

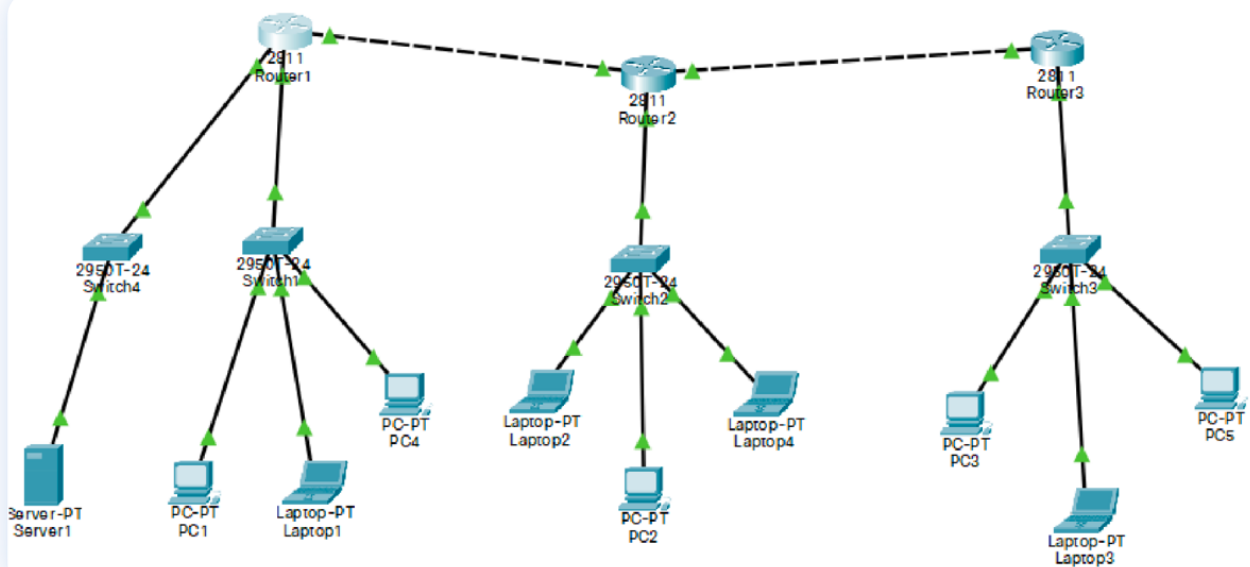
第二次实验

任务 6

过程概述

针对安全要求，对应的解决方案分别为：

1. 各权力机构内部的所有成员位于一个子网中，通过交换机实现相互通信；
2. 在每个路由器与该子网接口的入口方向设置访问控制列表（101），只允许目的 IP 为该权力机构联络人的包进入子网，绑定在 out 上；
3. ACL101 中允许来自领导人 IP，目的 IP 为该权力机构领导人的包；
4. 新建一个子网 192.168.4.1/24，添加一台交换机进行访问控制。设置 Server1 IP 为 192.168.4.2，对应的 ACL102 只允许 IP 为 192.168.1.2 且目的 IP 为 192.168.4.2 的包进入子网，并且只允许 IP 为 192.168.4.2 且目的 IP 为 192.168.1.2 的包传出子网。



终端设备的使用情况如下表所示：

设备名称	使用人	部门	备注	
PC1	凯撒/你	元老院	领导人	192.168.1.2
Server1	你	元老院	机密管理	192.168.4.2
Laptop1	布鲁图	元老院	联络人	192.168.1.4
PC4	财务官 A	元老院	---	192.168.1.5
Laptop2	庞培	执政官首府	领导人	192.168.2.3
PC2	卡西乌斯	执政官首府	联络人	192.168.2.2
Laptop4	辅助执政官 B	执政官首府		192.168.2.4
PC3	克拉苏	部族会议所	领导人	192.168.3.2
Laptop3	安东尼	部族会议所	联络人	192.168.3.3
PC5	大祭司 C	部族会议所	---	192.168.3.4

设置访问控制列表：

- Router1:

```
access 101 permit ip 192.168.2.0 0.0.0.255 host 192.168.1.4
access 101 permit ip 192.168.3.0 0.0.0.255 host 192.168.1.4
access 101 permit ip host 192.168.2.2 192.168.1.0 0.0.0.255
access 101 permit ip host 192.168.3.3 192.168.1.0 0.0.0.255

access 101 permit ip host 192.168.2.3 host 192.168.1.2
access 101 permit ip host 192.168.3.2 host 192.168.1.2

access 101 permit ip host 192.168.4.2 host 192.168.1.2

interface FastEthernet0/0
ip access-group 101 out

access 102 permit ip host 192.168.1.2 host 192.168.4.2
access 102 permit ip host 192.168.4.2 host 192.168.1.2

interface FastEthernet1/0
ip access-group 102 out
ip access-group 102 in
```

- Router2:

```
access 101 permit ip 192.168.1.0 0.0.0.255 host 192.168.2.2
access 101 permit ip 192.168.3.0 0.0.0.255 host 192.168.2.2
access 101 permit ip host 192.168.1.4 192.168.2.0 0.0.0.255
access 101 permit ip host 192.168.3.3 192.168.2.0 0.0.0.255

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

```
interface FastEthernet0/1
ip access-group 102 out
```

- Router3:

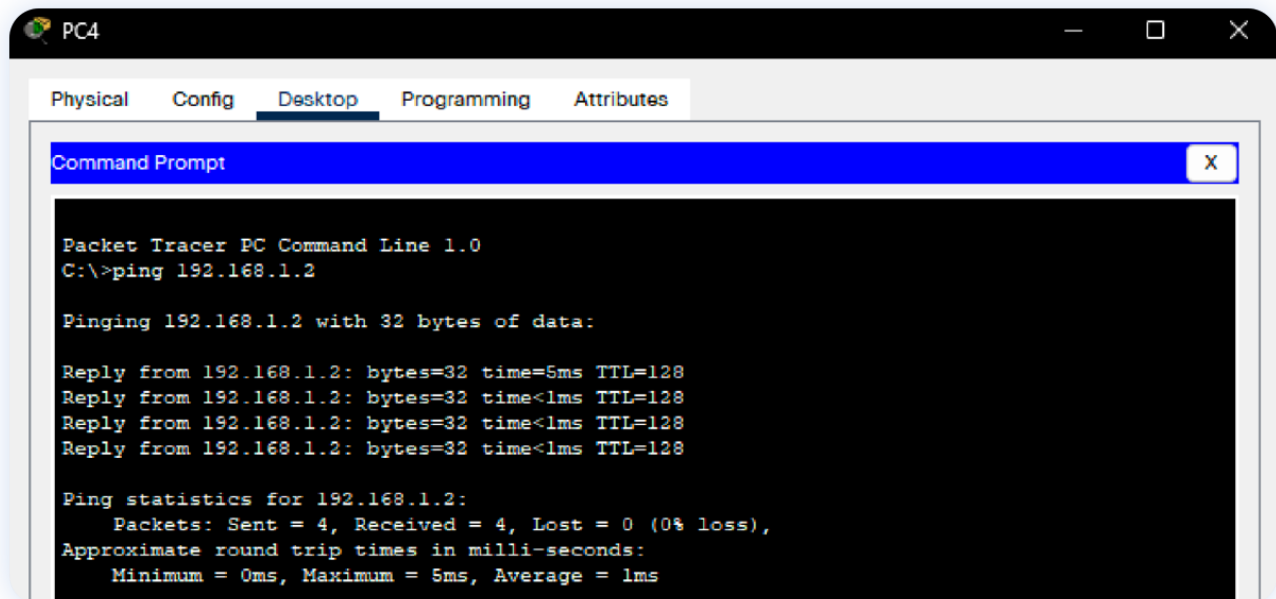
```
access 101 permit ip 192.168.1.0 0.0.0.255 host 192.168.3.3
access 101 permit ip 192.168.2.0 0.0.0.255 host 192.168.3.3
access 101 permit ip host 192.168.1.4 192.168.3.0 0.0.0.255
access 101 permit ip host 192.168.2.2 192.168.3.0 0.0.0.255

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

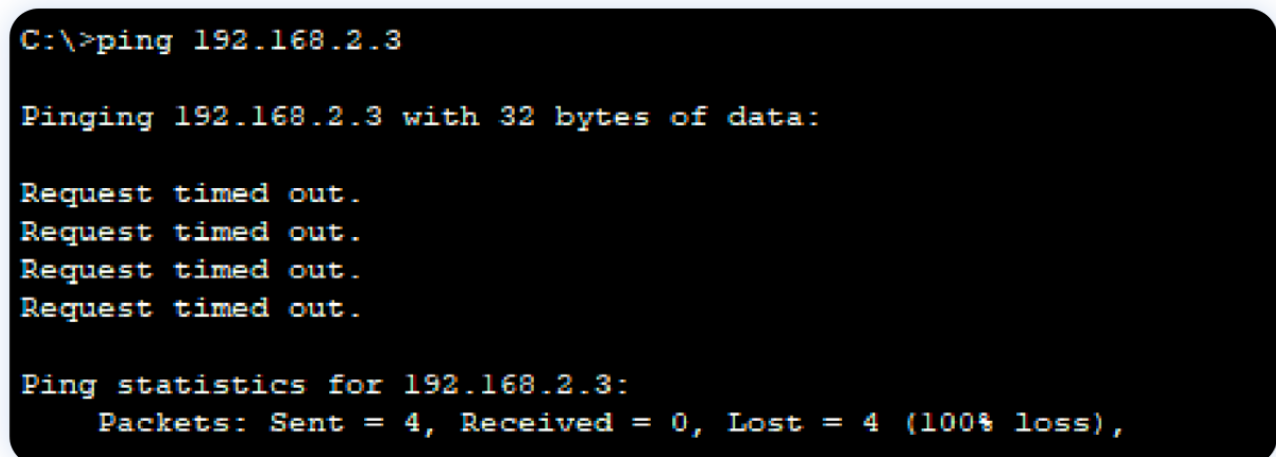
```
interface FastEthernet0/1
ip access-group 101 out
```

测试效果

内部成员间可以通信: PC4 -> PC1



权力机构间的通信：PC4 -> Laptop2 不能通信



权力机构间的通信：PC4 -> PC2 能通信

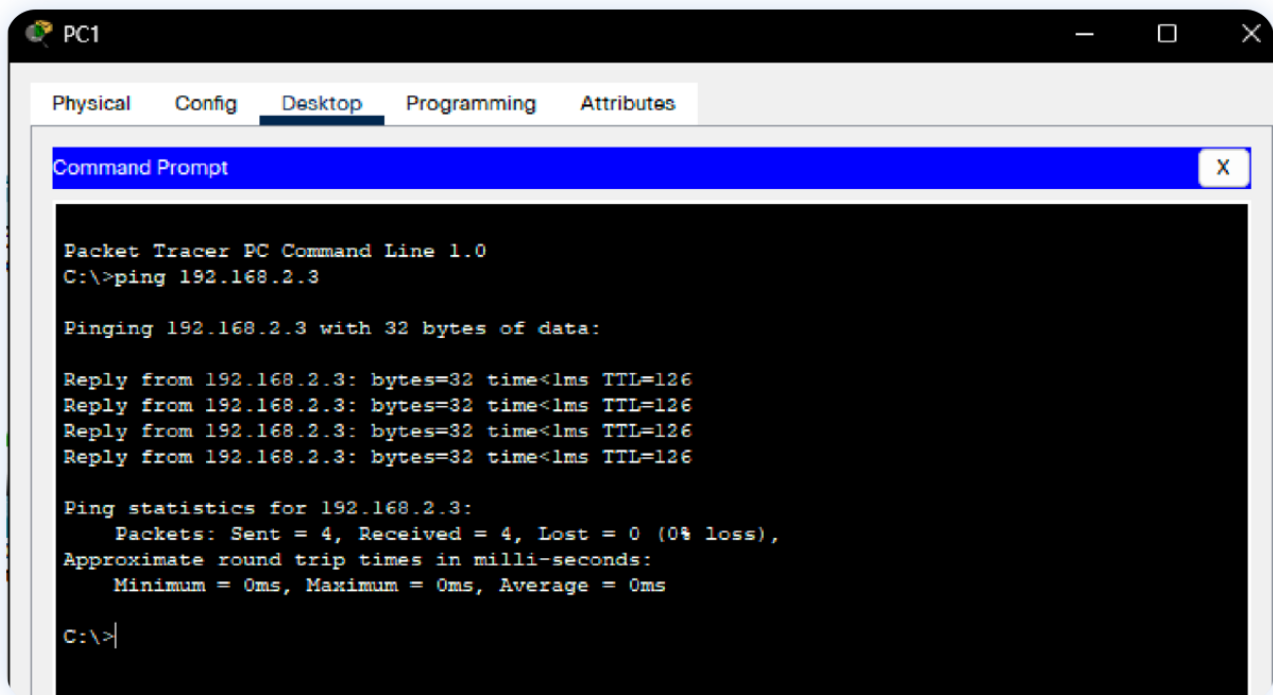
```
C:\>ping 192.168.2.2

Pinging 192.168.2.2 with 32 bytes of data:

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
Reply from 192.168.2.2: bytes=32 time=1ms TTL=126

Ping statistics for 192.168.2.2:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 1ms, Average = 0ms
```

联络人通信：PC1 -> Laptop2 能通信：



Server1 通信：凯撒PC1 -> Server1 可以通信

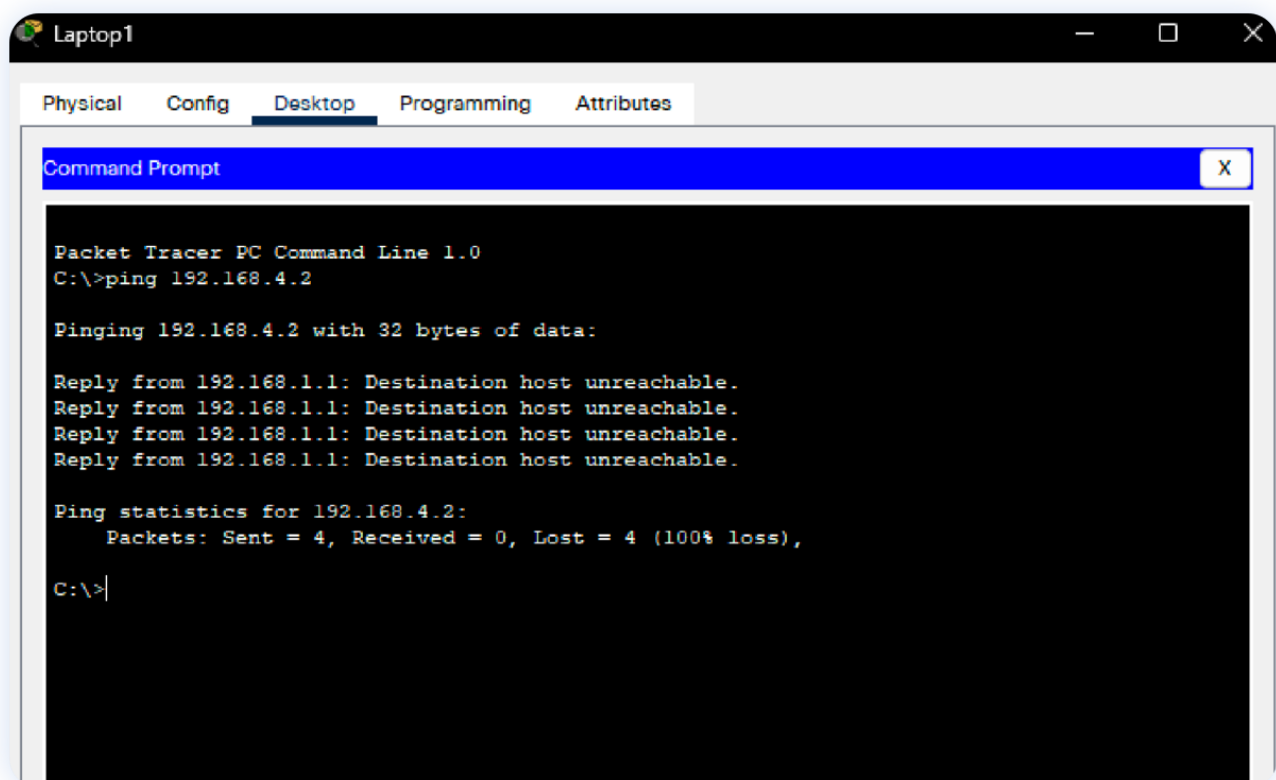
```
C:\>ping 192.168.4.2

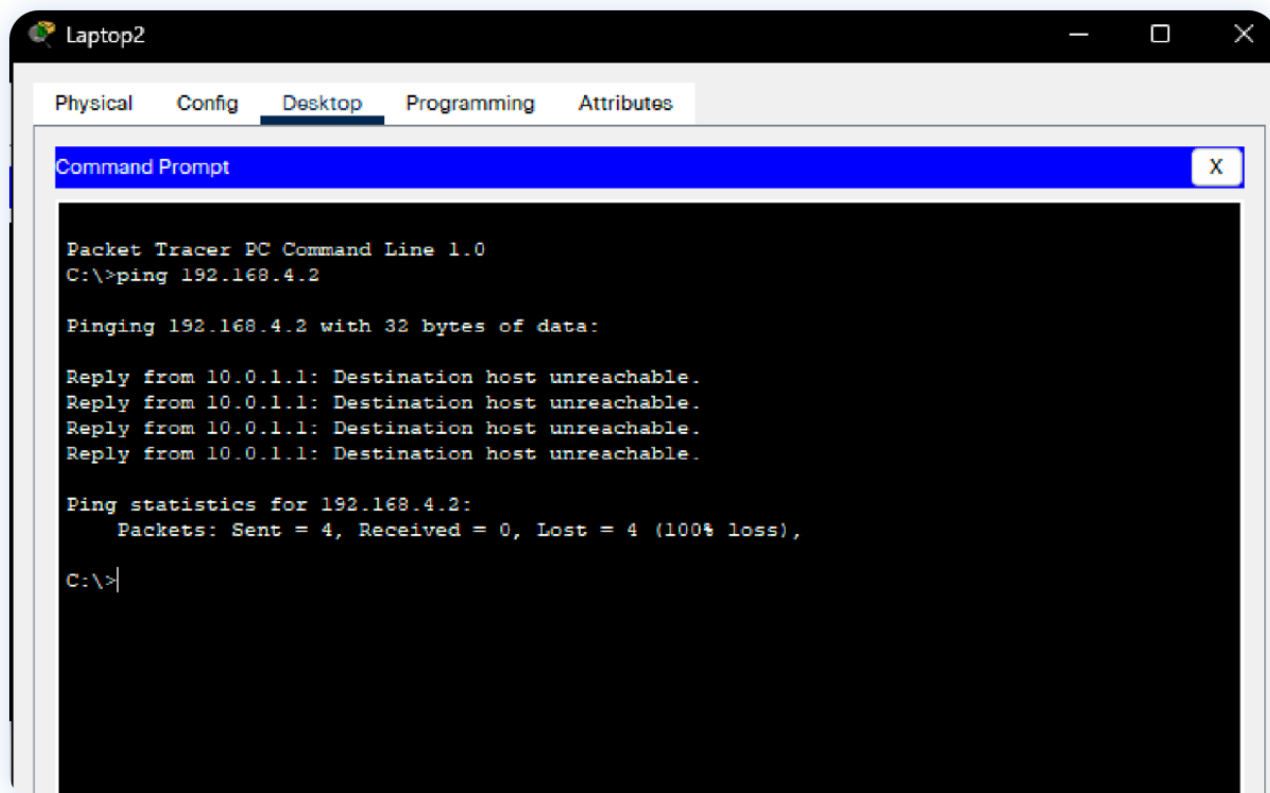
Pinging 192.168.4.2 with 32 bytes of data:

Reply from 192.168.4.2: bytes=32 time<1ms TTL=127
Reply from 192.168.4.2: bytes=32 time=4ms TTL=127
Reply from 192.168.4.2: bytes=32 time=5ms TTL=127
Reply from 192.168.4.2: bytes=32 time<1ms TTL=127

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 = 5ms, Average = 2ms
```

Server1 通信：其他设备均无法访问 Server1





任务 7

过程概述

允许 PC1 向外发送请求，修改 Router1:

```
access 101 permit ip 192.168.1.2 192.168.1.0 0.0.0.255  
access 101 permit ip 192.168.1.2 192.168.2.0 0.0.0.255  
access 101 permit ip 192.168.1.2 192.168.3.0 0.0.0.255
```

修改 Router2&Router3 设置 icmp 后门

Router2:

```
ip inspect name ex icmp  
interface FastEthernet0/1  
ip inspect ex out
```

Router3:

```
ip inspect name ex icmp
interface FastEthernet0/1
ip inspect ex out
```

测试效果

```
C:\>ping 192.168.2.4

Pinging 192.168.2.4 with 32 bytes of data:

Reply from 192.168.2.4: bytes=32 time<1ms TTL=126
Reply from 192.168.2.4: bytes=32 time<1ms TTL=126
Reply from 192.168.2.4: bytes=32 time<1ms TTL=126
Reply from 192.168.2.4: bytes=32 time<1ms TTL=126

Ping statistics for 192.168.2.4:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\>ping 192.168.3.4

Pinging 192.168.3.4 with 32 bytes of data:

Request timed out.
Reply from 192.168.3.4: bytes=32 time<1ms TTL=125
Reply from 192.168.3.4: bytes=32 time<1ms TTL=125
Reply from 192.168.3.4: bytes=32 time<1ms TTL=125

Ping statistics for 192.168.3.4:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

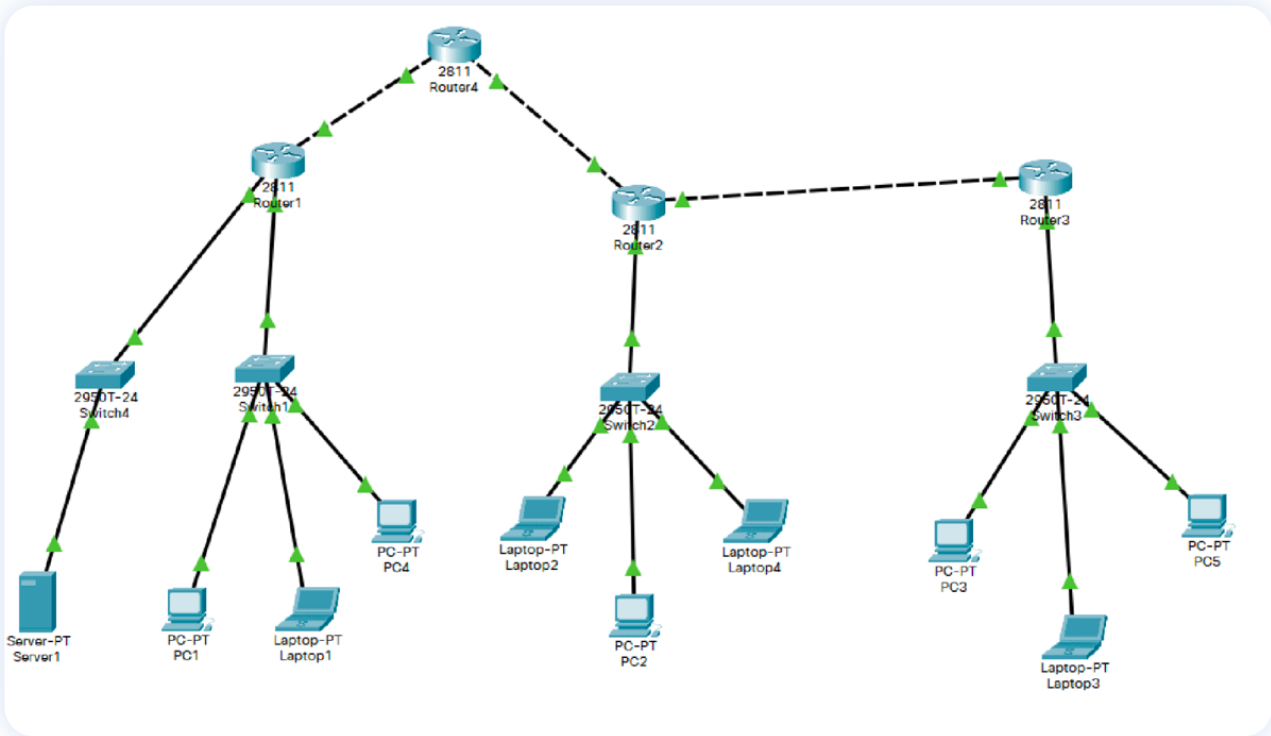
任务 8

过程概述

无法正常通信原因

在公网上难以做到直连，公网上的路由器不能由我们手动设置静态路由或者通过 RIP 学习路由关系。配置静态路由只能配置内网和内网与公网边界上的路由，而内网 IP 在没有 NAT 转换到公网 IP 的情况下无法直接作为有效的 IP 地址与外界通讯。因此使用配置静态路由的方法无法将各个权力机构正常通信。

配置



IP 地址分配：

Device	Port	IP	Mask	Gateway
Router1	FastEthernet0/1	10.0.1.1	255.255.255.0	-
Router4	FastEthernet0/0	10.0.1.2	255.255.255.0	-
Router4	FastEthernet0/1	10.0.3.1	255.255.255.0	-
Router2	FastEthernet0/0	10.0.3.2	255.255.255.0	-

配置静态路由，并按照要求配置 VPN：

Router1:

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

exit

crypto isakmp key 123 address 10.0.3.2

access-list 101 permit ip 192.168.1.0 0.0.0.255 192.168.2.0 0.0.0.255
access-list 101 permit ip 192.168.1.0 0.0.0.255 192.168.3.0 0.0.0.255

crypto ipsec transform-set exset esp-3des esp-md5-hmac
crypto map exmap 1 ipsec-isakmp
set peer 10.0.3.2
match address 101
set transform-set exset

exit

interface FastEthernet0/1
crypto map exmap
```

Router2:

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

exit

crypto isakmp key 123 address 10.0.1.1

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

```
crypto ipsec transform-set exset esp-3des esp-md5-hmac
crypto map exmap 1 ipsec-isakmp
set peer 10.0.1.1
match address 101
set transform-set exset

exit

interface FastEthernet0/0
crypto map exmap
```

同时为 ping 通子网三，为 Router2 配置 RIP 协议，添加 192.168.2.0 和 10.0.0.0，为 Router3 配置 RIP 协议，添加 192.168.3.0 和 10.0.0.0。

测试效果

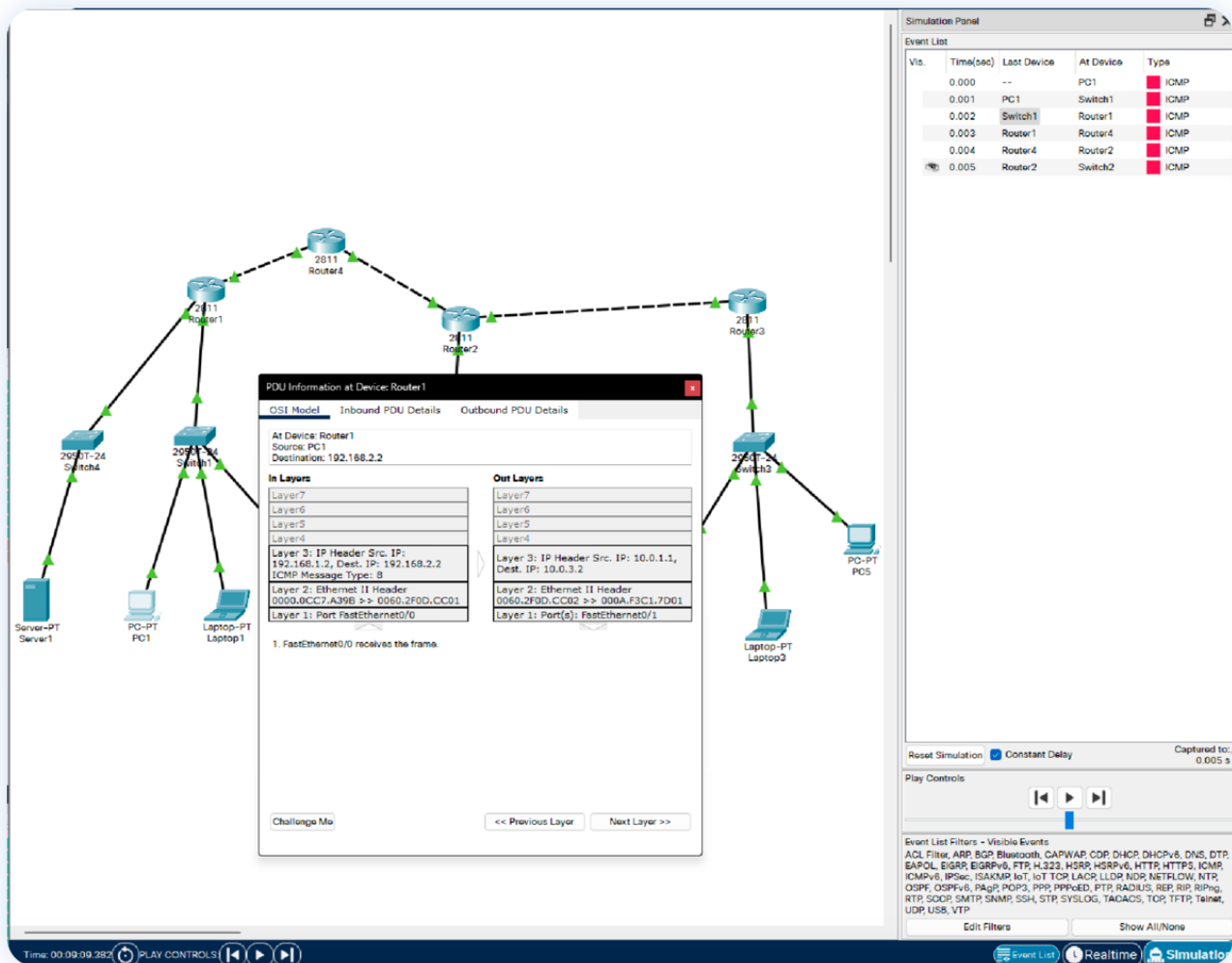
```
C:\>ping 192.168.2.2

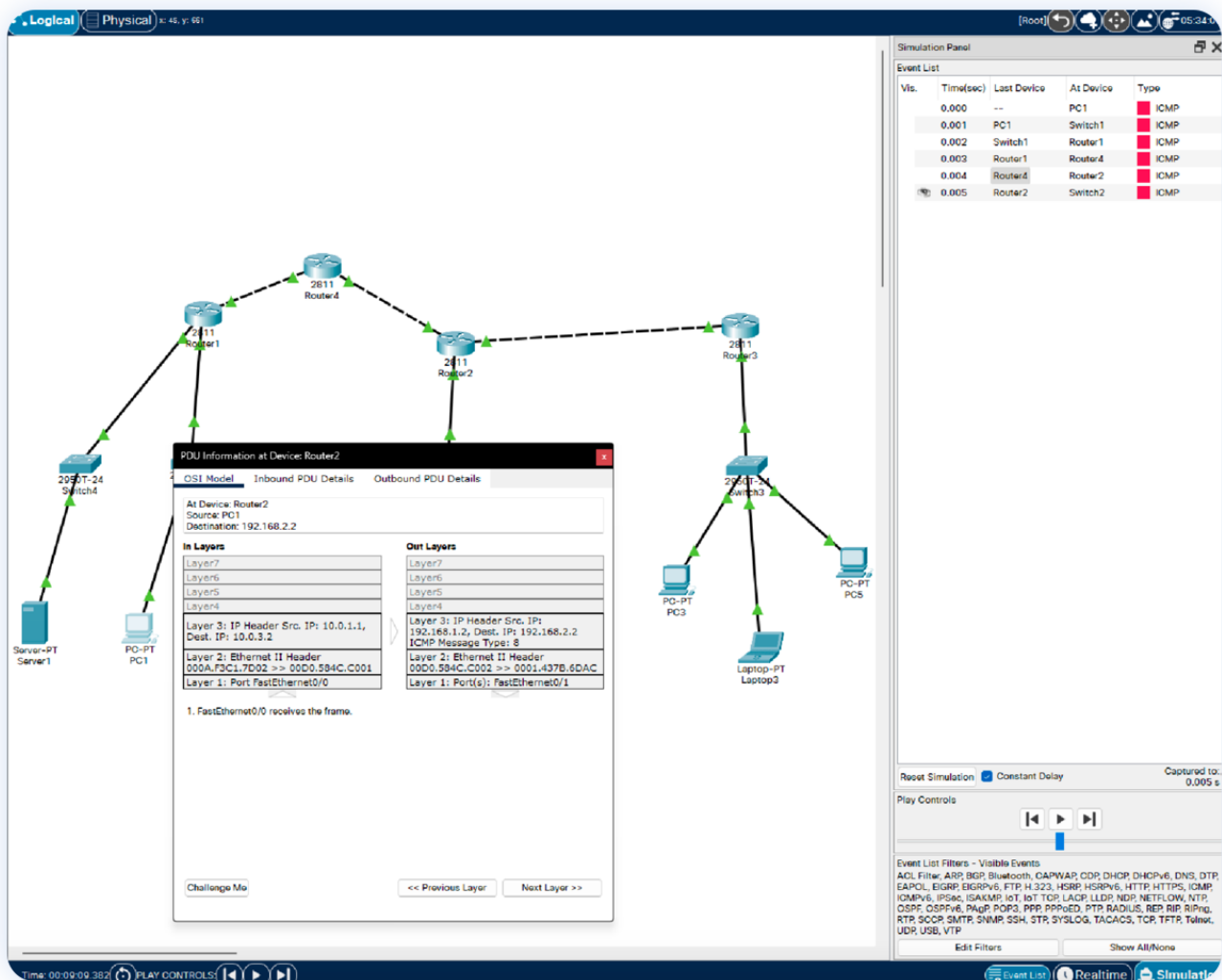
Pinging 192.168.2.2 with 32 bytes of data:

Reply from 192.168.2.2: bytes=32 time=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
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 = 1ms, Average = 0ms
```

抓包分析





可以看到 Router1 处的报文将源 IP 和目的 IP 均换成了公网 IP，在 Router2 处又被修改回内网 IP。在传输过程中 IP header 发生改变，因此 IPsec 使用的是隧道模式。

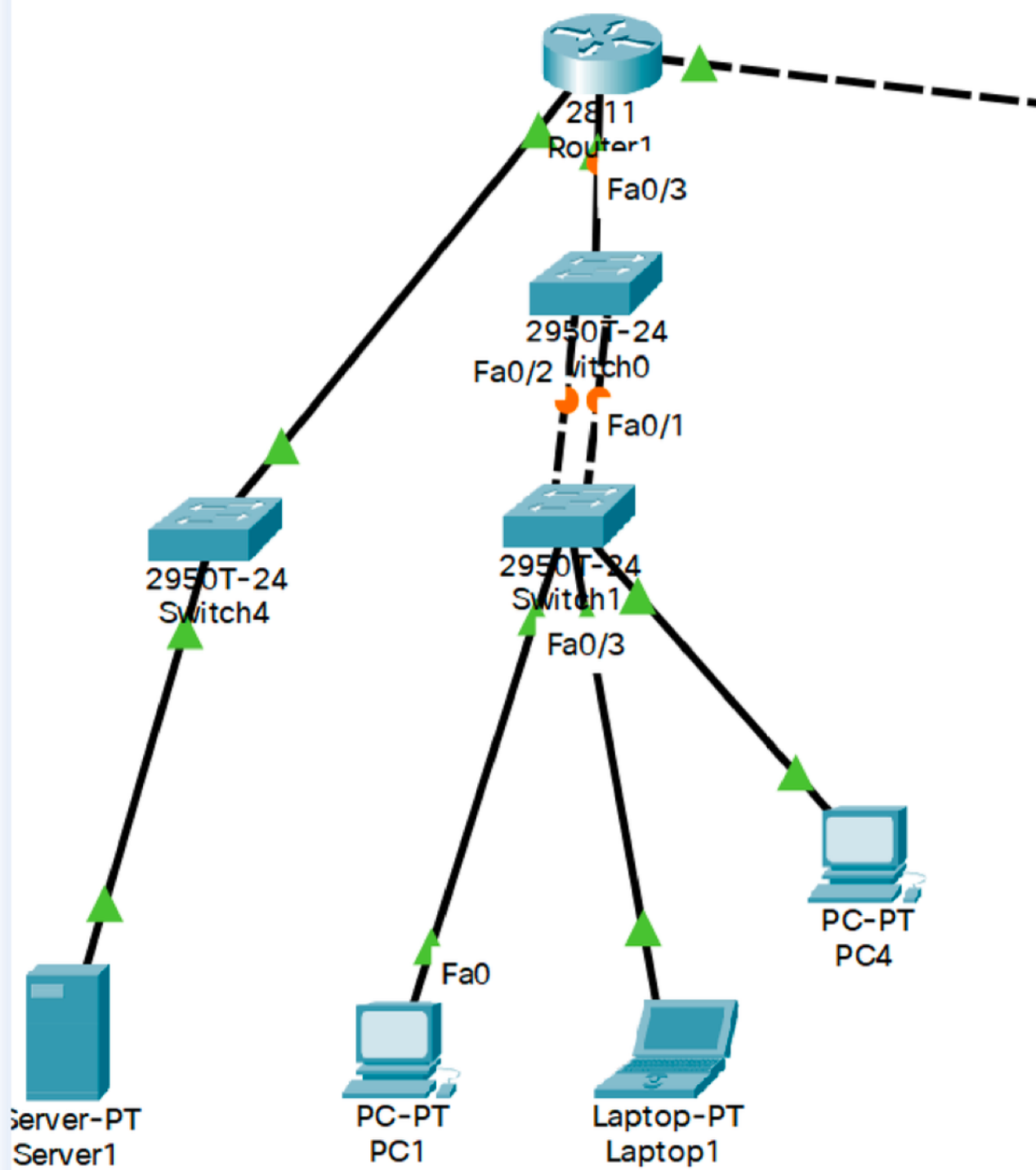
Bonus 布鲁图的烦恼

场景描述

随着科技的日益进步，凯撒将网络在全国范围内搭建起来，同时允许群众向权力部门的联络人进行通信反应需求。作为元老院的联络人，凯撒的代言人，布鲁图每天都要受到数倍于执政官首府和部族会议所的联络，布鲁图也发现自己经常被举报没有查看群众来信，但实际上所有的邮件他都查看了。于是他怀疑这是网络负载不够导致自己背黑锅。同时，凯撒由于近期有大量与机密管理相关的通信，也希望你能对元老院的网络进行最小程度的优化，以同时满足凯撒和布鲁图的要求。

过程概述

考虑在元老院中新增一个交换机，与 Scitch1 进行端口聚合，以使将两个链路聚合成一个链路，当其中一条链路出现故障时，另一条链路会继续工作，以增加元老院网络的可靠性。



配置 Switch1:

```

conf ter
interface range f0/1-2
Switchport mode trunk
channel-group 1 mode on
exit
port-channel load-balance dst-ip
exit
show etherchannel summary

```

```

Switch>enable
Switch#conf ter
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#interface range f0/1-2
Switch(config-if-range)#Switchport mode trunk

Switch(config-if-range)#
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed state to down

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/2, changed state to down

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/2, changed state to up

Switch(config-if-range)#channel-group 1 mode on
Switch(config-if-range)#
Creating a port-channel interface Port-channel 1

%LINK-5-CHANGED: Interface Port-channel1, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface Port-channel1, changed state to up

Switch(config-if-range)#exit
Switch(config)#port-channel load-balance dst-ip
Switch(config)#exit
Switch#
%SYS-5-CONFIG_I: Configured from console by console

Switch#show etherchannel summary
Flags:  D - down          P - in port-channel
        I - stand-alone s - suspended
        H - Hot-standby (LACP only)
        R - Layer3      S - Layer2
        U - in use      f - failed to allocate aggregator
        u - unsuitable for bundling
        w - waiting to be aggregated
        d - default port

Number of channel-groups in use: 1
Number of aggregators:          1

Group  Port-channel  Protocol    Ports
-----+-----+-----+-----
1      Pol(SU)          -          Fa0/1(P) Fa0/2(P)
Switch#

```

配置 Switch0:

```
conf ter
interface range f0/1-2
Switchport mode trunk
channel-group 1 mode on
exit
port-channel load-balance dst-ip
exit
show etherchannel summary
```

```
Switch#conf ter
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#interface range f0/1-2
Switch(config-if-range)#Switchport mode trunk

Switch(config-if-range)#channel-group 1 mode on
Switch(config-if-range)#exit
Switch(config)#port-channel load-balance dst-ip
Switch(config)#exit
Switch#show etherchannel summary
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed state to down
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/2, changed state to down
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/2, changed state to up
Creating a port-channel interface Port-channel 1
%LINK-5-CHANGED: Interface Port-channel1, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface Port-channel1, changed state to up
%SYS-5-CONFIG_I: Configured from console by console

Flags:  D - down          P - in port-channel
        I - stand-alone s - suspended
        H - Hot-standby (LACP only)
        R - Layer3        S - Layer2
        U - in use        f - failed to allocate aggregator
        u - unsuitable for bundling
        w - waiting to be aggregated
        d - default port

Number of channel-groups in use: 1
Number of aggregators:          1

Group  Port-channel  Protocol    Ports
-----+-----+-----+-----
1      Pol(SU)        -          Fa0/1(P) Fa0/2(P)
Switch#
```