实验6：NAT的配置

学号：2112066 姓名：于成俊 专业：密码科学与技术

一、实验内容：

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。

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。

二、实验原理：

1.NAT：

NAT（Network Address Translation）是一种网络地址转换技术，常用于在私有网络（例如家庭网络或企业内部网络）和公共互联网之间建立连接。NAT允许多个设备共享一个公共IP地址，通过将私有内部地址转换为一个公共IP地址，使得多个设备能够共享同一个公网IP地址进行上网。

2.静态NAT：

- **地址映射是一对一的：** 静态NAT建立了一个固定的、静态的映射关系，将内部网络中的每个设备映射到一个唯一的公共IP地址。每个内部设备都有一个预先配置好的对应关系。
- **适用于服务器和特定设备：** 静态NAT通常用于需要从外部网络访问内部服务器或特定设备的场景。由于是一对一的映射，每个内部设备都可以被唯一标识。

3.动态NAT：

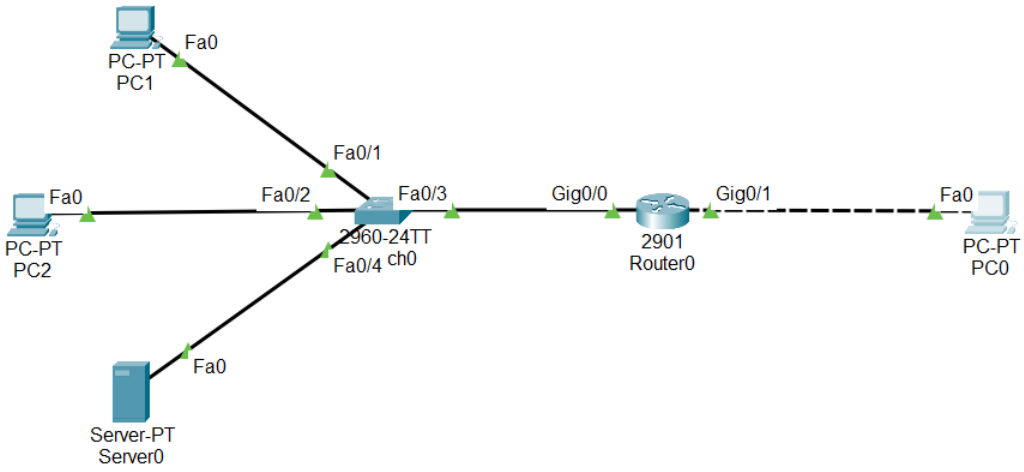
- **地址映射是动态的：** 动态NAT在需要的时候动态地为内部设备分配公共IP地址。每个内部设备在需要访问互联网时，都会被分配一个可用的公共IP地址，这个映射是临时的，通常在会话结束后释放。
- **适用于多设备共享公共IP：** 动态NAT适用于多个内部设备共享一组公共IP地址的场景。它可以更有效地利用有限的公共IP地址资源，因为公共IP地址是动态分配的。

4.共同点：

- **NAT转换表：** 静态NAT和动态NAT都使用NAT转换表，记录了内部私有IP地址和对应的公共IP地址之间的映射关系。
- **支持PAT：** 静态NAT和动态NAT都可以支持PAT（Port Address Translation），即将端口映射到不同的内部设备，以缓解地址冲突。
- **防止直接访问内部网络：** 两者都有助于隐藏内部网络结构，防止直接访问内部设备的私有IP地址。

三、实验过程

1.建立网络拓扑

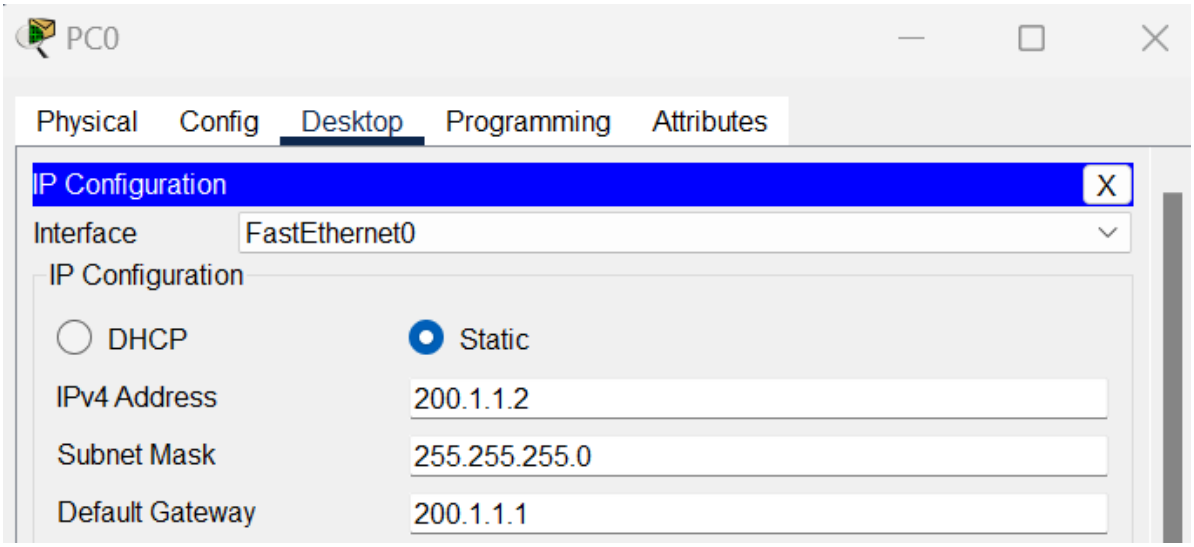


2.配置主机IP地址和路由器IP地址

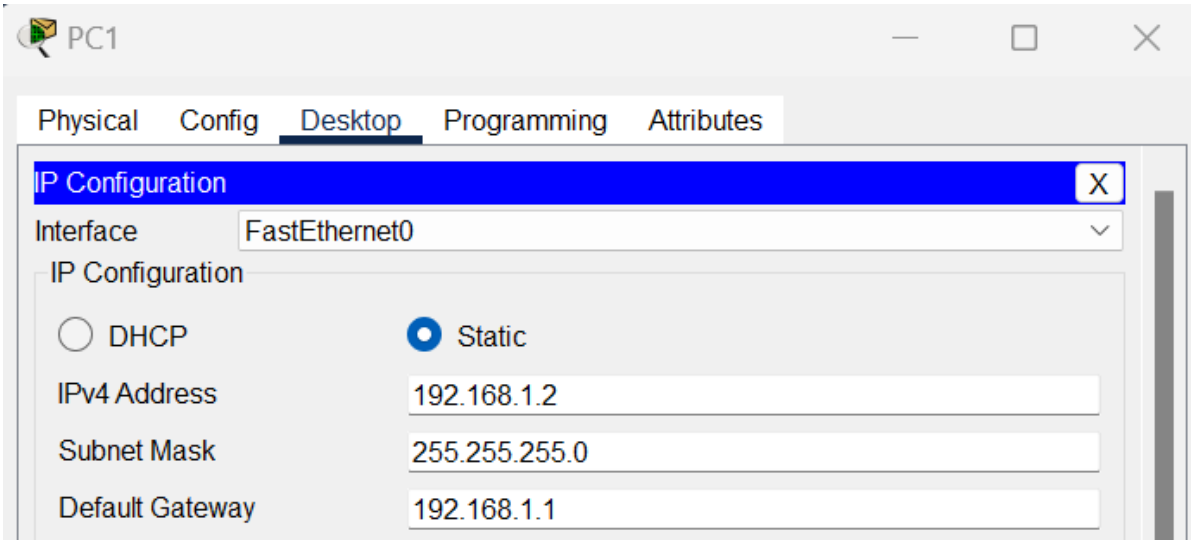
表格如下：

设备	IPv4 地址	子网掩码	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

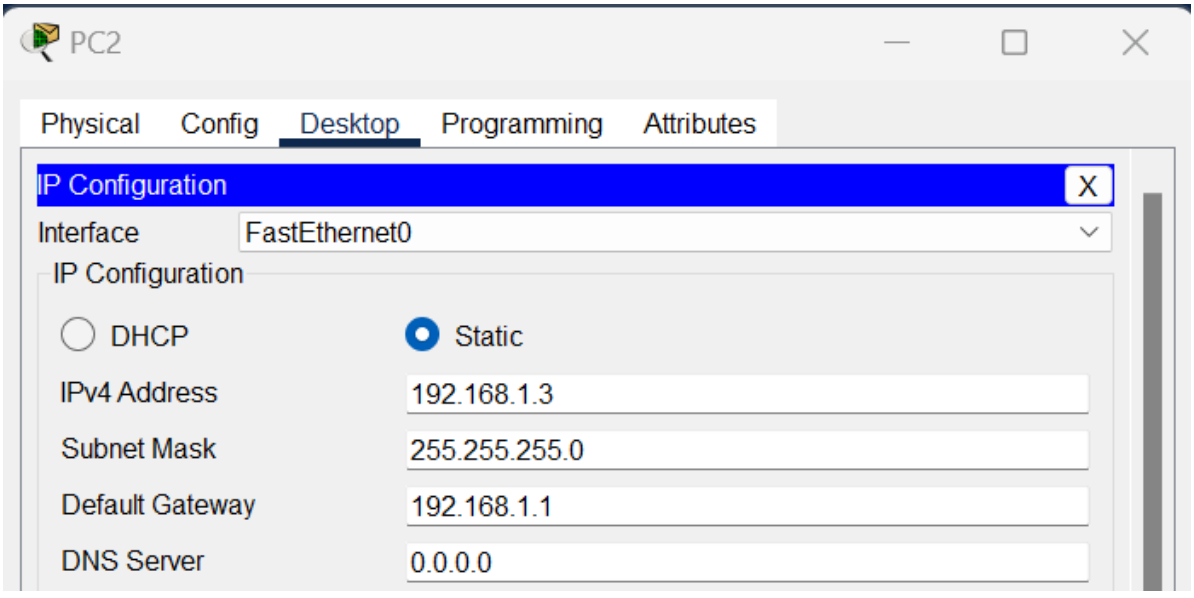
配置PC0：


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

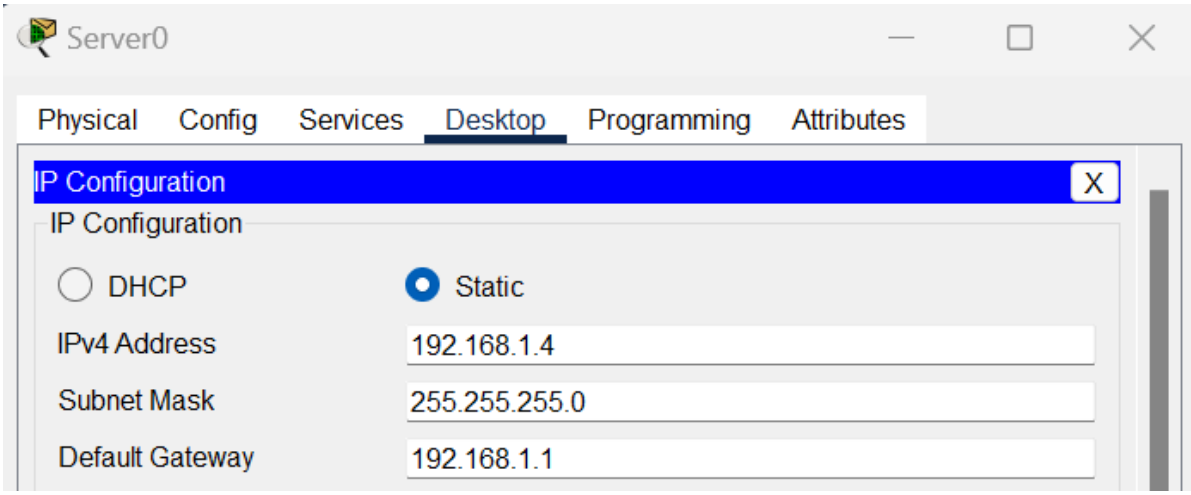
配置PC1：


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

配置PC2：


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

配置服务器：



配置路由器：

1.为路由器各个端口分配地址：

```
Router>en
Router#config t
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#int gig0/1
Router(config-if)#ip add 192.168.1.1 255.255.255.0
Router(config-if)#no shut

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

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
```

2.查看路由器各个接口的ip地址，保证操作正确：

```
Router>en
Router#show ip interface brief
Interface              IP-Address      OK? Method Status                Protocol
GigabitEthernet0/0     192.168.1.1     YES manual up                    up
GigabitEthernet0/1     200.1.1.1       YES manual up                    up
Vlan1                  unassigned      YES unset  administratively down down
```

3. NAT配置

1.配置地址池：

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表示该地址池的起始IP地址。
- EndIP表示该地址池的终止IP地址。
- Mask表示该地址池的掩码。

我设置为：`ip nat pool myNATPool 202.113.25.1 202.113.25.10 netmask 255.255.255.0`

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。

2.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。

我设置为：`access-list 6 permit 10.0.0.0 0.255.255.255`

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。

3.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。

我设置为：`ip nat inside source list 6 pool myNATPool overload`

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。

4.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。

以上命令运行如下：

```
Router>en
Router#config t
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 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)#
```

5.静态NAT

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，所以需要在路由器中编写静态NAT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。

运行如下：

```
Router>en
Router#config t
Enter configuration commands, one per line.  End with CNTL/Z.
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
Router#
%SYS-5-CONFIG_I: Configured from console by console
```

并将公网ip的80端口映射给Server服务器：

```
Router>en
Router#config t
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#ip nat inside source static tcp 192.168.1.4 80
200.1.1.5 80
```

四、实验结果展示

内网到外网

在主机PC1上 **ping** PC0（ip地址为200.1.1.2）

```
C:\>ping 200.1.1.2

Pinging 200.1.1.2 with 32 bytes of data:

Reply from 200.1.1.2: bytes=32 time<1ms TTL=127
Reply from 200.1.1.2: bytes=32 time<1ms TTL=127
Reply from 200.1.1.2: bytes=32 time<1ms TTL=127
Reply from 200.1.1.2: bytes=32 time<1ms TTL=127

Ping statistics for 200.1.1.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

在主机PC1上 **tracert** PC0

```
C:\>tracert 200.1.1.2

Tracing route to 200.1.1.2 over a maximum of 30 hops:

  1    0 ms      0 ms      0 ms      192.168.1.1
  2    0 ms      0 ms      0 ms      200.1.1.2

Trace complete.
```

外网到内网

在主机PC0上 **ping** PC1（ip地址为192.168.1.2）

```
Cisco Packet Tracer PC Command Line 1.0
C:\>ping 192.168.1.2

Pinging 192.168.1.2 with 32 bytes of data:

Reply from 200.1.1.3: bytes=32 time<1ms TTL=127
Reply from 200.1.1.3: bytes=32 time<1ms TTL=127
Reply from 200.1.1.3: bytes=32 time<1ms TTL=127
Reply from 200.1.1.3: bytes=32 time<1ms TTL=127

Ping statistics for 192.168.1.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

在主机PC0上 **tracert** PC1

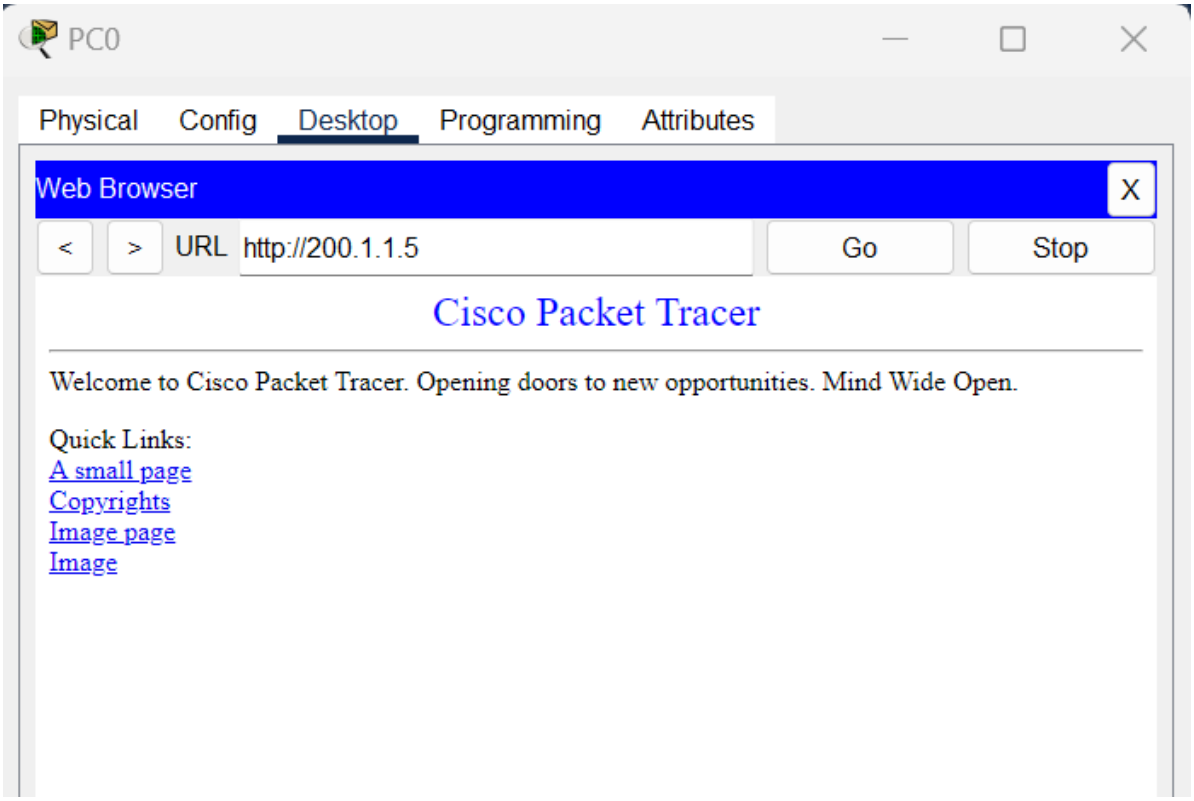
```
C:\>tracert 192.168.1.2

Tracing route to 192.168.1.2 over a maximum of 30 hops:

  1    0 ms      0 ms      0 ms      200.1.1.1
  2    0 ms      0 ms      0 ms      200.1.1.3

Trace complete.
```

在外网，即PC0上访问内网的服务器



查看NAT的工作状态

使用`show ip nat statistics`，查看有关活动转换总数，NAT配置参数，池中地址数量和已分配地址数量的信息。

```
Router#show ip nat statistics
Total translations: 5 (3 static, 2 dynamic, 2 extended)
Outside Interfaces: GigabitEthernet0/1
Inside Interfaces: GigabitEthernet0/0
Hits: 25  Misses: 33
Expired translations: 18
Dynamic mappings:
```

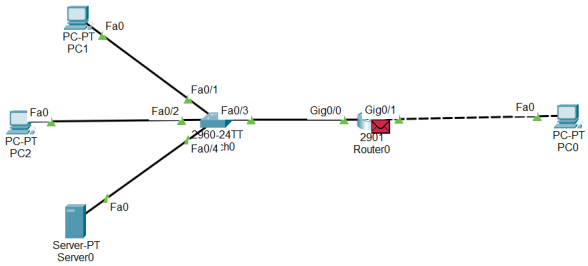
使用`show ip nat translations`**查看NAT转换表。**

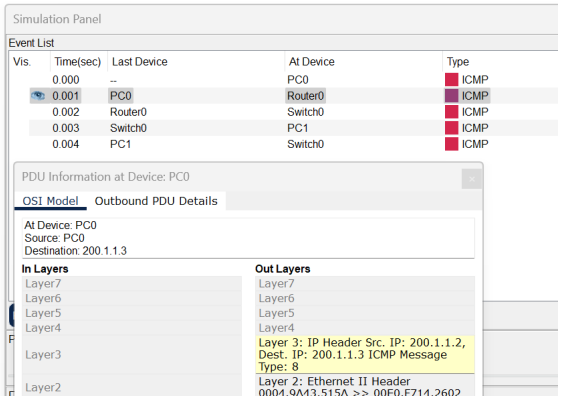
```
Router#show ip nat translations
Pro  Inside global     Inside local       Outside local
Outside global
---  200.1.1.3         192.168.1.2        ---
---
---  200.1.1.4         192.168.1.3        ---
---
---  200.1.1.5         192.168.1.4        ---
---
tcp 200.1.1.5:80       192.168.1.4:80     200.1.1.2:1025
200.1.1.2:1025
tcp 200.1.1.5:80       192.168.1.4:80     200.1.1.2:1026
200.1.1.2:1026
```

仿真环境的“模拟”方式中的传递过程

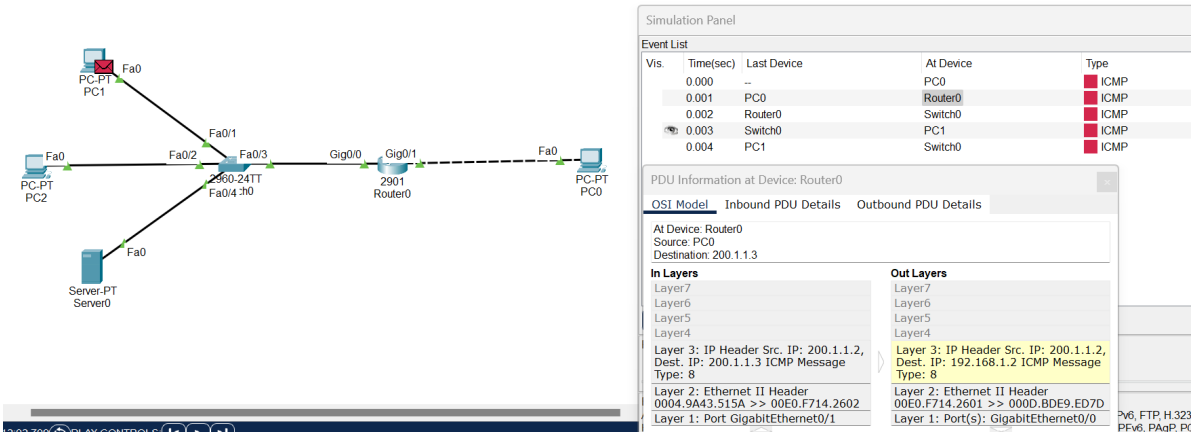
1.观察外网到内网的过程（PC0 ping PC1）ping PC1的外网地址，即200.1.1.3

首先PC0将数据包发给路由器Router0，数据包的目的IP地址为**200.1.1.3**



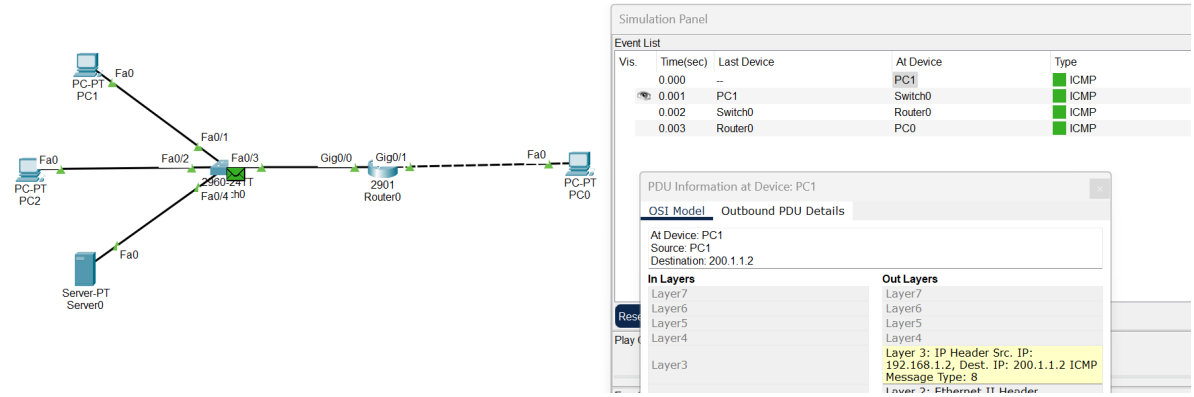


然后，路由器做NAT转换，可以看到目的地址变为**192.168.1.2**了。它将其发给交换机，最后交换机发给目的主机，即PC1。

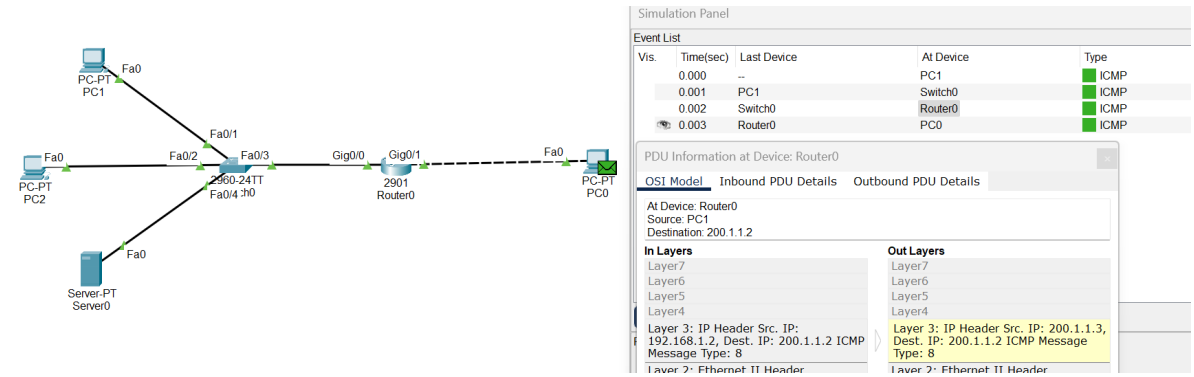


2.观察内网到外网的过程（PC1 ping PC0）

首先，PC1发送给交换机，然后由交换机发给路由器。此时，可以看到数据包的源IP地址是**192.168.1.2**



然后，路由器做NAT转换，将数据包的源IP地址转化为**200.1.1.3**，发给PC0



代码链接：https://github.com/happy206/Network-Technology-and-Applications