




# Network Security

## Homework 1

Boya Zhang

February 10, 2021

Engineering Science

# 1 Setup

## 1.1 Topology

- Router: 3 routers connected as the topology in Fig.1
- Interface: Router1 F0/0, Router 2 F0/0, Router 2 F0/1, Router 3 F0/0
- Subnet: 10.0.1.0/24, 172.16.1.0/24

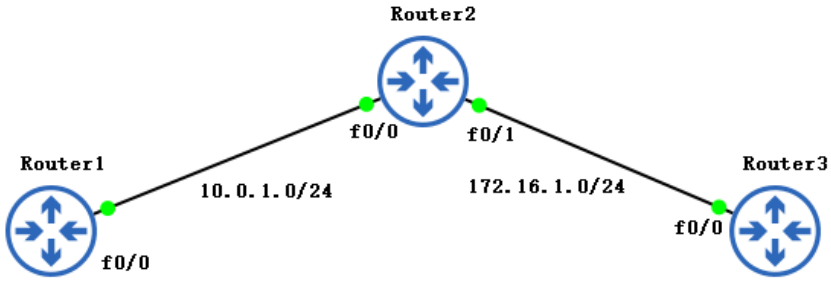


Figure 1: Topology

## 1.2 Configuration

We configure 4 interfaces through the CISCO commands.

- Router 1 F0/0 on 10.0.1.1/24, Router 2 F0/0 on 10.0.1.2/24
- Router 2 F0/1 on 172.16.1.1/24, Router 3 F0/0 on 172.16.1.2/24

The result is shown in Fig.2.

```
!
interface FastEthernet0/0
 ip address 10.0.1.1 255.255.255.0
 duplex auto
 speed auto
!
interface FastEthernet0/1
 no ip address
 shutdown
 duplex auto
 speed auto
!
interface FastEthernet1/0
!
interface FastEthernet1/1
!
```

(a) Router1

```
!
interface FastEthernet0/0
 ip address 10.0.1.2 255.255.255.0
 duplex auto
 speed auto
!
interface FastEthernet0/1
 ip address 172.16.1.1 255.255.255.0
 duplex auto
 speed auto
!
interface FastEthernet1/0
!
interface FastEthernet1/1
!
```

(b) Router2

```
interface FastEthernet0/0
 ip address 172.16.1.2 255.255.255.0
 duplex auto
 speed auto
!
interface FastEthernet0/1
 no ip address
 shutdown
 duplex auto
 speed auto
!
interface FastEthernet1/0
!
interface FastEthernet1/1
!
```

(c) Router3

Figure 2: Configuration of each router

# 2 Mission 1: RIPv2

We first configure dynamic routing on each router as shown in Fig.4. And when all routes are propagated, we use Wireshark to see the result. As shown in Fig.3 No.6 the source is 10.0.1.2 which represents interface R2 F0/0, the destination is 224.0.0.9 which represents the Routing Information Protocol (RIP) version 2 group address being used to send routing information to all RIP2-aware routers on the network segment. In the section Routing Information Protocol - IP address the value presented is 172.16.0.0/24, which is the subnet between R2 and R3. In this case we have only one subnet 172.16.1.0/24 from subnet 172.16.0.0/24 so we use the former one

to represent the link specifically. Therefore we have the packets sent in clear and unauthenticated among R1,R2 and R3 through the two subnets 10.0.1.0/24 and 172.16.1.0/24.

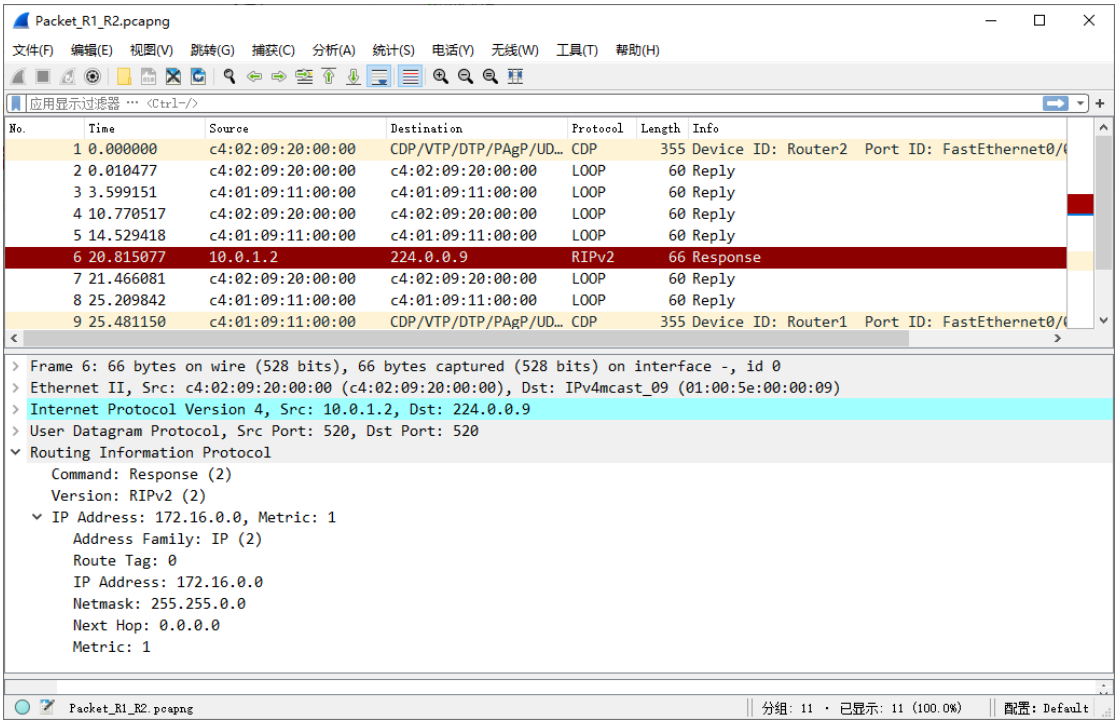


Figure 3: Packets on the link between R1 and R2 (RIPv2)

## 2.1 Code implementation

```
Router1#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Router1(config)#router rip
Router1(config-router)#version 2
Router1(config-router)#network 10.0.1.0
Router1(config-router)#exit
Router1(config)#exit
Router1#
*Mar  1 01:54:16.163: %SYS-5-CONFIG_I: Configured from console by console
Router1#sh ip rip database
10.0.0.0/8    auto-summary
10.0.1.0/24    directly connected, FastEthernet0/0
Router1#sh ip route
Codes: C - connected, S - static, 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
       i - IS-IS, su - IS-IS summary, 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, 1 subnets
C       10.0.1.0 is directly connected, FastEthernet0/0
```

(a) Router1

```
Router2#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Router2(config)#router rip
Router2(config-router)#version 2
Router2(config-router)#network 10.0.1.0
Router2(config-router)#exit
Router2(config)#exit
Router2#
*Mar  1 00:12:39.739: %SYS-5-CONFIG_I: Configured from console by console
Router2#sh ip rip database
10.0.0.0/8    auto-summary
10.0.1.0/24    directly connected, FastEthernet0/0
Router2#sh ip route
Codes: C - connected, S - static, 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
       i - IS-IS, su - IS-IS summary, 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

     172.16.0.0/24 is subnetted, 1 subnets
C       172.16.1.0 is directly connected, FastEthernet0/1
     10.0.0.0/24 is subnetted, 1 subnets
C       10.0.1.0 is directly connected, FastEthernet0/0
```

(b) Router2

```
Router2#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Router2(config)#router rip
Router2(config-router)#version 2
Router2(config-router)#network 172.16.1.0
Router2(config-router)#exit
Router2(config)#exit
Router2#
*Mar  1 00:41:46.619: %SYS-5-CONFIG_I: Configured from console by console
Router2#sh ip rip database
10.0.0.0/8    auto-summary
10.0.1.0/24    directly connected, FastEthernet0/0
172.16.0.0/16    auto-summary
172.16.1.0/24    directly connected, FastEthernet0/1
Router2#sh ip route
Codes: C - connected, S - static, 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
       i - IS-IS, su - IS-IS summary, 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

     172.16.0.0/24 is subnetted, 1 subnets
C       172.16.1.0 is directly connected, FastEthernet0/1
     10.0.0.0/24 is subnetted, 1 subnets
C       10.0.1.0 is directly connected, FastEthernet0/0
Router2#
```

(c) Router2

```
Router3#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Router3(config)#router rip
Router3(config-router)#version 2
Router3(config-router)#network 172.16.1.0
Router3(config-router)#exit
Router3(config)#exit
Router3#
*Mar  1 00:25:43.987: %SYS-5-CONFIG_I: Configured from console by console
Router3#sh ip rip database
172.16.0.0/16    auto-summary
172.16.1.0/24    directly connected, FastEthernet0/0
Router3#sh ip route
Codes: C - connected, S - static, 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
       i - IS-IS, su - IS-IS summary, 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

     172.16.0.0/24 is subnetted, 1 subnets
C       172.16.1.0 is directly connected, FastEthernet0/0
R    10.0.0.0/8 [120/1] via 172.16.1.1, 00:00:05, FastEthernet0/0
Router3#
```

(d) Router3

Figure 4: Configure dynamic routing on each router and validate

# 3 Mission 2 : authenticate RIP broadcast messages

The steps for authenticate RIP broadcast messages are:

1. Create a keychain to hold the key
2. Associate the keychain with an interface

The code implemented for R2 is shown in Fig.8. We first put the password on Router1 only. Because we didn't put the password on Router2, after a few minutes the RIP information is invalid. We perform the validation on Router1. The result is subnet disconnection as shown in Fig.5.

```
R    172.16.0.0/16 is possibly down, routing via 10.0.1.2, FastEthernet0/0
     10.0.0.0/24 is subnetted, 1 subnets
C       10.0.1.0 is directly connected, FastEthernet0/0
Router1#
```

Figure 5: Invalid RIP information

We then put the password both on Router1 and Router2. After a few seconds we perform the validation on Router2. The result is subnet reconnection as shown in Fig.6

```
     172.16.0.0/24 is subnetted, 1 subnets
C       172.16.1.0 is directly connected, FastEthernet0/1
     10.0.0.0/24 is subnetted, 1 subnets
C       10.0.1.0 is directly connected, FastEthernet0/0
Router2#
```

Figure 6: Valid RIP information

We use Wireshark to show the result as Fig.7. In the section Routing Information Protocol-Authentication, there is an authentication trailer with mode 5 of the password. Therefore the packets are sent in clear and authenticated.

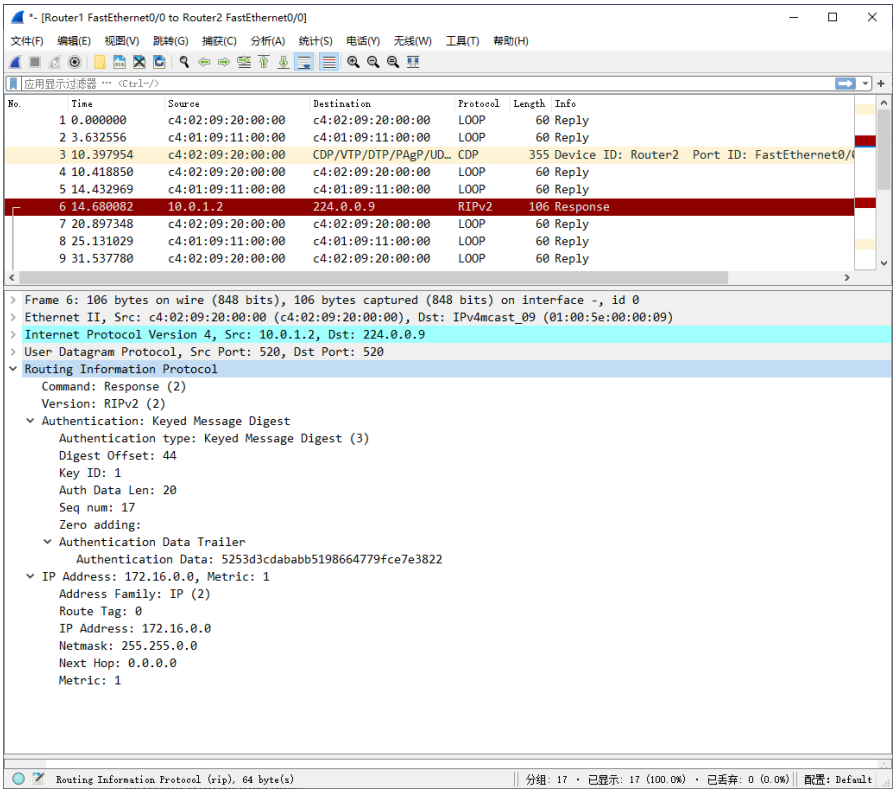


Figure 7: Packets on the link between R1 and R2 (Authenticated)

### 3.1 Code implementation

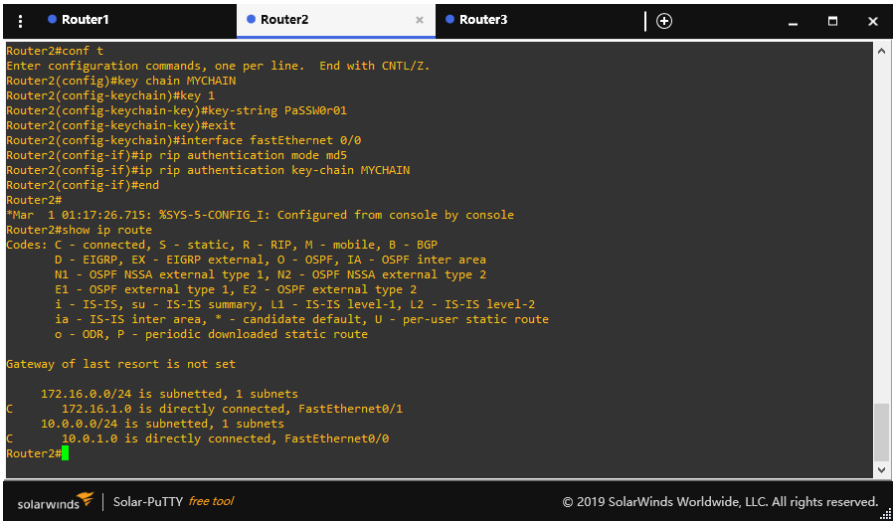


Figure 8: Authenticate RIP and validate on Router2

# 4 Conclusion

1. We have learnt basic CISCO commands including:
   (a) Interface configuration and validation
   (b) Dynamic routing configuration and validation
   (c) Authentication with keys in keychain
2. We need to wait for a few minutes before all routes are propagated in the following parts because the routers exchange information on a 30-seconds basis.
   (a) Protocol logging via wireshark in mission 1
   (b) Checking the invalid RIP information when the password not set on R2 in mission 2




# Network Security

## Homework 2: VLANs and Layer 2 security

Boya Zhang

February 10, 2021

Engineering Science

# 1 Topology

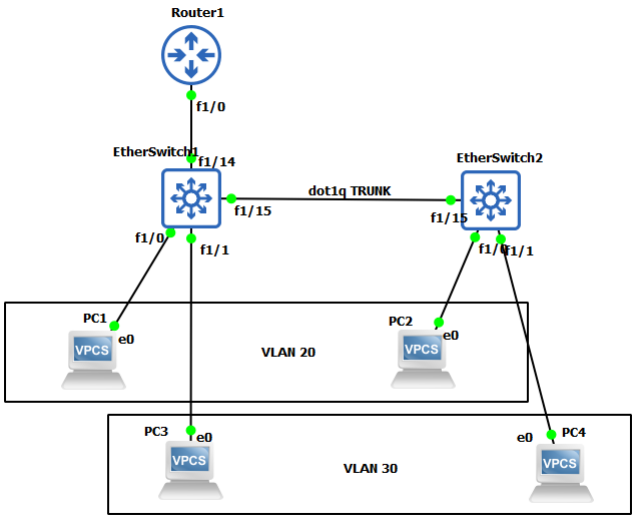


Figure 1: Topology

# 2 Mission 1: VLAN isolation and trunking

For mission 1 we adjust PC1 and PC3 mask to /16. In the beginning there are no VLANs, so PC1 and PC3 are able to ping to each other.(Fig.2)

```
PC1> ping 192.168.30.2
192.168.30.2 icmp_seq=1 timeout
84 bytes from 192.168.30.2 icmp_seq=2 ttl=63 time=19.595 ms
84 bytes from 192.168.30.2 icmp_seq=3 ttl=63 time=18.717 ms
84 bytes from 192.168.30.2 icmp_seq=4 ttl=63 time=17.071 ms
84 bytes from 192.168.30.2 icmp_seq=5 ttl=63 time=19.132 ms
```

Figure 2: PC1 ping to PC3(no VLAN)

Then the VLAN isolation is implemented. And interface VLAN20 is configured on port FastEthernet f1/0, VLAN30 is configured on f1/1.(Fig.4) The result is validated through a ping between PC1 and PC3.(Fig.3) They are not reachable anymore.

```
PC1> ping 192.168.30.2
host (192.168.20.1) not reachable
```

Figure 3: PC1 ping to PC3(VLAN)

```
EtherSwitch1#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
EtherSwitch1(config)#no ip routing
EtherSwitch1(config)#end
EtherSwitch1#
*Mar  1 00:11:32.247: %SYS-5-CONFIG_I: Configured from console by console
EtherSwitch1#vlan database
EtherSwitch1(vlan)#vlan 20
VLAN 20 modified:
EtherSwitch1(vlan)#vlan 30
VLAN 30 modified:
EtherSwitch1(vlan)#exit
APPLY completed.
Exiting....
EtherSwitch1#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
EtherSwitch1(config)#interface fastEthernet 1/0
EtherSwitch1(config-if)#switchport mode access
EtherSwitch1(config-if)#switchport access vlan 20
EtherSwitch1(config-if)#exit
EtherSwitch1(config)#interface fastEthernet 1/1
EtherSwitch1(config-if)#switchport mode access
EtherSwitch1(config-if)#switchport access vlan 30
EtherSwitch1(config-if)#exit
EtherSwitch1(config)#interface vlan 20
EtherSwitch1(config-if)#no shutdown
EtherSwitch1(config-if)#interface vlan 30
EtherSwitch1(config-if)#no shutdown
EtherSwitch1(config-if)#end
EtherSwitch1#
*Mar  1 00:13:57.283: %SYS-5-CONFIG_I: Configured from console by console
EtherSwitch1#show vlan-switch

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    Fa1/2, Fa1/3, Fa1/4, Fa1/5
                                                Fa1/6, Fa1/7, Fa1/8, Fa1/9
                                                Fa1/10, Fa1/11, Fa1/12, Fa1/13
20   VLAN0020                         active    Fa1/0
30   VLAN0030                         active    Fa1/1
1002 fddi-default                     active
1003 token-ring-default               active
1004 fddinet-default                  active
1005 trnet-default                    active

VLAN Type  SAID       MTU   Parent RingNo BridgeNo Stp  BrdgMode Trans1 Trans2
---- ----- ---------- ----- ------ ------ -------- ---- -------- ------ ------
1    enet  100001     1500  -      -      -        -    -        1002   1003
20   enet  100020     1500  -      -      -        -    -        0      0
30   enet  100030     1500  -      -      -        -    -        0      0
1002 fddi  101002     1500  -      -      -        -    -        1      1003
1003 tr    101003     1500  1005   0      -        -    srb      1      1002
1004 fdnet 101004     1500  -      -      1        ibm  -        0      0
1005 trnet 101005     1500  -      -      1        ibm  -        0      0
EtherSwitch1#write
Building configuration...
[OK]
EtherSwitch1#
```

Figure 4: CISCO EtherSwitch1

We make the same process for switch2. The results are same as the above. As shown in

Fig.5, we perform the VLAN isolation: VLAN20 is configured on f1/0, VLAN 30 is configured on f1/1. Fig.6 shows the connection when the is no VLANs.Fig.7 shows the disconnection when the VLAN isolation is implemented.

```
EtherSwitch2#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
EtherSwitch2(config)#no ip routing
EtherSwitch2(config)#end
EtherSwitch2#
*Mar  1 00:20:01.759: %SYS-5-CONFIG_I: Configured from console by console
EtherSwitch2#vlan database
EtherSwitch2(vlan)#vlan 20
VLAN 20 modified:
EtherSwitch2(vlan)#vlan 30
VLAN 30 modified:
EtherSwitch2(vlan)#exit
APPLY completed.
Exiting....
EtherSwitch2#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
EtherSwitch2(config)#interface fastEthernet 1/0
EtherSwitch2(config-if)#switchport mode access
EtherSwitch2(config-if)#switchport access vlan 20
EtherSwitch2(config-if)#exit
EtherSwitch2(config)#interface fastEthernet 1/1
EtherSwitch2(config-if)#switchport mode access
EtherSwitch2(config-if)#switchport access vlan 30
EtherSwitch2(config-if)#exit
EtherSwitch2(config)#interface vlan 20
EtherSwitch2(config-if)#no shutdown
EtherSwitch2(config-if)#interface vlan 30
EtherSwitch2(config-if)#no shutdown
EtherSwitch2(config-if)#end
EtherSwitch2#
*Mar  1 00:22:21.555: %SYS-5-CONFIG_I: Configured from console by console
EtherSwitch2#show vlan-switch

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    Fa1/2, Fa1/3, Fa1/4, Fa1/5
                                                Fa1/6, Fa1/7, Fa1/8, Fa1/9
                                                Fa1/10, Fa1/11, Fa1/12, Fa1/13
                                                Fa1/14
20   VLAN0020                         active    Fa1/0
30   VLAN0030                         active    Fa1/1
1002 fddi-default                     active
1003 token-ring-default               active
1004 fddinet-default                  active
1005 trnet-default                    active

VLAN Type  SAID       MTU   Parent RingNo BridgeNo Stp  BrdgMode Trans1 Trans2
---- ----- ---------- ----- ------ ------ -------- ---- -------- ------ ------
1    enet  100001     1500  -      -      -        -    -        1002   1003
20   enet  100020     1500  -      -      -        -    -        0      0
30   enet  100030     1500  -      -      -        -    -        0      0
1002 fddi  101002     1500  -      -      -        -    -        1      1003
1003 tr    101003     1500  1005   0      -        -    srb      1      1002
1004 fdnet 101004     1500  -      -      1        ibm  -        0      0
1005 trnet 101005     1500  -      -      1        ibm  -        0      0
EtherSwitch2#
```

Figure 5: CISCO EtherSwitch2

```
PC2> ping 192.168.30.3
192.168.30.3 icmp_seq=1 timeout
84 bytes from 192.168.30.3 icmp_seq=2 ttl=63 time=13.634 ms
84 bytes from 192.168.30.3 icmp_seq=3 ttl=63 time=20.104 ms
84 bytes from 192.168.30.3 icmp_seq=4 ttl=63 time=20.763 ms
84 bytes from 192.168.30.3 icmp_seq=5 ttl=63 time=16.199 ms

PC2>
```

Figure 6: PC2 ping to PC4(no VLAN)

```
PC2> ping 192.168.30.3
host (192.168.20.1) not reachable
```

Figure 7: PC2 ping to PC4(VLAN)

# 3 Mission 2: Trunking

We designate a port as a trunk between the two switches.

```
EtherSwitch1#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
EtherSwitch1(config)#interface fastEthernet 1/15
EtherSwitch1(config-if)#switchport mode trunk
EtherSwitch1(config-if)#switchport trunk allowed vlan all
EtherSwitch1(config-if)#no shutdown
EtherSwitch1(config-if)#exit
EtherSwitch1(config)#exit
EtherSwitch1#write
Building configuration...

*Mar  1 00:35:04.535: %SYS-5-CONFIG_I: Configured from console by console[OK]
EtherSwitch1#
```

Figure 8: Trunking implementation on switch1

```
EtherSwitch2#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
EtherSwitch2(config)#interface fastEthernet 1/15
EtherSwitch2(config-if)#switchport mode trunk
EtherSwitch2(config-if)#switchport trunk allowed vlan all
EtherSwitch2(config-if)#no shutdown
EtherSwitch2(config-if)#exit
EtherSwitch2(config)#exit
EtherSwitch2#wri
*Mar  1 00:42:28.667: %SYS-5-CONFIG_I: Configured from console by console
EtherSwitch2#write
Building configuration...
[OK]
EtherSwitch2#
```

Figure 9: Trunking implementation on switch2

The validation is to ping between PC1 and PC2.(Fig.10)PC1 and PC2 are connected through trunking.

```
PC1> ping 192.168.20.3
84 bytes from 192.168.20.3 icmp_seq=1 ttl=64 time=0.281 ms
84 bytes from 192.168.20.3 icmp_seq=2 ttl=64 time=0.969 ms
84 bytes from 192.168.20.3 icmp_seq=3 ttl=64 time=0.775 ms
84 bytes from 192.168.20.3 icmp_seq=4 ttl=64 time=0.485 ms
84 bytes from 192.168.20.3 icmp_seq=5 ttl=64 time=0.512 ms

PC1>
```

Figure 10: Trunking implementation on switch2

On Wireshark the traffic on the trunck line is analyzed.(Fig.11) The tag ID for ICMP echo ping packets is 20.

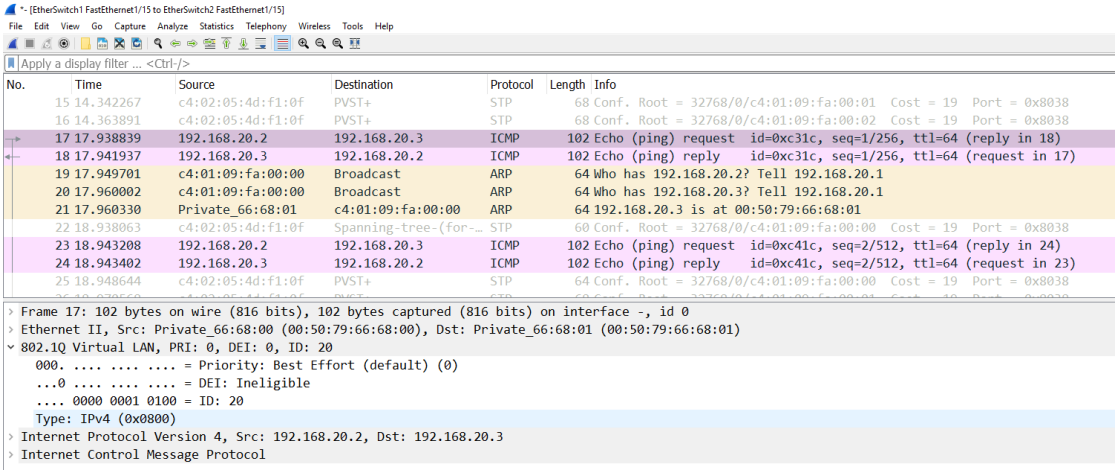


Figure 11: Capture on trunk line

# 4 Mission 3: inter-VLAN routing

We connect a router to the trunk lines of the switches and allow inter-vlan routing.(Fig.12)

```
Router1#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router1(config)#interface fastEthernet 1/0
Router1(config-if)#switchport mode trunk
Router1(config-if)#switchport trunk allowed vlan all
Router1(config-if)#no shutdown
Router1(config-if)#exit
Router1(config)#interface vlan 20
Router1(config-if)#ip address 192.168.20.1 255.255.255.0
Router1(config-if)#no shutdown
Router1(config-if)#exit
Router1(config)#interface vlan 30
Router1(config-if)#ip address 192.168.30.1 255.255.255.0
Router1(config-if)#no shutdown
Router1(config-if)#end
Router1#
*Mar  1 00:11:38.123: %SYS-5-CONFIG_I: Configured from console by console
Router1#write
Building configuration...
[OK]
Router1#
```

Figure 12: Capture on trunk line

To validate, we first ping between PC1 and the router interface. (Fig.13)They are connected.

```
PC1> ping 192.168.30.1
84 bytes from 192.168.30.1 icmp_seq=1 ttl=255 time=8.446 ms
84 bytes from 192.168.30.1 icmp_seq=2 ttl=255 time=4.085 ms
84 bytes from 192.168.30.1 icmp_seq=3 ttl=255 time=5.412 ms
84 bytes from 192.168.30.1 icmp_seq=4 ttl=255 time=8.922 ms
84 bytes from 192.168.30.1 icmp_seq=5 ttl=255 time=2.912 ms
```

Figure 13: Ping between the PC1 and the router interface

Then we ping from PC1 to PC3 and use wireshark to monitor the stick line.(Fig.14) PC1 and PC3 are connected.

```
PC1> ping 192.168.30.2
84 bytes from 192.168.30.2 icmp_seq=1 ttl=63 time=14.046 ms
84 bytes from 192.168.30.2 icmp_seq=2 ttl=63 time=13.856 ms
84 bytes from 192.168.30.2 icmp_seq=3 ttl=63 time=19.047 ms
84 bytes from 192.168.30.2 icmp_seq=4 ttl=63 time=12.483 ms
84 bytes from 192.168.30.2 icmp_seq=5 ttl=63 time=15.021 ms
```

Figure 14: Ping between the PC1 and the router interface

As shown in Fig.15 No.13, the packets are broadcasted from 192.168.20.2(PC1) through 192.168.20.1(router interface VLAN20). Then in No.23, the packets are broadcasted from 192.168.30.2(PC3) through 192.168.30.1(router interface VLAN30). So the packets movement is: PC1, router interface VLAN20, router interface VLAN30 , PC3. Vice versa.

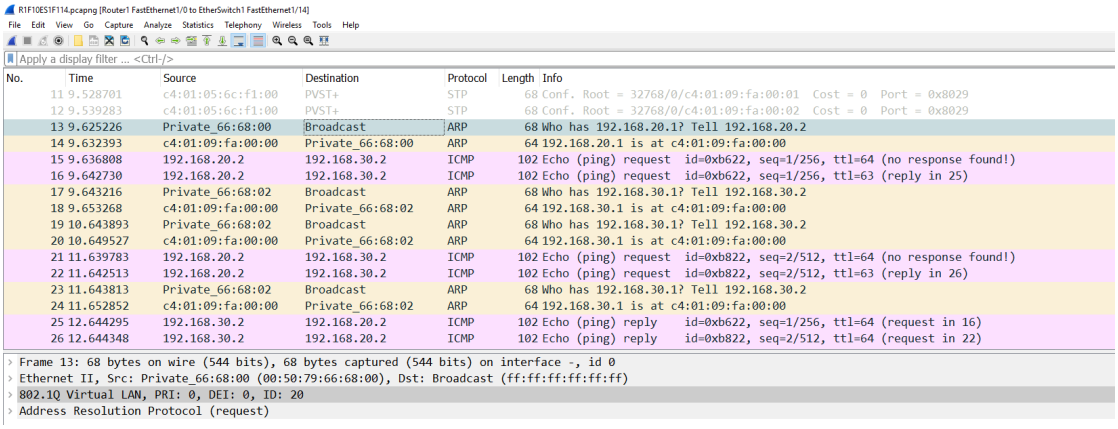


Figure 15: Connection between EtherSwitch1 and the router

# 5 Conclusion

- In mission 1, PC1 and PC3 are on the same subnet to ping to each other. In the rest missions, PC1,...,PC4 are on a /24 subnet via inter-VLAN routing.
- When disabling the routing in the EtherSwitch with the command in configure mode: no ip routing, after "write" we also need to stop and restart the router for the configuration to implement. In practice, we also need to reboot the routers to reconstruct the spanning trees and propagate VLANs.




# Network Security

## Homework 3: IPSec VPN

Boya Zhang

February 10, 2021

Engineering Science

# 1 Topology

Three routers are connected with three different PCs. At first we set up without IPsec VPN and check whether the link is in clear. Then we set the IPsec VPN and perform validation.

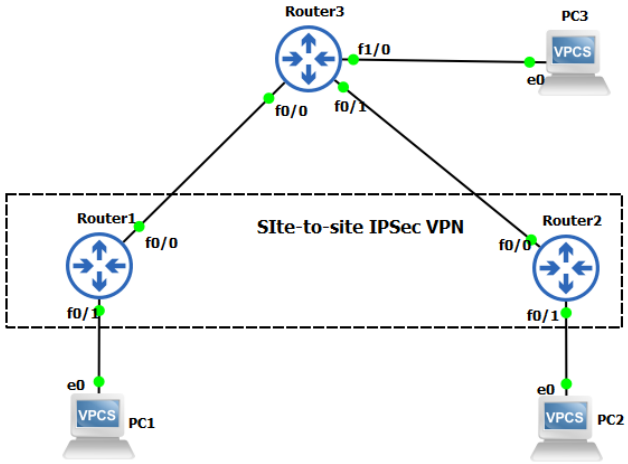


Figure 1: Topology

# 2 Setup

Dynamic routing are configured on R1,R2,and R3.

```
Router1#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router1(config)#interface fastEthernet 0/0
Router1(config-if)#ip address 10.0.1.1 255.255.255.0
Router1(config-if)#no shutdown
Router1(config-if)#exit
Router1(config)#interface fastEthernet 0/1
Router1(config-if)#ip address 192.168.10.1 255.255.255.0
Router1(config-if)#no shutdown
Router1(config-if)#exit
Router1(config)#router rip
Router1(config-router)#network 10.0.1.0
Router1(config-router)#network 192.168.10.0
Router1(config-router)#end
Router1#
*Mar  1 00:42:40.471: %SYS-5-CONFIG_I: Configured from console by console
Router1#write
Building configuration...
[OK]
Router1#
```

Figure 2: Router1

```
Router2#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router2(config)#interface fastEthernet 0/0
Router2(config-if)#ip address 10.0.2.1 255.255.255.0
Router2(config-if)#no shutdown
Router2(config-if)#exit
Router2(config)#interface fastEthernet 0/1
Router2(config-if)#ip address 192.168.20.1 255.255.255.0
Router2(config-if)#no shutdown
Router2(config-if)#exit
Router2(config)#router rip
Router2(config-router)#network 10.0.2.0
Router2(config-router)#network 192.168.20.0
Router2(config-router)#end
Router2#
*Mar  1 01:10:14.331: %SYS-5-CONFIG_I: Configured from console by console
Router2#write
Building configuration...
[OK]
Router2#
```

Figure 3: Router2

```
Router3#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router3(config)#interface fastEthernet 0/0
Router3(config-if)#ip address 10.0.1.2 255.255.255.0
Router3(config-if)#no shutdown
Router3(config-if)#exit
Router3(config)#interface fastEthernet 0/1
Router3(config-if)#ip address 10.0.2.2 255.255.255.0
Router3(config-if)#no shutdown
Router3(config-if)#exit
Router3(config)#interface fastEthernet 1/0
Router3(config-if)#ip address 192.168.30.1 255.255.255.0
Router3(config-if)#no shutdown
Router3(config-if)#exit
Router3(config)#router rip
Router3(config-router)#network 10.0.1.0
Router3(config-router)#network 10.0.2.0
Router3(config-router)#network 192.168.30.0
Router3(config-router)#end
Router3#w
*Mar  1 00:58:18.179: %SYS-5-CONFIG_I: Configured from console by console
Router3#write
Building configuration...
[OK]
Router3#
```

Figure 4: Router3

The VPCs are configured.

```
PC1> ip 192.168.10.2/24 192.168.10.1
Checking for duplicate address...
PC1 : 192.168.10.2 255.255.255.0 gateway 192.168.10.1
```

(a) PC1

```
PC2> ip 192.168.20.2/24 192.168.20.1
Checking for duplicate address...
PC1 : 192.168.20.2 255.255.255.0 gateway 192.168.20.1
```

(b) PC2

```
PC3> ip 192.168.30.2/24 192.168.30.1
Checking for duplicate address...
PC1 : 192.168.30.2 255.255.255.0 gateway 192.168.30.1
```

(c) PC3

Figure 5: Configuration of VPCs

We validate the settings from router3. We can see that for interfaces the IP-Addresses are well set and the networks are connected.

```
Router3#show ip interface brief
Interface                  IP-Address      OK? Method Status                Protocol
FastEthernet0/0            10.0.1.2        YES NVRAM  up                    up
FastEthernet0/1            10.0.2.2        YES NVRAM  up                    up
FastEthernet1/0            192.168.30.1    YES NVRAM  up                    up
Router3#show ip route
Codes: C - connected, S - static, 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
       i - IS-IS, su - IS-IS summary, 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    192.168.30.0/24 is directly connected, FastEthernet1/0
R    192.168.10.0/24 [120/1] via 10.0.1.1, 00:00:10, FastEthernet0/0
R    192.168.20.0/24 [120/1] via 10.0.2.1, 00:00:16, FastEthernet0/1
     10.0.0.0/24 is subnetted, 2 subnets
C       10.0.2.0 is directly connected, FastEthernet0/1
C       10.0.1.0 is directly connected, FastEthernet0/0
```

Figure 6: Validation from router

# 3 Mission 1: Traffic observation

We ping from PC1 to PC2 and also from PC1 to PC3. Wireshark is used to capture the traffic. We can see from figures below that ICMP ping messages are sent in clear.

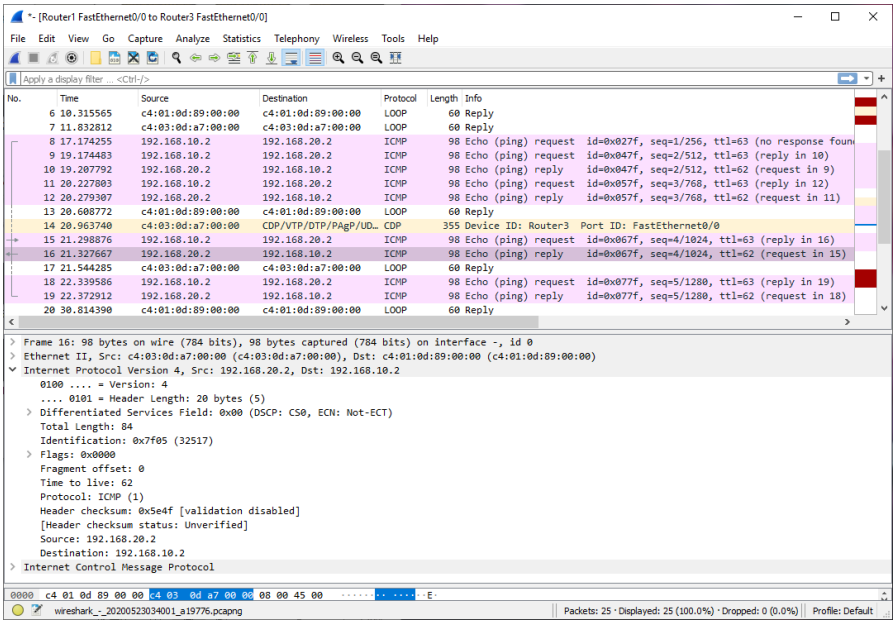


Figure 7: Traffic logging between Router1 and Router3(Ping from PC1 to PC2)

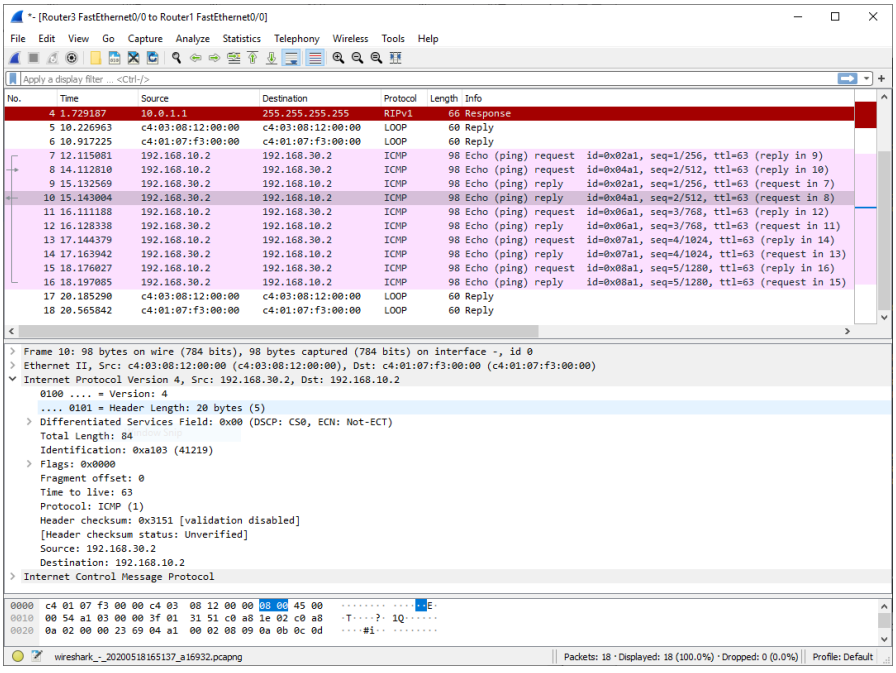


Figure 8: Traffic logging between Router1 and Router3(Ping from PC1 to PC3)

# 4 Mission 2: Site-to-site IPSec VPN

We select the IKE policy as encryption algorithm: AES-256, hash algorithm: SHA1 , authentication method: Pre-Shared Key , Diffie-Hellman group: 2, lifetime: 86400 seconds.

## 4.1 IPSec Phase 1 (aka IKE)

In phase 1 we first describe the parameters used for the SA relationship. Second, a pre-shared password is set for destination. For Router 1 the destination is Router 2, vise versa.

```
Router1#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router1(config)#crypto isakmp policy 1
Router1(config-isakmp)#encryption aes
Router1(config-isakmp)#hash sha
Router1(config-isakmp)#authentication pre-share
Router1(config-isakmp)#group 2
Router1(config-isakmp)#lifetime 86400
Router1(config-isakmp)#exit
Router1(config)#crypto isakmp key unicorn address 10.0.2.1
A pre-shared key for address mask 10.0.2.1 255.255.255.255 already exists!
```

Figure 9: Phase 1 for Router 1

```
Router2#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router2(config)#crypto isakmp policy 1
Router2(config-isakmp)#encryption aes
Router2(config-isakmp)#hash sha
Router2(config-isakmp)#authentication pre-share
Router2(config-isakmp)#group 2
Router2(config-isakmp)#lifetime 86400
Router2(config-isakmp)#exit
Router2(config)#crypto isakmp key unicorn address 10.0.1.1
A pre-shared key for address mask 10.0.1.1 255.255.255.255 already exists!
```

Figure 10: Phase 1 for Router 2

## 4.2 ISAKMP Phase 2 (aka crypto transformations and access control)

We configure IPsec in the following steps.

- Create extended ACL: We determine what packets are subject (or not) to transformation so that the normal traffic and the VPN traffic can be separated.
- Create IPSec Transform: We configure how packets will be ciphered.
- Create Crypto Map: We link a specific destination with a specific transform and filtered with the ACL.
- Apply crypto map to the public interface: We tell the router to analyze every packet passing by that interface for a possible crypto transformation

```
Router1#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router1(config)#ip access-list extended VPN-TRAFFIC
Router1(config-ext-nacl)#permit ip 192.168.10.0 0.0.0.255 192.168.20.0 0.0.0.2$
Router1(config-ext-nacl)#crypto ipsec transform-set myTS esp-aes esp-sha-hmac
Router1(cfg-crypto-trans)#exit
Router1(config)#crypto ipsec transform-set myTS esp-aes esp-sha-hmac
Router1(cfg-crypto-trans)#exit
Router1(config)#crypto map CMAP 10 ipsec-isakmp
Router1(config-crypto-map)#set peer 10.0.2.1
Router1(config-crypto-map)#set transform-set myTS
Router1(config-crypto-map)#match address VPN-TRAFFIC
Router1(config-crypto-map)#exit
Router1(config)#interface fastEthernet 0/0
Router1(config-if)#crypto map CMAP
Router1(config-if)#exit
Router1(config)#exit
```

Figure 11: Phase 2 for Router 1

```
Router2(config)#ip access-list extended VPN-TRAFFIC
Router2(config-ext-nacl)#$92.168.20.0 0.0.0.255 192.168.10.0 0.0.0.255
Router2(config-ext-nacl)#exit
Router2(config)#crypto ipsec transform-set myTS esp-aes esp-sha-hmac
Router2(cfg-crypto-trans)#crypto map CMAP 10 ipsec-isakmp
Router2(config-crypto-map)#set peer 10.0.1.1
Router2(config-crypto-map)#set transform-set myTS
Router2(config-crypto-map)#match address VPN-TRAFFIC
Router2(config-crypto-map)#interface fastEthernet 0/0
Router2(config-if)#crypto map CMAP
```

Figure 12: Phase 2 for Router 2

# 5 Mission 3: Validate

First, we capture the traffic on the line between Router3 and PC3.Then we ping the remote hosts from PC1 to PC3 (no VPN tunnel).We can see that ICMP ping messages sent in clear.

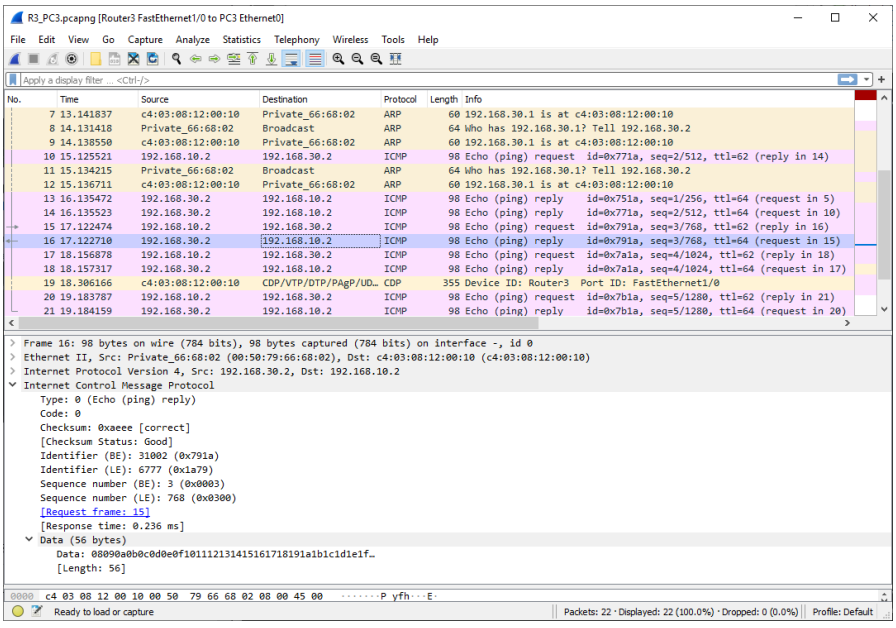


Figure 13: ICMP ping messages sent in clear

Second, we capture the traffic on the line between Router3 and Router2. Then we ping the remote hosts from PC1 to PC2 (with VPN tunnel).We can see that the packets are subject to the transform rule and are encapsulated in IPSec ESP. The first two ping packets are lost because of ARP requests and the time needed to negotiate the phase 1 and create the corresponding IPSec SA.

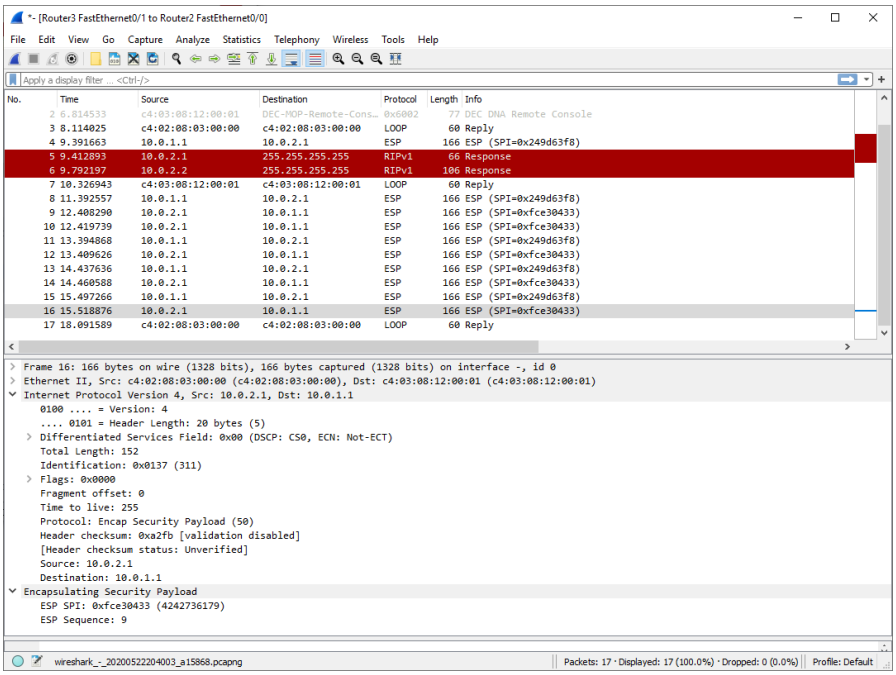


Figure 14: Packets encapsulated in IPSec ESP

Third, we perform validation on the tunnel (IKE Policies, transformations).

```
Router1#show crypto isakmp policy

Global IKE policy
Protection suite of priority 1
        encryption algorithm:   AES - Advanced Encryption Standard (128 bit keys).
        hash algorithm:         Secure Hash Standard
        authentication method:  Pre-Shared Key
        Diffie-Hellman group:   #2 (1024 bit)
        lifetime:               86400 seconds, no volume limit
Default protection suite
        encryption algorithm:   DES - Data Encryption Standard (56 bit keys).
        hash algorithm:         Secure Hash Standard
        authentication method:  Rivest-Shamir-Adleman Signature
        Diffie-Hellman group:   #1 (768 bit)
        lifetime:               86400 seconds, no volume limit
Router1#show crypto isakmp sa
dst             src             state          conn-id slot status
10.0.2.1        10.0.1.1        QM_IDLE              1    0 ACTIVE

Router1#show crypto isakmp peers
Peer: 10.0.2.1 Port: 500 Local: 10.0.1.1
 Phase1 id: 10.0.2.1
```

Figure 15: IKE Policies

```
Router1#show crypto ipsec sa

interface: FastEthernet0/0
    Crypto map tag: CMAP, local addr 10.0.1.1

   protected vrf: (none)
   local  ident (addr/mask/prot/port): (192.168.10.0/255.255.255.0/0/0)
   remote ident (addr/mask/prot/port): (192.168.20.0/255.255.255.0/0/0)
   current_peer 10.0.2.1 port 500
     PERMIT, flags={origin_is_acl,}
    #pkts encaps: 9, #pkts encrypt: 9, #pkts digest: 9
    #pkts decaps: 9, #pkts decrypt: 9, #pkts verify: 9
    #pkts compressed: 0, #pkts decompressed: 0
    #pkts not compressed: 0, #pkts compr. failed: 0
    #pkts not decompressed: 0, #pkts decompress failed: 0
    #send errors 1, #recv errors 0

     local crypto endpt.: 10.0.1.1, remote crypto endpt.: 10.0.2.1
     path mtu 1500, ip mtu 1500, ip mtu idb FastEthernet0/0
     current outbound spi: 0x0(0)
```

Figure 16: Transformations

# 6 Conclusion

During this lab we configured L3 (IP to IP) VPN and learnt the IPsec options with phase 1 and phase 2 negotiations. One small problem I met was that the IPsec has already been configured in the project provided and the clear command cannot deleted the configuration. In order to perform the setup and mission1. The topology is drawn on a new file.