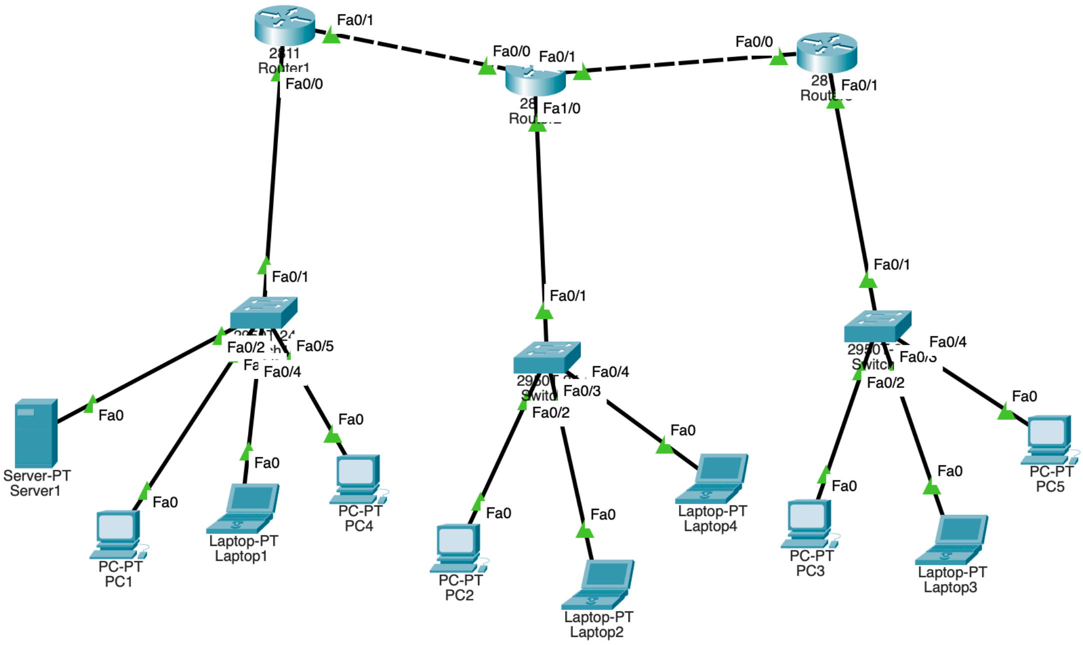
Lab 2

by flrs

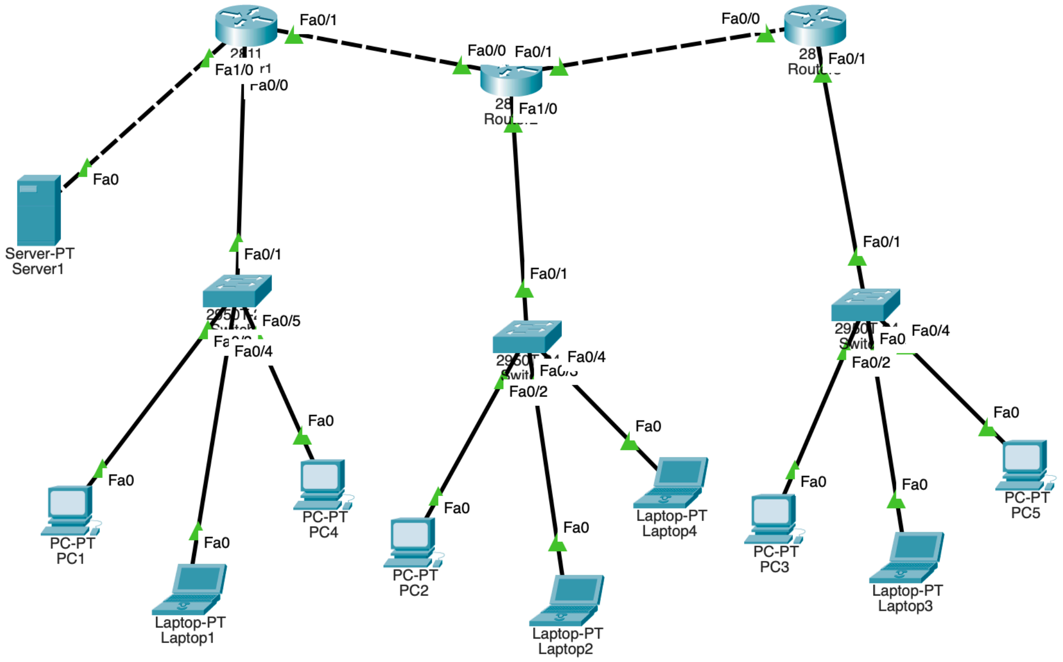
> 课程：计算机网络安全技术（2023秋）

实验背景



Task 6

为了适应需求，我对网络拓扑稍作了修改，并将 Server1 的 IP 地址修改为 `192.168.1.130/25`：



为使得非法请求也能尽快得到destination host unreachable 的回复而非等待 request timed out，也出于安全性的考虑，这里对相关端口的 in/out 均进行了 access-list 的配置。

各路由器的 access-list 和相关配置如下：

- Router1:

```
interface FastEthernet0/0
 ip address 192.168.1.1 255.255.255.0
 ip access-group 101 in
 ip access-group 100 out

interface FastEthernet1/0
 ip address 192.168.1.129 255.255.255.128
 ip access-group 103 in
 ip access-group 102 out
```

```
Extended IP access list 100
    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 host 192.168.2.2 any
    40 permit ip host 192.168.3.3 any
    50 permit ip any host 192.168.1.4
    60 permit ip host 192.168.1.130 host 192.168.1.2
Extended IP access list 101
```

```
    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 any host 192.168.2.2
    40 permit ip any host 192.168.3.3
    50 permit ip host 192.168.1.4 any
    60 permit ip host 192.168.1.2 host 192.168.1.130
Extended IP access list 102
    10 permit ip host 192.168.1.2 host 192.168.1.130
Extended IP access list 103
    10 permit ip host 192.168.1.130 host 192.168.1.2
```

- Router2:

```
interface FastEthernet1/0
 ip address 192.168.2.1 255.255.255.0
 ip access-group 101 in
 ip access-group 100 out
```

```
Extended IP access list 100
    10 permit ip host 192.168.1.2 host 192.168.2.3
    20 permit ip host 192.168.3.2 host 192.168.2.3
    30 permit ip host 192.168.1.4 any
    40 permit ip host 192.168.3.3 any
    50 permit ip any host 192.168.2.2
Extended IP access list 101
    10 permit ip host 192.168.2.3 host 192.168.1.2
    20 permit ip host 192.168.2.3 host 192.168.3.2
    30 permit ip any host 192.168.1.4
    40 permit ip any host 192.168.3.3
    50 permit ip host 192.168.2.2 any
```

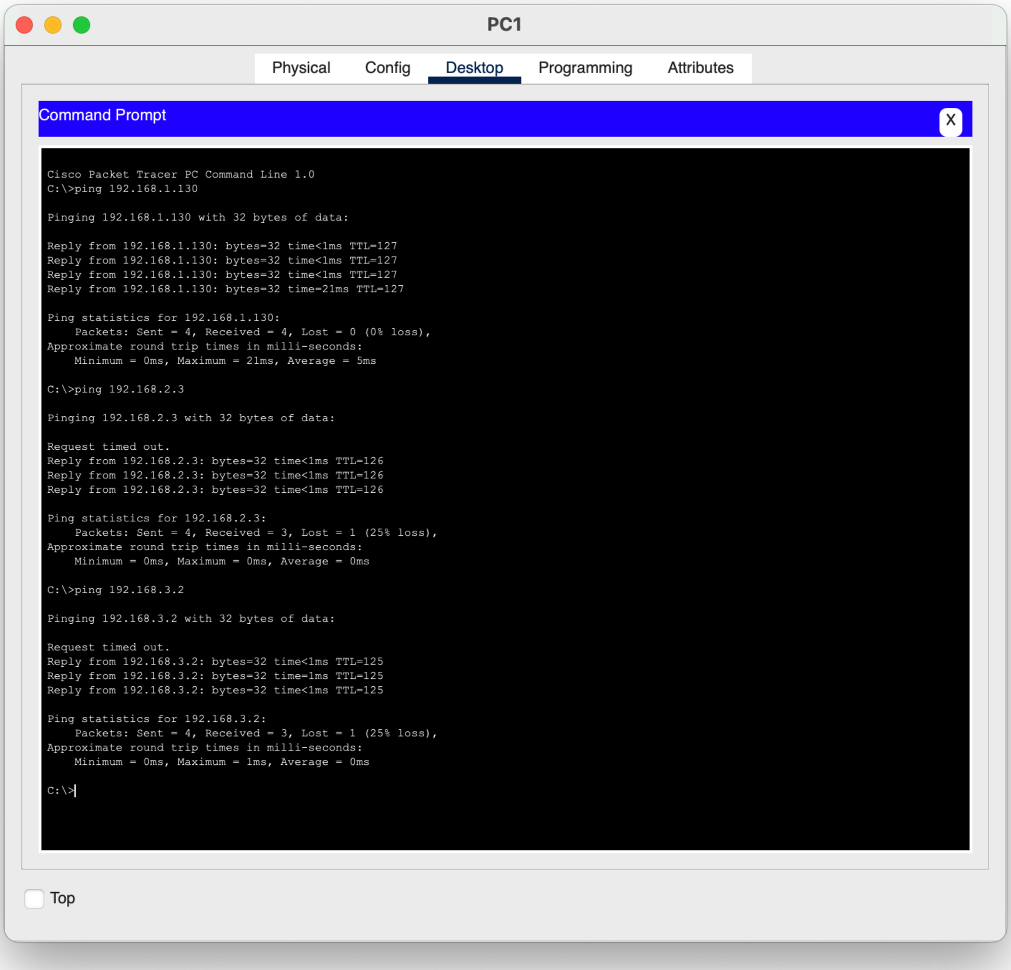
- Router3

```
interface FastEthernet0/1
 ip address 192.168.3.1 255.255.255.0
 ip access-group 101 in
 ip access-group 100 out
```

```
Extended IP access list 100
    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 host 192.168.1.4 any
    40 permit ip host 192.168.2.2 any
    50 permit ip any host 192.168.3.3
Extended IP access list 101
    10 permit ip host 192.168.3.2 host 192.168.1.2
    20 permit ip host 192.168.3.2 host 192.168.2.3
    30 permit ip any host 192.168.1.4
    40 permit ip any host 192.168.2.2
    50 permit ip host 192.168.3.3 any
```

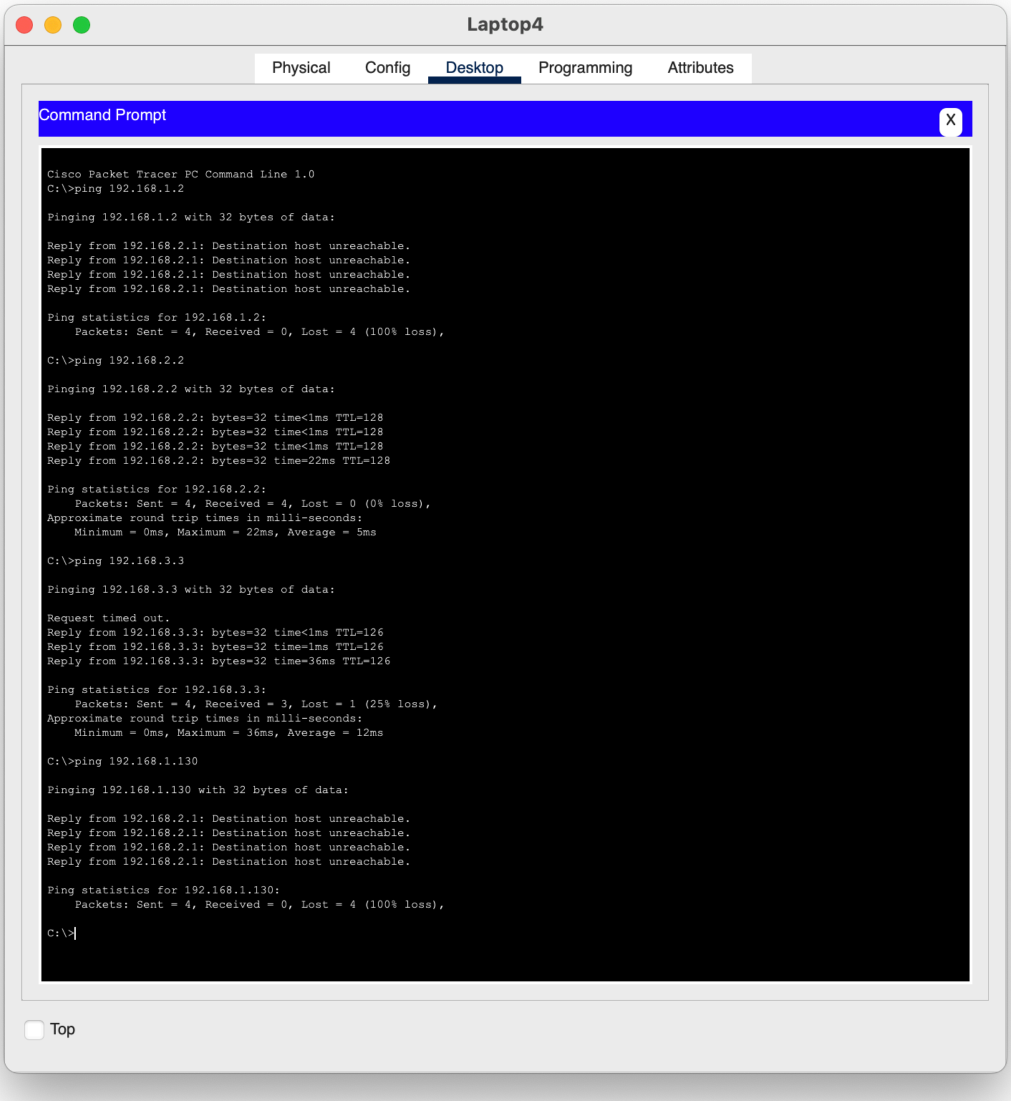
部分测试截图：

- 用 PC1 分别尝试与 Server1、Laptop2、PC3通信：



```
Cisco Packet Tracer PC Command Line 1.0
C:\>ping 192.168.1.130

Pinging 192.168.1.130 with 32 bytes of data:

Reply from 192.168.1.130: bytes=32 time<1ms TTL=127
Reply from 192.168.1.130: bytes=32 time<1ms TTL=127
Reply from 192.168.1.130: bytes=32 time<1ms TTL=127
Reply from 192.168.1.130: bytes=32 time=21ms TTL=127

Ping statistics for 192.168.1.130:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 21ms, Average = 5ms

C:\>ping 192.168.2.3

Pinging 192.168.2.3 with 32 bytes of data:

Request timed out.
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 = 3, Lost = 1 (25% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\>ping 192.168.3.2

Pinging 192.168.3.2 with 32 bytes of data:

Request timed out.
Reply from 192.168.3.2: bytes=32 time<1ms TTL=125
Reply from 192.168.3.2: bytes=32 time=1ms TTL=125
Reply from 192.168.3.2: bytes=32 time<1ms TTL=125

Ping statistics for 192.168.3.2:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 1ms, Average = 0ms

C:\>
```

- 用 Laptop4 分别尝试与 PC1、PC2、Laptop3、Server1 进行通信：



```
Cisco Packet Tracer PC Command Line 1.0
C:\>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),

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=128
Reply from 192.168.2.2: bytes=32 time<1ms TTL=128
Reply from 192.168.2.2: bytes=32 time<1ms TTL=128
Reply from 192.168.2.2: bytes=32 time=22ms TTL=128

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 = 22ms, Average = 5ms

C:\>ping 192.168.3.3

Pinging 192.168.3.3 with 32 bytes of data:

Request timed out.
Reply from 192.168.3.3: bytes=32 time<1ms TTL=126
Reply from 192.168.3.3: bytes=32 time=1ms TTL=126
Reply from 192.168.3.3: bytes=32 time=36ms TTL=126

Ping statistics for 192.168.3.3:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 36ms, Average = 12ms

C:\>ping 192.168.1.130

Pinging 192.168.1.130 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 192.168.1.130:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\>
```

Task 7

增加了新的 Extended ACL，使得 PC1 可以对所有设备进行 ping 测试，但只有符合上一任务的访问权限要求才能对 PC1 进行 ping 测试（只列举新添项）：

- Router1

```
Extended IP access list 100
    70 permit icmp any host 192.168.1.2 echo-reply
Extended IP access list 101
    70 permit icmp host 192.168.1.2 any
```

- Router2

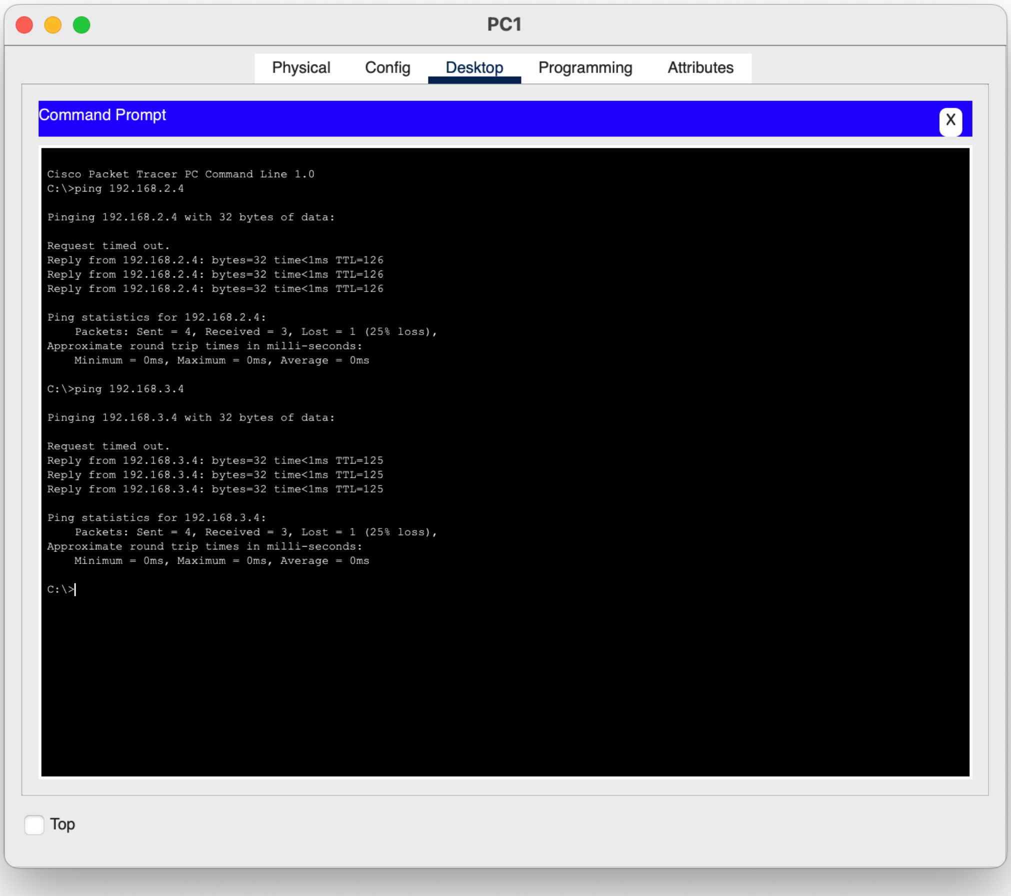
  ```
  Extended IP access list 100
      60 permit icmp host 192.168.1.2 any
  Extended IP access list 101
      60 permit icmp any host 192.168.1.2 echo-reply
  ```

- Router3

  ```
  Extended IP access list 100
      60 permit icmp host 192.168.1.2 any
  Extended IP access list 101
      60 permit icmp any host 192.168.1.2 echo-reply
  ```

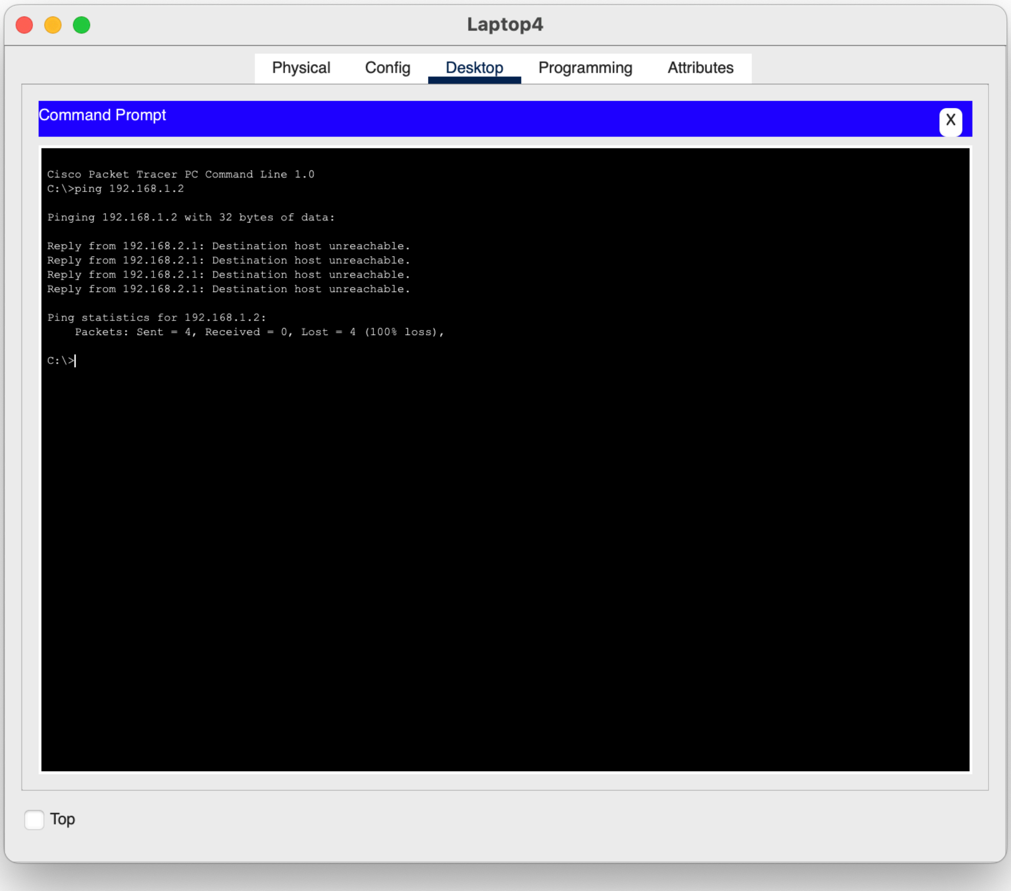
部分测试截图:

- 用 PC1 去 ping Laptop4 和 PC5，成功:



```
Cisco Packet Tracer PC Command Line 1.0
C:\>ping 192.168.2.4

Pinging 192.168.2.4 with 32 bytes of data:

Request timed out.
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 = 3, Lost = 1 (25% 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

C:\>
```

- 用 Laptop4 去 ping PC1，失败：

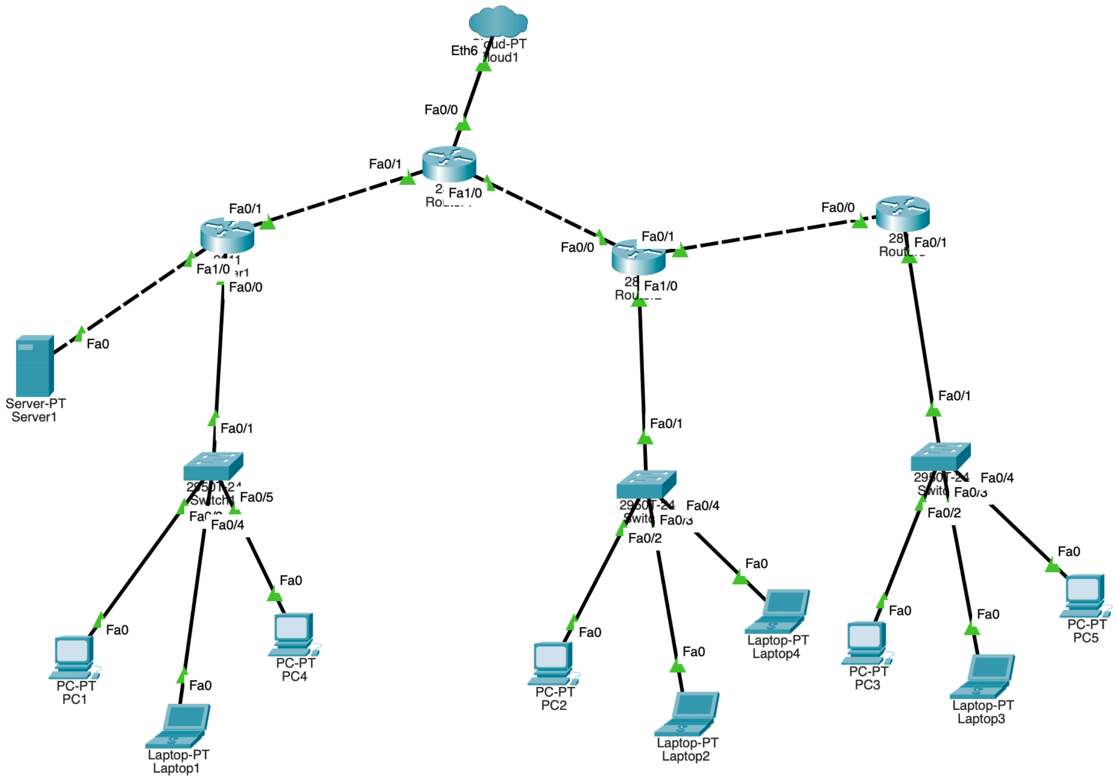


```
Cisco Packet Tracer PC Command Line 1.0
C:\>ping 192.168.1.2

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),

C:\>
```

Task 8

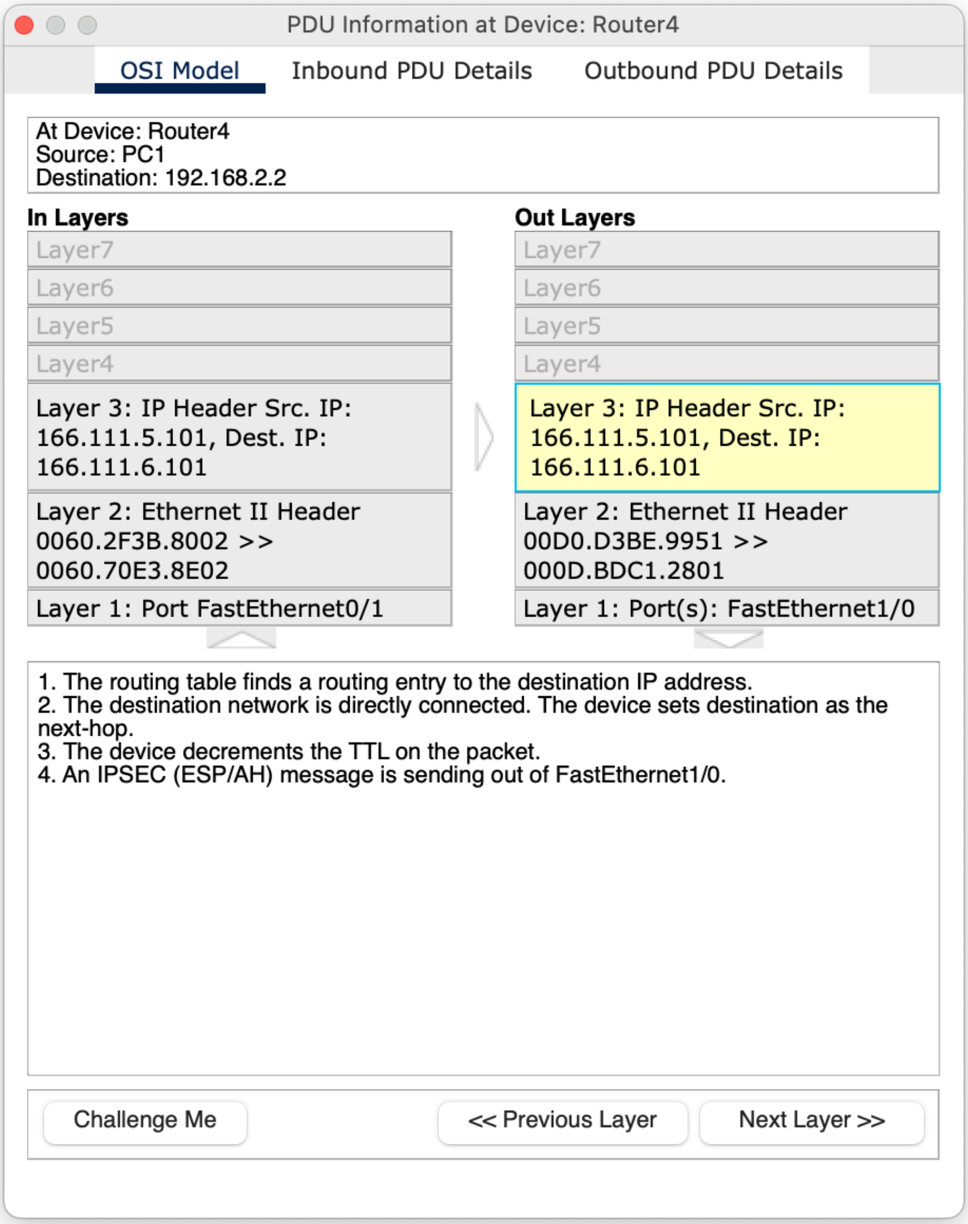
无法使用静态路由的原因：私有 IP 地址在公网上不可路由，也无法在公网路由上进行静态路由的配置。

重构后的网络拓扑：



按照习题课所述配置了 ISAKMP 和 IPSec。

根据仿真抓包，如上配置的 IPSec VPN 使用了隧道模式：



At Device: Router4
Source: PC1
Destination: 192.168.2.2

In Layers

Layer 3: IP Header Src. IP: 166.111.5.101, Dest. IP: 166.111.6.101

Layer 2: Ethernet II Header 0060.2F3B.8002 >> 0060.70E3.8E02

Layer 1: Port FastEthernet0/1

Out Layers

Layer 3: IP Header Src. IP: 166.111.5.101, Dest. IP: 166.111.6.101

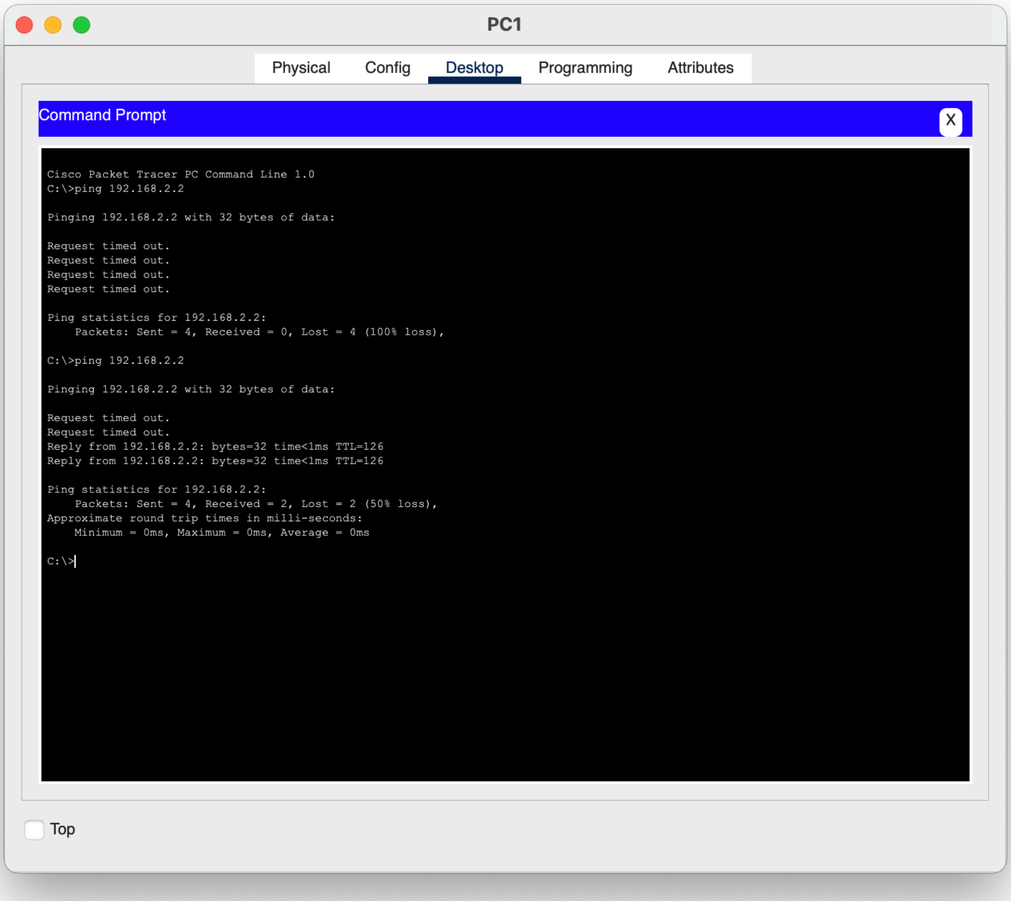
Layer 2: Ethernet II Header 00D0.D3BE.9951 >> 000D.BDC1.2801

Layer 1: Port(s): FastEthernet1/0

1. The routing table finds a routing entry to the destination IP address.
2. The destination network is directly connected. The device sets destination as the next-hop.
3. The device decrements the TTL on the packet.
4. An IPSEC (ESP/AH) message is sending out of FastEthernet1/0.

部分测试截图：

- 用 PC1 去 ping PC2，在数次学习后成功：

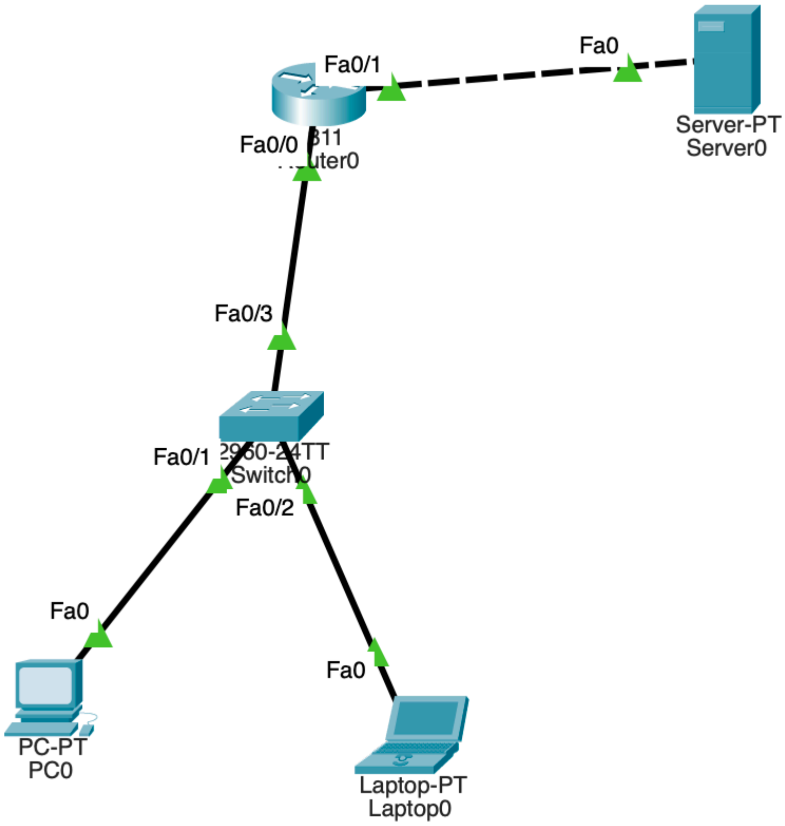


```
Cisco Packet Tracer PC Command Line 1.0
C:\>ping 192.168.2.2

Pinging 192.168.2.2 with 32 bytes of data:

Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 192.168.2.2:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

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:\>
```

Bonus Task

探究内容：网络地址转换（Network Address Translation）。

探究搭建的简单拓扑如下：



1. 首先分配 IP 地址：

Device	Port	IP	Mask	Gateway
Router0	Fa0/0	192.168.1.1	/24	-
	Fa0/1	1.1.1.1	/8	-
PC0	Fa0/0	192.168.1.2	/24	192.168.1.1
Laptop0	Fa0/0	192.168.1.3	/24	192.168.1.1
Server0	Fa0/1	1.1.1.2	/8	1.1.1.1

2. 配置 NAT：

```
 Router(config)# ip nat inside source list 1 interface FastEthernet0/1
overload
```

3. 创建 access-list：

   ```
   Router(config)# access-list 1 permit 192.168.1.0 0.0.0.255
   ```

4. 启用 NAT on Inside 接口：

   ```
   Router(config)# interface FastEthernet0/0
   Router(config-if)# ip nat inside
   Router(config-if)# exit
   ```

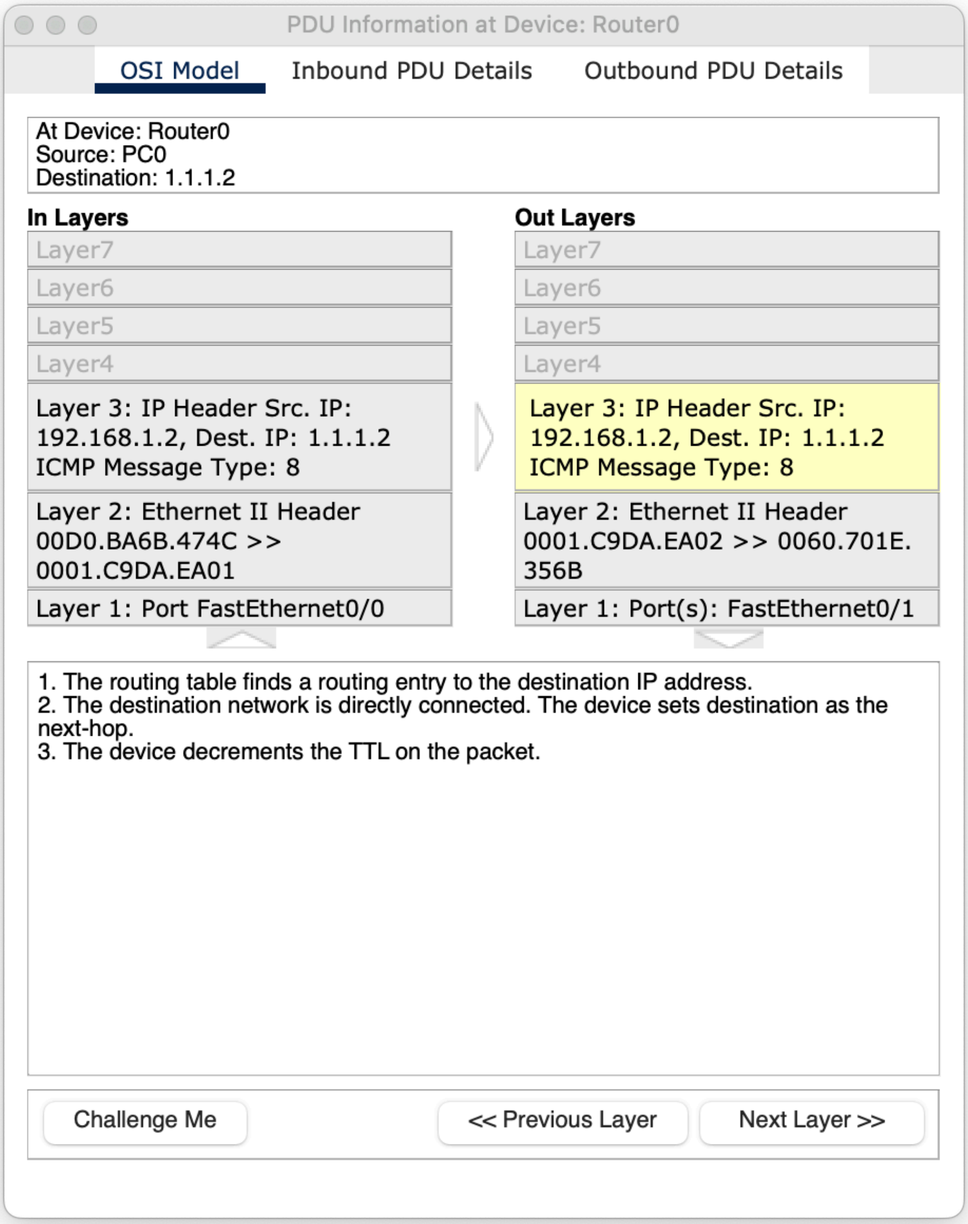
5. 启用 NAT on Outside 接口：

   ```
   Router(config)# interface FastEthernet0/1
   Router(config-if)# ip nat outside
   Router(config-if)# exit
   ```

6. 保存配置

   ```
   Router(config)# end
   Router# write memory
   ```

应用 NAT 前，包头 Src. IP 为 PC0 的 IP 地址：



At Device: Router0
Source: PC0
Destination: 1.1.1.2

In Layers

Layer 3: IP Header Src. IP: 192.168.1.2, Dest. IP: 1.1.1.2 ICMP Message Type: 8

Layer 2: Ethernet II Header 00D0.BA6B.474C >> 0001.C9DA.EA01

Layer 1: Port FastEthernet0/0

Out Layers

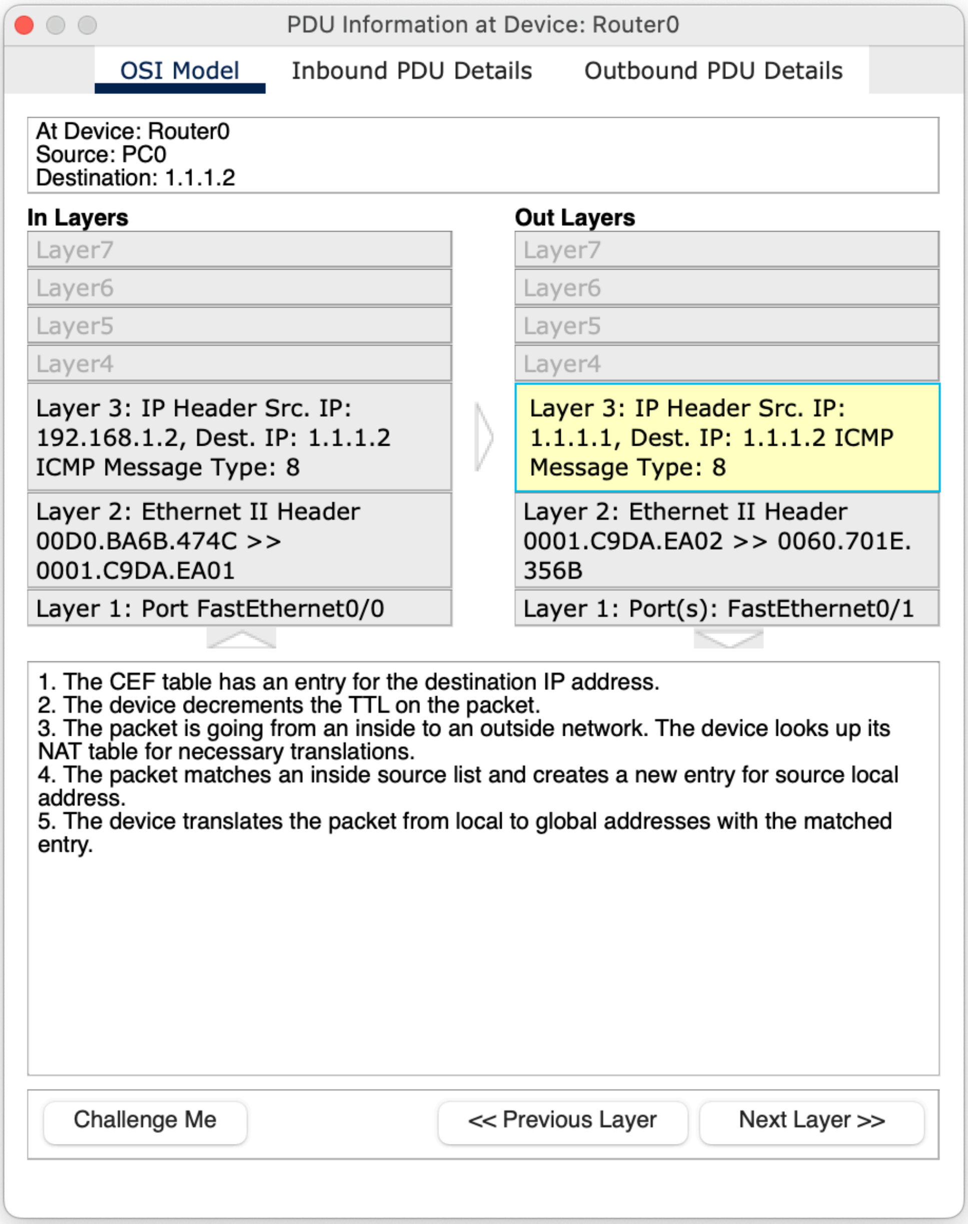
Layer 3: IP Header Src. IP: 192.168.1.2, Dest. IP: 1.1.1.2 ICMP Message Type: 8

Layer 2: Ethernet II Header 0001.C9DA.EA02 >> 0060.701E.356B

Layer 1: Port(s): FastEthernet0/1

1. The routing table finds a routing entry to the destination IP address.
2. The destination network is directly connected. The device sets destination as the next-hop.
3. The device decrements the TTL on the packet.

应用 NAT 前，包头 Src. IP 为 Router0 的 outside 端口地址：



At Device: Router0
Source: PC0
Destination: 1.1.1.2

In Layers	Out Layers
Layer7	Layer7
Layer6	Layer6
Layer5	Layer5
Layer4	Layer4
Layer 3: IP Header Src. IP: 192.168.1.2, Dest. IP: 1.1.1.2 ICMP Message Type: 8	Layer 3: IP Header Src. IP: 1.1.1.1, Dest. IP: 1.1.1.2 ICMP Message Type: 8
Layer 2: Ethernet II Header 00D0.BA6B.474C >> 0001.C9DA.EA01	Layer 2: Ethernet II Header 0001.C9DA.EA02 >> 0060.701E.356B
Layer 1: Port FastEthernet0/0	Layer 1: Port(s): FastEthernet0/1

1. The CEF table has an entry for the destination IP address.
2. The device decrements the TTL on the packet.
3. The packet is going from an inside to an outside network. The device looks up its NAT table for necessary translations.
4. The packet matches an inside source list and creates a new entry for source local address.
5. The device translates the packet from local to global addresses with the matched entry.