网络技术与应用课程报告

第五次实验报告

> **学号：2111033**
> **姓名：艾明旭**
> **年级：2021级**
> **专业：信息安全**

一、实验内容说明

1、仿真环境下的NAT服务器配置

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数据报的地址进行分析

网络地址转换（Network Address Translation，NAT）是一种网络技术，用于将私有网络内部的 IP 地址映射到公共网络上的一个或多个 IP 地址，从而实现多个内部设备共享一个或一组公共 IP 地址。这有助于缓解 IPv4 地址短缺问题，同时提供了一定的网络安全性。

NAT 的三种常见形式包括静态 NAT、动态 NAT 和 PAT（Port Address Translation）。

1. **静态 NAT（Static NAT）**：
    - **过程**：
        - 静态 NAT是一对一的映射方式，将内部私有 IP 地址映射到一个固定的外部公共 IP 地址。
        - 网络管理员手动配置映射关系，将内部设备的私有 IP 地址映射到一个公共 IP 地址。
        - 映射关系是静态的，不随内部设备的连接状态而改变。

- **优点**：
  - 固定映射关系，适用于需要对外提供服务的设备，如 Web 服务器。
- **缺点**：
  - 浪费公共 IP 地址，因为每个内部设备都需要一个对应的公共 IP 地址。

2. **动态 NAT（Dynamic NAT）**：
   - **过程**：
     - 动态 NAT也是一对一的映射方式，但映射关系是动态分配的。
     - 内部设备在向外发起连接时，NAT 设备动态地为其分配一个可用的公共 IP 地址。
     - 映射关系在一段时间内保持不变，但当连接关闭后，分配的公共 IP 地址就可以再次被其他设备使用。
   - **优点**：
     - 节省公共 IP 地址，因为映射关系是动态的，根据需要分配。
   - **缺点**：
     - 可能导致连接的状态管理复杂，需要定期清理不再使用的映射关系。
3. **PAT（Port Address Translation）**：
   - **过程**：
     - PAT是一种多对一的映射方式，通过使用不同的端口号来区分不同的内部设备。
     - 内部设备共享同一个公共 IP 地址，但通过不同的端口号进行区分。
     - 通过修改源端口号，NAT 设备能够在一个公共 IP 地址上同时支持多个内部设备与外部通信。
   - **优点**：
     - 节省公共 IP 地址，实现了端口级的多路复用。
   - **缺点**：
     - 可能导致某些应用无法正常工作，因为一些应用可能无法处理端口号的改变。

总体而言，这三种 NAT 的选择取决于网络的具体需求和配置。 PAT 是最常见的形式，因为它在节省 IP 地址的同时，也为多个内部设备提供了连接到外部网络的能力。

2、在仿真环境下完成如下实验

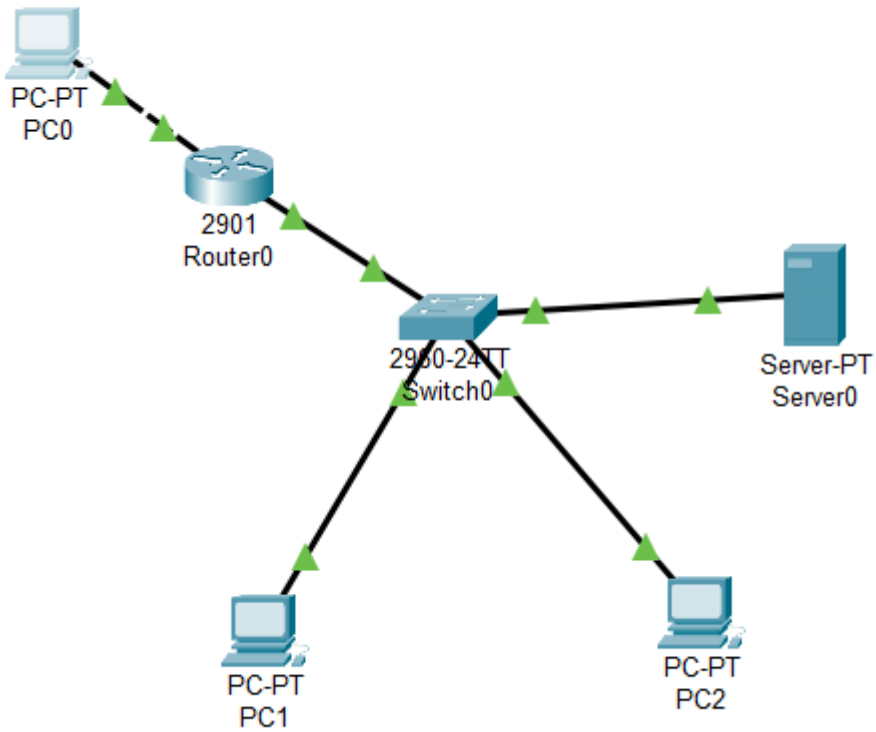
要求如下：

- 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、前期准备

(1)拓扑图

> 由于两部分实验采用相同的拓扑图，所以在此只列出一次



(2) `ip` 地址分配

> 由于两部分实验采用相同的`ip`地址分配，所以在此只列出一次

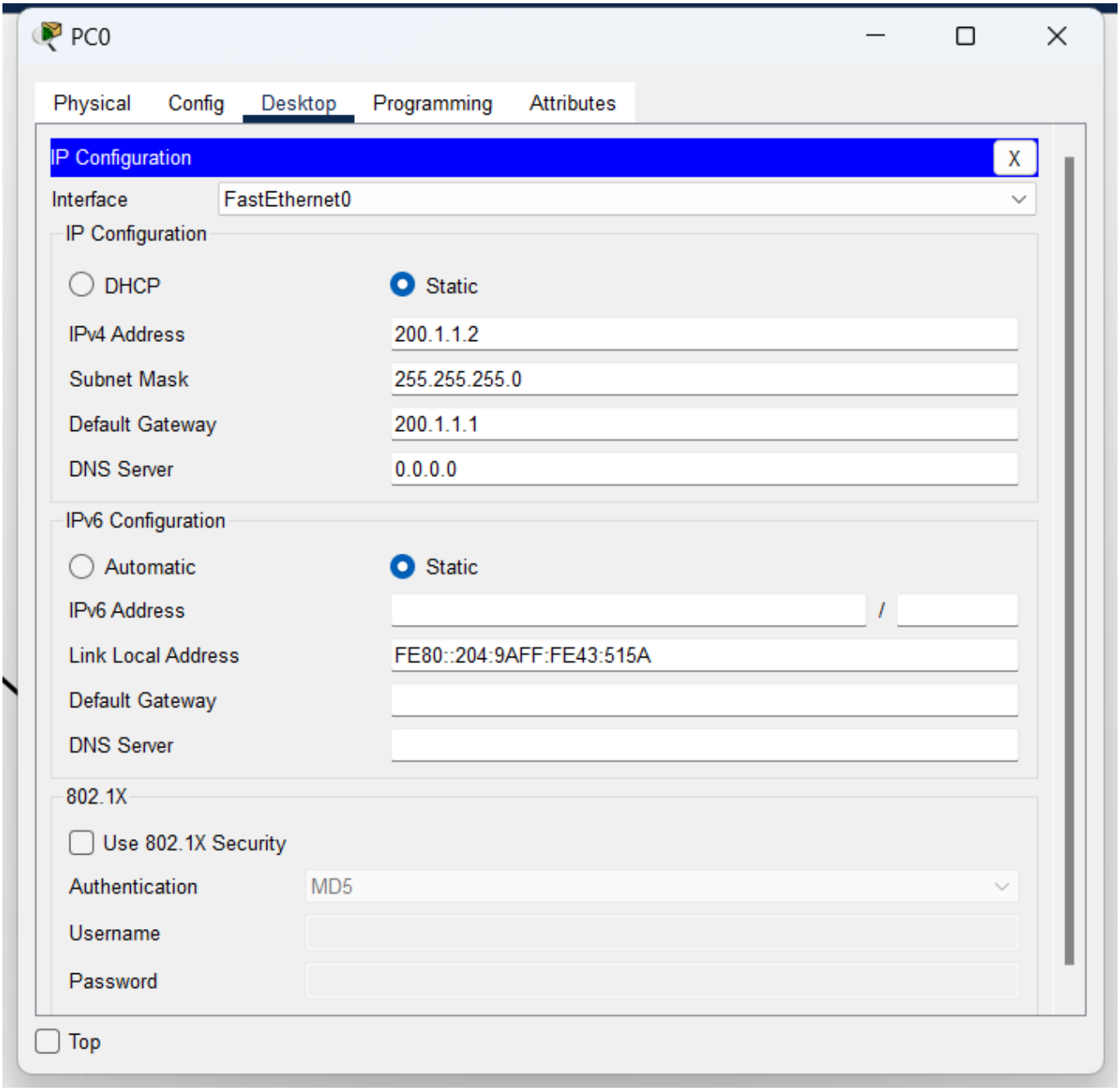
Machine	IPv4 Address	Subnet Mask	网关	内/外网
PC0	200.1.1.2	255.255.255.0	200.1.1.1	外网
PC1	192.168.1.2	255.255.255.0	192.168.1.1	内网
PC2	192.168.1.3	255.255.255.0	192.168.1.1	内网
Server0	192.168.1.4	255.255.255.0	192.168.1.1	内网
Router0 Gig0/0	192.168.1.1	255.255.255.0		内网
Router0 Gig0/1	200.1.1.1	255.255.255.0		外网

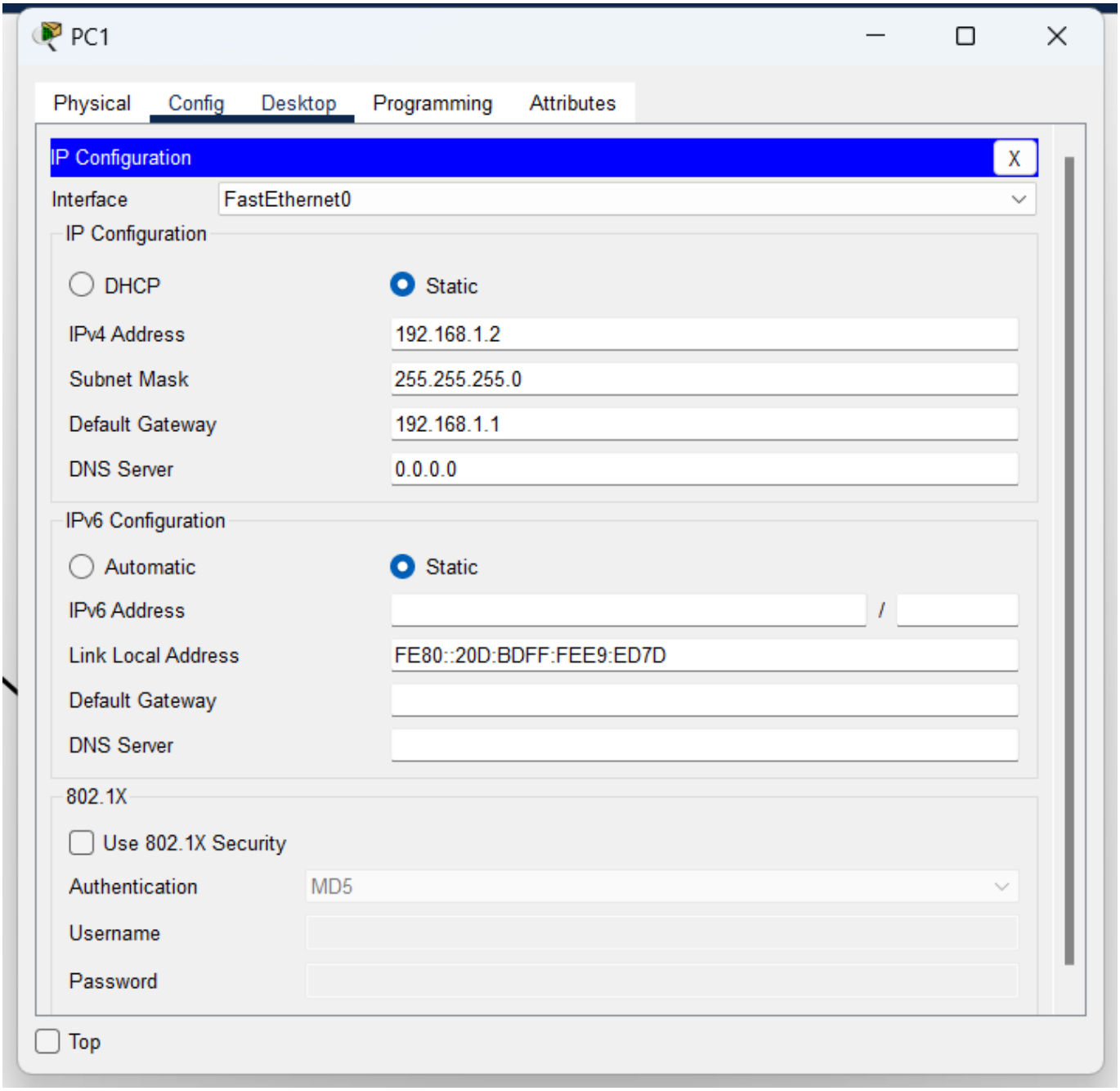
三、实验过程

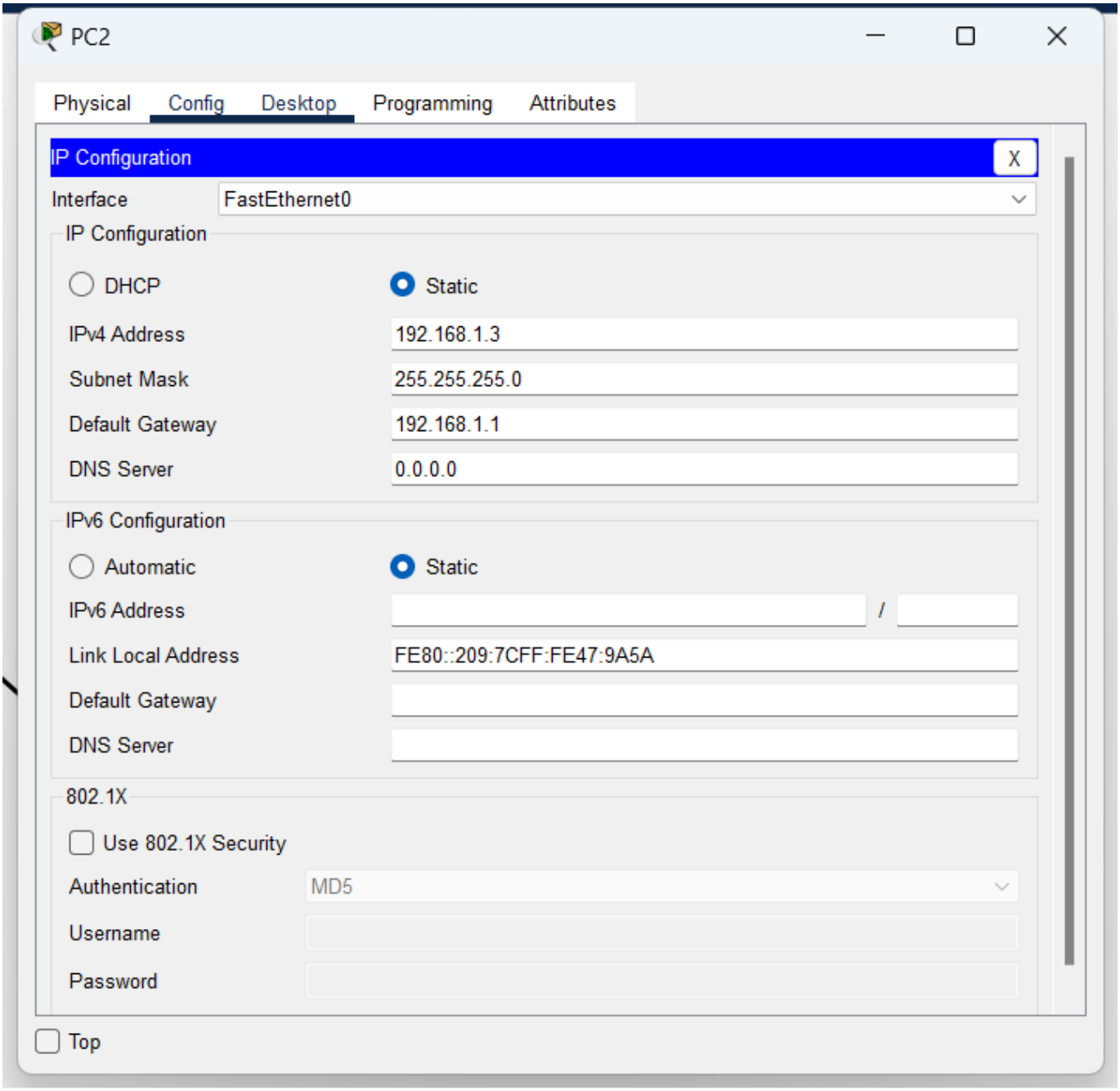
本次实验由两个部分组成，一个是组建由NAT连接的内网和外网并测试网络的连通性，观察网络地址映射表即传递过程，另一个是使外部主机能够顺利使用内部网络中服务器的Web服务，由于两部分实验采用同一个程序，所以下面将从整个项目来对本次实验过程进行介绍。

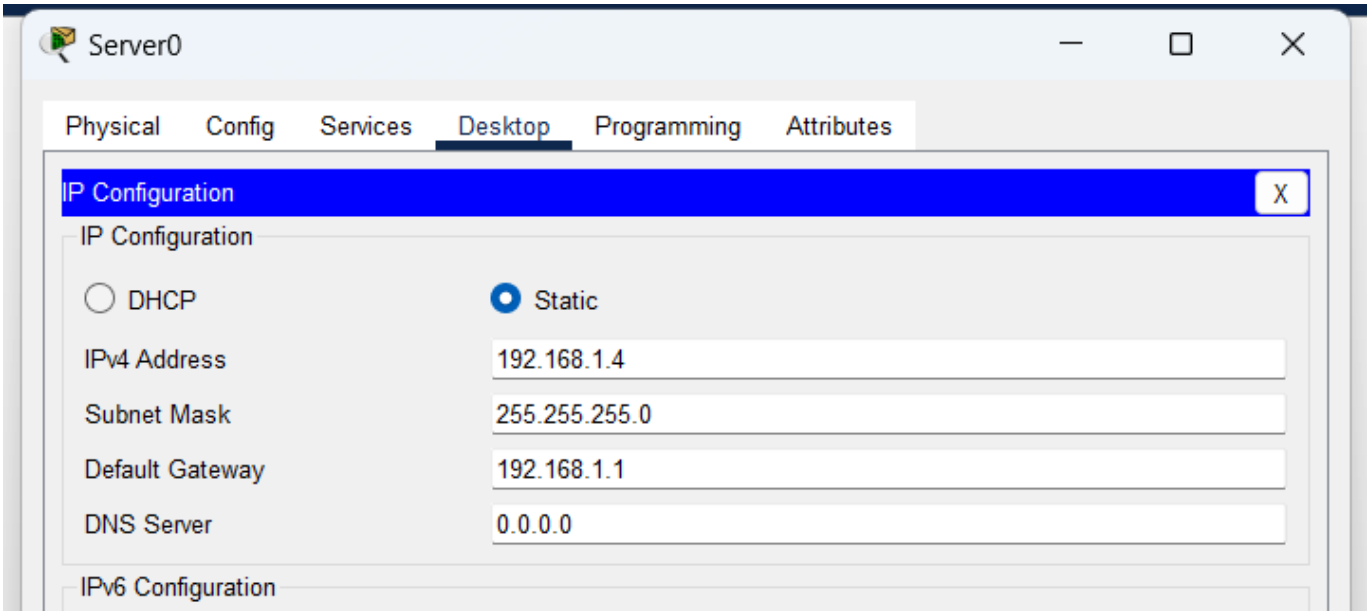
***(1)*配置各个机器的*IP*地址**

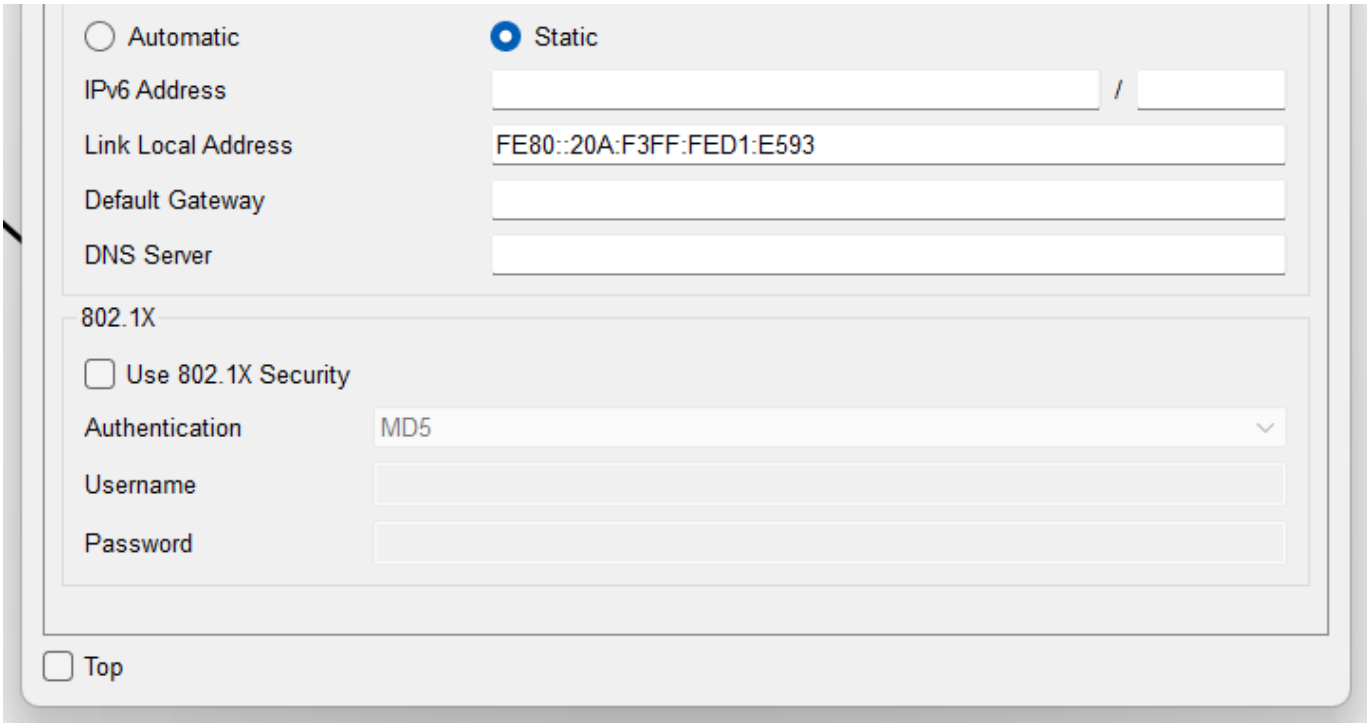
首先对三台主机以及服务器按照准备过程中的地址进行ip地址配置，配置完成后四个界面如下所示：


PC0
Physical
Config
Desktop
Programming
Attributes
IP Configuration
X
Interface
FastEthernet0
IP Configuration
DHCP
Static
IPv4 Address
200.1.1.2
Subnet Mask
255.255.255.0
Default Gateway
200.1.1.1
DNS Server
0.0.0.0
IPv6 Configuration
Automatic
Static
IPv6 Address
/
Link Local Address
FE80::204:9AFF:FE43:515A
Default Gateway
DNS Server
802.1X
Use 802.1X Security
Authentication
MD5
Username
Password
Top


PC1
Physical
Config
Desktop
Programming
Attributes
IP Configuration
X
Interface
FastEthernet0
IP Configuration
DHCP
Static
IPv4 Address
192.168.1.2
Subnet Mask
255.255.255.0
Default Gateway
192.168.1.1
DNS Server
0.0.0.0
IPv6 Configuration
Automatic
Static
IPv6 Address
/
Link Local Address
FE80::20D:BDFF:FEE9:ED7D
Default Gateway
DNS Server
802.1X
Use 802.1X Security
Authentication
MD5
Username
Password
Top


PC2
Physical
Config
Desktop
Programming
Attributes
IP Configuration
X
Interface
FastEthernet0
IP Configuration
DHCP
Static
IPv4 Address
192.168.1.3
Subnet Mask
255.255.255.0
Default Gateway
192.168.1.1
DNS Server
0.0.0.0
IPv6 Configuration
Automatic
Static
IPv6 Address
/
Link Local Address
FE80::209:7CFF:FE47:9A5A
Default Gateway
DNS Server
802.1X
Use 802.1X Security
Authentication
MD5
Username
Password
Top


Server0
Physical
Config
Services
Desktop
Programming
Attributes
IP Configuration
X
IP Configuration
DHCP
Static
IPv4 Address
192.168.1.4
Subnet Mask
255.255.255.0
Default Gateway
192.168.1.1
DNS Server
0.0.0.0
IPv6 Configuration

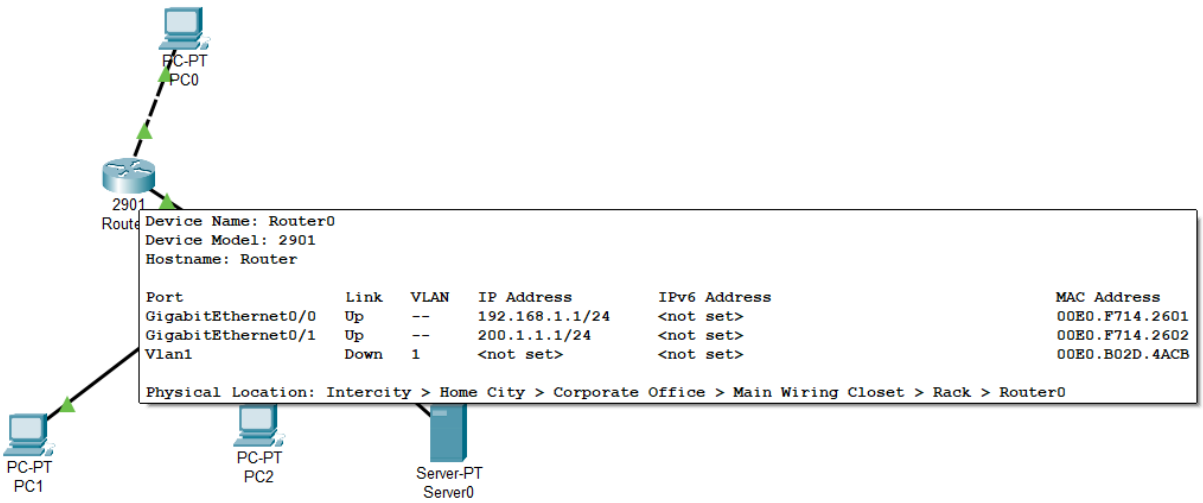


*(2)*配置路由器端口对应的*IP*

采用以下命令为路由器各个端口分配地址：

```
Router>en
Router#config t
Router(config)#int gig0/0
Router(config-if)#ip add 192.168.1.1 255.255.255.0
Router(config-if)#no shut
Router(config-if)#int gig0/1
Router(config-if)#ip add 200.1.1.1 255.255.255.0
Router(config-if)#no shut
Router(config-if)#exit
```

分配完之后可以看到路由器的对应IP地址如下图所示：



(3)NAPT方式

> 指定NAT使用的全局IP地址范围:

在路由器的全局配置模式下，使用命令`ip nat pool PoolName StartIP EndIP netmask Mask`定义一个IP地址池。

其中PoolName是一个用户选择的字符串，用于标识该IP地址池；StartIP、EndIP和Mask分别表示该地址池的起始IP地址、终止IP地址和掩码。

在NAT配置中，IP地址池定义了内网访问外网时可以使用的全局IP地址

> 设置内部网络使用的IP地址范围：

在全局配置模式下，使用命令`access-list LabelID permit IPAddr WildMask`定义一个允许通过的标准访问列表。

其中LabelID是一个用户选择的数字编号，编号的范围为1～99，标识该访问列表；IPAddr和WildMask分别表示起始IP地址和通配符，用于定义IP地址的范围。

在NAT配置中，访问列表用于指定内部网络的使用IP地址范围。

> 建立全局IP地址与内部私有IP地址之间的关联：

在全局模式下，利用`ip nat inside source list LabelID pool PoolName overload`建立全局IP地址与内部私有地址之间的关联。

其意义为访问列表LabelID中指定的IP地址可以转换为地址池PoolName中的IP地址访问外部网络。

overload关键词表示NAT转换中采用NAPT方式，PoolName中的IP地址可以重用。

以上命令执行效果如下图所示：

```
Router>
Router>
Router>
Router>enable
Router#config terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#interface gig0/0
Router(config-if)#ip address 10.0.0.1 255.0.0.0
Router(config-if)#no shutdown

Router(config-if)#
%LINK-5-CHANGED: Interface GigabitEthernet0/0, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0, changed state to up

Router(config-if)#
Router(config-if)#
Router(config-if)#
Router(config-if)#exit
Router(config)#interface gig0/1
Router(config-if)#ip address 202.113.25.1 255.255.255.0
Router(config-if)#no shutdown

Router(config-if)#
%LINK-5-CHANGED: Interface GigabitEthernet0/1, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/1, changed state to up

Router(config-if)#
Router(config-if)#exit
Router(config)#
Router(config)#
```

> 指定连接内部网络和外部网络的接口：

指定哪个接口连接内部网络，哪个接口连接外部网络需要在具体的接口配置模式下设定。

使用 `ip nat inside` 指定该接口连接内部网络；使用 `ip nat outside` 指定该接口连接外部网络，如下图所示：

```
Router(config-if)#exit
Router(config)#
Router(config)#
Router(config)#
Router(config)#
Router(config)#ip nat pool myNATPool 202.113.25.1 202.113.25.10 netmask 255.255.255.0
Router(config)#
Router(config)#access-list 6 permit 10.0.0.0 0.255.255.255
Router(config)#
Router(config)#ip nat inside source list 6 pool myNATPool overload
Router(config)#
Router(config)#interface gig0/0
Router(config-if)#
Router(config-if)#ip nat inside
Router(config-if)#exit
Router(config)#
Router(config)#interface gig0/1
Router(config-if)#ip nat outside
Router(config-if)#exit
Router(config)#
```

Command+F6 to exit CLI focus

> 查看NAT的工作状况：

- 启动服务器的Web服务，可以在不同的网络中访问另一个网络的服务器
- 可以在路由器中输入`show ip translations`查看其NAT转换表，如下图所示：

```
Router#
Router#
Router#show ip nat statistics
Total translations: 17 (0 static, 17 dynamic, 17 extended)
Outside Interfaces: GigabitEthernet0/1
Inside Interfaces: GigabitEthernet0/0
Hits: 223  Misses: 24
Expired translations: 7
Dynamic mappings:
-- Inside Source
access-list 6 pool myNATPool refCount 17
 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#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
tcp 202.113.25.1:1031  10.0.0.2:1031      202.113.25.100:80  202.113.25.100:80
tcp 202.113.25.1:1032  10.0.0.2:1032      202.113.25.100:80  202.113.25.100:80
tcp 202.113.25.1:1033  10.0.0.2:1033      202.113.25.100:80  202.113.25.100:80
tcp 202.113.25.1:1034  10.0.0.2:1034      202.113.25.100:80  202.113.25.100:80
tcp 202.113.25.1:1035  10.0.0.2:1035      202.113.25.100:80  202.113.25.100:80
tcp 202.113.25.1:1036  10.0.0.2:1036      202.113.25.100:80  202.113.25.100:80
tcp 202.113.25.1:1037  10.0.0.2:1037      202.113.25.100:80  202.113.25.100:80
tcp 202.113.25.1:1038  10.0.0.2:1038      202.113.25.100:80  202.113.25.100:80
tcp 202.113.25.1:1039  10.0.0.2:1039      202.113.25.100:80  202.113.25.100:80
tcp 202.113.25.1:1040  10.0.0.2:1040      202.113.25.100:80  202.113.25.100:80
tcp 202.113.25.1:1041  10.0.0.2:1041      202.113.25.100:80  202.113.25.100:80

Router#
```

(4)静态NAT方式

由于NAPT模式下虽然内网访问外网是成功的，但是从外部访问内部网络却被屏蔽了，所以当出现这种情况需要在路由器下编写静态NAT转换

> 配置内部和外部接口

由于方法在上边已经解释，这里就不在展开，直接给出代码：

```
Router(config)#int fa0/1
Router(config-if)#ip nat outside
Router(config-if)#exit

Router(config)#int fa0/0
Router(config-if)#ip nat inside
Router(config-if)#exit
```

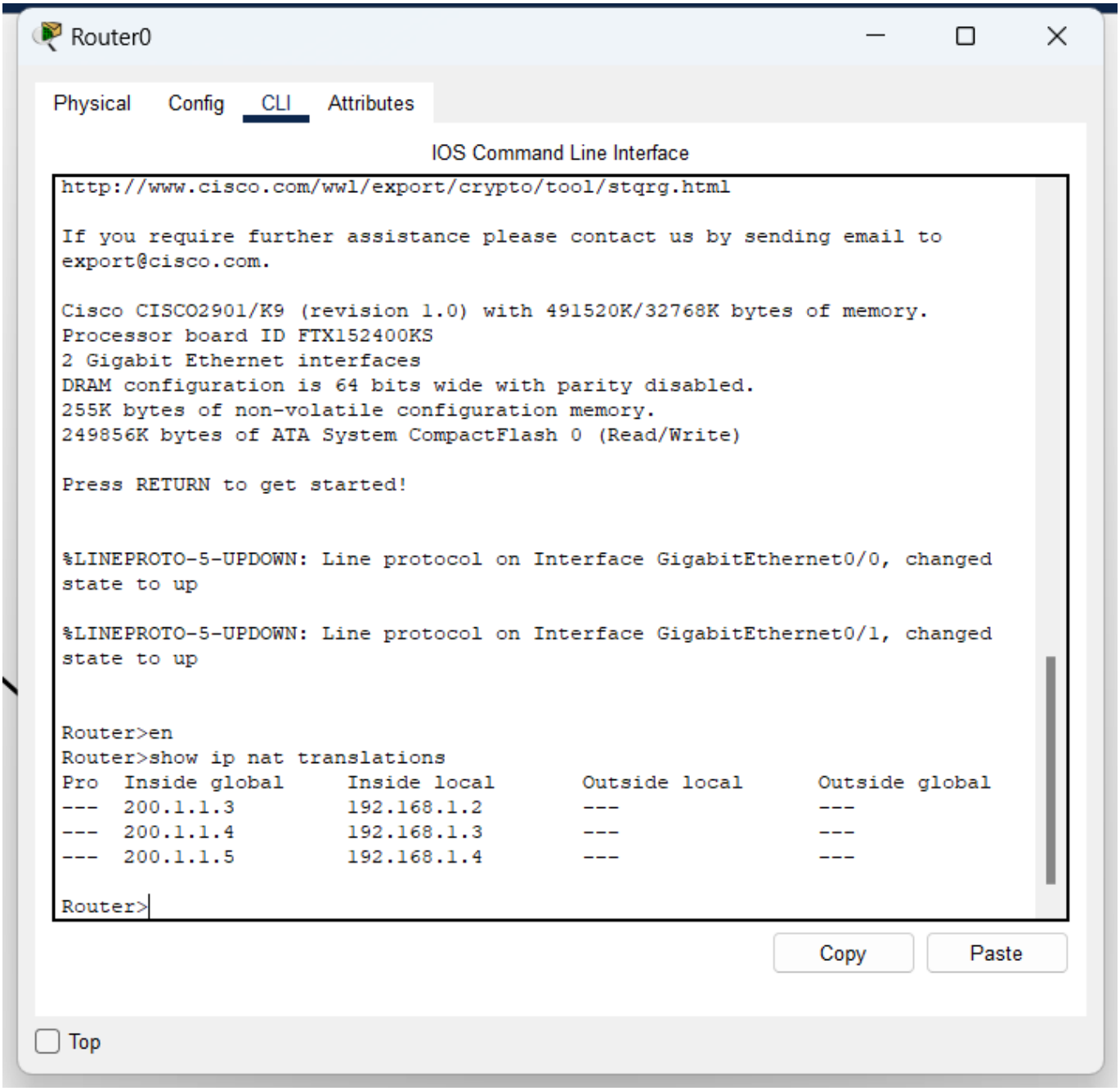
> 配置将内部局部地址与内部全局地址的静态转换

需要使用到`ip nat inside source static InsideIP OutsideIP`命令，其中InsideIP代表内部网络的地址，OutsideIP代表外部网络的地址，具体代码如下：

```
Router(config)#ip nat inside source static 192.168.1.2  200.1.1.3
Router(config)#ip nat inside source static 192.168.1.3  200.1.1.4
Router(config)#end
```

> 查看其NAT转换表

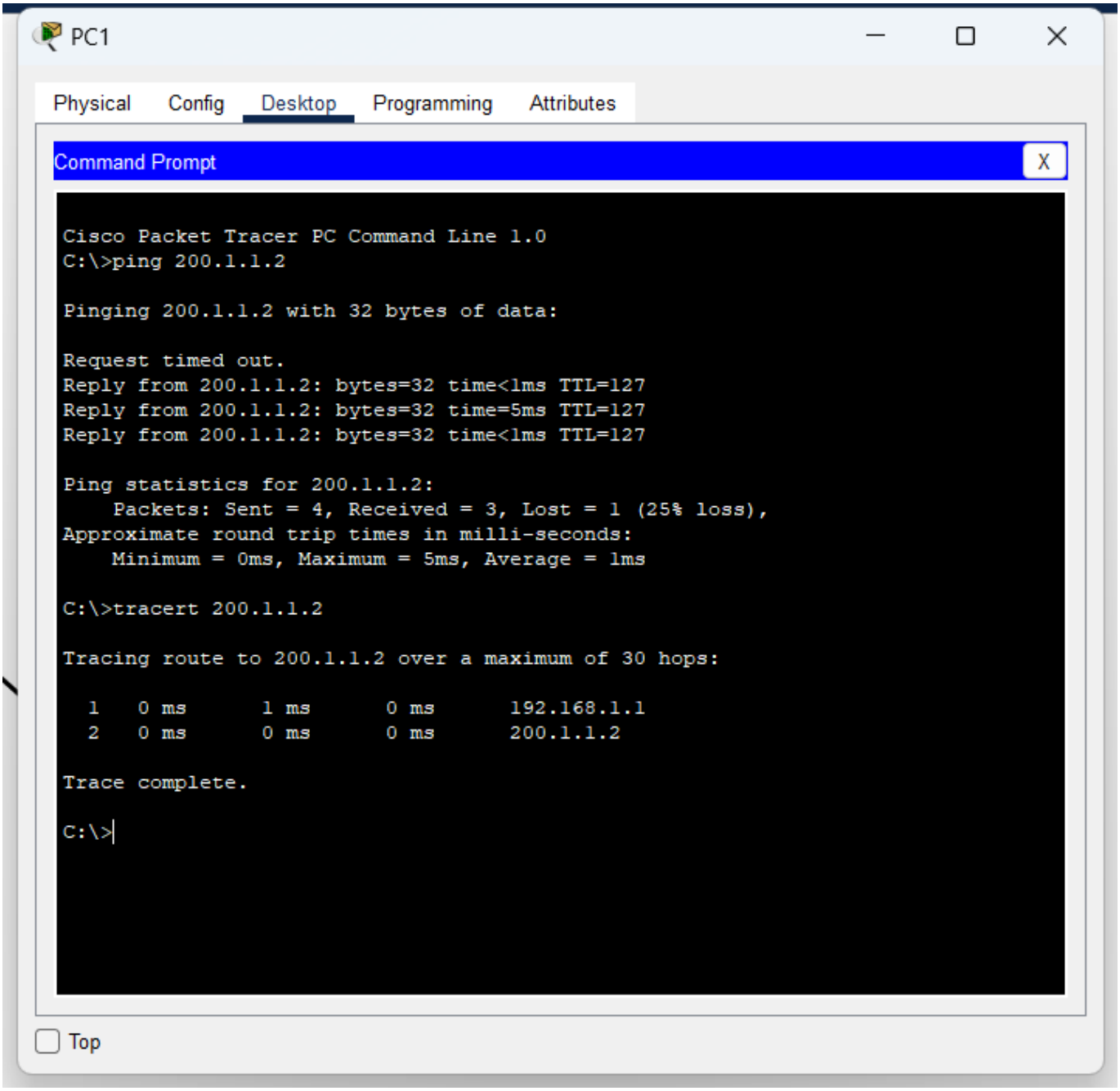
- 可以在路由器中输入`show ip translations`查看其NAT转换表，如下图所示：



***(5)*实验结果**

> 内网到外网

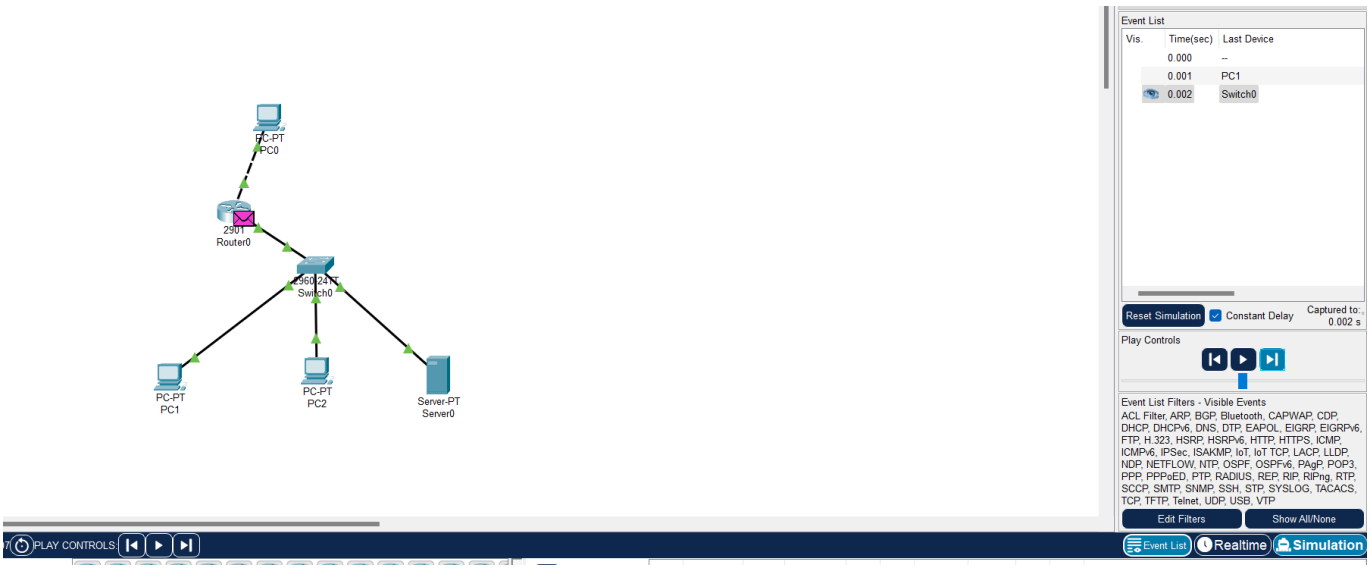
首先使用 PC1 去 ping PC0，如下图所示：



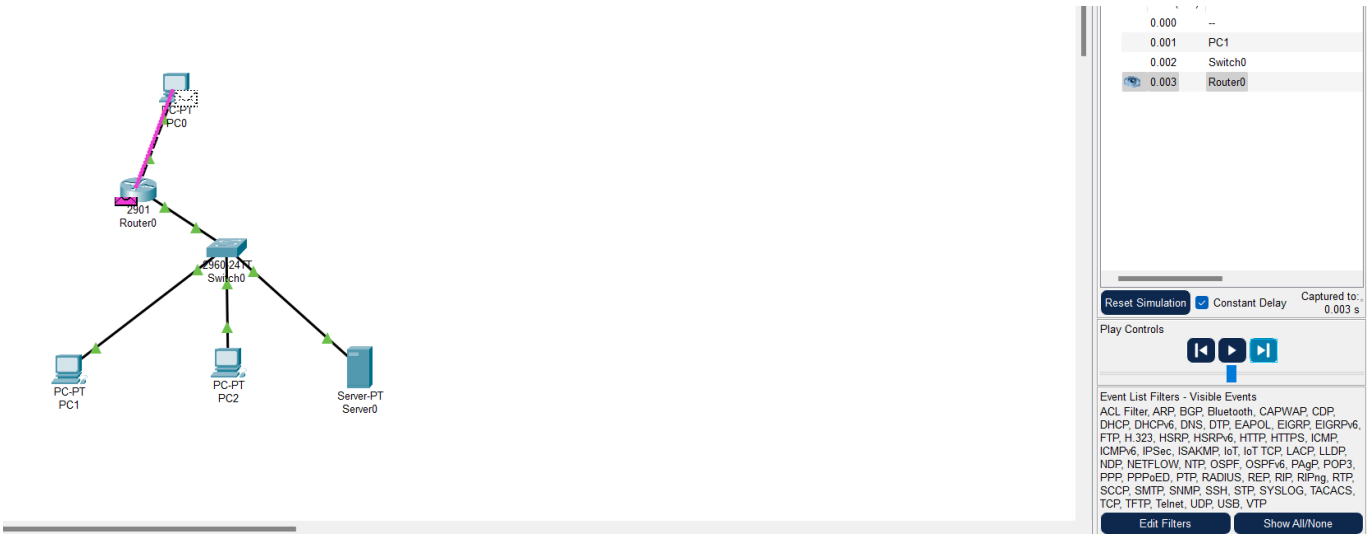
发现可以ping通，接下来使用tracert命令查看具体路径：

仿真环境的“模拟”方式中的传递过程

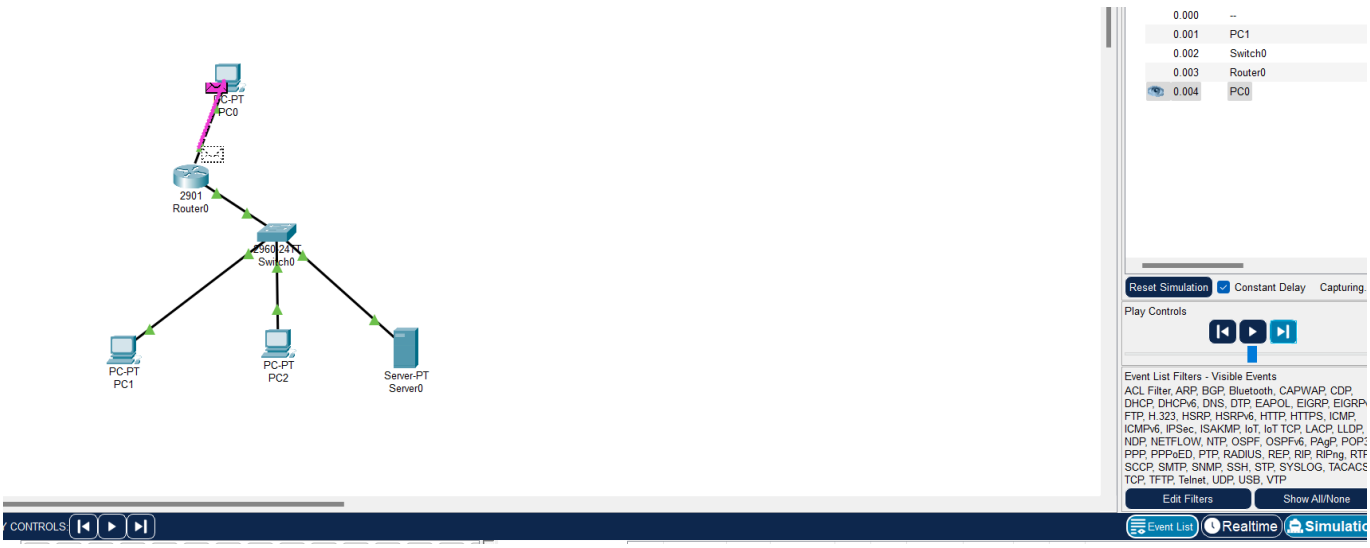
接下来在仿真环境的“模拟”方式中观察IP数据报在互联网中的传递过程，并对IP数据报的地址进行分析



- 首先由内网的PC1将数据报发向交换机

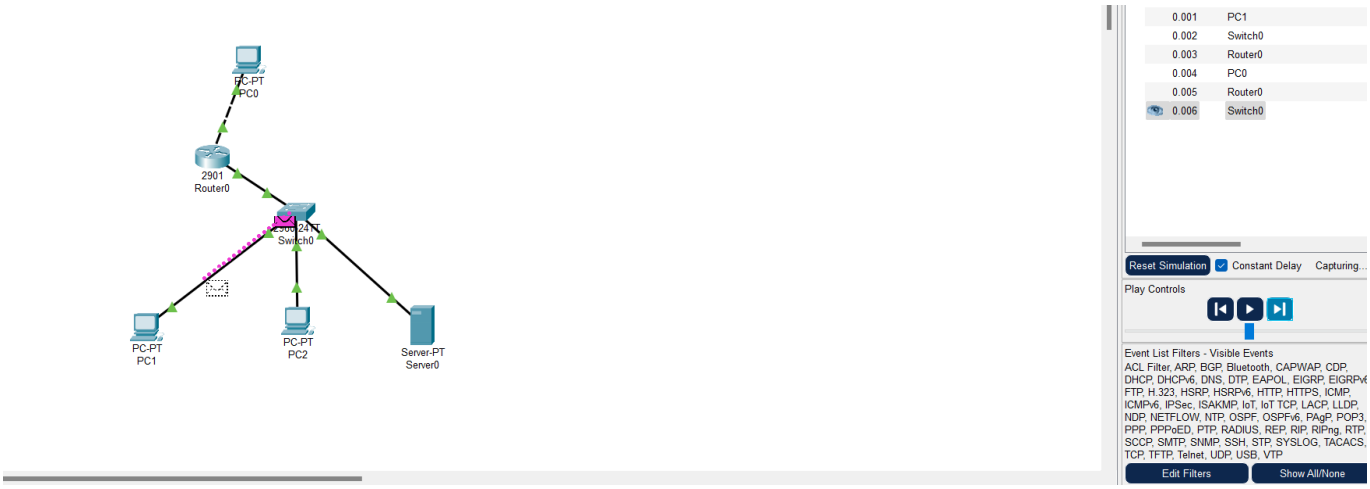


- 接下来由交换机判断地址并发向路由器

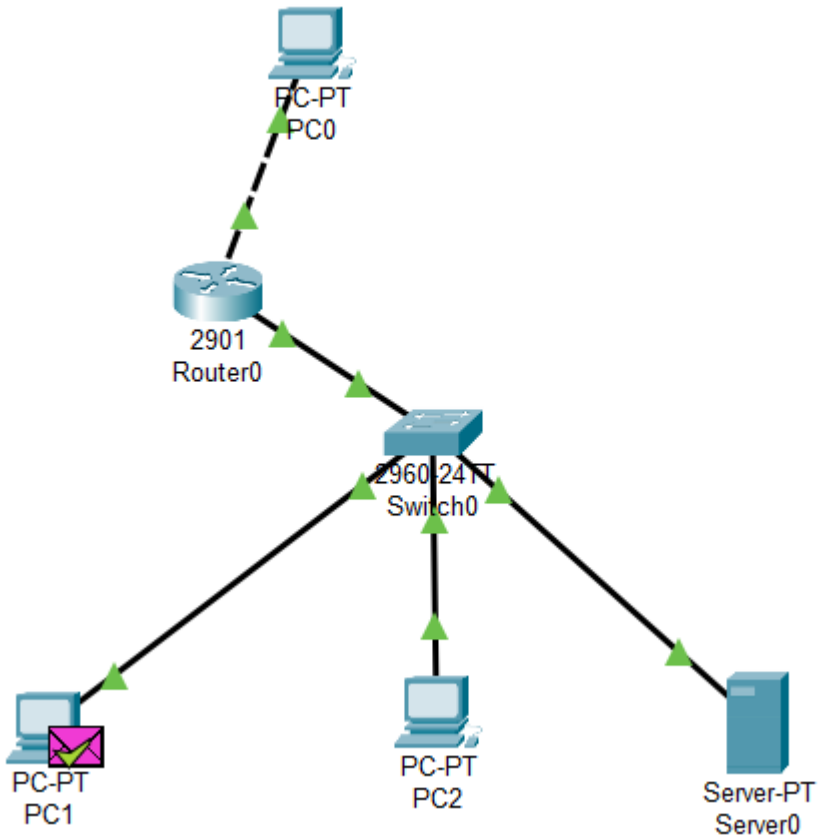


- 然后路由器进行NAT转换，并将其发向外网的PC0

- 随后就是反过程，由外网的PC0将数据报发向路由器



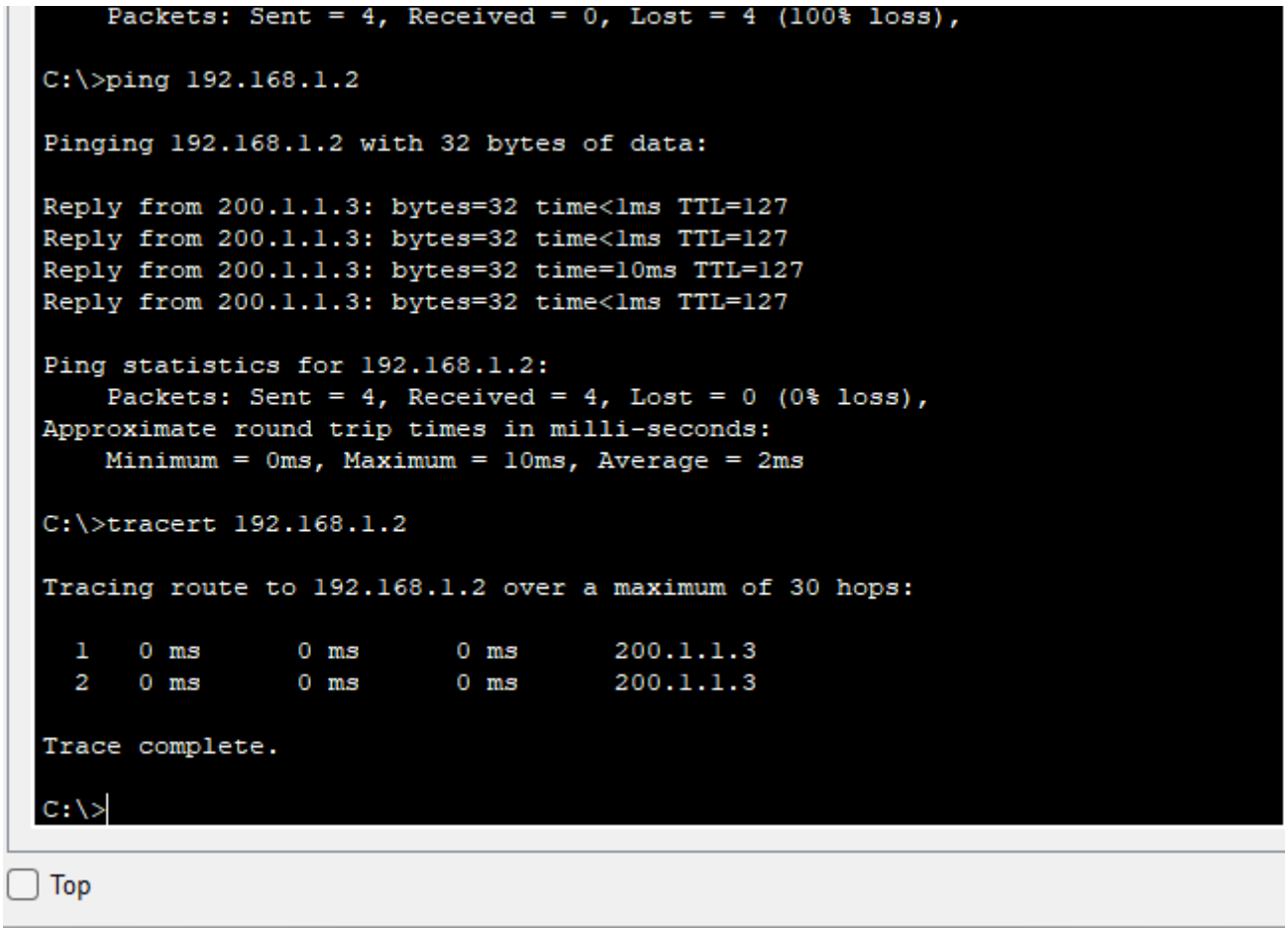
- 再由路由器做NAT转换，将其发向内网的交换机



- 最后再由交换机将其返还给PC1

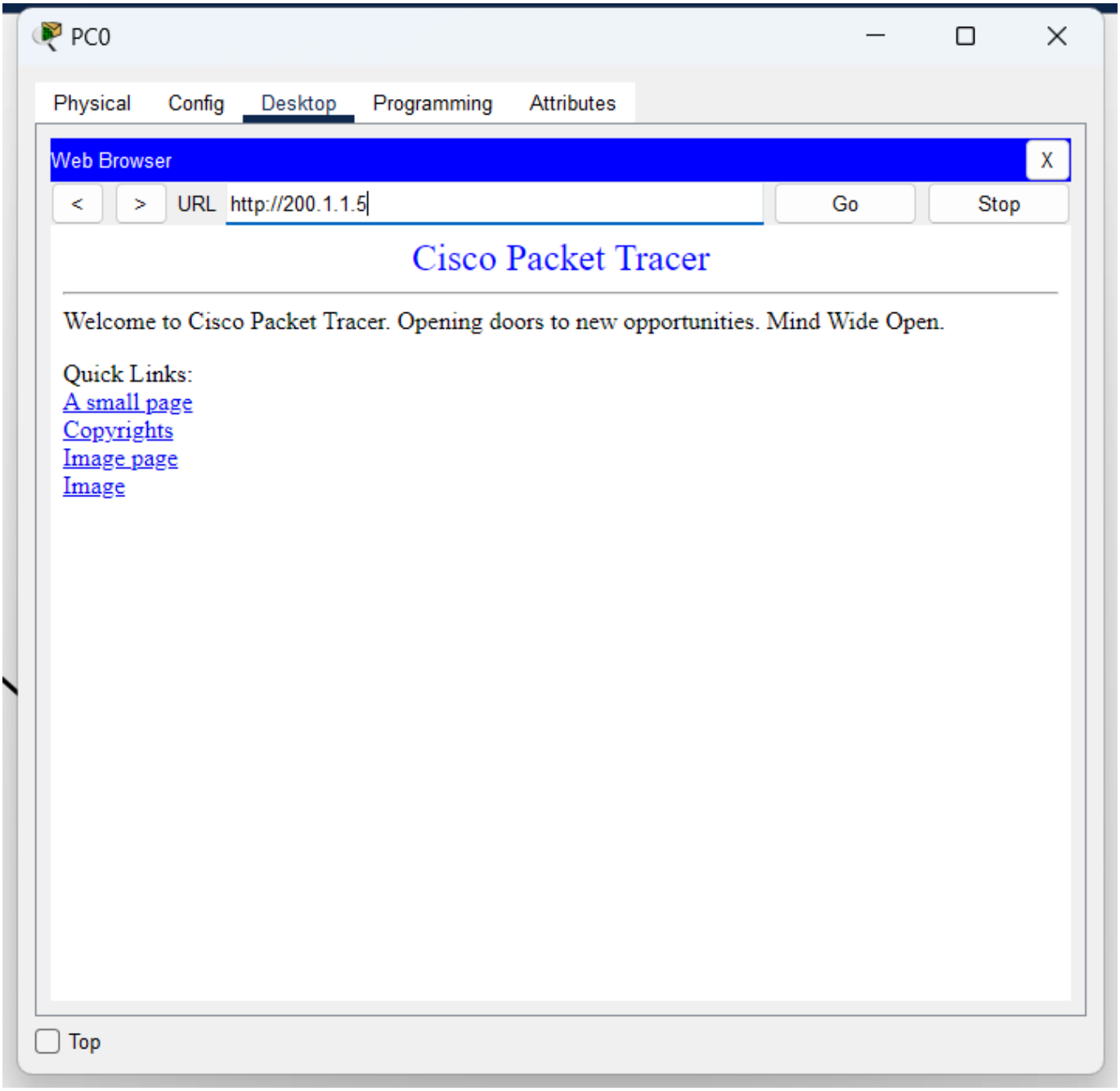
> 外网到内网

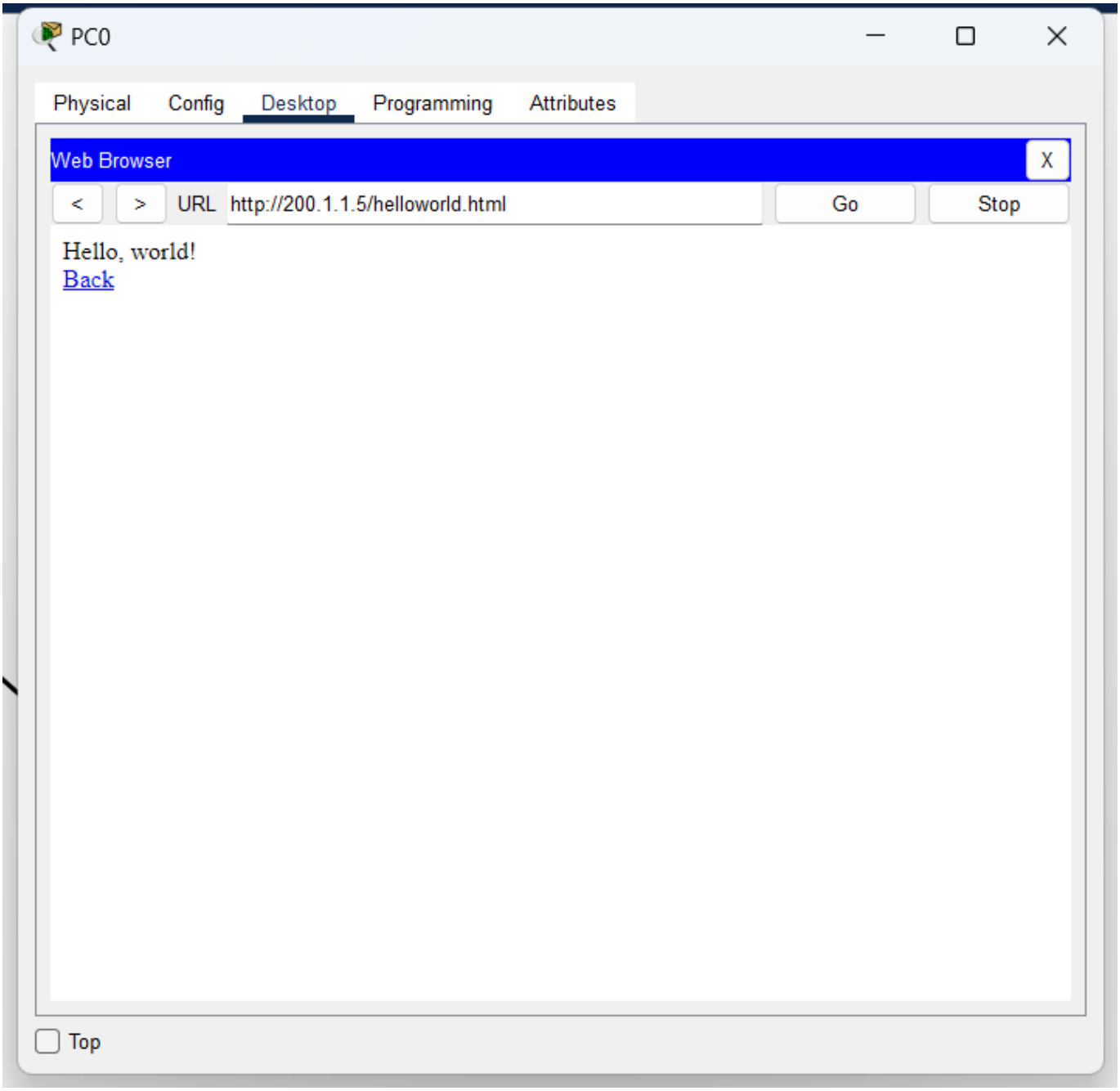
首先使用 PC0 去 ping PC1，如下图所示：



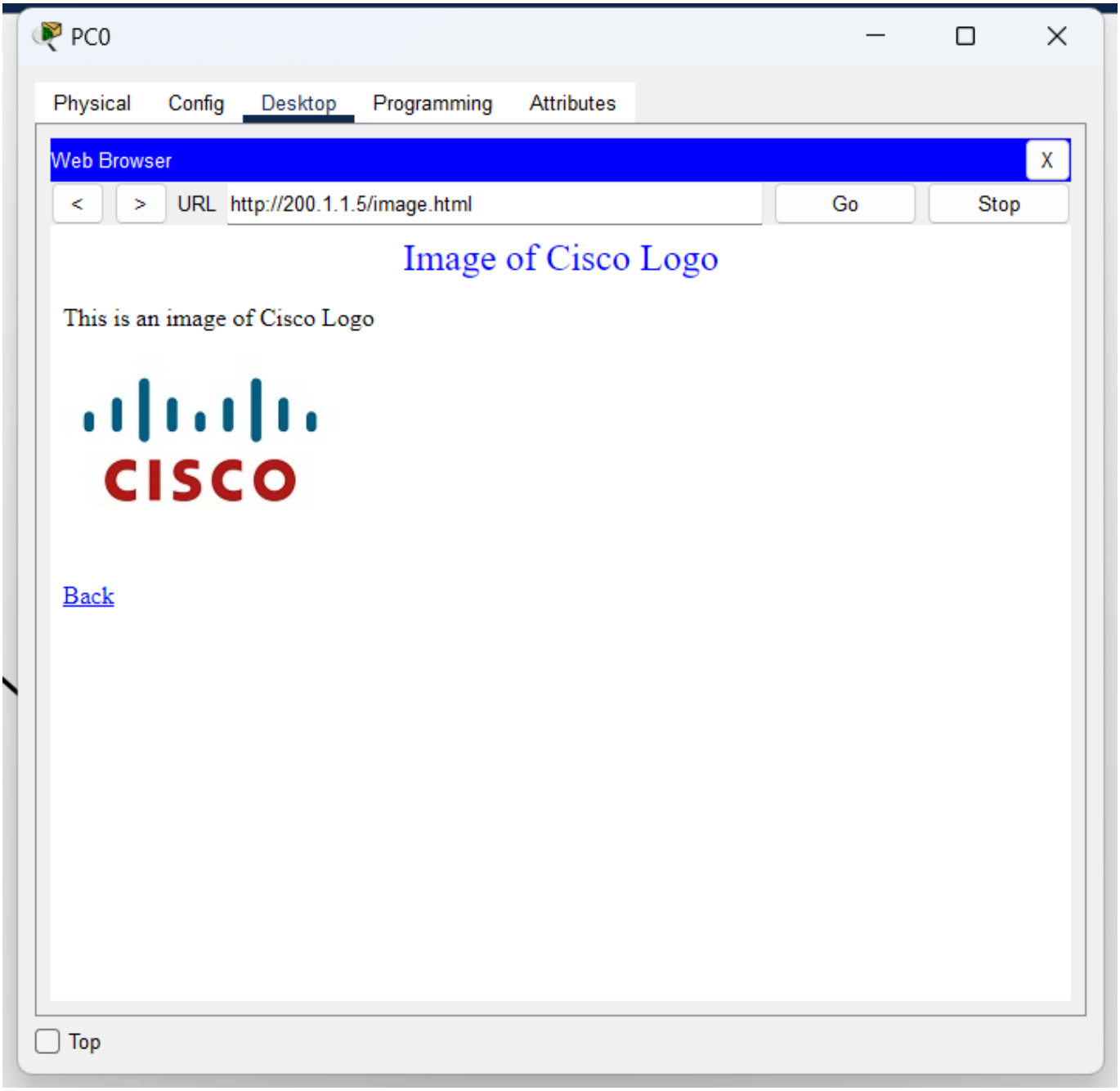
发现可以ping通，接下来使用tracert命令查看具体路径：

使用Web服务如下图所示：


PC0
Physical
Config
Desktop
Programming
Attributes
Web Browser
X
<
>
URL
http://200.1.1.5
Go
Stop
Cisco Packet Tracer
Welcome to Cisco Packet Tracer. Opening doors to new opportunities. Mind Wide Open.
Quick Links:
A small page
Copyrights
Image page
Image
Top



还可以查看其中的图片如下：



本次实验也到此结束！

四、特殊现象分析

本次在做实验的仿真实验出现了以下问题：

外部访问内部服务器

当一开始的时候使用的是`NAPT`的方式进行网络端口的转换，但这种方式却自动屏蔽了外网访问内网服务器的数据报，所以在理论课上完之后发现需要为其手动设置静态NAT连接关系，就为其设

置相应的关系。

在设置完关系后本以为大功告成了，因为已经可以从外网`ping`通内网中的主机和服务器，但当从外部主机打开内部服务器的时候又显示连接超时，最后发现在输入访问界面的时候应该输入的是相应的为其分配的NAT连接关系的地址，而不是直接的内网的对应的地址，在输入正确的网址之后本次实验也就圆满结束了。

五、总结与展望

(1)总结

本次实验是网络技术与应用的第五次实验，本次实验首先了解了NAT网络三种分配地址对应关系的方法，后又在仿真环境下进行相应的实验，NAT是我们学习计算机网络相关知识的重要部分，对我们全方面的理解网络在各个层次的传输和应用有很大的意义。对其分配的方式更加的熟悉，也对网络方面的知识更加的了解，在网络方面的认知也更上一层楼。对后续知识的学习也将不断进步，更加努力。

(2)展望

本门课程是与计算机网络课相辅相成的一门课，通过上这门课使得对计算机网络课有些不理解的地方有了更多的感悟，对网络也有了更多的兴趣，期望自己在这学期未来实验的更好的发展，也能在学习网络的过程当中不断进步，越来越强。