TRIBHUVAN UNIVERSITY

Institute of Engineering

Central Campus, Pulchowk

Pulchowk, Lalitpur

Computer Network

Lab 6: Dynamic Routing using RIP

Submitted by:

Mamata Maharjan (077BCT043)

Group (B)

Submitted to:

Department of Electronics and Computer Engineering,

Pulchowk Campus

Submission Date: July 8, 2024

LAB No: 6

Dynamic Routing using RIP

Objectives:

- To be familiar with dynamic routing and configuration with dynamic routing
- To be familiar with supernetting and classless addressing

Environmental Setup:

- Network simulation tool: Packet Tracer

Theory:

Routing Information Protocol (RIP) is one of the oldest and most straightforward distance-vector routing protocols used in computer networks to facilitate the dynamic routing of IP traffic. As a distance-vector protocol, RIP determines the best path to a destination based on the distance, measured in hop count, to that destination. Each hop represents a pass through a router, and RIP limits the maximum number of hops allowed in a path from source to destination to 15. This limit helps prevent routing loops but also confines RIP to smaller networks.

RIP operates by periodically broadcasting its entire routing table to its immediate neighbors every 30 seconds. This periodic update ensures that routing tables remain consistent across the network. When a RIP-enabled router starts up, it sends out a request packet to ask for the routing tables of neighboring routers. Upon receiving a request, RIP routers respond with their routing table information. They also send their entire routing table to all neighbors at regular intervals. When a router receives routing information from a neighbor, it compares the received information with its existing routing table. If the received route is better, i.e., has a lower hop count, the routing table is updated accordingly.

RIP includes mechanisms such as split horizon, route poisoning, and hold-down timers to prevent routing loops, ensuring stable and reliable network routing. However, if a route is not refreshed within 180 seconds, it is marked as invalid. After 240 seconds, the route is removed from the routing table, a process that helps maintain the accuracy and reliability of routing information within the network.

Despite its simplicity and ease of configuration, RIP has several limitations. The 15-hop limit restricts its use to smaller networks, making it unsuitable for large or complex network environments. Additionally, RIP has slower convergence times compared to more advanced protocols like OSPF (Open Shortest Path First) or EIGRP (Enhanced Interior Gateway Routing Protocol), meaning it can take longer to adapt to network changes. The periodic broadcasting of the entire routing table can also lead to unnecessary traffic on the network, especially if the network is large.

Configuring RIP on Cisco routers is straightforward. For example, enabling RIP version 2 and specifying the networks for RIP to advertise can be done with a few commands. Using the command `no auto-summary` prevents RIP from automatically summarizing subnets into major network boundaries, providing more granular control over routing updates.

In summary, RIP is a simple and effective routing protocol for smaller networks, offering ease of configuration and robust loop prevention mechanisms. However, its scalability issues, slower convergence times, and inefficient use of network resources make it less suitable for large or highly dynamic network environments.

Task Performed and Observations:

Activity A:

[1 - 2]The network was configured using Cisco Packet Tracer according to the given topology. The routers were named `Mamata_1`, `Mamata_2`, `Mamata_3`, and `Mamata_4`. Each router's hostname, console password, enable password, and Telnet access were configured. The console password was set to `cisco` and the enable password to `class`. Telnet was enabled with the password `cisco`, allowing for remote management.

[3] Each interface on the routers was configured with the appropriate IP addresses as specified in the topology diagram. For instance, `Mamata_1` had the IP addresses 202.60.1.1/24 and 202.60.2.1/24, while `Mamata_2` had 202.60.3.1/24 and 202.60.4.1/24. The computers within the network were also configured with the correct IP addresses, subnet masks, and default gateways to ensure proper communication within the network.

[4 - 8] The `show ip route` command was executed on each router to verify the routing table entries. The output from `Mamata_1` displayed directly connected routes for the 202.60.1.0/24 and 202.60.2.0/24 networks. Similarly, the other routers showed their respective connected networks. These outputs confirmed that the initial configuration of the network interfaces was successful. Ping tests were conducted from PC0 to various devices within the network, including Server0, Server1, PC1, PC2, PC3, Router0, Router1, Router2, and Router3. The tests confirmed that all devices were reachable, indicating that the network was functioning correctly. Similar tests from PC1 verified connectivity to all other computers, servers, and routers in the network.

[9 - 12] To enable dynamic routing, RIP version 2 was configured on each router. Starting with `Mamata_1`, Telnet was used to access the router and configure RIP. The network 202.60.0.0 was added to the RIP routing process, and auto-summarization was disabled to ensure precise routing information. This configuration was repeated for `Mamata_2`, `Mamata_3`, and `Mamata_4`. After configuring RIP, the `show ip route` command was run again on each router. The routing tables now included RIP-learned routes, showing the dynamic updates between routers. For example, `Mamata_1` had entries for the networks 202.60.3.0/24 and 202.60.4.0/24 learned via RIP, indicating that RIP was functioning as intended.

[13] Finally, the `tracert` command was executed from PC0 to the IP address 1.1.1.1 to observe the path taken by packets through the network. The trace showed the packets traversing through the routers `Mamata_1`, `Mamata_2`, and `Mamata_3` before reaching the destination, verifying the correct configuration of the routing paths.

Activity B:

To increase the reliability of the network, a new router was added to connect Switch0 with Switch1 as depicted in Figure 2. This router was configured with IP addresses for both interfaces: 202.60.1.2/24 and 202.60.5.1/24. The Routing Information Protocol (RIP) was also configured on this new router to dynamically manage routing information.

An example **tracert command** outputs are shown below for PC0:

Source-> Destination	Route
PC0 -> PC1	Mamata_0 -> Mamata_01 -> PC1
PC0 -> PC5	Mamata_0 -> Mamata_01 -> Mamata_01 -> PC5
PC0 -> PC3	Mamata_0 I Mamata_04 -> PC3

Here after the new router (Mamata_04) was introduced when tracert was commanded from PC0 to PC3, the routing paths configured on the routers preferred the route through Router 4. If static routes were configured, they might not always reflect the shortest physical path but follow the manually defined paths. But here dynamic routing protocols (like OSPF, EIGRP, etc.) are used, so the protocol determines the best path based on its algorithm.

[3] The show ip route of all the routers after connections,

```
     202.60.0.0/24 is variably subnetted, 2 subnets, 2 masks
C       202.60.0.0/24 is directly connected, GigabitEthernet0/0
L       202.60.0.1/32 is directly connected, GigabitEthernet0/0
     202.60.1.0/24 is variably subnetted, 2 subnets, 2 masks
C       202.60.1.0/24 is directly connected, GigabitEthernet0/1
L       202.60.1.1/32 is directly connected, GigabitEthernet0/1
R    202.60.2.0/24 [120/1] via 202.60.1.2, 00:00:16, GigabitEthernet0/1
R    202.60.3.0/24 [120/1] via 202.60.1.2, 00:00:16, GigabitEthernet0/1
R    202.60.4.0/24 [120/2] via 202.60.1.2, 00:00:16, GigabitEthernet0/1
R    202.60.5.0/24 [120/2] via 202.60.1.2, 00:00:16, GigabitEthernet0/1
                   [120/2] via 202.60.0.10, 00:00:04, GigabitEthernet0/0
R    202.60.6.0/24 [120/1] via 202.60.0.10, 00:00:04, GigabitEthernet0/0
```

After disconnection

```
Gateway of last resort is not set

     202.60.0.0/24 is variably subnetted, 2 subnets, 2 masks
C       202.60.0.0/24 is directly connected, GigabitEthernet0/0
L       202.60.0.1/32 is directly connected, GigabitEthernet0/0
R    202.60.3.0/24 [120/3] via 202.60.0.10, 00:00:04, GigabitEthernet0/0
R    202.60.4.0/24 [120/3] via 202.60.0.10, 00:00:04, GigabitEthernet0/0
R    202.60.5.0/24 [120/2] via 202.60.0.10, 00:00:04, GigabitEthernet0/0
R    202.60.6.0/24 [120/1] via 202.60.0.10, 00:00:04, GigabitEthernet0/0
```

After disconnecting Mamata_0 and Mamata_01

Source-> Destination	Route
PC0 -> PC1	Mamata0 -> Mamata_04 -> Mamata_03 -> Mamata_02 -> Mamata_01 -> PC1
PC0 -> PC5	Mamata0 -> Mamata_04 -> Mamata_03 -> Mamata_02 -> PC1

[4 - 5] Various links between routers were removed and reconnected to observe the impact on the routing tables and traceroute outputs. Each router's routing table was dynamically updated by RIP to reflect the optimal paths based on the current network topology. These observations confirmed that the dynamic routing protocol effectively handled changes and maintained network connectivity. The final notes highlighted how the dynamic routing protocol, specifically RIP, managed the network topology changes.

By continuously updating the routing tables and determining the optimal paths for data packets, the protocol ensured efficient and reliable network performance. The traceroute results showed that the packets consistently found the best paths, even when the network configuration changed.

Activity C:

[**Initial Evaluation and Allocations**] Based on the CIDR (slash notation) for the subnet mask, the given IP address of 200.50.40.0 /23 provided by APNIC (Asia Pacific Network Information Center) . It indicated that there can be a total of 510 usable hosts. And needs to be divided for different departments A, B, C, D, E and F, each department having 60, 70, 50, 10, 40 and 20 numbers of hosts respectively and G, H, and I having only two hosts in each.

In order to divide the provided IP address space into a hierarchy of subnets of different sizes, VLSM (Variable Length Subnet Mask) can be used which makes it possible to create subnets with very different host counts.

Available addresses (2^9 = 512) > Required addresses (70 + 60 + 50 + 40 +20 + 10 + 3 *2 = 256)

For the network topology as directed in labsheet, following would be the division of IP addresses:

Departments	Hosts	Network Address	Broadcast Address	Subnet Mask
B	70	222.22.22.0	222.22.22.127	255.255.255.128
A	60	222.22.22.128	222.22.22.191	255.255.255.192
C	50	222.22.22.192	222.22.22.255	255.255.255.192
E	40	222.22.23.0	222.22.23.63	255.255.255.192
F	20	222.22.23.64	222.22.2395	255.255.255.224
D	10	222.22.23.96	222.22.23.111	255.255.255.240
G	2	222.22.23.112	222.22.23.115	255.255.255.252
H	2	222.22.23.116	222.22.23.119	255.255.255.252
I	2	222.22.23.120	222.22.23.123	255.255.255.252

[1-4] The network has been configured according to the specified topology in Figure 3, where each network segment uses one PC connected to a router via a switch. The routers have been assigned hostnames based on my first name: Mamata_1, Mamata_2, and so on. For security purposes, a console password (cisco) and an enable password (class) have been set on each router. Additionally, Telnet access has been enabled on all routers, secured with the password cisco.

In alignment with the designed subnet, each router interface has been assigned appropriate IP addresses and subnet masks. Correspondingly, each PC has been configured with the necessary IP address, subnet mask, and default gateway to ensure seamless communication within the network.

The configuration has been verified using the show ip route command on each router, and the resulting routing tables confirm that the network routes have been properly established. The following are the details of the show ip route command outputs for each router:

Router Mamata_0

```
       +   periodic downloaded static route

Gateway of last resort is not set

     222.22.22.0/24 is variably subnetted, 3 subnets, 2 masks
C       222.22.22.0/25 is directly connected, FastEthernet1/0
C       222.22.22.128/26 is directly connected, FastEthernet0/0
C       222.22.22.192/26 is directly connected, FastEthernet2/0
     222.22.23.0/30 is subnetted, 1 subnets
C       222.22.23.112 is directly connected, Serial4/0
```

Router Mamata_01

```
Gateway of last resort is not set

     222.22.23.0/24 is variably subnetted, 4 subnets, 3 masks
C       222.22.23.0/26 is directly connected, FastEthernet2/0
C       222.22.23.96/28 is directly connected, FastEthernet0/0
C       222.22.23.112/30 is directly connected, Serial1/0
C       222.22.23.116/30 is directly connected, Serial3/0

Mamata_01#
```

Router Mamata_02

```
       P - periodic downloaded static route

Gateway of last resort is not set

     222.22.23.0/24 is variably subnetted, 3 subnets, 2 masks
C       222.22.23.64/27 is directly connected, FastEthernet0/0
C       222.22.23.116/30 is directly connected, Serial1/0
C       222.22.23.120/30 is directly connected, Serial2/0

Mamata_02#
```

Router Mamata_04

```
Gateway of last resort is not set

C    1.0.0.0/8 is directly connected, FastEthernet1/0
     222.22.23.0/30 is subnetted, 1 subnets
C       222.22.23.120 is directly connected, Serial2/0
```

[5-6] The following are the details of the show ip route command outputs for each router after version 2 RIP setup:

Mamata_0

```
Gateway of last resort is not set

R    1.0.0.0/8 [120/3] via 222.22.23.114, 00:00:18, Serial4/0
     222.22.22.0/24 is variably subnetted, 3 subnets, 2 masks
C       222.22.22.0/25 is directly connected, FastEthernet1/0
C       222.22.22.128/26 is directly connected, FastEthernet0/0
C       222.22.22.192/26 is directly connected, FastEthernet2/0
     222.22.23.0/24 is variably subnetted, 6 subnets, 4 masks
R       222.22.23.0/26 [120/1] via 222.22.23.114, 00:00:18, Serial4/0
R       222.22.23.64/27 [120/2] via 222.22.23.114, 00:00:18, Serial4/0
R       222.22.23.96/28 [120/1] via 222.22.23.114, 00:00:18, Serial4/0
C       222.22.23.112/30 is directly connected, Serial4/0
R       222.22.23.116/30 [120/1] via 222.22.23.114, 00:00:18, Serial4/0
R       222.22.23.120/30 [120/2] via 222.22.23.114, 00:00:18, Serial4/0
 --More--
```

Mamata_01

```
Gateway of last resort is not set

R    1.0.0.0/8 [120/2] via 222.22.23.118, 00:00:26, Serial3/0
R    222.22.22.0/24 [120/1] via 222.22.23.113, 00:00:17, Serial1/0
     222.22.23.0/24 is variably subnetted, 6 subnets, 4 masks
C       222.22.23.0/26 is directly connected, FastEthernet2/0
R       222.22.23.64/27 [120/1] via 222.22.23.118, 00:00:26, Serial3/0
C       222.22.23.96/28 is directly connected, FastEthernet0/0
C       222.22.23.112/30 is directly connected, Serial1/0
C       222.22.23.116/30 is directly connected, Serial3/0
R       222.22.23.120/30 [120/1] via 222.22.23.118, 00:00:26, Serial3/0

Mamata_01>
```

Mamata_02

```
R    1.0.0.0/8 [120/1] via 222.22.23.122, 00:00:17, Serial2/0
R    222.22.22.0/24 [120/2] via 222.22.23.117, 00:00:19, Serial1/0
     222.22.23.0/24 is variably subnetted, 6 subnets, 4 masks
R       222.22.23.0/26 [120/1] via 222.22.23.117, 00:00:19, Serial1/0
C       222.22.23.64/27 is directly connected, FastEthernet0/0
R       222.22.23.96/28 [120/1] via 222.22.23.117, 00:00:19, Serial1/0
R       222.22.23.112/30 [120/1] via 222.22.23.117, 00:00:19, Serial1/0
C       222.22.23.116/30 is directly connected, Serial1/0
C       222.22.23.120/30 is directly connected, Serial2/0

Mamata_02>
```

Mamata_03

```
Gateway of last resort is not set

C    1.0.0.0/8 is directly connected, FastEthernet1/0
R    222.22.22.0/24 [120/3] via 222.22.23.121, 00:00:01, Serial2/0
     222.22.23.0/24 is variably subnetted, 6 subnets, 4 masks
R       222.22.23.0/26 [120/2] via 222.22.23.121, 00:00:01, Serial2/0
R       222.22.23.64/27 [120/1] via 222.22.23.121, 00:00:01, Serial2/0
R       222.22.23.96/28 [120/2] via 222.22.23.121, 00:00:01, Serial2/0
R       222.22.23.112/30 [120/2] via 222.22.23.121, 00:00:01, Serial2/0
R       222.22.23.116/30 [120/1] via 222.22.23.121, 00:00:01, Serial2/0
C       222.22.23.120/30 is directly connected, Serial2/0
```

[7 - 9] The traceroute for various source destination:

Source-> Destination	Route
Network A -> Network B	Mamata_0 -> Network B
Network A -> Network D	Mamata_0 -> Mamata_01 -> Network D
Network A -> Network F	Mamata_0 -> Mamata_01 -> Mamata_02 -> Network F
Network A -> ISP	Mamata_0 -> Mamata_01 -> Mamata_02 -> Mamata_03 -> Network ISP

[8 - 10] After setting all the ip route of the routers to default and direct the traffic towards ISP router, the show ip route command had following outputs

Mamata_0

```
Gateway of last resort is 1.1.1.1 to network 0.0.0.0

R    1.0.0.0/8 is possibly down, routing via 222.22.23.114, Serial4/0
     222.22.22.0/24 is variably subnetted, 3 subnets, 2 masks
C       222.22.22.0/25 is directly connected, FastEthernet1/0
C       222.22.22.128/26 is directly connected, FastEthernet0/0
C       222.22.22.192/26 is directly connected, FastEthernet2/0
     222.22.23.0/24 is variably subnetted, 6 subnets, 4 masks
R       222.22.23.0/26 is possibly down, routing via 222.22.23.114, Serial4/0
R       222.22.23.64/27 is possibly down, routing via 222.22.23.114, Serial4/0
R       222.22.23.96/28 is possibly down, routing via 222.22.23.114, Serial4/0
C       222.22.23.112/30 is directly connected, Serial4/0
R       222.22.23.116/30 is possibly down, routing via 222.22.23.114, Serial4/0
R       222.22.23.120/30 is possibly down, routing via 222.22.23.114, Serial4/0
S*   0.0.0.0/0 [1/0] via 1.1.1.1
```

Mamata_01

```
       P - periodic downloaded static route

Gateway of last resort is 1.1.1.1 to network 0.0.0.0

R    1.0.0.0/8 is possibly down, routing via 222.22.23.118, Serial3/0
R    222.22.22.0/24 is possibly down, routing via 222.22.23.113, Serial1/0
     222.22.23.0/24 is variably subnetted, 6 subnets, 4 masks
C       222.22.23.0/26 is directly connected, FastEthernet2/0
R       222.22.23.64/27 is possibly down, routing via 222.22.23.118, Serial3/0
C       222.22.23.96/28 is directly connected, FastEthernet0/0
C       222.22.23.112/30 is directly connected, Serial1/0
C       222.22.23.116/30 is directly connected, Serial3/0
R       222.22.23.120/30 is possibly down, routing via 222.22.23.118, Serial3/0
S*   0.0.0.0/0 [1/0] via 1.1.1.1

Mamata_01#
```

Mamata_02

```
       P - periodic downloaded static route

Gateway of last resort is 1.1.1.1 to network 0.0.0.0

R    1.0.0.0/8 is possibly down, routing via 222.22.23.122, Serial2/0
R    222.22.22.0/24 is possibly down, routing via 222.22.23.117, Serial1/0
     222.22.23.0/24 is variably subnetted, 6 subnets, 4 masks
R       222.22.23.0/26 is possibly down, routing via 222.22.23.117, Serial1/0
C       222.22.23.64/27 is directly connected, FastEthernet0/0
R       222.22.23.96/28 is possibly down, routing via 222.22.23.117, Serial1/0
R       222.22.23.112/30 is possibly down, routing via 222.22.23.117, Serial1/0
C       222.22.23.116/30 is directly connected, Serial1/0
C       222.22.23.120/30 is directly connected, Serial2/0
S*   0.0.0.0/0 [1/0] via 1.1.1.1

Mamata_02#
```

Mamata_03

```
Gateway of last resort is 1.1.1.1 to network 0.0.0.0

C    1.0.0.0/8 is directly connected, FastEthernet1/0
R    222.22.22.0/24 is possibly down, routing via 222.22.23.121, Serial2/0
     222.22.23.0/24 is variably subnetted, 6 subnets, 4 masks
R       222.22.23.0/26 is possibly down, routing via 222.22.23.121, Serial2/0
R       222.22.23.64/27 is possibly down, routing via 222.22.23.121, Serial2/0
R       222.22.23.96/28 is possibly down, routing via 222.22.23.121, Serial2/0
R       222.22.23.112/30 is possibly down, routing via 222.22.23.121, Serial2/0
R       222.22.23.116/30 is possibly down, routing via 222.22.23.121, Serial2/0
C       222.22.23.120/30 is directly connected, Serial2/0
S*   0.0.0.0/0 [1/0] via 1.1.1.1
```

And the tracert had the similar output as that of the above version 2 RIP.

Exercise:

1. What is dynamic routing? How does it differ with static routing? Explain briefly.

Dynamic routing is a method in which routers automatically exchange routing information and adjust to changes in the network topology without manual intervention. This is achieved using routing protocols such as RIP, OSPF, or BGP. In contrast, static routing requires the network administrator to manually configure and update routing entries on each router. While static routing is simpler and provides more control, it is not scalable for large or frequently changing networks. Dynamic routing, on the other hand, offers flexibility and scalability, adapting to changes such as link failures or the addition of new routers by automatically recalculating the best paths for data packets.

2. List out the dynamic routing configuration commands of the router (that you have used in this lab) for RIP as well as RIP version 2 with the syntax and examples.

To configure RIP and RIP version 2 in a router, the following commands are used:

RIP Configuration:

Router(config)# router rip

Router(config-router)# network [network-address]

Router(config-router)# network [another-network-address]

Example:

Router(config)# router rip

Router(config-router)# network 202.60.0.0

Router(config-router)# network 202.60.1.0

RIP Version 2 Configuration:

Router(config)# router rip

Router(config-router)# version 2

Router(config-router)# no auto-summary

Router(config-router)# network [network-address]

Router(config-router)# network [another-network-address]

Example:

Router(config)# router rip

Router(config-router)# version 2

Router(config-router)# no auto-summary

Router(config-router)# network 222.22.22.0

Router(config-router)# network 222.22.23.0

3. How can dynamic routing address the changing topology of a network automatically? Explain with reference to the observation of your lab exercise.

Dynamic routing protocols like RIP automatically adjust to changes in the network topology by exchanging routing information between routers. During the lab exercise, various scenarios, such as disconnecting and reconnecting links between routers, demonstrated how RIP dynamically updated the routing tables to reflect the best available paths. When a link was disconnected, the routers recalculated the routes and updated their tables to route traffic through alternative paths. This automatic adjustment ensures continuous network connectivity and optimal routing, showcasing the robustness and efficiency of dynamic routing in managing network changes without manual reconfiguration.

LAB No: 5
Subnetting & Supernetting

Objectives:

- To be familiar with subnetting with FLSM and VLSM
- To be familiar with supernetting and classless addressing

Environmental Setup:

- Network simulation tool: Packet Tracer

Theory:

Routing involves directing data packets from a source to a destination through a network. Routers use routing tables and algorithms to determine the best path for data transmission. There are two main types of routing:

1. Static Routing:

   This type of routing are manually configured by network administrators and provides fixed routes to network destinations. Simplicity and security are some advantages of the static routing while its scalability for larger networks and requiring manual updates are its disadvantages.

2. Dynamic Routing:

Task Performed and Observations:

Activity A:

[1, 2] - The network topology was created and the IP addresses of the PCs were assigned as directed and the subnet mask of all these PCs were set to 255.255.255.0. Then the connectivity of all the computers were tested using the ping command, which showed proper connectivity between the computers.

[3, 5] - Now the subnetting mask of all computers was changed to 255.255.255.192. The ping command showed a proper connectivity between the PC1, PC2 and PC3 but the PC4 seemed to be disconnected. Again, the subnet mask of all the computers was changed to 255.255.255.224. The ping command showed connection between PC1 and PC2 but PC3 and PC4 seemed to have been disconnected from the network. Finally the subnet mask of all the computers was changed to 255.255.255.240. The ping command clearly demonstrated that only a single PC1 was connected to the network and all other computers were disconnected.

The reason these PCs were disconnected is because of the limited ip addresses that could be used as per the subnet mask. For example, when the subnet mask was changed to 255.255.255.240 (11111111.11111111.11111111.11110000), the last 4 bits of this address gave the range of host that could be used with in the network i.e. the number of hosts per subnet is given as

2^(32-28) - 2 = 2^4 - 2 = 16 - 2 = 14 hosts

These 14 hosts can have usable IP addresses from x.x.x.1 to x.x.x.14 And only PC1 has an IP address (202.22.22.11) that lies within the range of usable IP addresses, PC1 is connected to the network (belongs to the subnet) and other PCs with out of the range IP Addresses are disconnected from the network (belongs to a different subnet) even though they have a visible physical connection through switches.

[6, 7] - The **central switch was then replaced by a router i.e. Router0,** The hostname of the router was configured as Mavis021 and its interfaces were configured with directed IP addresses and subnet mask. Then each computer was configured with a default gateway i.e IP address of the corresponding interface of the router. The connectivity of each computer to all other computers were tested using the ping command. All the pings across PCs were successful even though they all belonged to different subnets.

Activity B:

[1] - The network topology was created and the IP addresses of the PCs were assigned as directed and the subnet mask of all these PCs were set to 255.255.255.0. Then the connectivity of all the computers were tested using the ping command, but all the pings replied **Request Time Out** indicating these PCs were not within the connectivity even though they were connected physically.

[2, 4] - The subnet mask of all the computers was now changed to 255.255.254.0. The ping command replied ‘ request time out ‘ for other PCs but showed proper connectivity for **PC1 and PC2**. Now when changing the subnet mask to 255.255.252.0, the ping command displayed the connectivity between **PC1, PC2 and PC3** but replied ‘ request time out ‘ for the PC4. Finally, the subnet mask of all the computers were replaced with 255.255.248.0, this time all the PCs were connected to a single subnet and were able to communicate with each other.

Activity C:

[**Initial Evaluation and Allocations**] Based on the CIDR (slash notation) for the subnet mask, the given IP Address 200.70.90.0 /24 belongs to class C. It indicated that there can be a total of 254 usable hosts. But we are assigned a task to divide this address range equally for different departments A, B, C, D and two networks E & F for interconnection between routers. In other words, these departments are divided into different subnets from the provided class C IP address.

Given 6 different departments, borrowing 3 bits (11111111.11111111.11111111.11100000) from the host portion will provide us with 8 networks and 30 hosts i.e. (8 - 2=6) usable ip addresses. Allocating the IP address range for each of the departments:

Departments	Binary	Network Address	Broadcast Address	Subnet Mask
A	.00100000	202.70.90.32	202.70.90.63	255.255.255.224
B	.01000000	202.70.90.64	202.70.90.95	255.255.255.224
C	.01100000	202.70.90.96	202.70.90.126	255.255.255.224
D	.10000000	202.70.90.128	202.70.90.159	255.255.255.224
E	.10100000	202.70.90.160	202.70.90.191	255.255.255.224
F	.11000000	202.70.90.192	202.70.90.223	255.255.255.224

Assuming the number of hosts to be the same in all the subnets, the division has been made with a Fixed Length Subnet Mask technique. The router interfaces have following addresses:

FastEthernet	Routers		
	Mamata_01	Mamata_02	Mamata_03
0/0	202.70.90.33	202.70.90.194	202.70.90.161
1/0	202.70.90.65	202.70.90.162	102.70.90.161
2/0	202.70.90.97	202.70.90.129	------
3/0	202.70.90.193	------	------

Let each department (subnets) be represented by a single pc, the ip addresses of each pc or router connected to the route interfaces are assigned as below:

FastEthernet	PC/next hop Addresses at the router interface		
	Mamata_01	Mamata_02	Mamata_03
0/0	202.70.90.34	202.70.90.193	202.70.90.162
1/0	202.70.90.66	202.70.90.161	102.70.90.162
2/0	202.70.90.98	202.70.90.130	------
3/0	202.70.90.194	------	------

Now configuring static routing in between each of the department's networks as well as to the Internet via ISP Router, For router Mamata_01

```
102.70.90.160 [1/0] via 202.70.90.194
202.70.90.128 [1/0] via 202.70.90.194
```

For router Mamata_02

```
102.0.0.0/27 is subnetted, 1 subnets
   102.70.90.160 [1/0] via 202.70.90.161
202.70.90.0/27 is subnetted, 6 subnets
   202.70.90.32 [1/0] via 202.70.90.193
   202.70.90.64 [1/0] via 202.70.90.193
                [1/0] via 202.70.90.33
   202.70.90.96 [1/0] via 202.70.90.193
                [1/0] via 202.70.90.33
```

For router Mamata_03

```
202.70.90.0/27 is subnetted, 5 subnets
   202.70.90.32 [1/0] via 202.70.90.162
   202.70.90.64 [1/0] via 202.70.90.162
   202.70.90.96 [1/0] via 202.70.90.162
   202.70.90.128 [1/0] via 202.70.90.162
```

[1] The internetwork is all set and done, the connectivity of networks with each other was tested using ping command which showed a 'Request Time Out' for the first packet on the first ping and then displayed a proper connectivity afterwards. The first packet went time out because the ARP message was taking a long time to identify the mac address of the destination device but once the mac address was known it had a smooth packed flow from the next time.

[2] The output of the traceroute from computers connected to the network presented the number of hops it took to reach to the destination. For instance, the tracert command from the PCA (network A) took a **single hop** to get to the department that belonged to the same network such as PCB and PCC and took **3 hops** to get to PCD and **4 hops** to move out of the ISP Router.

[3] When tracerouting to the destination address of 103.5.150.3, it reached the destination from PCA in 4 hops following Mamata_01 -> Mamata_02 -> Mamata_03 -> 103.5.150.3

Activity D:

[**Initial Evaluation and Allocations**] The IP address of 200.50.40.0 /23 was provided by APNIC (Asia Pacific Network Information Center) And needs to be divided for different departments A, B, C, D, E and F, each having 100, 40, 50, 60, 12 and 20 number of hosts respectively and G, H, and I having only two hosts in each.

In order to divide the provided IP address space into a hierarchy of subnets of different sizes, VLSM (Variable Length Subnet Mask) can be used which makes it possible to create subnets with very different host counts.

Available addresses (2^9 = 512) > Required addresses (100 + 60 + 50 + 40 +20 + 12 + 3 *2 = 288)

For the network topology as directed in labsheet, following would be the division of IP addresses:

Departments	Hosts	Network Address	Broadcast Address	Subnet Mask
A	100	200.50.40.0	200.50.40.127	255.255.255.128
D	60	200.50.40.128	200.50.40.191	255.255.255.192
C	50	200.50.40.192	200.50.40.255	255.255.255.192
B	40	200.50.41.0	200.50.41.63	255.255.255.192
F	20	200.50.41.64	200.50.41.95	255.255.255.224
E	12	200.50.41.96	200.50.41.111	255.255.255.240
G	2	200.50.41.112	200.50.41.115	255.255.255.252
H	2	200.50.41.116	200.50.41.119	255.255.255.252
I	2	200.50.41.120	200.50.41.123	255.255.255.252

Now configuring the network interfaces as follows:

FastEthernet	Routers			
	Mamata_01	Mamata_02	Mamata_03	Mamata_03
0/0	200.50.40.1	200.50.41.114	200.50.41.118	200.50.41.125
1/0	200.50.41.1	200.50.41.97	200.50.41.65	103.5.150.4
2/0	200.50.40.193	200.50.41.117	200.50.41.124	---
3/0	200.50.41.113	200.50.40.129	---	---

Similarly the computers representing each network has the following IP addresses:

Networks	IP Address	Default Gateway
PCA	200.50.40.2	200.50.40.1
PCB	200.50.41.2	200.50.41.1
PCC	200.50.40.194	200.50.40.193
PCD	200.50.41.130	200.50.41.129
PCE	200.50.41.98	200.50.41.97
PCF	200.50.41.66	200.50.41.65
PCOuter	103.5.150.3	103.5.150.4

Finally configuring the IP route for all the routers.

When configuring the IP route it was realized that the network D and network B both have 62 usable range but have subnet masks of /26 each. Network B had its network address as 202.50.41.0 which separated it from other networks that used the same router. In order to be able to use a **route aggregation technique** the Ip Addresses assigned to B and D were **switched.**

Now the three networks connected to Mamata_01 are:

[A] - 200.50.40.0/25 (128 addresses)

[B] - 200.50.40.128/26 (64 addresses)

[C] - 200.50.40.192/26 (64 addresses)

The range from 200.50.40.0 to 200.50.40.255 can be represented as a single /24 network. With this configuration, any packet from the networks 200.50.40.0/25, 200.50.40.128/26, and 200.50.40.192/26 destined for a network outside of these subnets will use the summarized route and be forwarded to the next hop IP address 200.50.41.114.

Hence, IP route configuration

For router Mamata_01 can be performed as:

```
%No matching route to delete
Mamata_01(config)#no ip route 200.50.40.0 255.255.255.0 200.50.41.114
Mamata_01(config)#ip route 200.50.41.0 255.255.255.0 200.50.41.114
Mamata_01(config)#ip route 103.5.150.0 255.255.255.0 200.50.41.114
Mamata_01(config)#
```

For router Mamata_02:

```
Enter configuration commands, one per line.  End with CNTL/Z.
Mamata_02(config)#ip route 200.50.40.0 255.255.255.0 200.50.41.113
Mamata_02(config)#ip route 200.50.41.64 255.255.255.224 202.50.41.118
Mamata_02(config)#ip route 103.5.150.0 255.255.255.0 202.50.41.118
Mamata_02(config)#
```

For router Mamata_03:

```
Mamata_03(config)#ip route 200.50.40.0 255.255.255.0 200.50.41.117
Mamata_03(config)#ip route 200.50.41.0 255.255.255.192 200.50.41.117
Mamata_03(config)#ip route 200.50.41.96 255.255.255.240 200.50.41.117
Mamata_03(config)#ip route 103.5.150.0 255.255.255.0 200.50.41.122
Mamata_03(config)#
```

For router Mamata_04:

```
Mamata_04(config)#ip route 200.50.40.0 255.255.255.0 200.50.41.121
Mamata_04(config)#ip route 200.50.41.0 255.255.255.0 200.50.41.121
Mamata_04(config)#
```

[1] The internetwork is all set and done, the connectivity of networks with each other was tested using ping command which showed a 'Request Time Out' for the first packet on the first ping and then displayed a proper connectivity afterwards. The first packet went time out because the ARP message was taking a long time to identify the mac address of the destination device but once the mac address was known it had a smooth packed flow from the next time.

[2] The output of the traceroute from computers connected to the network presented the number of hops it took to reach to the destination. For instance, the tracert command from the PCA (network A) took a **single hop** to get to the department that belonged to the same network such as PCB and PCC and took **3 hops** to get to PCD and PCE, took 4 hops to get to PCF and **5 hops** to move out of the ISP Router.

[3] When tracerouting to the destination address of 103.5.150.3, it reached the destination from PCA in 5 hops following Mamata_01 -> Mamata_02 -> Mamata_03 -> Mamata_04 -> 103.5.150.3

Exercise:

1. What is a Subnet Mask? Why is it Used? Explain with Examples.

   A subnet mask is a 32-bit number used in IP networking to divide an IP address into a network and host portion. It helps determine which part of an IP address refers to the network and which part refers to the host.

   Example:

   - IP Address: `192.168.1.10`

   - Subnet Mask: `255.255.255.0`

   In binary:

   - IP Address: `11000000.10101000.00000001.00001010`

   - Subnet Mask: `11111111.11111111.11111111.00000000`

   The first 24 bits (the network portion) are masked (indicated by the subnet mask's 1s), and the last 8 bits (the host portion) are left for host addresses.

2. What is Subnetting with FLSM and Subnetting with VLSM? Mention Their Importance in Networking with Suitable Examples.

   Subnetting is the process of dividing a larger network into smaller, more manageable sub-networks (subnets). In Fixed Length Subnet Masking (FLSM), all subnets created are of equal size. This method is simple to implement and manage but can lead to inefficient use of IP addresses.

   - Example: Dividing a `192.168.1.0/24` network into four subnets with a `255.255.255.192` subnet mask, each subnet has 64 addresses.

   In contrast, Variable Length Subnet Masking (VLSM) allows for subnets of different sizes, which makes more efficient use of IP addresses by assigning address spaces according to the specific needs of each subnet.

- Example: Dividing a `192.168.1.0/24` network into subnets with different masks, such as `192.168.1.0/26` (64 addresses), `192.168.1.64/26` (64 addresses), `192.168.1.128/27` (32 addresses), and so on.

Importance:

- FLSM: Easier to manage but can lead to wasted IP addresses.

- VLSM: Maximizes IP address usage, suitable for networks of varying sizes.

3. What is Classless Routing? Why is it Important in the Internet System? Explain with Suitable Examples.

   Classless routing, which uses CIDR (Classless Inter-Domain Routing), allocates IP addresses and routing without adhering to the traditional classful network boundaries (A, B, C classes). This flexibility prevents the wastage of IP addresses and supports the growth of the Internet. For example, a classful network might allocate a 192.168.0.0/24 network for an office that only needs 10 addresses, wasting the remaining addresses. With classless routing, a 192.168.0.0/28 network can be allocated, providing precisely 16 addresses, thus avoiding wastage. Classless routing's ability to allocate addresses efficiently and flexibly is crucial for managing the growing number of devices and networks on the Internet.

Conclusion:

This Lab Exercise was really helpful for understanding how Subnet masks help in defining network boundaries, while subnetting (both FLSM and VLSM) enables efficient use of IP addresses. And how Classless routing further enhances flexibility and efficiency.

LAB No: 1
Network Cables

Objectives:

- To be familiar with UTP cable, RJ-45 connector, Crimping tool and color coding of UTP network cable
- To be familiar with preparation of straight through and crossover cables and their uses

Equipment Required:

- Piece of UTP (Ethernet) cable
- RJ-45 jacks
- RJ-45 crimper
- LAN tester
- PCs
- Hub/Switch

Theory:

T568A and T568B are two widely used color codes for wiring eight-position RJ45 modular plugs. Both codes are allowed under the ANSI/TIA-568.2-D wiring standards, but they differ in their pin assignments for the green and orange pairs.

Differences between T568A and T568B:

- The main difference between T568A and T568B is the pin assignment for the green and orange pairs.
- T568A assigns the green pair to pins 1 and 2, while T568B assigns the green pair to pins 2 and 3.
- Similarly, T568A assigns the orange pair to pins 3 and 6, while T568B assigns the orange pair to pins 1 and 6.

The color codes for T568A and T568B:

T568A Color Code	T568B Color Code
Pin 1: White/Green Pin 2: Green Pin 3: White/Orange Pin 4: Blue Pin 5: White/Blue Pin 6: Orange Pin 7: White/Brown Pin 8: Brown	Pin 1: White/Orange Pin 2: Orange Pin 3: White/Green Pin 4: Blue Pin 5: White/Blue Pin 6: Green Pin 7: White/Brown Pin 8: Brown

Both T568A and T568B are compatible with each other, and either standard can be used in most cases. However, T568A is more commonly used in European and Pacific countries, while T568B is more widely used in the United States.

Straight-through Cable:

When two RJ-45 connectors of a cable are held side by side in the same orientation. Straight-through cable is used to connect a computer to a router, a switch to a hub, or a device to a network interface card (NIC).

Crossover cable:

When the RJ-45 connectors on both ends show that some of the wires are connected to different pins on each side of the cable i.e. the pins 1 and 2 on one connector connect to pins 3 and 6 on the other and vice versa. It is used to connect two computers, two switches, or a computer to a switch.

Exercises:

1. *Why is the use of color coding recommended while preparing a network cable? Explain the color coding standards of UTP cable.*

   The use of color coding is recommended while preparing a network cable as it helps in easy identification and differentiation of different pairs of wires within the cable. And also the color coding standards ensure consistency and standardization across network installations and help in maintaining the integrity and functionality of the network connections.

   T568A Color Code:

   Pair 1 (White-Blue, Blue)

   Pair 2 (White-Orange, Orange)

   Pair 3 (White-Green, Green)

   Pair 4 (White-Brown, Brown)

   T568B Color Code:

   Pair 1 (White-Orange, Orange)

   Pair 2 (White-Green, Green)

   Pair 3 (White-Blue, Blue)

   Pair 4 (White-Brown, Brown)

2. *Where do we need straight-through and crossover cable? Discuss briefly*

   Straight-through cables are commonly used to connect host devices, such as computers or servers, to network switches, hubs, or routers. They ensure proper communication between devices operating at different network layers.

On the other hand, crossover cables are used to directly connect similar devices or devices operating at the same network layer. This includes connecting two computers or connecting switches or hubs together. Crossover cables have specific wire pairs that are crossed over or swapped to facilitate effective communication.

3. *Which cable have you prepared during the lab session? How was that tested? Discuss each step.*

I prepared a crossover cable during the lab session following the steps listed below:

- Strip the outer jacket of the Ethernet cable using the wire cutters.
- Untwist each of four pairs and straighten the wires.
- Arrange the wires in the following order from left to right for A : white/green, green, white/orange, blue, white/blue, orange, white/brown, brown and white/orange, orange, white/green, blue, white/blue, green, white/brown, brown for B.
- Trim the wires to ensure they are all the same length, leaving a small portion exposed.
- Insert the wires into the RJ45 connector in the correct order, making sure the wires reach the end of the connector and are aligned properly.
- Use the crimping tool to crimp the connector onto the wires securely.

Afterwards the cable was tested using a cable tester, a diagnostic device to verify the proper connection of a LAN cable. Upon connecting the LAN cable to the tester, the power indicator illuminated, indicating operational functionality. The link indicator displayed a steady light confirming a successful connection between the cable ends. With the sequence of lights corresponding to the individual wires, it was determined that the T568A and T568B wiring standard was followed.

CONCLUSION:

This lab helped us get familiar with the UTP cables and RJ-45 connectors and the preparation of the straight through and crossover cables.

LAB No: 4
Static Routing & Default Route

Objectives:

- To be familiar with Static Routing and its configuration
- To be familiar with default route and its configuration
- To be familiar with route aggregation

Environmental Setup:

- Network simulation tool: Packet Tracer

Theory:

Routing involves directing data packets from a source to a destination through a network. Routers use routing tables and algorithms to determine the best path for data transmission. There are two main types of routing:

3. Static Routing:

   This type of routing are manually configured by network administrators and provides fixed routes to network destinations. Simplicity and security are some advantages of the static routing while its scalability for larger networks and requiring manual updates are its disadvantages.

4. Dynamic Routing:

   These routing techniques learn and update by routers using routing protocols such as OSPF and BGP. It has scalability, adaptability to network changes while it is complex and possesses potential security risks if not properly managed.

Task Performed and Observations:

1. **Activity A:**

   After constructing the network topology as mentioned in the lab sheet all the devices had their host name and passwords configured along. The routes of the network were configured with the mentioned IP addresses and subnet mask. Then all the devices had their subnet mask, ip addresses and default gateway configured.

   Then the ping command was used between the devices and routers in the network but they couldn't communicate with each other. Inorder to solve this issue the routers had their static route for each destinations configured individually. The ping command now was operational or the destinations were alive. And the tracert command displayed the route taken from the source to the destination and it searched for all the possible routes to find the 2.2.2.2 but was unsuccessful.

2. **Activity B:**

   All the static routes configured in activity A were removed using ‘no ip route’ command and the route entities were minimized by using the default route in each router. And the connection between different PCs were tested using the ping command which worked well.

   Then the tracert command gave the route to reach the destination from the source and could not figure out the trace for the unknown address 2.2.2.2.

3. **Activity C:**

   After creating the network topology in the packet tracer, the IP Address and subnet mask of the given computers were assigned and then the hostname and passwords were configured. Then the Interfaces of Routers were configured as directed in the lab sheet.

   The show Ip route command in the routers presented the interface connection configuration of those routers. The ping command showed the live destination for the devices in the local area network and displayed request time out for the ping to another LAN across routers.

Now the default gateway of each of the computers were assigned respectively. The Network 1 and Network 2 that are connected to the same router had the communication going on smoothly but the network 3 was said to be unreachable.

To solve this problem, router0 configured the static route for the destination network as Network 3. And from there router1 was configured to have static route for destination network of Network 1 and Network 2

Now there was a seamless communication between all three networks. The communication was smooth even after altering the static route for the destination network as an aggregation to use a single entry for the route.

Exercise:

1. How does a sending host know whether the destination computer is on the same network or on a different network? Explain.

The sending host uses the subnet mask and the destination IP address to determine if the destination is on the same network or a different network.

2. Explain, how the data is forwarded from sending host in each of the following cases:

a. When the destination computer is within the same network

The data is sent directly to the destination computer using the MAC address.

b. When the destination computer is on the different network

The data is sent to the default gateway, which then forwards it to the appropriate network.

3. What is routing? Discuss static routing and configuration of static routing in a router with its syntax briefly.

Routing is the process of selecting paths in a network along which to send network traffic. Static routing involves manually entering routes, while dynamic routing uses protocols to discover and maintain routes.

`ip route <Destination_Network> <Subnet_Mask> <next_hop_address>

4. What information can we get from the routing table? How can we observe the routing table of a router? Explain.

   The routing table contains network routes, including the destination network, subnet mask, next-hop IP address, and interface. It can be viewed using the ‘ show ip route ‘ command.

5. What is a default route? What is its importance? State the default route configuration command with its syntax.

   A default route is used when no specific route for a destination exists. It ensures packets are forwarded to a default gateway, typically leading to an Internet connection.

   ‘ ip route 0.0.0.0 0.0.0.0 <next-hop-address or outgoing interface>

Conclusion:

This lab exercise helped us get hands-on experience with static and default route configurations, reinforcing the theoretical concepts of routing in computer networks. Through various activities and exercises, the practical understanding of the routing behavior, configuration, and network management was enhanced.