南開大學
Nankai University

南　　开　　大　　学

网 络 空 间 安 全 学 院

网络技术与应用

仿真环境下的 NAT 配置

学号：2013018

姓名：许健

年级：2020 级

专业：信息安全

2022 年 11 月 24 日

目录

一、 实验内容说明 **1**
（一） 实验题目 1
（二） 实验要求 1

二、 内网访问外网 **1**
（一） 网络拓扑图 1
（二） 配置 NAT 和 Web 服务器 1
（三） 连通性测试 3
（四） 查看 NAT 工作状态 3
（五） 仿真模拟 IP 数据包的传递 4

三、 外网访问内网 **5**
（一） 网络拓扑图 5
（二） 配置静态 NAT 6
（三） 连通性测试 6

四、 扩展学习 **6**
（一） NAT 穿透 6
（二） SNAT 和 DNAT 7

一、 实验内容说明

(一) 实验题目

仿真环境下的 NAT 配置

(二) 实验要求

在仿真环境下完成 NAT 服务器的配置，要求如下：

1. 学习路由器的 NAT 配置过程
2. 组建由 NAT 连接的内网和外网
3. 测试网络的连通性，观察网络地址映射表
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 数据包的地址进行划分
5. 将内部网络中放置一台 Web 服务器，请设置 NAT 服务器，使外部主机能够顺利使用该 Web 服务

二、 内网访问外网

(一) 网络拓扑图

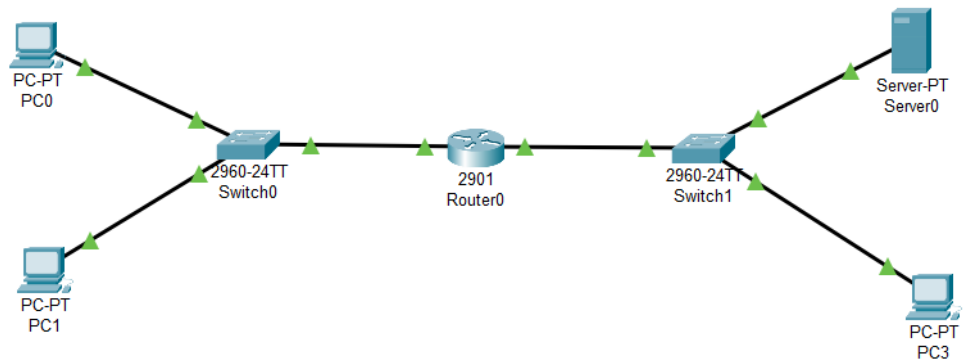

图 1: 网络拓扑图

(二) 配置 NAT 和 Web 服务器

在仿真环境下完成 NAT 服务器的配置，要求如下：

1. 指定 NAT 使用的全局 IP 地址范围
2. 设置内部网络使用的 IP 地址范围

3. 建立全局 IP 地址与内部私有地址之间的关联

4. 指定连接内部网络和外部网络的接口

5. 查看 NAT 的工作状况

```
Router#config terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#ip nat pool MyNATPool 202.113.25.1 202.113.25.10 netmask
255.255.255.0
Router(config)#access-list 6 permit 10.0.0.0 0.255.255.255
Router(config)#ip nat inside source list 6 pool MyNATPool overload
Router(config)#interface fa0/0
%Invalid interface type and number
Router(config)#interface gig0/0
Router(config-if)#ip nat inside
Router(config-if)#exit
Router(config)#interface gig0/1
Router(config-if)#ip nat outside
Router(config-if)#exit
Router(config)#
```

图 2: 配置 NAT

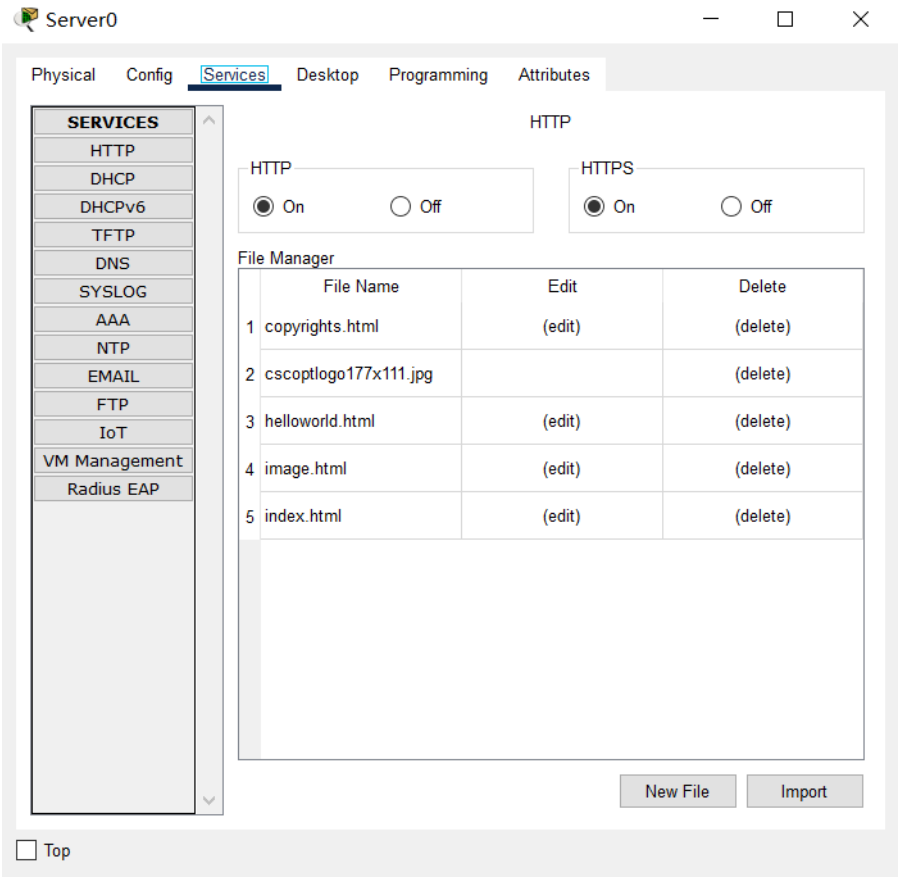

图 3: 配置 Web 服务器

(三) 连通性测试

```
C:\>ping 202.113.25.100

Pinging 202.113.25.100 with 32 bytes of data:

Request timed out.
Reply from 202.113.25.100: bytes=32 time<1ms TTL=127
Reply from 202.113.25.100: bytes=32 time<1ms TTL=127
Reply from 202.113.25.100: bytes=32 time<1ms TTL=127

Ping statistics for 202.113.25.100:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

图 4: ping 命令

```
C:\>tracert 202.113.25.100

Tracing route to 202.113.25.100 over a maximum of 30 hops:

  1    0 ms      0 ms      0 ms      10.0.0.1
  2    0 ms      0 ms      0 ms      202.113.25.100

Trace complete.
```

图 5: tracert 命令

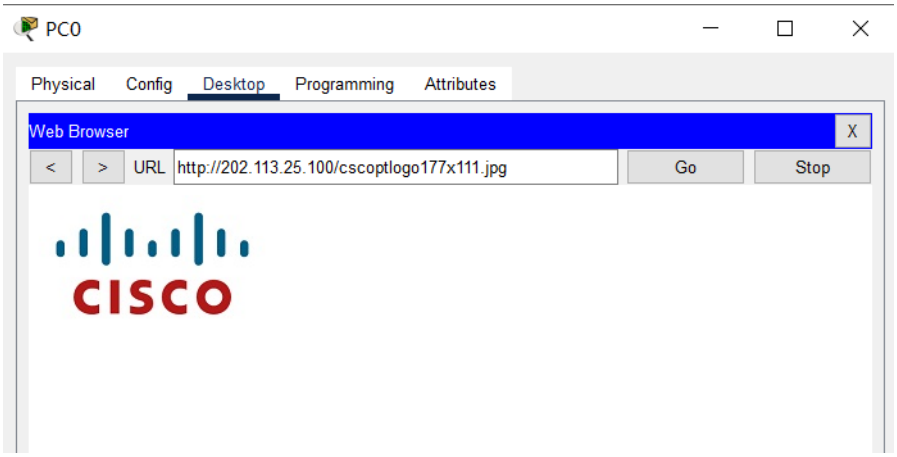

图 6: 访问 Web 服务器

(四) 查看 NAT 工作状态

可以看到我们之前配置的 NAT 信息：访问设备列表、IP 地址池、接口绑定信息等

```
Router#show ip nat statistics
Total translations: 6 (0 static, 6 dynamic, 6 extended)
Outside Interfaces: GigabitEthernet0/1
Inside Interfaces: GigabitEthernet0/0
Hits: 72  Misses: 13
Expired translations: 7
Dynamic mappings:
-- Inside Source
access-list 6 pool myNATPool refCount 6
 pool myNATPool: netmask 255.255.255.0
       start 202.113.25.1 end 202.113.25.10
       type generic, total addresses 10 , allocated 1 (10%), misses 0
Router#
```

图 7: NAT 转换统计信息

查看 NAT 地址转换表，每次访问 web 服务器都会重新分配一个 Port

```
Router#show ip nat translations
Pro  Inside global     Inside local       Outside local      Outside global
tcp 202.113.25.1:1025  10.0.0.2:1025      202.113.25.100:80
202.113.25.100:80
tcp 202.113.25.1:1026  10.0.0.2:1026      202.113.25.100:80
202.113.25.100:80
tcp 202.113.25.1:1027  10.0.0.2:1027      202.113.25.100:80
202.113.25.100:80
tcp 202.113.25.1:1028  10.0.0.2:1028      202.113.25.100:80
202.113.25.100:80
tcp 202.113.25.1:1029  10.0.0.2:1029      202.113.25.100:80
202.113.25.100:80
tcp 202.113.25.1:1030  10.0.0.2:1030      202.113.25.100:80
202.113.25.100:80
```

图 8: NAT 地址转换表

（五） 仿真模拟 IP 数据包的传递

在模拟情况下观察 IP 数据包的传递，对比经过 NAT 前后的 IP 数据包。当发出数据包时，IP 层的原来的内网地址被替换成分配的全局 IP 地址。接收数据包时，IP 层的目的 IP 地址被替换成内网 IP 地址，从而实现 NAT 转换过程。

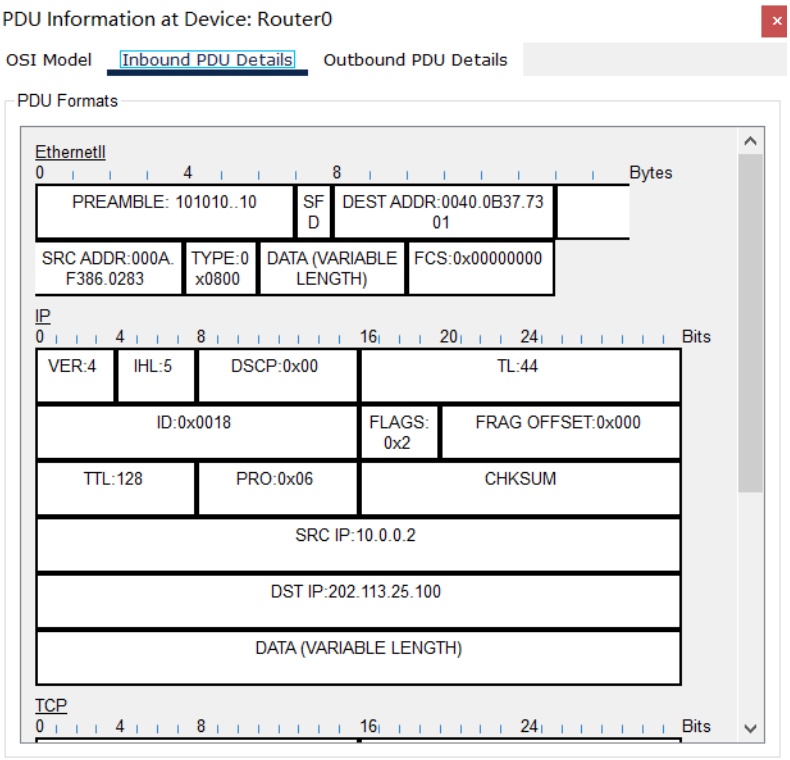

图 9: NAT 入口 IP 数据包

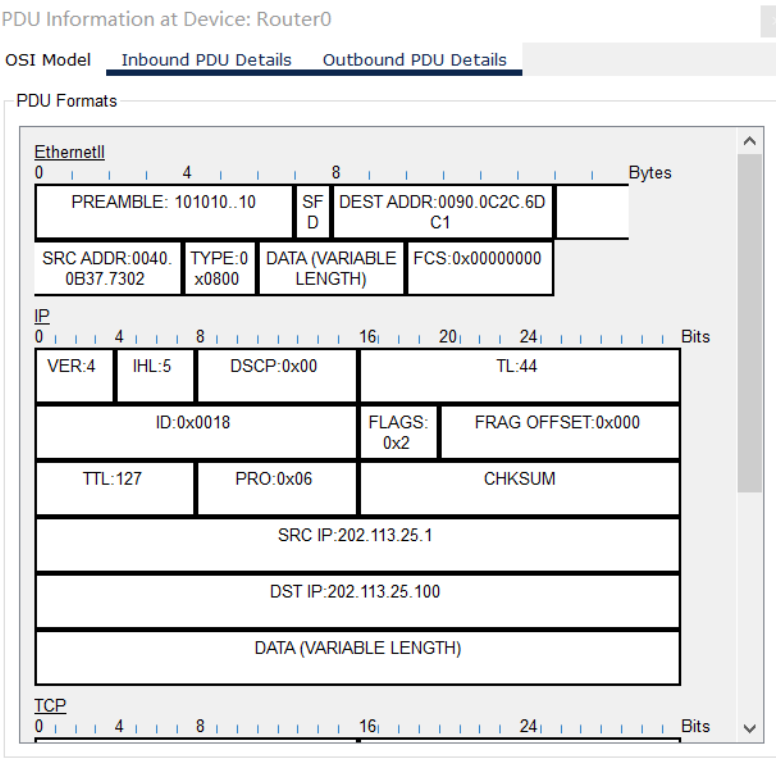

图 10: NAT 出口 IP 数据包

三、 外网访问内网

(一) 网络拓扑图

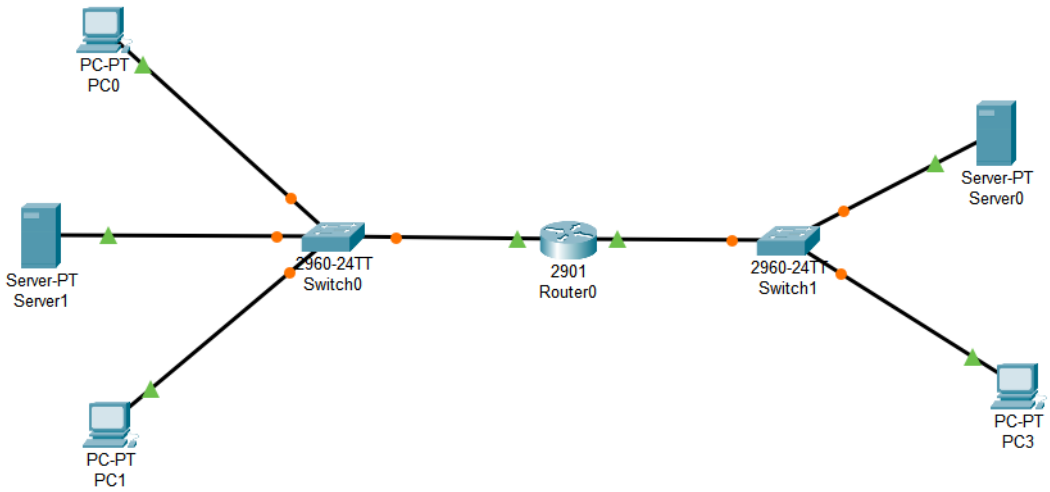

图 11: 网络拓扑图

(二) 配置静态 NAT

给内网服务器一个固定的映射 IP，这样外网主机可以通过访问该 IP，实现外网访问内网的功能

```
Router#show ip nat translations
Pro  Inside global     Inside local       Outside local      Outside global
---  202.113.25.2      10.0.0.4           ---                ---
tcp 202.113.25.2:80    10.0.0.4:80
202.113.25.101:1026202.113.25.101:1026
```

图 12: 配置 NAT 映射

(三) 连通性测试

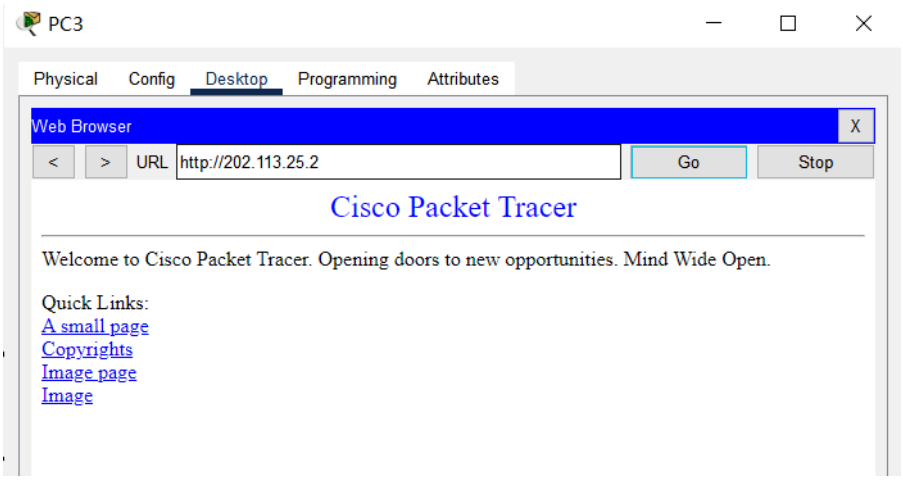

图 13: 外网访问内网 web 服务器

四、 扩展学习

(一) NAT 穿透

感谢张同学有关全锥形 NAT 和对称性 NAT 的知识分享，让我对 NAT 穿透技术了解更多，在此写下我浅薄的理解。

P2P 需要两个节点之间直接互相通信，而两个节点多数情况都位于防火墙内和内部局域网内，从内往外访问很容易，但反过来却无法直接进行，这就涉及到 NAT 穿透技术。因为 UDP 穿透简单，所以多数 P2P 的实现都是以 UDP 协议来实现的，UDP 穿透包含以下几种 NAT:

1. 全锥形 NAT

   全锥形 NAT 的 IP、端口都不受限。只要客户端由内到外打通一个洞之后（NatIP:NatPort -> A:P1），其他 IP 的主机 (B) 或端口 (A:P2) 都可以使用这个洞发送数据到客户端。映射关系为：Client->NatIP:NatPort->Any，即任何外部主机都可通过 NatIP:NatPort 发送数据到 Clietn 上。

2. 受限锥形 NAT

   受限锥形 NAT 的 IP 受限，端口不受限。当客户端由内到外打通一个洞之后 (NatIP:NatPort -> A:P1)，A 机器可以使用他的其他端口（P2）主动连接客户端，但 B 机器则不被允许。映

射关系为：Client-> NatIP:NatPort->A，即只有来自 A 的数据包才能通过 NatIP:NatPort 发送到 Client 上。

3. 端口受限锥型 NAT

   端口受限锥型 NAT 的 IP、端口都受限。返回的数据只接受曾经打洞成功的对象（A:P1），由 A:P2、B:P1 发起的数据将不被 NatIP:NatPort 接收。映射关系为：Client->NatIP:NatPort->A:P1，即只有来自 A:P1 的数据才可通过 NatIP:NatPort 发送到 Client 上。

4. 对称型 NAT

   对称型 NAT 具有端口受限锥型的受限特性。但更重要的是，他对每个外部主机或端口的会话都会映射为不同的端口（洞）。只有来自相同的内部地址（IP:PORT）并且发送到相同外部地址（X:x）的请求，在 NAT 上才映射为相同的外网端口，即相同的映射。一个外部地址（X:x）对应一个 NAT 上的映射，每个映射仅接收来自他绑定的外部地址的数据。关键点在到不同的目的地 (目的 IP: 目的端口) 分配不同的映射地址 (IP:Port)

```
Router>enable
Router#show ip nat translations
Pro  Inside global     Inside local       Outside local      Outside global
---  202.113.25.2      10.0.0.4           ---                ---
tcp 202.113.25.1:1025  10.0.0.2:1025      202.113.25.100:80
202.113.25.100:80
tcp 202.113.25.1:1026  10.0.0.2:1026      202.113.25.102:80
202.113.25.102:80
```

图 14: 对称型 NAT

TCP 也是可以穿透，只要符合 TCP 通信协议的规范就可以，主要在 SYN 消息如何准确的伪造出来。

(二) SNAT 和 DNAT

NAPT 包含两种转换方式：SNAT 和 DNAT。SNAT 修改数据包的源地址，实现数据包伪装。DNAT 修改数据包的目的地址，可以实现端口转发、平衡负载和透明代理等功能。

之前学习 DNS 解析时，我们知道内容分发网络 CDN 可以使用 DNS 重定向实现负载均衡，而通过地址转换方式也可以实现服务器的负载均衡，DNAT 可以重定向一些服务器的连接到其他随机选定的服务器。除此以外还可以采用服务器群集负载均衡、交换机负载均衡等方式。

DNAT 还可以用来提供高可靠性的服务，如果一个系统有一台通过路由器访问的关键服务器，一旦路由器检测到该服务器宕机，它可以使用目的地址转换 NAT 透明的把连接转移到一个备份服务器上。

DNAT 可以把连接到因特网的 HTTP 连接重定向到一个指定的 HTTP 代理服务器以缓存数据和过滤请求。一些因特网服务提供商就使用这种技术来减少带宽的使用而不用让他们的客户配置他们的浏览器支持代理连接。Linux 操作系统使用 NAT 和 TPROXY 实现透明代理。NAT 方式就是内核通过地址转换实现的；而 TPROXY 是内核通过对设置的数据包打标记，然后通过策略路由将打标记的数据包重定向到本地监听进程上。

感觉 SNAT 更像是前向代理，面向客户端；DNAT 更像是反向代理，面向服务器。