

# 计算机网络安全技术·实验2报告

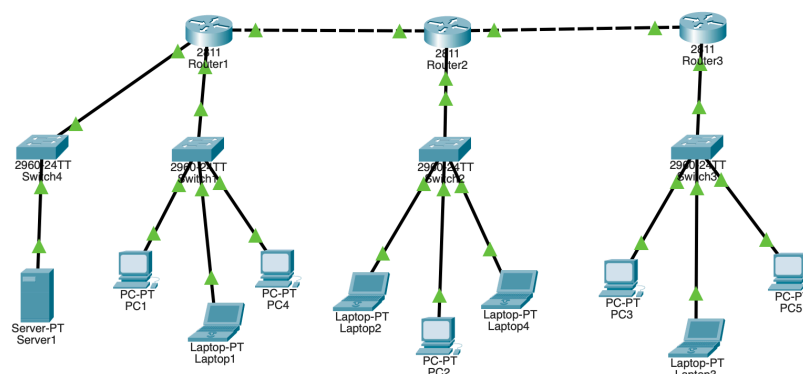
计01 容逸朗 2020010869

## 实验内容

### 任务 6：“三权”间的权限控制（6'）

条件 4 提到，仅有 PC1 可以和 Server1 通信，其余设备都不能和 Server1 通信。由于同一个网域内的设备会通过交换机转发到相邻的所有设备上，因此需要为 Server1 配置一个新的网域：

为此我增加了新的交换机，此交换机和 Router1 相连，新的拓扑如下：



其中，Server1 的新 IP 为 192.168.4.2。

同时，为了实现的可扩展性，我采用了扩展的 ACL，具体规则如下所示：

### 路由器配置

#### Router1

元老院网域：

```
1 # 外部人员只能和元老院联络人通信
2 access-list 101 permit ip 192.168.2.0 0.0.0.255 host 192.168.1.4
3 access-list 101 permit ip 192.168.3.0 0.0.0.255 host 192.168.1.4
4 # 外部联络人可以和元老院的所有成员通信
5 access-list 101 permit ip host 192.168.2.2 192.168.1.0 0.0.0.255
6 access-list 101 permit ip host 192.168.3.3 192.168.1.0 0.0.0.255
7 # 权力机构领导人互通
8 access-list 101 permit ip host 192.168.2.3 host 192.168.1.2
9 access-list 101 permit ip host 192.168.3.2 host 192.168.1.2
10 # 允许 PC1 和 Server1 通信
11 access-list 101 permit ip host 192.168.4.2 host 192.168.1.2
12 # 配置元老院网关 ACL
13 interface f0/0
14 ip access-group 101 out
```

Server1 网域：

```
1 # 允许 PC1 和 Server1 通信
2 access-list 102 permit ip host 192.168.1.2 host 192.168.4.2
3 access-list 102 permit ip host 192.168.4.2 host 192.168.1.2
4 interface f1/0
5 ip access-group 102 in
6 ip access-group 102 out
```

## Router2

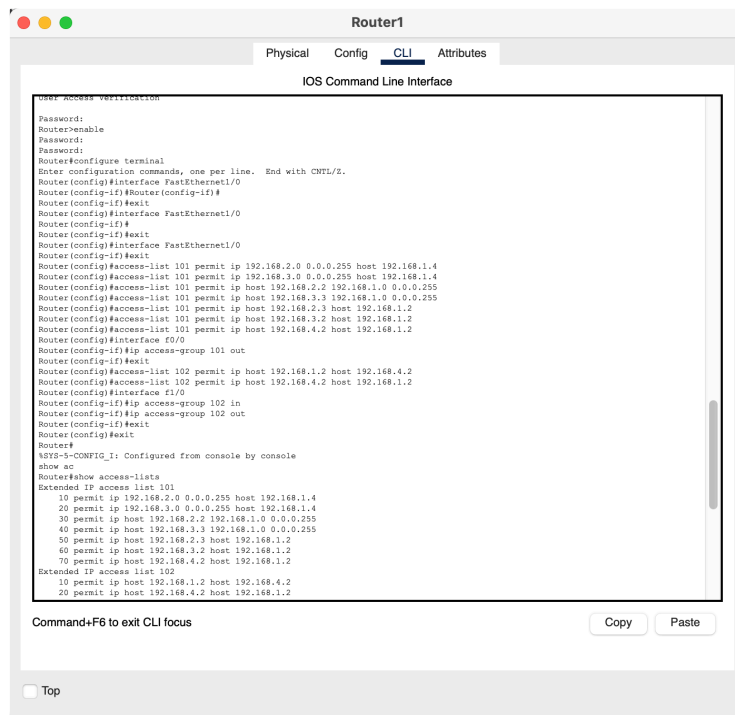
```
1 # 外部人员只能和执政官首府联络人通信
2 access-list 101 permit ip 192.168.1.0 0.0.0.255 host 192.168.2.2
3 access-list 101 permit ip 192.168.3.0 0.0.0.255 host 192.168.2.2
4 # 外部联络人可以和执政官首府的所有成员通信
5 access-list 101 permit ip host 192.168.1.4 192.168.2.0 0.0.0.255
6 access-list 101 permit ip host 192.168.3.3 192.168.2.0 0.0.0.255
7 # 权力机构领导人互通
8 access-list 101 permit ip host 192.168.1.2 host 192.168.2.3
9 access-list 101 permit ip host 192.168.3.2 host 192.168.2.3
10 # 配置执政官首府网关 ACL
11 interface f1/0
12 ip access-group 101 out
```

## Router3

```
1 # 外部人员只能和部族会议所联络人通信
2 access-list 101 permit ip 192.168.1.0 0.0.0.255 host 192.168.3.3
3 access-list 101 permit ip 192.168.2.0 0.0.0.255 host 192.168.3.3
4 # 外部联络人可以和部族会议所的所有成员通信
5 access-list 101 permit ip host 192.168.1.4 192.168.3.0 0.0.0.255
6 access-list 101 permit ip host 192.168.2.2 192.168.3.0 0.0.0.255
7 # 权力机构领导人互通
8 access-list 101 permit ip host 192.168.1.2 host 192.168.3.2
9 access-list 101 permit ip host 192.168.2.3 host 192.168.3.2
10 # 配置部族会议所网关 ACL
11 interface f0/1
12 ip access-group 101 out
```

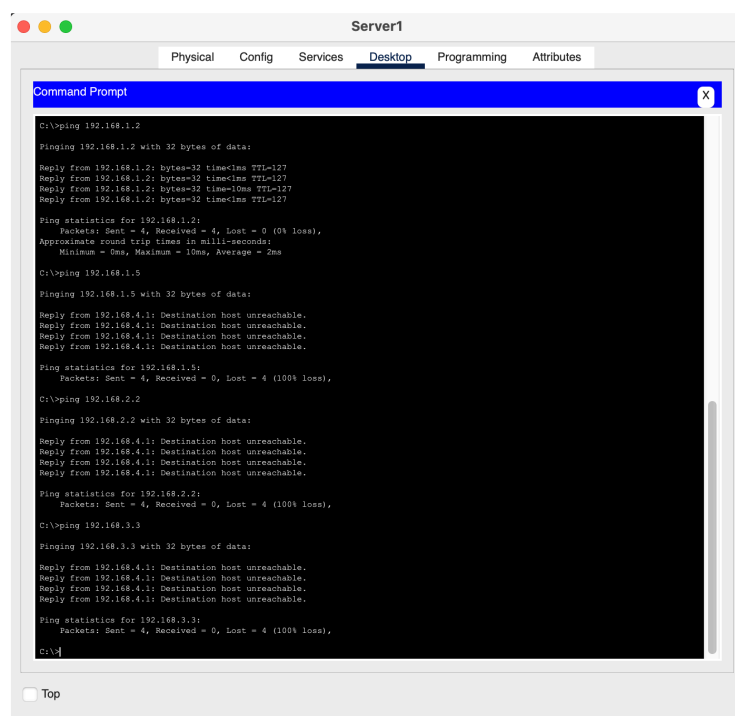
## 实验截图

路由器 ACL 配置



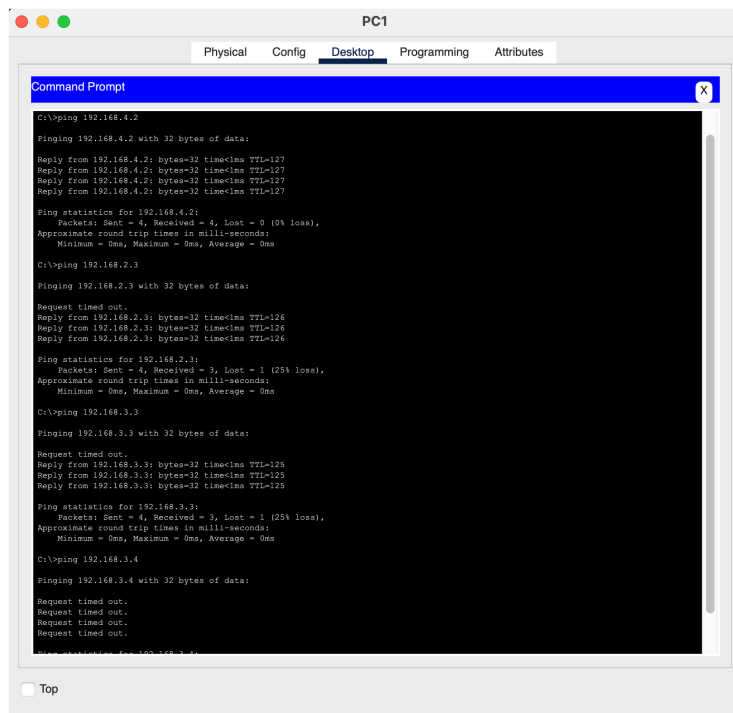
## 机密设备测试（Server1）

由下图可见，Server1 只能和 PC1 通信，和其他设备不能通信，说明配置成功。



## 领导人测试（以 PC1 为例）

元老院领导人 PC1 可以和 Server1、其他机构领导人及各部门联络人通信，但不能和其他机构的内部设备（如 PC5）通信：



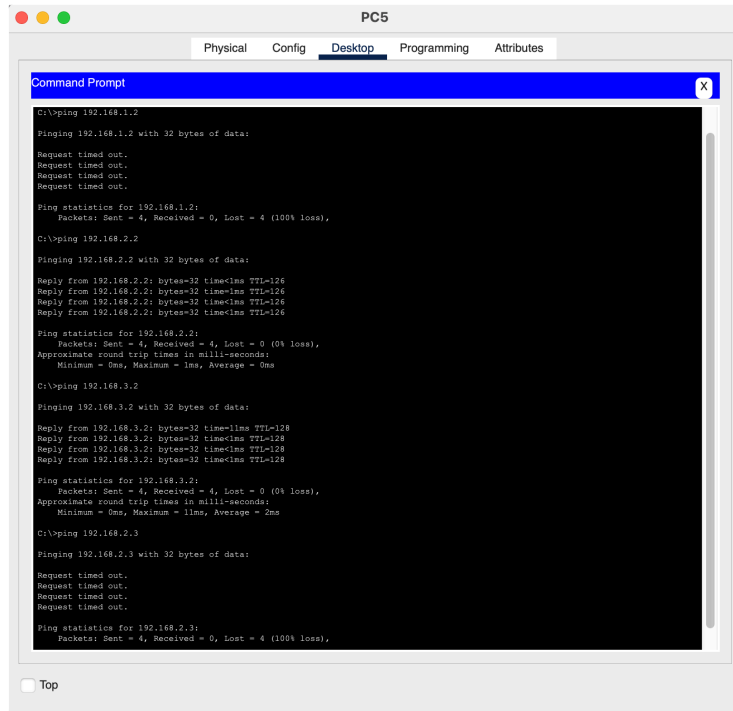
## 联络人测试（以 PC2 为例）

执政官首府联络人 PC2 除了不能和 Server1 通信以外，可以和所有设备（包括领导人、内部设备）通信。



## 其他设备测试（以 PC5 为例）

部族会议所大祭司 C 的设备 PC5 只可以和内网成员或其他机构的联络人通信，除此之外不能和其他人通信。



## 任务 7：凯撒赐予的“最高”权限（4'）

### 思路

由于允许 PC1 向网络内的所有设备进行 ping 测试，因此需要对各个路由器进行特别配置，使得源 IP 为 192.168.1.2 的 ICMP 包可以被转发。

### 路由器配置

#### Router1

允许来自 192.168.0.0/22（包含了 192.168.2.0/24 和 192.168.3.0/24）的 icmp 包访问 192.168.1.2：

```
1 access-list 101 permit icmp 192.168.0.0 0.0.3.255 host 192.168.1.2
2 ip inspect name icmp icmp
3 interface f0/0
4 ip inspect icmp out
```

#### Router2

对于路由器 2 和 3，只需要允许来自 192.168.1.2 的 ICMP 包进入网关即可，因此在 ACL 增加如下语句：

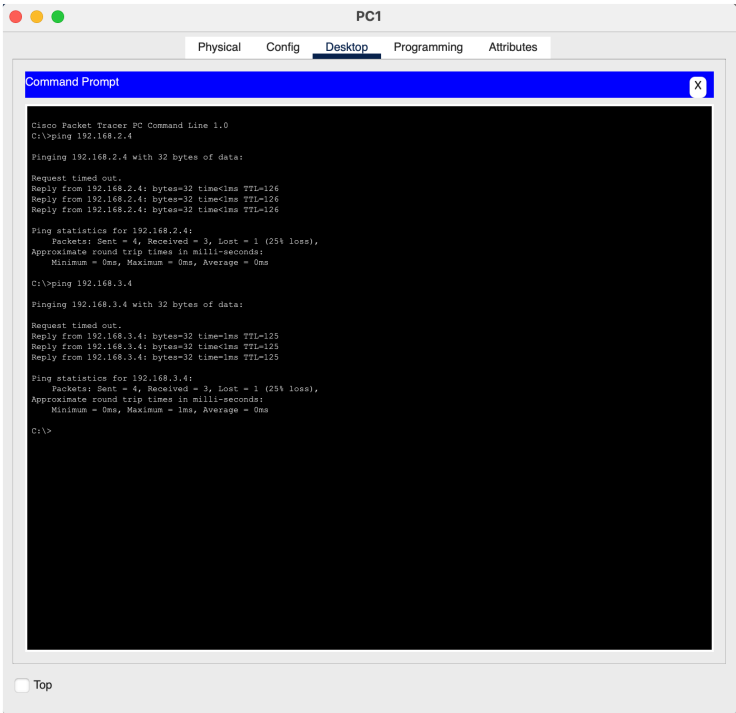
```
1 access-list 101 permit icmp host 192.168.1.2 192.168.2.0 0.0.0.255
2 ip inspect name icmp icmp
3 interface f1/0
4 ip inspect icmp out
```

Router3

```
1 | access-list 101 permit icmp host 192.168.1.2 192.168.3.0 0.0.0.255
2 | ip inspect name icmp icmp
3 | interface f0/1
4 | ip inspect icmp out
```

实验截图

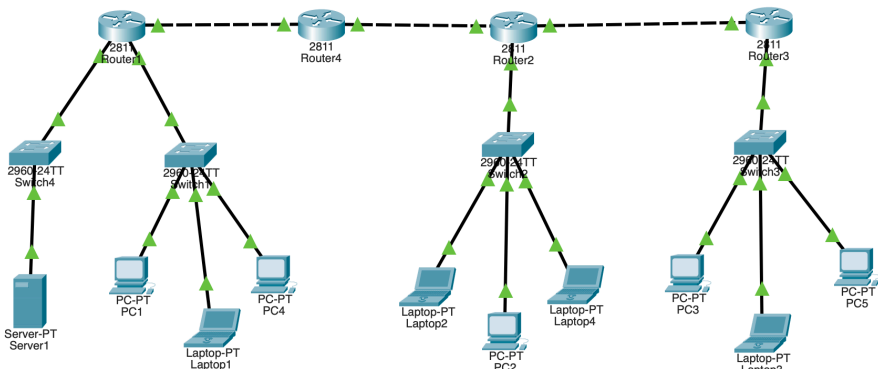
从下图中可知，PC1 可以对网络中的所有设备进行 ping 测试了：



任务 8：新的远征（10'）

网络拓扑

引入 Router4 为公网路由器后，新的拓扑如下：



其中，各路由器设备的新地址如下：

Router	Port	IP	Mask
Router1	2	13.0.0.2	/8
Router4	1	13.0.0.1	/8
Router4	2	23.0.0.1	/8
Router2	1	23.0.0.2	/8

在搬迁之后，使用配置静态路由的方法将无法让各个权力机构正常通信，请简述原因。

- 共和国内部使用内网 IP，除非在公网上能够找到直连线路，否则这些地址（在未经转换的情况下）是无法被公网路由器转发的，因此不能使用静态路由方法。

## 路由配置

### Router 1

对于流量出端口，按要求使用加密算法 3des、哈希算法 md5 及密钥协商算法 DH5：

```
1 crypto isakmp policy 1
2 encryption 3des
3 hash md5
4 authentication pre-share
5 group 5
```

首先预分配一个共享密钥用于身分认证：

```
1 crypto isakmp key mypassword address 23.0.0.2
```

再配置 IPsec 所用的算法策略：

```
1 crypto ipsec transform-set myset esp-3des esp-md5-hmac
```

然后配置 ACL：

```
1 access-list 101 permit ip 192.168.1.0 0.0.0.255 192.168.2.0 0.0.0.255
2 access-list 101 permit ip 192.168.1.0 0.0.0.255 192.168.3.0 0.0.0.255
```

定义 crypto map 策略：

```
1 crypto map mymap 1 ipsec-isakmp
2 set peer 23.0.0.2
3 set transform-set myset
4 match address 101
```

配置流量出口：

```
1 int f0/1
2 crypto map mymap
```

最后加上 RIP 路由配置即可：

```
1 router rip
2 network 192.168.1.0
3 network 192.168.4.0
4 network 13.0.0.0
```

## Router 2

对于二号路由器，也采用同样的方法建立 VPN 即可：

```
1 crypto isakmp policy 1
2 encryption 3des
3 hash md5
4 authentication pre-share
5 group 5
6 exit
7
8 crypto isakmp key mypassword address 13.0.0.2
9 crypto ipsec transform-set myset esp-3des esp-md5-hmac
10 access-list 101 permit ip 192.168.2.0 0.0.0.255 192.168.1.0 0.0.0.255
11 access-list 101 permit ip 192.168.3.0 0.0.0.255 192.168.1.0 0.0.0.255
12 crypto map mymap 1 ipsec-isakmp
13 set peer 13.0.0.2
14 set transform-set myset
15 match address 101
16 exit
17
18 int f0/0
19 crypto map mymap
20 exit
21
22 router rip
23 network 192.168.2.0
24 network 23.0.0.0
```

## Router 4

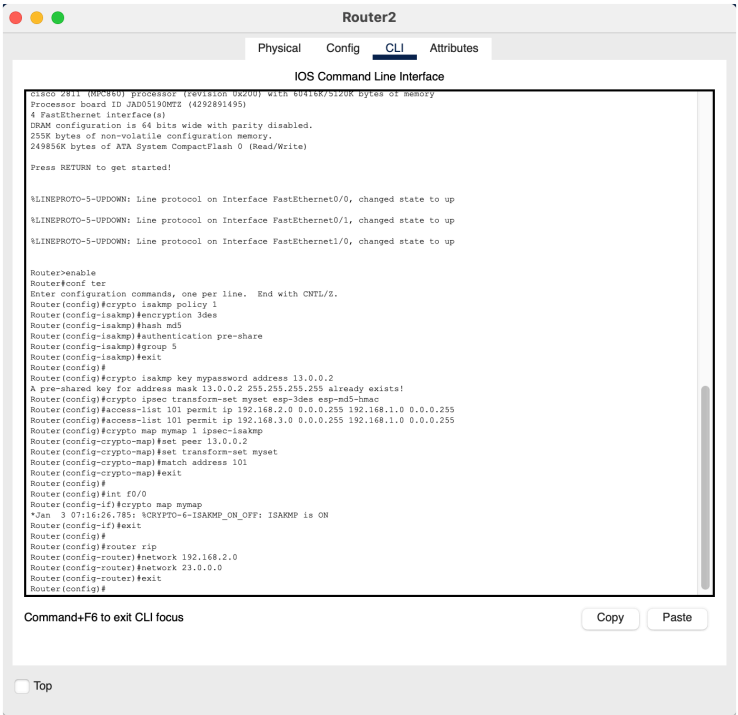
只配置 RIP 协议，模拟公网传输

```
1 router rip
2 network 13.0.0.0
3 network 23.0.0.0
```



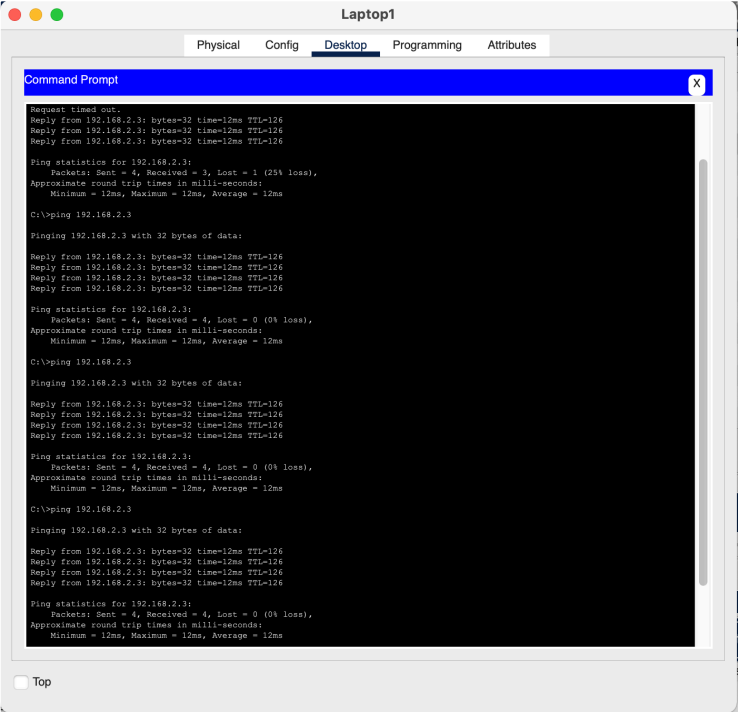
实验截图

路由器配置



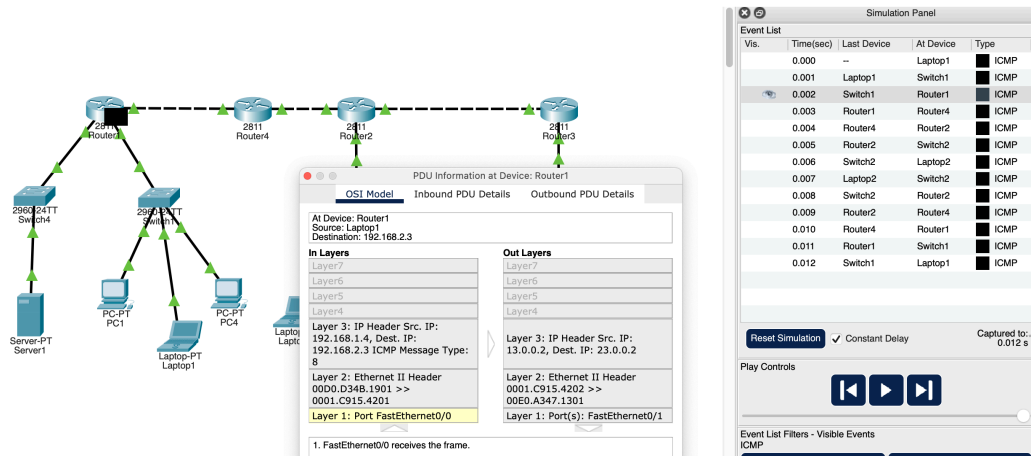
ping 通信测试

从下图可知，Laptop1（192.168.1.4）和 Laptop2（192.168.2.3）已经可以 ping 通了：

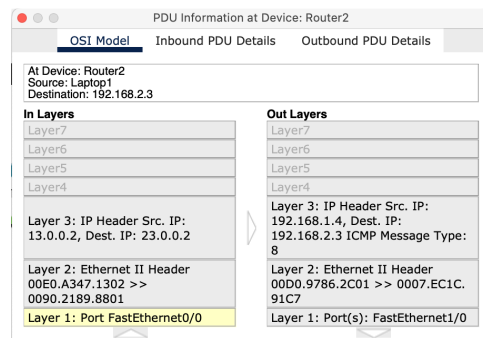


通过仿真抓包分析，如上配置的IPSec VPN使用了传输模式还是隧道模式，为什么？

- 从下图可见，当包经过 Router1 后：
  - 源地址由内网的 192.168.1.4 变为公网的 13.0.0.2（Router1 对应端口地址）
  - 目的地地址由内网 192.168.2.3 变为公网的 23.0.0.2（Router2 对应端口地址）



- 经过 Router2 后，地址又变回原来的内网 IP 了：



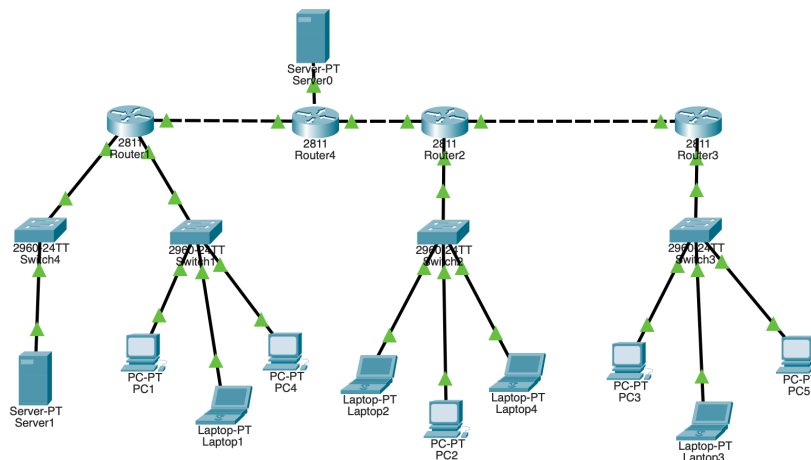
- 这说明我配置的 IPSec VPN 是使用隧道模式的，因为传输模式不会改变数据包的 IP 头。

## Bonus：凯撒的赏赐（3'）

本次实验中，我尝试使用 NAT 更改内网 IP 以获取公网的信息。

### 初始设置

在 Router4 处增加一个 IP 为 34.0.0.2 的 Server，此时拓扑如下：



然后要确定路由器的端口流量方向：

## Router1

```
1 int f0/0
2 ip nat inside
3 int f0/1
4 ip nat outside
5 int f1/0
6 ip nat inside
```

## Router2

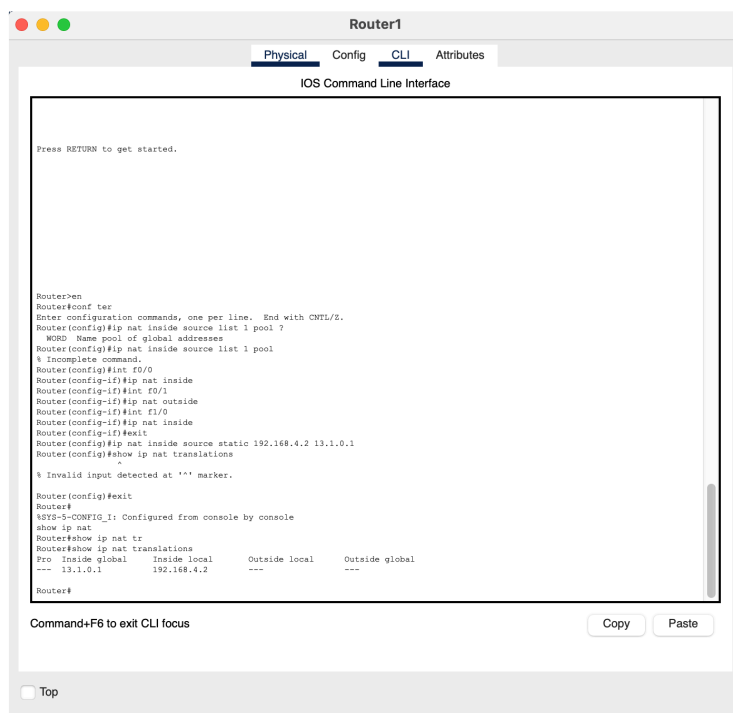
```
1 int f0/0
2 ip nat outside
3 int f0/1
4 ip nat inside
5 int f1/0
6 ip nat inside
```

## 静态转换 (Static Translation)

下面是 Server1 到公网路由器 Router4 的例子，本示例测试了内网到公网的通信：

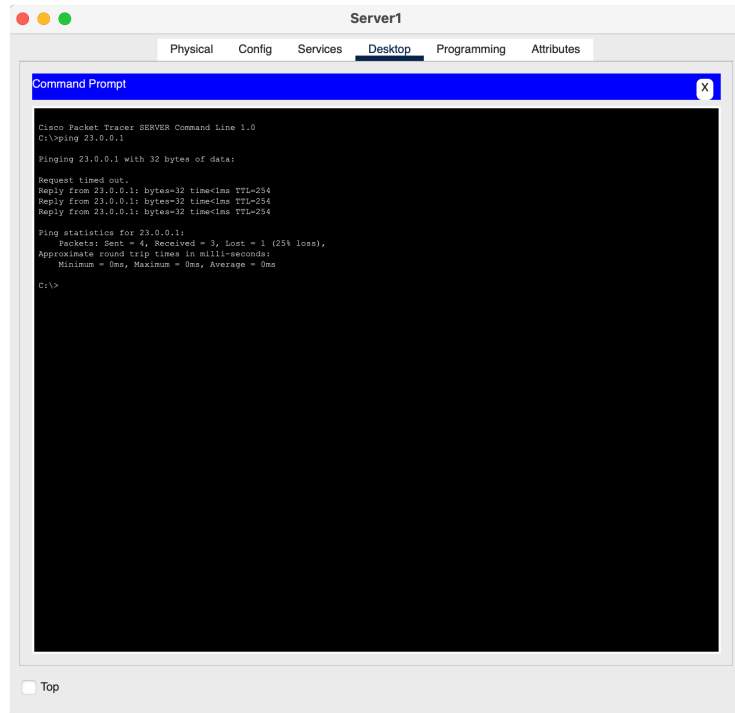
首先在 Router1 作如下改动：

```
1 ip nat inside source static 192.168.4.2 13.1.0.1
```

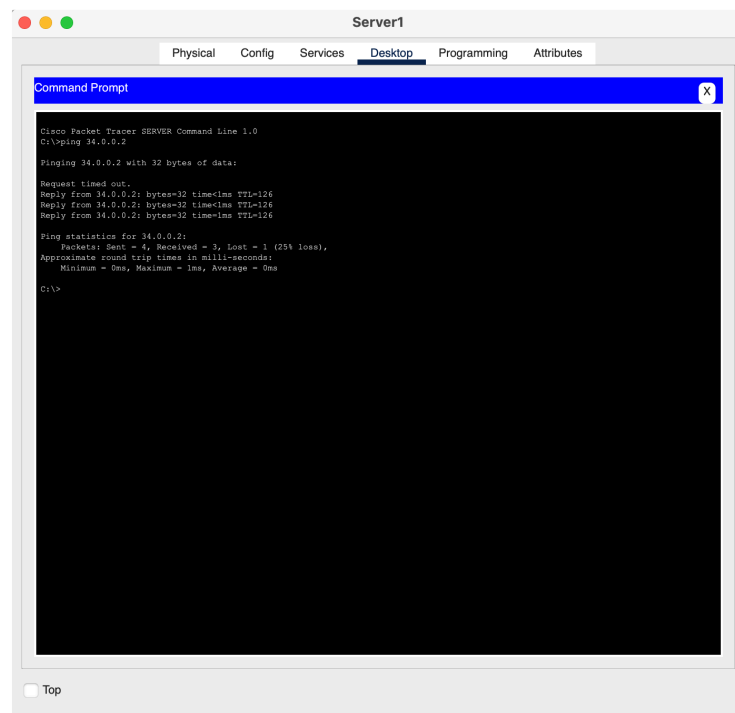


完成配置后，可以看到新的转换规则已经出现。

然后 Server1 可以和 Router4 做 ping 连通性测试了：

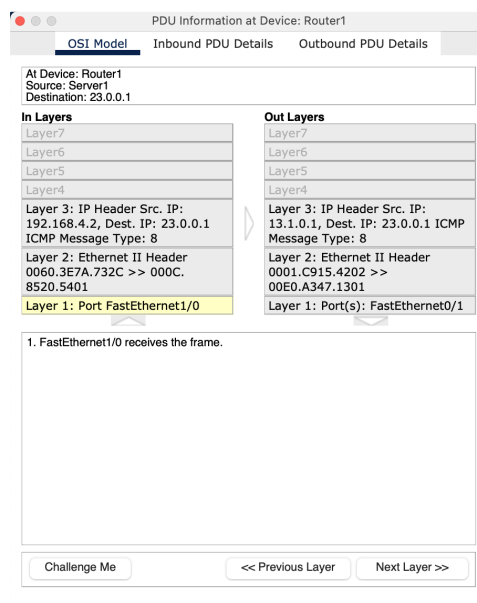


当然也可以和伺服器做 ping 测试了：

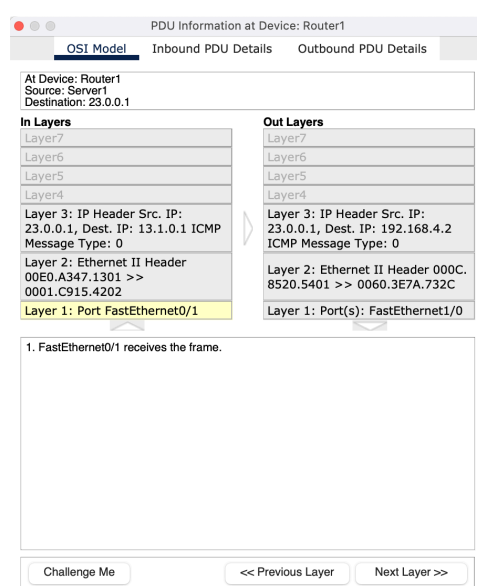


转换地址研究：

从内网经过 NAT 后，包的源地址从 192.168.4.2 变为 13.1.0.1:



包从路由器（公网）返回的时候，目的地地址由 Inside Global 地址 13.1.0.1 转为 Inside Local 地址 192.168.4.2 了：



显然，若子网内部的设备数量较多时，这样配置是十分麻烦的。

## 动态转换（Dynamic Translation）

接下来用动态转换的方式连接内网和公网。

以 PC1 到 Router2 为例

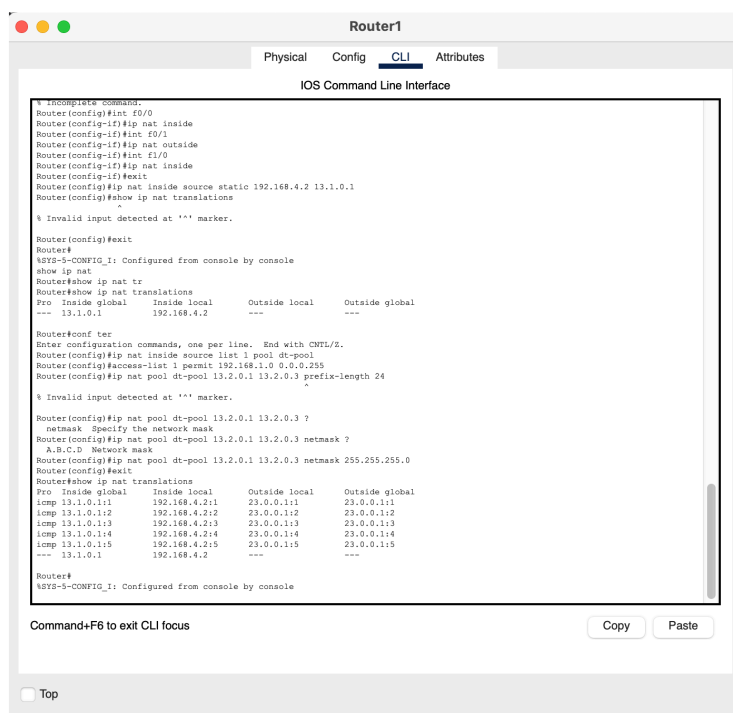
首先在 Router1 加入下面的语句；

```
1 ip nat inside source list 1 pool dt-pool
2 access-list 1 permit 192.168.1.0 0.0.0.255
3 ip nat pool dt-pool 13.2.0.1 13.2.0.3 netmask 255.255.255.0
```

然后输入下面语句查看 NAT 的转换表：

## 1 | show ip nat translations

可以看到，转换表除了刚才配好的静态路由外没有新的表项：



```
Router1
Physical Config CLI Attributes
IOS Command Line Interface

% Incomplete command.
Router(config)#int f0/0
Router(config-if)#ip nat inside
Router(config-if)#int f0/1
Router(config-if)#ip nat outside
Router(config-if)#int f1/0
Router(config-if)#ip nat inside
Router(config-if)#exit
Router(config)#ip nat inside source static 192.168.4.2 13.1.0.1
Router(config)#show ip nat translations
% Invalid input detected at '' marker.

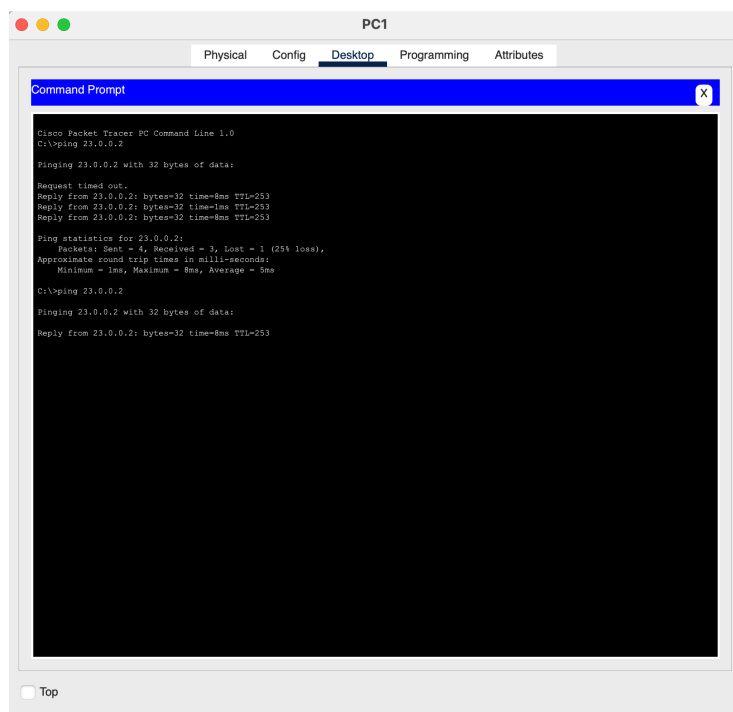
Router(config)#exit
Router#
%SYS-5-CONFIG_I: Configured from console by console
Router#show ip nat
Router#show ip nat tr
Router#show ip nat translations
Pro Inside global Inside local Outside local Outside global
--- 13.1.0.1 192.168.4.2 ---
Router#conf ter
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#ip nat inside source list 1 pool dt-pool
Router(config)#access-list 1 permit 192.168.1.0 0.0.0.255
Router(config)#ip nat pool dt-pool 13.2.0.1 13.2.0.3 prefix-length 24
% Invalid input detected at '' marker.

Router(config)#ip nat pool dt-pool 13.2.0.1 13.2.0.3 ?
netmask Specify the network mask
Router(config)#ip nat pool dt-pool 13.2.0.1 13.2.0.3 netmask ?
A.B.C.D Network mask
Router(config)#ip nat pool dt-pool 13.2.0.1 13.2.0.3 netmask 255.255.255.0
Router(config)#exit
Router#show ip nat translations
Pro Inside global Inside local Outside local Outside global
icmp 13.1.0.1:1 192.168.4.2:1 23.0.0.1:1 23.0.0.1:1
icmp 13.1.0.1:2 192.168.4.2:2 23.0.0.1:2 23.0.0.1:2
icmp 13.1.0.1:3 192.168.4.2:3 23.0.0.1:3 23.0.0.1:3
icmp 13.1.0.1:4 192.168.4.2:4 23.0.0.1:4 23.0.0.1:4
icmp 13.1.0.1:5 192.168.4.2:5 23.0.0.1:5 23.0.0.1:5
--- 13.1.0.1 192.168.4.2 ---
Router#
%SYS-5-CONFIG_I: Configured from console by console

Command+F6 to exit CLI focus
```

## Ping 测试

接下来用 PC1 向 Router2 作 ping 通信：



```
PC1
Physical Config Desktop Programming Attributes
Command Prompt

Cisco Packet Tracer PC Command Line 1.0
C:\>ping 23.0.0.2

Pinging 23.0.0.2 with 32 bytes of data:

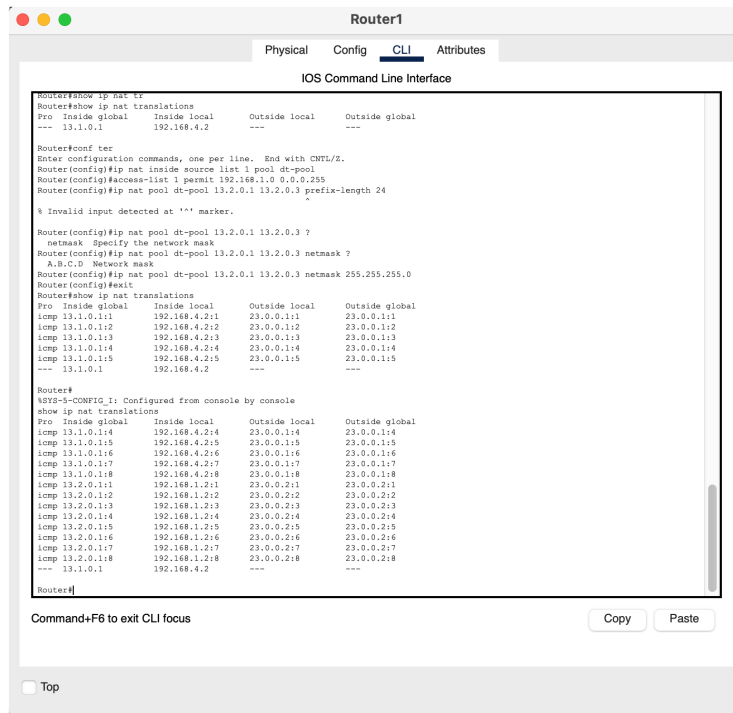
Request timed out.
Reply from 23.0.0.2: bytes=32 time=8ms TTL=253
Reply from 23.0.0.2: bytes=32 time=8ms TTL=253
Reply from 23.0.0.2: bytes=32 time=8ms TTL=253

Ping statistics for 23.0.0.2:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 8ms, Maximum = 8ms, Average = 8ms
C:\>ping 23.0.0.2

Pinging 23.0.0.2 with 32 bytes of data:

Reply from 23.0.0.2: bytes=32 time=8ms TTL=253
```

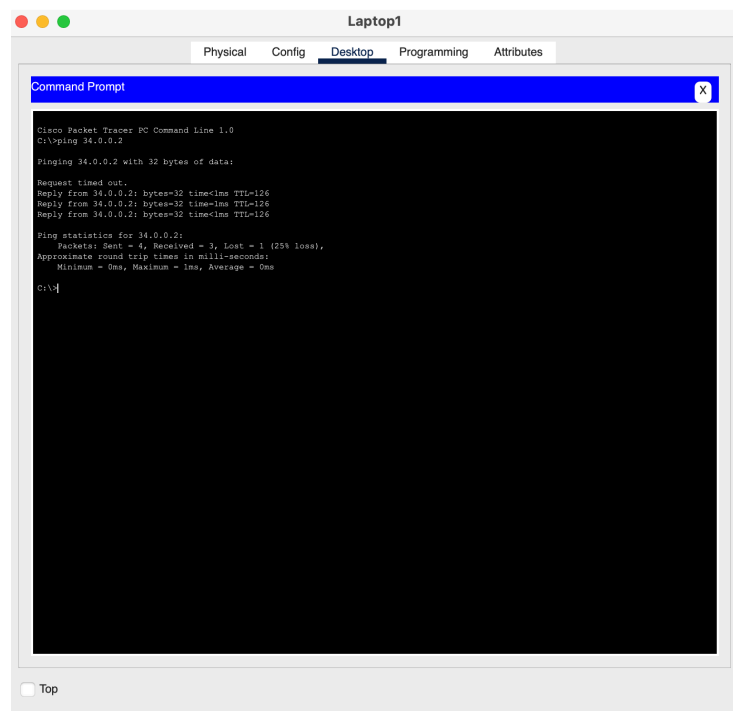
发现可以连通，此时再次查看转换表，可以看到新的表项已经出现：



这说明只有当新的位置发出数据包后才会进行地址分配。然而公网地址是有限的，比如上面只配置了三个地址（即：13.2.0.1 - 13.2.0.3），当设备数量大于 3 时，便会出现地址不足的问题。

## 伺服器 ping 测试

采用动态地址也可以和伺服器通信：



## PAT (Port Address Translation)

在不可能为所有设备都准备一组公网地址的情况下，我采用了 PAT。

PAT 会把源端口和目的地端口加入转换，在可用的地址数目不变的情况下可以允许更多的流量了。

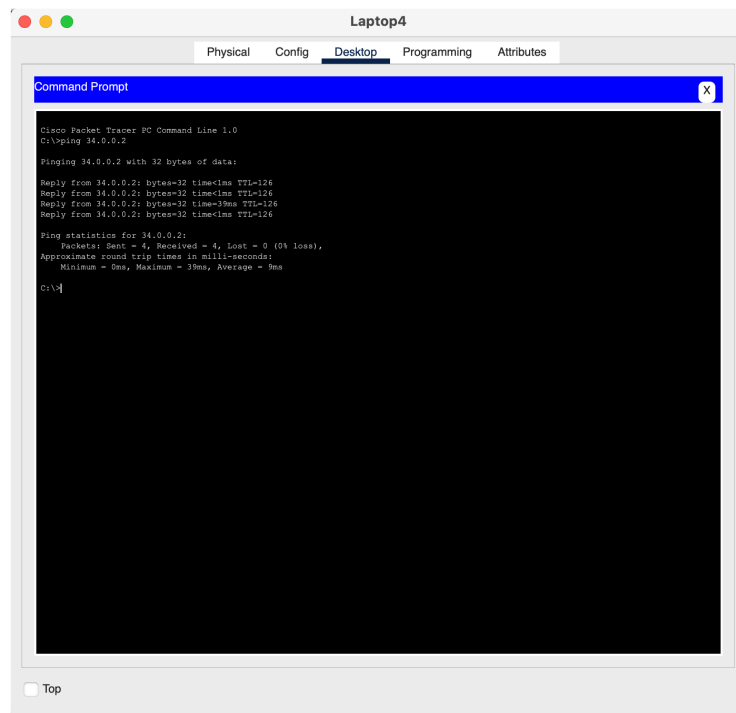
## Router2

对 Router2 加入如下配置：

```
1 ip nat inside source list 1 pool dt-pool overload
2 access-list 1 permit 192.168.2.0 0.0.0.255
3 access-list 1 permit 192.168.3.0 0.0.0.255
4 ip nat pool dt-pool 23.2.0.1 23.2.0.1 netmask 255.255.255.0
```

## 连通性测试

此时，网络内的所有设备都可以向服务器通信了！

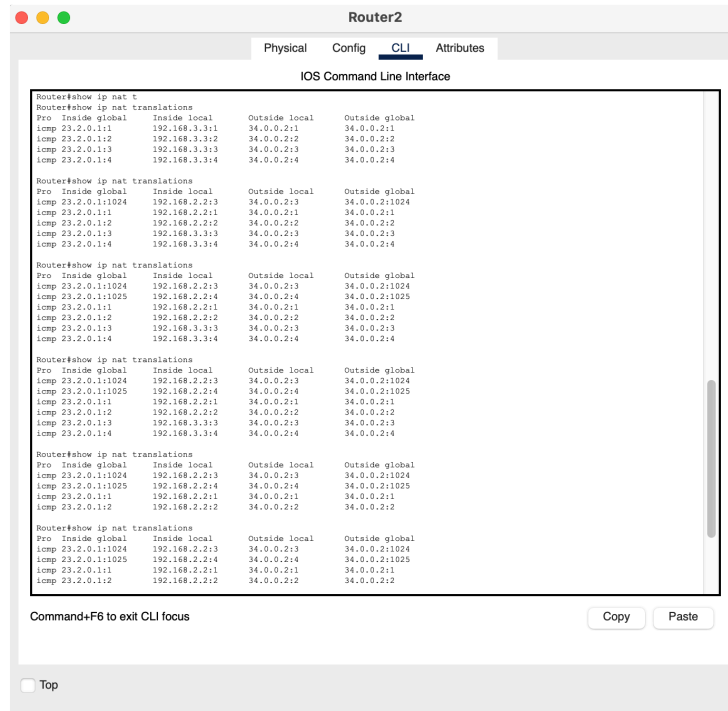


## PAT 特性

首先，从 192.168.3.3 向 Server 作通信；过一段时间后再用 192.168.2.2 向 Server 通信；

在过程中利用 `show ip nat translations` 查看 Router2 的 NAT 映射表，得到如下结果：





可以看到，当前者的通信完成（过期）后，后者会重用旧的端口号以节省 IP 资源。