Name: Irine May R. Ompaling **Student Number:** 202105203
Year & Section: BSIT 3-2 **Date:** January 30, 2024

The small scale and simplicity of this network makes RIP an appropriate routing protocol choice. RIP is easy to set up and manage in small to medium sized networks like this one with only a few routers interconnected by serial and ethernet links. With just 3 routers, RIP's limit of 15 hops between any two endpoints is more than sufficient. The protocol works efficiently in networks with limited subnets and hop counts. The standard /24 subnetting used also allows RIP to perform its automatic summarization successfully. Additionally, RIP is tried and tested on common layer 2 interfaces like ethernet and serial links which are exclusively used in this topology. The modest overhead of RIP updates is not a concern on the low bandwidth WAN serial connections. Since there are no special requirements like unequal cost routing stated, RIP's basic distance vector algorithm is adequate for routing traffic between the few subnets. Troubleshooting RIP also leverages simple show and debug commands familiar to most network engineers. Given these factors, RIP makes sense as an easy to manage, lightweight dynamic routing protocol tailored for small network designs like this one. RIP's simplicity, standard feature set and wide vendor support allows it to effectively route traffic between the routers and subnets in this basic topology.

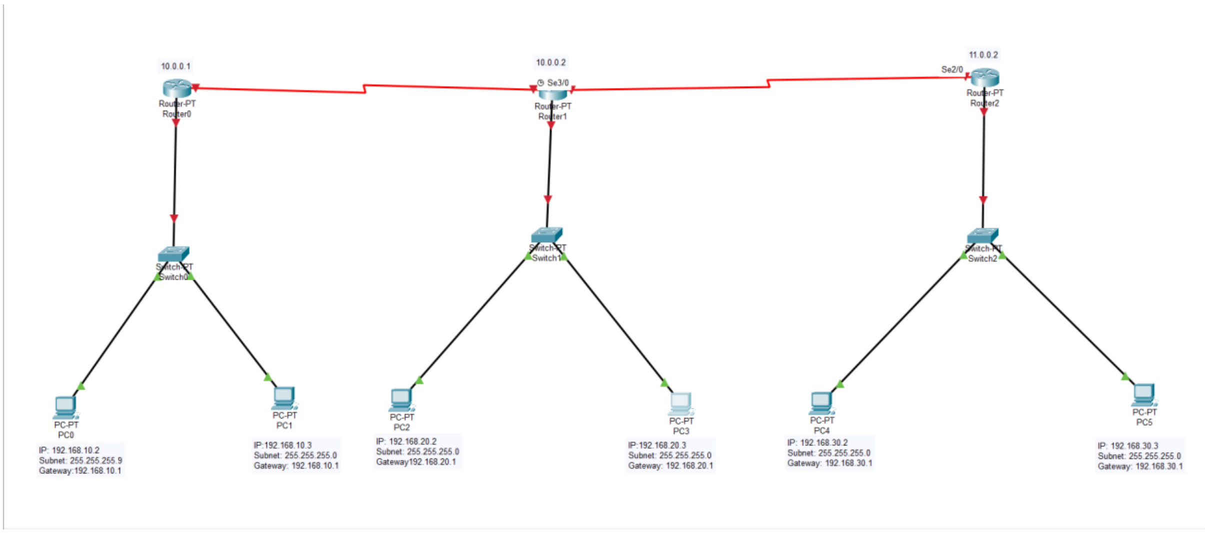

Figure 1: Network Topology of Routing Information Protocol (RIP)

The figure 1 topology shows a basic network setup with 3 routers (Router0, Router1, Router2) interconnected through serial links. There are also 4 PCs (PC0, PC1, PC2, PC3) connected to the network. Each PC is connected via an ethernet link to one of the router interfaces. The diagram uses standard symbols to depict the devices - a rectangle for the router, triangle for the serial WAN links between routers, and a square/circle for the PCs. The IP addresses assigned to each interface on the routers and PCs are noted. This defines the network subnets and host addressing used. For example, Router0's ethernet interface connecting to PC0 has an IP of 192.168.10.1/24. This means it is part of the 192.168.10.0/24 subnet. PC0 then has an IP address from this same subnet - 192.168.10.2/24.

The serial links between the routers also have IP addresses from different subnet ranges - 10.0.0.0/24 between Router0 and Router1, and 11.0.0.0/24 between Router1 and Router2.

This topology demonstrates how routers interconnect multiple LAN subnets where the PCs reside, using serial links over the WAN. The IP addressing scheme defines the various subnets. By analyzing the IP addressing and interfaces, we can understand the path that packets will take from a source PC to a destination PC, traversing multiple routers hops over serial and ethernet links.

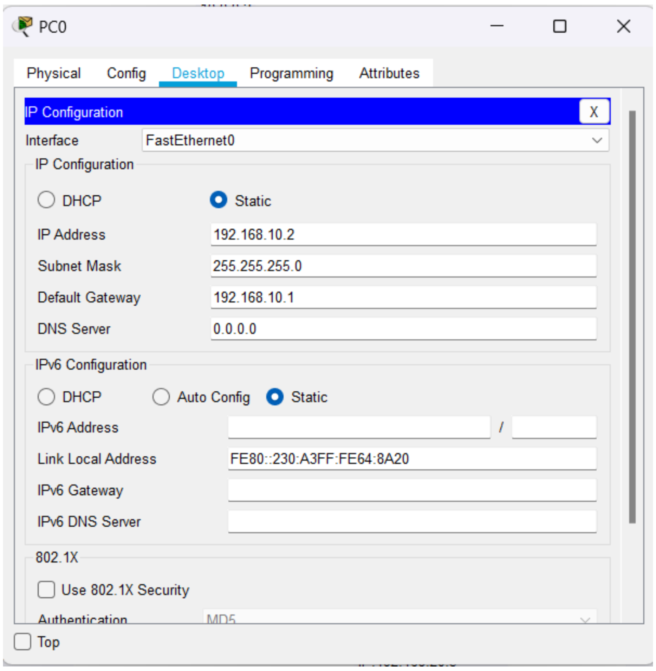

Figure 2: Network Topology of Routing Information Protocol (RIP)

The given topology diagram shows 4 PCs (PC0, PC1, PC2, PC3) connected to 3 routers (Router0, Router1, Router2) that are configured with RIP routing protocol. Before routing can work properly, the PCs need to be assigned IP addresses and subnet masks from their respective subnet ranges. For example, PC0 connects to Router0's ethernet interface with subnet 192.168.10.0/24. So PC0 needs to be configured with an IP address like 192.168.10.2 and subnet mask 255.255.255.0 from that range. This can be configured directly through the desktop GUI on the PC under IPv4 settings. Alternatively, the ipconfig command can be used on the PC's command prompt: ipconfig 192.168.10.2 255.255.255.0 This assigns the IP address 192.168.10.2/24 to PC0's ethernet interface. Similarly, PC1 can be assigned an address from its connecting subnet of 192.168.20.0/24 like 192.168.20.2/24. PC2 and PC3 will get addresses from 192.168.30.0/24 and 192.168.40.0/24 subnets respectively based on their router connections. The default gateway on each PC should also be configured as the IP address of the router interface in the same subnet. This allows the PCs to communicate with other networks through their default gateway router which has RIP enabled. Proper IP addressing of hosts in this way is crucial for successful routing between the PCs across different subnets using RIP.

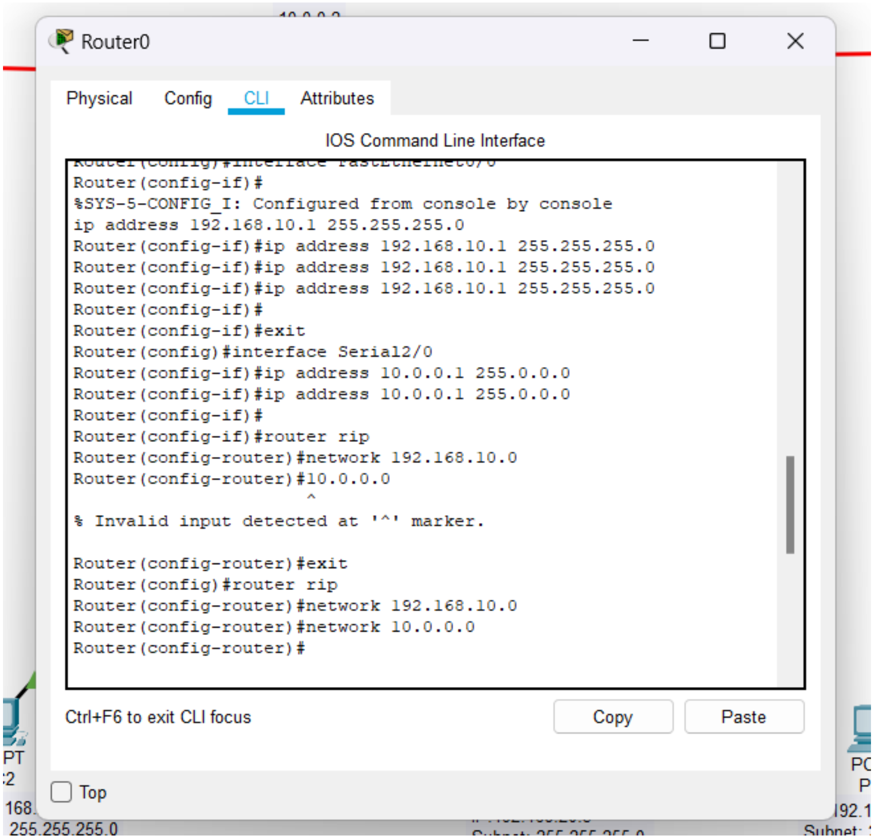

Figure 3: Routing on the routers of Routing Information Protocol (RIP)

In order to enable RIP routing on the routers, we first need to determine the directly connected networks on each router that need to participate in RIP routing. This is done by examining the interface IP addresses and subnets configured on each router. For example, Router0 has two directly connected networks - 192.168.10.0/24 and 10.0.0.0/24 based on its interface IP addresses. After identifying the directly connected networks, we need to enable the RIP routing process on each router and specify these network addresses using the 'network' command under router rip configuration mode.

For example on Router0, we enable RIP routing by entering the 'router rip' command and then specify the two connected networks 192.168.10.0/24 and 10.0.0.0/24 using the 'network' command. This tells Router0 to enable RIP on these interfaces and advertise these networks via RIP. The same process is repeated on Router1 and Router2, specifying their respective directly connected networks. By configuring RIP network statements like this, the routers will now have knowledge of the various subnets in the topology via RIP advertisements, and will be able to build routing tables to reach remote networks. This allows IP communication throughout the topology across multiple router hops, rather than just between directly connected subnets.

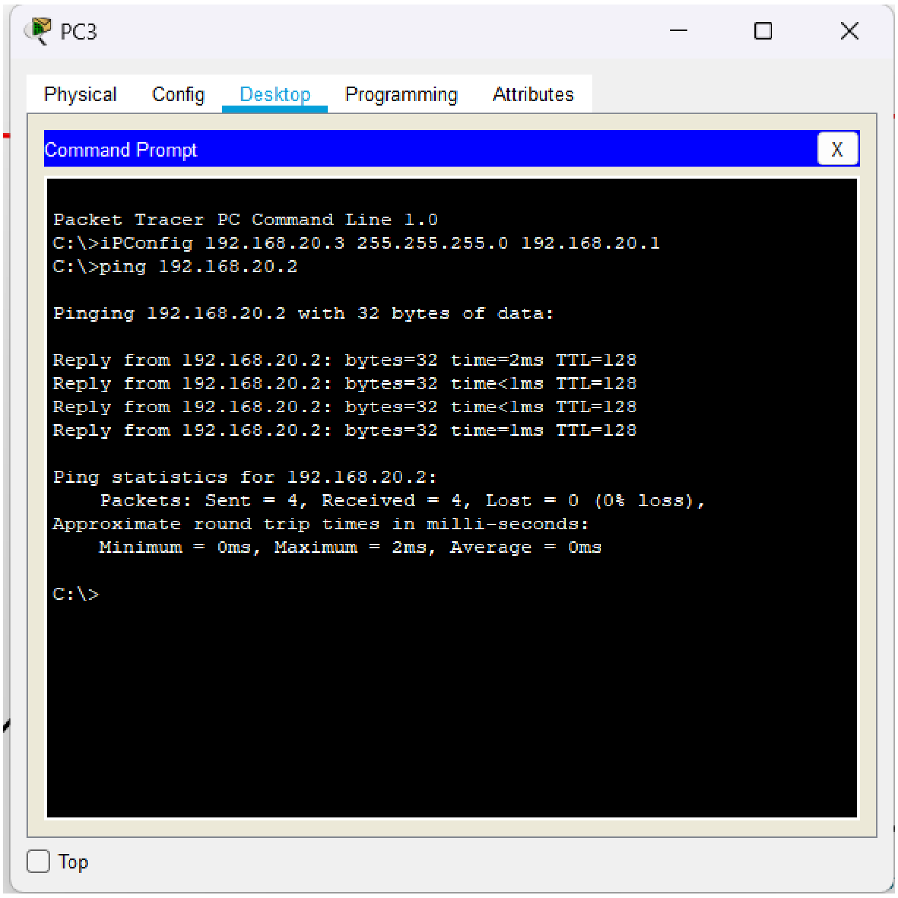

Figure 4: Pinging in Routing Information Protocol (RIP)

To verify end-to-end connectivity, we can ping from a host like PC3 to the IP address of another host in a different subnet, such as PC2. On PC3, we open up the command prompt and type 'ping' followed by the IP address of PC2.The ping command will send echo request packets that will be routed across the network to the destination host. If connectivity and routing is working correctly, PC2 will respond with echo reply packets back to PC3. Successful ping results with replies received back confirms that the path between the two hosts across the network is up. If ping fails, it indicates a problem exists somewhere in the network that is preventing ICMP packets from being exchanged.