Faculty of Engineering & Technology

Electrical & Computer Engineering Department

Computer Networks Laboratory – ENCS4130

EXP. No. 7. Switching and VLANs 1 - Router on Stick

Report#2

Prepared by: Rahaf Naser 1201319

Instructor: Dr. Ahmad Shawahna

Teaching Assistant: Eng. Katy Sadi

Section: 5

Date: 14/12/2023

Abstract
The aim of this experiment is to learn how to configure a Cisco IOS Switch using the IOS command-line interface (CLI), how to use switch simulator, how to split Cisco router interface into sub interfaces, and how to split Cisco switches into multiple virtual ones and create VLANS. In this experiment we will use two Cisco router, Six PCs, three Cisco switches, One Serial cable, and several CAT5 straight-wired cable.

Table of contents

Acronyms and Abbreviations

VLAN	Virtual Local Area Network
MAC	Media Access Network
CLI	Command-Line Interface
OSI	Open Systems Interconnection
ISP	Internet Service Providers
LAN	Local Area Network
IEEE	Institute of Electrical and Electronics Engineers
PCP	Priority Code Point
DEI	Drop Eligible Indicator
VID	VLAN Identifier
TPID	Tag Protocol Identifier
TCI	Tag Control Information
ID	Identifier

List of Figures

List of Tables

1.Introduction

1.1. How does a switch work

A network switch connects and transmits data packets to and from devices on a local area network (LAN). Far from a router, a switch only distributes information to the one device for which it was designed, including some other switch, a router, or a user’s computer, rather than to several devices in a network [1].

Nowadays, networks are critical for supporting companies, offering connected services, and enabling collaboration, among other things. As they link devices that share resources, network switches are a vital component of all networks [1].

A network switch works at the data link Layer 2 of the architecture of Open Systems Interconnection (OSI). It accepts packets from access points linked to physical ports and then sends them only via the ports going to a destination device [1].

These could also function where routing occurs at the network Layer 3. Switches are standard components in ethernet, fiber channels, InfiniBand, and asynchronous transfer mode (ATM) networks, to name a few. The majority of switches nowadays, however, utilize ethernet.

A network switch connects network devices (printers, computers, and wireless devices/access points, and enables users to exchange data packets. Switches may be both hardware and software-based virtual devices that govern physical systems. In today’s network systems, switches make up the vast bulk of network equipment.

They connect desktop PCs, industrial machinery, wireless access points, and specific internet of things (IoT) devices, including card entry systems for the internet [1].

1.2. IEEE 802.1Q VLAN

IEEE 802.1Q, often referred to as **Dot1q**, is the networking standard that supports virtual local area networking (VLANs) on an IEEE 802.3 ETHERNET network. The standard defines a system of **VLAN tagging** for Ethernet frames and the accompanying procedures to be used by bridges and switches in handling such frames. The standard also contains provisions for a quality-of-service prioritization scheme commonly known as IEEE 802.1p and defines the Generic Attribute Registration Protocol[2].

Portions of the network which are VLAN-aware (i.e., IEEE 802.1Q conformant) can include VLAN tags. When a frame enters the VLAN-aware portion of the network, a tag is added to represent the VLAN membership. Each frame must be distinguishable as being within exactly one VLAN. A frame in the VLAN-aware portion of the network that does not contain a VLAN tag is assumed to be flowing on the **native VLAN** [2].

1.2.1. Tagging

VLAN tagging is a method through which more than one VLAN is handled on a port. VLAN tagging is used to tell which packet belongs to which VLAN on the other side. To make recognition easier, a packet is tagged with a VLAN tag in the Ethernet frame. Independent logical systems can be formed accurately with the help of the VLAN tagging inside a physical network itself. Individual domains can be created with the help of this VLAN tagging system [3].

VLAN tagging is performed by the putting the VLAN ID into a header to identify which network it is present in. This helps in determining which interface or broadcast area the information packet needs to be sent to in order to receive the right information. The switches need to be configured beforehand for working properly with the process of VLAN tagging. With this system, multiple broadcast systems can be segregated into individual domains. Bridging traffic can be forwarded with the use of this system. Clients and information can be organized, configured and grouped logically. Overall, the functionality of the system is optimized [3].

1.2.2. VLAN numbering

VLANs are numbered in the range 1 to 4094. However, a maximum of 2048 (6200 Switch Series) or 512 (6000, 6100 Switch Series) VLANs are supported.

By default, VLAN 1 (the default VLAN) is associated with all interfaces on the switch. VLAN 1 cannot be removed from the switch [4].

1.3. Trunk and access ports

Trunk Port: A trunk port is a port, which is used to connect to another switch or router. It is a link that carries many signals simultaneously. Basically, it can transmit data from multiple VLANs. It uses tags in order to allow signals to get to the correct endpoint. Trunk Port offers higher bandwidth and lower latency. The Trunking takes place in layer 2 of the OSI model, which is known as the “data link layer”. The device uses the IEEE 802.1Q encapsulation or tagging method, in order to correctly deliver the traffic on a trunk port with several VLANs [5].

Access Port: The access port is a type of port that is like a type of connection on a switch that provides the virtual machines with connectivity via a switch or VLAN. Basically, it transmits data to and from a specific/single VLAN. This doesn’t cause signal issues because the frames remain within the same VLAN. For complex networks, it is not that efficient to work with. One can configure the port as a host port, to optimize the performance of the access port [5].

1.4. Sub interface on Routers

A subinterface is a virtual interface created by dividing one physical interface into multiple logical interfaces. A sub-interface in a Cisco Router uses the parent physical interface for sending and receiving data. Subinterfaces are used for a variety of purposes. If we have one Router with one physical interface, but needed to have the router connected to two IP networks to route traffic between two routers, we can create two sub interfaces within the physical interface, assign each sub interface an IP address within each subnet and then route the data between two subnets. We use Subinterfaces for inter VLAN traffic routing by using a Router-on-a-Stick configuration, NBMA (Non Broadcast Multiple Access) WAN solutions like frame-relay or ATM [6].

2.Procedure and Discussion

2.1. Building the topology

I built the topology shown in Figure 1 below. I used Router-PT for the routers and Switch-PT for the switches and PC-PT for PCs. I used automatically use connection type for the connections between the PCs, switches and routers.

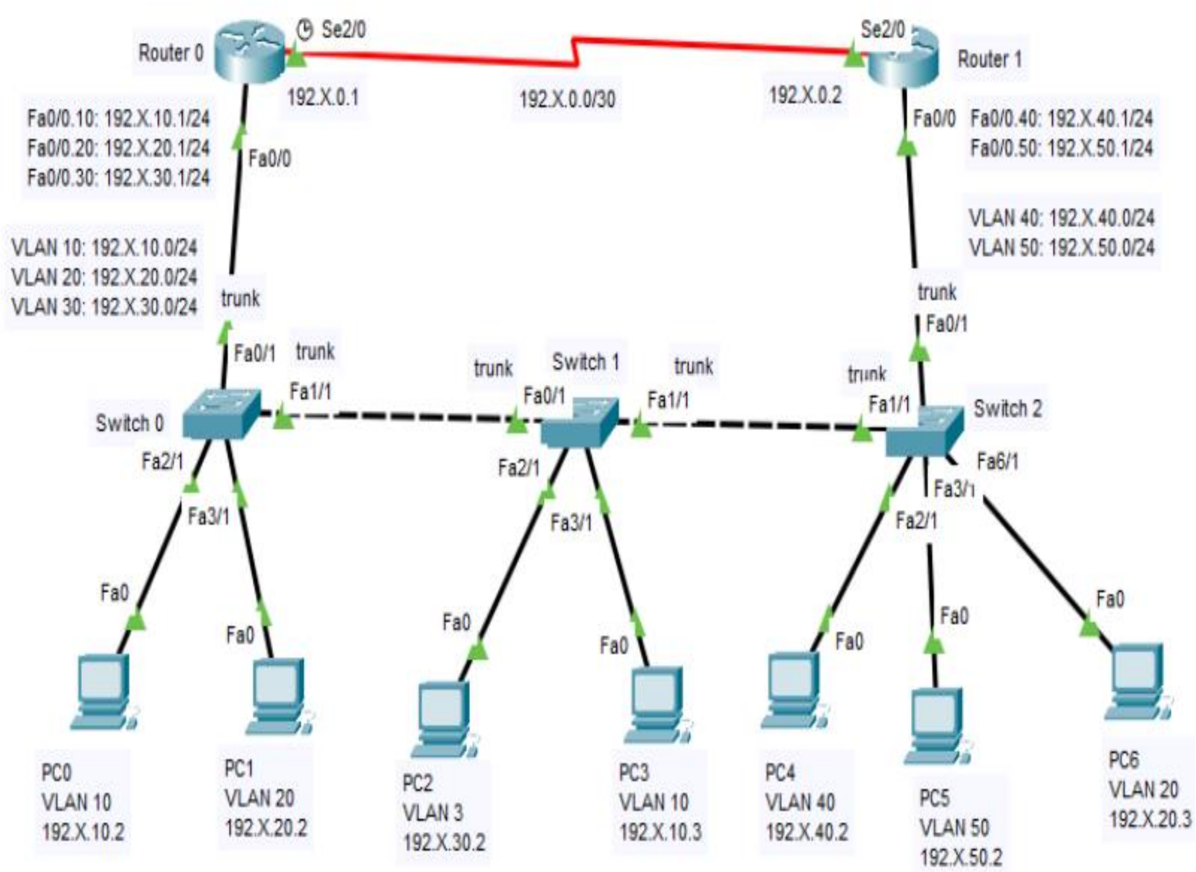

Figure 1: Lab Topology

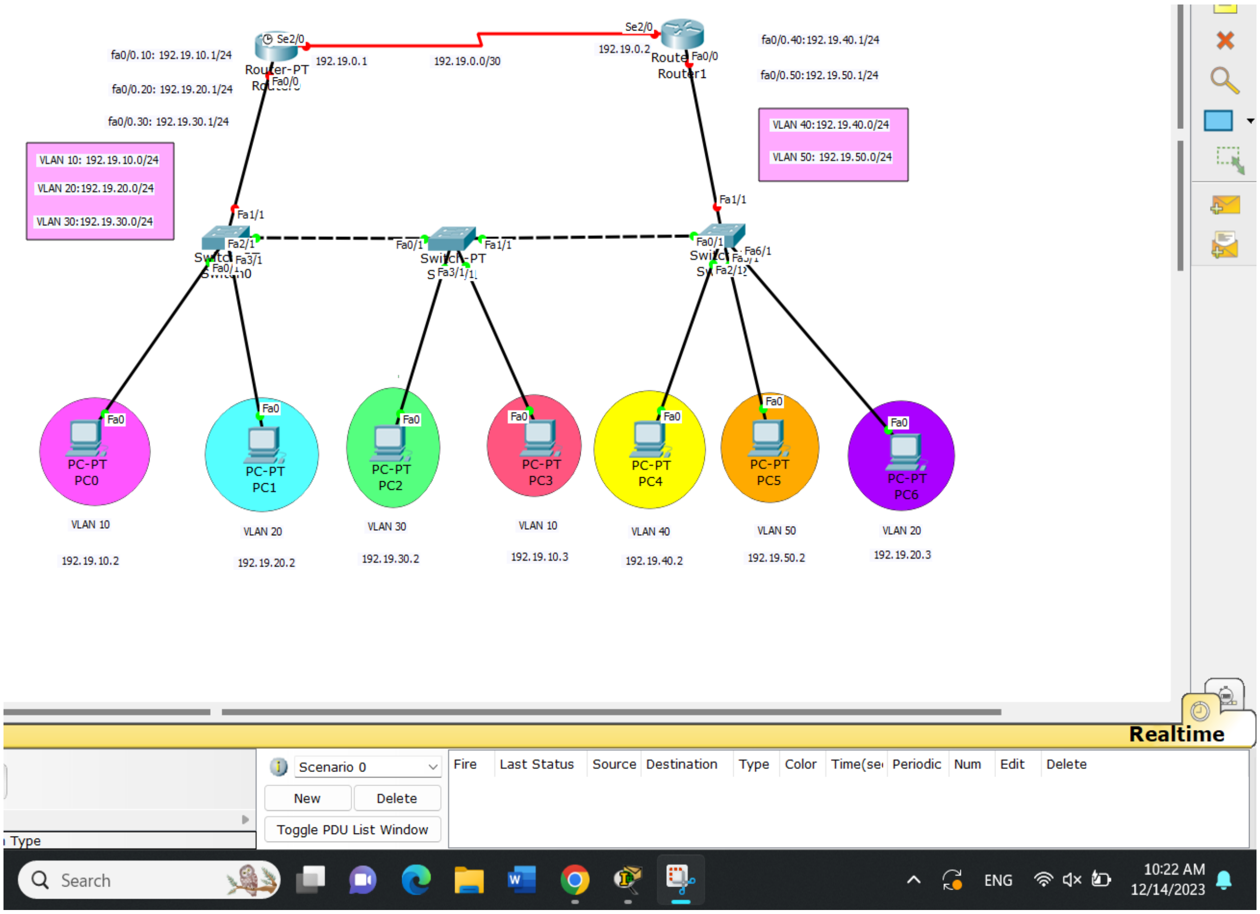

Figure 2: My Topology

Table 1 show the subnetting of network IP addresses and highlights the sections where router interfaces, sub-interfaces, and PCs should be configured. Each PC has its IP address, subnet mask, and gateway set up.

Table 1: Network IP's

Area	Network	Device	Interface	IP	Subnet Mask	Wildcard Mask	VLAN Id
Area 0	192.19.0.0/30	Router 1	Se2/0	192.19.0.2	255.255.255.252	0.0.0.3	VLAN 1
		Router 0	Se2/0	192.19.0.1	255.255.255.252	0.0.0.3	VLAN 1
	192.19.10.0/24	Router 0	Fa0/0.10	192.19.10.1	255.255.255.0	0.0.0.255	VLAN 10
		PC0	Fa0	192.19.10.2	255.255.255.0	0.0.0.255	VLAN 10
		PC3	Fa0	192.19.10.3	255.255.255.0	0.0.0.255	VLAN 10
	192.19.20.0/24	Router 0	Fa0/0.20	192.19.20.1	255.255.255.0	0.0.0.255	VLAN 20
		PC1	Fa0	192.19.20.2	255.255.255.0	0.0.0.255	VLAN 20
		PC6	Fa0	192.19.20.3	255.255.255.0	0.0.0.255	VLAN 20
	192.19.30.0/24	Router 0	Fa0/0.30	192.19.30.1	255.255.255.0	0.0.0.255	VLAN 30
		PC2	Fa0	192.19.30.2	255.255.255.0	0.0.0.255	VLAN 30
	192.19.40.0/24	Router 1	Fa0/0.40	192.19.40.1	255.255.255.0	0.0.0.255	VLAN 40
		PC4	Se2/0	192.19.40.2	255.255.255.0	0.0.0.255	VLAN 40
	192.19.50.0/24	Router 1	Fa0/0.50	192.19.50.1	255.255.255.0	0.0.0.255	VLAN 50
		PC5	Fa0	192.19.50.2	255.255.255.0	0.0.0.255	VLAN 50

For example this is the IP Configuration for PC2 according to above table.

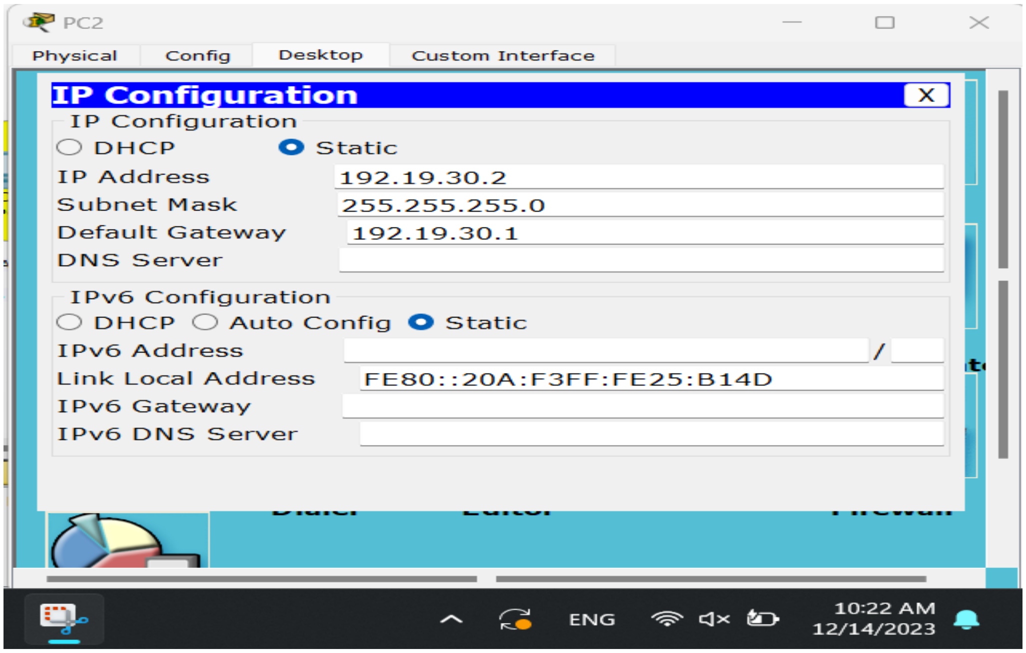

Figure 3: PC2 Configration

After powering down the switch, an additional port titled "PT-SWITCH-NM-1CFE Module" was installed for future use, as shown in Figure 4.

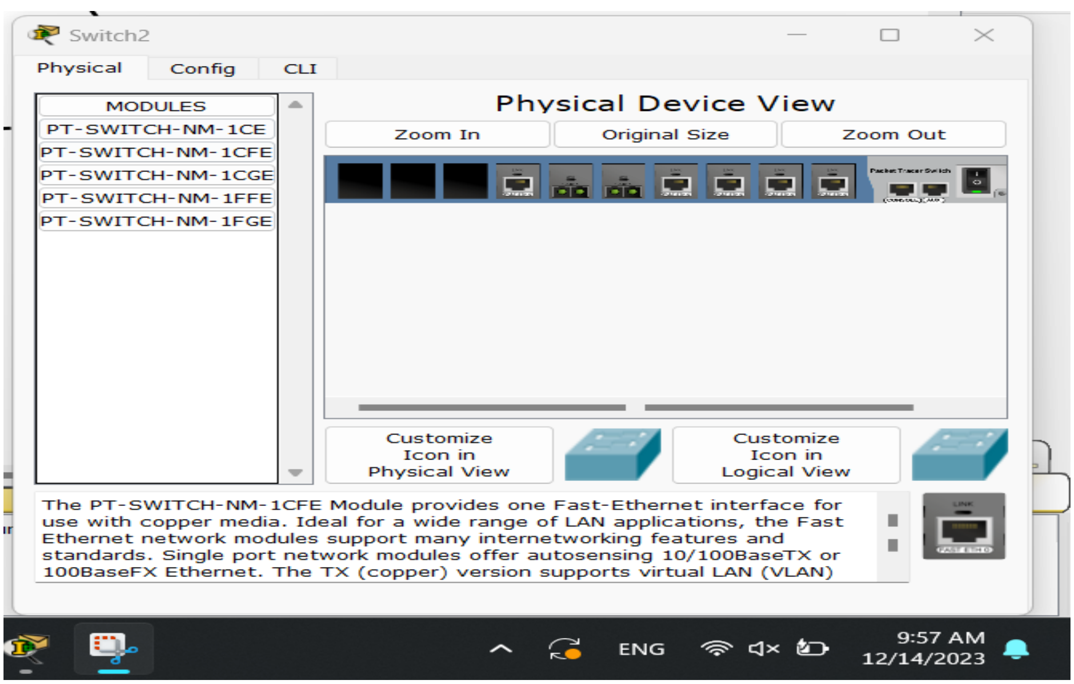

Figure 4: Adding an extra port for a Switch

2.2. Configuring Routers

2.2.1. Configuring Routers Sub Interfaces

To implement the "Router on a Stick" concept in VLAN, a sub-interface must be established for each VLAN set up on the switch. This sub-interface serves as the default gateway for its respective VLAN. In the presented topology, sub-interfaces are initialized on both Router0 and Router1. Specifically, on Router0's interface Fa0/0, three sub-interfaces representing VLANs 10, 20, and 30 are initialized. The setup process is as follows:

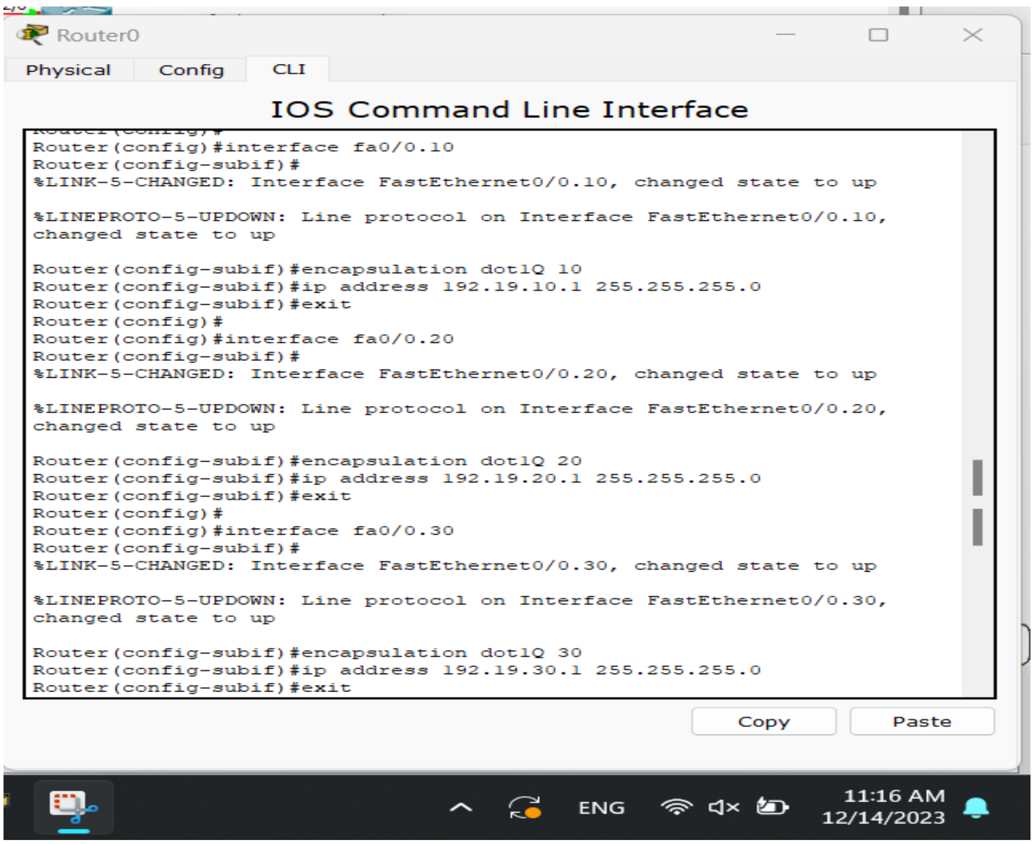

Figure 5: Configuration Router 0 Sub-Interfaces

Also VLANs 40 and 50 at Router1.

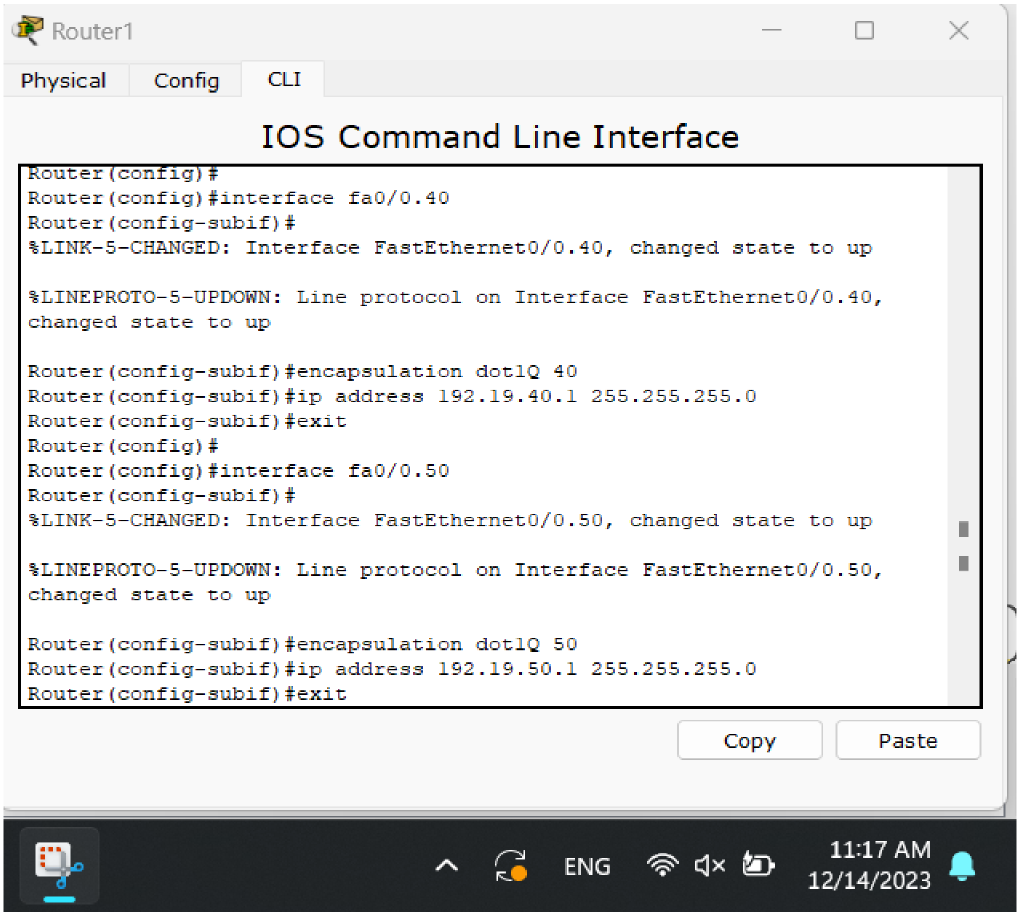

Figure 6: Configuration Router 1 Sub-Interfaces

2.2.2. Configuring OSPF Routing

Both Router0 and Router1 have been configured using the OSPF routing protocol. This involves specifying the process ID for OSPF, and then choosing the networks to be linked by entering the network ID, wildcard mask, and area number.

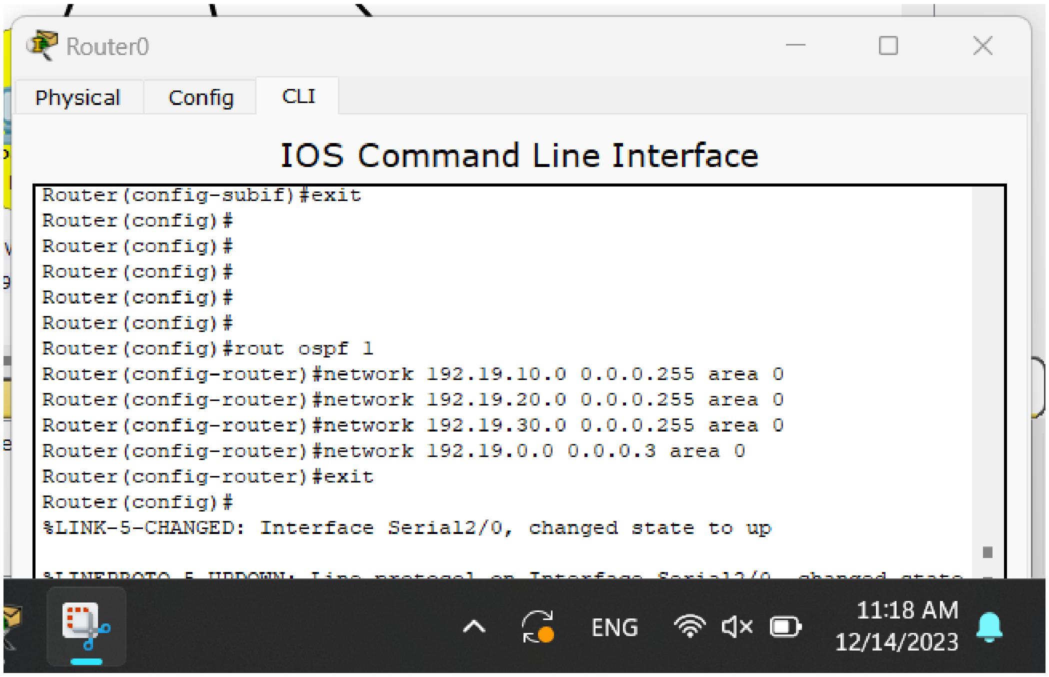

Figure 7: Configuring OSPF Routing for Router 0

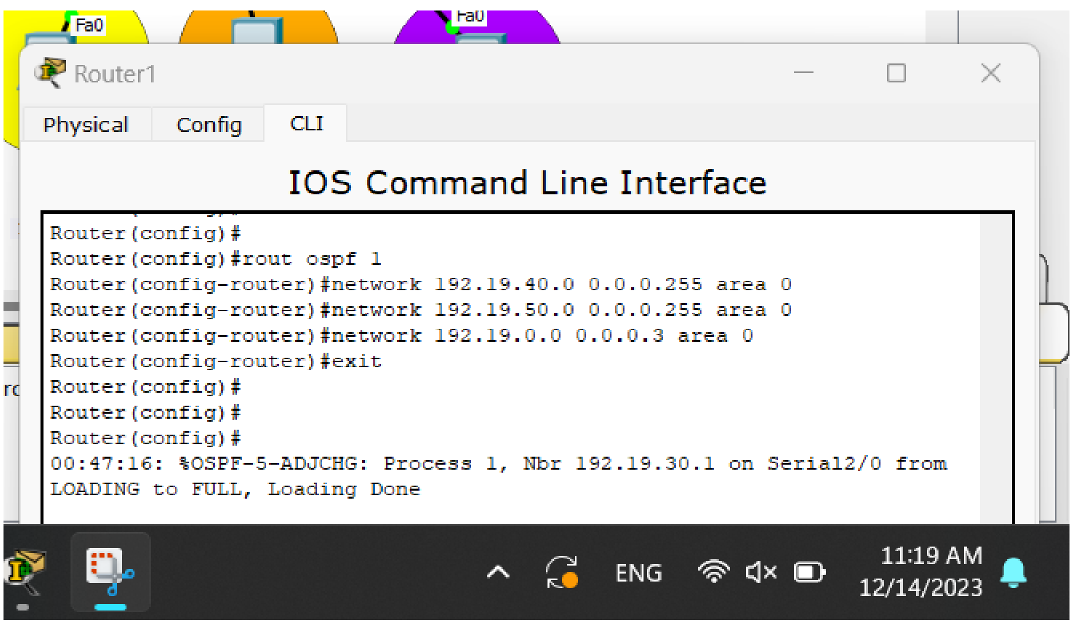

Figure 8: Configuring OSPF Routing for Router 1

2.3. Configuring Switches

Switches Configured as shown in Table 2 below.

Table 2: Switch Port

Switch	Port	Kind	VLAN
Switch 0	Fa0/1	Trunk	---
	Fa1/1	Trunk	---
	Fa2/1	Access	VLAN 10
	Fa3/1	Access	VLAN 20
Switch 1	Fa0/1	Trunk	---
	Fa1/1	Trunk	---
	Fa2/1	Access	VLAN 30
	Fa3/1	Access	VLAN 10
Switch 2	Fa0/1	Trunk	---
	Fa1/1	Trunk	---
	Fa2/1	Access	VLAN 40
	Fa3/1	Access	VLAN 50
	Fa6/1	Access	VLAN 20

2.3.1. Creating a VLAN

VLANs numbered from 10 to 50 have been established across the switches (Switch0, Switch1, and Switch2) to familiarize them with the specific VLAN setup within the topology. The configuration of these VLANs necessitates appropriate switch settings. The network encompasses five distinct VLANs, namely 10, 20, 30, 40, and 50. To avert connectivity issues among devices within the same VLAN but connected to different switches, it is imperative to define these VLANs on all switches.

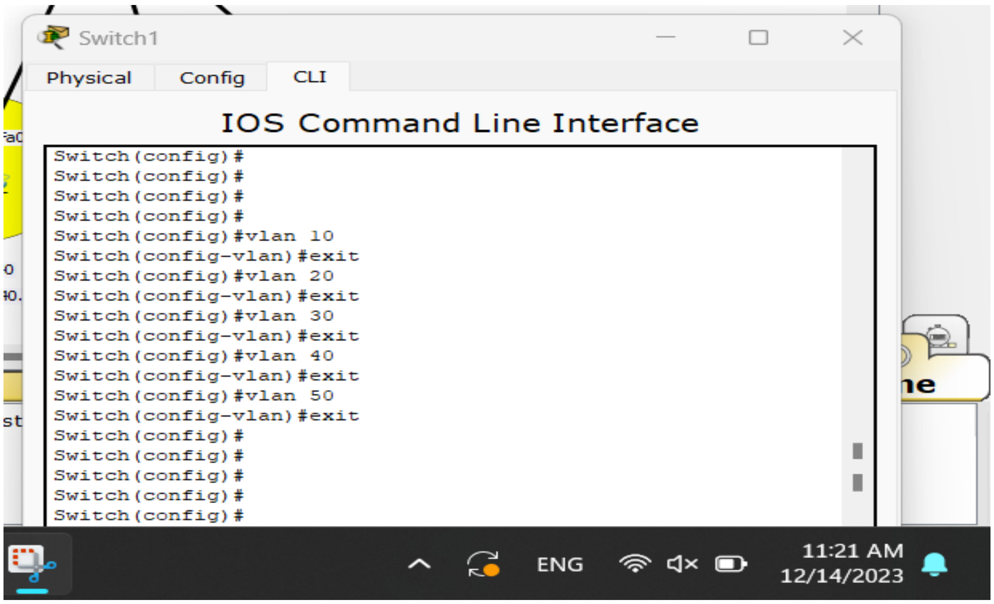

Figure 9: Creating vlans in switch1

For switch 1:

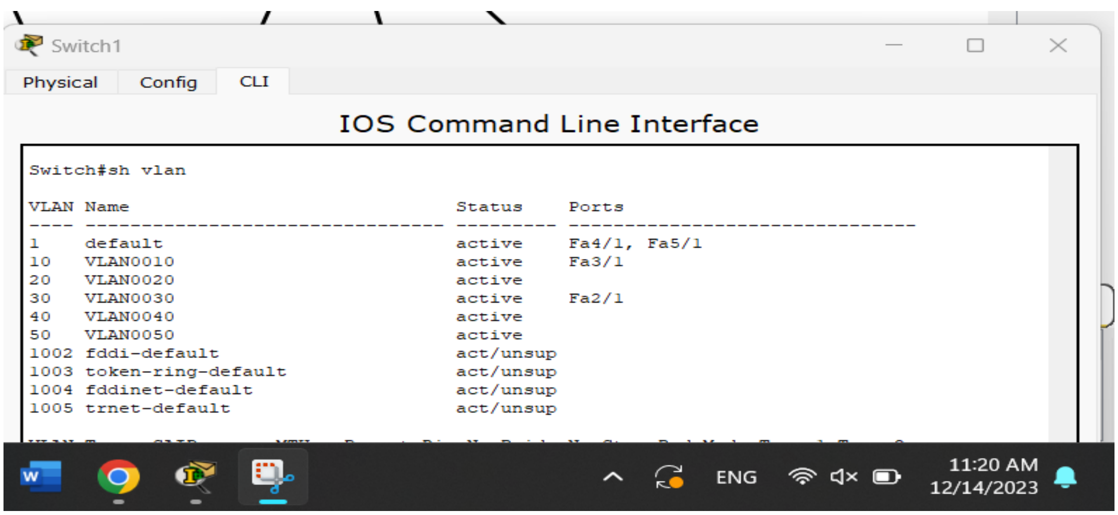

Figure 10: Switch 1 VLAN

We do the same thing with switch 0 and switch 2.

2.3.2. Configuring Switch Access

Assigning an interface to an existing VLAN we must access the needed port and perform the access command:

```
Switch(config-if)# switchport access VLAN <VLAN-NUMBER>
```

Figure 11: Configuring Switch0 Access

Figure 12: Configuring Switch1 Access

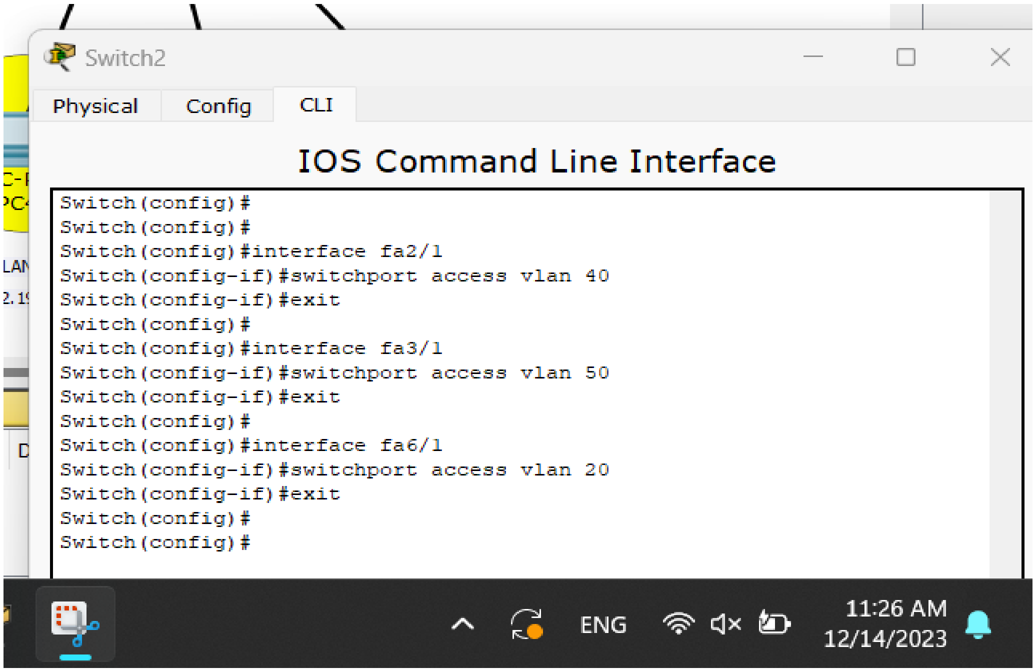

Figure 13: Configuring Switch2 Access

2.3.3. Configuring Switch Trunk

Assigning an interface to be a trunk is simple. We must access the needed port and perform the following command:

```
Switch(config -if)# switchport mode trunk
```

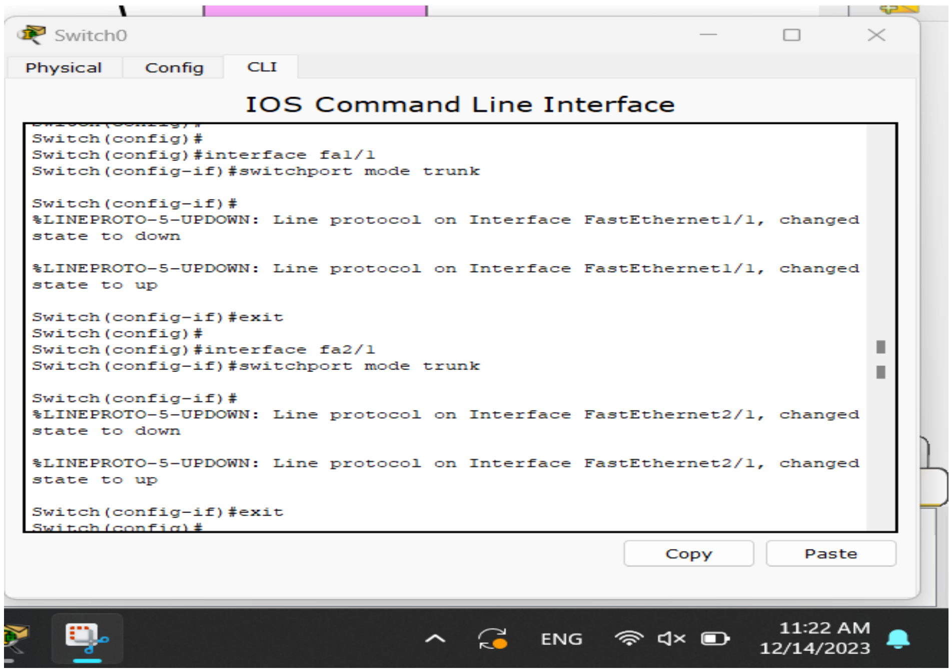

Figure 14: Configuring Switch0 Trunk

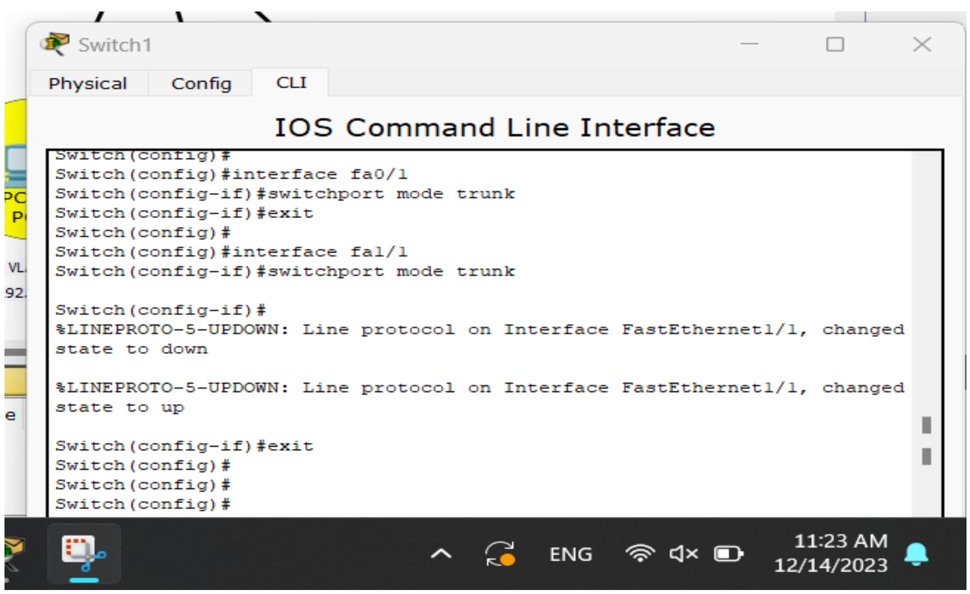

Figure 15: Configuring Switch1 Trunk

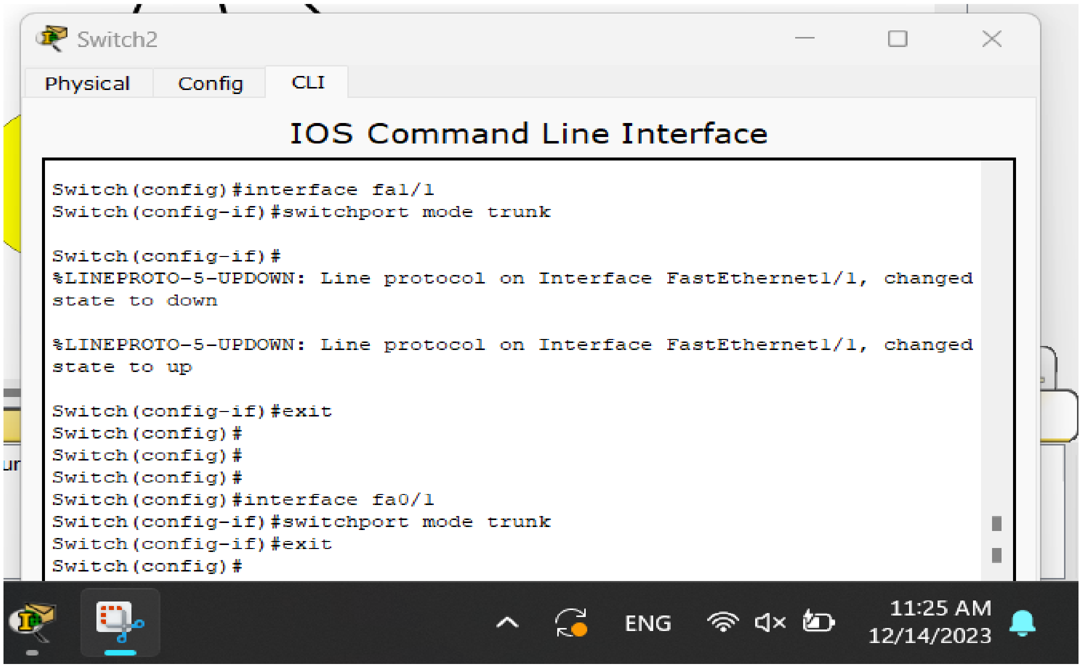

Figure 16: Configuring Switch2 Trunk

3.Results

3.1 Routing Tables

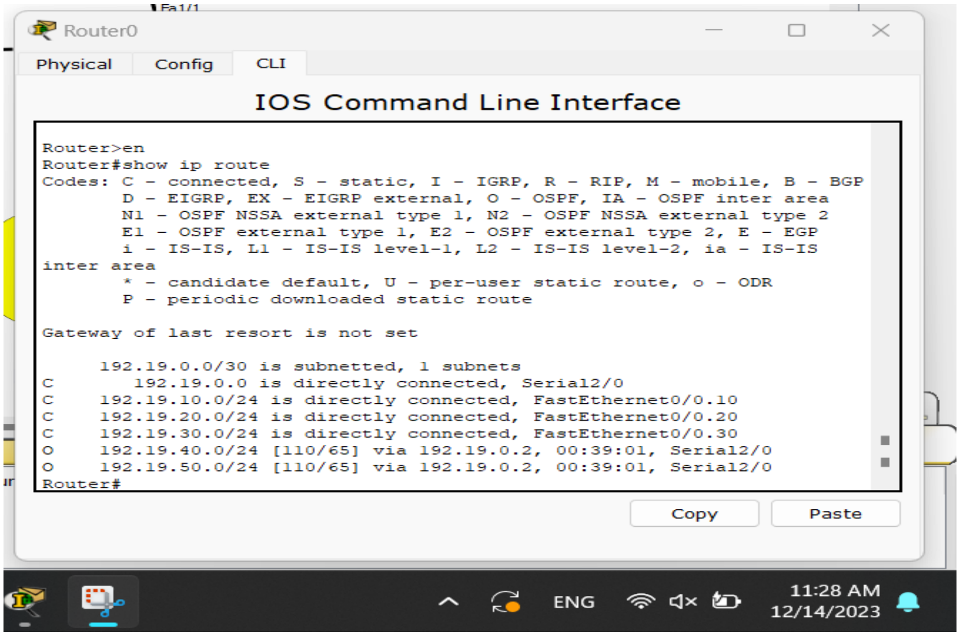

Figure 17: Routing Table for Router 0

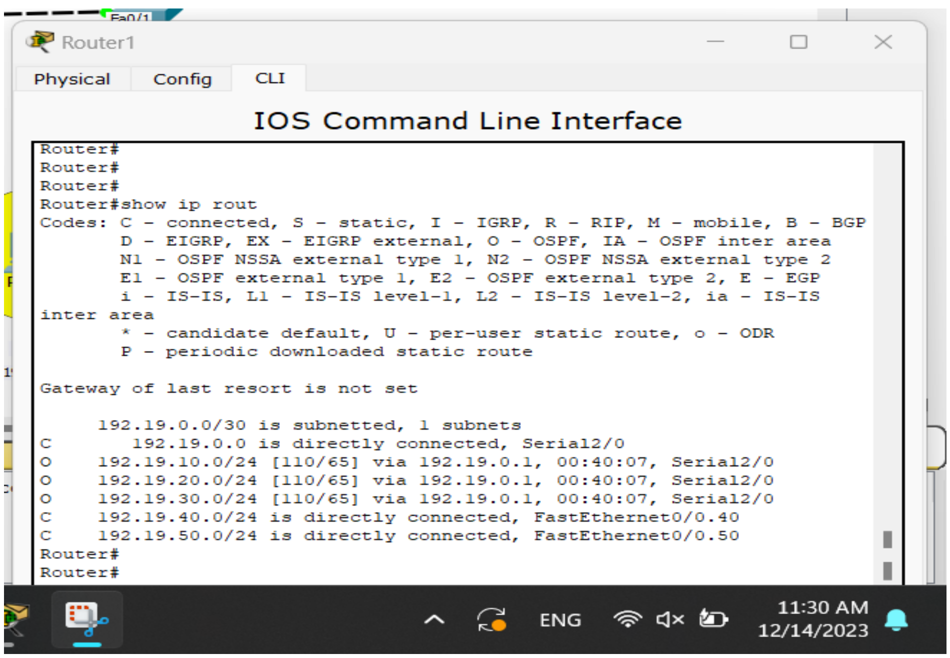

Figure 18: Routing Table for Router 1

'C' means that the router is directly connected to a network, 'O' means the use of the OSPF protocol for routing within the same AS.

3.2 Pings

Several methods were tested to confirm that all devices within the topology are interconnected and capable of communication and the routers can successfully establish connections and seamlessly transmit and receive packets, in this experiment I was used ping command.

Ping from PC5 to PC1:

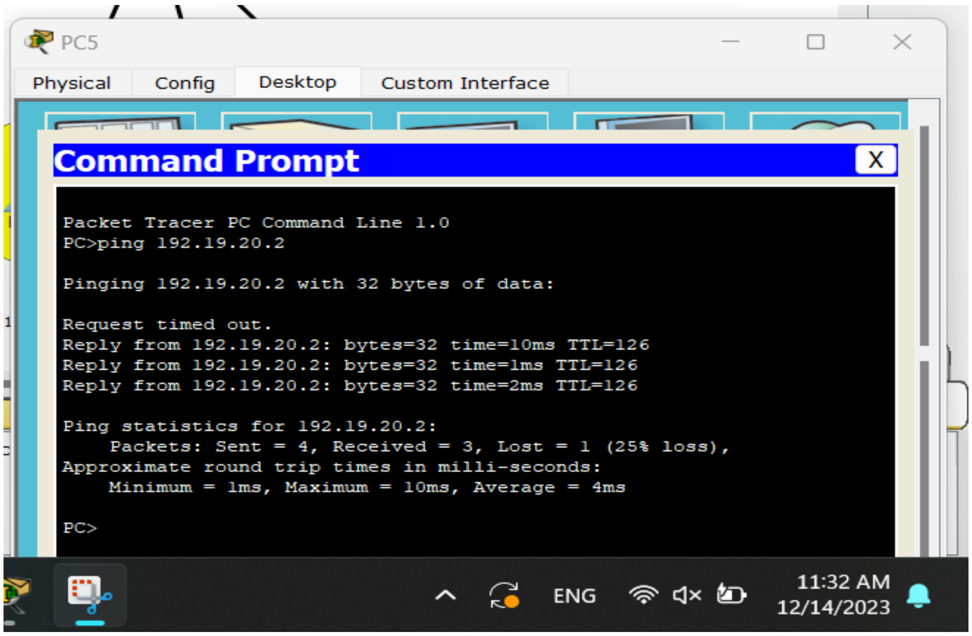

Figure 19: Ping from PC5 to PC1

Ping from PC4 to PC0:

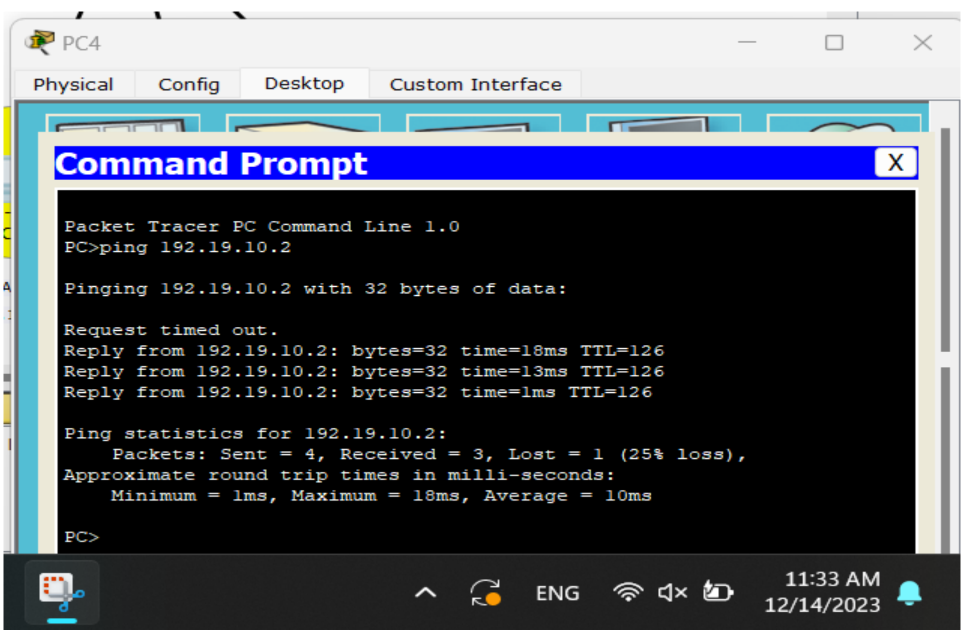

Figure 20: Ping from PC4 to PC0

Ping from PC3 to PC6:

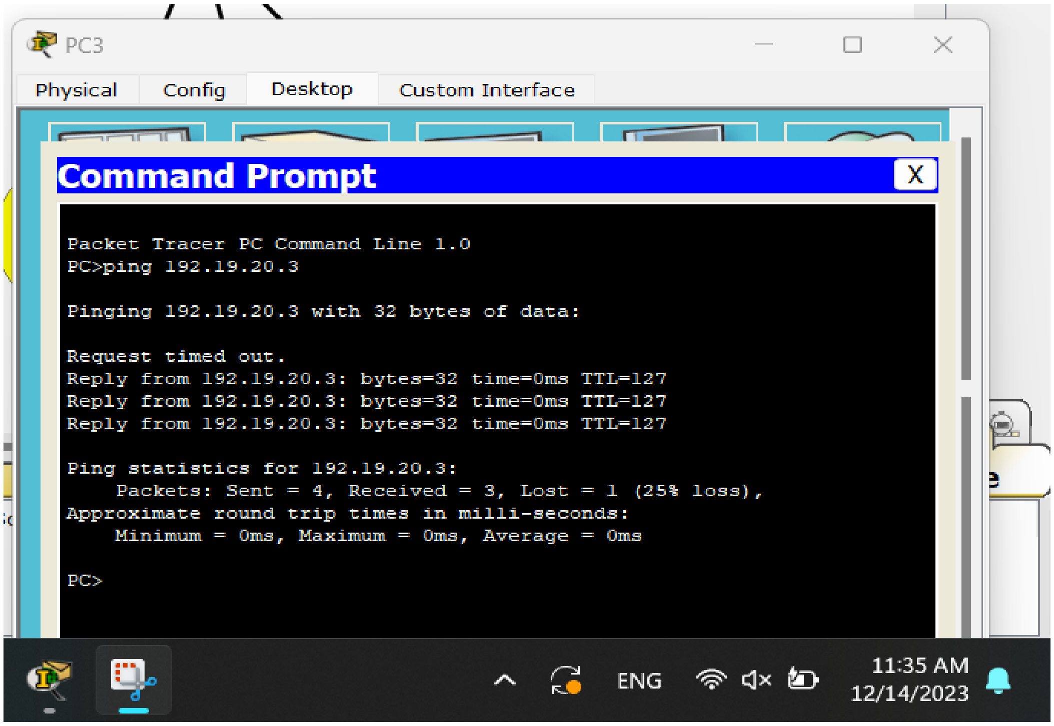

Figure 21: Ping from PC3 to PC6

Ping from PC2 to PC5:

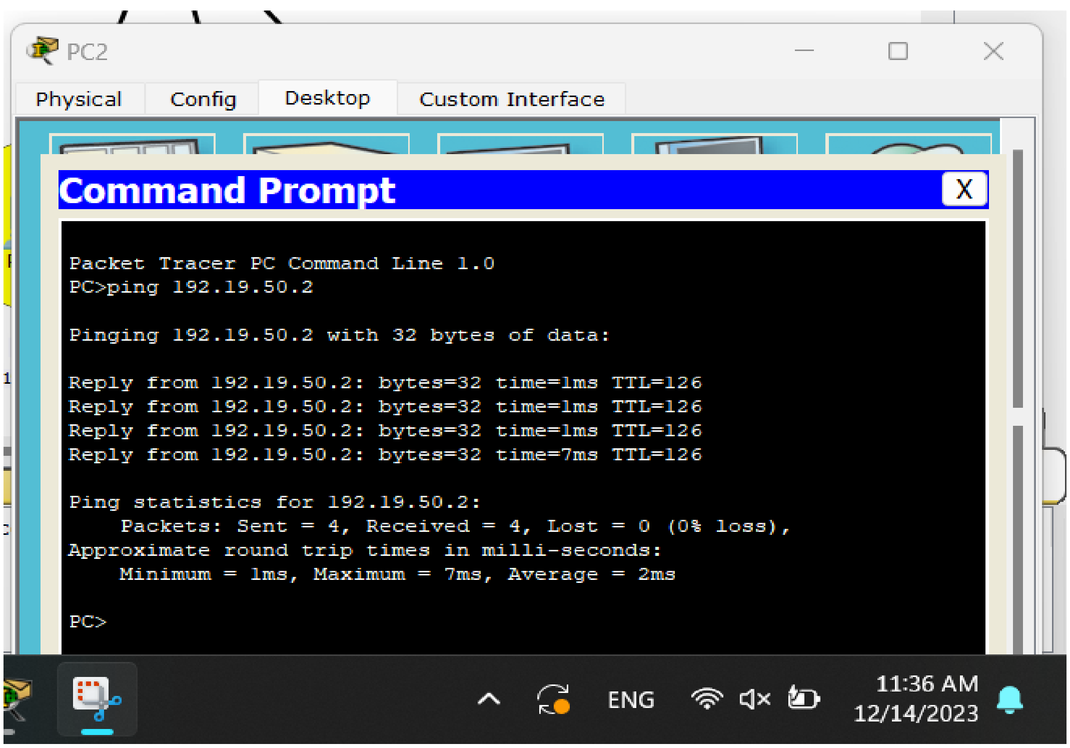

Figure 22: Ping from PC2 to PC5

4.Conclusion

In conclusion, after we finished this experiment we became able to configure a Cisco IOS Switch using the IOS command-line interface (CLI), and we learn how to use switch simulator, and how to split Cisco router interface into sub interfaces, also we learn how to split Cisco switches into multiple virtual ones and how to create VLANS.

5.References

[1]: https://www.spiceworks.com/tech/networking/articles/what-is-network-switch/

[Accessed 14 December 2023]

[2]: https://en.wikipedia.org/wiki/IEEE_802.1Q [Accessed 14 December 2023]

[3]: https://jumpcloud.com/blog/what-is-vlan-tagging [Accessed 14 December 2023]

[4]: https://www.arubanetworks.com/techdocs/AOS-CX/10.08/HTML/l2_bridging_4100i-6000-6100-6200/Content/Chp_vlans/vla-num.htm [Accessed 14 December 2023]

[5]: https://www.geeksforgeeks.org/difference-between-trunk-port-and-access-port/

[Accessed 14 December 2023]

[6]: https://www.omnisecu.com/cisco-certified-network-associate-ccna/what-is-a-subinterface-in-a-cisco-router.php [Accessed 14 December 2023]