一、引言

链路层的上层协议是网络层，IP协议是网络层协议中的最核心协议。ICMP/IGMP，TCP/UDP都是通过IP数据包传输的。IP协议提供非可靠的（unreliable）、无连接的（connectionless）。

- 非可靠的：IP协议不能保证数据能成功的到达目的地（传输层协议保证）。当IP数据包在传输的过程中，发生错误，路由器的处理是丢掉该数据包，然后发送ICMP给该IP数据包的源；
- 无连接的：表示IP协议不维护后续数据包的状态，每个IP数据包都是独立的，即IP数据包可以不按照顺序发送接收。

二、IP数据包

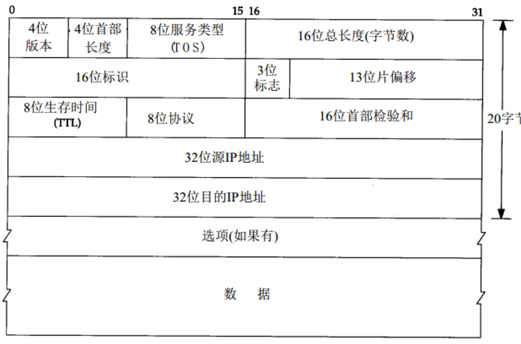

图1. IP数据包结构图

- IP版本号（Version）：IP协议版本号，长度4bit；目前常有IPv4的该域值是（0100）；
- 首部长度（Head Length）：表明IP数据包的首部长度，长度4bit，单位是32bit（4字节，图1中的一行），首部长度最大15*4=60字节，没有选填的选项，首部长度为20字节，该值为（0101）；
- 服务类型（Differentiated Services Field）：表明该IP数据包选择何种优先级服务传输，长度8bit，其中前3bit，后1bit没有用的，一般为0（000XXXX0）；有用的4bit部分（XXXX）表示服务类型，每一位表示一种类型，分别是最小延迟、最大吞吐量、最高可靠性、最小代价，这4bit每次最多只有一位为1，若全为0，表示普通的传输服务；
- 标识域（Identification）：唯一地标识主机发送的每一份IP数据包。通常每发送一份数据包它的值就会加 1；长度16bit；
- 协议类型（Protocol）：指明上层协议类型，长度8bit，常用协议值 0x01—ICMP，0x02—IGMP，0x06—TCP，0x11—UDP。
- 标志域（Flags）：在IP数据包分片使用，长度3bit。
- 片偏移（fragment offset）：在IP数据包分片使用，长度13bit。
- 生存时间（Time to Live，TTL）：IP数据包可以经过的最大路由跳转数，长度8bit，初值一般为0x40，IP数据包每经过一次路由，该值-1，当TTL为0的时候，IP数据包被丢弃，并发送一个ICMP包给该IP数据包的主机。
- 首部校验和（Header checknum）：校验首部，长度16bit，与以太帧的CRC校验不同，这个只校验IP数据包的首部。如果校验未通过，直接丢弃该数据包，不发送ICMP，由上层协议来控制。
- 源IP地址（Source IP）：告诉IP数据包，从哪来。长度32bit。
- 目标IP地址（Destination IP）：告诉IP数据包，要到哪去。长度32bit。
- 其他：可选。

三、子网

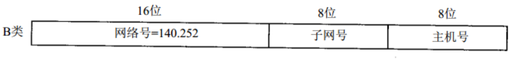

图2. B类IP的子网编址举例

我们不是把IP地址看成由单纯的一个网络号和一个主机号组成，而是把主机号再分成一个子网号和一个主机号。子网对外部路由器来说隐藏了内部网络组织（一个校园或公司内部）的细节。

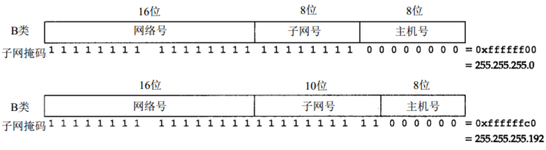

图3.两种不同的B类子网划分举例

子网掩码是一个32bit的值，其中值为 1的bit留给网络号和子网号，为0的bit留给主机号。0或1需要连续的。

四、特殊IP地址

IP类型	含义
127.x.x.x	常见的是127.0.0.1，环回地址，该地址是指电脑本身，会把发送给该ip的数据返回给当前主机。该IP被认为是一个网络接口。它是一个A类地址，没有进行子网划分
(10.x.x.x)，(172.16.x.x -172.31.x.x)，(192.168.x.x)	局域网IP地址，私有地址
0.0.0.0	IP地址收容所，所有不认识的IP地址，都丢这；已经不是真正意义上的ip地址了。
255.255.255.255	受限制的广播地址，对本机来说，这个地址指本网段内（同一个广播域）的所有主机。在任何情况下，路由器都会禁止转发目的地址为受限的广播地址的数据包，这样的数据包仅会出现在本地网络中。
xxx.255[.255]	网络号不全为1，主机号全为1，该网络的广播地址
224.0.0.0-239.255.255.255	这是一组组播地址，需要注意它与广播地址的区别，其中224.0.0.1特指所有的主机，224.0.0.2特指所有的路由器，224.0.0.5指所有的OSPF路由器地址，224.0.0.13指PIMV2路由器的地址。

五、IP数据包抓包