

COMPUTER NETWORKS PROJECT

Abstract

This work focuses on the development and deployment of a Local Area Network (LAN) tailored for a university simulating the MIU (CAN) Campus Area Network infrastructure, designed to deliver a secure, high-performance connectivity across multiple buildings/departments. - With the help of Cisco Packet Tracer for the simulation and design, the network will support key University functions emphasizing on three main components : Buildings (Main, N , S and R), the MIU-Branch, and the Wireless home network utilizing key technologies used in the design like : VLANs, EIGRP,OSPF,DHCP,NAT,PAT, NTP, syslog, wireless technology , and many more.

COMPUTER NETWORKS PROJECT

Abstract

Contents:

# 1-Table of Tables

A collection of all the used tables in the design phase in step 1 including:

* VLSM Design
* Addressing Table
* Router OSPF IDs
* DHCP Servers Table

# 2-System Description

Brief about the logical topology and diagram

# 3-Integration Screenshots

Includes screenshots to verify device configurations and result of command like:

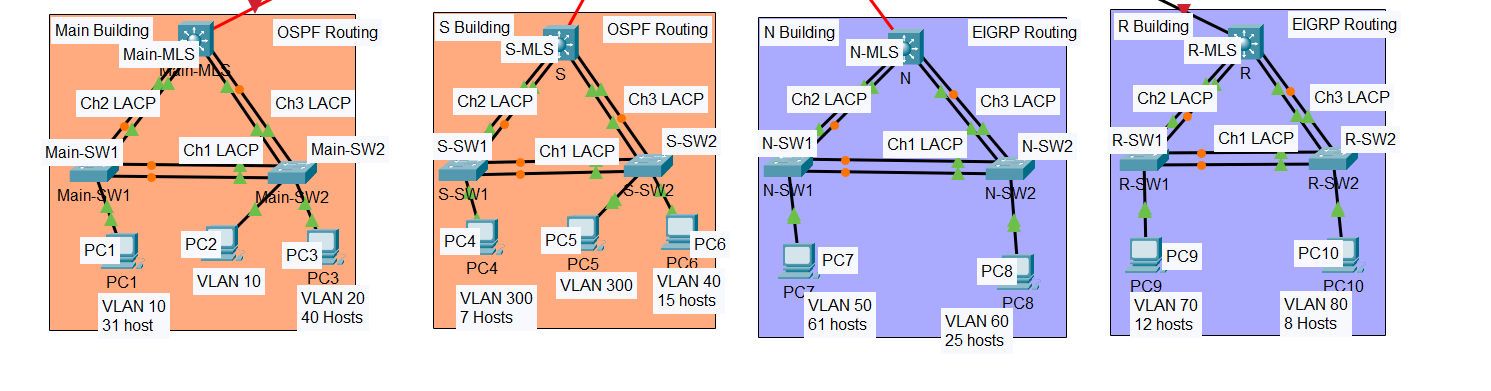
* MLS and layer 2 switches
  + VLANs
  + Trunks
  + EtherChannel
  + OSPF/EIGRP routing
  + DHCP
  + Nat /PAT
  + VPN
  + Wireless home network
* Pinging all devices

Table of Contents

# 1-VLSM Design:

**10.0.0.0/8 10.00000000.00000000.00000000/8 255.0.0.0**

1. **VLAN 10** will require **31** host IP address
2. **VLAN 20** will require **40** host IP address
3. **VLAN 300** will require **7** host IP address
4. **VLAN 40** will require **15** host IP address
5. **VLAN 50** will require **61** host IP address
6. **VLAN 60** will require **25** host IP address
7. **VLAN 70** will require **12** host IP address
8. **VLAN 80** will require **8** host IP address



**Reordering:**

1. **-VLAN 50** will require **61** host IP address No. of Hosts = 2h -2 = 26 -2= 62 host / 26
2. **-VLAN 20** will require **40** host IP address No. of Hosts = 2h -2 = 26 -2= 62 host / 26

1-VLSM Design(Cont.)

1. **-VLAN 10** will require **31** host IP address No. of Hosts = 2h -2 = 26 -2= 62 host / 2**-VLAN 60** will require **25** host IP address No. of Hosts = 2h -2 = 25 -2= 30 host / 27
2. **-VLAN 40** will require **15** host IP address No. of Hosts = 2h -2 = 25 -2= 30 host / 27
3. **-VLAN 70** will require **12** host IP address No. of Hosts = 2h -2 = 24 -2= 14 host / 28
4. **-VLAN 80** will require **8** host IP address No. of Hosts = 2h -2 = 24 -2= 14 host / 28
5. **-VLAN 300** will require **7** host IP address No. of Hosts = 2h -2 = 24 -2= 14 host / 28
6. **From Main-MLS to MIU-MIU-GW** will require will require **2** hosts IP address. No. of Hosts = 2h -2 = 22 -2= 4 host / 30
7. **From N-MLS to MIU-MIU-GW** will require will require **2** hosts IP address. No. of Hosts = 2h -2 = 22 -2= 4 host / 30
8. **From S-MLS to MIU-MIU-GW** will require **2** hosts IP address. No. of Hosts = 2h -2 = 22-2=

4 host / 30

1. **From SW-S to MIU-MIU-GW** will require **7** hosts IP address No No. of Hosts = 2h -2 = 24 -2= 14 host / 28

/26 255.255.255.11000000 /27 255.255.255.11100000 /28 255.255.255.11110000

255.255.255.192 255.255.255.224 255.255.255.240

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Subnet | Network Address | First Host Address | Last Host Address | Broadcast Address |
| VLAN 50 | **10.0.0.0 /26** | **10.0.0.1 /26** | **10.0.0.62 /26** | **10.0.0.63 /26**  0+63 |
| VLAN 20 | **10.0.0.64 /26** | **10.0.0.65 /26** | **10.0.0.126 /26** | **10.0.0.127 /26**  64+63 |
| VLAN 10 | **10.0.0.128 /26** | **10.0.0.129 /26** | **10.0.0.190 /26** | **10.0.0.191 /26**  128+63 |
| VLAN 60 | **10.0.0.192 /27** | **10.0.0.193 /27** | **10.0.0.222 /27** | **10.0.0.223 /27**  192+31 |
| VLAN 40 | **10.0.0.224 /27** | **10.0.0.225 /27** | **10.0.0.254 /27** | **10.0.0.255 /27**  224+31 |
| VLAN 70 | **10.0.1.0 /28** | **10.0.1.1 /28** | **10.0.1.14 /28** | **10.0.1.15 /28**  0+15 |
| VLAN 80 | **10.0.1.16 /28** | **10.0.1.17/28** | **10.0.1.30/28** | **10.0.1.31/28**  16+15 |
| VLAN 300 | **10.0.1.32 /28** | **10.0.1.33 /28** | **10.0.1.46/28** | **10.0.1.47/28**  32+15 |
| From Main-MLS to MIU-MIU-GW | **10.0.1.48/30** | **10.0.1.49/30** | **10.0.1.50/30** | **10.0.1.51/30**  **48+3** |
| From N-MLS to MIU-MIU-GW | **10.0.1.52/30** | **10.0.1.53/30** | **10.0.1.54/30** | **10.0.1.55/30**  **52+3** |
| From S-MLS to MIU-MIU-GW | **10.0.1.56/30** | **10.0.1.57/30** | **10.0.1.58/30** | **10.0.1.59/30**  **56+3** |
| From R-MLS to MIU-MIU-GW | **10.0.1.60/30** | **10.0.1.61/30** | **10.0.1.62/30** | **10.0.1.63/30**  **60+3** |
| From SW-S to MIU-MIU-GW | **10.0.1.64/28** | **10.0.1.65/28** | **10.0.1.78/28** | **10.0.1.79/28**  **64+15** |
| VLAN 2 | **192.168.2.0/24** | **192.168.2.1/24** | **192.168.2.254/24** | **192.168.2.255/24**  **0+255** |
| VLAN 3 | **192.168.3.0/24** | **192.168.3.1/24** | **192.168.3.254/24** | **192.168.3.255/24** |

Addressing Table PCs:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| PC-number | VLAN ID | IP Address | Subnet Mask | Default Gateway |
|  |  |  |  |  |
| MIU | | | | |
| PC-1 |  | **10.0.0.131 /26**  (From DHCP Server) | **255.255.255.192**  From DHCP Server | **10.0.0.129**  From DHCP Server |
| PC-2 |  | **10.0.0.132 /26**  (From DHCP Server) | **255.255.255.192**  From DHCP Server | **10.0.0.129**  From DHCP Server |
| PC-3 |  | **10.0.0.67 /26**  (From DHCP Server) | **255.255.255.192**  From DHCP Server | **10.0.0.65**  From DHCP Server |
| PC-4 |  | **10.0.1.35 /28**  (From DHCP Server) | **255.255.255.240**  (From DHCP Server) | **10.0.1.33**  From DHCP Server |
| PC-5 |  | **10.0.1.36 /28**  (From DHCP Server) | **255.255.255.240**  (From DHCP Server) | **10.0.1.33**  From DHCP Server |
| PC-6 |  | **10.0.0.227 /27**  (From DHCP Server) | **255.255.255.224**  (From DHCP Server) | **10.0.0.225**  (From DHCP Server) |
| PC-7 |  | **10.0.0.3 /26** | **255.255.255.192** | **10.0.0.1** |
| PC-8 |  | **10.0.0.195 /27** | **255.255.255.224** | **10.0.0.193** |
| PC-9 |  | **10.0.1.3 /28** | **255.255.255.240** | **10.0.1.1** |
| PC-10 |  | **10.0.1.19/28** | **255.255.255.240** | **10.0.1.17** |
| MIU\_ Branch 1 | | | | |
| PC-11 |  | **192.168.3.3/24**  From DHCP Server | **255.255.255.0**  From DHCP Server | From DHCP Server |
| PC-12 |  | **192.168.3.3/24**  From DHCP Server | **255.255.255.0**  From DHCP Server | From DHCP Server |
| Wireless Home Network | | | | |
| Laptop |  | 192.168.10.10/25 | 255.255.255.128 | **192.168.10.1** |
| Tablet |  | 192.168.10.30/25 | 255.255.255.128 | **192.168.10.1** |
| Smartphone |  | 192.168.10.20/25 | 255.255.255.128 | **192.168.10.1** |
| Servers | | | | |
| DHCP Server |  | 10.0.1.67 | 255.255.255.240 | 10.0.1.66 |
| Email Server |  | 10.0.1.68 | 255.255.255.240 | 10.0.1.66 |
| Web server |  | 10.0.1.70 | 255.255.255.240 | 10.0.1.66 |
| DNS server |  | 10.0.1.72 | 255.255.255.240 | 10.0.1.66 |
| NTP and Syslog server |  | 10.0.1.74 | 255.255.255.240 | 10.0.1.66 |

# Addressing Table:

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Device | Interface | Address | Subnet Mask | Default Gateway | VLAN ID |
| Main-MLS | G1/1/1 | **10.0.1.49/30** | **255.255.255.252** |  |  |
| VLAN 10 | **10.0.0.129 /26** | **255.255.255.192** |  | **10** |
| VLAN 20 | **10.0.0.65 /26** | **255.255.255.192** |  | **20** |
| S-MLS | G1/1/1 | **10.0.1.57/30** | **255.255.255.252** |  |  |
| VLAN  300 | **10.0.1.33 /28** | **255.255.255.240** |  | **300** |
| VLAN  40 | **10.0.0.225 /27** | **255.255.255.224** |  | **40** |
| N-MLS | G1/1/1 | **10.0.1.53/30** | **255.255.255.252** |  |  |
| VLAN  50 | **10.0.0.1 /26** | **255.255.255.192** |  | **50** |
| VLAN  60 | **10.0.0.193 /27** | **255.255.255.224** |  | **60** |
| R-MLS | G1/0/5 | **10.0.1.60/30** | **255.255.255.252** |  |  |
| VLAN  70 | **10.0.1.1 /28** | **255.255.255.240** |  | **70** |
| VLAN  80 | **10.0.1.17/28** | **255.255.255.240** |  | **80** |
| MIU-MIU-GW | Gig0/0 | **209.165.200.226/28** | **255.255.255.240** |  |  |
| Gig0/1 | **10.0.1.61/30** | **255.255.255.252** |  |  |
| Gig0/0/0 | **10.0.1.64/30** | **255.255.255.252** |  |  |
| Gig0/1/0 | **10.0.1.50/30** | **255.255.255.252** |  |  |
| Gig0/2/0 | **10.0.1.58/30** | **255.255.255.252** |  |  |
| Gig0/3/0 | |  | | --- | | **10.0.1.54/30** |  |  | | --- | |  | | **255.255.255.224** |  |  |
| ISP | **Gig 0/0** | **209.165.200.225** | **255.255.255.240** |  |  |
| **Gig 0/1** | **64.100.1.1** | **255.255.255.224** |  |  |
| **Gig 0/2** | **64.100.2.1** | **255.255.255.224** |  |  |
| Branch-GW | **Gig 0/0.2** | **192.168.2.1** | **255.255.255.0** |  |  |
| **Gig 0/0.3** | **192.168.3.1** | **255.255.255.0** |  |  |
| **Gig 0/1** | **64.100.1.2** | **255.255.255.224** |  |  |
| Wireless Home Router | **G0/1** | **64.100.2.2** | **255.255.255.224** |  |  |
| **Router IP** | **192.168.10.1** | **255.255.255.128** |  |  |

# Router OSPF IDs:

|  |  |
| --- | --- |
| Router/ Layer 3 switch | Router ID |
| MIU-GW | 1.1.1.1 |
| Main-MLS | 2.2.2.2 |
| S-MLS | 3.3.3.3 |
| SW-S | 4.4.4.4 |

System Description

# Step 1(**Design and Implement a VLSM Addressing Scheme**):

In this step, we have designed a VLSM addressing scheme given a network address   **10.0.0.0/8** and host requirements. Configuring the addressing on routers, switches, and network hosts.

First, we determined the number of hosts required for each subnet/VLSM and then reordering the vlans from most to least hosts. After that, we have determined the number of bits required to be taken from the host portion to the network portion to be the subnet bits by selecting the smallest number of bits n that when 2n-2 is greater than the subnet required host (Removing 2 addresses for the reserved host and broadcast address).

After that, we used each subnet to determine the first and last host address as well as the broadcast and the network address as seen in the VLSM design table as seen in the tables in the section above.

In the following step, we have setup the addressing table where we used the 2 host subnets between each buildings MLS the MIU-Default-gateway where one ip address (which is the first of the subnet) is set on the MLS side, where the other is the side of the MIU-GW on the physical interfaces both sides. Additionally, we selected the first usable address of each VLAN in the addressing to be configured in the router **(where first address for Router (MLS) second is for Layer 2 switch and the rest for the hosts connected).**

When it comes to the PCs configuration, each PC within each VLAN was assigned a temporary static IP address for testing with the VLAN range it is associated with. However, at the end we have configured the DHCP to dynamically assign the IP, Subnet mask, and default gateway.

Finally, the DHCP servers was assigned IP addresses of the range of its subnet as seen its table above.

Part 2 basic configuration

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

We Used the addressing table to manually configure the PCs IP addresses in order to be able to have them ping each other later on.

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

a.     Configure allDevices with the following:

1)     Prevent the router from attempting to resolve incorrectly entered commands as domain names. ***Command: S-MlS (Config)No IP domain lookup***

2)     Host name for all devices. ***Command: S-MlS (Config) hostname name***

3)     Set the minimum password length to **10** characters.

***Command: S-MlS (Config) Securtity Passwords min-length 10***

4)     Use the **MIU1234567**password for Console access password.

***Command: S-MlS (Config)line con 0***

***Command: S-MlS (Config)Password MIU1234567***

***Command: S-MlS (Config)login***

***Command: S-MlS (Config)exit***

5)     Use the **CSC1234567** secret password.

***Command: S-MlS (Config)enable secret CSC1234567***

6)     Encrypt the clear text passwords.

7)     Configure an appropriate MOTD Banner.

***Command: S-MlS (Config)banner motd #Unauthorized access is prohibited#***

b.     Configure addressing for all devices according to the Addressing Table.

c.      Configure SSH for all routers.

***Commands under config t:***

***Ip domain-name miu.edu***

***Crypto key generate rsa***

***1024***

***line vty 0 4***

***login local***

***transport input ssh***

***exit***

A screenshot of a computer

AI-generated content may be incorrect.

A screenshot of a computer

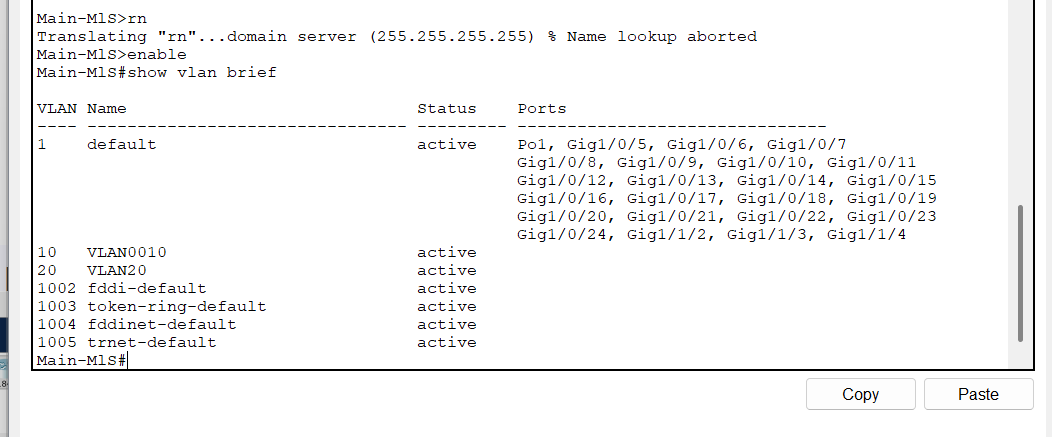
AI-generated content may be incorrect.

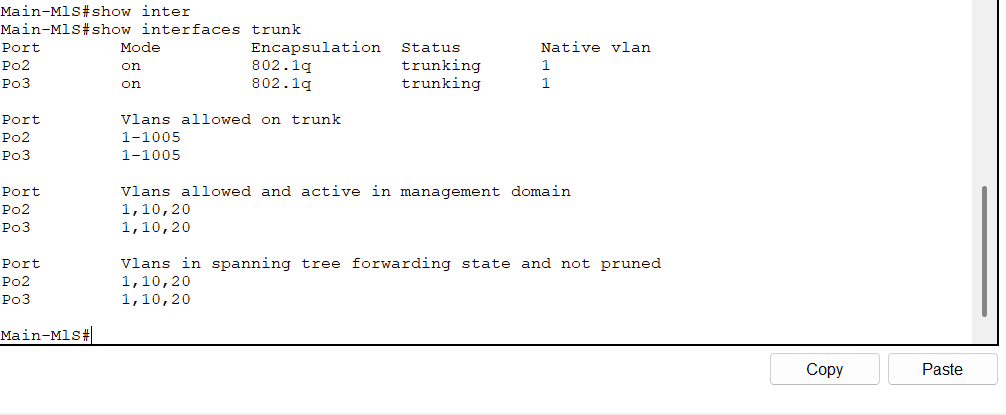
A screenshot of a computer

AI-generated content may be incorrect.

Step 3 **Configure Network Infrastructure Settings (VLANs, Trunking, Inter-VLAN Routing EtherChannel).**

When it comes to the switching phase, we started off by creating the required vlans by entering on each Layer 2 switch and defining the vlans connected to it using the interface vlan 10 for example and entering the associated vlan of the PCs followed by their IP address and subnet mask, and then writing no shutdown to ensure the network is UP.Additionally, we had to do the same with each multilayer switch to be able to communicate with every VLAN. Kindly find an example of vlans defined on a MLS (Main-MLS) using **the show vlan brief command**:



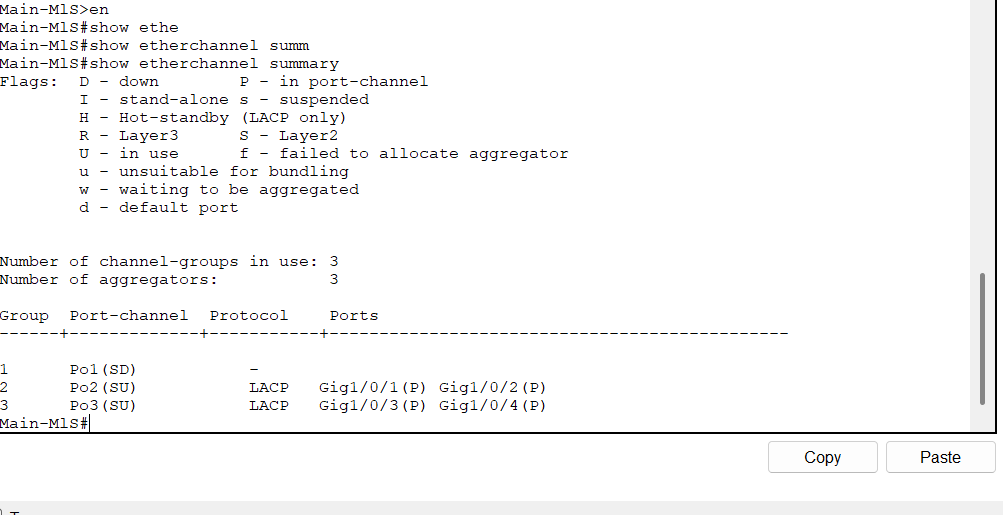
After that, comes the trunking between the switches (either Layer 2 or Layer 3) ;On the other side, configuring an access between the Layer 2 switch and the PCs.done by entering global config mode and then selecting the interface (either separately or using the **Ip interface range** command. Then, using the **switchport mode access** between the PC and the Switch and then **switchport mode trunk** between the switches please find below the trunk configuration showed by **show interface trunk** command using the 802.1Q encapsulation protocol:

In order to access the MLS(Multilayer Switch) remotely we have configured a SVI from the ip ranges between the building and the MIU-DG even for remote access.

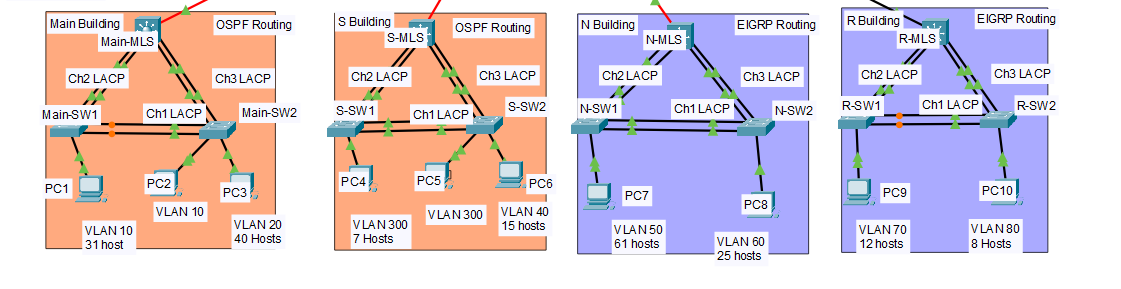
Due to many advantages, we have utilized an EtherChannel between each of the switches and others in order to have bonuses like:

* Reducing traffic Congestion
* Maximizing Bandwidth
* Redundancy for fault tolerance

Done by selecting each 2 physical interfaces visible and converting them to 1 logical interface by selecting them using **ip interface range** command and then using the **channel-protocol lacp** to set the etherchannel protocol to LACP. After that, used the **channel-group <number of group> mode active** to initiatenegotiation**.** Finally , in this section we used the **show etherchannel summary command** to view etherchannel configuration showing the details which have to be SU indicating its UP:



Find below the etherchannel buildings connection images:



# Step 4 **(Configure Routing Protocols)**:

In order to allow different LANs to communicate together using intermediary routers dynamic router protocols are used in order to allow discovery of networks such as: OSPF and EIGRP each configured in similar ways.

1-OSPF Routing (For the main and S building):

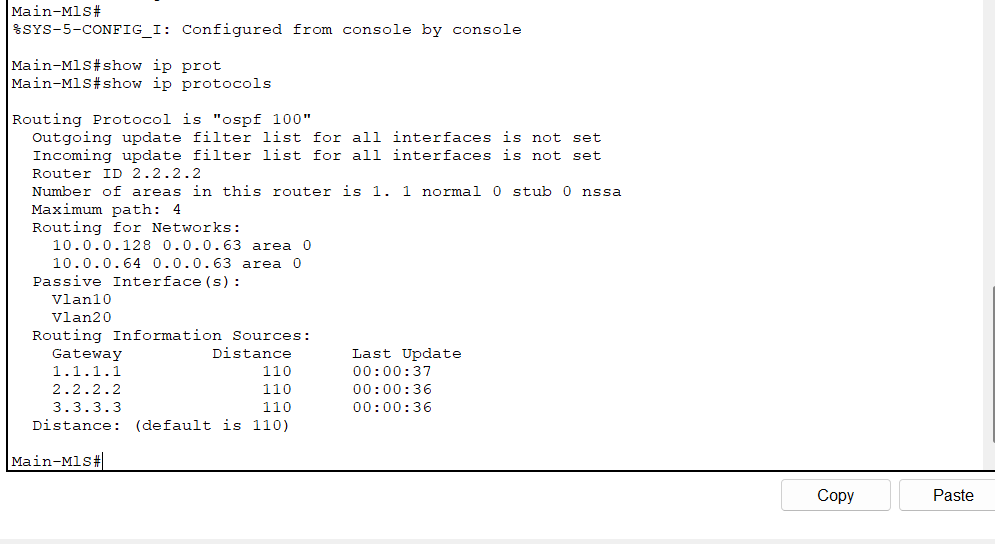
In order too configure the routers on OSPF routing an OSPF process ID has to be incorporated in our project process ID 100 used. Which was set up on the router by first entering global config mode and writing router ospf 100. Additionally, each router has to be assigned a unique router ID (which has its own table above) to uniquely identify a router in a routing domain using the router-id 1.1.1.1 (where 1.1.1.1 is an example).

When it comes to the interfaces for the router to be able to communicate with neighboring direct access/connected network by one of 3 methods. In Fact, the method we have used between the MLSs and the MIU-Gateway we have used to enter the interface between both and then writing ip ospf 100 area 0 (where the 100 is the process ID and 0 indicates area 0 as it’s a relatively small network ) after writing router ospf 100.On the contrary, the configuration of the MLS to OSPF was by using the network <network address> <wildcard mask> to configure vlan addresses and wildcard mask (where the wildcard mask is just the Inverse of the subnet mask)

The **default-information originate** router configuration command. This instructs R2 to be the source of the default route information and propagate the default static route in OSPF updates. Finally, the passive interface using the **passive interface** **<interface> (where <interface is the physical interface where sensitive info shouldn’t be sent).** was set to each MLS to prevent the sending of new updates regarding the OSPF to the layer 2 and switches in order to be immune from:

* Security issues by gaining sensitive information.
* Squandering network resources.

Kindly find below of OSPF routing verification:



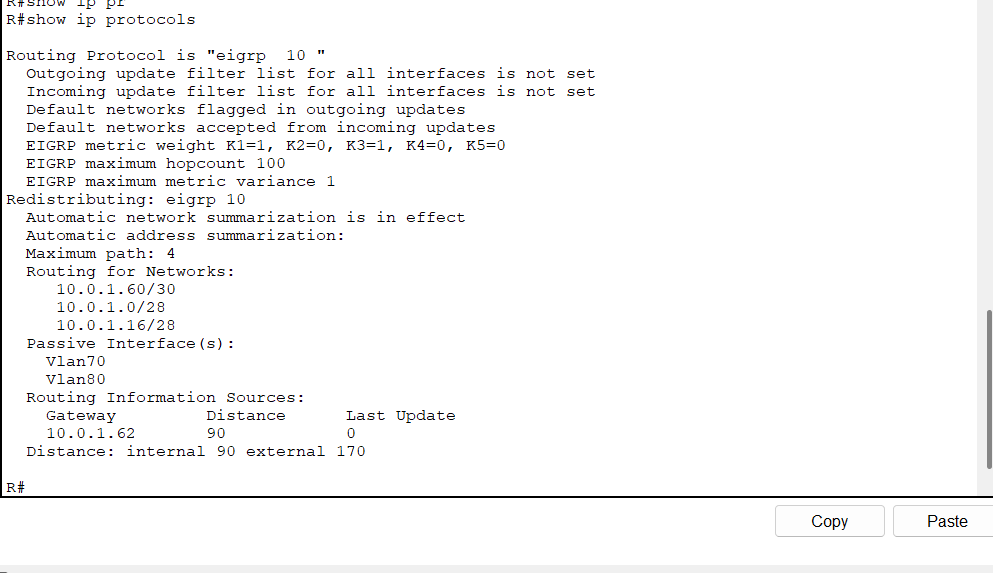
2-EIGRP Routing (For the n and R building):

EIGRP is a very similar routing protocol to OPSF when it comes to the configuration; however, unlike OSPF, EIGRP is a distance vector routing protocol not a link state routing protocol. Another difference is that EIGRP works with an AS(Autonomous System) rather than a process id (like in the OSPF).

First of all, the to configure or define the EIGRP we use the command **router eigrp <AS\_Number>** in the global privileged exec mode (where the AS\_Number is 10 in our case). The, we use the same **network <network\_address> [wildcard\_mask]** command

Where network address s the network address of the VLAN or neighboring routers and the wildcard mask is simply the inverse of the Subnet mask (Can be obtained by just subtracting the network address’s subnet mask from 255.255.255.255).

In order to verify the EIGRP connection we use the **show ip protocols** command in order to view and make sure it is correctly configured. Kindly find the EIGRP screenshot of verification below:



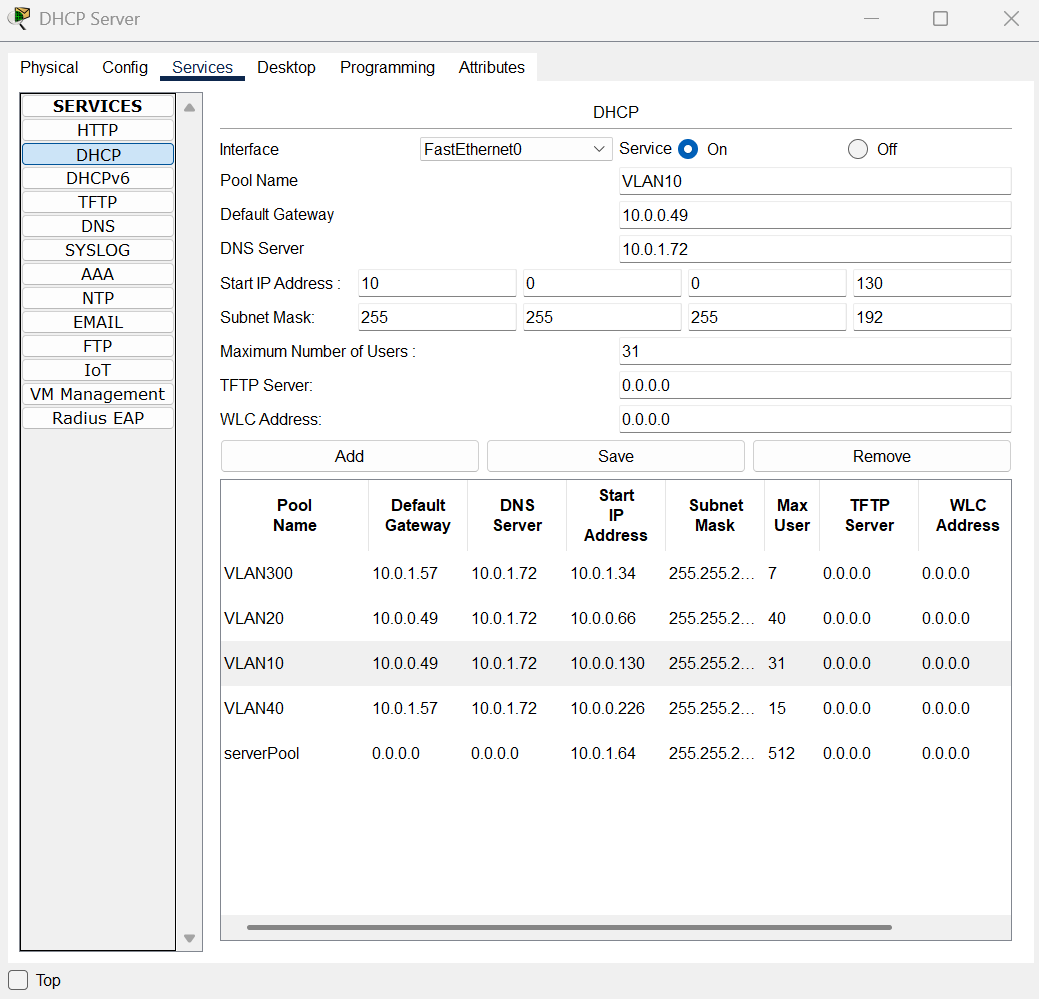
# Step 5 **(Configure DHCP Server):**

DHCP (Dynamic Host Configuration Protocol) is a network protocol that automatically assigns IP addresses and network configuration to devices (like PCs, phones, or servers) when they connect to a network.

1- ***Configure DHCP Server on Main Branch***

For the DHCP server to work we first have to set up different pools for each VLAN and set the assigned IP address range for said VLAN excluding the first 3 usable addresses from each of them.

We first start by turning on the service, then giving the pool its name according to its VLAN. After that we assign the default gateway according to the VLAN and the same DNS server for every pool. Then we could finally start giving each pool its start IP address and subnet mask for said VLAN, and last but not least give it the maximum amount of users on each pool.



After this step we need to set up the layer 3 switches for the main and S buildings (Main-MLS AND S-MLS) to act as relay agents to forward any DHCP requests from its PC’s straight to the DHCP server which has an IP of 10.0.1.67. To do this we need to use the helper address command on each VLAN interface for it to work

Main-MLS:

A number and numbers on a white background

AI-generated content may be incorrect.

S-MLS:

A white text with black numbers

AI-generated content may be incorrect.

A screenshot of a computer

AI-generated content may be incorrect.Now all that’s left to do is request an IP address for each PC in the Main and S buildings from the DHCP server.

A screenshot of a computer

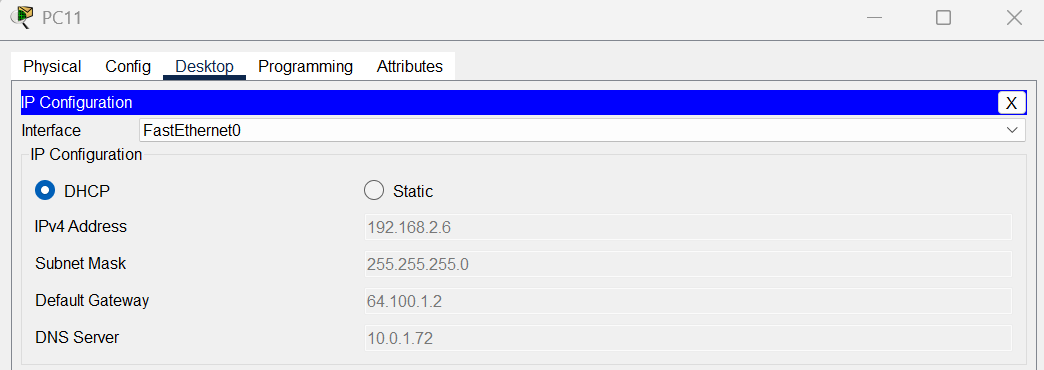
AI-generated content may be incorrect.

2- ***Configure a Branch\_GW Router as DHCP Server***

Now same goes for the Branch GW except this time instead of using a DHCP server we made the router act as one by making 2 DHCP pools for the VLAN’s and exclude the first 5 usable addresses.

A white background with numbers and letters

AI-generated content may be incorrect.

Now all we need to do is request an IP address for the PCs from the router (DHCP Server).

A screenshot of a computer

AI-generated content may be incorrect.

Part 6: **(Configure Dynamic NAT with PAT and Static NAT.)**

~ Here we started with configuring the NAT and created a NAT address pool and its named as MIU-NAT, and the IP’s we added are the starting and ending IP (same IP because 1 address)and its subnet mask:

MIU-GW(config)#ip nat pool MIU-NAT 209.165.200.224 209.165.200.224 netmask 255.255.255.240

~We are still configuring with the NAT, but here we are specifying NAT for traffic originated from the inside, also we are telling the router to use access-list 1 to identify which private IP’s should be translated, we also used the overload for the PAT method and to allow many private IP’s to use different port numbers:

MIU-GW(config)#ip nat inside source list 1 pool MIU-NAT overload

~Here we are making a static NAT rule for private IP’s (inside):

MIU-GW(config)# ip nat inside source static 10.0.1.70 209.165.200.224

~Now, we are creating a static route, we set it at default route, by sending all unknown traffic to the IP (209.165.200.224):

MIU-GW(config)#ip route 0.0.0.0 0.0.0.0 209.165.200.224

~These two bellow is to tell the router to forward traffic for the first two IP written in both lines to another router (64.100.1.2):

MIU-GW(config)#ip route 192.168.3.0 255.255.255.0 64.100.1.2

MIU-GW(config)#ip route 192.168.2.0 255.255.255.0 64.100.1.2

~Now here, we are informing which router is an inside and which is an outside for NAT:

MIU-GW(config)#interface g0/0/0

MIU-GW(config-if)#ip nat inside

MIU-GW(config-if)#interface g0/1/0

MIU-GW(config-if)#ip nat inside

MIU-GW(config-if)#interface g0/2/0

MIU-GW(config-if)#ip nat inside

MIU-GW(config-if)#interface g0/3/0

MIU-GW(config-if)#ip nat inside

MIU-GW(config-if)#interface g0/1

MIU-GW(config-if)#ip nat inside

MIU-GW(config-if)#interface g0/0

MIU-GW(config-if)#ip nat outside

Now why did we do all this?  
Because, We want to allow devices inside our private network, by accessing the internet or external networks, support multiple inside devices to use one public IP, allow specific device (10.0.1.70) to be reachable from outside, and to make sure the router knows where to send the packets.  
  
In simple words, we are enabling inside users to go out to the internet and possibly letting outside users reach a server inside, while making sure our router knows how to forward traffic correctly.

Part 7: Configure Network Management Features.

Step 1: NTP  
We start with editing the calendar in the NTP – Syslog Server  
Path: Services>NTP

A screenshot of a computer

AI-generated content may be incorrect.Along way the IP configuion  
A screenshot of a computer

AI-generated content may be incorrect.

Now we try and configure all routers to use ntp servers as the following:  
~ We also verify how it works using show ntp association & show clock also do the exact same for each and every router (main-mls, s-mls, n-mls, r-mls, etc.

A screenshot of a computer

AI-generated content may be incorrect.

Step 2: Syslog

Activate the syslog:

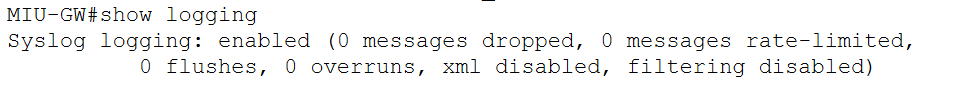
A screenshot of a computer

AI-generated content may be incorrect.

Routers configure:

A close up of a number

AI-generated content may be incorrect.

Testing:  


Keep repeating with all routers…  
  
Step 3: Web Server:

We click on (edit) in the index.html so we can edit the web page that appears in the PC’S:  
A screenshot of a computer

AI-generated content may be incorrect.

Then we write the command in index.html:  
A screenshot of a web page

AI-generated content may be incorrect.  
We imported “miu\_logo.png” for the image in the http page:

A screenshot of a computer

AI-generated content may be incorrect.  
  
We turn on the DNS service on, and add the domain name “miu.edu.eg” and IP address of the web server “10.0.1.70”:

A screenshot of a computer

AI-generated content may be incorrect.

Testing:  
A screenshot of a computer

AI-generated content may be incorrect.  
  
  
Step 4: Email server:  
We go to email server and go to Services>Email, turn on SMTP and POP3 Services, also set the domain name to “miu.edu.eg”,

adding 12 users for each PC and all with the same password “123”:  
A screenshot of a computer

AI-generated content may be incorrect.

Testing:   
~ Sender

A screenshot of a computer

AI-generated content may be incorrect.

~Receiver  
A screenshot of a computer

AI-generated content may be incorrect.

Step 5: DNS server:

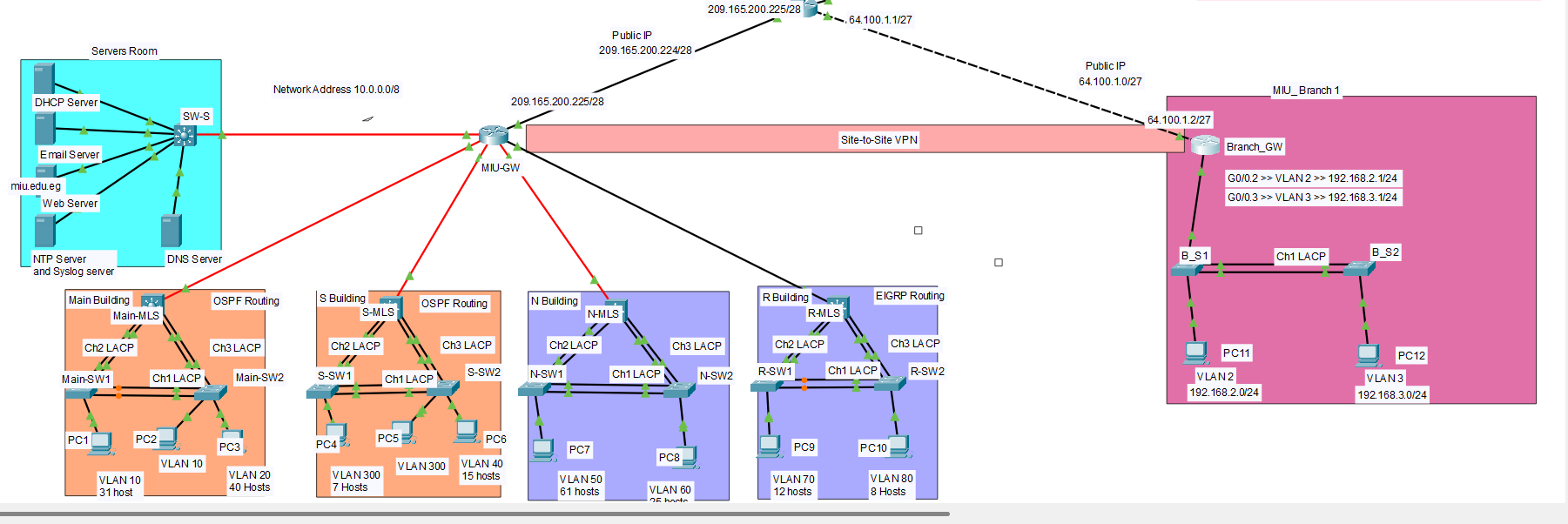
We go to DNS server and go to Services>DNS, turn on DNS Services and add the domain of the web server:  
A screenshot of a computer

AI-generated content may be incorrect.

# Step 8 **(Configure and Verify a Site-to-Site IPsec VPN):**

Site-to-Site VPN (Virtual Private Network) is a secure method to connect geographically separated networks over an untrusted network like the Internet. It allows the **Main Campus** and the **Branch network** to securely exchange data through a **tunnel** that encrypts traffic between them.

This implementation ensures that internal devices from both networks can communicate **securely**, without exposing data to the public internet.



(Refers to the attached image showing the Main Campus with IP: 209.165.200.225 and Branch with IP: 64.100.1.1, both connected via a public network)

**Step 1: Define IKE Phase 1 Policy (ISAKMP)**

This step defines how the two routers will securely negotiate the VPN tunnel parameters.

In global config mode:

**crypto isakmp policy 10**

**encr aes**

**hash sha**

**authentication pre-share**

**group 2**

**lifetime 86400**

| **Feature** | **Description** |
| --- | --- |
| Encryption (AES) | AES encryption for security |
| Hash (SHA) | SHA hash for data integrity |
| Authentication (Pre-share) | Uses a shared key |
| Group (DH Group 2) | DH group for key exchange |
| Lifetime (86400 seconds) | Validity of the session key (24 hours) |

**Step 2: Define the Pre-Shared Key**

**crypto isakmp key VPN123 address 64.100.1.1**

**crypto isakmp key VPN123 address 209.165.200.225**

**Step 3: Define IPsec Phase 2 Policy (Transform Set)**

This specifies how traffic will be encrypted after the tunnel is established.

crypto ipsec transform-set VPN-SET esp-aes esp-sha-hma

**Step 4: Define Interesting Traffic (Access List)**

**This access list tells the router which traffic should be protected by the VPN tunnel.**

**access-list 110 permit ip 10.0.0.0 0.255.255.255 192.168.2.0 0.0.0.255**

**access-list 110 permit ip 10.0.0.0 0.255.255.255 192.168.3.0 0.0.0.255**

**access-list 110 permit ip 192.168.2.0 0.0.0.255 10.0.0.0 0.255.255.255**

**access-list 110 permit ip 192.168.3.0 0.0.0.255 10.0.0.0 0.255.255.255**

**where 10.0.0.0 is the address of THE miu lan network and 192.168.2.0 AND 192.168.3.0 are the addresses of VLANS in the MIU branch to access the VPN.**

**Step 5: Configure Crypto Map and Bind to Interface**

**A crypto map links all the VPN components together and is applied to the outgoing interface**

**crypto map VPN-MAP 10 ipsec-isakmp**

**set peer 64.100.1.1**

**set transform-set VPN-SET**

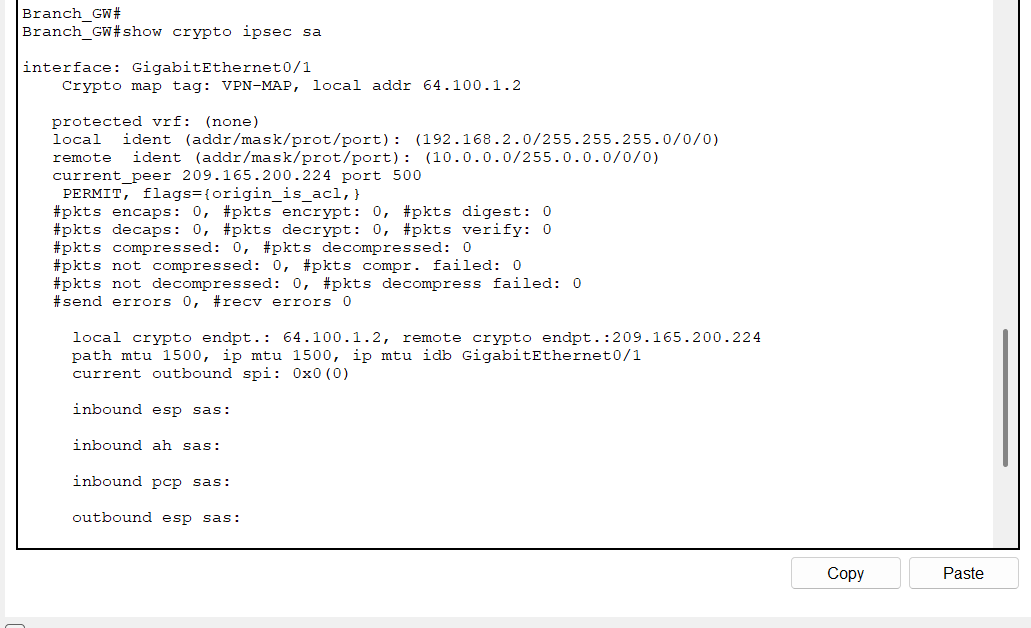
**match address 110**

**exit**

**interface GigabitEthernet0/0**

**crypto map VPN-MAP**

Finally, we use **show crypto isakmp sa** to show the vpn configuration as seen below



**Part 9 Wireless Home Network**

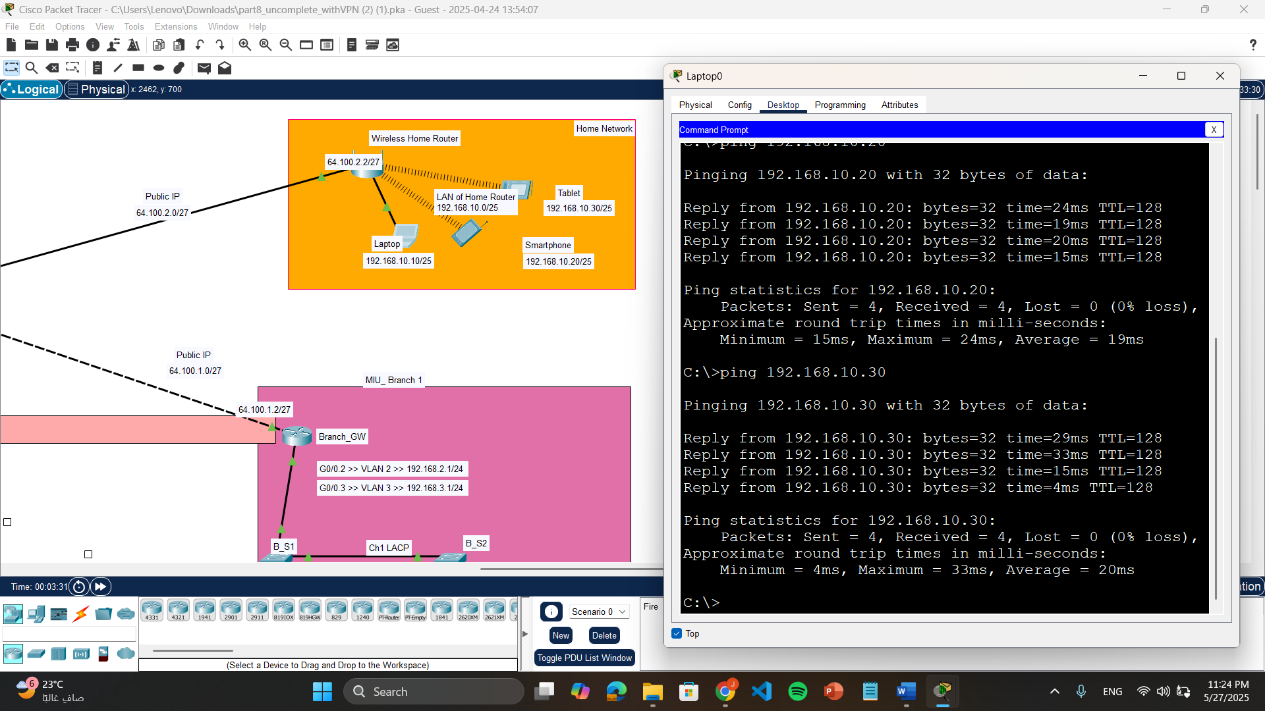
1. **Went on wireless home router’s GUI wireless section in order to change the ssid**

**2- Went onto wireless security to choose 2.4ghz changed to WPA2-PSK and added the passphrase**

**3- Configured the ip address to match the lan wireless home router one (192.168.10.1 not .0 because .0 is a network address)**

**4- Went on smartphone and tablet configured the ip addresses also changed to wpa2-psk and added the passphrases and finally I pinged the three devices together (phone to tablet and vice versa, phone to router, and tablet to router)**

**5- Connected a cable to the router from the laptop in order to be able to assign the laptop its ip address and also be able to ping the phone, tablet and router from the laptop itself and vice versa**

**A screenshot of a computer

AI-generated content may be incorrect.**

**A screenshot of a computer

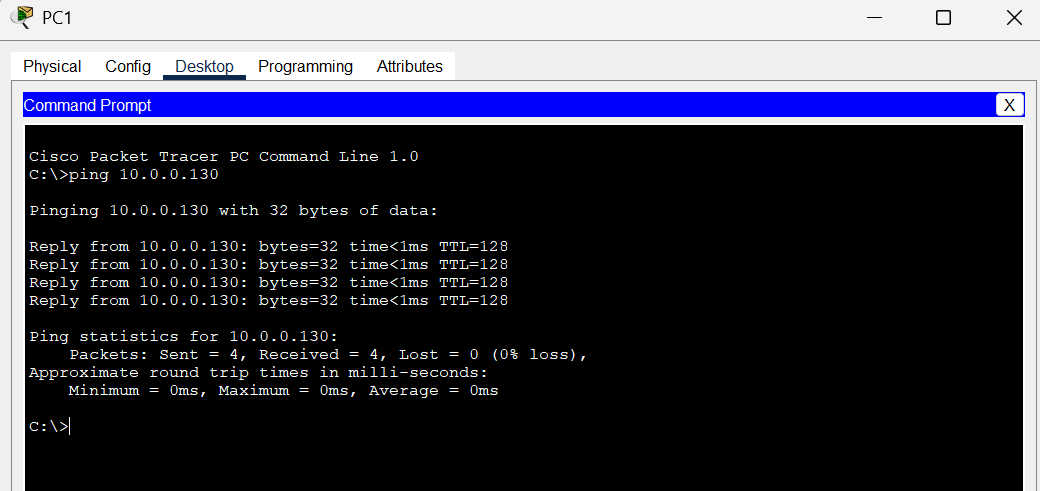
AI-generated content may be incorrect.A screenshot of a computer

AI-generated content may be incorrect.**

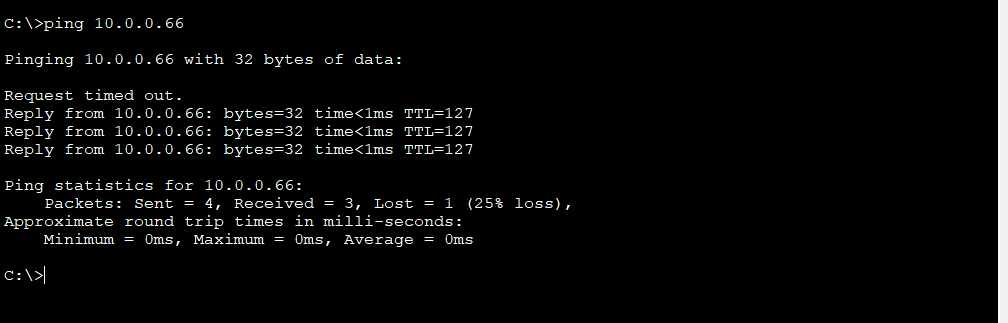
**Pinging Screenshots**

Same Buildings

1-Main Building:

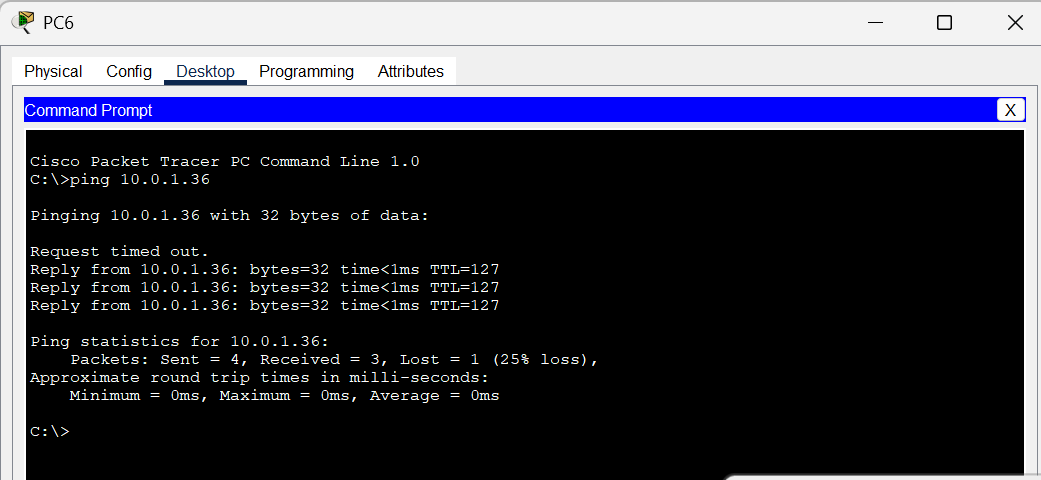


Pinging from PC1 to PC2 (Same VLAN)

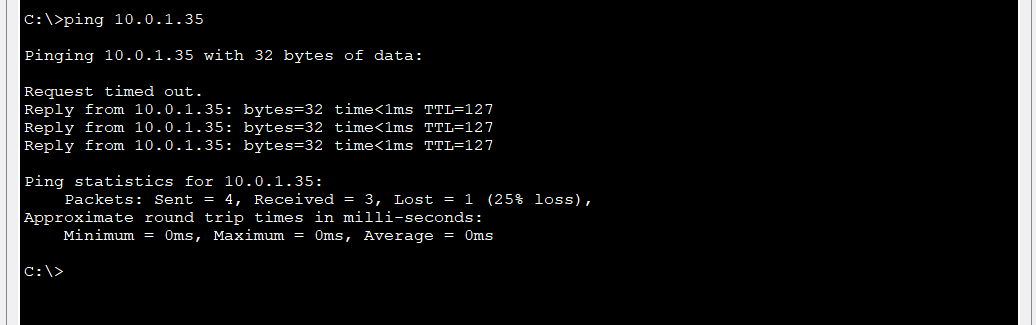


Pinging from PC1 to PC3 (Different VLANS)

2-S Building:

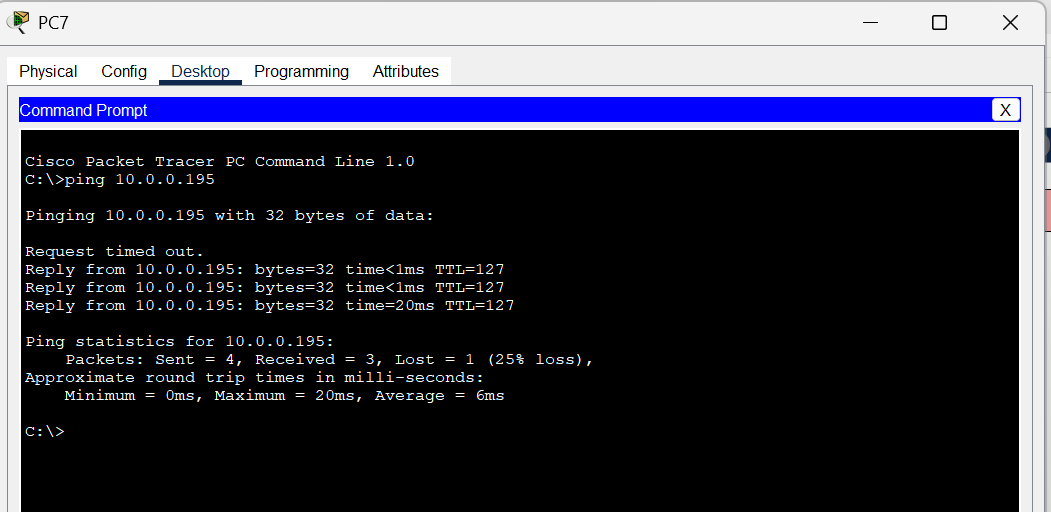
****

Pinging from PC6 to PC4 (Different VLANS)



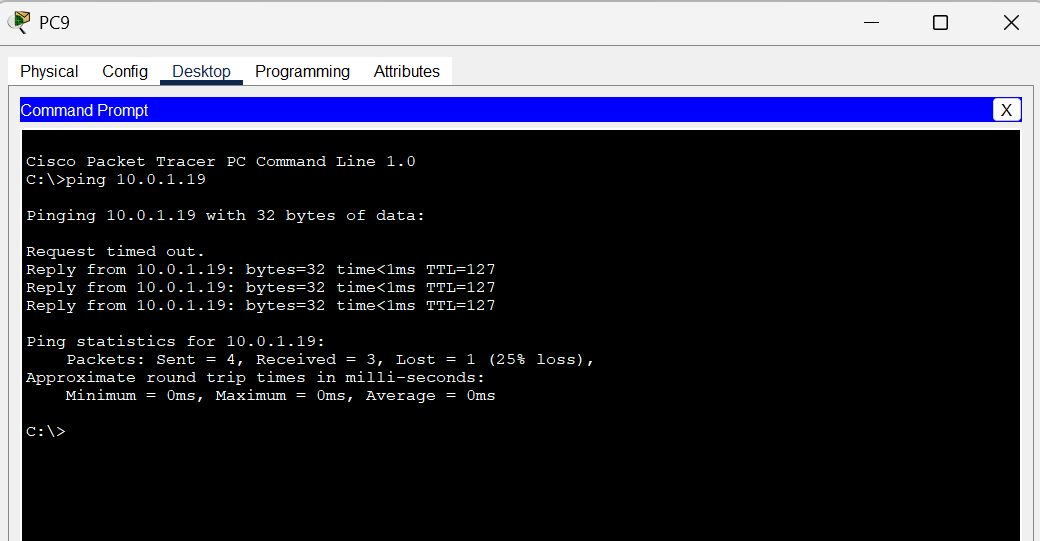
Pinging from PC6 to PC5 (Same VLAN)

3-N Building:



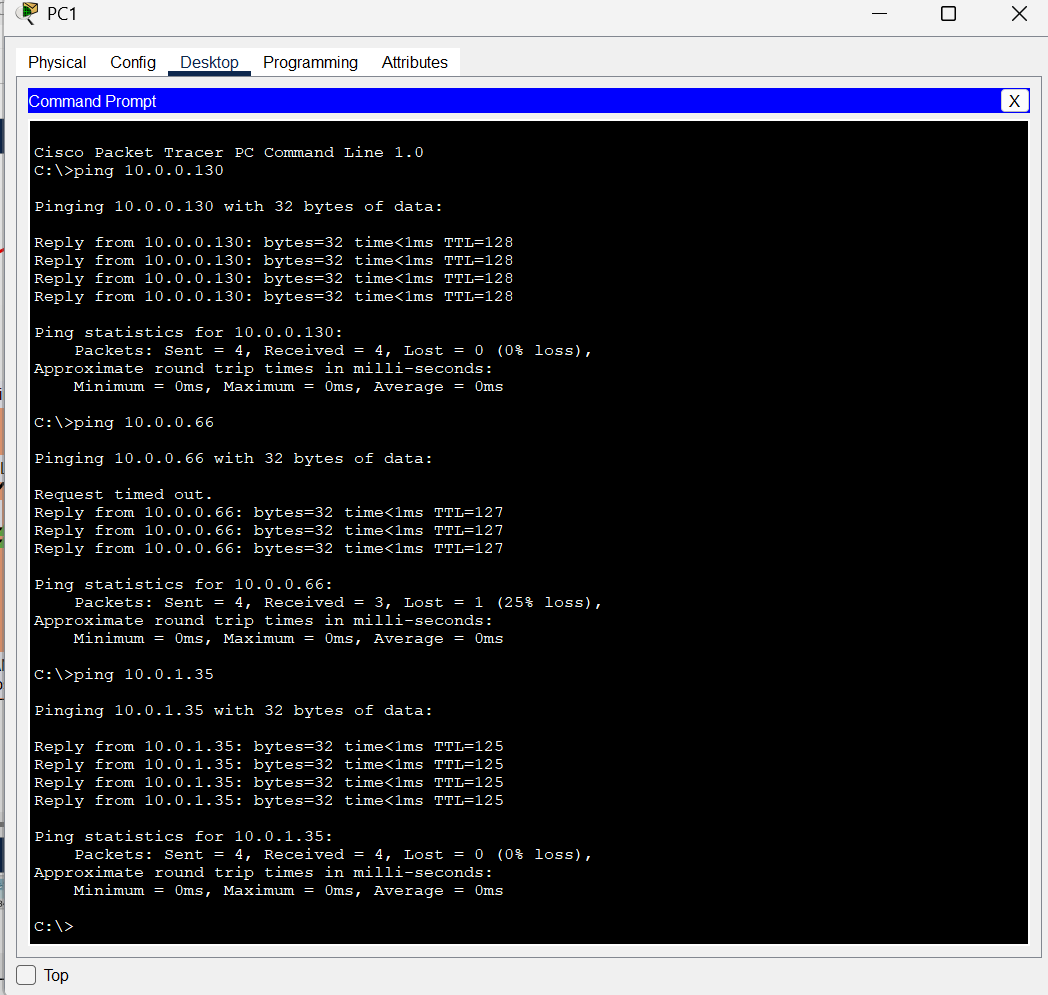
Pinging from PC7 to PC8 (Different VLANS)

4-R Building:

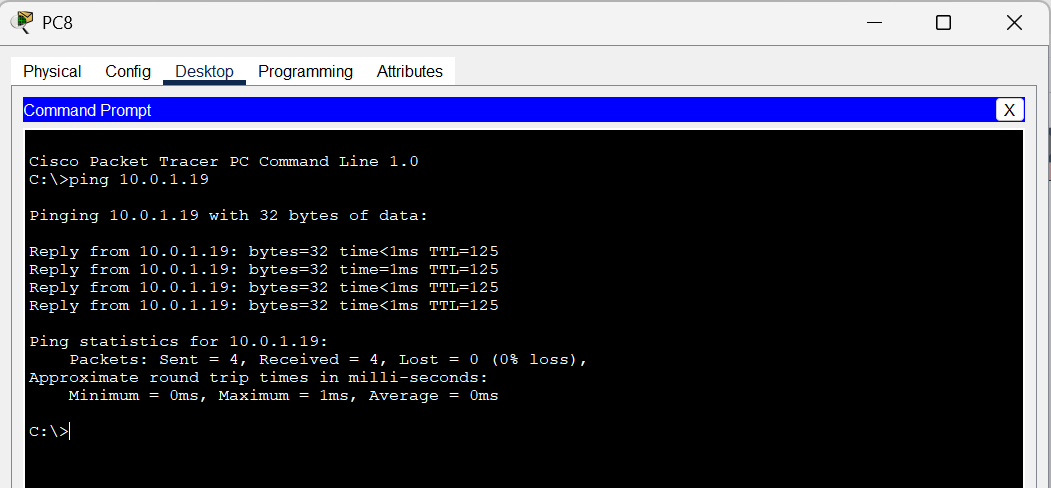


Pinging from PC9 to PC10 (Different VLANS)

Different Buildings Pinging

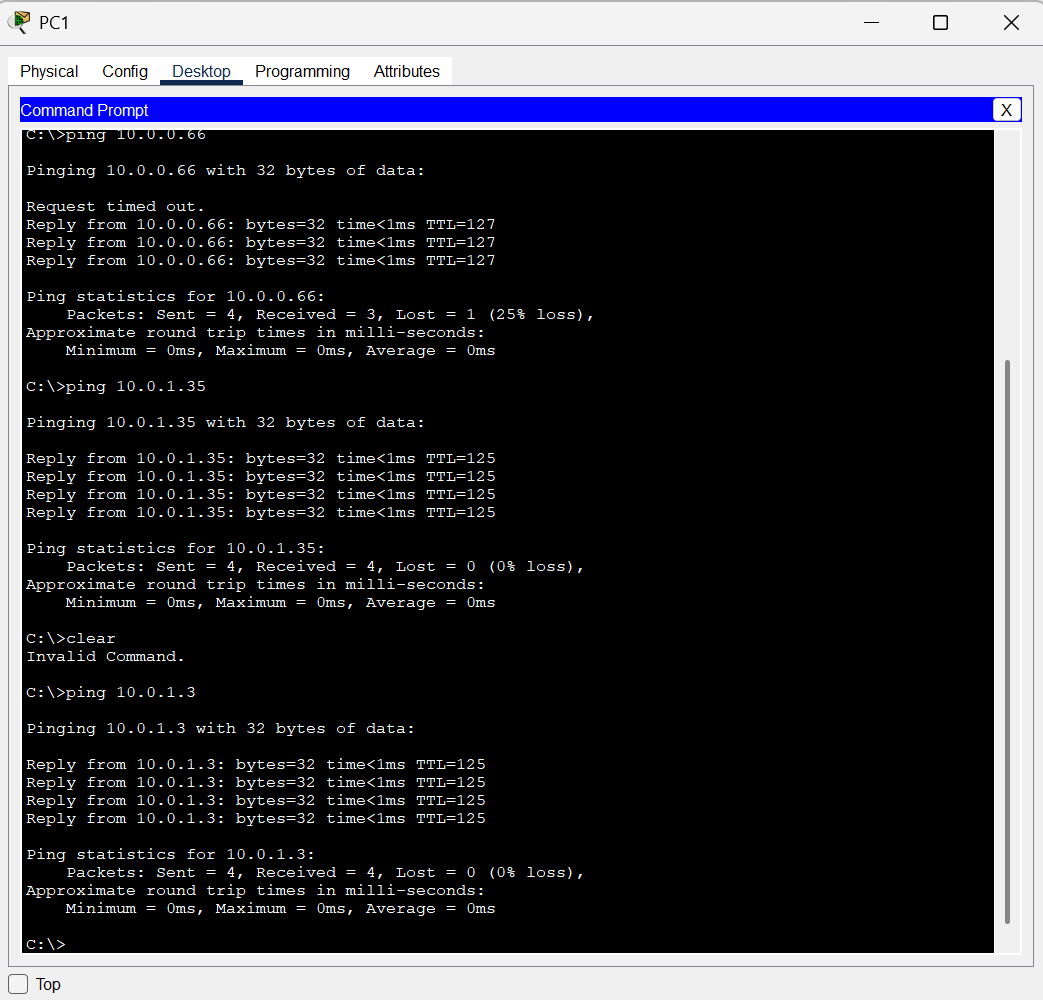


Pinging from PC1 (main building) to the PC5 in S building

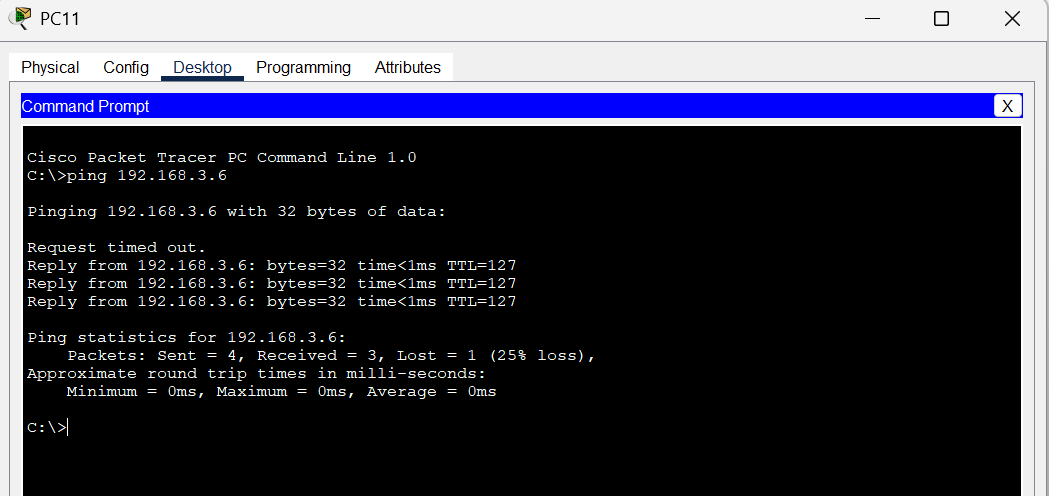


Pinging the PC10

(to R building) from PC8 (from N building)



Pinging from PC1(in the main building) and the PC 9 in the R building



Pinging PC12 from PC11 in MIU Branch