Group 1
Documentation

Name	ID
Ammar Alaa Bektash	2022/01210
Abdelrahman Mohamed Khalil	2022/02178
Youssef Mahmoud Abdelrahman	2022/07740
Youssef Mohamed Abdelshahid	2022/05890
Ziad Samy Abdelhalim Omran	2022/05959
Maged Hussein	2022/10494

Subnet Description	VLAN ID	VLAN Name	Required Number of hosts	Subnet Mask	CIDR Prefix	IP Range	Broadcast Address
Main	Vlan 10	VLAN0030	62	255.255.255.192	/26	192.168.0.1-192.168.0.62	192.168.0.63
	Vlan 20	VLAN0020	30	255.255.255.192	/26	192.168.0.193-192.168.0.222	192.168.0.223
S	Vlan 30	VLAN0030	14	255.255.255.240	/28	192.168.1.65-192.168.1.78	192.168.1.79
	Vlan 40	VLAN0040	30	255.255.255.224	/27	192.168.1.1-192.168.1.30	192.168.1.31
N	Vlan 50	VLAN0050	30	255.255.255.224	/27	192.168.1.33-192.168.1.62	192.168.1.63
	Vlan 60	VLAN0060	62	255.255.255.192	/26	192.168.0.65-192.168.0.126	192.168.0.127
R	Vlan 70	VLAN0070	30	255.255.255.224	/27	192.168.0.225-192.168.0.254	192.168.0.255
	Vlan 80	VLAN0080	62	255.255.255.192	/26	192.168.0.129-192.168.0.190	192.168.0.191
Server Room			6	255.255.255.248	/29	192.168.1.81-192.168.1.87	192.168.1.88
Main-MLS to GW			2	255.255.255.252	/30	192.168.1.90-192.168.1.91	192.168.1.92
N-MLS to GW			2	255.255.255.252	/30	192.168.1.94-192.168.1.95	192.168.1.96
S-MLS to GW			2	255.255.255.252	/30	192.168.1.98-192.168.1.99	192.168.1.100
R-MLS to GW			2	255.255.255.252	/30	192.168.1.101-192.168.1.102	192.168.1.103
GW to ISP			2	255.255.255.240	/31	209.165.200.224 - 209.165.200.225	209.165.200.226
ISP to Branch-GW			2	255.255.255.252	/30	64.100.1.1-64.100.1.5	64.100.1.6
ISP - Home			2	255.255.255.252	/30	64.100.2.1-64.100.2.4	64.100.2.5

Group 1
Documentation

PC- number	VLAN ID	IP Address/CIDR	Default Gateway
PC-0	10	192.168.0.61/26	192.168.0.1
PC-1	10	192.168.0.62/26	192.168.0.1
PC-2	20	192.168.0.222/27	192.168.0.193
PC-3	30	192.168.1.62/28	192.168.1.49
PC-4	40	192.168.1.30/27	192.168.1.1
PC-5	50	192.168.1.46/27	192.168.1.33
PC-6	60	192.168.0.126/26	192.168.0.65
PC-7	70	192.168.0.254/27	192.168.0.225
PC-8	80	192.168.0.190/26	192.168.0.129
PC-9	2	192.168.1.107/30	192.168.1.106
PC-10	3	192.168.1.111/30	192.168.1.110
PC-11	30	192.168.1.61/28	192.168.1.49
~~Laptop~~			
Tablet		192.168.1.119/29	192.168.1.114
Smartphone		192.168.1.120/29	192.168.1.114
DHCP Server		192.168.1.66/29	192.168.1.65
Email Server		192.168.1.67/29	192.168.1.65
Web Server		192.168.1.68/29	192.168.1.65
DNS Server		192.168.1.70/29	192.168.1.65
NTP Syslog server		192.168.1.69/29	192.168.1.65

Group 1
Documentation

Networking Device	Port-Number	VLAN ID	IP Address/CIDR
Main-MLS	Fa 0/1	10	
	Fa 0/2	10	
	Fa 0/3	20	
	Fa 0/4	20	
	Fa 0/5		
	Gig 0/1		
S-MLS	Fa 0/1	30	
	Fa 0/2	30	
	Fa 0/3	40	
	Fa 0/4	40	
	Fa 0/5		
	Gig 0/1		
N-MLS	Fa 0/1	50	
	Fa 0/2	50	
	Fa 0/3	60	
	Fa 0/4	60	
	Fa 0/5		
	Gig 0/1		
R-MLS	Fa 0/1	70	
	Fa 0/2	70	
	Fa 0/3	80	
	Fa 0/4	80	
	Fa 0/5		
	Gig 0/1		
GW	Gig 1/0/1	Main-MLS	
	Gig 1/0/2	S-MLS	
	Gig 1/0/3	N-MLS	
	Gig 1/0/4	R-MLS	
	Gig 1/0/5	Server Room	
	Gig 1/0/6	ISP	
ISP	Gig 0/0	Main-MLS	
	Gig 0/1	Branch-GW	
	Gig 0/2	Home Router	
Branch-GW	Gig 0/0/0		
	Gig 0/0/1		
Wireless Home Router	Wireless 1		
	Wireless 2		
	Wireless 3		

Group 1
Documentation

Part 1: Design and Implement a VLSM Addressing Scheme and fill in the required tables

We designed a full VLSM Addressing Scheme by first, calculating based on the required hosts in each VLAN the hosts and CIDR prefix. This is done by:

1. Reordering the subnets needed based on the number of hosts
2. Calculating the number of hosts provided by each subnet
3. Calculating the Network Address, Starting/Last IP and Broadcast Address

Note: Detailed steps are provided below regarding the IP Addresses.

192.168.0.00000000 /24

x	x	x	x	x	x	x	x
2^7	2^6	2^5	2^4	2^3	2^2	2^1	2^0
128	64	32	16	8	4	2	1

Reorder:

1. vlan 10 -> 60 host = 2^6 -2 = 62 host /26
2. vlan 60 -> 50 host = 2^6 -2 = 62 host /26
3. vlan 80 -> 40 host = 2^6 -2 = 62 host /26
4. vlan 20 ->30 host = 2^5 -2 = 30 host /27
5. vlan 70 ->30 host = 2^5 -2 = 30 host /27
6. vlan 40 ->20 host = 2^5 -2 = 30 host /28
7. vlan 50 ->15 host = 2^5 -2 = 30 host /28
8. vlan 30 -> 12 host = 2^4 -2 = 14 host /29

9. **Vlan Server Room 5 hosts = 2^3 -2 = 6 host /30**

10. **Main-MLS – GW, 2 host = 2^2 -2 = 2 host /30**
11. **N-MLS – GW, 2 host = 2^2 -2 = 2 host /30**
12. **S-MLS – GW, 2 host = 2^2 -2 = 2 host /30**
13. **R-MLS – GW, 2 host = 2^2 -2 = 2 host /30**
14. **Vlan2, 2 host = 2^2 -2 = 2 host /30**
15. **Vlan3, 2 host = 2^2 -2 = 2 host /30**
16. **Home Network, 2 host = 2^2-2 = 2 host /30**

Group 1
Documentation

Subnet	Network address	First host address Router	Last host address PC	Broadcast address
Subnet #1 Vlan 10	**192.168.0.0**	**192.168.0.1**	**192.168.0.62**	**192.168.0.63** **0+62+1 = 63**
Subnet #2 Vlan 60	**192.168.0.64**	**192.168.0.65**	**192.168.0.126**	**192.168.0.127** **64+62+1**
Subnet #3 Vlan 80	**192.168.0.128**	**192.168.0.129**	**192.168.0.190**	**192.168.0.191** **128+62+1**
Subnet #4 Vlan 20	**192.168.0.192**	**192.168.0.193**	**192.168.0.222**	**192.168.0.223** 192+30+1
Subnet #5 Vlan 70	**192.168.0.224**	**192.168.0.225**	**192.168.0.254**	**192.168.0.255** **224+30+1=255**
Subnet #6 Vlan 40	**192.168.1.0**	**192.168.1.1**	**192.168.1.30**	**192.168.1.31** **0+30+1**
Subnet #7 Vlan 50	**192.168.1.32**	**192.168.1.33**	**192.168.1.62**	**192.168.1.63** **32+30+1**
Subnet #8 Vlan 30	**192.168.1.64**	**192.168.1.65**	**192.168.1.78**	**192.168.1.79** **64+14+1**
Subnet #9 Server room	**192.168.1.80**	**192.168.1.81**	**192.168.1.87**	**192.168.1.88** **81+6+1**

Group 1
Documentation

Subnet #10 Main-GW	**192.168.1.89**	**192.168.1.90**	**192.168.1.91**	**192.168.1.92** **89+2+1**
Subnet #11 N-GW	**192.168.1.93**	**192.168.1.94**	**192.168.1.95**	**192.168.1.96** **93+2+1**
Subnet #12 S-GW	**192.168.1.97**	**192.168.1.98**	**192.168.1.99**	**192.168.1.100** **97+2+1**
Subnet #13 R-GW	**192.168.1.101**	**192.168.1.101**	**192.168.1.102**	**192.168.1.104** **101+2+1**
Subnet #14 Vlan2	**192.168.1.105**	**192.168.1.106**	**192.168.1.107**	**192.168.1.108** **105+2+1**
Subnet #15 Vlan3	**192.168.1.109**	**192.168.1.110**	**192.168.1.111**	**192.168.1.112** **109+2+1**
Subnet #16 Home Network	**192.168.1.113**	**192.168.1.114**	**192.168.1.115**	**192.168.1.116** **113+2+1**

Group 1
Documentation

Public IP's

MIU Branch-1

64.100.1.0 /27

2 host, 2^3 -2 = 6 /31

MIU Branch-0

209.165.200.224 /28

2 host, 2^2 -2 = 2 /31

Home Network

64.100.2.0 /27

2 host, 2^2 -2 = 2 /30

Subnet	Network address	First host address	Last host address	Broadcast address
Subnet #1 ISP-Branch GW Range : 5	**64.100.1.0 /30**	**64.100.1.1 /30**	**64.100.1.5 /30**	**64.100.1.6 /30** **0+5+1 = 6**
Subnet #2 GW – ISP Range: 2	**209.165.200.224 /31**	**209.165.200.224 /31**	**209.165.200.225/31**	**209.165.200.226/31**
Subnet #3 ISP-HR Range: 2	**64.100.2.0/30**	**64.100.2.1 /30**	**64.100.2.2/30**	**64.100.2.3 /30**

Group 1
Documentation

Part 2: Build the Network and Configure Basic Device Settings and Interface Addressing

Step 1: **Configure PCs with IPv4 addresses**

Use the addressing table to manually configure the PCs with full IP addressing.

In each PC, We configured the IP address by giving it the last host address in its corresponding subnet and VLAN from the addressing table.

For Example: PC-1:

- Open PC
- Go to Desktop, then go to IP Configuration, the enter the IP Address: 192.168.0.62
- Subnet Mask: 225.255.192.0 as the /16 Prefix configuration.
- Default Gateway is the first IP given to the multilayer switch.

Step 2: **Configure basic settings for each device.**

a. Configure all Devices with the following:

1) Prevent the router from attempting to resolve incorrectly entered commands as domain names.
   - Main-MLS(config)# no ip domain-lookup
2) Host name for all devices.
   - Main-MLS(config)# hostname Main-MLS
3) Encrypted privileged EXEC secret password
   - Main-MLS(config)# enable secret main123456789
4) Console access password.
   - Main-MLS(config)# line console 0
   - Main-MLS(config-line)# password main123456789
5) Set the minimum password length to **10** characters.
   - Main-MLS(config)# security passwords min-length 10
6) Encrypt the clear text passwords.
   - Main-MLS(config)# service password-encryption
7) Configure an appropriate MOTD Banner.
   - Main-MLS(config)# banner motd # Unauthorized access is prohibited! #

b. Configure the Interface Addressing of routers and switches.

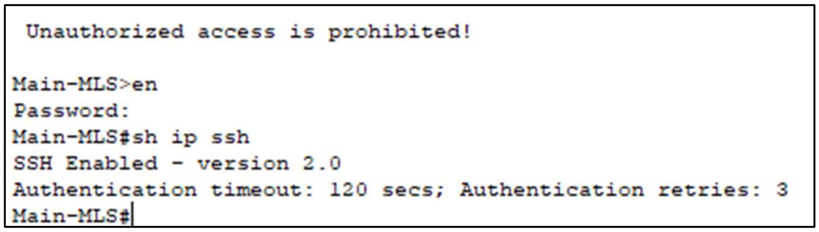
c. Configure SSH for all routers.
   - Main-MLS(config)# ip domain-name localdomain
   - Main-MLS(config)# crypto key generate rsa
   - Main-MLS(config)# username admin privilege 15 secret adminPassword
   - Main-MLS(config)# line vty 0 4
   - Main-MLS(config-line)# login local

- Main-MLS(config-line)# transport input ssh
- Main-MLS(config-line)# exit
- Main-MLS(config)# ip ssh version 2
- Main-MLS(config)# end
- Main-MLS# write memory

Here are the exact commands used in the main building to complete all the steps above as an example:

- Main-MLS> enable
- Main-MLS# configure terminal
- Main-MLS(config)# no ip domain-lookup
- Main-MLS(config)# hostname Main-MLS
- Main-MLS(config)# enable secret main123456789
- Main-MLS(config)# line console 0
- Main-MLS(config-line)# password main123456789
- Main-MLS(config-line)# login
- Main-MLS(config-line)# exit
- Main-MLS(config)# security passwords min-length 10
- Main-MLS(config)# service password-encryption
- Main-MLS(config)# banner motd # Unauthorized access is prohibited! #
- Main-MLS(config)# ip domain-name localdomain
- Main-MLS(config)# crypto key generate rsa
- Main-MLS(config)# username admin privilege 15 secret adminPassword
- Main-MLS(config)# line vty 0 4
- Main-MLS(config-line)# login local
- Main-MLS(config-line)# transport input ssh
- Main-MLS(config-line)# exit
- Main-MLS(config)# ip ssh version 2
- Main-MLS(config)# end
- Main-MLS# write memory

To show the functionality of this part, here is a screenshot from our CLI:



```
 Unauthorized access is prohibited!

Main-MLS>en
Password:
Main-MLS#sh ip ssh
SSH Enabled - version 2.0
Authentication timeout: 120 secs; Authentication retries: 3
Main-MLS#
```

Figure 1: Result of Testing Showing authorization and SSH Functionality

Part 3: Configure Network Infrastructure Settings (VLANs, Trunking, Inter-VLAN Routing EtherChannel)

To configure network infrastructure settings, VLANs were created, and switch ports were assigned accordingly. Then, an 802.1Q trunk was configured between the switches to facilitate VLAN traffic. Host access ports connecting to PCs were configured on all switches. Subsequently, inter-VLAN routing was set up on the router, allowing communication between VLANs. Finally, inter-VLAN routing was verified to ensure proper functionality.

Step 1: Create VLANs and Assign Switch Ports

- We created VLANS by assigning them in each switch by giving them default names like VLAN0030.

Step 2: Configure an 802.1Q Trunk between the Switches

- switchport trunk encapsulation dot1q.
    - This command configures the 802.1Q Trunk between the switches

Step 3: On all switches, configure host access ports connecting to PCs

- Main-S1(config)# interface fa0/1
- Main-S1(config-if-range)# switchport mode access
- Main-S1(config-if-range)# switchport access vlan 10
- Main-S1(config-if-range)# exit

Step 4: Configure Inter-VLAN Routing on the Router

- Main-MLS(config)# interface vlan 10
- Main-MLS(config-if)# ip address 192.168.0.1 255.255.255.192
- Main-MLS(config-if)# no shutdown
- Main-MLS(config-if)# exit
- Main-MLS(config)# interface vlan 20
- Main-MLS(config-if)# ip address 192.168.0.193 255.255.255.224
- Main-MLS(config-if)# no shutdown
- Main-MLS(config-if)# exit
- Main-MLS(config)# ip routing

Step 5: Verify Inter-VLAN Routing is working

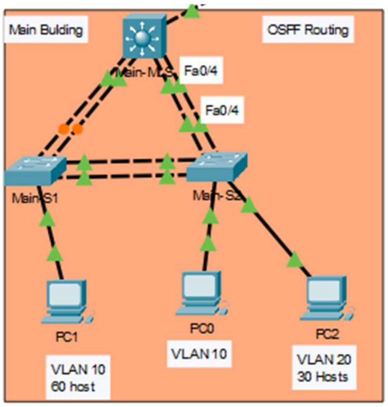
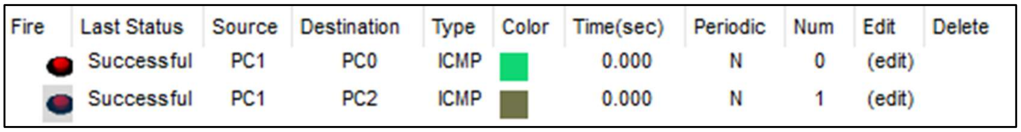


Figure 2: Main Building

This is the building we did the configuration on as an example. We sent a message from PC-1 in the Main building to PC-0 in the same building and from PC-1 to PC-2.

Here is a message screenshot to show this part fully working:



Fire	Last Status	Source	Destination	Type	Color	Time(sec)	Periodic	Num	Edit	Delete
●	Successful	PC1	PC0	ICMP	🟩	0.000	N	0	(edit)	
●	Successful	PC1	PC2	ICMP	🟫	0.000	N	1	(edit)	

Figure 3: Screenshot Showing Messages being sent successfully

All Commands for this part:

First Switch:

- Main-S1> enable
- Main-S1# configure terminal
- Main-S1(config)# vlan 10
- Main-S1(config-vlan)# exit
- Main-S1(config)# vlan 20
- Main-S1(config-vlan)# exit
- Main-S1(config)# interface fa0/10
- Main-S1(config-if)# switchport mode access
- Main-S1(config-if)# switchport access vlan 10
- Main-S1(config-if)# exit
- Main-S1(config)# interface fa0/1
- Main-S1(config-if-range)# switchport mode access
- Main-S1(config-if-range)# switchport access vlan 10
- Main-S1(config-if-range)# exit

Group 1
Documentation

- Main-S1(config)# interface fa0/10
- Main-S1(config-if-range)# switchport mode access
- Main-S1(config-if-range)# switchport access vlan 20
- Main-S1(config-if-range)# exit
- Main-S1(config)# interface range fa0/1-2
- Main-S1(config-if-range)# switchport mode trunk
- Main-S1(config)# interface range fa0/5-6
- Main-S1(config-if-range)# switchport mode trunk
- Main-S1(config)# interface range fa0/1-2

Second Switch:

- Main-S2> enable
- Main-S2# configure terminal
- Main-S2(config)# vlan 10
- Main-S2(config-vlan)# exit
- Main-S2(config)# vlan 20
- Main-S2(config-vlan)# exit
- Main-S2(config)# interface fa0/1
- Main-S2(config-if)# switchport mode access
- Main-S2(config-if)# switchport access vlan 10
- Main-S2(config-if)# exit
- Main-S2(config)# interface fa0/10
- Main-S2(config-if)# switchport mode access
- Main-S2(config-if)# switchport access vlan 20
- Main-S2(config-if)# exit
- Main-S2(config)# interface range fa0/3-6
- Main-S2(config-if-range)# switchport mode trunk

Multi-Layer Switch:

- Main-MLS> enable
- Main-MLS# configure terminal
- Main-MLS(config)# vlan 10
- Main-MLS(config-vlan)# exit
- Main-MLS(config)# vlan 20
- Main-MLS(config-vlan)# exit
- Main-MLS(config)# interface vlan 10
- Main-MLS(config-if)# ip address 192.168.0.1 255.255.255.192
- Main-MLS(config-if)# no shutdown
- Main-MLS(config-if)# exit
- Main-MLS(config)# interface vlan 20
- Main-MLS(config-if)# ip address 192.168.0.193 255.255.255.224
- Main-MLS(config-if)# no shutdown

- Main-MLS(config-if)# exit
- Main-MLS(config)# ip routing

Step 6: On all switches, create LACP EtherChannels as shown in the topology diagram.

- S1# configure terminal
- S1(config)# interface range gigabitEthernet 0/1-2
- S1(config-if-range)# channel-group 1 mode active
- S1(config-if-range)# exit
- S1(config)# interface port-channel 1
- S1(config-if)# switchport mode trunk
- S1(config-if)# exit
- S1(config)# interface range gigabitEthernet 0/5-6
- S1(config-if-range)# channel-group 2 mode active
- S1(config-if-range)# exit
- S1(config)# interface port-channel 2
- S1(config-if)# switchport mode trunk
- S1(config-if)# exit
- S1(config)# end

- S2# configure terminal
- S2(config)# interface range gigabitEthernet 0/3-4
- S2(config-if-range)# channel-group 1 mode active
- S2(config-if-range)# exit
- S2(config)# interface port-channel 1
- S2(config-if)# switchport mode trunk
- S2(config-if)# exit
- S2(config)# interface range gigabitEthernet 0/5-6
- S2(config-if-range)# channel-group 2 mode active
- S2(config-if-range)# exit
- S2(config)# interface port-channel 2
- S2(config-if)# switchport mode trunk
- S2(config-if)# exit
- S2(config)# end

Main Multi-layer Switch

- MLS# configure terminal
- MLS(config)# interface range gigabitEthernet 0/1 - 2
- MLS(config-if-range)# channel-group 1 mode active
- MLS(config-if-range)# exit
- MLS(config)# interface port-channel 1
- MLS(config-if)# switchport mode trunk
- MLS(config-if)# exit

- MLS(config)# interface range gigabitEthernet 0/3 - 4
- MLS(config-if-range)# channel-group 2 mode active
- MLS(config-if-range)# exit
- MLS(config)# interface port-channel 2
- MLS(config-if)# switchport mode trunk
- MLS(config-if)# exit
- MLS(config)# end

Part 4: Configure a Router as a DHCP Server.

In order to prevent conflicts, you must first configure the router as a DHCP server by excluding certain IPv4 addresses from dynamic assignment. Next, for the LAN segment connected to B_R1, construct a DHCP pool and configure its subnet, default gateway, and DNS server. Lastly, make sure that devices can dynamically receive IP addresses and easily access network resources by testing DHCP operation and connectivity.

Step 1: Configure the excluded IPv4 addresses.

Step 2: Create a DHCP pool on B_R1 LAN.

a. Create a DHCP pool named **B_R1 LAN**.

b. Configure the DHCP pool to include the network address, the default gateway, and the IP address of the DNS server.

Step 3: Verify DHCP and Connectivity

Here Are the commands:

- Branch-GW> enable
- Branch-GW# configure terminal
- Branch-GW(config)# interface gigabitethernet0/0/1.2
- Branch-GW(config-subif)# encapsulation dot1q 2
- Branch-GW(config-subif)# ip address 192.168.2.1 255.255.255.0
- Branch-GW(config-subif)# exit
- Branch-GW(config)# interface gigabitethernet0/0/1.3
- Branch-GW(config-subif)# encapsulation dot1q 3
- Branch-GW(config-subif)# ip address 192.168.3.1 255.255.255.0
- Branch-GW(config-subif)# exit
- Branch-GW(config)# ip dhcp excluded-address 192.168.2.1 192.168.2.10
- Branch-GW(config)# ip dhcp excluded-address 192.168.3.1 192.168.3.10
- Branch-GW(config)# ip dhcp pool B_R1_LAN
- Branch-GW(dhcp-config)# network 192.168.2.0 255.255.255.0
- Branch-GW(dhcp-config)# default-router 192.168.2.1
- Branch-GW(dhcp-config)# dns-server 8.8.8.8
- Branch-GW(dhcp-config)# exit
- Branch-GW(config)# ip dhcp pool B_R1_LAn
- Branch-GW(dhcp-config)# network 192.168.3.0 255.255.255.0
- Branch-GW(dhcp-config)# default-router 192.168.3.1
- Branch-GW(dhcp-config)# dns-server 8.8.8.8
- Branch-GW(dhcp-config)# exit

- Branch-GW(config)# exit

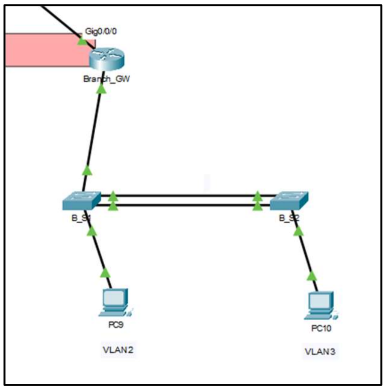
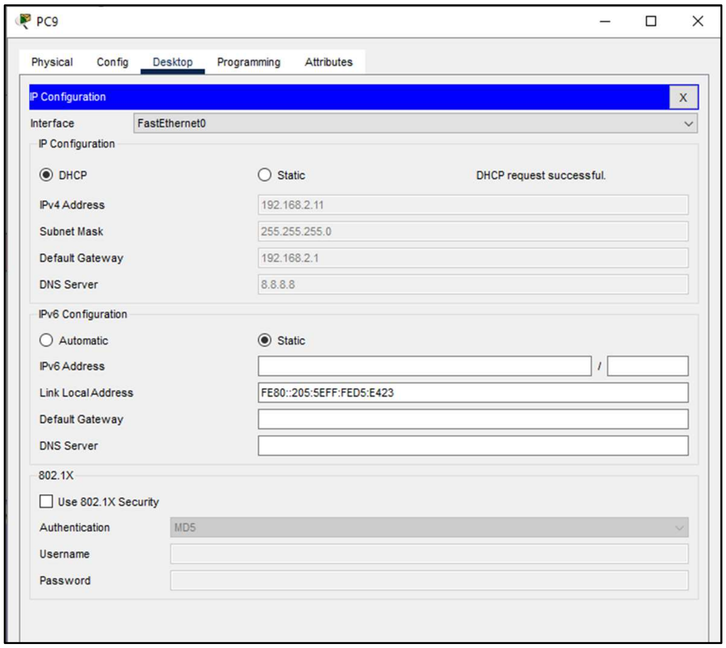


Figure 4: MIU Branch-1



IP Configuration

Interface: FastEthernet0

IP Configuration

● DHCP ○ Static DHCP request successful.

IPv4 Address: 192.168.2.11

Subnet Mask: 255.255.255.0

Default Gateway: 192.168.2.1

DNS Server: 8.8.8.8

IPv6 Configuration

○ Automatic ● Static

IPv6 Address: /

Link Local Address: FE80::205:5EFF:FED5:E423

Default Gateway:

DNS Server:

802.1X

□ Use 802.1X Security

Authentication: MD5

Username:

Password:

Figure 5: DHCP Configuration Successful

Here is the Branch-GW in the MIU Branch-1 with the configuration of the PC-9 as an example of the DHCP server. As you can see, the request was successful.

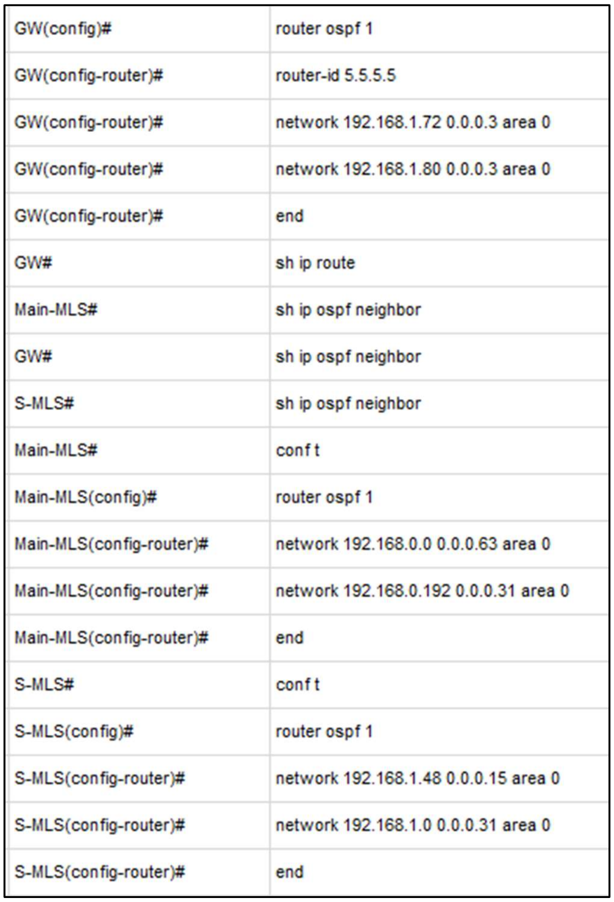
Part 5: Configure Routing Protocols

In order to ensure intra-area connection, we first configured Single Area OSPF for IPv4 on a few core and multilayer switches before configuring the network's routing protocols. Then, on additional core and multilayer switches, we set up Single Area EIGRP for IPv4 in order to create effective routing inside the EIGRP domain. Next, we made it possible for routes to be shared between OSPF and EIGRP by turning on route redistribution. Verification procedures made sure that connections were kept open throughout the network and that routes were effectively propagated, guaranteeing smooth interoperability.

Step 1: Configure and Verify Single Area OSPF for IPv4 on **Core_R1, Multilayer_Main_SW1, and Multilayer_S_SW2.**

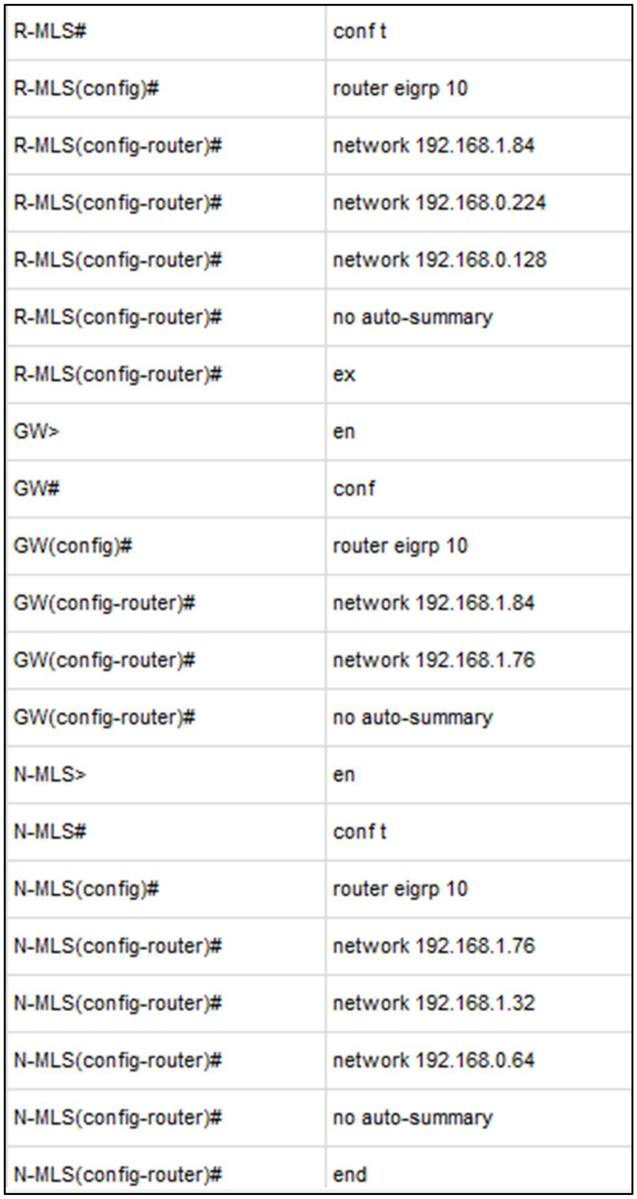
Step 2: Configure and Verify Single Area EIGRP for IPv4 on **Core_R1, Multilayer_N_SW3, and Multilayer_R_SW4.**

Step 3: Configure redistribution from OSPF into EIGRP for IPv4, and redistribution of EIGRP into OSPF for IPv4



GW(config)#	router ospf 1
GW(config-router)#	router-id 5.5.5.5
GW(config-router)#	network 192.168.1.72 0.0.0.3 area 0
GW(config-router)#	network 192.168.1.80 0.0.0.3 area 0
GW(config-router)#	end
GW#	sh ip route
Main-MLS#	sh ip ospf neighbor
GW#	sh ip ospf neighbor
S-MLS#	sh ip ospf neighbor
Main-MLS#	conf t
Main-MLS(config)#	router ospf 1
Main-MLS(config-router)#	network 192.168.0.0 0.0.0.63 area 0
Main-MLS(config-router)#	network 192.168.0.192 0.0.0.31 area 0
Main-MLS(config-router)#	end
S-MLS#	conf t
S-MLS(config)#	router ospf 1
S-MLS(config-router)#	network 192.168.1.48 0.0.0.15 area 0
S-MLS(config-router)#	network 192.168.1.0 0.0.0.31 area 0
S-MLS(config-router)#	end

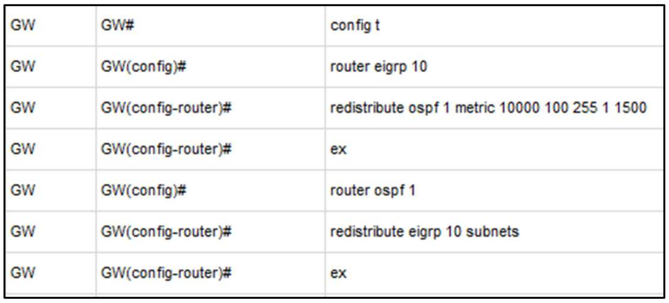
Figure 6: OSPF Configuration



R-MLS#	conf t
R-MLS(config)#	router eigrp 10
R-MLS(config-router)#	network 192.168.1.84
R-MLS(config-router)#	network 192.168.0.224
R-MLS(config-router)#	network 192.168.0.128
R-MLS(config-router)#	no auto-summary
R-MLS(config-router)#	ex
GW>	en
GW#	conf
GW(config)#	router eigrp 10
GW(config-router)#	network 192.168.1.84
GW(config-router)#	network 192.168.1.76
GW(config-router)#	no auto-summary
N-MLS>	en
N-MLS#	conf t
N-MLS(config)#	router eigrp 10
N-MLS(config-router)#	network 192.168.1.76
N-MLS(config-router)#	network 192.168.1.32
N-MLS(config-router)#	network 192.168.0.64
N-MLS(config-router)#	no auto-summary
N-MLS(config-router)#	end

Figure 7: EIGRP Configuration

Above is the command history showing our work regarding steps 1 & 2.

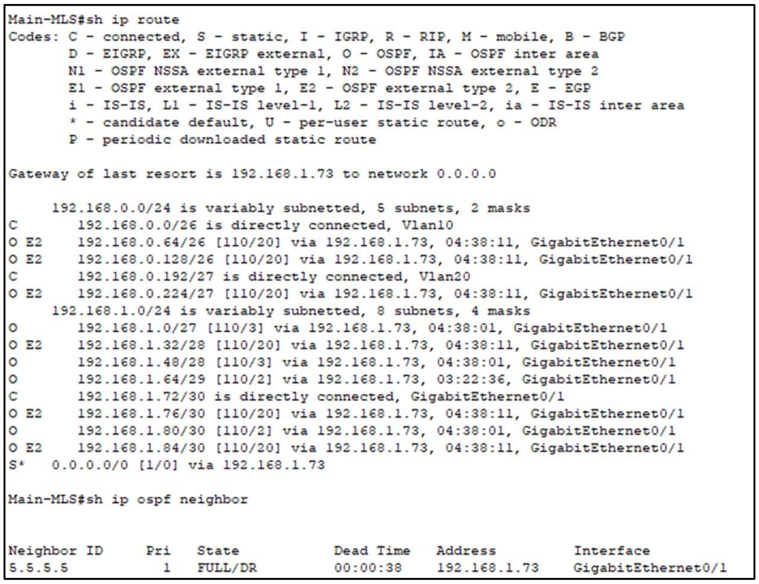


GW	GW#	config t
GW	GW(config)#	router eigrp 10
GW	GW(config-router)#	redistribute ospf 1 metric 10000 100 255 1 1500
GW	GW(config-router)#	ex
GW	GW(config)#	router ospf 1
GW	GW(config-router)#	redistribute eigrp 10 subnets
GW	GW(config-router)#	ex

Figure 8: Redistribution Between OSPF and EIGRP

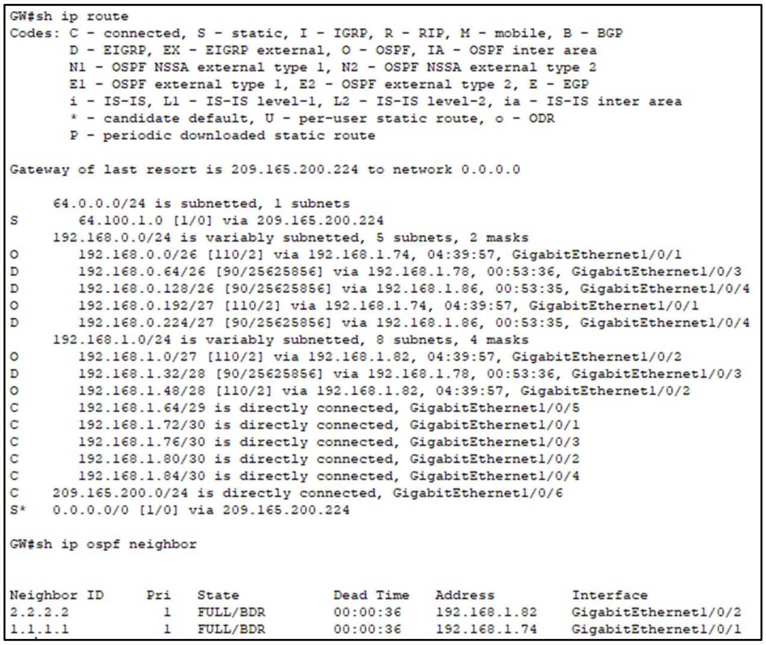
Above is the command history showing our work regarding the redistribution in step 3.

Step 4: Verify OSPF, EIGRP, and redistribution settings.



```
Main-MLS#sh ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is 192.168.1.73 to network 0.0.0.0

     192.168.0.0/24 is variably subnetted, 5 subnets, 2 masks
C       192.168.0.0/26 is directly connected, Vlan10
O E2    192.168.0.64/26 [110/20] via 192.168.1.73, 04:38:11, GigabitEthernet0/1
O E2    192.168.0.128/26 [110/20] via 192.168.1.73, 04:38:11, GigabitEthernet0/1
C       192.168.0.192/27 is directly connected, Vlan20
O E2    192.168.0.224/27 [110/20] via 192.168.1.73, 04:38:11, GigabitEthernet0/1
     192.168.1.0/24 is variably subnetted, 8 subnets, 4 masks
O       192.168.1.0/27 [110/3] via 192.168.1.73, 04:38:01, GigabitEthernet0/1
O E2    192.168.1.32/28 [110/20] via 192.168.1.73, 04:38:11, GigabitEthernet0/1
O       192.168.1.48/28 [110/3] via 192.168.1.73, 04:38:01, GigabitEthernet0/1
O       192.168.1.64/29 [110/2] via 192.168.1.73, 03:22:36, GigabitEthernet0/1
C       192.168.1.72/30 is directly connected, GigabitEthernet0/1
O E2    192.168.1.76/30 [110/20] via 192.168.1.73, 04:38:11, GigabitEthernet0/1
O       192.168.1.80/30 [110/2] via 192.168.1.73, 04:38:01, GigabitEthernet0/1
O E2    192.168.1.84/30 [110/20] via 192.168.1.73, 04:38:11, GigabitEthernet0/1
S*   0.0.0.0/0 [1/0] via 192.168.1.73

Main-MLS#sh ip ospf neighbor


Neighbor ID     Pri   State           Dead Time   Address         Interface
5.5.5.5           1   FULL/DR         00:00:38    192.168.1.73    GigabitEthernet0/1
```

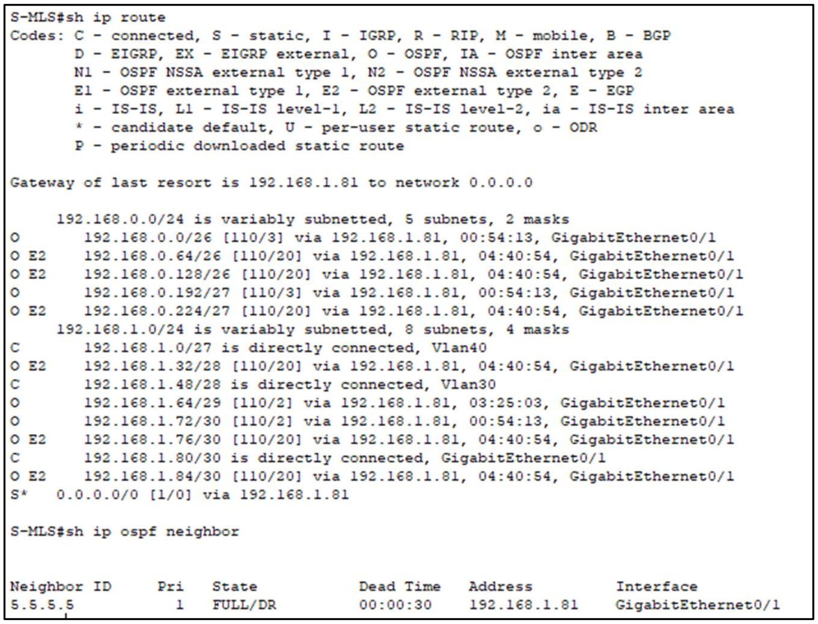
Figure 9: Verifying OSPF & EIGRP in Main-MLS



```
GW#sh ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is 209.165.200.224 to network 0.0.0.0

     64.0.0.0/24 is subnetted, 1 subnets
S       64.100.1.0 [1/0] via 209.165.200.224
     192.168.0.0/24 is variably subnetted, 5 subnets, 2 masks
O       192.168.0.0/26 [110/2] via 192.168.1.74, 04:39:57, GigabitEthernet1/0/1
D       192.168.0.64/26 [90/25625856] via 192.168.1.78, 00:53:36, GigabitEthernet1/0/3
D       192.168.0.128/26 [90/25625856] via 192.168.1.86, 00:53:35, GigabitEthernet1/0/4
O       192.168.0.192/27 [110/2] via 192.168.1.74, 04:39:57, GigabitEthernet1/0/1
D       192.168.0.224/27 [90/25625856] via 192.168.1.86, 00:53:35, GigabitEthernet1/0/4
     192.168.1.0/24 is variably subnetted, 8 subnets, 4 masks
O       192.168.1.0/27 [110/2] via 192.168.1.82, 04:39:57, GigabitEthernet1/0/2
D       192.168.1.32/28 [90/25625856] via 192.168.1.78, 00:53:36, GigabitEthernet1/0/3
O       192.168.1.48/28 [110/2] via 192.168.1.82, 04:39:57, GigabitEthernet1/0/2
C       192.168.1.64/29 is directly connected, GigabitEthernet1/0/5
C       192.168.1.72/30 is directly connected, GigabitEthernet1/0/1
C       192.168.1.76/30 is directly connected, GigabitEthernet1/0/3
C       192.168.1.80/30 is directly connected, GigabitEthernet1/0/2
C       192.168.1.84/30 is directly connected, GigabitEthernet1/0/4
C    209.165.200.0/24 is directly connected, GigabitEthernet1/0/6
S*   0.0.0.0/0 [1/0] via 209.165.200.224

GW#sh ip ospf neighbor


Neighbor ID     Pri   State           Dead Time   Address         Interface
2.2.2.2           1   FULL/BDR        00:00:36    192.168.1.82    GigabitEthernet1/0/2
1.1.1.1           1   FULL/BDR        00:00:36    192.168.1.74    GigabitEthernet1/0/1
```

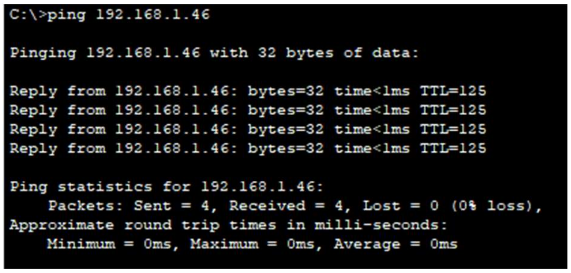
Figure 10: Verifying OSPF & EIGRP in GW

Group 1
Documentation



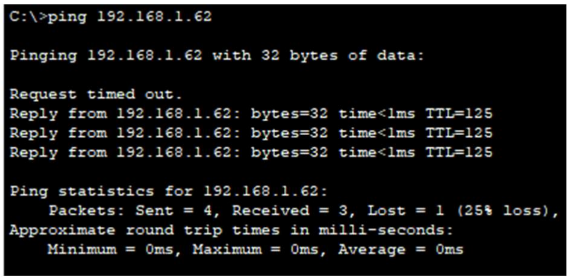
```
S-MLS#sh ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is 192.168.1.81 to network 0.0.0.0

     192.168.0.0/24 is variably subnetted, 5 subnets, 2 masks
O       192.168.0.0/26 [110/3] via 192.168.1.81, 00:54:13, GigabitEthernet0/1
O E2    192.168.0.64/26 [110/20] via 192.168.1.81, 04:40:54, GigabitEthernet0/1
O E2    192.168.0.128/26 [110/20] via 192.168.1.81, 04:40:54, GigabitEthernet0/1
O       192.168.0.192/27 [110/3] via 192.168.1.81, 00:54:13, GigabitEthernet0/1
O E2    192.168.0.224/27 [110/20] via 192.168.1.81, 04:40:54, GigabitEthernet0/1
     192.168.1.0/24 is variably subnetted, 8 subnets, 4 masks
C       192.168.1.0/27 is directly connected, Vlan40
O E2    192.168.1.32/28 [110/20] via 192.168.1.81, 04:40:54, GigabitEthernet0/1
C       192.168.1.48/28 is directly connected, Vlan30
O       192.168.1.64/29 [110/2] via 192.168.1.81, 03:25:03, GigabitEthernet0/1
O       192.168.1.72/30 [110/2] via 192.168.1.81, 00:54:13, GigabitEthernet0/1
O E2    192.168.1.76/30 [110/20] via 192.168.1.81, 04:40:54, GigabitEthernet0/1
C       192.168.1.80/30 is directly connected, GigabitEthernet0/1
O E2    192.168.1.84/30 [110/20] via 192.168.1.81, 04:40:54, GigabitEthernet0/1
S*   0.0.0.0/0 [1/0] via 192.168.1.81

S-MLS#sh ip ospf neighbor


Neighbor ID     Pri   State           Dead Time   Address         Interface
5.5.5.5           1   FULL/DR         00:00:30    192.168.1.81    GigabitEthernet0/1
```

Figure 11: Verifying OSPF & EIGRP in S-MLS



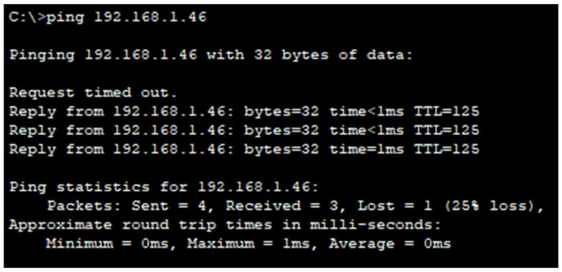
```
C:\>ping 192.168.1.46

Pinging 192.168.1.46 with 32 bytes of data:

Reply from 192.168.1.46: bytes=32 time<1ms TTL=125
Reply from 192.168.1.46: bytes=32 time<1ms TTL=125
Reply from 192.168.1.46: bytes=32 time<1ms TTL=125
Reply from 192.168.1.46: bytes=32 time<1ms TTL=125

Ping statistics for 192.168.1.46:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

Figure 12: Ping request after completing EIGRP



```
C:\>ping 192.168.1.62

Pinging 192.168.1.62 with 32 bytes of data:

Request timed out.
Reply from 192.168.1.62: bytes=32 time<1ms TTL=125
Reply from 192.168.1.62: bytes=32 time<1ms TTL=125
Reply from 192.168.1.62: bytes=32 time<1ms TTL=125

Ping statistics for 192.168.1.62:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

Figure 13: Ping Request after completing OSPF



```
C:\>ping 192.168.1.46

Pinging 192.168.1.46 with 32 bytes of data:

Request timed out.
Reply from 192.168.1.46: bytes=32 time<1ms TTL=125
Reply from 192.168.1.46: bytes=32 time<1ms TTL=125
Reply from 192.168.1.46: bytes=32 time=1ms TTL=125

Ping statistics for 192.168.1.46:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 1ms, Average = 0ms
```

Figure 14: Ping request after completing redistribution

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

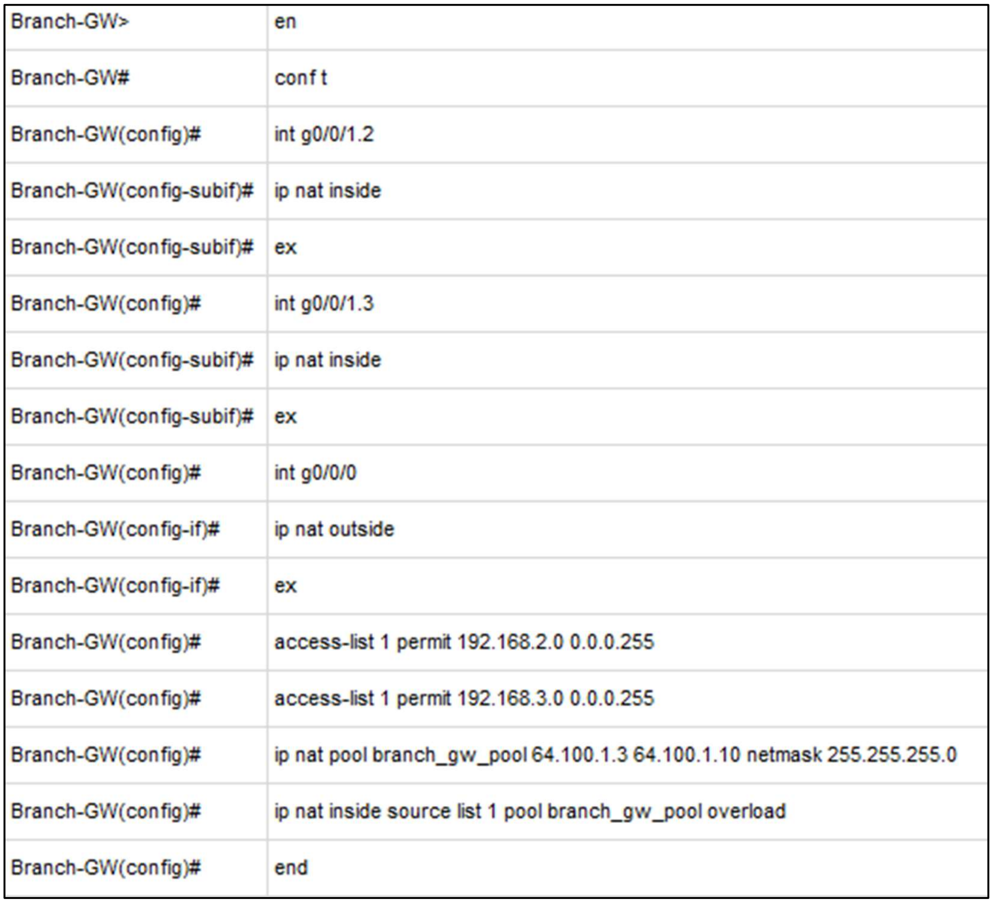
Step 1: Configure Dynamic NAT with PAT on **Core_R1**

- Multiple devices on a local network can be mapped to a single public IP address using dynamic NAT and PAT (Port Address Translation), but each session will use a separate port number. When numerous devices require internet connectivity at the same time, this is helpful for IP address conservation.

~~Step 2: Configure Static NAT on **Core_R1 for web server.**~~

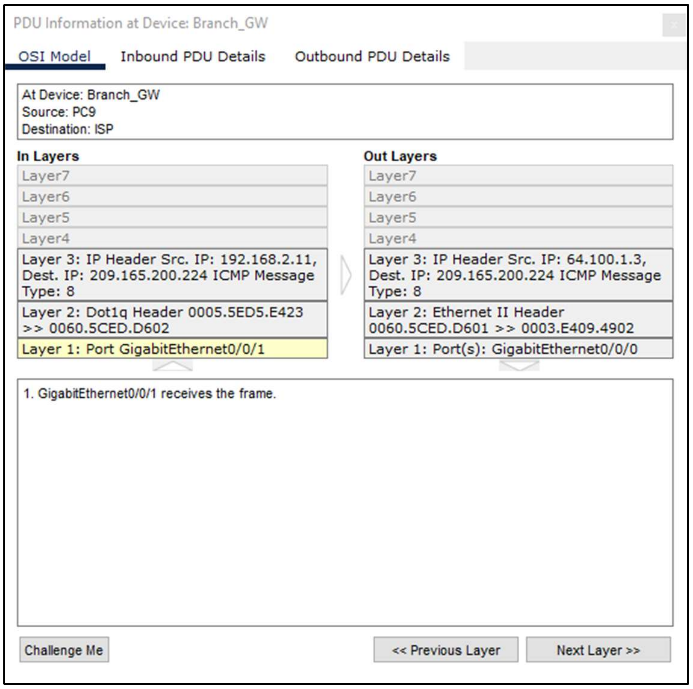
Step 3: Verify Dynamic NAT with PAT and static NAT Implementation.

- Check Figure 16 & 17.



Branch-GW>	en
Branch-GW#	conf t
Branch-GW(config)#	int g0/0/1.2
Branch-GW(config-subif)#	ip nat inside
Branch-GW(config-subif)#	ex
Branch-GW(config)#	int g0/0/1.3
Branch-GW(config-subif)#	ip nat inside
Branch-GW(config-subif)#	ex
Branch-GW(config)#	int g0/0/0
Branch-GW(config-if)#	ip nat outside
Branch-GW(config-if)#	ex
Branch-GW(config)#	access-list 1 permit 192.168.2.0 0.0.0.255
Branch-GW(config)#	access-list 1 permit 192.168.3.0 0.0.0.255
Branch-GW(config)#	ip nat pool branch_gw_pool 64.100.1.3 64.100.1.10 netmask 255.255.255.0
Branch-GW(config)#	ip nat inside source list 1 pool branch_gw_pool overload
Branch-GW(config)#	end

Figure 15: Step 1&2 Commands in Part 6

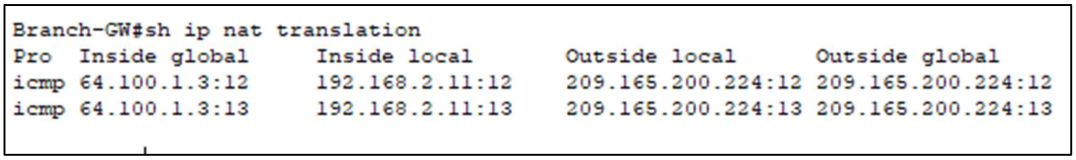


At Device: Branch_GW
Source: PC9
Destination: ISP

In Layers	Out Layers
Layer7	Layer7
Layer6	Layer6
Layer5	Layer5
Layer4	Layer4
Layer 3: IP Header Src. IP: 192.168.2.11, Dest. IP: 209.165.200.224 ICMP Message Type: 8	Layer 3: IP Header Src. IP: 64.100.1.3, Dest. IP: 209.165.200.224 ICMP Message Type: 8
Layer 2: Dot1q Header 0005.5ED5.E423 >> 0060.5CED.D602	Layer 2: Ethernet II Header 0060.5CED.D601 >> 0003.E409.4902
Layer 1: Port GigabitEthernet0/0/1	Layer 1: Port(s): GigabitEthernet0/0/0

1. GigabitEthernet0/0/1 receives the frame.

Figure 16: Verification of NAT via viewing details of message as it travels



```
Branch-GW#sh ip nat translation
Pro  Inside global     Inside local       Outside local      Outside global
icmp 64.100.1.3:12     192.168.2.11:12    209.165.200.224:12 209.165.200.224:12
icmp 64.100.1.3:13     192.168.2.11:13    209.165.200.224:13 209.165.200.224:13
```

Figure 17: Showing NAT IP Address Translation

Part 7: Configure Network Management Features

To configure network management features, first, set up NTP on all devices to synchronize time across the network, ensuring accurate timestamps for logs and events. Then, configure Syslog on all devices to centralize logging and facilitate monitoring and troubleshooting. Finally, enable SNMPv2c on all devices for network monitoring and management, allowing access to device status and performance information.

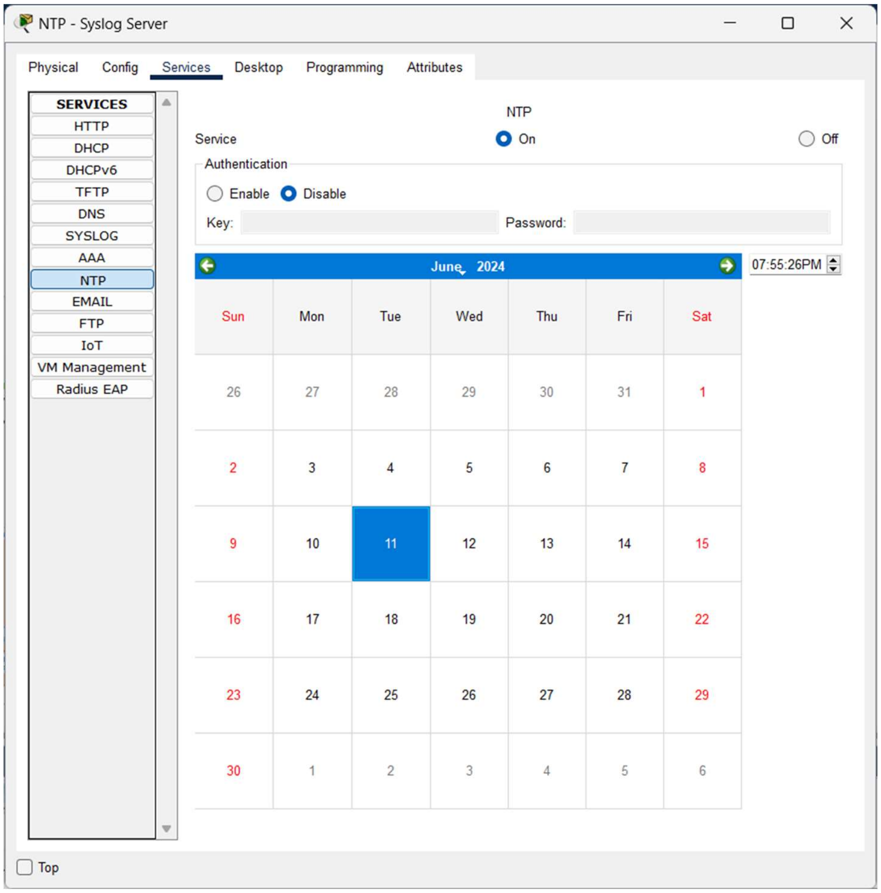
Step 1: Configure NTP on all devices.

- ntp server 192.168.1.69

Step 2: Configure Syslog on all devices

- logging 192.168.1.69
- logging on

Step 3: Configure SNMPv2c on all devices



NTP

Service ● On ○ Off

Authentication

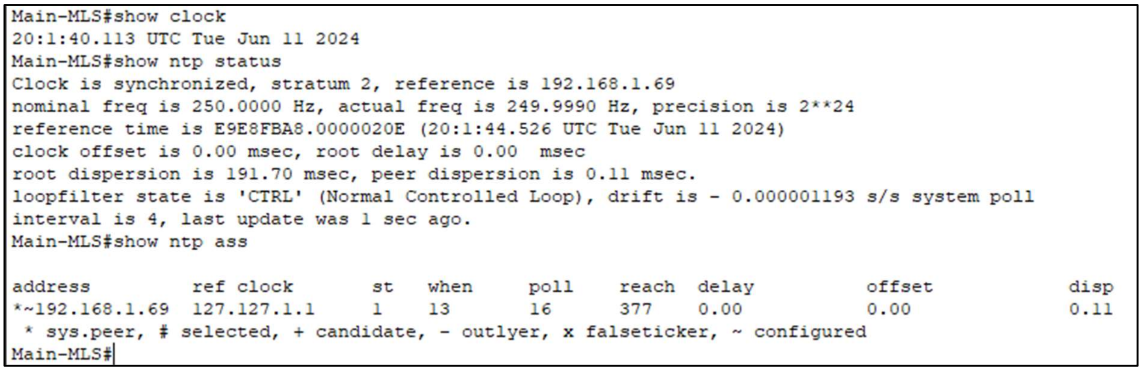
○ Enable ● Disable

Key: Password:

June 2024 07:55:26PM

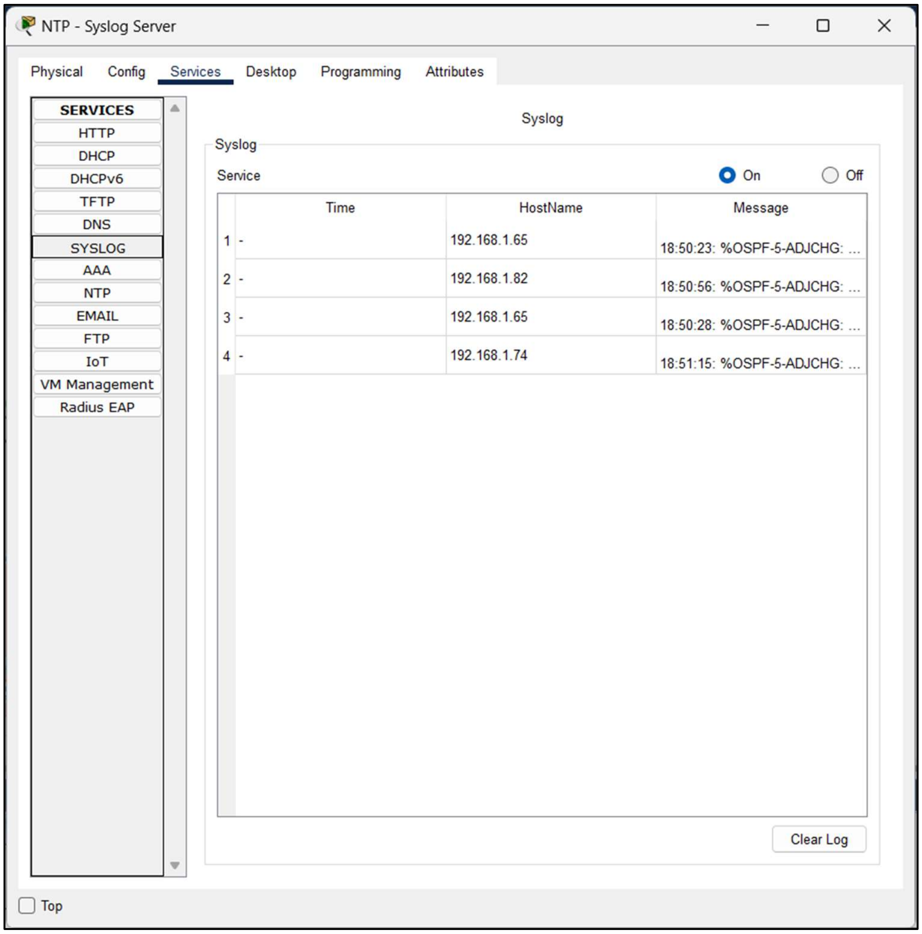
Sun	Mon	Tue	Wed	Thu	Fri	Sat
26	27	28	29	30	31	1
2	3	4	5	6	7	8
9	10	11	12	13	14	15
16	17	18	19	20	21	22
23	24	25	26	27	28	29
30	1	2	3	4	5	6

Figure 18: NTP Setting The Date



```
Main-MLS#show clock
20:1:40.113 UTC Tue Jun 11 2024
Main-MLS#show ntp status
Clock is synchronized, stratum 2, reference is 192.168.1.69
nominal freq is 250.0000 Hz, actual freq is 249.9990 Hz, precision is 2**24
reference time is E9E8FBA8.0000020E (20:1:44.526 UTC Tue Jun 11 2024)
clock offset is 0.00 msec, root delay is 0.00  msec
root dispersion is 191.70 msec, peer dispersion is 0.11 msec.
loopfilter state is 'CTRL' (Normal Controlled Loop), drift is - 0.000001193 s/s system poll
interval is 4, last update was 1 sec ago.
Main-MLS#show ntp ass

address         ref clock       st   when     poll    reach  delay          offset            disp
*~192.168.1.69  127.127.1.1     1    13       16      377    0.00           0.00              0.11
 * sys.peer, # selected, + candidate, - outlyer, x falseticker, ~ configured
Main-MLS#
```

Figure 19: Verifying Clock and NTP status



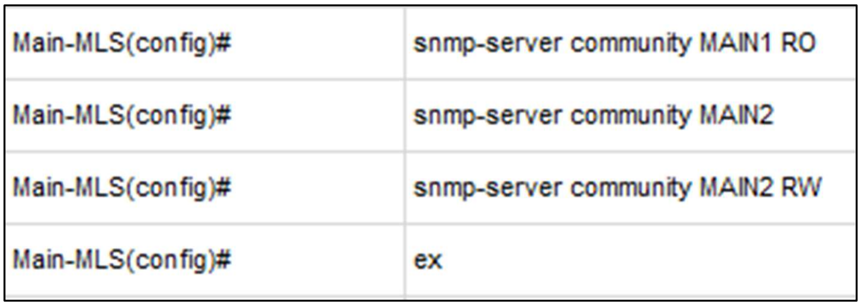
Syslog

Syslog

Service ● On ○ Off

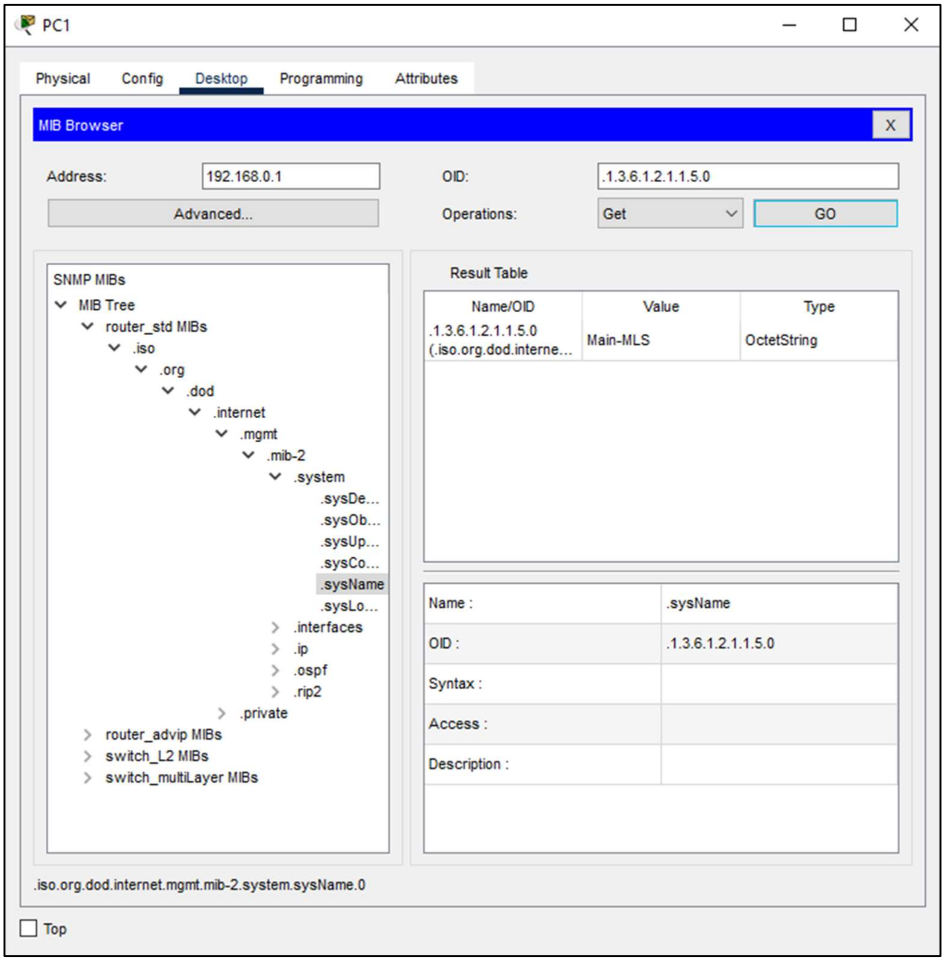
	Time	HostName	Message
1	-	192.168.1.65	18:50:23: %OSPF-5-ADJCHG: ...
2	-	192.168.1.82	18:50:56: %OSPF-5-ADJCHG: ...
3	-	192.168.1.65	18:50:28: %OSPF-5-ADJCHG: ...
4	-	192.168.1.74	18:51:15: %OSPF-5-ADJCHG: ...

Figure 20: SYSLOG Verification



Main-MLS(config)#	snmp-server community MAIN1 RO
Main-MLS(config)#	snmp-server community MAIN2
Main-MLS(config)#	snmp-server community MAIN2 RW
Main-MLS(config)#	ex

Figure 21: Configuration of Step 3



Address: 192.168.0.1

OID: .1.3.6.1.2.1.1.5.0

Operations: Get

Result Table

Name/OID	Value	Type
.1.3.6.1.2.1.1.5.0 (.iso.org.dod.interne...	Main-MLS	OctetString

Name :	.sysName
OID :	.1.3.6.1.2.1.1.5.0
Syntax :	
Access :	
Description :	

.iso.org.dod.internet.mgmt.mib-2.system.sysName.0

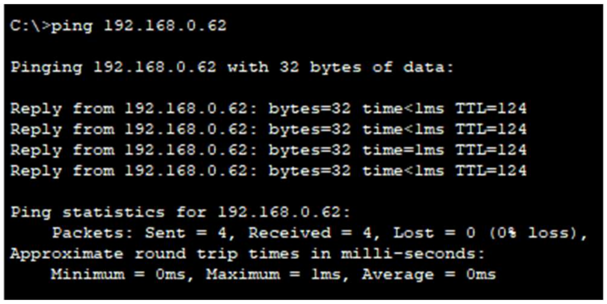
Figure 22: Verification of step 3

Part 8: Verify Connectivity

Verify that all PCs can ping each other.

- Regarding the verification of whether PC's can ping each other in the same area OSPF, recall Figure 13. We were pinging from PC-1 in the Main Building to PC-3 in the S-Building via OSPF.
- Regarding the verification of whether PC's can ping each other in the same area EIGRP, recall Figure 12. We were pinging from PC-7 in the R-Building to PC-5 in the N-Building via EIGRP.
- Regarding the verification of whether PC's can ping each other in multiple areas via different routing protocols, IE: OSPF, EIGRP. Recall figure 14, we were pinging from PC-1 in the Main Building to PC-5 in the N-Building via EIGRP.

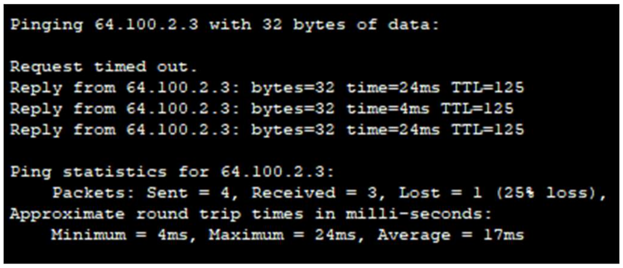
After applying static routing: Route to different networks through ISP.



```
C:\>ping 192.168.0.62

Pinging 192.168.0.62 with 32 bytes of data:

Reply from 192.168.0.62: bytes=32 time<1ms TTL=124
Reply from 192.168.0.62: bytes=32 time<1ms TTL=124
Reply from 192.168.0.62: bytes=32 time=1ms TTL=124
Reply from 192.168.0.62: bytes=32 time<1ms TTL=124

Ping statistics for 192.168.0.62:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 1ms, Average = 0ms
```

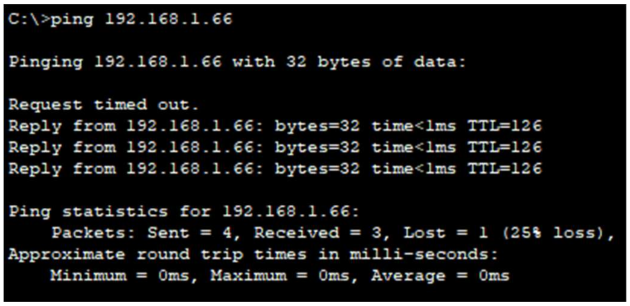
Figure 23: Ping Request From PC-9 (Miu Branch-1) to PC-1 (Main Building)

After applying static routing: after configuring Home Network.



```
Pinging 64.100.2.3 with 32 bytes of data:

Request timed out.
Reply from 64.100.2.3: bytes=32 time=24ms TTL=125
Reply from 64.100.2.3: bytes=32 time=4ms TTL=125
Reply from 64.100.2.3: bytes=32 time=24ms TTL=125

Ping statistics for 64.100.2.3:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
Approximate round trip times in milli-seconds:
    Minimum = 4ms, Maximum = 24ms, Average = 17ms
```

Figure 24: Ping Request From PC-1 (Main Building) to Tablet (Home Network)

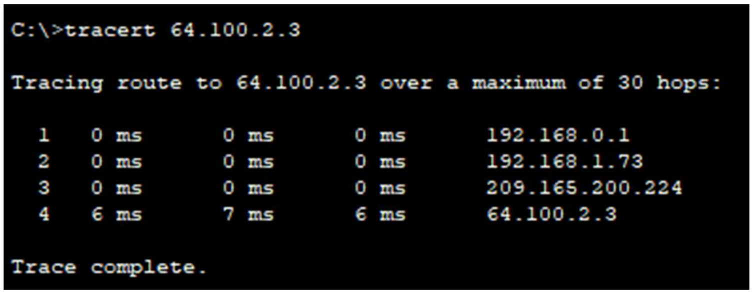


```
C:\>ping 192.168.1.66

Pinging 192.168.1.66 with 32 bytes of data:

Request timed out.
Reply from 192.168.1.66: bytes=32 time<1ms TTL=126
Reply from 192.168.1.66: bytes=32 time<1ms TTL=126
Reply from 192.168.1.66: bytes=32 time<1ms TTL=126

Ping statistics for 192.168.1.66:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

Figure 25: : Ping Request From PC-5 (N-Building) to DHCP Server (Server Room)

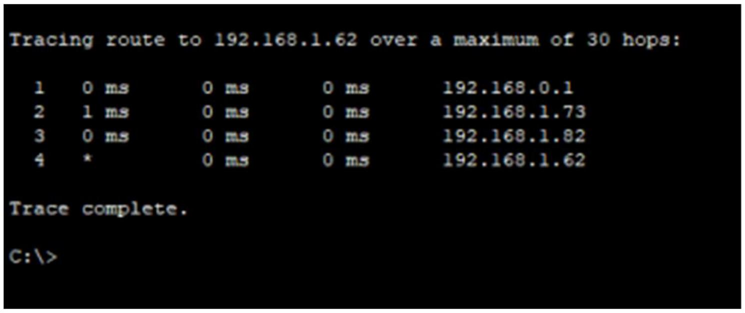
Regarding Figure 20: We were testing that a PC can ping any server in the server room, this was proved possible as presented in the figure.

Trace Routes:



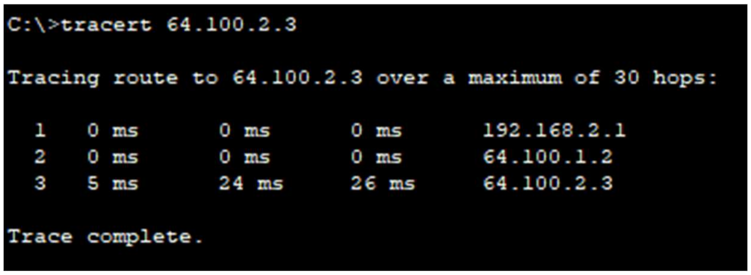
```
C:\>tracert 64.100.2.3

Tracing route to 64.100.2.3 over a maximum of 30 hops:

  1   0 ms      0 ms      0 ms      192.168.0.1
  2   0 ms      0 ms      0 ms      192.168.1.73
  3   0 ms      0 ms      0 ms      209.165.200.224
  4   6 ms      7 ms      6 ms      64.100.2.3

Trace complete.
```

Figure 26: PC-0 (Main Building) to Tablet (Home Network)



```
Tracing route to 192.168.1.62 over a maximum of 30 hops:

  1   0 ms      0 ms      0 ms      192.168.0.1
  2   1 ms      0 ms      0 ms      192.168.1.73
  3   0 ms      0 ms      0 ms      192.168.1.82
  4   *         0 ms      0 ms      192.168.1.62

Trace complete.

C:\>
```

Figure 27: PC-1 (Main Building) to PC-3 (S-Building)



```
C:\>tracert 64.100.2.3

Tracing route to 64.100.2.3 over a maximum of 30 hops:

  1   0 ms      0 ms      0 ms      192.168.2.1
  2   0 ms      0 ms      0 ms      64.100.1.2
  3   5 ms      24 ms     26 ms     64.100.2.3

Trace complete.
```

Figure 28: PC-9 (Miu Branch-1) to Tablet (Home Network)

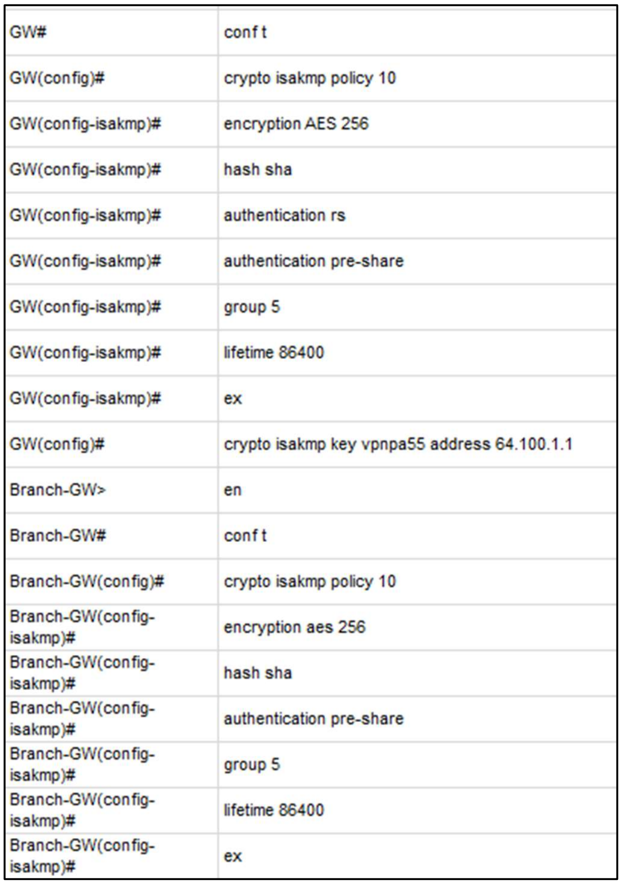
This Array of figures shows full capability of pinging/trace routing from any device to any device.

Extra: Configure Site to Site VPN

Establishing a secure connection between two networks is the first step in configuring a site-to-site VPN. We will create an IPsec VPN tunnel between two Cisco routers. The configuration involves applying the crypto map to the interfaces, specifying the IPsec transform set, ISAKMP (Internet Security Association and Key Management Protocol) policy, and so on.

The Implementation is established in three phases, each phase will have the same commands in both GW and Branch-GW.

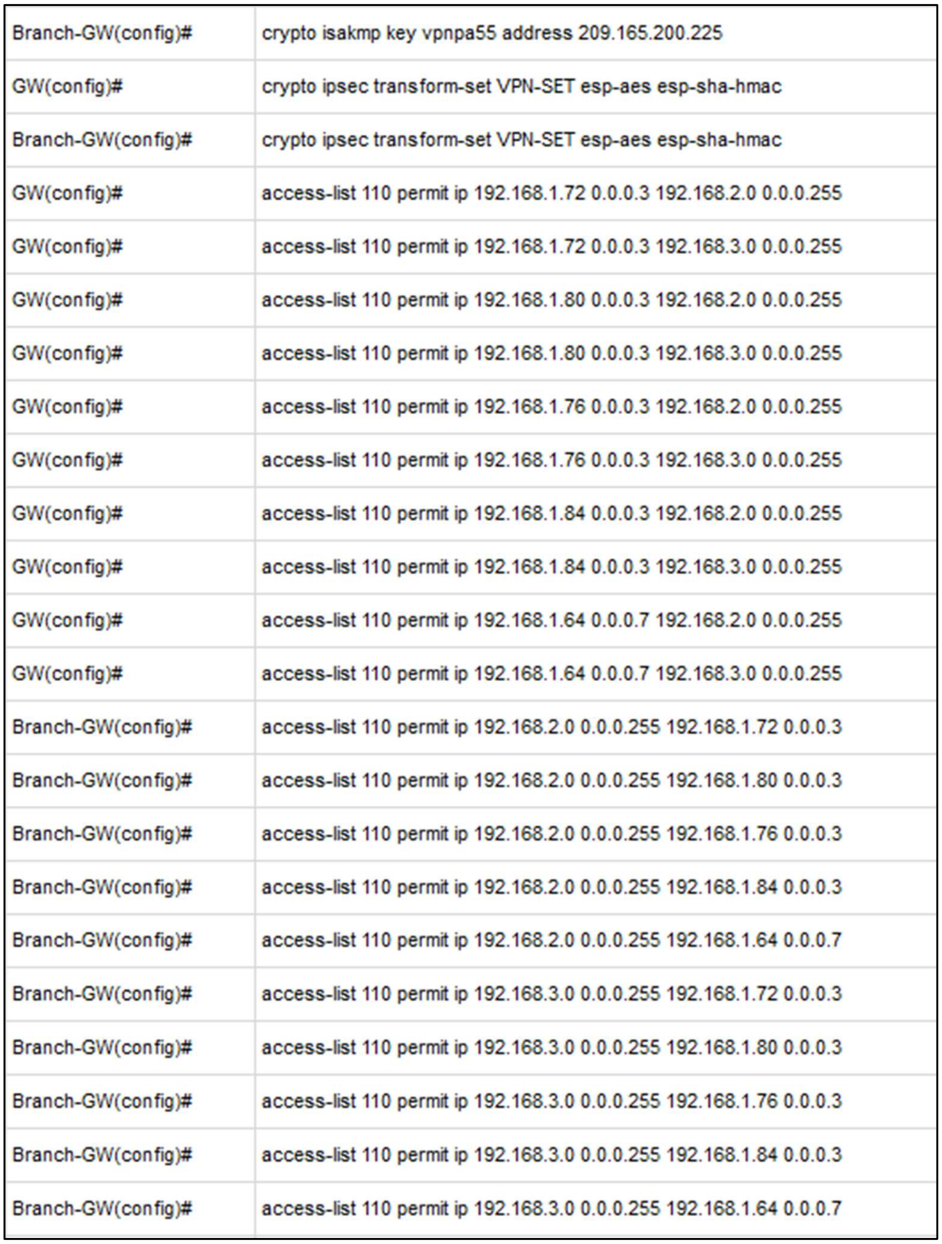
Phase 1: Configure ISAKMP Policy



GW#	conf t
GW(config)#	crypto isakmp policy 10
GW(config-isakmp)#	encryption AES 256
GW(config-isakmp)#	hash sha
GW(config-isakmp)#	authentication rs
GW(config-isakmp)#	authentication pre-share
GW(config-isakmp)#	group 5
GW(config-isakmp)#	lifetime 86400
GW(config-isakmp)#	ex
GW(config)#	crypto isakmp key vpnpa55 address 64.100.1.1
Branch-GW>	en
Branch-GW#	conf t
Branch-GW(config)#	crypto isakmp policy 10
Branch-GW(config-isakmp)#	encryption aes 256
Branch-GW(config-isakmp)#	hash sha
Branch-GW(config-isakmp)#	authentication pre-share
Branch-GW(config-isakmp)#	group 5
Branch-GW(config-isakmp)#	lifetime 86400
Branch-GW(config-isakmp)#	ex

Figure 29: Configuring ISAKMP Policy

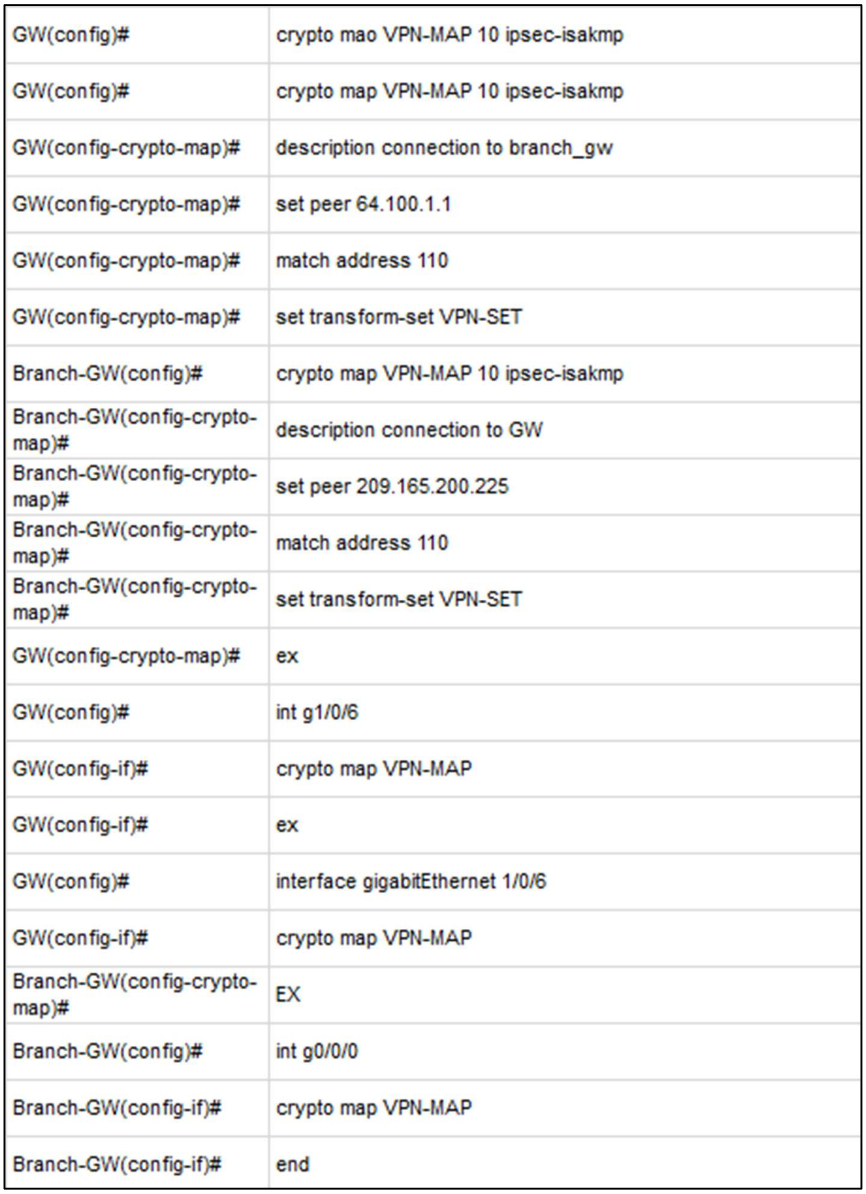
Phase 2: Create IPsec Transform Set and crypto map



Branch-GW(config)#	crypto isakmp key vpnpa55 address 209.165.200.225
GW(config)#	crypto ipsec transform-set VPN-SET esp-aes esp-sha-hmac
Branch-GW(config)#	crypto ipsec transform-set VPN-SET esp-aes esp-sha-hmac
GW(config)#	access-list 110 permit ip 192.168.1.72 0.0.0.3 192.168.2.0 0.0.0.255
GW(config)#	access-list 110 permit ip 192.168.1.72 0.0.0.3 192.168.3.0 0.0.0.255
GW(config)#	access-list 110 permit ip 192.168.1.80 0.0.0.3 192.168.2.0 0.0.0.255
GW(config)#	access-list 110 permit ip 192.168.1.80 0.0.0.3 192.168.3.0 0.0.0.255
GW(config)#	access-list 110 permit ip 192.168.1.76 0.0.0.3 192.168.2.0 0.0.0.255
GW(config)#	access-list 110 permit ip 192.168.1.76 0.0.0.3 192.168.3.0 0.0.0.255
GW(config)#	access-list 110 permit ip 192.168.1.84 0.0.0.3 192.168.2.0 0.0.0.255
GW(config)#	access-list 110 permit ip 192.168.1.84 0.0.0.3 192.168.3.0 0.0.0.255
GW(config)#	access-list 110 permit ip 192.168.1.64 0.0.0.7 192.168.2.0 0.0.0.255
GW(config)#	access-list 110 permit ip 192.168.1.64 0.0.0.7 192.168.3.0 0.0.0.255
Branch-GW(config)#	access-list 110 permit ip 192.168.2.0 0.0.0.255 192.168.1.72 0.0.0.3
Branch-GW(config)#	access-list 110 permit ip 192.168.2.0 0.0.0.255 192.168.1.80 0.0.0.3
Branch-GW(config)#	access-list 110 permit ip 192.168.2.0 0.0.0.255 192.168.1.76 0.0.0.3
Branch-GW(config)#	access-list 110 permit ip 192.168.2.0 0.0.0.255 192.168.1.84 0.0.0.3
Branch-GW(config)#	access-list 110 permit ip 192.168.2.0 0.0.0.255 192.168.1.64 0.0.0.7
Branch-GW(config)#	access-list 110 permit ip 192.168.3.0 0.0.0.255 192.168.1.72 0.0.0.3
Branch-GW(config)#	access-list 110 permit ip 192.168.3.0 0.0.0.255 192.168.1.80 0.0.0.3
Branch-GW(config)#	access-list 110 permit ip 192.168.3.0 0.0.0.255 192.168.1.76 0.0.0.3
Branch-GW(config)#	access-list 110 permit ip 192.168.3.0 0.0.0.255 192.168.1.84 0.0.0.3
Branch-GW(config)#	access-list 110 permit ip 192.168.3.0 0.0.0.255 192.168.1.64 0.0.0.7

Figure 30: Creating IPsec Transform Set and crypto map

Phase 3: Apply Crypto Map to the Interface



GW(config)#	crypto mao VPN-MAP 10 ipsec-isakmp
GW(config)#	crypto map VPN-MAP 10 ipsec-isakmp
GW(config-crypto-map)#	description connection to branch_gw
GW(config-crypto-map)#	set peer 64.100.1.1
GW(config-crypto-map)#	match address 110
GW(config-crypto-map)#	set transform-set VPN-SET
Branch-GW(config)#	crypto map VPN-MAP 10 ipsec-isakmp
Branch-GW(config-crypto-map)#	description connection to GW
Branch-GW(config-crypto-map)#	set peer 209.165.200.225
Branch-GW(config-crypto-map)#	match address 110
Branch-GW(config-crypto-map)#	set transform-set VPN-SET
GW(config-crypto-map)#	ex
GW(config)#	int g1/0/6
GW(config-if)#	crypto map VPN-MAP
GW(config-if)#	ex
GW(config)#	interface gigabitEthernet 1/0/6
GW(config-if)#	crypto map VPN-MAP
Branch-GW(config-crypto-map)#	EX
Branch-GW(config)#	int g0/0/0
Branch-GW(config-if)#	crypto map VPN-MAP
Branch-GW(config-if)#	end

Figure 31: Applying Crypto Map to the Interface

Through our extensive efforts in trying to make this work, it works with Branch-GW correctly, on the other hand, it does not work with GW. The reason for this is that the MLS in our model used for our project does not support site to site VPN, similar to how step 2 in Part 6.

The error we experienced happened in the last command (applying the crypto map to the interface) in the MLS-GW.