**《网络工程与组网技术》**

**课程实验报告**

（2022学年）

实验名称 IPSEC VPN配置

学 院

专业班级

学号姓名

2021年 8月25日

1. **实验说明**
2. 网络拓扑
3. 实验任务
4. IP配置

按照拓扑中IP标记配置IP，主机网关自定义。R1、R3、R4连接R2的IP地址设置成本段可用IP地址的第二位。

**R1配置：**

Router>en

Router#conf t

Router(config)#hostname R1

R1(config)#interface GigabitEthernet0/0/0 // 连接R2-ISP

R1(config-if)#no sh

R1(config-if)#ip addr 58.212.208.2 255.255.255.0

R1(config-if)#e

R1(config)#interface GigabitEthernet0/0/1 // 连接SW1

R1(config-if)#no sh

R1(config-if)#ip addr 192.168.0.1 255.255.255.252

R1(config-if)#e

R1(config)#ip route 192.168.1.0 255.255.255.0 192.168.0.2 // 路由转发：SERVER网段

R1(config)#ip route 192.168.2.0 255.255.255.0 192.168.0.2 // 路由转发：PC1网段

R1(config)#ip route 0.0.0.0 0.0.0.0 58.212.208.1 // 默认路由R2-ISP

**R2-ISP配置：**

R2-ISP>en

R2-ISP#conf t

R2-ISP(config)#interface GigabitEthernet0/0 // 连接R1

R2-ISP(config-if)#no sh

R2-ISP(config-if)#ip addr 58.212.208.1 255.255.255.0

R2-ISP(config-if)#e

R2-ISP(config)#interface GigabitEthernet0/1 // 连接R3

R2-ISP(config-if)#no sh

R2-ISP(config-if)#ip addr 58.32.166.1 255.255.255.0

R2-ISP(config-if)#e

R2-ISP(config)#interface GigabitEthernet0/2 // 连接R4

R2-ISP(config-if)#no sh

R2-ISP(config-if)#ip addr 222.94.88.1 255.255.255.0

R2-ISP(config-if)#e

R2-ISP(config)#ip route 192.168.0.0 255.255.255.252 58.212.208.2

R2-ISP(config)#ip route 192.168.1.0 255.255.255.0 58.212.208.2

R2-ISP(config)#ip route 192.168.2.0 255.255.255.0 58.212.208.2

R2-ISP(config)#ip route 192.168.0.4 255.255.255.252 58.32.166.2

R2-ISP(config)#ip route 192.168.4.0 255.255.255.0 58.32.166.2

R2-ISP(config)#ip route 192.168.5.0 255.255.255.0 58.32.166.2

R2-ISP(config)#ip route 192.168.3.0 255.255.255.0 222.94.88.2

**R3配置：**

Router>en

Router#conf t

Router(config)#hostname R3

R3(config)#interface GigabitEthernet0/0/0 // 连接R2-ISP

R3(config-if)#no sh

R3(config-if)#ip addr 58.32.166.2 255.255.255.0

R3(config-if)#e

R3(config)#interface GigabitEthernet0/0/1 // 连接SW2

R3(config-if)#no sh

R3(config-if)#ip addr 192.168.0.5 255.255.255.252

R3(config-if)#e

R3(config)#ip route 192.168.4.0 255.255.255.0 192.168.0.6 // 路由转发：PC2网段

R3(config)#ip route 192.168.5.0 255.255.255.0 192.168.0.6 // 路由转发：PC3网段

R3(config)#ip route 0.0.0.0 0.0.0.0 58.32.166.1 // 默认路由R2-ISP

**R4配置：**

Router>en

Router#conf t

Router(config)#hostname R4

R4(config)#interface GigabitEthernet0/0/0 // 连接R2-ISP

R4(config-if)#no sh

R4(config-if)#ip addr 222.94.88.2 255.255.255.0

R4(config-if)#e

R4(config)#interface GigabitEthernet0/0/1 // 连接PC4

R4(config-if)#no sh

R4(config-if)#ip addr 192.168.3.2 255.255.255.0

R4(config-if)#e

R4(config)#ip route 0.0.0.0 0.0.0.0 222.94.88.1 // 默认路由R2-ISP

**SW1配置：**

Switch>en

Switch#conf t

Switch(config)#hostname SW1

SW1(config)#vlan 10 // 连接SERVER

SW1(config-vlan)#name SEVER

SW1(config-vlan)#e

SW1(config)#int vlan 10

SW1(config-if)#ip addr 192.168.1.2 255.255.255.0

SW1(config-if)#no sh

SW1(config-if)#e

SW1(config)#vlan 20 // 连接PC1

SW1(config-vlan)#name PC1

SW1(config-vlan)#e

SW1(config)#int vlan 20

SW1(config-if)#ip addr 192.168.2.2 255.255.255.0

SW1(config-if)#no sh

SW1(config-if)#e

SW1(config)#vlan 30 // 连接R1

SW1(config-vlan)#name R1

SW1(config-vlan)#e

SW1(config)#int vlan 30

SW1(config-if)#ip addr 192.168.0.2 255.255.255.252

SW1(config-if)#no sh

SW1(config-if)#e

SW1(config)#interface GigabitEthernet1/0/1 // 连接SERVER

SW1(config-if)#no sh

SW1(config-if)#switchport access vlan 10

SW1(config-if)#e

SW1(config)#interface GigabitEthernet1/0/2 // 连接PC1

SW1(config-if)#no sh

SW1(config-if)#switchport access vlan 20

SW1(config-if)#e

SW1(config)#interface GigabitEthernet1/0/24 // 连接R2

SW1(config-if)#no sh

SW1(config-if)#switchport access vlan 30

SW1(config-if)#e

SW1(config)#ip route 0.0.0.0 0.0.0.0 192.168.0.1 // 默认路由R1

**SW2配置：**

Switch>en

Switch#conf t

Switch(config)#hostname SW2

SW2(config)#vlan 40 // 连接PC2

SW2(config-vlan)#name PC2

SW2(config-vlan)#e

SW2(config)#int vlan 40

SW2(config-if)#ip addr 192.168.4.2 255.255.255.0

SW2(config-if)#no sh

SW2(config-if)#e

SW2(config)#vlan 50 // 连接PC3

SW2(config-vlan)#name PC3

SW2(config-vlan)#e

SW2(config)#int vlan 50

SW2(config-if)#ip addr 192.168.5.2 255.255.255.0

SW2(config-if)#no sh

SW2(config-if)#e

SW2(config)#vlan 60 // 连接R3

SW2(config-vlan)#name R3

SW2(config-vlan)#e

SW2(config)#int vlan 60

SW2(config-if)#ip addr 192.168.0.6 255.255.255.252

SW2(config-if)#no sh

SW2(config-if)#e

SW2(config)#interface GigabitEthernet1/0/1 // 连接PC2

SW2(config-if)#no sh

SW2(config-if)#switchport access vlan 40

SW2(config-if)#e

SW2(config)#interface GigabitEthernet1/0/2 // 连接PC3

SW2(config-if)#no sh

SW2(config-if)#switchport access vlan 50

SW2(config-if)#e

SW2(config)#interface GigabitEthernet1/0/24 // 连接R3

SW2(config-if)#no sh

SW2(config-if)#switchport access vlan 60

SW2(config-if)#e

SW2(config)#ip route 0.0.0.0 0.0.0.0 192.168.0.5 // 默认路由R3

**PC1配置：**

IP地址：192.168.2.1/24，网关：192.168.2.2

**PC2配置：**

IP地址：192.168.4.1/24，网关：192.168.4.2

**PC3配置：**

IP地址：192.168.5.1/24，网关：192.168.5.2

**PC4配置：**

IP地址：192.168.3.1/24，网关：192.168.3.2

**SERVER配置：**

IP地址：192.168.1.1/24，网关：192.168.1.2

1. IPSEC VPN

由于中间R2设备为运营商设备无法控制，每个部门之间需要建立一条VPN隧道传输内部数据，并且要保证数据安全，所以需要在每个部门之间建立一条IPSEC VPN，具体参数要求如下: 隧道使用预共享秘钥进行身份验证s

* AES-256加密方式
* HASH算法为SHA
* 预共享密钥分别为
* 总部到上海分部：hq-to-sha
* 总部到南京分部：hq-to-nkg
* 南京分部到上海分部：nkg-to-sha
* 密钥位数group2

**R1配置：**

R1(config)#crypto isakmp policy 1 // 配置密码ISAKMP策略1

R1(config-isakmp)#encryption aes 256 // 指定加密方式为AES-256

R1(config-isakmp)#hash sha // 指定哈希算法为SHA

R1(config-isakmp)#authentication pre-share // 采用预共享密钥的方式

R1(config-isakmp)#group 2 // 配置密钥位数为group2（1024）

R1(config-isakmp)#exit

R1(config)#crypto isakmp key hq-to-sha address 58.32.166.2 // 配置总部到上海分部：预共享密钥为hq-to-sha，远程对等体ip地址为58.32.166.2

R1(config)#crypto isakmp key hq-to-nkg address 222.94.88.2 // 配置总部到南京分部：预共享密钥为hq-to-nkg，远程对等体ip地址为222.94.88.2

R1(config)#crypto ipsec transform-set R1 esp-aes 256 esp-sha-hmac // 配置IPSEC策略，名称R1，esp做封装，aes-256做加密，esp做封装，sha做哈希

R1(config)#access-list 100 permit ip any any

R1(config)#crypto map R1-map 1 ipsec-isakmp // 对策略做汇总，定义了一个加密图R1-map，优先级为1

R1(config-crypto-map)#match add 100

R1(config-crypto-map)#set transform-set R1 // 调用R1策略

R1(config-crypto-map)#set peer 58.32.166.2 // 配置对等体为R3

R1(config-crypto-map)#crypto map R1-map 2 ipsec-isakmp // 优先级为2

R1(config-crypto-map)#match add 100

R1(config-crypto-map)#set transform-set R1 // 调用R1策略

R1(config-crypto-map)#set peer 222.94.88.2 // 配置对等体为R4

R1(config-crypto-map)#e

R1(config)#interface GigabitEthernet0/0/0 // 连接R2-ISP

R1(config-if)#crypto map R1-map // 将R1-map配置到端口上

R1(config-if)#e

**R3配置：**

R3(config)#crypto isakmp policy 1 // 同上

R3(config-isakmp)#encryption aes 256

R3(config-isakmp)#hash sha

R3(config-isakmp)#authentication pre-share

R3(config-isakmp)#group 2

R3(config-isakmp)#exit

R3(config)#crypto isakmp key hq-to-sha address 58.212.208.2 // 总部到上海分部

R3(config)#crypto isakmp key nkg-to-sha address 222.94.88.2 // 南京分部到上海分部

R3(config)#crypto ipsec transform-set R3 esp-aes 256 esp-sha-hmac

R3(config)#access-list 100 permit ip any any

R3(config)#crypto map R3-map 1 ipsec-isakmp

R3(config-crypto-map)#match add 100

R3(config-crypto-map)#set transform-set R3

R3(config-crypto-map)#set peer 58.212.208.2 // 对等体为R1

R3(config-crypto-map)#crypto map R3-map 2 ipsec-isakmp

R3(config-crypto-map)#match add 100

R3(config-crypto-map)#set transform-set R3

R3(config-crypto-map)#set peer 222.94.88.2 // 对等体为R4

R3(config-crypto-map)#e

R3(config)#interface GigabitEthernet0/0/0 // 连接R2-ISP

R3(config-if)#crypto map R3-map

R3(config-if)#e

**R4配置：**

R4(config)#crypto isakmp policy 1 // 同上

R4(config-isakmp)#encryption aes 256

R4(config-isakmp)#hash sha

R4(config-isakmp)#authentication pre-share

R4(config-isakmp)#group 2

R4(config-isakmp)#exit

R4(config)#crypto isakmp key hq-to-nkg address 58.212.208.2 // 总部到南京分部

R4(config)#crypto isakmp key nkg-to-sha address 58.32.166.2 // 南京分部到上海分部

R4(config)#crypto ipsec transform-set R4 esp-aes 256 esp-sha-hmac

R4(config)#access-list 100 permit ip any any

R4(config)#crypto map R4-map 1 ipsec-isakmp

R4(config-crypto-map)#match add 100

R4(config-crypto-map)#set transform-set R4

R4(config-crypto-map)#set peer 58.212.208.2 // 对等体为R1

R4(config-crypto-map)#crypto map R4-map 2 ipsec-isakmp

R4(config-crypto-map)#match add 100

R4(config-crypto-map)#set transform-set R4

R4(config-crypto-map)#set peer 58.32.166.2 // 对等体为R3

R4(config-crypto-map)#e

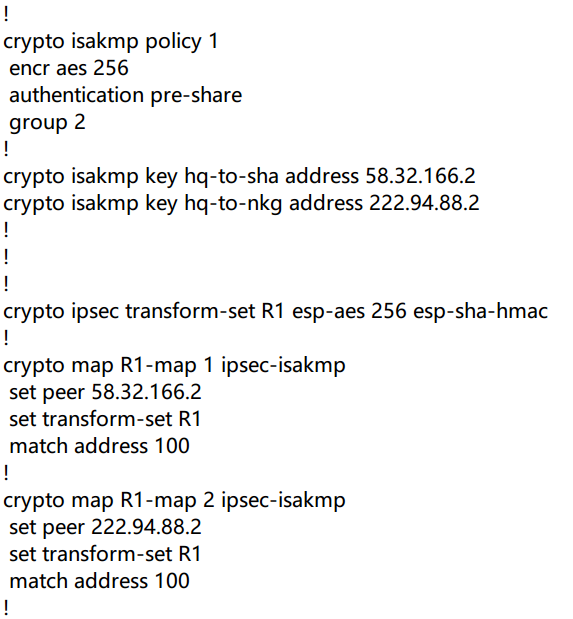
R4(config)#interface GigabitEthernet0/0/0 // 连接R2-ISP

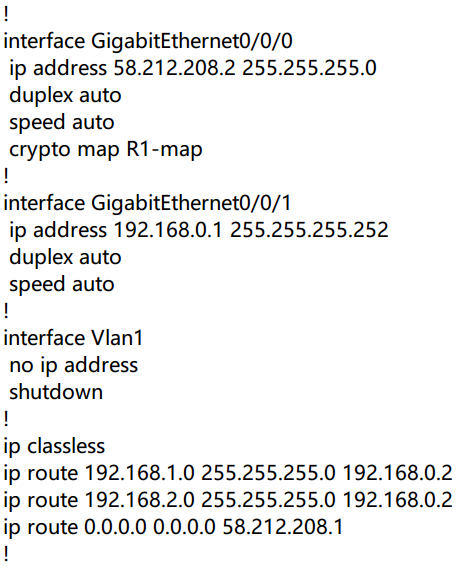
R4(config-if)#crypto map R4-map

R4(config-if)#e

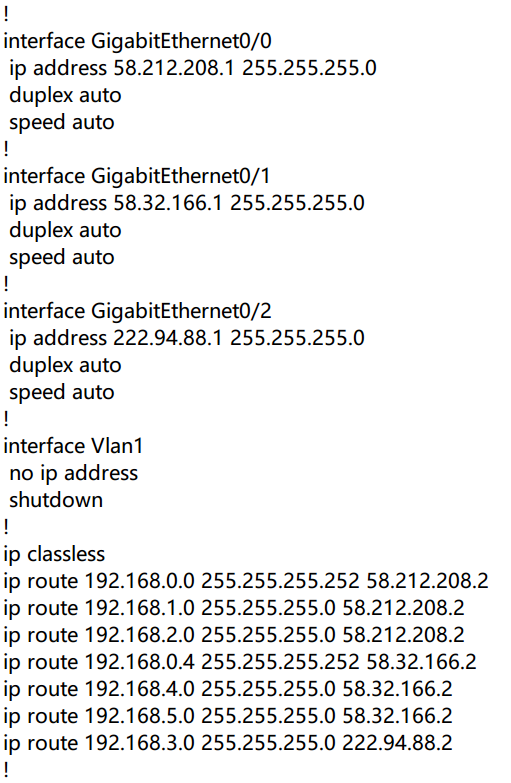
1. **网络节点配置**

* **R1部分配置文件信息：**

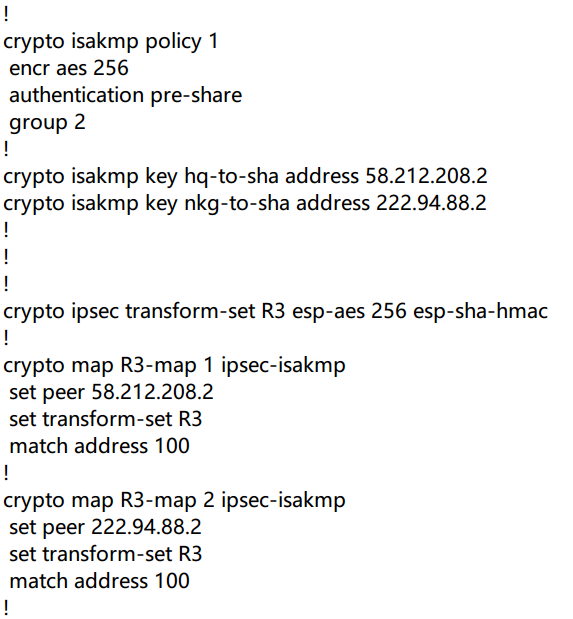


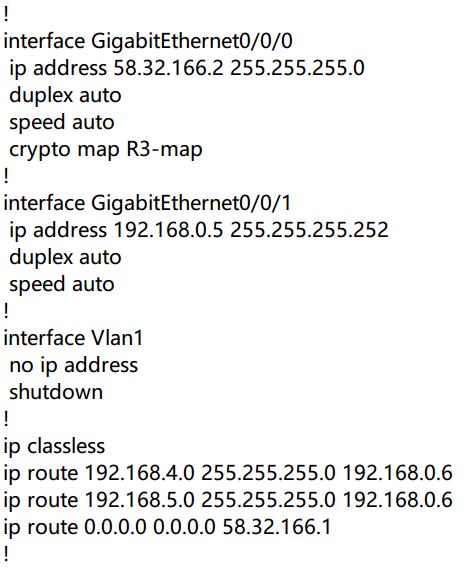


* **R2-ISP部分配置文件信息：**

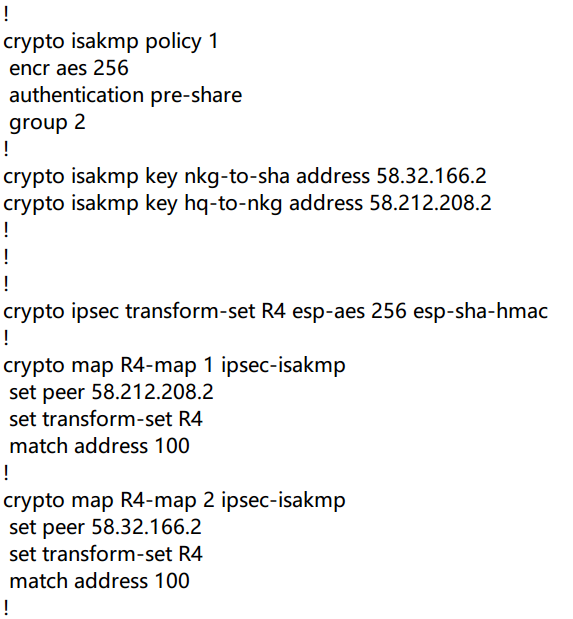


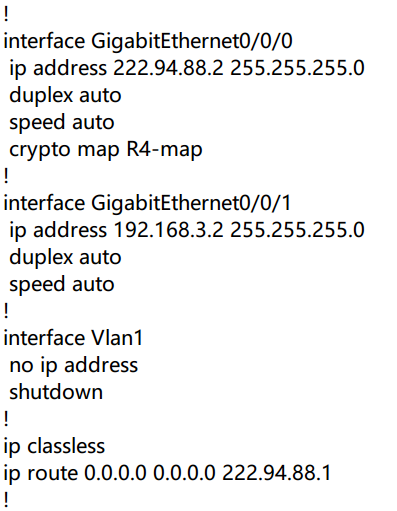
* **R3部分配置文件信息：**





* **R4部分配置文件信息：**



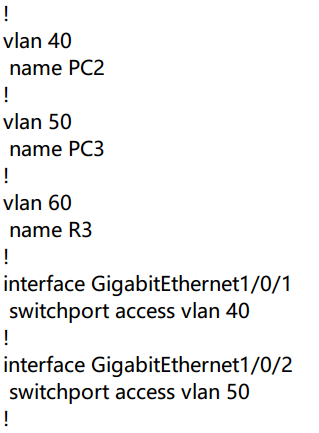


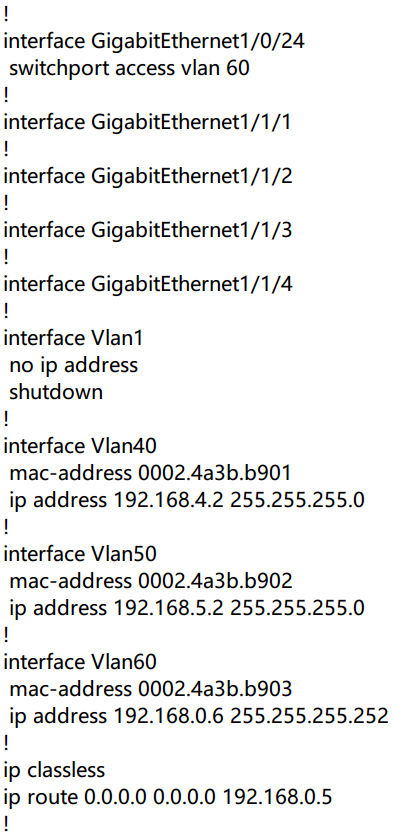
* **SW1部分配置文件信息：**





* **SW2部分配置文件信息：**





1. **功能测试**

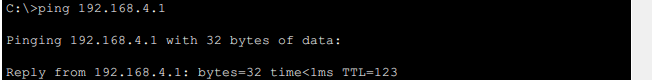
测试总部与南京分部和上海分部之间的互通性。

注：ping前和ping后在R1或R4上输入show crypto ipsec sa命令查看输出中的#pkts encrypt和#pkts decrypt值是否增加，如增加就表示已经成功加密了。

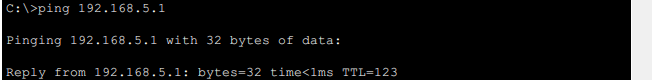
**测试连通性：**

**总部->上海分部：**

PC1->PC2:

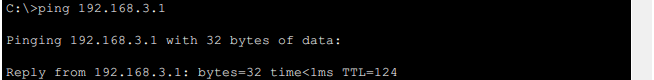


PC1->PC3:



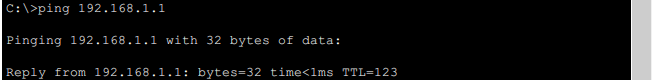
**总部->南京分部：**

PC1->PC4:

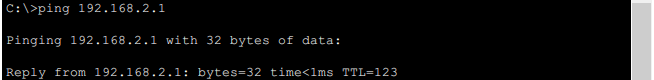


**上海分部->总部：**

PC2->SERVER:

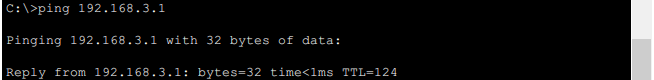


PC2->PC1:



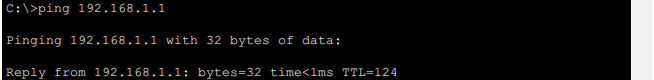
**上海分部->南京分部：**

PC2->PC4:

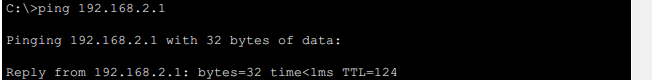


**南京分部->总部：**

PC4->SERVER:

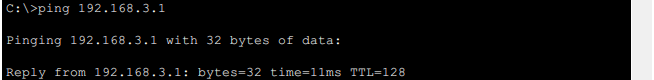


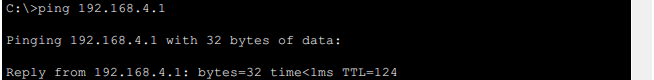
PC4->PC1:



**南京分部->上海分部：**

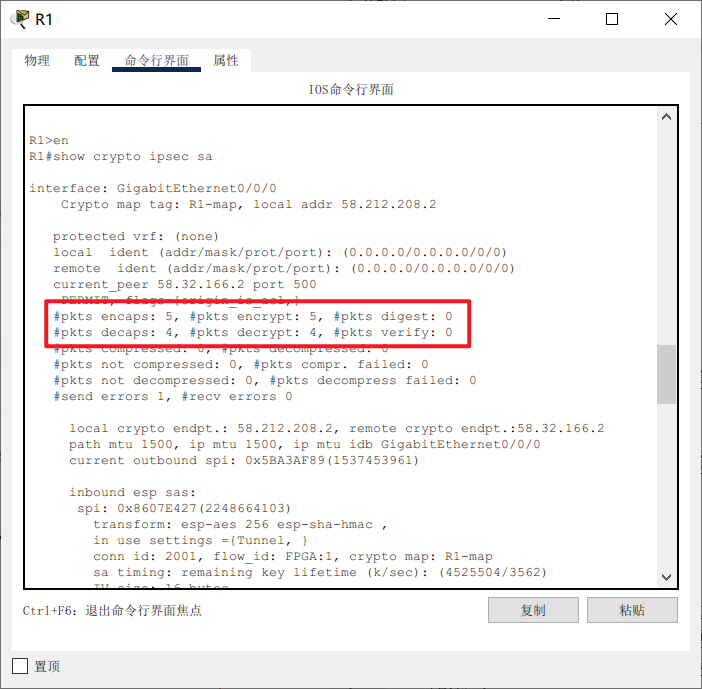
PC4->PC2:



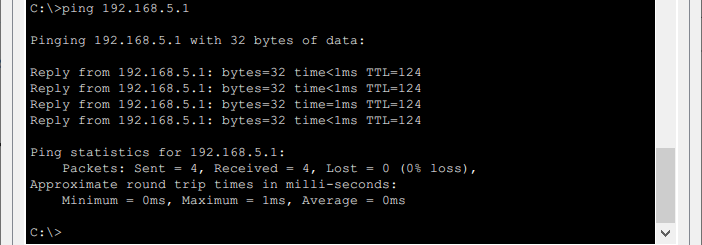
PC4->PC3:

**测试总部与上海分部之间IPSEC VPN功能：**

总部PC1 ping上海分部PC3前，在R1上输入show crypto ipsec sa，结果如下所示：

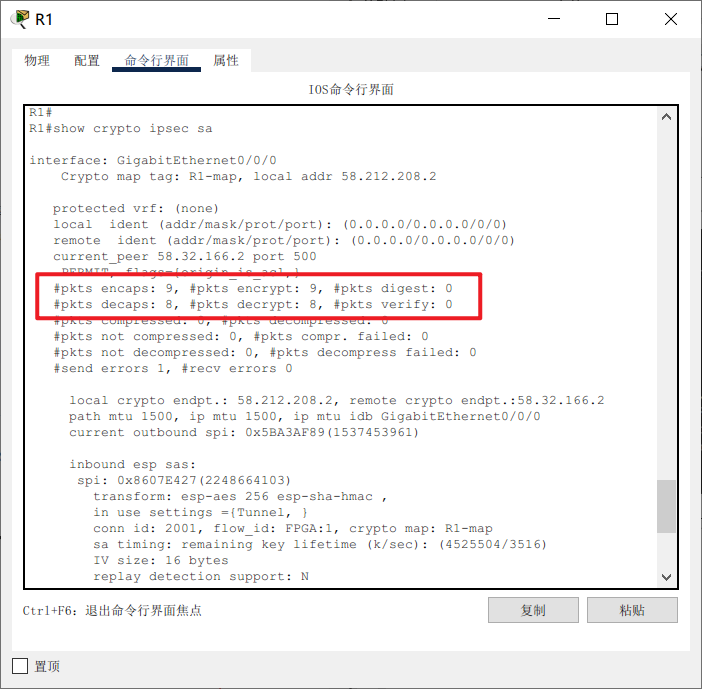


在总部PC1上ping 192.168.5.1（上海分部PC3）：



可以看到两个主机一共进行了4次会话。

之后再在R1上输入show crypto ipsec sa，结果如下：



与前面相比，pkts encrypt和pkts decrypt分别从5、4增加到了9、8，正好是对应着前面的4个ping命令。