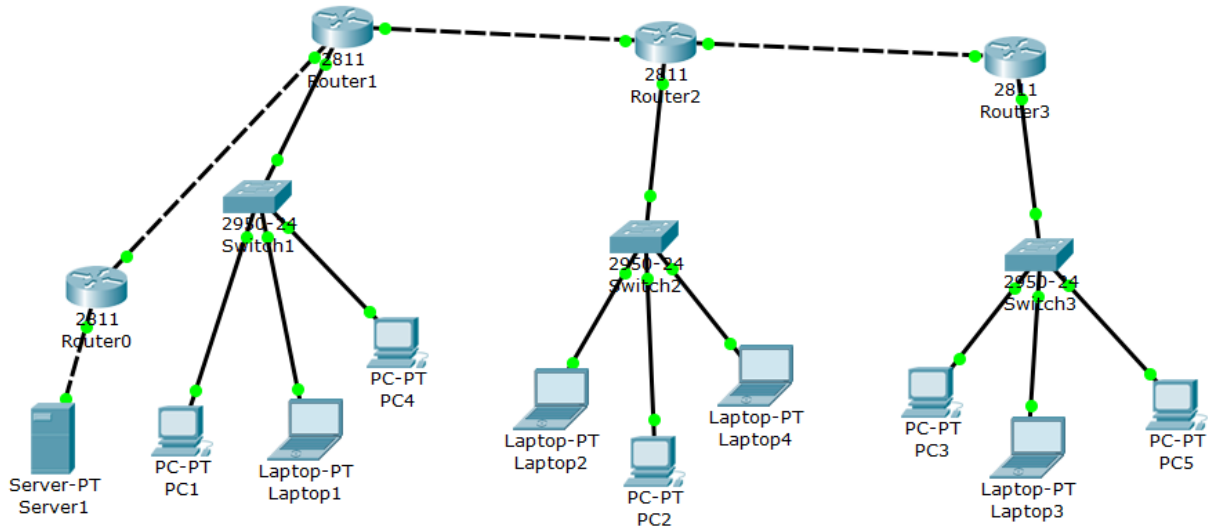
访问控制及 VPN 技术 实验报告

计 82 郑凯文 2018011314

1 任务 6

由于需要对 Server1 的访问进行控制，而 Server1 与子网内的设备通过交换机进行通信，无法控制。因此加入路由器 Router0，配置 Server1 的 ip 为 192.168.4.2，网关为 192.168.4.1，Router0 与 Server1 连接端口的 ip 为 192.168.4.1，与 Router1 连接端口的 ip 为 10.0.10.2，并配置好相关的静态路由（在实验 1 的基础上，仅需添加 Router1 和 Router0 之间的静态路由）。拓扑图如下：



1.各个权力机构内部的所有成员均能相互通信：由于处于同一子网，自然满足

2.权力机构之间的相互通信只通过联络人实现：分别在 Router1 Router2 Router3 与子网相连的 out 端设置 ACL，允许目的地址或源地址为联络人的数据通过。

3.领导人之间可以互相通信：分别在 Router1 Router2 Router3 与子网相连的 out 端设置 ACL，允许源地址为另外两个领导人地址，目的地址为该子网领导人地址的数据通过。

4.PC1 与 Server1 通信：在 Router0 与 Server1 连接端口的 in 端设置只允许目的地址为 PC1，out 端设置只允许源地址为 PC1。

对 Router1 进行如下配置：

```
Router(config)#access-list 101 permit ip any host 192.168.1.4
Router(config)#access-list 101 permit ip host 192.168.2.2 any
Router(config)#access-list 101 permit ip host 192.168.3.3 any
Router(config)#access-list 101 permit ip host 192.168.2.3 host 192.168.1.2
Router(config)#access-list 101 permit ip host 192.168.3.2 host 192.168.1.2
Router(config)#int f0/0
Router(config-if)#ip access-group 101 out
```

对 Router2 进行如下配置：

```
Router(config)#access-list 101 permit ip any host 192.168.2.2
Router(config)#access-list 101 permit ip host 192.168.1.4 any
Router(config)#access-list 101 permit ip host 192.168.3.3 any
Router(config)#access-list 101 permit ip host 192.168.1.2 host 192.168.2.3
Router(config)#access-list 101 permit ip host 192.168.3.2 host 192.168.2.3
Router(config)#int f1/0
Router(config-if)#ip access-group 101 out
```

对 Router3 进行如下配置：

```
Router(config)#access-list 101 permit ip any host 192.168.3.3
Router(config)#access-list 101 permit ip host 192.168.1.4 any
Router(config)#access-list 101 permit ip host 192.168.2.2 any
Router(config)#access-list 101 permit ip host 192.168.1.2 host 192.168.3.2
Router(config)#access-list 101 permit ip host 192.168.2.3 host 192.168.3.2
Router(config-if)#int f0/1
Router(config-if)#ip access-group 101 out
```

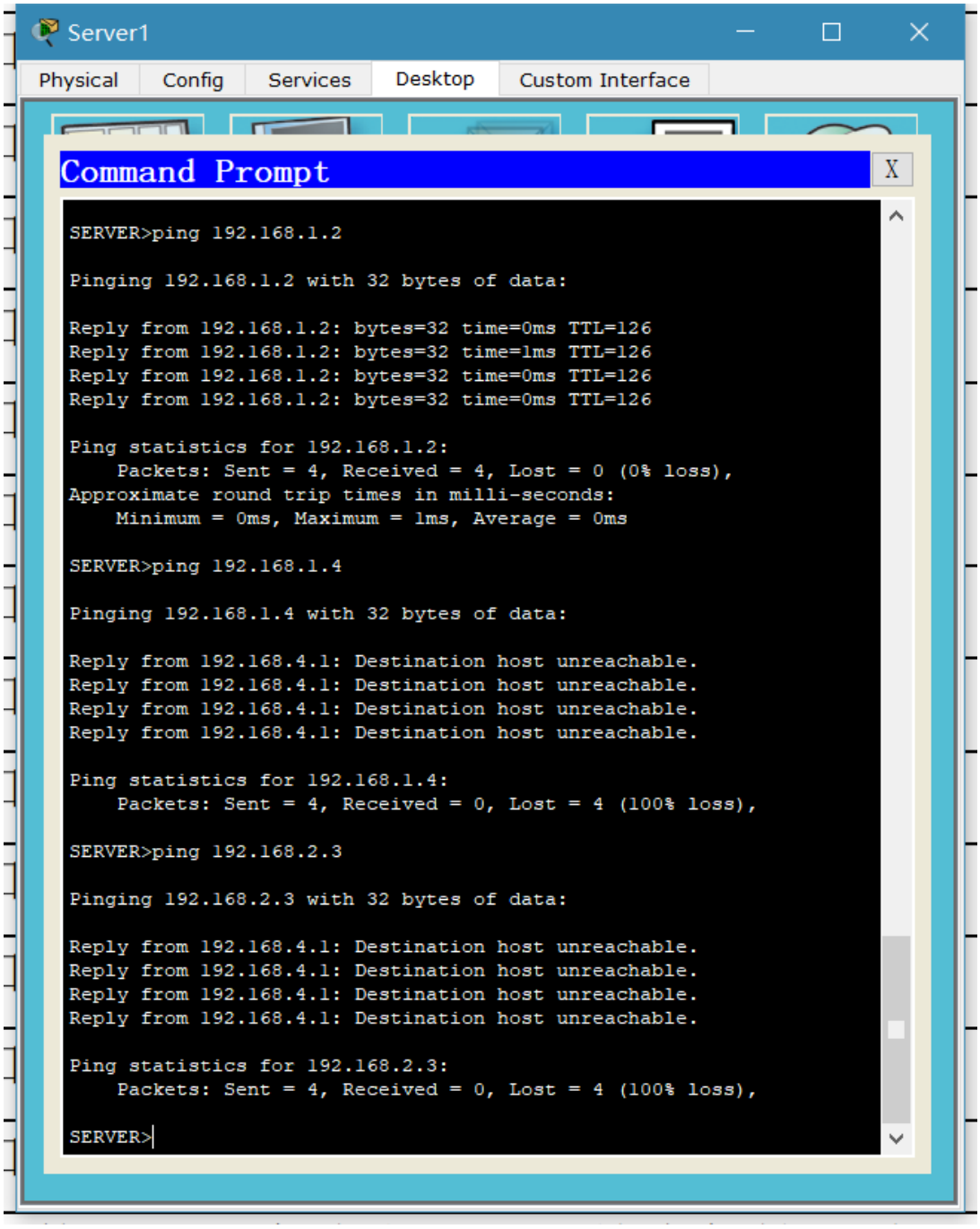
对 Router0 进行如下配置：

```
Router(config)#access-list 101 permit ip host 192.168.4.2 host 192.168.1.2
Router(config)#access-list 102 permit ip host 192.168.1.2 host 192.168.4.2
Router(config-if)#int f0/1
Router(config-if)#ip access-group 101 in
Router(config-if)#ip access-group 102 out
```

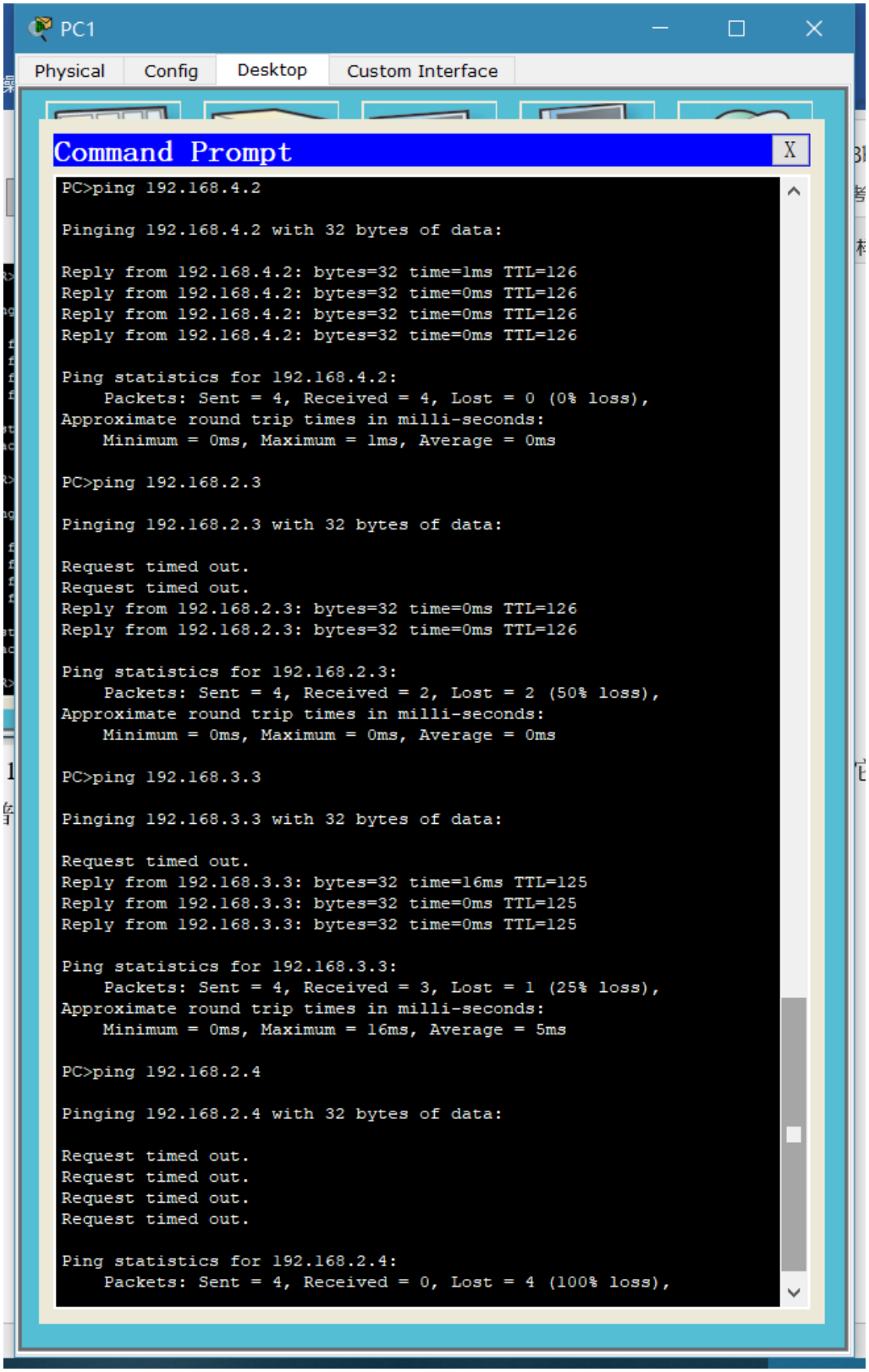
此时，PC1 和 Server1 不能互相 ping 通，这是因为 Router1 禁止了到 Router0 的转发。在 Router1 中加入 ACL：

```
Router(config)#access-list 101 permit ip host 192.168.1.2 host 192.168.4.2
Router(config)#access-list 101 permit ip host 192.168.4.2 host 192.168.1.2
```

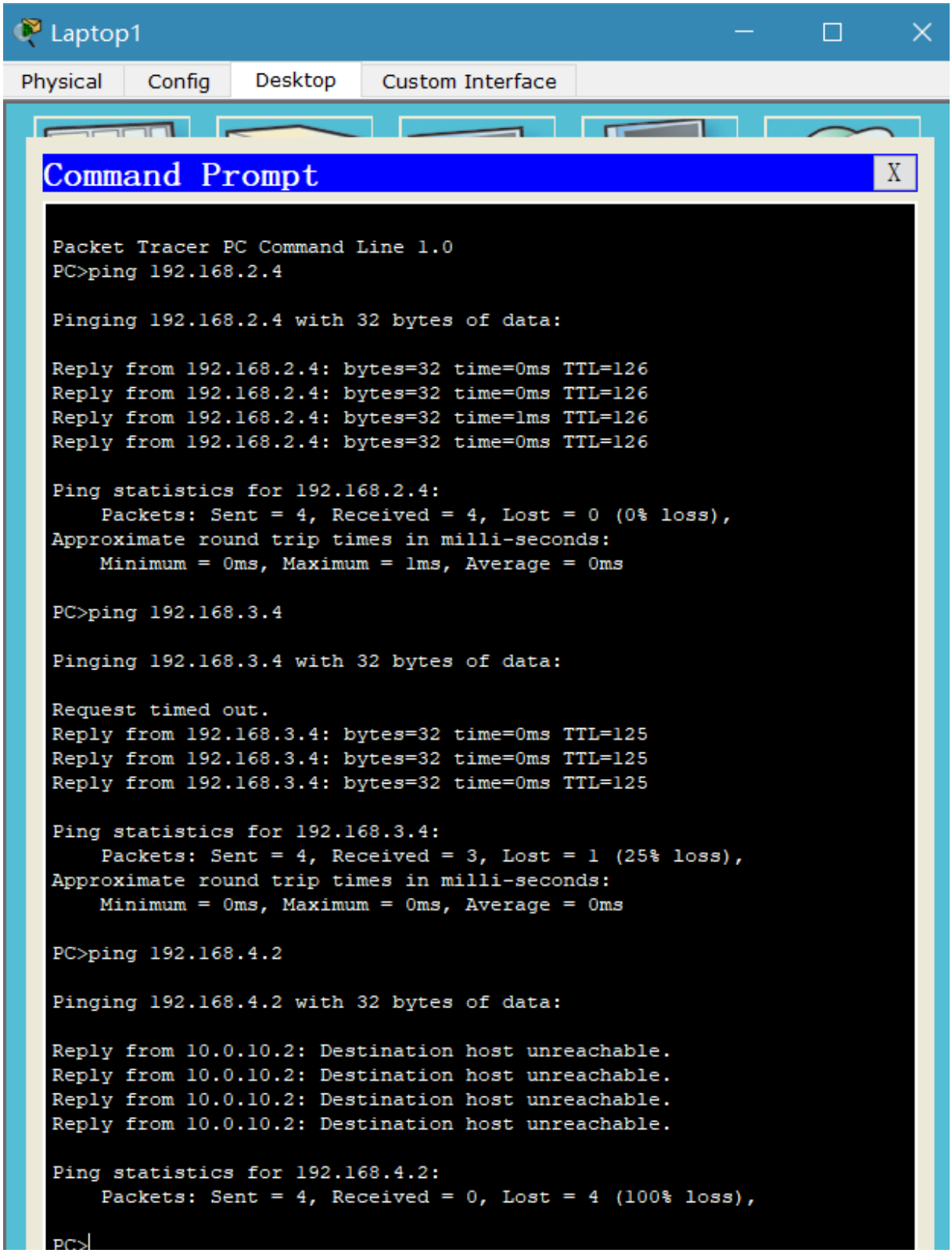
（1）Server1 可以 ping 通 pc1，ping 不通其它设备



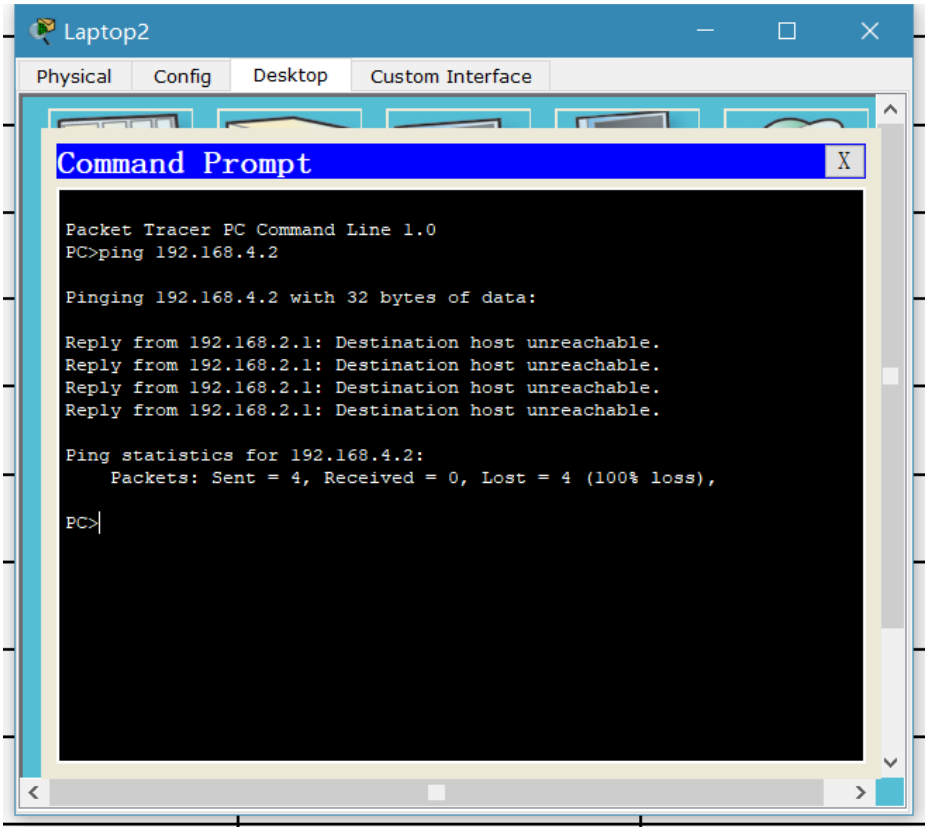
（2）PC1 可以 ping 通 Server1，其它领导人、联络人，ping 不通辅助执政官 B 等其它子网中的普通设备。这也证明了领导人不能同其它子网中的非领导人、非联络人通信。

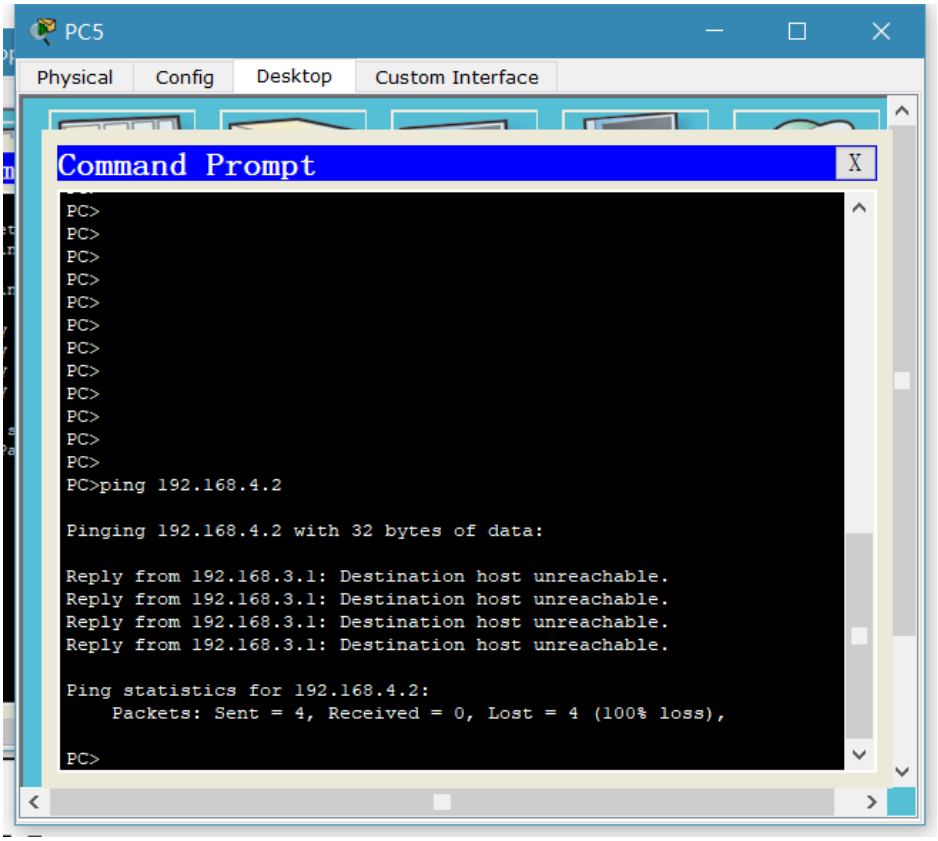


（3）联络人可以 ping 通除 Server1 外的任何设备



（4）除 PC1 外，其它领导人 ping 不通 Server1，其它普通设备也 ping 不通


Laptop2
Physical
Config
Desktop
Custom Interface
Command Prompt
X
Packet Tracer PC Command Line 1.0
PC>ping 192.168.4.2
Pinging 192.168.4.2 with 32 bytes of data:
Reply from 192.168.2.1: Destination host unreachable.
Reply from 192.168.2.1: Destination host unreachable.
Reply from 192.168.2.1: Destination host unreachable.
Reply from 192.168.2.1: Destination host unreachable.
Ping statistics for 192.168.4.2:
Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
PC>


PC5
Physical
Config
Desktop
Custom Interface
Command Prompt
X
PC>
PC>
PC>
PC>
PC>
PC>
PC>
PC>
PC>
PC>
PC>
PC>ping 192.168.4.2
Pinging 192.168.4.2 with 32 bytes of data:
Reply from 192.168.3.1: Destination host unreachable.
Reply from 192.168.3.1: Destination host unreachable.
Reply from 192.168.3.1: Destination host unreachable.
Reply from 192.168.3.1: Destination host unreachable.
Ping statistics for 192.168.4.2:
Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
PC>

2　任务 7

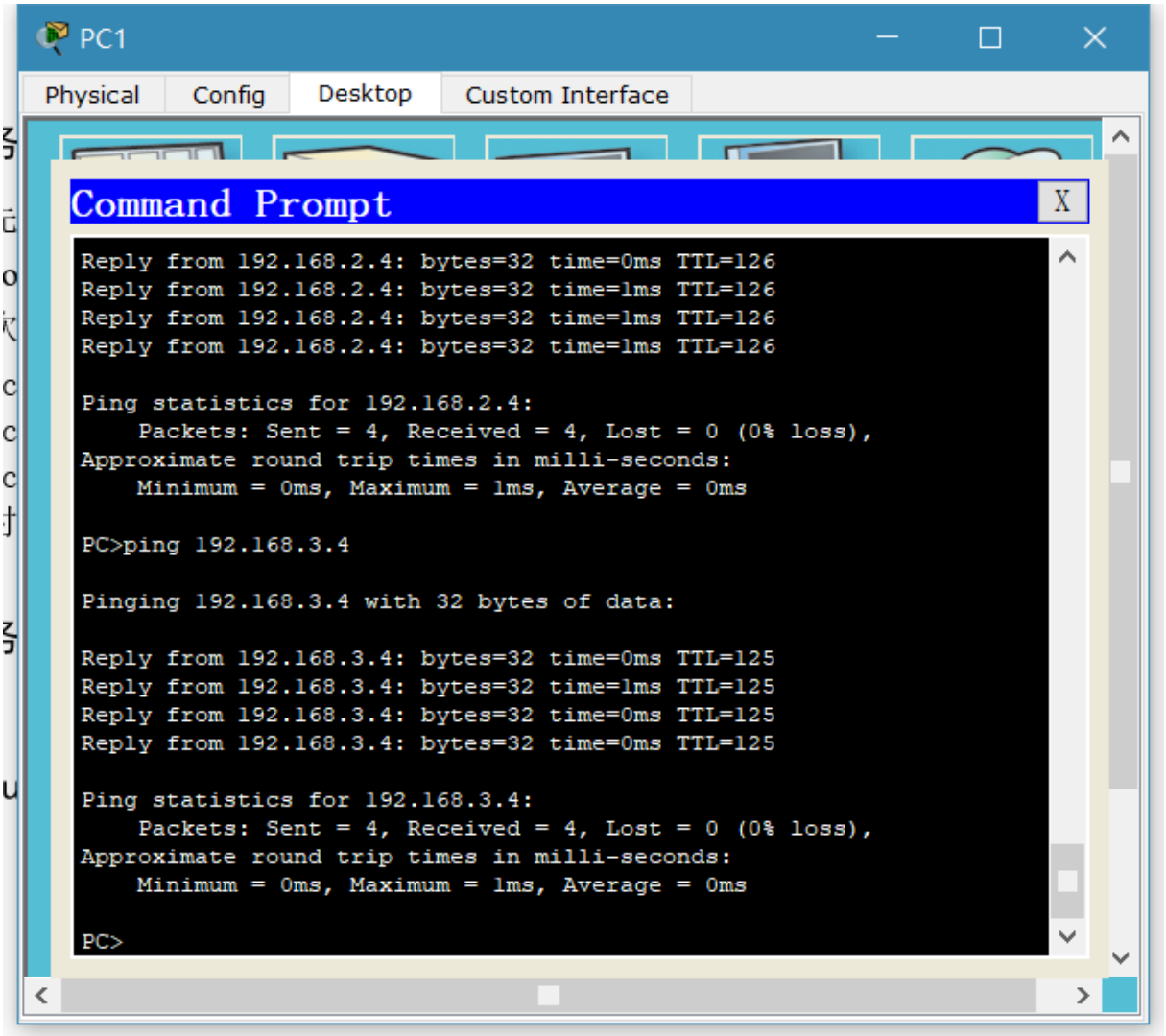
首先为 Router2 和 Router3 添加 ACL 允许来自 PC1 的 icmp 包通过

```
Router(config)#access-list 101 permit icmp host 192.168.1.2 any
```

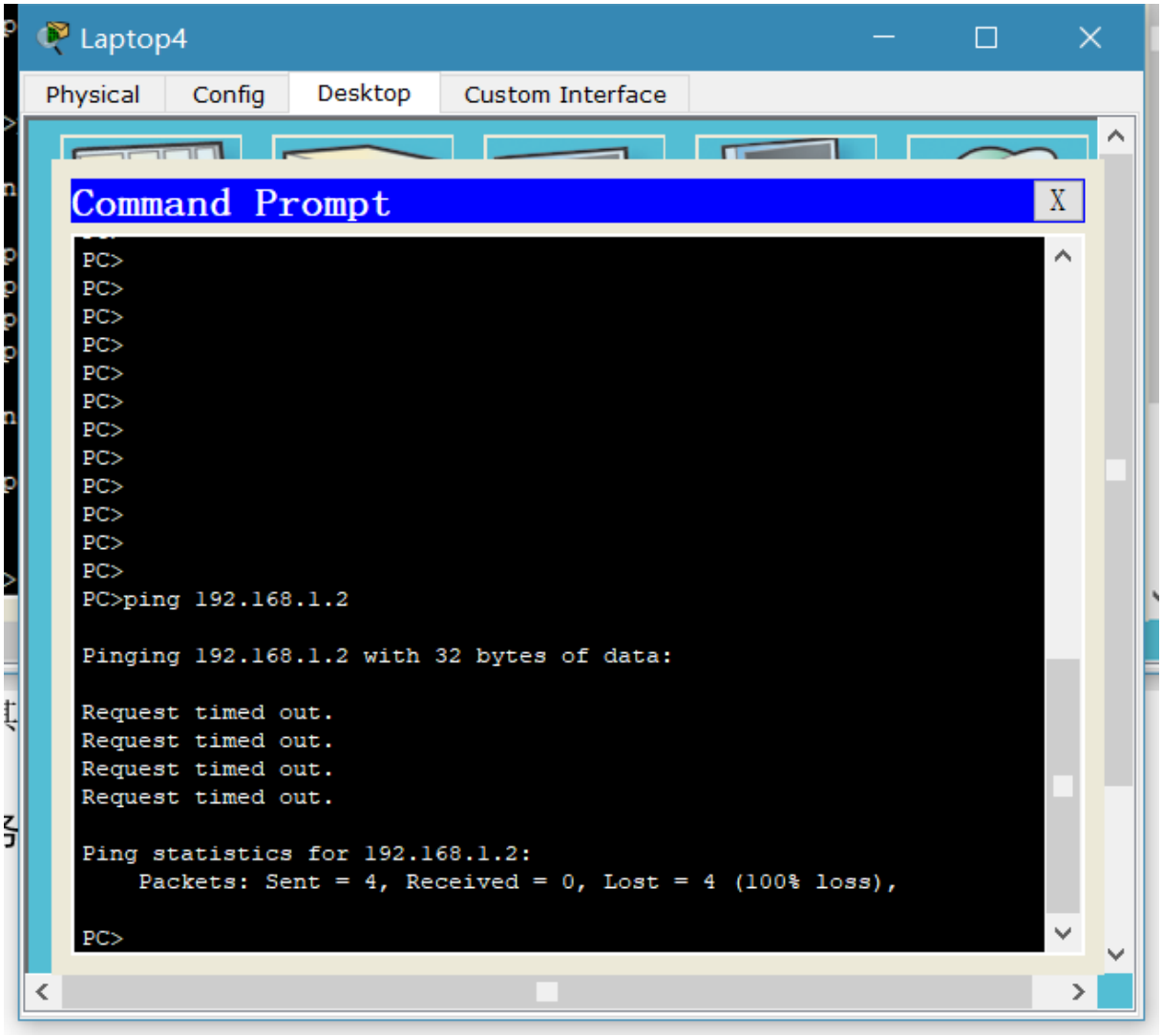
其次在 Router1 与子网相连的 in 端配置 CBAC，允许 ping 之后收到返回的包

```
Router(config)#ip inspect name pingtest icmp
Router(config)#int f0/0
Router(config-if)#ip inspect pingtest in
```

此时，PC1 可以 ping 通其它子网中的普通设备（在任务 6 中 ping 不通）



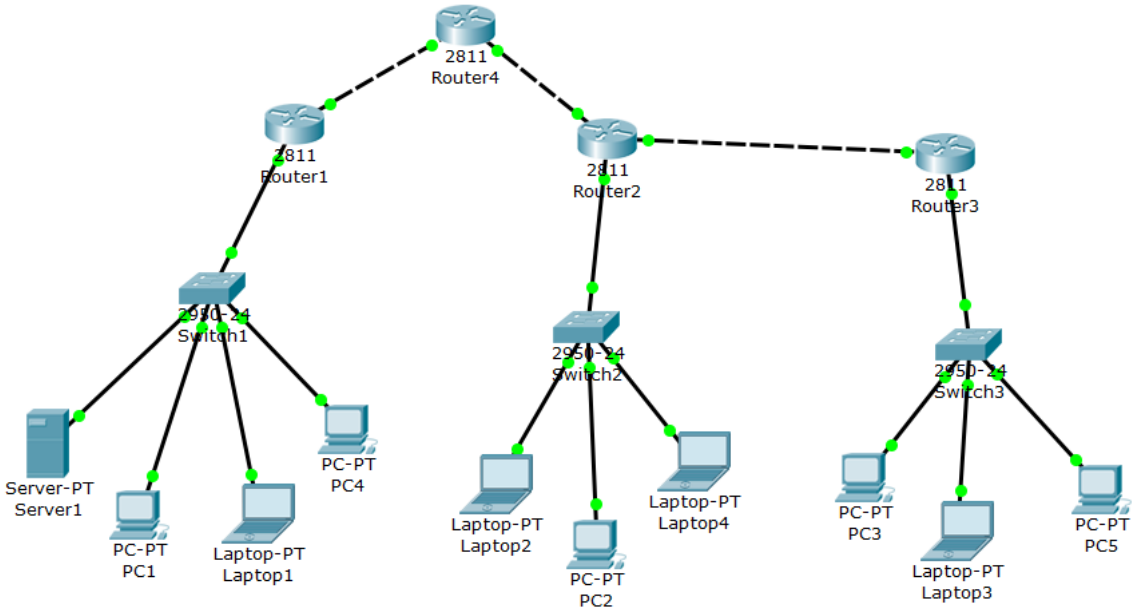
反之，其它子网中的普通设备 ping 不通 PC1



3 任务 8

静态路由失效的原因：私网 ip 地址需要经过 NAT 转换才能作为公网 ip 进行通信，而静态路由只能配置私网以及公网边界上的路由，因此若采用静态路由，公网上的路由器无法对 192.168.x.x 形式的私网 ip 进行转发。

恢复先前的网络拓扑，并添加 Router4。新的网络拓扑如下：

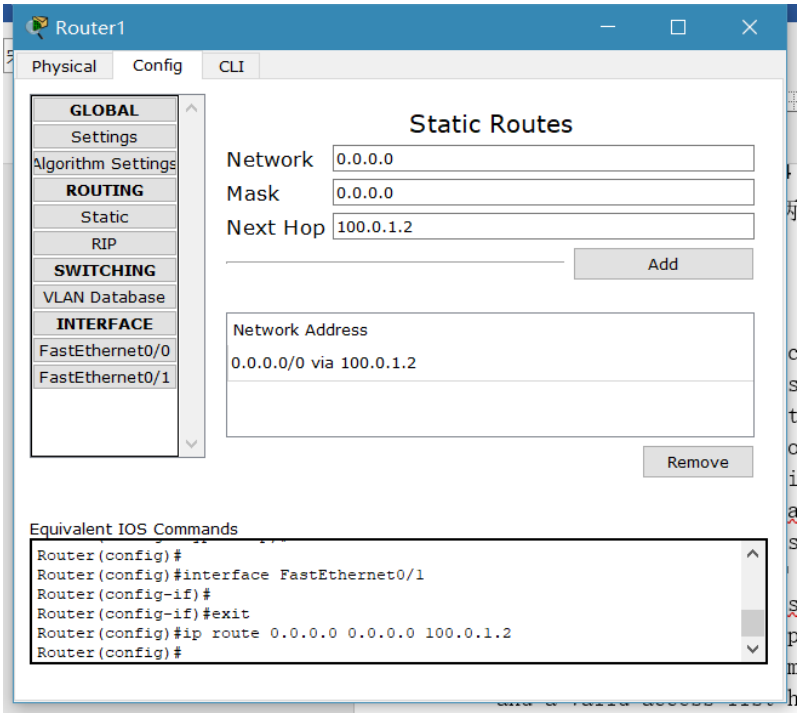


设置 Router1 与 Router4 相连的端口 ip 为 100.0.1.1，Router2 与 Router4 相连的端口 ip 为 100.0.2.1，Router4 的两个端口分别为 100.0.1.2 和 100.0.2.2。

在 Router1 上进行配置：

```
Router(config)#interface FastEthernet0/1
Router(config-if)#crypto isakmp policy 1
Router(config-isakmp)#encryption 3des
Router(config-isakmp)#hash md5
Router(config-isakmp)#authentication pre-share
Router(config-isakmp)#group 5
Router(config-isakmp)#exit
Router(config)#crypto isakmp key 123456 address 100.0.2.1
Router(config)#access-list 101 permit ip 192.168.0.0 0.0.255.255
192.168.0.0 0.0.255.255
Router(config)#crypto ipsec transform-set vpnset esp-3des esp-md5-hmac
Router(config)#crypto map vpnmap 1 ipsec-isakmp
% NOTE: This new crypto map will remain disabled until a peer
and a valid access list have been configured.
Router(config-crypto-map)#set peer 100.0.2.1
Router(config-crypto-map)#set transform-set vpnset
Router(config-crypto-map)#match address 101
Router(config-crypto-map)#exit
Router(config)#interface FastEthernet0/1
Router(config-if)#crypto map vpnmap
```

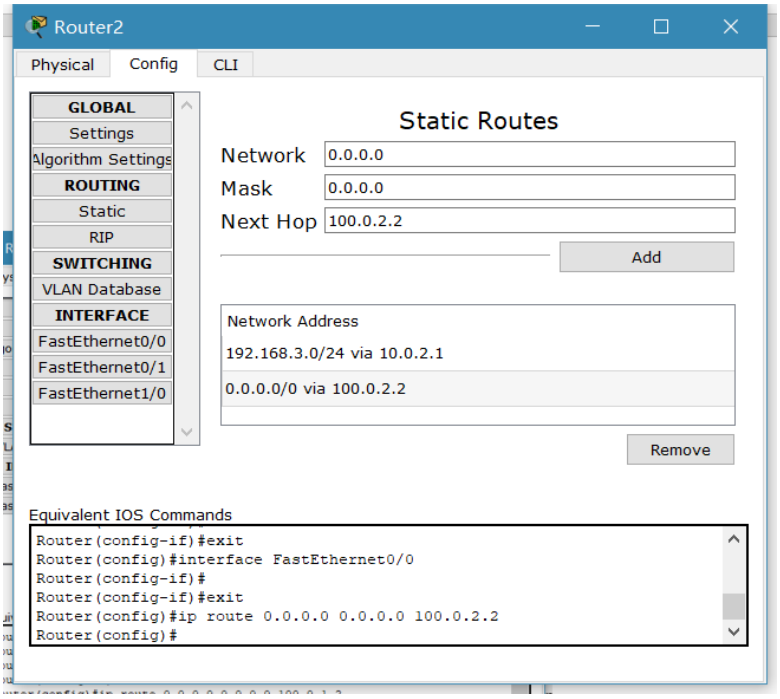
在 Router1 上配置静态路由：



在 Router2 上进行配置：

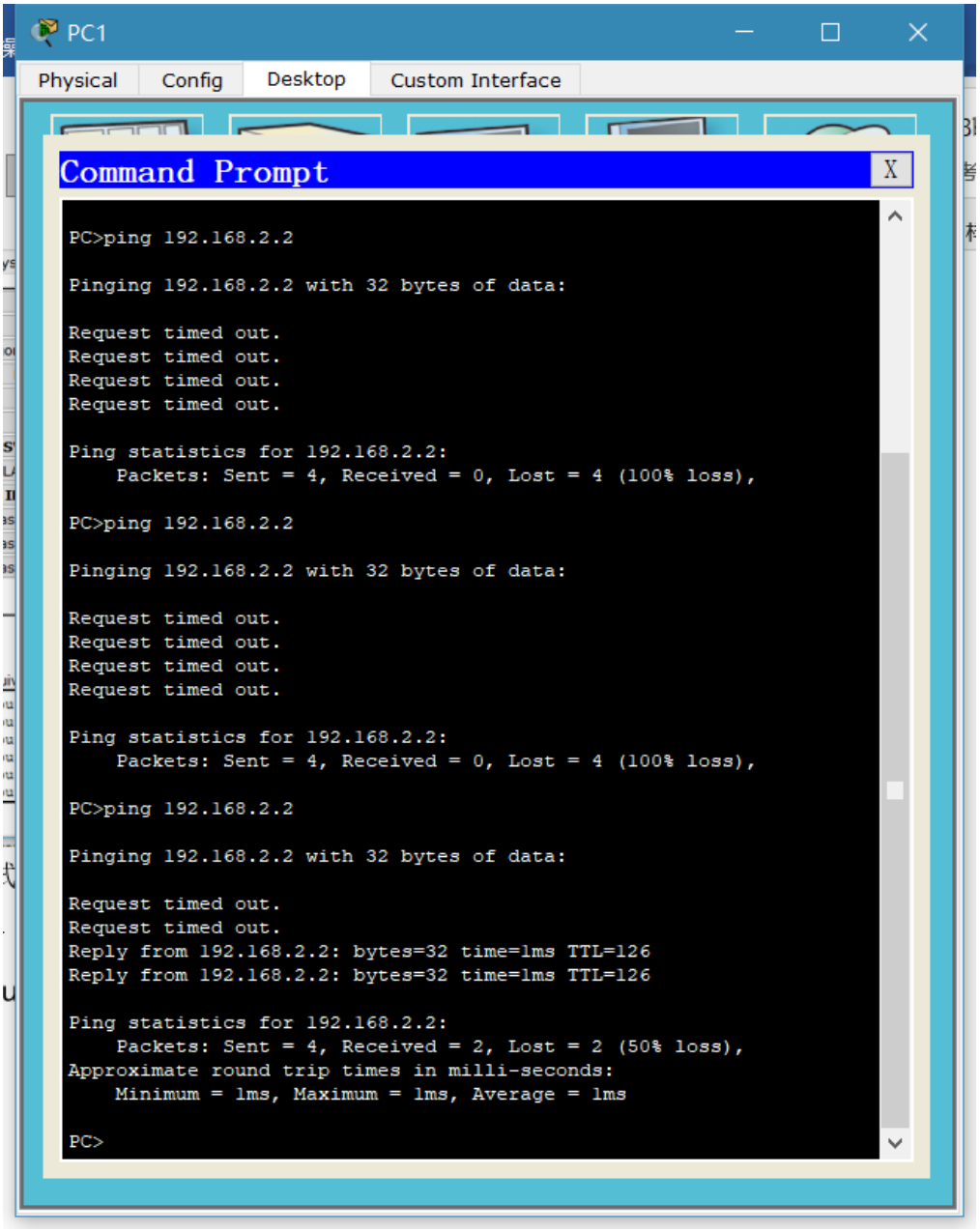
```
Router(config)#interface FastEthernet0/0
Router(config-if)#crypto isakmp policy 1
Router(config-isakmp)#encryption 3des
Router(config-isakmp)#hash md5
Router(config-isakmp)#authentication pre-share
Router(config-isakmp)#group 5
Router(config-isakmp)#exit
Router(config)#crypto isakmp key 123456 address 100.0.1.1
Router(config)#access-list 101 permit ip 192.168.0.0 0.0.255.255
192.168.0.0 0.0.255.255
Router(config)#crypto ipsec transform-set vpnset esp-3des esp-md5-hmac
Router(config)#crypto map vpnmap 1 ipsec-isakmp
% NOTE: This new crypto map will remain disabled until a peer
and a valid access list have been configured.
Router(config-crypto-map)#set peer 100.0.1.1
Router(config-crypto-map)#set transform-set vpnset
Router(config-crypto-map)#match address 101
Router(config-crypto-map)#exit
Router(config)#interface FastEthernet0/0
Router(config-if)#crypto map vpnmap
```

在 Router2 上配置静态路由：



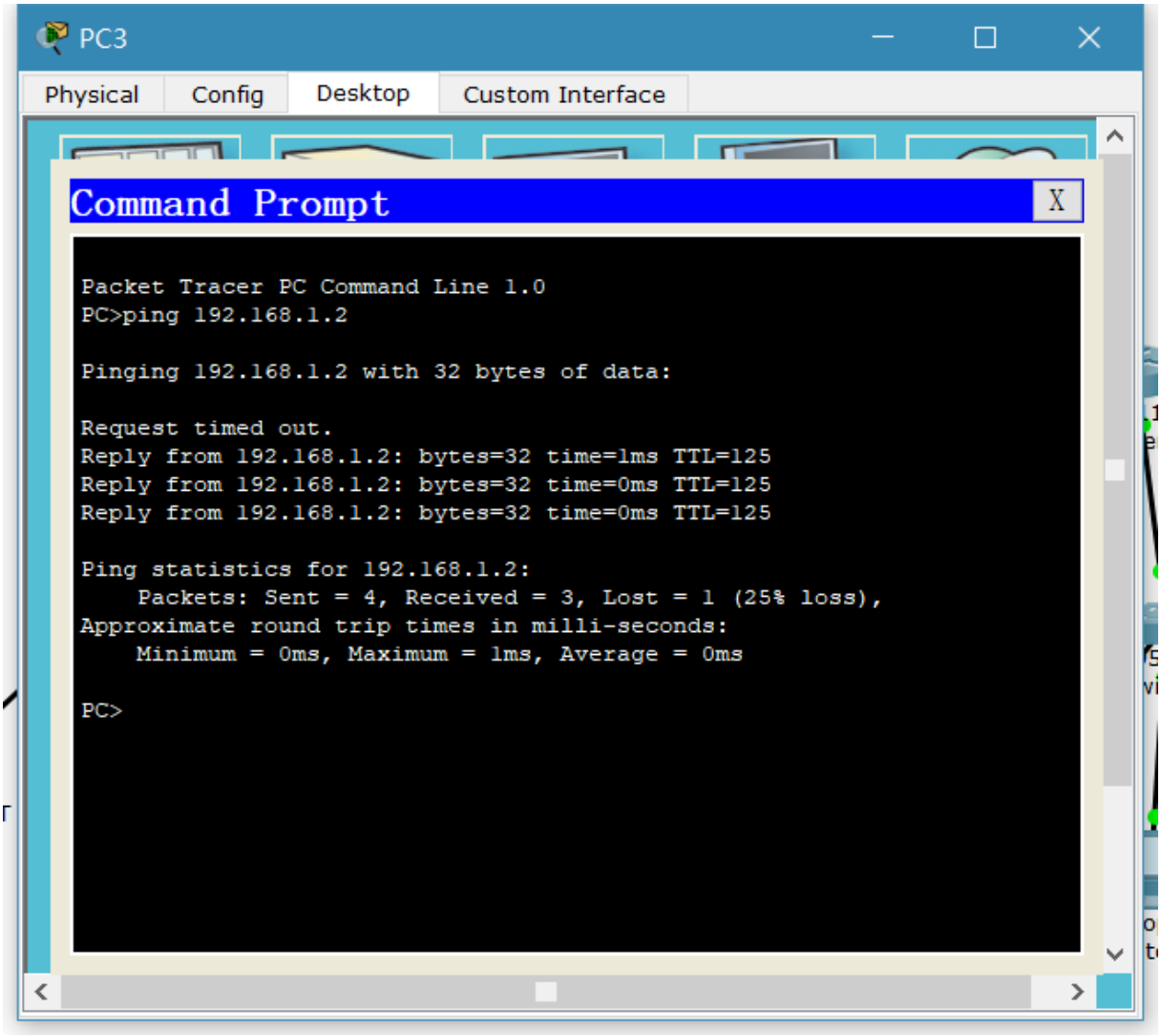
测试联通性：

PC1 ping 子网 2：



可以看到，经过一段时间后 ping 通了。

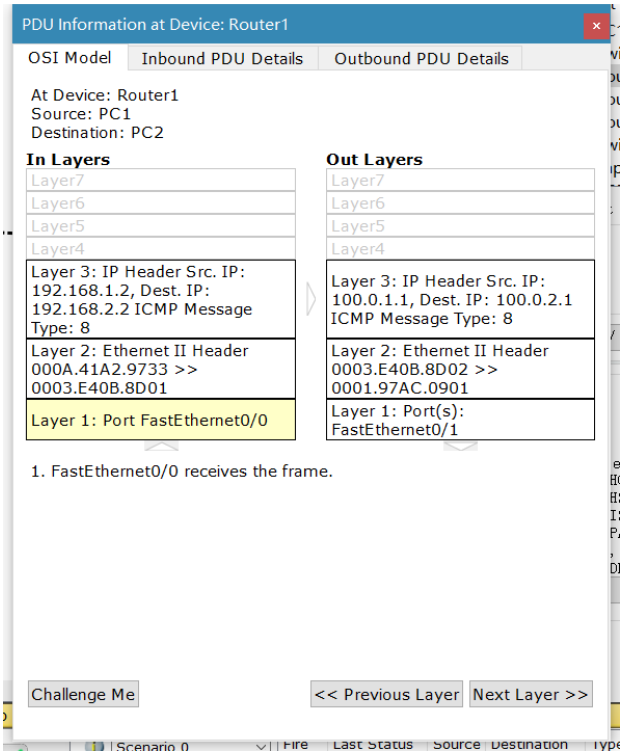
PC3 ping 子网 1：



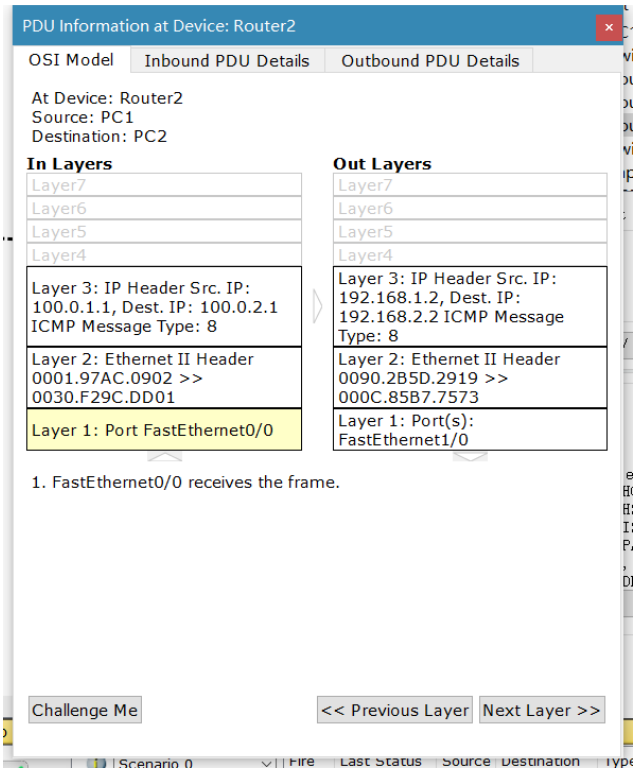
由于之前协商好了，这次很快就 ping 通了。

从 PC1 ping PC2，抓取报文：

Router1：


PDU Information at Device: Router1
OSI Model
Inbound PDU Details
Outbound PDU Details
At Device: Router1
Source: PC1
Destination: PC2
In Layers
Out Layers
Layer7
Layer6
Layer5
Layer4
Layer 3: IP Header Src. IP: 192.168.1.2, Dest. IP: 192.168.2.2 ICMP Message Type: 8
Layer 3: IP Header Src. IP: 100.0.1.1, Dest. IP: 100.0.2.1 ICMP Message Type: 8
Layer 2: Ethernet II Header 000A.41A2.9733 >> 0003.E40B.8D01
Layer 2: Ethernet II Header 0003.E40B.8D02 >> 0001.97AC.0901
Layer 1: Port FastEthernet0/0
Layer 1: Port(s): FastEthernet0/1
1. FastEthernet0/0 receives the frame.
Challenge Me
<< Previous Layer
Next Layer >>

Router2：

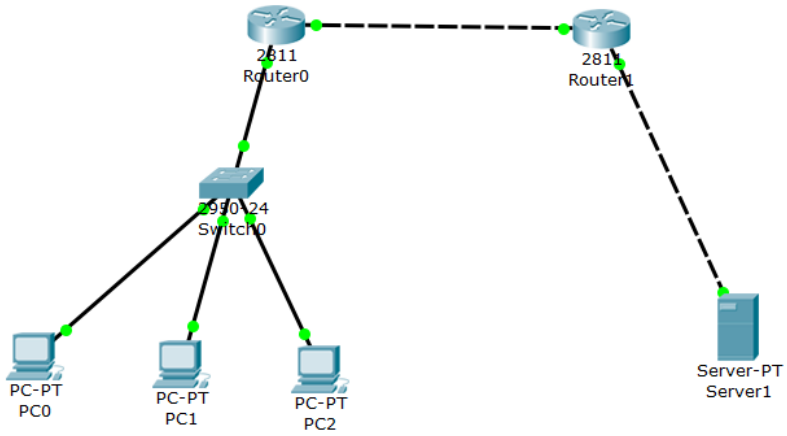

PDU Information at Device: Router2
OSI Model
Inbound PDU Details
Outbound PDU Details
At Device: Router2
Source: PC1
Destination: PC2
In Layers
Out Layers
Layer7
Layer6
Layer5
Layer4
Layer 3: IP Header Src. IP: 100.0.1.1, Dest. IP: 100.0.2.1 ICMP Message Type: 8
Layer 3: IP Header Src. IP: 192.168.1.2, Dest. IP: 192.168.2.2 ICMP Message Type: 8
Layer 2: Ethernet II Header 0001.97AC.0902 >> 0030.F29C.DD01
Layer 2: Ethernet II Header 0090.2B5D.2919 >> 000C.85B7.7573
Layer 1: Port FastEthernet0/0
Layer 1: Port(s): FastEthernet1/0
1. FastEthernet0/0 receives the frame.
Challenge Me
<< Previous Layer
Next Layer >>

可以看到 Router1 处报文的 ip 头中的目的地址被修改为公网 ip，在 Router2 处又被改回私网 ip，这说明采用了隧道模式，原先的数据包被包装后外加了新的 ip 头，以便于在公网上进行转发。

6 Bonus 任务

探究网络地址转换 NAT

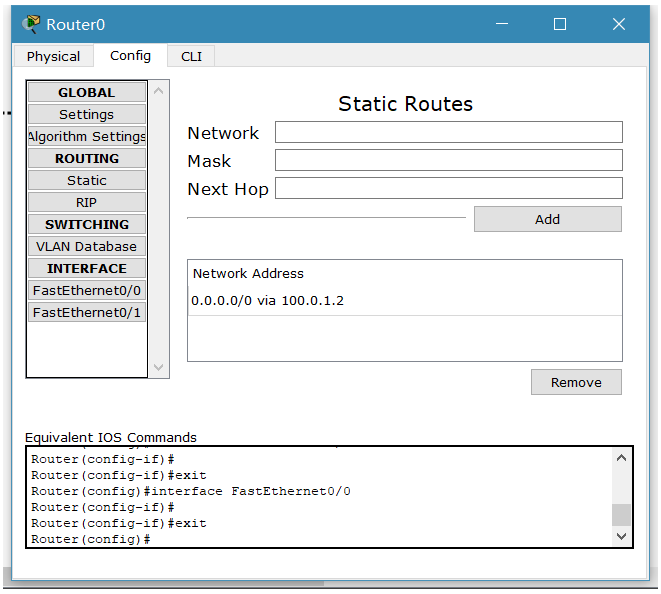
构建如下图所示的网络拓扑



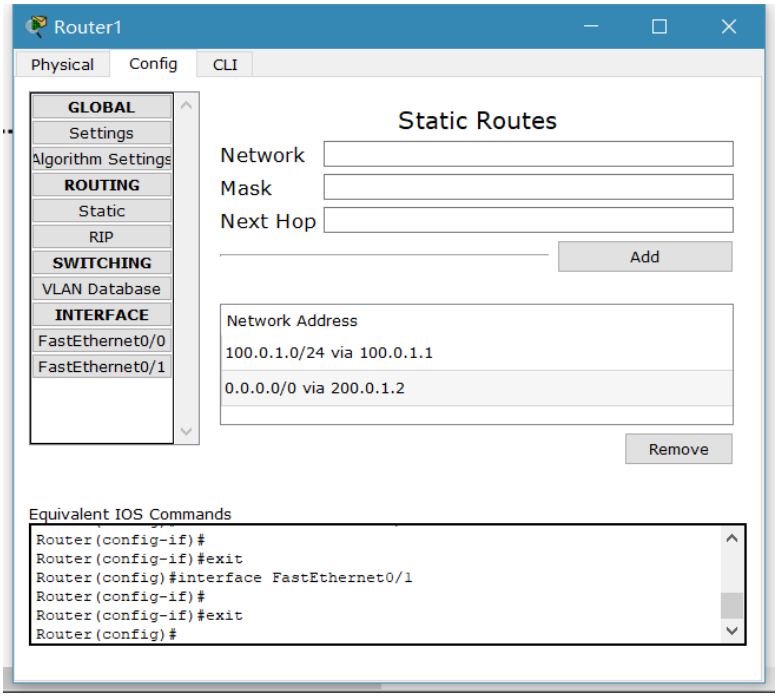
其中 Router0 及其子网为私网，右侧为公网。

配置 PC0 PC1 PC2 的 ip 分别为 192.168.1.2 192.168.1.3 192.168.1.4，网关为 192.168.1.1。Router0 左侧端口 ip 为 192.168.1.1，右侧端口 ip 为 100.0.1.1，Router2 左侧端口 ip 为 100.0.1.2，右侧端口 ip 为 200.0.1.1，Server1 ip 为 200.0.1.2.

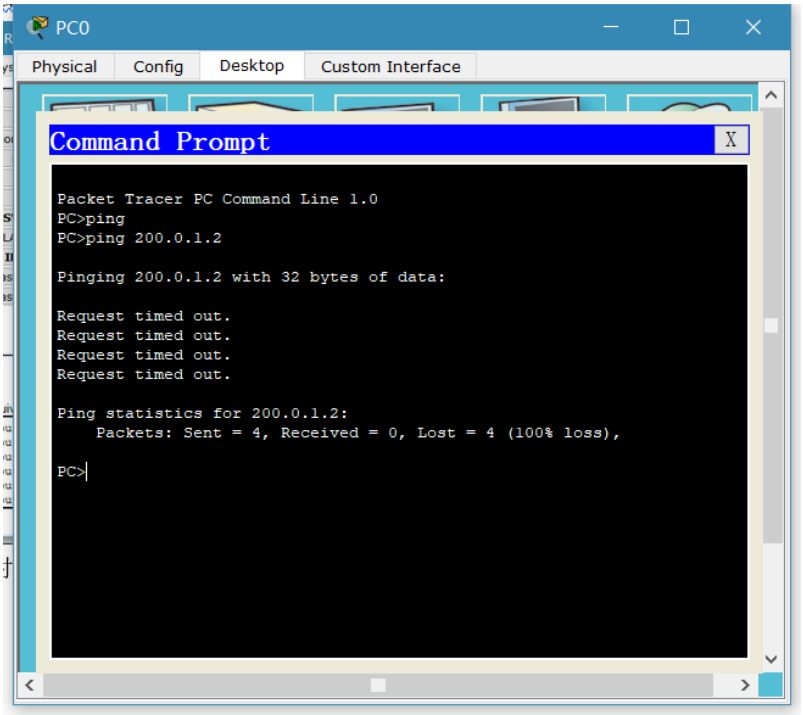
配置 Router0 静态路由为



即私网数据转发至公网。Router1 静态路由为



此时 PC0 ping Server1：

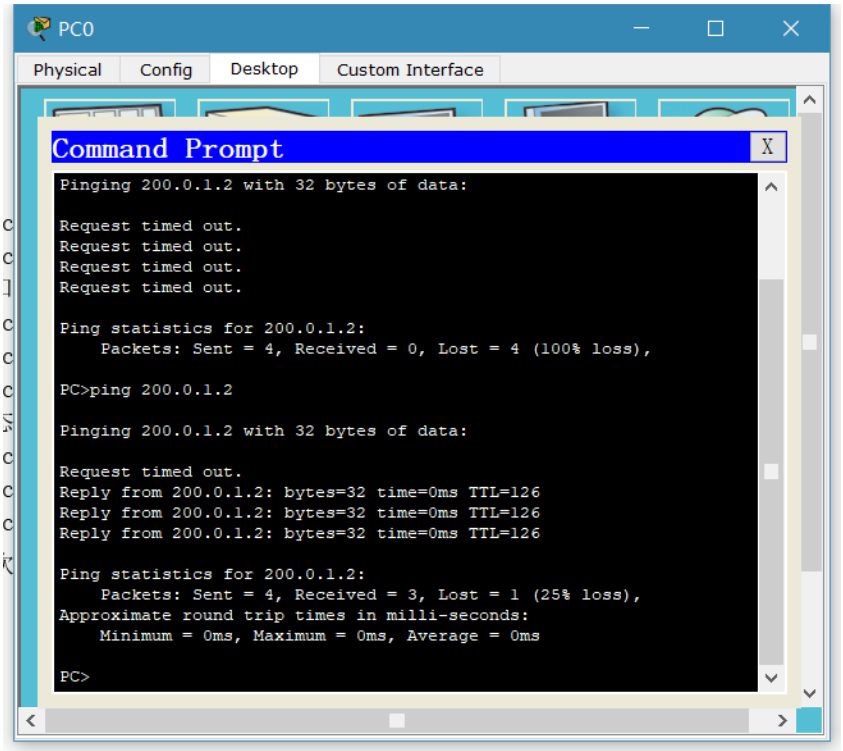


由于 icmp echo request 的源地址为私网 ip，公网路由器无法查询静态路由将 icmp echo reply 发回。

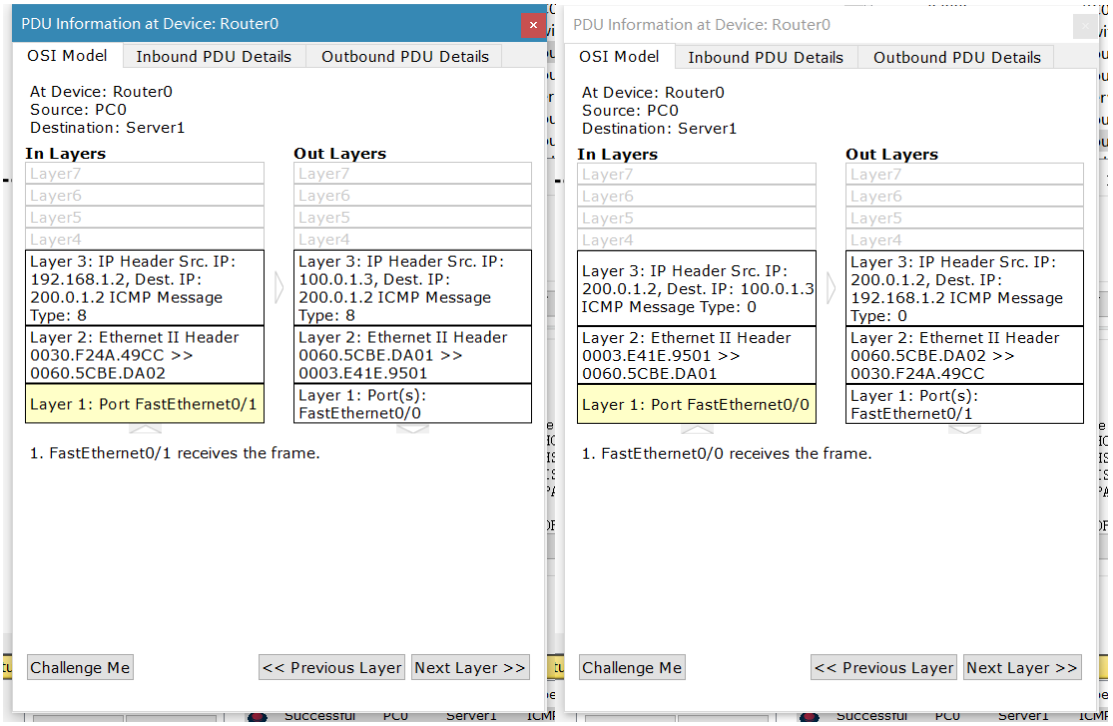
（1）在 Router0 配置静态 NAT：

左侧端口设置为内部：

```
Router(config)#int f0/1
Router(config-if)#ip nat inside
Router(config-if)#exit
```
右侧端口设置为外部：
```
Router(config)#int f0/0
Router(config-if)#ip nat outside
Router(config-if)#exit
```
配置静态 NAT：
```
Router(config)#ip nat inside source static 192.168.1.2 100.0.1.3
Router(config)#ip nat inside source static 192.168.1.3 100.0.1.4
Router(config)#ip nat inside source static 192.168.1.4 100.0.1.5
```
再次使用 PC0 ping Server1：



此时可以 ping 通。进行抓包分析：



可以看到，当数据经过 Router0 从私网到公网时，私网 ip 经过 NAT 转换为了公网 ip。而当数据经过 Router0 从公网到私网时，公网 ip 又被转换回了私网 ip。

（2）在 Router0 配置动态 NAT

首先清除原有静态 NAT：

Router(config)#no ip nat inside source static 192.168.1.2 100.0.1.3

Router(config)#no ip nat inside source static 192.168.1.3 100.0.1.4

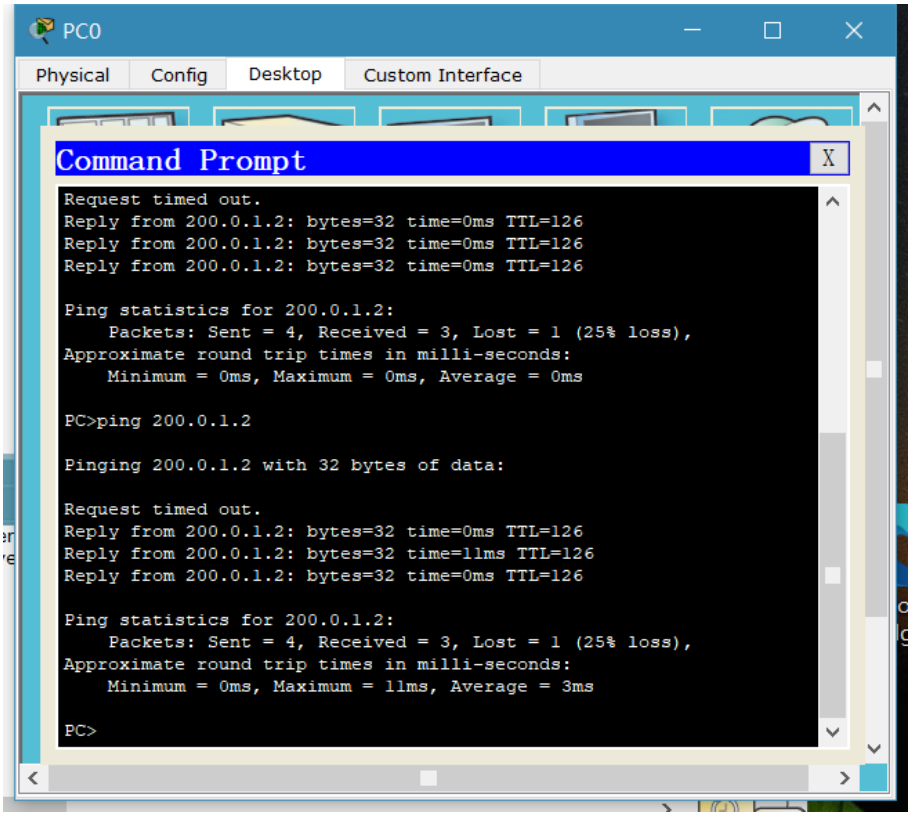
Router(config)#no ip nat inside source static 192.168.1.4 100.0.1.5

再配置动态 NAT：

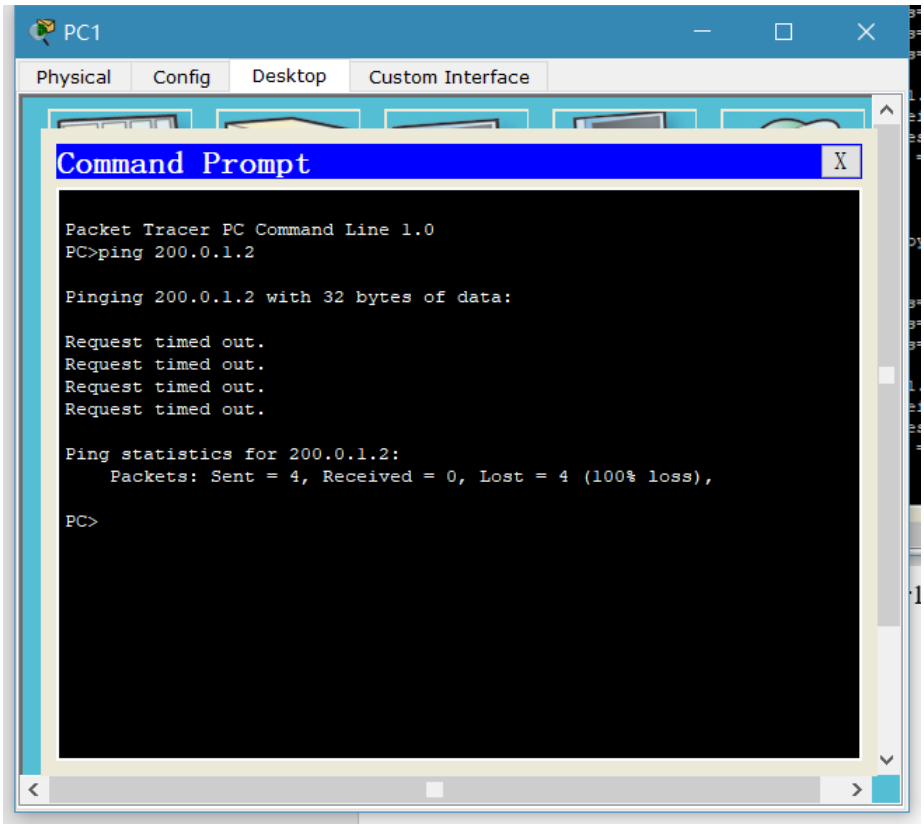
```
Router(config)#access-list 1 permit 192.168.1.0 0.0.0.255
Router(config)#ip nat pool todd 100.0.1.10 100.0.1.10 netmask 255.255.255.0
Router(config)#ip nat inside source list 1 pool todd
```

上述语句创建了公网地址池，含有一条地址 100.0.1.10。当访问外网时，会从池中随机分配一个公网 ip。

使用 PC0 ping Server1，仍可以 ping 通



此时再通过 PC1 ping Server1



无法 ping 通，这是因为公网 ip 池中的唯一一条 ip 已经被分配给了 PC0，没有多余公网 ip 可以使用。