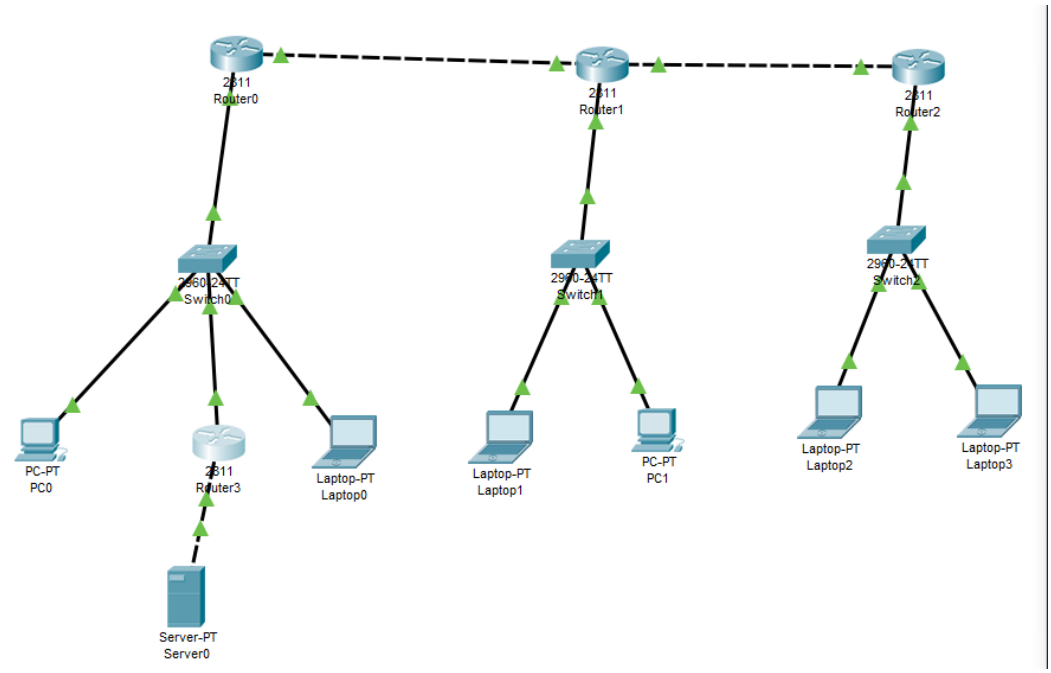
网络安全技术实践 HW2

计 71 张程远 2017011429

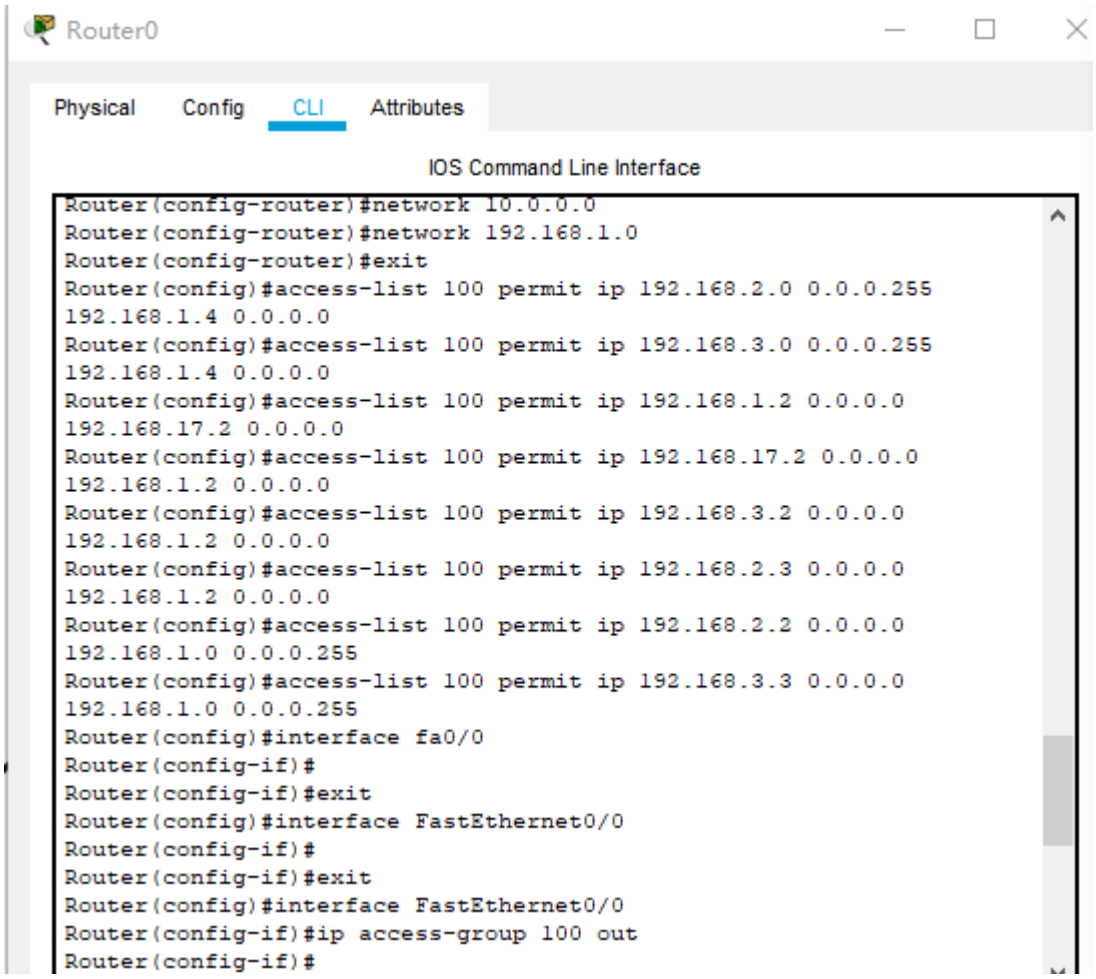
本次实验基于上一次的网络架构继续操作。

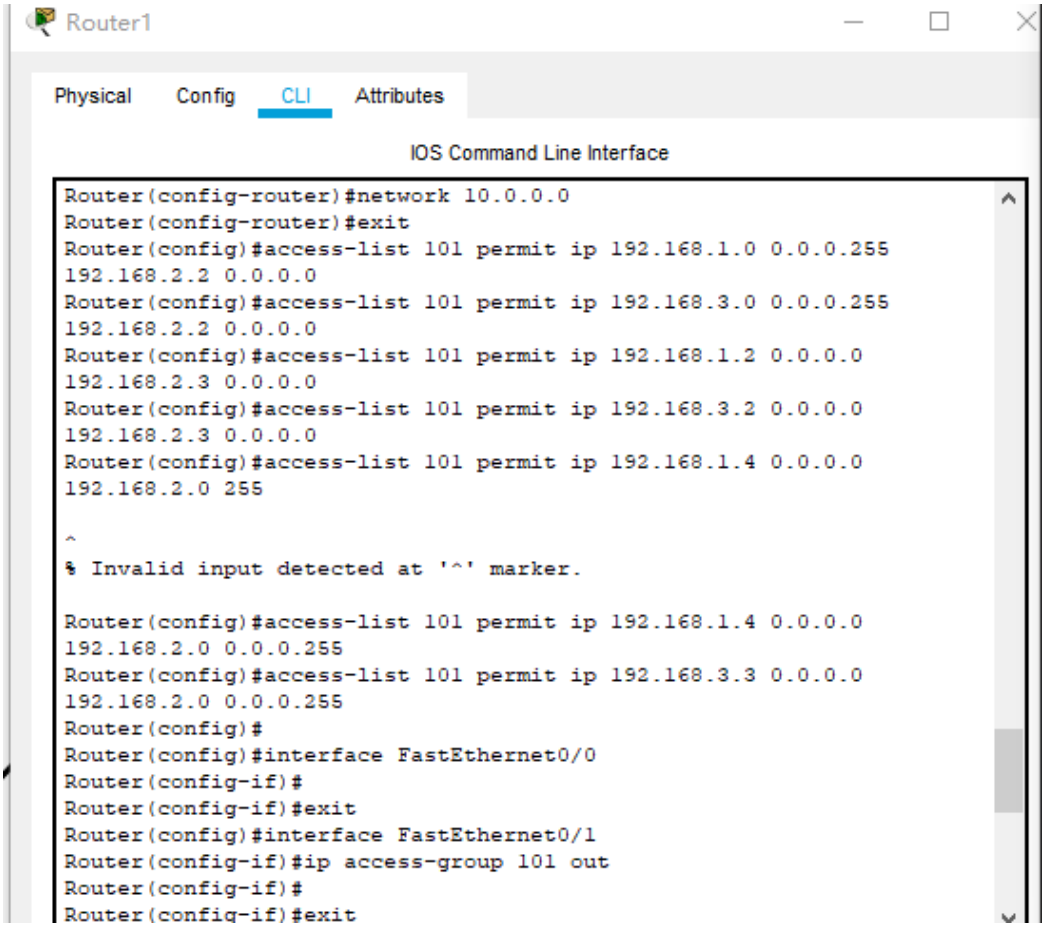
任务 6

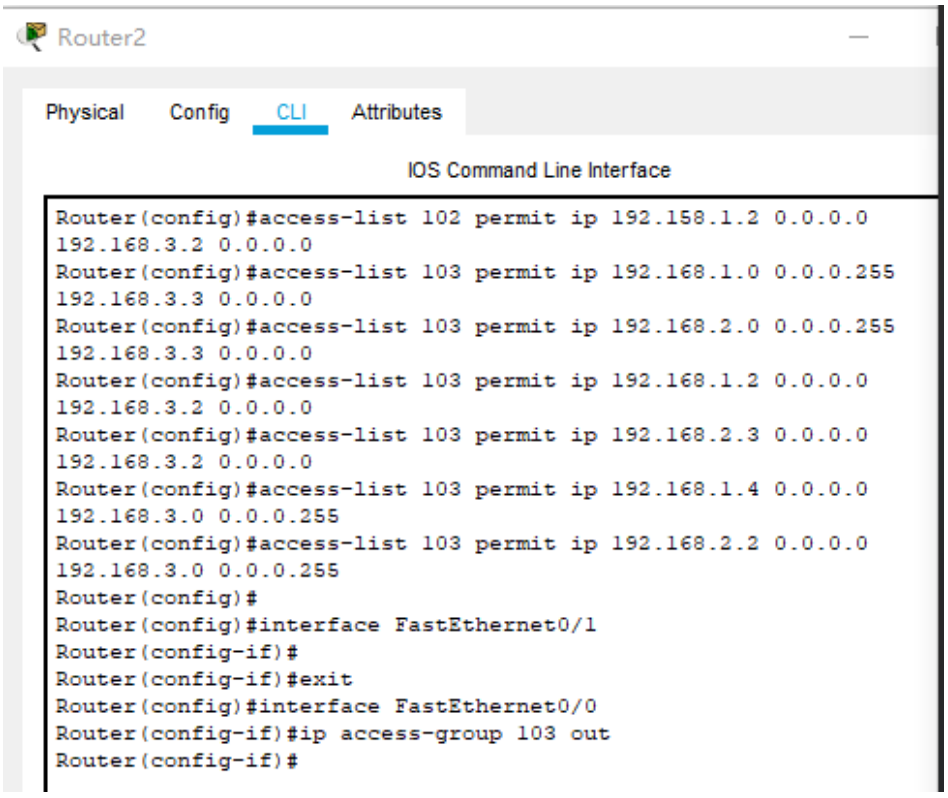
首先，题目要求 Laptop0 不能与 Server0 通信，因此一个自然的想法是把 Server0 置于另一个子网下，故添加一个 Router3，其位于 Switch1 和 Server0 之间。这里我给 Server0 设置的 IP 地址为 192.168.17.2，Router3 的两个端口的 IP 地址为 192.168.17.1 和 192.168.1.3。然后要给 Router3 设置 RIPv2 协议让其与网络其他部分能够通信。接下来设置 ACL，考虑到存在点对点的设置，因此采用扩展协议操作。对于每个 Router 控制子网的端口进行配置：让其他子网能与助手通信；让助手能访问到其他子网；让部长之间相互联系。对于 Server0 还需要单独配置。下面是修改过后的拓扑图。



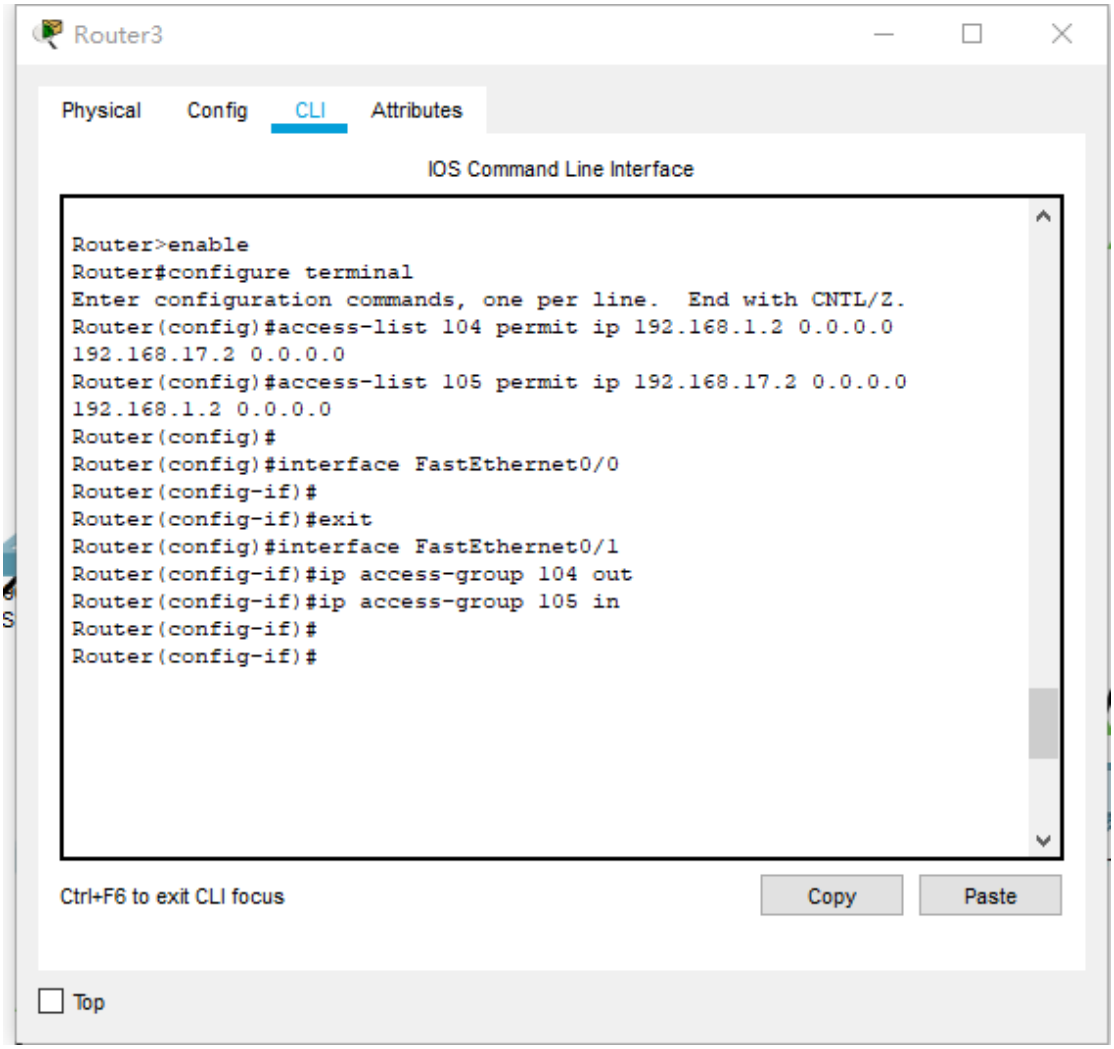
以下是对 4 个 Router 配置的命令。


Router0
Physical
Config
CLI
Attributes
IOS Command Line Interface
Router(config-router)#network 10.0.0.0
Router(config-router)#network 192.168.1.0
Router(config-router)#exit
Router(config)#access-list 100 permit ip 192.168.2.0 0.0.0.255
192.168.1.4 0.0.0.0
Router(config)#access-list 100 permit ip 192.168.3.0 0.0.0.255
192.168.1.4 0.0.0.0
Router(config)#access-list 100 permit ip 192.168.1.2 0.0.0.0
192.168.17.2 0.0.0.0
Router(config)#access-list 100 permit ip 192.168.17.2 0.0.0.0
192.168.1.2 0.0.0.0
Router(config)#access-list 100 permit ip 192.168.3.2 0.0.0.0
192.168.1.2 0.0.0.0
Router(config)#access-list 100 permit ip 192.168.2.3 0.0.0.0
192.168.1.2 0.0.0.0
Router(config)#access-list 100 permit ip 192.168.2.2 0.0.0.0
192.168.1.0 0.0.0.255
Router(config)#access-list 100 permit ip 192.168.3.3 0.0.0.0
192.168.1.0 0.0.0.255
Router(config)#interface fa0/0
Router(config-if)#
Router(config-if)#exit
Router(config)#interface FastEthernet0/0
Router(config-if)#
Router(config-if)#exit
Router(config)#interface FastEthernet0/0
Router(config-if)#ip access-group 100 out
Router(config-if)#

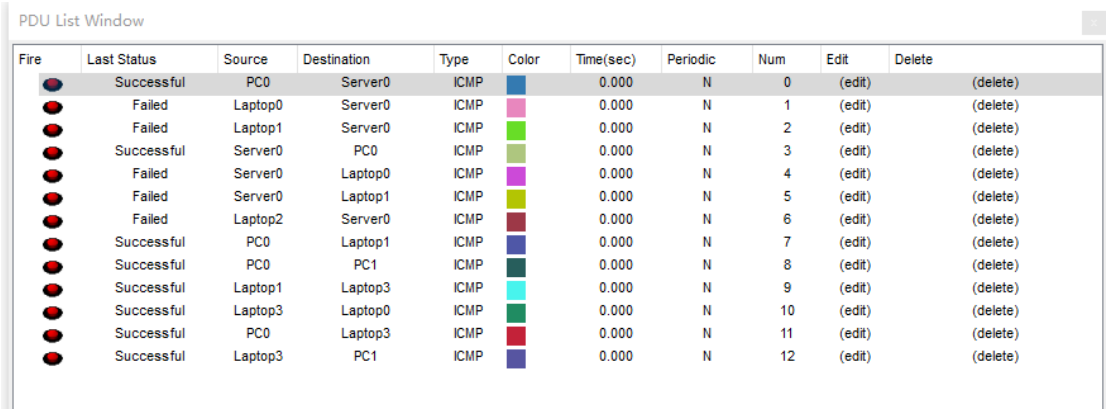




（这里 102 的配置出现了一些拼写错误，以 103 内容为准）



接下来设置几组 Simple PDU 的测试以查看设置效果。



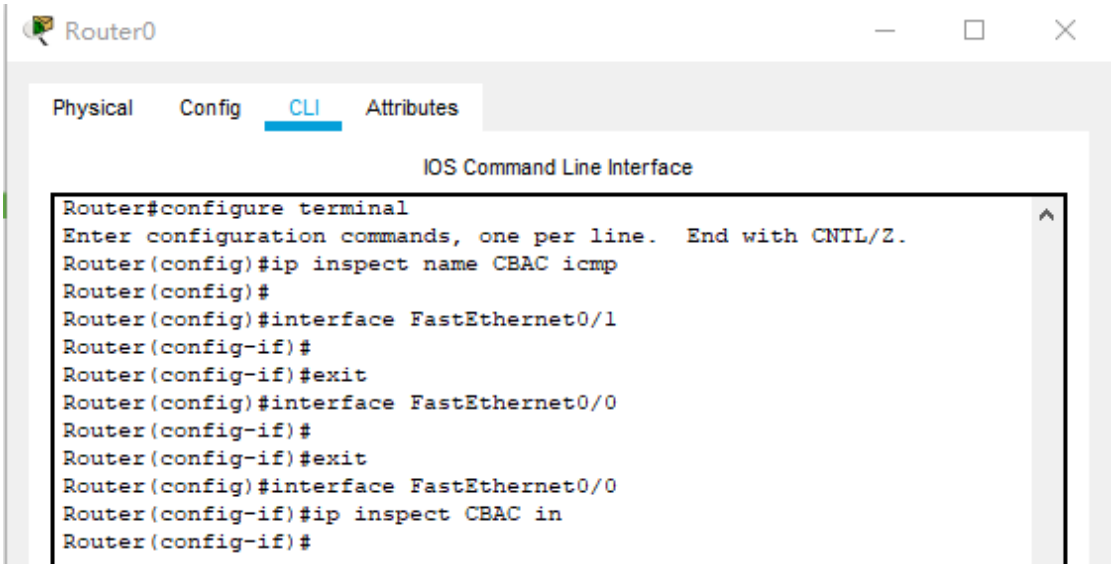
Fire	Last Status	Source	Destination	Type	Color	Time(sec)	Periodic	Num	Edit	Delete
	Successful	PC0	Server0	ICMP		0.000	N	0	(edit)	(delete)
	Failed	Laptop0	Server0	ICMP		0.000	N	1	(edit)	(delete)
	Failed	Laptop1	Server0	ICMP		0.000	N	2	(edit)	(delete)
	Successful	Server0	PC0	ICMP		0.000	N	3	(edit)	(delete)
	Failed	Server0	Laptop0	ICMP		0.000	N	4	(edit)	(delete)
	Failed	Server0	Laptop1	ICMP		0.000	N	5	(edit)	(delete)
	Failed	Laptop2	Server0	ICMP		0.000	N	6	(edit)	(delete)
	Successful	PC0	Laptop1	ICMP		0.000	N	7	(edit)	(delete)
	Successful	PC0	PC1	ICMP		0.000	N	8	(edit)	(delete)
	Successful	Laptop1	Laptop3	ICMP		0.000	N	9	(edit)	(delete)
	Successful	Laptop3	Laptop0	ICMP		0.000	N	10	(edit)	(delete)
	Successful	PC0	Laptop3	ICMP		0.000	N	11	(edit)	(delete)
	Successful	Laptop3	PC1	ICMP		0.000	N	12	(edit)	(delete)

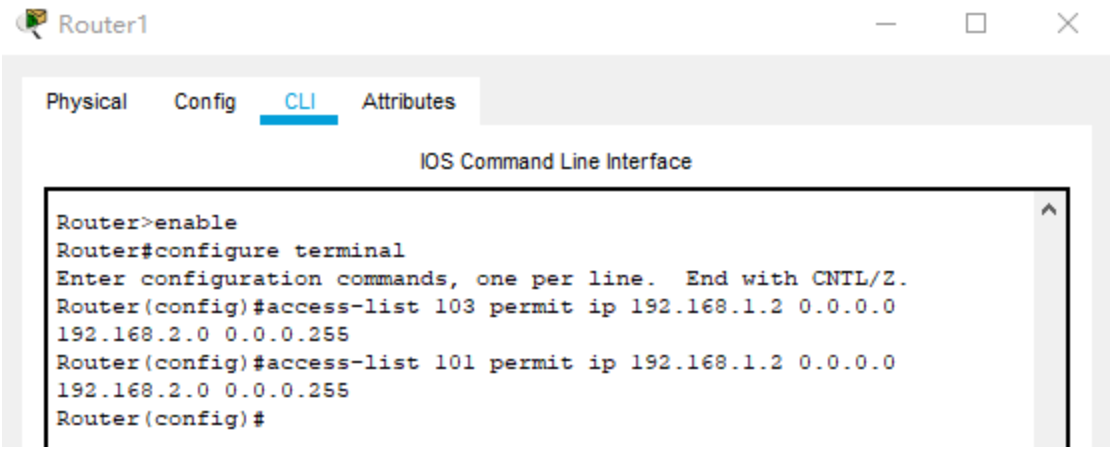
如图所示，前 7 组是网络中设备对 Server0 的访问情况，后面 6 组是网络中其他部分的互相访问情况。可以看到符合题目中的要求。

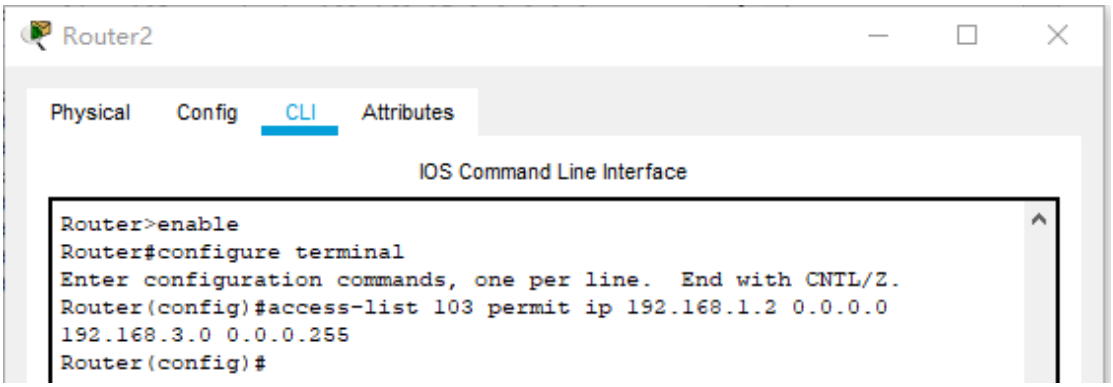
任务 7

按照题目要求，在 Router0 中使用 CBAC 过滤一下报文，然后在 Router1 和 Router2 的

ACL 中添加 192.168.1.2 的访问许可即可。下面是配置过程。







这时候，前面配置的 ACL 表项出现了冗余，应该把所有 PC0 在前的表项都删掉。即在 Router1 删除 access-list 101 permit ip 192.168.1.2 0.0.0.0 192.168.2.3 0.0.0.0 以及在 Router2 中删除 access-list 101 permit ip 192.168.1.2 0.0.0.0 192.168.3.2 0.0.0.0。具体做法是在 enable 模式下运行 sh access-lists，找到这两个表项的编号，然后输入 ip access-list extended 101（或 103），输入 no 编号 即可删除这一表项。这里要说明的是，虽然原本 PC0 也可以 ping

通助手，按理说也存在一定程度的冗余，但助手的表项是对子网内所有设备生效，所以无需对其进行修改。

下面是配置测试效果。

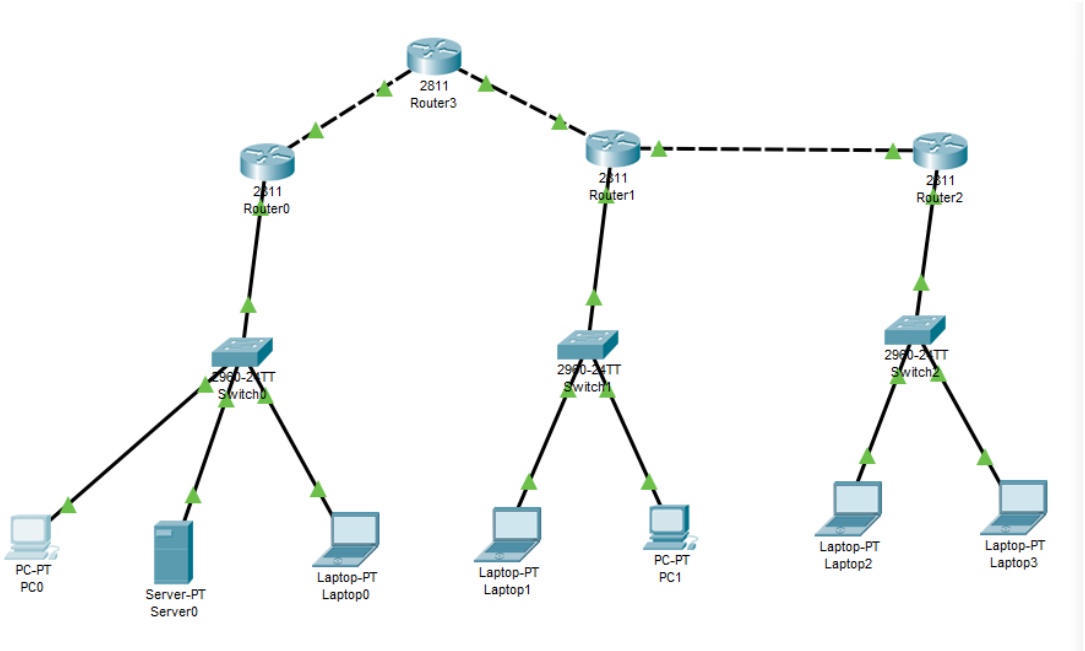
PDU List Window

Fire	Last Status	Source	Destination	Type	Color	Time(sec)	Periodic	Num	Edit	Delete
	Successful	PC0	Server0	ICMP		0.000	N	0	(edit)	(delete)
	Successful	PC0	Laptop0	ICMP		0.000	N	1	(edit)	(delete)
	Successful	PC0	Laptop1	ICMP		0.000	N	2	(edit)	(delete)
	Successful	PC0	PC1	ICMP		0.000	N	3	(edit)	(delete)
	Successful	PC0	Laptop3	ICMP		0.000	N	4	(edit)	(delete)
	Successful	PC0	Laptop2	ICMP		0.000	N	5	(edit)	(delete)

可以看到 PC0 能够访问到网络的所有设备。

任务 8

静态路由失效的原因是：公网无法转发 192.168 开头的路由，因为公网上基本不存在直连的情况。鉴于此，我们需要配置 IPSec VPN 来让公司内网穿越公网。按要求将网络的拓扑图修改如下：



经过 ping 我们发现，Router1 和 Router2 的设备可以互相 ping 通，因为它们没有走公网的 router；而此时 Router0 和另外两个子网下的设备无法通信。为此我们先给 Router3 配置一些基本信息：将 Router3 的端口 IP 分别设置为 169.224.1.1 和 169.225.1.1，Router0 与公网相连的端口设为 169.224.1.2，Router1 设置为 169.225.1.2。

接下来给 Router0 和 Router1 做配置。设置加密算法为 3des（enc 3des），认证算法为 md5（hash md5），密钥协商算法为 dh5（group 5），peer 为对方路由器的地址，然后设置 transform-set 为 chengyua17，设置 map 为 dogfarmap，绑定相应的 ACL，然后将 ACL 配

置到相应端口上并启动 map。具体流程为：

对 Router0 设置：

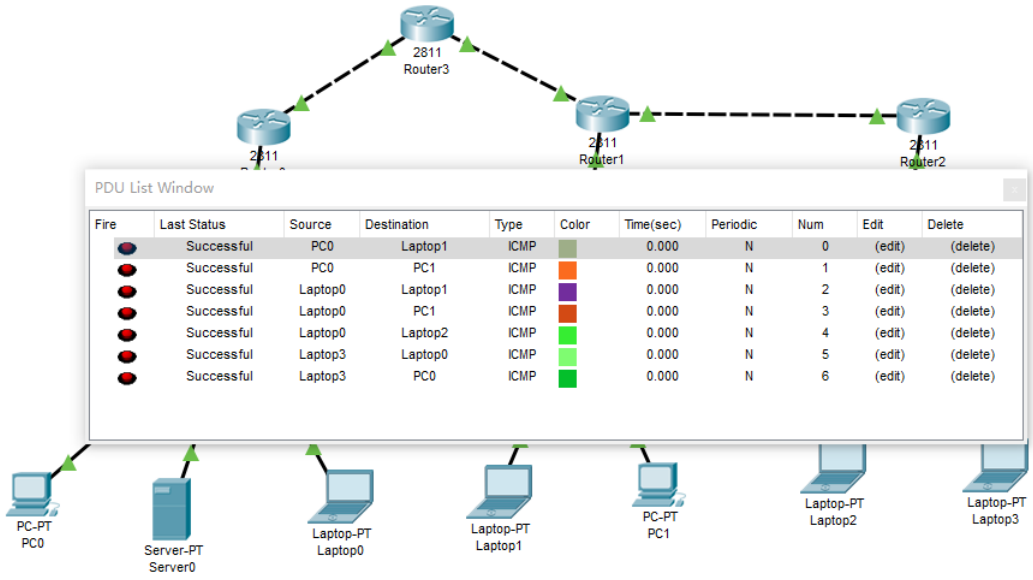
```
Router(config)#crypto isakmp policy 1
Router(config-isakmp)#enc 3des
Router(config-isakmp)#hash md5
Router(config-isakmp)#auth pre-share
Router(config-isakmp)#group 5
Router(config-isakmp)#exit
Router(config)#crypto isakmp key chengyual7 address 169.225.1.2
Router(config)#crypto ipsec transform-set chengyual7 esp-3des esp-md5
Router(config)#crypto map dogfarmap 1 ips
% NOTE: This new crypto map will remain disabled until a peer
        and a valid access list have been configured.
Router(config-crypto-map)#exit
Router(config)#access-list 100 permit ip 192.168.1.0 0.0.0.255 192.168.2.0 0.0.0.255
Router(config)#access-list 100 permit ip 192.168.1.0 0.0.0.255 192.168.3.0 0.0.0.255
Router(config)#
Router(config)#interface FastEthernet0/1
Router(config-if)#ip access-group 100 out
Router(config-if)#exit
Router(config)#crypto map dogfarmap 1 ips
Router(config-crypto-map)#set peer 169.225.1.2
Router(config-crypto-map)#set transform-set chengyual7
Router(config-crypto-map)#match addr 100
Router(config-crypto-map)#exit
Router(config)#
Router(config)#interface FastEthernet0/1
Router(config-if)#crypto map dogfarmap
*Jan  3 07:16:26.785: %CRYPTO-6-ISAKMP_ON_OFF: ISAKMP is ON
```

对 Router1 设置：

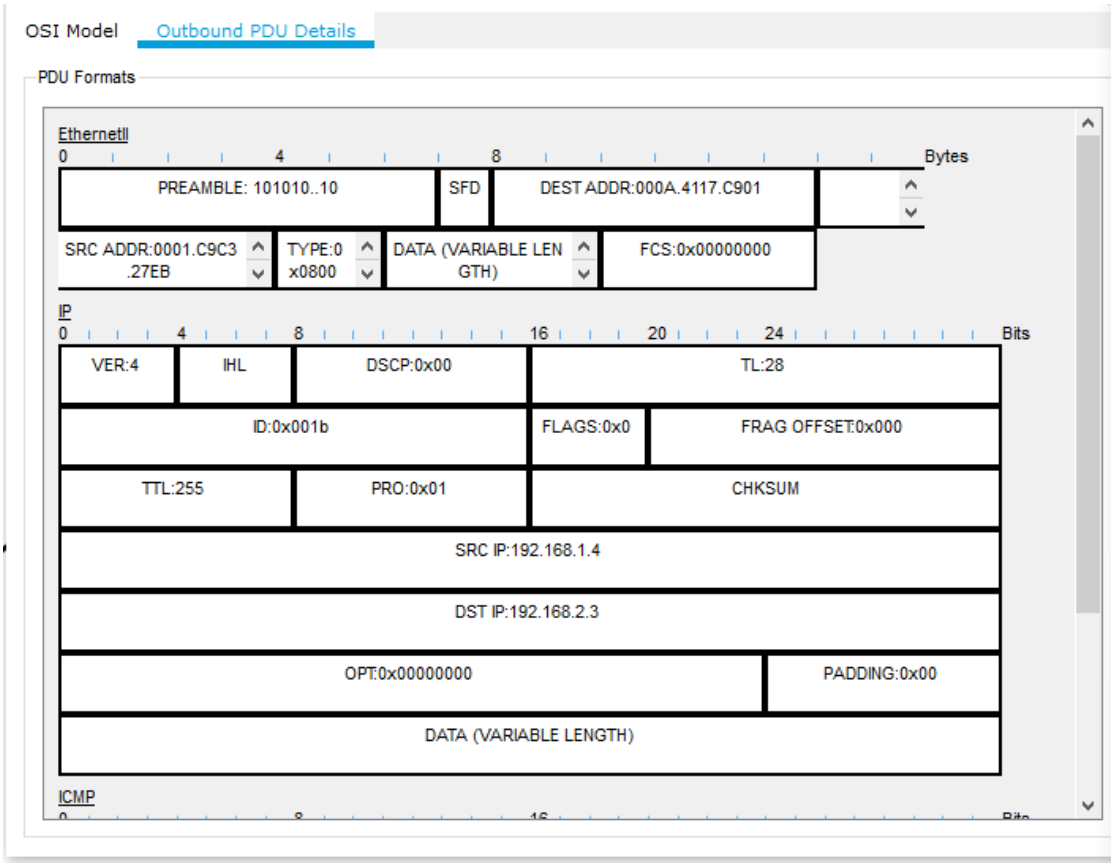
```
Router(config)#crypto isakmp policy 1
Router(config-isakmp)#enc 3des
Router(config-isakmp)#hash md5
Router(config-isakmp)#auth pre-share
Router(config-isakmp)#group 5
Router(config-isakmp)#exit
Router(config)#crypto isakmp chengyual7 address 169.224.1.2
                              ^
% Invalid input detected at '^' marker.

Router(config)#crypto isakmp key chengyual7 address 169.224.1.2
Router(config)#crypto ipsec transform-set chengyual7 esp-3des esp-md5
Router(config)#crypto map dogfarmap 1 ips
% NOTE: This new crypto map will remain disabled until a peer
        and a valid access list have been configured.
Router(config-crypto-map)#exit
Router(config)#access-list 101 permit ip 192.168.2.0 0.0.0.255 192.168.1.0 0.0.0.255
Router(config)#access-list 101 permit ip 192.168.3.0 0.0.0.255 192.168.1.0 0.0.0.255
Router(config)#
Router(config)#interface FastEthernet0/1
Router(config-if)#ip access-group 101 out
Router(config-if)#crypto map dogfarmap 1 ips
Router(config-crypto-map)#set peer 169.224.1.2
Router(config-crypto-map)#set transform-set chengyual7
Router(config-crypto-map)#match addr 101
Router(config-crypto-map)#exit
Router(config)#
Router(config)#interface FastEthernet0/1
Router(config-if)#crypto map dogfarmap
*Jan  3 07:16:26.785: %CRYPTO-6-ISAKMP_ON_OFF: ISAKMP is ON
Router(config-if)#
```

然后做测试，发现原来无法通信的 PC0 和 Laptop1 能 ping 通了，于是做了几组测试验证子网之间能够 Ping 通，如下图。



于是任务完成！接下来进行抓包。运行 Simulation 仿真，让 Laptop0 和 Laptop1 之间发送数据包，捕获到包的格式如下图：



IP 头并未被修改，因此使用的不是隧道模式，故为传输模式。