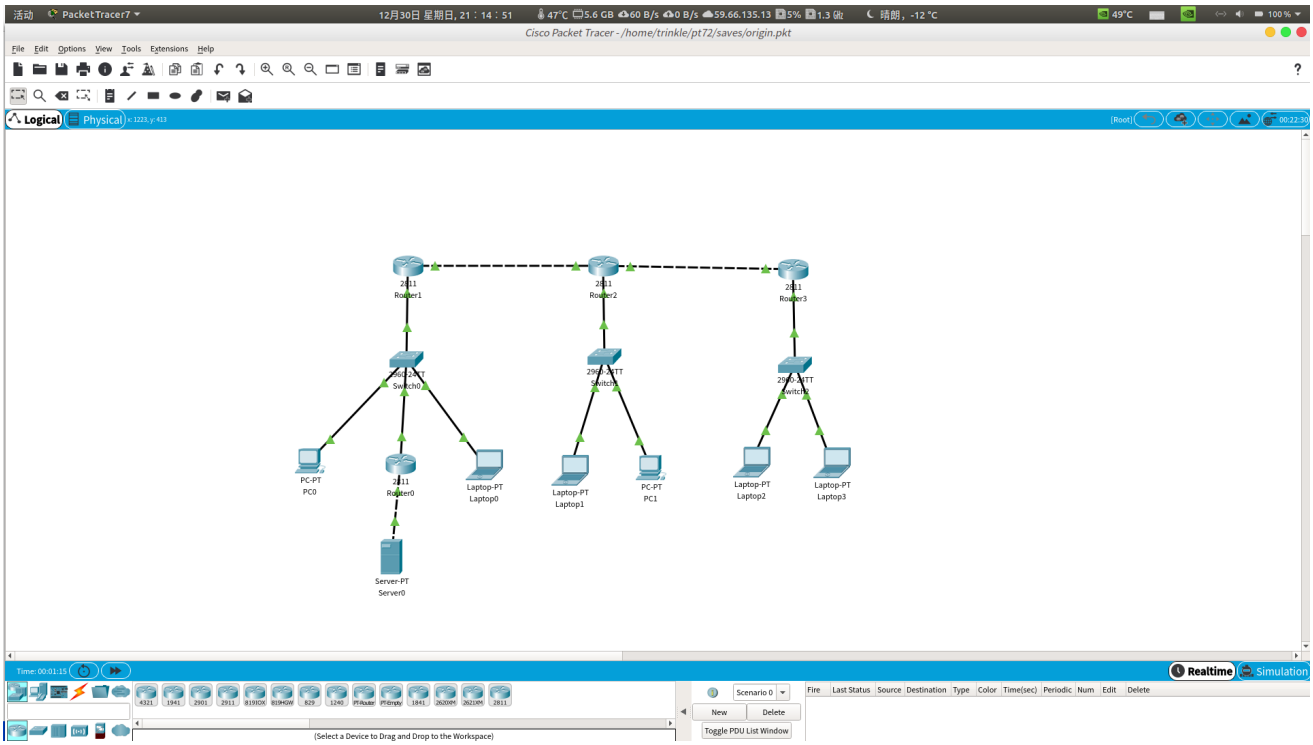
网络配置实验2

> 计64 翁家翌 2016011446

任务6

由于要对Server0进行严格的控制，所以将拓扑结构改为下图所示，增加了一个路由器Router0来控制Server0的访问，如下图所示：



对于所有Router，只配置其下方的端口，就是和子网连接的那个

Router1的out：

```
# 其他两个子网可以ping通助手
access-list 100 permit ip 192.168.2.0 0.0.0.255 192.168.1.4 0.0.0.0
access-list 100 permit ip 192.168.3.0 0.0.0.255 192.168.1.4 0.0.0.0
# 其他两个子网的秘书（助手）可以ping通本子网下所有机器
access-list 100 permit ip 192.168.2.2 0.0.0.0 192.168.1.0 0.0.0.255
access-list 100 permit ip 192.168.3.3 0.0.0.0 192.168.1.0 0.0.0.255
# 其他两个子网的部长，可以ping通本子网的助手和部长
access-list 100 permit ip 192.168.2.3 0.0.0.0 192.168.1.4 0.0.0.0
access-list 100 permit ip 192.168.2.3 0.0.0.0 192.168.1.2 0.0.0.0
access-list 100 permit ip 192.168.3.2 0.0.0.0 192.168.1.4 0.0.0.0
access-list 100 permit ip 192.168.3.2 0.0.0.0 192.168.1.2 0.0.0.0
# pc0可以ping通server0
access-list 100 permit ip 192.168.1.2 0.0.0.0 192.168.100.1 0.0.0.0
access-list 100 permit ip 192.168.100.1 0.0.0.0 192.168.1.2 0.0.0.0
```

```
# interface fa0/1
ip access-group 100 out
```

Router0用来限制Server0的访问

```
access-list 101 permit ip 192.168.100.1 0.0.0.0 192.168.1.2 0.0.0.0
access-list 102 permit ip 192.168.1.2 0.0.0.0 192.168.100.1 0.0.0.0
interface fa0/0
ip access-group 101 in
ip access-group 102 out
```

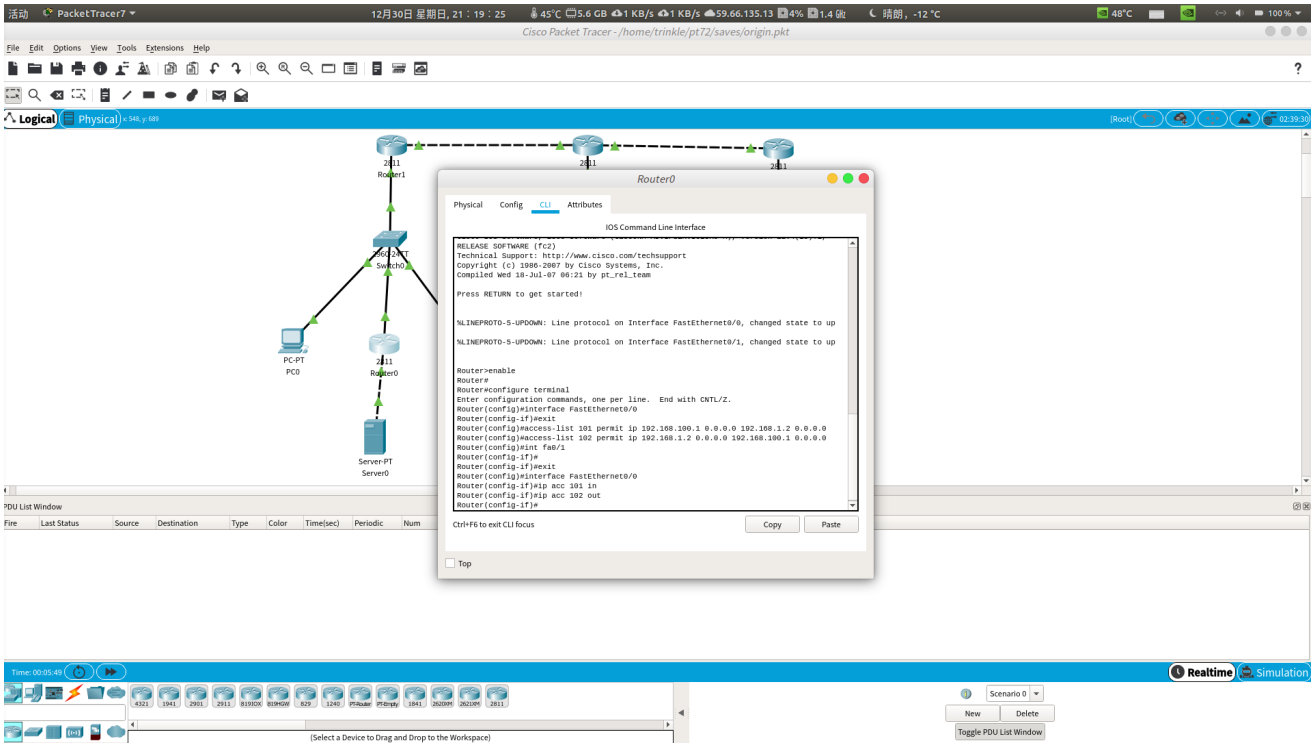
Router2的out:

```
access-list 103 permit ip 192.168.1.0 0.0.0.255 192.168.2.2 0.0.0.0
access-list 103 permit ip 192.168.3.0 0.0.0.255 192.168.2.2 0.0.0.0
access-list 103 permit ip 192.168.1.2 0.0.0.0 192.168.2.3 0.0.0.0
access-list 103 permit ip 192.168.1.4 0.0.0.0 192.168.2.3 0.0.0.0
access-list 103 permit ip 192.168.3.2 0.0.0.0 192.168.2.3 0.0.0.0
access-list 103 permit ip 192.168.3.3 0.0.0.0 192.168.2.3 0.0.0.0
interface fa0/1
ip access-group 103 out
```

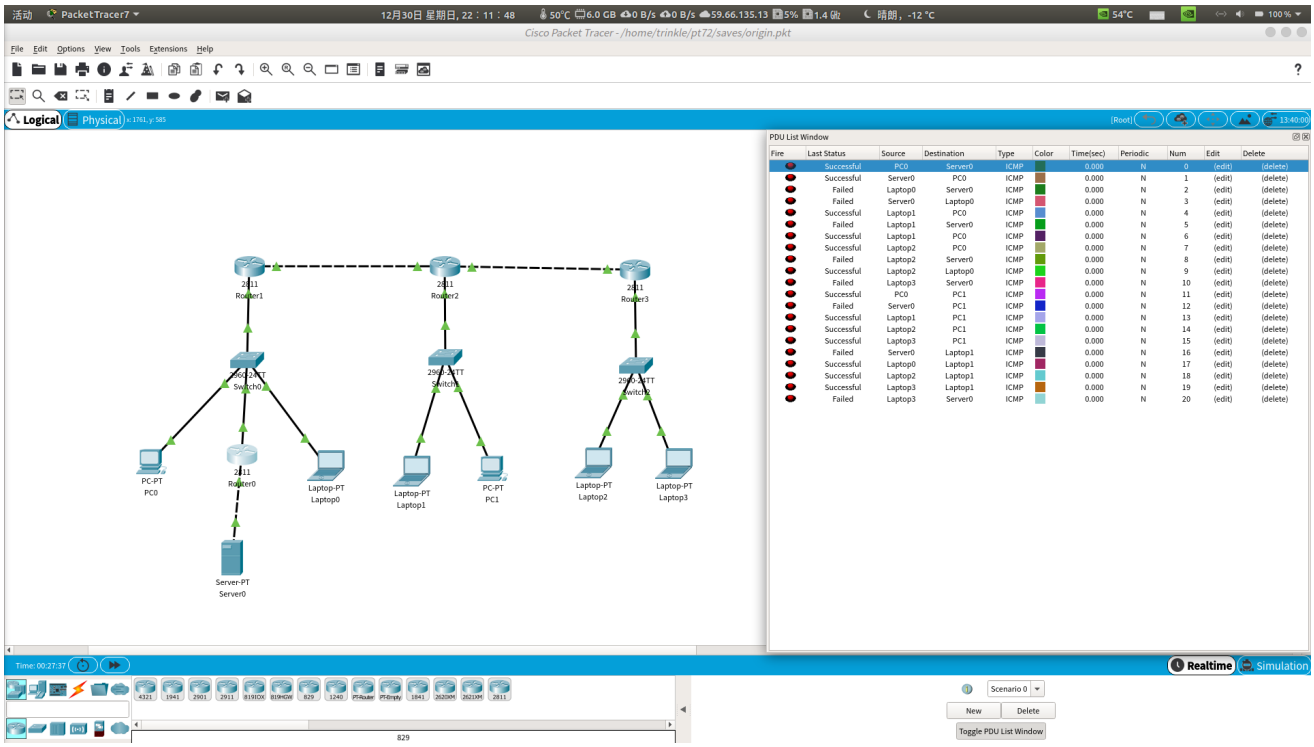
Router3的out:

```
access-list 104 permit ip 192.168.1.0 0.0.0.255 192.168.3.3 0.0.0.0
access-list 104 permit ip 192.168.2.0 0.0.0.255 192.168.3.3 0.0.0.0
access-list 104 permit ip 192.168.1.2 0.0.0.0 192.168.3.2 0.0.0.0
access-list 104 permit ip 192.168.1.4 0.0.0.0 192.168.3.2 0.0.0.0
access-list 104 permit ip 192.168.2.3 0.0.0.0 192.168.3.2 0.0.0.0
access-list 104 permit ip 192.168.2.2 0.0.0.0 192.168.3.2 0.0.0.0
interface fa0/1
ip access-group 104 out
```

配置现场截图如下:



测试结果如下：



从图中右侧的一系列测试结果，对照之前的表格，可以证明配置准确无误。具体解释如下：

number 0-10：第一个子网配好之后的功能测试，比如PC0可以ping通S0而其他机子不行；

number 11-19：第二、三个子网配好之后的功能测试，秘书之间能够相互ping通，部长之间能够相互ping通，等等。

任务7

在Router1上使用CBAC过滤icmp报文：

```
ip inspect name CBAC icmp
int fa0/1
ip inspect CBAC in
```

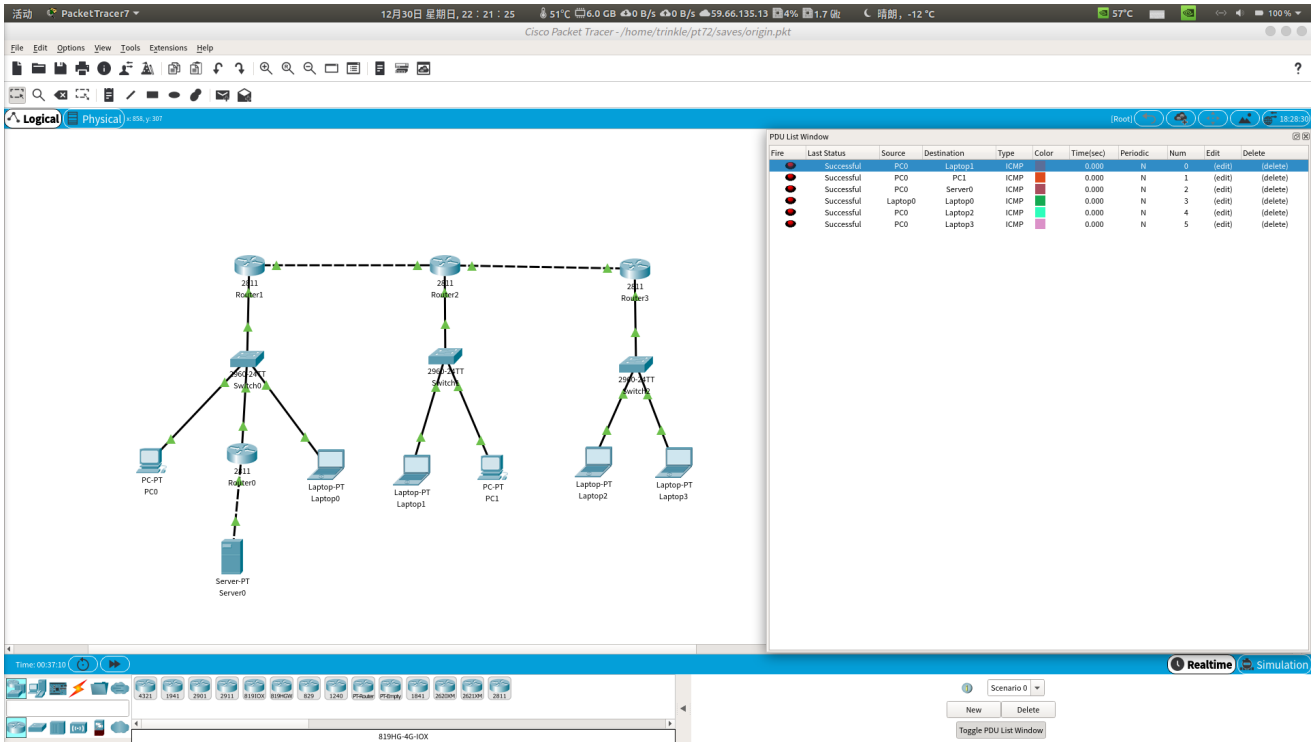
在Router2中的ACL 103增加

```
access-list 103 permit ip 192.168.1.2 0.0.0.0 192.168.2.0 0.0.0.255
```

在Router3中的ACL 104增加

```
access-list 104 permit ip 192.168.1.2 0.0.0.0 192.168.3.0 0.0.0.255
```

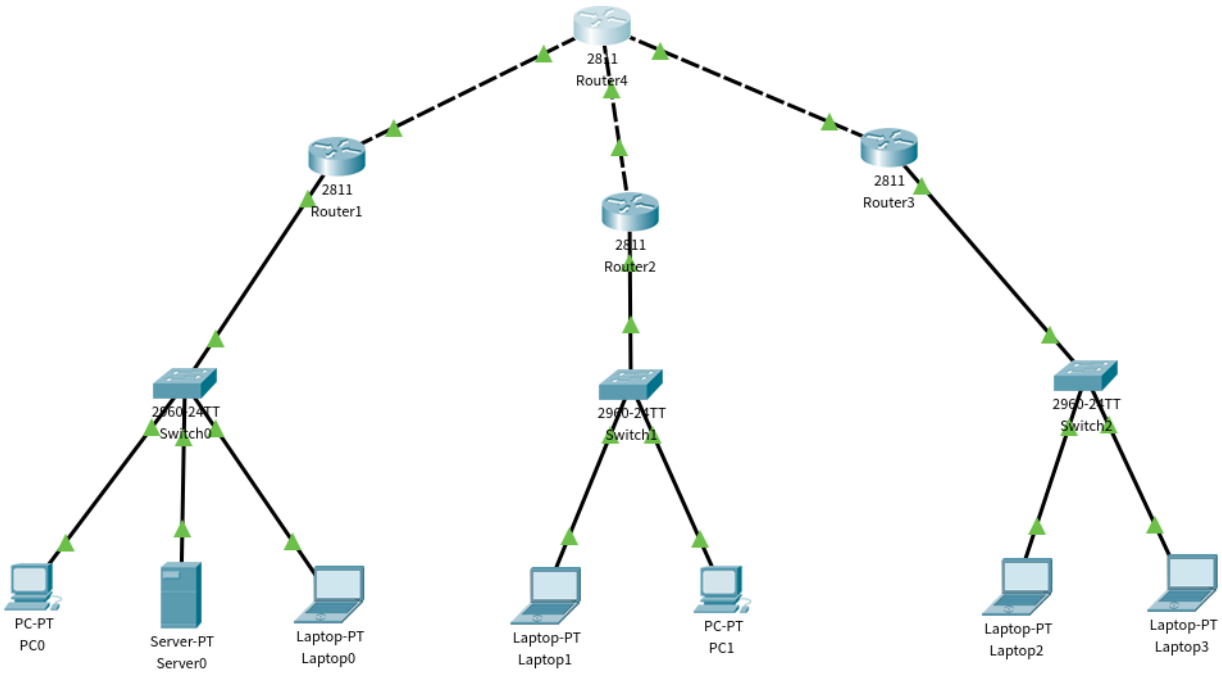
配置完成之后，结果如下所示：



可以看到PC0能够ping通所有子网中的机子。

任务8

恢复成最初的拓扑之后，添加Router4，给一块NM-2FE2W，Router1出口ip设置为100.1.1.4，Router2出口ip设置为100.2.2.4，Router3出口ip为100.3.3.4，Router4的3个公网ip分别为100.1.1.1、100.2.2.2、100.3.3.3，连通之后如下图所示：

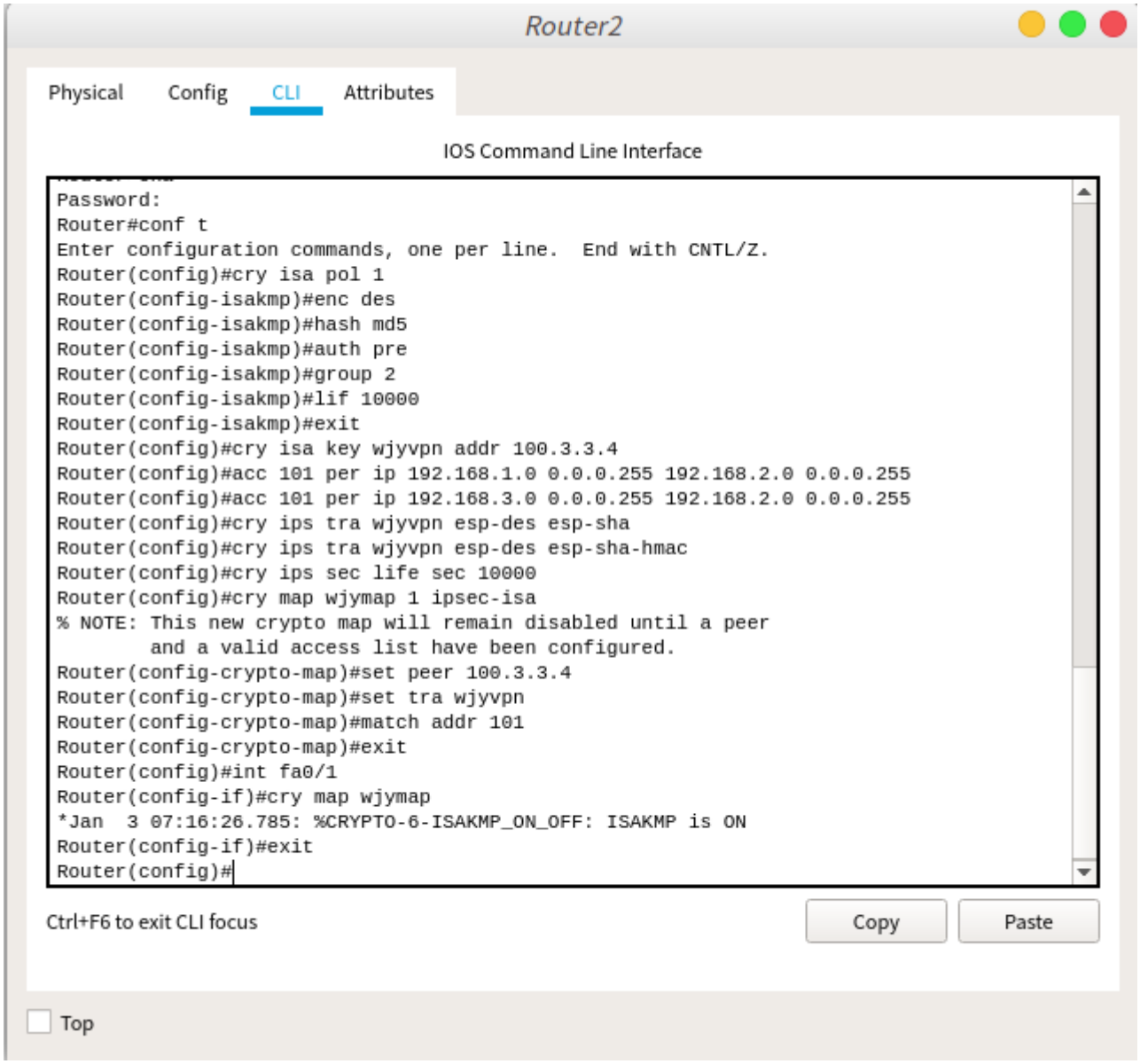


静态路由失效：公网上一般无法做到直连，因此在公网无法转发类似192.168.x.x/24的路由。

设置VPN我采取两两设置的方式，一共需要三对，以下以Router2-3之间为例。

Router2配置IPSec VPN如下：

主要思路是先设置IKE协商策略,设置加密算法为des，认证算法为md5，同时设置对端地址为另一个router（Router2则设置Router3 的地址，Router3设置Router2 的地址，同时确保加密密钥匹配。之后配置IPSec传输模式，定义VPN的认证类型。在最后配置加密映射crypto map，并将其应用到对应公网接口上，使VPN生效。



全部配置完成之后测试效果如下：

Laptop1

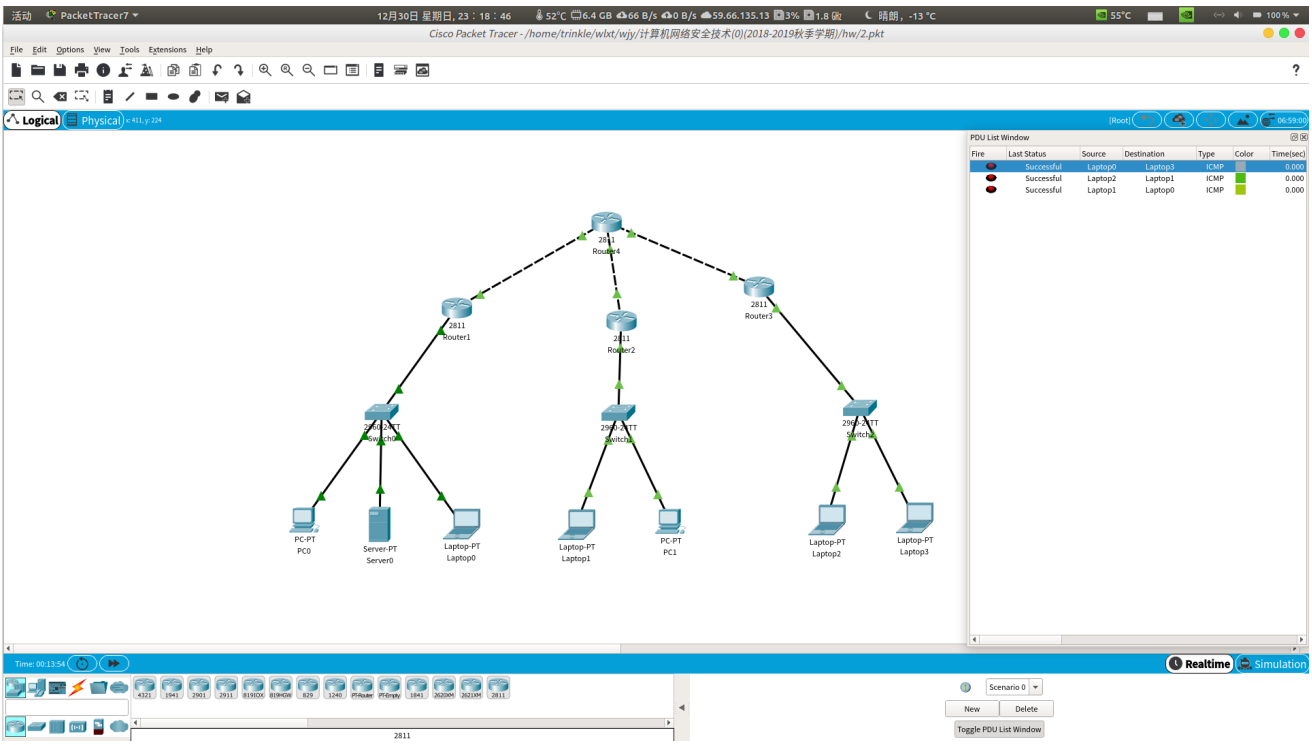
Physical Config Desktop Programming Attributes

Command Prompt

```
C:\>ping 192.168.1.3

Pinging 192.168.1.3 with 32 bytes of data:

Reply from 192.168.1.3: bytes=32 time=17ms TTL=125

Ping statistics for 192.168.1.3:
    Packets: Sent = 1, Received = 1, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 17ms, Maximum = 17ms, Average = 17ms

Control-C
^C
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=125

Ping statistics for 192.168.1.2:
    Packets: Sent = 1, Received = 1, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms

Control-C
^C
C:\>ping 192.168.3.2

Pinging 192.168.3.2 with 32 bytes of data:

Reply from 192.168.3.2: bytes=32 time<1ms TTL=125

Ping statistics for 192.168.3.2:
    Packets: Sent = 1, Received = 1, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms

Control-C
^C
C:\>
```

Top

从L1 ping 其他子网的终端设备均可成功ping通。



各个子网之间能够相互ping通。