ARQ=Automatic Repeat Request 自动重发请求

APR=Address Resolution Protocol 地址解析协议 负责将IP地址映射到MAC地址上

LLC=Logical Link Control 逻辑链路控制 包装从网络层取下来的数据

MAC=Media Access Control 如何分配信道

**1 请说明EthernetMAC地址与网络层的IP地址有什么区别？**

区别：

1. 对于网络上的某一设备，如一台计算机或一台路由器，其IP地址可变（但必须唯一），而MAC地址不可变。我们可以根据需要给一台主机指定任意的IP地址，如我们可以给局域网上的某台计算机分配IP地址为192.168.0.112 ，也可以将它改成192.168.0.200。而任一网络设备（如网卡，路由器）一旦生产出来以后，其MAC地址永远唯一且不能由用户改变。  
2. 长度不同。IP地址为32位，MAC地址为48位。  
3. 分配依据不同。IP地址的分配是基于网络拓朴，MAC地址的分配是基于制造商。  
4. 寻址协议层不同。IP地址应用于OSI第三层，即网络层，而MAC地址应用在OSI第二层，即数据链路层。 数据链路层协议可以使数据从一个节点传递到相同链路的另一个节点上（通过MAC地址），而网络层协议使数据可以从一个网络传递到另一个网络上（ARP根据目的IP地址，找到中间节点的MAC地址，通过中间节点传送，从而最终到达目的网络）。

关于MAC地址和IP地址：

MAC地址即网卡的物理地址是固化在网卡上的，是要在一个局域网内部找到这台计算机。

IP地址即网络层地址是动态的，标识所用的是什么网络，地区，运营商。

IP地址是有限的。所以要动态分配。上网时有个IP地址动态分配服务器（DHCP协议服务器）。计算机向网络发送DCHP请求消息，申请IP地址。DHCP服务器把IP地址回送给计算机，回送时需要区分不同的主机，需要一个办法唯一标识计算机，所以需要MAC地址，谁申请，谁获得。

假设没有IP地址，因为MAC地址是计算机的唯一标识，则路由器中的转发表要存所有计算机的MAC地址和地区信息；且当一台计算机移动位置，所有关于它的信息都要变化。存储冗余且繁杂，查找地址的计算量巨大，有变动时修改麻烦。所以需要IP地址，可以与子网对应，路由器中只需要存子网内部的记录即可。

**2 请说明数据链路层是如何进行差错控制和流量控制的？**

*参考网址：http://blog.csdn.net/xcl119xcl/article/details/6732960*

（一）差错控制

接收方通过对差错编码(奇偶校验码或CRC码)的检查，可以判定一帧在传输过程中是否发生了差错。

物理信道的突发噪声可能完全“淹没”一帧，即使得整个数据帧或反馈信息帧丢失，这将导致发送方永远收不到接受方发来的信息，从而使传输过程停滞。为了避免出现这种情况，通常引入计时器(Timer)

由于同一帧数据可能被重复发送多次，就可能引起接收方多次收到同一帧并将其递交给网络层的危险。帧编号

空闲RQ：[发送窗口](http://baike.baidu.com/view/497294.htm" \t "_blank)=1，接收窗口=1p

Go-back-N：发送窗口>1，接收窗口=1

GO-DACK-N策略的基本原理是，当接收方检测出失序的信息帧后，要求发送方重发最后一个正确接收的信息帧之后的所有未被确认的帧；或者当发送方发送了N个帧后，若发现该N帧的前一个帧在计时器超时后仍未返回其确认信息，则该帧被判为出错或丢失，此时发送方就不得不重新发送出错帧及其后的N帧。这就是GO-DACK-N(退回N)法名称的由来。因为，对接收方来说，由于这一帧出错，就不能以正常的序号向它的高层递交数据，对其后发送来的N帧也可能都不能接收而丢弃。GO-DACK-N法操作过程如图3.13所示。图中假定发送完8号帧后，发现2号帧的确认返回在计时器超时后还未收到，则发送方只能退回从2号帧开始重发。

---------------------------------------------------------------------------------------------------------------------------

选择重发：发送窗口>1，接收窗口>1

当接收方发现某帧出错后，其后继续送来的正确的帧虽然不能立即递交给接收方的高层，但接收方仍可收下来，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高层。这种方法称为选择重发(SELECTICE REPEAT)，其工作过程如图3.14所示。图中2号帧的否认返回信息NAK2要求发送方选择重发2号帧。显然，选择重发减少了浪费，但要求接收方有足够大的缓冲区空间。

-----------------------------------------------------------------------------------------------------------------------------

若帧序号采用3位[二进制编码](http://baike.baidu.com/view/802204.htm" \t "_blank)，则最大序号为SMAX=2^3－1=7。对于有序接收方式，[发送窗口](http://baike.baidu.com/view/497294.htm" \t "_blank)最大尺寸选为SMAX；对于无序接收方式，发送窗口最大尺寸至多是序号范围的一半。管理超时控制的计时器应等于发送缓冲器数，而不是序号空间的大小。实际上，每一个缓冲器应对应一个计时器，当计时器超时时，该对应缓冲器的内容重发。按收方必须设置的缓冲器数应该等于接收窗口尺寸，而不是序号空间的大小。

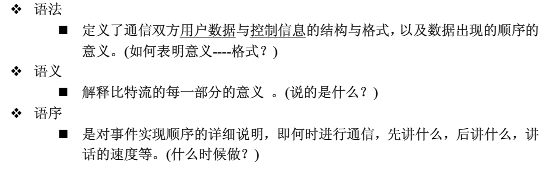
（二）流量控制

基于反馈的流量控制

基于速率的流量控制

**3 说明你对计算机网络协议的理解？要定义一个计算机网络协议，需要哪些内容？**

网络协议为[计算机网络](http://baike.baidu.com/view/25482.htm" \t "_blank)中进行数据交换而建立的规则、标准或约定的集合。



**4 为什么需要MAC层？**

用来确定多路访问信道下一个使用者

**5 说明以下命令的作用**

ipconfig：ipconfig实用程序可用于显示当前的TCP/IP配置的设置值。

route：Route就是用来显示、人工添加和修改[路由表](http://baike.baidu.com/view/149989.htm" \t "_blank)项目的。

ping：用于确定网络的连通性。ping能够以毫秒为单位显示发送请求到返回应答之间的时间量。ping还能显示TTL（Time To Live，生存时间）值，通过TTL值可以推算数据包通过了多少个路由器。

traceroute：道信息从你的计算机到互联网另一端的主机是走的什么路径

netstat：了解网络当前的状态。显示活动的TCP连接、计算机侦听的端口、以太网统计信息、IP路由表、IPv4统计信息（对于IP、ICMP、TCP和UDP协议）以及IPv6统计信息（对于IPv6、ICMPv6、通过IPv6的TCP以及UDP协议）。使用时如果不带参数，netstat显示活动的TCP连接

**6 各层协议举例**

属于物理层定义的典型规范代表包括：EIA/TIA [RS-232](https://www.baidu.com/s?wd=RS-232&tn=44039180_cpr&fenlei=mv6quAkxTZn0IZRqIHckPjm4nH00T1YLnAN9nj9buHmLnvRYuW640AP8IA3qPjfsn1bkrjKxmLKz0ZNzUjdCIZwsrBtEXh9GuA7EQhF9pywdQhPEUiqkIyN1IA-EUBtvn1nLPHm1P0" \t "_blank)、EIA/TIA RS-449、[V.35](https://www.baidu.com/s?wd=V.35&tn=44039180_cpr&fenlei=mv6quAkxTZn0IZRqIHckPjm4nH00T1YLnAN9nj9buHmLnvRYuW640AP8IA3qPjfsn1bkrjKxmLKz0ZNzUjdCIZwsrBtEXh9GuA7EQhF9pywdQhPEUiqkIyN1IA-EUBtvn1nLPHm1P0" \t "_blank)、[RJ-45](https://www.baidu.com/s?wd=RJ-45&tn=44039180_cpr&fenlei=mv6quAkxTZn0IZRqIHckPjm4nH00T1YLnAN9nj9buHmLnvRYuW640AP8IA3qPjfsn1bkrjKxmLKz0ZNzUjdCIZwsrBtEXh9GuA7EQhF9pywdQhPEUiqkIyN1IA-EUBtvn1nLPHm1P0" \t "_blank)等。

数据链路层协议的代表包括：SDLC、HDLC、PPP、STP、帧中继等。

网络层协议的代表包括：IP、IPX、RIP、OSPF等。

传输层协议的代表包括：TCP、UDP、SPX等。

应用层协议的代表包括：Telnet、FTP、HTTP、SNMP等

上课宣称有10分：

以太网标准：

经典以太网MAC子层协议：

前导码（8位）

标识目的地址（6位）：若目标地址第一位是0，则表示是一个普通地址；如果是1，则表示这是一个组地址。

组播：往一组地址的发送行为。广播：由全1组成的特殊地址保留用作广播。

源地址（6位）：站的源地址具有全球唯一性，地址字段的前3个字节用作该站锁在的组织唯一标识符。

类型或长度（2位）

数据字段（DATA 0-1500）

填充字段（0-46）：为了更加容易地区分有效帧和垃圾数据，以太网要求有效帧必须至少64字节长。如果一个站试图传送非常短的帧，则可以想象，虽然发生了冲突，但是在突发噪声回到发送方（2t）之前，传送已经结束。

校验和（4）

IP包头：

*参考网址：http://www.cnblogs.com/sunev/archive/2012/06/23/2559389.html*

**IP包头**

IP包头占有20个字节，即：

　　45 00 00 29 38 13 40 00 40 06 7d 60 c0 a8 02 0a c0 a8 02 01

　　(1) “45”，其中“4”是IP协议的版本（Version），说明是IP4。“5”是IHL位，表示IP头部的长度，是一个4bit字段，最大就是1111了，值为12，IP头部的最大长度就是60字节。而这里为“5”，说明是20字节，这是标准的IP头部长度，头部报文中没有发送可选部分数据。

　　(2) “00”，服务类型（Type of Service）。这个8bit字段由3bit的优先权子字段（现在已经被忽略），4 bit的TOS子字段以及1 bit的未用字段（现在为0）构成.4 bit的TOS子字段包含：最小延时、最大吞吐量、最高可靠性以及最小费用构成，这四个1bit位最多只能有一个为1，本例中都为0，表示是一般服务。

　　(3) “00 29”，IP数据报文总长，包含头部以及数据，这里表示41字节。这41字节由20字节的IP头部以及21字节的TCP头构成（最后的一个字节为数据）。因此目前最大的IP数据包长度是65535字节。

　　(4) “38 13”，两个字节的标志位，这个是让目的主机来判断新来的分段属于哪个分组。

　　(5) “40”，转换为二进制就是“0100 0000”，其中第一位是IP协议目前没有用上的，为0。接着的是两个标志DF和MF。DF为1表示不要分段，MF为1表示还有进一步的分段（本例为0）。然后的“0 0000”是分段便移（Fragment Offset）。

　　(6) “00”，待定。

　　(7) “40”这个字节就是TTL（Time To Live）了，表示一个IP数据流的生命周期，用Ping显示的结果，能得到TTL的值，很多文章就说通过TTL位来判别主机类型。因为一般主机都有默认的TTL值，不同系统的默认值不一样。比如WINDOWS为128。不过，一般Ping得到的都不是默认值，这是因为每次IP数据包经过一个路由器的时候TTL就减一，当减到0时，这个数据包就消亡了。这也时Tracert的原理。本例中为“40”，转换为十进制就是64了，我用的WinXP。

　　(8) “06”，这个字节表示传输层的协议类型（Protocol）。在RFC790中有定义，6表示传输层是TCP协议。

　　(9) “7d 60”这个16bit是头校验和（Header Checksum）。

　　(10) “c0 a8 02 0a”，这个是源地址，也就是PC的IP地址，转换为十进制的IP地址就是：192.168.2.10。

　　(11) “c0 a8 02 01”，这个是目标地址，也就是DIY\_DE2的地址，转换为十进制的IP地址就是：192.168.2.1。

*-------------------------------------------------------------------------------------------------------------------------------*

## ****TCP包头****

　　TCP包头占有20个字节，即：

　　18 98 00 17 37 8d 49 3b 00 46 74 e0 50 18 fe d9 ea f7 00 00

　　(1) “18 98”，表示本地端口号，转换为十进制就是3368。

　　(2) “00 15”，表示目标端口号，转换为十进制就是23，因为我是连接TELNET站点，所以，这个就是23。

　　(3) “37 8d 49 3b”，是顺序号（Sequence Number），简写为SEQ。

　　(4) “00 46 74 e0”，是确认号（Acknowledgment Number），简写为ACKNUM。

　　(5) “50 18”，转换为二进制，“0101 0000 0001 1000”。这两个字节，总共16bit，有好多东西。第一个4bit“0101”，是TCP头长，十进制为5，表示20个字节。接着的6bit现在TCP协议没有用上，都为0。最后的6bit“01 1000”是六个重要的标志。这是两个计算机数据交流的信息标志。接收和发送断根据这些标志来确定信息流的种类。下面是一些介绍：

　　URG：（Urgent Pointer field significant）紧急指针。用到的时候值为1，用来处理避免TCP数据流中断。

　　ACK：（Acknowledgment fieldsignificant）置1时表示确认号（AcknowledgmentNumber）为合法，为0的时候表示数据段不包含确认信息，确认号被忽略。

　　PSH：（Push Function），PUSH标志的数据，置1时请求的数据段在接收方得到后就可直接送到应用程序，而不必等到缓冲区满时才传送。

　　RST：（Reset the connection）用于复位因某种原因引起出现的错误连接，也用来拒绝非法数据和请求。如果接收到RST位时候，通常发生了某些错误。

　　SYN：（Synchronize sequence numbers）用来建立连接，在连接请求中，SYN=1，ACK=0，连接响应时，SYN=1，ACK=1。即，SYN和ACK来区分Connection Request和Connection Accepted。

　　FIN：（No more data from sender）用来释放连接，表明发送方已经没有数据发送了。

　　这6个标志位，对号入座。本例中SYN=0，ACK=1，当然就是表示连接请求了。在分析TCP包头时候，要注意这两位的变换。

　　(6) “fe d9”，窗口值，用来控制实现流量控制。

　　(7) “ea f7”，检验和，TCP的检验和是强制的。

　　(8) “00 00”，紧急指针。

路由算法：

 距离矢量路由算法（分布式Bellman-Ford路由算法/RIP协议）：  
          每个路由器维护一张路由表，表中列出了当前已知的到每个目标的最佳距离，以及所使用的链路，这些表通过邻居之间的相互交换信息而不断被更新，最终每个路由器都了解到达每个目的地的最佳链路。  
          每个路由器维护一张路由表，它以网络每个路由器为索引，每个路由器对应一个表项，表项包含两部分：到达该目标路由器的首选出境线路，以及到达该目标路由器的距离估计值。  
          无穷计算问题：  
               整个网络最佳路径的寻找过程称为收敛，虽然该算法总能收敛到正确答案，但速度非常缓慢。  
               对于好消息的反应非常迅速，而对于坏消息的反应异常迟缓。  
     链路状态路由算法：  
          当网络拓扑结构分发生变化后，距离矢量算法需要太长的时间才能收敛到稳定的状态。  
          （1）发现它的邻居节点，并了解其网络地址  
          （2）设置到每个邻居节点的距离或者成本度量       
          （3）构造一个包含所有刚刚获知的链路信息包：   
               构造数据包的时机：  
                    周期性的创建数据包。  
                    每当发生某些重要的事情时才创建数据包。  
          （4）将这个包发给所有其他的路由器，并接受来自所有其他路由器的信息包  
               泛洪。为了控制泛洪的规模，每个数据包都包含一个序号，序号随着每一个新数据包发出而逐一递增，路由器记录下它所看到的所有（源路由器，序号）对，当一个新的链路状态数据包到达时，路由器检查这个新来的数据包是否已经出现在上述观察到的列表中，如果是一个新的数据包，则把它转发到除入境线路之外的所有其他线路上。如果这是一个重复的数据包则丢弃；如果数据包的序号小于当前所看到的来自该源路由器的最大序列号，则它将被当做过时数据包而拒绝接受。  
               问题：如果序列号绕回，可能会产生混淆；如果一个路由器崩溃了，那么它将丢失所有的序号记录表，如果它再从0开始，那么，下一个数据包将呗作为重复数据包而拒绝；如果一个序号被破坏了，会被当做过时数据包而被拒绝接受。  
               解决方案：在每个数据包的序号之后包含一个年龄字段，并且每秒钟年龄减1，值为0时丢弃.                          
          （5）计算出到每个路由器的最短路径