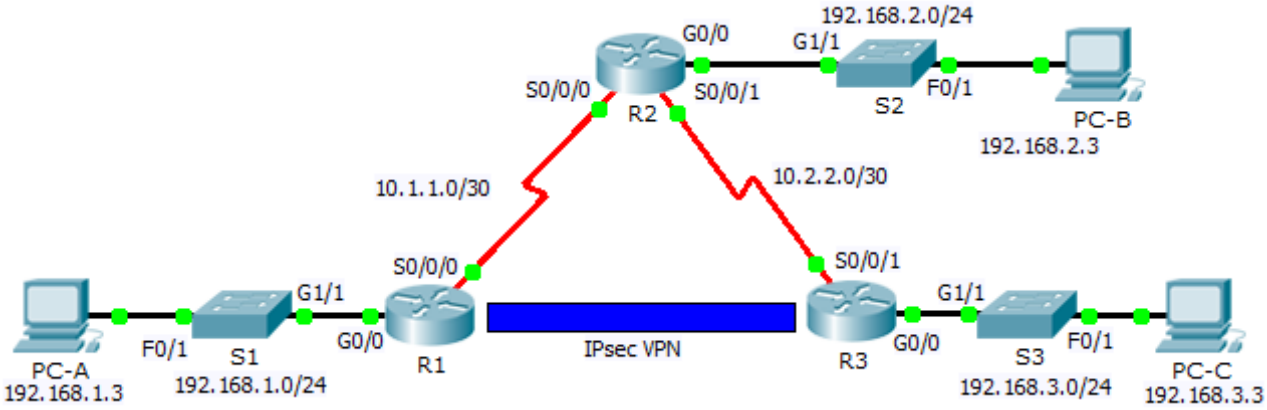
INSTITUTO POLITÉCNICO DE LEIRIA
Escola Superior de Tecnologia e Gestão
REDES DE DADOS

Laboratory work n.º09
VPN (Virtual Private Network)

Objectives:

Lab. I: Packet Tracer – Configuring VPNs (Optional)

Topology



Addressing Table

Device	Interface	IP Address	Subnet Mask	Default Gateway
R1	G0/0	192.168.1.1	255.255.255.0	N/A
	S0/0/0	10.1.1.2	255.255.255.252	N/A
R2	G0/0	192.168.2.1	255.255.255.0	N/A
	S0/0/0	10.1.1.1	255.255.255.252	N/A
	S0/0/1	10.2.2.1	255.255.255.252	N/A
R3	G0/0	192.168.3.1	255.255.255.0	N/A
	S0/0/1	10.2.2.2	255.255.255.252	N/A
PC-A	NIC	192.168.1.3	255.255.255.0	192.168.1.1
PC-B	NIC	192.168.2.3	255.255.255.0	192.168.2.1
PC-C	NIC	192.168.3.3	255.255.255.0	192.168.3.1

ISAKMP Phase 1 Policy Parameters

Parameters		R1	R3
Key distribution method	Manual or **ISAKMP**	ISAKMP	ISAKMP
Encryption algorithm	**DES**, 3DES, or AES	AES	AES
Hash algorithm	MD5 or **SHA-1**	SHA-1	SHA-1
Authentication method	Pre-shared keys or **RSA**	pre-share	pre-share
Key exchange	DH Group **1**, 2, or 5	DH 2	DH 2
IKE SA Lifetime	86400 seconds or less	86400	86400
ISAKMP Key		cisco	cisco

Bolded parameters are defaults. Other parameters need to be explicitly configured.

IPsec Phase 2 Policy Parameters

Parameters	R1	R3
Transform Set	VPN-SET	VPN-SET
Peer Hostname	R3	R1
Peer IP Address	10.2.2.2	10.1.1.2
Network to be encrypted	192.168.1.0/24	192.168.3.0/24
Crypto Map name	VPN-MAP	VPN-MAP
SA Establishment	ipsec-isakmp	ipsec-isakmp

Scenario

In this activity, you will configure two routers to support a site-to-site IPsec VPN for traffic flowing from their respective LANs. The IPsec VPN traffic will pass through another router that has no knowledge of the VPN. IPsec provides secure transmission of sensitive information over unprotected networks such as the Internet. IPsec acts at the network layer, protecting and authenticating IP packets between participating IPsec devices (peers), such as Cisco routers.

Part 1: Enable Security Features

Step 1: Activate securityk9 module.

The Security Technology Package license must be enabled to complete this activity.

Note: Both the user EXEC and privileged EXEX pass word is **cisco**.

a. Issue the **show version** command in the user EXEC or privileged EXEC mode to verify that the Security Technology Package license is activated.

```
-----------------------------------------------------------------
Technology    Technology-package          Technology-package
              Current       Type          Next reboot
-----------------------------------------------------------------
ipbase        ipbasek9      Permanent     ipbasek9
security      None          None          None
uc            None          None          None
data          None          None          None

Configuration register is 0x2102
```

b. If not, activate the **securityk9** module for the next boot of the router, accept the license, save the configuration, and reboot.

```
R1(config)# license boot module c2900 technology-package securityk9
R1(config)# end
R1# copy running-config startup-config
R1# reload
```

c. After the reloading is completed, issue the **show version** again to verify the Security Technology Package license activation.

```
Technology Package License Information for Module:'c2900'
```

```
-------------------------------------------------------------------
Technology    Technology-package          Technology-package
              Current       Type          Next reboot
-------------------------------------------------------------------
ipbase        ipbasek9      Permanent     ipbasek9
security      securityk9    Evaluation    securityk9
uc            None          None          None
data          None          None          None
```

d. Repeat Steps 1a to 1c with **R3**.

Part 2: Configure IPsec Parameters on R1

Step 1: Test connectivity.

Ping from **PC-A** to **PC-C**.

Step 2: Identify interesting traffic on R1.

Configure ACL 110 to identify the traffic from the LAN on **R1** to the LAN on **R3** as interesting. This interesting traffic will trigger the IPsec VPN to be implemented whenever there is traffic between **R1** to **R3** LANs. All other traffic sourced from the LANs will not be encrypted. Remember that due to the implicit deny any, there is no need to add the statement to the list.

```
R1(config)# access-list 110 permit ip 192.168.1.0 0.0.0.255
192.168.3.0 0.0.0.255
```

Step 3: Configure the ISAKMP Phase 1 properties on R1.

Configure the crypto ISAKMP policy **10** properties on **R1** along with the shared crypto key **cisco**. Refer to the ISAKMP Phase 1 table for the specific parameters to configure. Default values do not have to be configured therefore only the encryption, key exchange method, and DH method must be configured.

```
R1(config)# crypto isakmp policy 10
R1(config-isakmp)# encryption aes
R1(config-isakmp)# authentication pre-share
R1(config-isakmp)# group 2
R1(config-isakmp)# exit
R1(config)# crypto isakmp key cisco address 10.2.2.2
```

Step 4: Configure the ISAKMP Phase 2 properties on R1.

Create the transform-set **VPN-SET** to use **esp-3des** and **esp-sha-hmac**. Then create the crypto map **VPN-MAP** that binds all of the Phase 2 parameters together. Use sequence number **10** and identify it as an **ipsec-isakmp** map.

```
R1(config)# crypto ipsec transform-set VPN-SET esp-3des esp-sha-hmac
R1(config)# crypto map VPN-MAP 10 ipsec-isakmp
R1(config-crypto-map)# description VPN connection to R3
R1(config-crypto-map)# set peer 10.2.2.2
R1(config-crypto-map)# set transform-set VPN-SET
R1(config-crypto-map)# match address 110
R1(config-crypto-map)# exit
```

Step 5: Configure the crypto map on the outgoing interface.

Finally, bind the **VPN-MAP** crypto map to the outgoing Serial 0/0/0 interface. **Note:** This is not graded.

```
R1(config)# interface S0/0/0
R1(config-if)# crypto map VPN-MAP
```

Part 3: Configure IPsec Parameters on R3

Step 1: Configure router R3 to support a site-to-site VPN with R1.

Now configure reciprocating parameters on **R3**. Configure ACL **110** identifying the traffic from the LAN on **R3** to the LAN on **R1** as interesting.

```
R3(config)# access-list 110 permit ip 192.168.3.0 0.0.0.255
192.168.1.0 0.0.0.255
```

Step 2: Configure the ISAKMP Phase 1 properties on R3.

Configure the crypto ISAKMP policy **10** properties on **R3** along with the shared crypto key **cisco**.

```
R3(config)# crypto isakmp policy 10
R3(config-isakmp)# encryption aes
R3(config-isakmp)# authentication pre-share
R3(config-isakmp)# group 2
R3(config-isakmp)# exit
R3(config)# crypto isakmp key cisco address 10.1.1.2
```

Step 3: Configure the ISAKMP Phase 2 properties on R1.

Like you did on **R1**, create the transform-set **VPN-SET** to use **esp-3des** and **esp-sha-hmac**. Then create the crypto map **VPN-MAP** that binds all of the Phase 2 parameters together. Use sequence number **10** and identify it as an **ipsec-isakmp** map.

```
R3(config)# crypto ipsec transform-set VPN-SET esp-3des esp-sha-hmac
R3(config)# crypto map VPN-MAP 10 ipsec-isakmp
R3(config-crypto-map)# description VPN connection to R1
R3(config-crypto-map)# set peer 10.1.1.2
R3(config-crypto-map)# set transform-set VPN-SET
R3(config-crypto-map)# match address 110
R3(config-crypto-map)# exit
```

Step 4: Configure the crypto map on the outgoing interface.

Finally, bind the **VPN-MAP** crypto map to the outgoing Serial 0/0/1 interface. **Note**: This is not graded.

```
R3(config)# interface S0/0/1
R3(config-if)# crypto map VPN-MAP
```

Part 4: Verify the IPsec VPN

Step 1: Verify the tunnel prior to interesting traffic.

Issue the **show crypto ipsec sa** command on **R1**. Notice that the number of packets encapsulated, encrypted, decapsulated and decrypted are all set to 0.

```
R1# show crypto ipsec sa

interface: Serial0/0/0
    Crypto map tag: VPN-MAP, local addr 10.1.1.2

   protected vrf: (none)
   local  ident (addr/mask/prot/port): (192.168.1.0/255.255.255.0/0/0)
   remote  ident (addr/mask/prot/port): (192.168.3.0/255.255.255.0/0/0)
   current_peer 10.2.2.2 port 500
    PERMIT, flags={origin_is_acl,}
   #pkts encaps: 0, #pkts encrypt: 0, #pkts digest: 0
   #pkts decaps: 0, #pkts decrypt: 0, #pkts verify: 0
   #pkts compressed: 0, #pkts decompressed: 0
   #pkts not compressed: 0, #pkts compr. failed: 0
   #pkts not decompressed: 0, #pkts decompress failed: 0
   #send errors 0, #recv errors 0

     local crypto endpt.: 10.1.1.2, remote crypto endpt.:10.2.2.2
     path mtu 1500, ip mtu 1500, ip mtu idb Serial0/0/0
     current outbound spi: 0x0(0)
<output omitted>
```

Step 2: Create interesting traffic.

Ping **PC-C** from **PC-A**.

Step 3: Verify the tunnel after interesting traffic.

On **R1**, re-issue the **show crypto ipsec sa** command. Now notice that the number of packets is more than 0 indicating that the IPsec VPN tunnel is working.

```
R1# show crypto ipsec sa

interface: Serial0/0/0
    Crypto map tag: VPN-MAP, local addr 10.1.1.2

   protected vrf: (none)
   local  ident (addr/mask/prot/port): (192.168.1.0/255.255.255.0/0/0)
   remote  ident (addr/mask/prot/port): (192.168.3.0/255.255.255.0/0/0)
   current_peer 10.2.2.2 port 500
    PERMIT, flags={origin_is_acl,}
   #pkts encaps: 3, #pkts encrypt: 3, #pkts digest: 0
   #pkts decaps: 3, #pkts decrypt: 3, #pkts verify: 0
   #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.: 10.1.1.2, remote crypto endpt.:10.2.2.2
      path mtu 1500, ip mtu 1500, ip mtu idb Serial0/0/0
      current outbound spi: 0x0A496941(172583233)
<output omitted>
```

Step 4: Create uninteresting traffic.

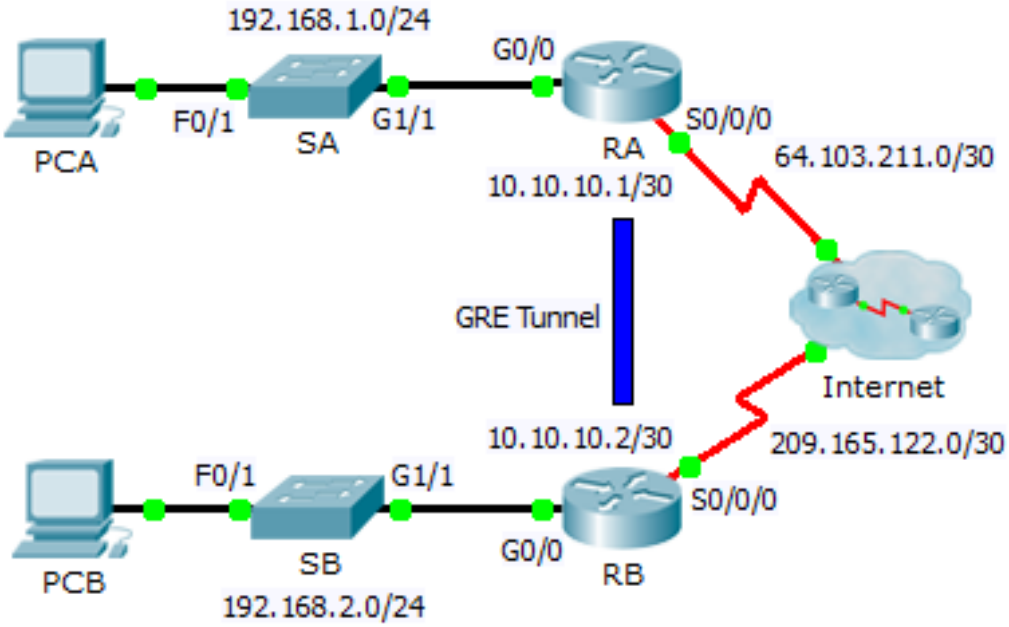
Ping **PC-B** from **PC-A**.

Step 5: Verify the tunnel.

On **R1**, re-issue the **show crypto ipsec sa** command. Finally, notice that the number of packets has not changed verifying that uninteresting traffic is not encrypted.

Lab. II: Packet Tracer – Configuring GRE

Topology



Addressing Table

Device	Interface	IP Address	Subnet Mask	Default Gateway
RA	G0/0	192.168.1.1	255.255.255.0	N/A
	S0/0/0	64.103.211.2	255.255.255.252	N/A
	Tunnel 0	10.10.10.1	255.255.255.252	N/A
RB	G0/0	192.168.2.1	255.255.255.0	N/A
	S0/0/0	209.165.122.2	255.255.255.252	N/A
	Tunnel 0	10.10.10.2	255.255.255.252	N/A
PC-A	NIC	192.168.1.2	255.255.255.0	192.168.1.1
PC-C	NIC	192.168.2.2	255.255.255.0	192.168.2.1

Scenario

You are the network administrator for a company which wants to set up a GRE (generic routing encapsulation) tunnel to a remote office. Both networks are locally configured, and need only the tunnel configured.

Part 1: Verify Router Connectivity

Step 1: Ping RA from RB.

a. Use the **show ip interface brief** command on **RA** to determine the IP address of the S0/0/0 port.

b. From **RB** ping the IP S0/0/0 address of **RA.**

Step 2: Ping PCA from PCB.

Attempt to ping the IP address of **PCA** from **PCB**. We will repeat this test after configuring the GRE tunnel. What were the ping results? Why?

_____

Part 2: Configure GRE Tunnels

Step 1: Configure the Tunnel 0 interface of RA.

a. Enter into the configuration mode for **RA** Tunnel 0.

```
RA(config)# interface tunnel 0
```

b. Set the IP address as indicated in the Addressing Table.

```
RA(config-if)# ip address 10.10.10.1 255.255.255.252
```

c. Set the source and destination for the endpoints of Tunnel 0.

```
RA(config-if)# tunnel source s0/0/0
RA(config-if)# tunnel destination 209.165.122.2
```

d. Configure Tunnel 0 to convey IP traffic over GRE.

```
RA(config-if)# tunnel mode gre ip
```

e. The Tunnel 0 interface should already be active. In the event that it is not, treat it like any other interface.

```
RA(config-if)# no shutdown
```

Step 2: Configure the Tunnel 0 interface of RB.

Repeat Steps 1a – e with **RB**. Be sure to change the IP addressing as appropriate.

_____

_____

_____

_____

Step 3: Configure a route for private IP traffic.

Establish a route between the 192.168.X.X networks using the 10.10.10.0/30 network as the destination.

```
RA(config)# ip route 192.168.2.0 255.255.255.0 10.10.10.2
RB(config)# ip route 192.168.1.0 255.255.255.0 10.10.10.1
```

Part 3: Verify Router Connectivity

Step 1: Ping PCA from PCB.

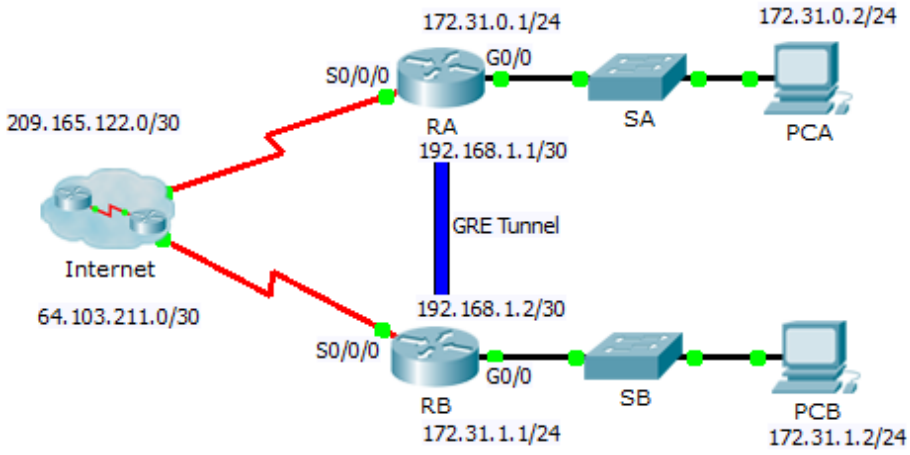
Attempt to ping the IP address of **PCA** from **PCB**. The ping should be successful.

Step 2: Trace the path from PCA to PCB.

Attempt to trace the path from **PCA** to **PCB**. Note the lack of public IP addresses in the output.

Lab III: Packet Tracer – Troubleshooting GRE

Topology



Addressing Table

Device	Interface	IP Address	Subnet Mask	Default Gateway
RA	G0/0	172.31.0.1	255.255.255.0	N/A
	S0/0/0	209.165.122.2	255.255.255.252	N/A
	Tunnel 0	192.168.1.1	255.255.255.252	N/A
RB	G0/0	172.31.1.1	255.255.255.0	N/A
	S0/0/0	64.103.211.2	255.255.255.252	N/A
	Tunnel 0	192.168.1.2	255.255.255.252	N/A
PC-A	NIC	172.31.0.2	255.255.255.0	172.31.0.1
PC-C	NIC	172.31.1.2	255.255.255.0	172.31.1.1

Scenario

A junior network administrator was hired to set up a GRE tunnel between two sites and was unable to complete the task. You have been asked to correct configuration errors in the company network.

Part 1: Find and Correct All Network Errors.

Device	Error	Correction
RA		
RA		
RA		
RB		
RB		

Part 2: Verify Connectivity

Step 1: Ping PCA from PCB.

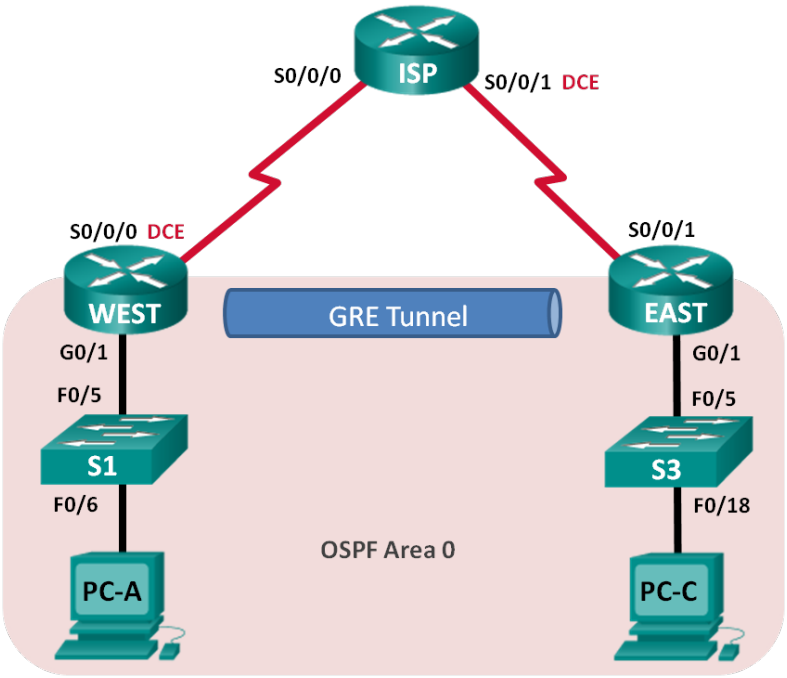
Attempt to ping the IP address of **PCA** from **PCB**. The ping should be successful.

Step 2: Trace the path from PCA to PCB.

Attempt to trace the path from **PCA** to **PCB**. Note the lack of public IP addresses in the output.

Lab. IV: Configuring a Point-to-Point GRE VPN Tunnel

Topology



Addressing Table

Device	Interface	IP Address	Subnet Mask	Default Gateway
WEST	G0/1	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	G0/1	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

Background / Scenario

Generic Routing Encapsulation (GRE) is a tunneling protocol that can encapsulate a variety of network layer protocols between two locations over a public network, such as the Internet.

GRE can be used with:

- Connecting IPv6 networks over IPv4 networks
- Multicast packets, such as OSPF, EIGRP, and streaming applications

In this lab, you will configure an unencrypted point-to-point GRE VPN tunnel and verify that network traffic is using the tunnel. You will also configure the OSPF routing protocol inside the GRE VPN tunnel. The GRE tunnel is between the WEST and EAST routers in OSPF area 0. The ISP has no knowledge of the GRE tunnel. Communication between the WEST and EAST routers and the ISP is accomplished using default static routes.

Note: The routers used with CCNA hands-on labs are Cisco 1941 Integrated Services Routers (ISRs) with Cisco IOS Release 15.2(4)M3 (universalk9 image). The switches used are Cisco Catalyst 2960s with Cisco IOS Release 15.0(2) (lanbasek9 image). Other routers, switches, and Cisco IOS versions can be used. Depending on the model and Cisco IOS version, the commands available and output produced might vary from what is shown in the labs. Refer to the Router Interface Summary Table at the end of this lab for the correct interface identifiers.

Note: Make sure that the routers and switches have been erased and have no startup configurations.

Required Resources

- 3 Routers (Cisco 1941 with Cisco IOS Release 15.2(4)M3 universal image or comparable)
- 2 Switches (Cisco 2960 with Cisco IOS Release 15.0(2) lanbasek9 image or comparable)
- 2 PCs
- Cables

Part 1: Configure Basic Device Settings

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

Step 1: Cable the network as shown in the topology.

Step 2: Initialize and reload the routers and switches.

Step 3: Configure basic settings for each router.

a. Disable DNS lookup.

b. Configure the device names.

c. Encrypt plain text passwords.

d. Create a message of the day (MOTD) banner warning users that unauthorized access is prohibited.

e. Assign **class** as the encrypted privileged EXEC mode password.

f. Assign **cisco** as the console and vty password and enable login.

g. Set console logging to synchronous mode.

h. Apply IP addresses to Serial and Gigabit Ethernet interfaces according to the Addressing Table and activate the physical interfaces. Do NOT configure the Tunnel0 interfaces at this time.

i. Set the clock rate to **128000** for DCE serial interfaces.

Step 4: Configure default routes to the ISP router.

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

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

Step 5: Configure the PCs.

Assign IP addresses and default gateways to the PCs according to the Addressing Table.

Step 6: Verify connectivity.

At this point, the PCs are unable to ping each other. Each PC should be able to ping its default gateway. The routers are able to ping the serial interfaces of the other routers in the topology. If not, troubleshoot until you can verify connectivity.

Step 7: Save your running configuration.

Part 2: Configure a GRE Tunnel

In Part 2, you will configure a GRE tunnel between the WEST and EAST routers.

Step 1: Configure the GRE tunnel interface.

a. 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.

```
WEST(config)# interface tunnel 0
WEST(config-if)# ip address 172.16.12.1 255.255.255.252
WEST(config-if)# tunnel source s0/0/0
WEST(config-if)# tunnel destination 10.2.2.1
```

b. Configure the tunnel interface on the EAST router. Use S0/0/1 on EAST as the tunnel source interface and 10.1.1.1 as the tunnel destination on the WEST router.

```
EAST(config)# interface tunnel 0
EAST(config-if)# ip address 172.16.12.2 255.255.255.252
EAST(config-if)# tunnel source s0/0/1
EAST(config-if)# tunnel destination 10.1.1.1
```

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.

a. Verify the status of the tunnel interface on the WEST and EAST routers.

```
WEST# show ip interface brief
Interface                  IP-Address      OK? Method Status
Protocol
Embedded-Service-Engine0/0 unassigned      YES unset  administratively down
down
GigabitEthernet0/0         unassigned      YES unset  administratively down
down
GigabitEthernet0/1         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

EAST# show ip interface brief
Interface                  IP-Address      OK? Method Status
Protocol
Embedded-Service-Engine0/0 unassigned      YES unset  administratively down
down
GigabitEthernet0/0         unassigned      YES unset  administratively down
down
GigabitEthernet0/1         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
```

b. Issue the **show interfaces tunnel 0** command to verify the tunneling protocol, tunnel source, and tunnel destination used in this tunnel.

What is the tunneling protocol used? What are the tunnel source and destination IP addresses associated with GRE tunnel on each router?

_____

_____

c. Ping across the tunnel from the WEST router to the EAST router using the IP address of the tunnel interface.

```
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 = 32/34/36 ms
```

d. Use the **traceroute** command on the WEST to determine the path to the tunnel interface on the EAST router. What is the path to the EAST router?

_____

e. Ping and trace the route across the tunnel from the EAST router to the WEST router using the IP address of the tunnel interface.

What is the path to the WEST router from the EAST router?

_____

With which interfaces are these IP addresses associated? Why?

_____

_____

f. The **ping** and **traceroute** commands should be successful. If not, troubleshoot before continuing to the next part.

Part 3: Enable Routing over the GRE Tunnel

In Part 3, you will configure OSPF routing so that the LANs on the WEST and EAST routers can communicate using the GRE tunnel.

After the GRE tunnel is set up, the routing protocol can be implemented. For GRE tunneling, a network statement will include the IP network of the tunnel, instead of the network associated with the serial interface. just like you would with other interfaces, such as Serial and Ethernet. Remember that the ISP router is not participating in this routing process.

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

a. 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.

```
WEST(config)# router ospf 1
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
```

b. 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.

```
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
```

Step 2: Verify OSPF routing.

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

```
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, GigabitEthernet0/1
L        172.16.1.1/32 is directly connected, GigabitEthernet0/1
O        172.16.2.0/24 [110/1001] via 172.16.12.2, 00:00:07, Tunnel0
C        172.16.12.0/30 is directly connected, Tunnel0
L        172.16.12.1/32 is directly connected, Tunnel0
```

What is the exit interface and IP address to reach the 172.16.2.0/24 network?

_____

b. From the EAST router issue the command to verify the route to 172.16.1.0/24 LAN on the WEST router.

What is the exit interface and IP address to reach the 172.16.1.0/24 network?

_____

Step 3: Verify end-to-end connectivity.

a. Ping from PC-A to PC-C. It should be successful. If not, troubleshoot until you have end-to-end connectivity.

Note: It may be necessary to disable the PC firewall to ping between PCs.

b. Traceroute from PC-A to PC-C. What is the path from PC-A to PC-C?

_____

Reflection

1. What other configurations are needed to create a secured GRE tunnel?

   _____

2. If you added more LANs to the WEST or EAST router, what would you need to do so that the network will use the GRE tunnel for traffic?

   _____

   _____