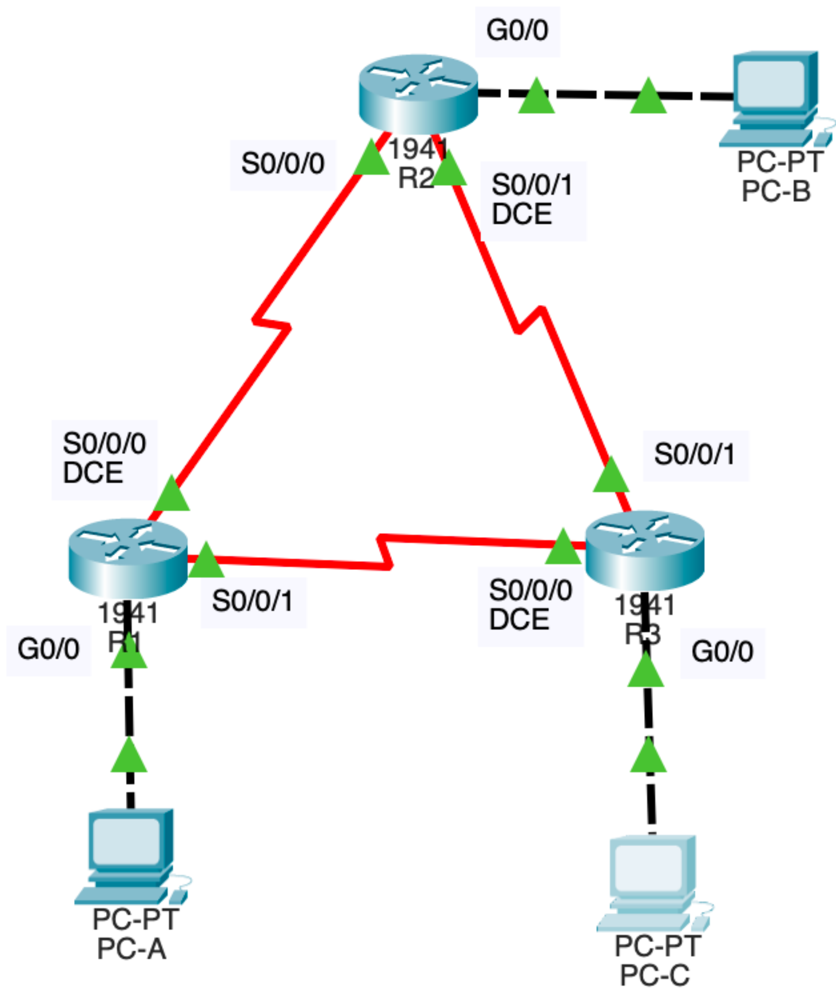
Lab 2: Configuring Basic EIGRP for IPv4

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 (DCE)	10.1.1.1	255.255.255.252	N/A
	S0/0/1	10.3.3.1	255.255.255.252	N/A
R2	G0/0	192.168.2.1	255.255.255.0	N/A
	S0/0/0	10.1.1.2	255.255.255.252	N/A
	S0/0/1 (DCE)	10.2.2.2	255.255.255.252	N/A
R3	G0/0	192.168.3.1	255.255.255.0	N/A

	S0/0/0 (DCE)	10.3.3.2	255.255.255.252	N/A
	S0/0/1	10.2.2.1	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

Objectives

1. Build the network and verify connectivity.
2. Configure EIGRP routing.
3. Verify EIGRP routing.
4. Configure bandwidth and passive interfaces.

Background / Scenario

Enhanced Interior Gateway Routing Protocol (EIGRP) is a powerful distance vector routing protocol and is relatively easy to configure for simple networks.

In this lab, you will configure EIGRP for the above topology and networks. You will modify the bandwidth and configure passive interfaces to allow EIGRP to function more efficiently.

Part 1: Build the Network and Verify Connectivity

In this part, you will set up the network topology in Packet Tracer and configure basic settings, such as the interface IP addresses, device access, and passwords.

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

Build a Packet Tracer network model using the Cisco 1941 routers, as shown in the diagram. You will first need to install a wide-area interface module in the routers. Use the HWIC-2T module and install it in slot 0 on the routers. Slot 0 is to the right when looking at the back of the device. Using slot 0 means the names of the serial interfaces will be Serial0/0/0 (or S0/0/0 as an abbreviation) and Serial0/0/1 (or S0/0/1). If you put the module in the other slot, the names of the interfaces change, making it harder for the instructor to evaluate your work.

When connecting the wide area link, *use the red “lightning bolt” cable that includes the clock*. **Make the DCE connection first**. You will later configure that end to be the “Data Communications Equipment” end of the connection. In real life, both routers at the end of a wide-area link would be connected to a CSU/DSU that converts the local data stream to a format suitable for long-distance transmission. The CSU/DSU would be the DCE, and the router would always be “Data Terminal Equipment” (DTE). However, in the Packet Tracer simulation (and with real devices in the lab), we will configure one of the routers to play the role of the DCE so that we do not need to include simulated CSU/DSUs in the model.

Use cross-over cables (dotted black lines) to connect the PCs to the routers. Although it is not technically necessary since Cisco devices have intelligent interfaces that can adapt to different cable configurations, it is more appropriate to cross over the lines when connecting an end system directly to a router.

Step 2: Configure PC hosts.

Configure the IP addresses, netmasks, and default gateways for the three PCs according to the addressing table above.

Step 3: Initialize and reload the routers if necessary.

This step is only necessary if you use physical devices to ensure that the routers start from a pristine initial configuration. If you are using Packet Tracer, this step is not needed.

Step 4: Configure basic settings for each router.

For each router, configure the *basic settings* as described in this document. You only need to configure the settings described in the Global and Console Access sections. We will use these settings as a standard starting point for most routers and switches we configure in this class. The basic settings provide a baseline level of functionality and access control that should be applied everywhere. Be sure to use the passwords provided so your instructor will be able to get access to your devices to evaluate their configuration.

Use the command **copy running-config startup-config** once you have configured a device to save your configuration. If you don't do this, you will lose configuration information after the device reboots.

Step 5: Configure network interfaces on the routers.

Configure the network interfaces on the routers according to the information in the addressing table above. Here are the commands needed for R1. The other routers are similar but with adjustments to the interface names and addresses.

```
R1(config)# interface GigabitEthernet0/0
R1(config-if)# ip address 192.168.1.1 255.255.255.0
R1(config-if)# no shutdown
R1(config-if)# exit
R1(config)# interface Serial0/0/0
R1(config-if)# ip address 10.1.1.1 255.255.255.252
R1(config-if)# clock rate 128000
R1(config-if)# no shutdown
R1(config-if)# exit
R1(config)# interface Serial0/0/1
R1(config-if)# ip address 10.3.3.1 255.255.255.252
R1(config-if)# no shutdown
R1(config-if)# exit
R1(config)# exit
R1# copy running-config startup-config
```

Record the commands you use for all three routers to include in your lab report. The clock rate must be set on the DCE side of the wide-area connections. For R1 above, the interface that needs the clock rate setting is Serial0/0/0. However, for the other routers, it might be a different interface.

Step 6: Verify connectivity.

The routers should be able to ping one another, and each PC should be able to ping its default gateway. The PCs can ping other PCs once EIGRP routing is configured. Verify this behavior and troubleshoot if necessary.

Part 2: Configure EIGRP Routing

In this part, you will configure the routers to use EIGRP routing. This will allow the PCs to ping each other despite being on different subnetworks.

Step 1: Enable EIGRP routing on R1. Use AS number 64496.

```
R1(config)# router eigrp 64496
```

The autonomous system number 64496 is in a special range of AS numbers reserved for documentation and testing purposes. Using a number from that range is appropriate since we do not intend to refer to any real-world entity. The range of 16-bit AS numbers reserved in this way is 64496—64511. There is a similar reserved range of 32-bit AS numbers (65536—65551) and a separate private use range of 32-bit AS numbers.

Step 2: Advertise the directly connected networks on R1 using the wildcard mask.

```
R1(config-router)# network 10.1.1.0 0.0.0.3
R1(config-router)# network 192.168.1.0 0.0.0.255
R1(config-router)# network 10.3.3.0 0.0.0.3
```

Why is it a good practice to use wildcard masks when advertising networks? Could the mask have been omitted from any of the network statements above? If so, which one(s)?

Step 3: Enable EIGRP routing and advertise the directly connected networks on R2 and R3.

Repeat the commands from the previous part on the other routers, R2 and R3. Be sure to adjust the addresses appropriately. Use the same autonomous system number for all routers. The intent is for the entire network to be in the same autonomous system. Include the commands you used in your lab report.

Step 4: Verify end-to-end connectivity.

The PCs should be able to ping each other if EIGRP is configured correctly. Verify that this is true. If everything works as expected, save the running configuration to the startup configuration on each router to "lock in" the configuration and preserve it over a router reboot.

It is best to do this only after you have verified the correct operation of the system. If you make a mistake, you can reboot the routers to restore them to a previous "known good" configuration.

Part 3: Verify EIGRP Routing

In this part, you will inspect information about the EIGRP routing to verify that it behaves as expected.

Step 1: Examine the EIGRP neighbor table.

On R1, issue the **`show ip eigrp neighbors`** command to verify that the adjacency has been established with its neighboring routers. Record the neighbor table for your report. Do the IP addresses for the neighbors make sense?

Step 2: Examine the IP EIGRP routing table.

On R1, issue the **`show ip route eigrp`** command to verify the routes created by EIGRP in the routing table. Note that a code letter of 'D' means an EIGRP route. Record the routing table for your report. Why does R1 have two paths to the 10.2.2.0/30 network? Is there an entry in the routing table to tell R1 how to forward packets destined to 192.168.2.3 (PC-B)? Which entry is it? There are two ways packets could go from R1 to PC-B, but only one routing table entry exists. Why?

Step 3: Examine the EIGRP topology table.

On R1, issue the **`show ip eigrp topology`** command to view the EIGRP topology table. Record the neighbor table for your report. How many successors does the 10.2.2.0/30 network have? What are they? How many successors does the 192.168.2.0/24 network have? What are they? Why are there no feasible successors listed in R1's routing table?

Step 4: Verify the EIGRP routing parameters and networks advertised.

On R1, issue the **`show ip protocols`** command to verify the EIGRP routing parameters used. Are the listed networks correct? Is the router ID what you expected?

Part 4: Configure Bandwidth and Passive Interfaces

EIGRP uses a default bandwidth based on the type of interface in the router. In Part 4, you will modify the bandwidth so that the link between R1 and R3 has a lower bandwidth than between R1/R2 and R2/R3. In addition, you will set passive interfaces on each router.

Step 1: Observe the current routing settings.

a. Issue the **show interface Serial0/0/1** command on R1 and note the bandwidth listed (shown as the value of "BW"). You should see 1544 Kbit/sec (or 1.544 Mbit/s, the speed of a T1 line). Notice that the clock rate setting you used when configuring the interface is ignored here.

b. Recheck the routing table by using the **show ip route** command. Notice there are multiple routes listed for the destination network 10.2.2.0/30. Also, notice the routes to the 192.168.2.0/24 and 192.168.3.0/24 networks.

Step 2: Modify the bandwidth on the routers.

a. Modify the bandwidth on R1 for the Serial0/0/1 interface.

```
R1(config)# interface Serial0/0/1
R1(config-if)# bandwidth 64
```

Use the **show interface Serial0/0/1** command again to verify that the change in bandwidth took effect.

b. Reissue the **show ip route** command on R1. What are the differences in the routing table, and why did they occur?

Step 3: Configure the GigabitEthernet0/0 interface as passive on R1, R2, and R3.

A passive interface does not allow outgoing and incoming routing updates over the configured interface. The **passive-interface *interface*** command causes the router to stop sending and receiving Hello packets over an interface; however, the network associated with the interface is still advertised to other routers through the non-passive interfaces. Router interfaces connected to LANs are typically configured as passive to reduce network congestion and improve security.

```
R1(config)# router eigrp 64496
R1(config-router)# passive-interface g0/0

R2(config)# router eigrp 64496
R2(config-router)# passive-interface g0/0

R3(config)# router eigrp 64496
R3(config-router)# passive-interface g0/0
```

Step 4: Verify the passive interface configuration.

Issue a **show ip protocols** command on R1, R2, and R3 and verify that the GigabitEthernet0/0 interface has been configured as passive. Are the appropriate interfaces shown as passive?

Submission

For this lab, submit your final Packet Tracer model with a document that includes the answers to the questions in red. The document can be in PDF, DOCX, TXT, or LibreOffice format (PDF preferred). It is convenient if you submit your material as two separate files.