Faculty of Engineering and Technology
Electrical and Computer Engineering Department

Computer Network

ENCS3320

Project 2 Report

Prepared by:

Tala Abahra 1201002

Maha Mali 1200746

Section: 1

Instructor: Dr. Abdalkarim Awad

Date: 14/2/2022

Abstract:

The goal of this project is to learn about and understand the principles of networking by

implementing a simple network with many routers, switches, PCs, and tunnels using the

Cisco packet tracer. And to capture the data (packet) transmission using different

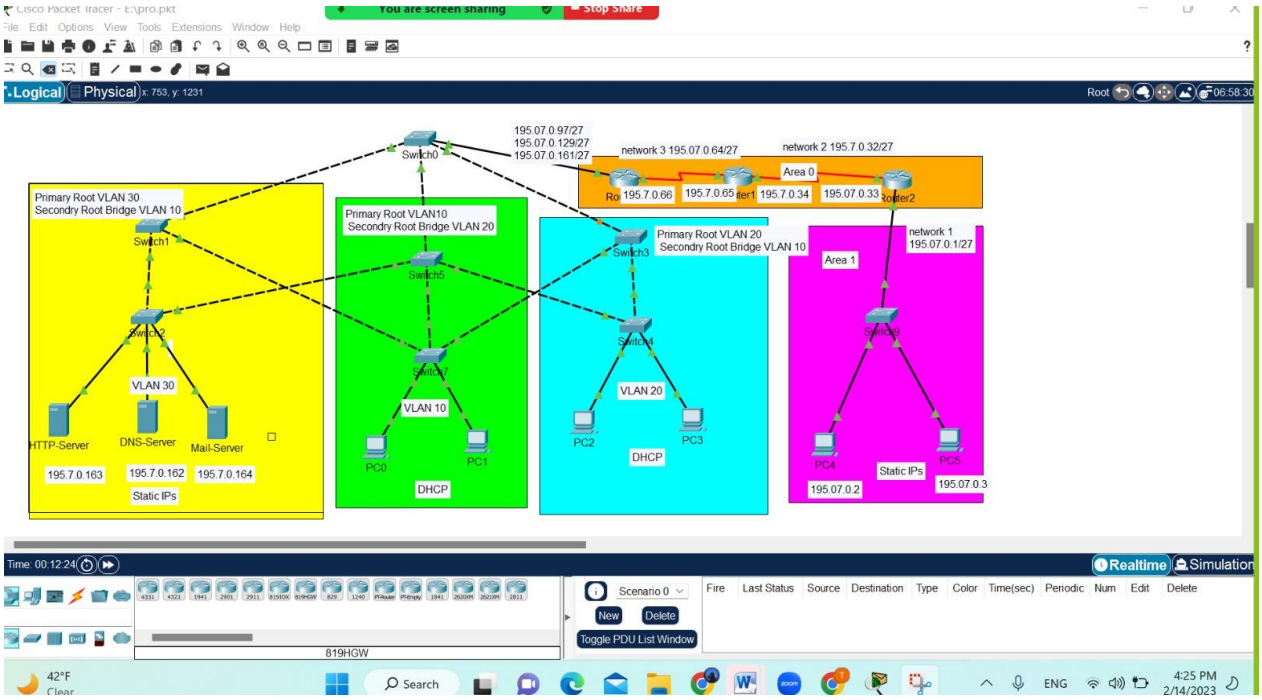
protocols as DHCP, ICMP and TCP.

Contents

Part 0: IP Assignment and Subnetting

IP assignment involves assigning unique IP addresses to devices on a network to enable communication. Subnetting involves dividing a larger network into smaller subnetworks, each with its own range of IP addresses. This can improve network performance and security by limiting the scope of broadcasts and controlling traffic flow. Both IP assignment and subnetting are important concepts in network design and management.

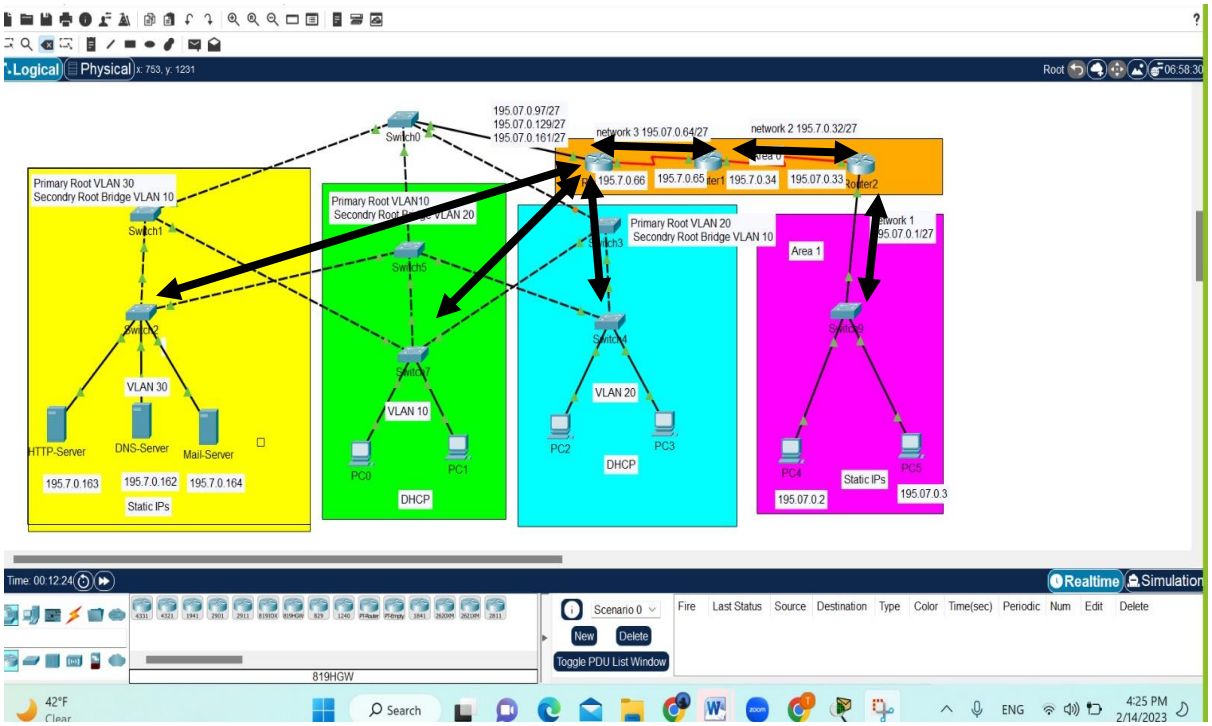
First, we assigned IP addresses to all PCs, Routers interfaces, and server according to student id (1200746), then the IP address will be 195.07.0.0/24.As shown in figure



2-Part 1: Building the Topology

2.1 Build the topology using packet tracer .

In this part, we have implemented a simple network that has 6 subnetworks as shown in figure and a tunnel, also we connected all the devices as what is required and given, by using the Cisco packet tracer version 8.2. The figure show building the topology.

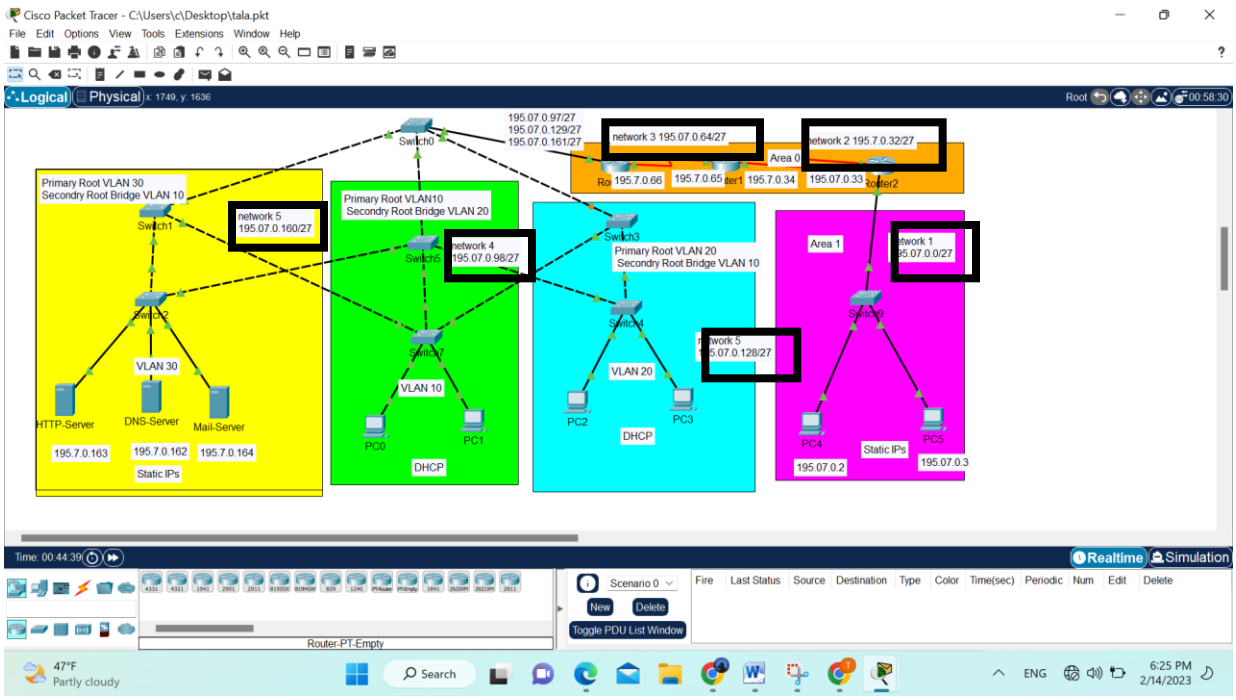


To divide the network 195.07.0.0/24 into 6 subnets, you can use the following steps:

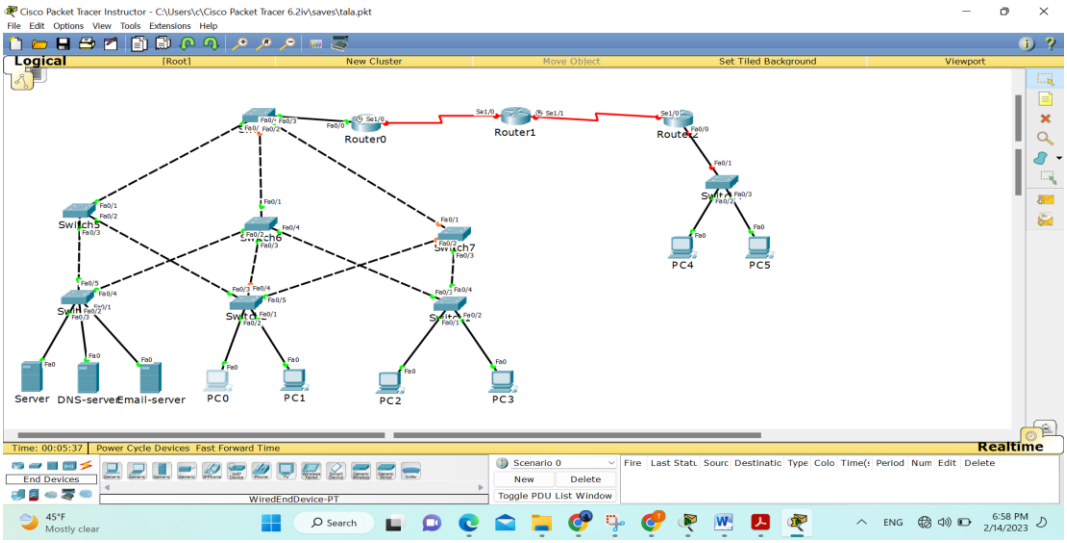
1. Determine the number of bits required to represent 6 subnets. In binary, 6 is represented as 00000110. Since 6 requires 3 bits to represent, you will need to borrow 3 bits from the host portion of the IP address.
2. Subtract the number of borrowed bits (3) from the total number of bits in the network address (24) to determine the new subnet mask. The new subnet mask will be 27 bits, which is represented as 255.255.255.224.
3. Determine the new subnet ranges by incrementing the third octet of the IP address by 32 for each subnet. The new subnet ranges will be:

- 195.07.0.0/27
- 195.07.0.32/27
- 195.07.0.64/27
- 195.07.0.96/27
- 195.07.0.128/27
- 195.07.0.160/27

Note that each subnet has a range of 32 IP addresses, with the first address reserved for the network address and the last address reserved for the broadcast address. The remaining 30 addresses can be used for assigning to devices on each subnet.



2.2Configure the interfaces of the three routers

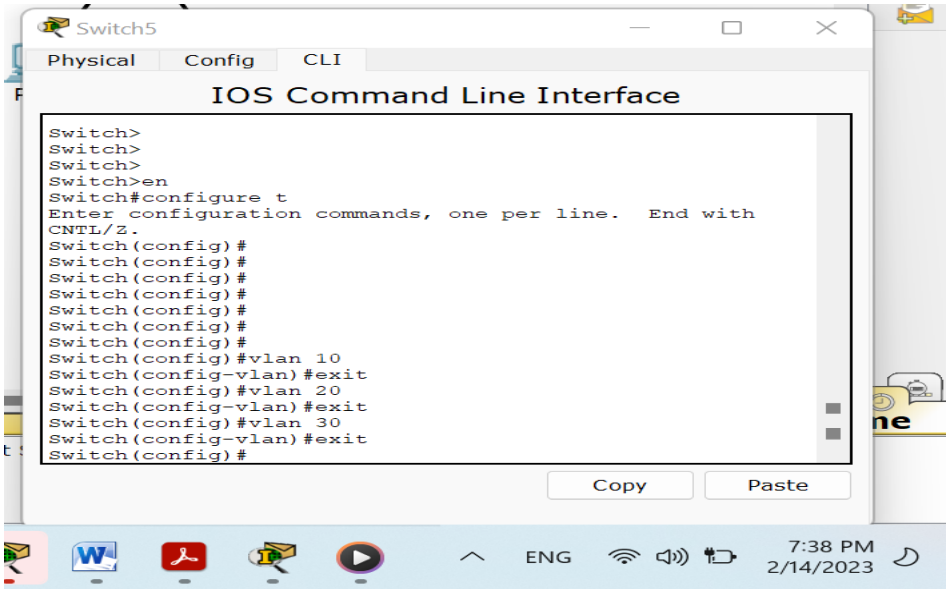


It's generally best practice to define your VLANs first, then assign those VLANs to the appropriate switch interfaces, and finally configure access or trunk ports as needed. After configuring your ports, you can then assign IP addresses to the relevant interfaces if necessary.

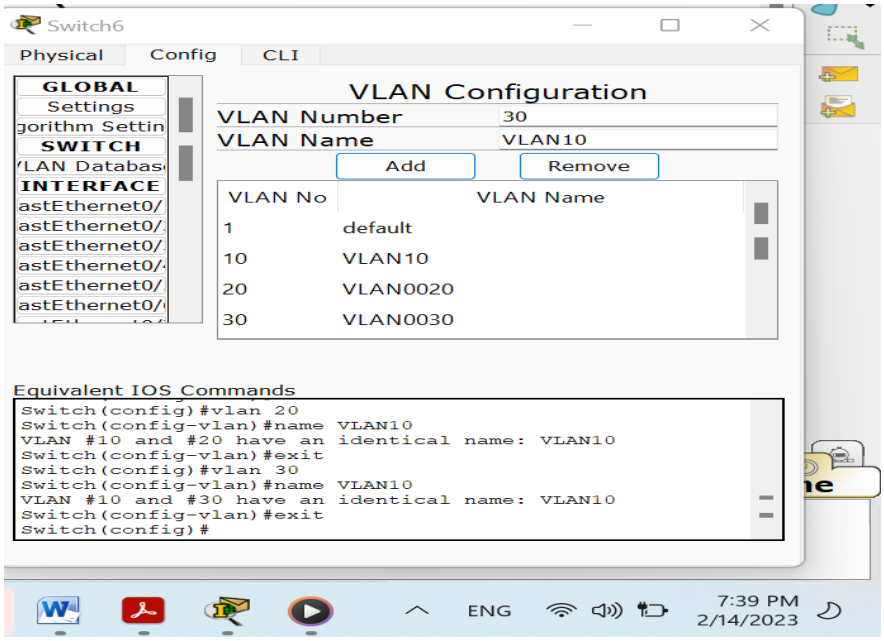
- **Step 1:** By first defining your VLANs, you can ensure that your network is properly segmented into logical groups, and you can assign appropriate access or trunk ports to each VLAN. Once your VLANs are properly configured and assigned to interfaces, you can then configure your access or trunk ports to allow the appropriate VLAN traffic to pass through.

  So with each switch will define 3 VLAN.

  We can define a vlan using CLI , like next:



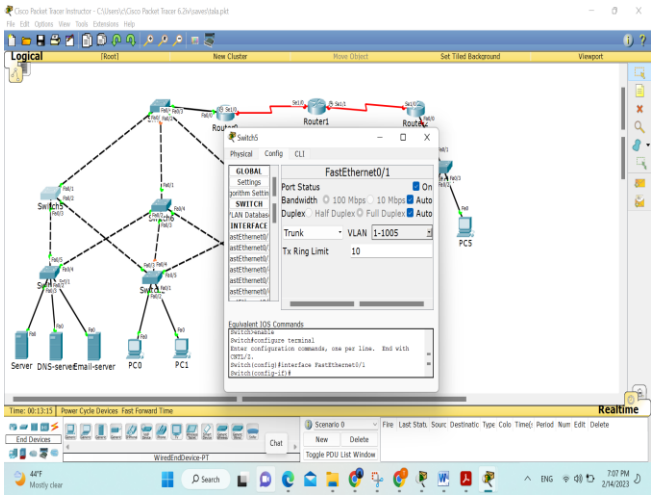
  Or using Config :

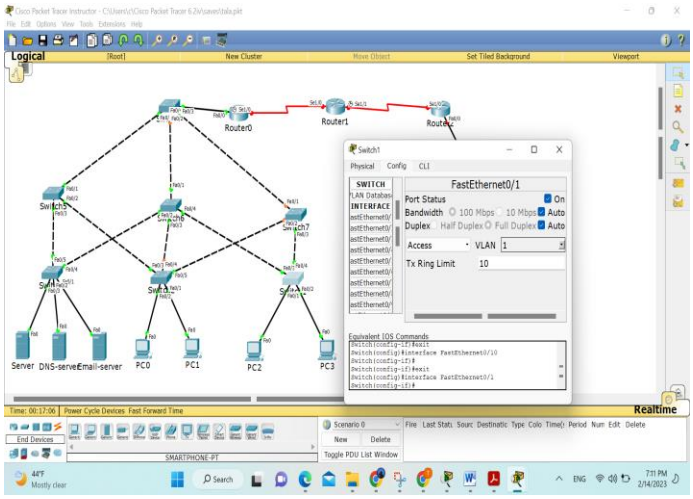


- **Step 2:** In networking, a "trunk" is a type of link that carries multiple VLANs between switches or between a switch and a router. Trunks allow a single link to carry traffic for multiple VLANs, which is useful for network segmentation and traffic management.

  On the other hand, "access" refers to a type of port on a switch that is assigned to a specific VLAN. Access ports are used to connect end devices, such as computers, printers, or IP phones, to a switch. Traffic from an access port is untagged, meaning that it does not include information about VLAN membership.

  In summary, a trunk is used to carry traffic for multiple VLANs between switches, while an access port is used to connect end devices to a specific VLAN on a switch.

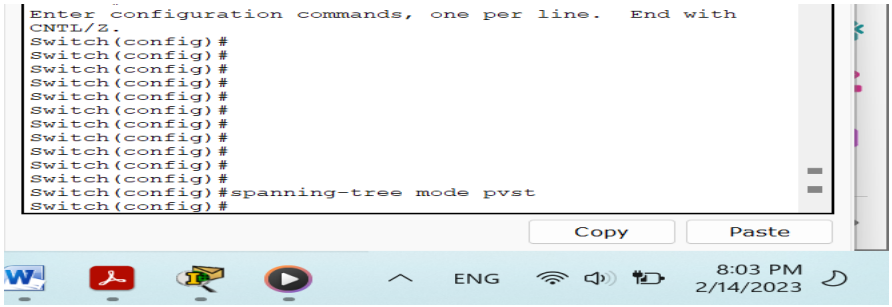




- **Step 3**: root bridge priority

  We set the root bridge priority for a VLAN in Spanning Tree Protocol (STP) to determine the root bridge for that VLAN. The root bridge is responsible for forwarding traffic in the network and preventing loops, and it's an important concept in STP. When multiple switches are connected in a network, STP ensures that only one switch becomes the root bridge for each VLAN, which helps to prevent loops and ensure that network traffic is forwarded efficiently and reliably.

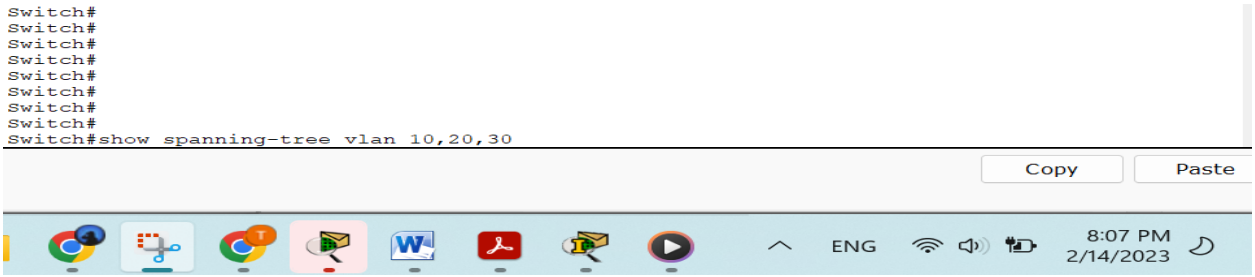
This in part3 6) Primary and secondary root bridge VLANs are used as illustrated in the figure.

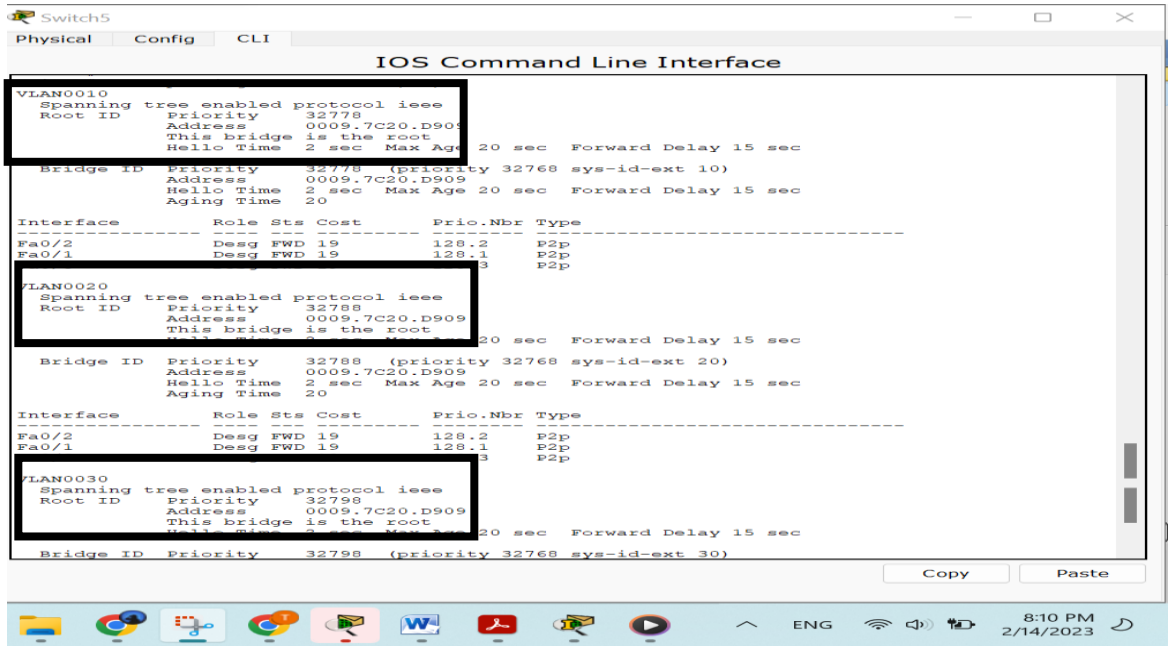


We use Spanning Tree Protocol (STP) mode PVST when we have multiple VLANs to prevent loops and ensure efficient network traffic forwarding. Each VLAN has its own root bridge, allowing us to optimize the network

topology for each VLAN and configure different STP parameters. PVST also supports Rapid Spanning Tree Protocol (RSTP), which provides faster convergence times and reduces network downtime.

How we get the priority for vlan:

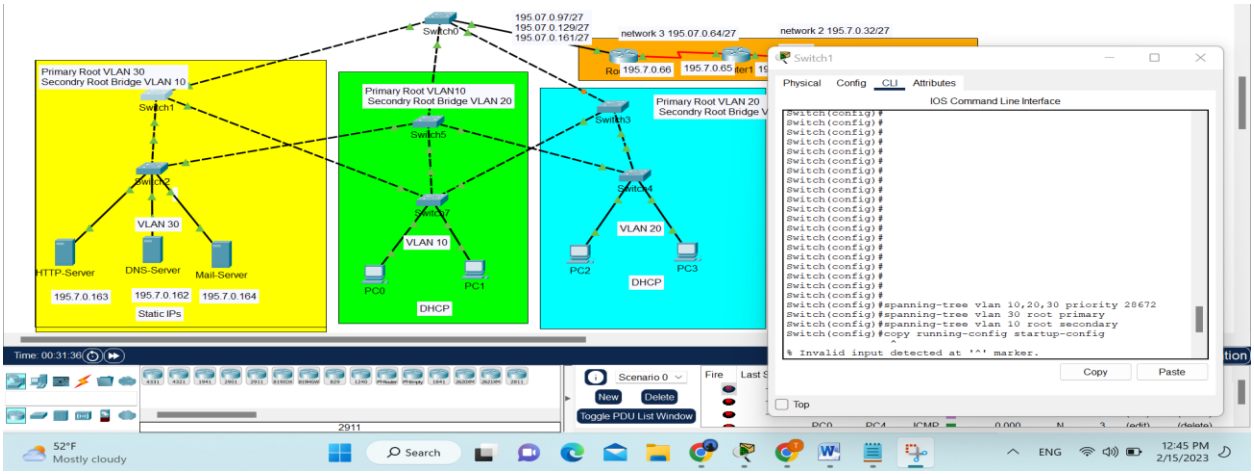




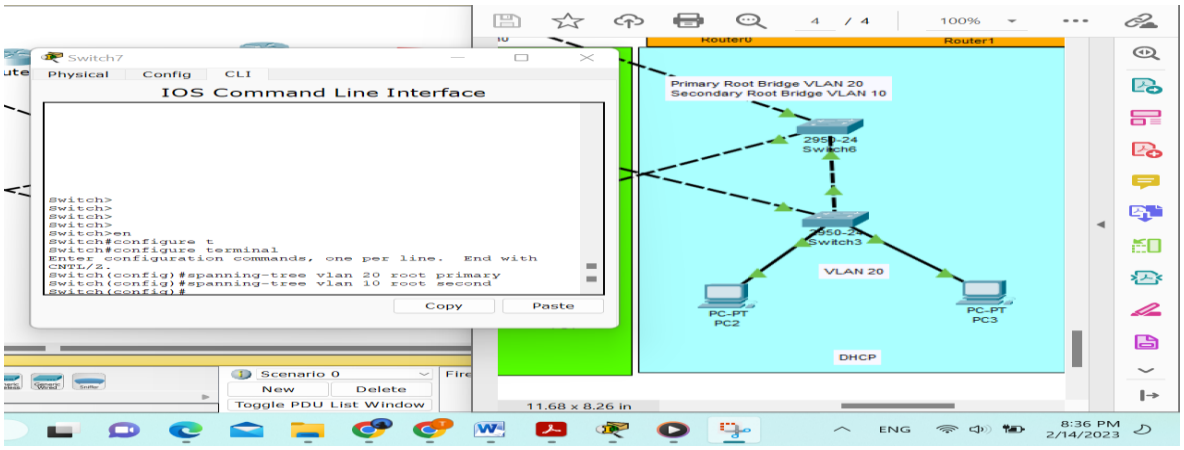
Now we will set the primary and secondary for each area :

```
switch(config)#vlan <num>
switch(config)#spanning-tree mode pvst
switch(config)#spanning-tree vlan <#> priority <#>
switch(config)#spanning-tree vlan <#> root primary
switch(config)#spanning-tree vlan <#> root second
switch(config)#no spanning-tree vlan 1
switch#show spanning-tree
```

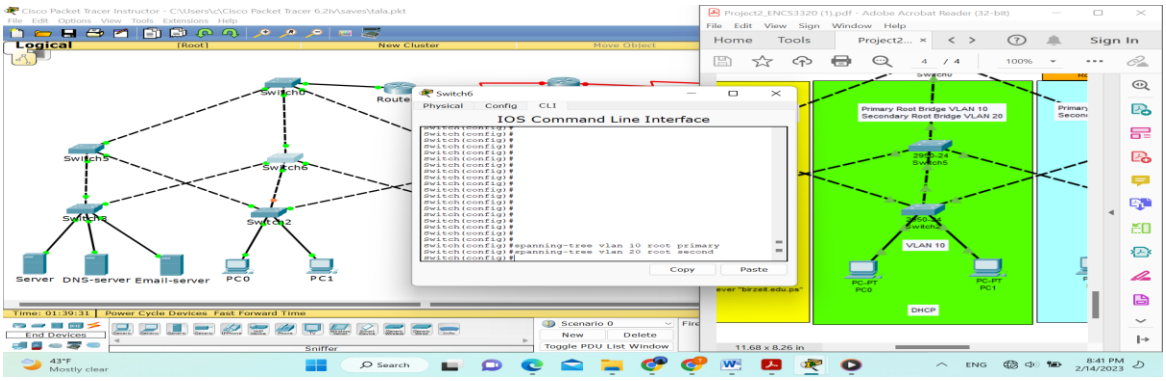
Vlan 20



Vlan =10



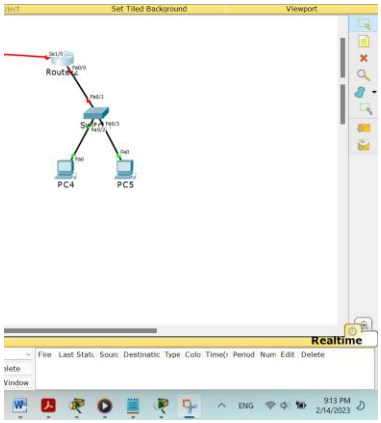
Valn =30 in switch number 1:

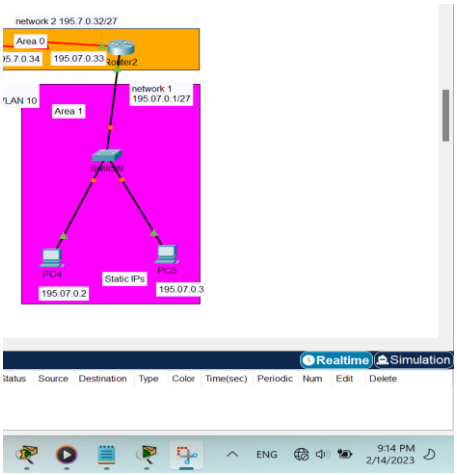


Step 4: Finally, after configuring your access or trunk ports, you can assign IP addresses to the relevant interfaces. This step is necessary if you want to enable devices on the VLAN to communicate with each other and with devices on other networks.

This in part3. 6) Configure the mode (access/trunk) of the switches links based on the connected devices.

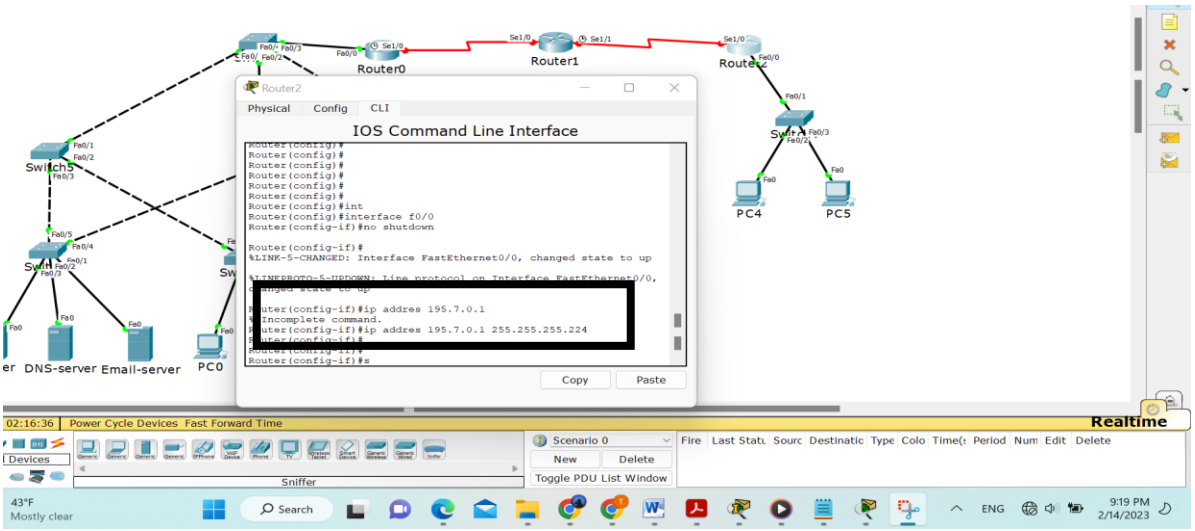
Lets start from the right :





Implemetation the Interface in Router2 :

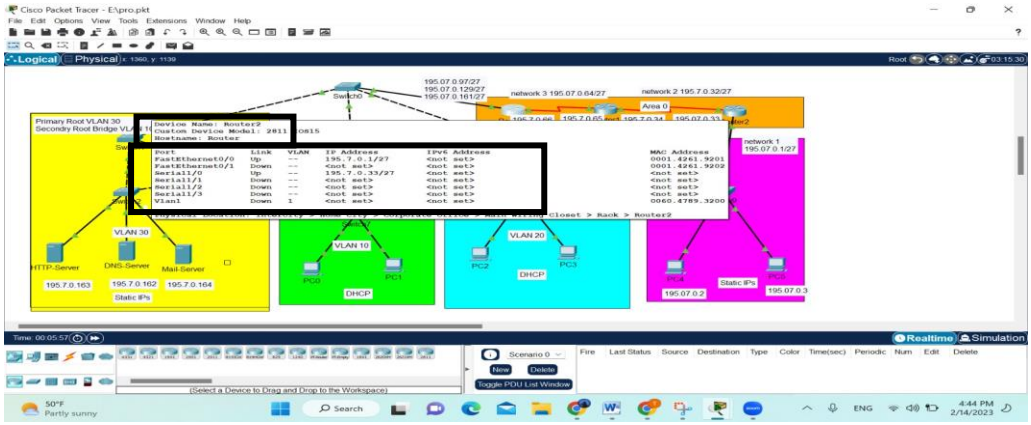
We have two inter face one with network 195.7.0.0 and another with network 195.7.0.32



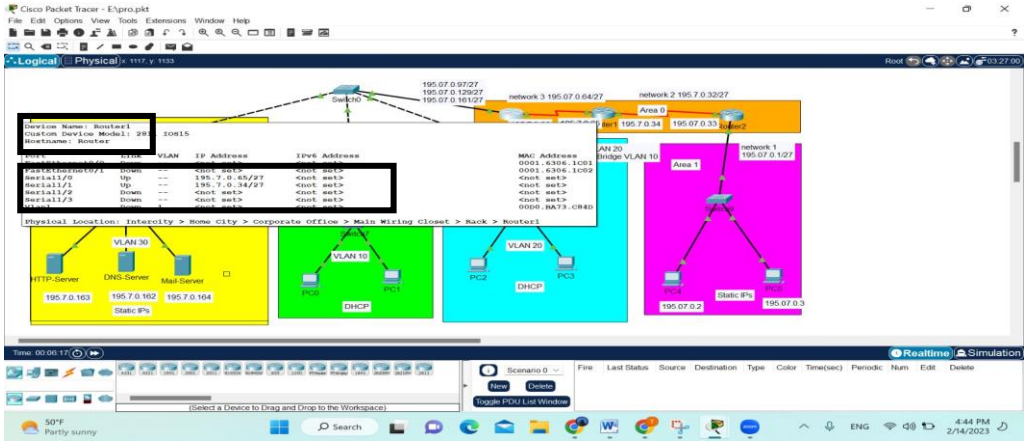

```
R1(config)#interface f0/0
R1(config-if)#no shut
R1(config-if)#ip address subnet
```

OUTPUT :

Router2



Router1:



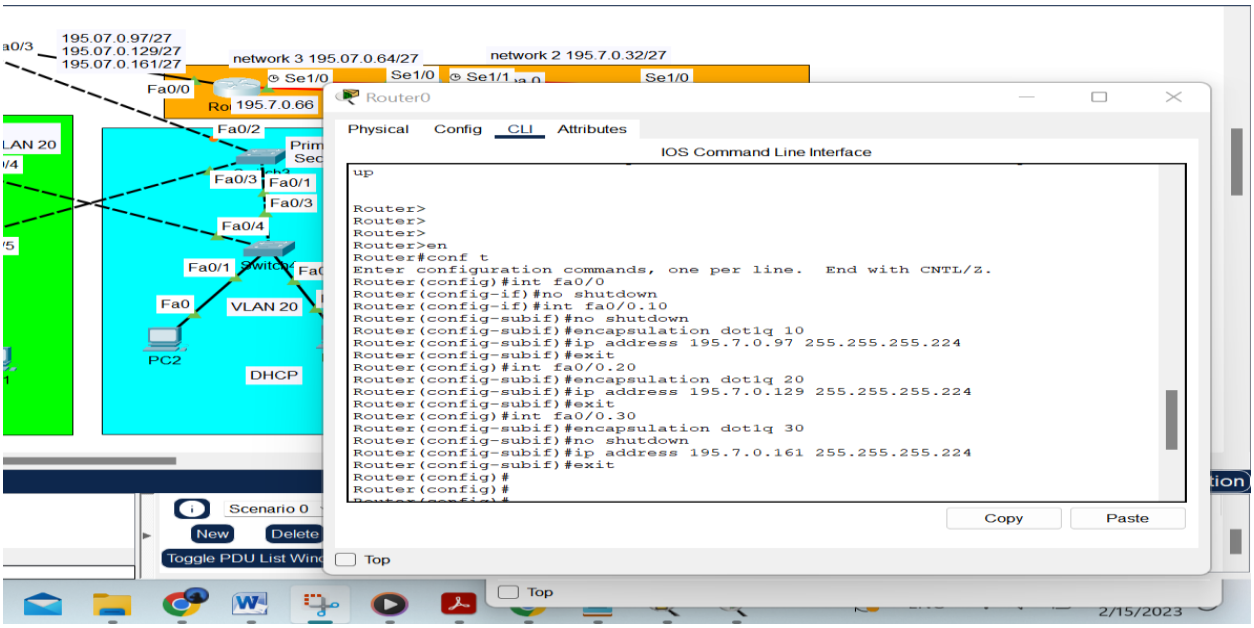
Router0:

Since in this we have 3 vlan to implemant will use : Router on a Stick

We use the "Router on a Stick" configuration when we have a network with multiple VLANs that need to communicate with each other, and there is no Layer 3 switch available to perform inter-VLAN routing.

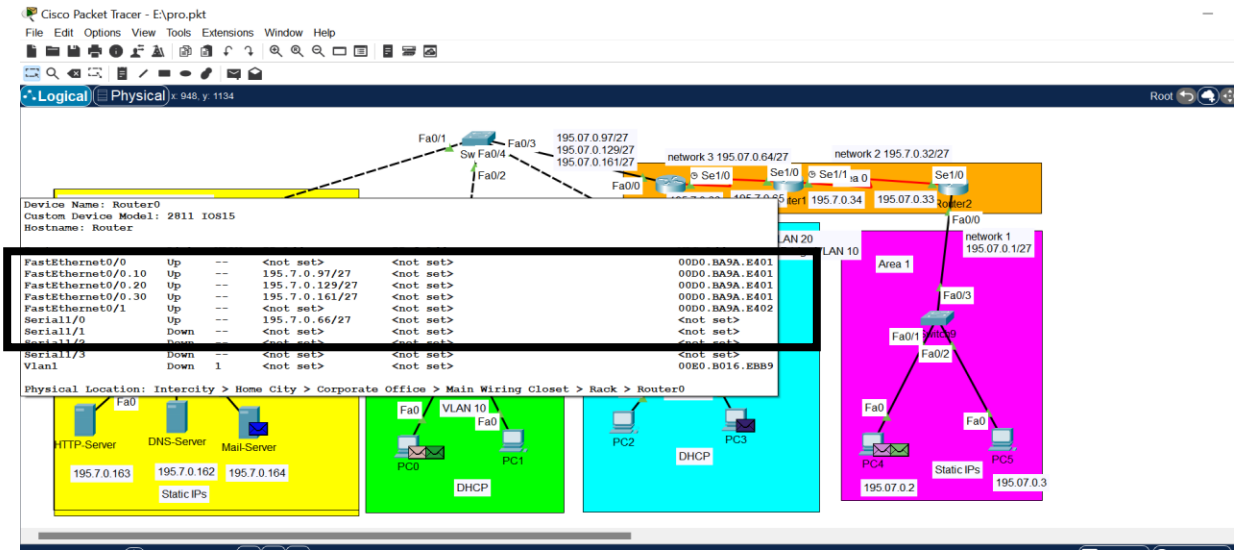
In this scenario, a single physical interface on the router is used to route traffic for multiple VLANs. The physical interface is configured as a trunk port, which carries traffic for all VLANs over a single link, and each VLAN is associated with a subinterface that is configured with an IP address for the VLAN.

The reason we use "Router on a Stick" with three VLANs, or any number of VLANs, is to enable communication between devices on different VLANs. Without this configuration, devices on different VLANs would not be able to communicate directly with each other. By routing traffic



between VLANs through the router, we can enable communication between devices on different VLANs.

Output:

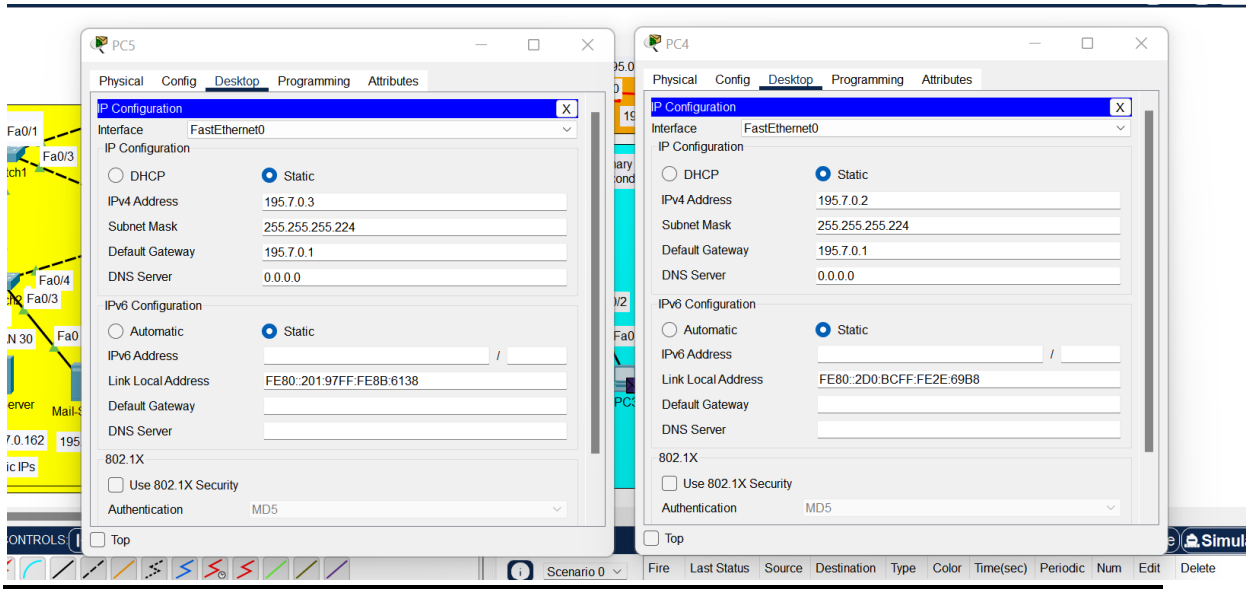


2.3 PCs in the home network (Purple).

the PCs in a home network (represented by the Purple color in your diagram) are getting their IP addresses in a static manner, it means that the IP addresses are manually configured on each device rather than being automatically assigned by a DHCP server. To assign a static IP address to a device, you would need to go into the network settings on the device and configure the IP address, subnet mask, default gateway, and DNS

server manually. While manually assigning static IP addresses can be a simpler and more predictable way to configure a small home network, it can also require more effort and can be more error-prone if not configured correctly.

This 2PC's in network 1 with ip 195.7.0.0 and default ip is 195.7.0.1 and after that I will add IP DNS server.



2.4 PCs in VLANs 10 and 20 (Green and Blue) are getting IPs from router .

If the PCs in VLANs 10 and 20 (Green and Blue) are getting their IP addresses from the router "Router0," it means that DHCP (Dynamic Host Configuration Protocol) has been configured on the router to assign IP addresses to devices on each VLAN.

To configure DHCP on a router, you would need to create a DHCP pool for each VLAN, and specify the range of IP addresses that can be assigned to devices, as well as other options such as the default gateway, subnet mask, and DNS server.

For example, to configure DHCP for VLAN 10, you would create a DHCP pool on the router and specify a range of IP addresses that can be assigned to devices on that VLAN. You would also specify the default gateway and subnet mask for the VLAN, and the DNS server that should be used by devices on the VLAN.

Once DHCP is configured on the router for each VLAN, devices on the VLANs should automatically receive an IP address from the DHCP server when they connect to the network. This can simplify network management and make it easier to manage IP addresses for a large number of devices.

Note that if the router is not the default gateway for the VLANs, you would also need to configure the switches to forward DHCP requests from devices to the router, and to forward DHCP replies from the router to the devices. This can be done by configuring the switch ports that connect to the router as trunk ports and allowing the VLANs to pass through the trunk.

we use next to implemant DHCP in router :

DHCP settings on a router:

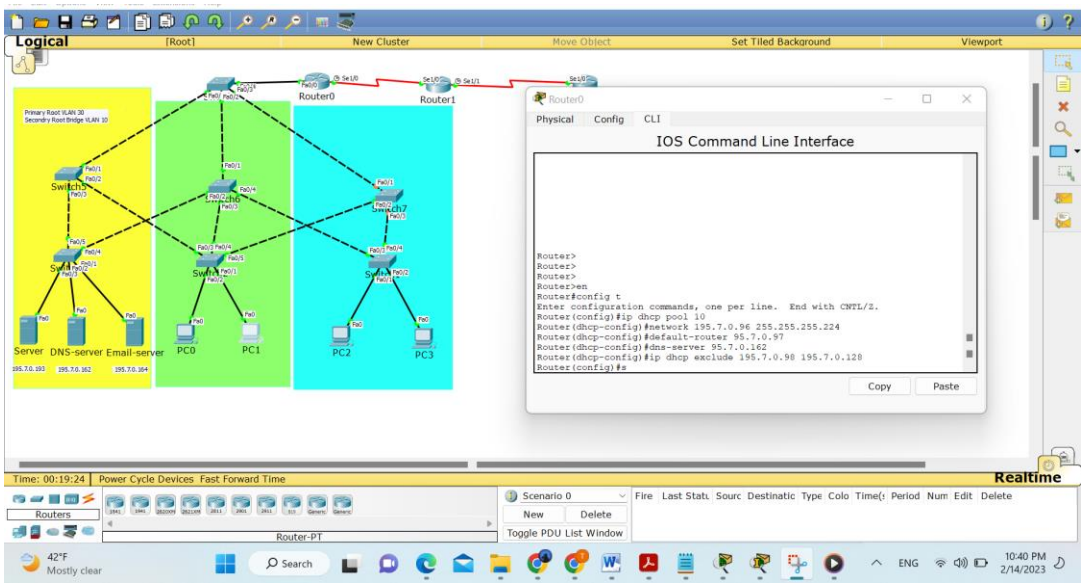
```
R1(config)#ip dhcp pool <poolName>
R1(dhcp-config)#network <Network given IP><Subnet>
R1(dhcp-config)#default <Router interface>
R1(dhcp-config)#dns-server <DNS sever>
R1(dhcp-config)#ip dhcp exclude <Start IP><End IP>
```

The commands you've provided are used to configure a DHCP pool on a router. Here's a breakdown of what each command does:

- R1(config)#ip dhcp pool <poolName>: Creates a DHCP pool and enters DHCP configuration mode.
- R1(dhcp-config)#network <Network given IP><Subnet>: Specifies the network address and subnet mask for the pool.
- R1(dhcp-config)#default <Router interface>: Specifies the default gateway (router interface) for the pool.
- R1(dhcp-config)#dns-server <DNS sever>: Specifies the DNS server address for the pool.
- R1(dhcp-config)#ip dhcp exclude <Start IP><End IP>: Excludes a range of IP addresses from the pool that should not be assigned to DHCP clients.

In summary, these commands are used to define a range of IP addresses that the DHCP server on the router can assign to clients on the network, along with other settings such as the default gateway and DNS server. The "ip dhcp exclude" command is used to reserve specific IP addresses that should not be assigned by the DHCP server.

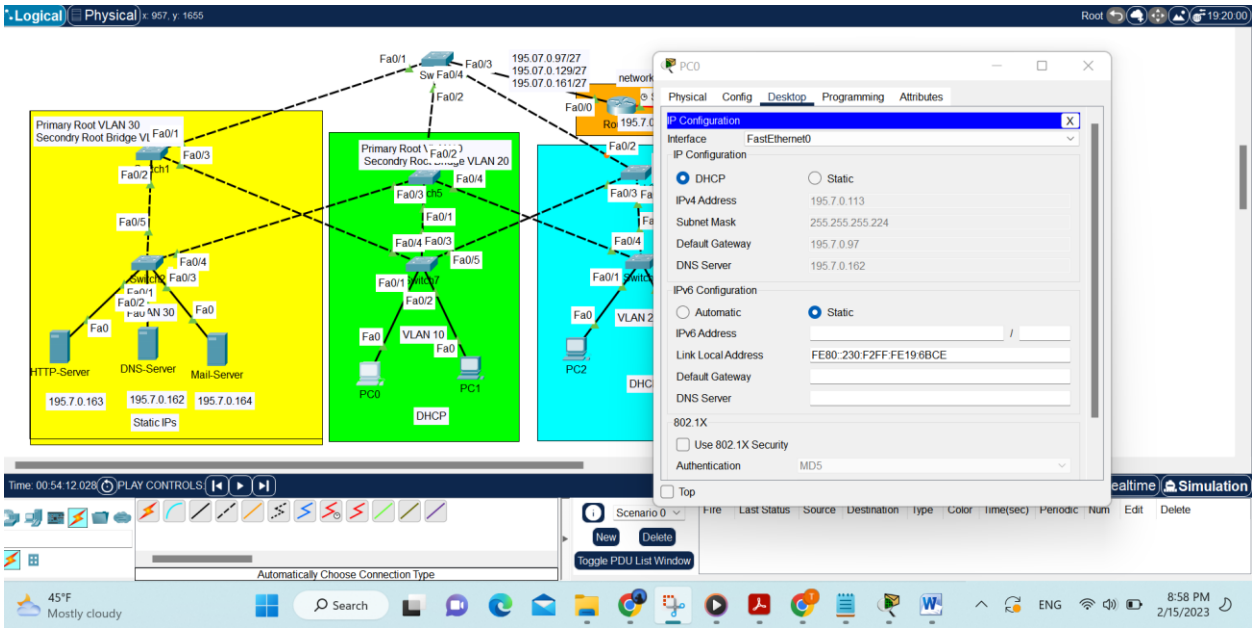
We do two pool one for each vlan :



This the output for PC0 as we can see

DHCP with ip 195.7.0.113 and the default Gatway is 197.7.0.97

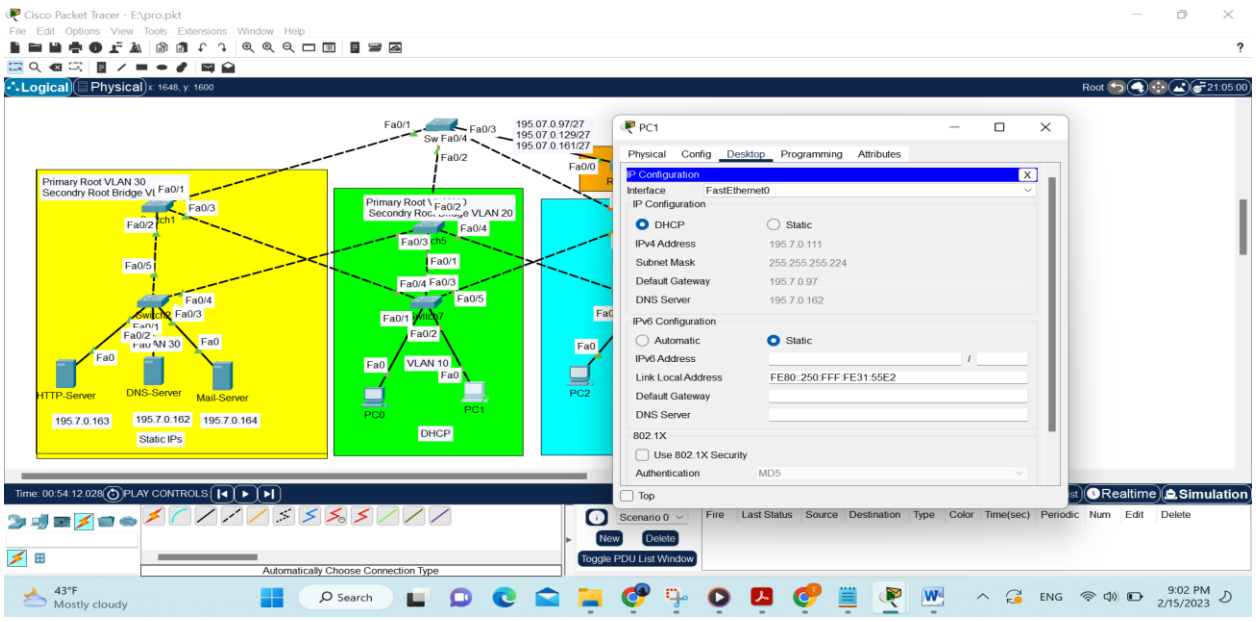
All in network 197.7.0.96



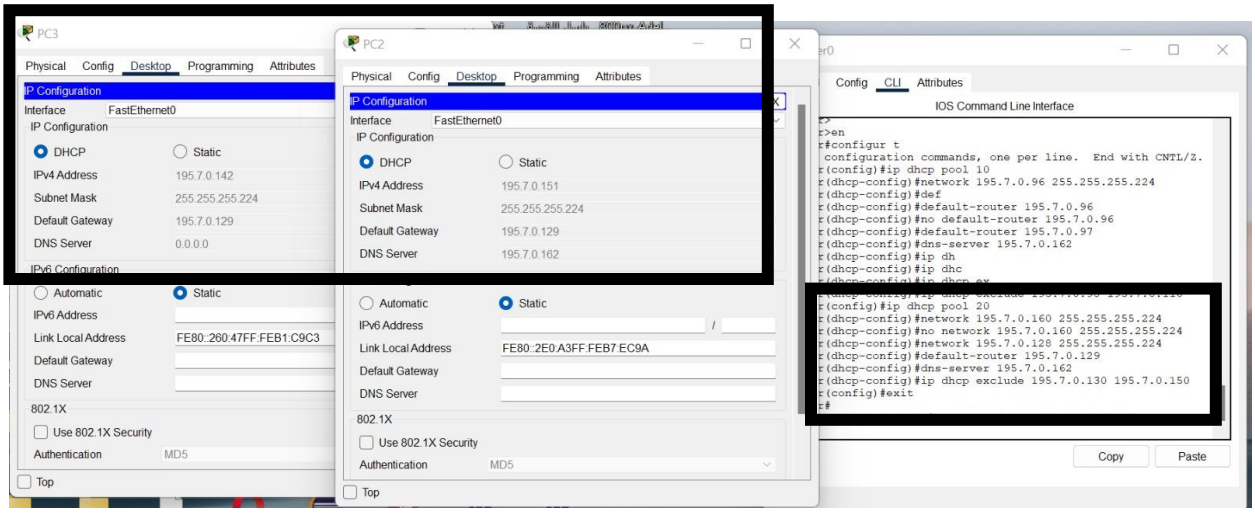
This the output for PC1

DHCP with ip 195.7.0.111 and the default Gatway is 197.7.0.97

All in network 197.7.0.96



the ruselt for vlan 20 in general :



2.5 Servers in VLAN 30 in the data center network (Yellow)

the servers in VLAN 30 of the data center network are using static IP addresses instead of obtaining IP addresses dynamically through DHCP.

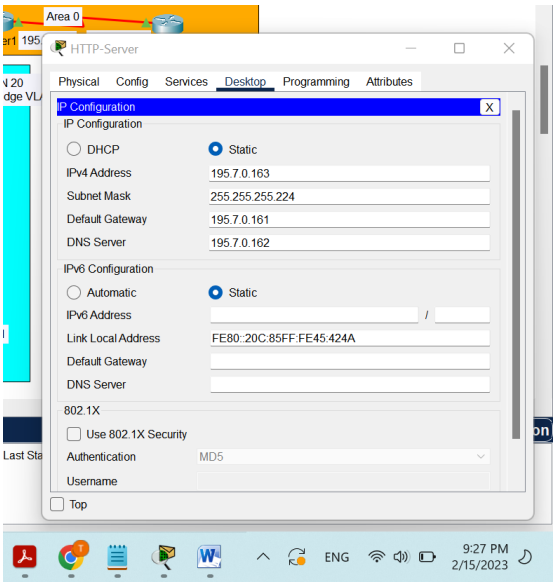
When a device is configured with a static IP address, the device administrator manually assigns the IP address to the device, rather than having it assigned automatically by a DHCP server. In this case, it seems like the network administrator has assigned IP addresses manually to the servers in VLAN 30 based on their assigned network IP addresses.

The network in vlan 30 is: 195.7.0.160

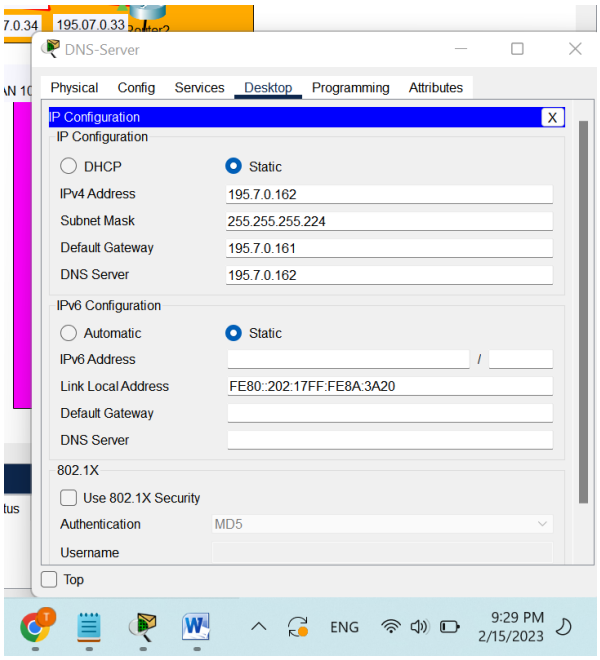
Default Gteway is : 195.7.0.161

DNS Server is : 195.7.0.162

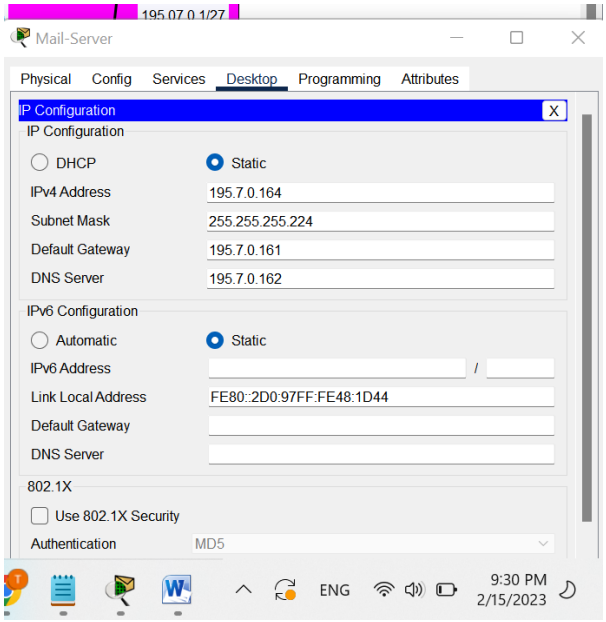
HTTP-Server



DNS-server

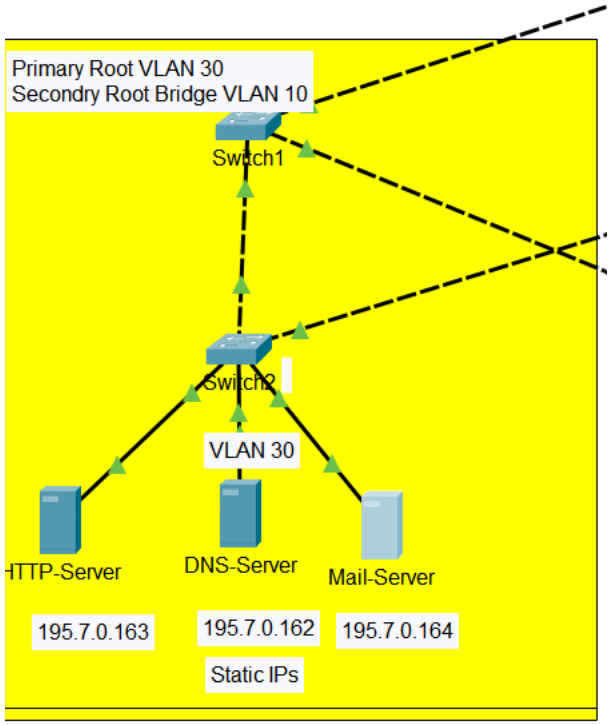


MAIL-Server



Part2: Configuring servers and VLANs

3.1- Three servers are used in this topology: HTTP/WEB server, DNS server, and Email server:

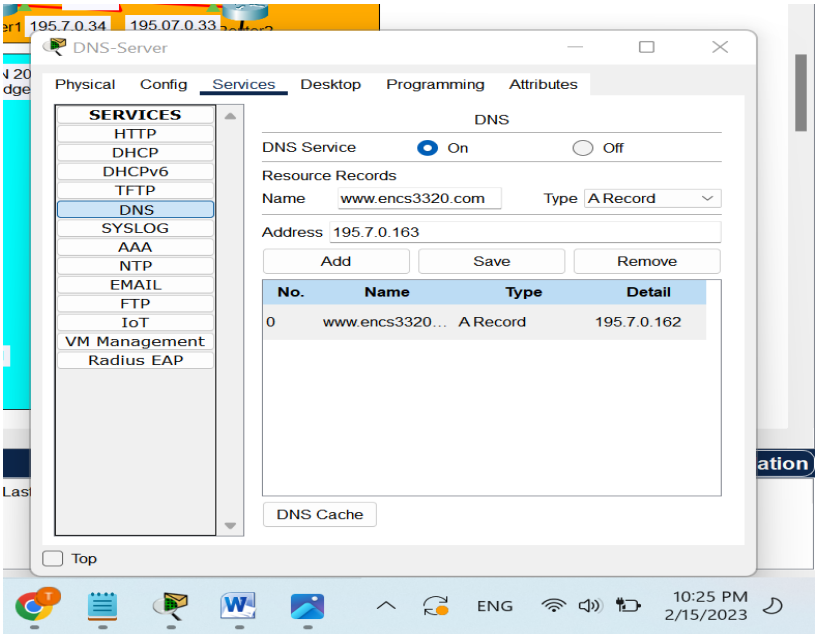


3.2-Configure the DNS server and WEB server with domain name www.ENCS3320.com.

Configuring a DNS server and web server with a domain name is an important task for network administrators. By doing so, they can provide users with an easy-to-remember domain name that they can use to access the website hosted on the web server. To accomplish this task, network administrators typically use a DNS server to translate the domain name into an IP address that the client's computer can use to connect to the web server. In addition, the web server must be configured to serve content for the domain name, which can be accomplished by creating a website that serves the desired content. Once the DNS server and web server are configured properly, clients on the network should be able to access the website at the domain name www.ENCS3320.com using their web browser.

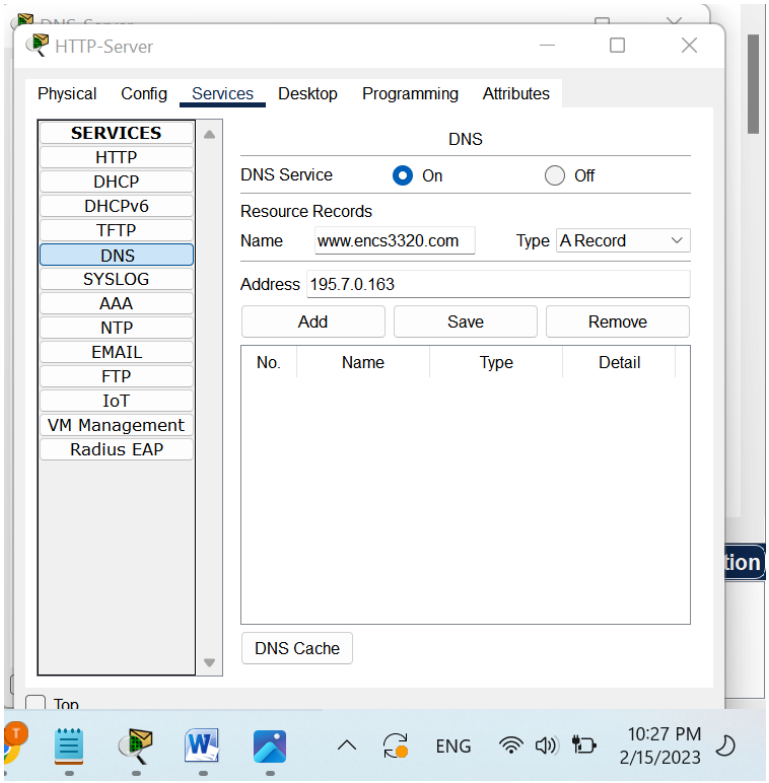
DNS-Server

So we add record for web server

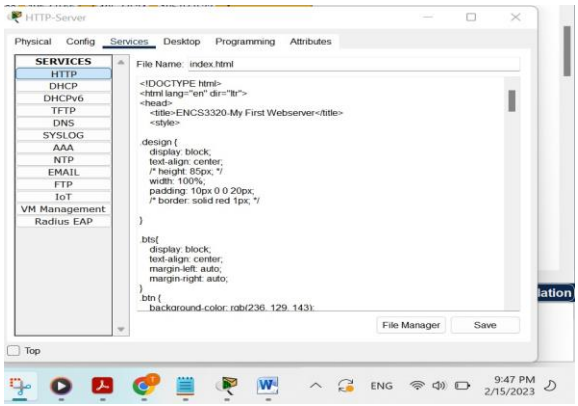


HTTP-Server

First make DNS on then,We add record type A with name :www.encs3330.com address =address of web server =195.7.0.163

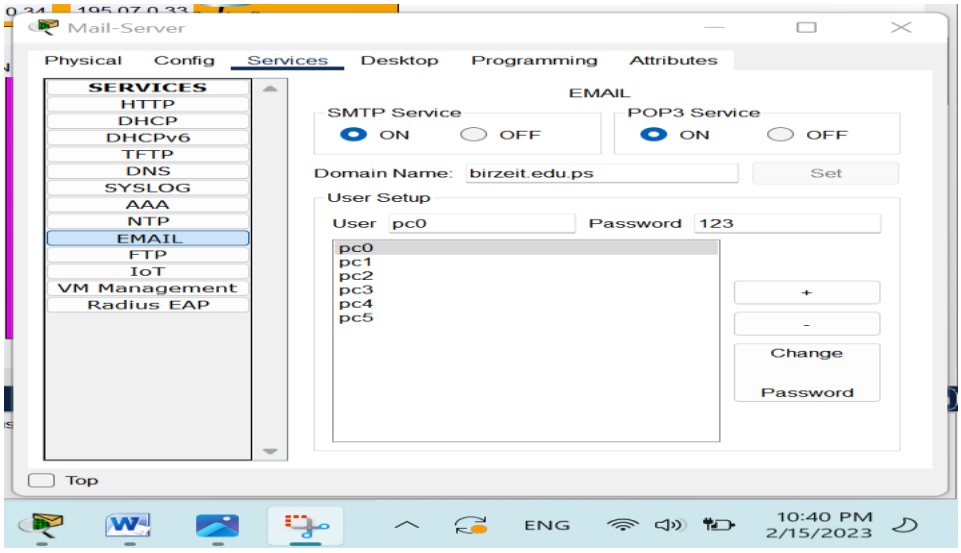


3.3 Create your website by modifying the index.html file in the HTTP server

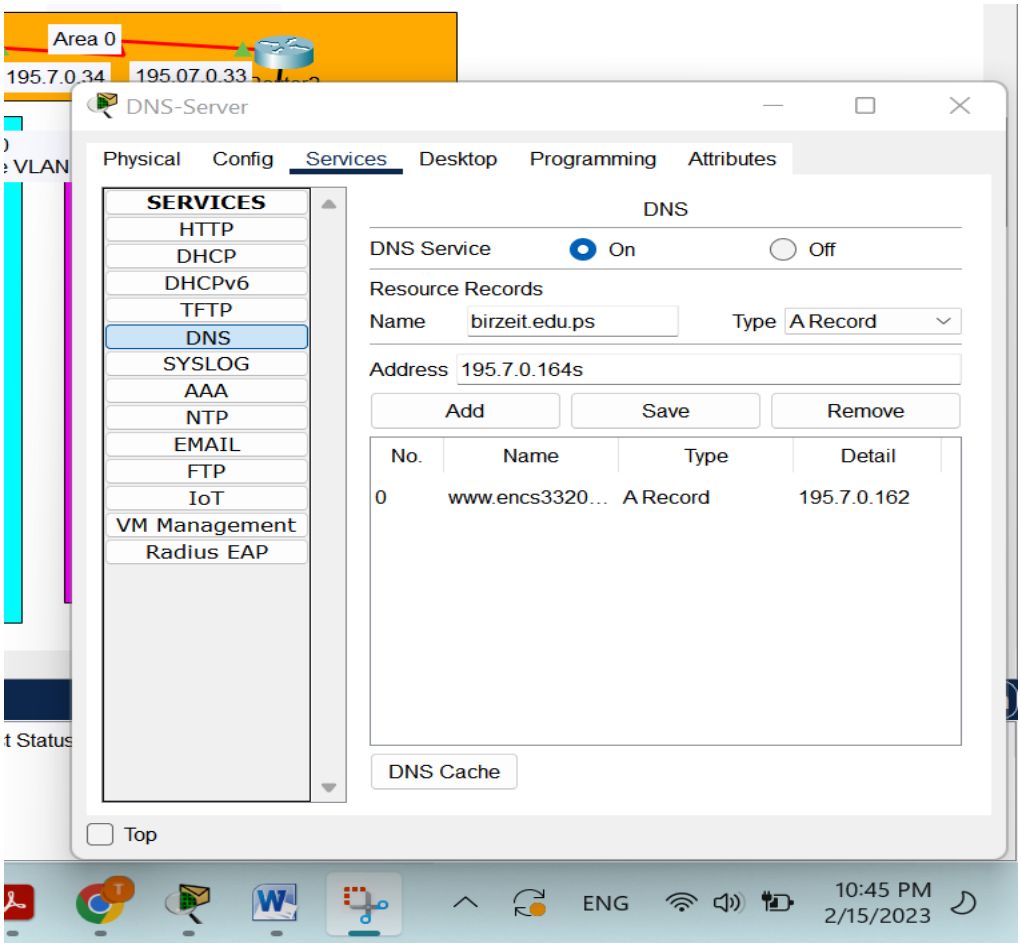


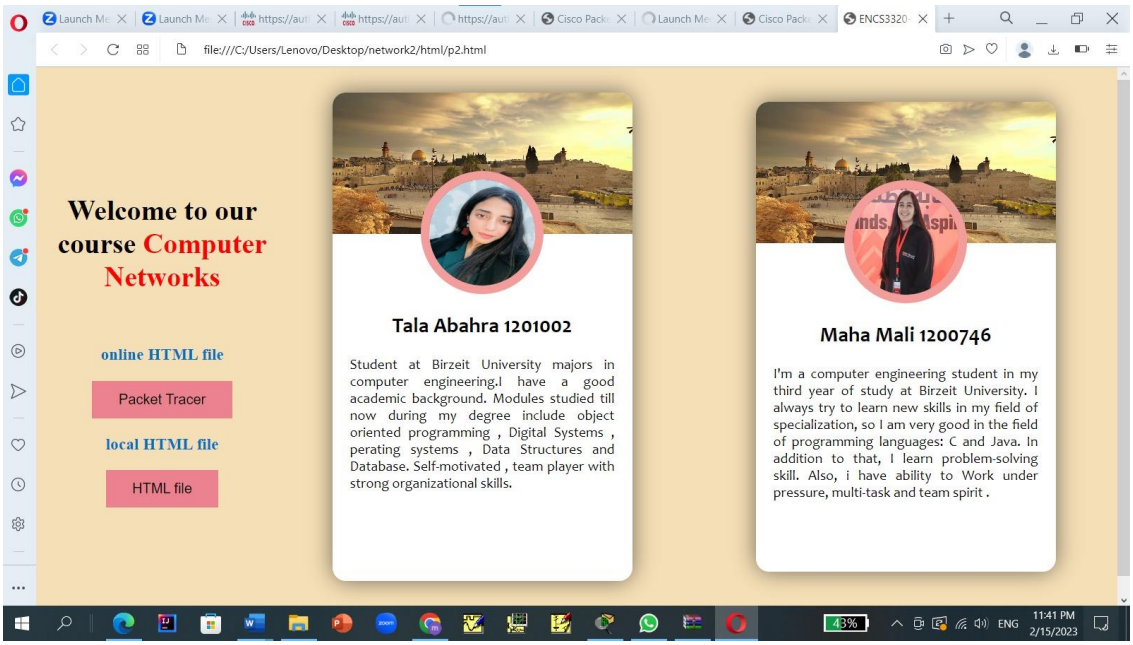
3.4 Create usernames/passwords for all PCs

We make it in mail server :



And add record DNS in server:


Area 0
195.7.0.34
195.07.0.33
DNS-Server
Physical
Config
Services
Desktop
Programming
Attributes
SERVICES
HTTP
DHCP
DHCPv6
TFTP
DNS
SYSLOG
AAA
NTP
EMAIL
FTP
IoT
VM Management
Radius EAP
DNS
DNS Service
On
Off
Resource Records
Name
birzeit.edu.ps
Type
A Record
Address
195.7.0.164s
Add
Save
Remove
No.
Name
Type
Detail
0
www.encs3320...
A Record
195.7.0.162
DNS Cache
Top
ENG
10:45 PM
2/15/2023

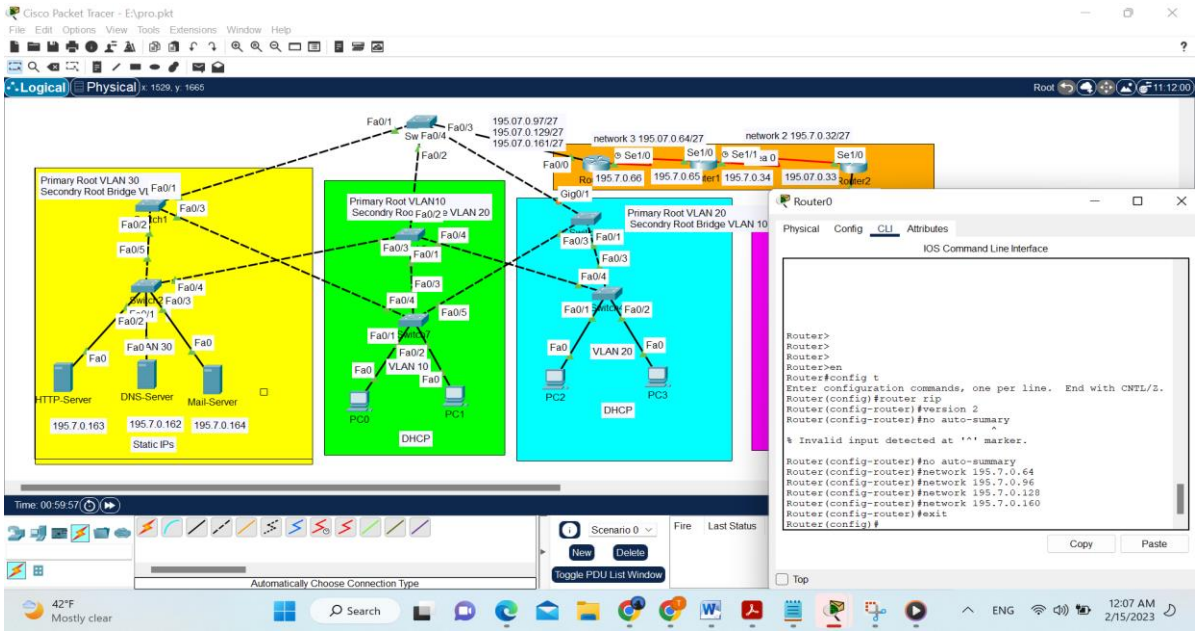

file:///C:/Users/Lenovo/Desktop/network2/html/p2.html
Welcome to our course Computer Networks
online HTML file
Packet Tracer
local HTML file
HTML file
Tala Abahra 1201002
Student at Birzeit University majors in computer engineering.I have a good academic background. Modules studied till now during my degree include object oriented programming , Digital Systems , perating systems , Data Structures and Database. Self-motivated , team player with strong organizational skills.
Maha Mali 1200746
I'm a computer engineering student in my third year of study at Birzeit University. I always try to learn new skills in my field of specialization, so I am very good in the field of programming languages: C and Java. In addition to that, I learn problem-solving skill. Also, i have ability to Work under pressure, multi-task and team spirit .
43%
ENG
11:41 PM
2/15/2023

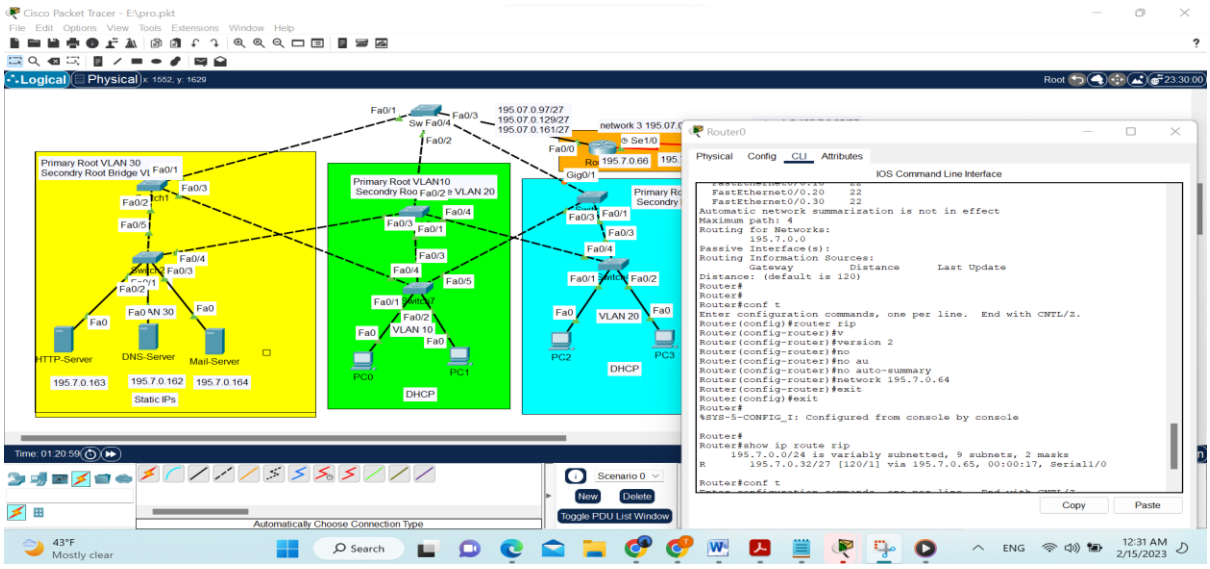
Part3: Applying the routing protocols

1) You need to use routing information protocol version 2 (RIPv2) on “Router0”.

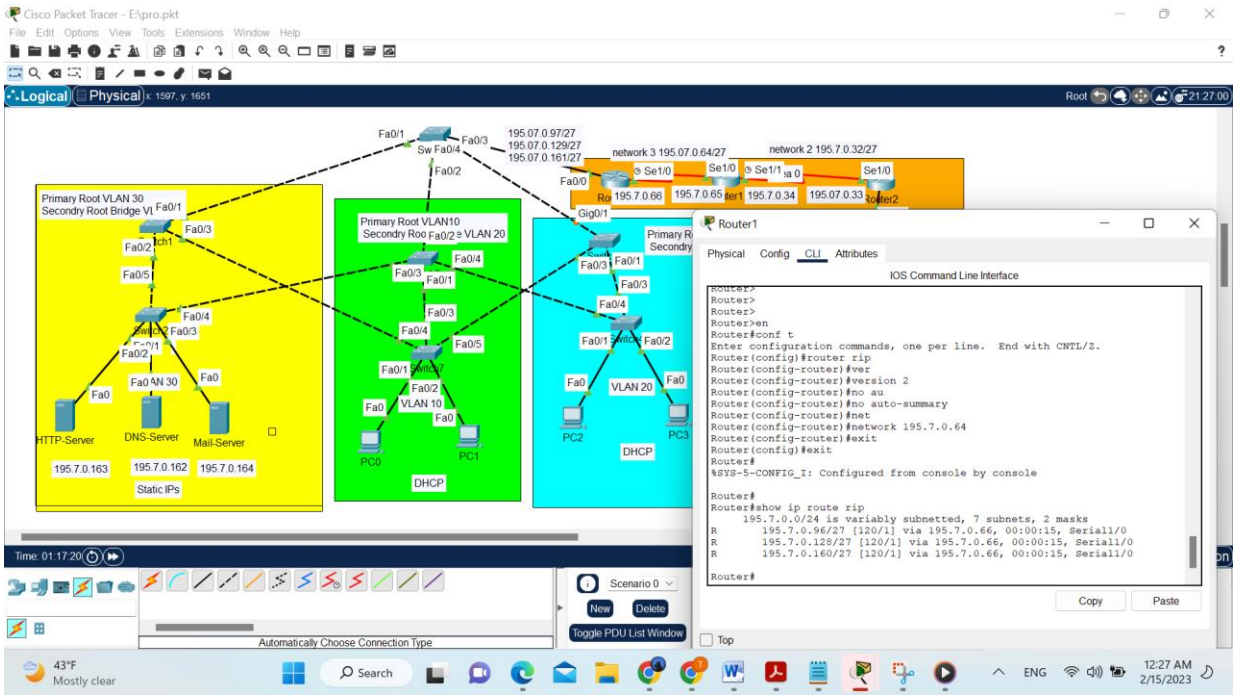
Routing Information Protocol version 2 (RIPv2) is a distance vector routing protocol used in local and wide area networks. It is used to exchange routing information between routers and make routing decisions based on the hop count to a destination network. RIPv2 supports classless routing and allows for the inclusion of subnet mask information in its routing updates. RIPv2 also includes features such as authentication, triggered updates, and route summarization.

In Router0 we have 4 subnet (4 network) to connect in RIPv2





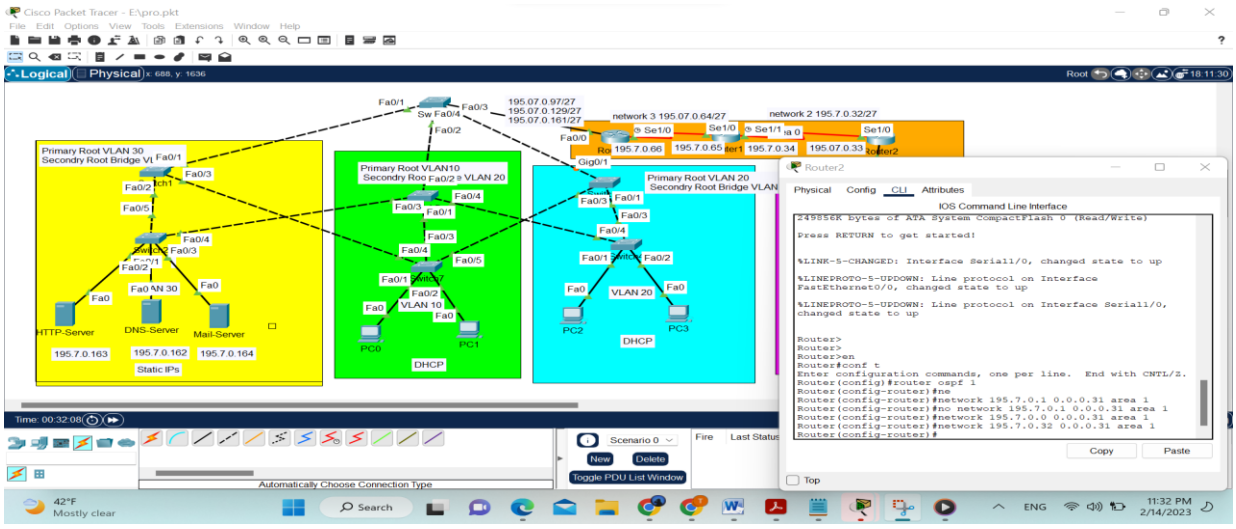
Next add Router1 and check:



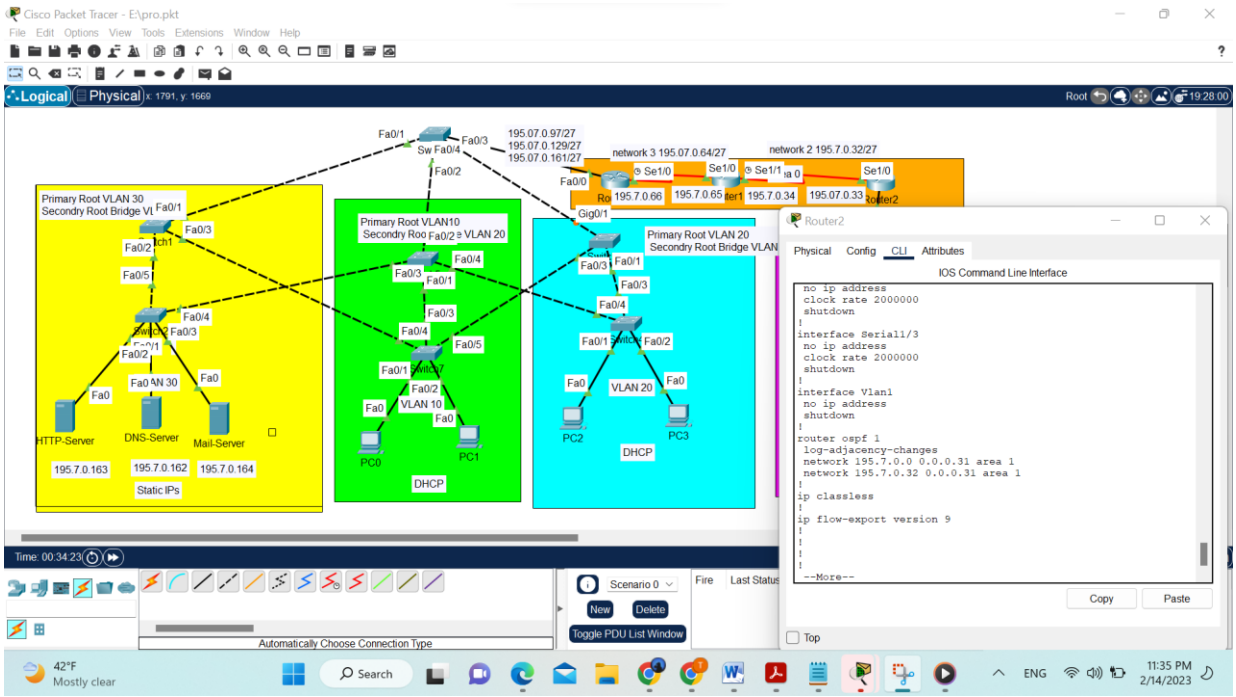
2) use open shortest path protocol (OSPF) on “Router2”.

Open Shortest Path First (OSPF) is a popular routing protocol used in computer networks. It is designed to find the shortest path between two points in a network, and it is used to share routing information between routers. OSPF is preferred over other protocols because it is fast and efficient, can handle large networks, and supports classless IP addressing. It also supports load balancing and can adapt to changes in the network topology, making it a reliable and flexible protocol for managing network traffic.

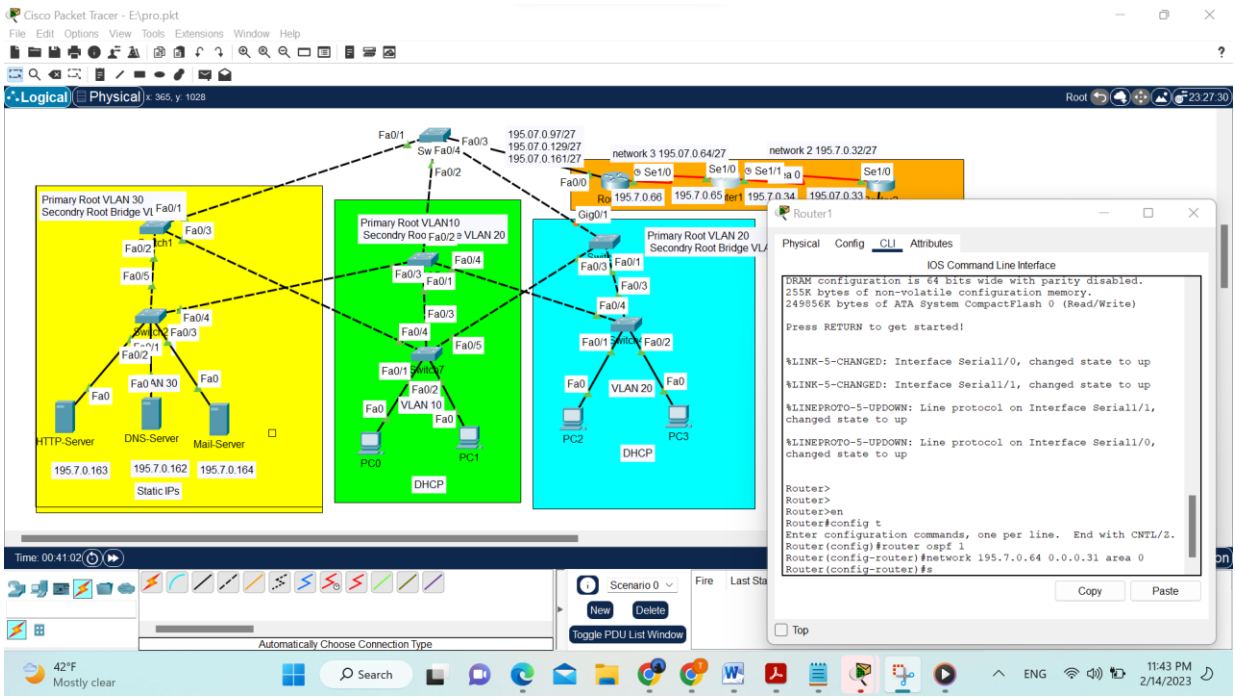
IN Router0:



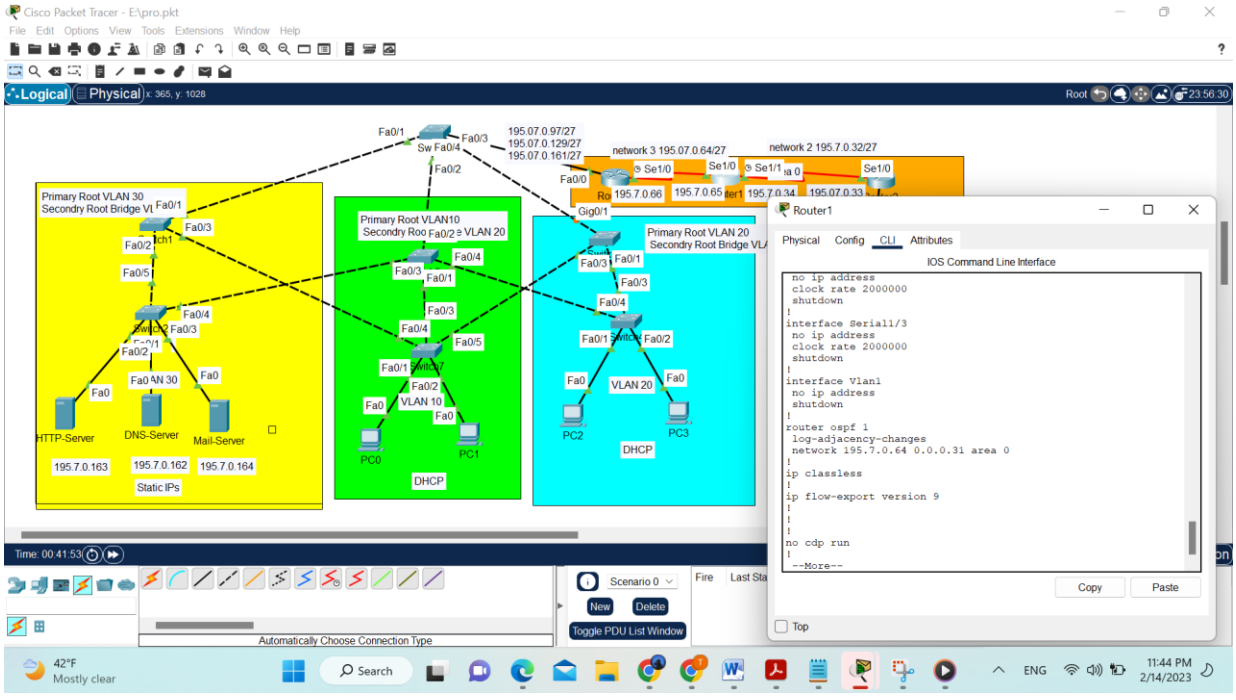
Check it using do show running :



In Router1:



Check it using do show running :



3) On “Router1”, you are required to apply the redistribution of the RIPv2 and OSPF.

To redistribute the RIPv2 and OSPF routes on "Router1", you can follow these steps:

Enable redistribution on "Router1" by entering the following command in global configuration mode:

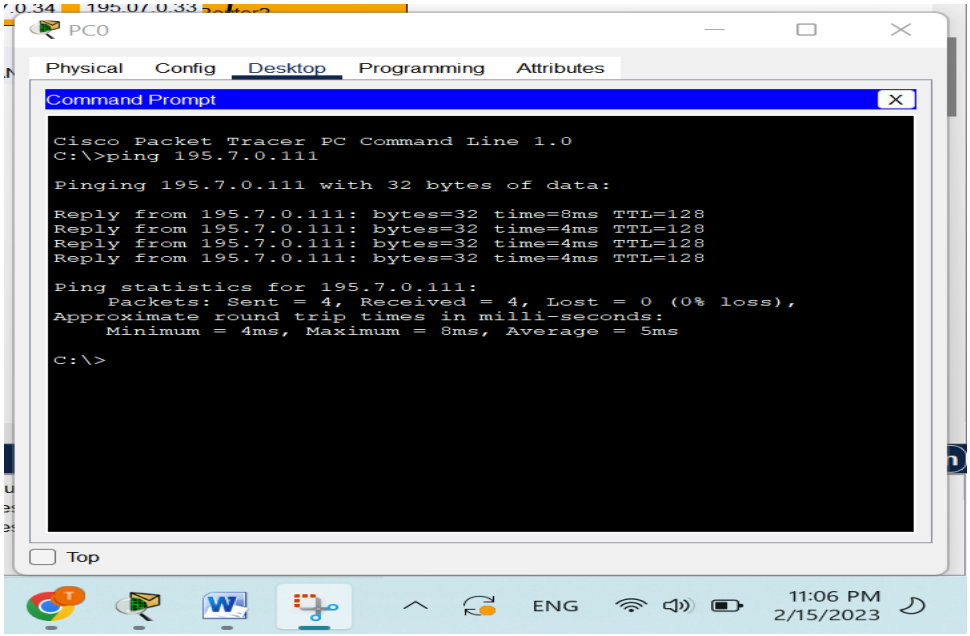
REDISTRIBUTING ROUTING PROTOCOLS

```
RT(config)#router rip
RT(config-router)#redistribute ospf <1-65535
ID> metric <0-16>
RT(config-router)#redistribute eigrp<1-65535
ID> metric <0-16>
RT(config)#router ospf <1-65535 Process ID>
RT(config-router)#redistribute rip subnets
RT(config-router)#redistribute eigrp <1-65535>
subnets
```

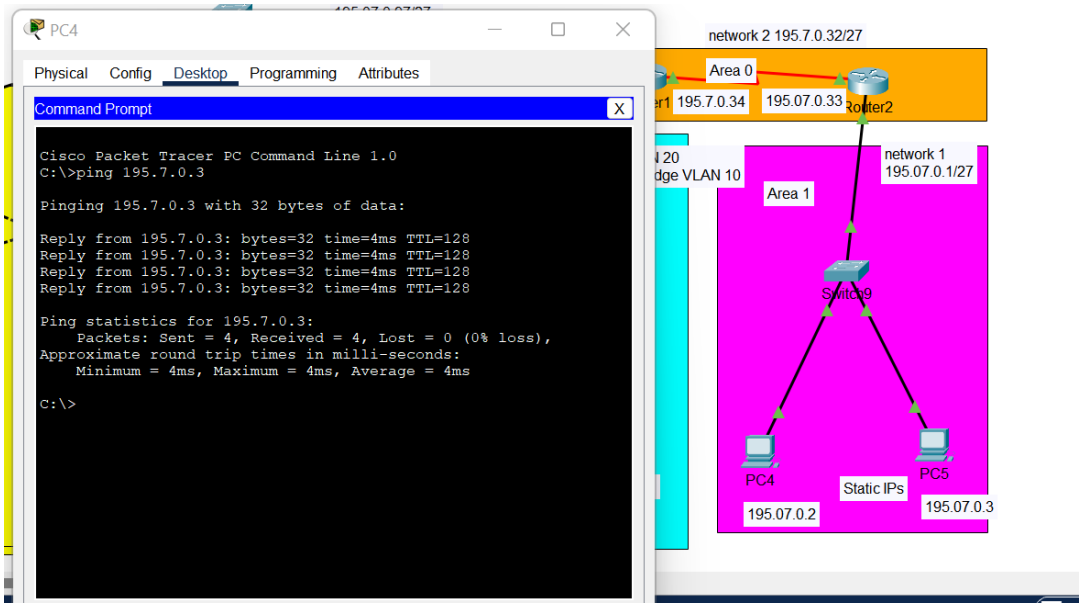
Part4: Testing the connectivity

4.1Test the connectivity between all PCs

Test 1) I try to send packet from pc0(195.7.0.113) to p1(195.7.0.115)(in the same network and i get next:

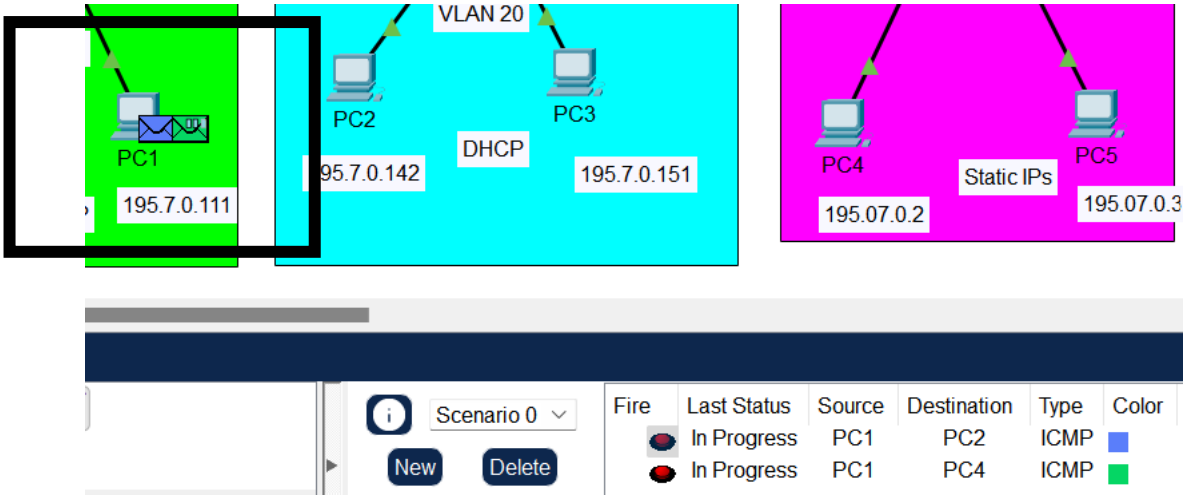


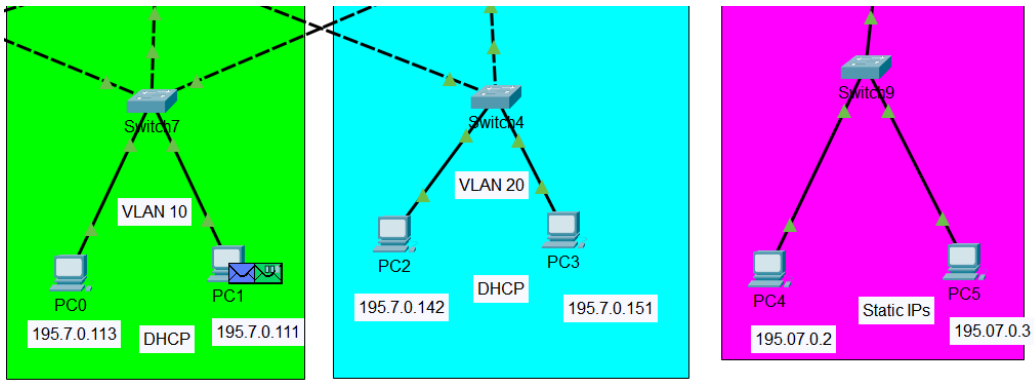
Test 2) send packet from pc0(195.7.0.2) to pc1(195.7.0.3)(in the same network and i get next:

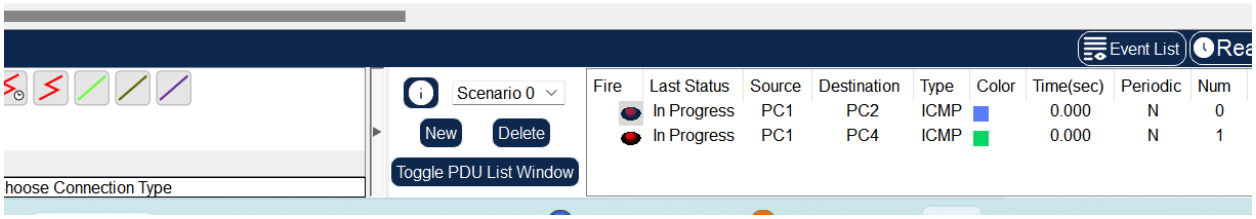


Test 3) send from PC1 to PC2 and PC3 (we can see queuing massage from pc1 to pc4)

Which are from different network.

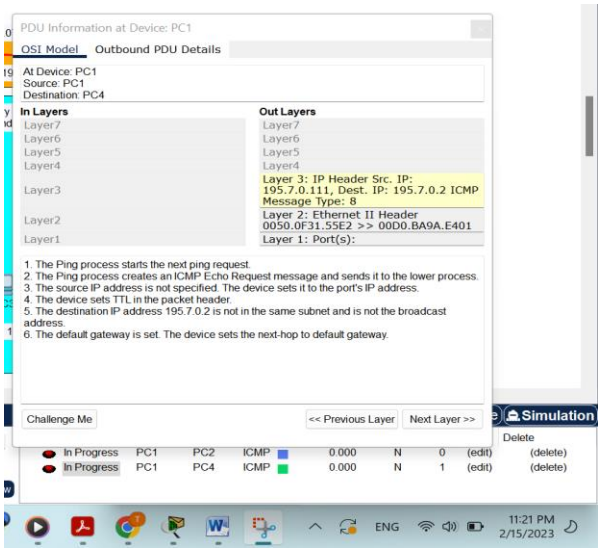


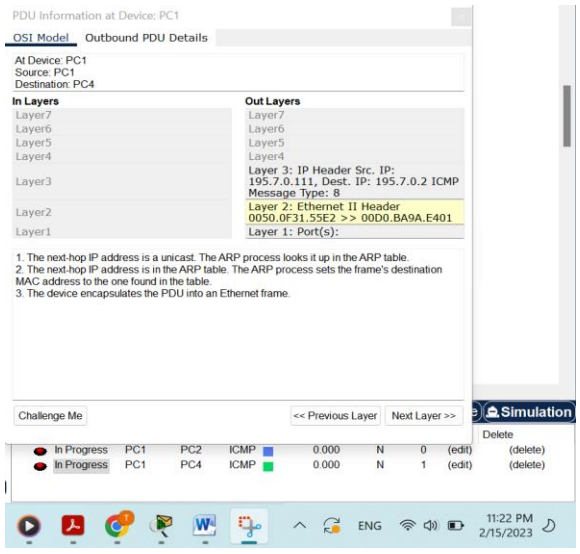


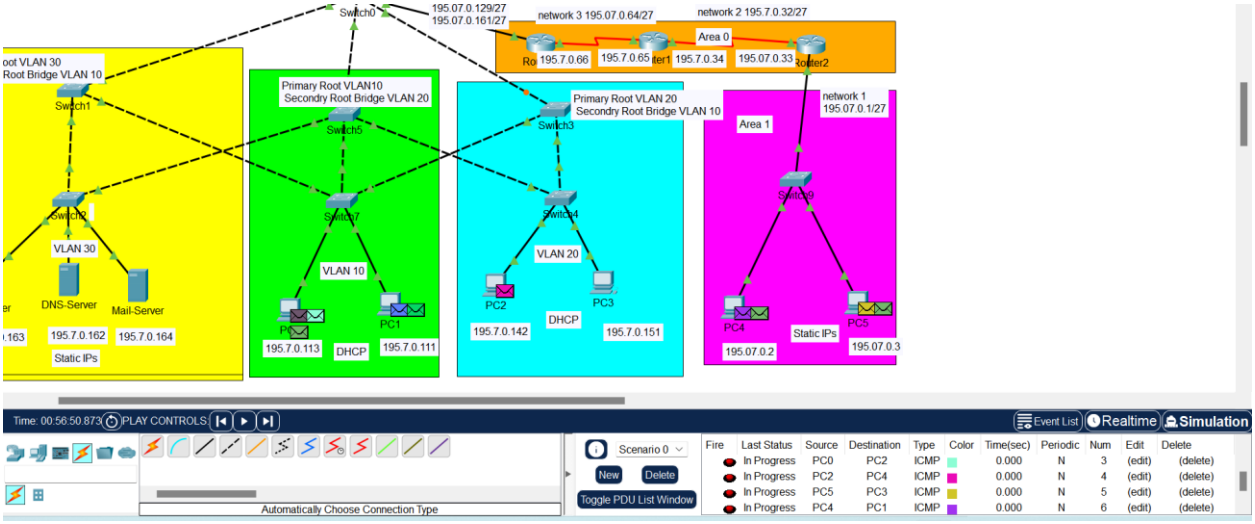


In general, the operation will succeed on the same network, but others will not..

The reason was either by the routing process or by the networking and Vlan process, as the process(PC1 to PC4) continued and did not stop.

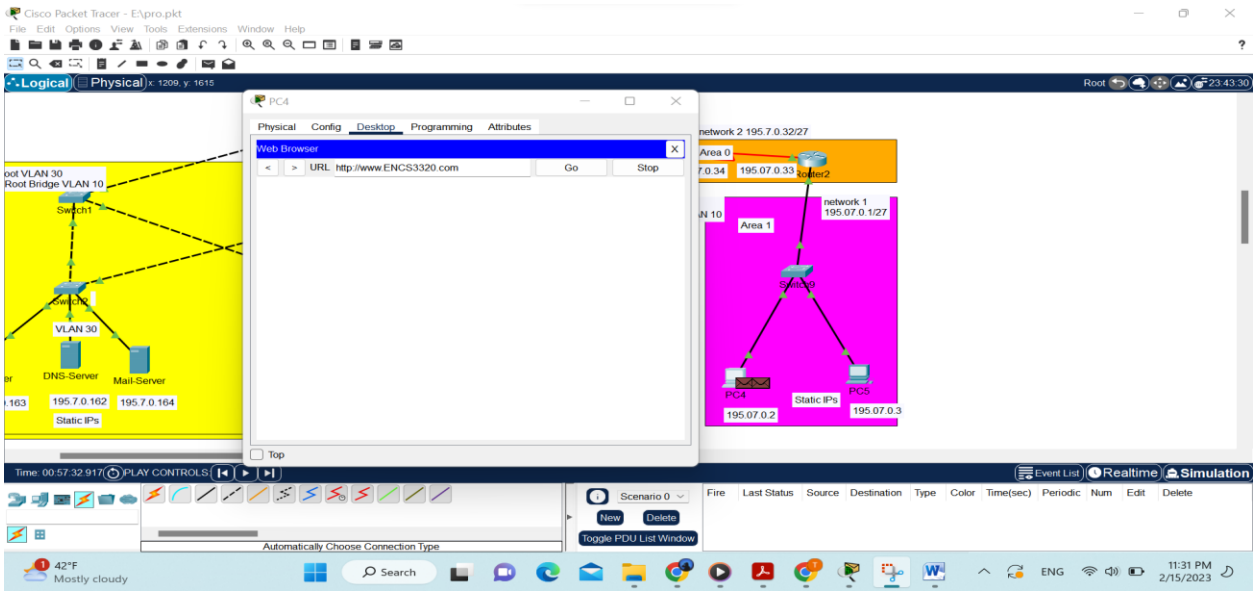




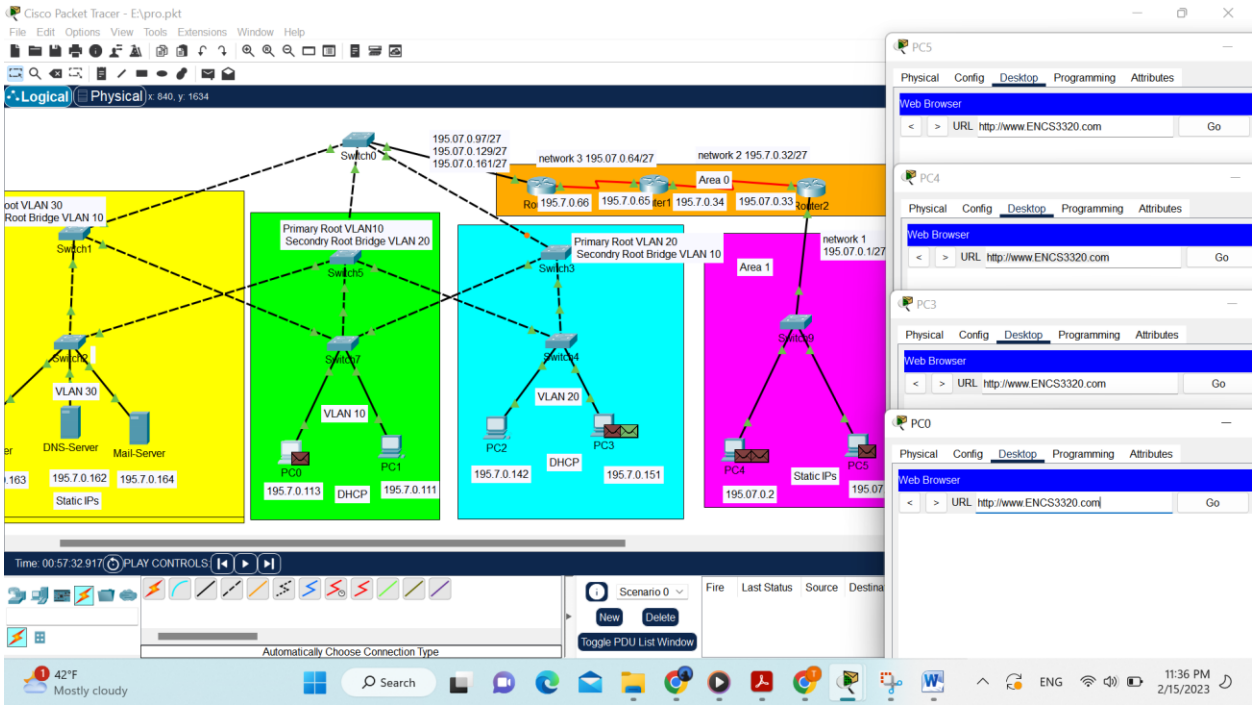


I try to test all case , without result ^_^

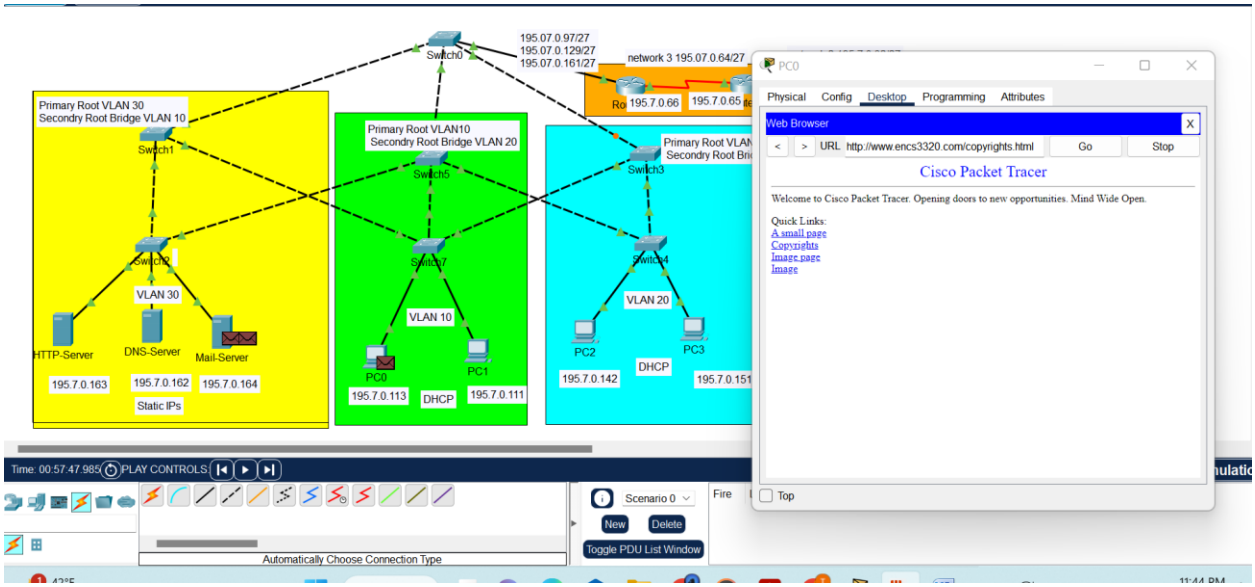
Access www.ENCS3320.com from all PCs



In general, I did what was supposed to be done, but there are several problems in the basic configuration of the process, so the packet remains unsent and is present at the sender without giving any errors.



After time :



- . Send emails from one PC to other PCs and take snapshots at the receiving PCs

4. References

[1] https://www.netacad.com/courses/packet-tracer . Accessed on 1-2-2023 at 6:22PM.

[2] https://www.geeksforgeeks.org/router-configuration-with-cisco-packet-tracer/ . Accessed on 1-2-2023 at 6:30PM.

[3] https://www.packettracernetwork.com/labs/lab1-basicswitchsetup.html . Accessed on 3-2-2023 at 6:38PM.

[4] https://www.youtube.com/watch?v=frUQMHXhnvs . Accessed on 3-2-2023 at 6:44PM.

[5] https://www.youtube.com/watch?v=uEC0t-o27jE . Accessed on 3-2-2023 at 7:04PM.