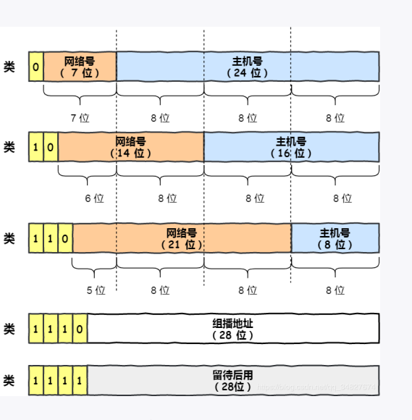
IP全家桶

IP基本认识

- IP的作用
  - IP在TCP/IP参考模型中处于第三层（网络层）
  - 网络层的主要作用是：实现主机与主机之间的通信，也叫点对点（end to end）通信。
- IP与MAC的关系
  - MAC 的作用则是实现「直连」的两个设备之间通信，而 IP 则负责在「没有直连」的两个网络之间进行通信传输
  - 计算机网络中也需要「数据链路层」和「网络层」这个分层才能实现向最终目标地址的通信
  - 源IP地址和目标IP地址在传输过程中是不会变化的，只有源 MAC 地址和目标 MAC 一直在变化。

IP的基础知识

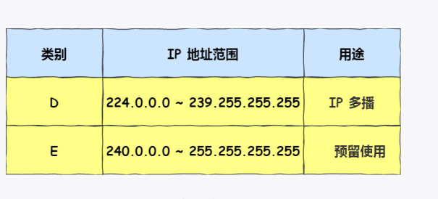
- IP地址的定义
  - IP 地址（IPv4 地址）由 32 位正整数来表示 人类方便记忆，采用「点分十进制」的标记方式（「32」位IP地址以每「8」位为组，共分为「4」组，每组以「.」隔开，再将每组转化为十进制）
  - IP地址并不是根据主机台数来配置的，而是以网卡。每块网卡可以分配一个以上的IP地址
- IP地址的分类



  - IP地址分类成5种类型，分别是「A、B、C、D、E」类

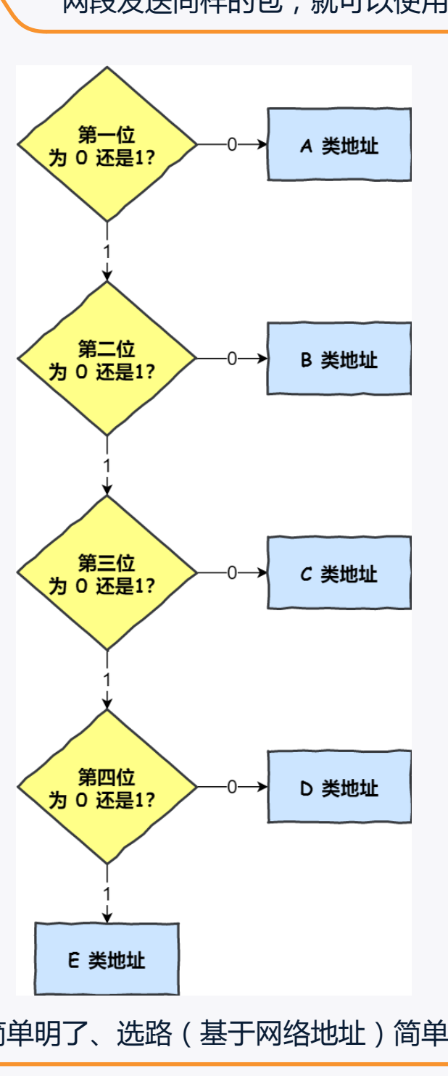
类别	IP 地址范围	最大主机数
A	0.0.0.0 ~ 127.255.255.255	16777214
B	128.0.0.0 ~ 191.255.255.255	65534
C	192.0.0.0 ~ 223.255.255.255	254

  - 什么是「A、B、C」类地址？
    - 「A、B、C」类主要分为两部分，分别是「网络号」、「主机号」
  - 「A、B、C」分类地址最大主机数如何计算？
    - 2^主机号位-2
  - 「A、B、C」分类地址最大主机数为什么要「-2」？
    - IP地址中有两特殊「IP」，分别是主机号全为「1」和全为「0」地址
    - 主机号全为「1」指定某个网络下的所有主机，用于广播
    - 主机号全为「0」指定某个网络
  - 广播地址用于什么？
    - 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
    - 广播地址可以分为
      - 本地广播
        - 在本网络内广播的叫做本地广播。因为这个广播地址的IP包会被路由器屏蔽，所有不会到达其他链路上
      - 直接广播
        - 在不同网络之间的广播叫做直接广播。由于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



类别	IP 地址范围	用途
D	224.0.0.0 ~ 239.255.255.255	IP 多播
E	240.0.0.0 ~ 255.255.255.255	预留使用

  - 什么是「D、E」类地址？
    - 「D、E」类地址没有主机号，所以不可用于主机IP，「D」类常被用于「多播」，「E」类时预留的分类，暂时未使用
  - 多播地址用于什么？
    - 多播用于将发送给特定组内的所有主机
    - 由于广播一般情况下无法穿透路由，若想给其他网段发送同样的包，就可以使用穿透路由的多播



  - IP分类的优点
    - 简单明了、选路（基于网络地址）简单
  - IP分类的缺点
    - 同一网络下没有地址层次
    - 「A、B、C」不能很好的与现实网络匹配
      - C类太少B类又过多
    - 解决IP分类的缺点，引入无分类IP（CIDR）
- 无分类IP地址
  - 怎么划分网络号和主机号？
    - 表示为「a.b.c.d/x」，其中「/x」属于网络号，x的范围是「0-32」

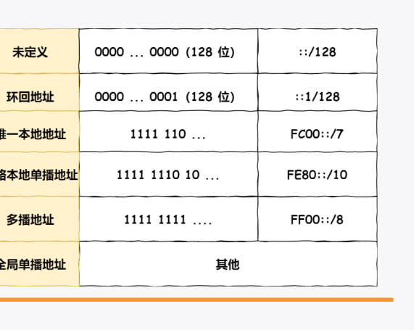
可用地址个数	254
子网掩码	255.255.255.0
网络号	10.100.122.0
第一个可用地址	10.100.122.1
最后可用地址	10.100.122.254
广播地址	10.100.122.255

    - 「10.100.122.2/24」「/24」表示前「24」位是网络号，剩余「8」位是主机号
    - 利用「子网掩码」与IP地址按位「与」，得到网络号
  - 为什么要分离网络和主机号？
    - 两台计算机通信，首先判断是否处于同一个广播域内（网络地址是否相同），如果相同就可以直接把数据包发送目的主机，否则转给路由器，路由器通过相同的方式找到对应网络号的路由器发送

  - 怎么进行子网划分？
    - 子网划分实际上是将主机地址分为两个部分：子网网络地址和子网主机地址
    - 未做子网划分的IP地址：「网络地址+主机地址」
    - 做了子网划分的IP地址：「网络地址+（子网网络地址+子网主机地址）」

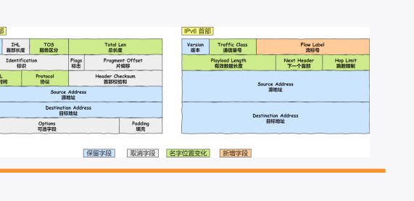
类别	IP 地址范围	最大主机数	私有 IP 地址范围
A	0.0.0.0 ~ 127.255.255.255	16777214	10.0.0.0 ~ 10.255.255.255
B	128.0.0.0 ~ 191.255.255.255	65534	172.16.0.0 ~ 172.31.255.255
C	192.0.0.0 ~ 223.255.255.255	254	192.168.0.0 ~ 192.168.255.255

- 公有IP地址与私有IP地址
  - 在「A、B、C」分类地址，区分「公有IP」和「私有IP」地址（每个公有IP是不能重复的）
  - 公有IP的管理组织
    - 「ICANN（互联网名称与数字地址分配机构）」
- IP地址与路由控制
  - IP地址的「网络地址」这一部分用于进行路由控制。路由控制表中记录着网络地址与下一步应该发送至路由器的地址（在主机和路由器上都会有各自的路由控制表）
  - 发送「IP」包，首先确认IP包首部的目标地址，再从路由控制表找到与该地址具有「相同网络地址」的记录，转发给相应的下一个路由器。如果路由控制表中存在多条相同网络地址记录，则会选择「相同位数」最多的网络地址，就是「最长匹配」
  - 回环地址「127.0.0.1/localhost」使用这个IP地址或主机名时，数据包不会流向网络
- IP分片与重组
  - 当「IP数据包」大于MTU时，「IP数据包」就会被分片，经过分片之后的「IP数据包」在被重组的时候，只能由目标主机进行，路由器是不会进行重组的
- IPV6基本认识
  - IPV6的地址是「128」位，可分配数量大到惊人
  - 亮点
    - 可自动配置，即使没有DHCP服务器也可以实现自动分配IP地址
    - 包头首部长度采用固定「40」字节，去掉了包头校验和，简化了首部结构，减轻路由负荷，大大「提高了传输的性能」
    - 有应对伪造「IP地址」的网络安全功能以及防止线路窃听功能，大大提升了安全性
  - IPV6地址的标识方法
    - IPv6 地址长度是 128 位，是以每 16 位作为一组，每组用冒号「:」隔开。
    - 如果出现连续的 0 时还可以将这些 0 省略，并用两个冒号「::」隔开。但是，一个 IP 地址中只允许出现一次两个连续的冒号。



未定义	0000 … 0000（128 位）	::/128
环回地址	0000 … 0001（128 位）	::1/128
唯一本地地址	1111 110 …	FC00::/7
链路本地单播地址	1111 1110 10 …	FE80::/10
多播地址	1111 1111 ….	FF00::/8
全局单播地址	其他	

  - IPV6地址的结构
    - 单播地址，用于一对一通信
      - 同一链路单播通信，不经过路由器，可以使用「链路本地单播地址」，IPV4没有此类型
      - 内网里单播通信，可以使用「唯一本地地址」，相当于IPV4的私有IP
      - 互联网通信，可以使用「全局单播地址」，相当于IPV4的公有IP
    - 组播地址，用于一对多通信
    - 任播地址，用于通信最近的节点，最近的节点是由路由协议决定
    - 没有广播地址



- IPV4首部与IPV6首部
  - 取消了首部校验和字段
  - 取消了分片/重组相关字段
  - 取消选项字段

IP协议相关技术

- DNS域名解析
  - DNS可以将域名网址自动转换为具体的IP地址
  - 域名的层级关系
    - DNS中的域名都是用「.」来分隔的
    - 在域名中，越靠「右」表示层级越高
- ARP与RARP协议
  - ARP可以通过IP地址找MAC地址
  - ARP借助「ARP请求」与「ARP响应」确定包的「MAC地址」
    - 主机会「广播」发送ARP请求，想要知道目的的「MAC地址」对应的「IP地址」
    - 对应「MAC地址」收到ARP请求，如果符合回复「ARP响应」否则丢弃
  - RARP则是通过MAC地址找对应的IP地址
- DHCP动态获取IP地址
  - DHCP客户端进程监听「68端口」DHCP服务端进行监听「67端口」
  - DHCP工作流程
    - 客户端首先发起「DHCP发现报文（DHCP DISCOVER）」的IP数据报，由于客户端没有「IP地址」，也不知道「DHCP服务器的地址」，所以使用「UDP广播」，广播地址「255.255.255.255（端口67）」并使用「0.0.0.0（端口68）」作为「源IP地址」。将该「IP数据报」传送给链路层，然后广播到所有网络中设备
    - 「DHCP服务器」收到「DHCP发现报文」，用「DHCP提供报文（DHCP OFFER）」向客户端做出响应，该报文信息携带服务器提供「可租约」的IP地址、子网掩码、默认网关、DNS服务器以及「IP地址租用期」
    - 客户端收到一个或多个服务器的「DHCP」提供报文，选中一个服务器，并发送「DHCP请求报文（DHCP REQUEEST）」进行响应，回显配置的参数
    - 服务端用「DHCP ACK报文」回应
    - 租约快到期后，客户端会向服务器发送「DHCP请求报文」，如果服务器同意则用「DHCP ACK」应答，客户端会延长租期，否则使用「DHCP NACK」应答，客户端停止使用租约的「IP地址」
  - DHCP中继代理
    - DHCP全程使用UDP，如果DHCP服务器和客户端不在一个局域网内，路由器不会转发广播包，为了解决出现「中继代理」
    - 「DHCP客户端」会向「DHCP中继代理」发送「DHCP请求包」，而「DHCP中继代理」收到这个广播包之后，再以「单播」的形式发送给「DHCP服务器」
    - 「DHCP服务器」收到包后再向「DHCP中继代理」返回应答，由「DHCP中继代理」将此包广播给「DHCP客户端」
- NAT网络地址转换
  - NAT将私有IP转化为公有IP地址 普通的NAT转换没什么意义。绝大多数网络应用都是使用传输层协议「TCP/UDP」来传输的，因此，可以吧「IP地址+端口号」一起转换。这种转换技术叫「网络地址与端口转化NAPT」
  - 生成一个NAPT路由器的转换表（转换表在NAT路由器上自动生成）例如：在建立TCP首次握手的时候，SYN包一发时就会生成这个表，收到关闭的FIN包的确认应答就会删除
  - NAT缺点
    - 外部无法主动与NAT内的服务器建立连接，因为NAPT转换表没有转换记录
    - 转换表的生成与转换操作都会产生性能开销
    - 通信过程中，如果NAT路由器重启了，所有的TCP连接都将被重置
  - 如何解决NAT的问题
    - 改用IPV6
    - NAT穿透技术
      - 客户端主动从NAT设备获取公有IP地址，自己建立端口映射关系，就不需要NAT设备搭桥，就可以与外通信了
- ICMP互联网控制报文协议
  - ICMP 全称是 Internet Control Message Protocol，也就是互联网「控制」报文协议。
  - ICMP 主要的功能包括：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。
  - 类型
    - 查询报文类型
    - 差错报文类型
- IGMP因特网组管理协议
  - IGMP 是因特网组管理协议，工作在主机（组播成员）和最后一跳路由之间
    - IGMP报文向路由器申请加入和退出组播组，默认情况下路由器是不会转发组播包到连接中的主机，除非主机通过「IGMP」加入到组播组，主机申请加入到组播组时，路由器就会记录「IGMP路由器表」，路由器后续就会转发组播包到对应主机
    - IGMP报文采用「IP封装」，IP头部的协议号为「2」，而且「TTL」字段通常为「1」，因为「IGMP」是工作在主机与连接的路由表之间
  - IGMP工作机制V2版本
    - 常规查询与响应工作
      - 路由器会周期性发送查询报文
      - 组内主机收到查询后会启动「报告延迟计时器」，计时器的时间是随机的，通常是0-10s，超时后发送「IGMP成员关系报告报文（源IP地址为自己主机，目的IP地址为组播地址）」。如果在定时器超时之前，收到同一个组内的其他主机发送的成员关系报文，则自己不再发送，减少网络中多余的「IGMP报文」数量
      - 路由器收到主机的「成员关系报文」后，就会在「IGMP路由表」中加入该组播，后续网络中一旦该组播地址的数据到达路由器就会把数据包转发出去
    - 离开组播工作机制
      - 网段中仍有该组组播
        - 继续常规查询与响应工作
      - 网段中没有该组组播
        - 删除对应信息，不会再向这个网段转发该组播的数据包