# IP 网际协议

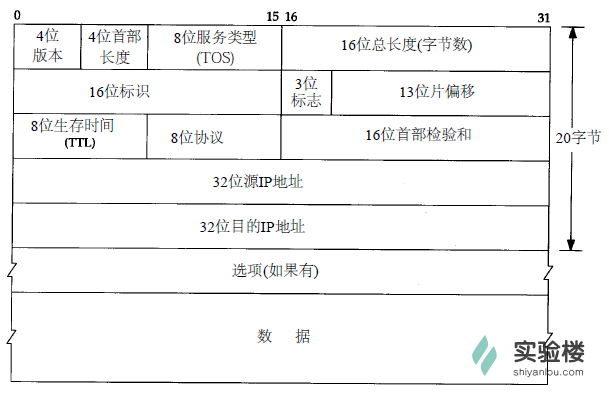
IP 协议位于网络层，它是 TCP/IP 协议族中最为核心的协议，所有的 TCP、UDP、ICMP 及 IGMP 数据都以 IP 数据报格式传输。IP 协议提供的是 **不可靠** 、 **无连接** 的数据报传送服务。

**不可靠**（unreliable）：IP 协议不能保证数据报能成功地到达目的地，它仅提供传输服务。当发生某种错误时，IP 协议会丢弃该数据报。传输的可靠性全由上层协议来提供。

**无连接**（connectionless）：IP 协议对每个数据报的处理是相互独立的。这也说明， IP 数据报可以不按发送顺序接收。如果发送方向接收方发送了两个连续的数据报（先是 A，然后是 B），每个数据报可以选择不同的路线，因此 B 可能在 A 到达之前先到达。

## 一、IP 数据报

首先看一下 IP 数据报的格式，其中没有一个字段是多余的，学习 IP 协议就应从学习它的报文字段意义和作用开始。

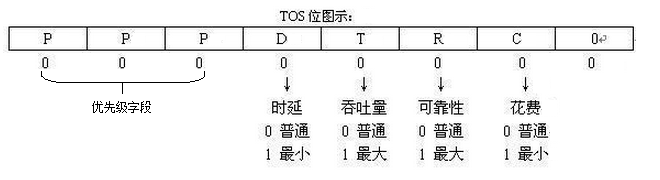


如上图所示，普通的 IP 数据报的**报头**长度 20 字节(除非有选项字段)，各个部分的作用：

**版本号** ：4 位，用于标明 IP 版本号，0100 表示 IPv4，0110 表示 IPv6。目前常见的是 IPv4。

**首部长度** ：4 位，表示 IP 报头长度，包括选项字段。

**服务类型(TOS)** ：分别有：最小时延、最大吞吐量、最高可靠性、最小花费 4 种服务，如下图所示。4 个标识位只能有一个被置为 1 ：



**总长度** ：16 位，报头长度加上数据部分长度，便是数据报的总长度。IP 数据报最长可达 65535 字节。

**标识** ：16 位，接收方根据分片中的标识字段相不相同来判断这些分片是不是同一个数据报的分片，从而进行分片的重组。通常每发送一份报文它的值就会加 1。

**标志** ：3 位，用于标识数据报是否分片。其中的第 2 位是不分段（DF）位。当 DF 位被设置为 1 时，则不对数据包进行分段处理；第 3 位是分段（MF）位，除了最后一个分段的 MF 位被设置为 0 外，其他的分段的 MF 位均设置为 1。

**偏移** ：13 位，在接收方进行数据报重组时用来标识分片的顺序。

**生存时间(TTL)** ：8 位，用于设置数据报可以经过的最多的路由器个数。TTL 的初始值由源主机设置（通常为 32 或 64），每经过一个处理它的路由器，TTL 值减 1。如果一个数据报的 TTL 值被减至 0，它将被丢弃。

**协议** ：8 位，用来标识是哪个协议向 IP 传送数据。ICMP 为 1，IGMP 为 2，TCP 为 6，UDP 为 17，GRE 为 47，ESP 为 50。

**首部校验和** ：根据 IP 首部计算的校验和码。

**源 IP 和目的 IP** ：数据报头还会包含该数据报的发送方 IP 和接收方 IP。

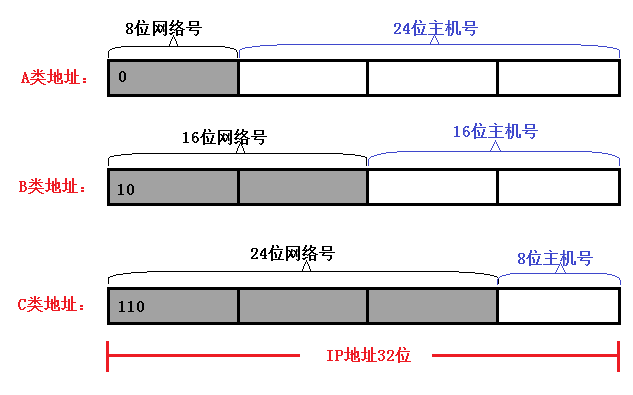
**选项** ：是数据报中的一个可变长、可选的信息，不常用，多用于安全、军事等领域。

## 二、IP 地址分类

为了便于寻址以及层次化构造网络，每个 IP 地址可被看作是分为两部分，即 **网络号** 和 **主机号** 。同一个区域的所有主机有相同的网络号(即 IP 地址的前半部分相同)，区域内的每个主机（包括路由器）都有一个主机号与其对应。

IP 地址被分为 A,B,C,D,E 五类，其中 A 类给大型网络或政府机构等，B 类分配给中型网络、跨国企业等，C 类分配给小型网络，D 类用于多播，E 类用于实验，各类可容纳的地址数目不同。其中我们最常见的为 A,B,C 这三类。

IP 地址用 32 位二进制数字表示的时候，A,B,C 类 IP 的网络号长度分别为 8 位、16 位、24 位：



**A 类地址**

A 类地址网络号范围：1.0.0.0---127.0.0.0

A 类 IP 地址范围：1.0.0.0---127.255.255.255

A 类 IP 的私有地址范围：10.0.0.0---10.255.255.255 （所谓的私有地址就是在互联网上不使用，而被用在局域网络中的地址）

127.X.X.X 是保留地址，用做循环测试用的

因为主机号有 24 位，所以一个 A 类网络号可以容纳 2^24-2=16777214 个主机号

**B 类地址**

B 类地址网络号范围：128.0.0.0---191.255.0.0

B 类 IP 地址范围：128.0.0.0---191.255.255.255

B 类 IP 的私有地址范围：172.16.0.0---172.31.255.255

169.254.X.X 是保留地址；191.255.255.255 是广播地址

因为主机号有 16 位，所以一个 B 类网络号可以容纳 2^16-2=65534 个主机号

**C 类地址**

C 类地址网络号范围：192.0.0.0---223.255.255.0

C 类 IP 地址范围：192.0.0.0---223.255.255.255

C 类 IP 的私有地址范围：192.168.0.0---192.168.255.255

因为主机号有 8 位，所以一个 C 类网络号可以容纳 2^8-2=254 个主机号

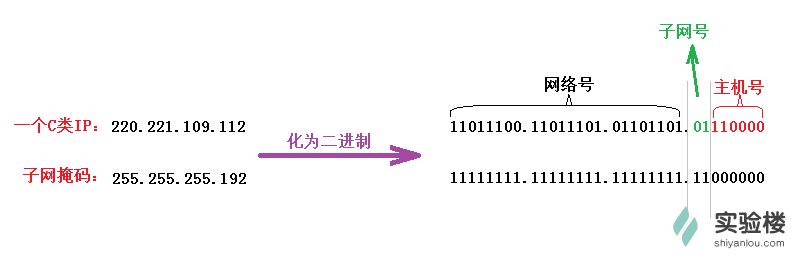
## 三、子网划分

IP 地址如果只使用 ABCDE 类来划分，会造成大量的浪费：一个有 500 台主机的网络，无法使用 C 类地址。但如果使用一个 B 类地址，6 万多个主机地址只有 500 个被使用，造成 IP 地址的大量浪费。

因此，可以在 ABC 类网络的基础上，进一步划分子网：**占用主机号的前几个位，用于表示子网号** 。

这样 IP 地址就可看作 IP = 网络号 + 子网号 + 主机号

子网号的位数没有硬性规定，于是我们用 **子网掩码** 来确定一个 IP 地址中哪几位是主机号，具体使用方法如图：



子网掩码中的 1 标识了 IP 地址中相应的网络号，0 标识了主机号。将 IP 地址和子网掩码进行 **逻辑与运算** ，结果就能得到网络号和子网号。

## 四、IP 路由选择

如果发送方与接收方直接相连（点对点）或都在一个共享网络上（以太网），那么 IP 数据报就能直接送达。 而大多数情况则是发送方与接收方通过若干个路由器(router)连接，那么数据报就需要经过若干个路由器的转发才能送达，它是怎么选择一个合适的路径来"送货"的呢？

IP 层在内存中有一个路由表（输入命令 **route -n** 可以查看路由表），当收到一份数据报并进行发送时，都要对该表进行搜索：

1、搜索路由表，如果能找到和目的 IP 地址完全一致的主机，则将 IP 数据报发向该主机；

2、搜索路由表，如果匹配主机失败，则匹配同子网的路由器(这需要子网掩码的协助)。如果找到路由器，则将 IP 该数据报发向该路由器；

3、搜索路由表，如果匹配同子网路由器失败，则匹配同网络号路由器，如果找到路由器，则将该 IP 数据报发向该路由器；

4、如果以上都失败了，就搜索默认路由，如果默认路由存在，则发报；

6、如果都失败了，就丢掉这个包；

7、接收到数据报的路由器再按照它自己的路由表继续转发，直到数据报被转发到目的主机；

8、如果在转发过程中，IP 数据报的 TTL（生命周期）已经被减为 0，则该 IP 数据报就被抛弃。

## 五、NAT 技术

当你用 ifconfig 查看 IP 地址时，有时你会发现自己的 IP 地址是这样的———192.186.X.X 或 172.16.X.X  
这是 C 类网和 B 类网的私有地址，这就是俗称的内网 IP。这是因为你的路由器采用了 NAT 技术。

NAT（Network Address Translation，网络地址转换）是 1994 年提出的。当在专用网内部的一些主机本来已经分配到了内网 IP 地址，但现在又想和因特网上的主机通信时，NAT 技术将其内网 IP 地址转换成全球 IP 地址，然后与因特网连接，也就是说，内网的数台主机使用了同一个全球 IP 地址在上网。

NAT 技术实现了宽带共享，而且有助于缓解 IP 地址空间枯竭的问题。

## 六、IP 的未来

我们现在使用的 IPv4 协议版本从理论上讲，可以编址 1600 万个网络、40 亿台主机。但采用 A、B、C 三类编址方式后，可用的网络地址和主机地址的数目大打折扣，以至 IP 地址 **已于 2011 年 2 月 3 日分配完毕** 。 其中北美占有 3/4，约 30 亿个，而人口最多的亚洲只有不到 4 亿个，中国截止 2010 年 6 月 IPv4 地址数量达到 2.5 亿，落后于 4.2 亿网民的需求。地址不足，严重地制约了中国及其他国家互联网的应用和发展。

随着网络技术的发展，计算机网络将进入人们的日常生活，可能身边的每一样东西都需要连入全球因特网，在这样的环境下，IPv6 应运而生。

IPv6 的地址长度是 128 位，通常将这 128 位的地址按每 16 位划分为一个段，将每个段转换成十六进制数字，并用冒号隔开，比如：2000:0000:0000:0000:0001:2345:6789:abcd 就是一个 IPv6 地址。

单从数量级上来说，IPv6 所拥有的地址容量是 IPv4 的约 8×10^28 倍，达到 2^128（算上全零的）个。这不但解决了网络地址资源数量的问题，同时也为除电脑外的设备连入互联网在数量限制上扫清了障碍。

随着 IPv4 不足，支持 IPv6 的网络迅速增长，现在全球已经有 5%的网络使用 IPv6

## 七、作业

1、查看 IP 路由表，并截图。

2、子网划分：现有两个 C 类网，202.203.204.0 和 202.203.224.0，分别把它们平均分成 4 个和 8 个子网，写出每个子网的起始、终结 IP 和子网掩码。