

2019 年秋学期《计算机网络安全技术》实验二

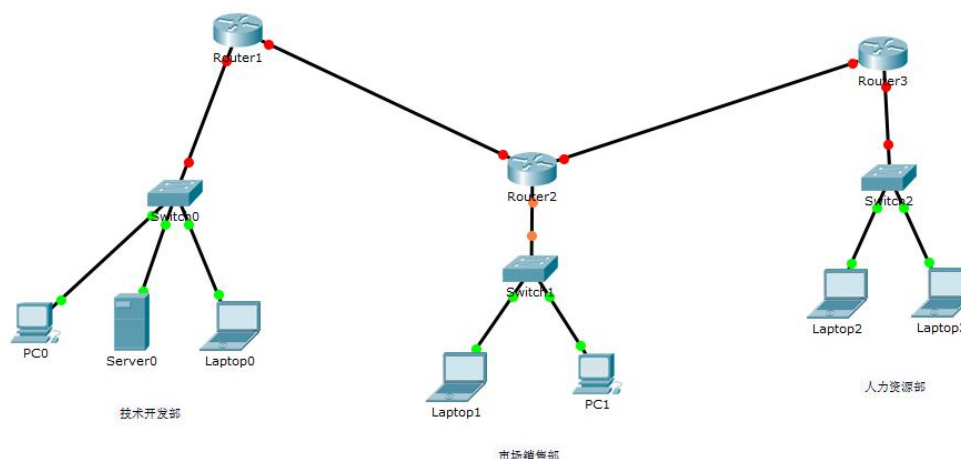
访问控制及 VPN 技术

请根据下面的实验介绍，完成各个任务。给出证明自己完成了实验的必要文字描述和截图。本实验要求提交实验报告，配置文件自存。

实验背景

近日，T 公司从大兴区搬迁至了宇宙中心五道口，因此身为公司网络管理员的你需要在公司新址进行内网的重新设计与部署。在这次重部署的过程中，你也希望使公司网络能够更加安全、高效地发挥作用。目前公司主要分为三个部门：技术开发部、市场销售部和人力资源部。由于分工不同，各个部门均选用不同的子网便于管理。您在前期已经初步搭建起了网络，并完成了路由部分，现在你将着手完成网络的安全化工作。

网络预拓扑



技术开发部 (192.168.1.0/24) : Router1, Switch0, Server0, PC0, Laptop0

市场销售部 (192.168.2.0/24) : Router2, Switch1, PC1, Laptop1

人力资源部 (192.168.3.0/24) : Router3, Switch2, Laptop2, Laptop3

注意：除图中设备外，各个部门内还有若干其他设备处于各自的子网中

任务 6 网络的职务权限控制 6'

为了便于公司的管理，你需要从技术层面对网络进行权限设置，以达到控制访问的效果。

公司部分设备的使用情况如下表所示:

设备名称	使用人	部门	备注	ip
PC0	X 部长 (你)	技术开发部	-	192.168.1.2
Server0	丁部员	技术开发部	资源管理	192.168.1.3
Laptop0	杨助手	技术开发部	联络人	192.168.1.4
Laptop1	王部长	市场销售部	-	192.168.2.3
PC1	李秘书	市场销售部	联络人	192.168.2.2
Laptop2	冯部长	人力资源部	-	192.168.3.2
Laptop3	刘秘书	人力资源部	联络人	192.168.3.3

为了便于进行安全管理,公司新购入了一台路由器和若干交换机。请在最合适的接口处配置访问控制列表,满足以下的安全要求,在必要时可以在部门内略微调整网络:

1. 一般地,各个部门内部的所有成员均能相互交流。
 2. 然而,在部门之间的相互通信只能通过几位助手和秘书进行,即 A 部门的成员只能与 B 部门的联络人(杨助手、李秘书和刘秘书)进行通信。
 3. 另外,三个部长可以互相讨论工作,进行部长会议。
 4. 特别地,由于 Server0 存放了大量的技术资源,在整个公司只有其直属上司你可以通信。
- 注:该任务中,不能通信指既不能收数据也不能发数据,可以通信指既能收数据也能发数据。

1.各个部门内部的所有成员均能相互交流,由于他们处于同一个子网当中,包在转发时是经过交换机实现的,所以这个条件天然成立。

2.也就是说,在每个部门中只有联络人可以收到从路由器转发来的消息、可以给其他部门的人发信息。

因此:

(1) 在每个路由器连到子网的端口处出方向设置访问控制列表 (101), 只允许目的 ip 为部门联络人的包、来自其他部门联络人的包进入子网

(2) 在每个路由器连到子网的端口的入方向设置访问控制列表 (102), 只允许目的 ip 为其他部门联络人的包、来自本部门联络人的包走出这个子网

在两个方向上都设置访问控制列表是为了保证安全性。同时也具有可扩展性,因为访问控制列表中只出现 permit 语句,当公司设置新的子网时在访问控制列表中加入新的 permit 语句即可。

3.三个部长可以互相讨论工作,也就是说:

(1) 在 ACL101 中允许来自其他部长,目的 ip 为本部部长的包转发

(2) 在 ACL102 中允许来自本部部长,目的 ip 为其他部长的包转发

综上,设置路由器的访问控制列表如下:

Router1

```
192.168.0.0#show ac
192.168.0.0#show access-lists
Extended IP access list be
Extended IP access list 101
 10 permit ip host 192.168.2.3 host 192.168.1.2
 20 permit ip host 192.168.3.2 host 192.168.1.2
 30 permit ip 192.168.2.0 0.0.0.255 host 192.168.1.4 (7 match(es))
 40 permit ip 192.168.3.0 0.0.0.255 host 192.168.1.4
 50 permit ip host 192.168.2.2 192.168.1.0 0.0.0.255 (7 match(es))
 60 permit ip host 192.168.3.3 192.168.1.0 0.0.0.255 (6 match(es))
Extended IP access list 102
 10 permit ip host 192.168.1.2 host 192.168.2.3
 20 permit ip host 192.168.1.2 host 192.168.3.2
 30 permit ip 192.168.1.0 0.0.0.255 host 192.168.2.2 (16 match(es))
 40 permit ip 192.168.1.0 0.0.0.255 host 192.168.3.3 (8 match(es))
 50 permit ip host 192.168.1.4 192.168.2.0 0.0.0.255 (4 match(es))
 60 permit ip host 192.168.1.4 192.168.3.0 0.0.0.255
192.168.0.0#
```

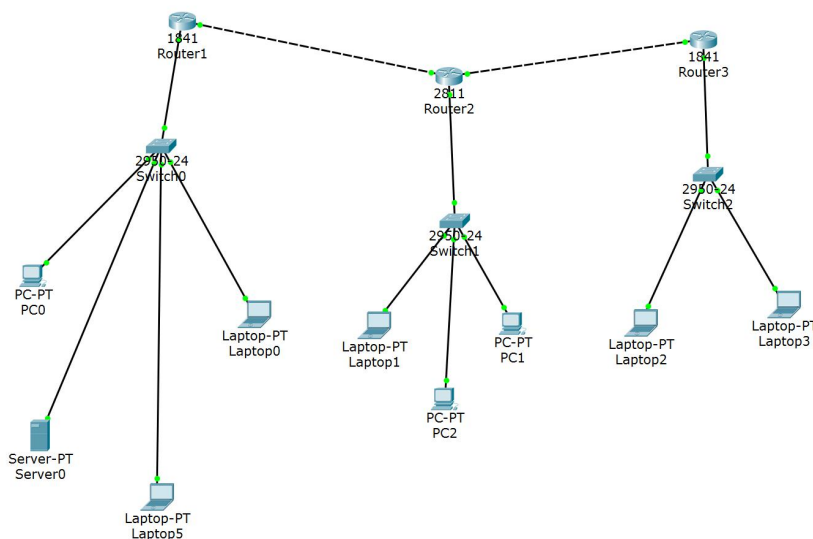
Router2

```
Router(config)#acc
Router(config)#access-list 101 perm
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)#access-list 101 permit ip host 192.168.1.4 192.168.2.0 0.0.0.255
Router(config)#access-list 101 permit ip host 192.168.3.3 192.168.2.0 0.0.0.255
Router(config)#access-list 101 permit ip 192.168.1.0 0.0.0.255 host 192.168.2.2
Router(config)#access-list 101 permit ip 192.168.3.0 0.0.0.255 host 192.168.2.2
Router(config)#acc
Router(config)#access-list 102 permit ip host 192.168.2.3 host 192.168.1.2
Router(config)#access-list 102 permit ip host 192.168.2.3 host 192.168.3.2
Router(config)#access-list 102 permit ip host 192.168.2.2 192.168.1.0 0.0.0.255
Router(config)#access-list 102 permit ip host 192.168.2.2 192.168.3.0 0.0.0.255
Router(config)#access-list 102 permit ip 192.168.2.0 0.0.0.255 host 192.168.1.4
Router(config)#access-list 102 permit ip 192.168.2.0 0.0.0.255 host 192.168.3.3
Router(config)#int f 0/0
Router(config-if)#ip ac
Router(config-if)#ip access-group 101 out
Router(config-if)#ip access-group 102 in
Router(config-if)#
```

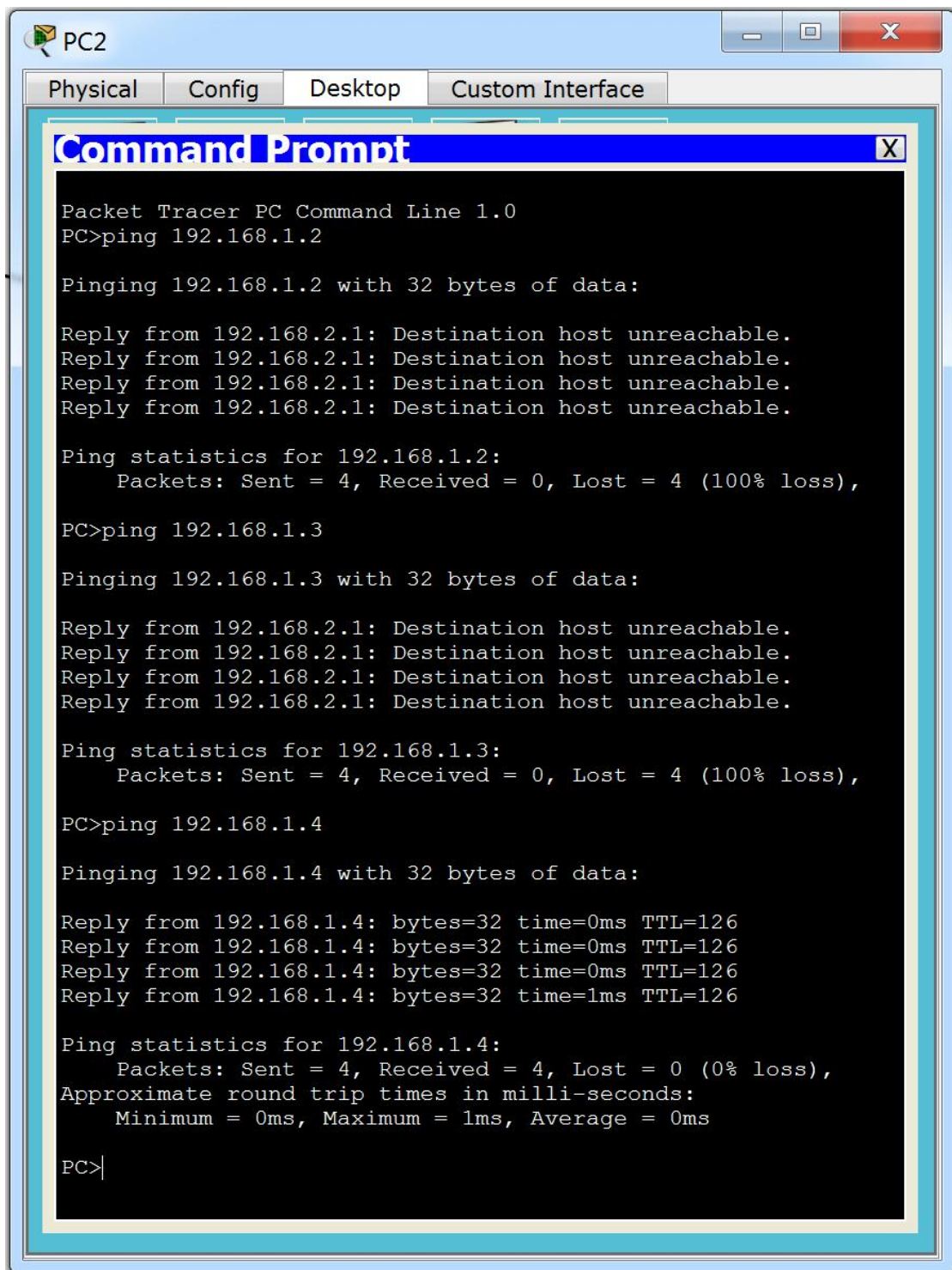
Router3

```
Router#show access-lists
Extended IP access list 101
 10 permit ip host 192.168.1.2 host 192.168.3.2
 20 permit ip host 192.168.2.3 host 192.168.3.2
 30 permit ip 192.168.1.0 0.0.0.255 host 192.168.3.3 (7 match(es))
 40 permit ip 192.168.2.0 0.0.0.255 host 192.168.3.3
 50 permit ip host 192.168.1.4 192.168.3.0 0.0.0.255
 60 permit ip host 192.168.2.2 192.168.3.0 0.0.0.255
Router#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#ac
Router(config)#access-list 102 permit ip host 192.168.3.2 host 192.168.1.2
Router(config)#access-list 102 permit ip host 192.168.3.2 host 192.168.2.3
Router(config)#access-list 102 permit ip host 192.168.3.3 192.168.1.0 0.0.0.255
Router(config)#access-list 102 permit ip host 192.168.3.3 192.168.2.0 0.0.0.255
Router(config)#access-list 102 permit ip 192.168.3.0 0.0.0.255 host 192.168.1.4
Router(config)#access-list 102 permit ip 192.168.3.0 0.0.0.255 host 192.168.2.2
Router(config)#int f 0/0
Router(config-if)#ip acc
Router(config-if)#ip access-group 101 out
Router(config-if)#ip access-group 102 in
Router(config-if)#
```

在网络中增加设备并验证结果:



(1)子网中非部长、非联系人的设备只能 ping 通其他子网的联系人



The screenshot shows a Packet Tracer PC2 window with the 'Command Prompt' tab selected. The command prompt displays the results of three ping commands. The first two pings (to 192.168.1.2 and 192.168.1.3) result in 100% loss because the destination hosts are unreachable. The third ping (to 192.168.1.4) is successful with 0% loss.

```
PC2
Physical Config Desktop Custom Interface
Command Prompt
Packet Tracer PC Command Line 1.0
PC>ping 192.168.1.2

Pinging 192.168.1.2 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 192.168.1.2:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

PC>ping 192.168.1.3

Pinging 192.168.1.3 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 192.168.1.3:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

PC>ping 192.168.1.4

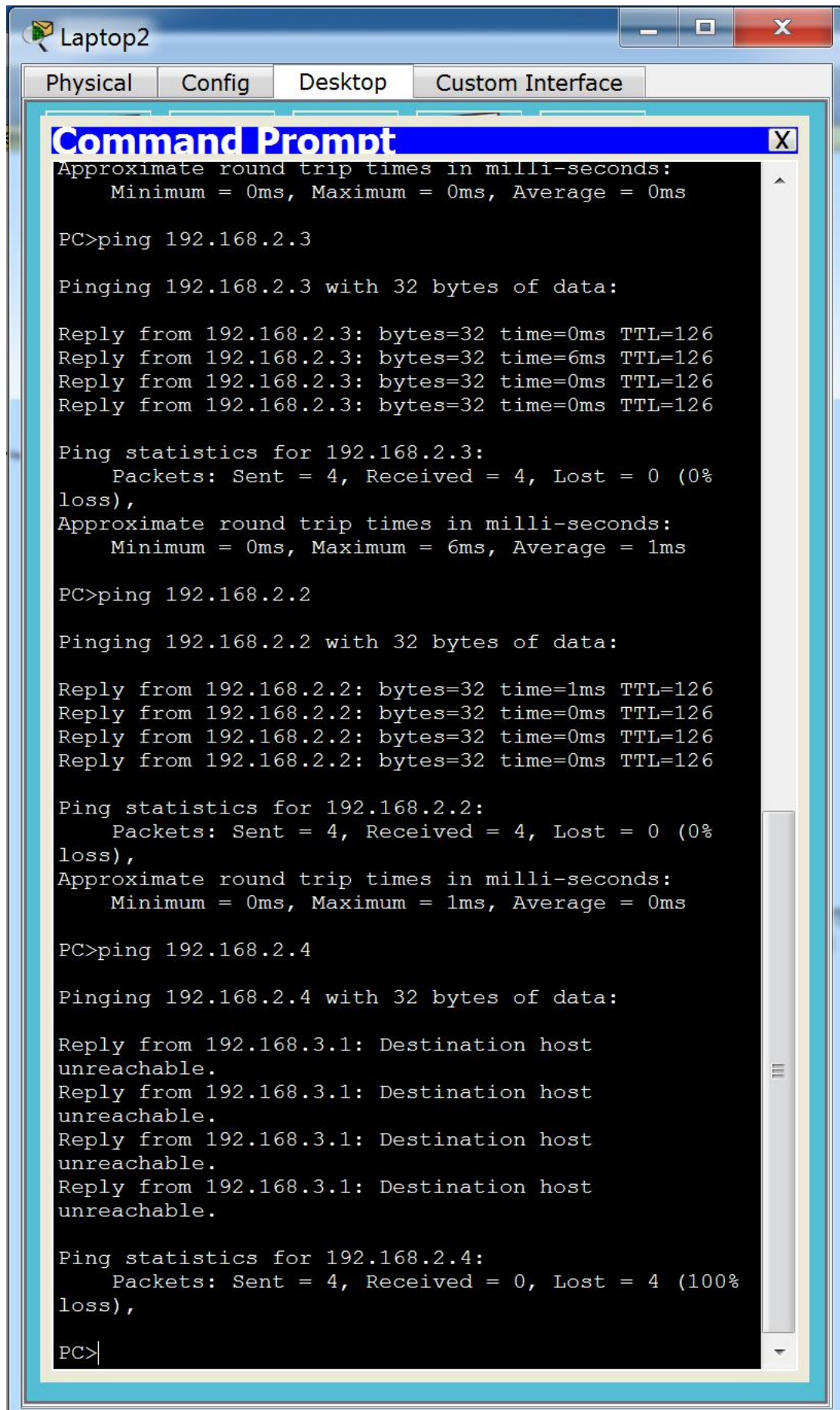
Pinging 192.168.1.4 with 32 bytes of data:

Reply from 192.168.1.4: bytes=32 time=0ms TTL=126
Reply from 192.168.1.4: bytes=32 time=0ms TTL=126
Reply from 192.168.1.4: bytes=32 time=0ms TTL=126
Reply from 192.168.1.4: bytes=32 time=1ms TTL=126

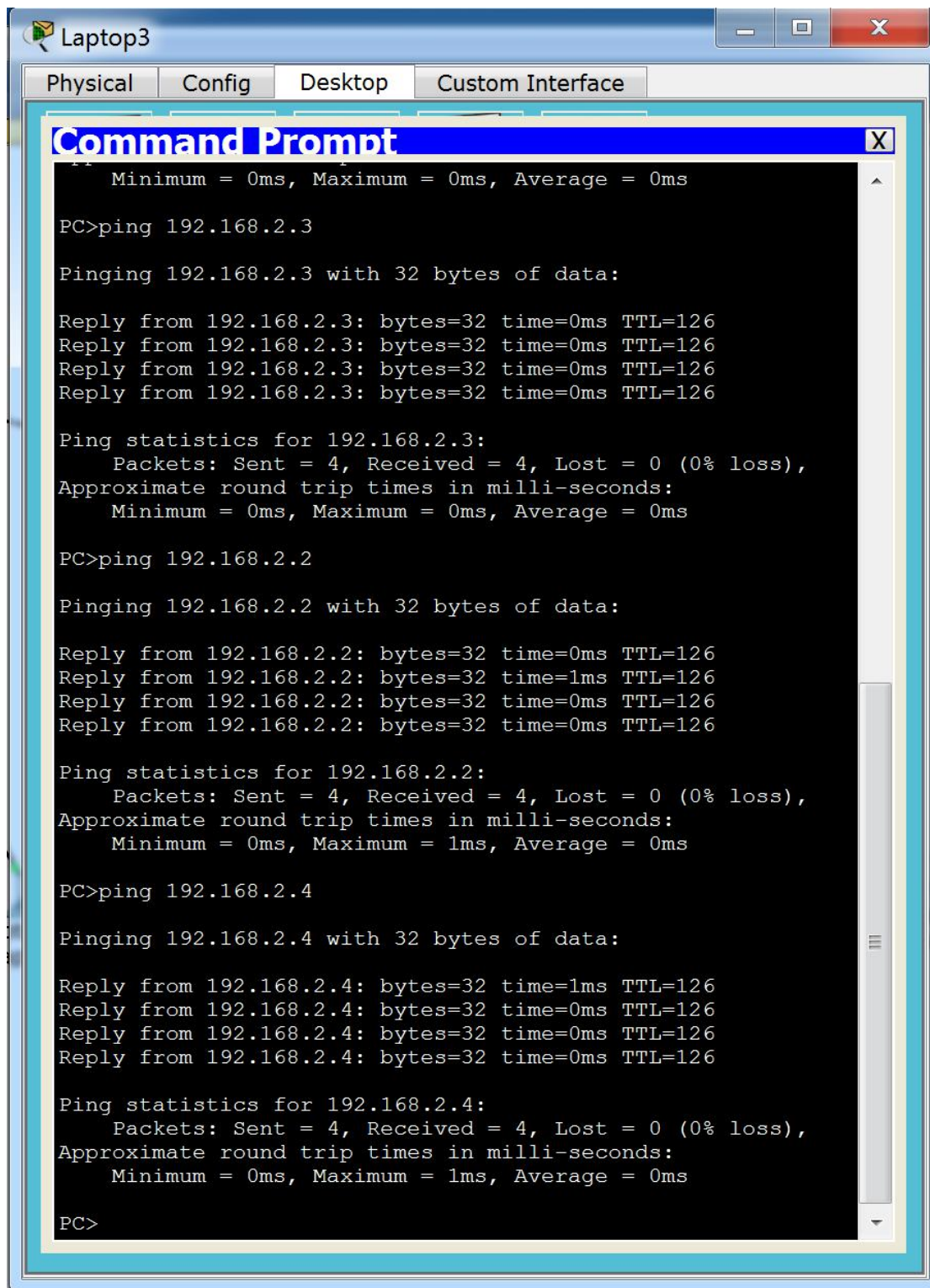
Ping statistics for 192.168.1.4:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 1ms, Average = 0ms

PC>|
```

(2)子网中部长的设备可以 ping 通其他子网的部长和联系人



(3)联系人的设备可以 ping 通其他子网中的任何设备



The screenshot shows a Packet Tracer interface for a device named 'Laptop3'. The 'Desktop' tab is selected, displaying a 'Command Prompt' window. The window contains the following text:

```
Minimum = 0ms, Maximum = 0ms, Average = 0ms

PC>ping 192.168.2.3

Pinging 192.168.2.3 with 32 bytes of data:

Reply from 192.168.2.3: bytes=32 time=0ms TTL=126
Reply from 192.168.2.3: bytes=32 time=0ms TTL=126
Reply from 192.168.2.3: bytes=32 time=0ms TTL=126
Reply from 192.168.2.3: bytes=32 time=0ms 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

PC>ping 192.168.2.2

Pinging 192.168.2.2 with 32 bytes of data:

Reply from 192.168.2.2: bytes=32 time=0ms TTL=126
Reply from 192.168.2.2: bytes=32 time=1ms TTL=126
Reply from 192.168.2.2: bytes=32 time=0ms TTL=126
Reply from 192.168.2.2: bytes=32 time=0ms 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

PC>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=0ms TTL=126
Reply from 192.168.2.4: bytes=32 time=0ms TTL=126
Reply from 192.168.2.4: bytes=32 time=0ms 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 = 1ms, Average = 0ms

PC>
```

4.在前 3 个任务中已经禁止了其他部门除联系人以外的设备访问 Server0，在这里需要禁止本子网内的设备和联系人访问 Server0，只允许 PC0 访问。

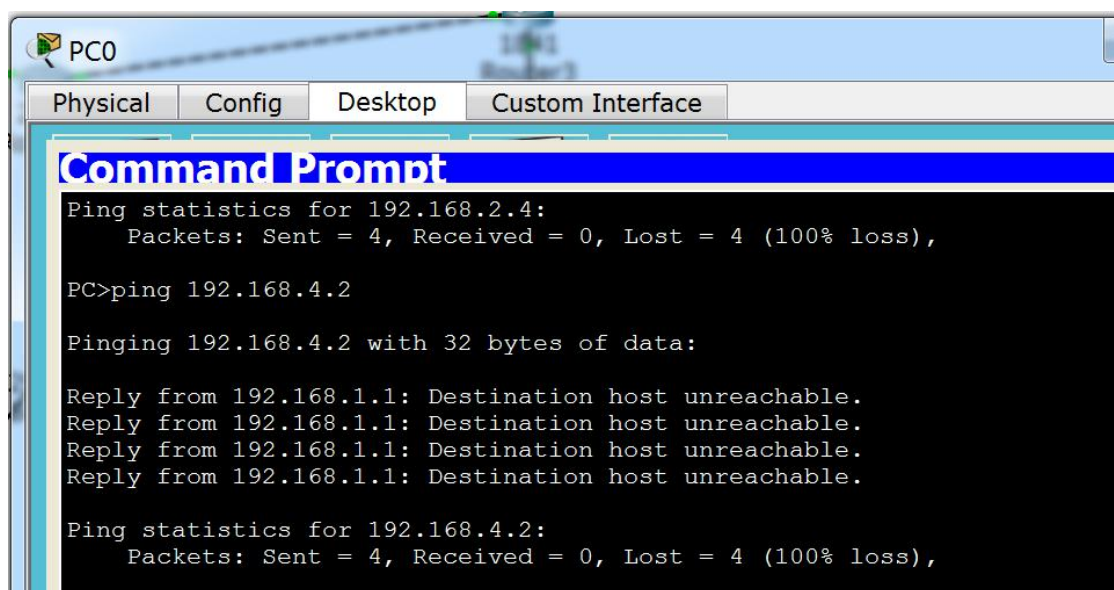
因为子网内部包转发是通过交换机进行的，并不会经过路由器，因此在 Router1 上设置访问控制列表并不能阻止本子网内设备访问 Server0。因此考虑改变网络结构，将服务器放在 192.168.4.0 网段，修改服务器 ip 为 192.168.4.2，网关 ip 为 192.168.4.1，并相应修改

rip 设置等信息。

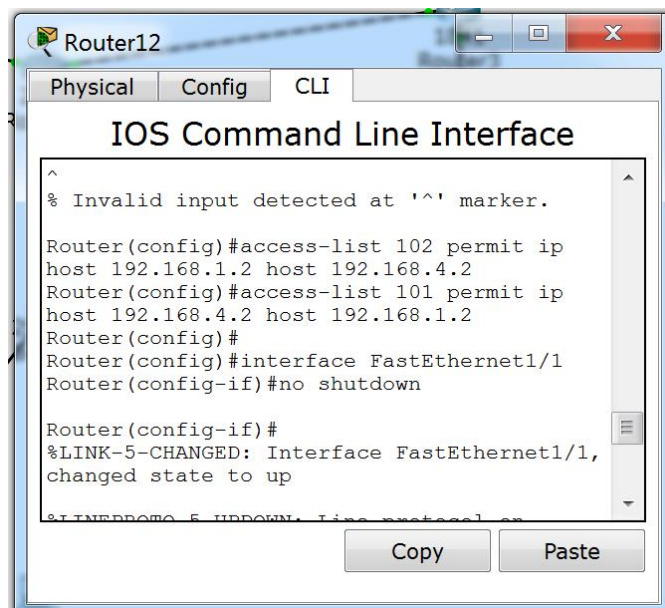
并在相应接口处设置路由表: 只允许 ip 为 192.168.1.2、目的 IP 为 192.168.4.2 的包进入子网, 只允许 ip 为 192.168.4.2、目的 ip 为 192.168.1.2 的包走出子网。

```
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#acc
Router(config)#access-list 103 permit ip host 192.168.1.2 host 192.168.4.2
Router(config)#ac
Router(config)#access-list 104 permit ip host 192.168.4.2 host 192.168.1.2
Router(config)#in
Router(config)#interface fa 1/0
Router(config-if)#ip acc
Router(config-if)#ip access-group 103 out
Router(config-if)#i[ip ac
Router(config-if)#ip access-group 104 in
Router(config-if)#exit
Router(config-if)#acc
```

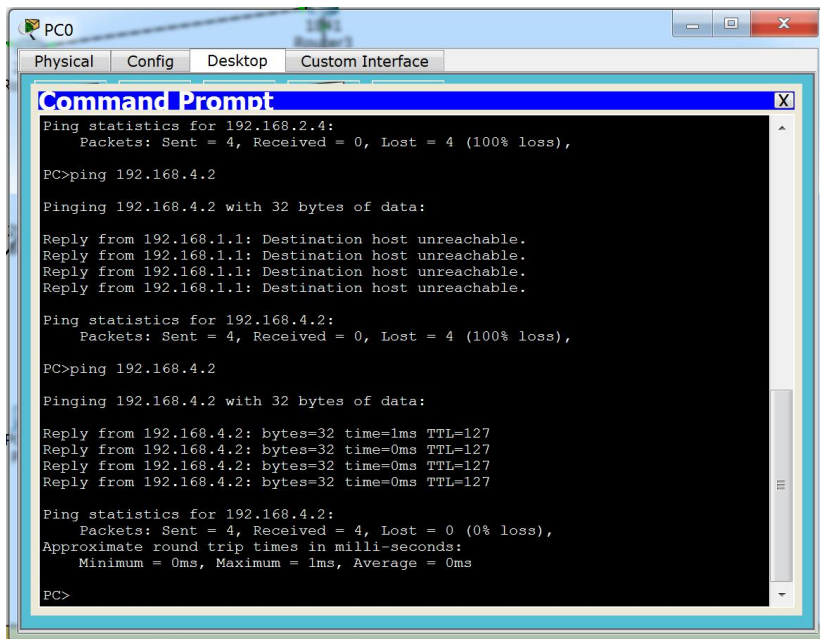
但是仅设置连接到子网 4 的端口还不够, 因为路由器连接到子网 1 的端口还不允许来自 192.168.1.2、目的 ip 为服务器的包转发。



因此在路由器连向子网 1 的端口做出相应设置 (修改 access-list 101、102)。



在修改后可以服务器和 PC0 可以互相通信:



The screenshot shows the Command Prompt window on PC0. It displays the results of two ping commands. The first command is 'ping 192.168.2.4', which shows a 100% loss of packets. The second command is 'ping 192.168.4.2', which shows successful replies from 192.168.4.2 with a 0% loss of packets.

```
PC0
Physical Config Desktop Custom Interface
Command Prompt
Ping statistics for 192.168.2.4:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

PC>ping 192.168.4.2

Pinging 192.168.4.2 with 32 bytes of data:

Reply from 192.168.4.2: Destination host unreachable.
Reply from 192.168.4.2: Destination host unreachable.
Reply from 192.168.4.2: Destination host unreachable.
Reply from 192.168.4.2: Destination host unreachable.

Ping statistics for 192.168.4.2:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

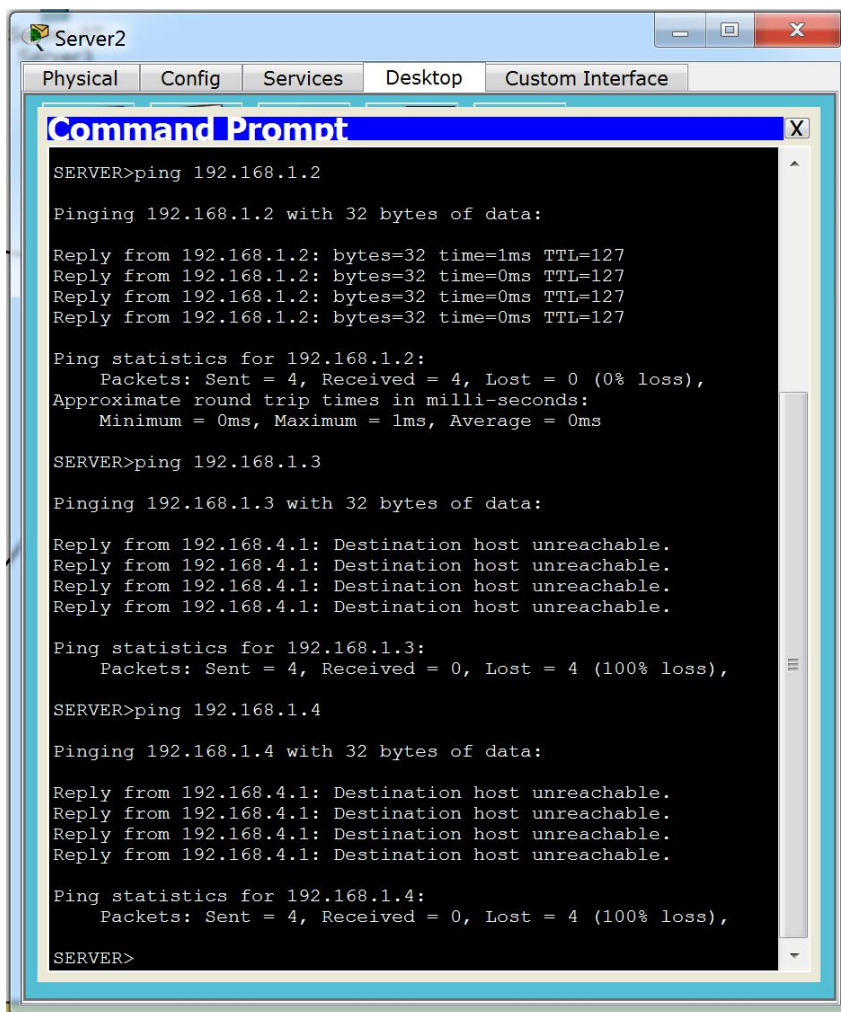
PC>ping 192.168.4.2

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=0ms TTL=127
Reply from 192.168.4.2: bytes=32 time=0ms TTL=127
Reply from 192.168.4.2: bytes=32 time=0ms 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 = 1ms, Average = 0ms

PC>
```



The screenshot shows the Command Prompt window on Server2. It displays the results of three ping commands. The first command is 'ping 192.168.1.2', which shows successful replies from 192.168.1.2 with a 0% loss of packets. The second command is 'ping 192.168.1.3', which shows a 100% loss of packets. The third command is 'ping 192.168.1.4', which shows a 100% loss of packets.

```
Server2
Physical Config Services Desktop Custom Interface
Command Prompt
SERVER>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=127
Reply from 192.168.1.2: bytes=32 time=0ms TTL=127
Reply from 192.168.1.2: bytes=32 time=0ms TTL=127
Reply from 192.168.1.2: bytes=32 time=0ms TTL=127

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 = 1ms, Average = 0ms

SERVER>ping 192.168.1.3

Pinging 192.168.1.3 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 192.168.1.3:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

SERVER>ping 192.168.1.4

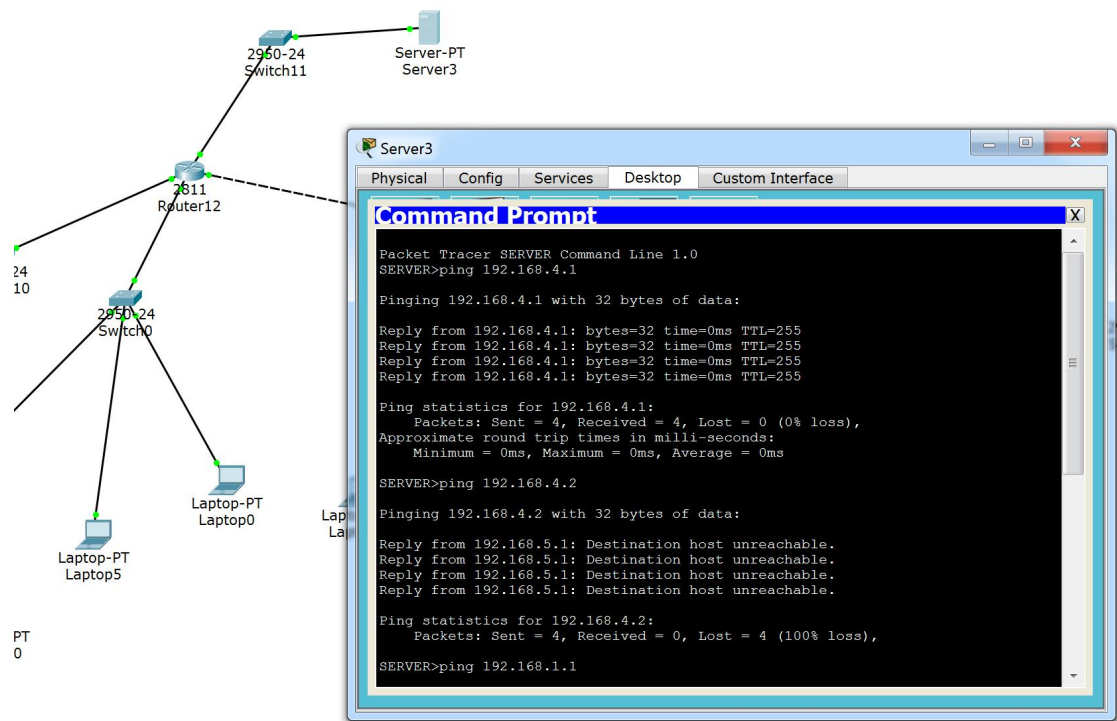
Pinging 192.168.1.4 with 32 bytes of data:

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.

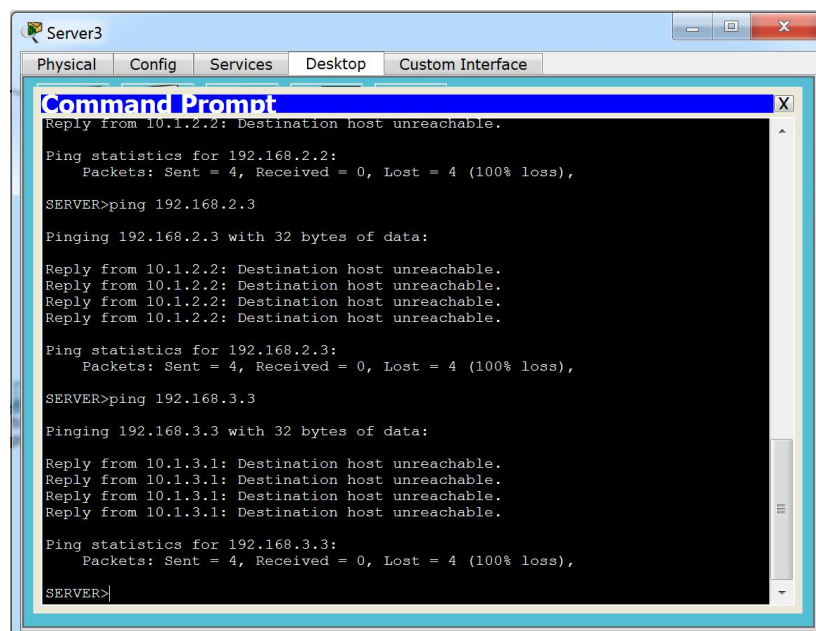
Ping statistics for 192.168.1.4:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

SERVER>
```

为了验证以上设置的安全性和可扩展性，新加入一个 192.168.5.0 子网，子网中增加设备 Server3, 设置 ip 地址为 192.168.5.2, 网关为 192.168.5.1。使用 Server3 ping 192.168.4.1 显示可以 ping 通，ping 192.168.4.2 显示 Destination host unreachable，说明 192.168.4.1 处的 access-list 起了访问控制的作用。



同理 ping 子网 2、3 中的设备，都会显示目的 ip 不可达。也就是说以上配置可以保证公司子网扩展后的安全性。



任务 7 程序员也可以有“最高”权限 4'

由于你兼任公司的网络管理者，所以你需要经常对各个设备的网络连通性进行探测。请在前一任务的基础上进行相应的配置，使得你能够对公司所有设备进行 ping 测试，且当你发起测试时，不受上个任务的访问权限影响。

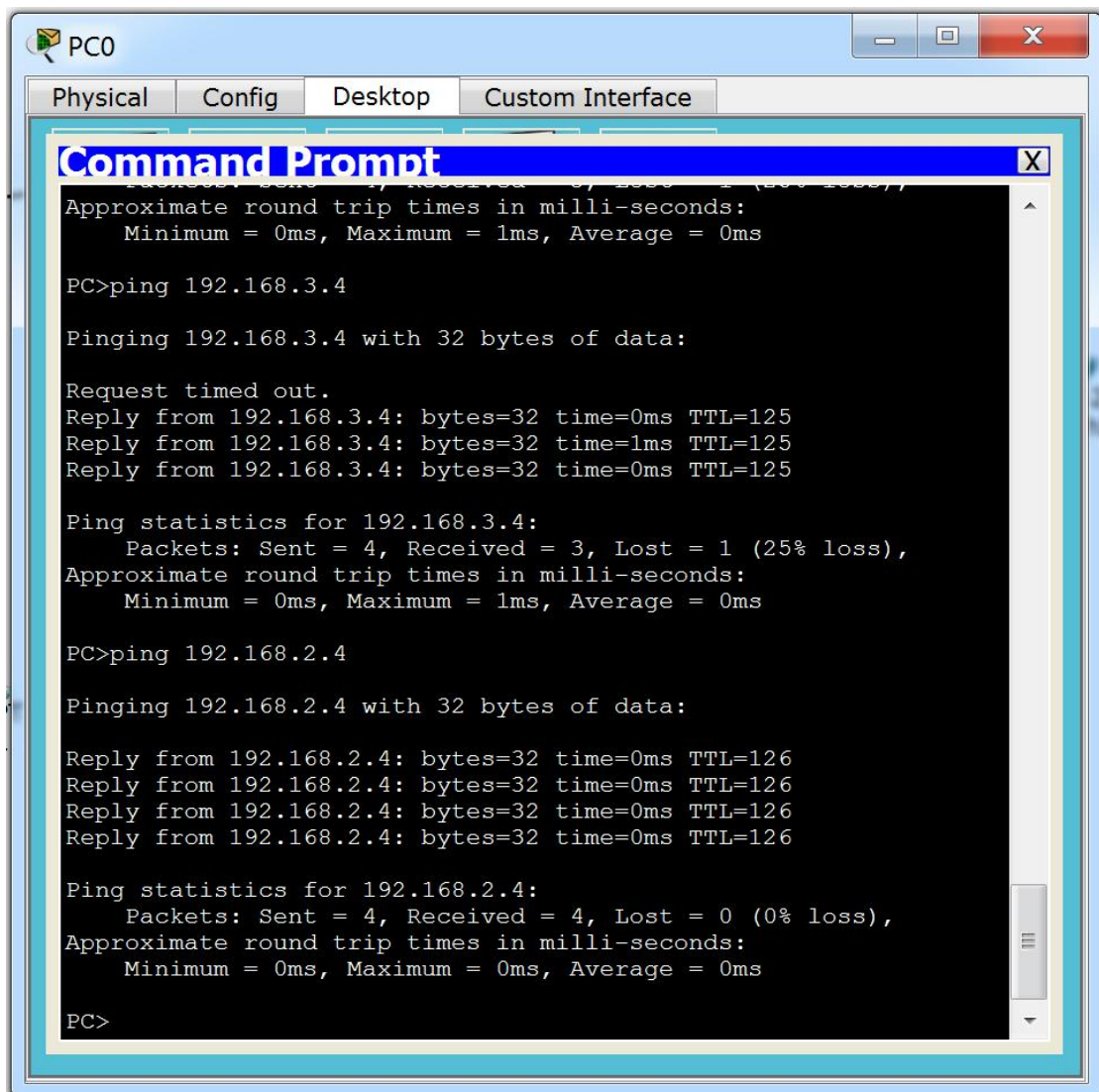
在这个任务中，需要首先允许来自 192.168.1.2 的 ping 包可以发出子网 1，因此修改 Router1 的快速以太 0/0 端口的 in 方向的 access-list 101，增加一条新的表项，允许来自 192.168.1.2 的 icmp 协议的包被转发出这个子网。同时在 in 方向开启 CBAC，允许 ping 之后可以收到返回的包。

```
Router(config)#acc
Router(config)#access-list 102 permit ic
Router(config)#access-list 102 permit icmp host 192.168.1.2 192.168.0.0 0.0.255.255
Router(config)#ip ins
Router(config)#ip inspect name ACCESS_ICMP IC
Router(config)#ip inspect name ACCESS_ICMP ICmp
Router(config)#int fa 0/0
Router(config-if)#ip ins
Router(config-if)#ip inspect ACCESS_ICMP in
Router(config-if)#
```

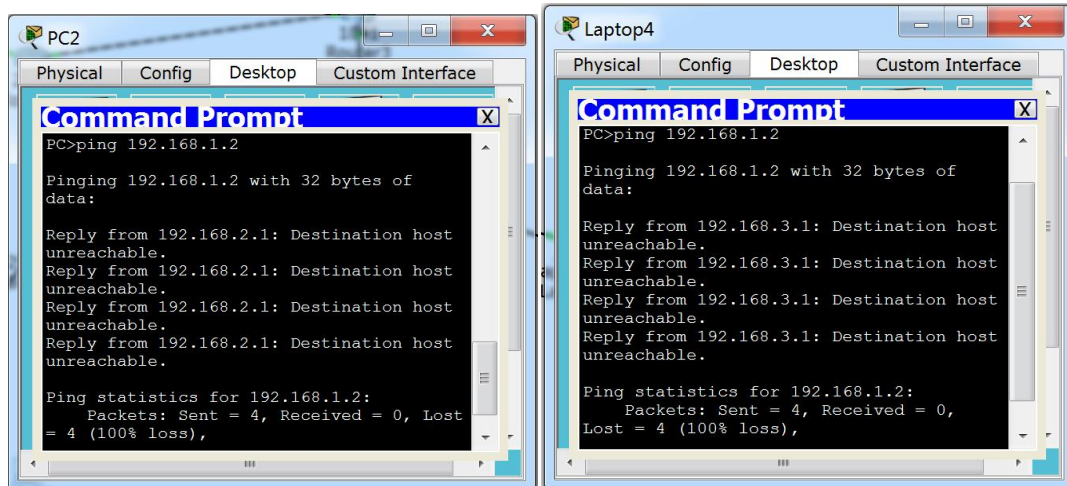
同时修改 Router2、Router3 的 access-list，在快速以太 0/0 端口的 out 方向做类似设置，允许来自 192.168.1.2 的包通过，并开启 CBAC，允许 ping 之后的 reply 包可以被转发走。

```
Router#conf terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#access
Router(config)#access-list 101 permit icmp host 192.168.1.2 192.168.3.0 0.0.0.255
Router(config)#ip ins
Router(config)#ip inspect n
Router(config)#ip inspect name ACCESS_ICMP ic
Router(config)#ip inspect name ACCESS_ICMP icmp
Router(config)#int fa 0/0
Router(config-if)#ip in
Router(config-if)#ip inspect ACCESS_ICMP out
Router(config-if)#
```

完成后进行测试，PC0 可以 ping 通子网中所有的设备，但其他设备并不能 ping 通 PC0



(注: Laptop4 是子网 3 中的普通设备, ip 地址为 192.168.3.4)



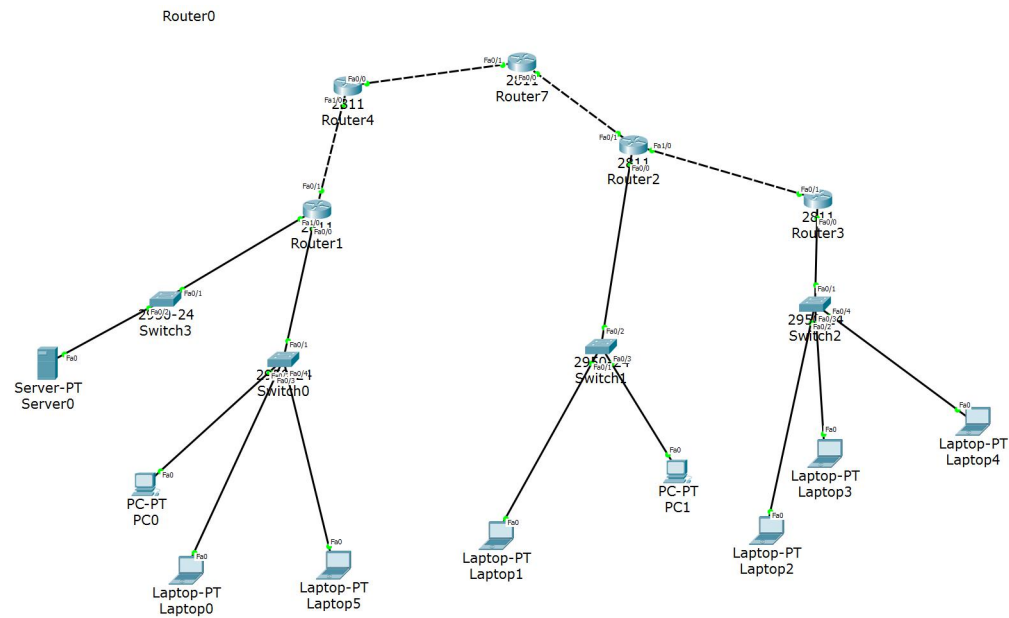
任务 8 蒸蒸日上 10'

由于公司事业蒸蒸日上，尹董事在三里屯购下了一处地皮成立分部，现决定将技术开发部搬迁至该处。由于公司总部与分部距离较远，因而公司的两个部分只能通过公网相连。请更改网络拓扑，在 Router1 和 Router2 中间增加公网路由器 Router4，使得 Router1 和 Router2 为公司分部与公司总部的两个边界路由器。

在搬迁之后，使用配置静态路由的方法将无法让各个部门正常通信，请简述原因。
在公网上一般无法做到直连，配置静态路由只能配置公司私网内以及私网和公网边界上的路由，因此如果使用静态路由配置，私网内的 PC 需要 ping 的话最多只能 ping 和边界路由直连的路由。而私网地址，如果没有 NAT 转换，是无法直接作为有效的 IP 地址与外界进行通信的，也就是说一个完全位于公网上的路由器无法转发 192.168.x.x/24 的路由。

为了解决通信问题，你使用了助手的提议，决定配置 IPSec VPN，让公司内网可以穿越公网。VPN 配置中涉及到的加密算法均使用 3des，哈希算法均使用 md5，秘钥协商算法使用 DH5 来协商具有一定强度的秘钥，并使用 esp 进行加密和认证。请完成相关配置，并表明配置步骤及最终结果。（由于网络重构，ACL 的配置将全部清空，重构后的公司内网暂不用考虑之前的 ACL 配置。）

- 1. 重新设计网络拓扑并配置 IP
清空之前的 ACL 配置。根据题目要求，新增加 Router4、7 用于模拟公网当中的路由器，设置 Router1、2 的边界端口。
重新设计网络拓扑如下：



新添加的端口以及 IP 如下：

Device	Port	IP	Mask	Gateway	实际使用的端口
Router1	端口 3	11.1.2.1	/8	-	0/1
Router2	端口 3	12.1.2.2	/8	-	0/1

Router4	端口 1	11.1.2.2	/8	-	1/0
	端口 2	13.1.2.2	/8	-	0/0
Router7	端口 1	13.1.2.1	/8	-	0/1
	端口 2	12.1.2.1	/8	-	0/0

2. 在 Router1:11.1.2.1 和 Router2:12.1.2.2 之间配置 IPsec VPN 通道

(1) R1 上进行配置

① 配置安全策略

```
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
```

② 配置预共享密钥

```
Router(config)#crypto isakmp key wangluoanquan2019fall address 12.1.2.2
```

③ 配置 Crypto ACL 需要保护的流量

```
Router(config)#access-list 101 permit ip 192.168.0.0 0.0.255.255 192.168.0.0
0.0.255.255
```

④ 配置 IPsec 传输集

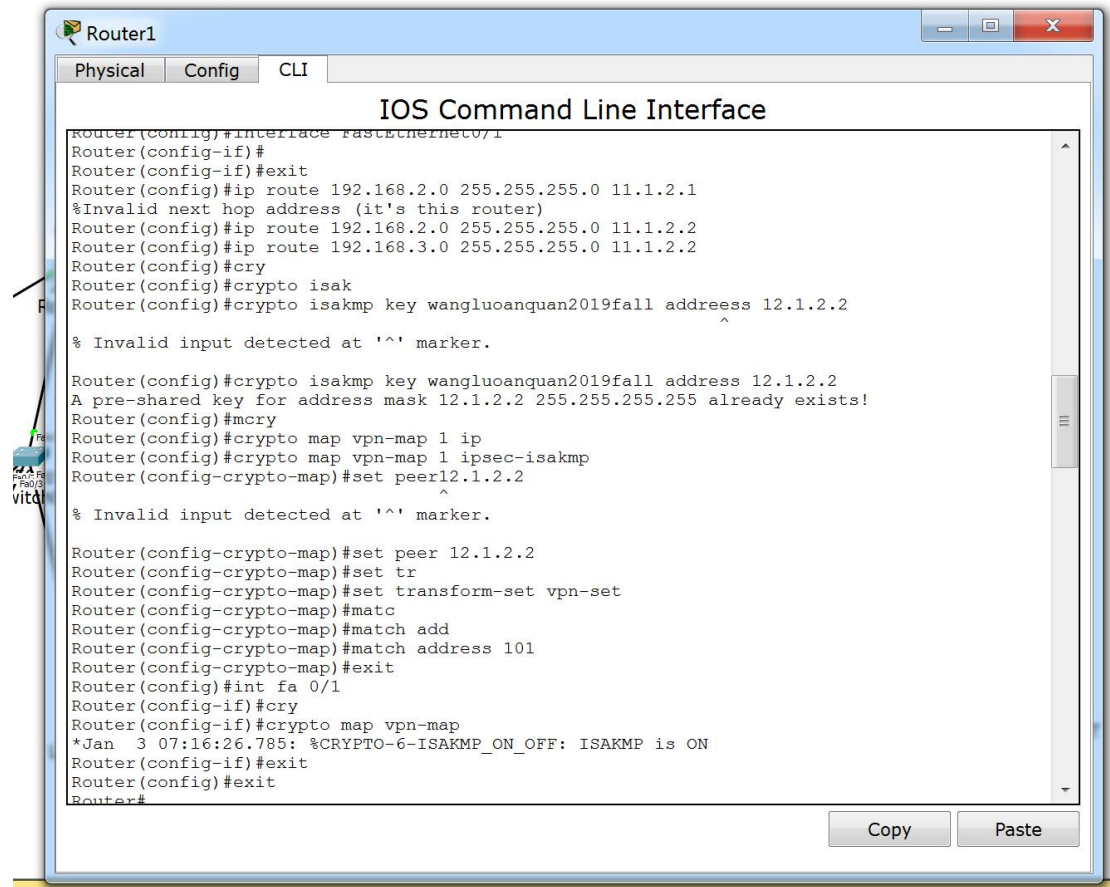
```
Router(config)#crypto ipsec transform-set vpn-set esp-des esp-sha-hmac
```

⑤ 配置 Crypto Map 加密映射，并将其应用到网关路由器外部接口

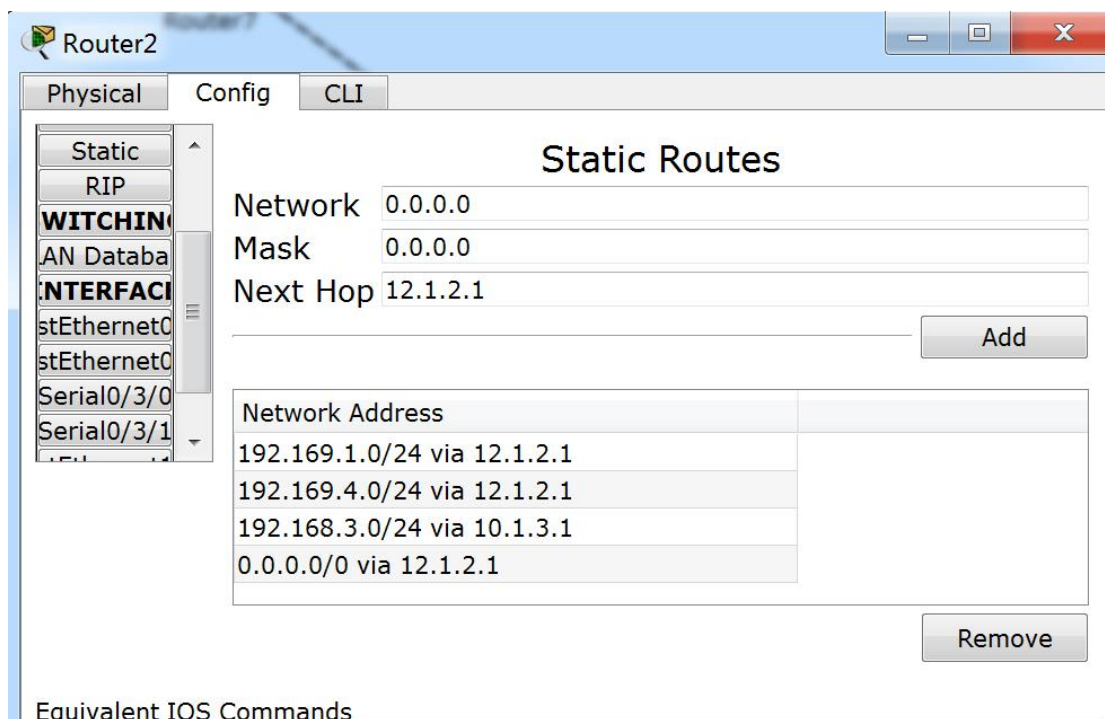
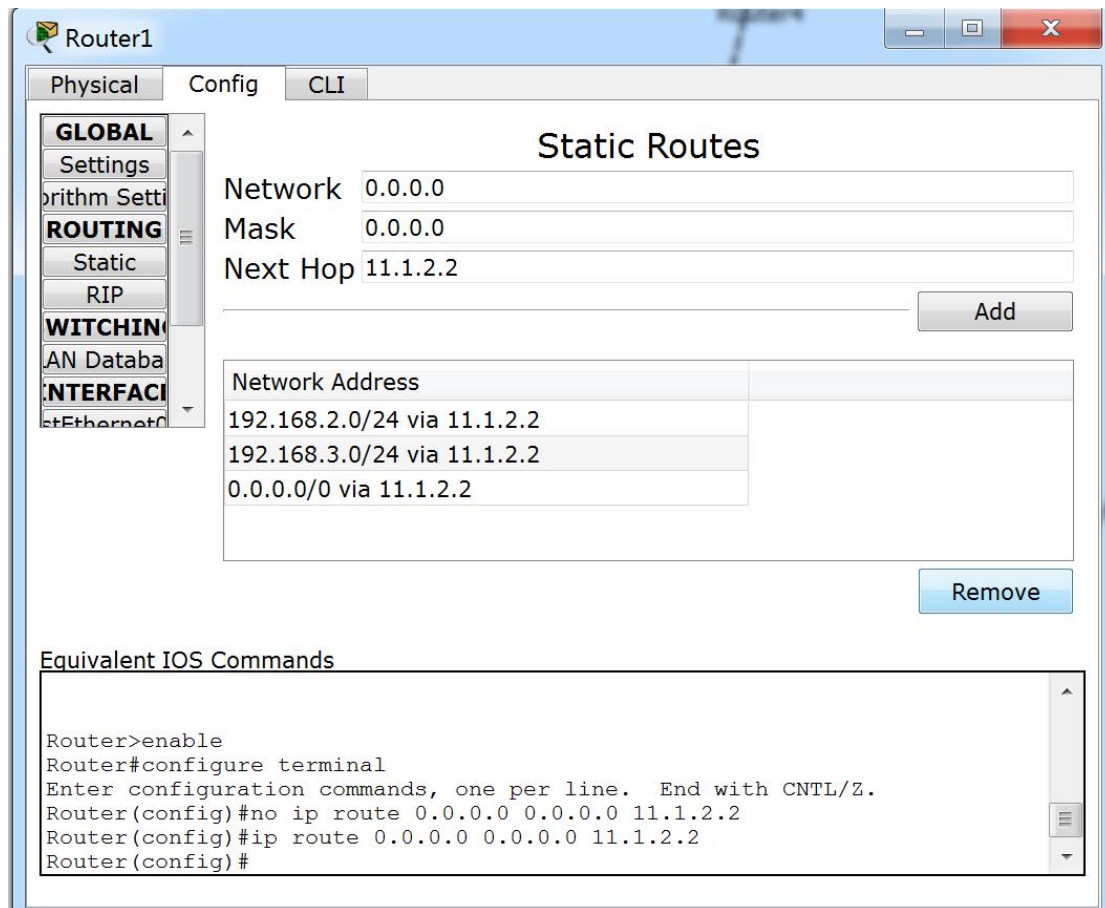
```
Router(config)#crypto map vpn-map 1 ipsec-isakmp
Router(config-crypto-map)#set peer 12.1.2.2
Router(config-crypto-map)#set transform-set vpn-set
Router(config-crypto-map)#match address 101
Router(config-crypto-map)#exit
```

⑥ 配置静态路由实现 VPN 数据通信

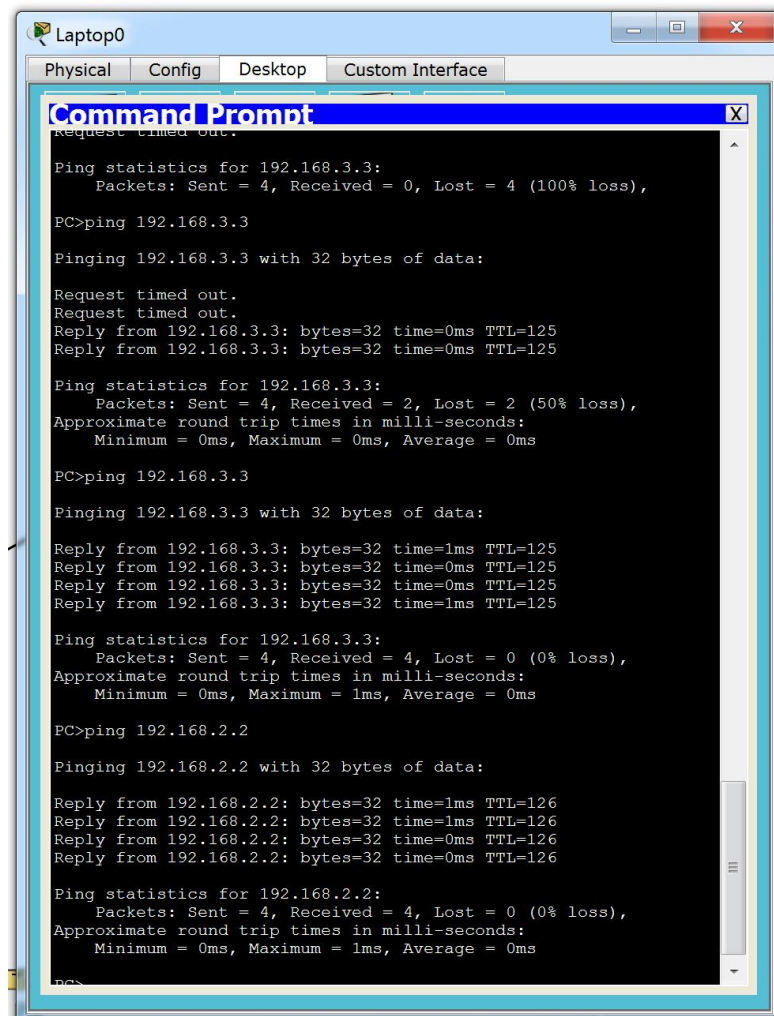
```
Router(config)#ip route 192.168.2.0 255.255.255.0 11.1.2.2
Router(config)#ip route 192.168.3.0 255.255.255.0 11.1.2.2
Router(config)#ip route 0.0.0.0 0.0.0.0 11.1.2.2
```



(2) R2 上进行配置同理。由于需要和 R1 通信，所以除了 isakmp policy 编号外其他都要和 R1 保持一致。另外静态路由的配置也不同。



- (3) 在 R4、R7 上配置 RIP 协议，用于模拟公网转发。
- (4) 连通性测试结果如下：



The screenshot shows a Packet Tracer interface for a device named 'Laptop0'. The 'Config' tab is selected. A 'Command Prompt' window is open, displaying the results of several ping commands. The first ping is to 192.168.3.3, which initially fails with 'Request timed out.' and '100% loss'. After a second attempt, it succeeds with '0% loss'. The second ping is to 192.168.2.2, which also succeeds with '0% loss'.

```
request timed out.

Ping statistics for 192.168.3.3:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

PC>ping 192.168.3.3

Pinging 192.168.3.3 with 32 bytes of data:

Request timed out.
Request timed out.
Reply from 192.168.3.3: bytes=32 time=0ms TTL=125
Reply from 192.168.3.3: bytes=32 time=0ms TTL=125

Ping statistics for 192.168.3.3:
    Packets: Sent = 4, Received = 2, Lost = 2 (50% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms

PC>ping 192.168.3.3

Pinging 192.168.3.3 with 32 bytes of data:

Reply from 192.168.3.3: bytes=32 time=1ms TTL=125
Reply from 192.168.3.3: bytes=32 time=0ms TTL=125
Reply from 192.168.3.3: bytes=32 time=0ms TTL=125
Reply from 192.168.3.3: bytes=32 time=1ms TTL=125

Ping statistics for 192.168.3.3:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 1ms, Average = 0ms

PC>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=0ms TTL=126
Reply from 192.168.2.2: bytes=32 time=0ms TTL=126

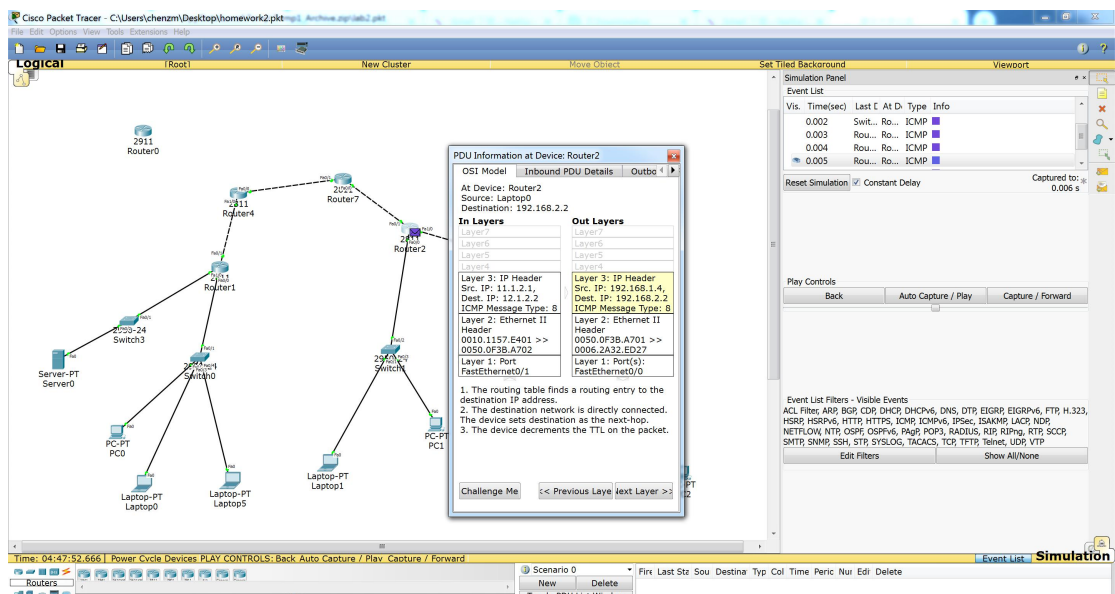
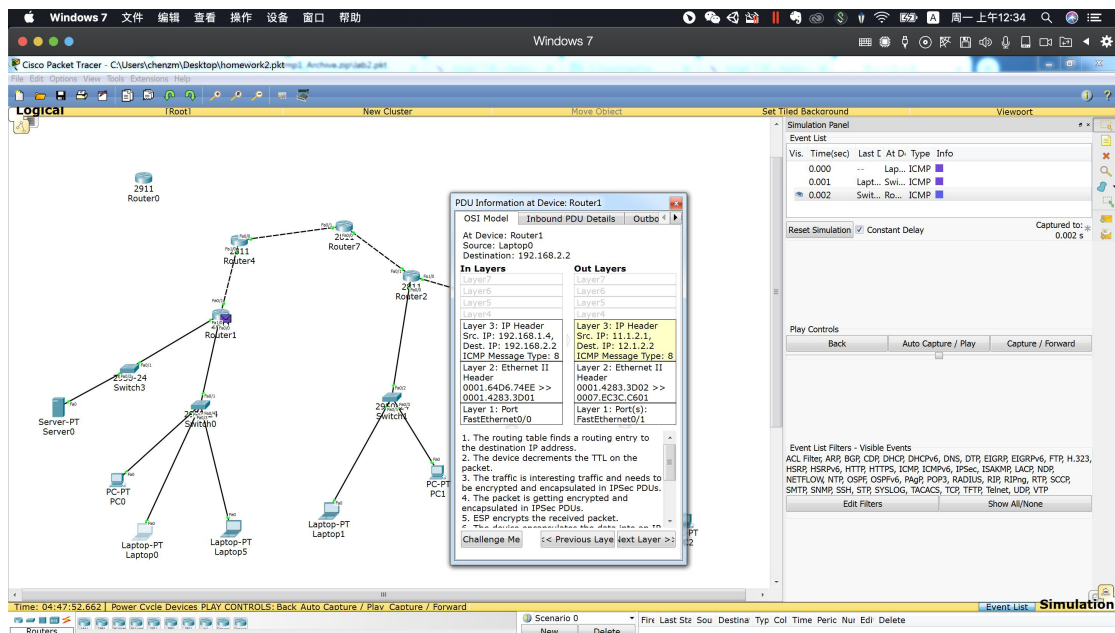
Ping statistics for 192.168.2.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 1ms, Average = 0ms

PC>
```

可见子网 1 中的设备可以正常和子网 2、3 中的设备进行通信。

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？

仿真抓包分析发现在 Router1 处报文的源 IP 和目的 IP 都会被修改公网 IP，在 Router2 处被修改回原来的私网 IP。可见在这里 IPSec VPN 使用了隧道模式。



传输模式不会修改 IP 头，而 192 开头的私网 IP 是不能在公网上被转发的。因此必须采用隧道模式。

Bonus 任务 探究新的应用场景 3'

探索 Packet Tracer 的功能，对已经学习过的其他网络知识进行关联和实践，说明其在网络安全的哪些应用中可以被使用，并设计一个场景进行尝试和研究。

可参考之前的同事曾经完成过的课题进行（最多 2'），也可以自行发现其他更有价值的场景（最多 3'），该任务根据难度及研究程度给分，每人仅可挑选一个探究方向。

可参考的探究方向：交换机的端口聚合、网络地址转换 NAT、DHCP 的配置、邮件服务器设置、NetFlow 流量监控、OSPF 协议研究.....