IP映射原理

由于公网IP地址有限，不少ISP(Internet Service Provider)互联网服务提供商，都采用多个内网用户通过代理和网关路由共用一个公网IP上INTERNET的方法，这样就限制了这些用户在自己计算机上架设个人网站，要实现在这些用户端架设网站，最关键的一点是，怎样把多用户的内网IP和一个他们唯一共享上网的IP进行映射！

先来介绍一下NAT，NAT（网络地址转换）是一种将一个IP地址域映射到另一个IP地址域技术，从而为终端主机提供透明路由。

NAT包括静态网络地址转换、动态网络地址转换、网络地址及端口转换、动态网络地址及端口转换、端口映射等。NAT常用于私有地址域与公用地址域的转换以解决IP地址匮乏问题。

在防火墙上实现NAT后，可以隐藏受保护网络的内部拓扑结构，在一定程度上提高网络的安全性。如果反向NAT提供动态网络地址及端口转换功能，还可以实现负载均衡等功能。

在TCP/IP协议中，我们需要了解两种IP地址，一个是可以直接访问Internet的公网IP地址，另一种是我们组建局域网时最常用到的私有IP地址。如192.168.1.2的IP地址，这个地址就是一个私有地址，它在全球网络中不具唯一性，可以在全球任何一个地方的网络中使用，而公网IP地址在全球网络中是唯一的，主要是起标识不同网络的作用。在互联网中，正是因为有这样的公网IP地址，我们的通信才可以得以实现。 　　但是由于目前公网主要采用的是IPv4，IP地址资源日益耗尽，我们不可能在一个网络中申请到很多个可以在互联网上直接通信的公有IP地址。这时，我们就会使用到NAT技术，它可以将局域网中的如192.168.1.2的私有地址转换为可以在Internet使用的IP地址。从而达到访问Internet的目的。 目前ADSL（Asymmetric Digital Subscriber Line）（ 非对称数字用户线路），普遍采用的是NAT技术中的PAT(Port Address Translation)技术，它将内部地址映射到路由器WAN广域网（WAN，Wide Area Network）端口上的的一个全球唯一的公网 IP 地址上，同时在该地址上加上一个由路由器选定的TCP或UDP端口号。

我的电脑的IP地址为192.168.1.88，路由器的WAN（广域网）端口自动探测到广州电信分配给它的一个公网IP地址，如121.33.117.131。当我的电脑开机后，与路由器连接上，路由器会分配一个端口号给我这条连接，如分配给我的是1444。当我要打开网页时，

我的电脑发送一个数据包到路由器默认网关192.168.1.1，当这个数据包到达路由器的时候，路由器会进行折解数据包的过程，

提取出这个数据包的头部源IP地址192.168.1.88:1444，路由器通过查看NAT表，将数据包的头部源IP地址改为121.33.117.131:1444,并以56.23.5.2:80(www访问的端口号为80)为目的地址将数据包发送到目的网络的服务器上，

服务器做出回应时，以56.23.5.2:80为源IP地址，121.33.117.131:1444为目的地址将数据包发送到路由器上，路由器再查NAT表，找到121.33.117.131:1444对应的内部地址192.168.1.88:1444，于是服务器发回的数据包就发送到了我的电脑上，而不是局域网（LAN）内其他主机上。公网上的服务器只知道IP地址为121.33.117.131的路由器在与它通信，并不知道是我的电脑在与它通信，这对于保护局域网内的主机是有好处的。

一个请求和应答的具体过程：

经以上可以看到，整个Router通过DHCP（Dynamic Host Configuration Protocol，动态主机配置协议）分配IP给LAN局域网（Local Area Network，LAN）上的主机（或手动设置），然而，这些IP是内网IP，无法直接访问外网的。在WAN设置中，使用PPPoE进行拨号后，ISP返回一个动态IP地址给Router，而LAN的主机，就是通过这个IP与外界通信的。

这里实现了NAT（网络地址转换），正是NAT，才能使我们能够共享ADSL上网。

具体实现过程：

NAT Box的位置和操作过程

当一个Packet离开Company Router，通过NAT Box，NAT Box会将该Packet的IP源地址转换为真实的IP地址：198.60.42.12；通常NAT Box都会被集成到Router上。

当应答分组被送回（如一个HTTP请求Web服务器回来的应答），它的目标地址是198.60.42.12,那么NAT Box怎样知道该用那一条地址，即将它转发到那一台主机上呢？

NAT的实际实现方法：现今大多数IP分组携带的要么是TCP净荷，要么就是UDP净荷，两者的Header都包含了一个16位的源端口和目标端口。现以TCP为例，这16位的端口指示了TCP连接从哪里开始，到哪里结束。

当一个进程想与另一远程进程进行TCP连接时，它将绑定到本地机器尚未使用的TCP端口上，即源端口，告诉TCP代码，凡是属于此TCP连接的进来的分组都应发送到该进程。同时，发起进程提供一个目标端口，指明分组被送到远程机器的那个进程。0～1023都是保留端口，用于一些知名的服务，我们熟悉的80端口（Web），21端口（FTP）。

这样，每个向外发送的TCP消息都包含了一个源端口和目标端口。NAT利用源端口解决主机映射问题。

发送分组：任何时候当一个向外发送的分组进入NAT Box时，源地址被真实IP地址取代，而TCP的源端口被索引值取代，该索引值指向NAT Box的地址转换表中的65536表项之一。然后NAT Box计算更新分组的IP头和TCP头的校验和。

接收分组：当一分组从ISP到达NAT盒时，NAT合从TCP头中提取成目标端口（即发送分组的源端口），用它作索引值从NAT Box映射表中找出对应的表项，取出表项的内部IP地址和原来的TCP端口，并将它们插入到分组中，然后重新计算更新分组中的IP头和TCP头的校验和，并将该分组转发到内网上，然后就可以使用内网IP地址进行正常路由了。

总结：这类Router的功能简单，内置包含了DHCP服务器和NAT转换功能，但不具备路由配置功能。

虽然内部地址可以随机挑选，但是通常使用的是下面的 地址：10.0.0.0~10.255.255.255，172.16.0.0~172.16.255.255，192.168.0.0~192.168.255.255。NAT将这些无法在互联网上使用的保留IP地址翻译成可以在互联网上使用的合法IP地址。而全 局地址，是指合法的IP地址，它是由NIC（网络信息中心）或者ISP(网络服务提供商)分配的地址，对外代表一个或多个内部局部地址，是全球统一的可寻 址的地址。