网络技术与应用第六次实验报告

物联网工程 2211999 邢清画

一、实验名称

实验6——NAT配置

二、实验要求

1.仿真环境下的**NAT**服务器配置在仿真环境下完成**NAT**服务器的配置实验，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**数据报的地址进行分析。

2.在仿真环境下完成如下实验：

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。

三、实验内容

3.0 相关内容

NAT是通过将私有**IP**地址转换为公共**IP**地址，或者反向转换，来解决地址短缺问题并提高网络安全性。

1. NAT的基本概念

- **NAT (Network Address Translation)**：网络地址转换，通常用来让多个设备共享一个公共**IP**地址访问互联网。**NAT**设备（通常是路由器）会修改数据包的源**IP**或目的**IP**地址，使私有网络中的设备能够通过公有**IP**与外部通信。
- **私有IP地址**：这些地址属于保留范围（如 **192.168.x.x**、**10.x.x.x** 等），只能在局域网内使用，不在互联网中路由。
- **公有IP地址**：由互联网服务提供商（**ISP**）分配，能够在互联网上路由。

2. NAT的工作方式

- **源地址转换 (Source NAT, SNAT)**：用于将私有网络中的源**IP**地址转换为公共**IP**地址。这是实现局域网设备访问互联网的最常见方式。
- **目的地址转换 (Destination NAT, DNAT)**：用于将外部请求的目标**IP**地址转换为内网设备的私有**IP**地址，常用于端口转发。
- **端口地址转换 (PAT, Port Address Translation)**：一种特殊的源**NAT**，其中多个内网设备通过不同的端口号共享一个公共**IP**地址。**PAT**使得路由器可以通过修改源端口来跟踪不同的连接。

3. NAT的配置过程

在路由器上进行NAT配置的过程通常包括以下几个步骤：

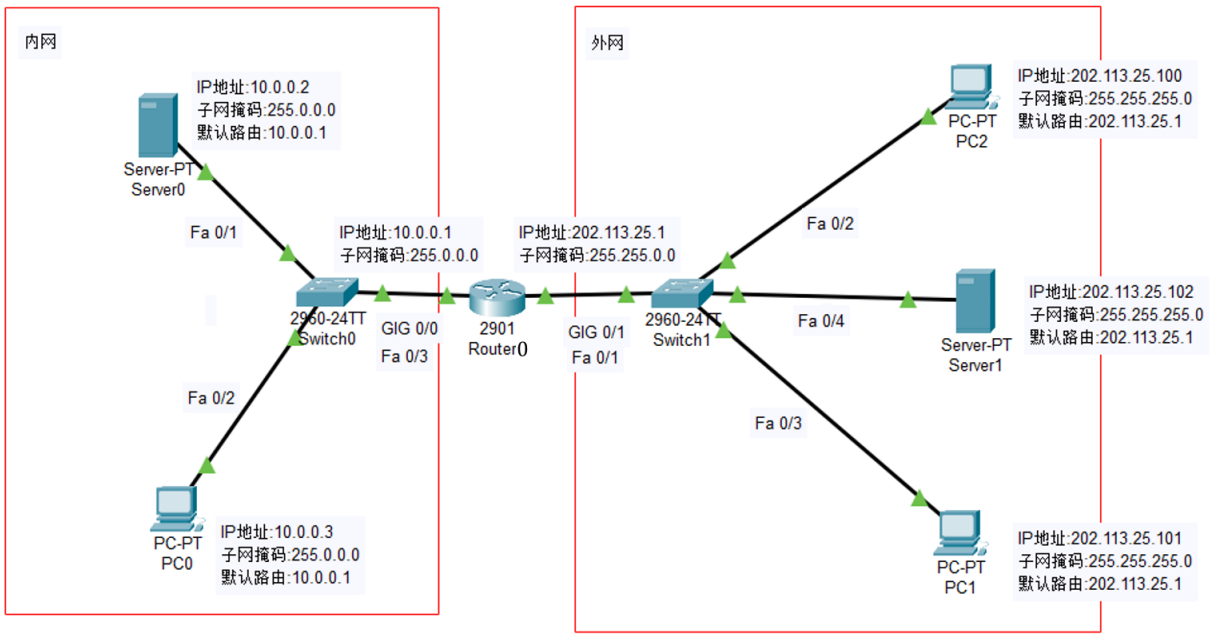
1. 配置路由器的接口：
    - 外网接口（连接到互联网）配置一个公共IP地址。
    - 内网接口（连接到局域网）配置一个私有IP地址。
2. 启用NAT功能：
    - 启用NAT服务，使得路由器能够执行地址转换操作。
3. 配置NAT规则：
    - 配置哪些流量需要被NAT处理。例如，可以配置内部网络的源IP地址转换为一个公共IP。
4. 验证和测试：
    - 测试NAT是否正确工作，检查路由器是否成功将内网设备的私有IP地址转换为公网IP地址，并确保内外网之间的通信正常。

4. NAT的地址映射表

- 在NAT设备上，通常会有一个“地址映射表”来记录地址转换的规则。这个表将跟踪内网IP地址与公共IP地址之间的映射关系。
- **动态NAT表**：当内网设备通过NAT设备访问外网时，NAT表会记录下哪些私有IP地址使用了哪些端口和公共IP地址。
- **静态NAT映射**：将内网设备的私有IP地址和公网IP地址建立永久映射，常用于外部访问内网服务（如Web服务器）。

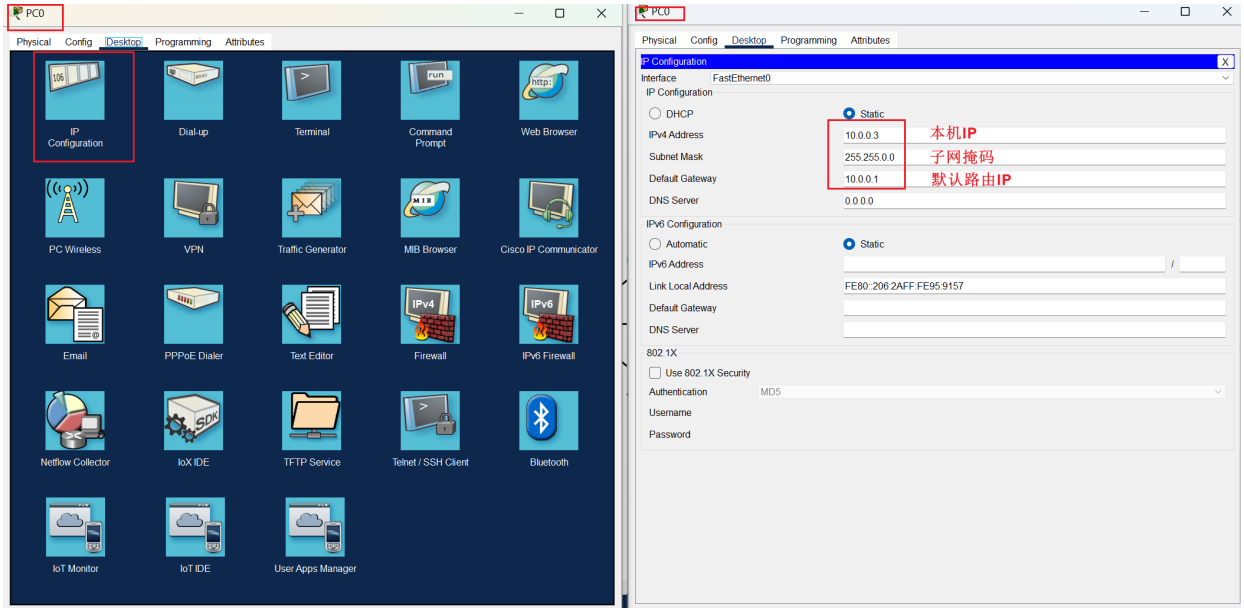
3.1 设计网络拓扑图

按下图方式连接线路：



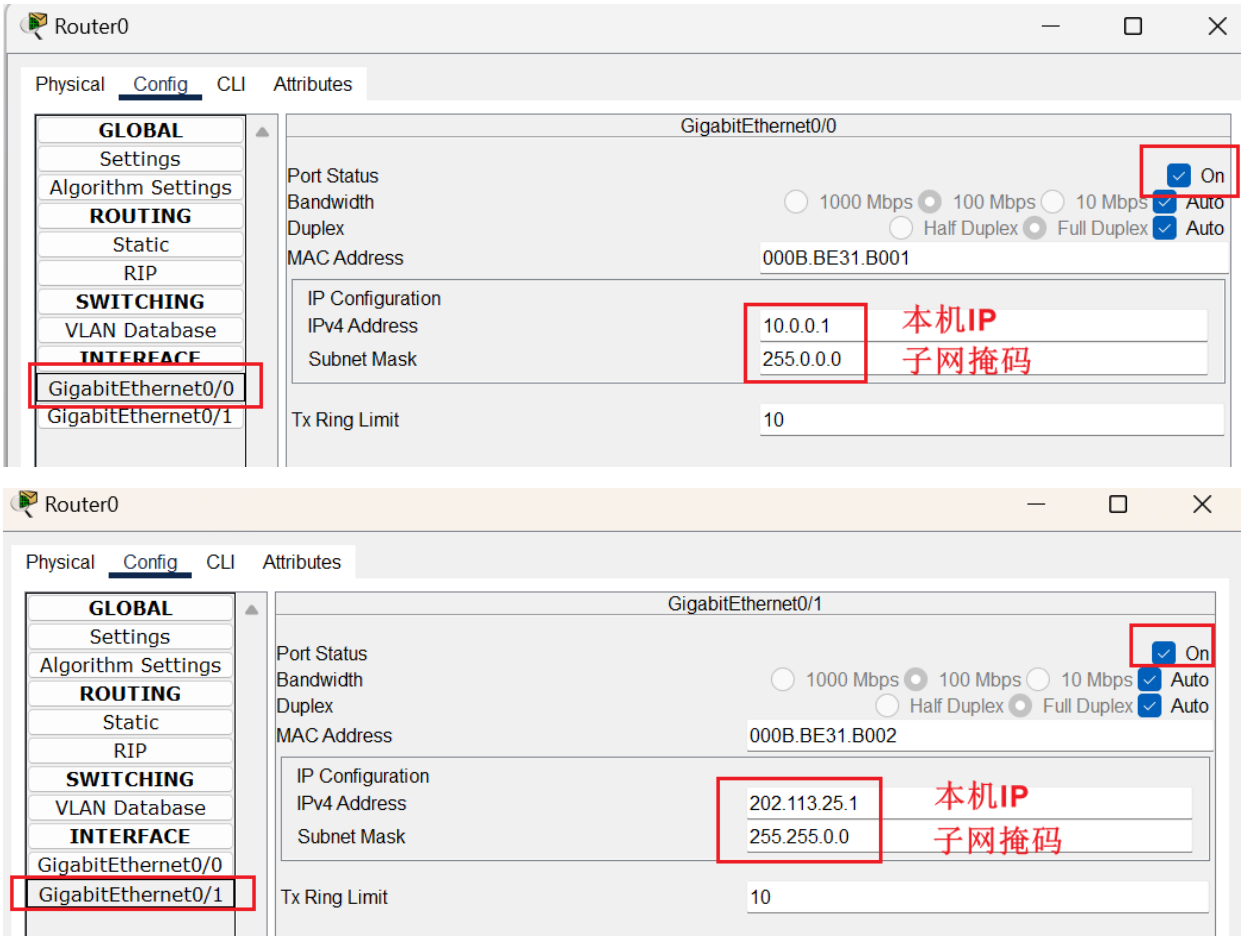
3.2 设置PC端信息

对于PC端更改IP地址、子网掩码、默认路由：



3.3 设置路由器信息

在左侧的**gig0/0**和**gig0/1**端选择修改**ip**地址和子网掩码，同时需要将右上角的**port status**勾选使得指令保持连通：



或者使用命令行输入以下代码：

```
enable   //进入使能模式
config terminal  //进入全局模式
interface gig0/0  //选中端口gig0/0
ip address 10.0.0.1 255.0.0.0   //配置IP地址和子网掩码
no shutdown  //使指令保持通畅
```

3.4 指定NAT使用的全局IP地址范围

将路由器两个端口的配置都完成后，就要指定NAT使用的全局IP地址范围。在全局配置模式下，使用命令：

```
ip nat pool mypool 202.113.25.1 202.113.25.10 netmask 255.255.255.0
```

定义一个名字为mypool的IP地址池，该IP地址池中的IP地址从202.113.25.1开始，到202.113.25.10为止，共10个IP地址，掩码为255.255.255.0。

```
Router(config-if)#exit
Router(config)#ip nat pool mypool 202.113.25.1 202.113.25.10 netmask 255.255.255.0
Router(config)#
```

3.5 设置内部网络使用的IP地址范围

使用命令：

```
access-list 6 permit 10.0.0.0 10.255.255.255
```

定义一个标号为6的访问列表，使得能够允许10.0.0.0到10.255.255.255的IP地址通过。

```
Router(config-if)#exit
Router(config)#ip nat pool mypool 202.113.25.1 202.113.25.10 netmask 255.255.255.0
Router(config)#access-list 6 permit 10.0.0.0 10.255.255.255
Router(config)#ip nat inside source list 6 pool mypool overload
Router(config)#interface gig 0/0
```

3.6 建立全局IP地址与内部私有IP地址之间的关联

使用命令：

```
ip nat inside source list 6 pool mypool overload
```

将访问列表6中指定10.0.0.0到10.255.255.255的IP地址转换成地址池 myPool中的202.113.25.1到202.113.25.10的IP地址来访问外部互联网。

```
Router(config-if)#exit
Router(config)#ip nat pool mypool 202.113.25.1 202.113.25.10 netmask 255.255.255.0
Router(config)#access-list 6 permit 10.0.0.0 10.255.255.255
Router(config)#ip nat inside source list 6 pool mypool overload
Router(config)#interface gig 0/0
Router(config-if)#ip nat inside
```

3.7 设置内部网络和外部网络

使用命令ip nat inside 将gig0/0接口配置为连接内部网络， ip nat outside 将gig0/1接口配置为连接外部网络：

```
Router(config)#ip nat inside source list 6 pool mypool overload
Router(config)#interface gig 0/0
Router(config-if)#ip nat inside
Router(config-if)#exit
Router(config)#interface gig 0/1
Router(config-if)#ip nat outside
```

3.8 设置NAT服务器，使外部主机能够访问内部服务器

在路由器中输入指令：

```
ip nat inside source static 10.0.0.2 202.113.25.25
```

为服务器建立**ip**转换关系，表示将内部服务器的**10.0.0.2**转换成外部可以访问的**202.113.25.25**。

```
Router(config-if)#exit
Router(config)#ip nat inside source static 10.0.0.2 202.113.25.25
```

四、实验结果

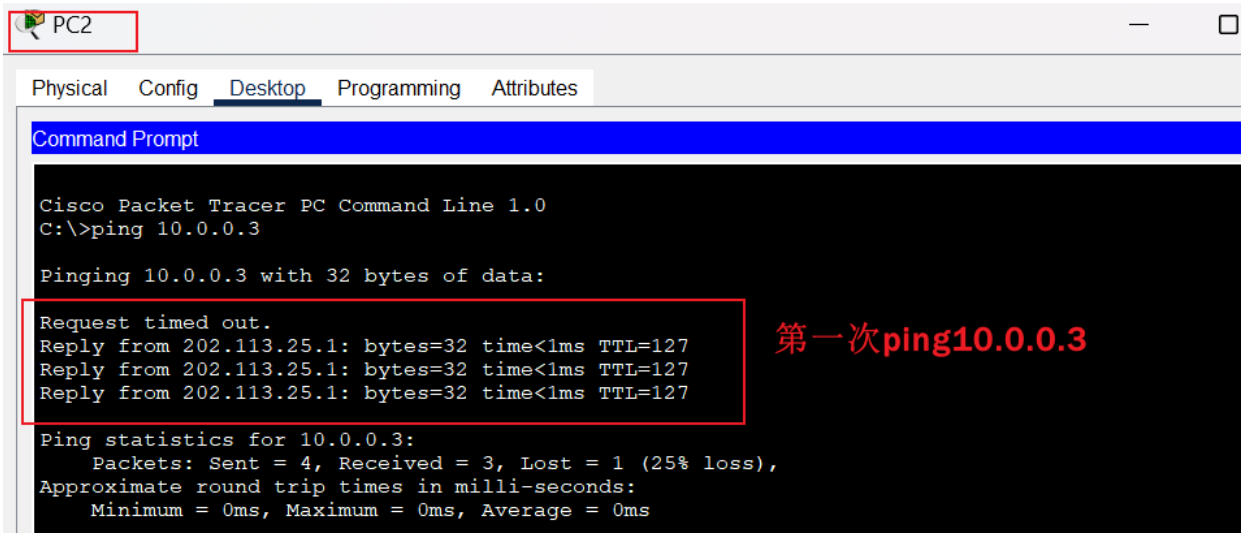
4.1 验证连通性

4.1.1 外部访问内部

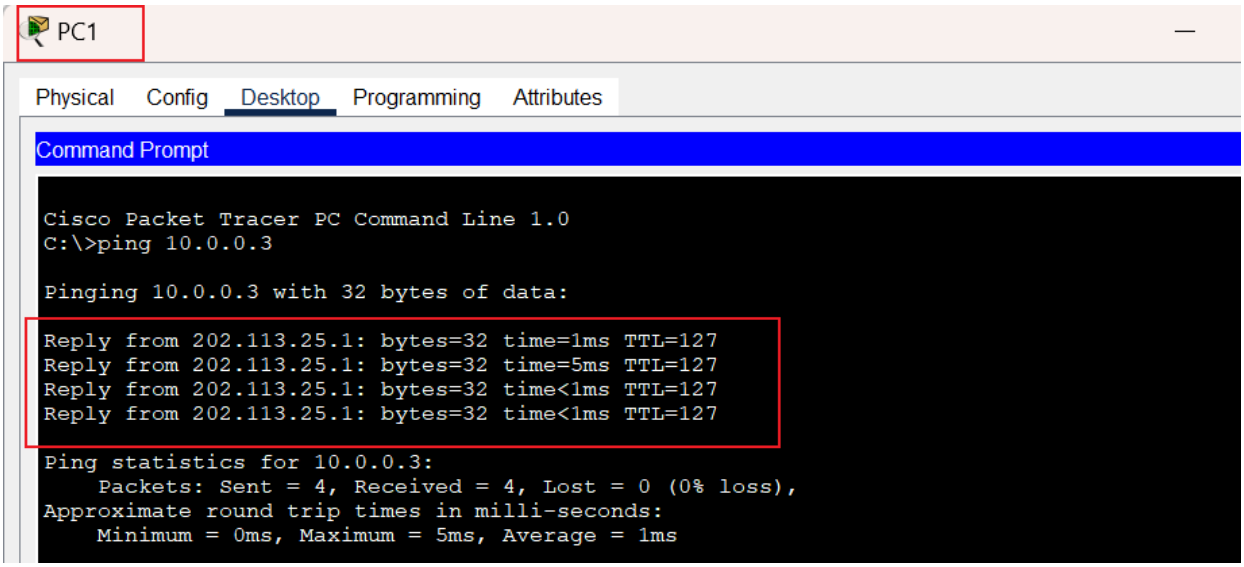
使用命令：

```
ping 10.0.0.3
```

通过**PC2**给**PC0**发送数据包，发现收到回复：



由于是第一次**ping**，所以开始建立连接会请求超时，这是正常的，如果之后再进行外部访问内部的操作就不会超时了，现在用**PC1**给**PC0**发送数据包：



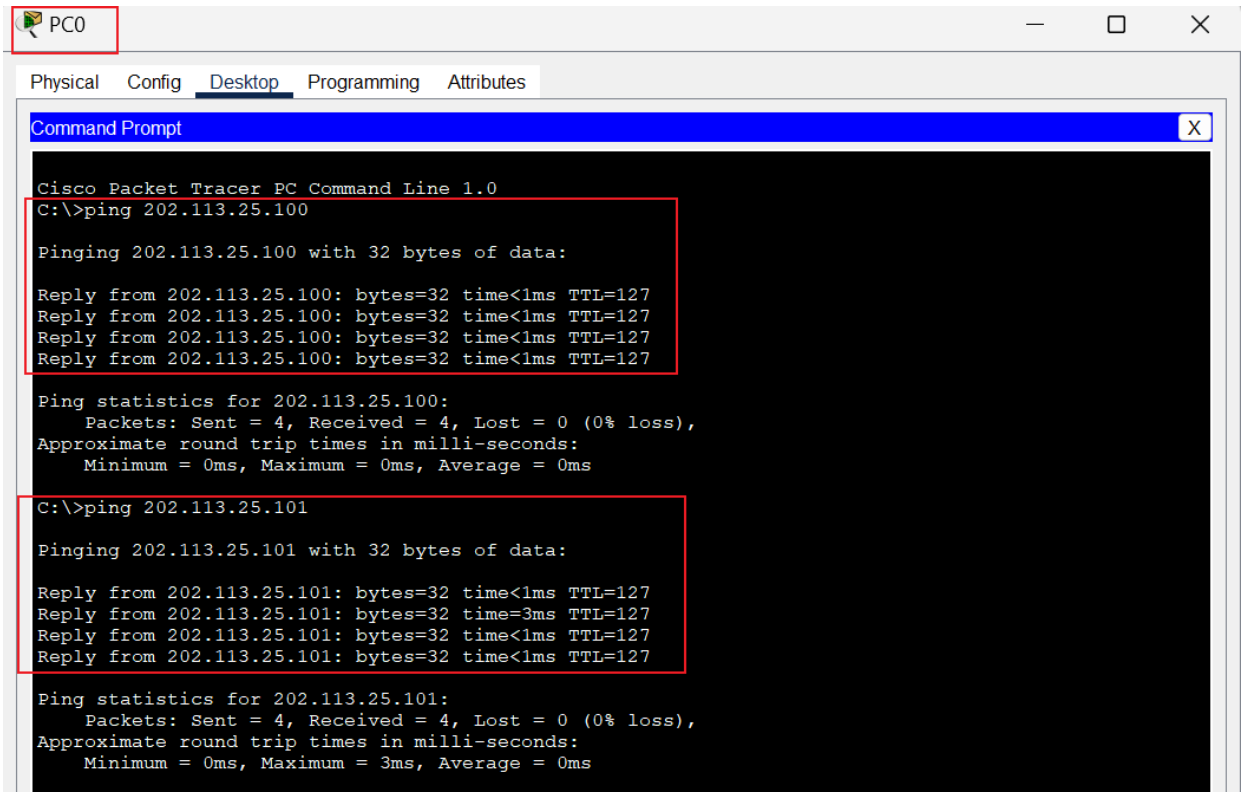
不会出现超时，且可以收到回复。

4.1.2 内部访问外部

使用命令：

```
ping 202.113.25.101
ping 202.113.25.100
```

通过**PC0**给**PC1**，**PC2**发送数据包，发现也能收到回复，证明连通性没问题：



由于刚才用**PC1**和**PC2**对**PC0**都进行了连接，所以不会出现请求超时的情况。

4.2 检查转发表

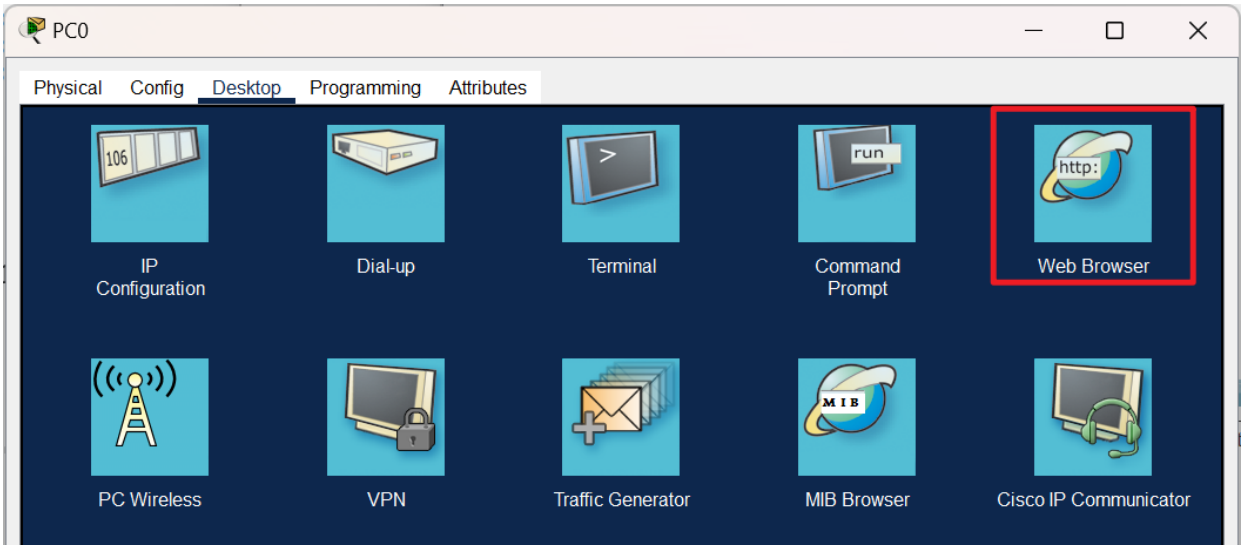
在全局模式下使用命令 **show ip nat tran**可以查看到转发表

```
Router#show ip nat tran
Pro  Inside global     Inside local       Outside local      Outside global
icmp 202.113.25.1:10   10.0.0.3:10        202.113.25.101:10  202.113.25.101:10
icmp 202.113.25.1:11   10.0.0.3:11        202.113.25.101:11  202.113.25.101:11
icmp 202.113.25.1:12   10.0.0.3:12        202.113.25.101:12  202.113.25.101:12
icmp 202.113.25.1:13   10.0.0.3:13        202.113.25.100:13  202.113.25.100:13
icmp 202.113.25.1:14   10.0.0.3:14        202.113.25.100:14  202.113.25.100:14
icmp 202.113.25.1:15   10.0.0.3:15        202.113.25.100:15  202.113.25.100:15
icmp 202.113.25.1:16   10.0.0.3:16        202.113.25.100:16  202.113.25.100:16
icmp 202.113.25.1:5    10.0.0.3:5         202.113.25.101:5   202.113.25.101:5
icmp 202.113.25.1:6    10.0.0.3:6         202.113.25.101:6   202.113.25.101:6
icmp 202.113.25.1:7    10.0.0.3:7         202.113.25.101:7   202.113.25.101:7
icmp 202.113.25.1:8    10.0.0.3:8         202.113.25.101:8   202.113.25.101:8
icmp 202.113.25.1:9    10.0.0.3:9         202.113.25.101:9   202.113.25.101:9
---  202.113.25.25     10.0.0.2           ---                ---
```

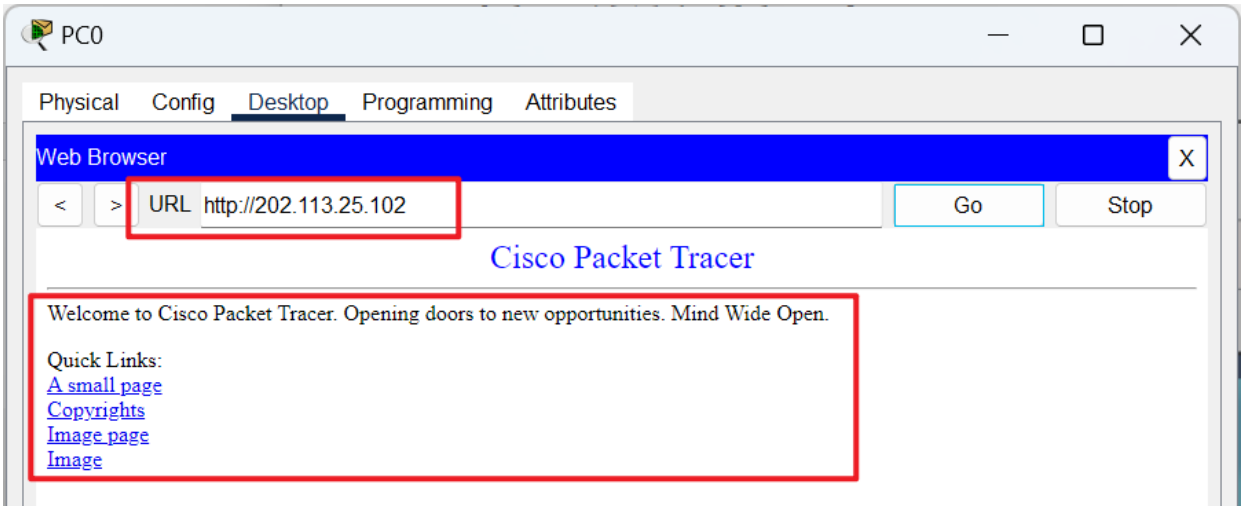
这里显示的是内部本地**ip**如**10.0.0.3**被转发成本地的可访问的**IP 202.113.25.1**，可以实现与外部网络的互通。

4.3 内部网络访问外部服务器

使用**PC0**的**Web Browser**来访问外部服务器的**IP**地址**202.113.25.102**，发现可以正常显示网页，表示内部网络可以访问外部服务器。

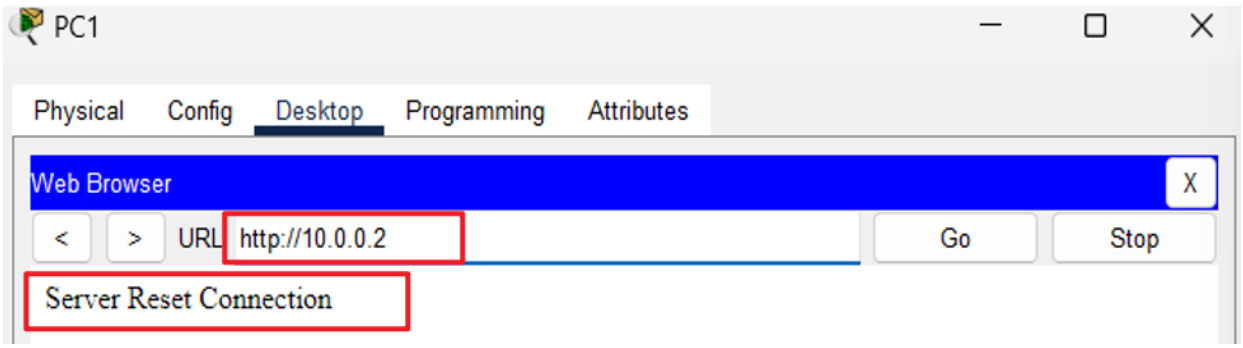


输入：http://202.113.25.102

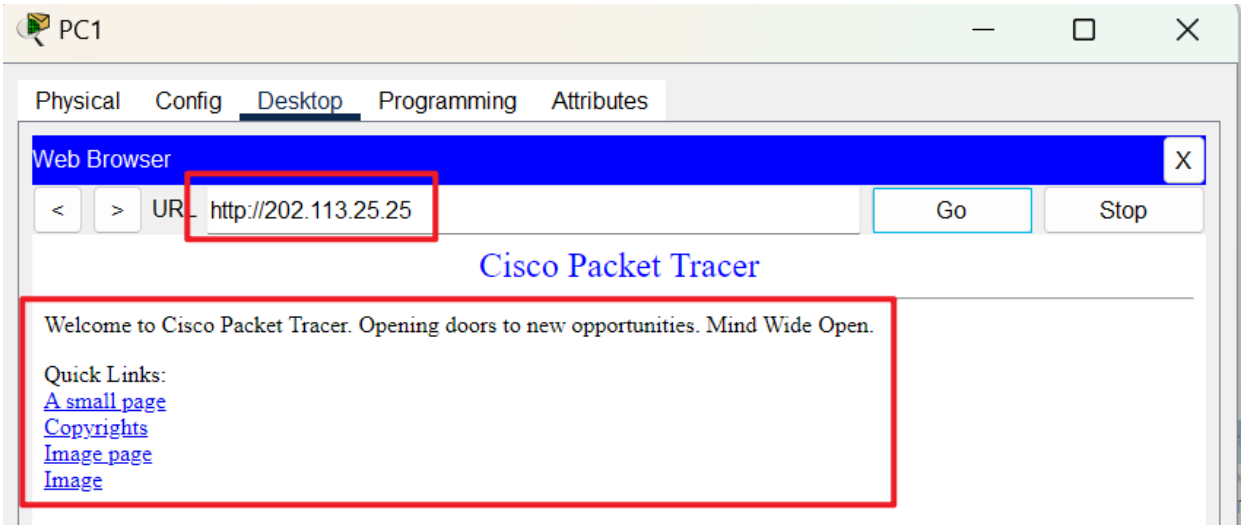


4.4 使用外部网络访问内部服务器

为服务器建立ip转换关系之前尝试直接访问内部地址10.0.0.2时，发现无法访问：



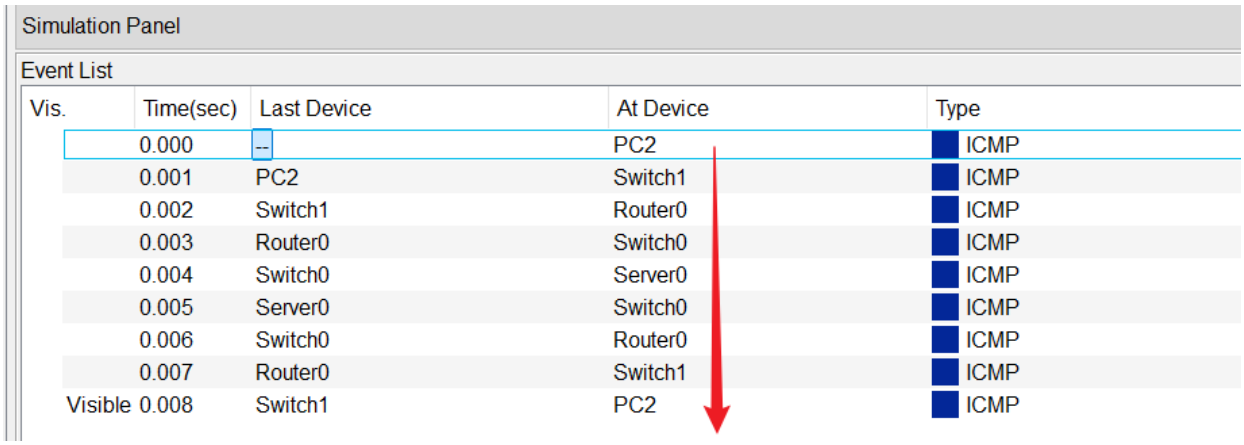
当建立转换关系10.0.0.2→202.113.25.25后再次访问发现成功：



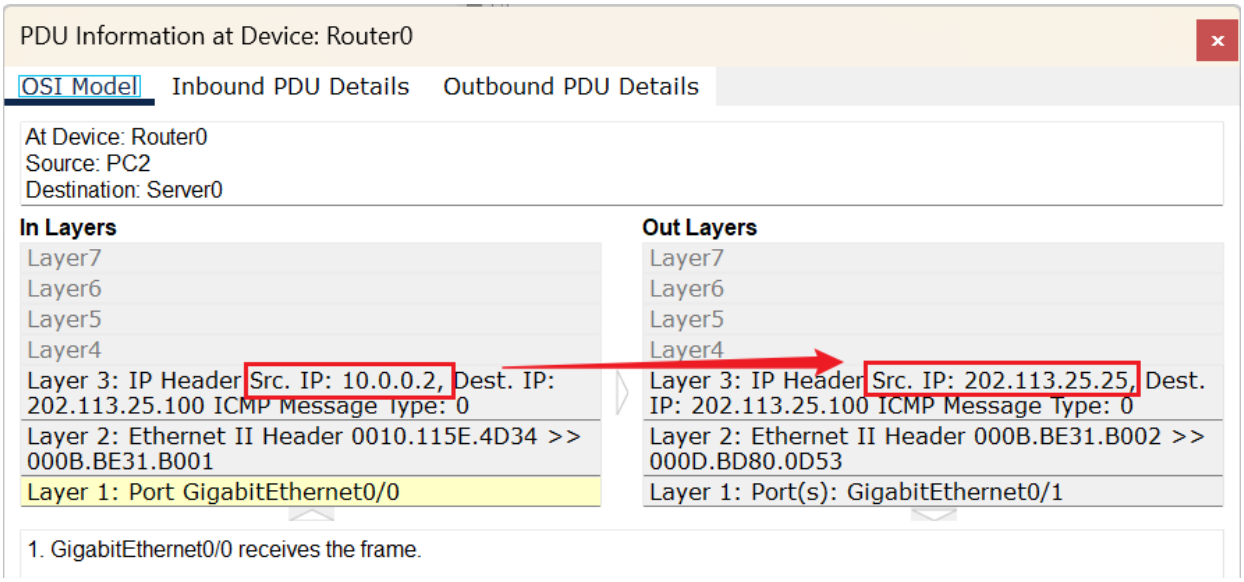
4.5 转发过程分析

让PC2给Server0发送数据，对仿真进行追踪发现转发路径如下：

PC2→Switch1→Router0→Switch0→Server0→Switch0→Routert0→Switch1→PC2



打开数据包发现对Server0的10.0.0.2的IP地址转发成202.113.25.25的IP，实现访问：



五、实验总结

（一）组建由 NAT 连接的内网和外网

1. 网络拓扑设计
   - 在仿真环境中，我设计了包含内网和外网的网络拓扑。内网包含诸如 PC、服务器等设备，外网则有其他 PC 和服务器，通过路由器进行连接。
   - 合理分配 IP 地址，内网使用私有 IP 地址（如 10.0.0.0/24 网段），外网使用公网 IP 地址（如 202.113.25.0/24 网段）。
2. 设备连接与配置
   - 对每台设备进行 IP 地址、子网掩码、默认网关等基本网络参数的配置，确保设备能够在各自的网络中正常通信。

（二）测试网络的连通性，观察网络地址映射表

1. 连通性测试
   - 使用 `ping` 命令从内网主机向外部主机发送 ICMP 数据包来测试网络连通性。如果配置正确，内网主机能够成功 ping 通外网主机。
   - 同理，从外网主机向配置了 NAT 的内网主机发送数据包时，NAT 会将内网主机的私有 IP 地址转换为外网接口的公网 IP 地址，从而实现通信。
2. 网络地址映射表观察
   - 在路由器上使用 `show ip nat translations` 命令可以查看网络地址映射表。这张表显示了内网私有 IP 地址与外网公网 IP 地址和端口的映射关系。
   - 通过观察映射表，我可以清楚地看到 NAT 是如何将内网主机的数据包进行地址转换后发送到外网，以及如何将外网返回的数据包正确转发到内网主机的。

（三）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 数据报的地址进行分析

1. IP 数据报传递过程观察
    - 在 Cisco Packet Tracer 的模拟模式下，我们可以启动网络通信（如从内网主机访问外网服务器的网页）。此时，我们能够看到 IP 数据报从源主机（内网主机）出发，经过路由器的 NAT 转换，然后在外部网络中传输，最终到达目的主机（外网服务器）的全过程。
    - 可以观察到数据报在每一个网络设备（如、路由器）上的处理情况，包括数据报的封装、解封装、转发等操作。
2. IP 数据报地址分析
    - 在内网主机发送数据报时，源 IP 地址是内网主机的私有 IP 地址。当数据报经过路由器的 NAT 转换后，源 IP 地址变为路由器外网接口的公网 IP 地址，并且源端口号也可能发生变化。
    - 在外网服务器返回数据报时，目的 IP 地址是路由器外网接口的公网 IP 地址。路由器根据网络地址映射表将数据报转发到相应的内网主机，此时目的 IP 地址会被转换回内网主机的私有 IP 地址。

通过本次 Cisco Packet Tracer 下的 NAT 服务器配置实验，我们对网络地址转换有了深入的理解。NAT 在现代网络中起着至关重要的作用，它不仅解决了 IP 地址短缺的问题，还能提供一定的网络安全保障（隐藏内网主机的真实 IP 地址）。

在实验过程中，我掌握了路由器 NAT 配置的具体步骤，以及 NAT 转换规则的设置。同时，我学会了如何组建由 NAT 连接的内网和外网，以及如何测试网络连通性和观察网络地址映射表。在仿真环境的模拟模式下，我直观地看到了 IP 数据报在网络中的传递过程和地址转换情况，这对于理解网络通信原理非常有帮助。此外，通过设置 NAT 服务器使外部主机能够访问内部网络中的 Web 服务，我进一步应用了 NAT 技术，提高了我在网络配置和故障排除方面的能力。