抓码计算机考研

计算机网络考前必背合集

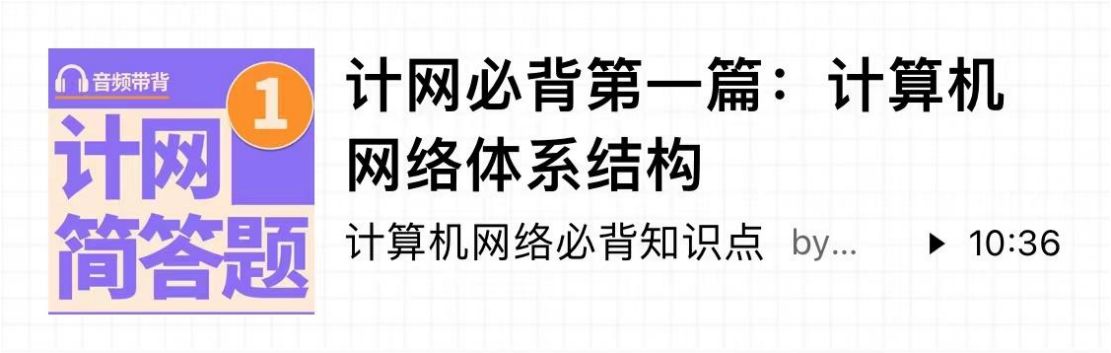
编前语：

计算机网络考前必背资料由抓码专业团队历时两年迭代完善，梳理计算机网络必背重要知识点，以简答题的形式呈现。

如果你是自命题考生，务必多背诵、理解记忆，这是重要考题之一。如果你是 408 考生，熟悉内容、消化理解即可，能够帮助你梳理掌握重要知识点。

此外，抓码运营组基于计算机网络必背文本制作了带背音频，方便大家在冲刺抢分阶段利用碎片化时间反复回顾、温习知识点。

音频带背：抓码计算机考研微信公众号回复关键词“音频带背”；网易云音乐/喜马拉雅扫码收听



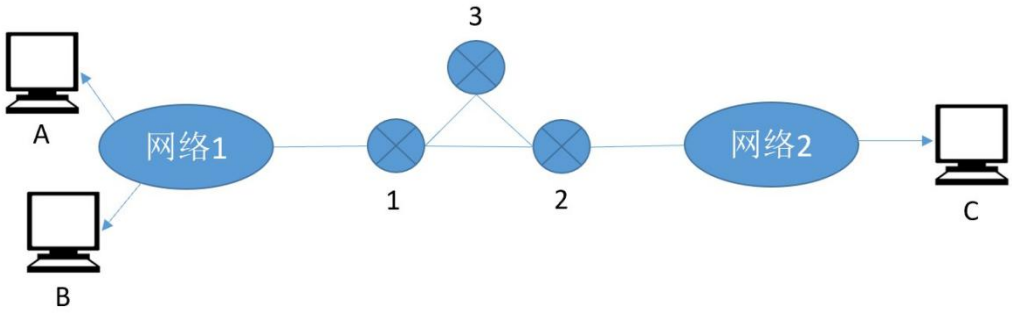
一、计算机网络体系结构

1. 端到端通信和点到点通信有什么区别?

答:

点到点的服务，是指直接相连的结点之间的通信叫点到点通信。它只提供一台机器（一个节点）到另一台机器（另一个节点）之间的通信，如下图所示，路由器 1 和路由器 2 之间的通信就是点到点通信。点到点通信并不能保证数据传输的可靠性，也不能说明具体是哪两个进程在通信。这部分工作需要传输层的端到端通信来完成。

端到端通信建立在点到点通信的基础上，由一段段的点到点通信信道构成的。如下图所示，主机 A 的某个进程和主机 C 的某个进程通信，就是端到端通信。它是比点到点通信更高一级的通信方式，以完成应用程序（进程）之间的通信。“端”是指用户程序的端口，端口号标识了应用层中不同的进程。



2. 比较 OSI 参考模型与 TCP / IP 参考模型的异同点。TCP / IP 协议实现网络互联的关键思想是什么?计算机网络协议为什么需要分层?为什么协议不能设计成 100％可靠的?

答:

（1）①OSI 参考模型有七层:

应用层：为用户提供使用网络的接口或手段。

表示层：数据格式转换、数据加密和解密等。

会话层：进行会话管理与会话同步。

传输层：在端到端之间可靠地传输报文。

网络层：在源和目的结点之间选择路由和控制拥塞。

数据链路层：在相邻结点之间无差错地传输帧。

物理层：透明地传输原始比特流。

发送数据时从应用层开始，每经过一层就封装上首部（包括控制信息），到数据链路层封装上首部和尾部（包括控制信息）后变成帧，经物理层发送到接收方。目的系统接收数据后按照相反的动作层层去掉控制信息，最后把数据传送给接收方。

TCP / IP 体系结构分为：网络接口层、网际层、传输层、应用层。

②相似点：都是独立的协议栈的概念；层的功能大体相似。

③不同点：

1、层次数量有差别， TCP / IP 没有会话层和表示层

2、OSI 更好地区分了服务、接口和协议的概念，因此比 TCP / IP 具有更好的隐藏性，能够比较容易地进行替换；

3、OSI 是先有的模型的概念，然后再进行协议的实现，而 TCP / IP 是先有协议，然后再建立描述该协议的模型；

4、TCP/IP 设计之初就考虑到异构网络互联问题，将 IP 作为重要层次，而 OSI 不支持异构网络互联；

5、OSI 参考模型网络层支持无连接和面向连接的通信，传输层只支持面向连接的通信；而 TCP/IP 模型的网络层只支持无连接的通信，传输层支持无连接和面向连接的通信。

（2）实现网络的互联，其**关键思想是在底层物理网络与高层应用程序和用户之间加入中间层次，屏蔽底层细节，向用户提供通用一致的网络服务**。

在用户看来，整个互联网是一个统一的整体，虽然在物理上由很多使用不同标准的各种类型网络互联而成，但在逻辑上是一个统一的网络，提供通用一致的网络服务。

（3）相互通信的两个计算机系统必须高度协调工作，**“分层”可将复杂的协调问题，转化为若干较小的局部问题，更易于研究和处理。**

分层后，各层之间是独立的；灵活性好；结构上可分割开；易于实现和维护；能促进标准化工作。

（4）假设某协议要求达到 100％可靠，则需要 A 和 B 双方交换信息共 N 次，而**这 N 次交换信息都是必不可少的**。

假定第 N 次交换的信息是从 B 发送给 A。因为已经是第 N 次交换信息了，所以这个信息不需要 A 的确认，这就说明 B 发送的信息丢失或出现差错都不要紧，那么 B 发送的这个信息就可以取消，因而**这个协议就只需要 A 和 B 交换信息 N-1 次而不是 N 次。**

这就和原有的假定不符。如果 B 最后发送的信息需要 A 加以确认，那么这个协议需要 A 和 B 交换信息的次数就不是 N 次，而是 N＋1 次。这和原来假定的“双方交换信息共 N 次”相矛盾。这样就**反证**了协议不能设计成 100％可靠的。

3. 面向连接服务与无连接服务各自的特点是什么?

答:

① **面向连接服务的特点是，在服务进行之前必须先建立连接然后再进行数据传输，传输完毕后，再释放连接。**在数据传输时，好像一直占用了一条这样的链路。它适合于在一定期间内要向同一目的地发送许多报文的情况。优点是数据传输安全，不容易丢失和失序。但链路的建立维护和释放要耗费一定的资源和时间。

② **无连接服务的特点，在服务过程中不需要先建立虚电路，链路资源在数据传输过程中动态进行分配。**这种方式灵活方便，比较迅速；但不能防止报文的丢失、重复或失序。它适合于传送少量零星的报文。

4. 试画出 OSI 参考模型结构示意图，并简述各层的主要功能

7	应用层
6	表示层
5	会话层
4	传输层
3	网络层
2	数据链路层
1	物理层

OSI 参考模型各层的主要功能如下：

（1）物理层：规定了激活、维持、关闭通信端点之间的**机械特性、电气特性、功能特性以及规程特性**。该层为上层协议提供了传输数据的物理介质。

（2）数据链路层：在不可靠的物理介质上**提供可靠的传输**。作用包括：物理地址寻址、数据的成帧、流量控制、数据的检错、重发等。

（3）网络层：负责对子网之间的数据包进行**路由选择**。网络层还可以实现拥塞控制、网际互连等功能。

（4）传输层：负责将上层数据分段并提供**端到端的、可靠的或不可靠的传输**。此外，传输层还要处理端到端的差错控制和流量控制问题。

（5）会话层：**管理主机之间的会话进程**，即负责建立、管理、终止进程之间的会话。会话层还利用在数据中插入校验点来实现数据的同步。

（6）表示层：**对上层数据或信息进行变换**以保证一个主机应用层信息可以被另一个主机的应用程序理解。

（7）应用层：**为应用程序提供访问网络**的服务。

5. 简述计算机网络采用层次化结构模型的优点

答:

计算机网络采用层次化结构模型的优点如下：

①**各层之间是独立的。**某一层并不需要知道它的下一层是如何实现的，而仅需知道该层是如何通过层间接口所提供服务。每一层实现相对独立的功能，将一个难以处理的复杂问题分解为若干个比较容易处理的更小问题。

②**灵活性好。**任何一层发生变化时，只要层间接口关系保持不变，则在这层以上或以下的各层均不受影响。

③**结构上可分割。**各层都可以采用最合适的技术实现。

④**易于实现和维护。**这种结构使得实现、调试和维护一个庞大而复杂的系统变得容易。

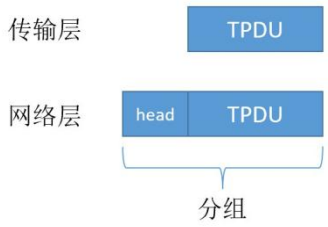
⑤**能够促进标准化工作。**每一层的功能及其所提供的服务都已有了精确的说明。

6. 在 OSI 模型中，是 TPDU(传输层协议数据单元) 封装网络层分组，还是网络层分组封装 TPDU?请讨论。

答:

网络层分组封装 TPDU。

当传输层的 TPDU 向下到达网络层的时候，整个 TPDU，包括其首部和数据，都被用作网络层分组的数据段。也就是说，整个 TPDU 都被放到一个网络层的分组中。如下图所示。



7. 什么是服务原语?服务原语的三要素是什么?服务原语的类型有哪几种?

答:

上层使用下层所提供的服务必须通过与下层交换一些命令，这些命令在 OSI 中称为服务原语。

服务是通过一组服务原语来执行的，原语供用户和其他实体访问该服务时调用。它们被用来通知服务提供者采取某些行动或向其相邻上层报告某个对等实体的活动。

服务原语包含四种类型：

1、请求（request）:一个实体希望得到完成某些操作的服务；

2、指示(indication):通知一个实体，有某个事件发生；

3、响应（response）:一个实体希望响应一个事件；

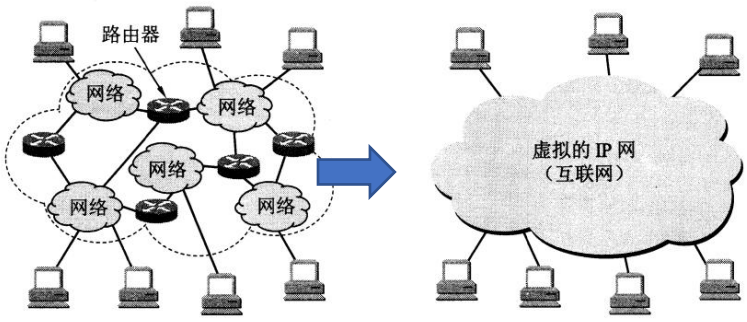
4、证实（confirm）:返回对先前请求的响应。

8. TCP/IP 的核心思想是什么?

答:

TCP/IP 的核心思想是“网络互联”，将使用不同低层次协议的异构网络，在传输层、网络层建立一个统一的虚拟逻辑网络。

如下图所示。



二、物理层

1. 试比较模拟通信方式与数字通信方式的优缺点。

答:

模拟通信方式:

（1）定义：在现在的数据通信中，模拟通信方式主要是通过调制解调器把数字信号转换成模拟信号在模拟信道上传输。

（2）优点：模拟通信方式可以利用目前覆盖面最广、普遍应用的模拟语音通信信道，用于语音通信信道的电话交换网技术较为成熟，造价较低

（3）缺点：数据传输速率较低，系统效率低。

数字通信方式：

（1）定义：数字通信方式是利用数字信道直接传输数字信号的方法。

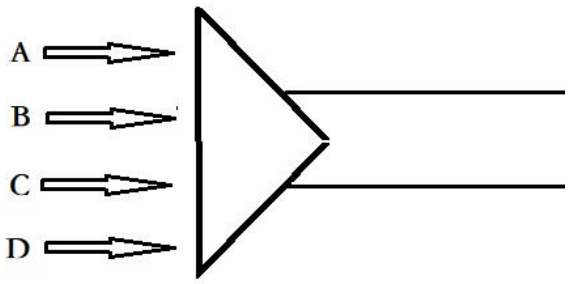
（2）优点：数字通信方式在基本不改变数字数据频带的情况下直接传输数字信号，可以达到很高的传输速率，这是目前积极发展与广泛应用的数据通信方式。

（3）缺点：数字通信中，要准确地恢复信号，接收端需要严格的同步系统，因此对设备要求较高。

2．什么是多路复用技术？有几种复用方法？

答：

多路复用技术是将若干个彼此独立的信号，合并为一个可以在同一个信道上同时传输和复合信号的方法。如下图所示，可以将多个信号合并为一个信号。



多路复用技术主要包括频分多路复用、时分多路复用、波分多路复用和码分多路复用。

频分多路复用：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，所有用户在同样的时间占用不同的带宽资源。

时分多路复用：是所有用户在不同的时间占用同样的频带宽度。

波分多路复用：是用一根光纤来同时传输不同波长的光载波信号。

码分多路复用是每一个用户可以在同样的时间使用同样的频带进行通信，靠不同的编码来区分各路原始信号的一种复用技术。

3．物理层的接口有哪几个方面的特性？各包含些什么内容？

答：

物理层的接口主要有四个方面的特性。

（1）机械特性。

接口所用接线器的形状和尺寸、引线数目和排列、固定和锁定装置等等。例如对各种规格的电源插头的尺寸都有严格的规定。

（2）电气特性。

说明在接口电缆的某条线上出现的电压应为什么范围，即什么样的电压表示 1 或 0。

（3）功能特性。

说明某条线上出现的某一电平的电压表示何种意义。

（4）规程特性。

说明对于不同功能的各种可能事件的出现顺序。

4. 什么是曼彻斯特编码和差分曼彻斯特编码？其特点是什么？

答:

曼彻斯特编码：

（1）定义：是将每一个码元再分成两个相等的间隔。码元 1 是处于前一个间隔为高电平，而后一个间隔为低电平。码元 0 则正好相反，从低电平变到高电平。

（2）优点：这种编码的好处是可以保证在每一个码元的正中间出现一次电平的转换，这对接收端的提取位同步信号是非常有利的。

（3）缺点：它所占的频带宽度比原始的基带信号增加了一倍。

差分曼彻斯特编码：

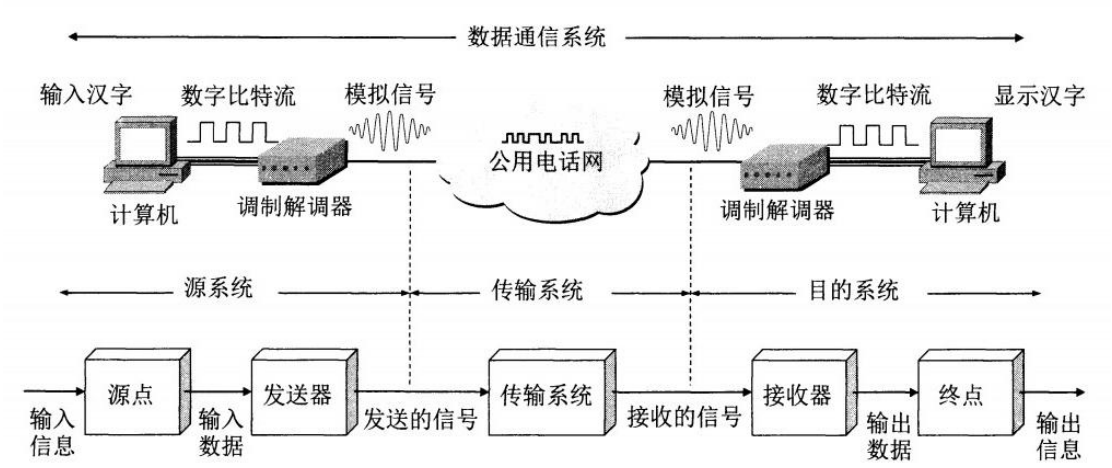
（1）定义：规则是若码元为 1，则其前半个码元的电平与上一个码元的后半个码元的电平相同；但若码元为 0，则其前半个码元的电平与上一个码元的后半个码元的电平相反。不论码元是 1 或 0，在每个码元的正中间时刻，一定要有一次电平的转换。

（2）优点：可以获得较好的抗干扰性能。

（3）缺点：差分曼彻斯特编码需要较复杂的技术作为支持。

5. 试给出数据通信系统的模型并说明其主要构件的作用。

如图所示，一个数据通信系统可划分为三大部分，即源系统（或发送端）、传输系统（或传输网络）和目的系统(或接收端)。



源系统一般包括以下两个部分：

1、**源点：**源点设备产生要传输的数据，源点又称为源站，或信源。

2、**发送器**：通常源点生成的数字比特流要通过发送器编码后才能够在传输系统中进行传输。

目的系统一般包括以下两个部分：

1、**接收器：**接收传输系统传送过来的信号，并把它转换为能够被目的设备处理的信息。

2、**终点：**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(例如，把汉字在计算机屏幕上显示出来)。终点又称为目的站，或信宿。

在源系统和目的系统之间的传输系统可以是简单的传输线，也可以是连接在源系统和之间的复杂网络系统，负责将信息传输到目的系统。

三、数据链路层

1．简述与传统共享式局域网相比，使用局域网交换机的交换式局域网为什么能改善网络的性能和服务质量？

答：

传统共享式局域网的核心设备是集线器，而交换式局域网的核心是以太网交换机。

在使用共享式集线器的传统局域网中，在任何一个时刻只能有一个结点通过共享通信信道发送数据。

而在使用交换机的交换式局域网中，交换机可以在它的多个端口之间建立多个并发连接，从而实现了结点之间数据的并发传输，有效地改善了网络性能和服务质量。

2．试比较分析中继器、集线器、网桥、交换机的区别和联系。

答：

中继器、集线器、网桥、交换机都是常见的用于互联、扩展局域网的连接设备，但工作的层次和实现的功能有所不同。

（1）**中继器**工作在物理层用来连接两个网段，主要功能是对信号进行再生和还原，以消除信号由于经过一长段电缆而造成的失真和衰减，使信号的波形和强度达到所需要的要求。

（2）**集线器**工作在物理层，它实质上相当于一种多端口中继器，可以将多个结点连接成一个共享式的局域网，但任何一个时刻只有一个结点通过公共信道发送数据。

（3）**网桥**工作在数据链路层，它可以在采用不同数据链路层协议、不同传输介质以及不同数据传输速率的局域网之间接收、过滤、存储与转发数据帧。

（4）**交换机**工作在数据链路层，它是交换式局域网的核心设备，本质是多端口网桥，允许端口之间建立多个并发的连接，实现多个结点之间的并发传输。

3．简述交换机工作原理。

答：

以太网交换机采用存储转发方式。

1、存储：接口有存储器，当输出接口繁忙起来时就把到来的帧进行暂存。

2、转发：交换机是多接口的网桥，当交换机收到一个帧时，并不是向所有的接口转发此帧，而是检测此帧的源 MAC 地址和目的 MAC 地址，并与系统内部的动态查找表进行比较，然后确定将该帧转发到哪一个接口，或是把它丢弃。若 MAC 地址不在查找表中，则将该地址加入查找表中。

4．以太网适配器（网卡）工作在哪一层？实现该层的哪些功能？

答：

以太网适配器（网卡）工作在数据链路层，实现介质访问控制(MAC)和物理层的功能。在 MAC 层可以：

（1）、发送时将数据组装成带有地址和差错检测段的帧；

（2）、接收时拆卸帧，执行地址识别和差错检测；

（3）、管理链路上的通信，执行 CSMA/CD

在物理层可以：

（1）、信号的编码/译码

（2）、前导码（前缀）的生成/除去（用于同步）

（3）、比特的发送/接收。

5. 什么是 CSMA / CD？并论述其发送过程。

答：

CSMA / CD，即载波监听多路访问 / 冲突检测方法，是一种争用型的介质访问控制协议，核心思想是：先听后发、边听边发、冲突停发、随机重发。

它的原理比较简单，技术上易实现，网络中各工作站处于平等地位，不需要集中控制，不提供优先级控制。但在网络负载增大时，发送时间增大，发送效率急剧下降。CSMA / CD 应用在 ISO 七层里的数据链路层。

它的工作原理是：发送数据前先监听信道是否空闲，若空闲则立即发送数据。在发送数据时，边发送边继续监听。若监听到冲突，则立即停止发送数据。等待一段随机时间后再重新尝试。

发送过程包含四个处理内容：侦听、发送、检测和冲突处理。

（1）侦听： 通过专门的检测机构，在站点准备发送前先侦听一下总线上是否有数据正在传送（线路是否忙），若“忙”则进入后续的“退避”处理程序，进而进一步反复进行侦听工作。

（2）发送： 当确定要发送后，向总线发送数据。

（3）检测： 数据发送后，仍可能发生数据碰撞。因此，要对数据边发送，边接收，以判断是否冲突。

（4）冲突处理： 当确认发生冲突后，进入冲突处理程序。有两种冲突情况：

①若在侦听中发现线路忙，则等待一个延时后再次侦听，若仍然忙，则继续延迟等待，一直等到可以发送为止。每次延时的时间不一致，由退避算法确定延时值。

②若发送过程中发现数据碰撞，先发送阻塞信息，强化冲突，再进行侦听工作，待下次重新发送（方法同①）。

6. 滑动窗口协议中，发送窗口和接收窗口的含义？

答：

发送窗口用来对发送端进行流量控制，而**发送窗口的大小代表在还没有收到对方确认的条件下发送端最多可以发送多少个数据帧**。

接收窗口是为了控制数据帧是否可以接收。在接收端只**有当收到的数据帧的发送序号落在接收窗口内才允许将该数据帧收下**。若接收到的数据帧落在接收窗口之外，则一律将其丢弃。

7. 简述选择重传 ARQ 协议的工作原理？

答：

为了进一步提高信道的利用率，可以设法只重传出现差错的数据帧或者是定时器判定为超时的数据帧。此时必须加大接收窗口（接收窗口大于 1），以便先收下发送序号不连续（错

误帧或者超时帧之后的帧）但仍处在接收窗口中的那些数据帧。等到所缺序号的数据帧收到之后再一并送交主机。

8.描述滑动窗口控制机制及其作用。比较停止–等待协议、多帧滑动窗口与后退 N 帧协议、多帧滑动窗口与选择重传协议的区别。

答:

（1）滑动窗口控制机制

滑动窗口是进行数据链路控制的一个重要机制，滑动窗口协议的基本原理是在任意时刻，发送方都维持了一个连续的允许发送的帧的序号，称为发送窗口；同时，接收方也维持了一个连续的允许接收的帧的序号，称为接收窗口。

滑动窗口机制在发送方和接收方分别设置发送窗口和接收窗口，使得在数据传输过程中受控地向前滑动，从而控制数据传输的过程。

（2）滑动窗口控制机制的作用

发送窗口用来对发送方进行流量控制，其大小指明在收到对方 ACK 之前发送方最多可以发送多少个数据帧，只有序号在窗口覆盖范围内的数据帧才是可以连续发送的。

接收窗口控制哪些数据帧可以接收，只有到达的数据帧的序号落在接收窗口之内时才可以被接收，否则将被丢弃。

一般情况下，当接收方收到一个按序且无差错的帧后，接收窗口向前滑动，准备接收下一个帧，并向发送方发出一个确认。为了提高效率，接收方可以采用累计确认或捎带确认。

当发送方收到接收方的确认后，发送窗口才能向前滑动，滑动的长度取决于接收方确认的序号。向前滑动后，又有新的帧落入发送窗口，它们可以被发送。滑动后被确认正确收到的帧落在窗口的后边，从而达到了对流量进行控制的作用。

（3）停止–等待协议

当发送窗口和接收窗口的大小固定为 1 时，滑动窗口协议就是停止–等待协议。

该协议规定发送方每发送一帧后就要停下来，等待接收方已正确接收的确认返回后才能继续发送下一帧。由于接收方需要判断接收到的帧是新发的帧还是重新发送的帧，因此**发送方要为每一个帧加上 1bit 的序号**，从而便于进行区分。

（4）多帧滑动窗口与后退 N 协议

发送方连续发送若干个数据帧，不停下来等待应答帧。发送方在每发送完一个数据帧时都要设置超时定时器。只要在额定时间内仍未收到确认帧，就要重发相应的数据帧及其后的全部帧。

（5）多帧滑动窗口与选择重传协议

当接收方发现某帧出错后，其后继续送来的正确帧被接收方存放在一个缓冲区中，同时要求发送方重新传送出错的那一帧。一旦收到重新传来的帧后，就可以原已存于缓冲区中的其余帧一并按正确的顺序递交给高层。

9. 简述以太网和令牌网这两种局域网的工作原理。

答:

（1）以太网 MAC 子层使用载波侦听多路访问 / 碰撞检测（CSMA / CD）的竞争访问技术。

通过让每个设备监听网络是否空闲（先听后发），从而来降低冲突的影响范围，要传递数据的设备只有等网络空闲时才能传递。

这样面临的一个问题就是：当多个设备同时监测到空闲后，同时传递数据，就会产生冲

突。所以设备传输数据时也需要继续侦听（边听边发），使它能检测到发生的冲突。

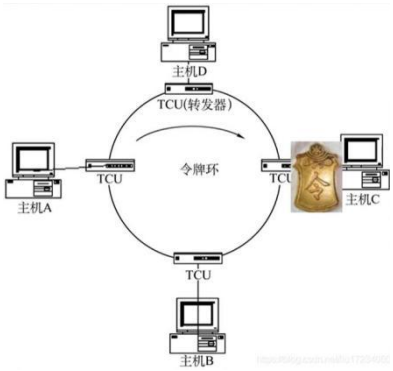
冲突发生时，所有的设备都停止传送（冲突停发），并发出一个“拥塞信号”，通知所有冲突的站点。每个设备在重新传递前，都需要等待一段随机的时间（随机重发），进一步降低了网络冲突。

（2）**令牌网的 MAC 子层使用令牌帧访问技术，物理拓扑是环型的，使用逻辑环逐站传递令牌。**

令牌网的每一站通过电缆与转发器相连，每个站点不处于发送数据的状态，就处于收听状态。

令牌实际上是一种特殊的帧，平时不停地在环路上流动，当一个站有数据要发送时，必须先截获令牌，一旦发现环路输入的比特流中出现令牌时，首先将令牌的独特标志转变为帧的标志（即称为截获），接着就将本站的转发器置为发送方式，并将发送缓冲区的数据从转发器的环路输出端发送出去。

如下图所示是令牌环网。



10．试述 p 持续 CSMA 和非持续 CSMA 之间的差别。

答:

CSMA（载波感应多路访问）方法结合使用了一种机制，即各个设备可以检测介质是否正在被使用。如果一个要发送的站“听到”在介质上有分组在传送，该站介质空闲之前必须等待。

采用 CSMA，需要一种算法，来决定当发现介质忙时如何处理。常用的算法有三种。

1、1—持续 CSMA。

1）、如果一个主机要发送消息，那么它先监听信道。

2）、空闲则直接传输，不必等待。

3）、忙则一直监听，直到空闲马上传输.

4）、如果有冲突（一段时间内未收到肯定回复），则等待一个随机长的时间再监听，重复上述过程。

2、非持续 CSMA（non—persistent CSMA）。

1）、如果一个主机要发送消息，那么它先监听信道。

2）、空闲则直接传输，不必等待。

3）、忙则等待一个随机的时间之后再进行监听。

4）、如果有冲突（一段时间内未收到肯定回复），则等待一个随机长的时间再监听，重复上述过程。

3、P—持续 CSMA(P—persistentCSMA)。

1）、如果一个主机要发送消息，那么它先监听信道。

2）、空闲则以 p 概率直接传输；1—p 的概率等待到下一个时间槽再传输。

3）、忙则持续监听直到信道空闲再以 p 概率发送。

4）、若冲突则等到下一个时间槽开始再监听并重复上述过程。

上述三种算法的比较如下表所示。

	信道空闲	信道忙
1-坚持CSMA	马上发	继续持续监听
非坚持CSMA	马上发	放弃监听，等一个随机时间再监听
p-坚持CSMA	p概率马上发，1-p概率下一个时隙再发	持续监听，等空闲时再以p概率发出

11．为什么在无线局域网中不能使用 CSMA/CD 协议而必须使用 CSMA/CA 协议？

答:

原则上讲，无线局域网的 MAC 协议与有线局域网并无本质上的区别。然而，无线局域网不能采用以太网的 CSMA/CD，其原因有三个方面。

1、无线环境不像有线广播媒体那样好控制，来自其他局域网中的用户传输会干扰 CSMA/CD 的操作。

2、在无线环境中，因为发送设备的功率通常要比接收设备的功率强得多，检测冲突是困难的。在这种情况下，设计一个能够帮助避免冲突的系统更有意义

3、无线局域网存在隐藏站问题。

4、大多数无线电都是半双工的，它们不能够在同一频率上于发送的同时监听突发噪音。

因此，802.11 采用了 CSMA/CA 技术，CA 表示冲突避免。这种协议实际上是在发送数据帧前需对信道进行预约。

12．二进制指数后退的含义是什么？

答:

在二进制指数后退算法中，如果一个发送设备检测到了一次冲突，它就退避，等待一个随机的时间长度。

推迟的时间必须是时隙（slot time）的整数倍。时隙是冲突处理的时间单位，它大于物理层往返传输时间，其值跟网络的具体实现有关，比如在基带类型 10BASE5 中该值是 512 位。

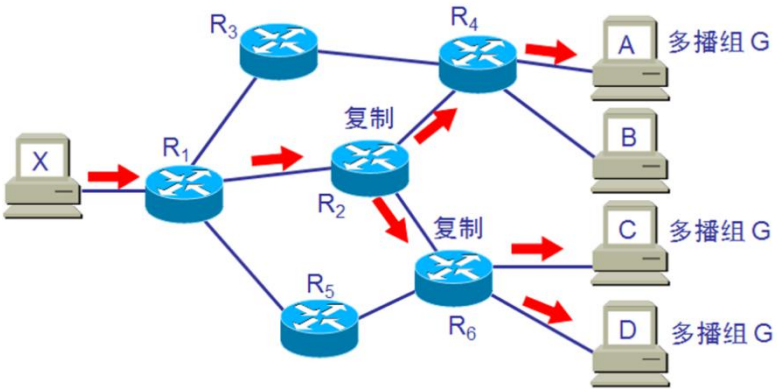
延长多少时隙选为均匀分布的随机参数 r，$0 \leqslant r \leqslant 2^k$，其中 k=min(n,10)，n 为重发次数。使用随机数 r，就可以使得任何两个站产生相关值的可能性最小。而使用重发次数 n，就可以使得在重发数据之后，如果又产生了冲突，那么退避的时间长度会增加。

四、网络层

1．什么是 IP 组播?

答:

IP 组播（IP muhicasting）是对硬件组播的抽象，是对标准 IP 网络层协议的扩展。它通过使用特定的 IP 组播地址，按照最大投递的原则，将 IP 数据报传输到一个组播群组（multicast group）的主机集合。如下图所示。



它的基本方法是：当某一个人向一组人发送数据时，它不必向每一个人都发送数据，**只需将数据发送到一个特定预约的组地址，所有加入该组的人均可以收到这份数据**。这样对发送者而言，只需发送一次就可以发送到所有接收者，大大减轻了网络的负载和发送者的负担。

2. 当一个移动主机不在居所的时候. 送往它的居所 LAN 的分组被它的居所代理截获，对于一个 802.3LAN 上的 IP 网络,居所代理如何完成这个截获任务?

答:

一种方法是让居所代理不加选择地读在 LAN 上传送的所有帧，**通过观察其中的目的 IP 地址是否指向移动主机**。但是，该方法的缺点是效率非常低。

通常采用的替代方法是通过响应 ARP 请求，让路由器认为居所代理就是异动主机。

当路由器得到一个目的 IP 地址为移动主机的 IP 分组时,它广播一个 ARP 查询请求，询问与目的地计算机（即移动主机）的 IP 地址相对应的 802.3MAC 地址。当移动主机不在居所时。居所代理响应该 ARP 请求。从而路由器把移动用户的 IP 地址与居所代理的 802.3MAC 地址相关联。

3. 简述转发器、交换机、路由器和网关的工作层次和作用。

答:

转发器：工作在物理层，作用是放大信号

交换机：工作在数据链路层，作用是隔离冲突域

路由器：工作在网络层，作用是实现数据的网络传递

网关：工作在网络层以上，作用是实现协议转换

4. 简述 Link-State 路由算法的工作过程及其特点。

答:

（1）Link-State（链路状态）路由算法的工作过程如下：

①发现邻居节点；

②测量线路开销；

③构造链路状态报文；
④广播链路状态报文；
⑤重新计算路由；
（2）Link-State（链路状态）路由算法的特点如下：
①考虑线路的带宽；
②算法的收敛性得到保证
③算法对路由器的要求高

5. 什么是域名地址、IP 地址和 MAC 地址？它们之间有什么关系？

答：

域名地址：IP 地址很难记忆，为了便于用户记忆和识别，引入域名。如 abc.x.y.com。

IP 地址：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唯一的 32 位标识符。如 192.168.1.1。

MAC 地址：也称为硬件地址或物理地址，固化在适配器的 ROM 中。如 00-9e-1a-36-87-8c。

域名地址、IP 地址、MAC 地址之间均没有一一对应的关系。域名系统用于将域名地址解析为 IP 地址，ARP 用于将 IP 地址解析为 MAC 地址。

6. （1）IP 地址与物理地址、主机名与 IP 地址怎样建立的对应关系，两者使用的协议有何相同、相异之处？

（2）若在以太网上运行 IP 协议，源主机 A 要和 IP 地址为 129.1.1.2 的主机 B 通信，请问怎样转换成 B 机的以太网地址(MAC 地址)？(说明采用的协议及查找过程)。

（3）采取了哪些措施提高 IP 地址与物理地址转换的效率？

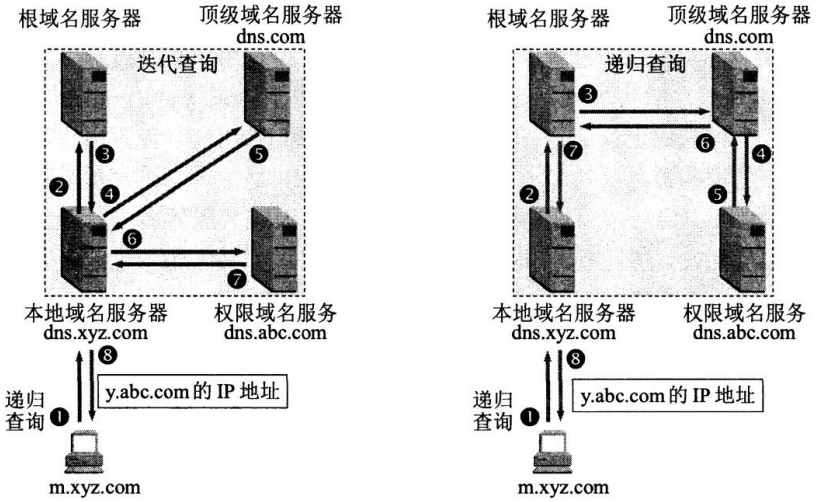
答：

（1）、**IP 地址与物理地址的映射，需要使用地址解析协议 ARP。**

当主机 A 向主机 B 发送报文时，先检查缓存区对照表，若未查到则主机 A 广播一个 ARP 请求，其中携带 A 的 IP 地址与物理地址以及 B 的 IP 地址，请求 B 主机回答自己的物理地址。当 B 主机收到这个请求后，向 A 发一个 ARP 响应，其中携带了自己的 IP 地址与物理地址。A 收到后，将 B 的 IP 地址与物理地址存入缓存备查。

主机名与 IP 地址的映射，需要使用域名解析系统 DNS。

当用户应用程序需要将域名（主机名）解析为 IP 地址时，就通过本地主机的地址解析器，先向本地域名服务器发出询问，是否是本地域名；若是，便进行本地解析；否则查高速缓存，看最近是否解析过；若是，则将查到的 IP 地址报告本地主机的地址解析器；否则，访问远程域名服务器，使用递归查询或者迭代查询的方式，向根域名服务器、顶级域名服务器和权限域名服务器发出请求。递归查询和迭代查询的方式如下图所示。



ARP 和 DNS 有**相似点**：都是主机发送出请求，然后从相应的服务器收到所需的回答。

ARP 和 DNS 有**相异点**：DNS 是应用层协议，用来请求域名服务器将连接在因特网上的某个主机的域名解析为 IP 地址，用于广域网。ARP 是网络层协议，它采用广播方式请求将连接在本以太网上的某个主机或路由器的 IP 地址解析为以太网硬件地址，用于局域网。

（2）将主机 B 的 IP 地址转换为以太网地址过程如下：

1、首先源端主机 A 要查询本地的 ARP 高速缓存，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。如果在 ARP 高速缓存查到了 IP 地址为 129.1.1.2 的主机的物理地址，则使用此物理地址封装 IP 报，成为一个以太帧，传给目的主机。

2、 如果在高速缓存中没有找到，A 主机就以广播方式在以太网中发送 ARP 请求，包中给出 A 主机的 IP 地址和物理地址，还有 IP 地址 129.1.1.2，向网内的所有主机询问 IP 地址为 129.1.1.2 的主机的物理地址：

3、每一个收到 A 主机的 ARP 包的主机都检查自己的 IP 地址是不是 129.1.1.2，如果不是，则不作回应；

4、IP 地址为 129.1.1.2 的主机收到 A 发来的 ARP 包后，将自己的物理地址填入 ARP 响应并发回给 A 主机。这样，A 主机就可以用此物理地址封装 IP 报，成为一个以太帧，传给目的主机，完成传输任务。

（3）ARP 采取如下措施提高地址转换的效率：

1、**使用高速缓存。**每台 ARP 的主机保留了一个专用的 ARP 缓存区存放最近获得的 IP 地址和物理地址的映射，ARP 先在缓存中查找 IP 地址对应的物理地址。

2、**在 ARP 请求报文中放入源站的 IP 地址和物理地址的映射**，以免目标机紧接着为解析源站的物理地址而再进行一次动态绑定操作。

3、**源站在广播自己的地址映射时，网上所有主机都将它存入自己的高速缓存。**

4、新的主机入网时，**主动广播自己的 IP 地址和物理地址的映射。**

五、传输层

1. 简述 TCP 和 UDP 协议的主要特点和应用场合。

答:

UDP 的主要特点是:

(1) 传送数据前无需建立连接，没有流量控制机制，数据到达后也无需确认。

(2) 不可靠交付，只有有限的差错控制机制。

(3) 报文头部短，传输开销小，时延较短。

因此，**UDP 协议简单，在一些特定的应用中运行效率高。**通常用于可靠性较高的网络环境（如局域网）或 不要求可靠传输的场合，另外也常用于客户机 / 服务器模式中。

TCP 的主要特点是:

(1) 面向连接，提供了可靠的建立连接和拆除连接的方法，还提供了流量控制和拥塞控制的机制。

(2) 可靠交付，提供了对报文段的检错、确认、重传和排序等功能。

(3) 报文段头部长，传输开销大。

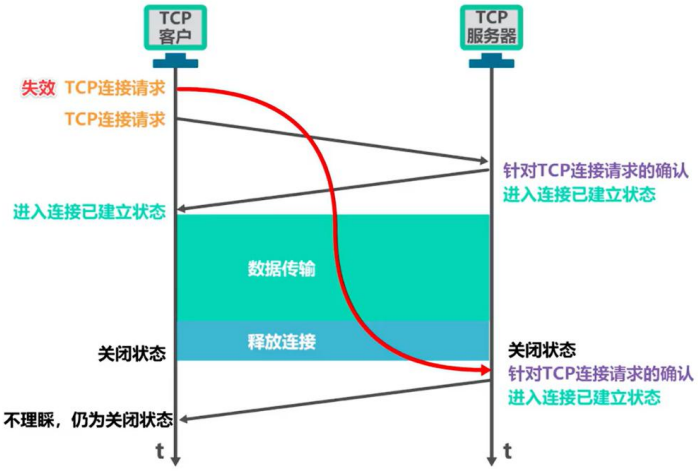
因此，TCP 常用于不可靠的互联网中为应用程序**提供面向连接的、可靠的、端到端的字节流服务。**

2. 假定 TCP 采用 2 次握手代替 3 次握手来建立连接，也就是说省去第三个报文，是否可能会发生死锁?

答:

3 次握手需要完成两个重要的功能，**既要双方做好发送数据的准备工作（双方都知道彼此已准备好），也要允许双方就初始序列号进行协商**，这个序列号在握手过程中被发送和确认。现在把三次握手改成仅需要两次握手，死锁是可能发生的。

假设两次握手就可以建立连接，考虑下面这个例子。



TCP 客户发送了第一个 TCP 连接请求（第一次握手），但是该请求因为网络问题或者其他原因，导致经过很长一段时间才到达 TCP 服务器。在这段时间内，TCP 客户已经超时重传了一个新的 TCP 请求连接报文，并通过两次握手建立连接、之后再传输数据，并断开连接。

当第一个 TCP 连接请求到达了 TCP 服务器（上图中红色箭头），TCP 服务器进程随即发送 TCP 连接请求确认报文段（第二次握手），并进入连接已建立状态，等待 TCP 客户发来的数据。

而 TCP 客户进程收到连接请求的确认报文段后，并不想建立连接，因此并不理睬 TCP 连接请求确认报文段（第二次握手），不进入连接已建立状态，自然也不会给 TCP 服务器进程发送数据。

在这种情况下，TCP 服务器进程会持续挂起对 TCP 客户进程的连接，但是始终等不到数据，就会造成大量的资源浪费。

而使用三次握手就能很好的解决这个问题。

如果 TCP 客户并不理睬 TCP 连接请求确认报文段（第二次握手），那么 TCP 服务器就始终收不到确认报文段（第三次握手），就不会进入连接已建立状态，也就不会持续挂起对 TCP 客户进程的连接，造成资源的浪费。

3. IP 数据报的分片和重组是由 IP 协议控制的，而对 TCP 协议而言是透明的。这是否意味着 TCP 不用担心 IP 数据报以错误的次序到达？为什么？

答:

尽管 IP 数据报的分片和重组是由 IP 协议控制的，但由于 IP 协议提供的是无连接、不可靠的网络服务，只通过 IP 协议并不能清楚地了解到数据报是否顺利地发送给目标计算机。TCP 协议必须提供差错控制、可靠传输等功能来处理这种情况。

TCP 是一种面向连接的、可靠的、基于字节流的运输层通信协议。

在使用 TCP 协议时，在该协议传输模式中数据报成功发送给目标计算机后。TCP 会要求发送一个确认；如果在某个时限内没有收到确认，那么 TCP 将重新发送数据报。

另外，在传输的过程中，如果接收到无序、丢失以及被破坏的数据报，TCP 还可以将其恢复。

4. 传输控制协议 TCP 与 UDP 的区别？

答:

TCP 与 UDP 有很大区别，在功能上 TCP 也比 UDP 强得多。

最主要的区别是 TCP 是面向连接的。它更好地利用了套接字抽象模型，尽管套接字 API 也允许访问 UDP。数据从应用程序中以字节流的形式传给 TCP。而在 UDP 中，应用程序发送的是数据块。

字节流被 TCP 缓存，一直积累到足够的程度才进行一个发送操作。然后 TCP 构造一个报文段，报文段由缓存的数据和 TCP 报头前缀组成。为了保证可靠性，数据的每个字节都被一个数字所标识。由发送者按次序指定。序号和确认号用来确保传输的可靠性。此外，TCP 还使用了窗口的概念来调节数据流，根据内部定时器能重发数据，识别和丢弃重复的数据。

5. UDP 和 TCP 都使用端口号表示报文投递的目的地实体。至少给出两条理由，说明这些协议为什么要采用一个新的抽象 ID（端口号）。而不使用在设计这些协议时就已经存在的进程 ID。

答:

有三个理由：

第一， 进程 ID 是操作系统特有的，使用进程 ID 将使得这些协议依赖于操作系统；

第二，单个进程有可能建立多个通信通道，把单个进程 ID 用于目的地标识符就不能够对这些通道相互区别；

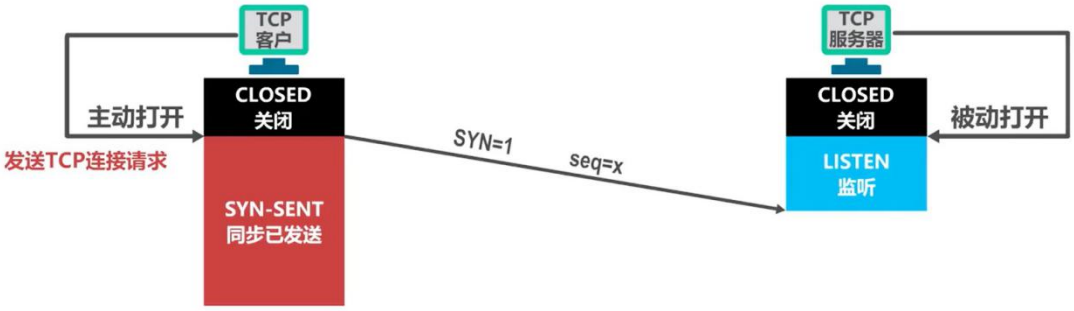
第三，让进程在端口上监听是可能的，但对进程 ID 监听是不可能的。

6. 将要相互通信的双方怎样进行建立 TCP 连接？在 TCP 报文段的首部中只有端口号而没有 IP 地址，当 TCP 将其报文段交给 IP 层时，IP 协议怎样知道目的 IP 地址呢？为什么把 IP 地址又称为“虚拟地址”，把 TCP 连接说成是“虚连接”？假设在建立连接时使用 2 次握手而非 3 次握手方案，即不再需要第 3 条报文，这时会发生什么情况？举例说明。

答：

（1）使用三次握手在将要相互通信的双方之间建立连接，过程如下：

① **第一次握手：**TCP 客户进程在打算建立 TCP 连接时，向 TCP 服务器进程发送 TCP 连接请求报文段，并进入同步已发送状态（SYN−SENT）。由于 TCP 连接建立是由 TCP 客户进程主动发起的，因此称为主动打开连接。 如下图所示。

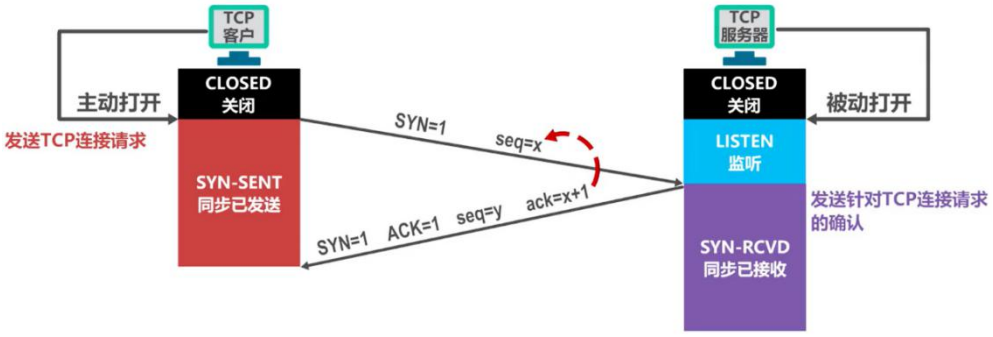


此时的 TCP 连接请求报文段的首部：

1、同步位 SYN 被置为 1（SYN = 1 表示连接请求或者连接同意，只在第一次和第二次握手中出现）。

2、序号字段 seq 被设置为一个初始值 x，作为 TCP 客户进程选择的初始序号。

② **第二次握手：**TCP 服务器收到 TCP 请求连接报文段后，如果同意建立连接，则向 TCP 客户进程发送 TCP 连接请求确认报文段，并进入同步已接收状态（SYN−RCVD）。如下图所示。



此时的 TCP 连接请求确认报文段的首部：

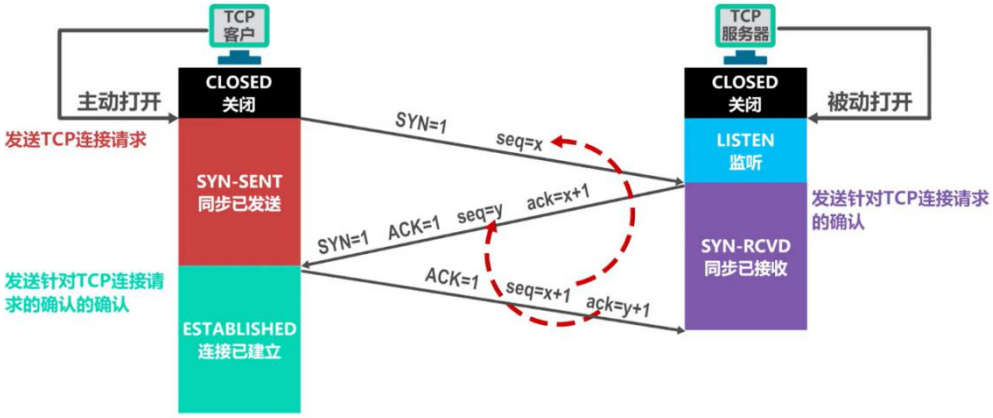
1、该报文段首部中的同步位 SYN 和确认位 ACK 都被置为 1，表示这是一个连接请求确认报文段。

2、序号段 seq 被设置为一个初始值 y，作为 TCP 服务器进程选择的初始序号。

3、确认号字段 ack 的值被设置成 x+1，这是对 TCP 客户进程所选择的初始序号 x 的确认。

请注意：TCP 规定 SYN = 1 的报文段不能携带数据，但要消耗掉一个序号。

③ **第三次握手：**TCP 客户进程收到 TCP 连接请求确认报文段后，还需要向 TCP 服务器进程发送一个普通的 TCP 确认报文段，并进入连接已建立（ESTAB-LISHED）状态。



此时的 TCP 确认报文段的首部：

1、该报文首部中的确认位 ACK 被置为 1，表明这是一个普通的 TCP 确认报文段。

2、确认号字段 ack 的值被设置成 y+1，这是对 TCP 服务器进程所选择的初始序号 y 的确认。

3、序号字段 seq 被设置为 x+1，这是因为第一次握手的序号 seq 为 x。

请注意，第三次握手是可以携带数据的，但如果该报文段不携带数据，则不消耗序号。

(2) 仅从 TCP 报文段的首部是无法得知目的 IP 地址，但是在 TCP 的伪首部中是有 IP 地址的，因此 TCP 知道目的 IP 地址是什么。**TCP 必须告诉 IP 层此报文段要发送给哪一个目的主机（给出其 IP 地址）。**

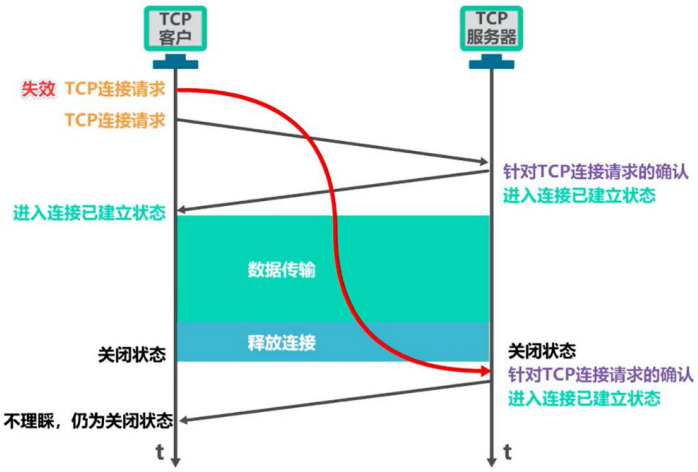
(3) 因为 **IP 地址是靠软件来维持的而不是硬件**。互联网也是虚拟的网络系统，它的通信系统是抽象的。虽然许多硬件和软件的组合看起来好像构成了一个很大的网络，但这样的大网络在实际中并不存在。这种虚拟网络的地址也是虚拟的，因此 IP 地址又称为“虚拟地址”。

同样，因为**在两个主机之间建立的 TCP 连接并非是真正的物理连接**。传输层并不知道所传送的报文段都经过哪些中间结点，在它看来，报文段好像是直接从发送端到了接收端。而在实际中，IP 数据报各自独立地选择路由，需要经过若干个中间结点（路由器）。

TCP 连接只是从传输层看来，好像在两个传输实体之间有一条连接，因此这条连接称之为“虚连接”。

(4) 现在把三次握手改成两次握手，可能发生死锁。

假设两次握手就可以建立连接，考虑下面这个例子。



TCP 客户发送了第一个 TCP 连接请求（第一次握手），但是该请求因为网络问题或者其他原因，导致经过很长一段时间才到达 TCP 服务器。在这段时间内，TCP 客户已经超时重传了一个新的 TCP 请求连接报文，并通过两次握手建立连接、之后再传输数据，并断开连接。

当第一个 TCP 连接请求到达了 TCP 服务器（上图中红色箭头），TCP 服务器进程随即发送 TCP 连接请求确认报文段（第二次握手），并进入连接已建立状态，等待 TCP 客户发来的数据。

而 TCP 客户进程收到连接请求的确认报文段后，并不想建立连接，因此并不理睬 TCP 连接请求确认报文段（第二次握手），不进入连接已建立状态，自然也不会给 TCP 服务器进程发送数据。

在这种情况下，TCP 服务器进程会持续挂起对 TCP 客户进程的连接，但是始终等不到数据，就会造成大量的资源浪费。

而使用三次握手就能很好的解决这个问题。

如果 TCP 客户并不理睬 TCP 连接请求确认报文段（第二次握手），那么 TCP 服务器就始终收不到确认报文段（第三次握手），就不会进入连接已建立状态，也就不会持续挂起对 TCP 客户进程的连接，造成资源的浪费。

7. 试述 UDP 检验和的计算过程。

答:

1、根据 IP 分组头中的信息计算出伪数据报头，跟 UDP 数据报头和数据一起进行 16 位的检验和计算。

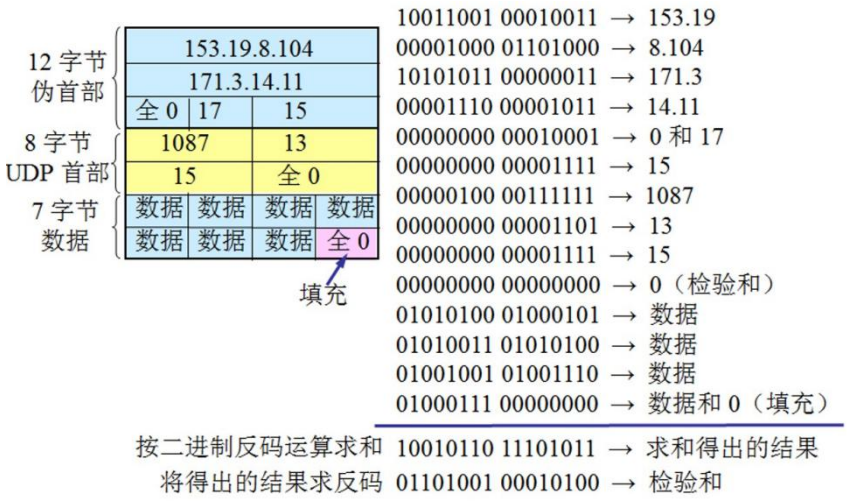
2、校验和字段全置为 0。

3、对数据部分为奇数字节的情况，增加全 0 使其成为偶数个字节后再行计算。检验和计算的方法如下。

4、伪首部 + 首部 + 数据部分进行反码算术运算。注意反码算术运算不是求反码后再求和，而是 0 和 0 相加为 0，0 和 1 相加是 1，1 和 1 相加是 0 但是要产生一个进位 1。

5、将计算出的结果填入校验和字段，该结果就是校验和。

整体过程如下所示：



8. 简述从发送方的高层协议通过 TCP 到达接收方的高层协议的数据传输的完整过程。

答:

(1) 发送方的高层协议发出一个数据"流"给它的 TCP 实体进行传输。

(2) **TCP 将此数据流分成段**。可能提供的传输措施包括全双工的定时重传、顺序传递、安全性指定和优先级指定、流量控制、错误检测等。然后将这段交给 IP。

(3) **IP 对这些报文段执行它的服务过程**，包括创建 IP 分组、数据报分割等，并在 IP 分组通过数据链路层和物理层后经过网络传给接收方的 IP。

(4) **接收方的 IP 在计算检验和以及可能的重组片段**的工作后，将分组中的报文段送给接收方的 TCP。

(5) 接收方的 TCP 完成它自己的服务，将报文段恢复成它原来的数据"流"形式，送给接收方的高层协议。

9.使用 TCP 对实时语音数据的传输有没有什么问题？使用 UDP 在传送数据文件时会有

什么问题?

答:

如果语音数据不是实时播放，就可以使用 TCP，因为 TCP 传输可靠。接收端用 TCP 将话音数据接收完毕后，可以再以后的任何时间进行播放。但如果是实时传输，则必须使用 UDP。

UDP 不保证可靠交付，但 UDP 比 TCP 的开销要小很多。因此，用它来传输文件可能会出现丢失数据、乱序的问题，但是速度要更快。只要应用程序接受这样的服务质量就可以使用 UDP。

10、简述 ICMP、DHCP、UDP 和 SMTP 的作用

答:

ICMP 的作用：网际控制报文协议，作用是检验传送数据时是否出现差错，确定发送错误的类型，并将出错信息告诉发送数据的主机。

DHCP 的作用：动态主机配置协议，作用是对加入网络的计算机进行 IP 地址与相关信息的配置。

UDP 的作用：用户数据报协议，作用是提供一种虽无连接、不可靠，但拥堵少、时延短的数据报服务。

STMP 的作用：简答邮件传送协议，作用是传送邮件。

六、应用层

1. SMTP 协议的用途是什么？

答:

简单文件传送协议 SMTP 是最常使用的电子邮件发送协议。

SMTP 通过 TCP 协议在电子邮件应用程序与邮件服务器之间建立传输连接，然后传输电子邮件，并在邮件传输完毕后关闭连接。

2. 为什么 FTP 协议要使用两个独立的连接，即控制连接和数据连接？

答:

在 FTP 协议的实现中，客户与服务器之间采用了两条传输连接，其中控**制连接用于传输各种 FTP 命令，而数据连接用于文件的传送。**

之所以这样设计，是因为使用两条独立的连接可以使 FTP 协议变得**更加简单、更容易实现、更有效率**。同时在文件传输过程中，还可以利用控制连接控制传输过程，如客户可以请求终止传输。

3. DNS 使用 UDP 而不是 TCP，如果一个 DNS 分组丢失了，没有自动回复，这会引起问题吗？如果会。如何解决？

答:

DNS 使用传输层的 UDP 而不是 TCP 的原因有两个：

1、DNS 解析过程可能会发生多次请求，若使用 **TCP 则需要多次建立连接，开销大**；

2、**DNS 不需要使用 TCP 在发生传输错误时执行的自动重传功能**。

解决方法：对于 DNS 服务器的访问，多次 DNS 请求都返回相同的结果，即做多次和做一次的效果一样。因此 DNS 操作可以重复执行。当一个进程做一个 DNS 请求时，它启动个定时器。如果定时器计满而未收到回复，那就再请求一次。

4. Internet 域名系统的主要用途是什么？它的交互过程由哪三种实体组成？试说明它们之间的交互过程。

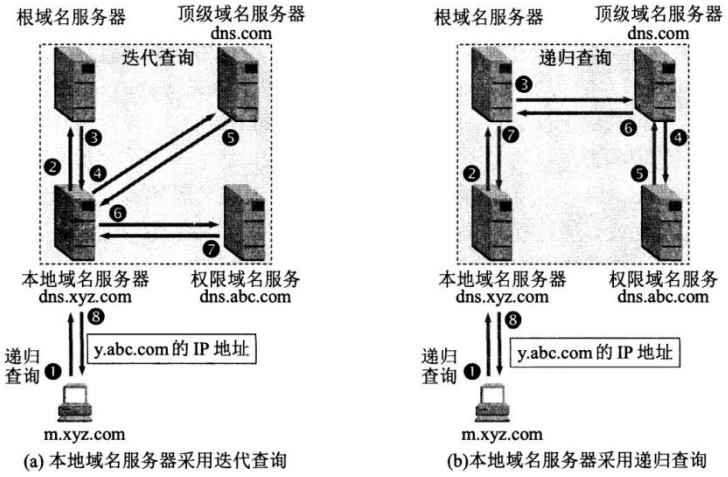
答:

Internet 域名系统就是因特网使用的命名系统，用来把便于人们使用的域名转换为 IP 地址。它的交互过程由主机、本地域名服务器和根域名服务器共同完成。

交互过程如下：

1、当客户端需要域名解析时，通过本机的域名解析器构造一个域名报文，发往本地域名服务器。域名请求报文指明了所要求的域名解析方法，包括递归解析与反复解析。

2、当本地域名服务器收到域名请求报文时，首先检查所要求的域名是否在管辖范围内。若是，便进行本地解析；否则查高速缓存，看最近是否解析过；若是，则将查到的 IP 地址报告本地主机的地址解析器；否则，访问远程域名服务器，使用递归查询或者迭代查询的方式，向根域名服务器、顶级域名服务器和权限域名服务器发出请求。递归查询和迭代查询的方式如下图所示。



5. 假定一个用户正在通过 HTTP 下载一个网页，该网页没有内嵌的对象，TCP 协议的慢启动窗口门限值为 30 个分组的大小。该网页长度为 14 个分组的大小，从用户主机到 www 服务器之间的往返时延 RTT 为 1s。不考虑其他损失因素（例如，域名解析、分组丢失、报文段处理），那么用户下载该网页大约需要多少时间?

答:

用户下载该网页的过程如下:

第 1 秒 TCP 三次握手的前两次握手建立;

第 2 秒 拥塞窗口值为 1 个分组的大小，发送第三次握手时，用户携带发送 HTTP 请求，并且收到第 1 个分组（网页的第 1 个分组）;

第 3 秒 拥塞窗口值为 2 个分组的大小，用户收到 2 个分组（网页的第 2—3 个分组）;

第 4 秒 拥塞窗口值为 4 个分组的大小，用户收到 4 个分组（网页的第 4—7 个分组）;

第 5 秒 拥塞窗口值为 8 个分组的大小，用户收到最后的 7 个分组（网页的第 8—14 个分组）。

因此，用户下载该网页的时间大约为 5 秒。

7. MIME 的用途是什么?

答:

MIME 的英文全称是"Multipurpose Internet Email Extension"多功能 Internet 邮件扩充服务，它是一种多用途网际邮件扩充协议，最初在 1992 年应用于电子邮件系统。但后来也应用到浏览器中，服务器会将它们发送的多媒体数据的类型通知浏览器，而通知手段就是说明该多媒体数据的 MIME 类型，从而让浏览器知道接收到的信息哪些是 MP3 文件，哪些是 Shockwave 文件等等。服务器将 MIME 标志符放入传送的数据中来通知浏览器使用哪种插件读取相关文件。

浏览器接收到文件后，会进入插件系统进行查找。查找出哪种插件可以识别读取接收到的文件。如果浏览器不清楚调用哪种插件系统，它会通知用户缺少某插件，或者直接选择某现有插件来试图读取接收到的文件，后者可能会导致系统的崩溃。传输的信息中缺少 MIME

标识可能导致的情况很难估计，某些计算机系统可能不会出现故障，但某些计算机系统可能就会因此而崩溃。

10. 什么是域名解析，域名解析中采取了什么措施提高效率？对同一个域名向 DNS 服务器发出多次的 DNS 请求报文后，得到 IP 地址都不一样，可能吗？为什么？

答:

DNS 是一个联机分布式数据库系统，负责主机名和 IP 地址之间的转换，需要进行域名查询的机器主动发起域名解析请求，域名服务器则随时准备做出响应。域名服务器的数据库中存放着它所管辖范围的主机名（域名）和 IP 地址之间的映射表，域名服务器之间又可以相互联络和协作，以便分布在 Internet 各个域名服务器数据库中的域名都能被有效地搜索，从而实现主机名与 IP 地址的映射。

为了提高解析效率，使用了域名缓存技术。在服务器、主机中设置一个专用的内存缓冲区。服务器用来存放近期解析过的域名及其对应的 IP 地址的映射。如果域名解析过程中在数据库中搜索不到相关记录，使用域名缓存进行解析，如果域名缓存也解析不到，再访问非本地的其他域名服务器。主机系统启动时解析器软件从本地域名服务器获取一个完整的域名—IP 地址映射数据库的副本，并维护一个近期使用的域名 IP 地址映射的缓冲区。

对同一个域名向 DNS 服务器发出多次的 DNS 请求报文后，得到 IP 地址都不一样是可能的。例如对某被访问频率很高的域名 www.baidu.com 进行解析时，**为了使服务器的负载得到平衡，网站就设有好几个计算机同时都运行同样的服务器软件。**这些计算机的 IP 地址是不一样的，但它们的域名却是相同的。这样，第一个访问该网址的就得到第一个计算机的 IP 地址，而第二个访问者就得到第二个计算机的 IP 地址等等。不会使某个计算机的负荷太大。

11. 试述 FTP 的工作原理。

答:

文件传送协议 FTP (File Transfer Protocol) 是互联网上使用得最广泛的文件传送协议。FTP 提供交互式的访问，允许客户指明文件的类型与格式（如指明是否使用 ASCII 码），并允许文件具有存取权限（如访问文件的用户必须经过授权，并输入有效的口令）。

FTP 工作在 TCP/IP 模型的应用层，基于的传输协议是 TCP，使用客户/服务器模型，FTP 客户端和服务器之间的连接是可靠的，面向连接的，为数据的传输提供了可靠的保证。

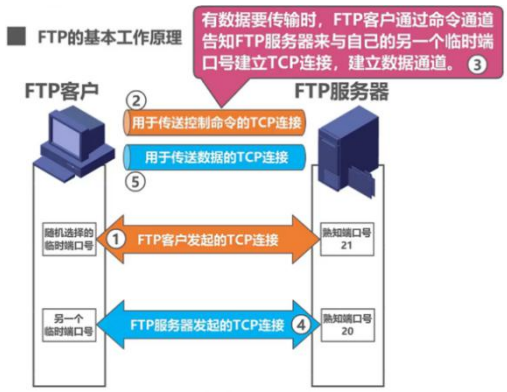
FTP 的服务器进程由主进程（负责接受新的请求）与若干个从属进程（负责处理单个请求）组成。

主进程的工作步骤如下：

①打开端口控制端口 21，使客户进程能够连接上；

②等待客户进程发出连接请求；

③启动从属进程（从属进程包括控制进程和数据传输进程）来处理客户进程发来的请求，如下图所示，从属进程对客户进程的请求处理完毕后即终止；



④回到等待状态，继续接受其他客户进程发来的请求。

【注意】主进程与从属进程的处理是并发地进行。

12．简述 HTTP 协议的特点和工作过程。

答:

HTTP（Hyper Text Transport Protocol，超文本传输协议）是传送信息的协议，从层次的角度看，HTTP 是面向事务的应用层协议。虽然 HTTP 使用了 TCP，但 HTTP 协议本身是无连接的，也是无状态的，这样可使读取网页信息完成得较迅速。

HTTP 的工作流程如下所示:

1、用户在点击鼠标链接某个万维网文档时，HTTP 协议首先要和服务器建立 TCP 连接。这需要使用三报文握手。

2、当建立 TCP 连接的三报文握手的前两部分完成后(即经过了一个 RTT 时间后)，万维网客户就把 HTTP 请求报文，作为建立 TCP 连接的三报文握手中的第三个报文的数据，发送给万维网服务器。

3、服务器收到 HTTP 请求报文后，就把所请求的文档作为响应报文返回给客户。

4、断开连接（非持久连接）/不断开连接，继续等待下一个请求（持久连接）。