计算机网络安全技术
实验二报告

2017011620 计 73 李家昊

2019 年 12 月 3 日

1 任务 6

对于任务 6 和任务 7，这里继承第一次作业的网络结构，Router1, 2, 3 均已配置好 RIP 路由协议，所有设备的 ip 设置与第一次作业相同。

由于部门之间只能通过助手和秘书通信，需要根据源 ip 和目标 ip 进行访问控制，因此这里采用扩展 ACL。

为了对 Server0 进行严格的访问控制,这里为其单独配置一个路由器 Router4，Router4 对外 ip 为 192.168.1.2，对内 ip 为 192.168.4.1，修改 Server0 的 ip 为 192.168.4.2，网关为 192.168.4.1，然后在 Router4 上配置好 RIP 路由协议，网络连接成功，拓扑结构如 Figure 1 所示。

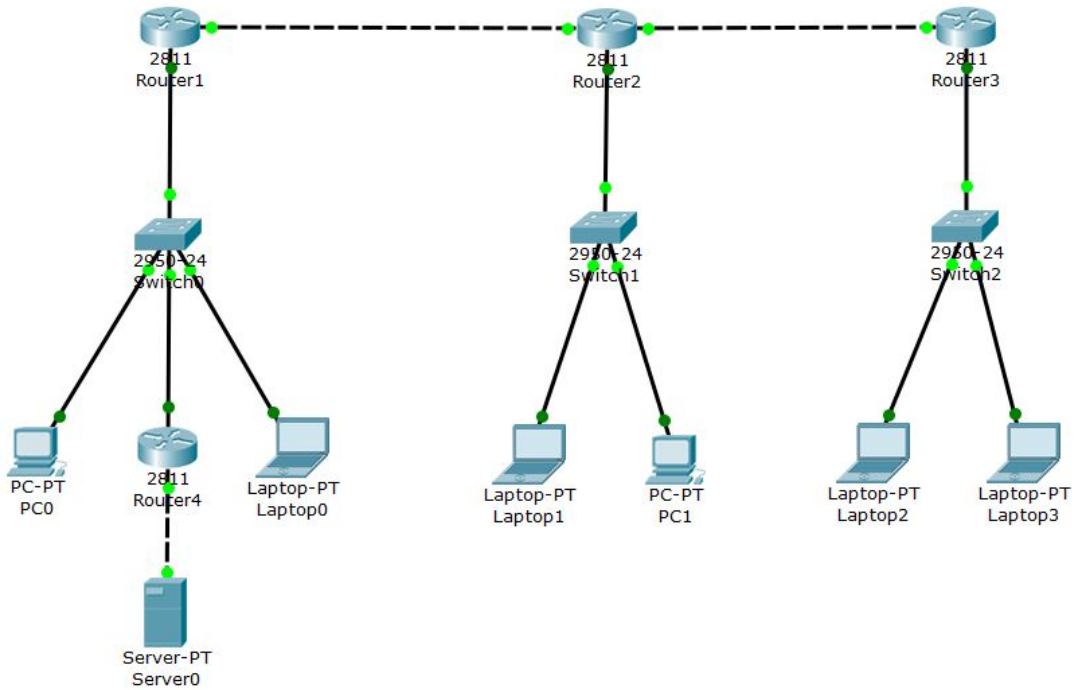


图 1: 网络拓扑

所有路由器仅配置对内（路由器下方）端口的 ACL，首先在技术研发部的 Router1 上配置 ACL。

使其他两个部门的所有成员能够与杨助手通信

```
Router(config)#access-list 101 permit ip 192.168.2.0 0.0.0.255
   192.168.1.4 0.0.0.0
Router(config)#access-list 101 permit ip 192.168.3.0 0.0.0.255
   192.168.1.4 0.0.0.0
```

使其他两个部门的助手能够与技术研发部的所有成员通信

```
Router(config)#access-list 101 permit ip 192.168.2.2 0.0.0.0
   192.168.1.0 0.0.0.255
Router(config)#access-list 101 permit ip 192.168.3.3 0.0.0.0
   192.168.1.0 0.0.0.255
```

使其他两个部门的部长能够与技术研发部的部长通信

```
Router(config)#access-list 101 permit ip 192.168.2.3 0.0.0.0
   192.168.1.2 0.0.0.0
Router(config)#access-list 101 permit ip 192.168.3.2 0.0.0.0
   192.168.1.2 0.0.0.0
```

使技术研发部的部长可以与 Server0 互相通信

```
Router(config)#access-list 101 permit ip 192.168.1.2 0.0.0.0
   192.168.4.2 0.0.0.0
Router(config)#access-list 101 permit ip 192.168.4.2 0.0.0.0
   192.168.1.2 0.0.0.0
```

将 ACL 绑定在 Router1 的 192.168.1.0 子网的 out 方向。

```
Router(config)#interface FastEthernet 0/0
Router(config-if)#ip access-group 101 out
```

同理，在 Router2 上配置 ACL。

```
Router(config)#access-list 102 permit ip 192.168.1.0 0.0.0.255
   192.168.2.2 0.0.0.0
Router(config)#access-list 102 permit ip 192.168.3.0 0.0.0.255
   192.168.2.2 0.0.0.0

Router(config)#access-list 102 permit ip 192.168.1.4 0.0.0.0
   192.168.2.0 0.0.0.255
Router(config)#access-list 102 permit ip 192.168.3.3 0.0.0.0
   192.168.2.0 0.0.0.255

Router(config)#access-list 102 permit ip 192.168.1.2 0.0.0.0
   192.168.2.3 0.0.0.0
```

```
Router(config)#access-list 102 permit ip 192.168.3.2 0.0.0.0
    192.168.2.3 0.0.0.0

Router(config)#interface FastEthernet 0/0
Router(config-if)#ip access-group 102 out
```

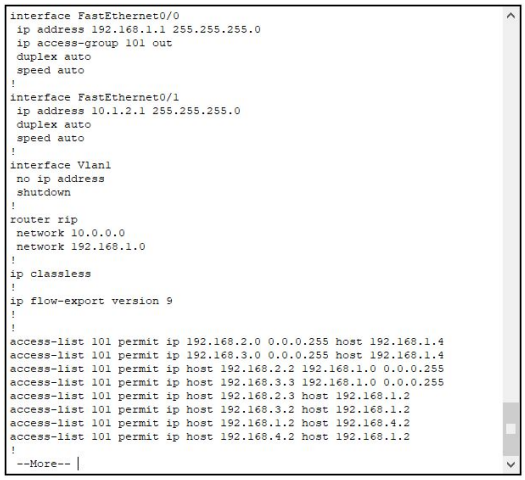
同理，在 Router3 上配置 ACL。

```
Router(config)#access-list 103 permit ip 192.168.1.0 0.0.0.255
    192.168.3.3 0.0.0.0
Router(config)#access-list 103 permit ip 192.168.2.0 0.0.0.255
    192.168.3.3 0.0.0.0

Router(config)#access-list 103 permit ip 192.168.1.4 0.0.0.0
    192.168.3.0 0.0.0.255
Router(config)#access-list 103 permit ip 192.168.2.2 0.0.0.0
    192.168.3.0 0.0.0.255

Router(config)#access-list 103 permit ip 192.168.1.2 0.0.0.0
    192.168.3.2 0.0.0.0
Router(config)#access-list 103 permit ip 192.168.2.3 0.0.0.0
    192.168.3.2 0.0.0.0

Router(config)#interface FastEthernet 0/0
Router(config-if)#ip access-group 103 out
```

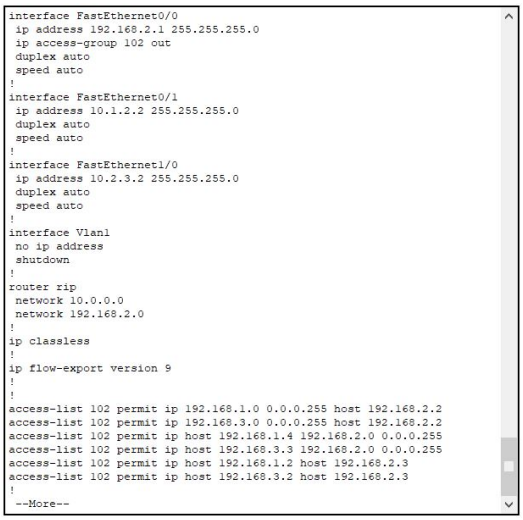
在 Router4 上配置 ACL，为严格管控出入 Server0 的流量，这里同时配置 in/out 端口。

```
Router(config)#access-list 104 permit ip 192.168.1.2 0.0.0.0
    192.168.4.2 0.0.0.0
Router(config)#access-list 105 permit ip 192.168.4.2 0.0.0.0
    192.168.1.2 0.0.0.0

Router(config)#interface FastEthernet 0/0
Router(config-if)#ip access-group 104 out
Router(config-if)#ip access-group 105 in
```

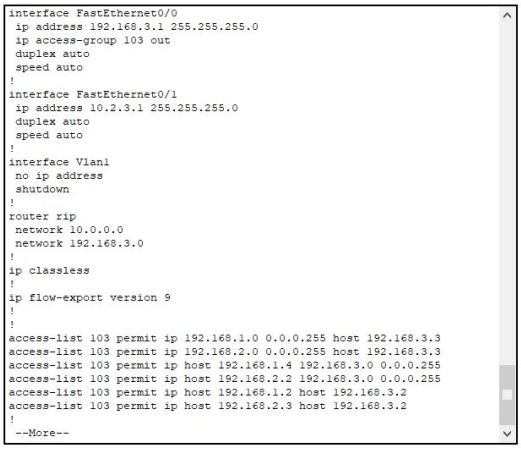
配置完成后，在 Router1, 2, 3, 4 执行`show running-config` 查看配置，如 Figure 2 所示。



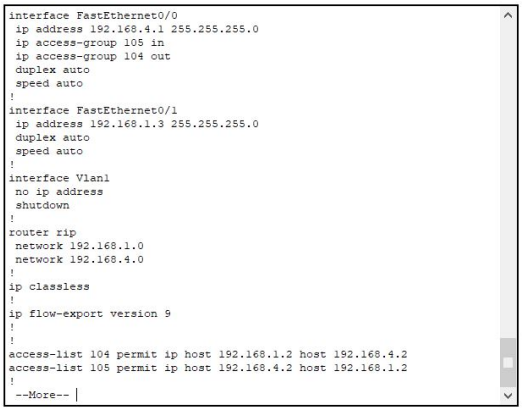
(a) Router1



(b) Router2



(c) Router3



(d) Router4

图 2: 四个路由器的 ACL 配置

为了对访问控制进行测试，这里在每个子网内都添加了一台测试设备，分别为 TEST1，TEST2 和 TEST3，测试结果如 Figure 3 所示。

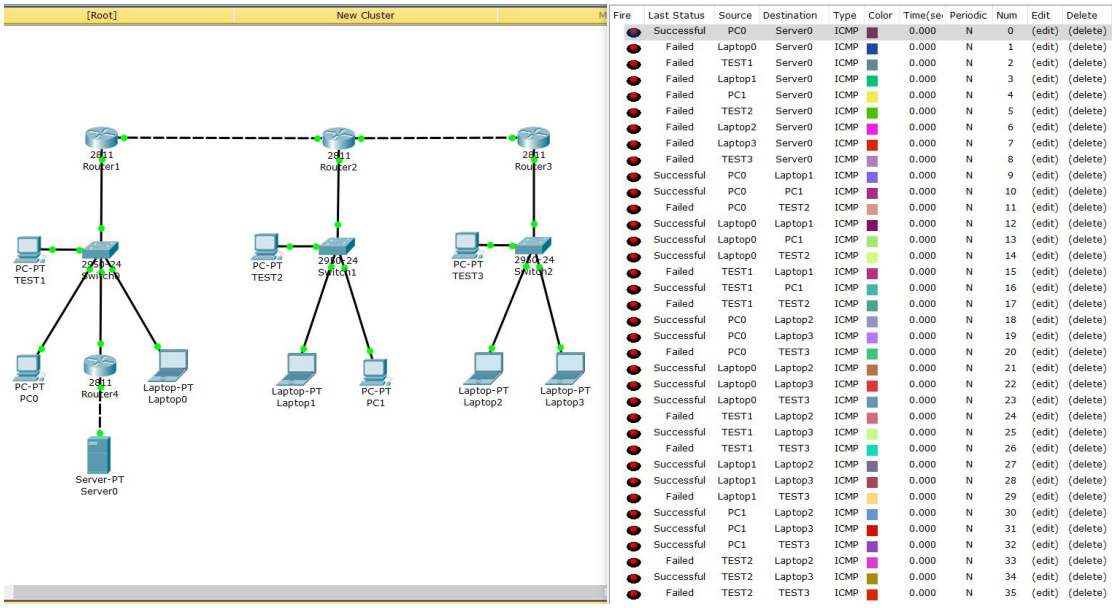


图 3: ACL 测试结果

其中，序号 0-8 为其他设备对 Server0 的访问控制测试，序号 9-17 是子网 192.168.1.0/24 和子网 192.168.2.0/24 之间的访问控制测试，序号 18-26 是子网 192.168.1.0/24 和子网 192.168.3.0/24，序号 27-35 是子网 192.168.2.0/24 和子网 192.168.3.0/24 之间的访问控制测试。从测试结果可以看出，此配置完全符合题目要求。

2 任务 7

为了让子网 192.168.2.0/24 和 192.168.3.0/24 内每一台设备收到 PC0 发来的 ICMP 请求，这里需要修改 Router2 和 Router3 的 ACL。

在 Router2 中

```
Router(config)#access-list 102 permit ip 192.168.1.2 0.0.0.0
    192.168.2.0 0.0.0.255
```

在 Router3 中

```
Router(config)#access-list 103 permit ip 192.168.1.2 0.0.0.0
    192.168.3.0 0.0.0.255
```

为了让 Router1 放行对方的应答，需要配置 CBAC

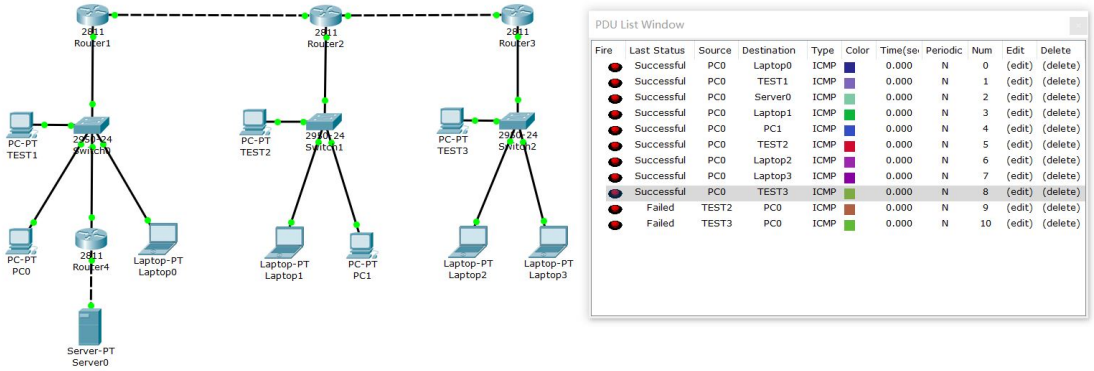
```
Router(config)#ip inspect name CBAC icmp
Router(config)#interface FastEthernet 0/0
Router(config-if)#ip inspect CBAC in
```

Router1 的 CBAC 配置如 Figure 4 所示

```
!
!
!
!
!
!
!
!
!
ip inspect name CBAC icmp timeout 10
spanning-tree mode pvst
!
!
!
!
!
!
interface FastEthernet0/0
 ip address 192.168.1.1 255.255.255.0
 ip access-group 101 out
 ip inspect CBAC in
 duplex auto
 speed auto
!
 --More--
```

图 4: Router1 的 CBAC 配置

配置完成后，测试结果如 Figure 5 所示



Fire	Last Status	Source	Destination	Type	Color	Time(se	Periodic	Num	Edit	Delete
	Successful	PC0	Laptop0	ICMP		0.000	N	0	(edit)	(delete)
	Successful	PC0	TEST1	ICMP		0.000	N	1	(edit)	(delete)
	Successful	PC0	Server0	ICMP		0.000	N	2	(edit)	(delete)
	Successful	PC0	Laptop1	ICMP		0.000	N	3	(edit)	(delete)
	Successful	PC0	PC1	ICMP		0.000	N	4	(edit)	(delete)
	Successful	PC0	TEST2	ICMP		0.000	N	5	(edit)	(delete)
	Successful	PC0	Laptop2	ICMP		0.000	N	6	(edit)	(delete)
	Successful	PC0	Laptop3	ICMP		0.000	N	7	(edit)	(delete)
	Successful	PC0	TEST3	ICMP		0.000	N	8	(edit)	(delete)
	Failed	TEST2	PC0	ICMP		0.000	N	9	(edit)	(delete)
	Failed	TEST3	PC0	ICMP		0.000	N	10	(edit)	(delete)

图 5: CBAC 测试结果

从序号 0-8 可以看出，PC0 能 ping 通所有设备，从最后两行可以看出，测试设备 TEST2 和 TEST3 不能主动 ping 通 PC0，说明 CBAC 配置成功，网络配置符合要求。

3 任务 8

在公网上，公司的两台边界路由器一般不能直连，而公网上的中继路由器一般不能转发类似 192.168.1.1 这样的内网 ip 请求，因此静态路由失效。

配置 Router1 公网出口为 100.1.1.2，Router2 公网出口为 200.1.1.2，Router4 两个子网分别为 100.1.1.0/24 和 200.1.1.0/24。

接下来配置 VPN，首先配置 IKE 策略，配置加密算法为 3des，哈希算法为 md5，密钥协商算法为 DH5，采用预共享密钥认证方法，并使用 esp 进行加密和认证。

然后配置加密映射，设置对方边界路由器的公网 ip，指定 esp 加密和认证，配置 ACL 并绑定到对应 VPN 出口上。

具体来说，在 Router1 上配置如下，注意需要配置一条默认路由，使得非子网的流量走公网路由器。

```
Router(config)#crypto isakmp policy 1
Router(config-isakmp)#encryption 3des
Router(config-isakmp)#hash md5
Router(config-isakmp)#group 5
Router(config-isakmp)#authentication pre-share
Router(config-isakmp)#exit

Router(config)#crypto isakmp key ljhkey address 200.1.1.2
Router(config)#crypto ipsec transform-set ljhset esp-3des esp-md5-
   hmac
Router(config)#access-list 111 permit ip 192.168.1.0 0.0.0.255
   192.168.2.0 0.0.0.255
Router(config)#access-list 111 permit ip 192.168.1.0 0.0.0.255
   192.168.3.0 0.0.0.255

Router(config)#crypto map ljhmap 1 ipsec-isakmp
Router(config-crypto-map)#set peer 200.1.1.2
Router(config-crypto-map)#set transform-set ljhset
Router(config-crypto-map)#match address 111
Router(config-crypto-map)#exit

Router(config)#interface FastEthernet 0/1
Router(config-if)#crypto map ljhmap
Router(config-if)#exit

Router(config)#ip route 0.0.0.0 0.0.0.0 100.1.1.1
```

同理在 Router2 上配置，Router2 需要配一条到子网 192.168.3.0/24 的静态路由，并将默认路由设为 200.1.1.1。

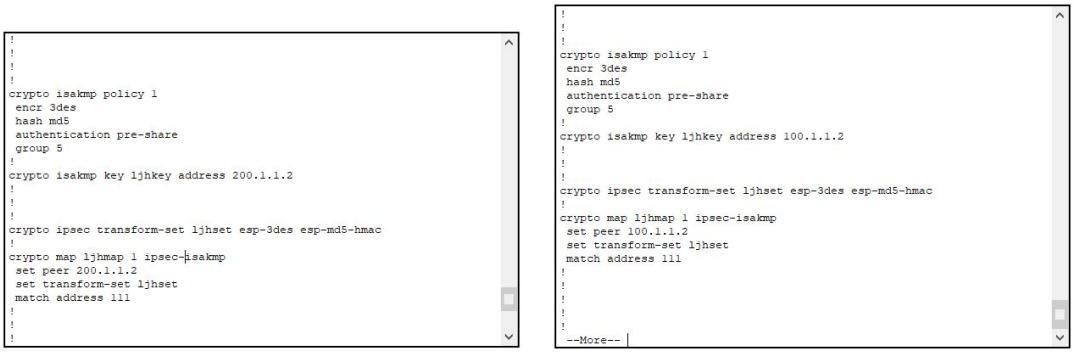
```
Router(config)#crypto isakmp policy 1
Router(config-isakmp)#encryption 3des
Router(config-isakmp)#hash md5
Router(config-isakmp)#group 5
Router(config-isakmp)#authentication pre-share
```

```
Router(config-isakmp)#exit

Router(config)#crypto ipsec transform-set ljhset esp-3des esp-md5-
    hmac
Router(config)#crypto isakmp key ljhkey address 100.1.1.2
Router(config)#access-list 111 permit ip 192.168.2.0 0.0.0.255
    192.168.1.0 0.0.0.255
Router(config)#access-list 111 permit ip 192.168.3.0 0.0.0.255
    192.168.1.0 0.0.0.255

Router(config)#crypto map ljhmap 1 ipsec-isakmp
Router(config-crypto-map)#set peer 100.1.1.2
Router(config-crypto-map)#set transform-set ljhset
Router(config-crypto-map)#match address 111
Router(config-crypto-map)#exit

Router(config)#interface FastEthernet 0/1
Router(config-if)#crypto map ljhmap
Router(config-if)#exit

Router(config)#ip route 192.168.3.0 255.255.255.0 10.2.3.1
Router(config)#ip route 0.0.0.0 0.0.0.0 200.1.1.1
```

Router3 将默认路由设为 10.2.3.2。

```
Router(config)#ip route 0.0.0.0 0.0.0.0 10.2.3.2
```

配置完成后，在 Router1, 2 内执行`show running-config` 查看配置，如 Figure 6 所示。



(a) Router1　　(b) Router2

图 6: VPN 配置

接下来对 VPN 连接进行测试，测试结果如 Figure 7 所示，可以看到分部的所有设备均能与总部的所有设备通信。

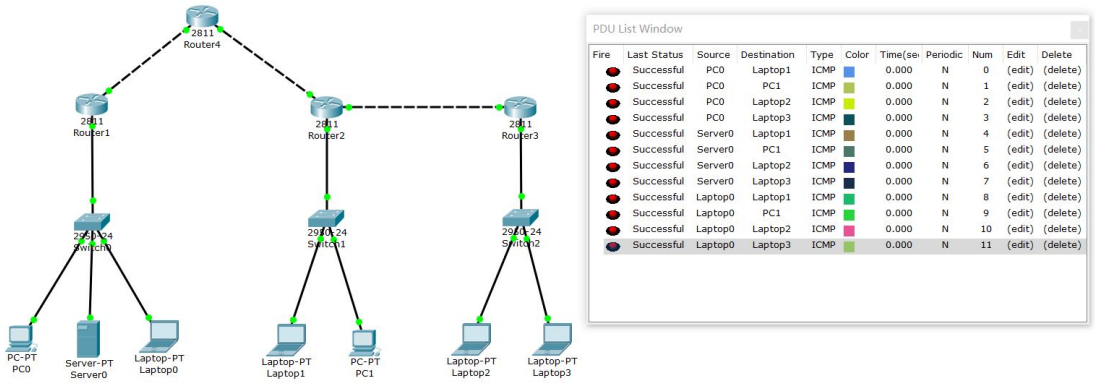


图 7: VPN 测试结果

为了判断传输模式还是隧道模式，这里从 PC0 发一个 ICMP 包到 Laptop1，利用抓包功能抓取 Router1 处的包，如 Figure 8所示。

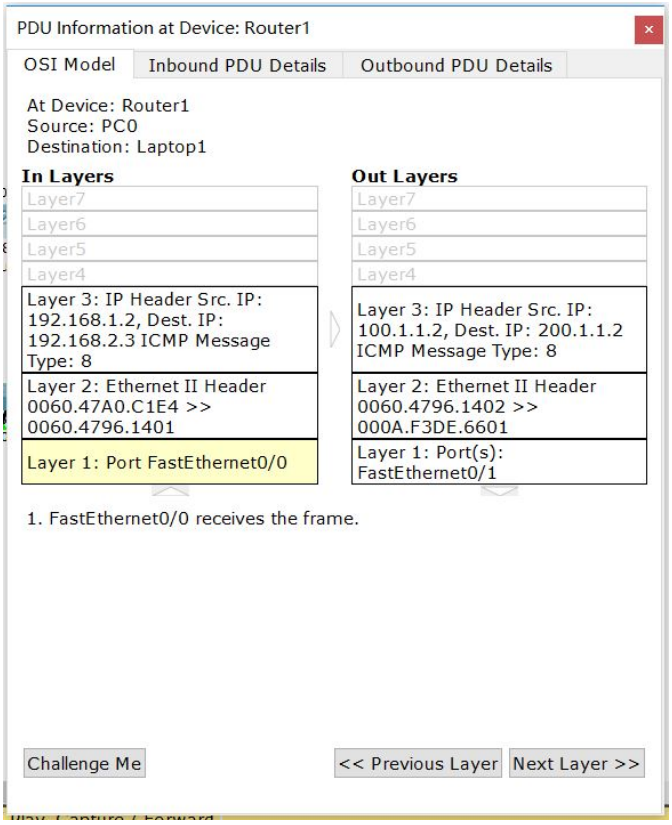
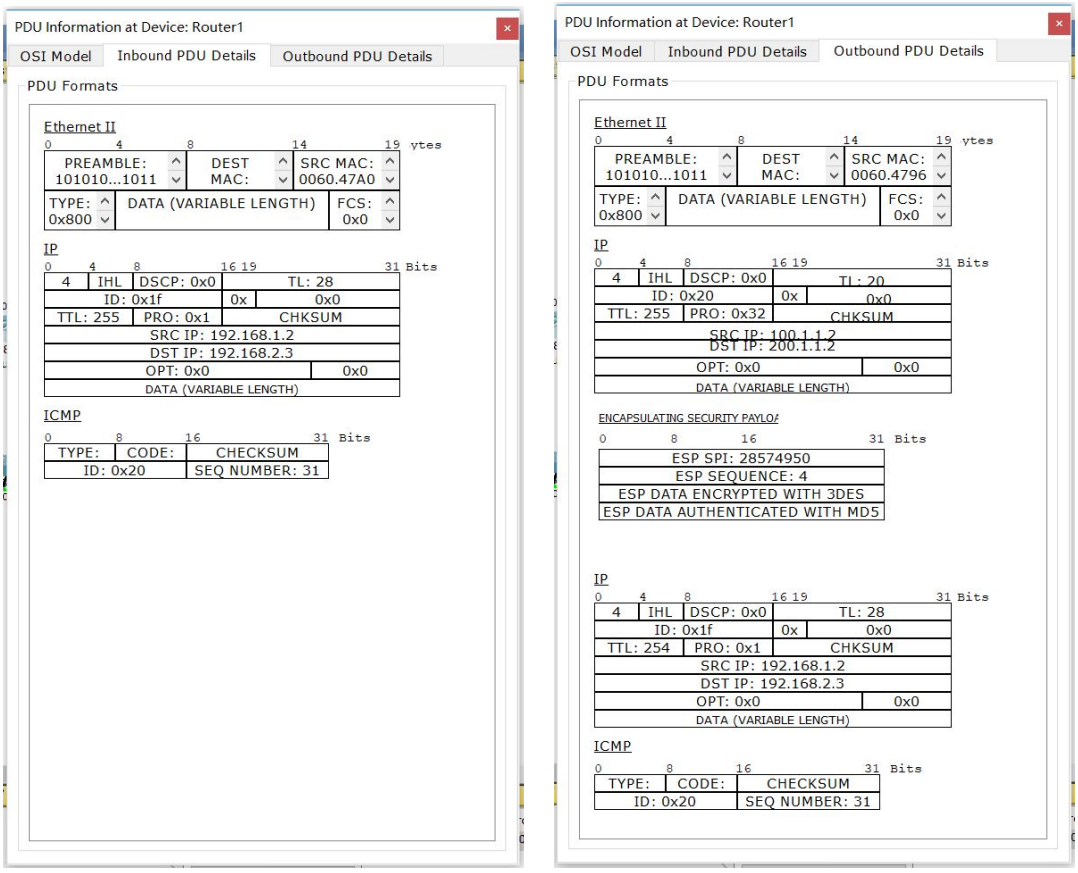


图 8: Router1 处的 ICMP 包

可见 ip 报头的源地址和目标地址均从内网 ip 被修改为边界路由器的出口 ip，进一步分析 Inbound 和 Outbound 的包结构，如 Figure 9 所示。



(a) Inbound (b) Outbound

图 9: Router1 处 In/Out 方向的 ICMP 包

可以看出 Outbound 的包在 Inbound 的 ip 报头前面增加了 ESP 头和新的 ip 报头，因此可以断定该 VPN 使用了隧道模式。

4 Bonus 任务

我选择的 bonus 任务是网络地址转换，包括静态 NAT，动态 NAT 和 NAPT 的配置。

网络拓扑如 Figure 10 所示，左边模拟一个公司内网，右边模拟公网路由器，以及一个公网上的服务器。现在需要使公司内网设备能够访问外网，即能够与 Server0 通信。

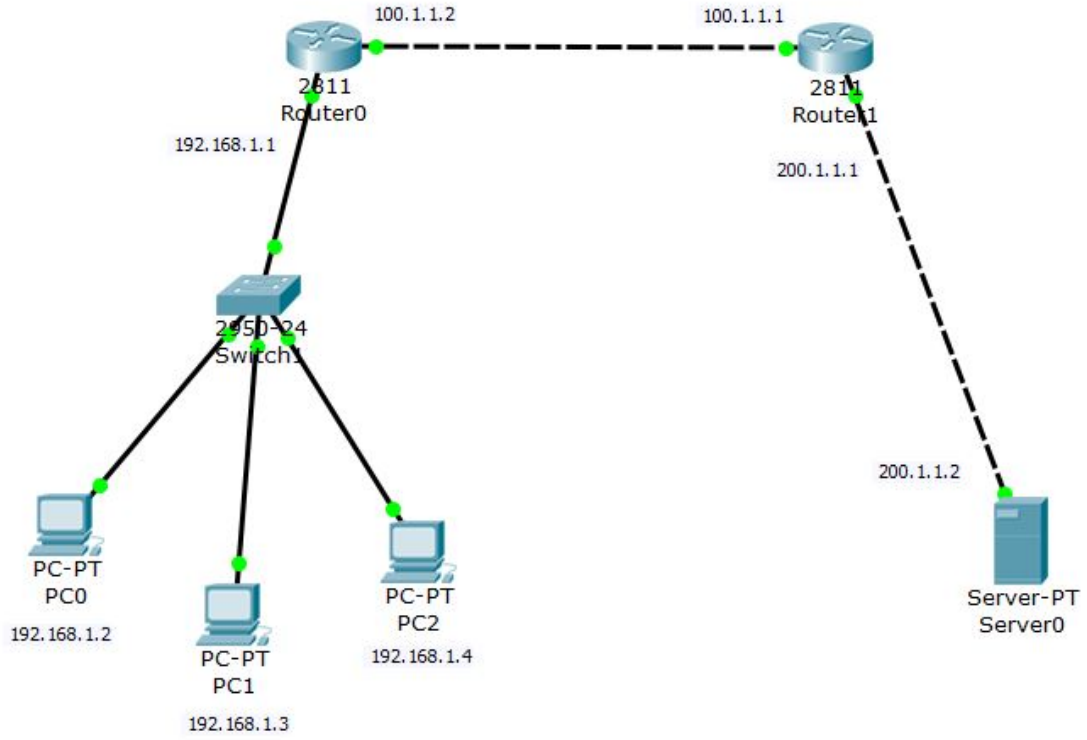


图 10: 网络拓扑

首先配置 Router0 的默认路由为 100.1.1.1，配置 Router1 的默认路由为 100.1.1.2，配置好后 PC0/1/2 不能 ping 通 Server0，因为它们没有公网 ip。

4.1 静态 NAT

接下来在 Router0 上配置静态 NAT，配置 192.168.1.0/24 为 inside，配置 100.1.1.0/24 为 outside，为 PC0/1/2 分别分配公网 ip。

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

Router(config)#interface FastEthernet 0/1
Router(config-if)#ip nat outside
Router(config-if)#exit

Router(config)#ip nat inside source static 192.168.1.2 100.1.1.12
Router(config)#ip nat inside source static 192.168.1.3 100.1.1.13
Router(config)#ip nat inside source static 192.168.1.4 100.1.1.14
```

然后从 PC0/1/2 ping Server0，结果如 Figure 11 所示。

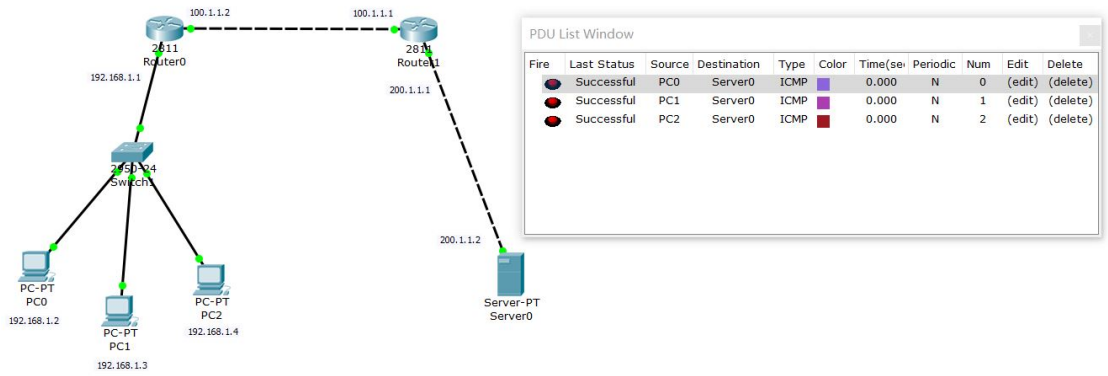


图 11: 静态 NAT 测试结果

4.2 动态 NAT

静态 NAT 只适用于公网 ip 充足的情况下，现在假设公司只申请到两个公网 ip：100.1.1.11 和 100.1.1.12，需要支持两台设备同时上网，此时需要配置动态 NAT。

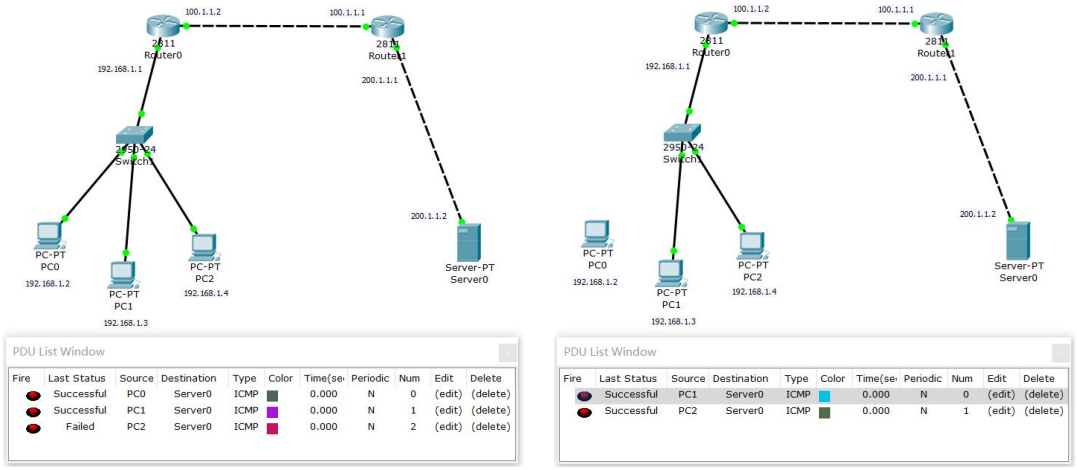
首先在 Router0 上清除静态 NAT

```
Router(config)#no ip nat inside source static 192.168.1.2 100.1.1.12
Router(config)#no ip nat inside source static 192.168.1.3 100.1.1.13
Router(config)#no ip nat inside source static 192.168.1.4 100.1.1.14
```

定义公网地址池，允许从 100.1.1.11 到 100.1.1.12 的公网 ip，定义 ACL 允许内网 ip 出路由器，并将 ACL 绑定到公网地址池。

```
Router(config)#ip nat pool ljhpool 100.1.1.11 100.1.1.12 netmask
    255.255.255.0
Router(config)#access-list 10 permit 192.168.1.0 0.0.0.255
Router(config)#ip nat inside source list 10 pool ljhpool
```

配置完成后，测试结果如 Figure 12所示。首先连上三台设备，发现仅有 PC0 和 PC1 能够 ping 通 Server0，然后将 PC0 的网线断开，再次测试，发现 PC1 和 PC2 均能 ping 通 Server0，测试结果符合预期。



(a) 三台设备同时联网　　(b) 两台设备同时联网

图 12: 动态 NAT 测试结果

4.3 NAPT

为了使公司内网设备能够同时上网，需要配置 NAPT，利用多路复用技术达到要求。现在假设公司只申请到 100.1.1.11 这一个公网 ip，在 Router0 上配置

```
Router(config)#access-list 10 permit 192.168.1.0 0.0.0.255
Router(config)#ip nat pool ljhpool 100.1.1.11 100.1.1.11 netmask
    255.255.255.0
Router(config)#ip nat inside source list 10 pool ljhpool overload
```

测试结果如 Figure 13 所示。

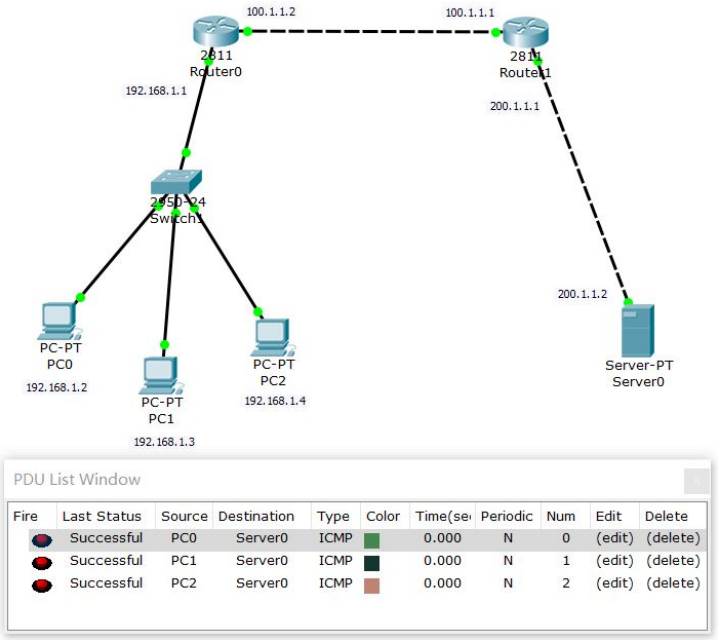


图 13: NAPT 测试结果

在 PC0 和 PC1 上同时通过 http 访问 Server0，如 Figure 14 所示。

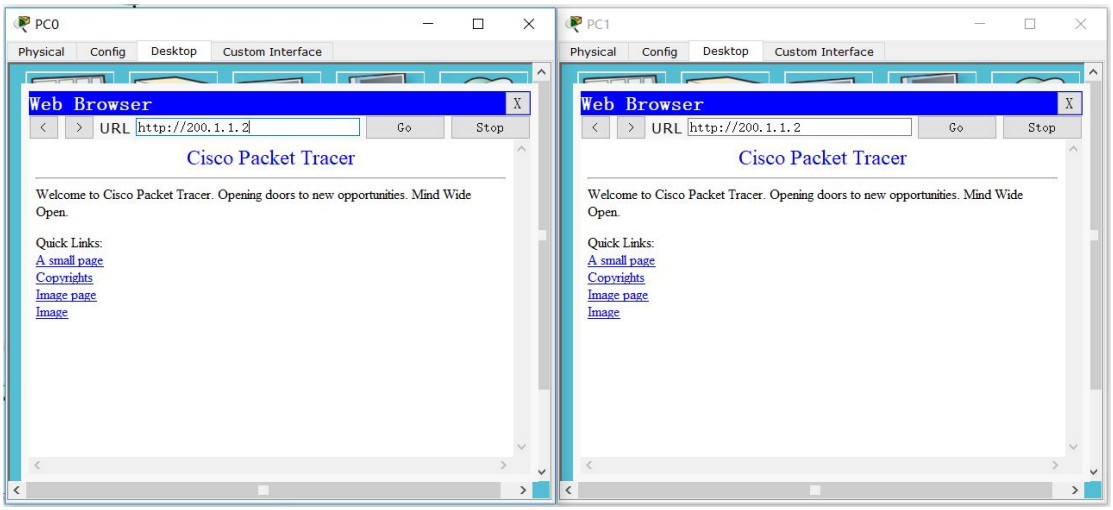


图 14: PC0/1 通过 http 访问 Server0

在 Router0 执行`show ip nat translations`查看 NAT 转换表，如 Figure 15 所示。

```
Router#show ip nat translations
Pro  Inside global     Inside local       Outside local      Outside global
tcp 100.1.1.11:1028    192.168.1.3:1028   200.1.1.2:80       200.1.1.2:80
tcp 100.1.1.11:1032    192.168.1.2:1032   200.1.1.2:80       200.1.1.2:80

Router#
```

图 15: NAT 转换表

可以看到不同内网 ip 被映射到同一公网 ip 的不同端口，说明 NAPT 配置成功。