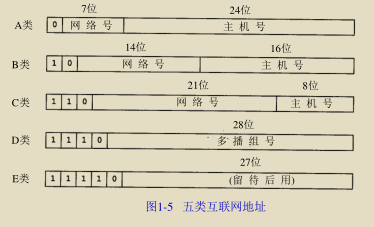
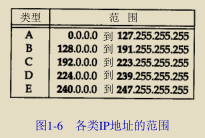
IP地址分类：





域名系统：

域名系统（DNS）是一个分布式的数据库，由它来提供IP地址和主机名之间的映射信息。

封装:

当应用程序用TCP传送数据时，数据被送入协议栈中，然后逐个通过每一层直到被当作一串比特流送入网络。其中每一层对收到的数据都要增加一些首部信息（有时还要增加尾部信息）。TCP传给IP的数据单元称作TCP报文段或简称为TCP段（TCP segment）。IP传给网络接口层的数据单元称作IP数据报(IP datagram)。通过以太网传输的比特

流称作帧(Frame)。

关于公网地址和私网地址：公网地址是指能连接上互联网的地址，私网地址是局域网内部的地址。私网地址是不能穿透路由器到达互联网上的，那么局域网内部的多台电脑是如何通过同一个公网地址来链接互联网的？原理是使用了端口映射。比如局域网内部IP地址为192.1.1.10的主机中端口号为2000的应用程序要向外网发送IP报文，则IP报文在通过路由器时IP地址被替换成了路由器中能连接互联网的IP地址。然后路由器寻找映射表中还没有被使用的端口，并用这个端口替换掉IP报文中的端口号，并在映射表中作映射记录，则路由器的端口就对应上了子网中某个主机的IP地址和端口号。当路由器接收到远程主机回应的IP报文时，通过查表然后将报文中的公网IP转成对应的私网IP和对应的端口。也就是说私网中每一个主机中正在收发数据的端口都对应了路由器中的一个端口。一个C类子网最多能有255-2个主机，即使每个主机有100个端口在使用网络，那么也才占用24800个端口而已，完全不担心路由器端口不够用的情况。

子网掩码：

子网掩码的主要作用是为了将IP地址划分成网络地址和主机地址两部分。如果两个IP地址属于同一个子网，则它们和子网掩码相的结果相等，这样路由器在转发IP数据报时就可以进行路由选择，决定是将IP数据报发给外网还是发给子网内部的设备。

|  |  |
| --- | --- |
| TCP/IP四层模型 | |
| 应用层 | FTP协议、Telnet协议、DNS、HTTP以及各种邮件协议等等 |
| 传输层 | TCP传输控制协议、UDP用户数据报协议 |
| 网络层 | IP网际协议、ICMP互联网控制消息协议、IGMP协议 |
| 数据链路层 | 设备驱动、网卡接口、ARP地址解析协议、RARP逆地址解析协议 |

一．数据链路层。

数据连路层主要的三个功能：(1)为IP模块发送和接收IP数据报。(2)为ARP模块发送ARP请求和应答ARP请求。(3)为RARP发送RARP请求和接收RARP请求。

TCP/IP支持多种不同的链路层协议，这取决于网络使用的硬件，比如以太网、令牌环、FDDI（光纤分布式数据接口）以及RS-232串行线路等。

ARP的作用是提供IP地址到硬件地址的映射。ARP高效运行的关键是每台主机都有一个ARP高速缓存，这个缓存存放最近20分钟里IP地址到硬件地址的映射记录。

RARP的作用是使无盘工作站从其它主机读取无盘工作站的IP地址。

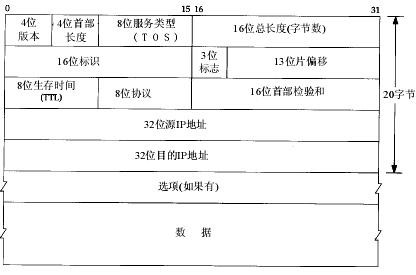
ARP和RARP都是广播请求，而它们的回应都是单播。

二．网络层。

1. IP协议(网际协议)是TCP/IP协议族中是为核心的协议。所有的TCP、UDP、ICMP以及IGMP数据报都以IP数据报的模式传输。虽然ICMP数据报是以IP数据报的形式传输但它却是属于网络层的内容。

2. IP协议提供不可靠、无连接的数据报传输服务。不可靠是指它不能保证数据报能到达目的地。比如某个路由器暂时用完了缓冲区，则IP协议规定直接丢弃该数据报，然后发送ICMP消息给信源端。无连接指IP协议不维护任何关于后续数据报的状态信息，每个数据报的处理都是独立的。

3. IP数据报首部格式：



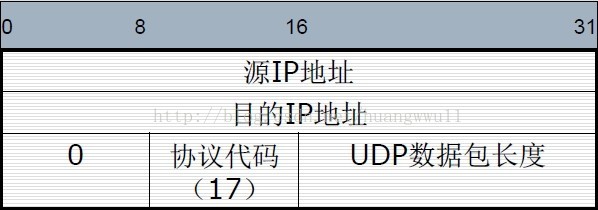
1. 版本字段：4位版本字段用来表示是IPv4或者IPv6。
2. 首部长度字段：4位首部长度字段用来表示IP数据报的首部长度。它能表示的最大值为15，而IP协议规定该字段一个值表示4个字节，所以IP首部最大长度为15x6=60个字节。一般情况下IP首部没有选项部分，则固定20个字节。如果有选项部分，IP首部的最大长度不能超过60个字节。
3. 服务类型字段。8位服务类型字段包括3bit的优先子字段（现已被忽略），4bit的TOS子字段和1bit的未用位必须置0。4bit的TOS子字段分别表示：最小延时、最大吞吐量、最高可靠性和最小费用。
4. IP报文总长度字段。16bit的总长度字段能表示的最大值为65535，但大多数的链路层都的数据帧都比65535要小。比如以太网限制数据帧的长度为1500字节，IEEE802.3限制数据帧的长度为1492字节，此时就必须在IP层进行分片和重组。这种限制称为MTU（最大传输单元）。
5. 标识字段：IP层软件在存储器中维持一个计数器，每产生一个数据报，计数器就加 1，并将此值赋给标识字段。但这个“标识”并不是序号，因为 IP是无连接的服务，数据报不存在按序接收的问题。当数据报由于长度超过网络的 MTU 而必须分片时，这个标识字段的值就被复制到所有分片的的数据报的标识字段中。相同的标识字段的值使分片后的各数据报片最后能正确地重装成为原来的数据报。
6. 标志字段(Flag)：占3位，但目前只有2位有意义。标志字段中的最低位记为 MF (More Fragment)。MF=1即表示后面“还有分片”的数据报。MF=0表示这已是若干数据报片中的最后一个。标志字段中间的一位记为 DF(Don't Fragment)，意思是“不能分片”。只有当 DF=0时才允许分片。
7. 片偏移字段：占 13位。表明IP数据报在分片后，某片在原数据报中的相对位置。也就是说，相对用户数据字段的起点，该片从何处开始。片偏移以 8个字节为偏移单位。这就是说，每个分片的长度一定是 8字节 (64位)的整数倍。
8. 生存时间字段：占8位。生存时间字段常用的英文缩写是TTL (Time To Live)，其表明数据报在网络中的寿命。由发出数据报的源点设置这个字段。其目的是防止无法交付的数据报无限制地在因特网中兜围子，因而白白消耗网络资源。IP数据报每经过一个路由器，就把TTL值减 1。当 TTL值为 0时，就丢弃这个数据报，并发送ICMP报文通知源主机。
9. 协议字段：占8位。协议字段指出此数据报携带的数据是使用何种协议，比如TCP协议或者UDP协议。主机的IP层通过协议字段来将数据部分交给相应处理过程。
10. 首部检验和字段：占 16位。这个字段只检验数据报的首部。

校验方式为：对于发送端，首先将校验和字段置0，然后对首部中每个16bit二进制反码求和（包括校验和字段），其结果存在校验和字段中，这样就完成了发送端的IP校验。对于接收端，收到数据报后对IP首部的每个16bit二进制反码求和（包括校验和字段），如果校验的结果为全1则校验成功，否则为校验失败。如果校验失败则丢弃数据报，但不生成差错报文。

1. 源地址字段、目的地址字段、可选项。

4. 关于IP数据报分片：任何时候IP层接收到一份要发送的IP数据报时，它要判断向本地的哪个接口发送数据（选路），并查询该接口获得其MTU。然后把MTU和数据报长度进行比较，如果需要则进行分片。分片可能发生在原始发送端主机上，也可能发生在中间路由器上。一份IP数据报被分片以后，只有到达目的地才会进行重组。当IP数据报被分片以后，每一片都成为一个分组，拥有自己的IP首部，并且在选择路由时与其它分组独立。如果在重组被分片的IP数据报的分组时，只要发现有一个分组丢失，就需要重传整个IP数据报。如果IP数据报需要分片，但是IP首部标志字段中设置了不分片，则会导致IP数据报被丢弃，并返回一个ICMP差错报文。

1. 传输层
2. 关于TCP和UDP的伪首部：由于IP层中只对IP首部进行校验，而TCP/UDP只对TCP/UDP首部和数据部分进行校验，那么如果在组装IP数据报或者传输的过程中发生路由选择错误时，无法发现问题。所以在校验TCP/UDP数据报时多校验了一个伪首部，而实际的TCP/UDP数据报中没有这个伪首部。伪首部的格式为：



1. TCP/UDP的校验和：IP数据报的校验和只包含IP首部，不包含IP数据报的数据部分。而TCP/UDP的校验和不仅包含了数据报首部而且包含了数据报的数据部分。不仅如此，在进行校验时还会校验一个不存在伪首部。校验伪首部的目的是为了防止出现路由选择错误的情况。

TCP/UDP的校验原理和IP首部的校验原理一样，但是IP首部的长度一定为2个字节的整数倍，而TCP/UDP由于包含数据部分所以不一定是2字节的整数倍，如果不是2字节的整数倍则后面补0以满足2字节(16bit)整数倍的要求。