

之前说过：Internet是一个由很多网络组成的更庞大的网络，互联网好像一间迷宫，而互连的网络就像这个大迷宫里的一个个小隔间一样。从入口到出口，我们要经过其中很多的小隔间。对于互联网来说也是如此，一台主机访问另一台数据，中间也需要跨越很多的网络。



那么路由是啥意思呢？路由使我们能够向自己所属的网络之外发送消息，我们可以看到，我们发一条消息到其他网络是有很多路径可以选择的，也可以容易想到，肯定有比较快的路径可以到达，这个选择一条合适的路径完成消息的送达就是路由。这是一片广袤的学习区，需要慢慢去探索，这其中涉及一个很关键的硬件，那就是路由器。

## 一、路由器

首先，自然而然地就可以得到一个知识点：**路由器是OSI第三层即网络层（网际层）的硬件设备。**

路由器到底是啥呢？路由器就是一个具有多个网络接口（对应多个网卡）的机器，每个接口可连接到一个网络，它的作用是把接收到的数据报分发到不同的网络。

因此如果你的电脑有两个及以上网卡的时候，理论上就可以作为路由器使用的。只是我们普通的电脑如果没有激活路由功能的话，会将不是发给我们的数据报给丢弃，而不是像路由器一样将不是发给自己的数据报准确分发出去。

wait, wait...你咋拿出了你家的路由器出来呢？哦，你是想问，咱们这里说的路由器是不是就是家里用作为我们提供wifi的路由器啊？？？

家庭路由器功能比较简单，性能也没法跟企业级的路由器比较，毕竟每家的路由器也就最多十几个设备在连接，核心功能就是能上网。那么家庭路由器有哪些功能呢？

家庭无线路由器集成了AP + Switch + Firewall + Router 的功能。看起来是一个多功能结合体的产品。



- AP：无线接入点：就是你电脑要连wifi，需要输入用户名密码来认证。
- Switch：就是我们之前说的交换机，路由器一般留了四个lan口让设备通过网线连接，因此这里提供了交换机的功能，交换机我们了解，不赘述。
- DHCP服务器：给用户分配私网IP、缺省网关、DNS服务器等上网必要参数，这时用户设备才算连上网了。（家庭无线路由器也提供DNS服务器功能），DHCP将在后续进行学习，暂时只要知道它可以动态分配IP即可，比如你的笔记本连接无线路由器后会自动分配一个类似192.168.101.2的IP，这个都要归功于DHCP服务。
- Firewall：可以阻止Internet访问局域网，还可以禁止内部用户访问特定网站，其实就是黑白名单的功能。
- 当访问Internet的流量到达Router时，路由器会根据NAT策略，会做NAT（IP地址转换），然后发到Internet。这里先简单知道下NAT功能即可，即实现私有IP地址和共有IP地址的转换，NAT将在后面文章详细说明，其实也是很简单的，不必担心。

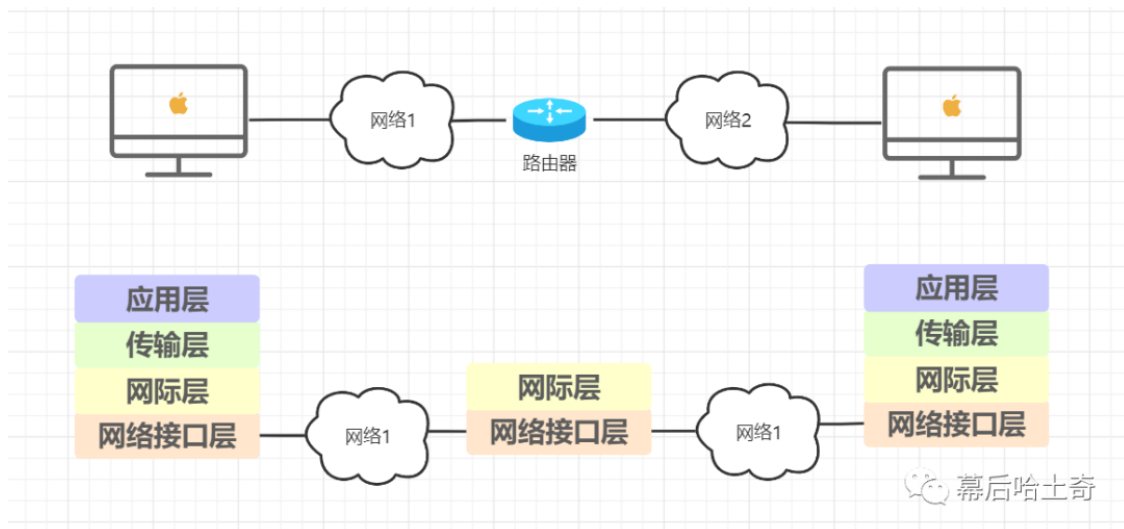
家用路由器跟企业级路由器还是有区别的，无论是功能还是性能上，就好像现在的旗舰智能机和老人机的区别。

企业级路由器一般用在中、大型网络，大企业用于网络寻址，跑复杂OSPF，ISIS路由协议，BGP，对性能、吞吐量、稳定性要求很高。绝没有那些花哨的功能（无线、交换机等功能），钢铁打造，工业级标准，防火防盗防震，价格几万，几十万不等！

这里提到了关键词：路由。这里就有很大的区别了。家用路由器向导配置完，有一条默认路由指向运营商，也就是说，家用路由器真正干的并不是路由这件事（注意这里用的是真正，实际默认路由也算是路由功能，哈哈），而是DNS解析、DHCP、WIFI等功能的大杂烩产品。

对了，路由器还有一个重要功能是隔绝广播域，这个实际上在《17 | 数据链路层篇：虚拟局域网VLAN》中进行过说明，还请读者朋友们记得回顾，不要忘记这个重要知识点。

用于网络互连的路由器中，也带有符合TCP/IP体系结构标准的TCP/IP协议族，只不过路由器一般只包含网络接口层和网际层。由此可以知道路由器只关心IP数据报，那么下面讨论的重点自然就是路由器如何转发的IP数据报，即IP数据报的转发过程。



## 二、IP数据报转发过程

首先GET一个知识点：数据报在被转发的过程中源、目的MAC地址会被修改，但是相关的IP地址不会被修改。（除非NAT做了转换）

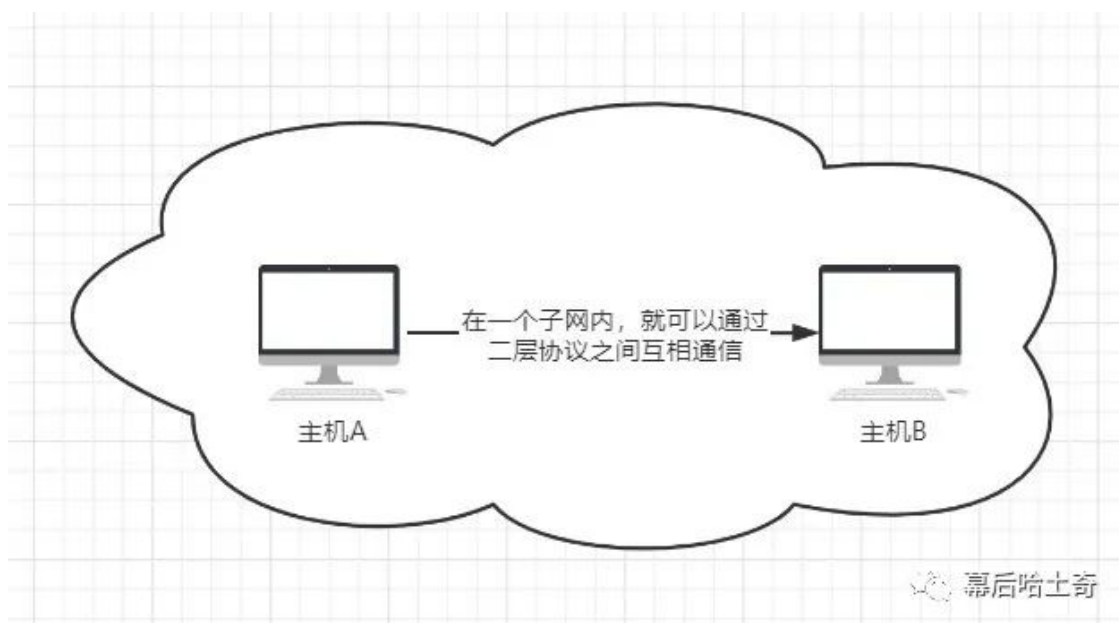
下面就详细说明一下数据包的转发过程。

- 1、主机A打算通过IP地址向主机B发送信息，首先在主机A的网络层中对数据进行组装，其中：
  - 源IP地址：A的IP地址
  - 目的IP地址：B的IP地址



在主机A的网络层，首先判断主机B的IP地址与主机A是否属于同一个子网，具体的做法是：主机A使用自己的子网掩码与主机B的IP地址进行“与”运算，得到的结果跟主机A的网络地址进行对比，如果相同则表示A和B属于同一子网，否则属于不同的子网。

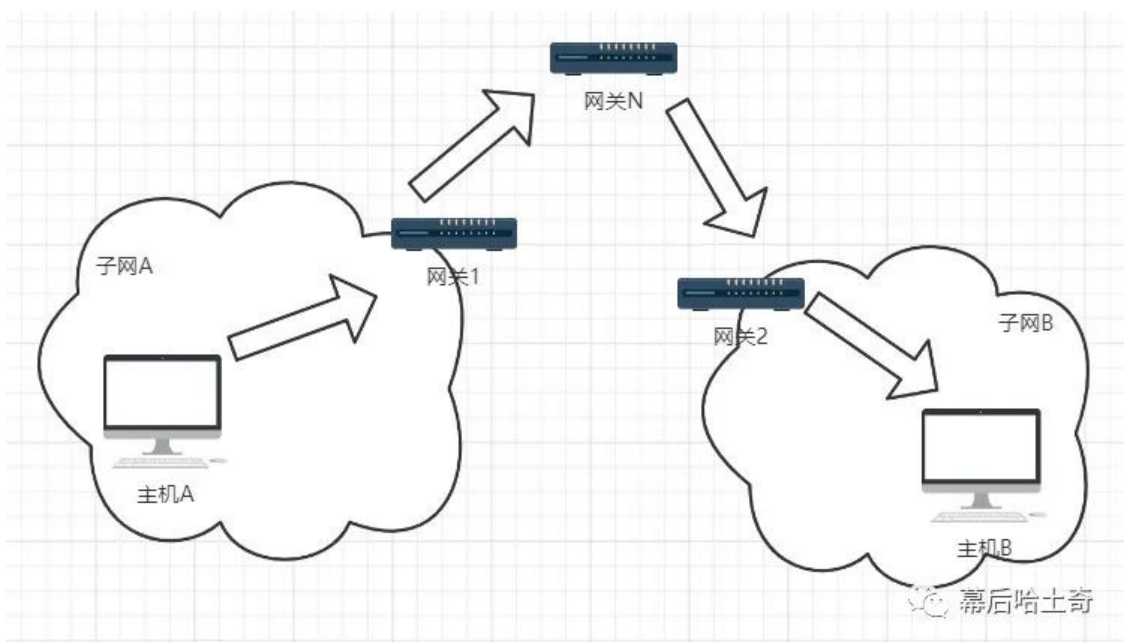
- 2、若A和B属于同一子网，如果A知道B的MAC地址，则在主机A的数据链路层把IP数据包封装成“帧”的形式，其中：
  - 源MAC地址：A的MAC地址
  - 目的MAC地址：B的MAC地址
  - 源IP地址：A的IP地址
  - 目的IP地址：B的IP地址



如果A不知道B的MAC地址，则使用**ARP协议**，发送一个数据包来获取B的MAC地址，获得之后，再使用同样的方法来对IP数据包进行封装。然后直接发给主机B，至此完成数据传输。

关于ARP协议，后续会学习，现在只要明白一点：借助 ARP 协议，我们可以根据 IP 地址获取 MAC 地址。

- 3、若A和B属于不同的子网，A会使用ARP协议发送一个ARP数据包来获取与A相连接的路由器1（即下图的网关1）的MAC地址，之后再在数据链路层对IP数据包进行封装，其中：
  - 源MAC地址：A的MAC地址
  - 目的MAC地址：路由器1（网关1）的MAC地址
  - 源IP地址：A的IP地址
  - 目的IP地址：B的IP地址
- 4、路由器1收到来自内部主机A的数据帧后，知道主机A希望自己转发这个数据帧，于是它就查找自己的路由表，路由器的路由表可以有两种方式进行获得：一是管理员手动添加，称为**静态配置**，另一种是通过路由器转发的记录自动获得，称为**动态配置**。在路由表中查到有与目的IP地址网络地址相对应的下一个路由地址后，这里假设为路由器2，就会对来自A的数据帧进行重组，重组后：
  - 源MAC地址：路由器1的MAC地址
  - 目的MAC地址：路由器2的MAC地址
  - 源IP地址：A的IP地址
  - 目的IP地址：B的IP地址



- 5、路由器2在接收到路由器1发来的数据后，首先进行判断目的IP地址即主机B的IP地址是不是自己的本地网络内的，如果是自己所在的子网，则不再进行转发，将接收的数据进行重新封装：
  - 源MAC地址：路由器2的MAC地址
  - 目的MAC地址：主机B的MAC地址
  - 源IP地址：A的IP地址

- **目的IP地址：B的IP地址**

其中主机B的MAC地址可以通过ARP协议获得。封装后再发给主机B，至此数据传输完成。如果不是，所做的事情跟之前路由器1一样，对其重新进行封装后再转发。

从这个过程，其实我们可以总结几句话：

- 沿途所经过的转发的路由器它们并不知道从主机A到主机B完整的路由路径，它们只是知道自己应该转发的下一个的路由地址。
- 数据包在被转发的过程中源、目的MAC地址会被修改，一般情况下相关的IP地址不会被修改。
- 以上所讲的路由器也可以理解为网关。
- 可通过ARP协议获取下一跳的MAC地址，这个后续文章会详细说明ARP协议，我们目前只要知道这个ARP协议功能是什么即可。

可以看到路由器的关键在于路由表，这个表可以是静态配置的，也可以是学习而来，前者适合小型网络，后者适合大型网络，下一篇文章将详细来叨叨路由表，并且尝试来手工配置下路由表。