

NAT 网络地址转换技术教学实例

赵 涛

(兰州石化职业技术大学, 甘肃 兰州 730000)

摘要：相信很多网络的使用者经常会看到某一台局域网内的 PC 的 IP 地址是 10、172、192 开头的，这三类分别属于 IPV4 地址的 A 类、B 类和 C 类地址的私网 IP 地址，并不是真正能用来上因特网的公网 IP 地址；而且，如果局域网内的某一台 PC 的 IP 地址直接被广域网的另一台 PC 看到的话，安全性也大打折扣。以下是本人总结的一个案例，是解决了私网 IP 转换为公网 IP 地址以实现上网功能，又可以保护局域网 PC 不受外网攻击的一个案例。

关键词: NAT; 网络地址转换; 共有 IP 地址; 地址耗尽

公网 IP 地址是全球唯一的，就像网上买东西，你的地址不唯一自然也不能精准的发到你家。既然私网 IP 地址不能直接用来上网，那为什么不直接使用公网 IP 地址呢？首先是因为全球公网 IPv4 地址枯竭，没有更多的 IP 用来随意浪费；其次，公网 IP 地址都要从 IPS 网络运营商那里购买，需要成本支出。所以私网 IP 地址应运而生，A 类、B 类和 C 类都有自己的私网 IP 地址，而且这些私网 IP 可以在任何局域网内重复出现，从而保证 IPv4 的用户和业务能平稳过渡到 IPv6。

一、NAT 网络地址转换技术介绍

（一）NAT 的含义

首先 NAT (Network Address Translation) 是一种 IP 地址转换技术, 可以实现多个 PC 共享已经快要用尽的公网 IPv4 地址来访问外部网络 (因特网)。PC 访问公网 (因特网) 时, 可以利用具备 NAT 功能的设备将用户局域网的私网 IPv4 地址转换为公网的 IPv4 地址, 暂时记录这种映射关系。这样一来可以很大程度上降低 IPV4 地址的用尽速度, 延长了 IPV4 的使用寿命, 除此之外, NAT 技术在网络迁移、融合及服务器负载和共享等方面也很常用, 接下来将针对 NAT 网络地址转换技术的实现过程做大概介绍。

（二）NAT 网络地址转换技术的分类

1. 静态 NAT

功能：一对一转换，将一个静态且唯一的本地 IP 地址映射到一个唯一的公网 IP 地址，使得内网的服务器处于一个更安全的运行环境，多用在企业和内部服务器的网络地址转换，当然，一对一的 NAT 网络地址转换并不能起到节约公网 IP 地址的作用。指令：

```
ip nat inside source static 192.168.1.2 203.10.5.23
```

（将一个 C 类私网 IP 地址替换为内部全局地址）同时还需要向 NAT 设备声明所用端口是内网端口还是外网：ip nat inside 或 ip nat outside

2. 动态 NAT

功能：多对一或多对多，可以将大量的私网 IP 地址转换为存于创建好的地址池当中的一个或多个公网 IP 地址的技术。配合

ACL 访问控制列表使用。配置：

创建公网 IP 地址池（私网全局地址池 pool）：`ip nat pool`
`dizhichi 203.10.5.25 203.10.5.30 netmask 255.255.255.0` 结合 ACL
访问控制列表来声明哪些私网 IP 地址需要转换：`access-list 1-99`
`permit host 192.168.1.0` 最后将 ACL 列表投入到公网 IP 地址池当
中进行投射转换：`ip nat inside source list 1-99 pool dizhichi` 当
然也需要像 NAT 设备声明所用端口是内网口还是外网口：`ip nat`
`inside` 及 `ip nat outside`

二、静态 NAT 网络地址转换技术案例说明

**** 实验目的：**实现局域网内部服务器上网，并保护服务器 IP 地址不受外网攻击

(一) 拓扑图

以下利用思科模拟器 Packet Tracer 做了一个静态 NAT 网络地址转换的案例，其主要作用有 2 点，1——在节省上网成本的前提下使得内网的服务器可以利用公网 IP 地址进行上网；2——从外网不能直接看到内网服务器的 IP 地址，起到保护内网服务器的作用。详细图文过程如下图 1。

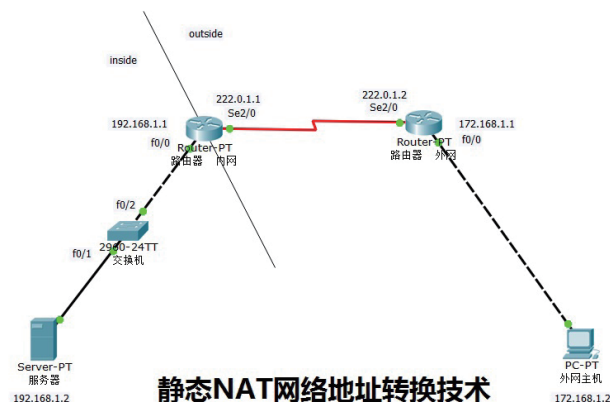


图 1 静态 NAT 网络地址转换

（二）开启路由器各个端口并配置 IP 地址

此案例拓扑图中包含一台服务器 Server、一台外网主机、一个二层交换机、两台可扩展路由器，以及用到的线路，包括直连线、

交叉线和 DCE 同步串口线。

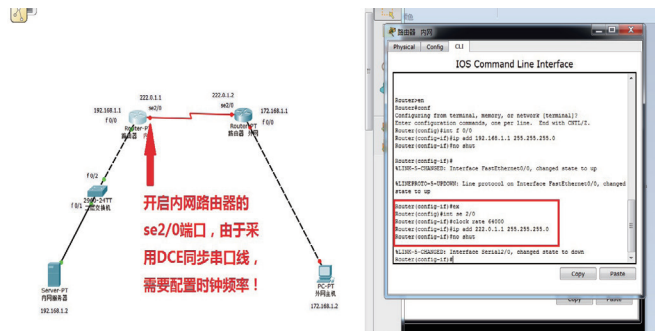


图2 开启内网路由器的串口 se2/0 端口, 并配置时钟频率和公网 IP 地址

(三) 开启外网路由器的端口, 并配置 IP 地址

(四) 配置两台路由器的静态路由协议, 使得全网互通

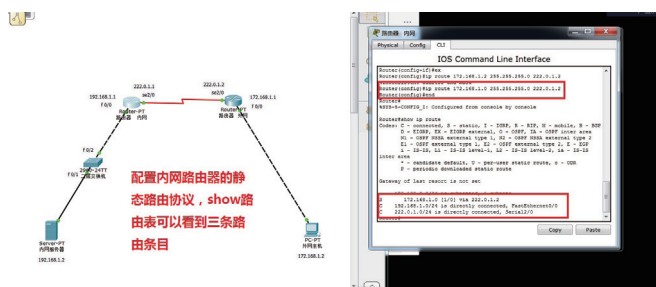


图3 配置路由器的静态路由

(五) 给内网路由器宣告内网端口和外网端口, 并标注转换公网的 IP 地址

Interface f0/0; Interface se2/0

ip nat inside 或 ip nat outside

(六) 展示 NAT 转换情况

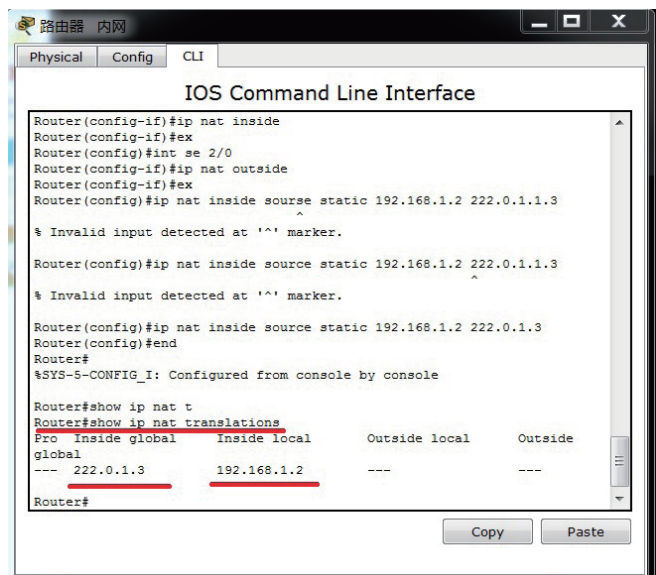


图4 show ip nat translations

可以从上图看到, 此时 show ip nat translations 还只能看到内网的转换情况, 并没有访问外网服务器的信息。

(七) 通过外网主机访问内网服务器

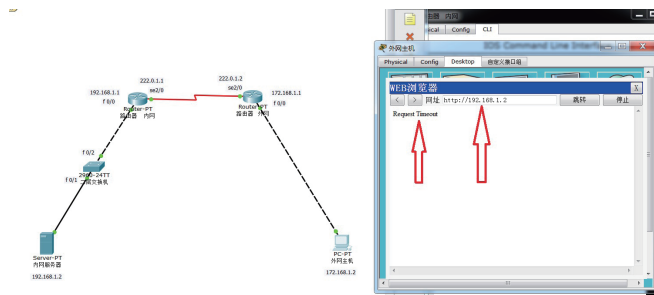


图5 通过外网 PC 浏览器访问内网 IP 地址

很显然 Request Timeout 告诉我们, 用外网主机访问内网服务器的 C 类私网 IP 地址时不能访问, 只能用 NAT 网络地址转换后的公网 IP 地址进行访问。

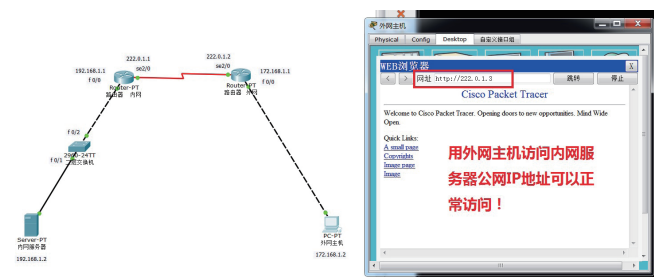


图6 访问转换后的公网 IP 地址

三、结语

综上所述, 通过此案例, 我们详细地分析了静态 NAT 网络地址转换技术在局域网当中的作用, 既可以保护内网的服务器不受外网的威胁, 又可以给内网的主机或服务器提供少量或者唯一的公网 IP 地址来提供上网服务。

参考文献:

- [1] 杨晓鸣, 孙晓亮, 王彪. 下一代互联网网部署及其物联网应用实例 [J]. 物联网技术, 2014, 4 (11) : 5.
- [2] 周赞山. 语音数据报 NAT/FW 隧道穿越的实例研究 [J]. 数字技术与应用, 2011 (5) : 3.
- [3] 李清平. 校园虚拟局域网 DHCP 结合 PAT 技术的综合应用 [J]. 黄冈职业技术学院学报, 2019, 21 (1) : 5.