# IP协议及其配套协议

## IP协议

工作在网络层，使用32位长度的地址，格式为

|  |
| --- |
| IP地址=网络地址+主机地址 |

分为四类IP地址，A,B,C,D类地址，如图所示

|  |  |
| --- | --- |
| A类IP地址 | 0网络：（网络地址的最高位必须是0）位网络地址+24位主机地址；A类的地址空间为0-127，最大网络数为126，0.0.0.0不能用，127网段是特殊网段，不能用于任何网络  A类私有地址范围：10.0.0.0-10.255.255.255 |
| B类IP地址 | 10网络：14位网络地址+16位主机地址；B类地址空间为128-191，最大网络数为16384，最大主机数65534；B类私有地址范围：172.16.0.0-172.31.255.255；网络位的最高位必须是10开头 |
| C类IP地址 | 110网络：21位网络地址+8位主机地址；C类地址空间为192-223，范围是192.0.0.0~223.255.255.255，私有地址为： 192.168.0.0~192.168.255.255 |
| D类IP地址 | 1110网络：28位通信地址；D类地址空间为224-254 |

判断两台计算机是否在同一个网段，将两台计算机的IP地址和子网掩码进行与运算（同1为1，否则为0），如果得出的结果一致，则在同一网段内；

子网掩码的作用有两个：判断是否在同一个网段内，以及在局域网中划分多个子网

实例：比如在一段子网掩码255.255.255.224(1111 1111 1111 1111 1111 1111 1110 0000)

这是c类IP地址，前三个字节表示网络号，后一个字节表示主机号，也表示网络号，还可以说明两个IP是否在同一个网段内；如果在同一个网段内，则信息交换不需要经过路由器；否则，必须进过路由器；

比如：ip：210.73.140.5 ，主机标识为5==》00000101

Ip: 210.73.140.16 , 主机标识为16==》00010000

主机标识的前三位都一样，则在同一个网段内

再比如：ip: 210.73.60.1 , 主机标识为1==》00000001

Ip: 210.73.60.252,主机标识为252==》11111100

主机标识前三位不一致，则不在同一个网段内

子网掩码的表示方法：192.168.0.1/24表示网络标识位为24位，即子网掩码为255.255.255.0

比如子网掩码为255.225.255.128

分解为11111111 11111111 11111111 10000000

所以内部网络ip地址为xxxxxxxx xxxxxxxx xxxxxxxx 0??????? 到 xxxxxxxx xxxxxxxx xxxxxxxx 0???????

也就是25位网络位，7位主机位，主机位从0-255，最后一个字节，由于有网络位，则变为0

主机位和网络位的划分是按照从左到右的顺序，比如c类地址默认子网掩码，前24位都为1，后面全为0，不能出现0和1交互出现的情况，所以，子网掩码的第四个字节只能是128,192,224,248,252,254,255；

## ARP地址解析协议

|  |  |
| --- | --- |
| 概念 | 根据IP地址获取物理地址，主机发送带有本身IP地址和物理地址的arp数据包到局域网内所有主机，和目标主机相配的那个主机会匹配IP地址，并返回物理地址给主机，主机以此确定目标的物理地址； |
| 原理 | 1.主机A和主机B通信，主机A要发送数据包到B，需要知道B的IP地址和物理地址，首先会在本地arp缓存表中查找，如果没有，则进行广播通信  2.局域网内所有主机接收到arp请求，判断自己的IP地址和数据包内的IP是否一致，如果不一致，则丢弃；如果一致，则查找自己所对应的那个MAC地址，将自己的IP地址和Mac地址打包在一起，发送给主机A  3.主机A 接收到B的数据包，查找到了B的Mac地址，将它更新到本地arp缓存表中，开始和B的IP通信 |
| Arp命令 | Arp –a 查看所有网卡接口的arp缓存信息 |

Arp是通过报文发送请求的，下面是报文格式：



Arp缓存表

缓存表实际上是一个ip地址—>Mac地址 的映射表，每一条记录了网络上主机的IP地址对应的Mac地址；本地arp缓存表是有生存期的，在一定的时间后，将重复上述的动作更新自己的缓存表；

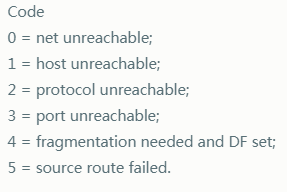
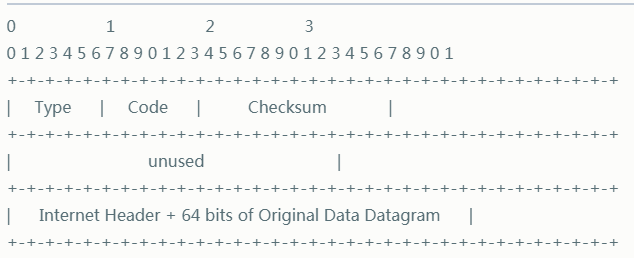
当地址解析协议被要求询问一个主机的Mac地址时，会首先查询arp缓存表，如果没有匹配，才会向网络中发出arp请求；

## ICMP因特网报文协议

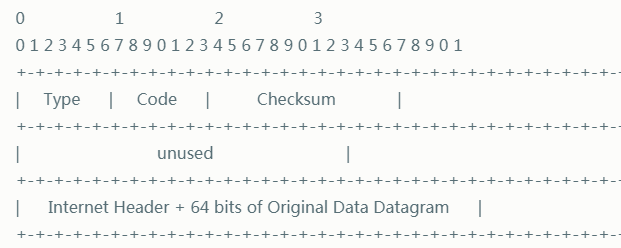
|  |  |
| --- | --- |
| 概念 | 传输控制报文协议，它是ip协议下的一个子协议，用于在IP主机和路由器之间传递控制消息；控制消息指网络是否通畅，主机是否可达等；它属于网络层协议。 |
| 原理 | 当主机发送IP数据包到目的主机时，经过多个路由，如果在某个路由不可达时或者目标主机不通时，相关路由就会发送icmp数据包给源主机，发送的出错报文信息会回到源设备上，根据此消息，源设备判断错误类型；它只能报告错误，无法纠正错误； |

### Icmp出错报文类型

目的不可达类型：数据包传递要经过很多环节，在任何一个环节无法传递下去，都会返回到源地址，并附上原因；当路由器遇到无法继续传递下去的情况时，就会发送icmp的（目的不可达类型）报文，type=3，code表示失败的原因



超时数据包：如果在IP数据包传输中，ttl的值逐渐减为0，则需要丢弃数据包，这时，icmp就会发送“超时报文”（type=11,code=0）表示传输过程中超时了



还有其他类型的出错控制，这篇博客讲的非常详细

<http://www.cnblogs.com/jingmoxukong/p/3811262.html>

### ping 命令详解

在window上，默认ping会发送4个icmp协议数据包，每个32字节，如果网络通畅，则会得到4个回送请求；使用TTL值（time to live）可以推测经过了多少个路由器网段（比如，返回ttl为119，说明源地址出发时ttl应该是128，最接近的2的次方数,应该经过了128-119=9个网段），但结果不一定准确；

其他的内容很常用，不需要在这里赘述

## IGMP因特网组管理协议

|  |  |  |
| --- | --- | --- |
| 三种通信方式 | | |
| 单播通信 | 以“点对点通信”为主的通信方式，此时信息的接收和传递只在两个节点间进行；网络中绝大多数数据都是以单播形式传输，比如发邮件，浏览网页；路由器和交换机将文件发送到指定地址 | 优点：服务器及时响应客户端请求；服务器可以针对用户的不同需求提供个性化的服务  缺点：服务器的流量压力非常大，在p2p中，经常性的主干道堵塞就是这个原因 |
| 组播通信 | 实现“一对一组”的通信方式，将相同的信息发送到同一组的所有用户中，交换机和路由器只向有需求用户发送所需的数据；路由器会有选择的复制和发送数据；使用D类IP地址，224.0.0.0~239.255.255.255  Window中的dhcp支持组播地址的分配； | 优点：具有相同需求的主机会接收到同样的信息，节省了服务器的负载；服务器的总带宽不受客户机数量的限制，ip协议允许有2.6亿多个组播，可以提供非常多的服务；  缺点：没有纠错机制，发错包或者丢包时没有处理机制；不过有其他措施可以弥补  典型应用：网上视频会议； |
| 广播通信 | 实现“一对多”的通信方式，网络中对每一台主机发送的信号进行无条件转发，所有主机都会受到信息（不论是否需要），网络成本很低，但在数据网络中广播通信仅仅被限定在二层交换机内，防止广播穿透路由器，造成广播风暴 | 优点：网络设备简单，成本低，易于维护，网络负载低  缺点：网络允许数据提供的带宽有限，客户机总带宽=服务器总带宽，比如有限电视线路只支持100个频道，即使传输变成光纤，也无法超过100个频道的极限；  典型应用：有线电视  注意：广播网禁止在Internet上传输 |

IGMP协议，是一个组播通信协议，运行在主机和组播路由器之间，用于发送消息给组播的成员，查询，添加组播成员等一系列功能的实现；