Al-Najah National University
Computer Network and Information Security
Network security lab

Point-to-Point GRE VPN Tunnel

Instructor: Dr. Ahmed Awad

Mohammed Adnan
Dima Bshara
Sineen Bazyan

1 Abstract

The purpose of this experiment is to know how the Point-to-Point GRE VPN Tunnel protocol works, and to describe the mechanism of it.

2 Introduction

Tunneling provides a mechanism to transport packets of one protocol within another protocol. The protocol that is carried is called as the passenger protocol. Which is protocol you want to carry over a network that does not understand it. For example, you may want to tunnel IPv6 packets over an IPv4-only network. Thus, the IPv6 would become the passenger protocol here. The carrier protocol is the one that is used to encapsulate the passenger's protocol packets as its own payload like ipv4. What's more, a tunneling protocol is one that encloses in its datagram another complete data packet that uses a different communications protocol. They essentially create a tunnel between two points on a network that can securely transmit any kind of data between them. Generally, these types of protocols are used to send private network data over a public network, usually when creating a virtual private network (VPN), but can also be used to increase the security of unencrypted data when it is sent over a public network. There are a number of popular tunneling protocols, such as Secure Socket (SSH), Point-to-Point Tunneling (PPTP) and IPsec, with each being tailored for a different specific tunneling purpose. Briefly, this Protocol used to facilitate tunneling like Generic Routing Encapsulation (GRE) which is a tunneling protocol allows the encapsulation of a wide variety of network layer protocols inside point-to-point links. A GRE tunnel is used when packets need to be sent from one network to another over the Internet or an insecure network. With GRE, a virtual tunnel is created between the two endpoints (Cisco routers) and packets are sent through the GRE tunnel. It is important to note that packets travelling inside a GRE tunnel are not encrypted as GRE does not encrypt the tunnel but encapsulates it with a GRE header. If data protection is required, IPsec must be configured to provide data confidentiality – this is when a GRE tunnel is transformed into a secure VPN GRE tunnel. While many might think a GRE IPsec tunnel between two routers is similar to a site to site IPsec VPN (crypto), it is not. A major difference is that GRE tunnels allow multicast packets to traverse the tunnel whereas IPsec VPN does not support multicast packets. In large networks where routing protocols such as OSPF, EIGRP are necessary. For this reason, plus the fact that GRE tunnels are much easier to configure, engineers prefer to use GRE rather than IPsec VPN.

3 Required Resources

- 3 Routers
- 2 PCs
- Console cables to configure the Cisco IOS devices via the console ports
- Ethernet and serial cables as shown in the topology

• We will connect them as figure 1 show.

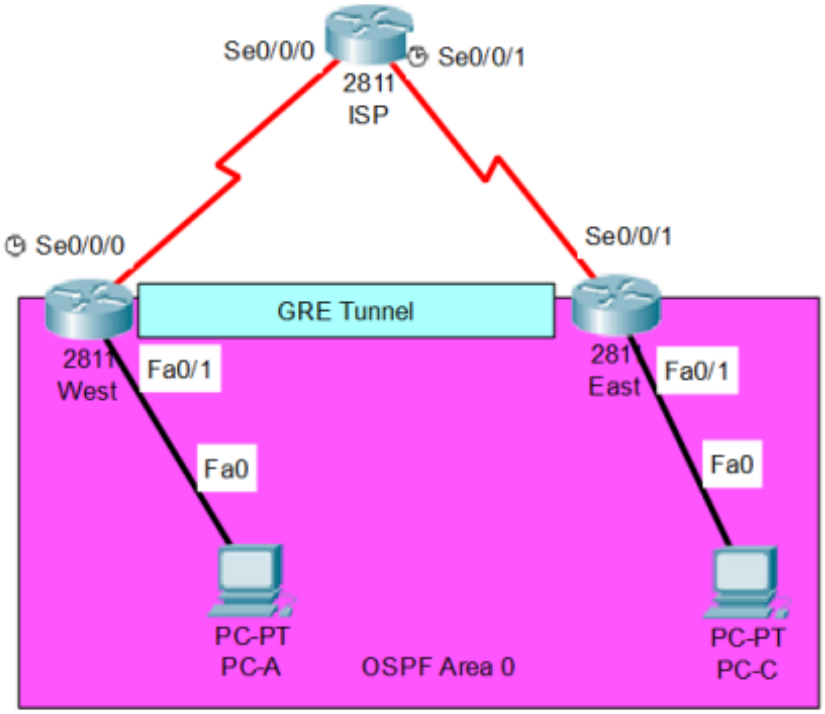

Figure 1: Topology Experiment

- We also apply IP addresses to Serial and Fast Ethernet interfaces according to the Addressing Table and activate the physical interfaces. Figure 2 shows the address table.

Addressing Table

Device	Interface	IP Address	Subnet Mask	Default Gateway
WEST	F0/1	172.16.1.1	255.255.255.0	N/A
	S0/0/0 (DCE)	10.1.1.1	255.255.255.252	N/A
	Tunnel0	172.16.12.1	255.255.255.252	N/A
ISP	S0/0/0	10.1.1.2	255.255.255.252	N/A
	S0/0/1 (DCE)	10.2.2.2	255.255.255.252	N/A
EAST	F0/1	172.16.2.1	255.255.255.0	N/A
	S0/0/1	10.2.2.1	255.255.255.252	N/A
	Tunnel0	172.16.12.2	255.255.255.252	N/A
PC-A	NIC	172.16.1.3	255.255.255.0	172.16.1.1
PC-C	NIC	172.16.2.3	255.255.255.0	172.16.2.1

Figure 2: Address Table

4 Procedure

4.1 Part 1: Configure Basic Device Settings

In Part 1, we set up the network topology and configure basic router settings in **step 1**, such as the interface IP addresses, routing, device access, and passwords.

- Step 1: Configure basic settings for each router.
  - Disable DNS lookup.
  - Configure the device names.
  - Encrypt plain text passwords.
  - Create a message of the day (MOTD) banner warning users that unauthorized access is prohibited.
  - Assign pass as the encrypted privileged EXEC mode password.
  - Set console logging to synchronous mode.
  - Apply IP addresses to Serial and Fast Ethernet interfaces according to the Addressing Table and activate the physical interfaces. Do NOT configure the Tunnel0 interfaces at this time.
  - Set the clock rate to 128000 for DCE serial interfaces.

  figure 3 shows the basic setting on ISP, figure 4 shows the basic setting on West, and figure 5 shows the basic setting on East.

```
ISP(config)#no ip domain-lo
ISP(config)#no ip domain-lookup
ISP(config)#serv
ISP(config)#service pas
ISP(config)#service password-encryption
ISP(config)#ban
ISP(config)#banner motd *you are in sev=c place *
ISP(config)#banner motd * unauthorized access is prohibited *
ISP(config)#enable sec
ISP(config)#enable secret pass
ISP(config)#line cons 0
ISP(config-line)#pass pass
ISP(config-line)#logg
ISP(config-line)#logging s
ISP(config-line)#logging synchronous
ISP(config-line)#exit
ISP(config)#line vty 0 4
ISP(config-line)#pass pass
ISP(config-line)#log
ISP(config-line)#login
ISP(config-line)#ex
% Ambiguous command:  "ex"
ISP(config-line)#exi
ISP(config)#int s0/0/0
ISP(config-if)#ip add 10.1.1.2 255.255.255.252
ISP(config-if)#no shut
ISP(config-if)#int s0/0/1
ISP(config-if)#ip add 10.2.2.2 255.255.255.252
ISP(config-if)#no shut
ISP(config-if)#cl
ISP(config-if)#clo
ISP(config-if)#clock r
ISP(config-if)#clock rate 128000
ISP(config-if)#end
```

Figure 3: Basic settings for ISP

```
Router(config)#no ip domain-lookup
Router(config)#hostn WEST
WEST(config)#serv paa
WEST(config)#ser
WEST(config)#service pas
WEST(config)#service password-encryption
WEST(config)#banner motd % unathorized access is prohibited
Enter TEXT message.  End with the character '%'.

banner motd % unathorized access is prohibited %
WEST(config)#ena secr pass
WEST(config)#lin vty 0 4
WEST(config-line)#pass pass
WEST(config-line)#login
WEST(config-line)#lin con 0
WEST(config-line)#pass pass
WEST(config-line)#logg
WEST(config-line)#logging sy
WEST(config-line)#logging synchronous
WEST(config-line)#exi
WEST(config)#int f0/1
WEST(config-if)#ip add 172.16.1.1 255.255.255.0
WEST(config-if)#no shu
WEST(config-if)#int s0/
*Apr 26 10:52:58.631: %LINK-3-UPDOWN: Interface FastEthernet0/1, changed state t
o up
WEST(config-if)#int s0/0/0
WEST(config-if)#
*Apr 26 10:53:01.627: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthern
et0/1, changed state to up
WEST(config-if)#ip add 10.1.1.1 255.255.255.252
WEST(config-if)#no shut
WEST(config-if)#
*Apr 26 10:53:20.591: %LINK-3-UPDOWN: Interface Serial0/0/0, changed state to up
*Apr 26 10:53:21.591: %LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/
0, changed state to up
WEST(config-if)#clo
WEST(config-if)#clock ra
WEST(config-if)#clock rate 128000
```

Figure 4: Basic settings for WEST

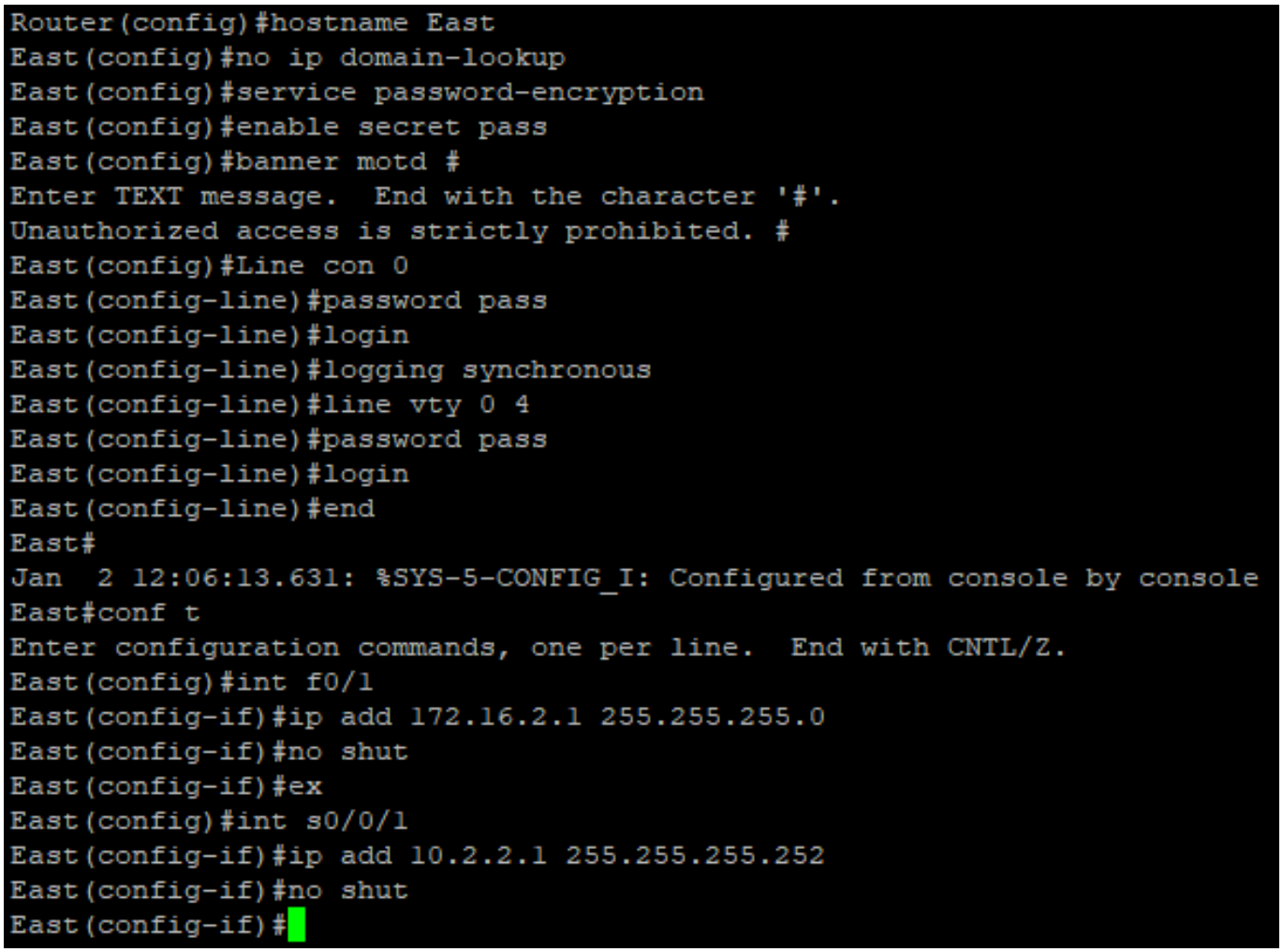

Figure 5: Basic settings for EAST

- Step 2: Configure default routes to the ISP router.
  We will configure the default route so when no specific route can be determined for a given internet protocol (IP) destination address. All packets for destinations not established in the routing table, are sent via the default route, which is ISP in our experiment.
  1. We configure default route on WEST as figure 6 shown.

```
WEST(config)#ip route 0.0.0.0 0.0.0.0 10.1.1.2
```

Figure 6: Default route on WEST.

  2. We configure default route on East as figure 7 shown.

```
East(config)#ip route 0.0.0.0 0.0.0.0 10.2.2.2
```

Figure 7: Default route on East.

- Step 3: Configure the PCs
  We configure the Pcs with IP address as in the address table.
  Figure 8 show PC-A,and Figure 9 show PC-C.

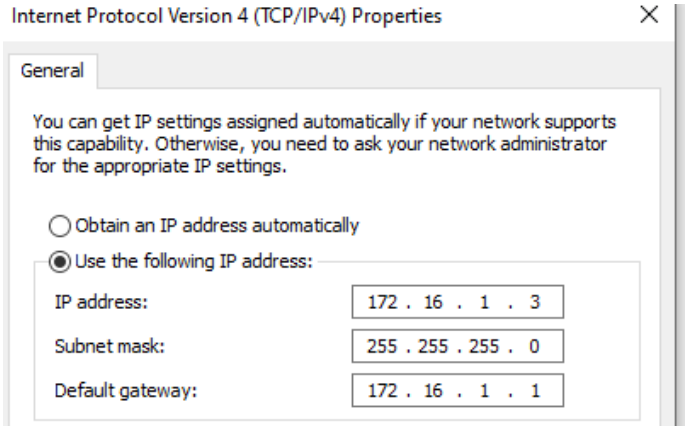

Figure 8: PC-A configuration.

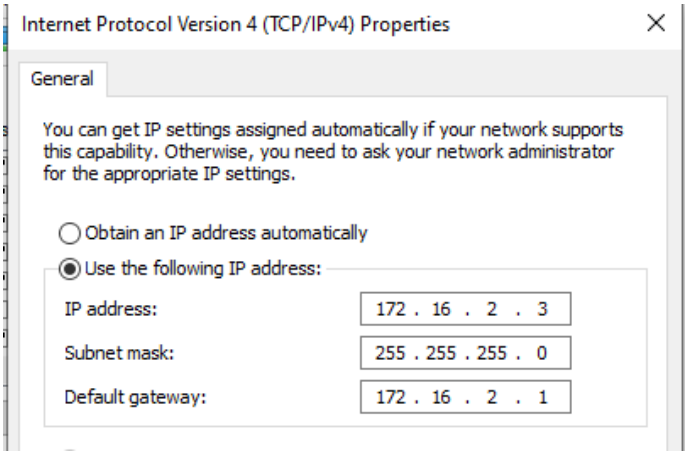

Figure 9: PC-C configuration.

- Step 4:Verify connectivity
  At this point, the PCs are unable to ping each other because we do not define her network on both sides. Each PC can ping its default gateway, as figures (10,11) shown.

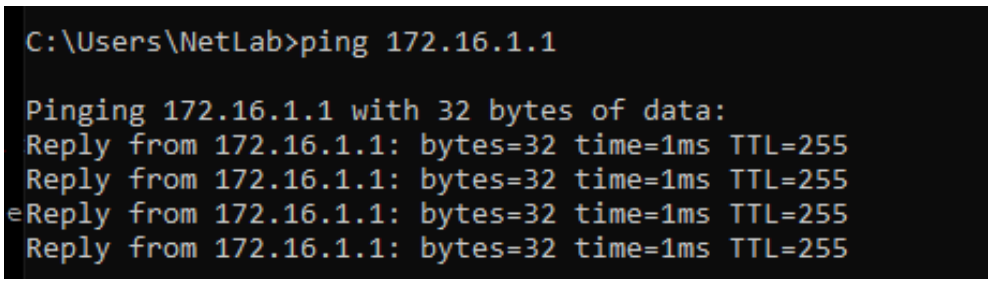

Figure 10: Ping pc-A to GW.

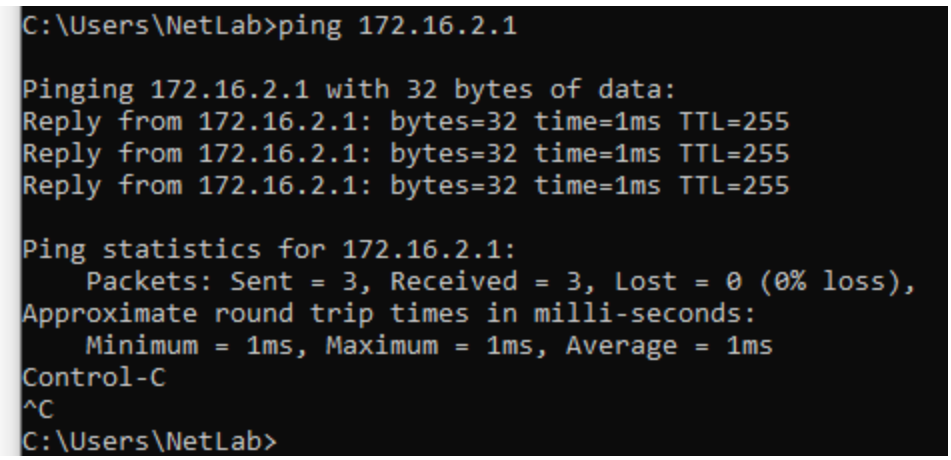

Figure 11: Ping pc-C to GW.

- Step 5 :Save running configuration Figure 14 show the saving command.

Figure 12: Save running configuration.

4.2 Part 2: Configure a GRE Tunnel

In Part 2, we configure a GRE tunnel between the WEST and EAST routers. The tunnels behave as virtual point-to-point links that have two endpoints identified by the tunnel source and tunnel destination addresses at each endpoint.

1. In first, we Configure the tunnel interface on the WEST router. Use S0/0/0 on WEST as the tunnel source interface and 10.2.2.1 as the tunnel destination on the EAST router, as shown figure 13.

```
WEST(config)#int tunnel 0
WEST(config-if)#ip add
*Apr 26 11:12:59.887: %LINEPROTO-5-UPDOWN: Line protocol on Interface Tunnel0, changed state to down
WEST(config-if)#ip add 172.16.12.1 255.255.255.252
WEST(config-if)#tun
WEST(config-if)#tunnel s
WEST(config-if)#tunnel so
WEST(config-if)#tunnel source s0/0/0
WEST(config-if)#tun
WEST(config-if)#tunnel des
WEST(config-if)#tunnel destination 10.2.2.1
WEST(config-if)#
*Apr 26 11:14:09.555: %LINEPROTO-5-UPDOWN: Line protocol on Interface Tunnel0, changed state to up
```

Figure 13: configure GRE tunnel (WEST)

2. We also configure the tunnel interface on the EAST router, by used S0/0/1 on EAST as the tunnel source interface and 10.1.1.1 as the tunnel destination on the WEST router, figure 14 show how it done.

```
East(config)#interface tunnel 0
East(config-if)#
Jan  2 12:24:59.487: %LINEPROTO-5-UPDOWN: Line protocol on Inter
tate to down
East(config-if)# ip address 172.16.12.2 255.255.255.252
East(config-if)#tunnel source 10.2.2.1
East(config-if)#tunnel destination 10.1.1.1
East(config-if)#
Jan  2 12:25:25.599: %LINEPROTO-5-UPDOWN: Line protocol on Inter
tate to up
East(config-if)#
```

Figure 14: configure GRE tunnel (EAST)

- Note: For the tunnel source command, either the interface name or the IP address can be used as the source.

- **Step 2: Verify that the GRE tunnel is functional.**

3. We verify the status of the tunnel interface on the WEST and EAST routers, figures 16 and 27 shows how we do that.

```
WEST(config)#do show ip int br
Interface                  IP-Address      OK? Method Status                Protocol
FastEthernet0/0            unassigned      YES unset  administratively down down
FastEthernet0/1            172.16.1.1      YES manual up                    up
Serial0/0/0                10.1.1.1        YES manual up                    up
Serial0/0/1                unassigned      YES unset  administratively down down
Tunnel0                    172.16.12.1     YES manual up                    up
WEST(config)#
```

Figure 15: status of the WEST tunnel interface

```
East#show ip int br
Interface                  IP-Address      OK? Method Status                Protocol
FastEthernet0/0            unassigned      YES unset  administratively down down
FastEthernet0/1            172.16.2.1      YES manual up                    up
Serial0/0/0                unassigned      YES unset  administratively down down
Serial0/0/1                10.2.2.1        YES manual up                    up
Tunnel0                    172.16.12.2     YES manual up                    up
East#
```

Figure 16: status of the EAST tunnel interface

4. After that we issue the **show interfaces tunnel 0** command in both EAST and WEST to verify the tunneling protocol, tunnel source, and tunnel destination used in this tunnel. As shown in figures 17 and 18.

```
WEST#show interfaces tunnel 0
Tunnel0 is up, line protocol is up
  Hardware is Tunnel
  Internet address is 172.16.12.1/30
  MTU 17916 bytes, BW 100 Kbit/sec, DLY 50000 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation TUNNEL, loopback not set
  Keepalive not set
  Tunnel source 10.1.1.1 (Serial0/0/0), destination 10.2.2.1
   Tunnel Subblocks:
      src-track:
         Tunnel0 source tracking subblock associated with Serial0/0/0
          Set of tunnels with source Serial0/0/0, 1 member (includes iterators), on interface <OK>
  Tunnel protocol/transport GRE/IP
```

Figure 17: show interfaces tunnel 0 in WEST

```
East# show interfaces tunnel 0
Tunnel0 is up, line protocol is up
  Hardware is Tunnel
  Internet address is 172.16.12.2/30
  MTU 17916 bytes, BW 100 Kbit/sec, DLY 50000 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation TUNNEL, loopback not set
  Keepalive not set
  Tunnel source 10.2.2.1, destination 10.1.1.1
  Tunnel protocol/transport GRE/IP
```

Figure 18: show interfaces tunnel 0 in EAST

5. We Ping across the tunnel from the WEST router to the EAST router using the IP address of the tunnel interface. Then we used the traceroute command on the WEST to determine the path to the tunnel interface on the EAST router. Figures 19 and 20 shows these steps .

```
WEST#ping 172.16.12.2
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.16.12.2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 36/36/40 ms
```

Figure 19: ping across tunnle WEST-EAST

```
WEST#traceroute 172.16.12.2
Type escape sequence to abort.
Tracing the route to 172.16.12.2
VRF info: (vrf in name/id, vrf out name/id)
  1 172.16.12.2 24 msec *  20 msec
```

Figure 20: Traceroute across tunnle EAST-WEST

6. We also Ping and trace the route across the tunnel from the EAST router to the WEST router using the IP address of the tunnel interface, figures 21and 23 show the result.

```
East#ping 172.16.12.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.16.12.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 36/36/36 ms
East#
```

Figure 21: Ping across tunnle EAST-WEST

```
East#traceroute 172.16.12.1
Type escape sequence to abort.
Tracing the route to 172.16.12.1
VRF info: (vrf in name/id, vrf out name/id)
  1 172.16.12.1 24 msec *  20 msec
```

Figure 22: Traceroute across tunnle EAST-WEST

4.3 Part 3: Enable Routing over the GRE Tunnel

In Part 3, we configure OSPF routing so that the LANs on the WEST and EAST routers can communicate using the GRE tunnel. After the GRE tunnel is setting up, the routing protocol has been implemented. For GRE tunneling, a network statement will include the IP network of the tunnel instead of the network associated with the serial interface. Like, would with other interfaces, such as Serial and Ethernet.

- Step 1: Configure OSPF routing for area 0 over the tunnel.

1. We configure OSPF process ID 1 using area 0 on the WEST router for the 172.16.1.0/24 and 172.16.12.0/24 networks,as figure 23 shown .

```
WEST(config)#router ospf 1
WEST(config-router)#net
WEST(config-router)#network 172.16.1.0 0.0.0.255 area 0
WEST(config-router)#network 172.16.12.0 0.0.0.3 area 0
WEST(config-router)#
```

Figure 23: OSPF configuration (WEST).

2. We configure OSPF process ID 1 using area 0 on the EAST router for the 172.16.2.0/24 and 172.16.12.0/24 networks, as figure 25 shown .

```
East(config)#router ospf 1
East(config-router)#network 172.16.2.0 0.0.0.255 area 0
East(config-router)#network 172.16.12.0 0.0.0.3 area 0
East(config-router)#
```

Figure 24: OSPF configuration (EAST).

- Step 2: Verify OSPF routing

3. From the WEST router, we issue the **show ip route** command to verify the route to 172.16.2.0/24 LAN on the EAST router.

```
WEST#sho
*Apr 26 11:40:30.415: %SYS-5-CONFIG_I: Configured from console by console
WEST#show ip route
Codes: L - local, 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, H - NHRP, l - LISP
       + - replicated route, % - next hop override

Gateway of last resort is 10.1.1.2 to network 0.0.0.0

S*    0.0.0.0/0 [1/0] via 10.1.1.2
      10.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
C        10.1.1.0/30 is directly connected, Serial0/0/0
L        10.1.1.1/32 is directly connected, Serial0/0/0
      172.16.0.0/16 is variably subnetted, 5 subnets, 3 masks
C        172.16.1.0/24 is directly connected, FastEthernet0/1
L        172.16.1.1/32 is directly connected, FastEthernet0/1
O        172.16.2.0/24 [110/1001] via 172.16.12.2, 00:03:40, Tunnel0
C        172.16.12.0/30 is directly connected, Tunnel0
L        172.16.12.1/32 is directly connected, Tunnel0
```

Figure 25: Routing Table.

Question: What is the exit interface and IP address to reach the 172.16.2.0/24 network?
The exit interface is : 172.16.12.2

4. From the EAST router we issue the command to verify the route to 172.16.1.0/24 LAN on the WEST router, as figure 26 shown .

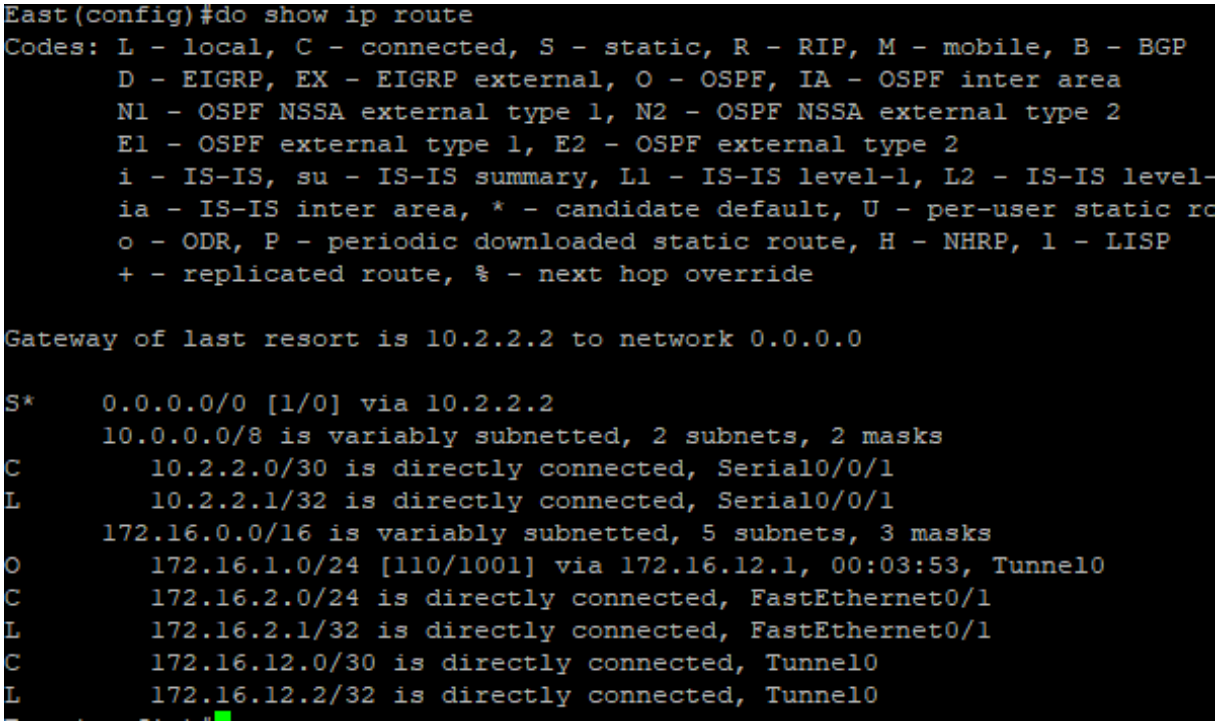

Figure 26: Routing Table.

Question: What is the exit interface and IP address to reach the 172.16.1.0/24 network?
The exit interface is : 172.16.12.1

- Step 3: Verify end-to-end connectivity

1. After that we Ping from PC-A to PC-C, as shown in figure 27.

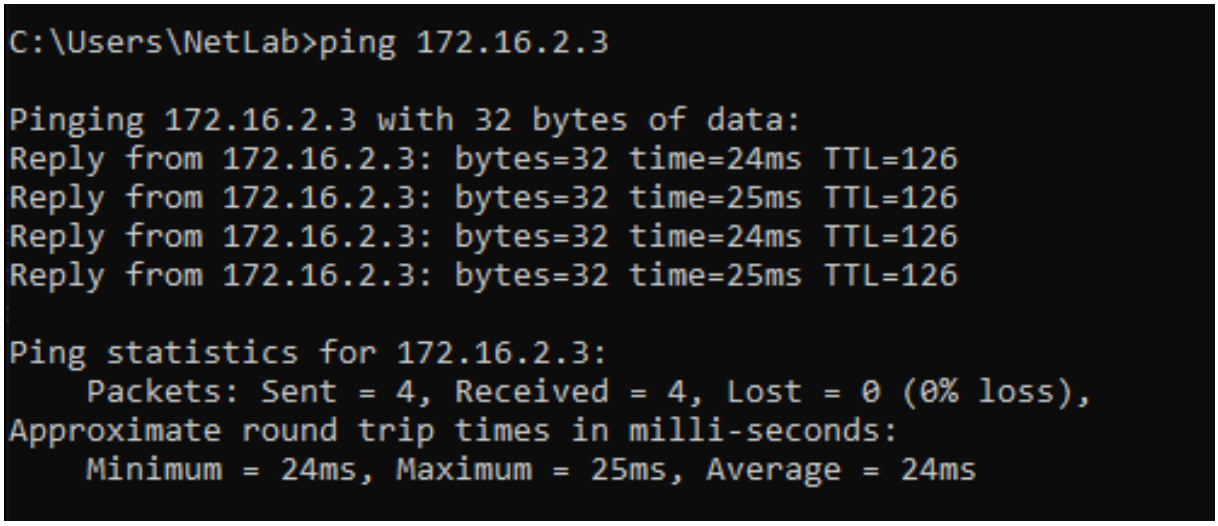

Figure 27: ping PC-A to PC-C (after ospf over tunnle)

2. At the end we Traceroute from PC-C to PC-A, as shown in figure 28.

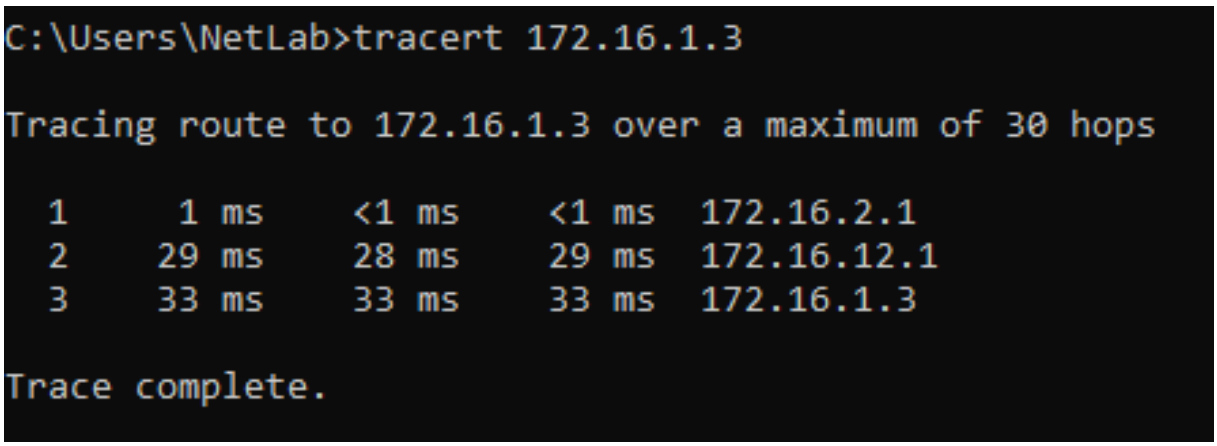

Figure 28: Traceroute from PC-C PC-A.PNG

5 Conclusion

GRE tunnels allow routing protocols such as RIP and OSPF to forward data packets from one switch to another switch across the Internet. With GRE we are able to configure a virtual point-to-point link between two endpoints.

6 References

http://blog.boson.com/bid/92815/What-are-the-differences-between-an-IPSec-VPN-and-a-GRE-Tunnel

https://www.cisco.com/c/en/us/td/docs/solutions/Enterprise/WAN-and-MAN/P2P-GRE-IPSec/P2P-GRE

http://www.firewall.cx/cisco-technical-knowledgebase/cisco-routers/868-cisco-router-gre-ipsec.html

https://www.cisco.com/P2P-GRE-IPSec