PROGRAM -5:

Aim: To understand the modes of operation in a Router and explore basic Router and Switch commands for configuring and managing network devices.

Theoretical Description:

A Router operates in various modes, each allowing different levels of configuration and command execution. The most common modes in a router are:

1. User EXEC Mode: This is the initial mode when accessing the router, which has limited functionality, mainly for viewing basic information.
    - Prompt: Router>
2. Privileged EXEC Mode: Provides access to all the show commands, debugging, and basic device management commands. You can also enter global configuration mode from here.
    - Prompt: Router#
    - Command to enter: enable
3. Global Configuration Mode: Used to make system-wide configurations. You can configure interfaces, routing protocols, and other features.
    - Prompt: Router(config)#
    - Command to enter: configure terminal
4. Interface Configuration Mode: Used to configure the individual interfaces (ports) of the router.
    - Prompt: Router(config-if)#
    - Command to enter: interface [type/number] (e.g., interface GigabitEthernet0/0)

Switches also have a similar hierarchy of command modes and allow management through VLANs, port configurations, etc.

Algorithm:

1. Access the Router or Switch:
    a. Open a terminal or console session to the Router/Switch.
2. Switch to Privileged EXEC Mode:

a. Enter the enable command to switch from user mode to privileged EXEC mode.

3. Enter Global Configuration Mode:

   a. Use the configure terminal command to enter global configuration mode.

4. Configure Interfaces (For Routers):

   a. Use interface commands to configure IP addresses, enable/disable interfaces, etc.

   b. Example: interface GigabitEthernet0/0

5. View Status and Information:

   a. Use commands like show ip interface brief, show running-config, etc., to view current configurations.

6. Basic Switch Commands:

   a. Set the hostname, password, and manage VLANs.

Output:

1. **Router Hostname Configuration:**

   MyRouter(config)# hostname MyRouter

   MyRouter#

2. **Interface IP Configuration:**

   MyRouter(config-if)# ip address 192.168.1.1 255.255.255.0

   MyRouter(config-if)# no shutdown

3. **Switch VLAN Configuration:**

   MySwitch# show vlan brief

   VLAN Name Status Ports

   ---- -------------------------------- --------- -------------------------------

10 Sales active Fa0/1

4. Interface Status on Router:

MyRouter# show ip interface brief

Interface	IP-Address	OK?	Method	Status	Protocol
GigabitEthernet0/0	192.168.1.1	YES	manual	up	up

Conclusion: In this experiment, we explored the different modes of a router and basic switch commands. We configured a router's hostname, IP address, and interfaces, and also set up VLANs on a switch.

Viva Questions:

1. **What is the difference between User EXEC Mode and Privileged EXEC Mode?**
2. **Why do we use the no shutdown command after configuring an interface?**
3. **What is the purpose of setting a default gateway on a router?**

PROGRAM -6:

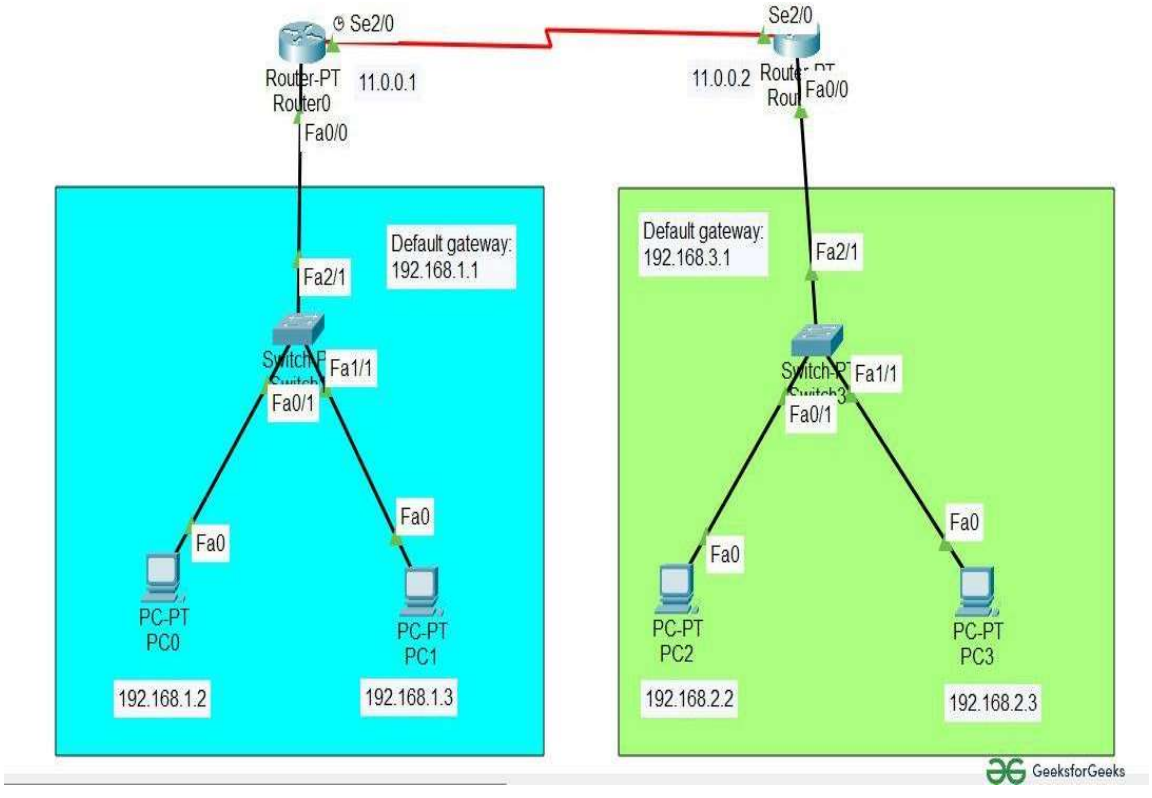
Aim: To configure Static Routing on a network using routers, ensuring data packets are directed to the correct destination networks via predefined paths.

Theoretical Description: Static routing is a routing technique in which a network administrator manually adds routes to a routing table. Unlike dynamic routing protocols, static routing does not adjust automatically to network topology changes. It is commonly used in small, simple networks or where specific routes need to be enforced due to security or performance requirements.

Algorithm:

1. Network Setup:
   - Design the network topology with at least two routers, connected via serial or Ethernet links, along with some end devices (PCs or switches) connected to each router.
2. Access Each Router's CLI:
   - Open the terminal on each router and switch to Privileged EXEC Mode using the enable command.
3. Assign IP Addresses to Router Interfaces:
   - Configure IP addresses for the router interfaces that connect to each other and to the local networks.
4. Define Static Routes:
   - For each network, define the next-hop router IP address (or exit interface) for routing traffic.
5. Test Connectivity:
   - Use the ping and traceroute commands to verify that the devices in different networks can communicate.

Output:



Conclusion: In this experiment, we successfully configured Static Routing between two routers. By defining static routes, we manually instructed each router on how to reach the other network. This allowed communication between devices in different networks.

Viva Questions:

1. **What is the difference between static routing and dynamic routing?**
2. **What are the advantages and disadvantages of static routing?**
3. **Explain the next-hop IP address in static routing.**
4. **How can you verify that a static route has been correctly configured on a router?**

PROGRAM -7:

Aim: To configure Routing Information Protocol (RIP) on a set of routers to enable dynamic routing between multiple networks**.**

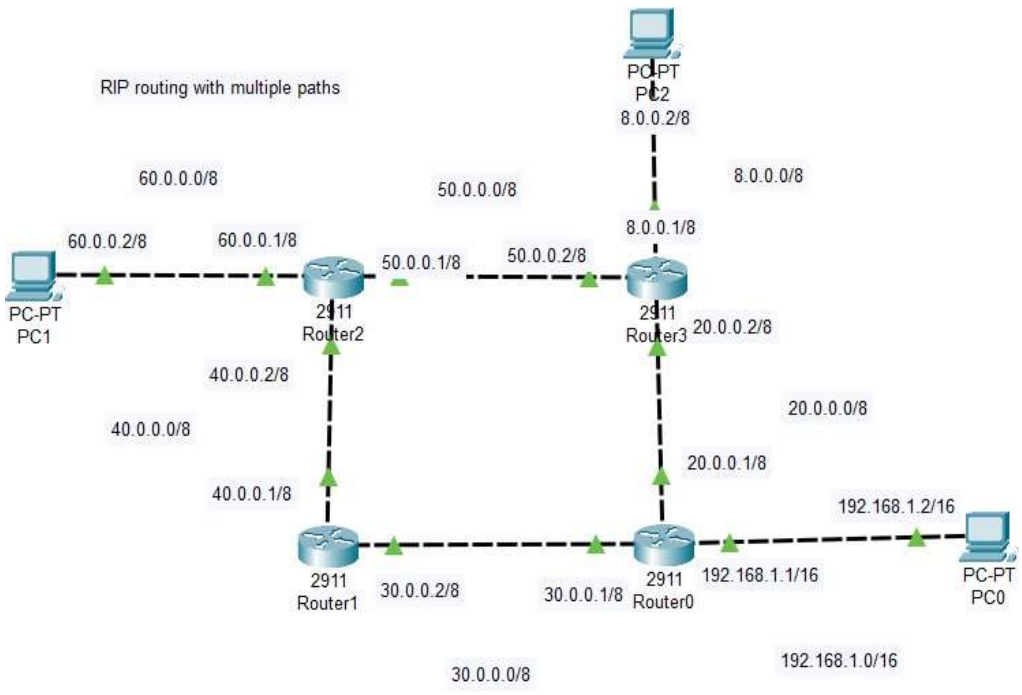
Theoretical Description: Routing Information Protocol (RIP) is a dynamic routing protocol used in local and wide area networks. RIP is a distance-vector routing protocol that uses hop count as the metric for path selection. RIP has two versions, RIPv1 and RIPv2, with some key differences:

- RIPv1: A classful routing protocol that does not support subnet information and works without sending subnet masks, making it unsuitable for Variable Length Subnet Masking (VLSM) or Classless Inter-Domain Routing (CIDR).
- RIPv2: A classless routing protocol that supports subnet masks and includes VLSM and CIDR support. RIPv2 also supports authentication and multicast for route updates.

Algorithm:

1. Setup Network Topology:
    - Design a network with at least two or more routers connected via serial or Ethernet links. Configure IP addresses on each router's interface.
2. Enter Global Configuration Mode:
    - On each router, access the command-line interface (CLI) and switch to privileged EXEC mode.
3. Enable RIP:
    - Enable RIP on each router and specify the version (RIPv1 or RIPv2).
4. Advertise Networks:
    - For each router, advertise the connected networks so RIP can propagate the routes dynamically.
5. Verify Configuration:
    - Check that the routers have dynamically learned the routes from other routers using the RIP protocol.

Output:



Conclusion: In this experiment, we configured both RIPv1 and RIPv2. RIPv1 does not support subnetting, which limits its usefulness in modern networks. RIPv2, however, is classless and supports VLSM and CIDR, making it more flexible. By configuring RIP, we were able to dynamically propagate routes between routers and verify communication between different networks.

Viva Questions:

1. **What is the maximum hop count allowed by RIP?**
2. **Explain the differences between RIPv1 and RIPv2.**
3. **Why is RIPv1 considered a classful routing protocol?**
4. **What are the limitations of RIPv1 in modern networks?**

PROGRAM -8:

Aim: To configure Open Shortest Path First (OSPF) routing protocol on multiple routers in a network and troubleshoot common OSPF configuration issues.

Theoretical Description: OSPF (Open Shortest Path First) is a link-state routing protocol used in Internet Protocol (IP) networks to find the best path for data to travel. OSPF is more efficient and scalable compared to distance-vector routing protocols like RIP. It is widely used in both small and large enterprise networks and is part of the Interior Gateway Protocol (IGP) suite.

Algorithm:

1. Define Network Topology:

a. Create a network with at least two routers connected via serial or Ethernet links. Each router should be connected to end devices like PCs or switches.

2. Configure IP Addresses:

a. Assign IP addresses to all router interfaces connecting them to each other and to local networks.

3. Enable OSPF:

a. On each router, enable OSPF, assign a process ID, and specify the OSPF area (typically Area 0).

4. Advertise Networks:

a. Use the network command to define the networks that OSPF will advertise to other routers.

5. Verify and Troubleshoot:

a. Check OSPF neighbors, routing tables, and troubleshoot any connectivity issues.

Output:

Conclusion: In this experiment, we successfully configured OSPF on multiple routers and dynamically propagated routes between them. OSPF's link-state nature ensures fast convergence and efficient path selection based on the cost metric. Additionally, we troubleshooted common OSPF configuration errors, such as incorrect network statements, mismatched OSPF timers, and neighbor adjacency issues.

Viva Questions:

1. **What is the main difference between OSPF and RIP?**
2. **How does OSPF calculate the best route?**
3. **What is the purpose of the OSPF area and why is Area 0 important?**
4. **Explain the difference between OSPF broadcast and non-broadcast networks.**
5. **What is the hello and dead interval in OSPF, and why are they important?**

PROGRAM -9:

Aim: To configure VLAN (Virtual Local Area Network) on a switch and verify its functionality by assigning ports to different VLANs. Additionally, troubleshoot VLAN-related issues to ensure proper network segmentation**.**

Theoretical Description: VLAN (Virtual Local Area Network) is a logical grouping of devices within a network that allows segmentation of a network into different broadcast domains. This segmentation enhances security, improves network performance, and simplifies network management by grouping devices logically instead of physically.

A **VLAN** operates at **Layer 2** (Data Link Layer) of the OSI model, and each VLAN acts as a separate network segment, even if the devices are connected to the same physical switch. Devices in the same VLAN can communicate with each other, while devices in different VLANs require a **Layer 3 device** (like a router) to communicate.

Common VLAN types:

- **Default VLAN**: All switch ports belong to VLAN 1 by default.
- **Data VLAN**: Carries user-generated traffic (e.g., VLAN 10 for HR, VLAN 20 for Sales).
- **Voice VLAN**: Carries voice traffic, typically prioritized over data traffic.
- **Management VLAN**: Used for network management traffic (e.g., SSH, Telnet).

Algorithm:

1. Define Network Topology:

a. Identify the switch and end devices (PCs) that need to be assigned to different VLANs.

2. Access Switch:

a. Log into the switch and enter global configuration mode.

3. Create VLANs:

a. Create and name VLANs as per the network requirements.

4. Assign Ports to VLANs:

a. Assign specific switch ports to the desired VLANs.

5. Configure Trunk Ports (Optional):

a. If multiple switches are connected, configure trunking on the switch-to-switch link to allow traffic from multiple VLANs to pass through.

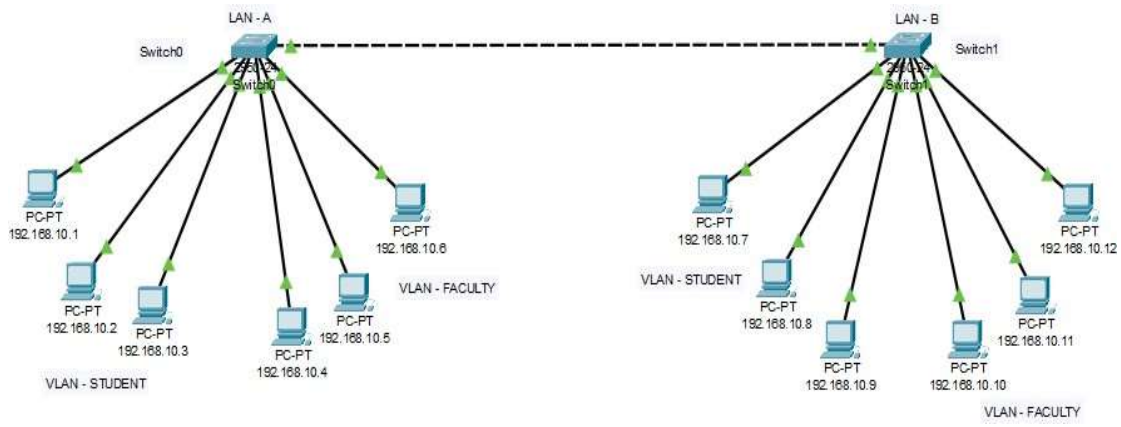
6. Verify VLAN Configuration:

a. Verify VLANs and ensure devices within the same VLAN can communicate.

7. Troubleshoot VLAN Issues:

a. Check the VLAN configuration for any misconfigured ports or VLAN assignments**.**

Output:



Conclusion: In this experiment, we successfully configured VLANs on a switch, segmented the network into different broadcast domains, and tested communication between devices within the same VLAN. We also learned to troubleshoot common VLAN issues such as misconfigured ports and trunk links.

Viva Questions:

1. **How does a switch handle VLAN traffic?**
2. **What is the difference between an access port and a trunk port?**
3. **How do you configure inter-VLAN routing?**
4. **What command would you use to verify VLANs configured on a switch?**
5. **Why is trunking necessary when connecting multiple switches?**

6. What is the difference between tagged and untagged VLAN traffic?

PROGRAM -10:

Aim: To implement and analyze the Network Address Translation (NAT) protocol in a simulated network environment to understand its configuration, operation, and troubleshooting techniques.

Theoretical Description: Network Address Translation (NAT) is a technique used in networking to translate private (non-routable) IP addresses to a public (routable) IP address and vice versa. NAT is crucial for conserving the limited number of public IP addresses and enhancing security by hiding internal IP addresses from external networks.

Types of NAT:

1. Static NAT: A fixed mapping between a private IP and a public IP, allowing external devices to access internal servers.
2. Dynamic NAT: Maps private IPs to a public IP from a defined pool.
3. PAT (Port Address Translation): Allows multiple devices on a local network to be mapped to a single public IP address, differentiated by unique port numbers.

Key Concepts:

- NAT Inside: Refers to the internal network.
- NAT Outside: Refers to the external network (internet).
- Translation Table: Maintains the mapping between private and public IP addresses.

Algorithm:

1. Define Access List:
   a. Create an access list to identify internal IPs that should be translated.
2. Configure NAT Pool (for Dynamic NAT):
   a. Define a pool of public IP addresses for translation.
3. Specify Interfaces:
   a. Configure the router interfaces as NAT inside or outside.
4. Associate Access List with NAT Configuration:
   a. Link the access list to the NAT pool or define overload for PAT.

5. Test Connectivity:

   a. Check if devices can access external networks and whether NAT translations are happening.

6. Troubleshoot if Necessary:

   a. Use commands to check NAT translations and statistics to diagnose issues.

Output:

- Successful translation of private IP addresses to a public IP address.
- Connectivity from devices on the private network to external networks.
- Display of NAT translation table showing active mappings between internal and external addresses.

Conclusion:

The implementation of NAT demonstrates its critical role in modern networking by enabling multiple devices to share a single public IP address while providing security by masking internal IP addresses. Understanding NAT configuration and troubleshooting enhances network management skills, ensuring efficient operation and connectivity in various network scenarios.

Viva Questions:

1. **What is the primary purpose of NAT in networking?**
2. **Explain the difference between static NAT and dynamic NAT.**
3. **How does PAT work, and why is it useful?**
4. **What are the advantages and disadvantages of using NAT?**
5. **Describe the steps involved in configuring NAT on a router.**