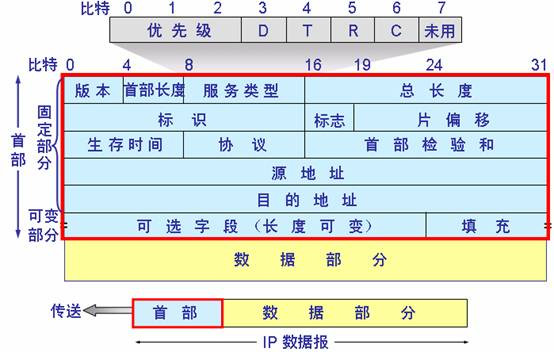
1. **IP 数据报首部**



TCP/IP 协议定义了一个在因特网上传输的包，称为 IP 数据报 (IP Datagram)。这是一个与硬件无关的虚拟包，由首部和数据两部分组成。

首部的前一部分是固定长度，共 20 字节，是所有 IP 数据报必须具有的。在首部的固定部分的后面是一些可选字段，其长度是可变的。首都中的源地址和目的地址都是 IP 协议地址。

**二、IP 数据报首部的固定部分中的各字段：**

1）版本：占4位，指IP协议的版本。

通信双方使用的 IP 协议版本必须一致。日前广泛使用的 IP 协议版本号为 4 (即 IPv4)。IPv6 目前还处于起步阶段。

2）首部长度：占 4 位，可表示的最大十进制数值是 15。

请注意，这个字段所表示数的单位是32位字 ( 1 个 32 位字长是 4  字节)，因此，当 IP 的首部长度为 1111 时 ( 即十进制的 15 )，首部长度就达到 60 字节。

最常用的首部长度就是 20 字节 (即首部长度为 0101)，这时不使用任何选项。

3）服务：占 8 位，用来获得更好的服务，一般不使用。

服务类型字段实际上被划分为 2 个部分，一部分为优先权一部分为 TOS。优先权用来设定报文的优先级，就像邮包分为挂号和平信一样。TOS 允许按照吞吐量、时延、可靠性和费用方式选择传输服务，在早期的时候，TOS 还被用来进行路由选择。在 QOS 中有时也会使用优先权，常见的优先权队列。

这个字段在旧标准中叫做服务类型，但实际上一直没有被使用过。1998 年 IETF 把这个字段改名为区分服务 DS ( DifferentiatedServices )。只有在使用区分服务时，这个字段才起作用。

4）总长度：总长度指首都及数据之和的长度，单位为字节。

因为总长度字段为 16 位，所以数据报的最大长度为 65535 字节。在 IP 层下面的每一种数据链路层都有自己的帧格式，其中包括帧格式中的数据字段的最大长度，即最大传送单元 MTU (Maximum Transfer Unit)。当一个数据报封装成链路层的帧时，此数据报的总长度 ( 即首部加上数据部分 )一定不能超过下面的数据链路层的 MTU 值。

如果报文总长度大于数据链路可传输的最大传输单元（MTU），那么就会对报文进行分片

5）标识 ( Identification )：占 16位。

IP 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 ( Flag )：占3 位，但目前只有2位有意义，  其中第一位没有被使用。

  第二位是不分片位，当 DF 位被置1，表示路由器不能对数据报文进行分片处理，如果报文由于不能被分片而不能被转发，那么路由器将丢弃这个数据包，并向源地址发送错误报告。这一功能可以用来测试线路的最大传输单元。只有当 DF = 0 时才允许分片。

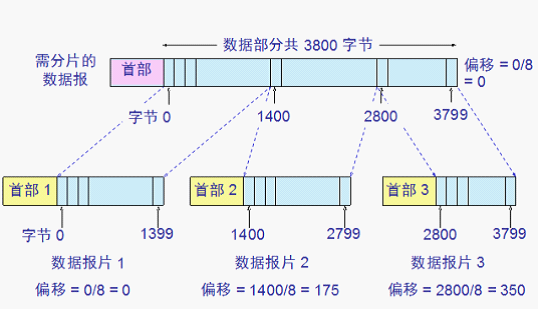
第三位为 MF，当路由器对数据进行分片时，除了最后一个分片的 MF 位为 0 外，其他所有的 MF 全部为 1，表示其后面还有其他的分片。

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。

7）片偏移：占 13位。较长的分组在分片后，某片在原分组中的相对位置。

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：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。

最初的设计是以秒作为 TTL 的单位。每经过一个路由器时，就把 TTL 减去数据报在路由器消耗掉的一段时间。若数据报在路由器消耗的时间小于 1 秒，就把 TTL 值减 1。当 TTL 值为 0 时，就丢弃这个数据报。当 TTL 为零的时候，就会丢弃这个报文，同时向源地址发送错误报告，促使重新发送。

9）协议：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，以便使目的主机的 IP 层知道应将数据部分上交给哪个处理过程，常用的有ICMP(1), IGMP(2), TCP(6), UDP(17), IPv6（41）

10）首部检验和：占 16 位。这个字段只检验数据报的首部，但不包括数据部分。

这是因为数据报每经过一个路由器，都要重新计算一下首都检验和 ( 一些字段，如生存时间、标志、片偏移等都可能发生变化 )。不检验数据部分可减少计算的工作量。

11）源地址：发送方IP地址

12）目的地址：接收方IP地址

**三、IP 数据报首部的可变部分：**

IP 首都的可变部分就是一个可选字段。选项字段用来支持排错、测量以及安全等措施，内容很丰富。此字段的长度可变，从 1 个字节到 40 个字节不等，取决于所选择的项目。

某些选项只需要 1 个字节，它只包括 1 个字节的选项代码。但还有些选项需要多个字节，这些选项一个个拼接起来，中间不需要有分隔符，最后用全 0 的填充字段补齐成为 4字节的整数倍。增加首都的可变部分是为了增加 IP 数据报的功能，但这同时也使得 IP 数据报的首部长度成为可变的。这就增加了每一个路由器处理数据报的开销。

实际上这些选项很少被使用。新的 IPv6就将 IP数据报的首部长度做成固定的。