

执行指令如下图所示

```

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)#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

```

(2) 指定 nat 使用的全局 ip 地址范围

设置地址池 myNATPool，起始地址为 202.113.25.1，结束地址为 202.113.25.10，掩码为 255.255.255.0

```

Router(config)#
Router(config)#ip nat pool myNATPool 202.113.25.1 202.113.25.10 netmask 255.255.255.0
Router(config)#

```

(3) 设置内部网络使用的 ip 地址范围

使用标准访问控制列表来控制内部网络访问的 ip 地址，定义编号为 6 的访问控制列表，允许从 10.0.0.0 开始的 ip 地址进行 NAT 转换

```

Router(config)#
Router(config)#access-list 6 permit 10.0.0.0 0.255.255.255
Router(config)#

```

(4) 将使用的地址池与访问控制列表相关联

```

Router(config)#
Router(config)#ip nat inside source list 6 pool myNATPool overload
Router(config)#

```

(5) 指定连接外部网络和内部网络的接口，将 gig0/0 设置为内部接口，将 gig0/1 设置为外部接口

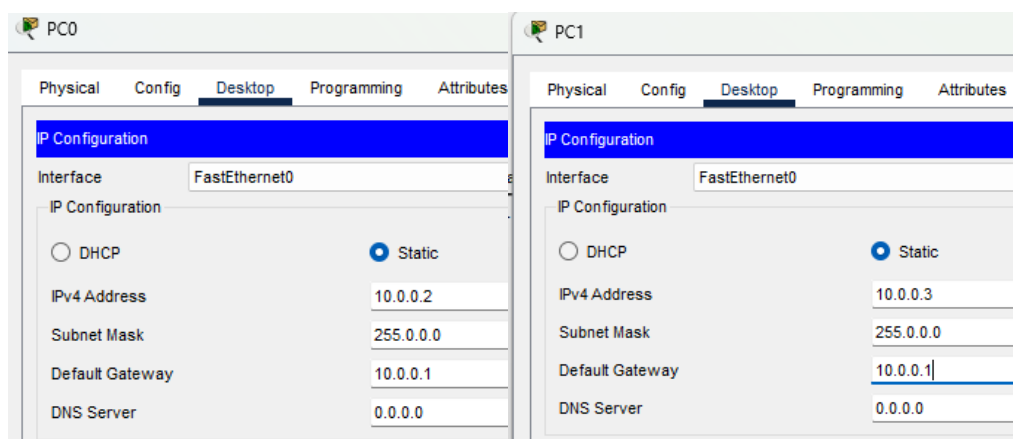
```

Router(config)#
Router(config)#interface gig0/0
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)#

```

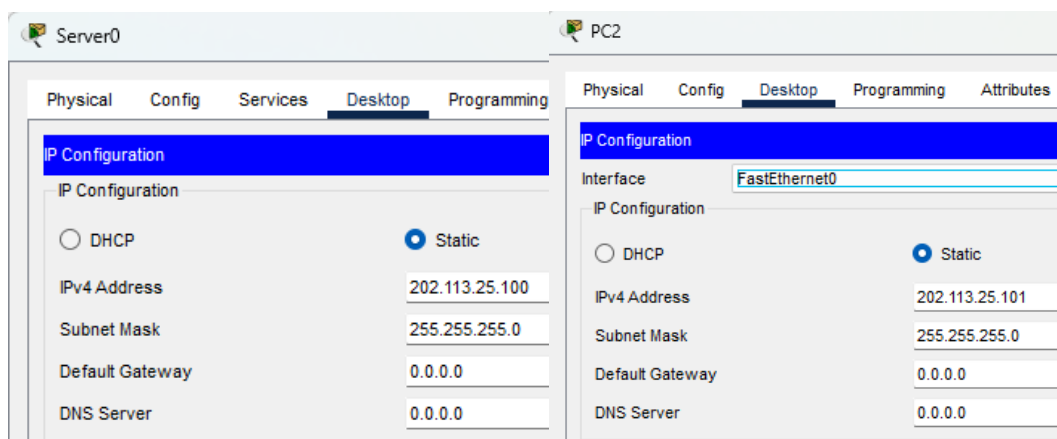
3. 配置内网主机 IP 地址

	IP 地址	子网掩码	默认网关
主机 A	10.0.0.2	255.0.0.0	10.0.0.1
主机 B	10.0.0.3	255.0.0.0	10.0.0.1



4. 配置外网主机 IP 地址

	IP 地址	子网掩码
WEB 服务器	202.113.25.100	255.255.255.0
主机 C	202.113.25.101	255.255.255.0



5. 测试网络连通性

使用主机 A ping WEB 服务器，并使用 tracert 查看发送数据报经过的路径。

通过下图可以看出，数据包首先被主机 A 发至默认网关 10.0.0.1，然后被路由器转发至目标服务器。

在使用 ping 命令时，第一个数据包丢失原因分析：第一次访问时，主机 A 需要通过 ARP 获取路由器接口 10.0.0.1 的 MAC 地址，所以第一次数据包未到达服务器，后续数据包成功到达服务器。

```

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

C:\>tracert 202.113.25.100

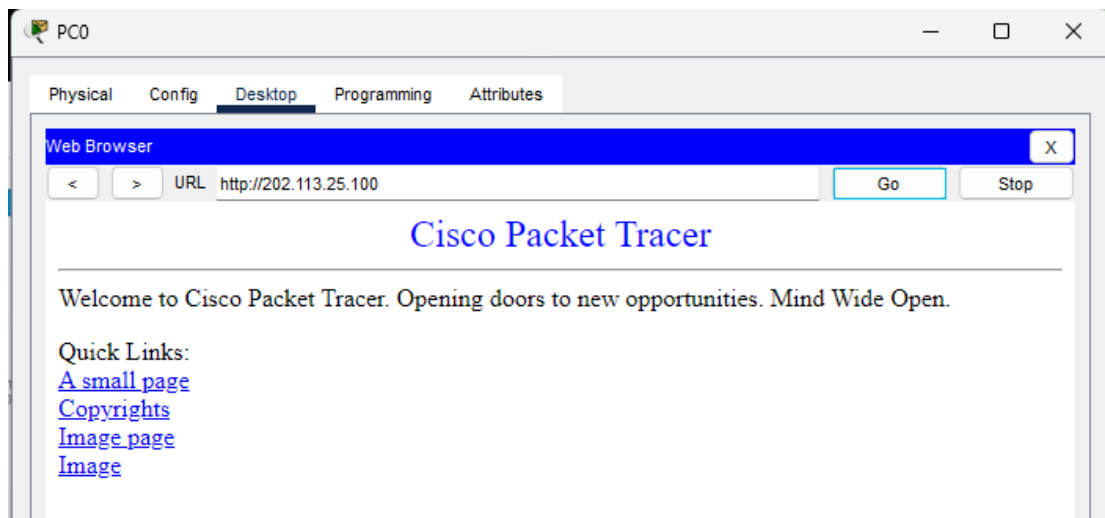
Tracing route to 202.113.25.100 over a maximum of 30 hops:

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

Trace complete.

```

6. 使用内部主机浏览 WEB 服务器的 web 页面



7. 查看 nat 对 tcp 报文的转换情况

(1) 使用 show ip nat statistics 命令监控 NAT 统计信息

```

Router#show ip nat statistics
Total translations: 10 (0 static, 10 dynamic, 10 extended)
Outside Interfaces: GigabitEthernet0/1
Inside Interfaces: GigabitEthernet0/0
Hits: 125 Misses: 17
Expired translations: 7
Dynamic mappings:
-- Inside Source
access-list 6 pool myNATPool refCount 10
 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

```

(2) 使用 show ip nat translations 命令查看 nat 地址转换列表

```

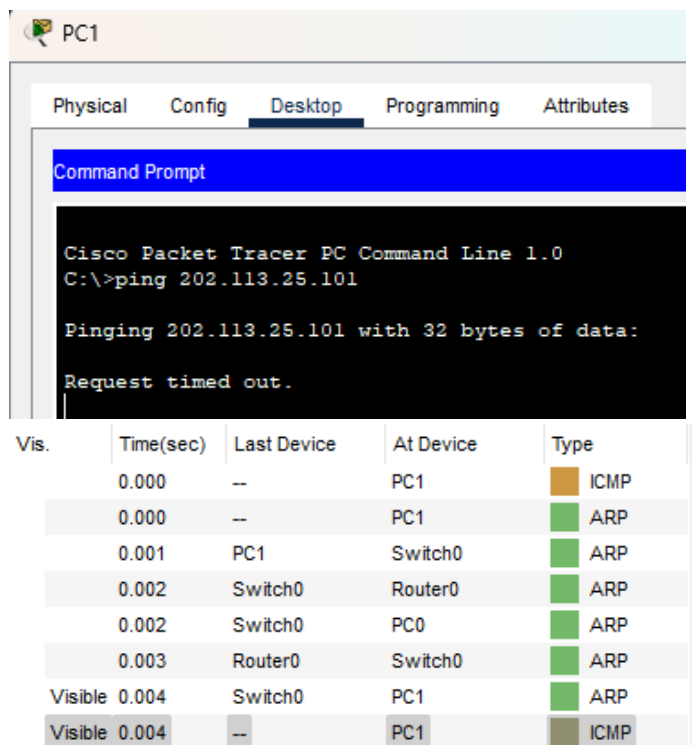
Router#show ip nat translations
Pro Inside global      Inside local      Outside local      Outside global
tcp 202.113.25.1:1025  10.0.0.2:1025     202.113.25.100:80 202.113.25.100:80
tcp 202.113.25.1:1026  10.0.0.2:1026     202.113.25.100:80 202.113.25.100:80
tcp 202.113.25.1:1027  10.0.0.2:1027   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

```

8. 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

主机 B ping 主机 C

- (1) 第一次报文超时，查看仿真，发现第一次主机 B 获取到了 Router0 的 MAC 地址



PC1

Physical Config Desktop Programming Attributes

Command Prompt

```

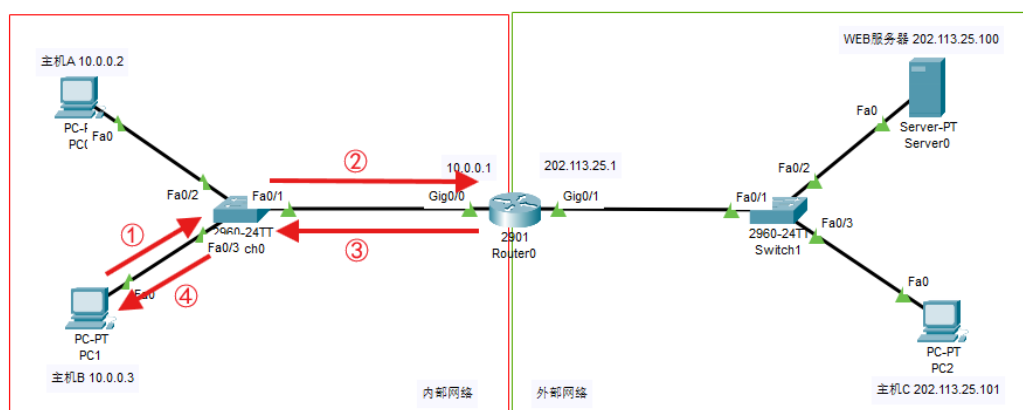
Cisco Packet Tracer PC Command Line 1.0
C:\>ping 202.113.25.101

Pinging 202.113.25.101 with 32 bytes of data:

Request timed out.

```

Vis.	Time(sec)	Last Device	At Device	Type
	0.000	--	PC1	ICMP
	0.000	--	PC1	ARP
	0.001	PC1	Switch0	ARP
	0.002	Switch0	Router0	ARP
	0.002	Switch0	PC0	ARP
	0.003	Router0	Switch0	ARP
Visible	0.004	Switch0	PC1	ARP
Visible	0.004	--	PC1	ICMP



(2) 第二次收到回复，查看仿真

```
C:\>ping 202.113.25.101

Pinging 202.113.25.101 with 32 bytes of data:

Request timed out.
Reply from 202.113.25.101: bytes=32 time=8ms TTL=127
```

6.005	--	PC1	ICMP
6.006	PC1	Switch0	ICMP
6.007	Switch0	Router0	ICMP
6.008	Router0	Switch1	ICMP
6.009	Switch1	PC2	ICMP
6.010	PC2	Switch1	ICMP
6.011	Switch1	Router0	ICMP
6.012	Router0	Switch0	ICMP
6.013	Switch0	PC1	ICMP

分析具体数据包

- ① 主机 B 打包数据包，源 IP 地址为主机 B 的 IP 地址 10.0.0.3，目的 IP 地址为主机 C 的 IP 地址 202.113.25.101

PDU Information at Device: PC1

OSI Model Outbound PDU Details

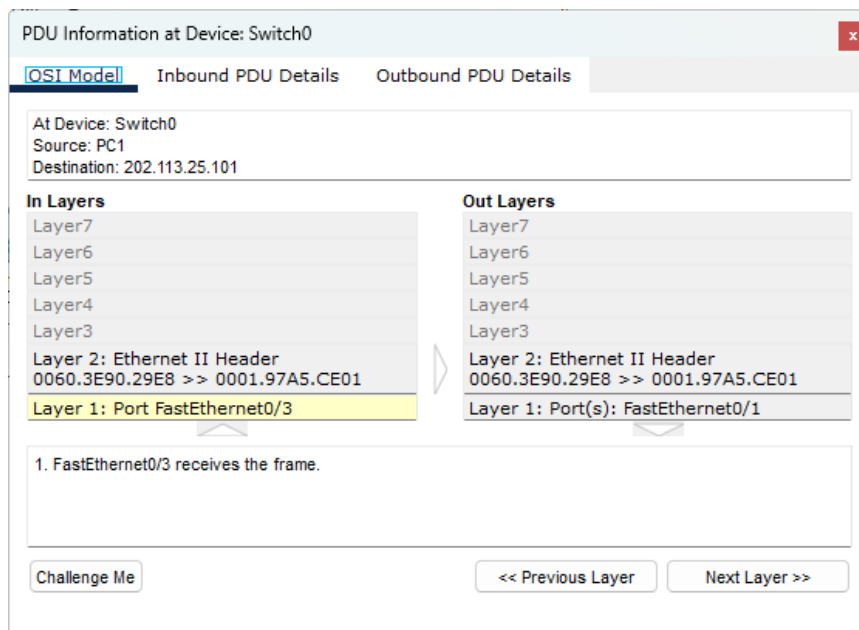
At Device: PC1
Source: PC1
Destination: 202.113.25.101

In Layers	Out Layers
Layer7	Layer7
Layer6	Layer6
Layer5	Layer5
Layer4	Layer4
Layer3	Layer 3: IP Header Src. IP: 10.0.0.3, Dest. IP: 202.113.25.101 ICMP Message Type: 8
Layer2	Layer 2: Ethernet II Header 0060.3E90.29E8 >> 0001.97A5.CE01
Layer1	Layer 1: Port(s): FastEthernet0

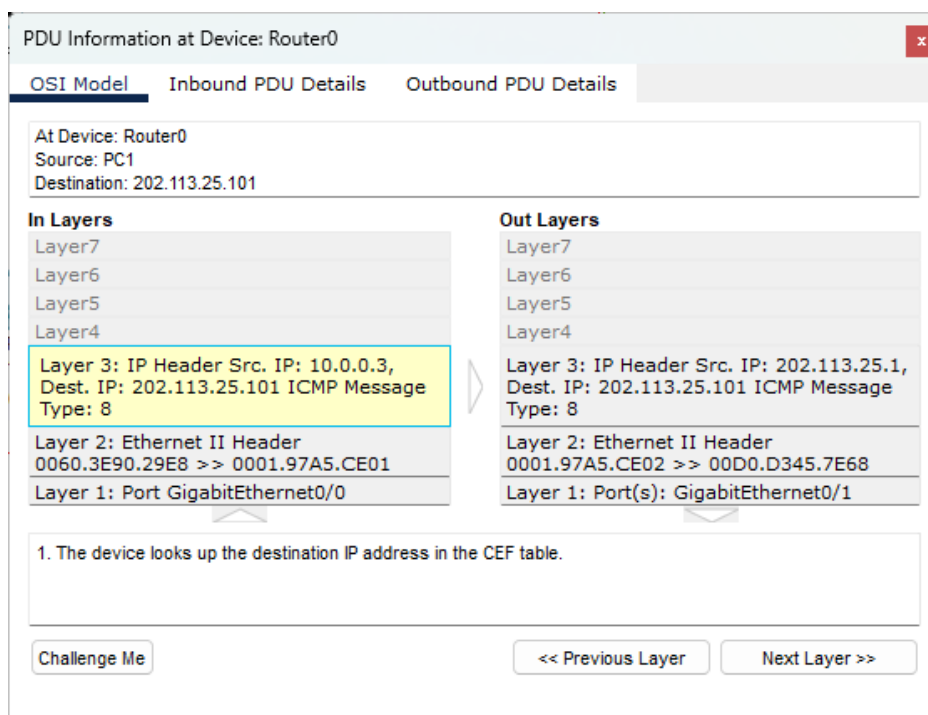
1. The Ping process starts the next ping request.
2. The Ping process creates an ICMP Echo Request message and sends it to the lower process.
3. The source IP address is not specified. The device sets it to the port's IP address.
4. The destination IP address 202.113.25.101 is not in the same subnet and is not the broadcast address.
5. The default gateway is set. The device sets the next-hop to default gateway.

Challenge Me << Previous Layer Next Layer >>

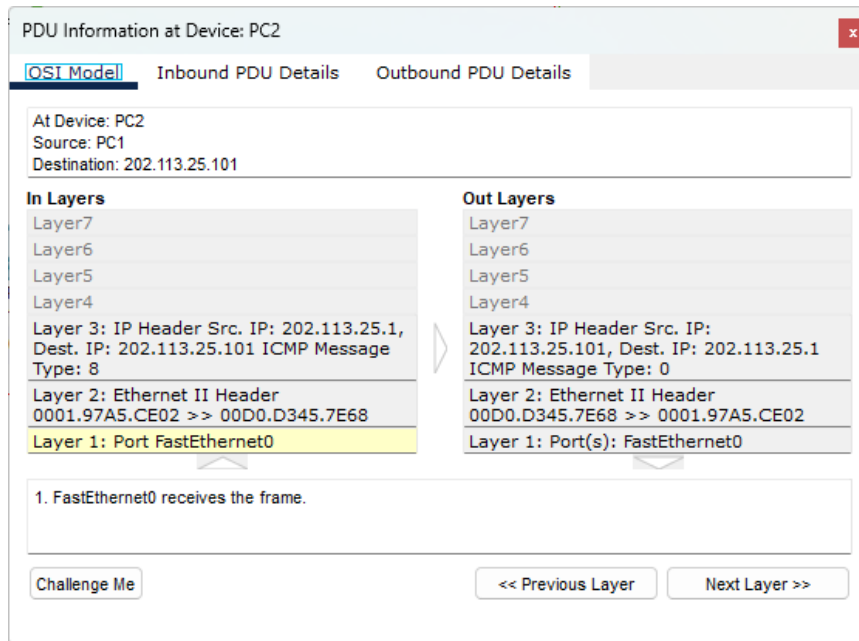
- ② Switch0 收到数据包，进行转发，从主机 B 发至路由器



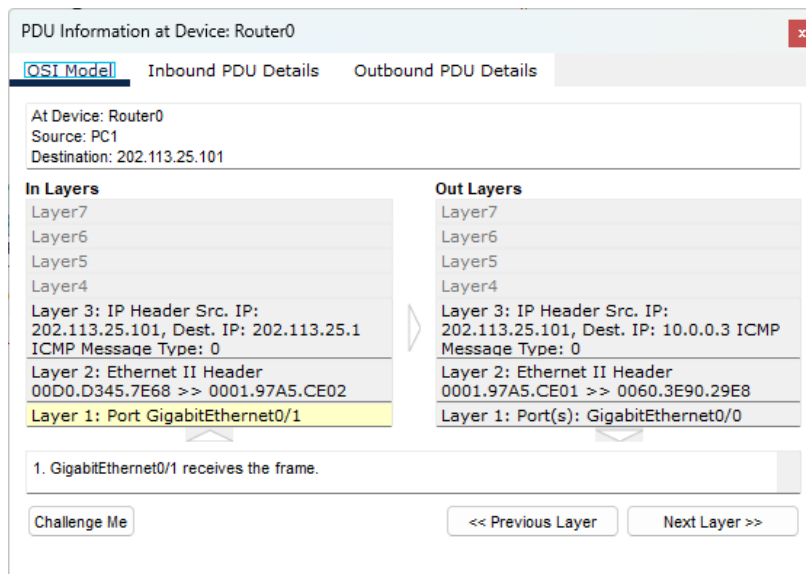
- ③ 路由器收到数据包后，可以看到，源 IP 地址由 10.0.0.3（内网地址）转换为 202.113.25.1（外网地址），目的 IP 地址不变，依旧为主机 C 的 IP 地址



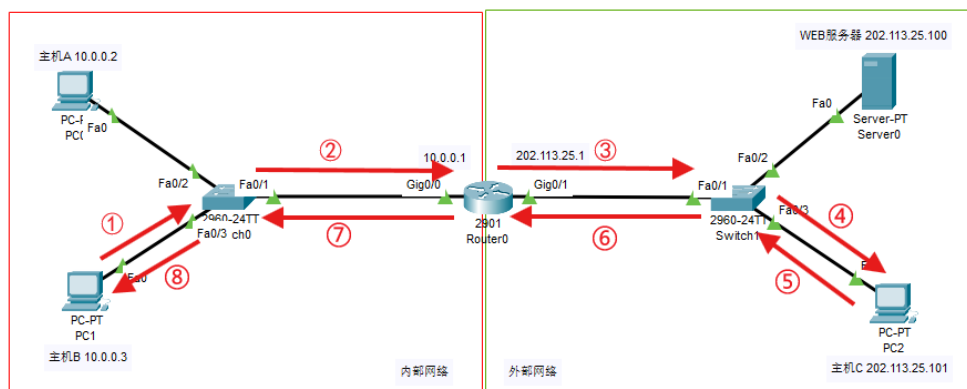
- ④ 而后经过 switch1，数据包到达主机 C，主机 C 设置回复报文。
可以看到，源 IP 地址为主机 C 的 IP 地址 202.113.25.101，而目的 IP 地址为外网地址 202.113.25.1



- ⑤ 数据包经过 switch1 到达 router0，此时目的 IP 由外网地址 202.113.25.1 转换为内网地址 10.0.0.3，源 IP 地址不变

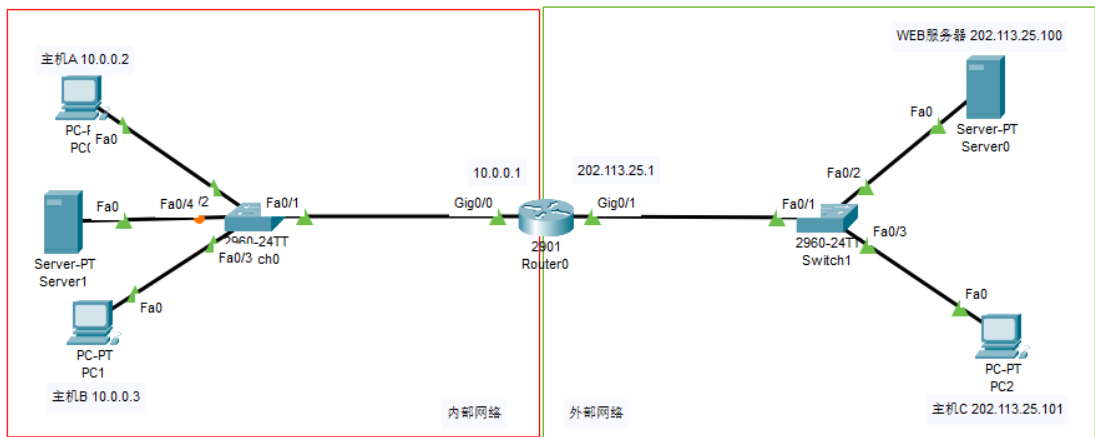


- ⑥ 数据包经 switch0 到达主机 B，完成一次请求响应

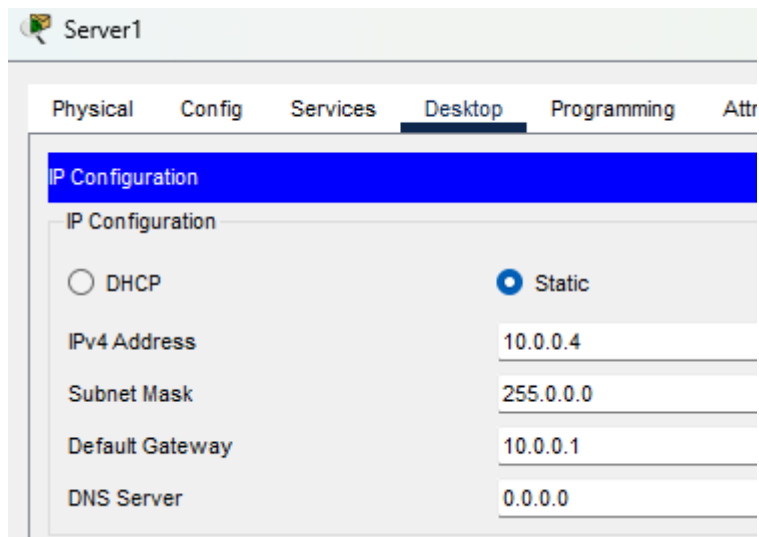


(二) 将内部网络中放置一台 Web 服务器，请设置 NAT 服务器，使外部主机能够顺利使用该 Web 服务

1. 拓扑结构如下图所示，路由器 Router0 完成 NAT 地址转换功能，路由器左边红色框为内部网络，路由器右边绿色框为外部网络



2. 配置内网服务器 IP 地址，子网掩码，默认网关

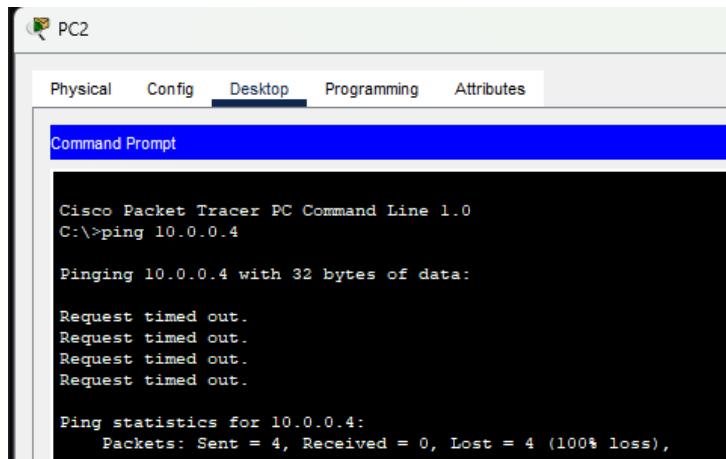


3. 利用静态 NAT 映射，将内网服务器 10.0.0.4 映射到外网网段 202.113.25.2

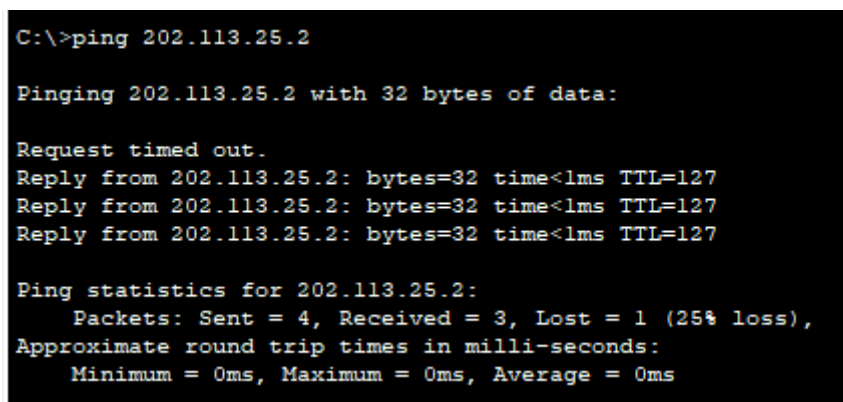
```
Router#config terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#ip nat inside source static 10.0.0.4 202.113.25.2
Router(config)#exit
Router#
%SYS-5-CONFIG_I: Configured from console by console
```

4. 测试网络连通性

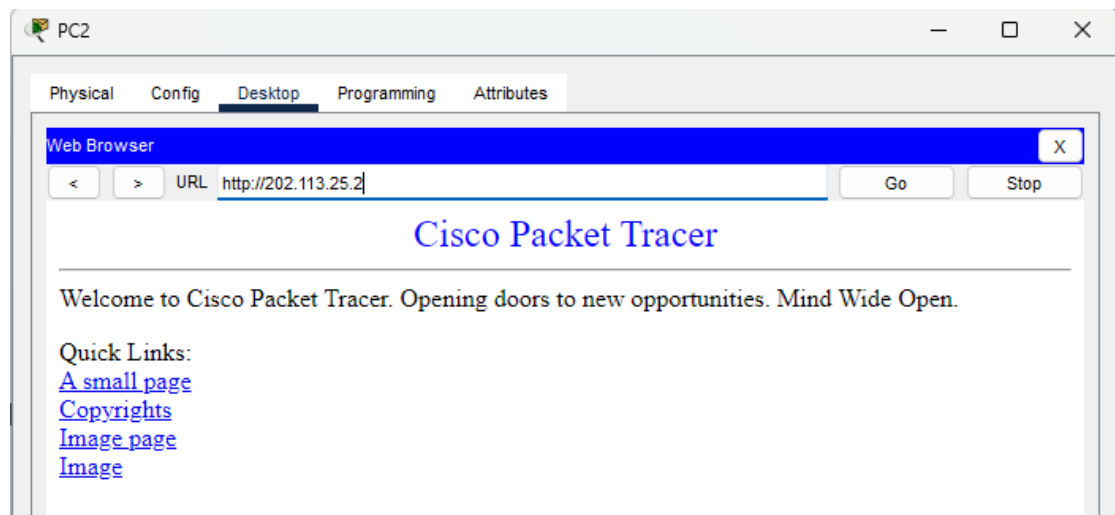
使用外网主机 C ping 内网服务器，运行结果如下图所示，可以看到四个数据包均丢失，这是因为外网主机无法访问内网。



但是我们已经将内网的服务器 ip 地址静态映射到了外网的 202.113.25.2，所以可以通过访问外网这个 ip 实现访问内网服务器



5. 使用外网主机 C 浏览内网服务器的 web 页面



6. 查看 nat 地址转换列表，可以看到实现了内网 10.0.0.4 到外网 202.113.25.2 的映射

```

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     202.113.25.100:80 202.113.25.100:80
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  202.113.25.2:80     10.0.0.4:80       202.113.25.101:1025 202.113.25.101:1025
tcp  202.113.25.2:80     10.0.0.4:80       202.113.25.101:1026 202.113.25.101:1026
tcp  202.113.25.2:80     10.0.0.4:80       202.113.25.101:1027 202.113.25.101:1027
tcp  202.113.25.2:80     10.0.0.4:80       202.113.25.101:1028 202.113.25.101:1028
tcp  202.113.25.2:80     10.0.0.4:80       202.113.25.101:1029 202.113.25.101:1029
tcp  202.113.25.2:80     10.0.0.4:80       202.113.25.101:1030 202.113.25.101:1030
tcp  202.113.25.2:80     10.0.0.4:80       202.113.25.101:1031 202.113.25.101:1031
tcp  202.113.25.2:80     10.0.0.4:80       202.113.25.101:1032 202.113.25.101:1032
tcp  202.113.25.2:80     10.0.0.4:80       202.113.25.101:1033 202.113.25.101:1033
tcp  202.113.25.2:80     10.0.0.4:80       202.113.25.101:1034 202.113.25.101:1034
Router#

```

三、实验总结

在家庭或企业网络中，多个设备通常共享一个公有 IP 地址进行外网通信。这些设备各自有私有 IP 地址。当这些设备需要访问互联网时，它们的数据包首先发送到局域网中的 NAT 路由器。

NAT 路由器接收到来自内部网络的数据包后，会修改这些数据包。它将数据包的源 IP 地址（私有 IP）更改为路由器的公有 IP 地址。同时，NAT 路由器会为每个连接分配一个唯一的端口号，以区分来自同一公有 IP 的多个内部设备的流量。

修改后的数据包通过路由器的公有 IP 地址发送到互联网上。当外部服务器响应请求时，它会将响应发送回路路由器的公有 IP 地址。路由器收到响应数据包后，会根据之前分配的端口号确定响应应该发送到内部网络中的哪个设备。

路由器再次修改数据包，这次将目的 IP 地址从公有 IP 更改为相应的私有 IP 地址。然后将数据包转发到内部网络中的对应设备。

通过这种方式，NAT 允许多个设备共享单个公有 IP 地址，大大节省了 IP 地址资源。

动态 NAT 允许一组内部本地地址映射到一组全局（公共）地址。当内部主机发起对外连接时，路由器会临时分配一个可用的公共 IP 地址给该连接，并在 NAT 表中记录下这个映射关系。一旦连接关闭，这个公共 IP 地址就可以被释放并重新分配给其他内部主机使用。

静态 NAT 是将内部网络中的一个特定私有 IP 地址永久性地映射到一个唯一的公共 IP 地址。这种映射是一对一的关系，通常用于让外部用户能够直接访问内部网络中的服务器等服务。