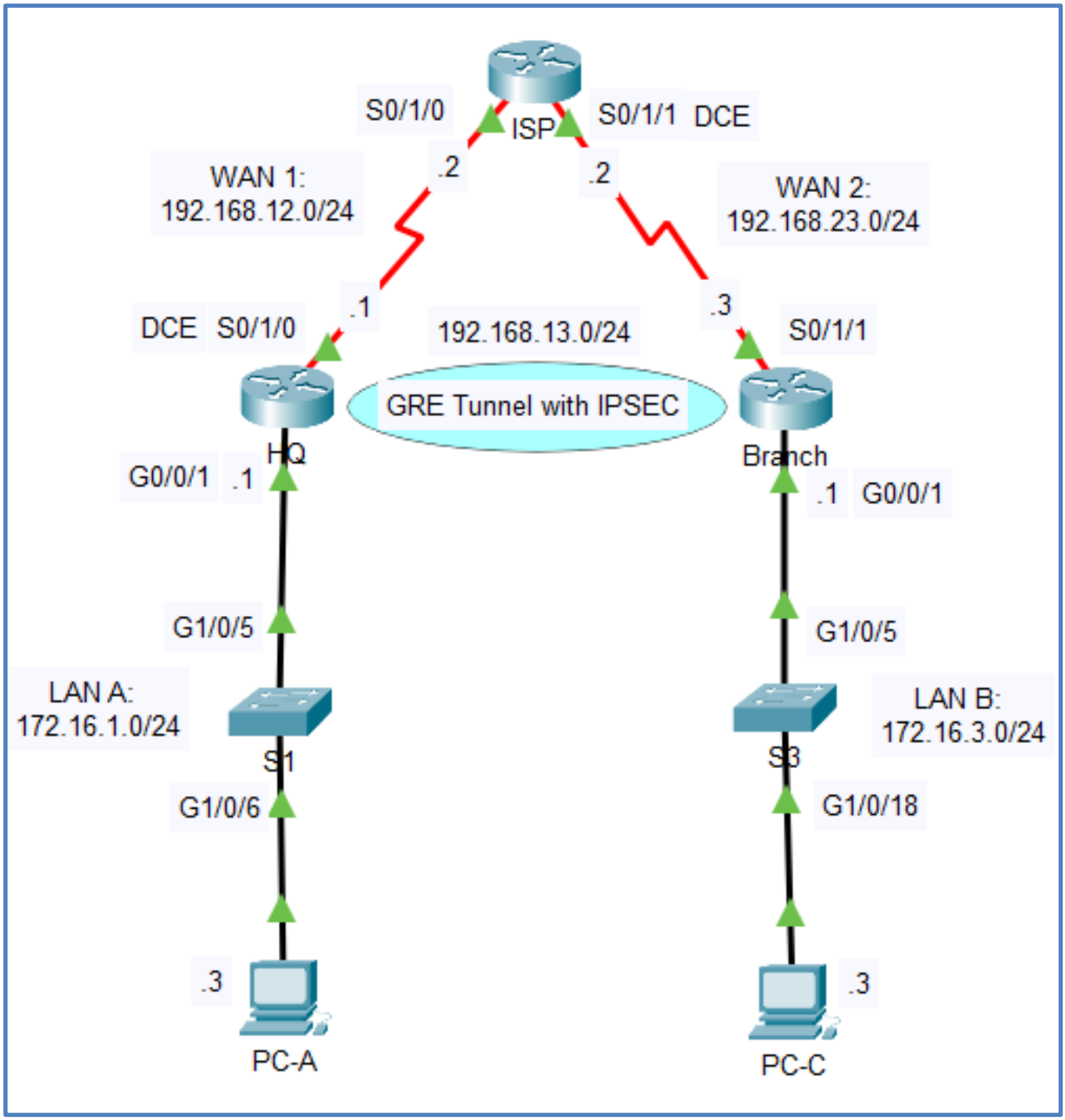
Lab Objective :

Configuring Encrypted GRE Tunnel with IPSEC

Lab – Encrypted GRE Tunnel with IPSEC:

There are two LANs and two WANs in following the topology. Please develop the following topology on the physical pod/rack in the lab room.



Addressing Table

Device	Interface	IP Address	Subnet Mask	Default Gateway
HQ	G0/0/1	172.16.1.1	255.255.255.0	N/A
	S0/1/0 (DCE)	192.168.12.1	255.255.255.0	N/A
	Tunnel 1	192.168.13.1	255.255.255.0	N/A
ISP	S0/1/0	192.168.12.2	255.255.255.0	N/A
	S0/1/1 (DCE)	192.168.23.2	255.255.255.0	N/A
Branch	G0/0/1	172.16.3.1	255.255.255.0	N/A
	S0/1/1	192.168.23.3	255.255.255.0	N/A
	Tunnel 1	192.168.13.3	255.255.255.0	N/A
PC-A	NIC	172.16.1.3	255.255.255.0	172.16.1.1
PC-C	NIC	172.16.3.3	255.255.255.0	172.16.3.1

Objectives

Part 1: Configure Basic Device Settings

Part 2: Configure a GRE Tunnel

Part 3: Enable Routing over the GRE Tunnel

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

Generic Routing Encapsulation (GRE), developed by Cisco, is a versatile tunneling protocol that enables the encapsulation of various network layer protocols within point-to-point links. GRE tunnels are particularly useful for routing unicast, multicast, and broadcast traffic between routers, making them ideal for connecting different sites and supporting routing protocols.

However, one significant drawback of GRE tunneling is that it transmits data in clear text, offering no inherent protection. To address this security concern, Cisco IOS routers can utilize IPSec to encrypt the entire GRE tunnel. This combination ensures a secure and protected site-to-site connection.

When packets need to traverse the Internet or any insecure network, a GRE tunnel creates a virtual pathway between two endpoints (typically Cisco routers), allowing the packets to be sent securely through this tunnel. It's crucial to understand that while GRE encapsulates the packets with a GRE header, it does not encrypt them. For data confidentiality, IPSec must be configured alongside GRE. This transforms a standard GRE tunnel into a secure VPN GRE tunnel, providing the necessary data protection.

Many might assume that a GRE IPSec tunnel between two routers is akin to a site-to-site IPSec VPN (crypto), but there are key differences. One major distinction is that GRE tunnels support the traversal of multicast packets, whereas IPSec VPNs do not. This capability makes GRE tunnels particularly advantageous in large networks where routing protocols like OSPF and EIGRP are essential. Additionally, GRE tunnels are generally easier to configure, which is why network engineers often favor them over IPSec VPNs.

In this lab. we will create a GRE tunnel between the HQ and Branch router and ensure that the 172.16.1.0 /24 and 172.16.3.0 /24 can reach each other while all traffic between the two networks is encrypted with IPSEC.

Note: The routers used with CCNA Packet Tracer hands-on labs are Cisco 4331 Integrated Services Routers (ISRs) with Cisco IOS Release 17.6+ image. The switches used in Packet Tracer are Cisco Catalyst 1000 series with Cisco IOS Release 15.1+ 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. If you are unsure, contact your instructor.

Required Resources

- 3 Routers (Cisco 4331 with Cisco IOS Release 17.6+ image)
- 2 Layer-3/Multilayer Switches (Cisco Catalyst 1000 Series with Cisco IOS Release 15.1+ image)
- 2 PCs (Windows with terminal emulation program)
- Console cables to configure the Cisco IOS devices via the console ports
- Ethernet and serial cables as shown in the topology

Part 1: Configure Basic Device Settings

Part 2: Configure a GRE Tunnel

In Part 2, you will configure a GRE tunnel between the HQ and Branch routers.

Task 1: Configure the GRE tunnel interface.

Task 2: Verify that the GRE tunnel is functional.

Part 3: Enable Routing over the GRE Tunnel

In Part 3, you will configure OSPF routing so that the LANs on the HQ and Branch 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.

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

Task 2: Verify OSPF routing.

Step 1: From the HQ router, issue the **show ip route ospf** command to verify the OSPF neighbor adjacency.

Part 4: Configure IPSEC

Task 1: Configure an ISAKMP Policy.

Step 1: Don't forget to configure the pre-shared key on both routers. The word "PASS" is used as a pre-shared key on both routers.

Step 2: Now in the next step an IPSEC transform-set called as "TRANS" will be created, that specifies ESP AES 256 and HMAC-SHA Authentication will be used.

Step 3: Now a crypto map called "MYMAP" will be created that tells the router what traffic to encrypt and what transform-set to use:

Step 4: In the above configuration the access-list 100 is being referred but never created. Now access-list 100 needs to be created. In access-list 100, the permit statement will be used to only match GRE traffic.

Step 5: Now the final step is to activate crypto map by applying it to the appropriate interfaces.

Step 6: Now some traffic will be sent between the 172.16.1.0/24 and 172.16.3.0/24 to see if it's getting encrypted or not.