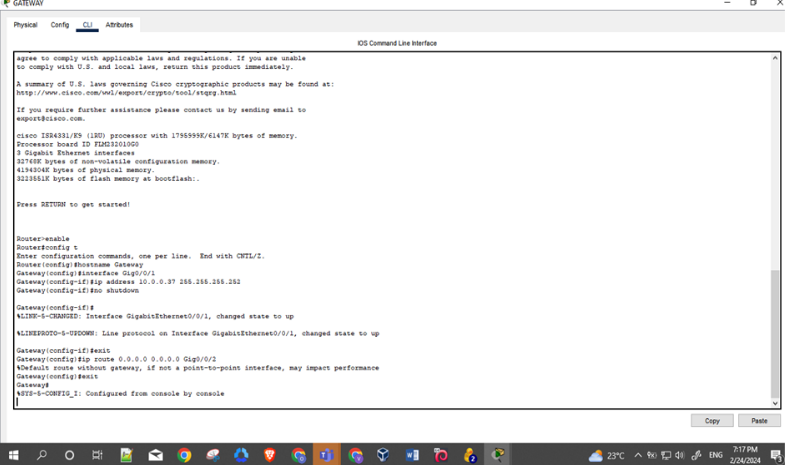
## **Instructions:**

* Answer **ALL** questions
* The exam should **NOT** be worked on in groups or with assistance from others.
* Submit your **write-up/report** as you have been doing in weekly assignments.
* Use this file as your **write-up reporting** template as you complete each task outlined and answer the questions.
* **Rename this file (.docx) and your packet tracer file (.pka)** with your **full names**.
* You **MUST have your camera on** throughout the session.
* Once you have completed your work, save the file and upload it together with your final Packet Tracer file (.pka) for marking.
* Before leaving the exam, **ensure you have uploaded the two correct files** capturing all the work you have submitted for marking.
* Use this document to compile a detailed write-up that outlines your approach to addressing the various exam challenges. Ensure that your write up is authentic. **Show screenshots of the working for all answers showing how you got your answers.**
* **Any answers without supporting screenshots will not be graded.**
* The screenshots should capture your full screen and display the command you ran to get the answer. Include a taskbar showing your machine taskbar and time stamp. Here’s a sample.



**Introduction**

This lab exercise allowed me to apply critical security configurations to a Cisco network, focusing on Layers 1-3 of the OSI model. My goal was to enhance the security of the switch and router configurations, implementing best practices such as switch port security, DHCP snooping, and IOS device password management.

Through this exercise, I aimed to reinforce the network's defences against common threats, ensuring robust protection for our cloud and on-premises environments.

**Background**

**This lab aims to provide a hands-on test on ensuring security for Layers 1 – 3 in reference to the OSI model. It is important to note that the lab will not be a comprehensive spectrum of the security measures to be taken when securing the aforementioned layers but rather focus on configuring the following; switch port security, DHCP snooping, Dynamic Arp Inspection (DAI), ACLs, and IOS Device passwords.**

**Total Marks = 50 marks**

**NOTE 1: Save the packet tracer file as your first name and last name e.g Jane Doe.pka**

**NOTE 2: The activity begins with 17% completion. This is intended. Proceed with the rest of the instructions**

**Lab Topology:**

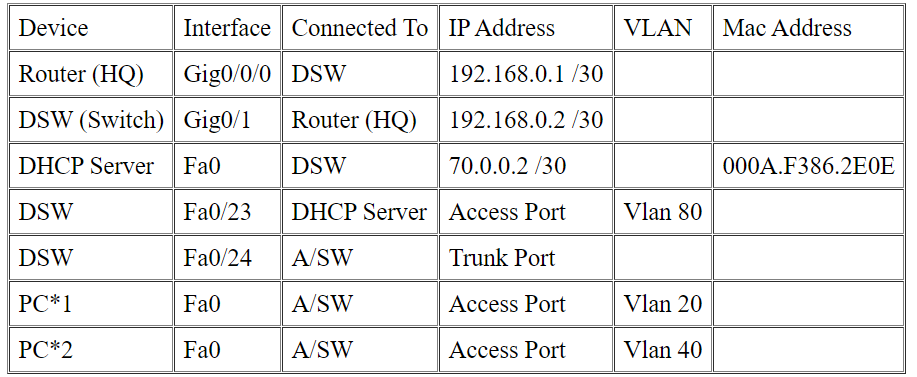
**1 Router: Cisco 4331**

**1 Switch: 3560 24PS**

**1 Server**

**1 Switch: Cisco 2960**

**2 PCs**

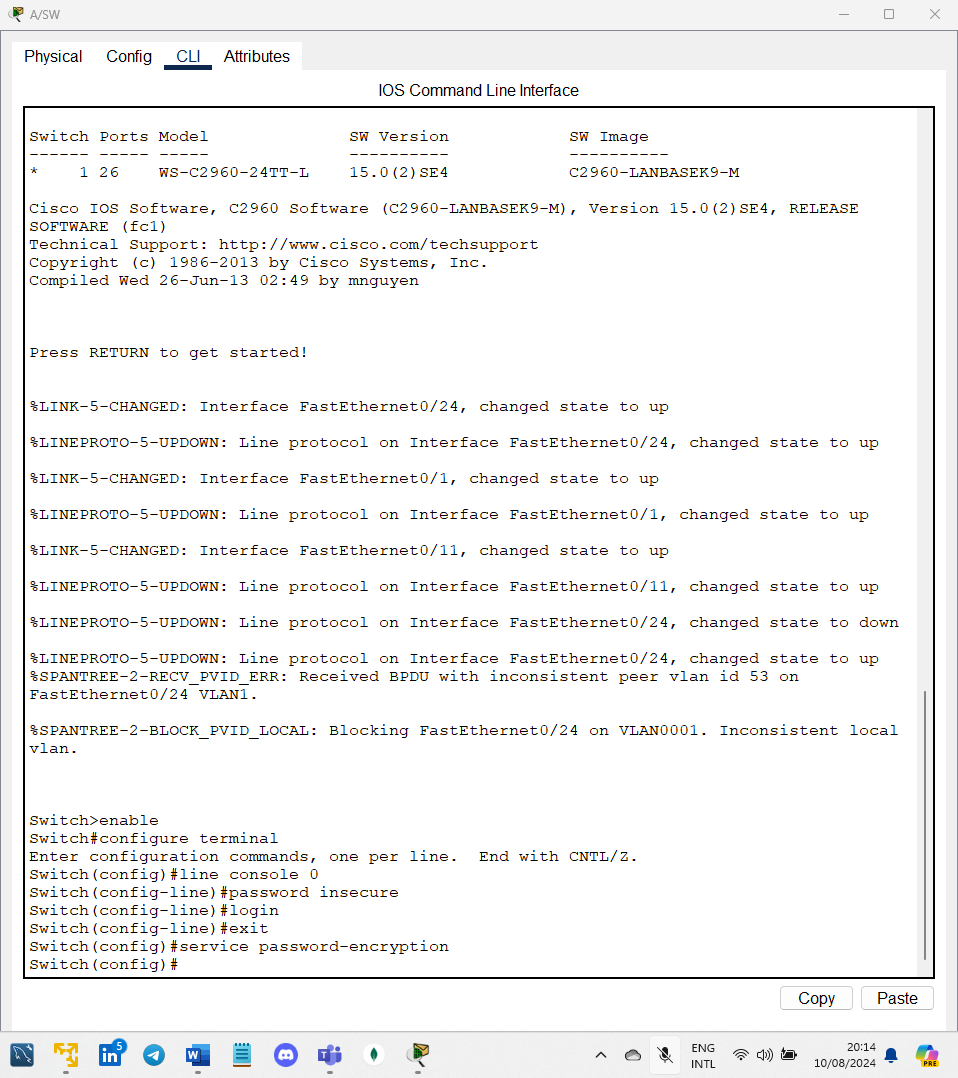
****

**Instructions:**

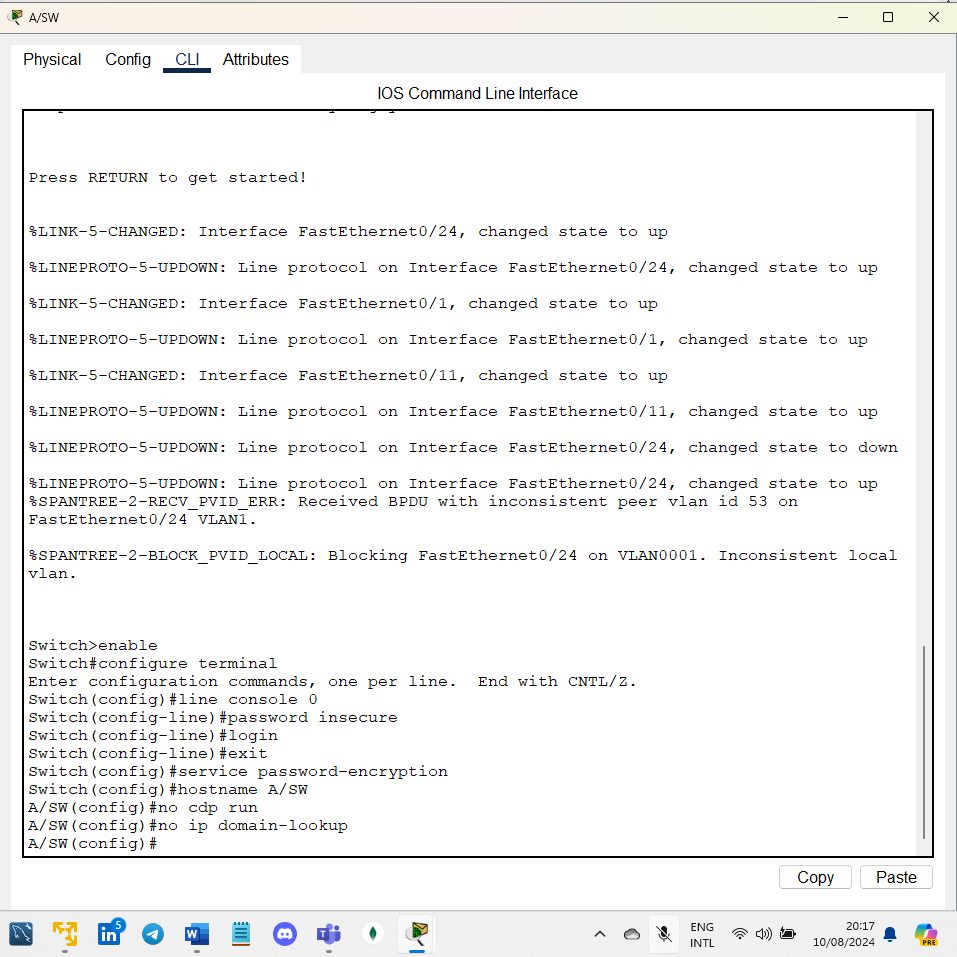
**SECTION 1: Configure Switch A/SW:**

1. Configure a password of "insecure" for line console and ensure that this password is required before accessing the USER mode of the switch. (1mk)
2. Use the following command to encrypt the set password;

* service password-encryption. (1mk)

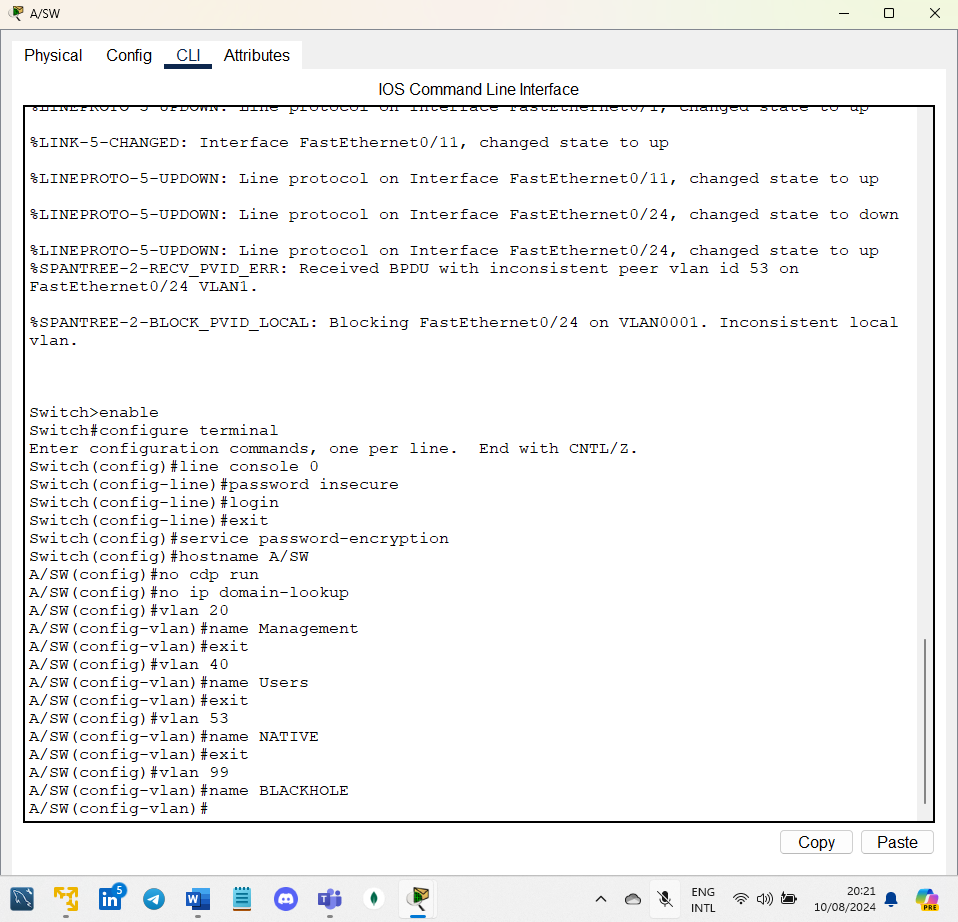
**

1. Rename the switch as A/SW (1mk)
2. Disable CDP (1mk)
3. Disable IP domain lookup (1mk)



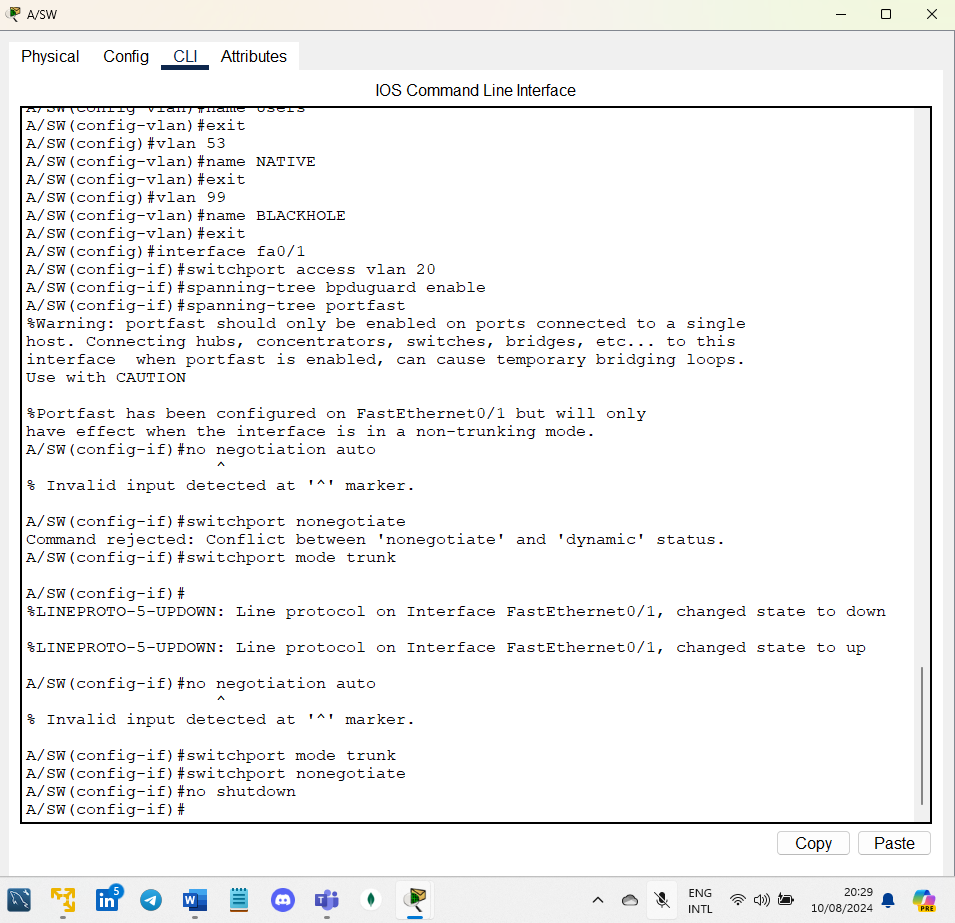
1. Create the following VLANs: (4mks)

* Vlan 20 and name it as “Management”
* Vlan 40 and name it as “Users”
* Vlan 53 and name it as “NATIVE”
* Vlan 99 and name it as “BLACKHOLE”



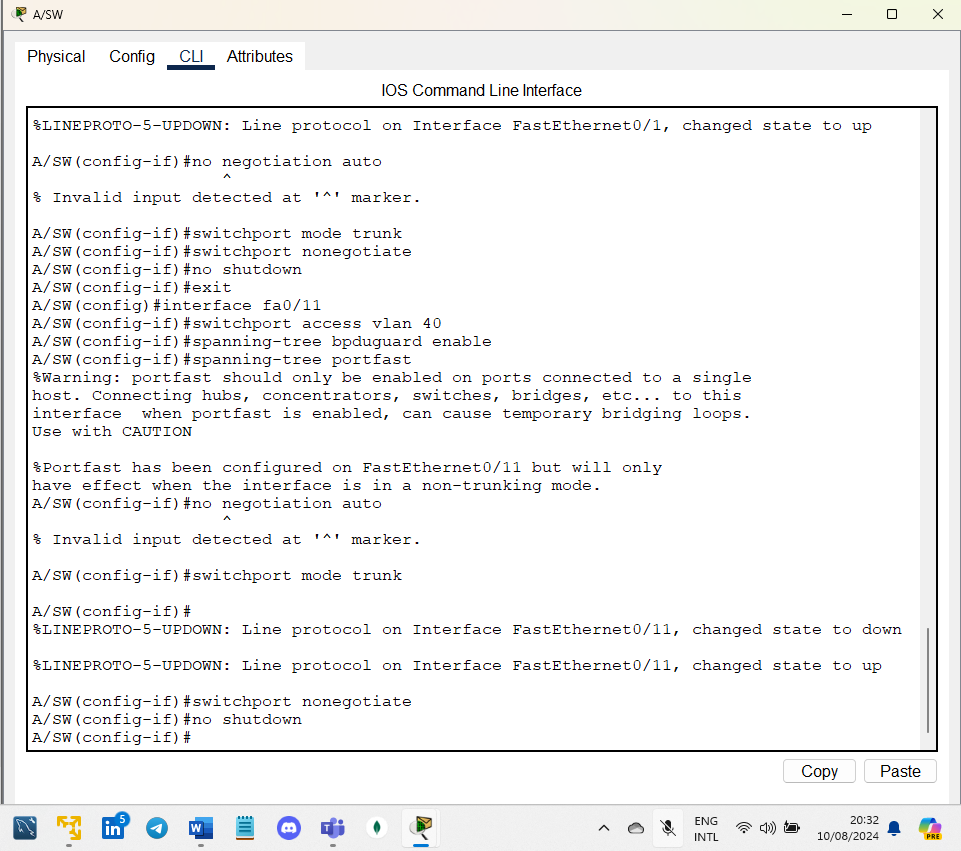
1. Configure port Fa0/1 with the following parameters: (5mks)

* Have access to Vlan 20
* Enable BPDU guard
* Enable portfast to allow the interface to come up faster
* Disable port negotiation
* Ensure that the port is not in a shutdown state



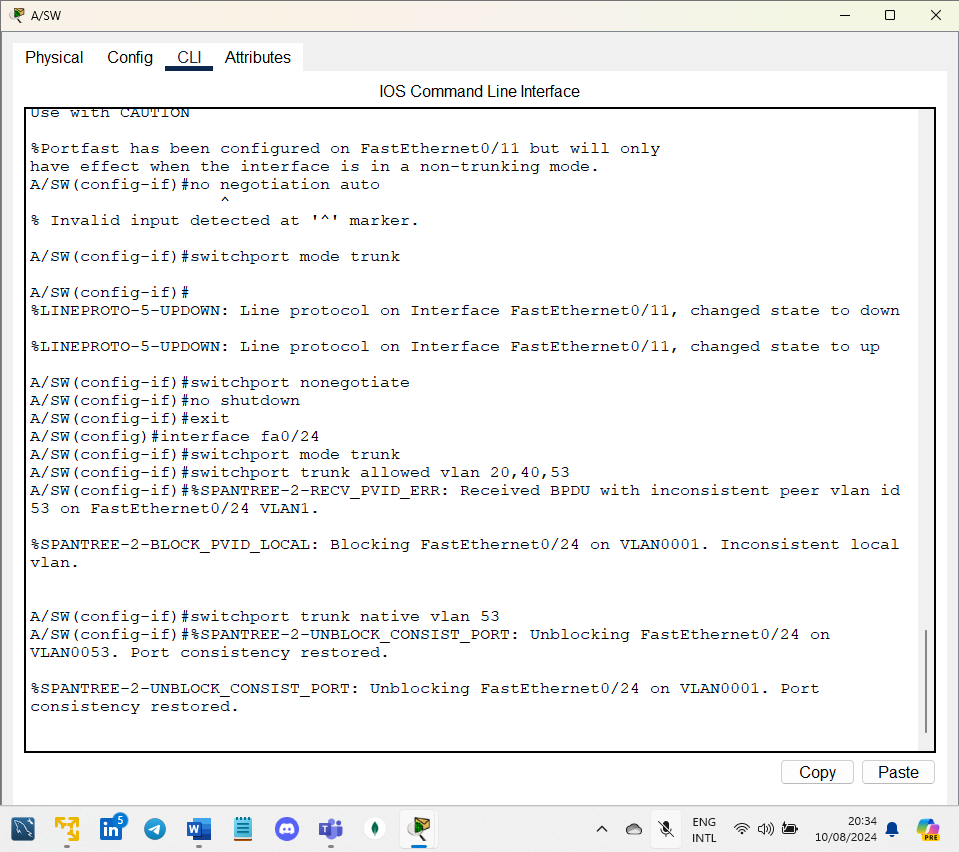
1. Configure port Fa0/11 with the following parameters: (5mks)

* Have access to Vlan 40
* Enable BPDU guard
* Enable portfast to allow the interface to come up faster
* Disable port negotiation
* Ensure that the port is not in a shutdown state

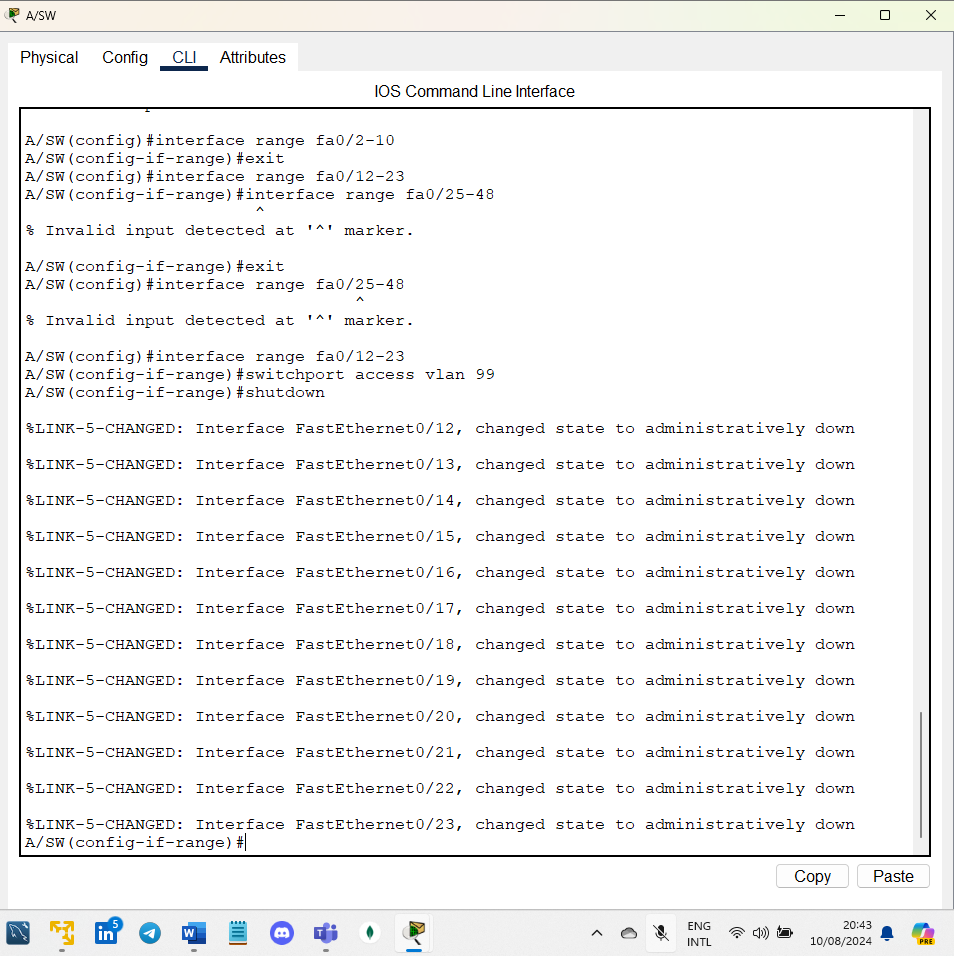


1. Configure port Fa0/24 with the following parameters:

* Trunk port (2mks)
* Explicitly allow traffic from Vlans 20, 40 and 53 only (3mks)
* Set the native Vlan as Vlan 53 (1mk)

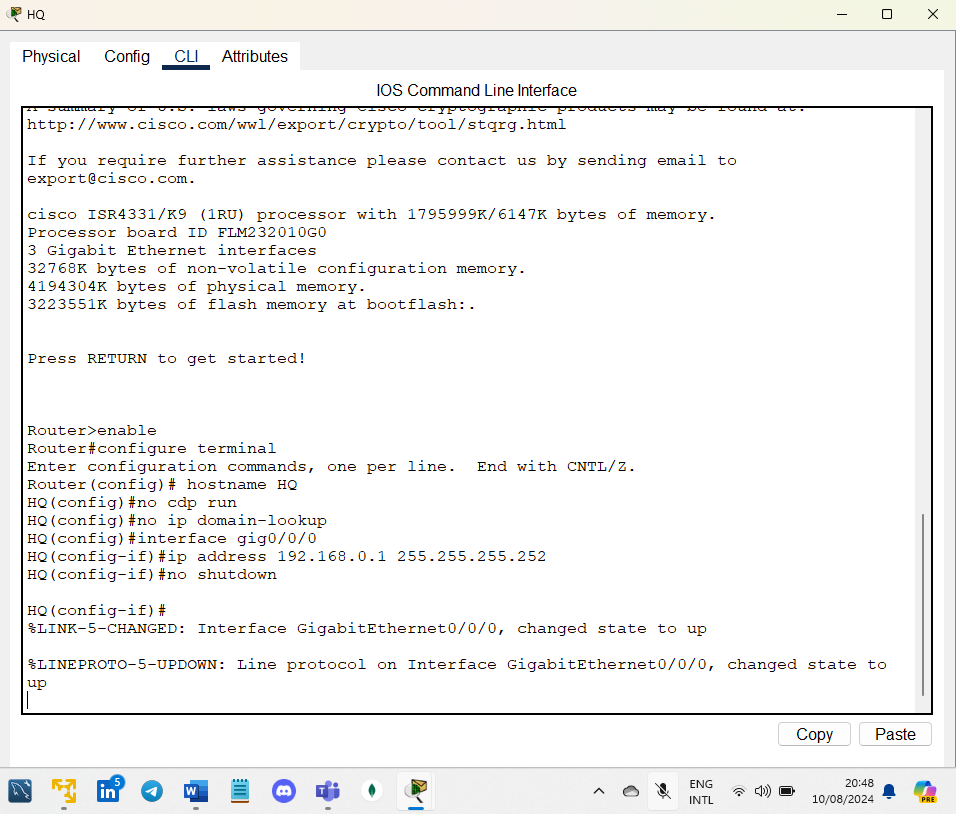
**

1. Put all unused ports in an administratively shutdown mode under Vlan 99. (2mks)



**SECTION 2: Configure the Router:**

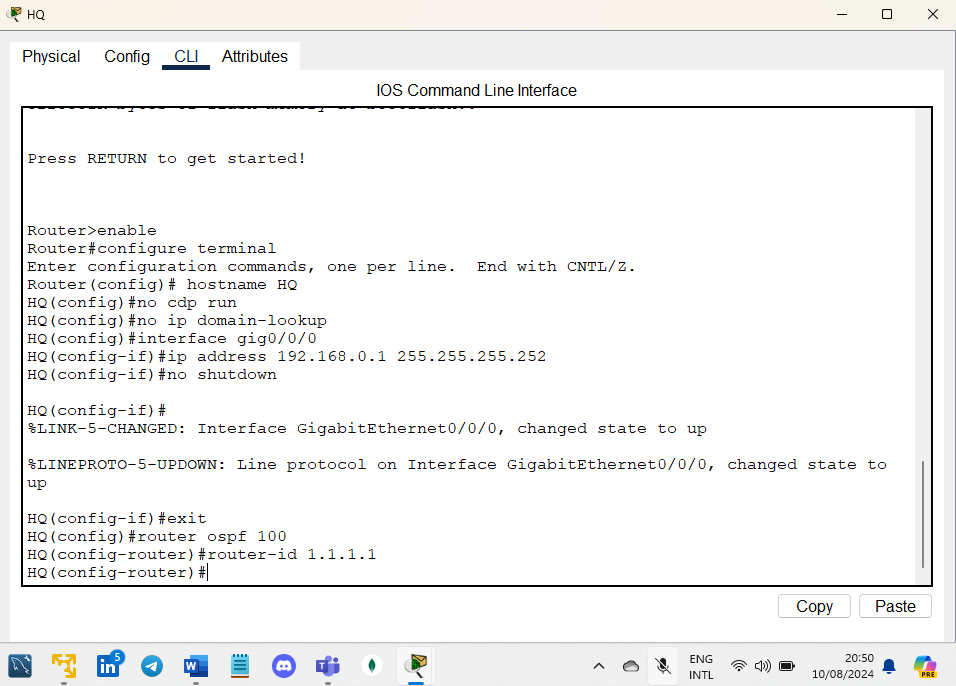
1. Rename the router as HQ (1mk)
2. Disable CDP (1mk)
3. Disable IP domain lookup (1mk)
4. Assign an IP address of 192.168.0.1/30 on interface Gig0/0/0 (1mk)



**SECTION 3: OSPF setup**

On the HQ router and the D/SW, set up OSPF.

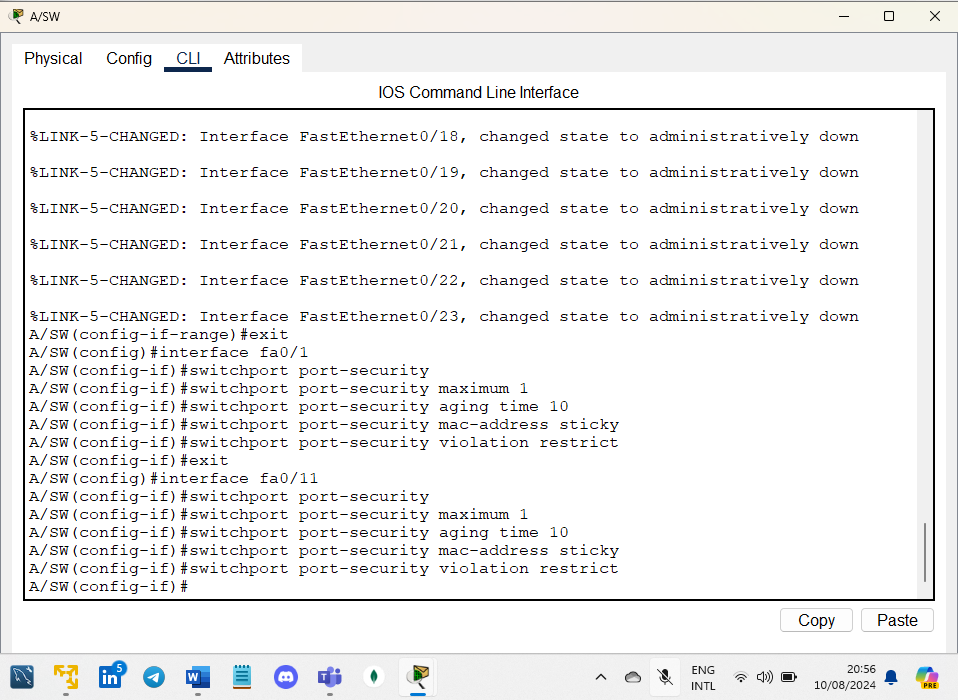
* Use the following parameters for the OSPF configuration;
* Configure the process ID as 100 on both devices (2mks)
* For the HQ Router, use a router ID of 1.1.1.1 (1mk)
* For the D/SW switch, use a router ID of 2.2.2.2 (1mk)



**SECTION 4: Port security**

On switch A/SW enable port security on ports Fa0/1 and Fa0/11 with the following parameters: (4mks)

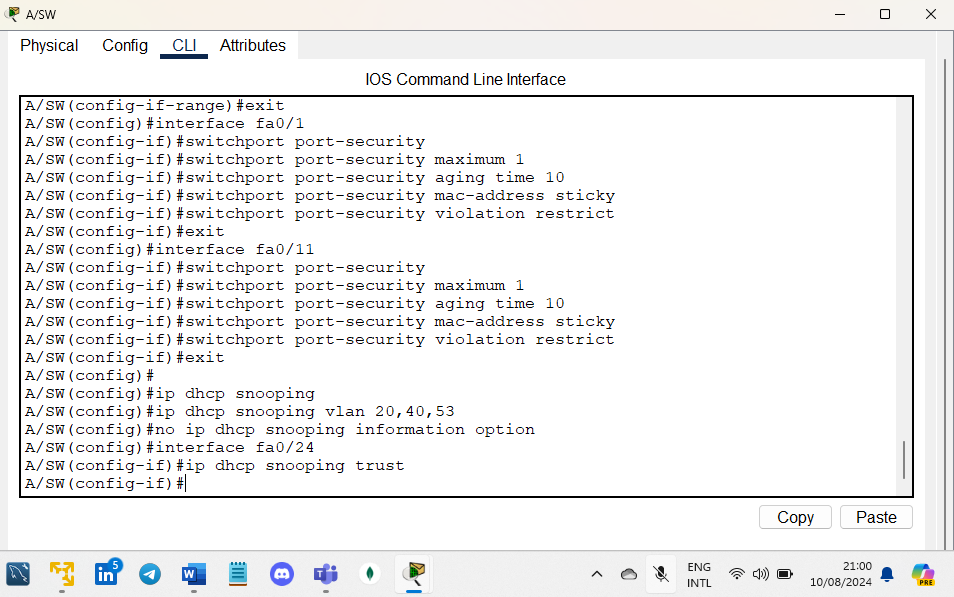
* Maximum of 1 mac address to be learned
* Aging time of 10 minutes
* Dynamically learned mac-address (sticky)
* Violation mode to be "restrict"



**SECTION 5: DHCP Snooping**

Enable DHCP snooping on switch A/SW for Vlans 20, 40 and 53 observing the following requirements:

* Disable switch A/SW from acting as a dhcp relay agent. In global config mode issue the command (no ip dhcp snooping information option) (2mks)
* Port Fa0/24 to be set as trusted (1mk)
* Leave everything else as default



**Conclusion**

This lab exercise reinforced my understanding of securing network layers in a Cisco environment. By implementing switch port security, DHCP snooping, and ensuring strong password management, I was able to effectively protect the network against potential threats.

These configurations are essential in maintaining the integrity and security of the network infrastructure, and they serve as basic practices for protecting sensitive data and systems.