[面试·网络] TCP/IP（三）：IP协议相关技术

[面试·网络] TCP/IP（三）：IP协议相关技术

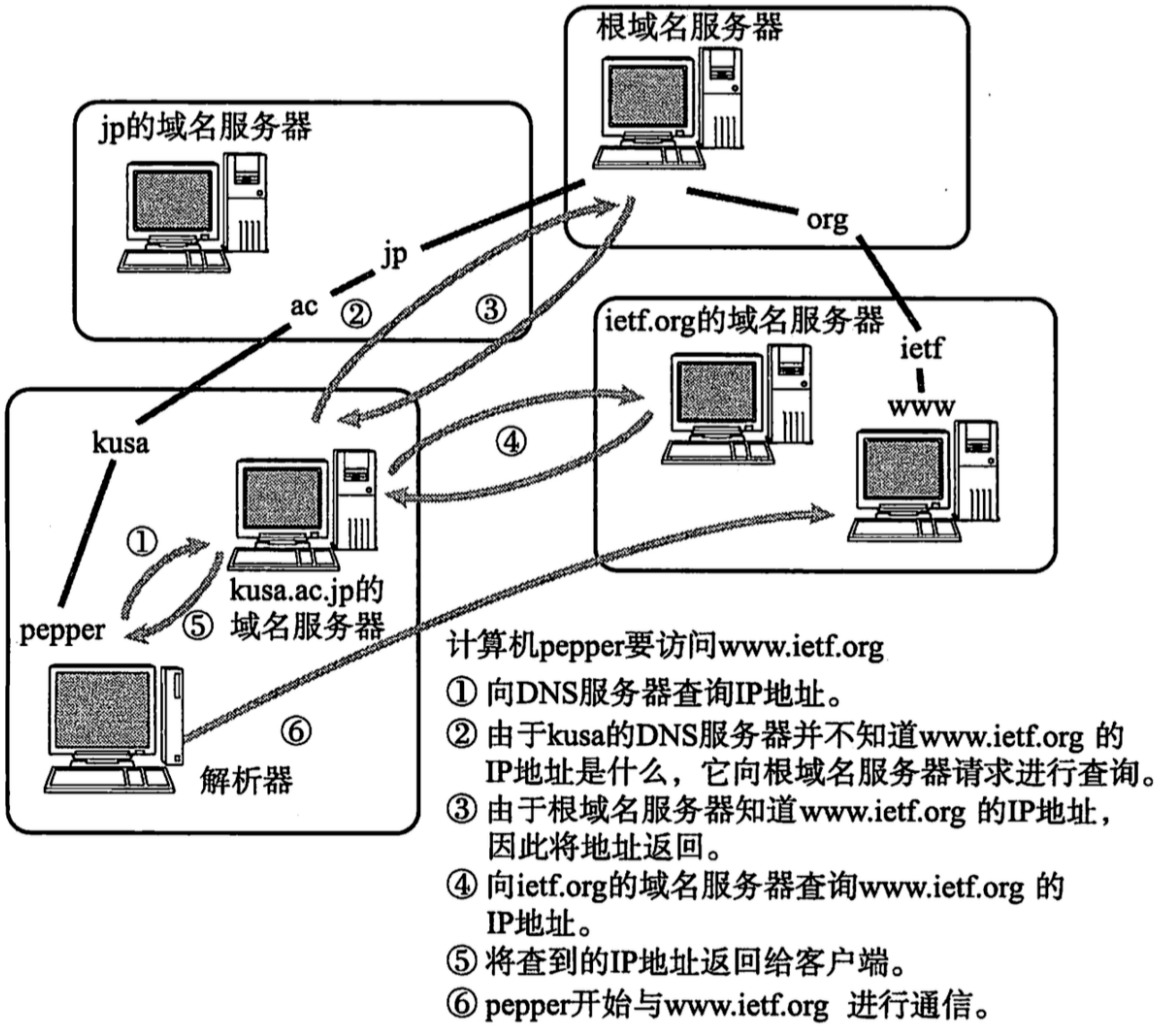
在前两篇文章中，我分别介绍了数据链路层和网络层的IP协议。虽然这个系列教程的重点是搞定 TCP/IP，不过不用着急，本文简要介绍完与 IP 协议相关的技术，下一篇文章就会正式、详细的介绍 传输层与 TCP 协议。这篇文章会介绍 `DNS`、`ARP`、`NAT` 协议，这些内容虽然与 TCP 没有直接关联，但理解它们的原理有助于巩固基础知识，更好的理解网络的工作原理。

DNS 解析

IP地址用于识别通信双方的地址，但它是一串长数字，不方便记忆，人们希望主机有自己自己的名字，这个名字是唯一的，而且容易记住。于是，诞生了“域名”的概念。域名是一种为了识别主机名称和机构名的具有分层的名称，比如在域名 `neu.edu.cn` 中，`neu` 是主机名，`edu` 和 `cn` 是不同层次下的机构名。

域名和 IP 地址都可以唯一对应一台主机，DNS 协议的作用就是将自身具有意义的域名转换成不容易记住的 IP 地址。

域名是分层的，每层都有自己的 DNS 服务器用于处理 DNS 解析的请求。这样的好处在于每层的服务器不用关注过多的信息，它只要知道自己这一层下的域名服务器信息即可。以解析域名：`www.ietf.org` 为例：



DNS解析过程

根服务器其实并不知道 `www.ietf.org` 的 IP 地址，但是它知道 `itef.org` 域名服务器的地址，所以它把这条查询请求转发给 `itef.org` 域名服务器。DNS请求被逐层下发，直到找到对应的 IP 地址为止。

ARP 协议

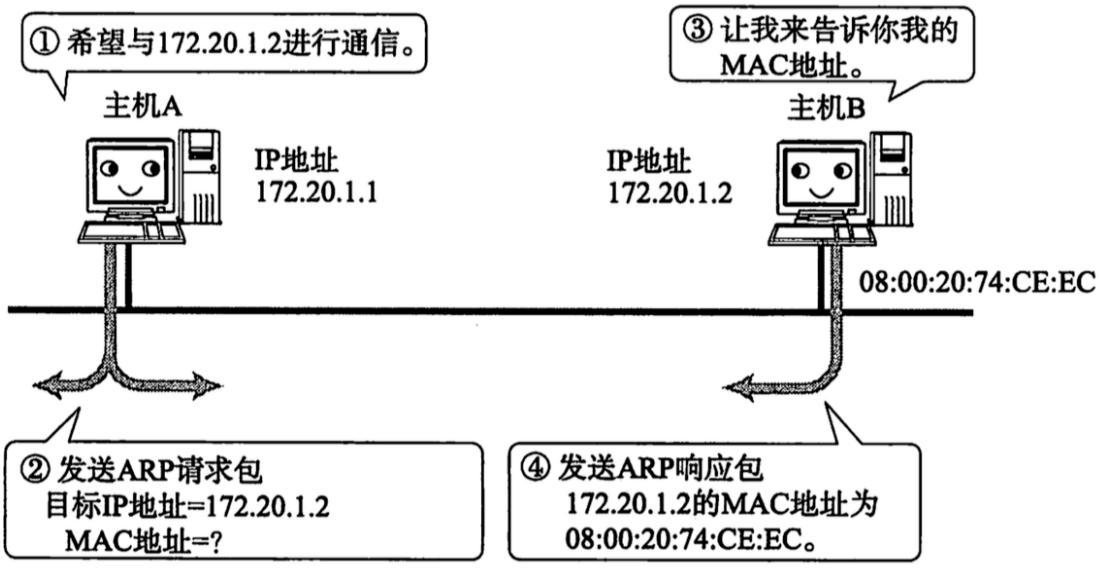
ARP 协议(Address Resolution Protocol)用于通过目标 IP 地址，定位下一个接收数据包的网络设备的 MAC 地址。如果目标主机处在同一个数据链路上，那么可以直接得到目标主机的 MAC 地址，否则会得到下一条路由器的 MAC 地址。

ARP 协议的工作原理可以分为两部分：ARP 请求和 ARP 响应。 首先，源主机会通过广播发送一个 ARP 请求包：“我要与 IP 地址为 `xxx` 的主机通话，谁知道它的 MAC地

址？”。

数据链路上的所有主机都会收到这条消息并检查自己的 IP 地址，如果与 ARP 请求包中的 IP 地址一致，主机就会发送 ARP 响应包：“我就是 IP 地址为 `xxx` 的主机，我的 MAC 地址是：`xxxx`”。

下图表示了 ARP 协议的工作机制：



ARP机制

在实际的使用过程中，每次往目标主机发送数据都要使用 ARP 是很低效的，通常的做法是把获取到的 MAC 地址缓存一段时间。一般来说，一旦源主机向目标地址发送一个数据包，接下来继续发送多次的概率非常大，因此这种缓存非常容易命中。

当下一次发送 ARP 请求或超过一定时间后，缓存都会失效，这保证了即使 MAC 地址与 IP 地址的对应关系发生了变化，数据包依然能够被正确的发往目标地址。

再次强调一下，MAC 和 IP 地址虽然看上去功能类似(都是用于唯一区分主机)，但是两者缺一不可。如果只有 IP 地址，虽然可以跳过 ARP，直接在数据链路上发一个广播，但是这仅适用于通信双方处于同一个数据链路下的情况。如果双方处于不同的数据链路，数据报无法穿透中间的路由器。

如果全世界只用 MAC 地址，那么请参考交换机的自学过程，可以想象这个过程会带来庞大的，不必要的流量。

正因为 MAC 和 IP 地址缺一不可，所以才产生了 ARP 这样的协议将两者关联起来。

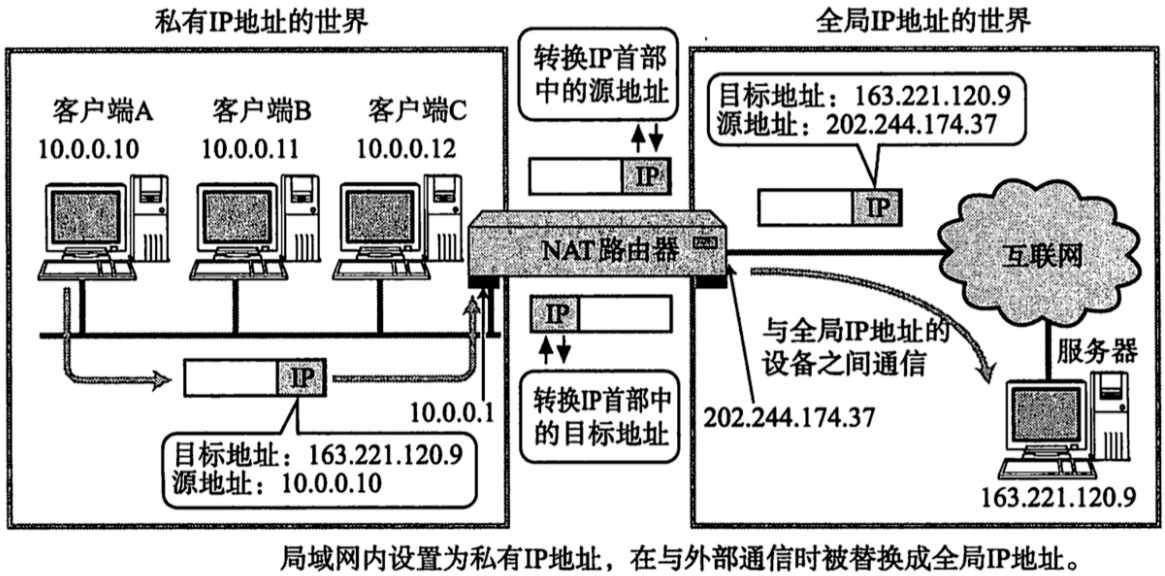
NAT 和 NAPT 技术

NAT (Network Address Translator) 是一种用于将局域网中的私有地址转换成全局 IP 地址的技术。

在连接上无线路由器的时候，如果检查一下设备的 IP 地址，也许你会发现是类似于 `192.168.1.1` 这样的局域网 IP 地址。那不同网段中，IP 地址都是 `192.168.1.1` 的主机改如何通信呢?

下图描绘了 NAT 的工作原理:

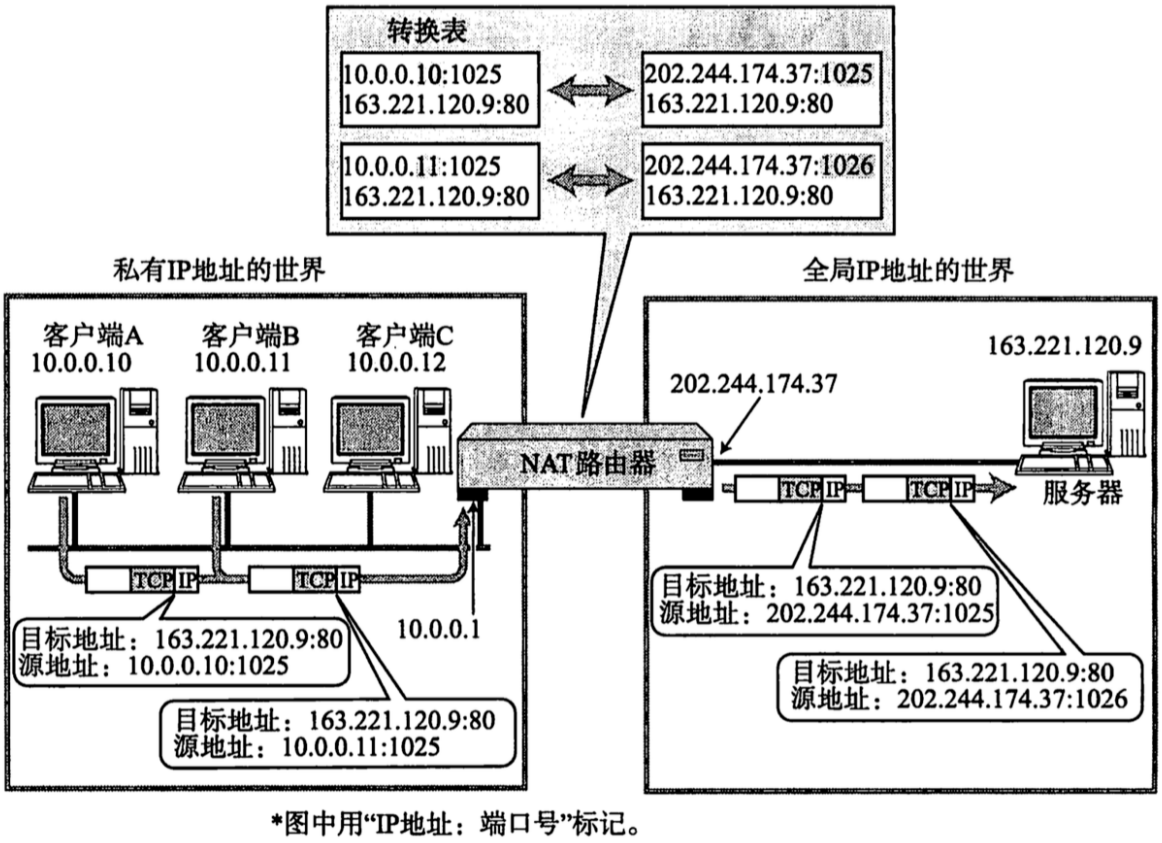
局域网中 IP 地址为 `10.0.0.10` 的主机向全局 IP 地址 `163.221.120.9` 发送数据。NAT 路由器将数据包的源地址修改成自己的全局 IP 地址：`202.244.174.37`。同理，接收数据时，路由器把目标地址 `202.244.174.37` 翻译成内网地址：`10.0.0.10`



NAT工作原理

路由器只有一个对外的全局 IP 地址，如果有多个内网主机都向外部通讯怎么办呢？这时就要使用 NAPT 技术，它和 NAT 从原理上类似，但它可以转换 TCP 和 UDP 端口号。

使用 NAPT 技术时，不同的内网 IP 被转换成同一个公共 IP 地址，也就是路由器对外显示的全局 IP 地址，但是被附加不同的端口号以示区分：



NAPT工作原理

不管是 NAT 还是 NAPT，都需要路由器路由器内部维护一张自动生成的地址转换表。以 TCP 为例，建立 TCP 连接首次握手的 SYN 包发出时会生成这个表，关闭连接时会发出 FIN 包，收到这个包的应答时转换表被删除。

如果暂时不了解 TCP 协议和三次握手也没有关系，下一篇文章将会有详细的讲解。