

# 实验 5 学习 NAT 技术

## 实验 1：学习 PAT 配置

参考资料：

<https://blog.51cto.com/victoryan/40266>  
<https://wenku.baidu.com/view/8d176093d1f34693dbef3e36.html>

- 1. 实验目的
  - (1) 掌握内部网络设计过程和私有地址使用方法。
  - (2) 学习 PAT 工作机制。
  - (3) 熟练掌握 PAT 的配置过程。

- 2. 技术原理

由于 NAT 实现是私有 IP 和 NAT 的公共 IP 之间的转换，那么，私有网中同时与公共网进行通信的主机数量就受到 NAT 的公共 IP 地址数量的限制。为了克服这种限制，NAT 被进一步扩展到在进行 IP 地址转换的同时进行 Port 的转换，这就是 PAT 技术。

PAT 适用于网络中只有一个内部全局地址的情况，将多个内部终端私有 IP 地址映射为一个公网 IP 地址。

PAT 与 NAT 的区别在于，PAT 不仅转换 IP 包中的 IP 地址，还对 IP 包中 TCP 和 UDP 的 Port 进行转换。

### 3. 实验场景描述



图 1 学习 PAT 技术的网络拓扑图

- 4. 任务要求：
  - (1) 构建如图 1 所示的拓扑图，根据拓扑图进行试验；

(2) 为各个路由器接口配置 IP 地址和子网掩码, 指定某些路由器接口为内部接口(ip nat inside)和外部接口(ip nat outside), 并开启端口;

(3) 对 router1 进行 PAT 配置: 1) 定义允许进行地址转换的私有地址范围 (access-list access-list-number permit source); 2) 定义一个全球地址池 (ip nat pool name start-ip end-ip netmask netmask); 3) 将允许进行地址转换的私有地址范围与某个公网 IP 地址进行绑定 (ip nat inside source list access-list-number pool name); 4) 创建本地 IP 地址和端口号与公网 IP 地址和端口号的映射 (ip nat inside source static tcp local-ip local-port global-ip global-port)

(4) 配置各 PC 终端的 IP、子网掩码和默认网关, 并通过 ping 命令验证网络的连通性;

(5) 内部网络终端可以通过浏览器访问公共网络中的服务器。

(6) 查看路由器的 NAT 转换表 (show ip nat translations)。

(7) 进入模拟操作模式, 在终端 A 上捕获终端 A 发送给服务器 2 的 IP 分组, 再在服务器 2 上查看终端 A 发给服务器 2 的 IP 分组。

## 实验 2: 学习动态 NAT 和静态 NAT

参考资料: [https://blog.csdn.net/m0\\_37681914/article/details/72860274](https://blog.csdn.net/m0_37681914/article/details/72860274)  
[https://blog.csdn.net/qj\\_37992321/article/details/84866133](https://blog.csdn.net/qj_37992321/article/details/84866133)

### 1. 实验目的

- (1) 掌握内部网络设计过程和私有地址使用方法。
- (2) 学习 NAT 工作机制。
- (3) 熟练掌握 NAT 的配置过程。

### 2. 技术原理

为了解决 IP 地址短缺的问题, 人们提出了许多解决方案, 在众多的解决方案中, 网络地址转换 NAT (Network Address Translation) 技术提供了一种完全将私有网和公共网隔离的方法, 从而得到了广泛的应用。

NAT 技术的基本功能就是, 用 1 个或几个 IP 地址来实现 1 个私有网中的所有主机和公共网中主机的 IP 通信。NAT 技术可为 TCP、UDP 以及 ICMP 数据包提供透明转发。

NAT 的基本工作原理是, 当私有网主机和公共网主机通信的 IP 包经过 NAT 网关时, 将 IP 包中的源 IP 或目的 IP 在私有 IP 和 NAT 的公共 IP 之间进行转换。

### 3. 实验场景描述

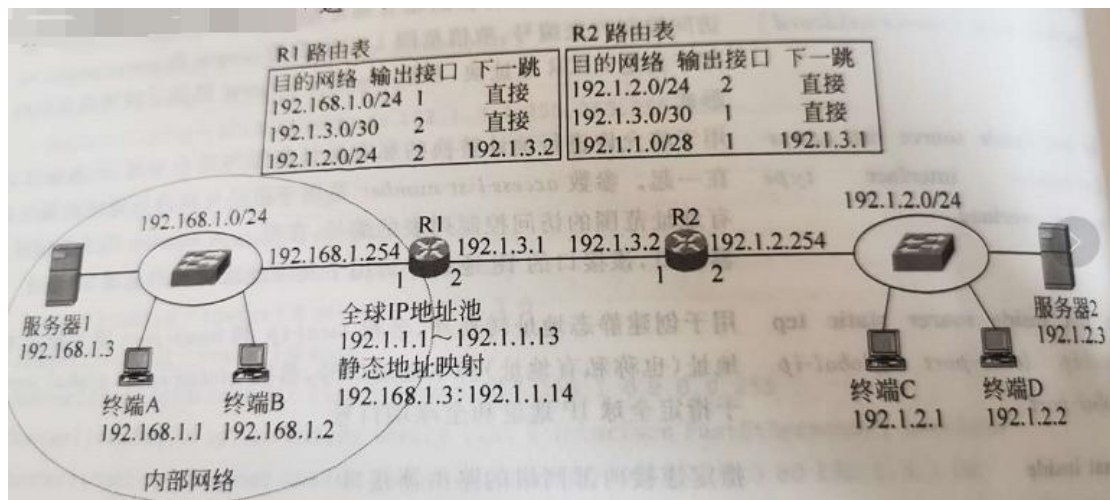


图2 学习动态 NAT 和静态 NAT 的网络拓扑图

#### 4. 任务要求：

- (1) 构建如图2所示的拓扑图，根据拓扑图进行试验；
- (2) 为各个路由器接口配置 IP 地址和子网掩码，指定某些路由器接口为内部接口(p nat inside)和外部接口(ip nat outside)，并开启端口；
- (3) 对 router1 进行动态 NAT 和静态 NAT 配置(全局配置)：1) 定义允许进行地址转换的私有地址范围 (access-list access-list-number permit source)；2) 定义一个全球地址池 (ip nat pool name start-ip end-ip netmask netmask)；3) 将允许进行地址转换的私有地址范围与某个公网 IP 地址进行绑定 (ip nat inside source list access-list-number pool name)；4) 创建私有地址与全球地址之间关联的静态地址转换项 (ip nat inside source static local-ip pool global-ip)。
- (4) 配置各 PC 终端的 IP、子网掩码和默认网关，并通过 ping 命令验证网络的连通性；
- (5) 内部网络终端可以通过浏览器访问公共网络中的服务器。
- (6) 查看路由器的 NAT 转换表 (show ip nat translations)。
- (7) 进入模拟操作模式,在终端 A 上捕获终端 A 发送给服务器 2 的 IP 分组，再在服务器 2 上查看终端 A 发给服务器 2 的 IP 分组。