一、IP基本认识

IP在TCP/IP模型中处于网络层

网络层的主要作用是：实现主机与主机之间的通信。

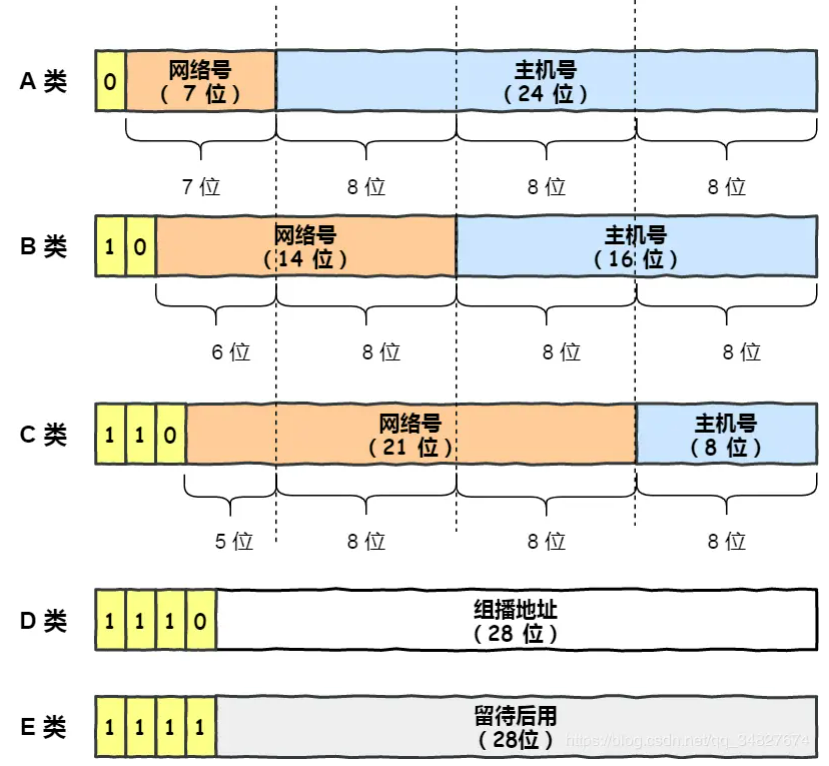
IP（网络层）和MAC（数据链路层）之间的区别和关系：

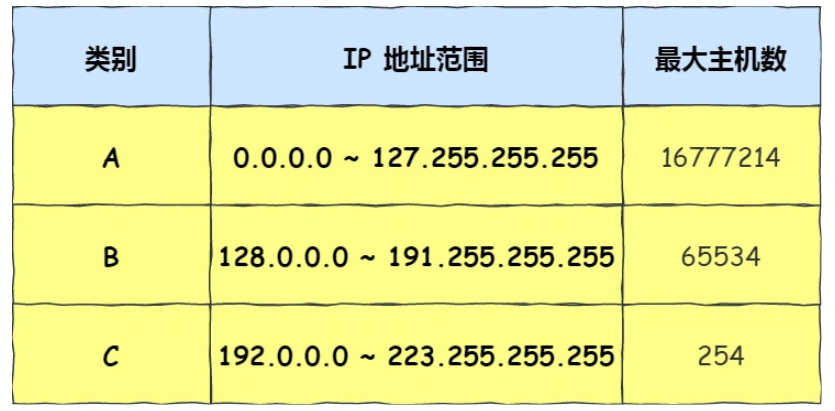
MAC的作用是实现**直连**的两个设备间的通信，IP负责在**没有直连**的两个网络间进行通信传输。数据包在网络的传输中，源IP地址和目标IP地址不会变化（前提：没用使用NAT网络），只有源MAC地址和目标MAC地址一直在变化。

二、IP地址基础知识

IP地址（IPv4）由32位二进制整数表示，使用点分十进制的标记方式将32位IP地址以每8位为一组分为4组并以 . 隔开再将每组转换成十进制。

1.IP地址分类：





网络中最大主机数为2的主机号次幂 – 2，因为主机号全为1为广播地址，指定某个网络下的所有主机；主机号全为0指定某个网络。

广播地址用于在同一个链路中相互连接的主机之间发送数据包，分为本地广播和直接广播。在本网络内的广播叫做本地广播，如网络地址为192.168.0.0/24，广播地址为192.168.0.255，这个广播地址的IP包会被路由器屏蔽，不会到达192.168.0.0/24以为的其他链路。在不同网络间的广播叫做直接广播，如192.168.0.0/24的主机向192.168.1.255/24的目标地址发送IP包，收到这个包的路由器将数据转发给192.168.1.0/24，使所有主机都能收到，直接广播有一定的安全问题，多数情况下会在路由器上设置不转发。

D类和E类地址没有主机号，不可用于主机IP，D类用于多播，E类是预留的分类暂未使用。多播用于将包发送给特定组内的所有主机。

2.IP分类的优缺点

优点：简单、选路简单（通过解析前几位就可以判断地址类型，从而确定网络地址和主机地址）

缺点：

a. 同一网络下没有地址层次（不能在同一网络下按需求对主机进一步划分）

b. 不能很好的与现实地址匹配（C类地址最大主机数只有254个，太少，而B类地址最大主机数6万多，太多）

这两个缺点可以用CIDR无分类地址解决

3.无分类地址CIDR

不再有分类的概念，32比特的IP地址被分为两部分，前面是网络号，后面是主机号，表示形式a.b.c.d/x，其中/x表示前x位属于网络号

还有一种用子网掩码划分网络号的主机号的方式，掩码的意思是掩盖掉主机号剩余的是网络号，将子网掩码和IP地址按位与就可以得到网络号。

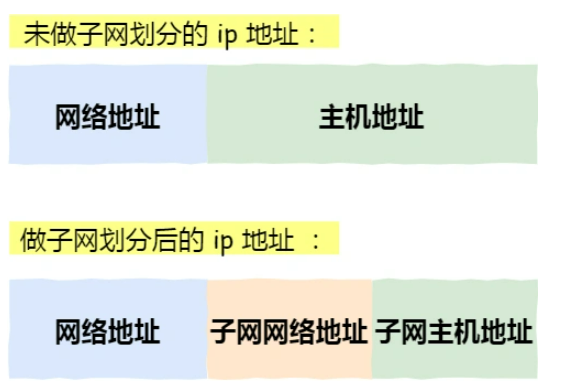
4. 为什么要分离网络号和主机号

两台计算机要通讯首先要判断是否处于同一个广播域内，即网络地址是否相同。路由器寻址工作中也是通过这样的方式来找到对应的网络号，进而把数据包转发给对应的网络。

5. 怎么进行子网划分

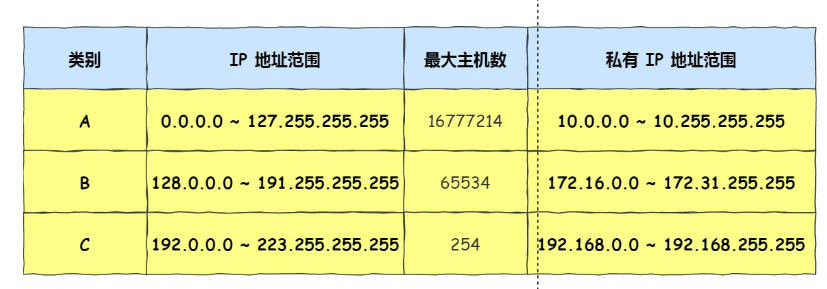
子网掩码还有一个作用是划分子网

子网划分实际上是将主机地址分为两个部分：子网络地址和子网主机地址。



如子网掩码255.255.255.192对C类地址进行子网划分，从8位主机号中借用2位作为子网号

6. 公有IP和私有IP地址



私有IP允许组织内部自己管理、分配，不同组织间的私有IP是可以重复的

公有IP是国际组织管理的，并且公有IP地址基本上要在整个互联网内保持唯一

7. IP地址与路由控制

IP地址的网络地址部分用于路由控制，路由控制表中记录着下一步应该发送至的路由器的地址。

环回地址不会流向网络：环回地址是在同一台计算机上的程序之间进行网络通信时所使用的默认地址，127.0.0.1是环回地址，与环回地址具有相同意义的是localhost主机名，使用这个IP或主机名时数据包不会流向网络。

7. IP分片与重组

刚IP数据包大于MTU时就会被分片，经过分片之后的IP数据包只能由目标主机进行重组，路由器是不会重组的。在分片传输中一旦某个分片丢失会造成整个IP数据报作废，TCP引入了MSS在TCP层进行分片不由IP分片，对于UDP尽量不要发送大于MTU的报文。

8. IPv6

IPv4地址是32位，不够用，IPv6 128位， 但不兼容IPv4，因此普及较慢

IPv6即插即用、提高了传输性能、提高了安全性

IPv6 每16位一组，每组用：隔开，出现连续的0可以省略用：：隔开（一个地址只允许一次）

IPv6与IPv4相比首部：取消了首部校验字段、取消了分片/重新组装相关字段、取消了选项字段

三、IP协议相关技术

1. DNS：将域名网址自动转换为具体的IP地址

DNS中域名用句点分隔，越靠右层级越高

域名的层级关系：

根域名服务器

顶级域名服务器

权威域名服务器

域名解析的工作流程：

缓存->hosts->本地域名服务器->根域名服务器->顶级域名服务器->权威域名服务器->本地域名服务器->客户端

只指路不带路（本地域名服务器访问服务器获得下一层服务器的IP，然后访问下一层的服务器）

2. ARP：获得下一跳的MAC地址

借助ARP请求和ARP响应：主机广播ARP请求，包含想要得到MAC地址的主机的IP；同一链路的设备收到ARP请求时解析ARP请求，如果目标IP与自己的IP一致就将自己的MAC地址塞入ARP响应包返回给主机

RARP协议通过MAC地址求IP

3. DHCP：动态获取IP地址，省去了配IP的过程

客户端广播DHCP发现报文

DHCP服务器收到DHCP发现报文后，用DHCP提供报文向客户端响应

客户端收到DHCP提供报文后，选择一个DHCP服务器发送DHCP请求报文

DHCP服务器用DHCP ACK报文应答

DHCP全程使用UDP广播通信

4. NAT：将私有地址转换成公有地址

IPv4地址紧缺，NAT是一种网络地址转换方法，缓解了IPv4地址耗尽的问题

NAT一个私有地址对应一个公有地址，不能解决IPv4地址耗尽

NAPT网路地址与端口转换，将不同的私有IP地址转换为相同的公有IP地址，但是以不同的端口号区分

5. ICMP互联网控制报文协议

确认IP包是否成功送达目标地址、报告发送过程中IP包被废弃的原因和改善网络设置等

6. IGMP 因特网组管理协议

用来控制组播的成员