

网络技术与应用课程实验报告

实验6：NAT配置

姓名：孟启轩 学号：2212452 专业：计算机科学与技术

一、实验内容说明

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。

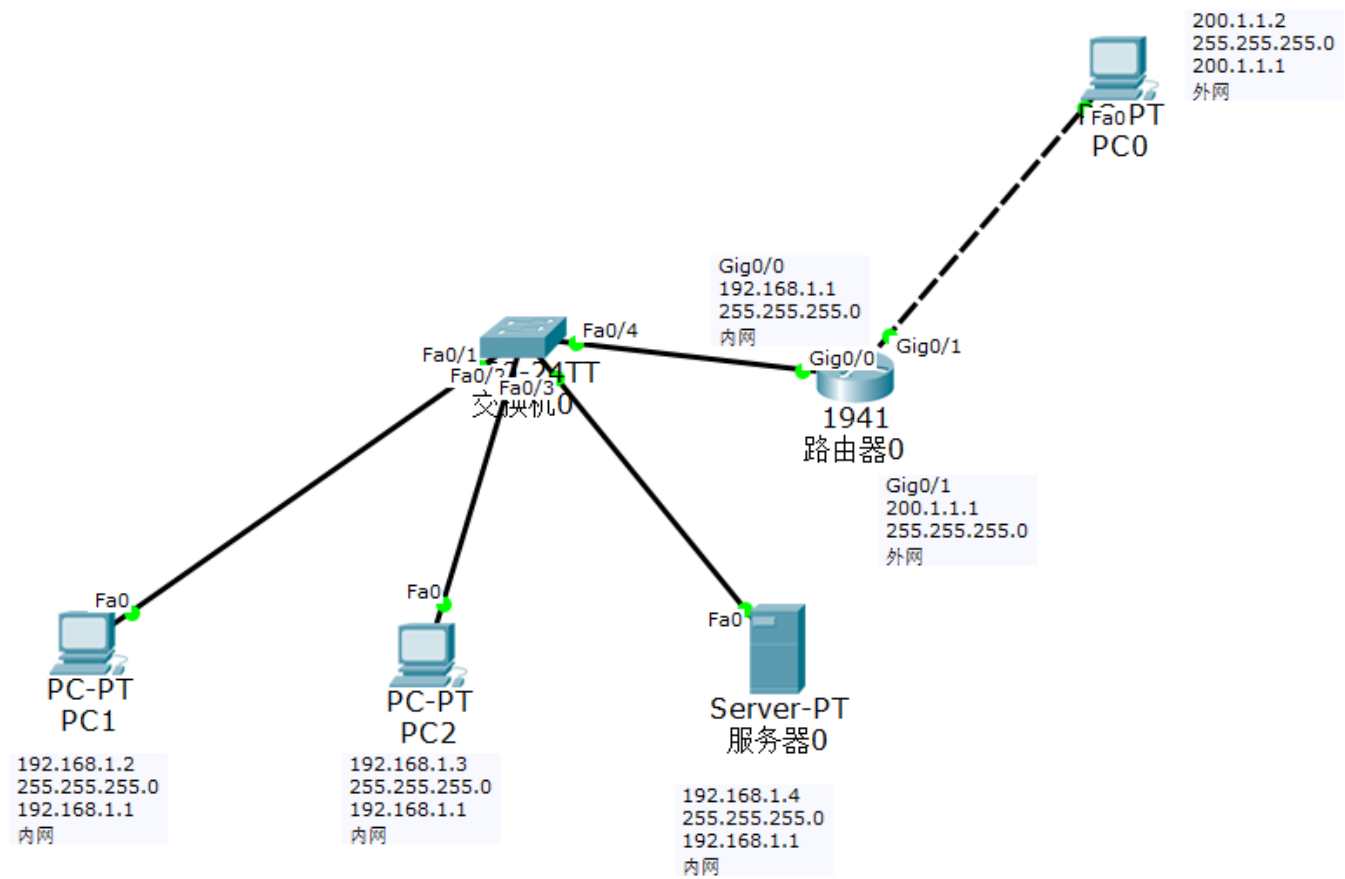
2、在仿真环境下完成如下实验

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。

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

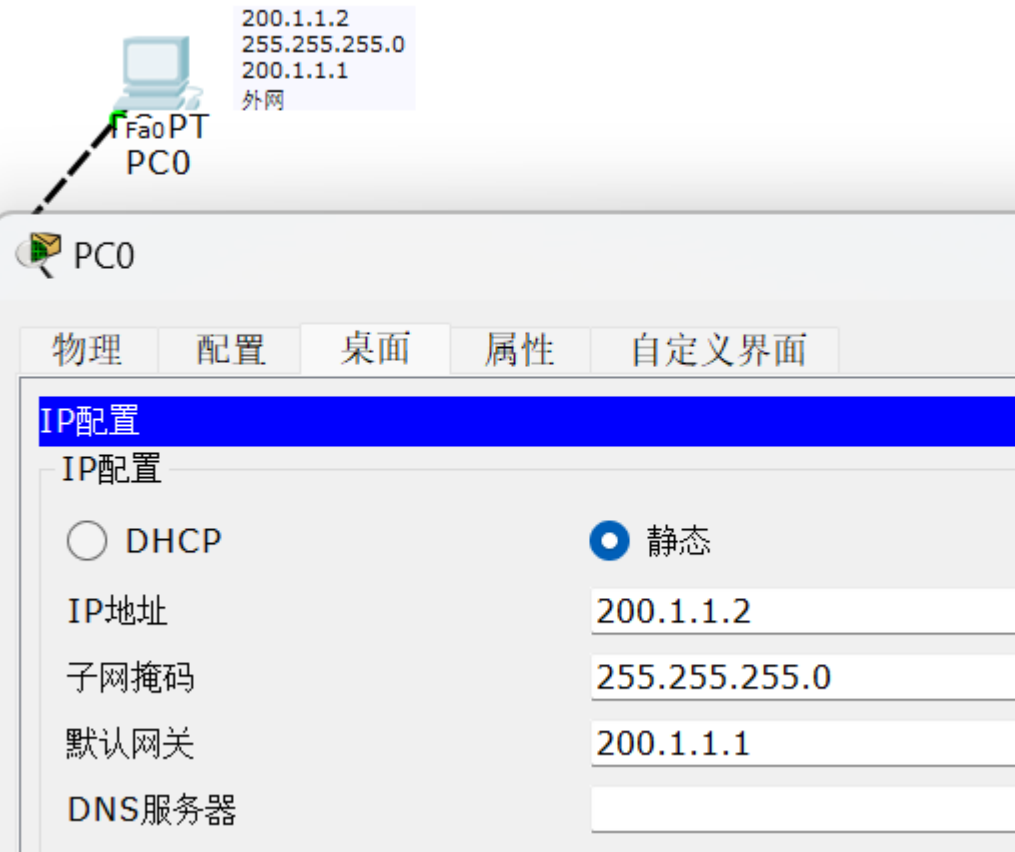
Machine	IPv4 Address	Subnet Mask	网关	内/外网
PC0	200.1.1.2	255.255.255.0	200.1.1.1	外网
PC1	192.168.1.2	255.255.255.0	192.168.1.1	内网
PC2	192.168.1.3	255.255.255.0	192.168.1.1	内网
Server0	192.168.1.4	255.255.255.0	192.168.1.1	内网
Router0 Gig0/0	192.168.1.1	255.255.255.0		内网
Router0 Gig0/1	200.1.1.1	255.255.255.0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

三、实验过程

本次实验分为两个主要部分：首先，我学习了路由器的NAT配置过程，组建了一个由NAT连接的内网和外网，并测试了网络的连通性，同时观察了网络地址映射表及其传递过程。其次，确保外部主机能够顺利访问内部网络中的服务器提供的Web服务。由于这两部分实验使用相同的程序，因此接下来我将从整个项目的角度来详细介绍实验过程。

(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：



Fa0

PC-PT

PC1

192.168.1.2

255.255.255.0

192.168.1.1

内网

PC1

物理

配置

桌面

属性

自定义界面

IP配置

IP配置

DHCP

静态

IP地址

192.168.1.2

子网掩码

255.255.255.0

默认网关

192.168.1.1

DNS服务器

Fa0

PC-PT

PC2

192.168.1.3

255.255.255.0

192.168.1.1

内网

PC2

物理

配置

桌面

属性

自定义界面

IP配置

IP配置

DHCP

静态

IP地址

192.168.1.3

子网掩码

255.255.255.0

默认网关

192.168.1.1

DNS服务器

Fa0

Server-PT

服务器0

192.168.1.4

255.255.255.0

192.168.1.1

内网

服务器0

物理

配置

服务

桌面

属性

自定义界面

IP配置

接口FastEthernet0

IP配置

DHCP

静态

IP地址

192.168.1.4

子网掩码

255.255.255.0

默认网关

192.168.1.1

DNS服务器

(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是用户选择的标识符，StartIP和EndIP分别表示地址池的起始和终止IP地址，Mask则是掩码。

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（范围为1 ~ 99），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IP地址之间的关联。

这里的LabelID是之前定义的访问列表编号，PoolName是IP地址池的名称，overload关键词表示采用NAPT方式，允许地址池中的IP地址重用。

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)#
```

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
```

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#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

在NAPT模式下，内网设备可以成功访问外网，但外部网络却无法直接访问内网设备。这是因为NAPT模式主要用于单向的地址转换，即从内网到外网的转换，而不支持外网到内网的转换。因此，当需要从外部网络访问内部网络时，需要在路由器上配置静态NAT，以实现双向的地址转换。

配置内部和外部接口

```
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：

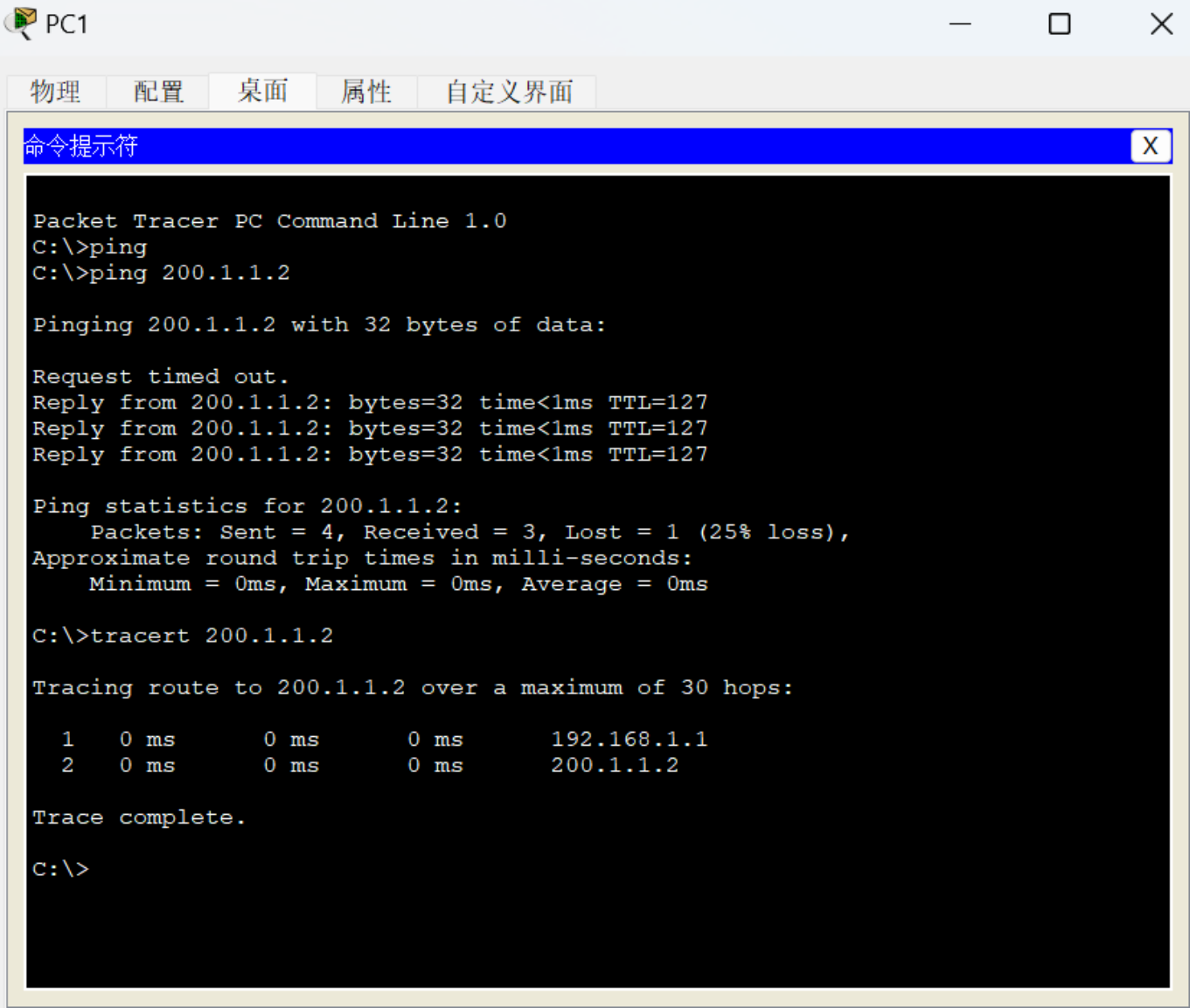
```
Router>
Router>enable
Router#show ip nat translations
Pro  Inside global      Inside local      Outside local      Outside global
---  200.1.1.3           192.168.1.2      ---               ---
---  200.1.1.4           192.168.1.3      ---               ---
---  200.1.1.5           192.168.1.4      ---               ---

Router#|
```

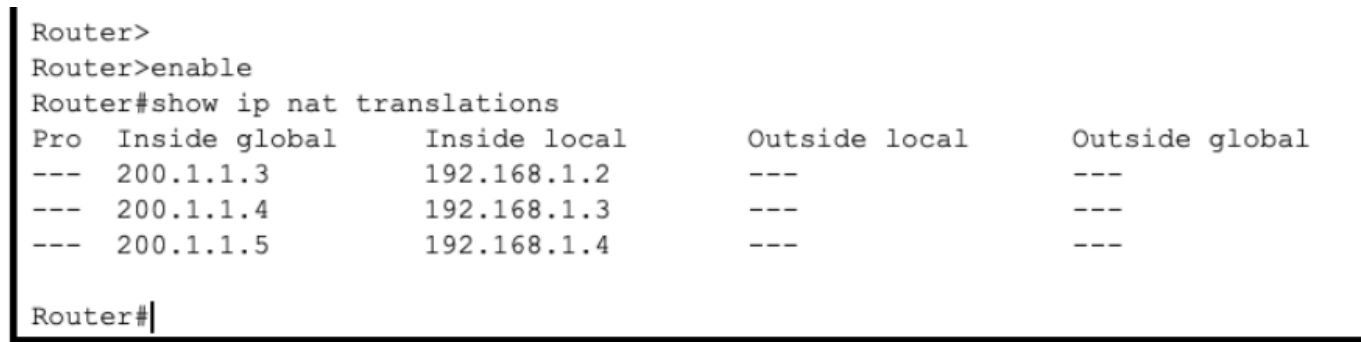
(5)实验结果

内网到外网

使用 PC1 去 `ping` PC0，并使用`tracert`命令查看过程，如下图所示：



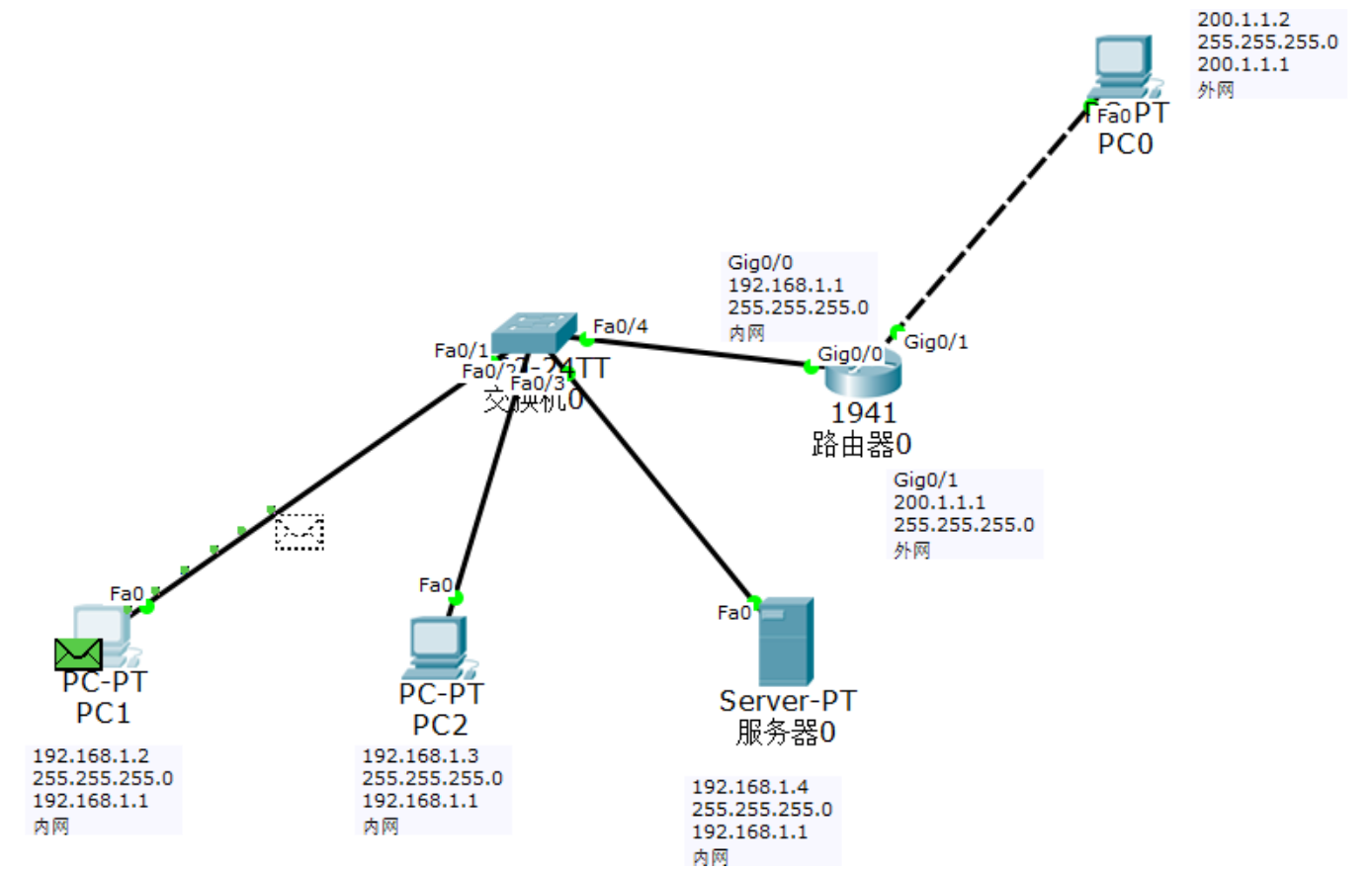
网络地址映射表如下图所示：



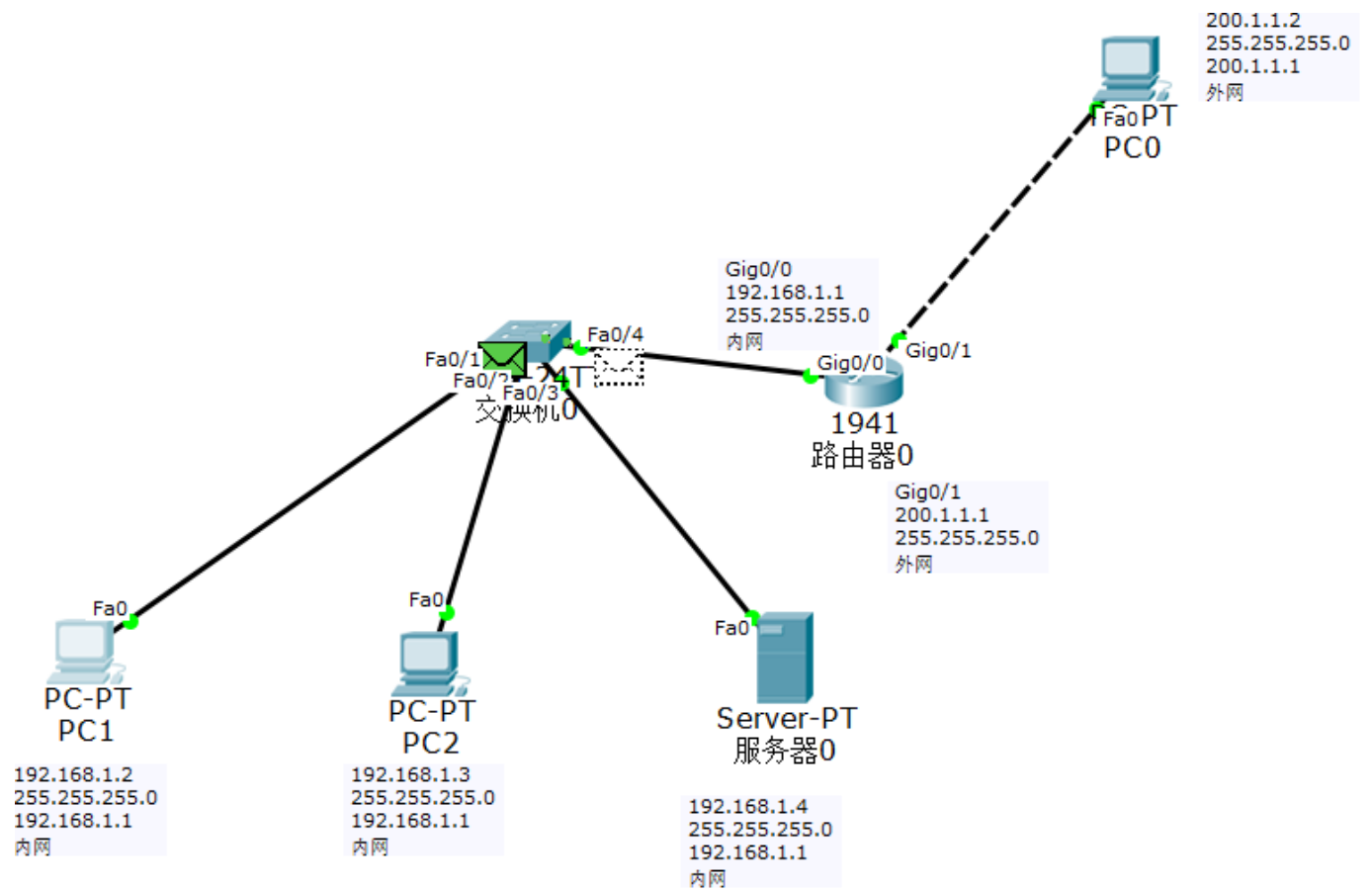
仿真环境的“模拟”方式中的传递过程

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

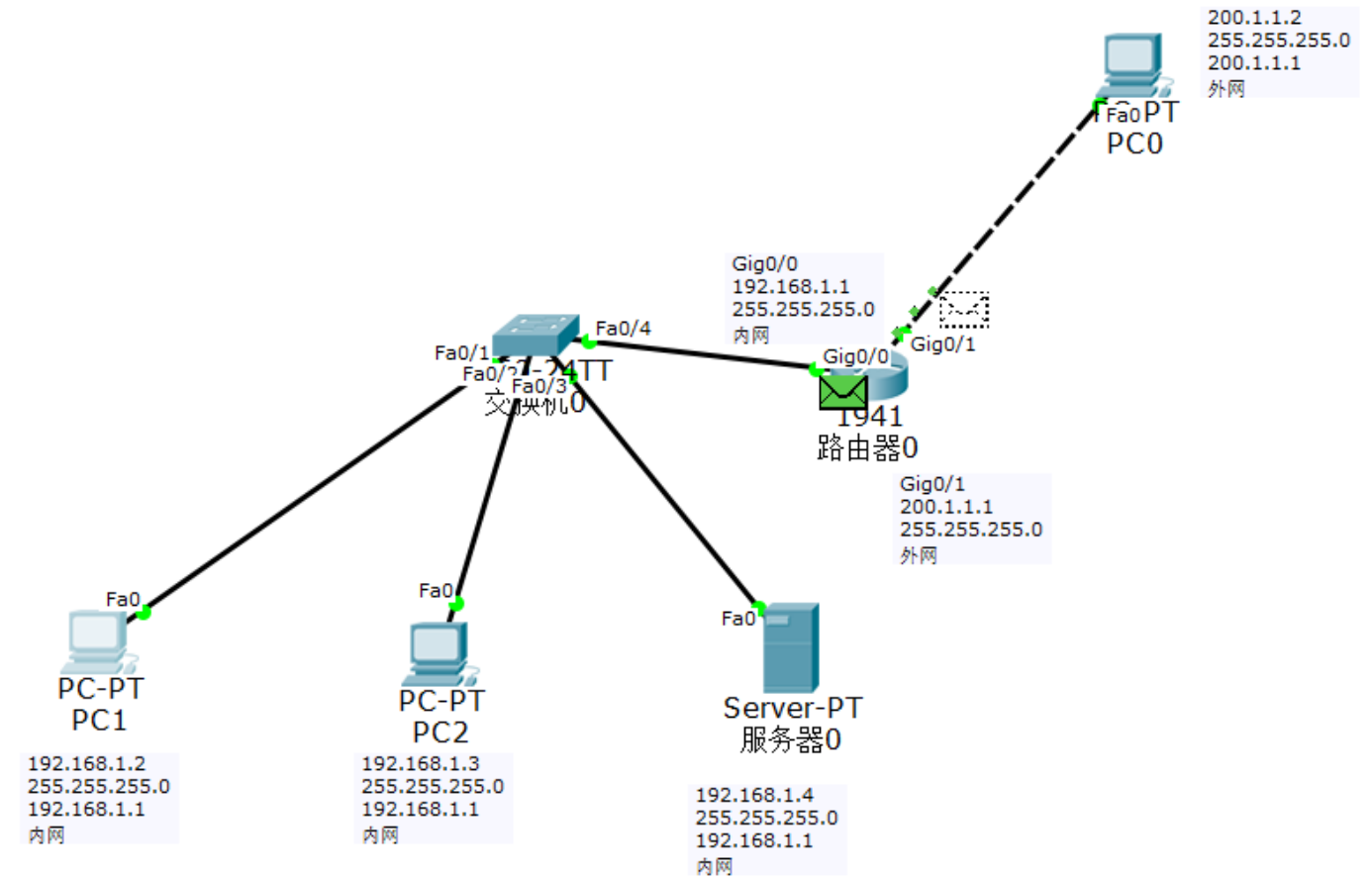
- 首先由内网的PC1将数据报发向交换机



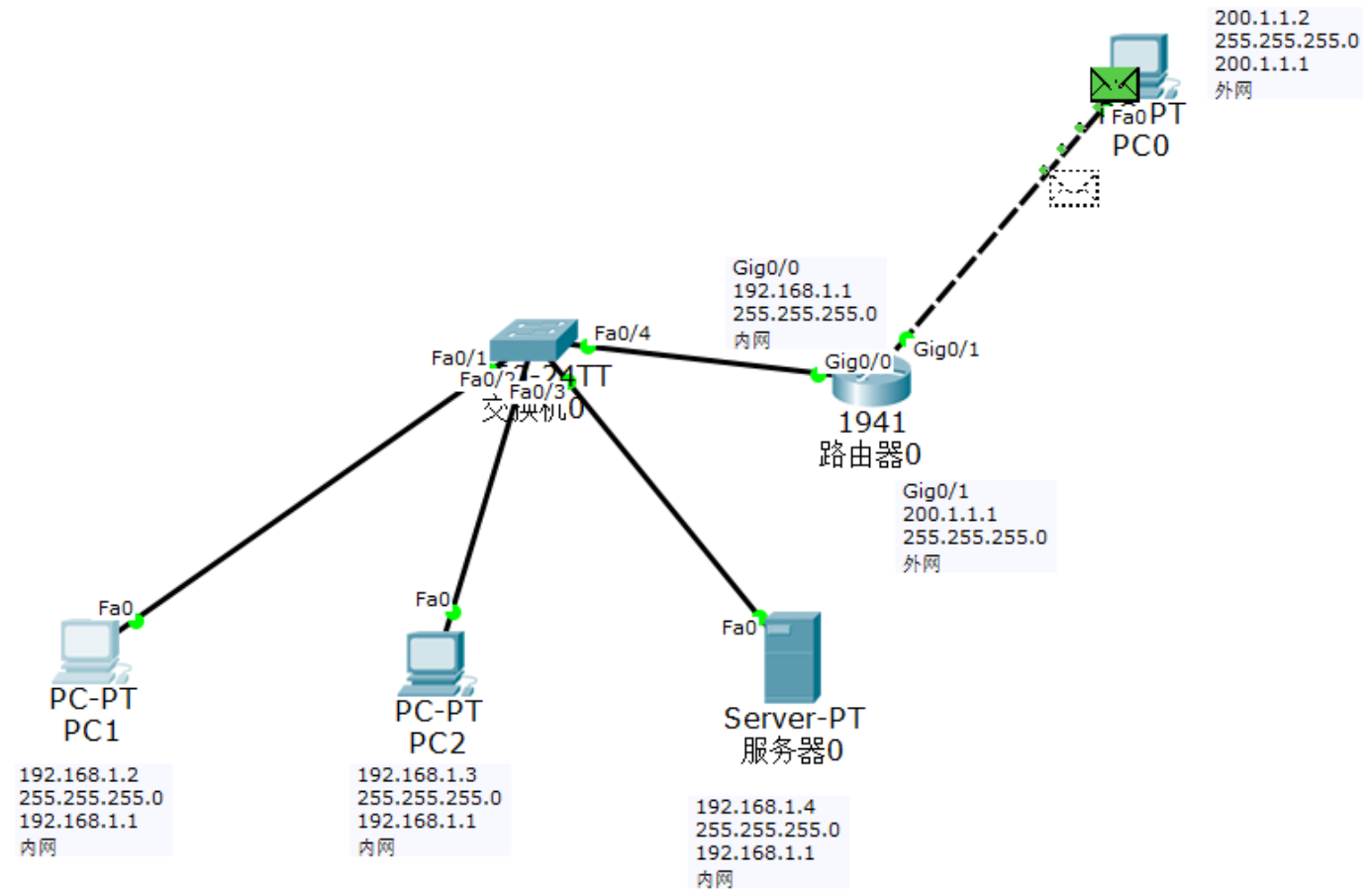
- 接下来由交换机判断地址并发向路由器



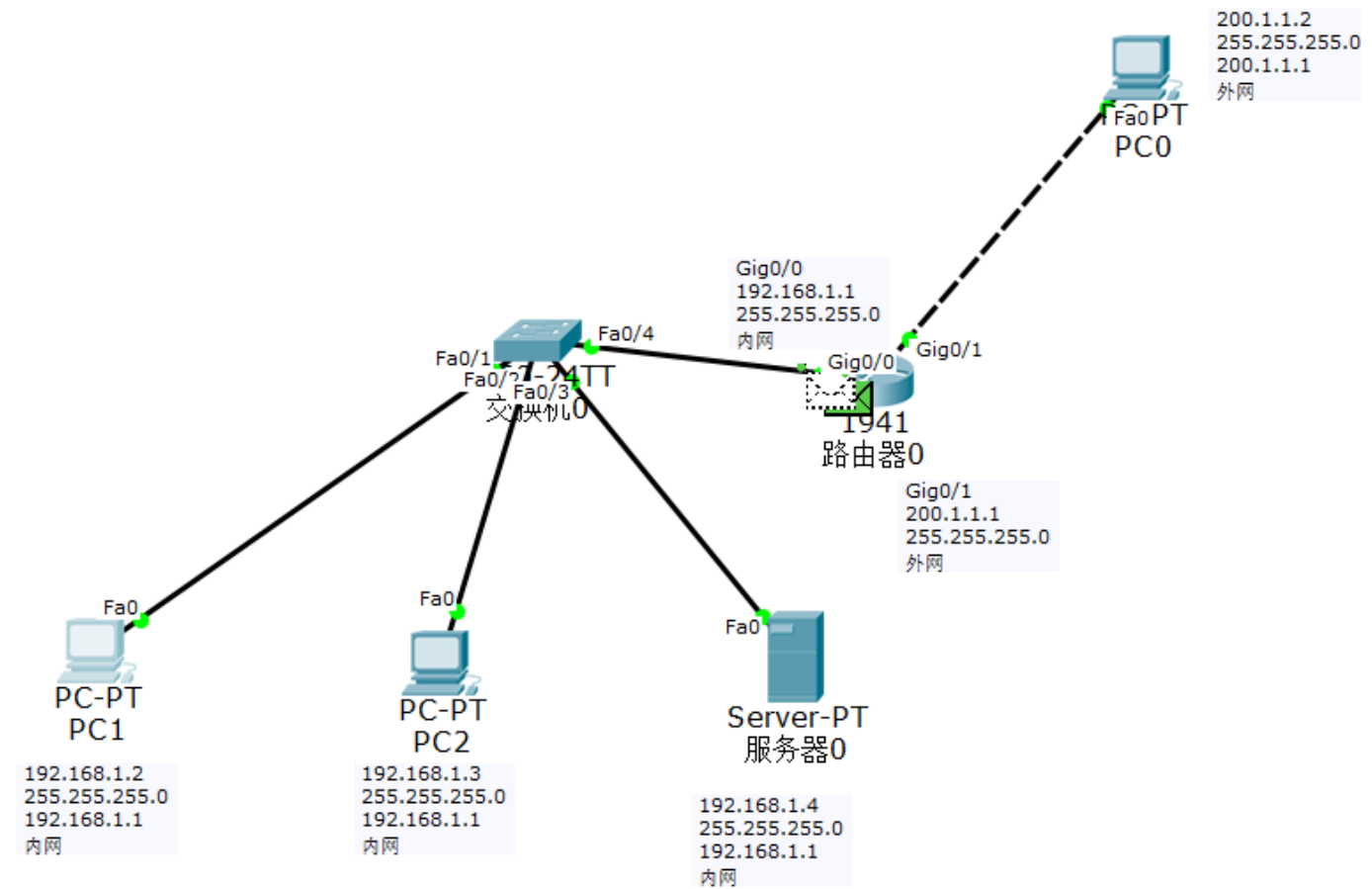
- 然后路由器进行NAT转换，并将其发向外网的PC0



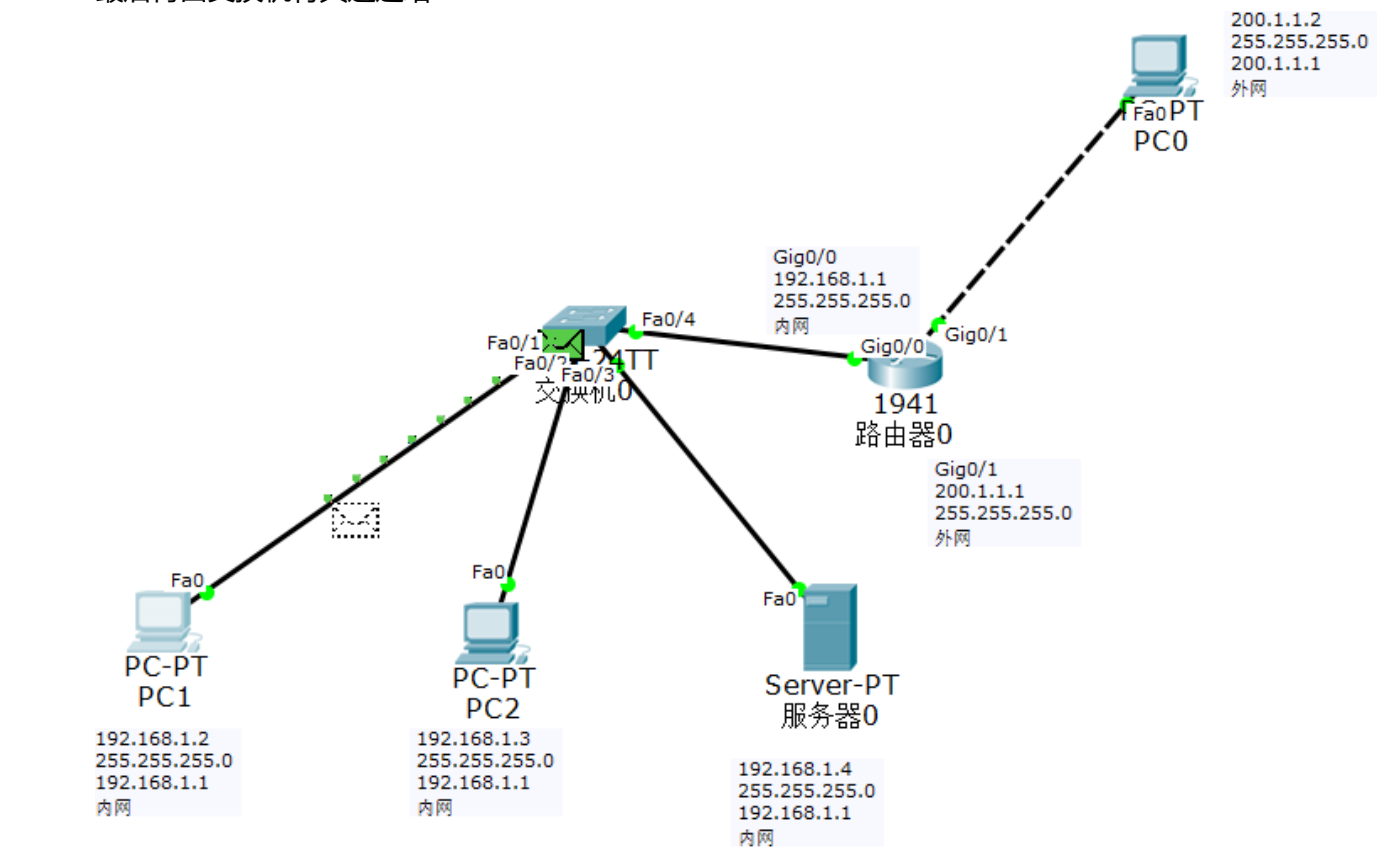
- 随后就是反过程，由外网的PC0将数据报发向路由器



- 再由路由器做NAT转换，将其发向内网的交换机

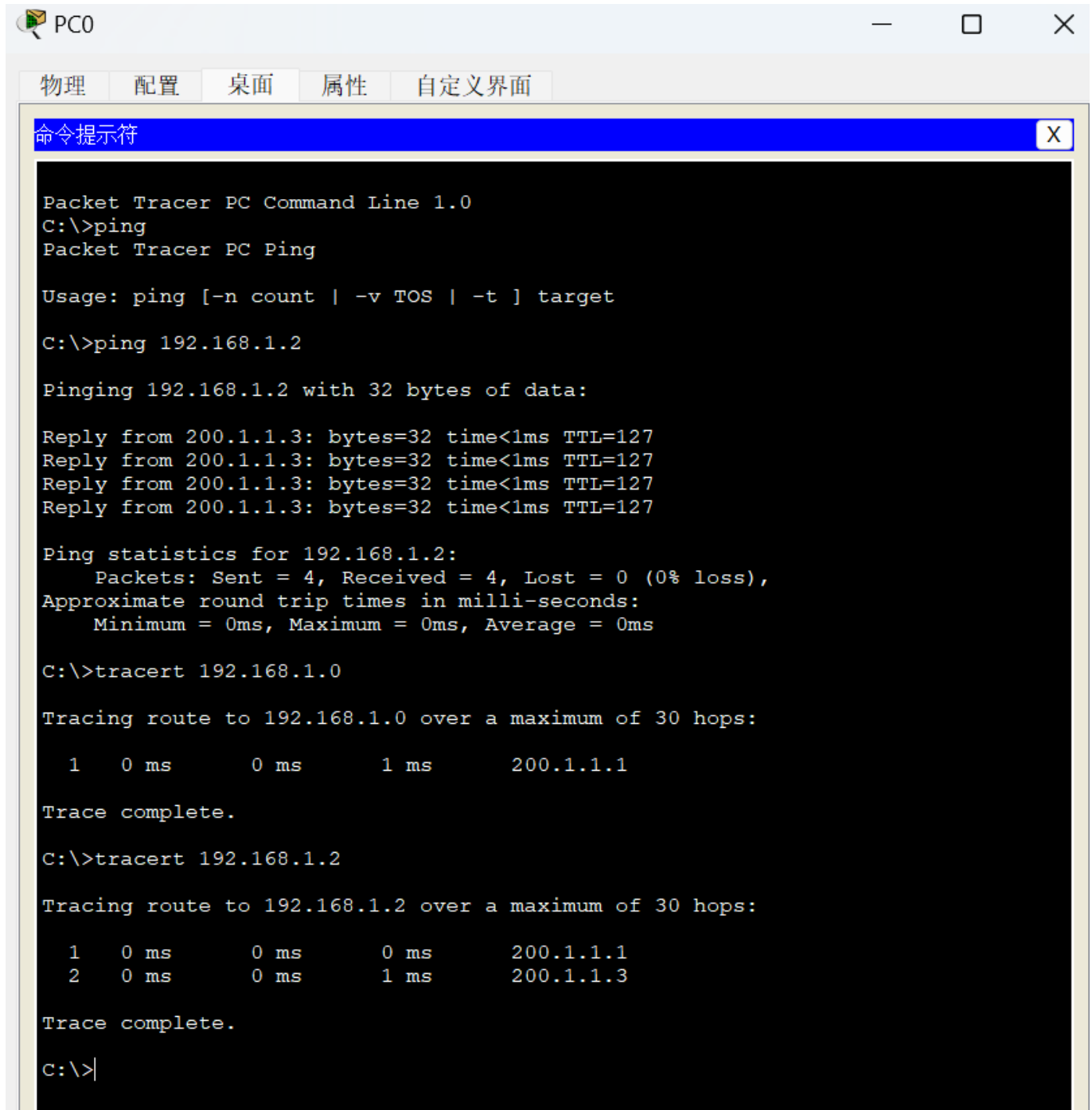


- 最后再由交换机将其返还给PC1



外网到内网

使用 PC0 去 ping PC1，并使用tracert命令查看过程，如下图所示：



```
PC0
物理 配置 桌面 属性 自定义界面
命令提示符 X
Packet Tracer PC Command Line 1.0
C:\>ping
Packet Tracer PC Ping
Usage: ping [-n count | -v TOS | -t ] target
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
C:\>tracert 192.168.1.0
Tracing route to 192.168.1.0 over a maximum of 30 hops:
  1    0 ms      0 ms      1 ms      200.1.1.1
Trace complete.
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      1 ms      200.1.1.3
Trace complete.
C:\>|
```

使用Web服务如下图所示：



还可以查看其中的图片如下：



四、遇到的问题

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，发现还需要为其手动设置静态NAT连接关系。

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就成功了。

五、总结与感悟

通过本次实验，我深入学习了路由器的NAT（网络地址转换）配置过程，并成功组建了一个由NAT连接的内网和外网环境。在配置过程中，我不仅设置了基本的NAT规则以允许内部网络用户通过单一的公共IP地址访问互联网，还特别为内部网络中的Web服务器配置了端口转发规则，使得外部主机能够顺利访问Web服务。此外，通过对网络连通性的测试以及对IP数据报传递过程的观察，我更加直观地理解了NAT的工作机制及其在网络通信中扮演的重要角色，包括它如何有效隐藏内部网络结构、增强网络安全，以及提高公共IP地址的使用效率。本实验为我提供了宝贵的实践经验，加深了对网络协议和数据传输原理的理解。