



Faculty of Engineering & Technology

Electrical & Computer Engineering Department

COMPUTER NETWORKS LABORATORY ENCS4130

EXP.8 Switching and VLANs - Switch Virtual Interface

Prepared by: Maisam alaa

ID: 1200650

Instructor's Name: Dr. Ibrahim Nemer

Assistant's Name: Eng. Ahed Mafarjeh

Section: 1

Date: 1/9/2023

Abstract

The aim of the experiment is to learn how to configure a Cisco IOS Multi-layer Switch using the IOS command-line interface (CLI). Also learn how to use switch simulator and how to split Cisco Multi-layer Switch into multiple virtual ones and create VLANs and split Cisco router interface into sub interfaces.

We used two Cisco router, three PCs, four laptops, one server, two Cisco switches, one Cisco multi-layer switch 3560-24PS, several CAT5 straight-wired cable and one Serial cable (male and female).

Table of Contents

Abstract	I
Acronyms and Abbreviations	III
List of figures	IV
List of tables.....	IV
1.Introduction.....	1
1.1. How does a switch work?.....	1
1.2. IEEE 802.1Q VLAN	1
1.3. Sub interface on Routers	1
1.4. Third layer switch.....	2
1.5. Features of a layer 3 switch	2
1.6. Benefits of a layer 3 switch	2
1.7. Disadvantages of layer 3 switch	3
2.Procedure & Discussion.....	4
2.1. Building the topology	4
2.2. Configure the IPs for the PCs and Routers and multi-layer switch	4
2.3. switch Configuration	7
2.3.1. Multi-Layer Switch to Router link	7
2.3.2. Multi-Layer Switch Configuring VLAN Interfaces IPs (Switch Virtual Interfaces)	8
2.3.3. Enable routing on Multi-Layer Switch and configuring OSPF	9
2.3.4. Configuring VLANs on Multi-Layer Switch	11
2.3.5. Configuring Access Ports on Multi-Layer Switch	12
2.3.6. Configuring Trunk on Multi-Layer Switch	12
3.Results	14
4.Conclusion	19
5.References	20

Acronyms and Abbreviations

OSPF	Open Shortest Path First
AS	Autonomous systems
SVI	Switch Virtual Interface

List of figures

Figure 1 IEEE 802.1Q VLAN tagging	1
Figure 2 Multi-layer switch.....	2
Figure 3 multi-layer switch configuration	2
Figure 4 topology configuration	4
Figure 5 multi-layer switch to router configuration.....	7
Figure 6 multi-layer IP configuration on VLANs	8
Figure 7 multi-layer OSPF configuration	9
Figure 8 OSPF configuration on router 1.....	10
Figure 9 OSPF configuration on router 0.....	10
Figure 10 multi-layer VLAN configuration	11
Figure 11 multi-layer trunk configuration	13
Figure 12 pinging result from PC0 to laptop 1	14
Figure 13 pinging result from laptop 2 to laptop 3	15
Figure 14 pinging result from laptop 0 to server 0.....	16
Figure 15 http request result from laptop 1 to server 0	17
Figure 16 http request result from PC 2 to server 0.....	17
Figure 17 http request result from laptop 2 to server 0	18

List of tables

Table 1 IP's for routers, PC's and laptops 5

Table 2 IP's for routers and multi-layer switch 5

1.Introduction

1.1. How does a switch work?

A network switch connects devices in a network to each other, enabling them to talk by exchanging data packets. Switches can be hardware devices that manage physical networks or software-based virtual devices.

A network switch operates on the data-link layer, or Layer 2, of the Open Systems Interconnection (OSI) model. In a local area network (LAN) using Ethernet, a network switch determines where to send each incoming message frame by looking at the media access control (MAC) address. Switches maintain tables that match each MAC address to the port receiving the MAC address. [1]

1.2. IEEE 802.1Q VLAN

IEEE 802.1Q VLAN is a networking standard that enables the creation of virtual LANs within a physical network. It uses tagging to segregate network traffic, improving performance, security, and management. VLANs group devices into logical networks, and each VLAN is identified by a unique VLAN ID. Trunk ports interconnect switches and carry traffic for multiple VLANs, while access ports belong to a single VLAN. VLANs can enhance security, reduce broadcast traffic, and enable quality of service (QoS) policies. [2]

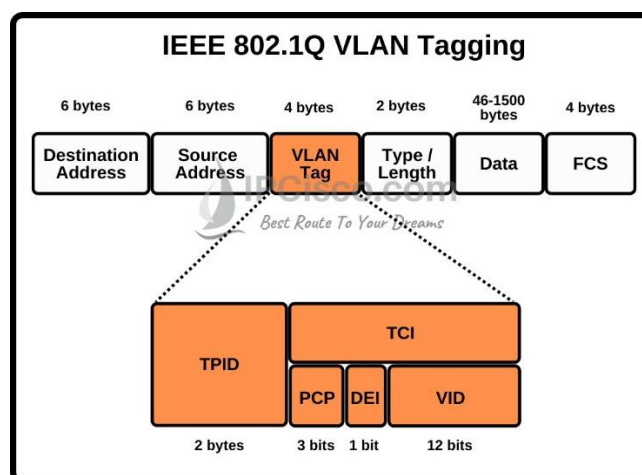


Figure 1 IEEE 802.1Q VLAN tagging

1.3. Sub interface on Routers

Subinterfaces on routers are virtual interfaces created on a single physical router interface to enable routing between multiple VLANs or subnets. They use 802.1Q VLAN tagging to differentiate traffic from different VLANs, and each subinterface has its own IP address, acting as the default gateway for devices in its VLAN. This setup is commonly used for inter-VLAN routing and enhances network security and management. [3]

1.4. Third layer switch

Also called a multilayer switch, it is a specialized hardware device that has a lot in common with the traditional router—both in physical appearance and function. Layer 3 switches support the same routing protocols as routers and inspect incoming packets, as well as make vital routing decisions the same way routers do. And they do these routing tasks in addition to performing switching duties. Like routers, Layer 3 switches can be configured to support such routing protocols as:

- Routing Information Protocol (RIP)
- Open Shortest Path First (OSPF)
- Enhanced Interior Gateway Routing Protocol (EIGRP) [4]

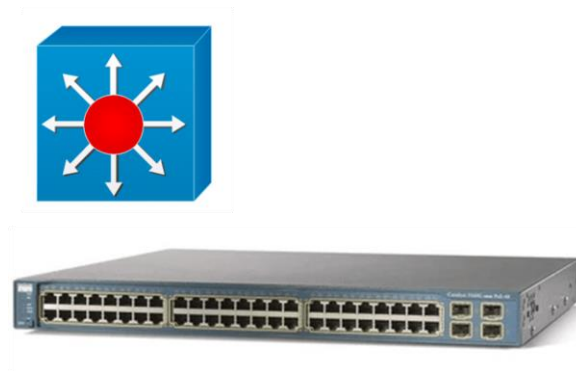


Figure 2 Multi-layer switch

1.5. Features of a layer 3 switch

These switches feature the following:

- Performance on two OSI layers: Layer 2 and Layer3
- Usually come in 24 or 48 Ethernet port models—however, without the WAN interface
- Connects devices within the same subnet
- Uses a simple switching algorithm
- Routing protocols are simple [4]



Figure 3 multi-layer switch configuration

1.6. Benefits of a layer 3 switch

These switches have many uses in an extensive, busy network. They:

- Support routing between VLANs
- Enhance fault isolation
- Streamline security management
- Reduce the volume of broadcast traffic
- Ease the configuration process for VLANs (Note: A separate router is not needed between each VLAN.)
- Separate routing tables, thus separating traffic better
- Support flow accounting and high-speed scalability
- Lower network latency because a packet does not have to make extra hops to go through a router. [4]

1.7. Disadvantages of layer 3 switch

When deciding whether to add a Layer 3 switch to a network, it is advisable to look at some of the device's downsides. Here are some things to consider before purchasing them:

- Cost: A Layer 3 switch costs significantly more than a traditional Layer 2 switch. In addition, configuring and managing Layer 3 switches is more complex—so money and extra resources should be earmarked to set up these switches.
- Limited application: Layer 3 switches are designed only for large enterprise networks with numerous device subnets and lots of traffic. Small to medium-sized organizations do not need a Layer 3 switch.
- No WAN capabilities: The Layer 3 switch's lack of WAN functionality means routers cannot be eliminated from the network. Both Layer 3 switches and traditional routers will be needed to route traffic within and outside the organization.
- Layer 3 switches are slower: Layer 3 switches are slower than Layer 2 switches, which can be a concern when spanning VLAN over multiple switches to support diverse tenants and visualization.
- Lack of flexibility: Because Layer 3 switches route at the access layer, each VLAN will be tied to one switch. This limitation requires careful planning to prevent one VLAN from using multiple switches. [4]

2.Procedure & Discussion

In this Lab we connected two routers and several PCs on different networks with switches, we also add a multi-layer switch to the topology and added VLANS which are VLAN 10, 20, 30, 40 and VLAN 50. We configured dynamic routing (OSPF) and access and trunk ports on the switches and the multi-layer switch.

2.1. Building the topology

We build the topology shown in Figure 1.

For the Third layer switch we used user multi-layer switch **3560-24PS**, for the PCs use PC-PT, for the connections between the PCs and multi-layer switch use Automatically use connection type.

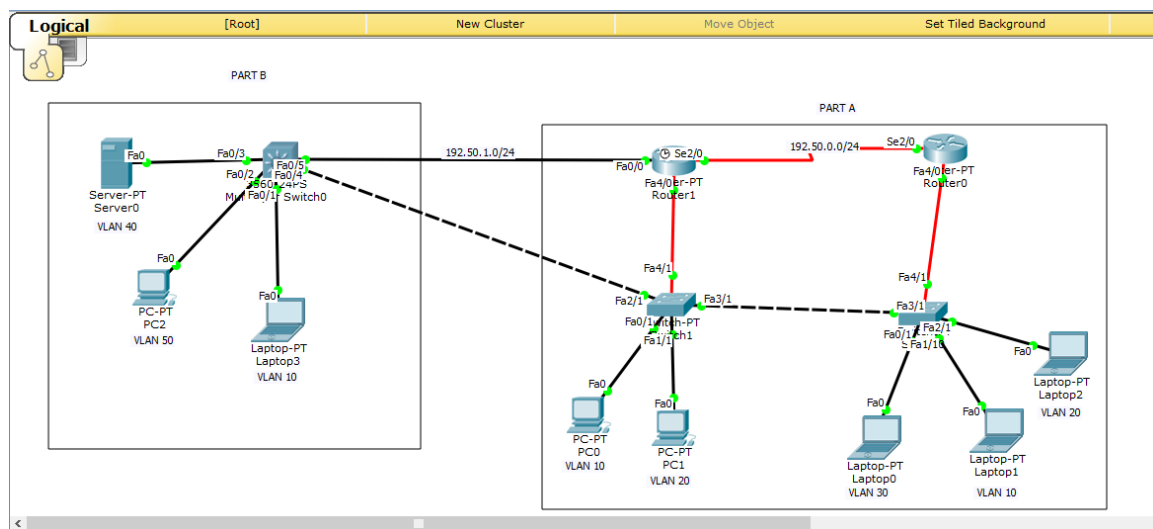


Figure 4 topology configuration

2.2. Configure the IPs for the PCs and Routers and multi-layer switch

We used the following IPs shown in Table 1 and Table 2 for the configuration. In order to configure the IPs for the PCs, Routers and Multi-layer switch.

Table 1 IP's for routers, PC's and laptops

192.50.0.0/24	Router 0	Se2/0	192.50.0.1	255.255.255.0	0.0.0.255	VLAN 1
192.50.0.0/24	Router 1	Se2/0	192.50.0.2	255.255.255.0	0.0.0.255	VLAN 1
192.X.10.0/24	Router 0	Fa0/0.10	192.X.10.1	255.255.255.0	0.0.0.255	VLAN 10
	Laptop 1	Fa0	192.X.10.2	255.255.255.0	0.0.0.255	VLAN 10
192.X.20.0/24	Router 0	Fa0/0.20	192.X.20.1	255.255.255.0	0.0.0.255	VLAN 20
	Laptop 2	Fa0	192.X.20.2	255.255.255.0	0.0.0.255	VLAN 20
192.X.30.0/24	Router 1	Fa0/0.30	192.X.30.1	255.255.255.0	0.0.0.255	VLAN 30
	PC0	Fa0	192.50.10.3	255.255.255.0	0.0.0.255	VLAN 10
	PC1	Fa0	192.50.20.3	255.255.255.0	0.0.0.255	VLAN 20
	Laptop 0	Fa0	192.X.30.2	255.255.255.0	0.0.0.255	VLAN 30

Table 2 IP's for routers and multi-layer switch

Area	Network	Device	Interface	IP	Subnet Mask	Wildcard Mask	VLAN Id
Area 0	192.X.1.0/24	Router 1	Fa0/0	192.X.1.1	255.255.255.0	0.0.0.255	VLAN 1
		MLS 0	Fa0/5	192.X.1.2	255.255.255.0	0.0.0.255	VLAN 1
	192.X.10.0/24	Laptop3	Fa0	192.X.10.5	255.255.255.0	0.0.0.255	VLAN 10
	192.X.40.0/24	Server0	Fa0	192.X.40.3	255.255.255.0	0.0.0.255	VLAN 40

	192.X.50.0/24	PC2	Fa0	192.X.50.3	255.255.255.0	0.0.0.255	VLAN 50
		PC8	Fa0	192.X.60.2	255.255.255.0	0.0.0.255	VLAN 60
	192.X.70.0/24	MLS 0	VLAN 70	192.X.70.1	255.255.255.0	0.0.0.255	VLAN 70
		PC7	Fa0	192.X.70.2	255.255.255.0	0.0.0.255	VLAN 70

2.3. switch Configuration

2.3.1. Multi-Layer Switch to Router link

We need to add an IP address to the switch port connected to the router, so firstly we need to change the switch port to a router port and then add an IP address, to do that we will use the following command:

```
Switch(config-if)#no switchport
Switch(config-if)#ip address <IP-ADDRESS> <SUBNET-MASK>
```

To add IP address 192.50.1.2/24 to port Fa0/5 on the multi-layer switch we use the commands below:

```
Switch(config)#interface fa0/5
Switch(config-if)#no switchport
Switch(config-if)#ip address 192.50.1.2 255.255.255.0
```



Figure 5 multi-layer switch to router configuration

2.3.2. Multi-Layer Switch Configuring VLAN Interfaces IPs (Switch Virtual Interfaces)

We used the following commands to configure switch virtual interfaces on the switch to act as default gateways for the new VLANs

```
Switch(config)#interface vlan <VLAN-NUMBER>  
Switch(config-if)# ip address <IP-ADDRESS> <SUBNET-MASK>
```

To configure an IP address for VLAN 40 with an IP of 192.50.40.1 use the following commands:

```
Switch(config)#interface vlan 40  
Switch(config-if)# ip address 192.50.40.1 255.255.255.0
```

To configure an IP address for VLAN 50 with an IP of 192.50.50.1 use the following commands:

```
Switch(config)#interface vlan 50  
Switch(config-if)# ip address 192.50.50.1 255.255.255.0
```

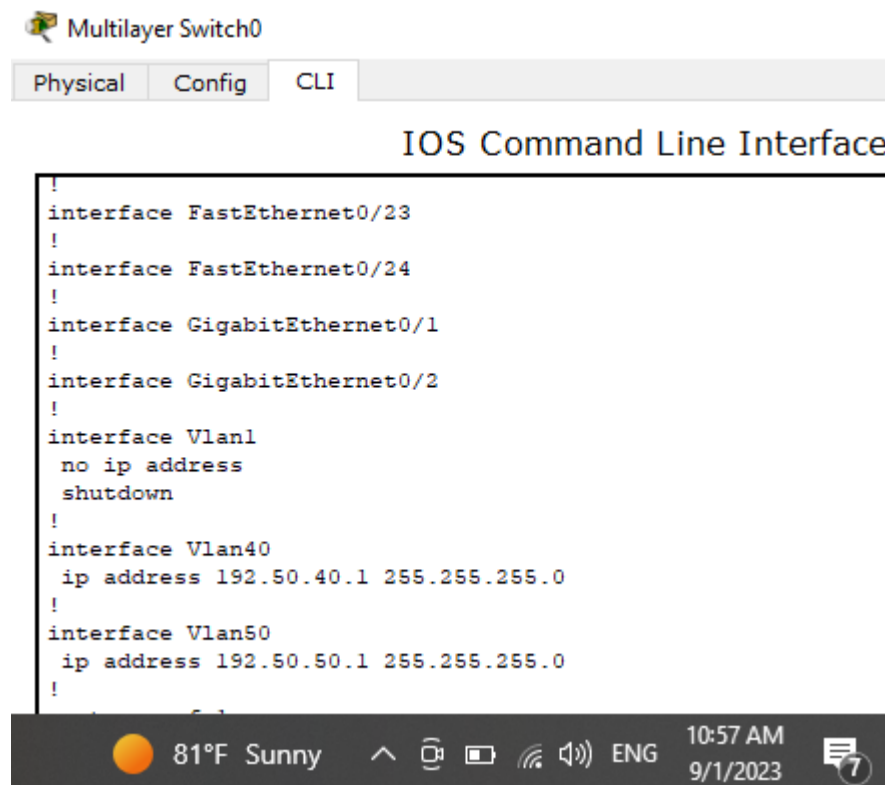


Figure 6 multi-layer IP configuration on VLANs

2.3.3. Enable routing on Multi-Layer Switch and configuring OSPF

We configured OSPF routing protocol for both routers & the Multi-layer switch. By default, the routing is disabled on the third layer switch, in order to enable it we used the following command:

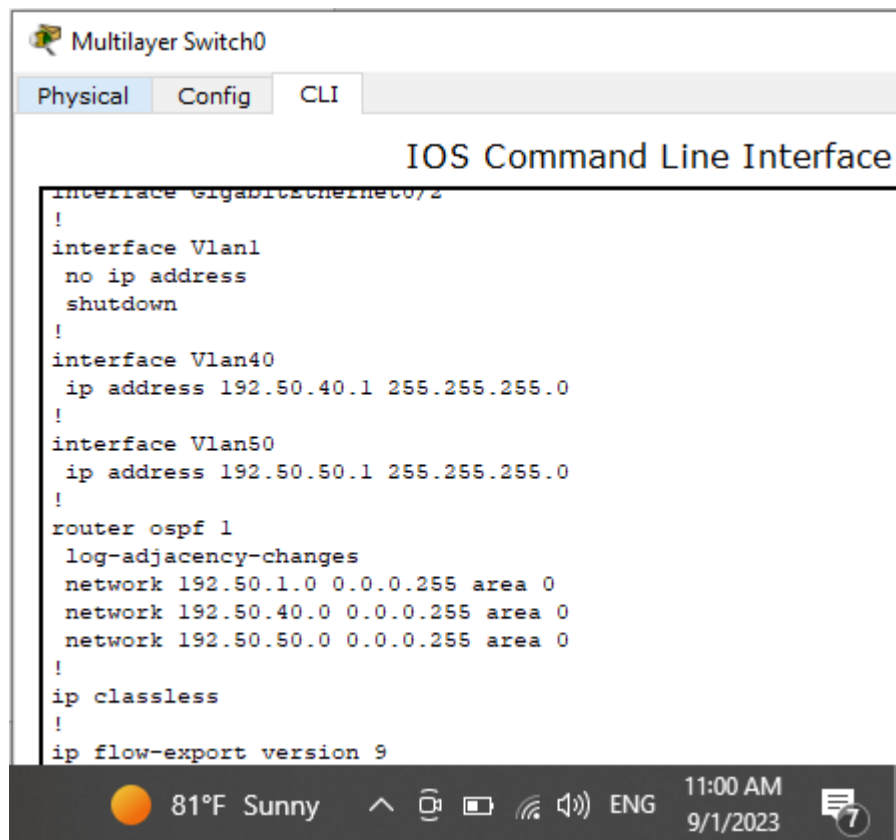
```
Switch(config)# ip routing
```

To enable OSPF routing on a router or a multi-layer switch the following command will be executed:

```
Router(config)# router ospf <PROCESS-ID>
```

```
Router(config-router)# network <ID-ADDRESS> <WILDCARD-MASK> area <AREA-ID>
```

OSPF routing configuration of multi-layer switch:

The image shows a screenshot of a network device's command-line interface (CLI) for a 'Multilayer Switch0'. The interface has tabs for 'Physical', 'Config', and 'CLI', with 'CLI' being the active tab. The title 'IOS Command Line Interface' is displayed at the top of the CLI window. The configuration text is as follows:

```
interface GigabitEthernet0/2
!
interface Vlan1
  no ip address
  shutdown
!
interface Vlan40
  ip address 192.50.40.1 255.255.255.0
!
interface Vlan50
  ip address 192.50.50.1 255.255.255.0
!
router ospf 1
  log-adjacency-changes
  network 192.50.1.0 0.0.0.255 area 0
  network 192.50.40.0 0.0.0.255 area 0
  network 192.50.50.0 0.0.0.255 area 0
!
ip classless
!
ip flow-export version 9
```

The bottom of the screen shows a status bar with a weather icon (81°F Sunny), system icons (up arrow, Wi-Fi, battery, speaker), language (ENG), time (11:00 AM), date (9/1/2023), and a notification icon with the number 7.

Figure 7 multi-layer OSPF configuration

OSPF routing configuration of router 1:

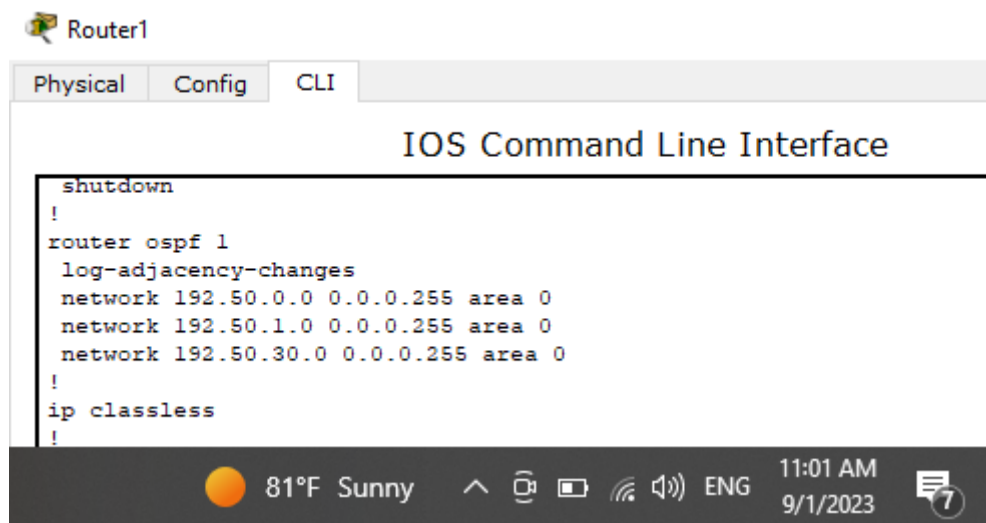


Figure 8 OSPF configuration on router 1

OSPF routing configuration of router 0:

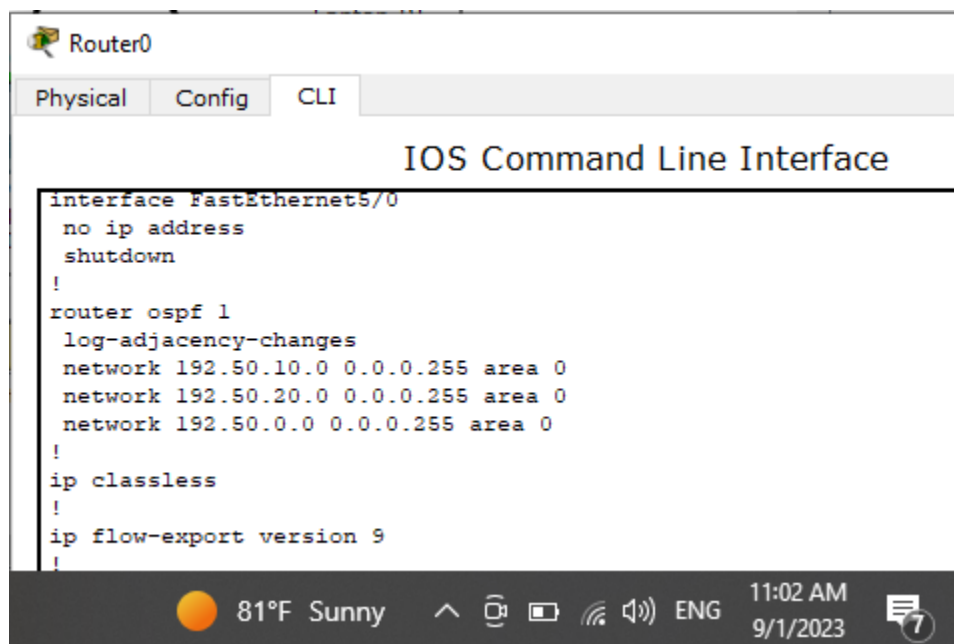


Figure 9 OSPF configuration on router 0

2.3.4. Configuring VLANs on Multi-Layer Switch

Configuring VLANs on a multi-layer switch is the same as configuring them on a normal switch, we can create a specific VLAN on a switch using the following command:

```
Switch(config)# VLAN <VLAN-NUMBER>
```

To initialize VLAN 40 of multi-layer switch we used:

```
Switch(config)# VLAN 40  
Switch(config-vlan)# exit
```

To initialize VLAN 50 of multi-layer switch we used:

```
Switch(config)# VLAN 50  
Switch(config-vlan)# exit
```

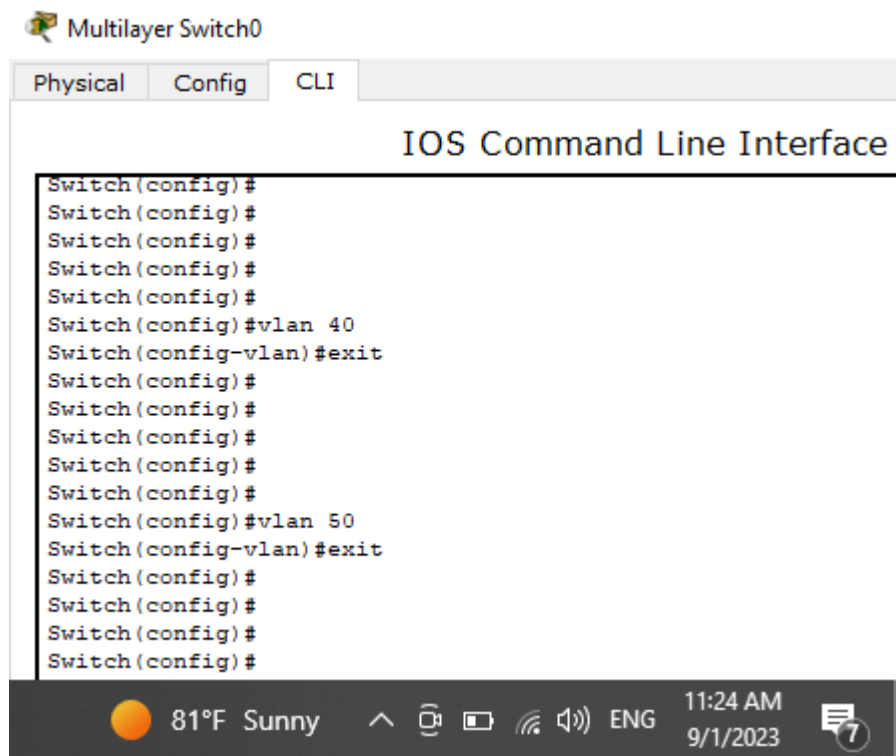


Figure 10 multi-layer VLAN configuration

2.3.5. Configuring Access Ports on Multi-Layer Switch

Configuring access ports on a multi-layer switch is the same as configuring them on a normal switch. 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>
```

To Assign port Fa0/3 on multi-layer switch to VLAN 40 we use the following commands.

```
Switch(config)# interface Fa0/3  
Switch(config-if)# switchport access VLAN 40
```

To Assign port Fa0/2 on multi-layer switch to VLAN 50 we use the following commands.

```
Switch(config)# interface Fa0/2  
Switch(config-if)# switchport access VLAN 50
```

2.3.6. Configuring Trunk on Multi-Layer Switch

To configure a trunk on a third layer switch, we need to encapsulate that switch, to do this we used the following commands:

```
Switch(config)#interface <interface-num>  
Switch(config-if)#switchport trunk encapsulation dot1q  
Switch(config-if)#switchport mode trunk
```

To Assign port Fa0/4 on multi-layer switch to be a trunk we use the following commands.

```
Switch(config)#interface Fa0/4  
Switch(config-if)#switchport trunk encapsulation dot1q  
Switch(config-if)#switchport mode trunk
```

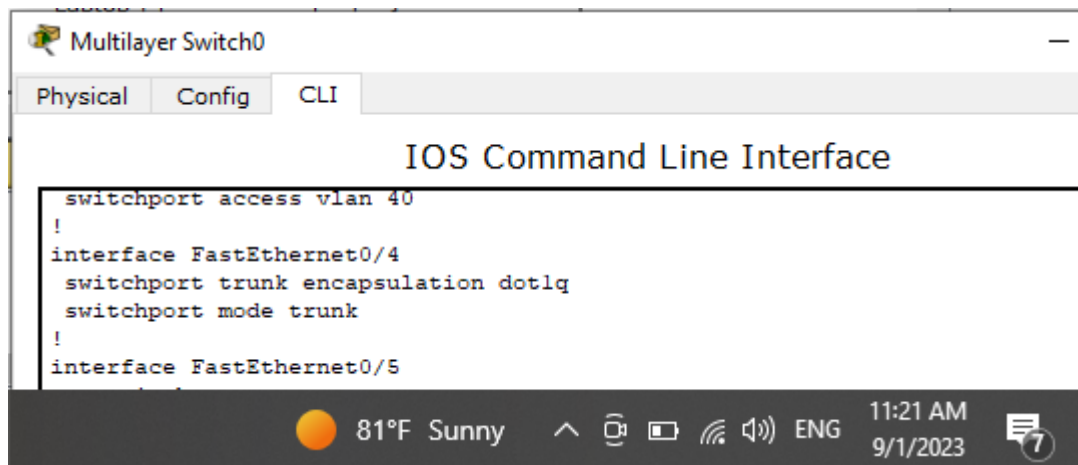
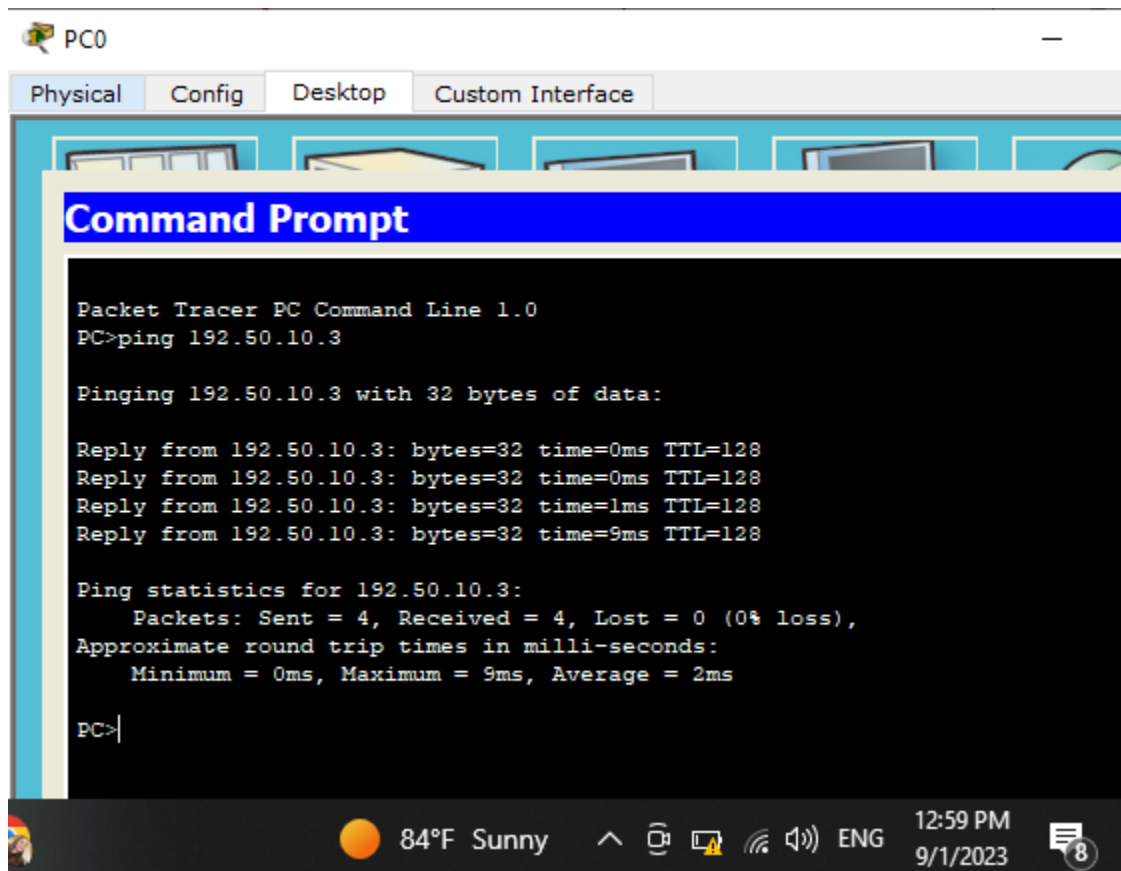


Figure 11 multi-layer trunk configuration

3.Results

Figure 12 shows the output of pinging from PC0 to Laptop 1 with ip 192.50.10.3/24 on the same VLAN (10). All messages were sent correctly with no loss or time out which means the VLAN configuration is correctly entered.



```
PC0
Physical Config Desktop Custom Interface
Command Prompt
Packet Tracer PC Command Line 1.0
PC>ping 192.50.10.3

Pinging 192.50.10.3 with 32 bytes of data:

Reply from 192.50.10.3: bytes=32 time=0ms TTL=128
Reply from 192.50.10.3: bytes=32 time=0ms TTL=128
Reply from 192.50.10.3: bytes=32 time=1ms TTL=128
Reply from 192.50.10.3: bytes=32 time=9ms TTL=128

Ping statistics for 192.50.10.3:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 9ms, Average = 2ms

PC>
```

Figure 12 pinging result from PC0 to laptop 1

Figure 13 shows the output of pinging from Laptop 2 with ip 192.50.20.3/24 on VLAN 20 to Laptop 3 with ip 192.50.10.5/24 on VLAN 10. All messages were sent correctly with no loss or time out which means the VLAN configuration is correctly entered.

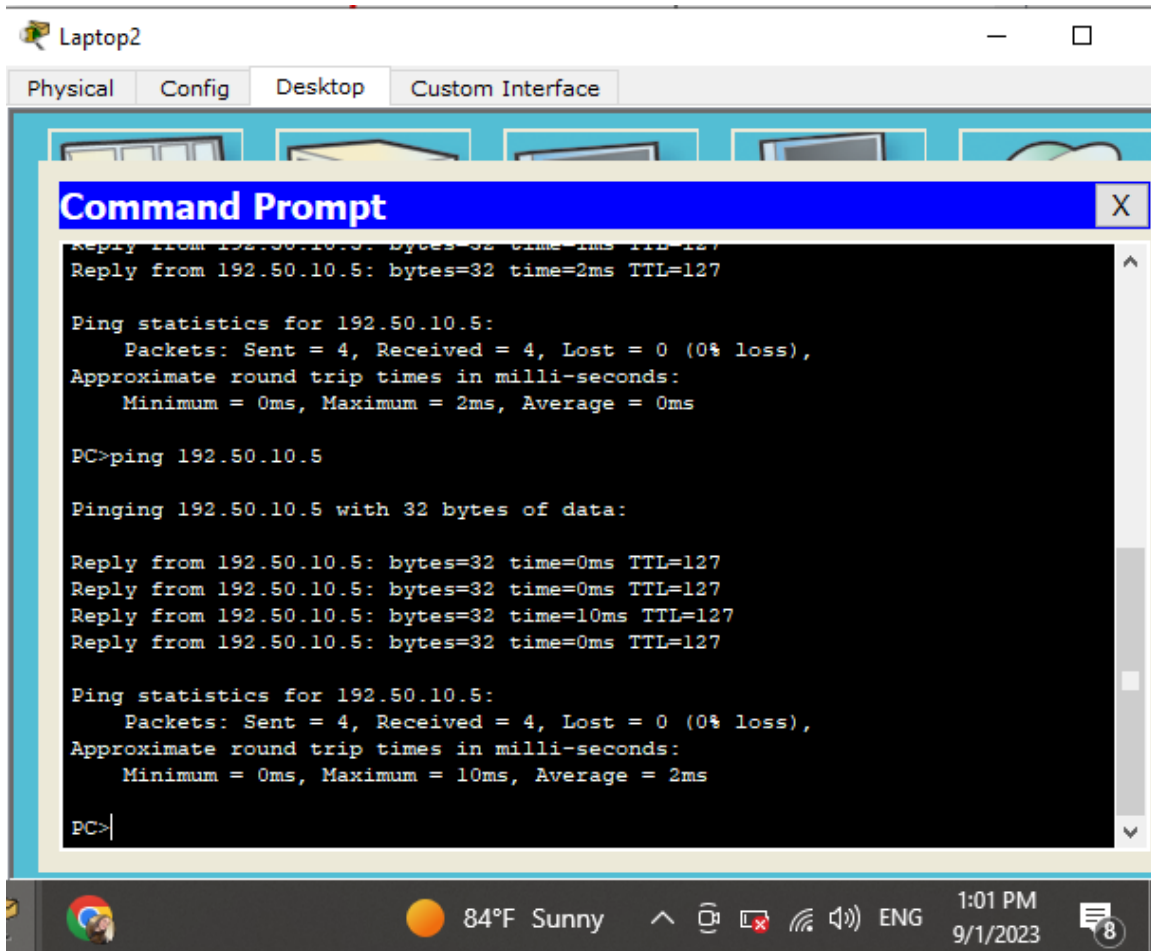


Figure 13 pinging result from laptop 2 to laptop 3

Figure 14 shows the output of pinging from Laptop 0 with ip 192.50.30.3/24 on VLAN 30 to Server 0 with ip 192.50.40.3/24 on VLAN 40. All messages were sent correctly with no loss or time out which means the VLAN configuration is correctly entered.

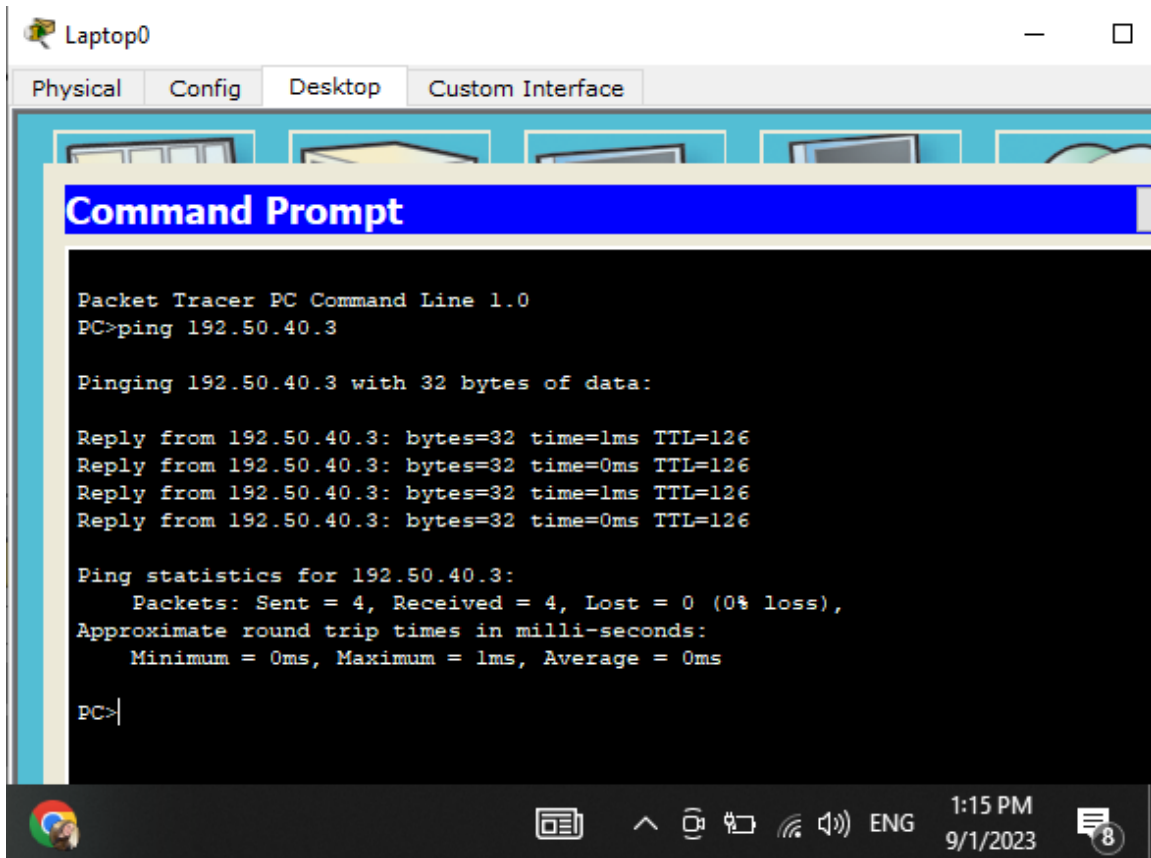


Figure 14 pinging result from laptop 0 to server 0

Task: only allow devices with VLAN 10 and 50 making http request on the server and deny all other http request.

In figures 15 & 16 shows the http request from laptop 1 in VLAN 10, and from pc2 in VLAN 50 to the server, the request is acceptable, which means the access list is correct.

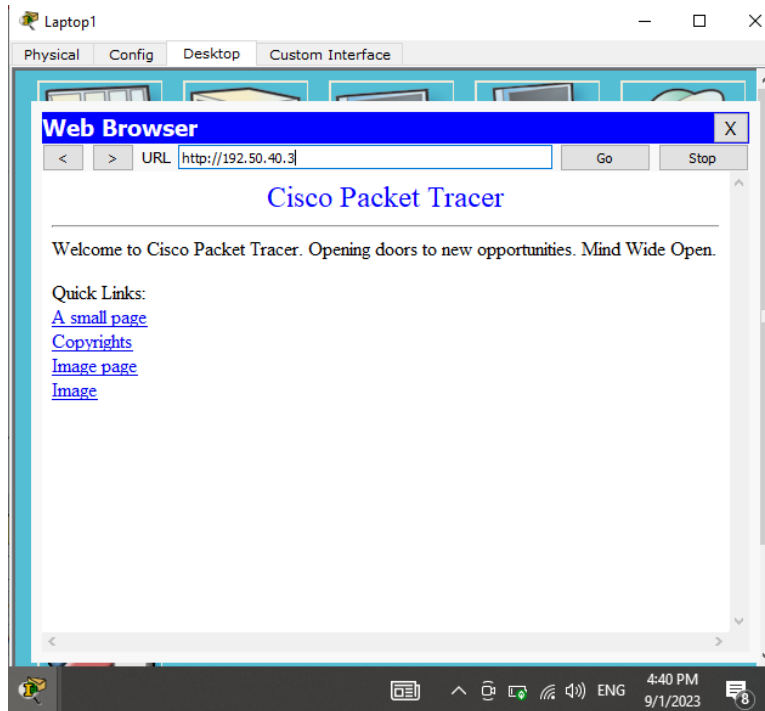


Figure 15 http request result from laptop 1 to server 0

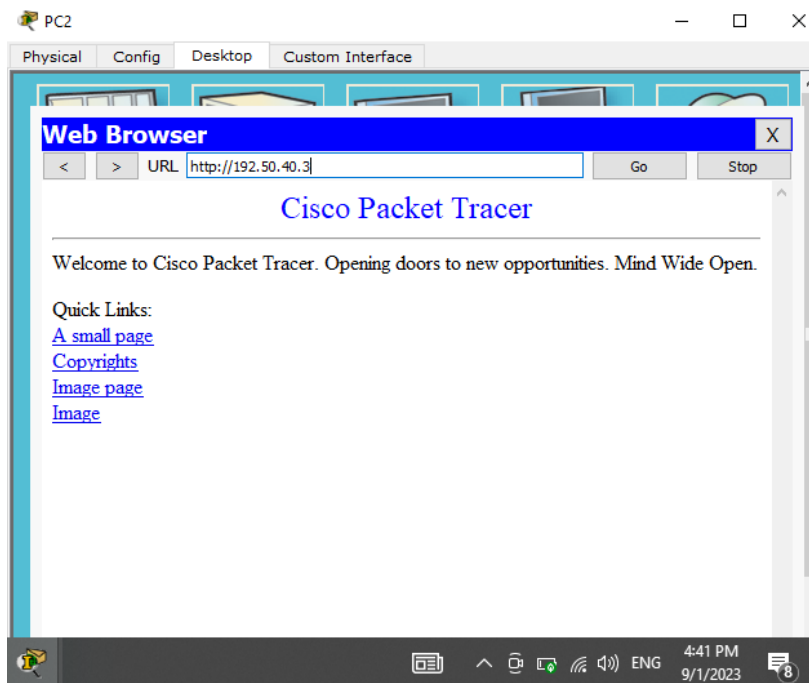


Figure 16 http request result from PC 2 to server 0

In figure 17 shows the http request from laptop 2 in VLAN 20, request is not acceptable, which means the access list is correct.

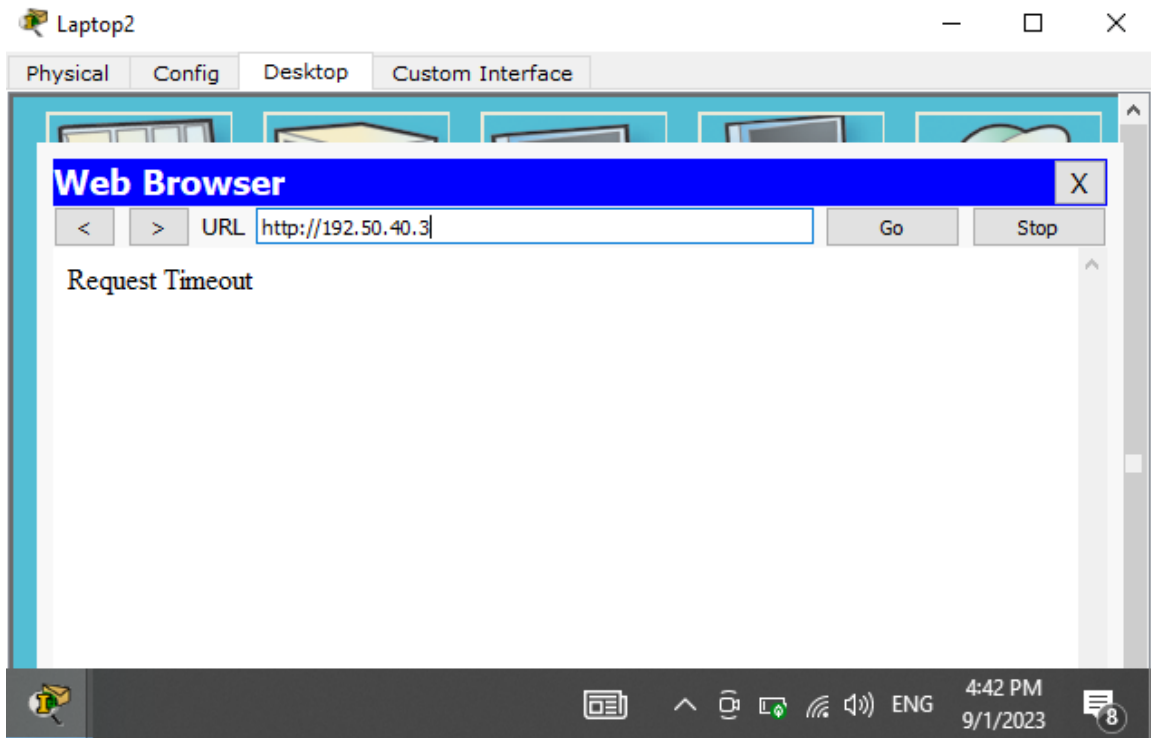


Figure 17 http request result from laptop 2 to server 0

4. Conclusion

In conclusion, this experiment has provided an exploration of Switched Virtual Interfaces (SVIs) and the role of switching, particularly in the context of multi-layer switches. These devices combine the functionalities of traditional layer 2 switches with the routing capabilities of layer 3 routers, resulting in more efficient and responsive networks. The integration of SVIs into multi-layer switches allows for seamless communication between VLANs and provides a robust framework for managing traffic and optimizing network performance. It also come with a range of features, advantages, and disadvantages that network administrators must consider when designing and managing their network infrastructure.

5.References

[1] [https://www.techtarget.com/searchnetworking/definition/switch#:~:text=A%20network%20switch%20connects%20devices,Systems%20Interconnection%20\(OSI\)%20model.](https://www.techtarget.com/searchnetworking/definition/switch#:~:text=A%20network%20switch%20connects%20devices,Systems%20Interconnection%20(OSI)%20model.)

[2] <https://chat.openai.com/>

[3] https://www.arubanetworks.com/techdocs/AOS-CX/10.08/HTML/fundamentals_83xx/Content/Chp_sub_int_cfg/cfg-subint.htm#:~:text=A%20subinterface%20is%20a%20virtual,for%20sending%20and%20receiving%20data.

[4] <https://planetechusa.com/what-is-a-layer-3-switch/>