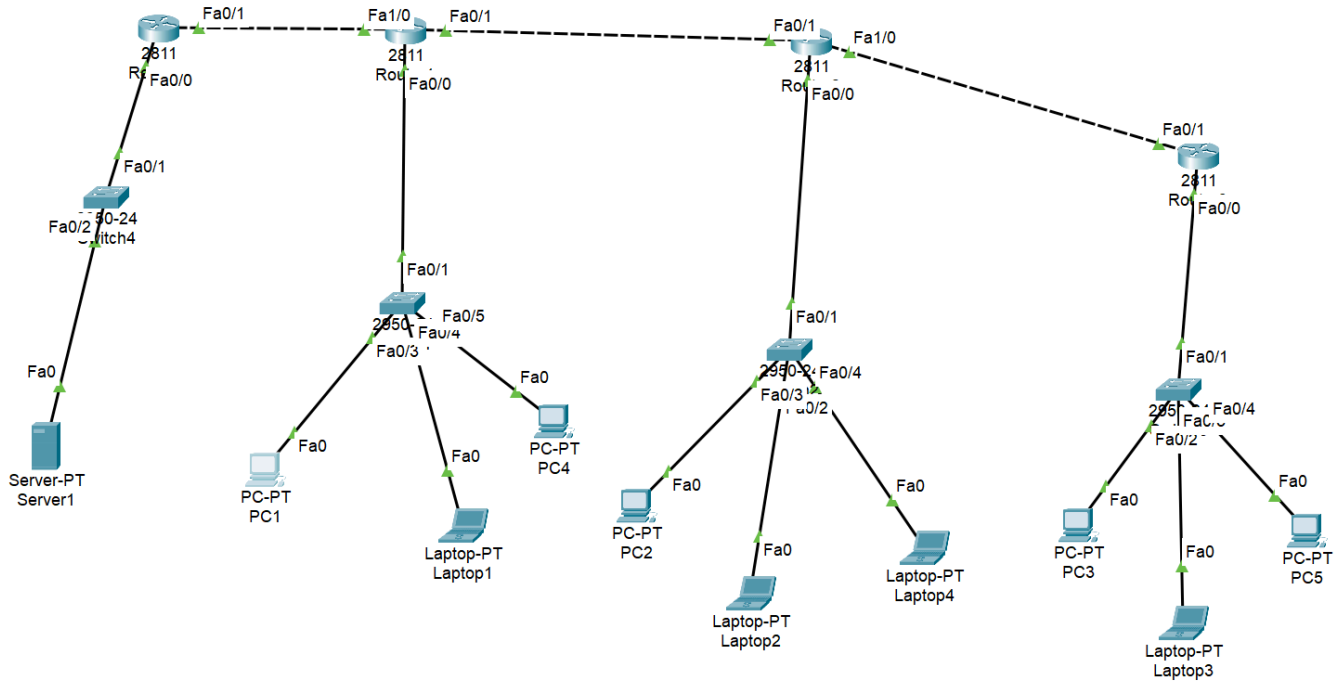
task6

网络拓扑图

网络拓扑图如下：



为了能够管理server1的通信权限，将其独立出来与新的router4相连。

设置server1地址为 `192.168.4.2`

ACL配置

对每个路由器的ACL配置如下

router1

（领导人相互通信）

```
access-list 101 permit ip host 192.168.2.3 host 192.168.1.2
access-list 101 permit ip host 192.168.3.2 host 192.168.1.2
```

（别的机构和本机构联络人的通信）
access-list 101 permit ip 192.168.2.0 0.0.0.255 host 192.168.1.4
access-list 101 permit ip 192.168.3.0 0.0.0.255 host 192.168.1.4

（别的机构联络人和本机构的相互通信）
access-list 101 permit ip host 192.168.2.2 192.168.1.0 0.0.0.255
access-list 101 permit ip host 192.168.3.3 192.168.1.0 0.0.0.255

（对于PC1，可以与server1通信）
access-list 101 permit ip host 192.168.4.2 host 192.168.1.2

router2

access-list 101 permit ip host 192.168.1.2 host 192.168.2.3
access-list 101 permit ip host 192.168.3.2 host 192.168.2.3
access-list 101 permit ip 192.168.1.0 0.0.0.255 host 192.168.2.2
access-list 101 permit ip 192.168.3.0 0.0.0.255 host 192.168.2.2
access-list 101 permit ip host 192.168.1.4 192.168.2.0 0.0.0.255
access-list 101 permit ip host 192.168.3.3 192.168.2.0 0.0.0.255

router3

access-list 101 permit ip host 192.168.1.2 host 192.168.3.2
access-list 101 permit ip host 192.168.2.3 host 192.168.3.2
access-list 101 permit ip 192.168.1.0 0.0.0.255 host 192.168.3.3
access-list 101 permit ip 192.168.2.0 0.0.0.255 host 192.168.3.3
access-list 101 permit ip host 192.168.1.4 192.168.3.0 0.0.0.255
access-list 101 permit ip host 192.168.2.2 192.168.3.0 0.0.0.255

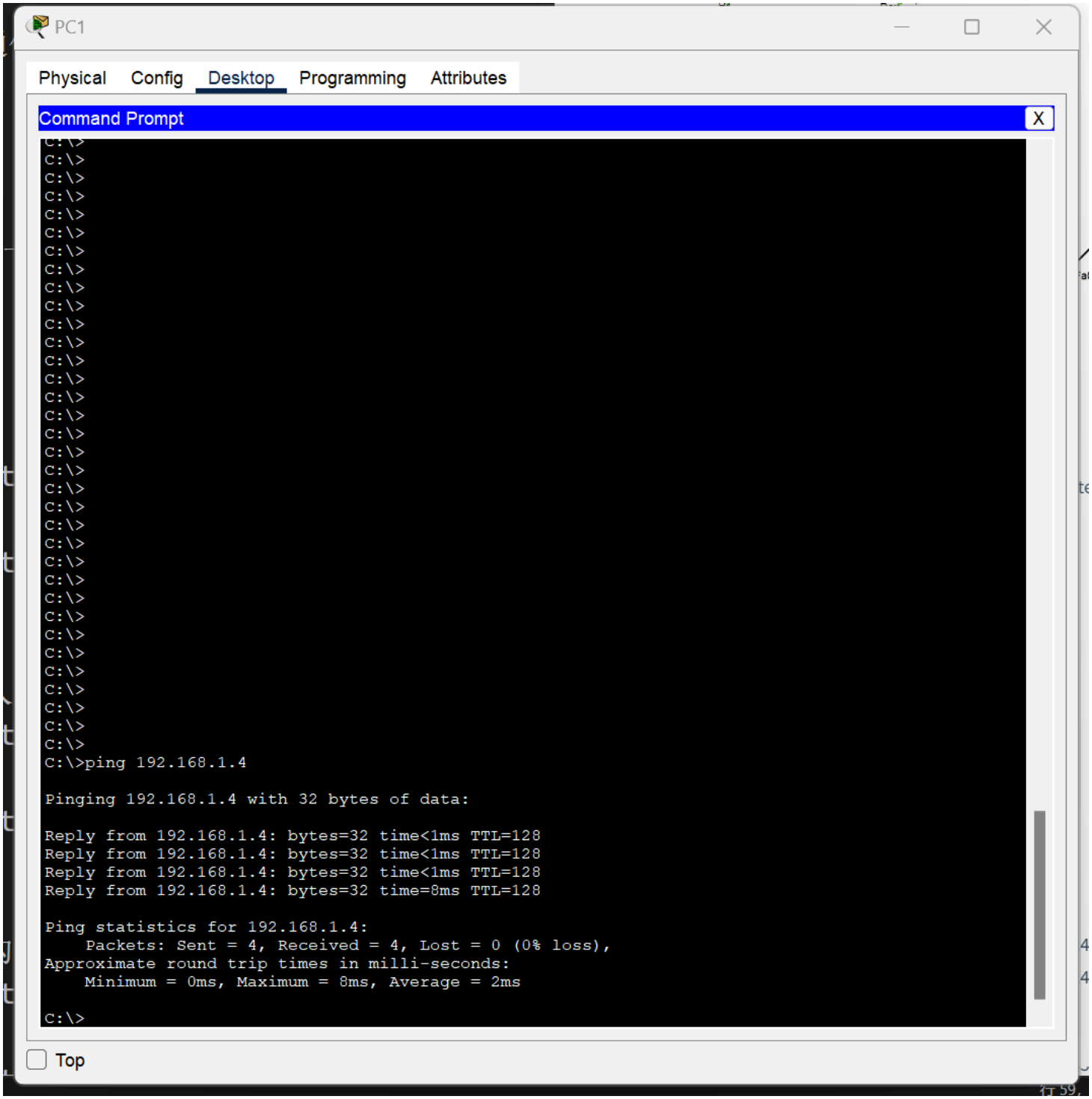
router4

access-list 101 permit ip host 192.168.1.2 host 192.168.4.2

测试

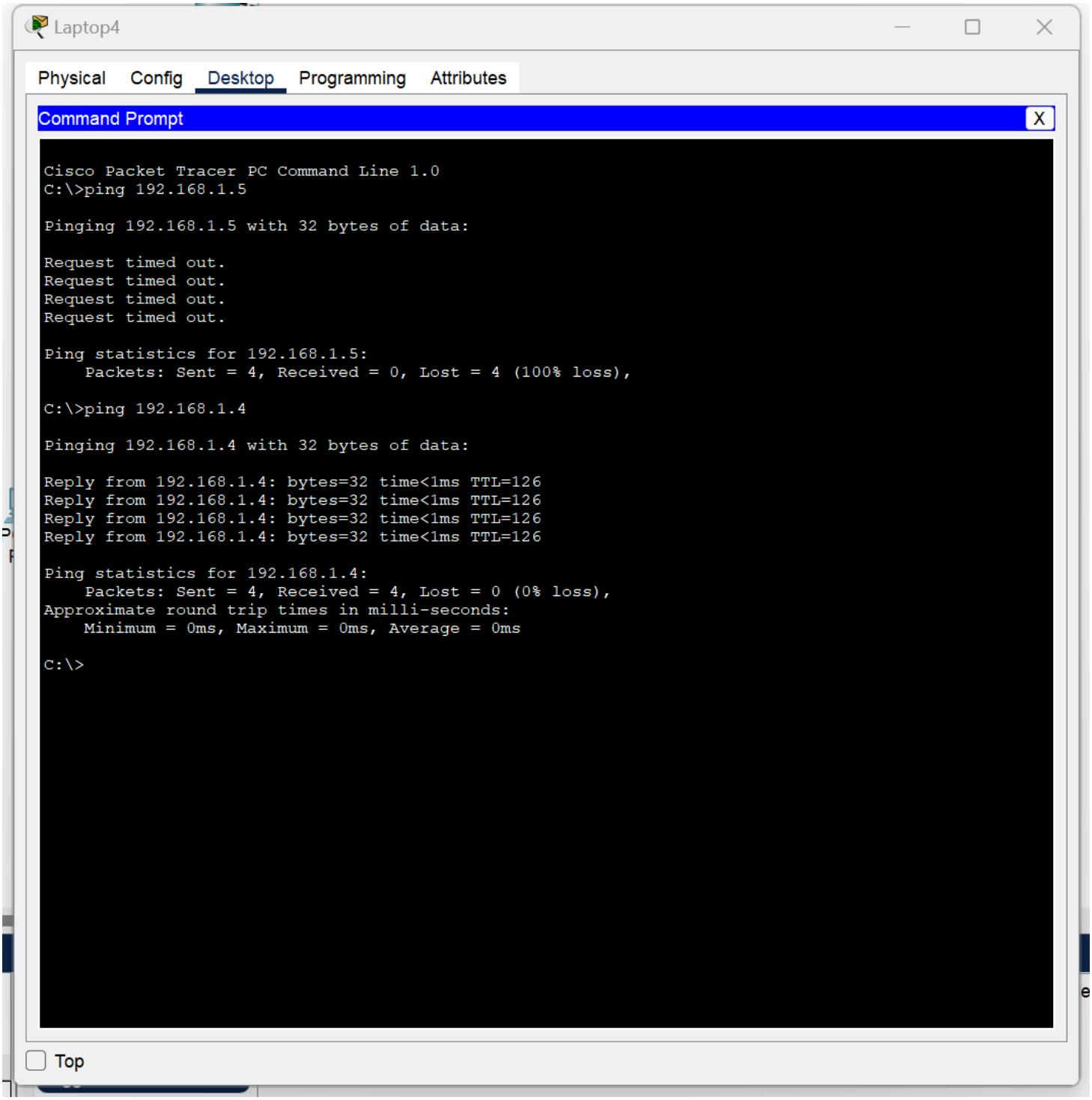
权力机构内部人员相互通信

权力机构内部可以通过switch通信，无需经过router。



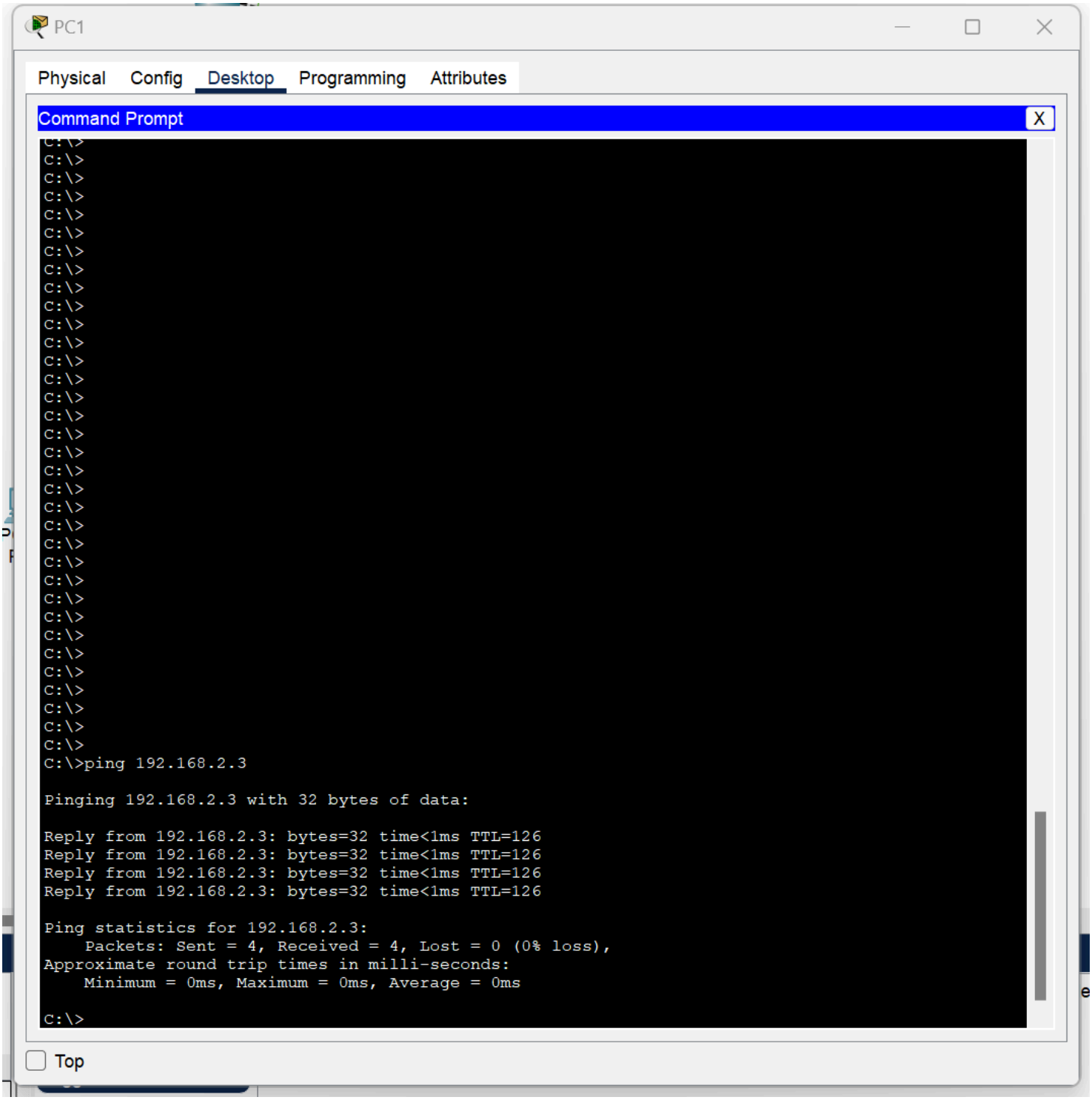
权力机构通过联络人的通信

不同的权力机构不能直接通信，但可以与联络人通信。



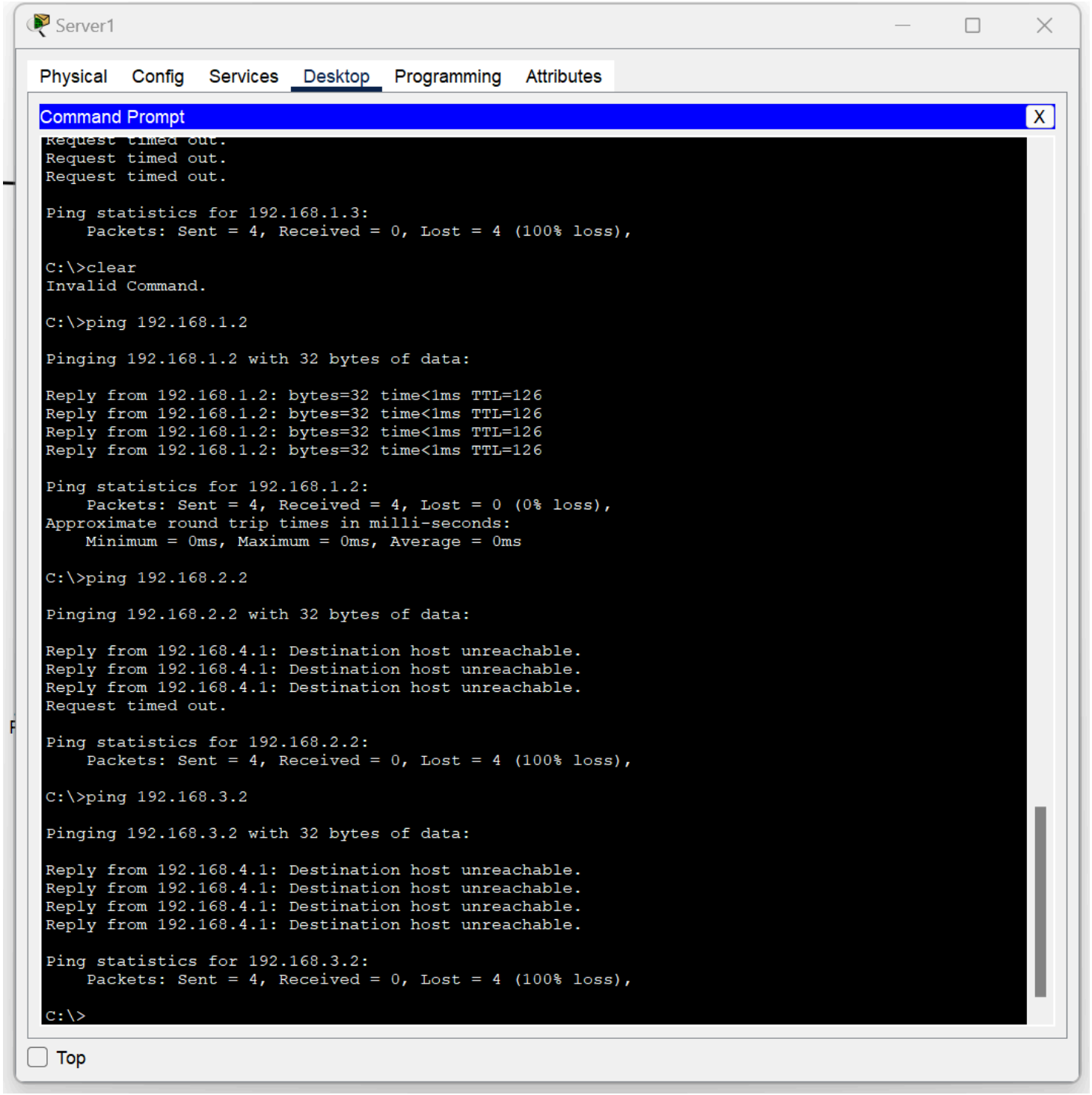
领导人相互通信

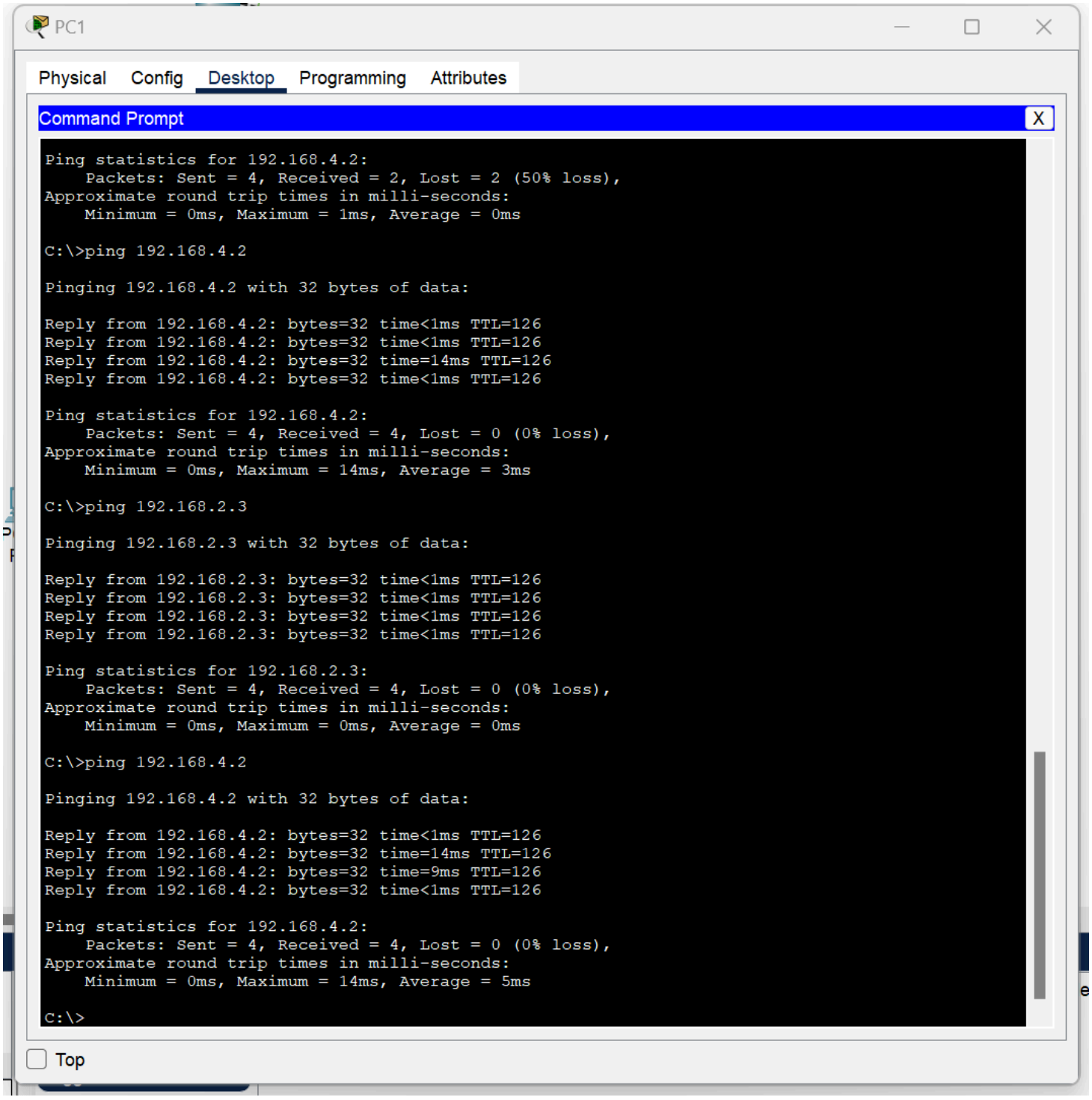
领导人可以相互通信。

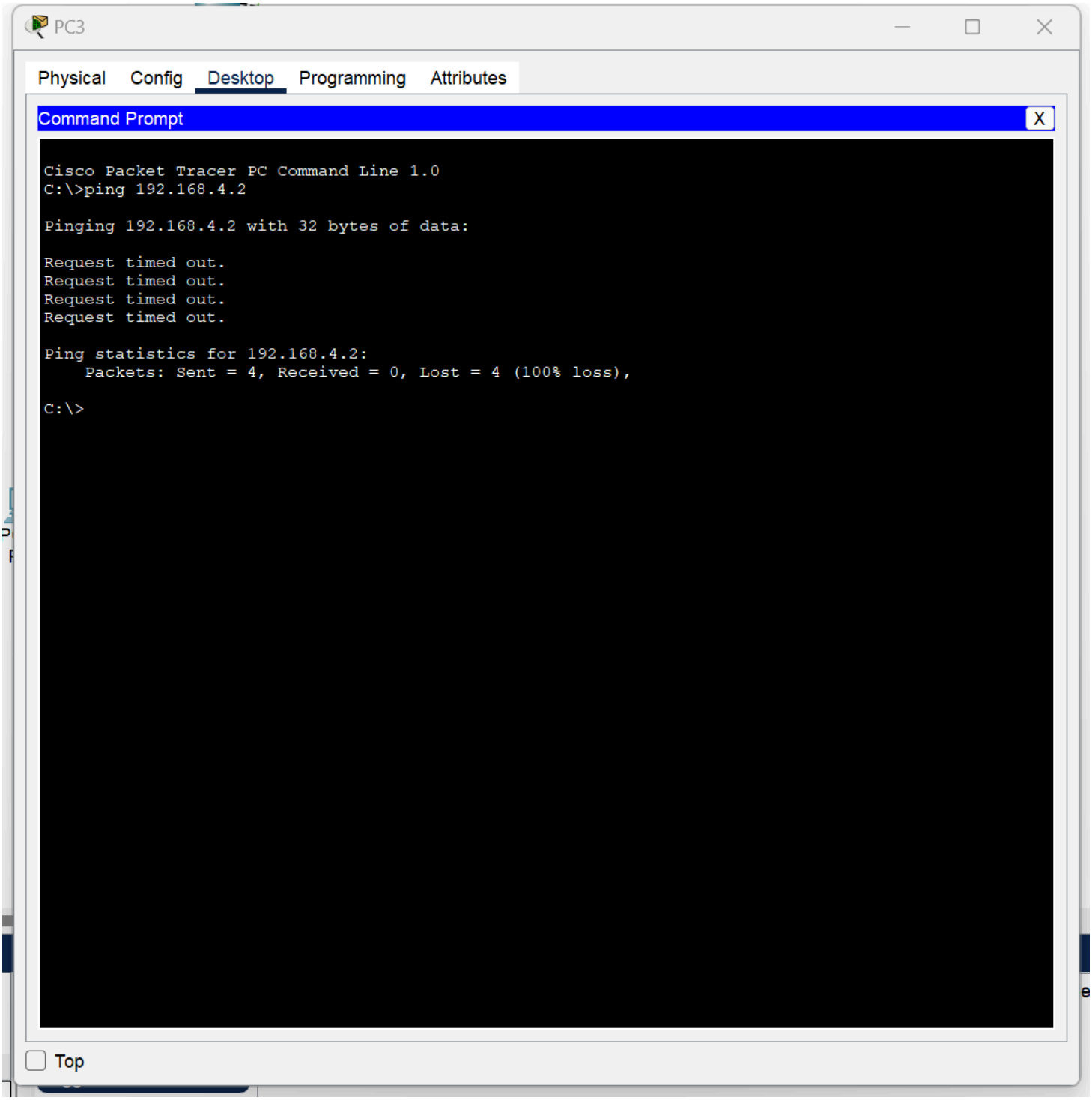


server1与PC1通信

server1只能与pc1通信，别的设备不能与server1通信。


Server1
Physical
Config
Services
Desktop
Programming
Attributes
Command Prompt
X
Request timed out.
Request timed out.
Request timed out.
Ping statistics for 192.168.1.3:
Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
C:\>clear
Invalid Command.
C:\>ping 192.168.1.2
Pinging 192.168.1.2 with 32 bytes of data:
Reply from 192.168.1.2: bytes=32 time<1ms TTL=126
Reply from 192.168.1.2: bytes=32 time<1ms TTL=126
Reply from 192.168.1.2: bytes=32 time<1ms TTL=126
Reply from 192.168.1.2: bytes=32 time<1ms TTL=126
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:\>ping 192.168.2.2
Pinging 192.168.2.2 with 32 bytes of data:
Reply from 192.168.4.1: Destination host unreachable.
Reply from 192.168.4.1: Destination host unreachable.
Reply from 192.168.4.1: Destination host unreachable.
Request timed out.
Ping statistics for 192.168.2.2:
Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
C:\>ping 192.168.3.2
Pinging 192.168.3.2 with 32 bytes of data:
Reply from 192.168.4.1: Destination host unreachable.
Reply from 192.168.4.1: Destination host unreachable.
Reply from 192.168.4.1: Destination host unreachable.
Reply from 192.168.4.1: Destination host unreachable.
Ping statistics for 192.168.3.2:
Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
C:\>
Top


PC1
Physical
Config
Desktop
Programming
Attributes
Command Prompt
X
Ping statistics for 192.168.4.2:
Packets: Sent = 4, Received = 2, Lost = 2 (50% loss),
Approximate round trip times in milli-seconds:
Minimum = 0ms, Maximum = 1ms, Average = 0ms
C:\>ping 192.168.4.2
Pinging 192.168.4.2 with 32 bytes of data:
Reply from 192.168.4.2: bytes=32 time<1ms TTL=126
Reply from 192.168.4.2: bytes=32 time<1ms TTL=126
Reply from 192.168.4.2: bytes=32 time=14ms TTL=126
Reply from 192.168.4.2: bytes=32 time<1ms TTL=126
Ping statistics for 192.168.4.2:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 0ms, Maximum = 14ms, Average = 3ms
C:\>ping 192.168.2.3
Pinging 192.168.2.3 with 32 bytes of data:
Reply from 192.168.2.3: bytes=32 time<1ms TTL=126
Reply from 192.168.2.3: bytes=32 time<1ms TTL=126
Reply from 192.168.2.3: bytes=32 time<1ms TTL=126
Reply from 192.168.2.3: bytes=32 time<1ms TTL=126
Ping statistics for 192.168.2.3:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 0ms, Maximum = 0ms, Average = 0ms
C:\>ping 192.168.4.2
Pinging 192.168.4.2 with 32 bytes of data:
Reply from 192.168.4.2: bytes=32 time<1ms TTL=126
Reply from 192.168.4.2: bytes=32 time=14ms TTL=126
Reply from 192.168.4.2: bytes=32 time=9ms TTL=126
Reply from 192.168.4.2: bytes=32 time<1ms TTL=126
Ping statistics for 192.168.4.2:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 0ms, Maximum = 14ms, Average = 5ms
C:\>
Top



task7

需要在router1,router2,router3相应端口放行对应的icmp流量

router1

在in方向设置，保证ping的流量能发出去

access-list 102 permit icmp host 192.168.1.2 192.168.0.0 0.0.255.255
ip inspect name ICMP icmp
int fastEthernet 0/0
ip inspect ICMP in

router2

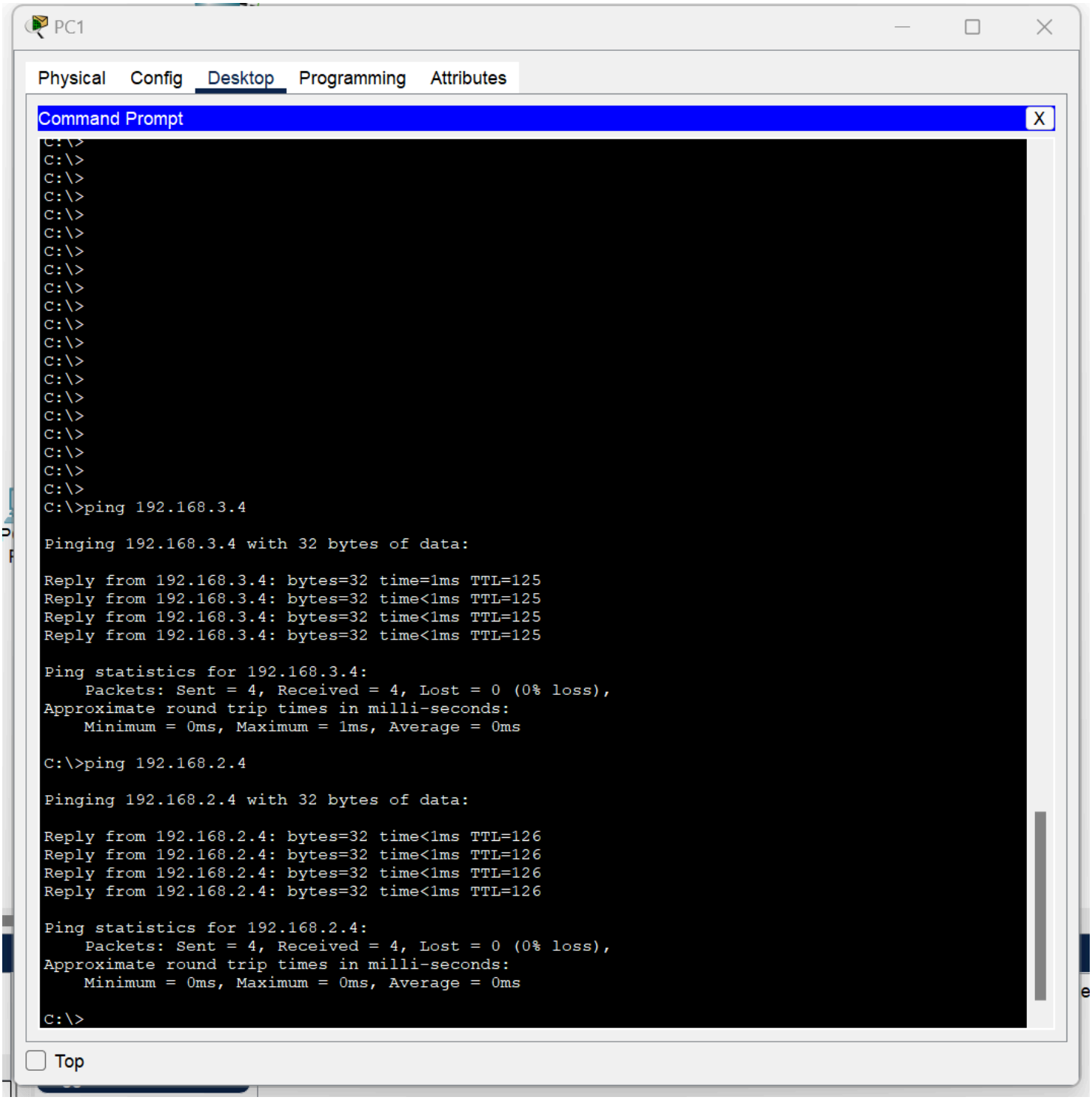
在out方向设置

access-list 101 permit icmp host 192.168.1.2 192.168.2.0 0.0.0.255
ip inspect name ICMP icmp
int fastEthernet 0/0
ip inspect ICMP out

router3

access-list 101 permit icmp host 192.168.1.2 192.168.3.0 0.0.0.255
ip inspect name ICMP icmp
int fastEthernet 0/0
ip inspect ICMP out

pc1可以ping通其他设备，但是laptop4不能ping通pc1。



task8

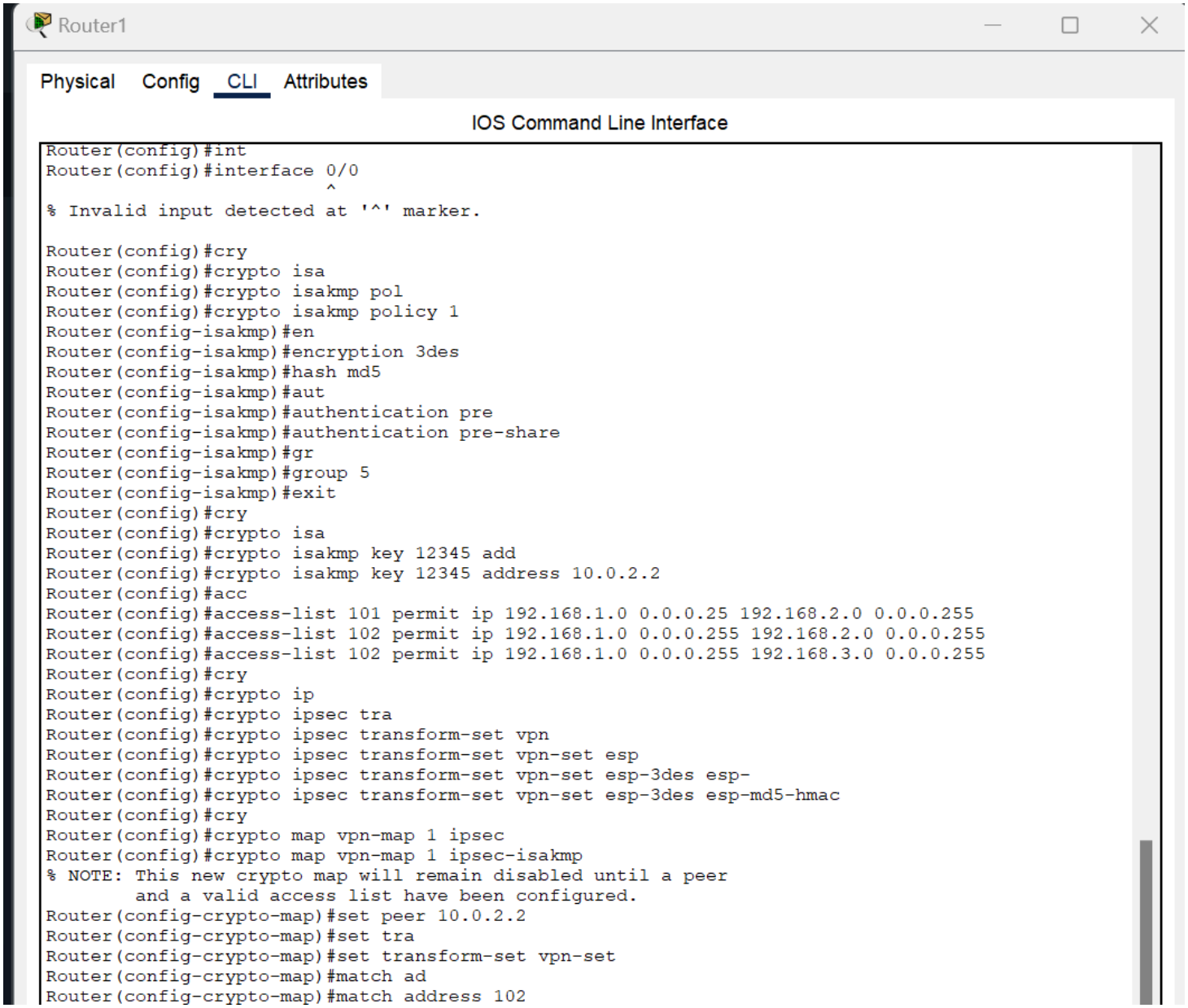
不能通信原因

静态路由只能配置内网以及内网外网边界上的路由，在不更改公网路由器的条件下，公网路由器并不识别内网的IP，因而无法转发。

配置

router1

```
configure terminal
interface FastEthernet0/1
（创建 ISAKMP 策略）
crypto isakmp policy 1
（设置加密算法）
encryption 3des
（设置哈希算法）
hash md5
（设置身份验证方法）
authentication pre-share
（设置 DH 组）
group 5
exit
（配置预共享密钥）
crypto isakmp key 12345 address 2.0.0.2
（配置访问控制列表）
access-list 102 permit ip 192.168.1.0 0.0.0.255 192.168.2.0 0.0.0.255
access-list 102 permit ip 192.168.1.0 0.0.0.255 192.168.3.0 0.0.0.255
（创建 IPsec 转换集）
crypto ipsec transform-set vpn-set esp-3des esp-md5-hmac
（创建加密映射）
crypto map vpn-map 1 ipsec-isakmp
（设置对等体）
set peer 2.0.0.2
（设置转换集）
set transform-set vpn-set
（匹配访问控制列表）
match address 102
exit
ip route 192.168.2.0 255.255.255.0 1.0.0.1
ip route 192.168.3.0 255.255.255.0 1.0.0.1
interface FastEthernet0/1
（应用加密映射到接口）
crypto map vpn-map
```



同时，设置rip路由为1.0.0.0和192.168.0.0

rouetr2

类似router1，修改部分路径即可

configure terminal
interface FastEthernet0/1
crypto isakmp policy 1
encryption 3des
hash md5
authentication pre-share
group 5
exit

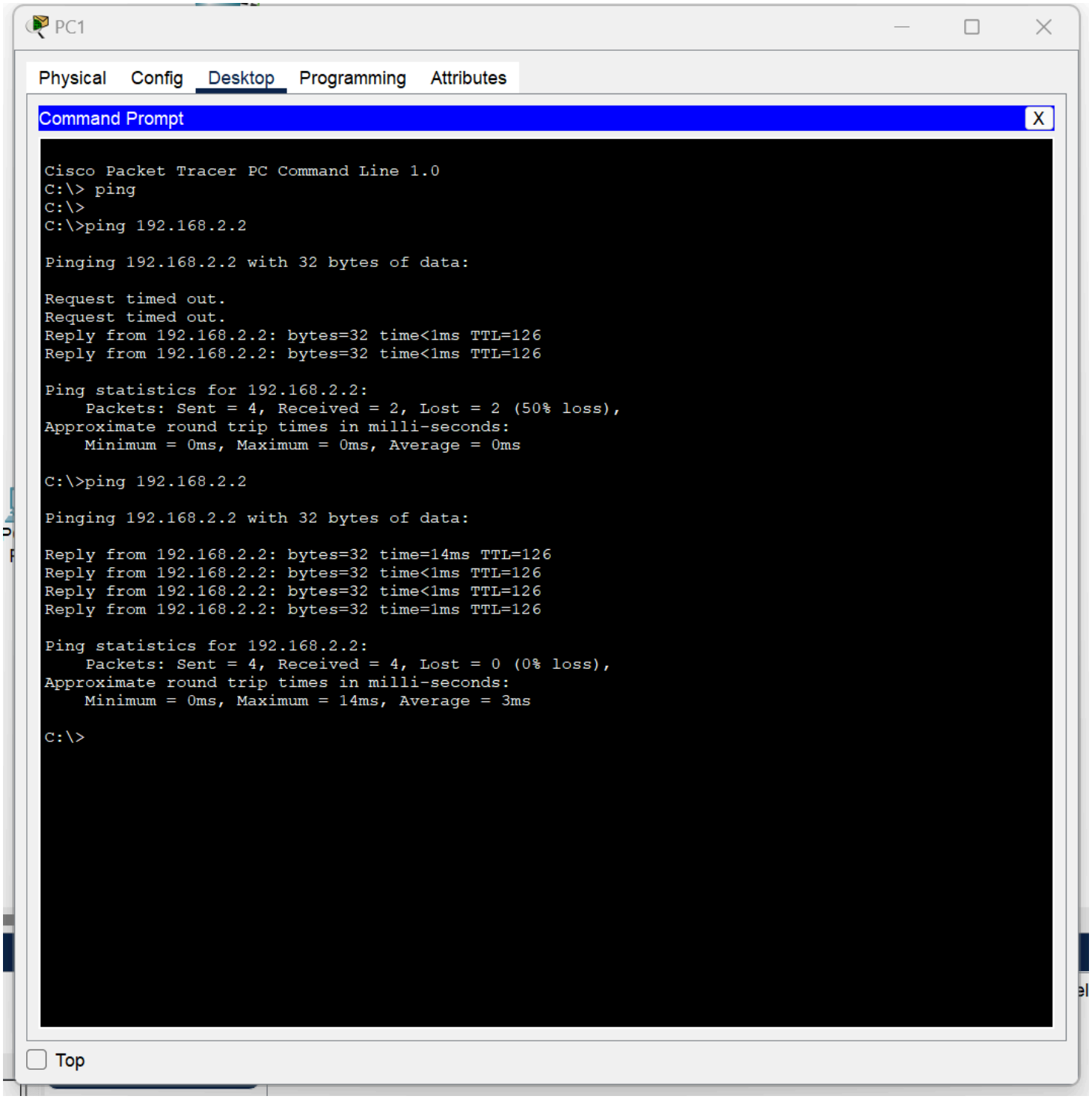
crypto isakmp key 12345 address 1.0.0.2
access-list 102 permit ip 192.168.2.0 0.0.0.255 192.168.1.0 0.0.0.255
access-list 102 permit ip 192.168.2.0 0.0.0.255 192.168.3.0 0.0.0.255
access-list 102 permit ip 192.168.3.0 0.0.0.255 192.168.1.0 0.0.0.255
access-list 102 permit ip 192.168.3.0 0.0.0.255 192.168.2.0 0.0.0.255
crypto ipsec transform-set vpn-set esp-3des esp-md5-hmac
crypto map vpn-map 1 ipsec-isakmp
set peer 1.0.0.2
set transform-set vpn-set
match address 102
exit
ip route 192.168.1.0 255.255.255.0 2.0.0.1
ip route 192.168.3.0 255.255.255.0 2.0.0.1
interface FastEthernet0/1
crypto map vpn-map

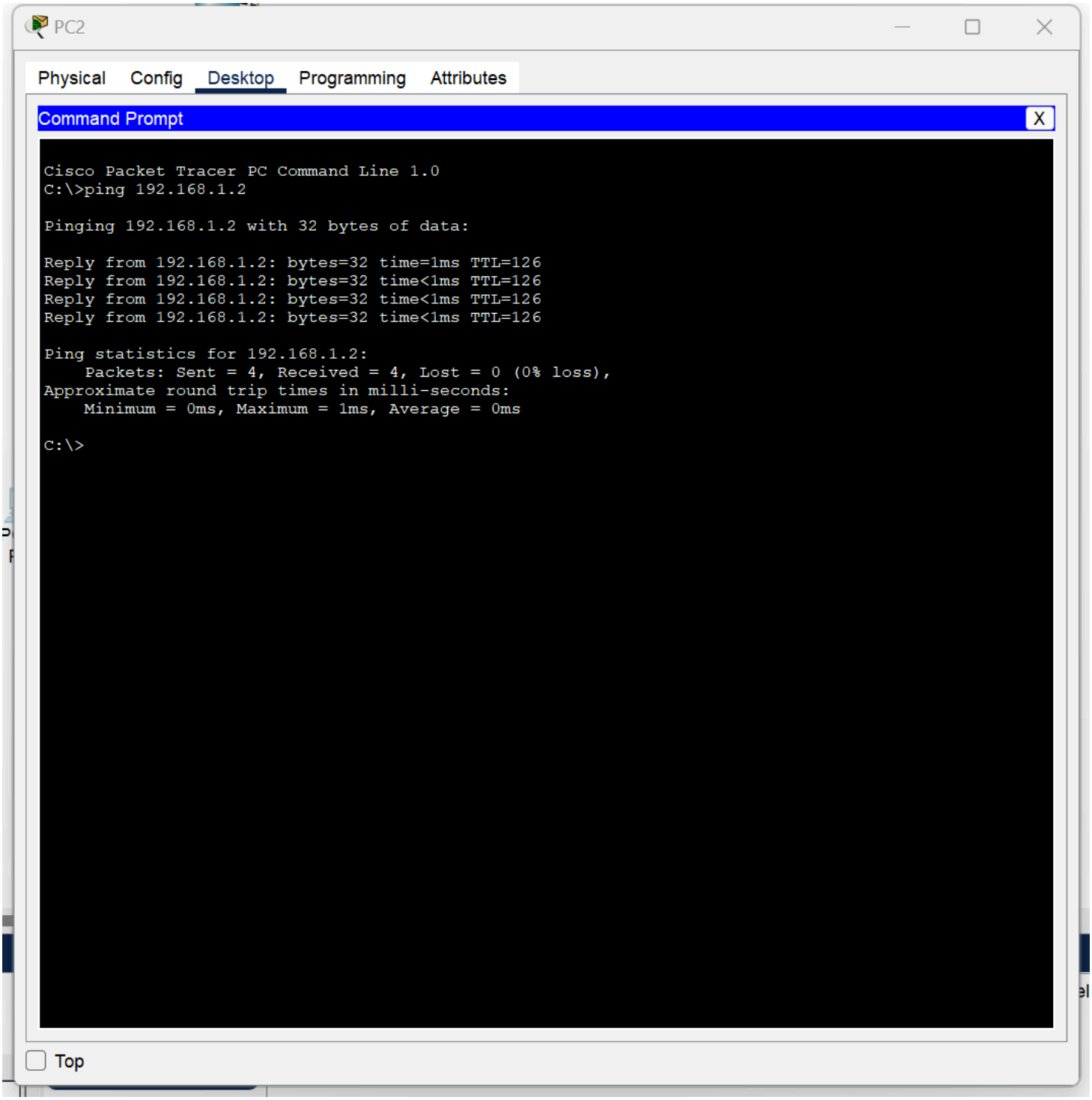
rip路由为2.0.0.0和192.168.0.0

router4

只需设置rip路由为1.0.0.0和2.0.0.0即可

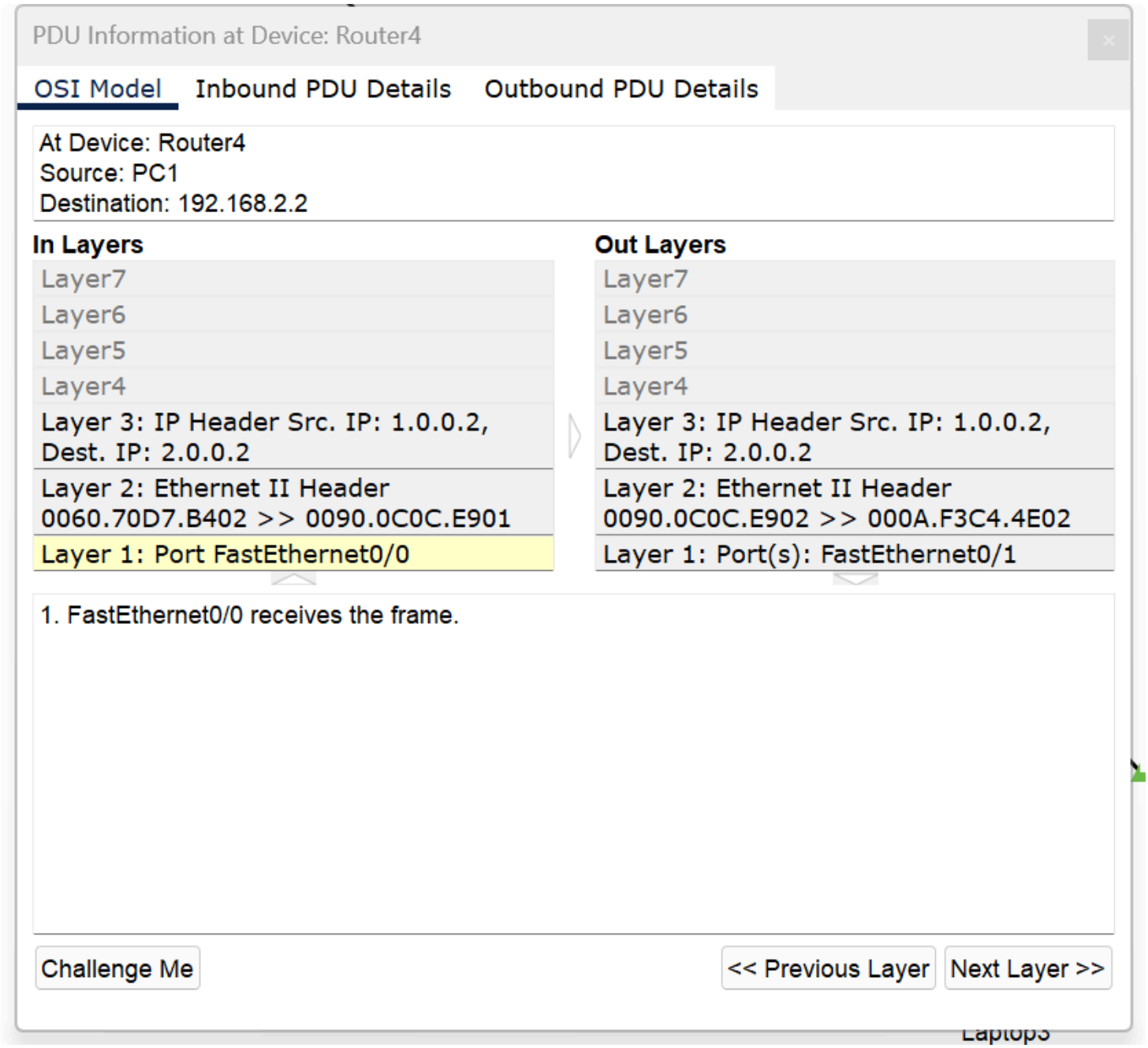
验证PC1(192.168.1.2)和PC2(192.168.2.2)


PC1
Physical
Config
Desktop
Programming
Attributes
Command Prompt
X
Cisco Packet Tracer PC Command Line 1.0
C:\> ping
C:\>
C:\>ping 192.168.2.2
Pinging 192.168.2.2 with 32 bytes of data:
Request timed out.
Request timed out.
Reply from 192.168.2.2: bytes=32 time<1ms TTL=126
Reply from 192.168.2.2: bytes=32 time<1ms TTL=126
Ping statistics for 192.168.2.2:
Packets: Sent = 4, Received = 2, Lost = 2 (50% loss),
Approximate round trip times in milli-seconds:
Minimum = 0ms, Maximum = 0ms, Average = 0ms
C:\>ping 192.168.2.2
Pinging 192.168.2.2 with 32 bytes of data:
Reply from 192.168.2.2: bytes=32 time=14ms TTL=126
Reply from 192.168.2.2: bytes=32 time<1ms TTL=126
Reply from 192.168.2.2: bytes=32 time<1ms TTL=126
Reply from 192.168.2.2: bytes=32 time=1ms TTL=126
Ping statistics for 192.168.2.2:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 0ms, Maximum = 14ms, Average = 3ms
C:\>
Top



如果要ping通PC3，在对应router配置路由即可。

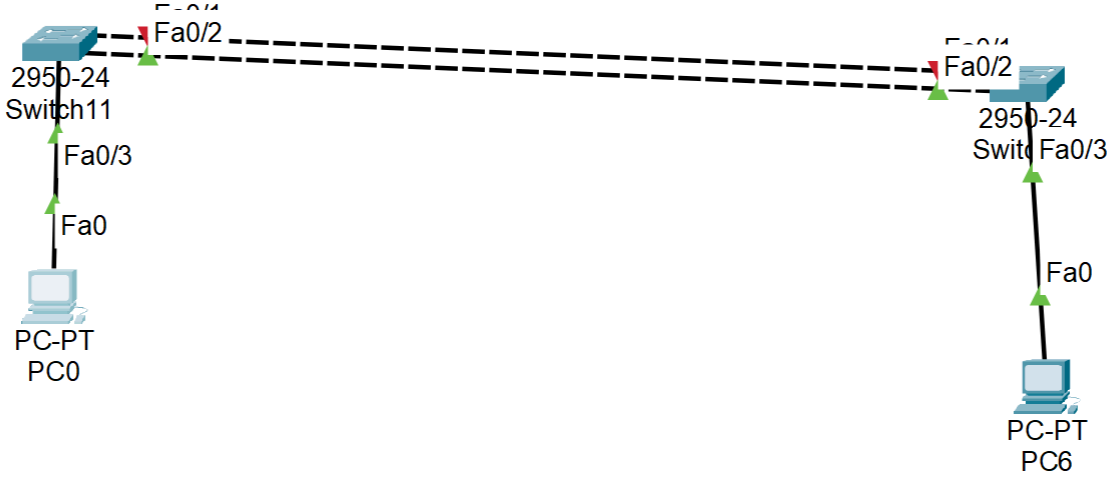
仿真抓包分析



在router4处抓包分析，可见ICMP包的目的地址和源地址都被修改成了公网ip，在router1和router2处恢复为内网ip，所以使用的是隧道模式。传输模式并不会修改ip地址。

bonus switch端口聚合

网络拓扑如下



PC0地址192.168.10.1

PC1地址192.168.10.2

switch 11

interface range f0/1-2

（设置端口模式为trunk）

Switchport mode trunk

（加入链路组1并开启）

channel-group 1 mode on

exit

（进入该聚合端口配置模式）

int port-channel 1

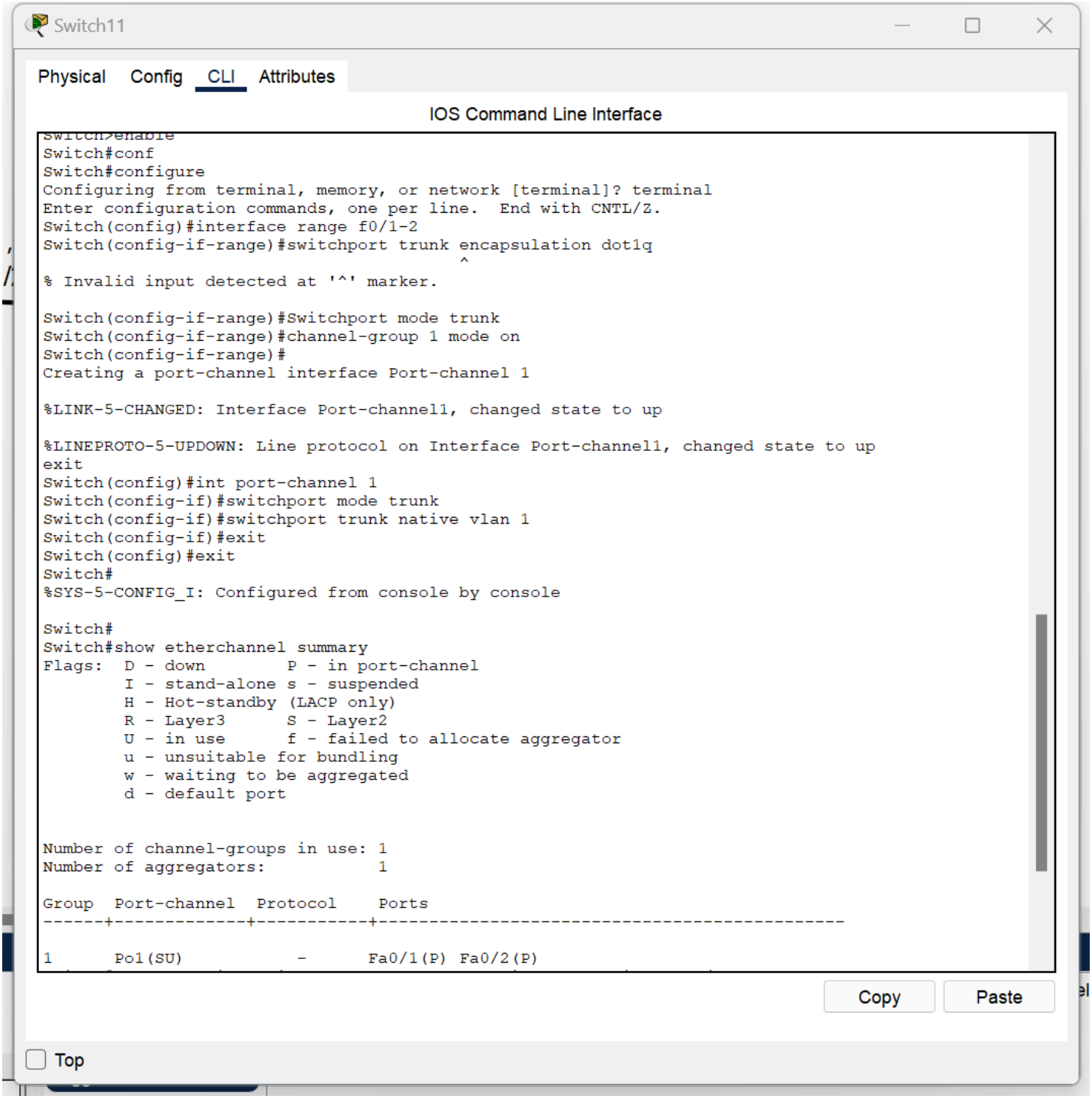
（设置该聚合端口为trunk模式）

switchport mode trunk

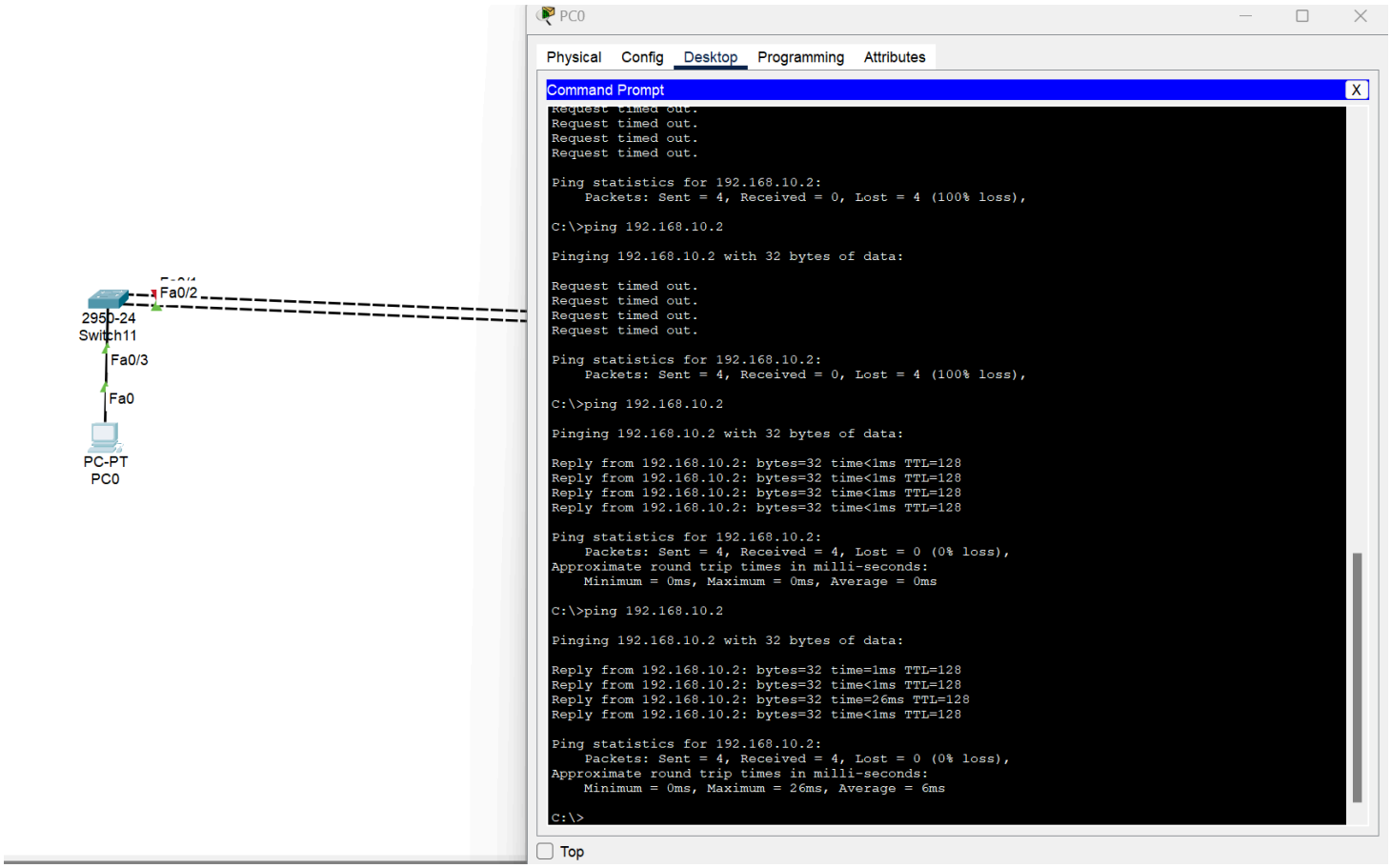
（设置缺省VLAN为1）

switchport trunk native vlan 1

对另一个switch配置是一样的



最终，关闭两个switch的f0/1，依然能ping通


Fa0/2
2950-24
Switch11
Fa0/3
Fa0
PC-PT
PC0
PC0
Physical
Config
Desktop
Programming
Attributes
Command Prompt
X
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Ping statistics for 192.168.10.2:
Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
C:\>ping 192.168.10.2
Pinging 192.168.10.2 with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Ping statistics for 192.168.10.2:
Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
C:\>ping 192.168.10.2
Pinging 192.168.10.2 with 32 bytes of data:
Reply from 192.168.10.2: bytes=32 time<1ms TTL=128
Reply from 192.168.10.2: bytes=32 time<1ms TTL=128
Reply from 192.168.10.2: bytes=32 time<1ms TTL=128
Reply from 192.168.10.2: bytes=32 time<1ms TTL=128
Ping statistics for 192.168.10.2:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 0ms, Maximum = 0ms, Average = 0ms
C:\>ping 192.168.10.2
Pinging 192.168.10.2 with 32 bytes of data:
Reply from 192.168.10.2: bytes=32 time=1ms TTL=128
Reply from 192.168.10.2: bytes=32 time<1ms TTL=128
Reply from 192.168.10.2: bytes=32 time=26ms TTL=128
Reply from 192.168.10.2: bytes=32 time<1ms TTL=128
Ping statistics for 192.168.10.2:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 0ms, Maximum = 26ms, Average = 6ms
C:\>
Top