个报文。在接收端，UDP一次交付一个完整的报文。
* UDP没有拥塞控制，网络出现的拥塞不会使源主机的发送速率降低。
* UDP支持一对一、一对多、多对一和多对多的交互通信。
* 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。

**3、区别**

* TCP协议面向连接，UDP协议面向非连接
* TCP协议传输速度慢，UDP协议传输速度快
* TCP协议保证数据顺序，UDP协议不保证
* TCP协议保证数据正确性，UDP协议可能丢包
* TCP协议对系统资源要求多，UDP协议要求少

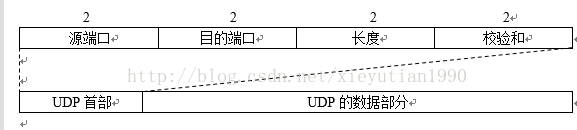
**4、使用情况**

TCP协议适用于对效率要求相对低，但对准确性要求相对高的场景下，或者是有一种连接概念的场景下；而UDP协议适用于对效率要求相对高，对准确性要求相对低的场景。  
21.UDP报文的格式，字段的意义。

1、UDP有两个字段：数据字段和首部字段。

* 首部字段

首部字段很简单，只有8个字节，由4个字段组成，每个字段的长度都是两个字节。



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要使用到。

3）长度： UDP用户数据报的长度，其最小值是8（仅有首部）。

4）校验和：检测UDP用户数据报在传输中是否有错。有错就丢弃。

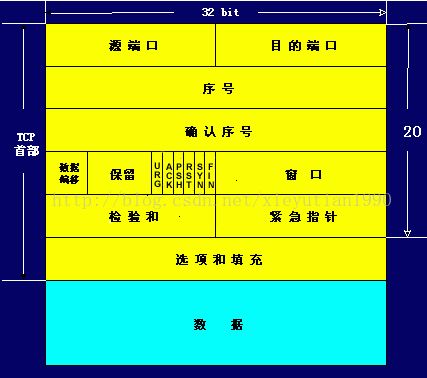
2、要注意的地方

* UDP首部中校验和的计算方法有些特殊。在计算校验和时，要在UDP用户数据报之前增加12个字节的伪首部。伪首部既不向下传送也不向上递交，而仅仅是为了计算校验和。与IP数据报的校验和只校验IP数据报的首部不同，UDP的校验和是把首部和数据部分一起都校验。

伪首部：

http://img.blog.csdn.net/20140503103753906?watermark/2/text/aHR0cDovL2Jsb2cuY3Nkbi5uZXQveGlleXV0aWFuMTk5MA==/font/5a6L5L2T/fontsize/400/fill/I0JBQkFCMA==/dissolve/70/gravity/Center  
22. TCP 报文的格式，字段的意义。

TCP报文段分为首部和数据两部分。



     TCP报文段首部的前20个字节是固定的，后面有4N字节是根据需要而增加的选项（N是整数）。因此TCP首部的最小长度是20字节。

首部固定部分各字段的意义如下：

* **源端口和目的端口：**各占2个字节，分别写入源端口号和目的端口号。
* **序号：**占4个字节。序号使用mod运算。TCP是面向字节流的，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。故该字段也叫做“报文段序号”。
* **确认序号：**占4个字节，是期望收到对方下一个报文段的第一个数据字节的序号。若确认序号=N,则表明：到序号N-1为止的所有数据都已正确收到。
* **数据偏移：**占4位，表示TCP报文段的首部长度。注意，“数据偏移”的单位是32位字（即以4字节长的字为计算单位）。故TCP首部的最大长度为60字节。
* **保留：**占6位，保留为今后使用，目前置为0；
* **紧急URG：**当URG=1，表明紧急指针字段有效。这时发送方TCP就把紧急数据插入到本报文段数据的最前面，而在紧急数据后面的数据仍是普通数据。
* **确认ACK：**当ACK=1时，确认字段才有效。当ACK=0时，确认号无效。TCP规定，在连接建立后所有传送的报文段都必须把ACK置1。
* **推送PSH：**接收方TCP收到PSH=1的报文段，就尽快地交付给接收应用进程，而不再等到整个缓存都填满了后再向上交付。
* **复位RST：**当RST=1时，表明TCP连接中出现严重差错，必须释放连接，然后再重新建立运输连接。
* **同步SYN：**在连接建立时用来同步序号。当SYN=1而ACK=0时，表明这是一个连接请求报文段。对方若同意建立连接，则应在响应的报文段中使SYN=1和ACK=1。故SYN置为1，就表示这是一个连接请求和连接接收报文。
* **终止FIN：**用来释放连接。当FIN=1时，表明此报文段的发送方的数据已发送完毕，并要求释放运输连接。
* **窗口：**占2个字节。窗口值作为接收方让发送方设置其发送窗口的依据。
* **检验和：**占2字节。检验和字段检验的范围包括首部和数据这两部分。和UDP数据报一样，在计算检验和时，也要在TCP报文段的前面加上12字节的伪首部。伪首部的格式与UDP用户数据报的伪首部一样，但要将伪首部第四个字段中的17 改为6（协议号），把第5字段中的UDP长度改为TCP长度。

**紧急指针：**占2字节。紧急指针仅在URG=1时才有意义，它指出本报文段中的紧急数据的字节数。  
23.TCP通过哪些措施，保证传输可靠？

24. 三次握手，四次断开过程。

在TCP连接建立过程中要解决以下3个问题：

（1）要使每一方能够确知对方的存在

（2）要允许双方协商一些参数（如最大窗口值，是否使用窗口扩大选项和时间戳选项以及服务质量）

（3）能够对运输实体资源（如缓存大小、连接表中的项目等）进行分配

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是客户，而被动等待连接建立的应用进程是服务器。

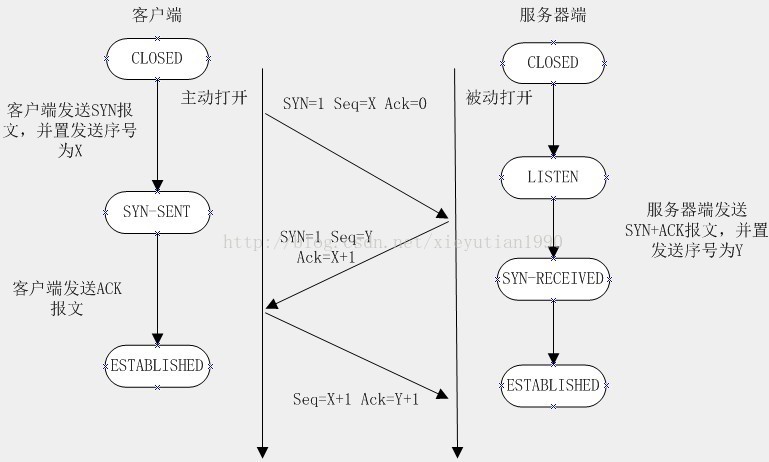
* **三次握手**

     1)第一次握手：客户端创建传输控制块TCB，向服务器端发送连接请求报文段。该报文段的同步位SYN=1，同时选择一个初始序号Seq=x。此时TCP客户端进入SYN-SENT(同步已发送)状态。

     2)第二次握手：服务器端收到连接请求报文段后，如同意连接，则向客户端发送确认报文段。该报文段的SYN和ACK都置1，确认号为ack=x+1，同时选择一个初始序号Seq=y。此时TCP服务器端进入SYN-RCVD(同步收到)状态。

     3)第三次握手：TCP客户端收到服务器端的的确认后，还要向服务器端给出确认报文段。该报文段的ACK置1，确认号ack=y+1，而序号为Seq=x+1。此时TCP连接已经建立，A进入ESTABLISHED（已建立连接)状态。当服务器端收到客户端的确认后，也进入ESTABLISHED（已建立连接)状态。

     第三次握手的作用：防止已失效的连接请求报文段突然有传送到了服务器。



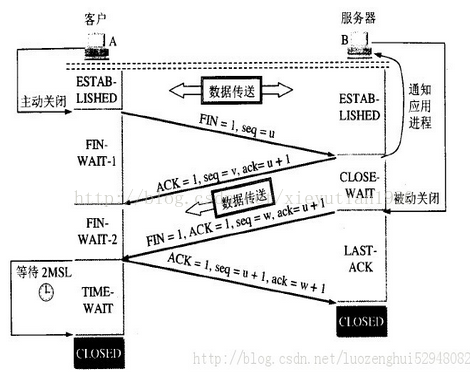
* **四次断开**

     1)一次断开：客户端向服务器端发送连接释放报文段，并停止再发送数据，主动关闭TCP连接。该报文段的首部的FIN置1，序号为seq=u（前面已传输过的数据的最后一个字节的序号加1）。此时客户端进入FIN-WAIT-1(终止等待1)状态，等待服务器端的确认。

     2)二次断开：服务器端收到连接释放报文段后，就发出确认报文段，确认号是ack=u+1，序号是v（前面已传输过的数据的最后一个字节的序号加1）。然后服务器就进入CLOSE-WAIT（关闭等待）状态。此时从客户端到服务器这个方向的连接就释放了，此时TCP连接处于半关闭状态，因为服务器若发送数据，客户端仍要接收。

     3)三次断开：客户端收到来自服务器端的确认后，就进入FIN-WAIT-2（终止等待2）状态，等待服务器发出的连接释放报文段。若服务器已经没有要发送的数据，其应用进程就通知TCP释放连接，并且发送连接释放报文段，该报文段的首部的FIN置1。此时服务器就进入了LAST-ACK（最后确认）状态，等待客户端的确认，收到客户端的确认后，服务器就进入CLOSED状态。

     4)四次断开：客户端收到服务器的连接释放报文段后，就发出确认报文段。然后进入TIME-WAIT(时间等待）状态。此时TCP连接还未完全释放，必须经过时间等到计时器设置的时间2MSL后，客户端才进入CLOSED状态。

  
25. TIME\_WAIT状态的概念及意义。

客户端与服务器端建立TCP/IP连接后关闭SOCKET后，服务器端连接的端口  
状态为TIME\_WAIT  
是不是所有执行主动关闭的socket都会进入TIME\_WAIT状态呢？  
有没有什么情况使主动关闭的socket直接进入CLOSED状态呢？  
主动关闭的一方在发送最后一个ack 后  
就会进入TIME\_WAIT 状态 停留2MSL（max segment lifetime）时间  
这个是TCP/IP必不可少的，也就是“解决”不了的。  
也就是TCP/IP设计者本来是这么设计的  
主要有两个原因  
1。防止上一次连接中的包，迷路后重新出现，影响新连接  
  （经过2MSL，上一次连接中所有的重复包都会消失）  
2。可靠的关闭TCP连接  
  在主动关闭方发送的最后一个ack(fin) ，有可能丢失，这时被动方会重新发  
  fin, 如果这时主动方处于CLOSED 状态 ，就会响应rst 而不是ack。所以  
  主动方要处于TIME\_WAIT 状态，而不能是CLOSED 。  
TIME\_WAIT 并不会占用很大资源的，除非受到攻击。  
还有，如果一方send 或recv 超时，就会直接进入CLOSED 状态  
26.滑动窗口协议 与停止等待协议的区别。

滑动窗口协议中，允许发送方发送多个分组（当有多个分组可用时）而不需等待确认，但它受限于在流水线 中为未确认的分组数不能超过某个最大允许数N。滑动窗口协议是TCP使用的一种流量控制方法，此协议能够加速数据的传输。 只有在接收窗口向前滑动时（与此同时也发送了确认），发送窗口才有可能向前滑动。

收发两端的窗口按照以上规律不断地向前滑动，因此这种协议称为滑动窗口协议。

当发送窗口和接收窗口的大小都等于1时，就是停止等待协议。  
27. TCP的流量控制和拥塞控制实现原理(会画拥塞控制的典型图)。  
28.TCP的快速重传与快速恢复算法。  
29.TFTP 与 FTP的区别。

FTP（File Transfer Protocol，文件传输协议）协议在TCP/IP协议族中属于应用层协议，用于在远端服务器和本地客户端之间传输文件，使用TCP端口20和21进行传输。端口20用于传输数据，端口21用于传输控制消息。  
TFTP（Trivial File Transfer Protocol，简单文件传输协议）也是用于在远端服务器和本地主机之间传输文件的，相对于FTP，TFTP没有复杂的交互存取接口和认证控制，适用于客户端和服务器之间不需要复杂交互的环境。TFTP协议的运行基于UDP协议，使用UDP端口69进行数据传输。  
基于的传输协议不一样：FTP是基于TCP TFTP是基于UDP   
端口号不一样：FTP是用21.20 TFTP是69  
速度和安全方面：FTP在速度方面没有TFTP快但是FTP安全好  
30.阻塞方式和非阻塞方式，阻塞connect与非阻塞connect。(比较难，有兴趣可以了解)  
31. HTTP基本格式。（java程序员必须掌握）