体验网络配置 实验报告

计 52 路橙 2015010137

Part 1：粗心的同事

1. IP 分配：

   a) Server0 的 Gateway 应该和 Laptop0、PC0 一致，即为 192.168.1.1

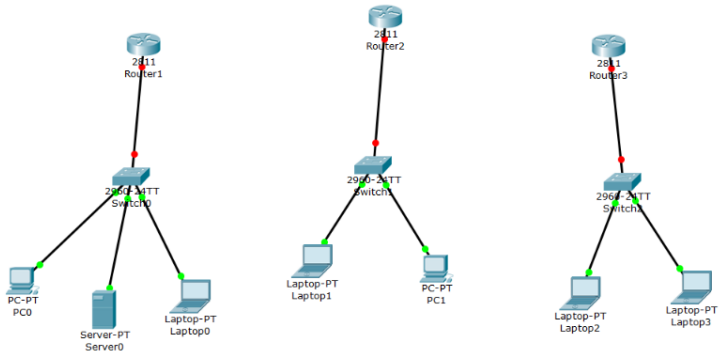
   b) Router3 的端口 1 错误分配成公网 ip，应重新分配为内网 ip

   此处，我的分配方案为：10.2.3.2

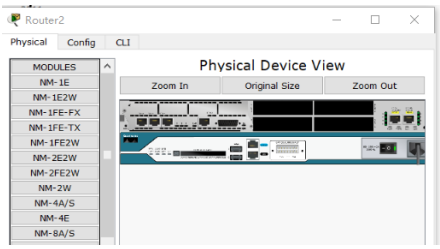
   c) 分析可知，Router2 的端口 2 应与 Router3 相连，基于（b）中的 ip 分配，因此将 Router2 的端口 2 分配 ip 为 10.2.3.3

2. 铺设网络：

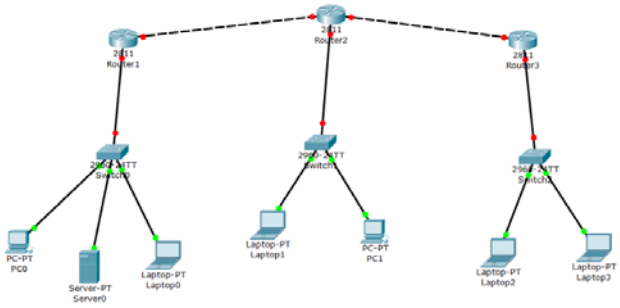
   a) 选用交换机全部为 2960-24TT，路由器全部为 2811.初步连线如下：



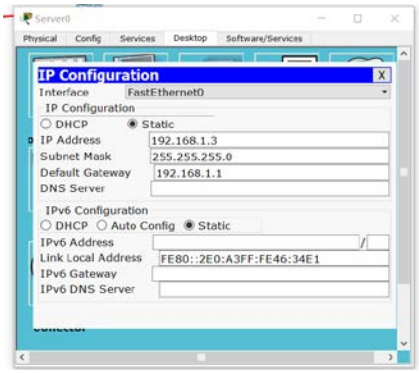
   b) 为 Router2 配置 NM-4E Module（断电后配置）：



   c) 将路由器连接：

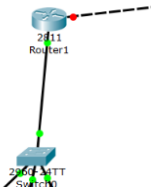


d) 配置终端设备的 ip（以 Server0 为例）：



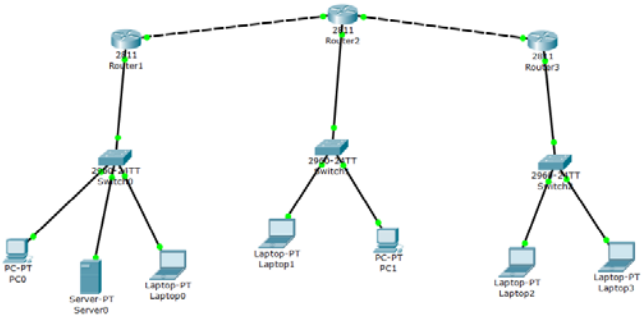
e) 配置路由器的端口与 ip：

```
Router>enable
Router#confi term
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#int f0/0
Router(config-if)#ip add 192.168.1.1 255.255.255.0
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
```



可以看到，路由器与交换机已经连接通。重复以上步骤设置所有路由器的 ip。

全部配置好后，网络拓扑如下，可见所有圆点变成了绿色：



Part 2：公网网关安全

1. 为 Router1 设置登录口令：

   a) 设置通过 console 口进入用户模式的口令：

```
Router(config)#line console 0
Router(config-line)#password G&(JBIg0vjuj45390
Router(config-line)#
```

   b) 设置用户模式进入特权模式的口令：

```
Router(config)#enable password *&N$G_H$#U()jrt543
Router(config)#
```

   c) 通过 telnet 方式登录路由器的口令：

```
Router(config)#line console 0
Router(config-line)#login
Router(config-line)#line vty 0 4
Router(config-line)#password )(@JU)NGOI79834jil
Router(config-line)#
```

   通过 show running-config 查看密码，可见密码均以明文形式存储：

```
Router#show running-config
Building configuration...

Current configuration : 974 bytes
!
version 12.4
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
!
hostname Router
!
!
!
enable password *&N$G_H$#U()jrt543
!
!
```

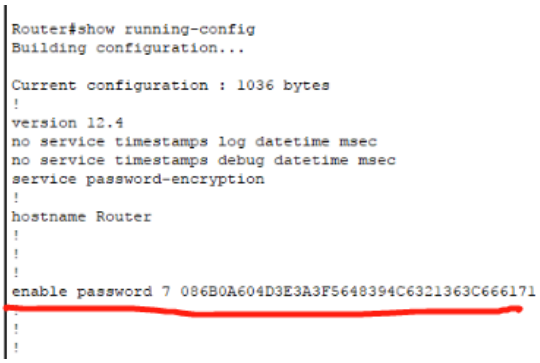
```
!
!
!
line con 0
 password G&(JBIg0vjuj45390
 login
!
line aux 0
!
line vty 0 4
 password )(@JU)NGOI79834jil
 login
!
!
!
```

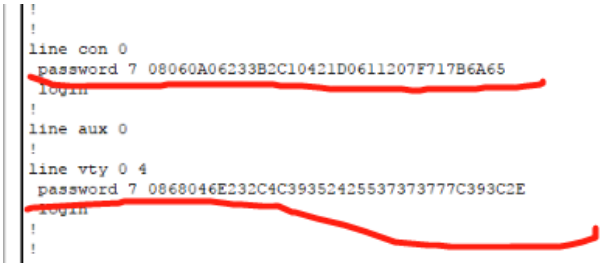
2. 使用密文形式存储密码：

   当路由器配置文件可能被泄露时，**使用密文存储密码**，即使用命令 service password-encryption.

```
Router#conf term
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#service password-encryption
Router(config)#end
Router#
```

   再次使用 show running-config 查看配置文件：





可以看到，所有的密码都以密文的形式存储在了路由器的配置文件中。因此，当路由器的配置文件遭到泄露时，依然有安全保障。

Part 3：各部门的正常通信

1. 设置路由器的静态路由表：

如下图进行配置，以 Router1 的配置为例，将所有无法由 Router1 直达的网段全部配置路由。

```
Router#
Router#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#ip route 192.168.2.0 255.255.255.0 10.1.2.2
Router(config)#ip route 192.168.3.0 255.255.255.0 10.1.2.2
Router(config)#ip route 10.2.3.0 255.255.255.0 10.1.2.2
Router(config)#
```

2. 通过 show ip route 查看路由表：

Router1:

```
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

     10.0.0.0/24 is subnetted, 2 subnets
C       10.1.2.0 is directly connected, FastEthernet0/1
S       10.2.3.0 [1/0] via 10.1.2.2
C    192.168.1.0/24 is directly connected, FastEthernet0/0
S    192.168.2.0/24 [1/0] via 10.1.2.2
S    192.168.3.0/24 [1/0] via 10.1.2.2
Router#
```

Router2:

```
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

     10.0.0.0/24 is subnetted, 2 subnets
C       10.1.2.0 is directly connected, FastEthernet0/0
C       10.2.3.0 is directly connected, FastEthernet0/1
S    192.168.1.0/24 [1/0] via 10.1.2.1
C    192.168.2.0/24 is directly connected, Ethernet1/0
S    192.168.3.0/24 [1/0] via 10.2.3.2
Router#
```

Router3:

```
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

     10.0.0.0/24 is subnetted, 2 subnets
S       10.1.2.0 [1/0] via 10.2.3.3
C       10.2.3.0 is directly connected, FastEthernet0/0
S    192.168.1.0/24 [1/0] via 10.2.3.3
S    192.168.2.0/24 [1/0] via 10.2.3.3
C    192.168.3.0/24 is directly connected, FastEthernet0/1
```

3. 通过 ping 命令查看是否能正常通信：

   以 PC0 ping laptop2 为例：

```
PC>ping 192.168.3.2

Pinging 192.168.3.2 with 32 bytes of data:

Reply from 192.168.3.2: bytes=32 time=2ms TTL=125
Reply from 192.168.3.2: bytes=32 time=0ms TTL=125
Reply from 192.168.3.2: bytes=32 time=1ms TTL=125
Reply from 192.168.3.2: bytes=32 time=0ms TTL=125

Ping statistics for 192.168.3.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 2ms, Average = 0ms
```

经过测试，所有的设备之间均可以 ping 成功。

Part 4：避免设备故障带来的影响

1. 在 Router1 和 Router2 之间增加一条链路，中间用路由器连接。仿照任务 1 设置 ip.

   下图为 Router4 的端口 ip 设置：

```
     10.0.0.0/24 is subnetted, 2 subnets
C       10.1.3.0 is directly connected, FastEthernet0/0
C       10.1.4.0 is directly connected, FastEthernet0/1
```

2. 配置 Router1，Router2 和 Router4 的路由表：

Router1 中通过设置 metric 来规定优先级，优先选择直连 Router2 所在的路径，其次选择 Router4 所在路径。Router2 同理，优先选择直连 Router1，其次选择 Router4.

首先把任务 3 中的 route 设置成带有 metric 的指令，其次添加 Router4 相关的路由。这里以 Router1 为例，Router2 同理：

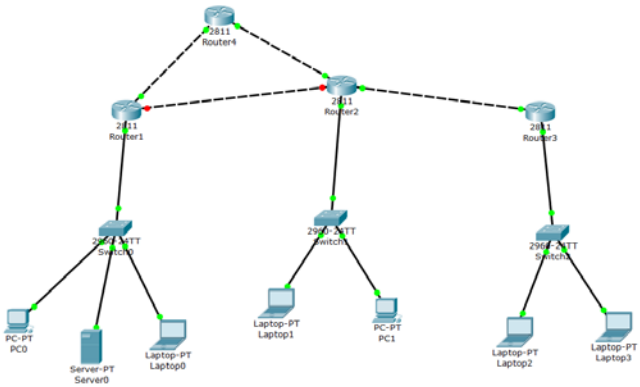
```
Router(config)#no ip route 192.168.2.0 255.255.255.0 10.1.2.2
Router(config)#no ip route 192.168.3.0 255.255.255.0 10.1.2.2
Router(config)#no ip route 10.2.3.0 255.255.255.0 10.1.2.2
Router(config)#ip route 192.168.3.0 255.255.255.0 10.1.2.2 1
Router(config)#ip route 192.168.2.0 255.255.255.0 10.1.2.2 1
Router(config)#ip route 10.2.3.0 255.255.255.0 10.1.2.2 1
```

```
Router(config)#ip route 192.168.2.0 255.255.255.0 10.1.3.2 2
Router(config)#
Router(config)#ip route 192.168.3.0 255.255.255.0 10.1.3.2 2
Router(config)#ip route 10.2.3.0 255.255.255.0 10.1.3.2 2
```

Router4 的静态路由表配置同任务 3，配置好后如下：

```
     10.0.0.0/24 is subnetted, 2 subnets
C       10.1.3.0 is directly connected, FastEthernet0/0
C       10.1.4.0 is directly connected, FastEthernet0/1
S    192.168.1.0/24 [1/0] via 10.1.3.1
S    192.168.2.0/24 [1/0] via 10.1.4.1
S    192.168.3.0/24 [1/0] via 10.1.4.1
```

3. 当 Router1 与 Router2 之间的线路断开时：



使用 PC0 尝试 Ping Laptop3：

```
PC>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=124
Reply from 192.168.3.2: bytes=32 time=11ms TTL=124
Reply from 192.168.3.2: bytes=32 time=11ms TTL=124
Reply from 192.168.3.2: bytes=32 time=12ms TTL=124

Ping statistics for 192.168.3.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 1ms, Maximum = 12ms, Average = 8ms
```

Part 5：人员精简计划

1. 只允许 PC0 和 PC1 对 Laptop3 访问：

   允许二者的报文到达 Laptop3，允许 Laptop3 的报文到达 PC0 和 PC1.

   ```
   access-list 102 permit ip 192.168.1.2 0.0.0.0 192.168.3.3 0.0.0.0

   access-list 102 permit ip 192.168.2.2 0.0.0.0 192.168.3.3 0.0.0.0

   access-list 103 permit ip 192.168.3.3 0.0.0.0 192.168.1.2 0.0.0.0

   access-list 103 permit ip 192.168.3.3 0.0.0.0 192.168.2.2 0.0.0.0
   ```

2. 允许 Server0 ping，但无法访问：

   允许 Server0 的报文到达 Laptop3, 但只允许 Laptop3 返回的 ICMP 报文通过 Router3

   ```
   access-list 102 permit ip 192.168.1.3 0.0.0.0 192.168.3.3 0.0.0.0

   ip inspect name cbac_icmp icmp

   int Fa0/0

   ip inspect cbac_icmp in
   ```

   （注：这里的 Fa0/0 为 Router2 与 Router3 相连的线中 Router3 的端点）

3. 允许任意网络与 Laptop2 通信：

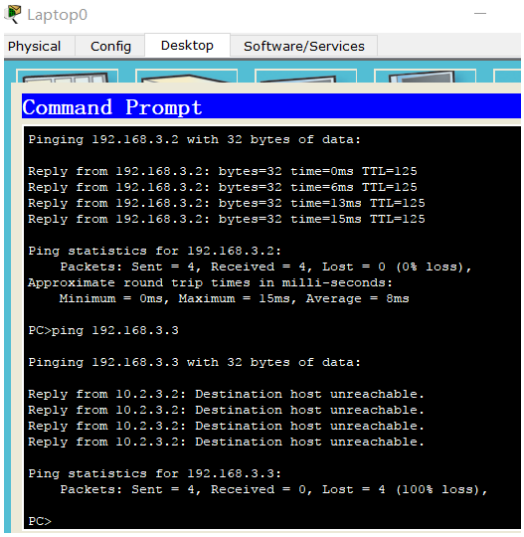
   ```
   access-list 102 permit ip any 192.168.3.2 0.0.0.0

   access-list 103 permit ip 192.168.3.2 0.0.0.0 any
   ```

4. 应用 access-list：

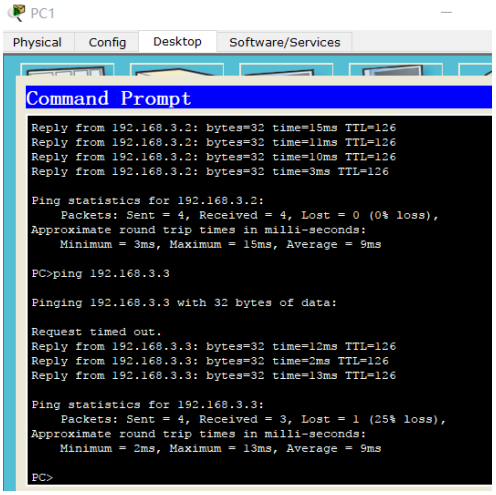
   ```
   int Fa0/0

   ip access-group 102 in

   ip access-group 103 out
   ```

测试：

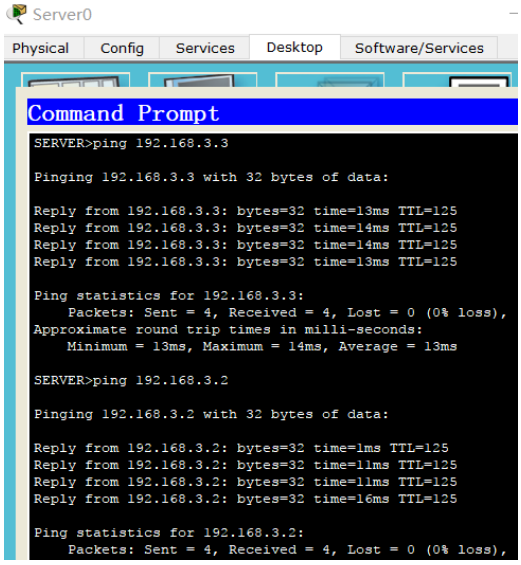
在 Laptop0 中 ping Laptop3：



在 PC1 中 ping Laptop2 和 Laptop3：



在 Server0 中 ping Laptop2 和 Laptop3：



Part 6：利用协议进行路由管理

选择 RIP 协议：

配置 Router1：

```
Router(config)#router rip
Router(config-router)#network 192.168.1.0
Router(config-router)#network 10.0.0.0
Router(config-router)#
```

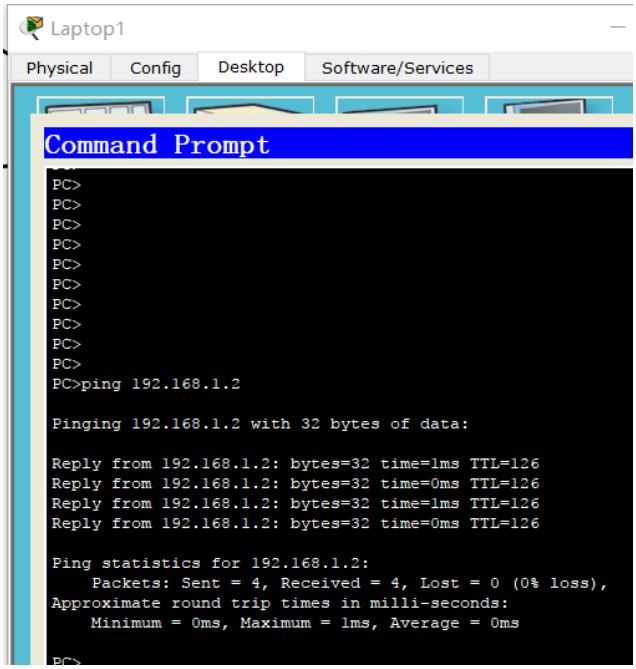
配置 Router2：

```
Router(config)#router rip
Router(config-router)#network 192.168.2.0
Router(config-router)#network 10.0.0.0
```

配置 Router3：

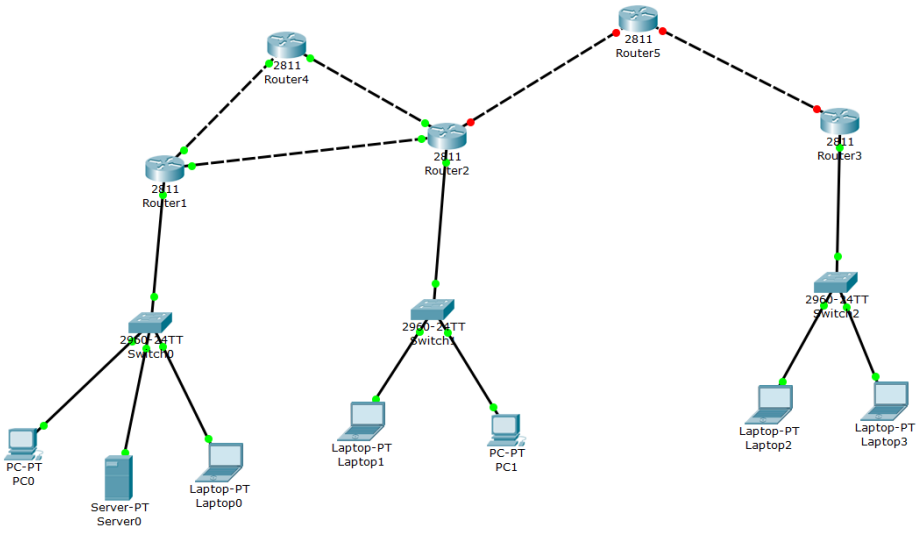
```
Router(config)#router rip
Router(config-router)#network 192.168.3.0
Router(config-router)#network 10.0.0.0
```

进行测试：



Part 7：IPSec VPN 跨越公网

加入新路由器表示公网，并配置静态路由如下：



Router2：

```
Router(config)#interface FastEthernet0/1
Router(config-if)#ip address 122.1.1.2 255.255.255.0
Router(config-if)#shutdown
```

```
Router(config)#no ip route 192.168.3.0 255.255.255.0 10.2.3.2
Router(config)#ip route 192.168.3.0 255.255.255.0 122.1.1.1
Router(config)#
```

Router5：

```
Router(config)#interface FastEthernet0/0
Router(config-if)#ip address 122.1.1.2 255.0.0.0
Router(config-if)#ip address 122.1.1.2 255.255.255.0
Router(config-if)#no shutdown
```

```
Router(config)#
Router(config)#ip route 192.168.1.0 255.255.255.0 122.1.1.2
Router(config)#ip route 192.168.2.0 255.255.255.0 122.1.1.2
```

```
Router(config)#interface FastEthernet0/1
Router(config-if)#
Router(config-if)#exit
Router(config)#router rip
Router(config-router)#
Router(config-router)#exit
Router(config)#
Router(config)#ip route 192.168.1.0 255.255.255.0 122.1.1.2
Router(config)#ip route 192.168.2.0 255.255.255.0 122.1.1.2
```

```
Router(config)#ip route 192.168.3.0 255.255.255.0 133.1.1.2
Router(config)#
```

Router3：

```
Router(config)#no ip route 192.168.1.0 255.255.255.0 10.2.3.3
Router(config)#no ip route 192.168.2.0 255.255.255.0 10.2.3.3
Router(config)#no ip route 10.1.2.0 255.255.255.0 10.2.3.3
Router(config)#
Router(config)#ip route 192.168.2.0 255.255.255.0 133.1.1.1
Router(config)#ip route 192.168.1.0 255.255.255.0 133.1.1.1
Router(config)#
Router(config)#interface FastEthernet0/1
Router(config-if)#
Router(config-if)#exit
Router(config)#interface FastEthernet0/0
Router(config-if)#ip address 133.1.1.2 255.255.255.0
Router(config-if)#
Router(config-if)#exit
Router(config)#interface FastEthernet0/0
Router(config-if)#shutdown
```

配置 Router2 和 Router3：（以 Router2 为例）

```
crypto isakmp policy 3

encryption 3des

hash md5

authentication pre-share

crypto isakmp key example address 133.1.1.2

crypto ipsec transform-set testtag ah -md5-hmac esp-3des

access-list 101 permit ip 192.168.1.0 0.0.0.255 192.168.3.0 0.0.0.255

access-list 101 permit ip 192.168.2.0 0.0.0.255 192.168.3.0 0.0.0.255

crypto map test 11 ipsec-isakmp

set peer 133.1.1.2

set transform-set testtag

match address 101

crypto map test
```

最终可以 ping 通：

```
PC>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
Reply from 192.168.3.2: bytes=32 time=0ms TTL=125
Reply from 192.168.3.2: bytes=32 time=1ms TTL=125
Reply from 192.168.3.2: bytes=32 time=0ms TTL=125

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