网络技术与应用课程实验报告

实验六：NAT 的配置

学　　院　密码与网络空间安全学院

专　　业　信息安全、法学双学位班

学　　号　2313815

姓　　名　段俊宇

班　　级　信息安全、法学双学位班

一、实验目的

1. 仿真环境下学习路由器的NAT配置过程，参考实体实验，组建由NAT连接的内网和外网，测试网络的连通性，观察网络地址映射表，通过“模拟”方式观察IP数据报在互联网中的传递过程，并对IP数据报的地址进行分析。

2. 在仿真环境下的内部网络中放置一台Web服务器，设置NAT服务器并使外部主机能够顺利使用该Web服务。

二、实验原理

1. NAT网络地址转换

网络地址转换（NAT） 是一种在IP数据包通过路由器时修改其源或目的IP地址的技术，主要用于解决IPv4地址短缺问题。它允许多个内网设备共享一个或少数几个公网IP地址访问互联网，同时对外隐藏内网拓扑结构，提供基础的安全防护。NAT通过维护地址映射表实现内外网地址的动态转换，常见类型包括静态NAT、动态NAT和PAT。虽然NAT延长了IPv4的生命周期，但也增加了网络复杂性，可能影响某些网络协议的正常工作。

三、实验过程

1.仿真环境下的NAT服务器配置

1.1 学习路由器的NAT配置过程

路由器的NAT配置需要定义内网访问控制列表，配置内网和外网的接口，最后还需要配置端口地址转换，明确转换规则。命令如下：

命令名称	命令作用
ip nat inside	标记该接口为内网接口
ip nat outside	标记该接口为外网接口
access-list <number> permit <内网网络地址><通配符掩码>	访问编号为number的控制列表，允许所有源IP地址属于指定网段的数据包通过，通配符掩码是子网掩码取反得到的，内网网络地址和通配符掩码共同构成了指定网段，例如192.168.1.0/24网段的网络地址是

	192.168.1.0，通配符掩码是 0.0.0.255
ip nat inside source <内网访问控制列表> <外网接口的 IP 地址> overload	该命令用于指定 NAT 转换方向，inside 表示内网的转换方向，内网控制列表就是前面的编号，例如 list 1。overload 表示启用端口地址转换

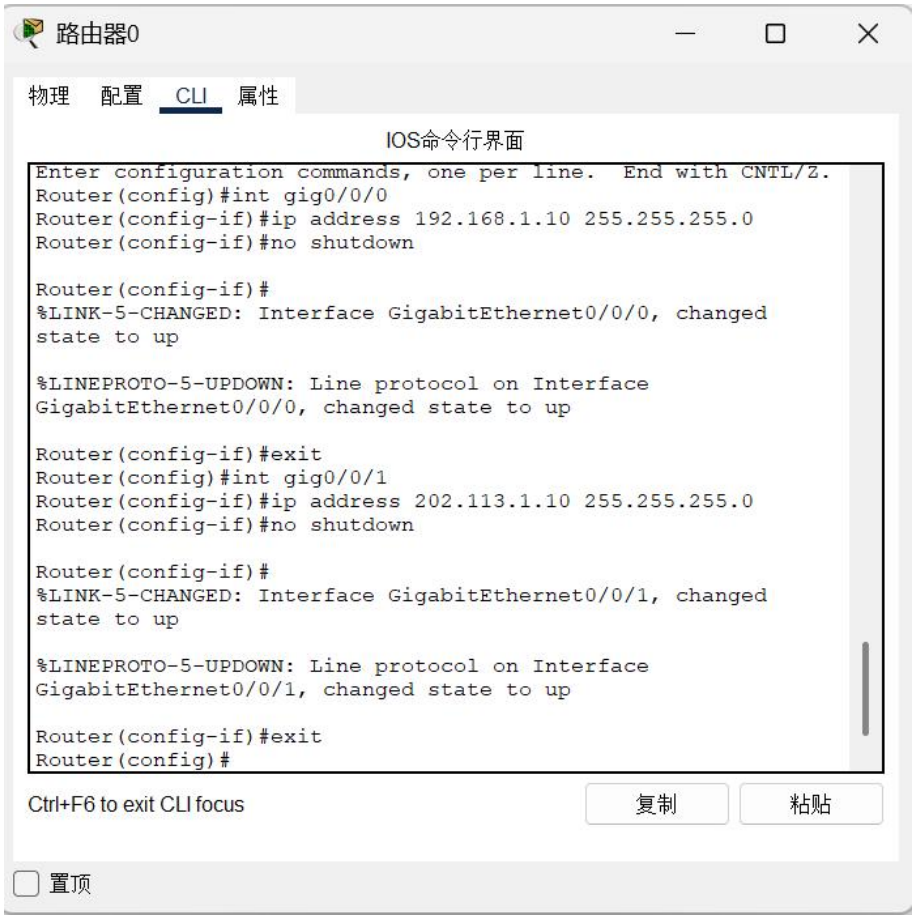
1.2 参考实体实验，组建由 NAT 连接的内网和外网

在组建内网和外网时，我一共用到了 3 台主机、1 台服务器、2 台交换机和 1 台路由器，网络拓扑图如下所示：

主机和服务器的 IP 配置如下所示：

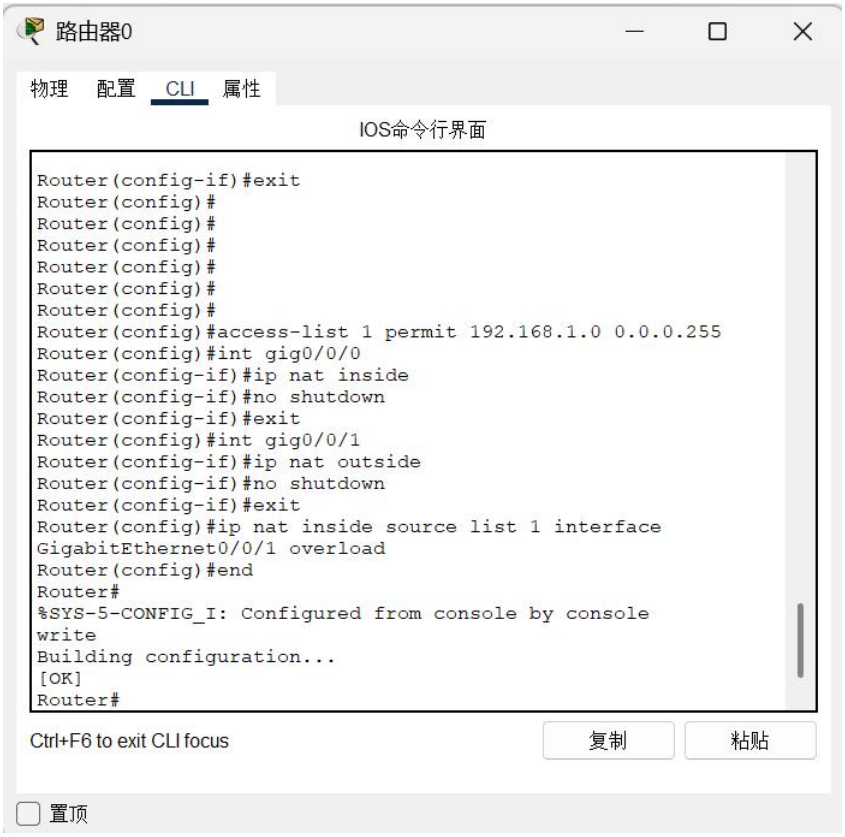
设备名称	IP 地址	子网掩码	网关地址
PC0	192.168.1.1	255.255.255.0	192.168.1.10
PC1	192.168.1.2	255.255.255.0	192.168.1.10
PC2	202.113.1.1	255.255.255.0	202.113.1.10
服务器 0	202.113.1.2	255.255.255.0	202.113.1.10

接下来配置路由器的端口，内网包含 PC0 和 PC1，路由器接口为 GigabitEthernet0/0/0；外网包含 PC2 和服务器 0，路由器接口为 GigabitEthernet0/0/1。配置内网接口时，先进入该接口，然后使用 ip address 192.168.1.10 255.255.255.0 配置，外网同理。配置如下所示：



接下来配置 NAT，命令如下：

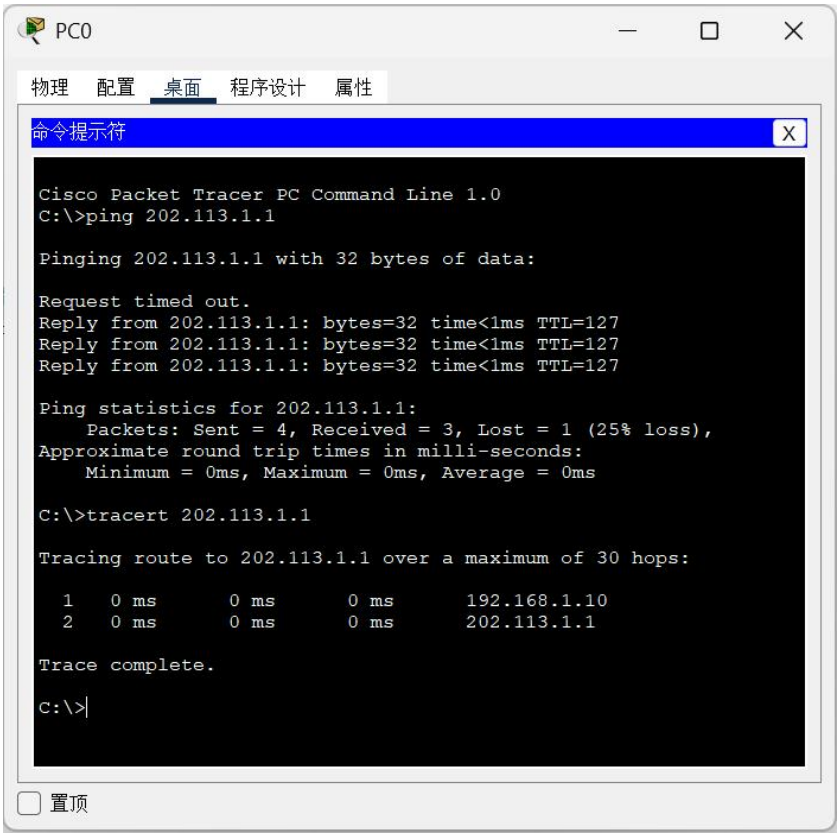
```
configure terminal
// 定义内网访问控制列表
access-list 1 permit 192.168.1.0 0.0.0.255
// 配置内网
interface GigabitEthernet0/1
 ip nat outside
 exit
// 配置外网
interface GigabitEthernet0/0
 ip nat inside
 exit
// 配置端口地址转换
ip nat inside source list 1 interface GigabitEthernet0/0/1 overload
```



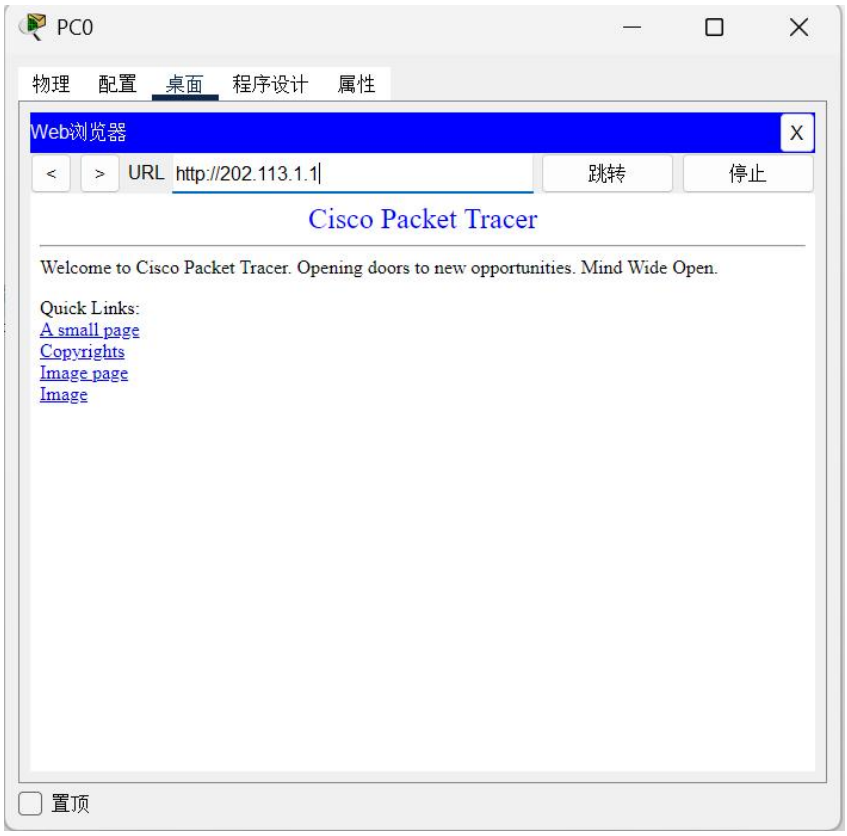
这样就配置好了路由器的 NAT 部分，下面进行连通性测试。

1.3 测试网络的连通性，观察网络地址映射表

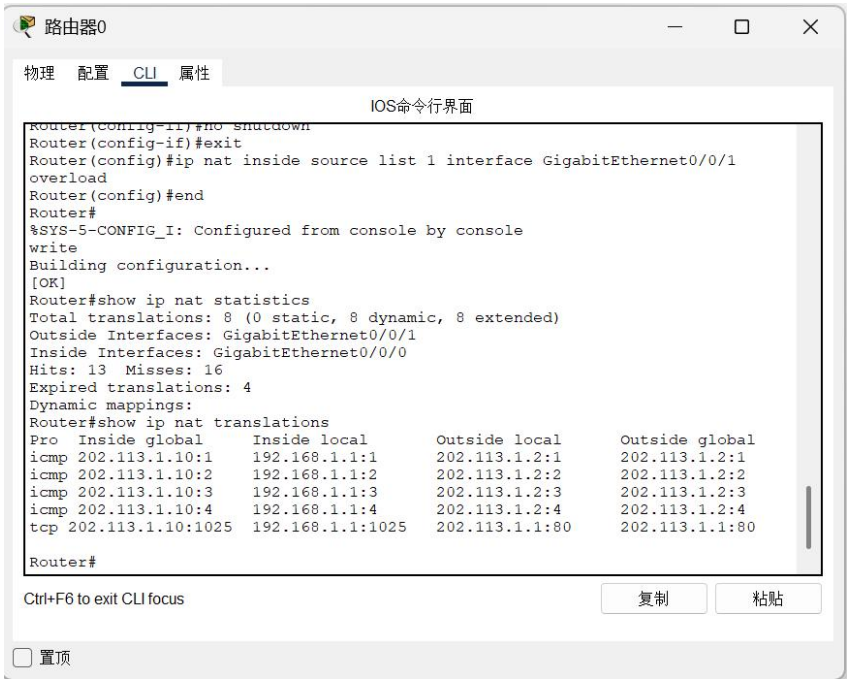
首先测试 PC0 是否能够访问外网服务器，结果如下所示：



说明内网访问外网没有问题，然后在 PC0 的浏览器中访问外网服务器，发现也成功，说明配置没有问题



接下来观察网络地址映射表，使用 ip nat statistics 命令查看 NAT 运行状态和统计信息，使用 ip nat translations 命令查看当前活动的 NAT 转换表，结果如下所示：



从上图可以发现动态创建了 8 个活动状态，其中四个已经过期了，而下面展示了网络地址的映射，inside global 是外网“看到”的内网主机，此处是路由器接口 IP；inside local 是内网真实主机的 IP；outside local 是内网主机“看到”的外网主机 IP；outside global 是外网主机真实的 IP，这些非常详细地展现了网络地址的映射过程。

1.4 在仿真环境的“模拟”方式中观察 IP 数据报在互联网中的传递过程，并对 IP 数据包的地址进行分析

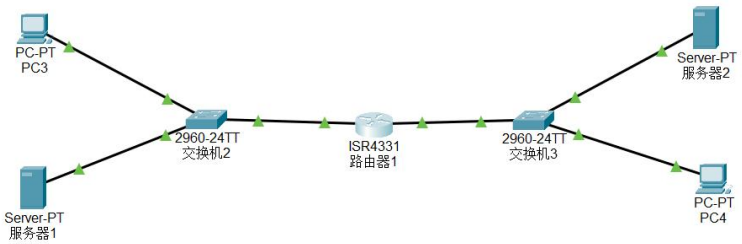
下面使用仿真的形式观察数据包的传递，结果如下所示：

Vis.	时间(秒)	上一台设备	在设备上	类型
	0.000	--	PC0	ICMP
	0.001	PC0	交换机0	ICMP
	0.002	交换机0	路由器0	ICMP
	0.003	路由器0	交换机1	ICMP
	0.004	交换机1	服务器0	ICMP
	0.005	服务器0	交换机1	ICMP
	0.006	交换机1	路由器0	ICMP
	0.007	路由器0	交换机0	ICMP
Visible	0.008	交换机0	PC0	ICMP

从上图可以发现，所有的协议都是 ICMP 协议，数据包情况正常。在传输时依次经过了内网交换机、路由器、外网交换机，然后到达外网服务器，返回的数据包经过了外网交换机、路由器、内网交换机，最终到达了内网主机被接收。

2. 在仿真环境下完成外网主机访问内网服务器的实验

该实验在上面实验的基础上进行，需要在内网中放置一台服务器，实现外网设备对内网服务器的访问。网络拓扑图如下所示：



主机和服务器的 IP 地址如下所示：

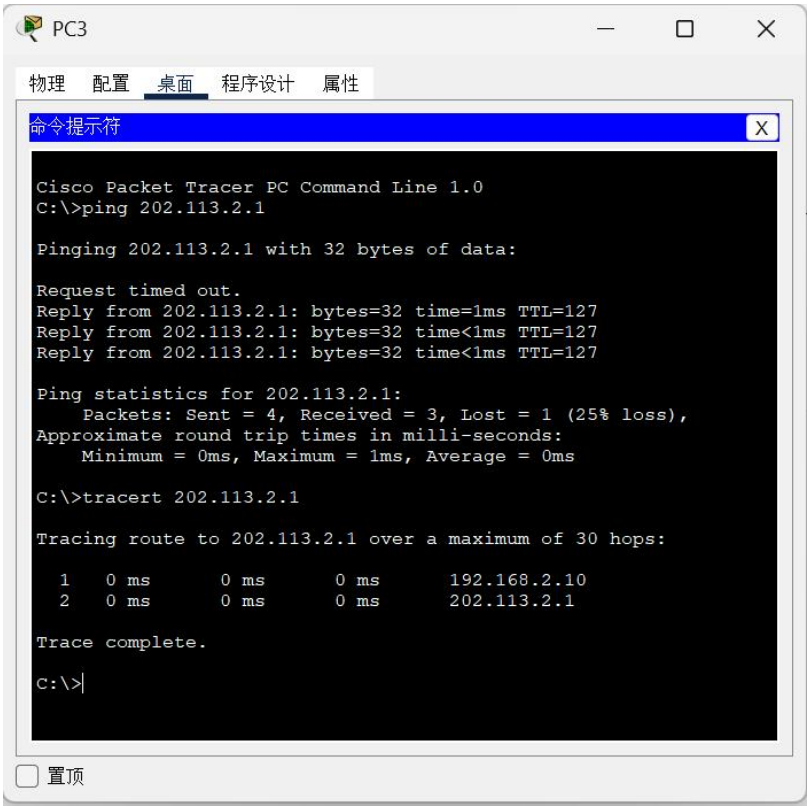
设备名称	IP 地址	子网掩码	网关地址
PC3	192.168.2.1	255.255.255.0	192.168.2.10

服务器 1	192.168.2.2	255.255.255.0	192.168.2.10
服务器 2	202.113.2.1	255.255.255.0	202.113.2.10
PC4	202.113.2.2	255.255.255.0	202.113.2.10

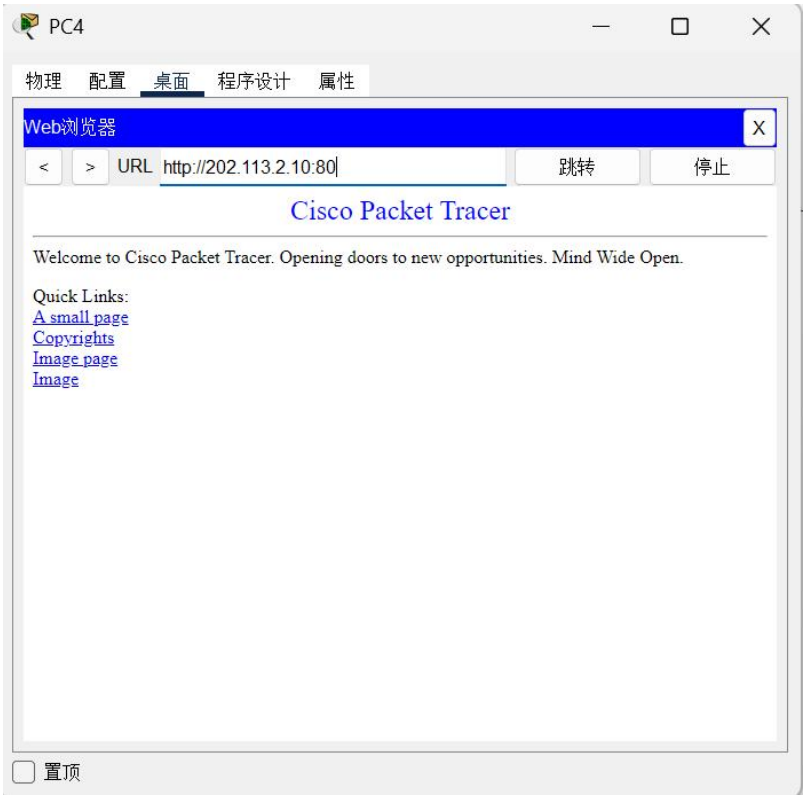
基础配置与上面相同，不再赘述。配置好上一个实验的环境后，需要在路由器添加外网主机访问内网服务器接口，命令为 ip nat inside source static tcp 192.168.2.2 80 202.113.2.10 80，配置如下所示：

```
Router#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#ip nat inside source static tcp 192.168.2.2 80
202.113.2.10 80
Router(config)#exit
Router#
%SYS-5-CONFIG_I: Configured from console by console
write
Building configuration...
[OK]
```

这里说明内网服务器的开放端口为 80，而路由器转发端口也为 80。先测试内网主机和外网主机的连通性，结果如下所示：



这说明连通性没问题，接下来使用外网主机访问内网服务器，注意地址栏中需要输入的是外网网关 IP，也就是路由器的外网接口，而不能直接访问内网服务器。访问后发现成功，结果如下所示：



这样就完成了实验的全部内容！

四、实验结论及心得体会

本次实验我在仿真环境下配置了 NAT，并实现了外网主机访问内网服务器。在实验过程中，配置 NAT 时因为没有指定 NAT 方向而出现了问题，后来经过排查成功解决了问题。这次实验加深了我对 NAT 以及内网和外网的理解，也让我明白了外网主机访问内网服务器需要访问的是路由器接口，而不是内网服务器的 IP，巩固了课上学习的知识。