**ARP协议的工作原理**：

1. 首先，每个主机都自己的ARP缓冲区中建立一个ARP列表，以表示IP地址和MAC地址之间的对应关系。
2. 当源主机发送数据报，首先检查ARP列表中是否有对应的IP地址的目的主机的MAC地址，如果有则直接发送数据。如果没有，就向本网段的所有主机发送ARP数据包，该数据包包括的内容有：源主机IP地址，源主机MAC地址，目的主机的IP地址
3. 当本网路的所有住居收到该ARP数据包时，首先检查数据包中的目的IP地址是否是自己的，如果不是，则忽略该数据包；如果是，则首先从数据包中取出源主机的IP和MAC地址写入到ARP列表中；如果存在则覆盖，然后将自己的MAC地址写入ARP响应包中，告诉源主机自己是它想要找的MAC地址。
4. 源主机收到ARP响应包后，将目的主机的IP和MAC地址写入ARP列表，并利用此信息发送数据。如果源主机一直没有收到ARP响应数据包，表示ARP查询失败。

**各种协议介绍**：

**ICMP协议**：因特网控制报文协议。ICMP是Internet Control Message Protocol，因特网控制报文协议。它是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、路由器是否可用等网络本身的消息。这些控制消息虽然并不传输用户数据，但是对于用户数据的传递起着重要的作用。ICMP报文有两种：差错报告报文和询问报文。

**FTP协议**：是TCP/IP协议族中的一个用来在客户机与服务器之间进行简单文件传输的协议，提供不复杂、开销不大的文件传输服务。

**HTTP协议**：超文本传输协议，是一个属于应用层的面向对象的协议，由于其简捷、快速的方式，适用于分布式超媒体信息系统。

**NAT协议**：网络地址转换属接入广域网(WAN)技术，是一种将私有（保留）地址转化为合法IP地址的转换技术，

**DHCP协议**：动态主机配置协议，一个局域网的网络协议，使用UDP协议工作，用途：给内部网络或网络服务供应商自动分配IP地址，给用户或者内部网络管理员作为对所有计算机作中央管理的手段。

**容易混淆的协议所在层**：

**ARP**：属于网络层，工作在数据链路层。

**ICMP**：网络层。

**在浏览器中输入www.baidu.com后执行的全部过程**：

1. 客户端浏览器通过DNS解析到www.baidu.com的IP地址220.181.27.48，通过这个IP地址找到客户端到服务器的路径。客户端浏览器发起一个HTTP会话到220.161.27.48，然后通过TCP进行封装数据包，输入到网络层。
2. 在客户端的传输层，把HTTP会话请求分成报文段，添加源和目的端口，如服务器使用80端口监听客户端的请求，客户端由系统随机选择一个端口如5000，与服务器进行交换，服务器把相应的请求返回给客户端的5000端口。然后使用IP层的IP地址查找目的端。
3. 客户端的网络层不用不用关心应用层或者传输层的东西，主要做的是通过查找路由表确定如何达到服务器，期间可能经过多个路由器，这些都是由路由器完成的工作。
4. 客户端的链路层，数据包通过链路层发送到路由器，通过ARP协议查找给定IP地址的MAC地址，然后通过发送IP数据包达到服务器的地址。

TCP三次握手和四次挥手的全过程：

**三次握手**：

**第一次握手**：客户端发送syn包到服务器，并进入SYN\_SEND状态，等待服务器确认。

**第二次握手**：服务端收到syn包，必须确认客户的SYN，同时自己也发送一个SYN包，此时服务其进入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，此包发送完毕，，客户端和服务端都进入ESTABLISHED状态，完成三次握手。

**四次挥手**：

**第一次挥手**：主动方关闭发送一个FIN

**第二次挥手**：服务器收到FIN包后，发送一个ACK给对方，确认序号为收到序号+1

**第三次挥手**：服务端发送FIN，用来关闭服务端到客户端的数据传送，也就是告诉客户端，我的数据发送完了，不会再给你发数据了。

**第四次挥手**：客户端受到FIN，发送一个ACK给被动关闭方。

**TCP和UDP的区别**：

1、TCP提供面向连接的、可靠的数据流传输，而UDP提供的是非面向连接的、不可靠的数据流传输。

2、TCP传输单位称为TCP报文段，UDP传输单位称为用户数据报。

TCP注重数据安全性，UDP数据传输快，因为不需要连接等待，少了许多操作，但是其安全性却一般

DNS域名系统，简单描述其工作原理。

**面向连接和面向非连接的服务的特点是什么**：

面向连接的服务，通信双方在进行通信之前，要先在双方建立一个完整的可以彼此沟通的通道，在通信过程中，整个连接的情况一直可以被实时地监控和管理。

非面向连接的服务，不需要预先建立一个联络两个通信结点的连接，需要通信的时候，发送结点就可以往网络上发送信息，让信息主动地在网络上船，一般在传输的过程中加以监控。

**交换机**：类似路由的转发功能，工作在链路层。交换机拥有一条高带宽的背部总线和内部交换矩阵。交换机的所有端口都挂接在这条背部总线上，当控制电路收到数据包以后，处理端口会查找内存中的地址对照表以确定目的MAC的网卡挂接在哪个端口，通过内部交换矩阵迅速将数据包传送到目的端口。目的MAC若不存在，交换机广播所有端口，接收端口回应后交换机会学习新的地址，并把它添加如内部地址表中。

路由器：提供路由选择和转发功能。路由选择：确定源地址到目的地址进过的路由。转发：将数据包发送到对应的端口。

**网关**：

**IP层为什么不对数据部分进行差错检验**：

网路层是尽最大努力完整的传输数据包，差错检测已由数据链路层实现，IP层没必要进行依次较验。

**优点**：不负责差错检测和纠错，可获得较高的传输性能。

**缺点**：IP不负责差错检验和检测，那么错误只能在传输层或应用层被发现，是纠正错误的时间增加了。

**各层重要知识点**：

**应用层**：HTTP，FTP，DNS，P2P

**传输层**：TCP和UDP

**网路层**：IP，ICMP，路由选择协议；DHCP协议

**链路层**：ARP协议，MAC地址

**物理层**：

**DNS工作原理：**

假设输入mail.163.com。

1. 主机先查找自己的**缓存文件**，如果有mail.163.com的信息，则返回，否则递归查找下一步。
2. 主机向**本地域名服务器**进行查询，如果该服务器有mail.163.com的IP信息，则返回；否则进行下一步。
3. 该DNS服务器向**根域名服务器**发起查询。根域名服务器告诉本地域名服务器下一次应查询dns.com的**顶级域名服务器**。
4. **本地域名服务器**向dns.com顶级域名服务器进行查询，如果该服务器有mail.163.com的IP信息，如有返回；否则下一步。
5. dns.com顶级域名服务器向本地域名服务器指出向dns.163.com发起查询，网易公司的DNS服务器有他的IP信息，然后发给本地域名服务器。
6. 本地域名服务器收到解析的内容，送回给主机。
7. 主机获得IP信息。

**DNS记录和报文**：

Type=A，提供主机名到IP地址的映射

Type=NS，则Name是一个域，而Value是个知道如何获得该域中主机IP地址的权威DNS服务器的主机名

Type=CNAME，则value是别名为Name的主机对应的规范主机名。

Type=MX，则Value是个别名为Name的邮件服务器的规范主机名。

TCP的可靠性如何保证：

TCP为了保证不发生丢包，就给每个包一个序号，同时序号也保证了传送到接收端实体的包按序接收。然后接收端实体对以成功收到的字节发回一个相应的确认；如果发送端实体在合理的往返时延内为收到确认，那么对应的数据会被重传。

DHCP协议：动态主机配置协议。主机连接进一个网络时，需要一个IP地址。DHCP允许主机自动获取一个IP地址。这个IP地址可以是同一个，或者仅被分配一个临时的IP地址。

子网掩码的作用：将IP地址分为网路地址和主机地址。

**应用层**：是网路应用程序以及它们的应用层协议存留的地方。

**运输层**：在应用程序端点之间传送应用层报文。

**网络层**：负责将数据报从一台主机移动到另一台主机。

**链路层**：负责将帧从网络路径上的一个结点移动到另一个结点。

**物理层**：将帧中的一个一个比特从一个结点移动到下一个结点。

**网桥的作用**：用于连接两个局域网。

**防火墙的端口防护是指**：

指通过对防火墙的端口开关的设置，关闭一些非必需端口，达到一定安全防护目的的行为。

**IP、TCP和UDP数据包的格式**。

HTTP协议中post和get的区别：

1. get是从服务器上获取数据，post是向服务器传送数据。
2. get是把参数放到URL中，post将数据放在entity body中
3. get传送的数据量小，不能大于2KB；post传送的数据量较大，一般被默认为不受限制。

**http协议包括哪些请求**：

get：请求读取由url所标志的信息。

post：给服务器添加信息。

put：在给定url下存储一个文档。

delete：删除给定url所标志的资源。

**运输层协议与网络层协议的区别**：

网路层协议负责提供主机间的逻辑通信；

运输层协议负责的是提供进程间的逻辑通信。

**每个路由器在寻找路由时需要知道哪5部分的信息**：

目的地址：报文发送的目的地址

邻站的确定：

路由的发现：

选择路由：

保持路由信息：

**路由表是做什么用的**？

路由表是用来决定如何将一个数据包从一个子网传送到另一个子网，换句话来说决定从一个网卡接收到的包应该送到哪一个网卡上去。当路由器从一个网卡接收到一个包时，它扫描路由表的每一行，用里面的子网掩码与数据包中的目标IP电子hi做逻辑与运算，找出目标网络号。如果得出的结果网络号与者一行的网络号相同，就将这条路由表留下了作为备用路由。如果已经有了备用路由，就将这两条路由里将网络号最长的留下来，另一条丢掉。如此接着扫描下一行直到结束。如果扫描结束没有找到任何路由，就用默认的路由。确定路由后，直接将数据包送到对应的网卡上去。在具体的实现中，路由表可能包含更多的信息作为路由算法的细节所用。

**网络接口卡的功能**：

1. 进行串行/并行转换
2. 对数据进行缓存
3. 在计算机的操作系统安装设备驱动程序
4. 实现以太网协议。

**DHCP协议：**

DHCP服务器发现：使用广播目的地址255.255.255.255并且使用本主机的源地址0.0.0.0来发送DHCP发现报文。

DHCP服务器提供：用一个DHCP提供报文向客户作出相应，仍然使用IP广播地址255.255.255.255。可能有几个DHCP服务器，该客户也许会发现他处于能在几个提供者之间选择的优越位置。报文包含有收到发现报文的事务ID、向客户推荐的IP地址、网络掩码以及IP地址租用期。

DHCP请求：新到达的客户从一个或多个服务器提供选择一个，并向选中的服务器提供以DHCP请求报文进行相应，回显配置参数。

DHCP ACK：服务器用DHCP ACK报文对DHCP的请求报文进行相应，真是所要求的参数。

注：所有过程目的IP地址都是广播地址。

IPv4是数据包格式：

1. 版本号
2. 首部长度：数据包包含一些可变数量的选项。
3. 服务类型：
4. 数据报长度：IP数据报的总长度，以字节记。
5. 标识、标志、片偏移量。
6. 寿命
7. 协议
8. 首部检验和
9. 源和目的IP地址
10. 选项
11. 数据：有效载荷

IPv6数据报格式：

扩大的地址容量，简化高效的40字节首部。留标签和优先级

1、IPv6不允许在中间路由器上进行分片与重新组装。这种操作只能在源与目的上执行。

2、首部检验和

3、选项：并没有消失，而是出现在下一个首部出现的字段。

4、下一个首部：标识数据报中的内容需要交付给哪个协议。