

1.OSPF 路由项欺骗攻击和防御实验

1.1 实验内容

构建如图 1 所示的由 3 台路由器互连 4 个网络的互联网，通过 OSPF 生成终端 A 至终端 B 的 IP 传输路径，实现 IP 分组终端 A 至终端 B 的传输过程。然后在网络地址为 192.1.2.0/24 的以太网上接入入侵路由器，由入侵路由器伪造与网络 192.1.4.0/24 直接连接的路由项，用伪造的路由项改变终端 A 至终端 B 的 IP 传输路径，使终端 A 传输给终端 B 的 IP 分组被路由器 R1 错误地转发给入侵路由器。

启动路由器 R1、R2 和 R3 的路由消息源端鉴别功能，要求路由器 R1、R2 和 R3 发送的路由消息携带消息鉴别码(Message Authentication Code,MAC)，配置相应路由器接口之间的共享密钥。使路由器 R1 不再接收和处理入侵路由器发送的路由消息，从而使路由器 R1 的路由表恢复正常。

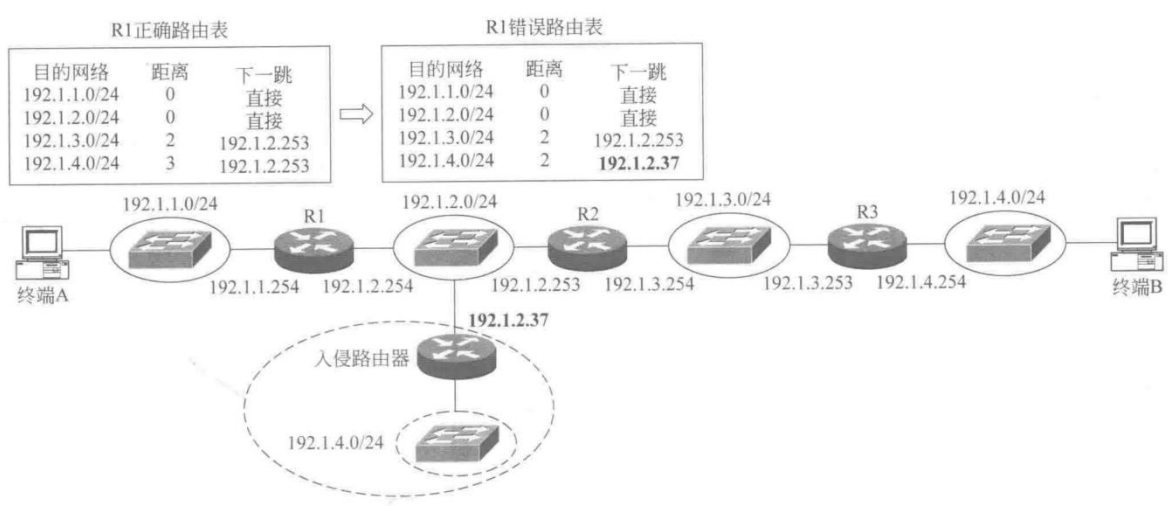


图 1 OSPF 路由项欺骗攻击和防御过程

1.2 实验目的

- (1) 验证路由器 OSPF 配置过程。
- (2) 验证 OSPF 建立动态路由项过程。
- (3) 验证 OSPF 路由项欺骗攻击过程。
- (4) 验证 OSPF 源端鉴别功能的配置过程。
- (5) 验证 OSPF 防路由项欺骗攻击功能的实现过程。

1.3 实验原理

路由项欺骗攻击过程如图 1 所示，入侵路由器伪造了和网络 192.1.4.0/24 直接连接的链路状态信息，导致路由器 R1 通过 OSPF 生成的动态路由项发生错误，如图 1 中 R1 错误路由表所示。解决路由项欺骗攻击问题的关键有三点：一是建立邻接关系的路由器的身份进行鉴别，只和授权路由器建立邻接关系；二是对相互交换的链路状态信息进行完整性检测，只接收和处理完整性检测通过的链路状态信息；三是通过链路状态信息中携带的序号确定该链路状态信息不是黑客截获后重放的链路状态信息。实现上述功能的基础是在相邻路由器中配置相同的共享密钥，相互交换的链路状态信息和 Hello 报文携带由共享密钥加密的序号和由共享密钥生成的 MAC（消息鉴别码），通过消息鉴别码实现路由消息的源端鉴别和完整性检测，全部过程如图 2 所示。

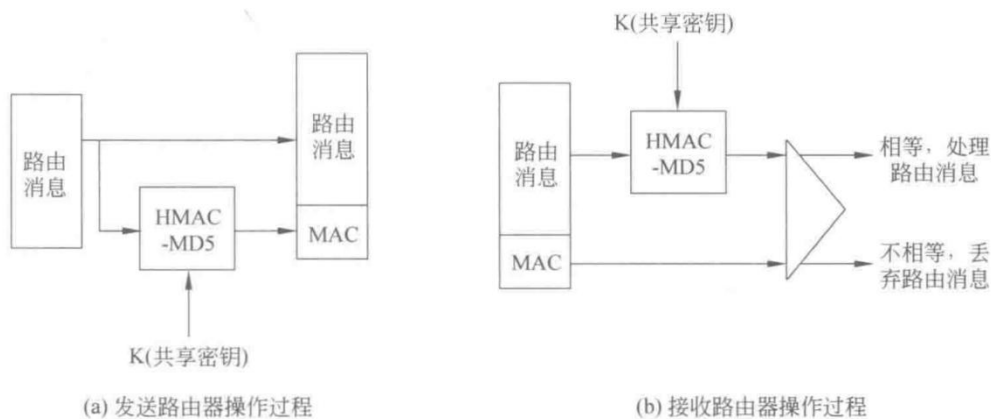


图 2 路由消息源端鉴别和完整性检测过程

1.4 实验步骤

- (1) 在如图 1 所示的互连网结构中去掉入侵路由器,根据去掉入侵路由器后的互连网结构放置和连接设备,完成设备放置和连接后的逻辑工作区界面如图 3 所示。

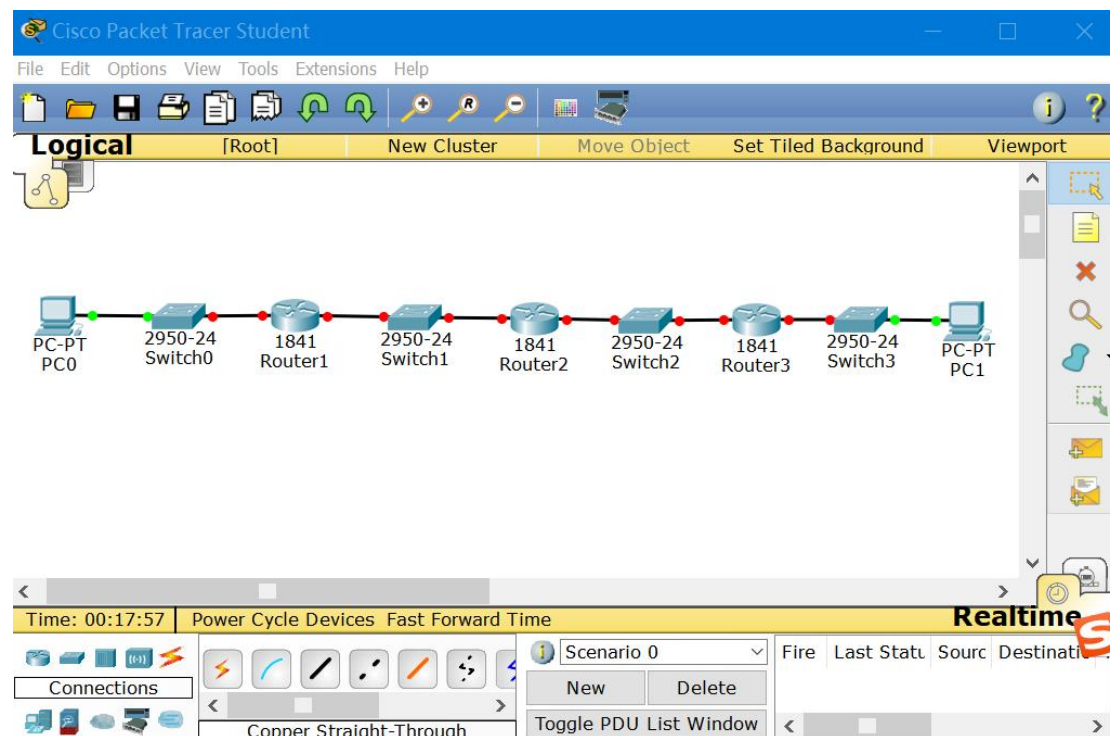
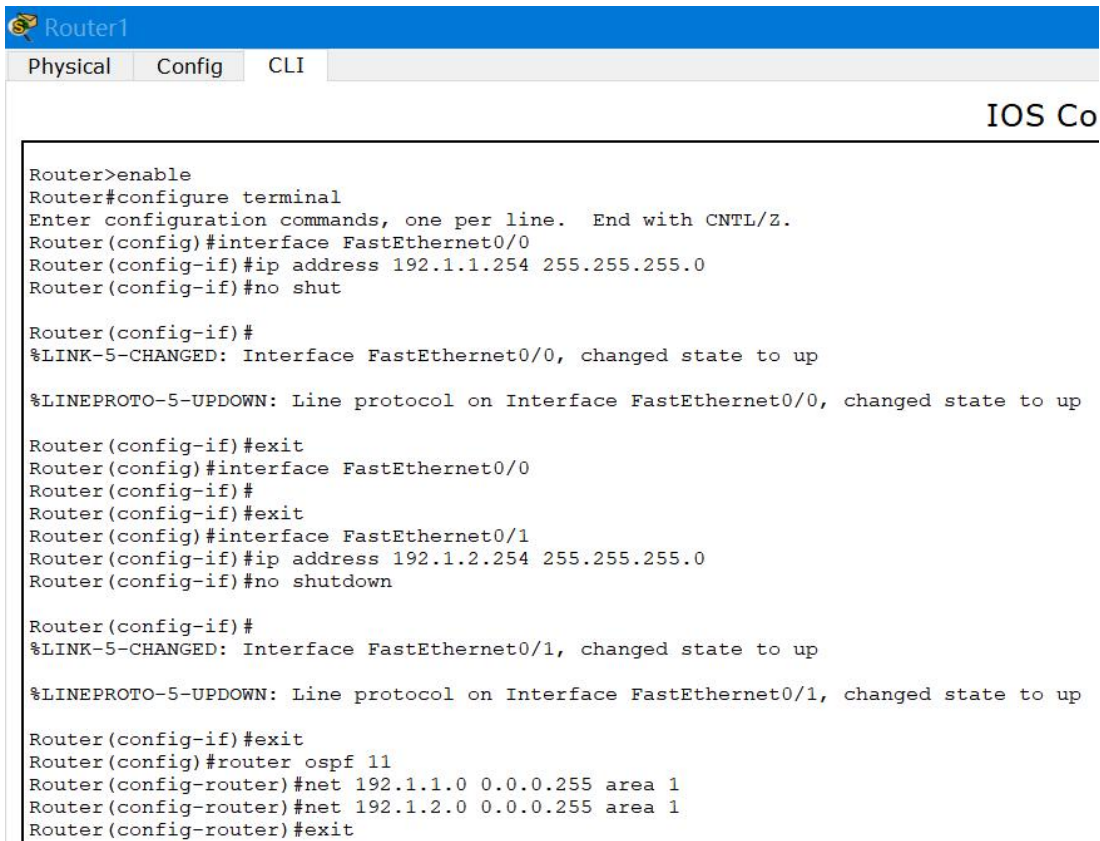


图 3 完成设备放置和连接后的逻辑工作区界面

- (2) 根据如图 1 所示的各个路由器接口的网络信息完成路由器接口 IP 地址和子网掩码配置过程。CLI（命令行接口）配置方式下,完成路由器 OSPF 配置过程。其具体配置过程如图 4、5、6 所示。完成上述配置过程后,路由器 Router1 生成如图 7 所示的路由表。

The image shows the CLI interface of a Cisco router named Router1. At the top, there is a blue header bar with the router's name and a small icon. Below the header, there are three tabs: 'Physical', 'Config', and 'CLI', with 'CLI' being the active tab. On the right side, the text 'IOS Co' is visible. The main area contains a series of commands and their outputs. The commands include enabling the terminal, configuring interfaces FastEthernet0/0 and FastEthernet0/1 with IP addresses, and configuring OSPF. The outputs show the state changes for the interfaces and the OSPF configuration process.

```
Router1>enable
Router#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#interface FastEthernet0/0
Router(config-if)#ip address 192.1.1.254 255.255.255.0
Router(config-if)#no shut

Router(config-if)#
%LINK-5-CHANGED: Interface FastEthernet0/0, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0, changed state to up

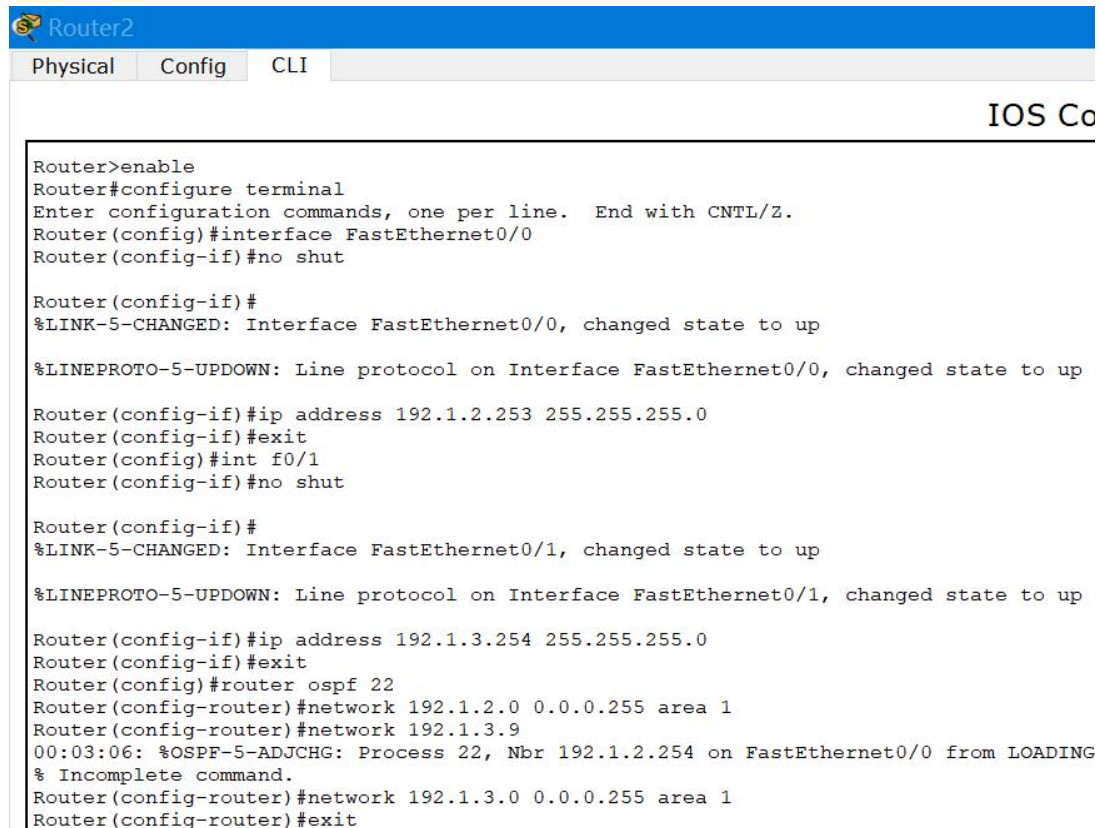
Router(config-if)#exit
Router(config)#interface FastEthernet0/0
Router(config-if)#
Router(config-if)#exit
Router(config)#interface FastEthernet0/1
Router(config-if)#ip address 192.1.2.254 255.255.255.0
Router(config-if)#no shutdown

Router(config-if)#
%LINK-5-CHANGED: Interface FastEthernet0/1, changed state to up

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

Router(config-if)#exit
Router(config)#router ospf 11
Router(config-router)#net 192.1.1.0 0.0.0.255 area 1
Router(config-router)#net 192.1.2.0 0.0.0.255 area 1
Router(config-router)#exit
```

图 4 Router1 接口和 OSPF 配置过程

The image shows the CLI interface of a Cisco router named Router2. It has the same layout as Router1, with a blue header bar, tabs for 'Physical', 'Config', and 'CLI', and the text 'IOS Co' on the right. The CLI shows commands for enabling the terminal, configuring interfaces FastEthernet0/0 and FastEthernet0/1 with IP addresses, and configuring OSPF. The outputs show the state changes for the interfaces and the OSPF configuration process, including a message about the OSPF process starting.

```
Router2>enable
Router#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#interface FastEthernet0/0
Router(config-if)#no shut

Router(config-if)#
%LINK-5-CHANGED: Interface FastEthernet0/0, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0, changed state to up

Router(config-if)#ip address 192.1.2.253 255.255.255.0
Router(config-if)#exit
Router(config)#int f0/1
Router(config-if)#no shut

Router(config-if)#
%LINK-5-CHANGED: Interface FastEthernet0/1, changed state to up

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

Router(config-if)#ip address 192.1.3.254 255.255.255.0
Router(config-if)#exit
Router(config)#router ospf 22
Router(config-router)#network 192.1.2.0 0.0.0.255 area 1
Router(config-router)#network 192.1.3.9
00:03:06: %OSPF-5-ADJCHG: Process 22, Nbr 192.1.2.254 on FastEthernet0/0 from LOADING
% Incomplete command.
Router(config-router)#network 192.1.3.0 0.0.0.255 area 1
Router(config-router)#exit
```

图 5 Router2 接口和 OSPF 配置过程

```

Router3
Physical Config CLI
IOS Co

Router>enable
Router#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#interface FastEthernet0/0
Router(config-if)#no shut

Router(config-if)#
%LINK-5-CHANGED: Interface FastEthernet0/0, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0, changed state to up

Router(config-if)#ip address 192.1.3.253 255.255.255.0
Router(config-if)#exit
Router(config)#int f0/1
Router(config-if)#no shut

Router(config-if)#
%LINK-5-CHANGED: Interface FastEthernet0/1, changed state to up

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

Router(config-if)#ip address 192.1.4.254 255.255.255.0
Router(config-if)#exit
Router(config)#router ospf 33
Router(config-router)#net 192.1.3.0 0.0.0.255 area 1
Router(config-router)#net 192.1.4.0 0.0.0.255 area 1
00:03:07: %OSPF-5-ADJCHG: Process 33, Nbr 192.1.3.254 on FastEthernet0/0 from LOADING

^
% Invalid input detected at '^' marker.

Router(config-router)#net 192.1.4.0 0.0.0.255 area 1
Router(config-router)#exit

```

图6 Router3 接口和 OSPF 配置过程

```

Router1
Physical Config CLI
IOS

Router#show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is not set

C    192.1.1.0/24 is directly connected, FastEthernet0/0
C    192.1.2.0/24 is directly connected, FastEthernet0/1
O    192.1.3.0/24 [110/2] via 192.1.2.253, 01:24:59, FastEthernet0/1
O    192.1.4.0/24 [110/3] via 192.1.2.253, 00:28:20, FastEthernet0/1

```

图7 路由器 Router1 路由表

- (3) 通过启动 PC0 与 PC1 之间的 ICMP 报文传输过程，如图 8 所示，验证 PC0 与 PC1 之间存在 IP 传输路径。（注意配置 PC0 和 PC1 的合理 ip 地址和网关）

| Fire | Last Statu | Sourc | Destinatio | Type | Colo | Time(s) | Period | Num | Edit | Delete |
|------|------------|-------|------------|-------|------|---------|--------|-----|--------|----------|
| ● | Successful | PC0 | PC1 | IC... | | 0.000 | N | 0 | (ed... | (delete) |

图8 PC0 传输 ICMP 到 PC1

- (4) 如图 9 所示，用路由器 Router 作为入侵路由器，Router 其中一个接口连接网络 192.1.2.0/24，分配 IP 地址 192.1.2.37 和子网掩码 255.255.255.0。Router 的另一个接口分配 IP 地址 192.1.4.37 和子网掩码 255.255.255.0，以此将该接口伪造成与网络 192.1.4.0/24 直接连接的接口。在 CLI(命令行接口)配置方式下，完成路由器 Router OSPF 配置过程(如图 10 所示)，路由器 Router 发送表明与网络 192.1.4.0/24 直接连接的路由消息。该路由消息将路由器 Router1 的路由表改变为如图 11 所示的错误路由表，错误路由表中的路由项 <192.1.4.0/24, 192.1.2.37> 表明，路由器 Router1 通往网络 192.1.4.0/24 的传输路径上的下一跳是由路由器 Router 连接网络 192.1.2.0/24 的接口。

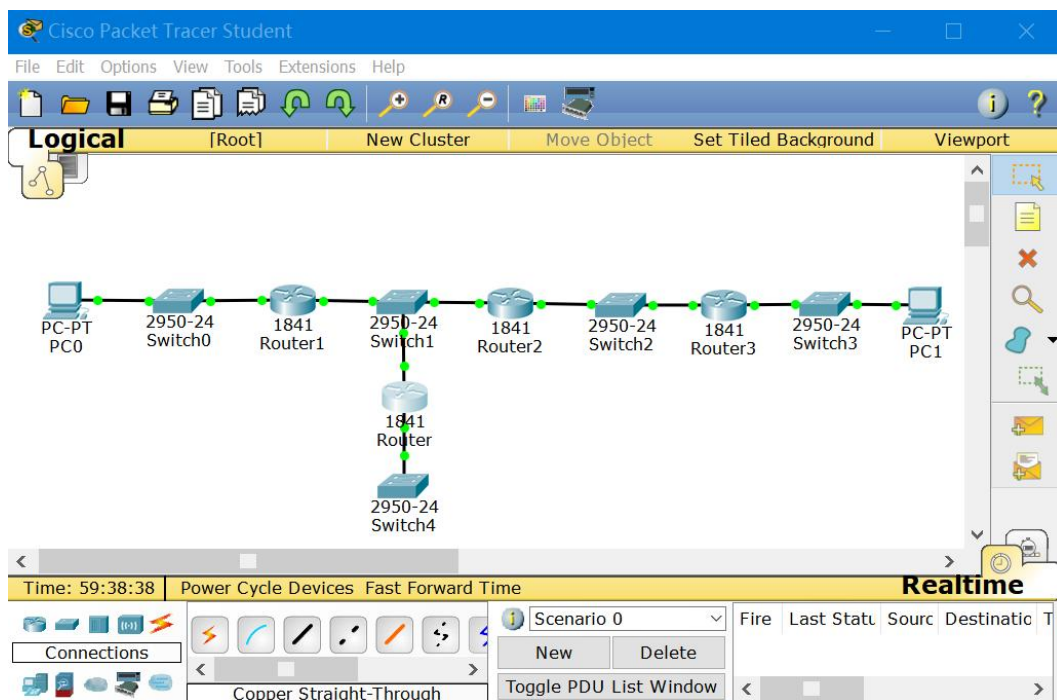
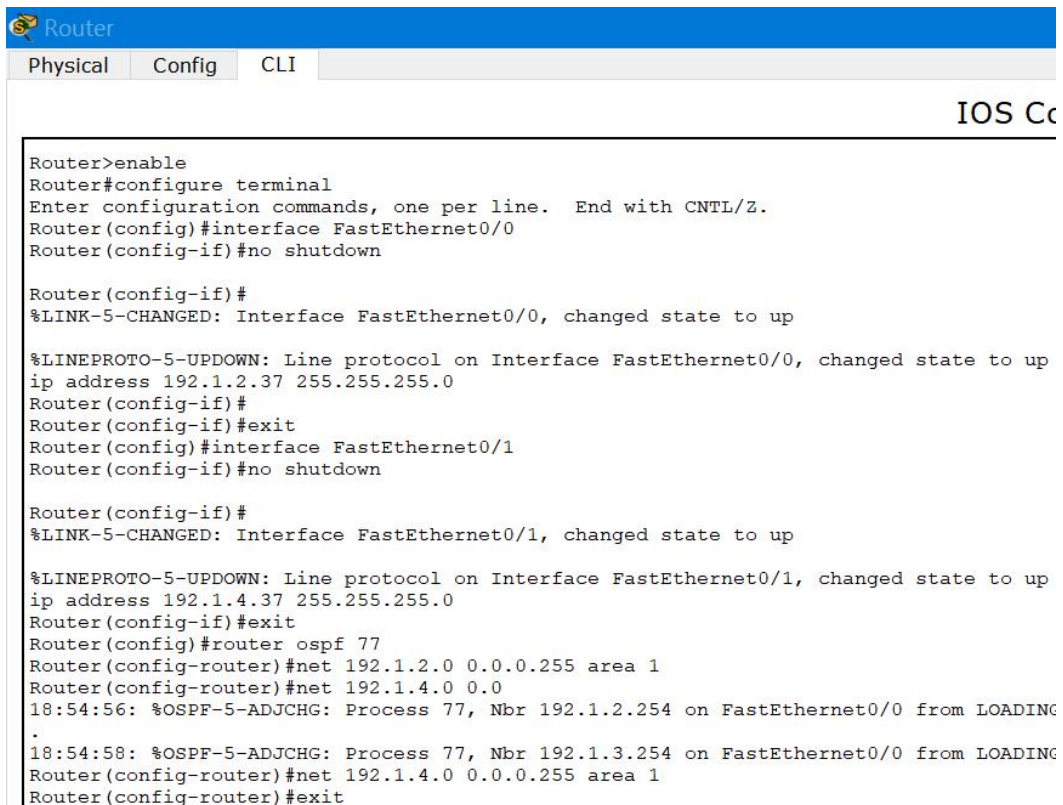


图 9 接入入侵路由器后的逻辑工作区界面



```
Router>enable
Router#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#interface FastEthernet0/0
Router(config-if)#no shutdown

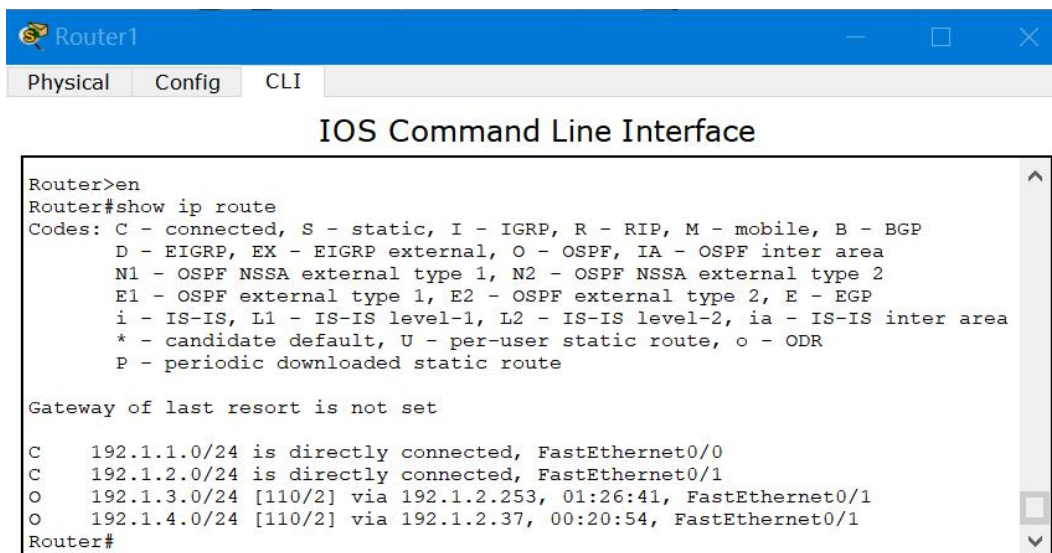
Router(config-if)#
%LINK-5-CHANGED: Interface FastEthernet0/0, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0, changed state to up
ip address 192.1.2.37 255.255.255.0
Router(config-if)#
Router(config-if)#exit
Router(config)#interface FastEthernet0/1
Router(config-if)#no shutdown

Router(config-if)#
%LINK-5-CHANGED: Interface FastEthernet0/1, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed state to up
ip address 192.1.4.37 255.255.255.0
Router(config-if)#exit
Router(config)#router ospf 77
Router(config-router)#net 192.1.2.0 0.0.0.255 area 1
Router(config-router)#net 192.1.4.0 0.0
18:54:56: %OSPF-5-ADJCHG: Process 77, Nbr 192.1.2.254 on FastEthernet0/0 from LOADING
.
18:54:58: %OSPF-5-ADJCHG: Process 77, Nbr 192.1.3.254 on FastEthernet0/0 from LOADING
Router(config-router)#net 192.1.4.0 0.0.0.255 area 1
Router(config-router)#exit
```

图 10 Router 接口和 OSPF 配置过程



```
Router1>en
Router1#show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is not set

C    192.1.1.0/24 is directly connected, FastEthernet0/0
C    192.1.2.0/24 is directly connected, FastEthernet0/1
O    192.1.3.0/24 [110/2] via 192.1.2.253, 01:26:41, FastEthernet0/1
O    192.1.4.0/24 [110/2] via 192.1.2.37, 00:20:54, FastEthernet0/1
Router1#
```

图 11 接入入侵路由器后的路由器 Router1 路由表

- (5) 进入模拟操作模式，启动 PC0 至 PC1 的 IP 分组传输过程（如图 12 所示），发现路由器 Router1 将该 IP 分组转发给路由器 Router，导致该 IP 分组无法到达 PC1。

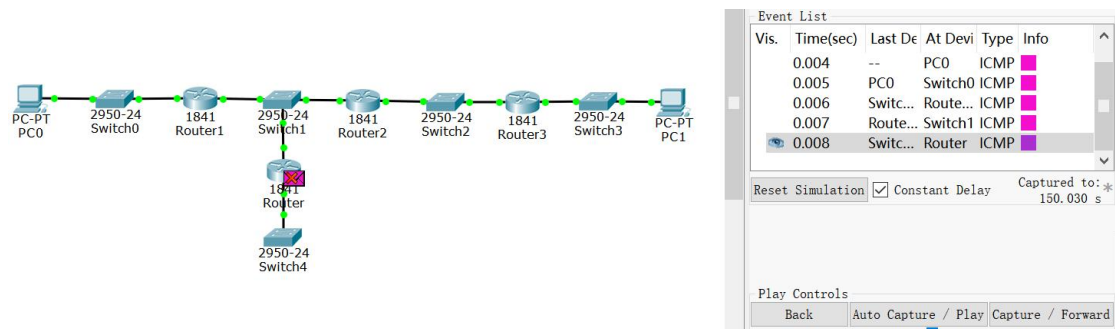


图 12 接入入侵路由器后的 ICMP 传输过程

- (6) CLI（命令行接口）配置方式下，如图 13、14 和 15 所示，完成路由器 Router1、Router2 和 Router3 与源端鉴别和完整性检测功能相关的配置过程，为相邻路由器实现互连的接口配置相同的密钥。完成上述配置过程后，路由器 Router1 的路由表如图 16 所示。路由器 Router1 通往网络 192.1.4.0/24 的传输路径上的下一跳重新变为路由器 Router2 连接网络 192.1.2.0/24 的接口。

```

Router1
Physical Config CLI
IOS Command Line Interface
Router>en
Router#config
Configuring from terminal, memory, or network [terminal]?
Enter configuration commands, one per line. End with CNTL
Router(config)#router ospf 11
Router(config-router)#area 1 authentication message-digest
Router(config-router)#exit
Router(config)#int f0/1
Router(config-if)#ip ospf authentication message-digest
Router(config-if)#ip ospf message-digest-key 1 md5 222222
Router(config-if)#exit

```


图 13 Router1 源端鉴别与完整性检测配置过程

```

Router2
Physical Config CLI
IOS Command Line Interface
Enter configuration commands, one per line. End with
CNTL/Z.
Router(config)#router ospf 22
Router(config-router)#area 1 authentication message-digest
Router(config-router)#exit
Router(config)#int f0/0
Router(config-if)#ip ospf authentication message-digest
Router(config-if)#ip ospf message-digest-key 1 md5 222222
Router(config-if)#exit
Router(config)#int f0/1
Router(config-if)#ip ospf authentication message-digest
Router(config-if)#ip ospf message-digest-key 1 md5 333333
Router(config-if)#exit


```

图 14 Router2 源端鉴别与完整性检测配置过程



```
Router3
Physical Config CLI
IOS Command Line Interface
Router#config
Configuring from terminal, memory, or network [terminal]?
Enter configuration commands, one per line. End with
CNTL/Z.
Router(config)#router ospf 33
Router(config-router)#area 1 authentication message-digest
Router(config-router)#exit
Router(config)#int f0/0
Router(config-if)#ip ospf authentication message-digest
Router(config-if)#ip ospf message-digest-key 1 md5 333333
Router(config-if)#exit
```

图 15 Router3 源端鉴别与完整性检测配置过程



```
Router1
Physical Config CLI
IOS Command Line Interface
Router>en
Router#show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is not set

C    192.1.1.0/24 is directly connected, FastEthernet0/0
C    192.1.2.0/24 is directly connected, FastEthernet0/1
O    192.1.3.0/24 [110/2] via 192.1.2.253, 01:50:22, FastEthernet0/1
O    192.1.4.0/24 [110/3] via 192.1.2.253, 00:11:49, FastEthernet0/1
```

图 16 完成源端鉴别与完整性检测功能配置后的 Router1 路由表

2. 策略路由项实验

2.1 实验内容

互联网结构如图 17 所示，根据最短路径原则，RIP 生成的路由器 R1 通往网络 NET2 的传输路径是 R1→R5→R4→NET2。如果基于安全原因，不允许目的终端是终端 C 的 IP 分组经过路由器 R5，需要在路由器 R1 中配置静态路由项，静态路由项将通往终端 C 的传输路径上的下一跳设置成路由器 R2，由于静态路由项的优先级高于 RIP 生成的动态路由项，因此，路由器 R1 将目的 IP 地址为 IP C 的 IP 分组转发给路由器 R2。由于 Packet Tracer 中的路由器不支持策略路由功能，因此，用静态路由项仿真策略路由过程。

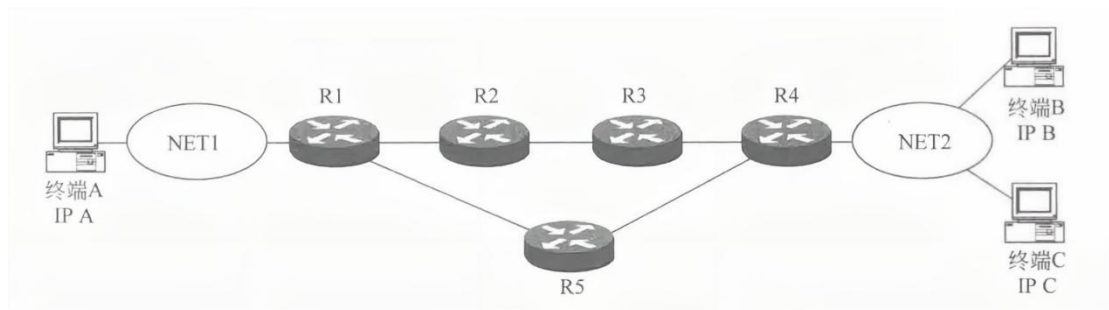


图 17 互连网结构

2.2 实验目的

- (1) 验证 RIP 生成动态路由项的过程。
- (2) 验证最长前缀匹配过程。
- (3) 验证静态路由项改变 IP 分组传输路径的过程。
- (4) 验证基于安全理由规避特定路由器的过程。

2.3 实验原理

为特殊目的终端选择 IP 分组传输路径的关键是路由表，当如图 17 所示的互连网中的各台路由器完成每一个接口的 IP 地址、子网掩码和 RIP 配置后，即可生成完整路由表。路由器 R1 生成的完整路由表如图 18(a)所示，由直连路由项和 RIP 生成的动态路由项组成。用类型 C 表示直连路由项，用类型 R 表示 RIP 生成的动态路由项。如果在路由器 R1 的路由表中添加一项目的网络是 IP C/32，下一跳是路由器 R2 的静态路由项，路由器 R1 完整路由表如图 18(b)所示，用类型 S 表示静态路由项。当路由器 R1 接收到目的 IP 地址是 IP C 的 IP 分组时，由于 IP C 属于 NET2，因此，该 IP 分组分别与目的网络是 NET2 和目的网络是 IP C/32 的两项路由项匹配。由于 IP C/32 的网络前缀位数是 32，大于 NET2 的网络前缀位数，因此，根据最长前缀匹配原则，最终用于转发该 IP 分组的项是目的网络为 IP C/32 的路由项，路由器 R1 将该 IP 分组传输给下一跳路由器 R2。

R1路由表一

| 类型 | 目的网络 | 下一跳 | 距离 |
|----|------|-----|----|
| C | NET1 | 直接 | 0 |
| R | NET2 | R5 | 2 |

(a) R1路由表一

R1路由表二

| 类型 | 目的网络 | 下一跳 | 距离 |
|----|---------|-----|----|
| C | NET1 | 直接 | 0 |
| R | NET2 | R5 | 2 |
| S | IP C/32 | R2 | |

(b) R1路由表二

图 18 路由器 R1 路由表

2.4 实验步骤

- 由于如图 17 所示的路由器 R1 需要三个以太网接口，默认状态下，Ciso 2811 只有两个以太网接口，因此，需要添加一个以太网接口。添加过程如下：单击路由器 Router1，在弹出的配置界面中选择 Physical（物理）配置选项，关闭路由器电源，在左边模块栏中选中模块 NM-1FE-TX，然后将其拖放到路由器的空插槽中，全部过程如图 19 所示。模块 NM-1FE-TX 提供单个 100BASE-TX 接口。重新打开路由器电源。R4 同样如此。

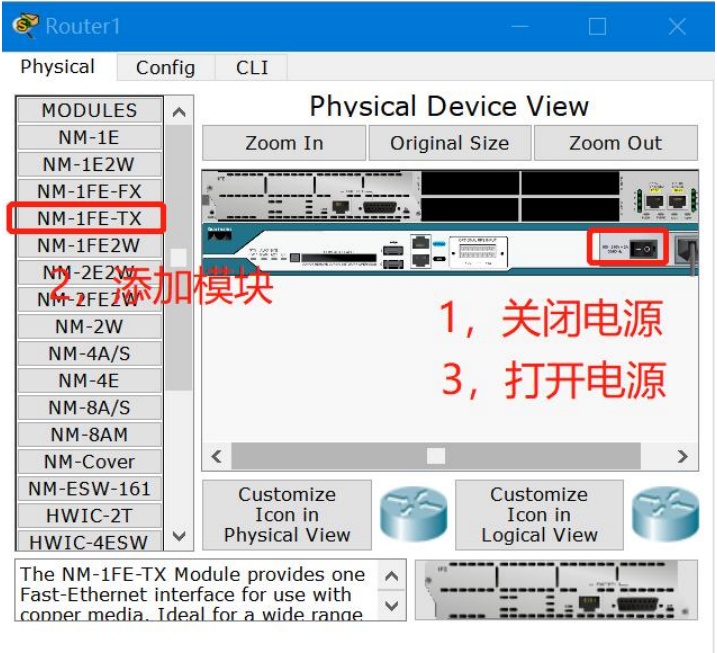


图 19 添加接口过程

- (2) 根据如图 17 所示互连网结构放置和连接设备，完成设备放置和连接后的逻辑工作区界面如图 20 所示。

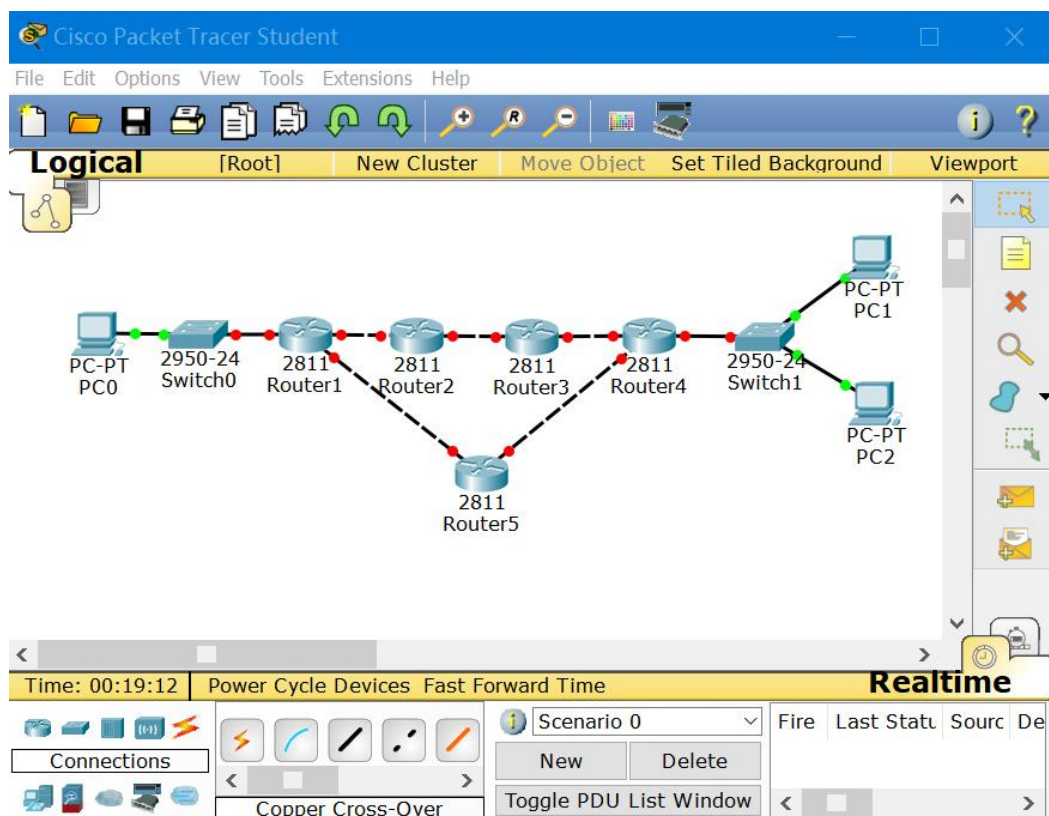


图 20 完成设备放置和连接后的逻辑工作区界面

- (3) 完成各台路由器中每一个接口的 IP 地址、子网掩码配置过程（如图 21 所示），完成各台路由器 RIP 配置过程（如图 22 为 Router4 配置过程，其余类似）。各台路由器完成完整路由表。路由器 Router1 的完整路由表如图 23 所示。通往网络 192.1.5.0/24 的传输路径上的下一跳是由路由器 Router5(192.1.6.253 是路由器 Router5 连接路由器 Router1 的接口的 IP 地址)。

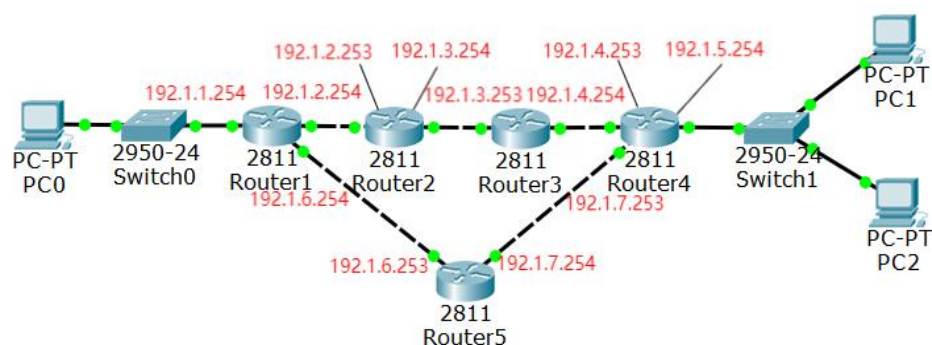


图 21 路由器接口 ip 配置参考

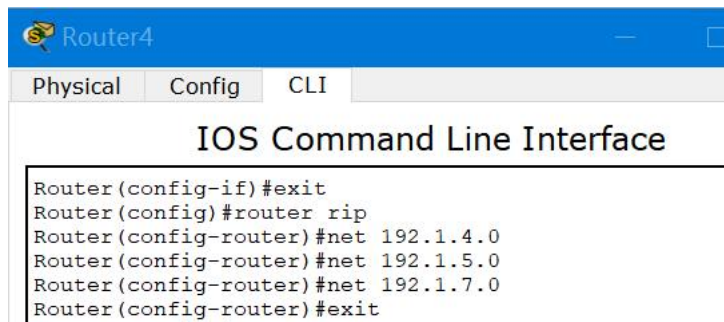


图 22 Router4 RIP 配置过程

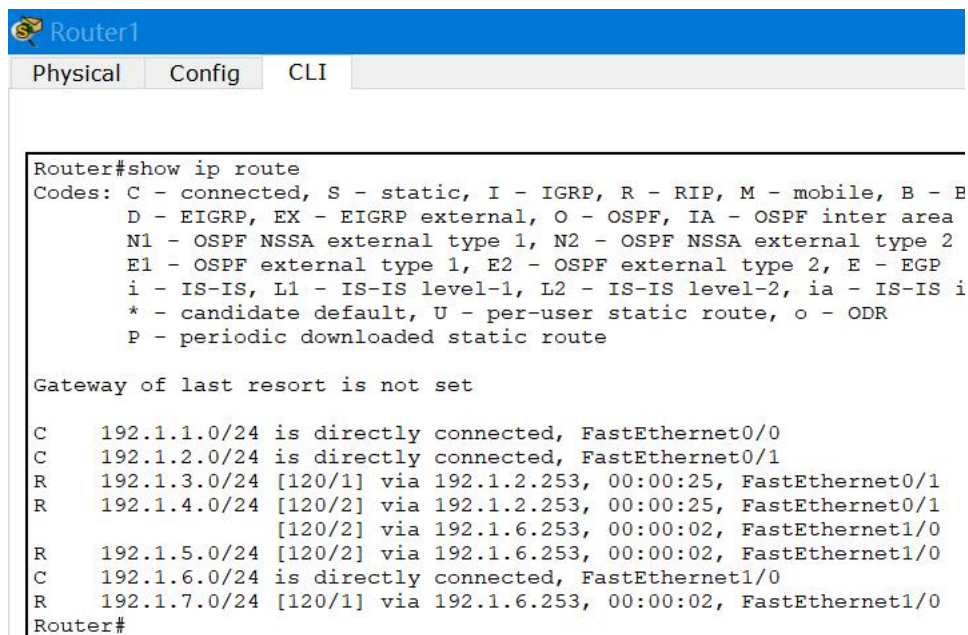


图 23 路由器 Router1 路由表一

- (4) 切换到模拟操作模式, 查看 PC0 发送给 PC2 的 ICMP 报文, 该 ICMP 报文经路由器 Router5, 如图 24 所示。(注意配置 PC0 和 PC2 的 IP 地址, 掩码和网关)

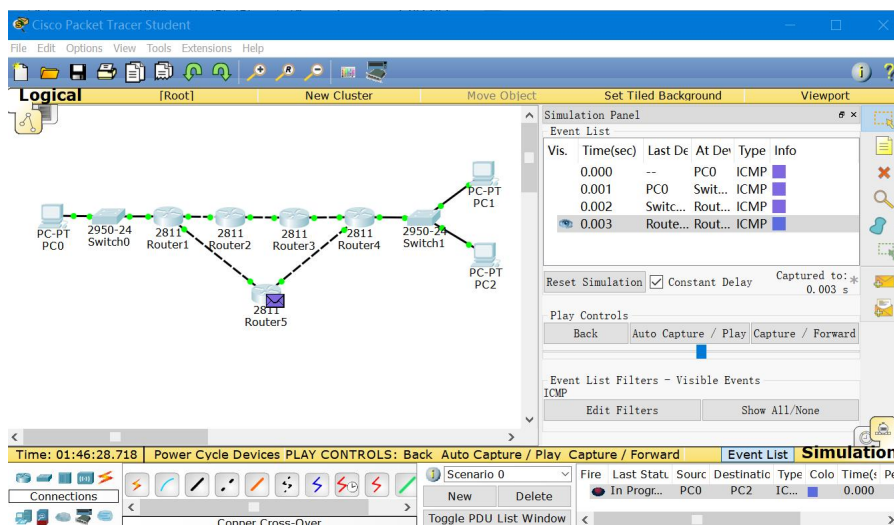


图 24 PC0 至 PC2 ICMP 报文经过 Router5

- (5) 切换到实时操作模式，在路由器 Router1 中配置一项静态路由项，如图 25 所示，目的网络是 192.1.5.2/32，下一跳是 192.1.2.253。其中 192.1.5.2 是 PC2 的 IP 地址，前缀长度等于 32 的子网掩码表示目的网络只包含单个 IP 地址。192.1.2.253 是路由器 Router2 连接路由器 Router1 的接口的 IP 地址。配置静态路由项后的路由器 Router1 的路由表如图 26 所示。

Router1

Physical Config CLI

GLOBAL

Settings

Algorithm Settings

ROUTING

Static

RIP

SWITCHING

LAN Database

INTERFACE

FastEthernet0/0

FastEthernet0/1

FastEthernet1/0

Static Routes

Network 192.1.5.2

Mask 255.255.255.255

Next Hop 192.1.2.253

Add

Network Address

192.1.5.2/32 via 192.1.2.253

Remove

Equivalent IOS Commands

```
Router#configure terminal
Enter configuration commands, one per line. End with
CNTL/Z.
Router(config)#ip route 192.1.5.2 255.255.255.255
192.1.2.253
Router(config)#
```

图 25 静态路由项配置界面

```
Router#show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS int
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is not set

C    192.1.1.0/24 is directly connected, FastEthernet0/0
C    192.1.2.0/24 is directly connected, FastEthernet0/1
R    192.1.3.0/24 [120/1] via 192.1.2.253, 00:00:01, FastEthernet0/1
R    192.1.4.0/24 [120/2] via 192.1.2.253, 00:00:01, FastEthernet0/1
       [120/2] via 192.1.6.253, 00:00:00, FastEthernet1/0
R    192.1.5.0/24 is variably subnetted, 2 subnets, 2 masks
       192.1.5.0/24 [120/2] via 192.1.6.253, 00:00:00, FastEthernet1/0
S    192.1.5.2/32 [1/0] via 192.1.2.253
C    192.1.6.0/24 is directly connected, FastEthernet1/0
R    192.1.7.0/24 [120/1] via 192.1.6.253, 00:00:00, FastEthernet1/0
```

图 26 路由器 Router1 路由表二

- (6) 切换到模拟操作模式，查看 PC0 发送给 PC2 的 ICMP 报文，路由器 Router1 将该 ICMP 报文转发给路由器 Router2，如图 27 所示。查看 PC0 发送给 PC1 的 ICMP 报文，路由器 Router1 将该 ICMP 报文转发给路由器 Router5，如图 28 所示。

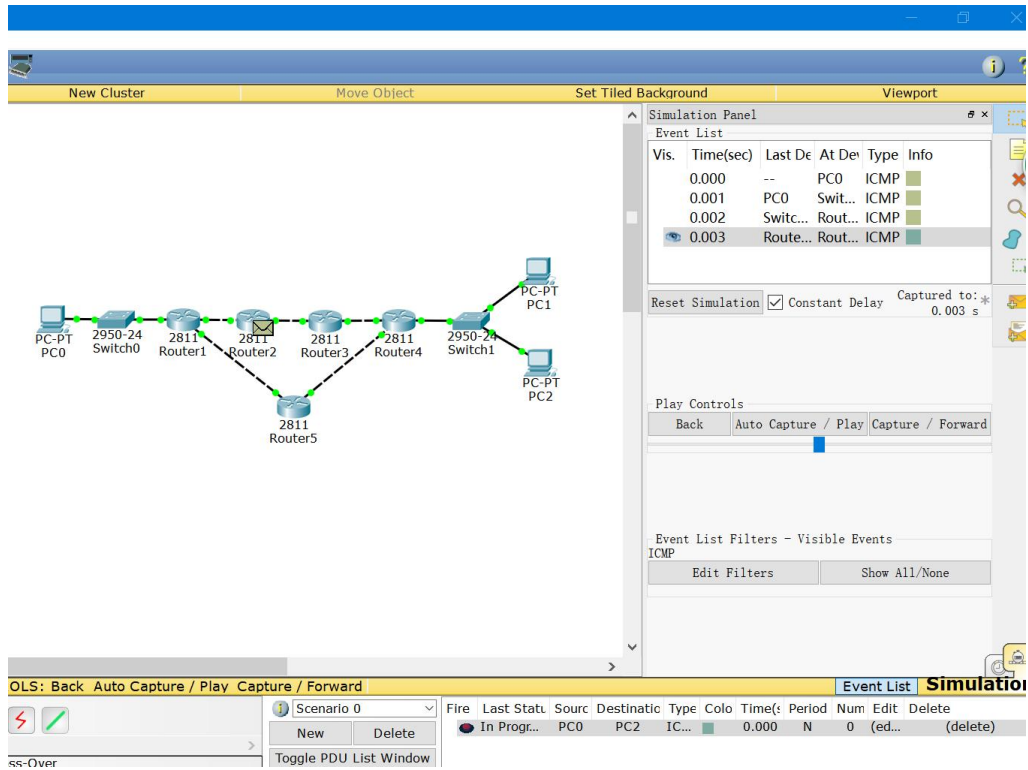


图 27 PC0 至 PC2 ICMP 报文经过 Router2

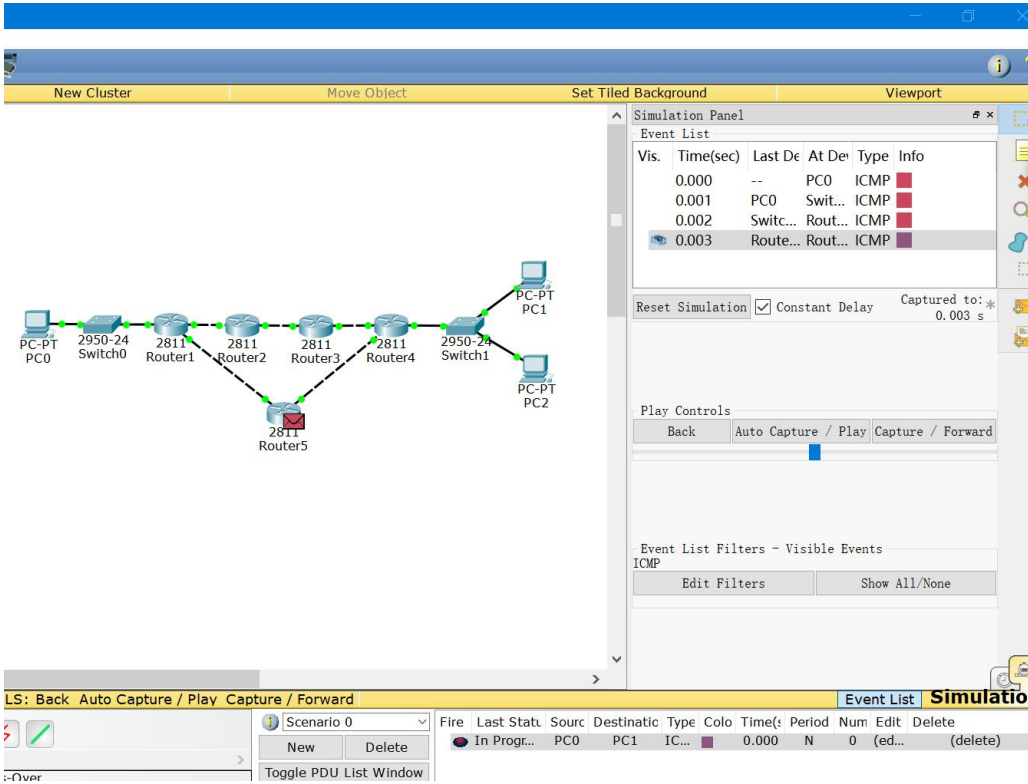


图 28 PC0 至 PC1 ICMP 报文经过 Router5