1,什么是计算机网络及主要功能有哪些?

计算机网络是把分布在不同地理区域的计算机与专门的外部设备用通信线路互连成一个规模大、功能强的网络系统,从而使众多计算机可以方便地互相传递信息,共享硬件、软件、数据信息等资源.

计算机网络的功能有资源共享(硬件、软件和数据共享)、数据通信能力(数据传输)、均衡负荷互相协作、实现分布式处理和提高计算机的可靠性。其中最重要的是资源共享和数据传输。

2, 什么是计算机网络的组成、拓扑结构、协议体系结构

[计算机网络](https://www.baidu.com/s?wd=%E8%AE%A1%E7%AE%97%E6%9C%BA%E7%BD%91%E7%BB%9C&tn=44039180_cpr&fenlei=mv6quAkxTZn0IZRqIHckPjm4nH00T1d9ujw9mWDdPAD1n1RLPAPb0ZwV5Hcvrjm3rH6sPfKWUMw85HfYnjn4nH6sgvPsT6KdThsqpZwYTjCEQLGCpyw9Uz4Bmy-bIi4WUvYETgN-TLwGUv3En101PWfvrjcs)是由：服务器、工作站、通信设备、传输介质组成。

[计算机网络](https://www.baidu.com/s?wd=%E8%AE%A1%E7%AE%97%E6%9C%BA%E7%BD%91%E7%BB%9C&tn=44039180_cpr&fenlei=mv6quAkxTZn0IZRqIHckPjm4nH00T1dBm1RduW6vmyD1PjRLnHmL0ZwV5Hcvrjm3rH6sPfKWUMw85HfYnjn4nH6sgvPsT6KdThsqpZwYTjCEQLGCpyw9Uz4Bmy-bIi4WUvYETgN-TLwGUv3En16zPW0vP16)拓扑结构是指网络中各个站点相互连接的形式，在局域网中明确一点讲就是文件服务器、工作站和电缆等的连接形式。现在最主要的拓扑结构有总线型拓扑、星形拓扑、环形拓扑、树形拓扑（由总线型演变而来）以及它们的混合型。

常见的网络拓扑结构有：

1、总线型拓扑。总线型拓扑是一种基于多点连接的拓扑结构,是将网络中的所有的设备通过相应的硬件接口直接连接在共同的传输介质上。

2、环型拓扑。

3、树形拓扑结构。树形拓扑从总线拓扑演变而来，形状像一棵倒置的树，顶端是树根，树根以下带分支，每个分支还可再带子分支。

4、星形拓扑结构。星形拓扑结构是一种以中央节点为中心，把若干外围节点连接起来的辐射式互联结构，各结点与中央结点通过点与点方式连接，中央结点执行集中式通信控制策略，因此中央结点相当复杂，负担也重。

5、网状拓扑。网状拓扑又称作无规则结构，结点之间的联结是任意的，没有规律。

计算机网络体系结构是网络协议的层次划分与各层协议的集合，同一层中的协议根据该层所要实现的功能来确定。各对等层之间的协议功能由相应的底层提供服务完成。

OSI是由国际标准化组织制定的标准，它概念清楚，理论完善，但是复杂又不实用。OSI的体系结构

7 应用层6 表示层5 会话层4 运输层3 网络层2 数据链路层1物理层

TCP/IP体系结构得到了非常广泛的应用。

TCP/IP体系结构4 应用层(各种应用层协议如FTP,DNS等)3运输层(TCP或UDP)

2 网际层(又名网络互联层)1 数据链路层(又名网络接口层)

学习网络原理时的体系结构，结合OSI和TCP/IP的优点。

5应用层4 运输层3 网络层2数据链路层1物理层

3,什么是ISO/OSI基本参考模型

第7层 应用层：OSI中的最高层。为特定类型的网络应用提供了访问OSI环境的手段。应用层确定进程之间通信的性质，以满足用户的需要。应用层不仅要提供应用进程所需要的[信息交换](https://www.baidu.com/s?wd=%E4%BF%A1%E6%81%AF%E4%BA%A4%E6%8D%A2&tn=44039180_cpr&fenlei=mv6quAkxTZn0IZRqIHckPjm4nH00T1dBuyNbmWmsnADdrHfdujm40ZwV5Hcvrjm3rH6sPfKWUMw85HfYnjn4nH6sgvPsT6KdThsqpZwYTjCEQLGCpyw9Uz4Bmy-bIi4WUvYETgN-TLwGUv3EnWfkrHmzPjfk" \t "_blank)和远程操作，而且还要作为应用进程的[用户代理](https://www.baidu.com/s?wd=%E7%94%A8%E6%88%B7%E4%BB%A3%E7%90%86&tn=44039180_cpr&fenlei=mv6quAkxTZn0IZRqIHckPjm4nH00T1dBuyNbmWmsnADdrHfdujm40ZwV5Hcvrjm3rH6sPfKWUMw85HfYnjn4nH6sgvPsT6KdThsqpZwYTjCEQLGCpyw9Uz4Bmy-bIi4WUvYETgN-TLwGUv3EnWfkrHmzPjfk)，来完成一些为进行[信息交换](https://www.baidu.com/s?wd=%E4%BF%A1%E6%81%AF%E4%BA%A4%E6%8D%A2&tn=44039180_cpr&fenlei=mv6quAkxTZn0IZRqIHckPjm4nH00T1dBuyNbmWmsnADdrHfdujm40ZwV5Hcvrjm3rH6sPfKWUMw85HfYnjn4nH6sgvPsT6KdThsqpZwYTjCEQLGCpyw9Uz4Bmy-bIi4WUvYETgN-TLwGUv3EnWfkrHmzPjfk)所必需的功能。它包括：文件传送访问和管理FTAM、[虚拟终端](https://www.baidu.com/s?wd=%E8%99%9A%E6%8B%9F%E7%BB%88%E7%AB%AF&tn=44039180_cpr&fenlei=mv6quAkxTZn0IZRqIHckPjm4nH00T1dBuyNbmWmsnADdrHfdujm40ZwV5Hcvrjm3rH6sPfKWUMw85HfYnjn4nH6sgvPsT6KdThsqpZwYTjCEQLGCpyw9Uz4Bmy-bIi4WUvYETgN-TLwGUv3EnWfkrHmzPjfk" \t "_blank)VT、事务处理TP、远程数据库访问RDA、制造业报文规范MMS、目录服务DS等协议；第6层 表示层：主要用于处理两个通信系统中交换信息的表示方式。为上层用户解决用户信息的语法问题。它包括数据格式交换、数据加密与解密、数据压缩与恢复等功能； 　　第5层 会话层：—在两个节点之间建立端连接。为端系统的应用程序之间提供了对话控制机制。此服务包括建立连接是以全双工还是以半双工的方式进行设置，尽管可以在层4中处理双工方式 ； 　　第4层 传输层：—常规数据递送－面向连接或无连接。为会话层用户提供一个端到端的可靠、透明和优化的数据传输服务机制。包括全双工或半双工、流控制和错误恢复服务； 　　第3层 网络层：—本层通过寻址来建立两个节点之间的连接，为源端的运输层送来的分组，选择合适的路由和交换节点，正确无误地按照地址传送给目的端的运输层。它包括通过互连网络来路由和中继数据 ； 　　第2层 数据链路层：—在此层将数据分帧，并处理流控制。屏蔽物理层，为网络层提供一个数据链路的连接，在一条有可能出差错的物理连接上，进行几乎无差错的数据传输。本层指定拓扑结构并提供硬件寻址； 　　第1层 物理层：处于OSI参考模型的最底层。物理层的主要功能是利用物理传输介质为数据链路层提供物理连接，以便透明的传送比特流。

什么是TCP/IP协议族？

TCP/IP也称"国际协议簇"， 即不仅指 TCP/IP协议本身，而且包括与其有关的协议。 TCP为传输控制协议，IP为网际协议，是网络层最重要的协议。采用TCP/IP协议通过互联网传送信息可减少网络中的传输阻塞，方便大批量的数据在网上传输，从而提高网络的传输效率。 TCP/IP协议族中包括上百个互为关联的协议，其中有：Telnet（Remote Login）： 提供远程登录功能； FTP （FileTransfer Protocol)：远程文件传输协议，允许用户将远程主机上的文件拷贝到自己的计算机上； SMTP （Simple Messagetransfer Protocol)：简单信息传输协议，主要用于传输电子邮件；NFS(Network File Server)：网络文件服务器，可使多台计算机透明地访问彼此的目录 ；UDP （ User DatagramProtocol)：用户数据包协议。

什么是IPv6

IPv6是Internet Protocol Version 6的缩写，其中Internet Protocol译为“互联网协议”。IPv6是IETF（互联网工程任务组，Internet Engineering Task Force）设计的用于替代现行版本IP协议（IPv4）的下一代IP协议，号称可以为全世界的每一粒沙子编上一个网址 。

由于IPv4最大的问题在于网络地址资源有限，严重制约了互联网的应用和发展。IPv6的使用，不仅能解决网络地址资源数量的问题，而且也解决了多种接入设备连入互联网的障碍.

什么是IEEE802：

IEEE 802又称为LMSC（LAN /MAN Standards Committee， 局域网/城域网标准委员会），致力于研究局域网和城域网的物理层和MAC层中定义的服务和协议，对应OSI网络参考模型的最低两层（即物理层和数据链路层）。

网络层次结构概念？ 见协议体系结构

什么是网络协议？协议和接口的关系？

网络协议为计算机网络中进行数据交换而建立的规则、标准或约定的集合。

网络协议是由三个要素组成：

(1) 语义。语义是解释控制信息每个部分的意义。它规定了需要发出何种控制信息，以及完成的动作与做出什么样的响应。

(2) 语法。语法是用户数据与控制信息的结构与格式，以及数据出现的顺序。

(3) 时序。时序是对事件发生顺序的详细说明。（也可称为“同步”）

人们形象地把这三个要素描述为：语义表示要做什么，语法表示要怎么做，时序表示做的顺序。

协议与接口的关系？

接口是统一结点内相邻两层间交换信息的连接点，是一个系统内部的规定。每一层只能为紧邻的层次之间定义接口，不能跨层定义接口。在典型的接口上， 同一结点相邻两层的实体通过服务访问点（Service Access Point，SAP）进行交互。服务是通过服务访问点SAP提供给上层使用的，第n层的SAP就是第n+1层可以访问第n层服务的地方。每个SAP都有一个能够标识它的地址。服务访问点SAP是一个抽象的概念，它实际上就是一个逻辑接口（类似于邮政信箱），但和通常所说的两个设备之间的硬件接口是很不一样的。

接口是信息调用的出口 ，服务是建立在 协议的基础上。

各层封装的基本数据单元是？

数据单元（data unit）指许多信息单元。常用的数据单元有服务数据单元（SDU）、协议数据单元（PDU）。

物理层：比特流

数据链路层的PDU叫做Frame（帧）；

网络层的PDU叫做Packet（数据包）；

传输层：段；

TCP的叫做Segment（数据段）；

UDP的叫做Datagram。（数据报）

什么是服务原语，有哪些类型？

服务原语包含四种类型：

请求（request）:一个实体希望得到完成某些操作的服务

指示(indication):通知一个实体，有某个事件发生

响应（response）:一个实体希望响应一个事件

证实（confirm）:返回对先前请求的响应

扩展：在网络体系结构中，什么是接口，服务和服务原语？服务原语有哪几类？

答：接口：在网络的层次结构中，每相邻层间有一接口，该接口定义下层向上层提供的原语操作和服务；服务：是指各层间交换信息时必须遵守的规则；

服务原语：服务在形式上是由一组接口原语(或操作)来描述的，服务原语可分为四类：请求(Request)，指示(Indicate)，响应(Response)，确认(Confirm)。

分组交换的特点是？

在分组交换网络中，采用存储转发方式工作，数据以短的分组形式传送。如果一个源站有一个长的报文要发送，该报文就会被分割成一系列的分组。每个分组包含用户数据的一部分加上一些控制信息。控制信息至少要包括网络为了把分组送到目的地做路由选择所需要的信息。在路径上的每个结点，分组被接收，短时间存储，然后传递给下一结点。

分组交换网的主要优点：① 高效。② 灵活。③ 迅速。④ 可靠。

缺点：分组在节点转发时因排队而造成一定的延时;分组必须携带一些控制信息而产生额外开销;

分组交换仍采用报文交换的”存储－转发”技术．在分组交换网中，有两种常采用的处理整个报文的方法：数据报方式和虚电路方式．

计算机网络性能指标？

性能指标从不同的方面来度量[计算机网络](https://www.baidu.com/s?wd=%E8%AE%A1%E7%AE%97%E6%9C%BA%E7%BD%91%E7%BB%9C&tn=44039180_cpr&fenlei=mv6quAkxTZn0IZRqIHckPjm4nH00T1Y3uhcknWcznjTvuyFWPhR30ZwV5Hcvrjm3rH6sPfKWUMw85HfYnjn4nH6sgvPsT6KdThsqpZwYTjCEQLGCpyw9Uz4Bmy-bIi4WUvYETgN-TLwGUv3EPjbknWbknjcLPHfdnWD4njRz)的性能。下面总结下常用的七个性能指标。

1、速率

　　计算机发送出的信号都是数字形式的。比特(bit)是计算机中的数据量的单位，也是信息论中使用的信息量单位。网络技术中的速率指的是链接在计算机网络上的主机在数字信道上传送数据的速率，也称为数据率(data rate)或者比特率(bit rate)。速率的单位是b/s(比特每秒)或者bit/s，也可以写为bps，即bit per second。现在一般常用更简单并不是很严格的记法来描述网络的速率，如100M以太网，而省略了b/s，意思为数据率为100Mb/s的以太网。这里的数据率通常指额定速率。

　　2、带宽

　　带宽本上包含两种含义：

　　(1)带宽本来指某个信号具有的频带宽度。信号的带宽是指该信号所包含的各种不同频率成分所占据的频率范围。因此，表示通信线路允许通过的信号频带范围即为线路的带宽。

　　(2)在计算机网络中，带宽用来表示网络的通信线路所能传送数据的能力，因此网络带宽表示在单位时间内从网络的某一点到另一点所能通过的“最高数据量“。这种意义的带宽的单位是”比特每秒“，即为b/s。子这种单位的前面也通常加上千(k)、兆(M)、吉(G)、太(T)这样的倍数。

　　3、吞吐量

　　吞吐量(throughput)表示在单位时间内通过某个网络(或信道、接口)的数据量。吞吐量进场用于对现实世界中的网络的一种测量，以便知道实际上到底有多少数据量能够通过网络。显然，吞吐量受到网络的带宽或网络的额定速率的限制。例如，对于一个100Mb/s的以太网，其额定速率为100Mb/s，那么这个数值也是该以太网的吞吐量的绝对上限值。因此，对100Mb/s的以太网，其典型的吞吐量可能只有70Mb/s。

　　4、时延

　　时延指数据(一个报文或者分组)从网络(或链路)的一端传送到另一端所需的时间。时延是一个非常重要的性能指标，也可以称为延迟或者迟延。

　　网络中的时延由以下几部分组成：

　　(1)发送时延 发送时延是主机或路由器发送数据帧所需要的时间，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时间。发送时延也可以称为传输时延。发送的时延=数据帧长度(b)/发送速率(b/s)。

　　对于一定的网络，发送时延并非固定不变，而是与发送的帧长成正比，与发送数率成反比。

　　(2)传播时延 传播时延是电磁波在信道中传播一定的距离需要花费的时间。

　　传播时延=信道长度(m)/电磁波在信道上的传播数率(m/s)

　　电磁波在自由空间的传播速率是光速，即3.0×10^5 km/s。电磁波在网络传输媒体中的传播速率比在自由空间低一些，在铜线电缆中的传播速率约为2.3×10^5 km/s，在光纤中的传播速率约为2.0×10^5 km/s。

　　(3)处理时延 主机或路由器在收到分组时需要花费一定的时间处理，分析分组首部、从分组中提取数据部分、进行差错检验、查到适当路由等，这就产生了处理时延。

　　(4)排队时延 分组在经过网络传输时，要经过许多的路由器。但分组在进入路由器后要先在输入队列中排队等待处理。在路由器确定了转发接口后，还要在输出队列中排队等待转发。这就产生了排队延时。排队延时通常取决于网络当时的通信量。

　　这样数据在网络中尽力的总延时就是

　　总延时 = 发送延时 + 传播延时 + 处理延时 + 排队延时

　　对于高速网络链路，提高的仅仅是数据的发送数率而不是比特在链路上的传播速率。荷载信息的电磁波在通信线路上的传播速率与数据的发送速率并无关系。提高的数据的发送速率只是减小了数据的发送时延。

　　5、时延带宽积

　　时延带宽积 = 传播时延 × 带宽

　　例如，传播时延为20ms，带宽为10Mb/s，则时延带宽积 = 20 × 10 × 10^3 /1000 = 2 × 10^5 bit。这就表示，若发送端连续发送数据，则在发送的第一个比特即将达到终点时，发送端就已经发送了20万个比特，而这20万个bit都在链路上向前移动。

　　6、往返时间RTT

　　在计算机网络中，往返时间RTT也是一个重要的性能指标，表示从发送方发送数据开始，到发送方收到来自接收方的确认，总共经历的时间。对于上面提到的例子，往返时间RTT就是40ms，而往返时间和带宽的乘积是4×10^5(bit)。

　　显然，往返时间与所发送的分组长度有关。发送很长的数据块的往返时间，应当比发送很短的数据块往返时间要多些。

　　往返时间带宽积的意义就是当发送方连续发送数据时，即能够及时收到对方的确认，但已经将许多比特发送到链路上了。

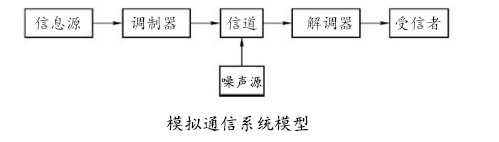
　　7、利用率

　　利用率有信道利用率和网络利用率。信道利用率指出某信道有百分之几的时间是被利用的。网络利用率则是全网络的信道利用率的加权平均值。信道利用率并非越高越好

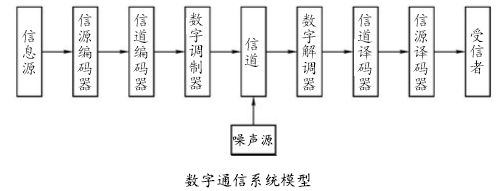
**物理层：**

什么是模拟信号，什么是数字信号？

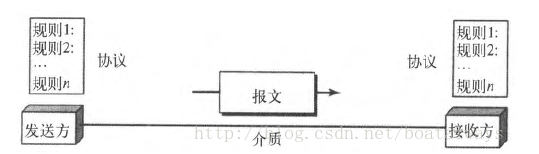
模拟信号指幅度的取值是连续的（幅值可由无限个数值表示）。时间上连续的模拟信号连续变化的图像（电视、传真）信号等，时间上离散的模拟信号是一种抽样信号。



数字信号指幅度的取值是离散的，幅值表示被限制在有限个数值之内。二进制码就是一种数字信号。二进制码受噪声的影响小，易于有数字电路进行处理，所以得到了广泛的应用。



画出数据通信系统的基本组成？



报文(message) 是进行通信的信息(数据) ，它可以是文本、数字、图片、声音、视频等信息形式。

发送方(sender) 是指发送数据报文的设备，它可以是计算机、工作站、手机、摄像机等。

接收方(receiver) 是指接收报文的设备，它可以是计算机、工作站、手机、电视等。

传输介质(transmission medium) 是报文从发送方到接收方之间所经过的物理通路，它可以是双绞线、同轴电缆、光纤和无线电波。

协议(protocol) 是管理数据通信的一组规则，它表示通信设备之间的一组约定。如果没有协议，即使两台设备之间可能是连接的，那也无怯通信，就像一个说陆语的人无陆被一个只说日语的人理解一样。再正式一点的说法是，两者通信的时候交换的报文的格式和次序，以及在接收或者发送报文，或者其他事情时候，采取的动作。

基本的数据编码？

为了便于使用，容易记忆，常常要对计算机加工处理的对象进行编码，用一个编码符合代表一条信息或一串数据，这就是数据编码。几种常用的编码方案有：单极性码、极性码、双极性码、归零码、双相码、不归零码、曼彻斯特编码、差分曼彻斯特编码、多电平编码、4B/5B编码等。

数据传输控制方式有哪几种？

有四种：程序I／O控制方式,中断控制方式,DMA控制方式,通道控制方式。

基带传输与频带传输的定义？

基带传输又叫数字传输，是指把要传输的数据转换为数字信号，使用固定的频率在信道上传输。例如计算机网络中的信号就是基带传输的。

和基带相对的是频带传输，又叫模拟传输，是指信号在电话线等这样的普通线路上，以正弦波形式传播的方式。我们现有的电话、模拟电视信号等，都是属于频带传输。

什么是同步传输和异步传输？

异步传输（Asynchronous Transmission）： 异步传输将比特分成小组进行传送，小组可以是8位的1个字符或更长。发送方可以在任何时刻发送这些比特组，而接收方从不知道它们会在什么时候到达。一个常见的例子是计算机键盘与主机的通信。按下一个字母键、数字键或特殊字符键，就发送一个8比特位的ASCII代码。键盘可以在任何时刻发送代码，这取决于用户的输入速度，内部的硬件必须能够在任何时刻接收一个键入的字符。

同步传输（Synchronous Transmission）：同步传输的比特分组要大得多。它不是独立地发送每个字符，每个字符都有自己的开始位和停止位，而是把它们组合起来一起发送。我们将这些组合称为数据帧，或简称为帧。

同步与异步传输的区别

1,异步传输是面向字符的传输，而同步传输是面向比特的传输。

2,异步传输的单位是字符而同步传输的单位是桢。

3,异步传输通过字符起止的开始和停止码抓住再同步的机会，而同步传输则是以数据中抽取同步信息。

4,异步传输对时序的要求较低，同步传输往往通过特定的时钟线路协调时序。

5,异步传输相对于同步传输效率较低。

多路复用概念及常用技术？

多路复用技术是把多个低速信道组合成一个高速信道的技术，它可以有效的提高数据链路的利用率，从而使得一条高速的主干链路同时为多条低速的接入链路提供服务，也就是使得网络干线可以同时运载大量的语音和数据传输。多路复用技术是为了充分利用传输媒体，人们研究了在一条物理线路上建立多个通信信道的技术。多路复用技术的实质是，将一个区域的多个用户数据通过发送多路复用器进行汇集，然后将汇集后的数据通过一个物理线路进行传送，接收多路复用器再对数据进行分离，分发到多个用户。多路复用通常分为频分多路复用、时分多路复用、波分多路复用、码分多址和空分多址。

**数据链路层：**

**数据链路层提供的基本功能有哪些？**

**答：保证数据的正常传送，帧的控制(定界与同步)，差错控制(最主要的功能)，包括查错、纠错、出错重传，流量控制，顺序控制(保证重传可行)。**

1,什么是CSMA/CD、Token-Ring、CSMA/CA?

CSMA/CD和CSMA/CA的主要差别

　CSMA/CD：带有冲突检测的载波监听多路访问，可以检测冲突，但无法“避免”.CSMA/CA：带有冲突避免的载波侦听多路访问，发送包的同时不能检测到信道上有无冲突，只能尽量“避免”；

1.两者的传输介质不同,CSMA/CD用于总线式以太网,而CSMA/CA则用于无线局域网802.11a/b/g/n等等；

2.检测方式不同,CSMA/CD通过电缆中电压的变化来检测，当数据发生碰撞时，电缆中的电压就会随着发生变化；而CSMA/CA采用能量检测(ED)、载波检测(CS)和能量载波混合检测三种检测信道空闲的方式；

3.WLAN中，对某个节点来说，其刚刚发出的信号强度要远高于来自其他节点的信号强度，也就是说它自己的信号会把其他的信号给覆盖掉；

4.本节点处有冲突并不意味着在接收节点处就有冲突。

综上，在WLAN中实现CSMA/CD是比较困难的。

CSMA/CD的工作流程是：（1）侦听；（2）发送；（3）检测；（4）冲突处理；

CD可以一边检测冲突，一边收发数据，一旦检测到冲突，立刻停止数据收发。

CA则是必须先检测是否有冲突，得到对端确认后，再发送数据，而不能同时进行，是根据无线网络的特点设计出来的

令牌环网（Token Ring）是一种 LAN 协议，定义在 IEEE 802.5 中，其中所有的工作站都连接到一个环上，每个工作站只能同直接相邻的工作站传输数据。通过围绕环的令牌信息授予工作站传输权限。

IEEE 802.5 中定义的令牌环源自 IBM 令牌环 LAN 技术。两种方式都基于令牌传递（Token Passing）技术。虽有少许差别，但总体而言，两种方式是相互兼容的。

令牌环网（Token Ring）适合于低速网络，光纤分布式数据接口（FDDI）适合于高速网络。

令牌环（Token-Ring）是定义在IEEE 802.5标准中的一种局域网接入方式。

令牌环网络的基本原理是利用令牌（代表发讯号的许可）来避免网络中的冲突，与使用冲突检测算法CSMA/CD的以太网相比，提高网络的数据传送率。此外，还可以设定传送的优先度。

2,PPP协议主要特点：

PPP协议的主要特点是：PPP协议是一种面向字节的协议,所有的帧长度都是整数个字节；使用一种特殊的字符填充法完成数据的填充；不提供使用序号和确认得可靠传输。

PPP不使用序号和确认机制是出于以下的考虑： (1)在数据链路层出现差错的概率不大使用比较简单的：PPP协议较为合理； (2)数据链路层的可靠传输不能够保证网络层的传输也是可靠的； (3)通过CRC检验可以保证无差错接受。 PPP适用于噪声不大的工作环境。 PPP协议不使用序号和确认机制所以无法实现可靠传输。

3,快速以太网和千兆以太网的特点

快速以太网（Fast Ethernet）也就是我们常说的百兆以太网，它在保持帧格式、MAC（介质存取控制）机制和MTU（最大传送单元）质量的前提下，其速率比10Base－T的以太网增加了10倍。二者之间的相似性使得10Base－T以太网现有的应用程序和网络管理工具能够在快速以太网上使用。快速以太网是基于扩充的IEEE802.3标准。

千兆以太网：

千兆位以太网是一种新型高速局域网，它可以提供1Gbps的通信带宽，采用和传统10M、100M以太网同样的CSMA/CD协议、帧格式和帧长，因此可以实现在原有低速以太网基础上平滑、连续性的网络升级。只用于Point to Point，连接介质以光纤为主，最大传输距离已达到70km，可用于MAN的建设。

在对千兆以太网和快速以太网的共同特点的描述中，以下哪种说法是错误的\_\_\_B\_\_\_。

A．相同的数据帧格式

B．相同的物理层实现技术

C．相同的组网方法

D．相同的介质访问控制方法

[解析] 该题考查千兆以太网和快速以太网的特点。千兆以太网的传输速率比快速以太网快10倍，数据传输速率达到1000Mbps。千兆以太网和快速以太网都保留着传统10Mbps速率以太网的所有特征：

A)相同的数据帧格式、C)相同的组网方法、D)相同的介质访问控制方法，只是千兆以太网将传统以太网每个比特的发送时间由100ns降低到1ns，快速以太网降低到10ns。以太网、快速以太网和千兆以太网之间的速率是10倍递乘，而发送时间是10倍递除，考生可以一同记忆。快速以太网标准IEEE 802.3u在LLC子层使用IEEE 802.2标准。

4，交换机、路由器、网桥、集线器 作用和区别、实现功能？

集线器是属于物理层的设备，可以理解为一根网线中间串接出了多个接口，这么多接口共享这一根网线的带宽，因此这些接口上的设备在使得网络时就会出现冲突，或者‘道路’挤占的情况。（所有的设备在一个广播域，冲突域中），集线器现在很少使用了。

交换机、网桥都是数据链路层的设备，网桥的出现就是为了解决集线器多个接口共处于一个冲突域的问题，网桥具有2个接口，且每个接口设备发送接收数据都是独立的互不影响（每个接口是一个冲突域）。现在这种设备不再使用。

交换机可以理解为是一个多接口的网桥，当然具备了网桥分割冲突的功能（每个接口是一个冲突域）。但是交换机（2层交换机）所有接口都在一个广播域中。

路由器属于网络层设备，路由器不但可以隔离冲突域，同时也可以隔离广播。每个接口是一个冲突域，一个广播域。路由器对于广播数据包不做转发。路由器根据3层地址（现用的IP地址）进行转发数据包到相应的接口。实现不同的IP网段互相通讯。

交换机的每个接口相当于使用独立的物理线缆，各自的数据互不影响。

5，虚拟局域网的工作原理

VLAN（Virtual Local Area Network）又称虚拟局域网，是指在交换局域网的基础上，采用网络管理软件构建的可跨越不同网段、不同网络的端到端的逻辑网络。一个VLAN组成一个逻辑子网，即一个逻辑广播域，它可以覆盖多个网络设备，允许处于不同地理位置的网络用户加入到一个逻辑子网中。

VLAN，是英文Virtual Local Area Network的缩写，中文名为"虚拟局域网” VLAN是 一种将局域网（LAN）设备从逻辑上划分（注意，不是从物理上划分）成一个个网段（或者 说是更小的局域网LAN），从而实现虚拟工作组（单元）的数据交换技术。

VLAN这一新兴技术主要应用于交换机和路由器中，但目前主流应用还是在交换机之中

6,可靠传输机制包括哪些方法？分析流量控制和滑动窗口协议的基本原理？

数据链路层的可靠传输通常使用确认和超时重传两种机制来完成。

确认是一种无数据的控制帧，这种控制帧使得接收方可以让发送方知道哪些内容被正确接收。有些情况下为了提高传输效率，将确认捎带在一个回复帧中，称为捎带确认。

超时重传是指发送方在发送某一个数据帧以后就开始一个计时器，在一定时间内如果没有得到发送的数据帧的确认帧，那么就重新发送该数据帧，直到发送成功为止。

自动重传请求（Auto Repeat reQuest，ARQ），通过接收方请求发送方重传出错的数据帧来恢复出错的帧，是通信中用于处理信道所带来差错的方法之一。传统自动重传请求分为三种，即停等式（Stop-and-Wait）ARQ、后退N帧（Go-Back-N）ARQ以及选择性重传（Selective Repeat）ARQ。后两种协议是滑动窗口技术与请求重发技术的结合，由于窗口尺寸开到足够大，帧在线路上可以连续地流动，因此又称为连续ARQ协议.

TCP这个协议是网络中使用的比较广泛，他是一个面向连接的可靠的传输协议。既然是一个可靠的传输协议就需要对数据进行确认。TCP协议里窗口机制有2种：一种是固定的窗口大小；一种是滑动的窗口。这个窗口大小就是我们一次传输几个数据。对所有数据帧按顺序赋予编号，发送方在发送过程中始终保持着一个发送窗口，只有落在发送窗口内的帧才允许被发送；同时接收方也维持着一个接收窗口，只有落在接收窗口内的帧才允许接收。这样通过调整发送方窗口和接收方窗口的大小可以实现流量控制。

TCP滑动窗口技术通过动态改变窗口大小来调节两台主机间数据传输。每个TCP/IP主机支持全双工数据传输，因此TCP有两个滑动窗口：一个用于接收数据，另一个用于发送数据。TCP使用肯定确认技术，其确认号指的是下一个所期待的字节。 假定发送方设备以每一次三个数据包的方式发送数据，也就是说，窗口大小为3。发送方发送序列号为1、2、3的三个数据包，接收方设备成功接收数据包，用序列号4确认。发送方设备收到确认，继续以窗口大小3发送数据。当接收方设备要求降低或者增大网络流量时，可以对窗口大小进行减小或者增加，本例降低窗口大小为2，每一次发送两个数据包。当接收方设备要求窗口大小为0，表明接收方已经接收了全部数据，或者接收方应用程序没有时间读取数据，要求暂停发送。发送方接收到携带窗口号为0的确认，停止这一方向的数据传输。

**网络层**

1. 网络层的基本功能是什么？向上层提供哪两种服务？

网络层为在一个网络连接的两个传送实体间交换网络服务数据单元，提供功能的和规程的方法，它使传送实体的访问独立于路由的选择和交换的方法。为用户提供的服务包括无连接的服务和面向连接的服务。

1. 什么是ARP协议，什么是ICMP协议？

ARP协议（Address Resolution Protocol），或称地址解析协议。ARP协议的基本功能就是通过目标设备的IP地址，查询目标设备的MAC地址，以保证通信的顺利进行。他是IPv4中网络层必不可少的协议，不过在IPv6中已不再适用，并被ICMPv6所替代。

ICMP：互联网控制消息协议（Internet Control Message Protocol 或简写 ICMP）是网路协议族的核心协议之一。它用于 TCP/IP 网络中发送控制消息，提供可能发生在通信环境中的各种问题反馈，通过这些信息，令管理者可以对所发生的问题作出诊断，然后采取适当的措施解决。

ICMP 依靠IP来完成它的任务，它是IP的主要部分。它与传输协议，如TCP和UDP显著不同：它一般不用于在两点间传输数据。它通常不由网络程序直接使用，除了ping和traceroute这两个特别的例子。

IPv4的ICMP也叫ICMPv4。IPv6的也有一个相似的协议，叫ICMPv6。

一.ARP与ICMP的区别

1.定义的不同: A.ARP含义是address resolution protocol，地址解析协议，用于将网络层的IP地址解析为数据链路层的物理地址（mac地址）。

B.ICMP是TCP/IP协议族的一个子协议，用于在IP主机、路由器之间传递控制消息。控制消息是指网络通不通、主机是否可达、路由是否可用等网络本身的消息。

2.工作原理的不同:A.在主机启动时，主机上的ARP映射表为空；当一条动态ARP映射表项在规定时间没有使用时，主机将其从ARP映射表中删除掉，以便节省内存空间和ARP映射表的查找时间。如果在ARP映射表中找不到对应的mac地址，主机创建一个ARP request，并以广播方式在以太网上发送。该网段上的所有主机都可以接收到该请求，但只有被请求的主机会对该请求进行处理。

B.在基于IP数据报的网络体系中，网关必须自己处理数据报的传输工作，而IP协议自身没有内在机制来获取差错信息并处理。为了处理这些错误，TCP/IP设计了ICMP协议，当某个网关发现传输错误时，立即向信源主机发送ICMP报文，报告出错信息，让信源主机采取相应处理措施，它是一种差错和控制报文协议，不仅用于传输差错报文，还传输控制报文。

3.使用范围不同: A. ARP被设计成支持硬件广播的网络上使用，这就意味着ARP将不能在X.25网络上工作。B. 所用使用IP的主机和路由器都必须使用ICMP。

3，IP分组的分片和重组是如何进行的？

IP分片是网络上传输IP报文的一种技术手段。IP协议在传输数据包时，将数据报文分为若干分片进行传输，并在目标系统中进行重组。这一过程称为分片（ fragmentation）。

为什么要进行IP分片

通常要传输的IP报文的大小超过最大传输单位MTU(Maximum Transmission Unit)时就会产生IP分片情况。IP分片通常发生在网络环境中。比如说，在以太网（Ethernet）环境中可传输最大IP报文大小（MTU）为1500字节。而传输的报文大小要比1500字节(不包括以太协议的首部和尾部18个字节)大，这个时候就需要利用到分片技术，经分片后才能传输此报文。另外，使用UDP很容易导致IP分片，而很难强迫TCP发送一个需要进行分片的报文。

1. NAT的基本原理

NAT英文全称是“Network Address Translation”，中文意思是“网络地址转换”。 顾名思义，它是一种把内部私有网络地址（IP地址）翻译成合法网络IP地址的技术。NAT就是在局域网内部网络中使用内部地址，而当内部节点要与外部网络进行通讯时，就在网关（可以理解为出口，打个比方就像院子的门一样）处，将内部地址替换成公用地址，从而在外部公网（internet）上正常使用，NAT可以使多台计算机共享Internet连接，这一功能很好地解决了公共 IP地址紧缺的问题。通过这种方法，可以只申请一个合法IP地址，就把整个局域网中的计算机接入Internet中。这时，NAT屏蔽了内部网络，所有内部网计算机对于公共网络来说是不可见的，而内部网计算机用户通常不会意识到NAT的存在。

1. 子网划分的基本原理，CIDR的基本原理？

网划分定义：Internet组织机构定义了五种IP地址，有A、B、C三类地址。

CIDR（Classless Inter-Domain Routing，无类域间路由选择）它消除了传统的A类、B类和C类地址以及划分子网的概念，因而可以更加有效地分配IPv4的地址空间。它可以将好几个IP网络结合在一起，使用一种无类别的域际路由选择算法，使它们合并成一条路由从而较少路由表中的路由条目减轻Internet路由器的负担。

1. 什么是路由算法，路由算法分哪两类？

通信子网络源节点和目的节点提供了多条传输路径的可能性。网络节点在收到一个分组后，要确定向下一节点传送的路径，这就是路由选择。在数据报方式中 网络节点要为每个分组路由做出选择；而在虚电路方式中，只需在连接建立时确定路由。确定路由选择的策略称路由算法。

　路由选择算法可以分为两大类：非自适应的和自适应的。非自适应算法（no adaptive algorithm） 不根据实测或估计的网络的当前通信量和拓扑结构来作路由选择。从I到J的路由对于所有的I和J是事先脱线地（off-line）计算好的，在网络启动时就下载到路由器中，这一过程有时称作静态路由选择（static routing）

静态：选择策略不用测量也无须利用网络信息，这种策略按某种固定规则进行路由选择。其中还可分为泛射路由选择、固定路由选择和随机路由选择三种算法。

动态：节点路由选择要依靠网络当前的状态信息来决定的策略称动态路由选择策略，这种策略能较好地适应网络流量、拓扑结构的变化，有利于改善网络的性能。但由于算法复杂，会增加网络的负担，有时会因反应太快引起振荡或反应太慢不起作用。独立路由选择、集中路由选择和分布路由选择是三种动态路由选择策略的具体算法。

1. 路由协议可以分为哪两大类

首先路由协议分两类,一种是静态路由协议：手动写目的和下一跳,大量路由数目的时候不适合使用,因为命令写起来比较复杂,多线路的时候选路死板不够灵活.

第二种是动态路由协议,可以根据自己的算法决定选择合适的路径

动态路由协议分两类：内部网关协议.igp，内部协议分两类,一类是距离矢量协议目前常见的是RIP和EIGRP,各大银行都有在用,不能说好坏全凭习惯和初建时的情况.尤其是eigrp的快速收敛,可以满足网络的敏感度要求；第二类是链路状态协议.最常见的是OSPF和is-is,一般城域网都是这两种在跑,还有大型的企业网都在用,是比较安静稳定的路由协议,算法复杂相对灵活扩展性好.

外部网关协议.egp

外部目前只有bgp,没有其他的选项.因为它的算法足够复杂,提供超强的选路原则.稳定性极强.

常见的动态路由协议有:rip(路由信息协议)、ospf(开放最短路径优先)还有 cisco专有的 igrp、eigrp (增强型内部网关路由协议) 这些都是 内部网关路由协议;另外还有 BGP 这个是外部网关路由协议。

1、RIP协议-路由信息协议，属于最早的动态路由协议优点:节约成本，对资源消耗较低，配置简单，对硬件要求低，占用CPU、内存低，所以在小型网络中还有使用到。缺点:计算路由慢，链路变化了收敛慢，能够保存的路由表相对较小，最多只能支持15台设备的网络，只适用于小型网络。

2、OSPF协议-开放最短路径优先协议，企业网主要使用的协议优点:技术成熟，碰到的问题基本上在资料上都能够查到，收敛快，由于cisco的力推，会使用的人多缺点:收敛速度，安全性较ISIS差。

3、ISIS协议-中间系统到中间系统协议，传输网/运营商网络主要使用的协议优点:算法与OSPF类似，收敛快，安全性高缺点:异常处理资料不如OSPF丰富。

4、BGP协议-边界网关协议，用于核心网的路由的传递无所谓优缺点，因为它和其他的不重叠，一个简单的应用，比如BGP可以用于网通和电信之间路由的相互传递，如果使用其它IGP(OSPF或者ISIS)的话，会由于路由数量太多，无法计算出来路由，或者路由计算非常慢，可以支持百万级别的路由的计算和传递，对设备要求较高，对资源占用较大。

8，RIP协议的基本原理

RIP（Routing information Protocol，路由信息协议）是应用较早、使用较普遍的内部网关协议（Interior Gateway Protocol，IGP），适用于小型同类网络的一个自治系统（AS）内的路由信息的传递。RIP协议是基于距离矢量算法（Distance Vector Algorithms，DVA）的。它使用“跳数”，即metric来衡量到达目标地址的路由距离，它是一个用于路由器和主机间交换路由信息的距离向量协议。

自治系统：autonomous system。在互联网中，一个自治系统(AS)是一个有权自主地决定在本系统中应采用何种路由协议的小型单位。这个网络单位可以是一个简单的网络也可以是一个由一个或多个普通的网络管理员来控制的网络群体，它是一个单独的可管理的网络单元（例如一所大学，一个企业或者一个公司个体）。一个自治系统有时也被称为是一个路由选择域（routing domain）。一个自治系统将会分配一个全局的唯一的16位号码，有时我们把这个号码叫做自治系统号（ASN）。

AS（autonomous system）系统指的是处于一个管理机构控制之下的路由器和网络群组。它可以是一个路由器直接连接到一个LAN上，同时也连到Internet上；它可以是一个由企业骨干网互连的多个局域网。在一个自治系统中的所有路由器必须相互连接，运行相同的路由协议，同时分配同一个自治系统编号。一个AS只能运行一种路由协议。

9,OSPF协议的基本原理

RIP的缺点：存在最大跳数是15跳，无法应用在大型网络中；周期性的发送自己的全部的路由信息，浪费流量，收敛速度缓慢；本身的算法存在环路的可能性很大。

OSPF的特别：采用组播更新的方式进行更新（224.0.0.5、224.0.0.6），增量更新（只发送别人没有的），以cost作为度量值，有效的避免了环路（在单区域中可以完全避免环路，但是在多区域中并不能完全避免环路）。OSPF主要特点：

1. 可适应大规模网络2、路由变化收敛快3、无路由环4、支持可变长子网掩码VLSM，5、支持区域划分6、支持以组播地址发送协议报

10，BGP协议的基本原理

边界网关协议BGP（Border Gateway Protocol）是一种自治系统间的动态路由协议，它的基本功能是在自治系统间自动交换无环路的路由信息，通过交换带有自治系统号序列属性的路径可达信息，来构造自治区域的拓扑图，从而消除路由环路并实施用户配置的路由策略。

11，IP6相对于IP4有哪些变化

IPv6具有比IPv4大得多的地址空间。这是因为IPv6使用了128位的地址，而IPv4只用32位。

IPv6二进位制下为128位长度，以16位为一组，每组以冒号":"隔开，可以分为8组，每组以4位十六进制方式表示。例如：2001:0db8:85a3:08d3:1319:8a2e:0370:7344。

IPv4中规定IP地址长度为32，即有2^32-1个地址；而IPv6中IP地址的长度为128，即有2^128-1个地址。

一、扩展了路由和寻址的能力

IPv6 把 IP 地址由 32 位增加到 128 位，从而能够支持更大的地址空间，估计在地球表面每平米有 4\*10^18 个 IPv6 地址，使 IP 地址在可预见的将来不会用完。

IPv6 地址的编码采用类似于 CIDR 的分层分级结构，如同电话号码。简化了路由， 加快了路由速度。

在多点传播地址中增加了一个“范围”域，从而使多点传播不仅仅局限在子网 内，可以横跨不同的子网，不同的局域网。

二、报头格式的简化

IPv 4 报头格式中一些冗余的域或被丢弃或被列为扩展报头，从而降低了包处理和 报头带宽的开销。虽然 IPv6 的地址是 IPv4 地址的 4 倍。但报头只有它的 2 倍大。

三、对可选项更大的支持

IPv6 的可选项不放入报头，而是放在一个个独立的扩展头部。如果不指定路由器不会打开处理扩展头部 . 这大大改变了路由性能。 IPv6 放宽了对可选项长度的严 格要 求 (IPv4 的可选项总长最多为 40 字节 ) ，并可根据需要随时引入新选项。 IPV6 的很多新的特点就是由选项来提供的，如对 IP 层安全 (IPSEC) 的支持，对巨报 (jumbogram) 的支持以及对 IP 层漫游 (Mobile-IP) 的支持等。

四、 QoS 的功能

因特网不仅可以提供各种信息，缩短人们的距离 . 还可以进行网上娱乐。网上 VOD 现正被商家炒得热火朝天，而大多还只是准 VOD 的水平，且只能在局域网上实现， 因特网上的 VOD 都很不理想 . 问题在于 IPv4 的报头虽然有服务类型的字段，实际上 现在的路由器实现中都忽略了这一字段。在 IPv6 的头部，有两个相应的优先权和 流标识字段，允许把数据报指定为某一信息流的组成部分，并可对这些数据报进 行流量控制。如对于实时通信即使所有分组都丢失也要保持恒速，所以优先权最 高，而一个新闻分组延迟几秒钟也没什么感觉，所以其优先权较低。 IPv6 指定这 两字段是每一 IPv6 节点都必须实现的。

五、身份验证和保密

在 IPv6 中加入了关于身份验证、数据一致性和保密性的内容。

IPV6与现在的IPV4比能够提供更多的IP，更高的带宽，基本可以解决现在IP资源缺乏的问题。

**五：传输层：**

1，传输层的基本功能，说明传输层与网络层的关系？

运输层：运输层的任务是向上一层的进行通信的两个进程之间提供一个可靠的端到端服务，使它们看不见运输层以下的搜索数据通信的细节。

传输层的主要功能：

为端到端连接提供可靠的传输服务.

为端到端连接提供流量控制,差错控制,服务质量(Quality of Service,QoS)等管理服务. 具有传输层功能的协议：TCP 、SPX 、NetBIOS。

网络层负责ip数据报的产生以及ip数据包在逻辑网络上的路由转发。

传输层提供端到端通信服务层次,提供可靠及非可靠连接。

网络层只是根据网络地址将源结点发出的数据包传送到目的结点（点到点），其主要任务是：通过路由选择算法，为报文或分组通过通信子网选择最适当的路径。该层控制数据链路层与传输层之间的信息转发，建立、维持和终止网络的连接。具体地说，数据链路层的数据在这一层被转换为数据包，然后通过路径选择、分段组合、顺序、进/出路由等控制，将信息从一个网络设备传送到另一个网络设备。

而传输层则负责将数据可靠地传送到相应的端口（端到端），传输层提供了主机应用程序进程之间的端到端的服务。传输层利用网络层提供的服务，并通过传输层地址提供给高层用户传输数据的通信端口，使高层用户看到的只是在两个传输实体间的一条端到端的、可由用户控制和设定的、可靠的数据通路。

2. tcp协议和udp协议的特点

TCP的优点： 可靠，稳定 TCP的可靠体现在TCP在传递数据之前，会有三次握手来建立连接，而且在数据传递时，有确认、窗口、重传、拥塞控制机制，在数据传完后，还会断开连接用来节约系统资源。 TCP的缺点： 慢，效率低，占用系统资源高，易被攻击 TCP在传递数据之前，要先建连接，这会消耗时间，而且在数据传递时，确认机制、重传机制、拥塞控制机制等都会消耗大量的时间，而且要在每台设备上维护所有的传输连接，事实上，每个连接都会占用系统的CPU、内存等硬件资源。 而且，因为TCP有确认机制、三次握手机制，这些也导致TCP容易被人利用，实现DOS、DDOS、CC等攻击。

UDP的优点： 快，比TCP稍安全 UDP没有TCP的握手、确认、窗口、重传、拥塞控制等机制，UDP是一个无状态的传输协议，所以它在传递数据时非常快。没有TCP的这些机制，UDP较TCP被攻击者利用的漏洞就要少一些。但UDP也是无法避免攻击的，比如：UDP Flood攻击…… UDP的缺点： 不可靠，不稳定 因为UDP没有TCP那些可靠的机制，在数据传递时，如果网络质量不好，就会很容易丢包。 基于上面的优缺点，那么： 什么时候应该使用TCP： 当对网络通讯质量有要求的时候，比如：整个数据要准确无误的传递给对方，这往往用于一些要求可靠的应用，比如HTTP、HTTPS、FTP等传输文件的协议，POP、SMTP等邮件传输的协议。 在日常生活中，常见使用TCP协议的应用如下： 浏览器，用的HTTP FlashFXP，用的FTP Outlook，用的POP、SMTP Putty，用的Telnet、SSH QQ文件传输 ………… 什么时候应该使用UDP： 当对网络通讯质量要求不高的时候，要求网络通讯速度能尽量的快，这时就可以使用UDP。 比如，日常生活中，常见使用UDP协议的应用如下： QQ语音 QQ视频 TFTP ……

一 TCP与UDP区别总结：

1)TCP面向连接（如打电话要先拨号建立连接）;UDP是无连接的，即发送数据之前不需要建立连接

2)TCP提供可靠的服务。也就是说，通过TCP连接传送的数据，无差错，不丢失，不重复，且按序到达;UDP尽最大努力交付，即不保证可靠交付;Tcp通过校验和，重传控制，序号标识，滑动窗口、确认应答实现可靠传输。如丢包时的重发控制，还可以对次序乱掉的分包进行顺序控制。

3)UDP具有较好的实时性，工作效率比TCP高，适用于对高速传输和实时性有较高的通信或广播通信。

4)每一条TCP连接只能是点到点的;UDP支持一对一，一对多，多对一和多对多的交互通信

5)TCP对系统资源要求较多，UDP对系统资源要求较少。

**3，TCP链接建立和拆除过程**

第一次握手：建立连接时，客户端发送syn包(seq=x)到服务器，并进入SYN\_SEND状态，等待服务器确认；

第二次握手：服务器收到syn包，必须确认客户的SYN（ack=j+1），同时自己也发送一个SYN包（seq=y），即SYN+ACK包，此时服务器进入SYN\_RECV状态；

第三次握手：客户端收到服务器的SYN＋ACK包，向服务器发送确认包ACK(ack=y+1)，此包发送完毕，客户端和服务器进入ESTABLISHED状态，完成三次握手。

关闭：

由于TCP连接是全双工的， 因此每个方向都必须单独进行关闭。这原则是当一方完成它的数据发送任务后就能发送一个FIN来终止这个方向的连接。收到一个 FIN只意味着这一方向上没有数据流动，一个TCP连接在收到一个FIN后仍能发送数据。首先进行关闭的一方将执行主动关闭，而另一方执行被动关闭。

TCP客户端发送一个FIN，用来关闭客户到服务器的数据传送（报文段4）。

服务器收到这个FIN，它发回一个ACK，确认序号为收到的序号加1（报文段5）。和SYN一样，一个FIN将占用一个序号。

服务器关闭客户端的连接，发送一个FIN给客户端（报文段6）。

客户段发回ACK报文确认，并将确认序号设置为收到序号加1（报文段7）。

1．为什么建立连接协议是三次握手，而关闭连接却是四次握手呢？

这是因为服务端的LISTEN状态下的SOCKET当收到SYN报文的建连请求后，它可以把ACK和SYN（ACK起应答作用，而SYN起同步作用）放在一个报文里来发送。但关闭连接时，当收到对方的FIN报文通知时，它仅仅表示对方没有数据发送给你了；但未必你所有的数据都全部发送给对方了，所以你可以未必会马上会关闭SOCKET,也即你可能还需要发送一些数据给对方之后，再发送FIN报文给对方来表示你同意现在可以关闭连接了，所以它这里的ACK报文和FIN报文多数情况下都是分开发送的。

什么是拥塞控制：

1. 拥塞：即对资源的需求超过了可用的资源。若网络中许多资源同时供应不足，网络的性能就要明显变坏，整个网络的吞吐量随之负荷的增大而下降。

拥塞控制：防止过多的数据注入到网络中，这样可以使网络中的路由器或链路不致过载。拥塞控制所要做的都有一个前提：网络能够承受现有的网络负荷。拥塞控制是一个全局性的过程，涉及到所有的主机、路由器，以及与降低网络传输性能有关的所有因素。

流量控制：指点对点通信量的控制，是端到端正的问题。流量控制所要做的就是抑制发送端发送数据的速率，以便使接收端来得及接收。

拥塞控制代价：需要获得网络内部流量分布的信息。在实施拥塞控制之前，还需要在结点之间交换信息和各种命令，以便选择控制的策略和实施控制。这样就产生了额外的开销。拥塞控制还需要将一些资源分配给各个用户单独使用，使得网络资源不能更好地实现共享。

几种拥塞控制方法：慢开始( slow-start )、拥塞避免( congestion avoidance )、快重传( fast retransmit )和快恢复( fast recovery )

什么是慢启动：

慢启动算法的思路：主机开发发送数据报时，如果立即将大量的数据注入到网络中，可能会出现网络的拥塞。慢启动算法就是在主机刚开始发送数据报的时候先探测一下网络的状况，如果网络状况良好，发送方每发送一次文段都能正确的接受确认报文段。那么就从小到大的增加拥塞窗口的大小，即增加发送窗口的大小。

六：应用层

1. DNS基本工作原理

　DNS工作原理：

　　第一步：客户机提出域名解析请求，并将该请求发送给本地的域名服务器。

　　第二步：当本地的域名服务器收到请求后，就先查询本地的缓存，如果有该纪录项，则本地的域名服务器就直接把查询的结果返回。

　　第三步：如果本地的缓存中没有该纪录，则本地域名服务器就直接把请求发给根域名服务器，然后根域名服务器再返回给本地域名服务器一个所查询域(根的子域) 的主域名服务器的地址。

　　第四步：本地服务器再向上一步返回的域名服务器发送请求，然后接受请求的服务器查询自己的缓存，如果没有该纪录，则返回相关的下级的域名服务器的地址。

　　第五步：重复第四步，直到找到正确的纪录。

第六步：本地域名服务器把返回的结果保存到缓存，以备下一次使用，同时还将结果返回给客户机。

2，网络管理基本功能编辑

1、故障管理（Fault Management）

故障管理是网络管理中最基本的功能之一。当网络发生故障时：

a.必须尽可能快地找出故障发生的确切位置

b.将网络其它部分与故障部分隔离，以确保网络其它部分能不受干扰继续运行

c.重新配置或重组网络，尽可能降低由于隔离故障后给网络带来的影响

d.修复或替换故障部分，将网络恢复为初始状态。

2、计费管理（Accounting Management）

a.统计那些用户、使用何信道、传输多少数据，访问什么资源等信息

b.统计不同线路和各类资源的利用情况

3、配置管理（Configuration Management）

a.识别被管理网络的拓扑结构、标识网络中的各种现象、自动修复指定设备的配置、动态维护网络配置数据库等内容

4、性能管理（Performance Management）

a.使用最少的网络资源和具有最小的延迟前提下，确保网络能提供可靠、连续的通信能力，并使网络资源的使用达到最优化的程度

5、安全管理（Security Management）

a.确保网络资源不被非法使用，防止网络资源由于入侵者攻击而遭到破坏

3，　SNMP简单概述

SNMP是英文"Simple Network Management Protocol"的缩写，中文意思是"简单网络管理协议"。SNMP是一种简单网络管理协议，它属于TCP/IP五层协议中的应用层协议，用于网络管理的协议。SNMP主要用于网络设备的管理。由于SNMP协议简单可靠 ，受到了众多厂商的欢迎，成为了目前最为广泛的网管协议。

　SNMP的基本思想：为不同种类的设备、不同厂家生产的设备、不同型号的设备，定义为一个统一的接口和协议，使得管理员可以是使用统一的外观面对这些需要管理的网络设备进行管理。通过网络，管理员可以管理位于不同物理空间的设备，从而大大提高网络管理的效率，简化网络管理员的工作。

第七章：网络安全

1，计算机安全包括内容：

计算机安全是指计算机资产安全，即计算机信息系统资源和信息资源不受自然和人为有害因素的威胁和危害。包括计算机硬件安全和存储数据安全。

计算机安全中最重要的是存储数据的安全，其面临的主要威胁包括：计算机病毒、非法访问、计算机电磁辐射、硬件损坏等。

2，比较对称秘钥体制和公钥体制的特点

对称体制加解密算法一致，速度快，但密钥不能泄露；公钥体制加解密算法不一致（非对称），速度慢，但可以公开公钥，因而用于数字证书

两者结合就是数据用对称体制，取其速度快，适合较多数据，再对对称体制中的密钥用公钥体制加密，取其保密性好，因为密钥数据量小，所以加密它不至于太慢

3，说明数字签名的原理

数字签名采用了双重加密的方法来实现防伪、防赖。其原理为：

（1） 被发送文件用SHA编码加密产生128bit的数字摘要（见上节）。

（2） 发送方用自己的私用密钥对摘要再加密，这就形成了数字签名。

（3） 将原文和加密的摘要同时传给对方。

（4） 对方用发送方的公共密钥对摘要解密，同时对收到的文件用SHA编码加密产生又一摘要。

（5） 将解密后的摘要和收到的文件在接收方重新加密产生的摘要相互对比。如两者一致，则说明传送过程中信息没有被破坏或篡改过。否则不然。

疑问：

摘要使用A的私钥加密，如果被拥有A的公钥的第三者截获，不就可以获取到摘要了么？会不会对安全造成威胁。

不会。因为摘要是不可逆推出原文的。

4，IPsec

Internet 协议安全性 (IPSec), IPSec定义了在网际层使用的安全服务，其功能包括数据加密、对网络单元的访问控制、数据源地址验证、数据完整性检查和防止重放攻击。

IPsec虚拟隧道接口对报文的加封装/解封装发生在隧道接口上。用户流量到达实施IPsec配置的设备后，需要IPsec处理的报文会被转发到IPsec虚拟隧道接口上进行加封装/解封装。

5，什么是防火墙

所谓防火墙指的是一个由软件和硬件设备组合而成、在内部网和外部网之间、专用网与公共网之间的界面上构造的保护屏障.是一种获取安全性方法的形象说法，它是一种计算机硬件和软件的结合，使Internet与Intranet之间建立起一个安全网关（Security Gateway），从而保护内部网免受非法用户的侵入，防火墙主要由服务访问规则、验证工具、包过滤和应用网关4个部分组成，防火墙就是一个位于计算机和它所连接的网络之间的软件或硬件。该计算机流入流出的所有网络通信和数据包均要经过此防火墙。

主要类型：1，网络层防火墙 2，应用层防火墙 3，数据库防火墙

6，什么是计算机蠕虫

蠕虫病毒是一种常见的计算机病毒。它是利用网络进行复制和传播，传染途径是通过网络和电子邮件。最初的蠕虫病毒定义是因为在DOS环境下，病毒发作时会在屏幕上出现一条类似虫子的东西，胡乱吞吃屏幕上的字母并将其改形。蠕虫病毒是自包含的程序（或是一套程序），它能传播自身功能的拷贝或自身的某些部分到其他的计算机系统中（通常是经过网络连接）。

蠕虫病毒是自包含的程序(或是一套程序),它能传播它自身功能的拷贝或它的某些部分到其他的计算机系统中(通常是经过网络连接)。请注意，与一般病毒不同，蠕虫不需要将其自身附着到宿主程序，有两种类型的蠕虫：主机蠕虫与网络蠕虫。主计算机蠕虫完全包含在它们运行的计算机中，并且使用网络的连接仅将自身拷贝到其他的计算机中，主计算机蠕虫在将其自身的拷贝加入到另外的主机后，就会终止它自身(因此在任意给定的时刻，只有一个蠕虫的拷贝运行)，这种蠕虫有时也叫"野兔"，蠕虫病毒一般是通过1434端口漏洞传播

7，什么是分布式拒绝服务

分布式拒绝[服务](https://baike.baidu.com/item/%E6%9C%8D%E5%8A%A1)(DDoS:Distributed Denial of Service)攻击指借助于客户/服务器技术，将多个计算机联合起来作为攻击平台，对一个或多个目标发动DDoS攻击，从而成倍地提高拒绝服务攻击的威力。通常，攻击者使用一个偷窃帐号将DDoS主控程序安装在一个计算机上，在一个设定的时间主控程序将与大量代理程序[通讯](https://baike.baidu.com/item/%E9%80%9A%E8%AE%AF)，代理程序已经被安装在网络上的许多计算机上。代理程序收到指令时就发动攻击。利用客户/[服务](https://baike.baidu.com/item/%E6%9C%8D%E5%8A%A1)器技术，主控程序能在几秒钟内激活成百上千次代理程序的运行。

[DdoS](https://baike.baidu.com/item/DdoS)的攻击方式有很多种，最基本的[DoS攻击](https://baike.baidu.com/item/DoS%E6%94%BB%E5%87%BB)就是利用合理的[服务](https://baike.baidu.com/item/%E6%9C%8D%E5%8A%A1)请求来占用过多的服务资源，从而使合法用户无法得到服务的响应。