**简述2种地址解析的方法的原理。**

答：(1)查表(Table lookup)

地址联编或映射信息存储在内存当中的一张表里，当软件要解析一个地址时，可在其中找到所需结果。查表方法需要一张包含地址联编信息的表，表中的每一项是一个二元组(P，H)，P是协议地址,H是指等价的物理地址。每一项对应于网络中的一个站。项包含两个域,一个是站的IP地址，另一个是站的硬件地址。给出下一站的IP地址N，软件就开始搜索表，直到发现某一项的IP地址域与N匹配，则该项的硬件地址域中的值被输出。

(2)相近形式计算

仔细地为每一台计算机挑选协议地址，使得每台计算机的硬件地址可通过简单的布尔和算术运算得出它的协议地址。当一台计算机连入一个动态编址的网络时，该网的管理员必须为它挑选一个硬件地址和一个IP地址，并且所挑选的两个地址值应使地址解析非常简单。

**简述ARP发送和接收端的操作过程。**

答：第1步：通讯时主机A确定主机B的IP地址后A主机A在自己的本地ARP缓存中检查主机B的匹配MAC地址。

第2步：如果主机A在ARP缓存中没有找到映射，它将询问主机B的IP地址的硬件地址，从而将ARP请求帧广播到本地网络上的所有主机。源主机A的IP地址和MAC地址都包括在ARP请求中。本地网络上的每台主机都接收到ARP请求并且检查是否与自己的IP地址匹配。如果主机发现请求的IP地址与自己的IP地址不匹配，它将丢弃ARP请求。

第3步：主机B确定ARP请求中的IP地址与自己的IP地址匹配，则将主机A的IP地址和MAC地址映射添加到本地ARP缓存中。

第4步：主机B将包含其MAC地址的ARP单播回复主机A。

第5步：当主机A收到从主机B发来的ARP回复消息时，会用主机B的IP和MAC地址映射更新ARP缓存。本机缓存有生存期（180S），生存期结束后，将再次重复上面的过程。主机B的MAC地址一旦确定，主机A就能向主机B发送IP通信了。

**ICMP对IP数据传输采取了哪些控制措施？**

答：



**理解TraceRoute和PING的原理。**

答：TraceRoute:是利用ICMP及IPheader的TTL (Time To Live）。首先，traceroute送出一个TTL是1的IP datagram到目的地，当路径上的第一个路由器收到这个datagram时，它将TTL减1。此时，TTL变为0了，所以该路由器会将此datagram丢掉，并送回一个「ICMPtime exceeded」消息，traceroute 收到这个消息后，便知道这个路由器存在于这个路径上，接着traceroute再送出另一个TTL是2的datagram，发现第2个路由器...... traceroute每次将送出的datagram的TTL加1来发现另一个路由器，这个重复的动作一直持续到某个datagram 抵达目的地。

Ping:使用ICMP回应请求和回应应答报文来实现。当调用ping程序时，它发送一个包含ICMP回应请求的报文给目的地，然后等待一段很短的时间。如果没有收到应答，则重新传送请求。如果重传的请求仍没有收到应答（或收到一个ICMP目的不可达报文）, ping声称该远程机器为不可达。远端主机上的ICMP软件应答该回应请求报文。按照协议只要收到回应请求，ICMP软件必须发送回应应答。

**考虑如何利用ICMP协议对一个网络上的时延性能进行监控？**

答：使用ping命令向目标主机发送ICMP回显请求，即ping目标主机的IP地址。

目标主机接收到ping请求后会自动发送ICMP回显响应，即ping请求的回复。通过记录ping请求发出的时间戳和收到回复的时间戳，可以计算出从源主机到目标主机的往返时延（Round Trip Time，简称RTT）。分析保存的RTT数据，可以得到网络的时延性能情况，如平均时延、最大时延、最小时延、丢包率等指标。

**TCP如何考虑数据传输连接的建立和拆除？**

答：TCP使用三次握手建立连接，四次挥手终止连接。

在建立连接时，客户端首先向服务器发送一个SYN(Synchronize Sequence Numbers)包，其中包含一个随机数x用于加密数据，然后等待服务器的回应。服务器接收到SYN包后，向客户端回应SYN+ACK(Synchronize and Acknowledgment)，其中包含一个随机数y和确认号a=x+1，表示已经接收到了客户端的SYN包，并准备好建立连接。客户端最后发送ACK(Acknowledgment)包，其中包含序列号b=y+1，表示已经收到了服务器的SYN+ACK包，并同意建立连接。此时连接建立完成，双方开始传输数据。

在终止连接时，一方（通常是客户端）发送FIN(Finish)包给对方，表示已经没有更多数据要发送。对方接收到FIN包后，回复ACK包进行确认，并进入CLOSE\_WAIT状态，表示自己可以继续发送数据，但不再接收数据。一段时间后，对方也发送FIN包，另一方回复ACK包确认，进入TIME\_WAIT状态，等待两个MSL(Maximum Segment Lifetime)时间（即为两倍的最长报文寿命），以确保对方已经收到了ACK确认包，然后关闭连接。

**TCP如何考虑流量控制和拥塞控制？**

答：流量控制：TCP发送方根据接收方的处理能力，动态调整自己的传输速率。TCP双方在建立连接时，会协商一个窗口大小（Window Size），即发送方可以连续发送多少个字节的数据，而不需要等待对方的ACK确认。接收方可以通过调整窗口大小来告知发送方自己的处理能力，从而限制发送方的传输速率。如果发送方发送过快而导致接收方缓冲区溢出，则接收方可以减小窗口大小或者发送一个零窗口通知（Zero Window），暂停发送直到缓冲区有空间。

拥塞控制：TCP根据网络的负载情况，动态调整自己的传输速率，以避免网络拥塞。TCP通过一系列算法来检测网络拥塞的情况，包括慢启动、拥塞避免、快重传、快恢复等。当网络拥塞时，TCP会降低自己的传输速率，以减轻网络负荷，并通过发送一些特殊的报文来告诉对方网络拥塞的情况。如果对方也检测到网络拥塞，则会协同减少传输速率，从而避免网络拥塞的进一步加剧。