**Part 1: VLSM Design and addressing tables:**

In this phase of the implementation, we developed a VLSM (Variable Length Subnet Masking) scheme using the given network address 172.16.0.0/16. The objective was to assign IP addresses efficiently, ensuring that each VLAN and point-to-point link received the necessary number of hosts while keeping IP address wastage to a minimum.

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| Subnet Description | VLAN ID | Hosts | Network Address | CIDR | First Host | Last Host | Broadcast |
| VLAN 40 | VLAN 35 | 61 | 172.16.0.0 | /26 | 172.16.0.1 | 172.16.0.62 | 172.16.0.63 |
| VLAN 20 | VLAN 15 | 31 | 172.16.0.64 | /26 | 172.16.0.65 | 172.16.0.126 | 172.16.0.127 |
| VLAN 50 | VLAN 45 | 30 | 172.16.0.128 | /27 | 172.16.0.129 | 172.16.0.158 | 172.16.0.159 |
| VLAN 10 | VLAN 5 | 25 | 172.16.0.160 | /27 | 172.16.0.161 | 172.16.0.190 | 172.16.0.191 |
| VLAN 70 | VLAN 65 | 20 | 172.16.0.192 | /27 | 172.16.0.193 | 172.16.0.222 | 172.16.0.223 |
| VLAN 25 | VLAN 25 | 12 | 172.16.0.224 | /28 | 172.16.0.225 | 172.16.0.238 | 172.16.0.239 |
| VLAN 60 | VLAN 55 | 12 | 172.16.0.240 | /28 | 172.16.0.241 | 172.16.0.254 | 172.16.0.255 |
| SW-S to MIU-MIUGW | - | 7 | 172.16.1.0 | /28 | 172.16.1.1 | 172.16.1.14 | 172.16.1.15 |
| VLAN 80 | VLAN 75 | 7 | 172.16.1.16 | /28 | 172.16.1.17 | 172.16.1.130 | 172.16.1.131 |
| Main-MLS to MIUMIU-GW | - | 2 | 172.16.1.32 | /30 | 172.16.1.33 | 172.16.1.34 | 172.16.1.35 |
| N-MLS to MIU-MIUGW | - | 2 | 172.16.1.36 | /30 | 172.16.1.37 | 172.16.1.38 | 172.16.1.39 |
| S-MLS to MIU-MIUGW | - | 2 | 172.16.1.40 | /30 | 172.16.1.41 | 172.16.1.42 | 172.16.1.43 |
| R-MLS to MIU-MIUGW | - | 2 | 172.16.1.44 | /30 | 172.16.1.45 | 172.16.1.46 | 172.16.1.47 |

**Subnet Table:**

**Addressing Table:**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Devices | Interface | IP Address | Subnet Mask | Default Gateway | VLAN ID |
| Main-MLS | **G1/1/1** | **172.16.1.33** | **255.255.255.252 (/30)** | **-** | **-** |
|  | **VLAN 5** | **172.16.0.161** | **255.255.255.224 (/27)** | **-** | **VLAN 5** |
|  | **VLAN 15** | **172.16.0.65** | **255.255.255.224 (/27)** | **-** | **VLAN 15** |
| S-MLS | **G1/1/1** | **172.16.1.41** | **255.255.255.252 (/30)** | **-** | **-** |
|  | **VLAN 25** | **172.16.0.225** | **255.255.255.240 (/28)** | **-** | **VLAN 25** |
|  | **VLAN 35** | **172.16.0.1** | **255.255.255.192 (/26)** | **-** | **VLAN 35** |
| N-MLS | **G1/1/1** | **172.16.1.37** | **255.255.255.252 (/30)** | **-** | **-** |
|  | **VLAN 45** | **172.16.0.129** | **255.255.255.224 (/27)** | **-** | **VLAN 45** |
|  | **VLAN 55** | **172.16.0.241** | **255.255.255.240 (/28)** | **-** | **VLAN 55** |
| R-MLS | **G1/0/5** | **172.16.1.45** | **255.255.255.252 (/30)** | **-** | **-** |
|  | **VLAN 65** | **172.16.0.193** | **255.255.255.224 (/27)** | **-** | **VLAN 65** |
|  | **VLAN 75** | **172.16.1.1** | **255.255.255.240 (/28)** | **-** | **VLAN 75** |
| MIU-MIU-GW | **G0/0** | **209.165.200.226** | **255.255.255.240 (/28)** | **-** |  |
|  | **G0/1** | **172.16.1.46** | **255.255.255.252 (/30)** | **-** | **-** |
|  | **G0/0/0** | **172.16.1.41** | **255.255.255.240 (/28)** | **-** | **-** |
|  | **G0/1/0** | **172.16.1.34** | **255.255.255.252 (/30)** | **-** | **-** |
|  | **G0/2/0** | **172.16.1.42** | **255.255.255.252 (/30)** | **-** | **-** |
|  | **G0/3/0** | **172.16.1.38** | **255.255.255.252 (/30)** | **-** | **-** |
| ISP | **Gig0/0** | **209.165.200.225** | **255.255.255.240 (/28)** | **-** | **-** |
|  | **Gig0/1** | **64.100.1.1** | **255.255.255.224 (/27)** | **-** | **-** |
|  | **Gig0/2** | **64.100.2.1** | **255.255.255.224 (/27)** | **-** | **-** |
| Branch\_GW | **Gig0/0.2** | **192.168.2.1** | **255.255.255.0(/24)** | **-** | **-** |
|  | **Gig0/0.3** | **192.168.3.1** | **255.255.255.0(/24)** | **-** | **-** |
|  | **Gig0/1** | **64.100.1.2** | **255.255.255.224 (/27)** | **-** | **-** |
| Home Router | **G0/1** | **64.100.2.2** | **255.255.255.224 (/27)** | **-** | **-** |
|  | **Router IP** | **192.168.10.1** | **255.255.255.128(/25)** | **-** | **-** |

**Hosts Table:**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| PC-Number | VLAN ID | IP Address | Subnet Mask | Default Gateway |
| MIU | | | | |
| PC-1 | VLAN 5 | 172.16.0.162 | 255.255.255.224 (/27) | 172.16.0.161 |
| PC-2 | VLAN 5 | 172.16.0.163 | 255.255.255.224 (/27) | 172.16.0.161 |
| PC-3 | VLAN 15 | 172.16.0.66 | 255.255.255.192 (/26) | 172.16.0.65 |
| PC-4 | VLAN 25 | 172.16.0.226 | 255.255.255.240 (/28) | 172.16.0.225 |
| PC-5 | VLAN 25 | 172.16.0.227 | 255.255.255.240 (/28) | 172.16.0.225 |
| PC-6 | VLAN 35 | 172.16.0.2 | 255.255.255.192 (/26) | 172.16.0.1 |
| PC-7 | VLAN 45 | 172.16.0.130 | 255.255.255.224 (/27) | 172.16.0.129 |
| PC-8 | VLAN 55 | 172.16.0.242 | 255.255.255.240 (/28) | 172.16.0.241 |
| PC-9 | VLAN 65 | 172.16.0.194 | 255.255.255.224 (/27) | 172.16.0.193 |
| PC-10 | VLAN 75 | 172.16.1.18 | 255.255.255.240 (/28) | 172.16.1.17 |
| MIU-Branch 1 | | | | |
| PC-11 | VLAN 2 | 192.168.2.2 | 255.255.255.0 (/24) | 192.168.2.1 |
| PC-12 | VLAN 3 | 192.168.3.2 | 255.255.255.0 (/24) | 192.168.3.1 |
| Wireless Home Network | | | | |
| Laptop | **-** | 192.168.10.104 | 255.255.255.128 | 192.168.10.1 |
| Tablet | **-** | 192.168.10.103 | 255.255.255.128 | 192.168.10.1 |
| Smartphone | **-** | 192.168.10.100 | 255.255.255.128 | 192.168.10.1 |
| Server | | | | |
| DHCP Server | **-** | 172.16.1.3 | 255.255.255.240 (/28) | 172.16.1.1 |
| Email Server | **-** | 172.16.1.4 | 255.255.255.240 (/28) | 172.16.1.1 |
| Web Server | **-** | 172.16.1.5 | 255.255.255.240 (/28) | 172.16.1.1 |
| DNS Server | **-** | 172.16.1.2 | 255.255.255.240 (/28) | 172.16.1.1 |
| NTP and Syslog Server | **-** | 172.16.1.6 | 255.255.255.240 (/28) | 172.16.1.1 |

**Why We Chose VLSM**  
We opted for VLSM (Variable Length Subnet Masking) to achieve greater efficiency and flexibility in IP address allocation. Since the VLANs had varying host requirements, using uniform subnet sizes would have led to significant address wastage. VLSM enabled us to assign IP ranges tailored to each subnet’s specific needs, allowing for optimal utilization of our 172.16.0.0/16 address space.

**Subnet Planning and Address Allocation**  
Our approach started with analyzing the host requirements for each VLAN, arranging them in descending order. This allowed us to allocate the largest subnets first and avoid potential overlaps. For instance, VLAN 40 needed 61 hosts, which fits neatly into a /26 subnet (offering 62 usable addresses), so we began with 172.16.0.0/26.  
We followed this by assigning progressively smaller subnets as host demands decreased. Point-to-point connections were given /30 subnets, as each link only required two usable IP addresses—one for each end. This approach supported logical segmentation and made the network plan easy to follow and document.

Here’s a reworded version of that section with the same meaning:

**Part 2: Network Construction and Basic Setup**  
In this part, we assembled the network topology and began configuring all devices with the essential IP settings and initial configurations.

**Step 1: Assigning IP Addresses to PCs**  
We manually assigned IPv4 addresses to each PC according to the addressing scheme developed in Part 1. This ensured proper connectivity within each respective subnet.

**Step 2: Initial Device Configuration**  
We applied foundational settings to all routers and switches to enable network communication and manageability:

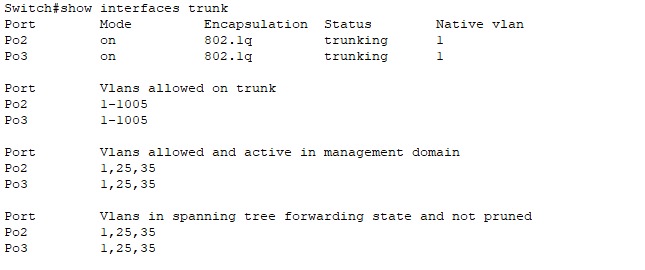
* Disabled DNS lookup to prevent delays from mistyped commands.
* Assigned meaningful hostnames to all devices for easy identification.
* Enforced a minimum password length of 10 characters for enhanced security.
* Set console access passwords using the specified value (MIU1234567).
* Configured a secret password (CSC1234567) for privileged EXEC mode access.
* Enabled encryption for all plaintext passwords to secure credentials.
* Configured a Message of the Day (MOTD) banner to warn unauthorized users.

**Part 3: Network Infrastructure Configuration**  
(VLANs, Trunking, Inter-VLAN Routing, EtherChannel)  
In this phase, we completed the Layer 2 setup to ensure that all switches could communicate effectively and that devices in separate VLANs were able to reach each other.

**Step 1: VLAN Setup**  
We created all necessary VLANs on each switch according to the network plan. This helped logically segment network traffic by department or function as required.

**Step 2: Access Port Configuration**  
We configured all switch ports connected to PCs as access ports and assigned them to their designated VLANs.

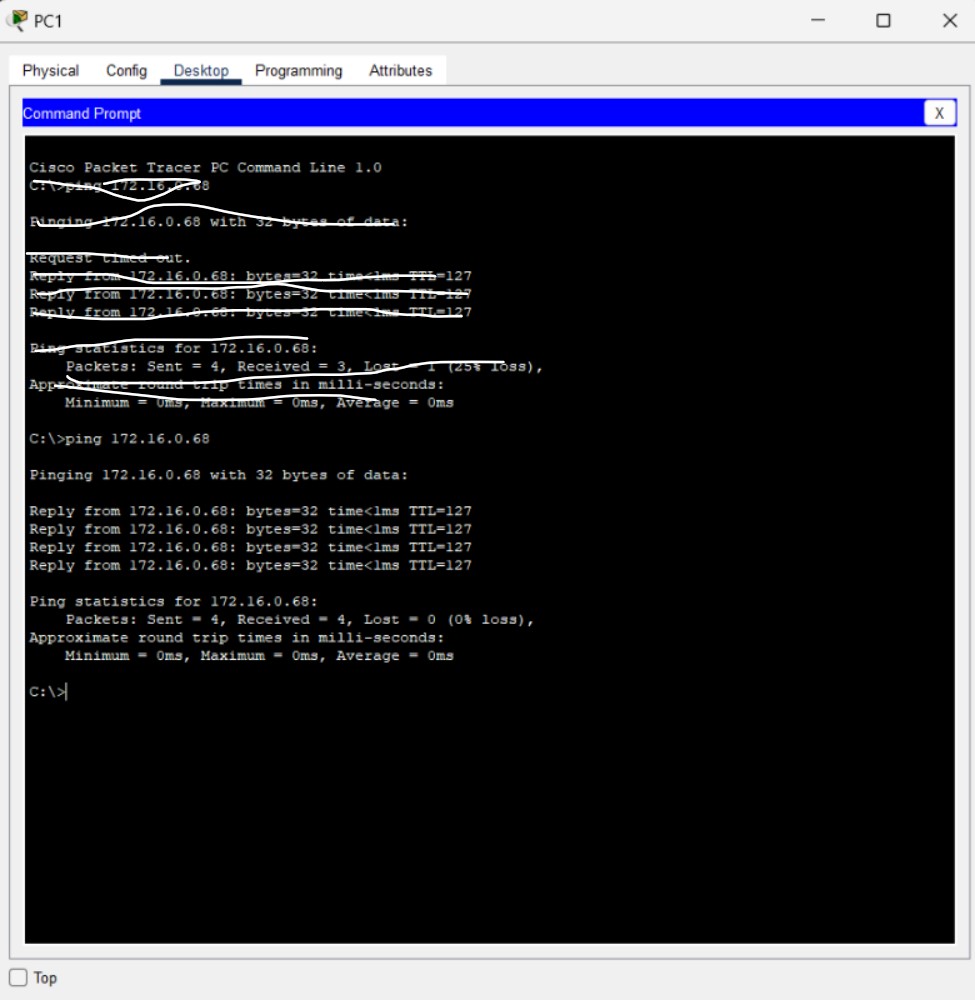
To verify proper setup, we used the Show vlan brief command to confirm VLAN assignments.

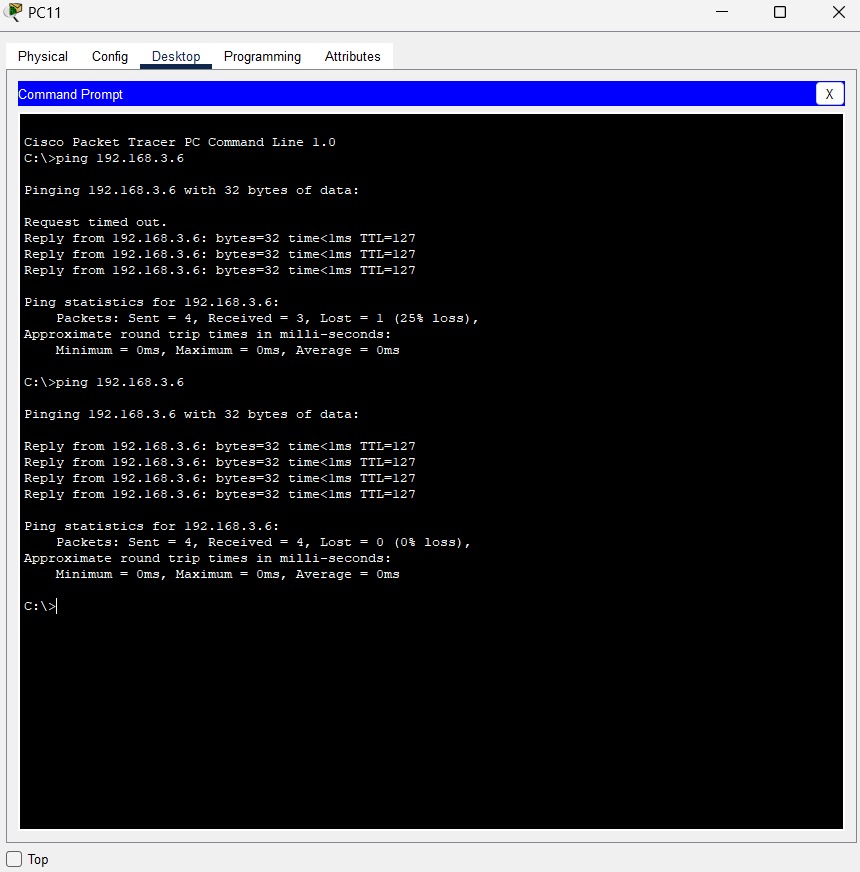
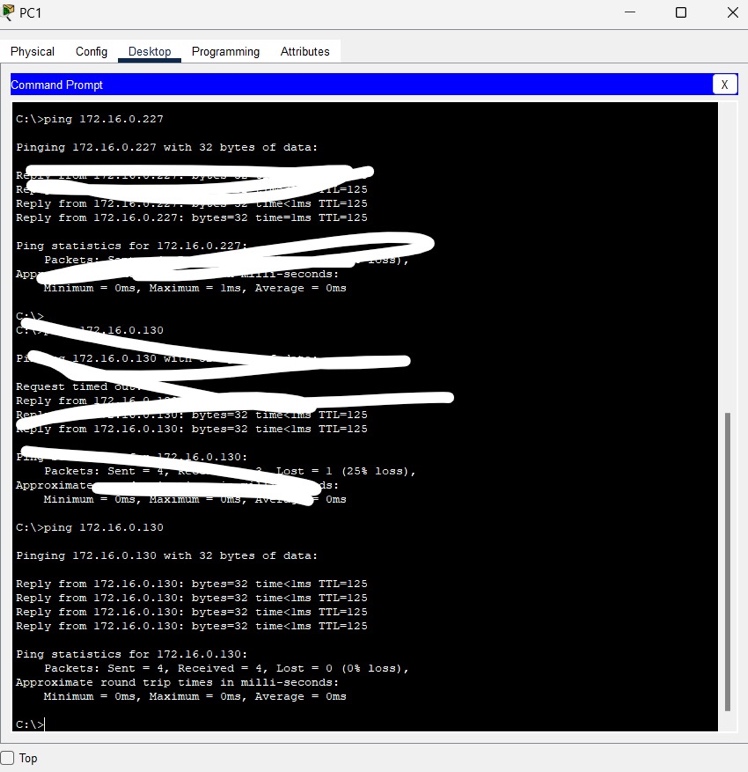
**Step 3: Trunk Configuration Between Switches**  
We configured 802.1Q trunk links on the ports connecting the switches to enable VLAN traffic to traverse between them. This allows VLAN communication across multiple switches.  
  


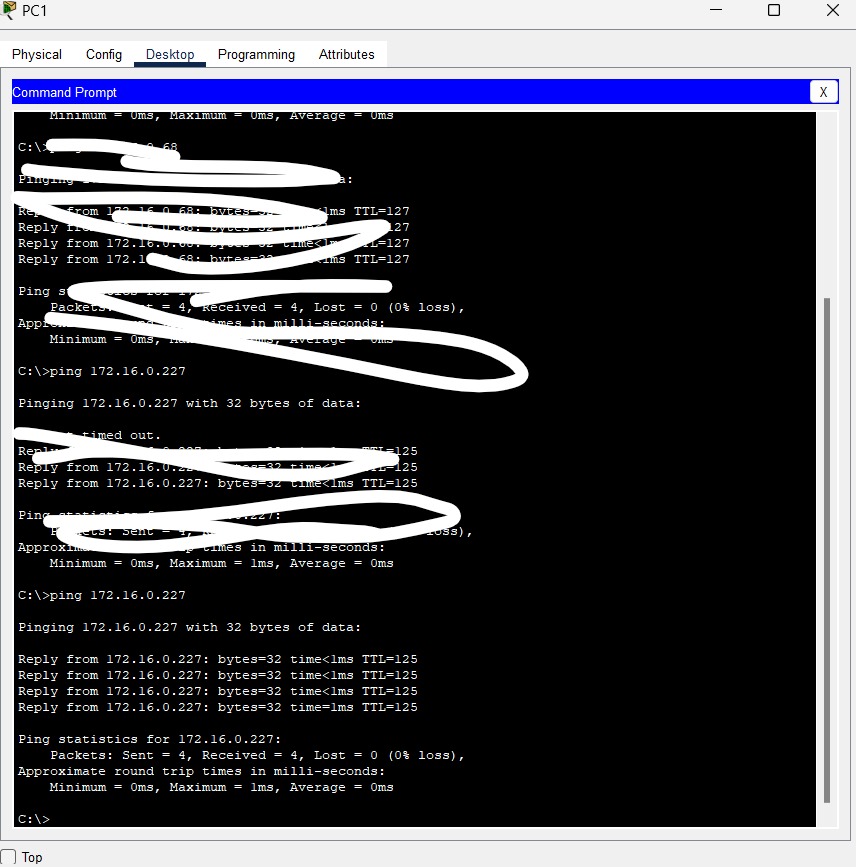
**Step 4: Inter-VLAN Routing Setup**  
a. **On Layer 3 Switches (Main Branch):**

* Configured the port connecting to the MIU-MIU-GW router as a routed interface with an assigned IP address.

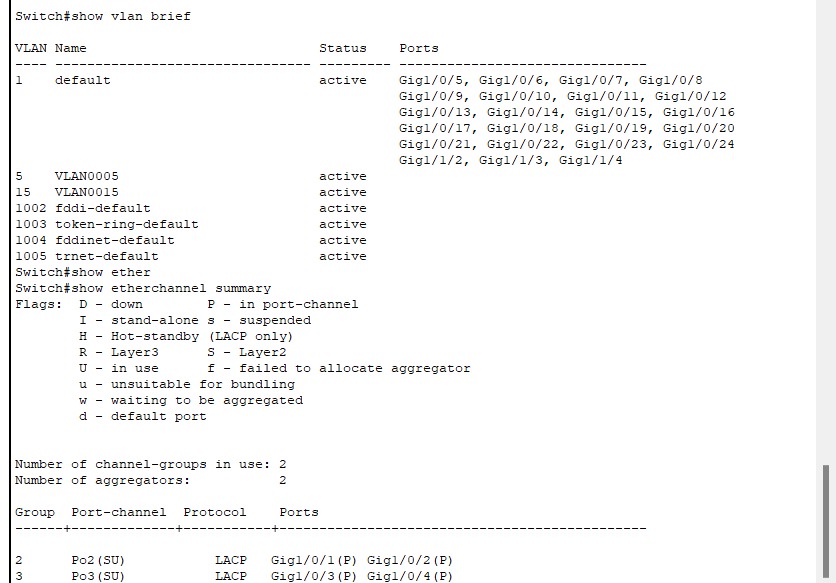
Created and activated SVI (Switch Virtual Interface) interfaces for each VLAN based on the IP addressing plan.  
  
b. **On the Router (MIU Branch):**

* Set up subinterfaces on the router using 802.1Q encapsulation for VLAN tagging.
* Configured a subinterface for VLAN 10 with the appropriate IP address.
* 

**Step 5: Inter-VLAN Routing Verification**  
We tested connectivity between PCs in different VLANs using ping commands to verify that routing was functioning correctly.  
  
  
  




**Step 6: EtherChannel Configuration**  
We set up LACP-based EtherChannels between the switches according to the network topology. This allowed us to aggregate multiple physical links into a single logical connection, enhancing both bandwidth and fault tolerance.

**Step 7: EtherChannel Verification**  
We verified the successful formation and operation of EtherChannels using the relevant show commands.  


**Part 4: Point-to-Point Single-Area OSPFv2 Configuration**  
In this section, we implemented IPv4 routing protocols including OSPF and EIGRP, along with route redistribution and static routes to ensure full network convergence and proper route exchange among all routers.

a. We initiated the OSPF routing process on the MIU-GW router, Main-MLS, and S-MLS using process ID 100.

**I. OSPF Configuration on MIU-MIU-GW Router**  
Addresses:

The interfaces were initially down, so we used the no shutdown command to activate **GigabitEthernet 0/1/0**, which enabled us to proceed with OSPF configuration. After starting OSPF with process ID 100, we added the following networks under the OSPF process:

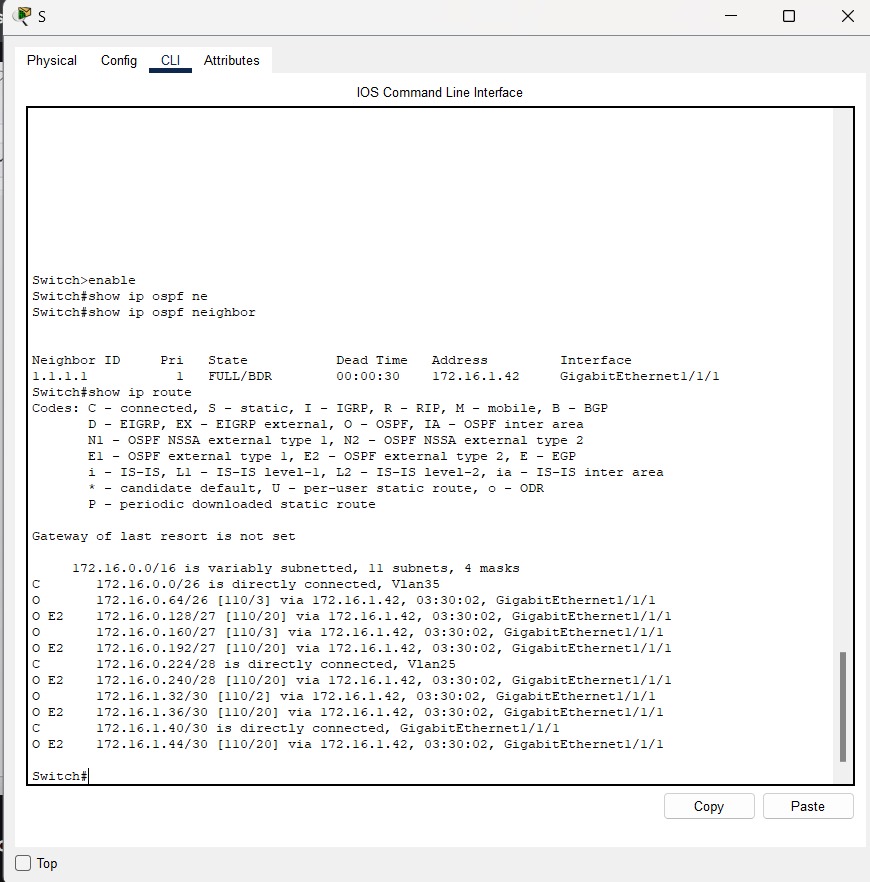
* 172.16.1.32 0.0.0.3
* 172.16.1.36 0.0.0.3
* 172.16.1.40 0.0.0.3
* 172.16.1.44 0.0.0.3

II. OSPF Configuration on Main-MLS  
  
We then configured OSPF process 100 and assigned the following networks to **area 0**:

* 172.16.1.32 0.0.0.3
* 172.16.0.160 0.0.0.31
* 172.16.0.64 0.0.0.63  
    
    
  **III. S-MLS OSPF Configuration**Initially, OSPF failed to detect neighboring devices due to missing IP addresses on key interfaces. Once the correct IPs were assigned, OSPF successfully established neighbor relationships.

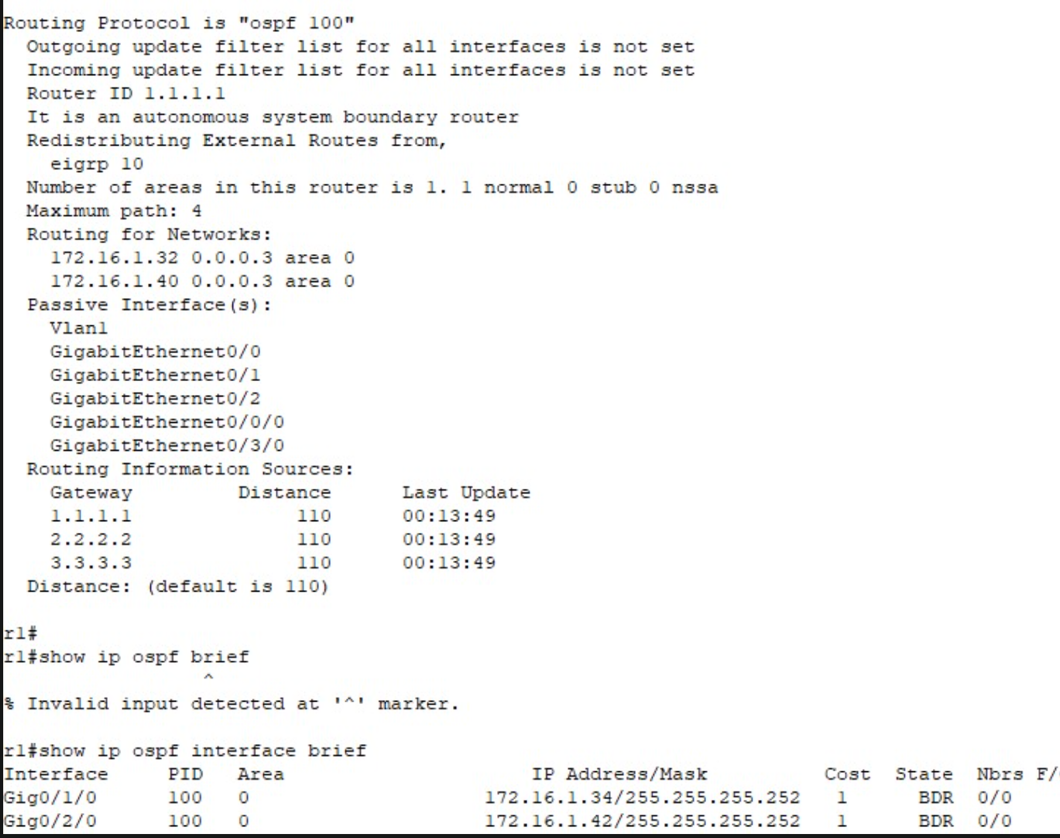
**Assigned IP Addresses:**

* **GigabitEthernet 0/1/0:** 172.16.1.84 /30
* **GigabitEthernet 0/2/0:** 172.16.1.42 /30
* **GigabitEthernet 0/3/0:** 172.16.1.38 /30
* **GigabitEthernet 0/1/0 (duplicate entry likely referring to another device):** 172.16.1.46 /30

**Gave S-MLS a manual Router ID: 1.1.1.1**  
  
**Step 1: Part B – Router IDs**  
We manually set the OSPF router IDs to ensure consistent identification across the network:

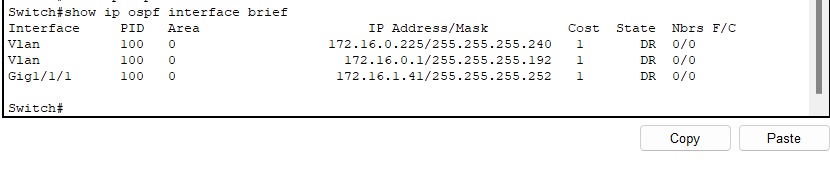
* **MIU-GW:** 1.1.1.1
* **Main-MLS:** 2.2.2.2
* **S-MLS:** 3.3.3.3

After configuring the router IDs, we used the clear ip ospf process command on each router to force the OSPF process to restart and apply the new IDs, as they were initially assigned automatically.

To verify the OSPF configuration and router IDs, we used the command:  
show ip protocols  
  


**Part C: OSPF Network Configuration**  
We configured OSPF routing on all three routers by advertising the appropriate networks under process ID 100. This was done sequentially on each router—first on the one with Router ID **1.1.1.1**, followed by **2.2.2.2**, and then **3.3.3.3**—ensuring all relevant interfaces were included in the OSPF area.

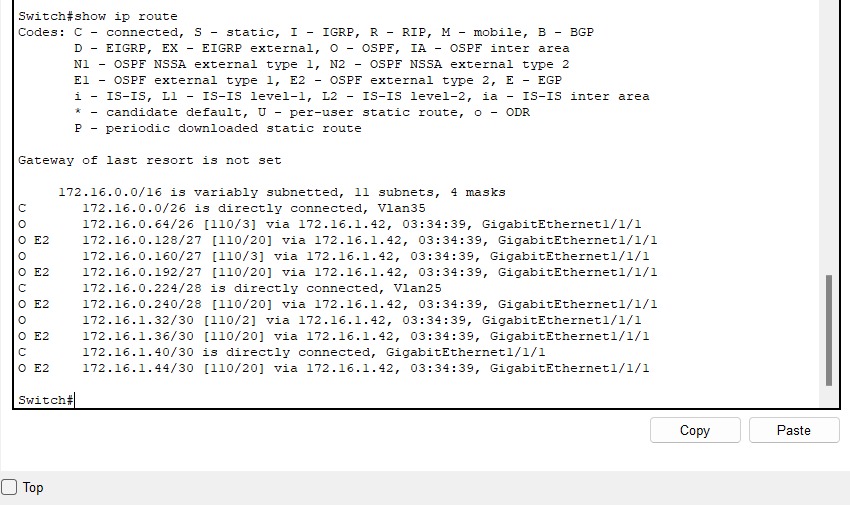
**Part D: Passive Interfaces**  
To optimize routing and enhance security, we configured **passive interfaces** on all routers. This prevented the OSPF process from sending unnecessary routing updates on LAN-facing interfaces that do not connect to other routers.



**Part E: Default Route Propagation in OSPF**  
On the **MIU-GW router**, we configured OSPF to advertise a default route (0.0.0.0/0) so that other routers in the OSPF domain could use it as a gateway of last resort.

**Part F: Verification**  
We verified the OSPF configuration and neighbor relationships using the following commands:

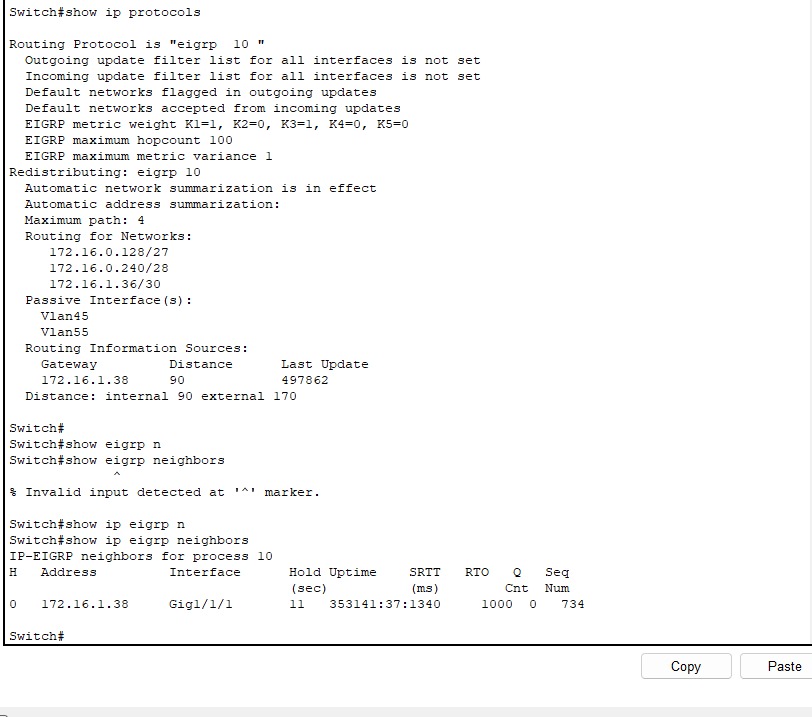
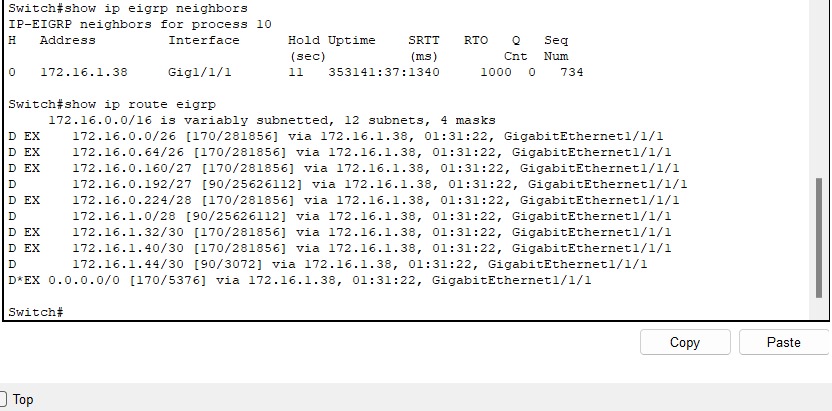
* show ip protocols – to confirm OSPF is running and advertising correctly
* show ip ospf neighbor – to check established OSPF adjacencies
* show ip ospf interface brief – to view OSPF-enabled interfaces and their statuses
* Reviewed the **running-config** under router ospf 100 to ensure all settings were correctly applied

  
  
 **Step 2: Basic EIGRP Configuration**

* We enabled **EIGRP** with **Autonomous System (AS) number 10** on **MIU-GW**, **N-MLS**, and **R-MLS**.
* Each router was configured to advertise its **directly connected networks** into the EIGRP process.
* To reduce unnecessary routing traffic, **LAN interfaces were set as passive**.
* On **MIU-GW**, we configured the propagation of a **default route** into EIGRP so other routers could use it as a gateway of last resort.

**Verification Commands Used:**

* show ip protocols – to verify EIGRP is enabled and advertising the correct networks
* show ip eigrp neighbors – to confirm neighbor relationships
* show ip route eigrp – to view learned routes through EIGRP

**Step 3: Route Redistribution Between EIGRP and OSPF**  
We implemented **mutual route redistribution** on the **MIU-GW router** to enable seamless communication between the OSPF and EIGRP routing domains:

* Redistributed routes **from OSPF into EIGRP**
* Redistributed routes **from EIGRP into OSPF**

**Verification Commands Used:**

* show ip route – to confirm the routing table includes redistributed routes
* show ip protocols – to verify redistribution settings under each protocol
* show ip ospf database – to check OSPF-learned LSAs
* show ip eigrp topology – to confirm EIGRP is receiving and processing redistributed routes

### **Step 4: Static and Default Routes**

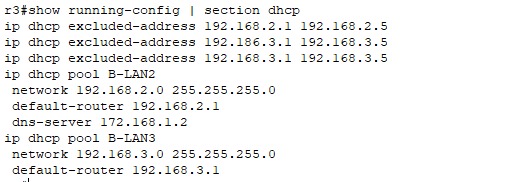
* **Default static routes** were configured on both **MIU-GW** and **Branch-GW**, pointing to the **ISP** as the next hop.
* The **ISP router** was set up with **static routes** directing traffic back to:
  + **MIU-GW**
  + **Branch-GW**
  + The **Home Network**

**Part 5: Configure a DHCP Server**

**Step 1: DHCP Server Setup on Main Branch**

* **Address Exclusion:**  
  The first three usable IP addresses in each VLAN subnet (VLAN 10, 20, 25, and 30) were excluded from dynamic assignment. This reserved those addresses for network devices like gateways and management interfaces.
* **DHCP Pool Configuration:**  
  Separate DHCP pools were created for each VLAN, configured to distribute the correct **IP address range**, **default gateway**, and **DNS server**. These pools supported hosts across the Main Building and S-Building.
* **Relay Agent Configuration:**  
  **Main-MLS** and **S-MLS** were set as **DHCP relay agents**, allowing them to forward client DHCP requests to the centralized DHCP server on the Main Branch.
* **Client Testing:**  
  PCs (PC1–PC6) were tested to ensure proper DHCP functionality. All successfully received dynamic IP configurations (IP address, gateway, and DNS), confirming the setup was working correctly.

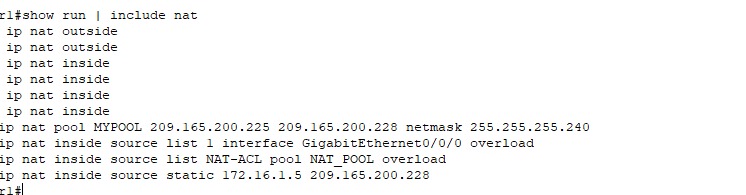
**Step 2: DHCP Server Setup on Branch-GW Router**

* **Address Exclusion:**  
  The first five usable IP addresses in each subnet were excluded to avoid conflicts with statically assigned devices.
* **DHCP Pool Creation:**  
  Two separate pools were created:
  + **B-LAN2** (for VLAN 2)
  + **B-LAN3** (for VLAN 3)  
    Each was configured with its subnet address, default gateway, and DNS server.
* **Verification:**  
  Devices in the Branch network were tested and successfully obtained IP addresses and could communicate within the network, confirming correct DHCP operation.  
    
  

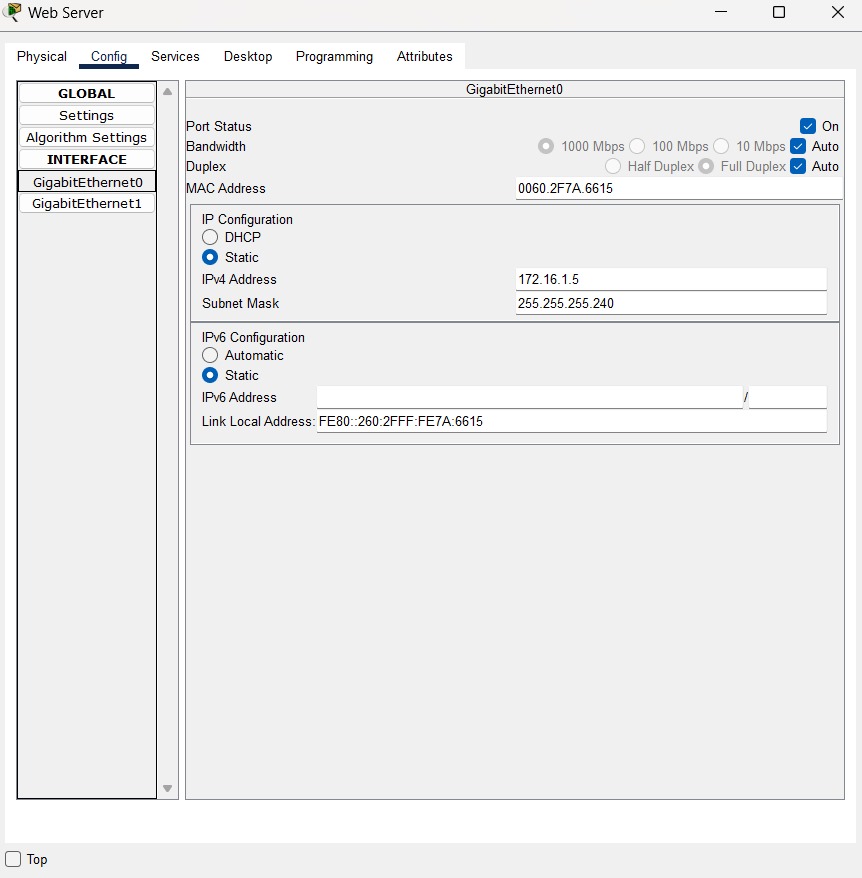
### Part 6: Configure Dynamic NAT with PAT and Static NAT

We set up **Dynamic NAT with Port Address Translation (PAT)** on the **MIU-GW router** to allow internal devices to access the internet using a single public IP address. The **third IP** from the **209.165.200.224/28** public range was used for PAT.

Additionally, we configured **Static NAT** on **MIU-GW** to map the internal IP address of the **miu.edu.eg server** to the **fourth IP** from the same public range. All relevant interfaces were properly configured to participate in NAT.

The setup was then **verified and tested**, confirming that internal hosts could reach external destinations and that the server was accessible from outside.   
  


## Part 7: Configure Network Management Features

* **We configured all devices to use NTP server to ensure synchronization**
* **Enabled Syslog on All Devices:**  
  All network devices were configured to send log messages to a centralized **Syslog server**, ensuring consistent monitoring and easier troubleshooting.
* **Web Server Configuration:**
  + **DNS and HTTP/HTTPS services** were activated on the web server. The **domain name** was correctly set to **miu.edu.eg**.
  + The web content was customized by modifying the **HTML files**, including adding the **MIU logo** to the homepage.
*   
    
    
    
    
    
  **Email Server Configuration:**
  + The **Email Service** was enabled, and the **domain name** was set to **miu.edu.eg**.
  + A **user account** was created on the server to test email functionality.
* **DNS Server Configuration:**
  + The **DNS service** was activated on the server.
  + DNS entries were configured to correctly resolve the domain **miu.edu.eg** to the appropriate **IP addresses** for both the **Web Server** and **Email Server**.

**A screenshot of a computer

AI-generated content may be incorrect.**  
  
  
  
  
**Part 8: Configure and Verify a Site-to-Site IPsec VPN**

**Step 1: Connectivity Verification**

**Before establishing the VPN tunnel, full connectivity across the network was verified to ensure all underlying routing and addressing configurations were functioning correctly. This included successful ping tests and path validation between MIU-GW and Branch\_GW.**

**Step 2: Site-to-Site IPsec VPN Configuration**

**A site-to-site IPsec VPN tunnel was configured between MIU-GW and Branch\_GW to ensure secure and encrypted communication between the two sites. The configuration included the setup of ISAKMP and IPsec policies, defining the peer IP addresses, pre-shared keys, and access lists specifying the interesting traffic.  
Once the tunnel was established, encrypted traffic was tested to confirm that sensitive data could securely traverse the public network. The VPN status and data encapsulation were monitored to ensure the tunnel was active and functioning as expected.  
  
  
  
  
Part 9: Configure a Wireless Home Router**

**In this section, we set up a wireless router to enable Wi-Fi access for home or small office users.**

#### Step 1: Access the Wireless Router

**We started by logging into the wireless router's web-based management interface to begin the configuration.**

#### Step 2: Wireless Configuration

* **The** SSID **for the** 2.4 GHz **wireless network was updated to** MIU-CSC230**. Since SSIDs are** case-sensitive**, special care was taken to input the name correctly.**
* **Wireless security settings were adjusted under the 2.4 GHz configuration:**
* Security Mode **was set to** WPA2 Personal
* Encryption Type **remained as the default,** AES
  + **The** Wi-Fi passphrase **was set to** miu\_csc230

#### **Step 3: Connect Devices and Test**

Several wireless devices (such as laptops and smartphones) were connected to the newly configured SSID. Each client successfully obtained an IP address and demonstrated full network functionality. Connectivity was validated by accessing local network resources and confirming internet access through the router