

Assignment Submission

# Heading: Challenge 01

**Approach:** Initially, I examined the interface statuses and attempted to connect to the server at 10.0.0.1 without success. To troubleshoot further, I accessed the switch directly, navigated to the Config tab, and reviewed the configuration of FastEthernet 0/1. Through this, I gained access to the CLI and executed

commands to exit and save the running configuration to non-volatile memory. This action allowed me to retrieve the setup commands used for the network, where I discovered a specific command revealing the username 'net' and the password 'game'.

**Solution:** I went to the switch this time directly, went to the Config tab and tried seeing the config of fastEthernet 0/1, this gave me access to the CLI and I ran the following commands:

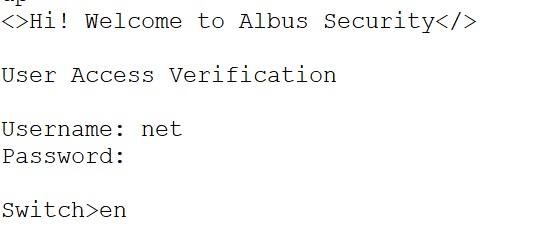
(config)#exit

#copy running-config startup-config

These commands helped me recover the running config which is in the primary memory of the switch making it volatile, further when exporting these files I got a file stating all the commands used for setting up the network. One command in particular caught my attention: username net privilege 1 password 0 game

This gave me the username ‘net’ and the password ‘game'





Heading: Challenge 02

**Approach:** The problem was to understand and configure a Cisco Catalyst 2960

Series switch to experience the MAC learning process and switch forwarding logic. The approach involved thoroughly reading and understanding the lab instructions, researching Cisco switch configuration commands, and verifying configurations.

Challenges were addressed by referring to Cisco documentation, seeking help from colleagues, and troubleshooting as needed.

**Solution:** I entered privileged EXEC mode for administrative access by using the command “enable”.

To see the current running configuration of the switch I used the command “show running-config”.

I used the command- “interface FastEthernet0/1” to accesses global configuration mode to make changes to the switch configuration.



Then used “speed auto” command that specifies the interface type and number to access for configuration.

“duplex auto” command sets the duplex mode of the interface to automatically negotiate with connected devices.

“no shutdown” command for enabling the specified interface to allow traffic to pass through.

“show interface FastEthernet0/1” to display the configuration details of the specified interface.

Used the “show mac address-table” command to show the MAC address table containing learned MAC addresses and associated interfaces.

Then “end” command to exit the current configuration mode.

“Write memory” command to write the current configuration to memory, ensuring it is saved even after a reboot.

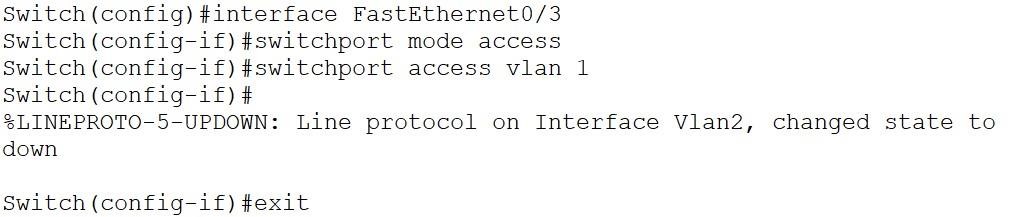
# Heading: Challenge 03

**Approach:** Initially, I investigated the VLAN status to identify any issues and rectify them. Upon examining packet communication, I observed that 'bob' and 'vicer' were



assigned to different VLANs, obstructing their communication. To resolve this, I changed the VLAN of FastEthernet 0/3 on the admin switch from VLAN 2 to VLAN

**Solution:** While checking the communication of packets, we see bob and vicer are configured to 2 different VLANs, hence hindering in their communication. To make them work, we switch the VLAN of fastEthernet 0/3 of admin switch to 1 instead of 2 to make it work. I did it with the following step:



# Heading: Challenge 04

**Approach:** Understand the problem of configuring the hostname on a switch. Researched methods for Cisco switches running IOS. Analyse with available commands.

# Solution:

Utilized the following command for Cisco switches running IOS: Switch# configure terminal

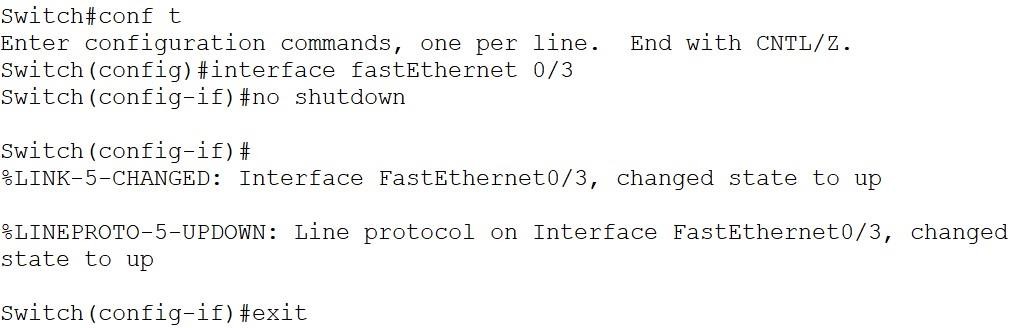
Switch(config)# hostname R1



**Heading: Challenge 05**

**Approach: Understand the problem between lines and solve them.**

**Solution: line status of fastEthernet 0/3 of the Junior switch was down, brought that up by using the following commands:**



**Heading: Challenge 06**

**Approach:** Troubleshoot for the error in the network and fix it with the pre-requisite knowledge.

# Solution:

**Configure the switches firstAdmin:**

Switch(config)#interface gig0/1

Switch(config-if)#switchport mode trunk Switch(config)#interface fa0/3

Switch(config-if)#switchport mode access Switch(config-if)#switchport access vlan 2 Switch(config-if)#exit

Switch(config)#interface fa0/2

Switch(config-if)#switchport mode access



Switch(config-if)#switchport access vlan 1 Switch(config-if)#exit

Switch(config)#interface fa0/1

Switch(config-if)#switchport mode access Switch(config-if)#switchport access vlan 3 Switch(config-if)#exit

Switch(config)#end Switch#write memory

# Senior:

Switch(config)#interface gig0/1

Switch(config-if)#switchport mode trunk Switch(config)#interface fa0/1

Switch(config-if)#switchport mode access Switch(config-if)#switchport access vlan 2 Switch(config-if)#exit

Switch(config)#interface fa0/2

Switch(config-if)#switchport mode access Switch(config-if)#switchport access vlan 3 Switch(config-if)#exit

Switch(config)#interface fa0/3

Switch(config-if)#switchport access vlan 1 Switch(config-if)#switchport mode access Switch(config-if)#switchport access vlan 1 Switch(config-if)#exit

Switch(config)#end Switch#write memory



# Now I changed the following IPs:

VLAN1 On Senior: 10.0.0.2

VLAN2 on Senior: 30.0.0.2 VLAN3 on Senior: 40.0.0.2 Bob’s IP: 192.168.2.1

Hope’s IP: 192.168.1.1

Vicer’s IP: 192.168.3.1

Carlos’s IP: 192.168.2.2

Jack’s IP: 192.168.3.2

Harry’s IP: 192.168.1.2

# All of this made the network work again.

**Heading: Challenge 07**

**Approach:** To address a layer 1 issue on working interfaces, particularly duplex mismatches indicated by late collisions, I followed these steps:

Problem Understanding: Recognized late collisions as indicators of duplex mismatches. Research and Analysis: Researched late collisions and their relation to duplex mismatches. Approach: Verified interface status and examined late collision counters.

Methods Used: Employed commands like show interfaces to gather information. Challenges: Addressed by consulting documentation and seeking assistance if needed.

Solution:

1. I used “enable” command to enter privileged EXEC mode for administrative access.
2. To enter global configuration mode I used “crypto key generate rsa modulus 2048” command to make changes to the switch's configuration.
3. Then used “configure terminal” command to enter global configuration mode to make changes to the switch's configuration.



1. Used “hostname <hostname>” to set the hostname of the switch to the specified value.
2. Then used “ip domain-name <domain\_name>” to cofigure the domain name for the switch.
3. Then I used “ip ssh version 2 crypto key generate rsa” to enable SSH version 2 and generates an RSA key pair for secure communication.

# Heading: Challenge 08

**Approach:** Identified SSH's security significance over Telnet and configured symmetric encryption using "crypto key generate rsa." Employed researched commands and sought assistance as required.

# Solution:

1. Used "crypto key generate rsa" to generate an RSA key pair for SSH encryption.
2. Used "line vty 0 15" to access line configuration mode for virtual terminal lines 0 through 15.
3. Configured the timeout period for inactive connections on virtual terminal lines using "exec-timeout <minutes> <seconds>".
4. Exited the current configuration mode with the "end" command.
5. Saved the configuration changes to non-volatile memory with "write memory" to ensure persistence after a reboot.
6. Utilized "show ssh" to display information about the SSH configuration, including version,

status, and configured parameters.

**Heading: Challenge 09 Approach:** Learn about SSH timeouts **Solution: Disable SSH timeout:**

Switch(config)#line vty 0 15

Switch(config-line)#exec-timeout 0 0



# Disable console timeout:

Switch(config)# line console 0 Switch(config-line)# exec-timeout 0 0

# Don’t forget to save the settings using : write memory

Heading: Challenge 10

**Approach:**

1. Grasped VLAN and trunking issues in the lab.
2. Adopted a systematic troubleshooting approach post-research.
3. Utilized configuration commands within Packet Tracer.
4. Addressed challenges through consultation with resources and peers when necessary.

# Solution:

Used “enable” command to enter privileged EXEC mode for administrative access.

Then “configure terminal” to enter global configuration mode to make changes to the switch's configuration.

Then used “vlan <vlan\_id>” to create a VLAN with the specified VLAN ID.

After that “name <vlan\_name>” to assign a name to the VLAN for easier identification.



Then “interface <interface\_id>” to select the interface to configure.

Used “switchport mode access” command to configure the interface as an access port, allowing devices in the specified VLAN to connect.

Using “switchport access vlan <vlan\_id>” to assign the specified VLAN to the access port, restricting traffic to that VLAN.

Using “interface <interface\_id>” to select the interface to configure as a trunk port.

Used “switchport mode trunk” to configure the interface as a trunk port, allowing traffic from multiple VLANs to pass through.

“switchport trunk allowed vlan <vlan\_list>” command to specifie which VLANs are allowed to traverse the trunk port.

“vtp mode <mode>” command to set the VLAN Trunking Protocol (VTP) mode for the switch.

“vtp domain <domain\_name>” command to specifie the VTP domain name for the switch.

Then “end” command to exit the current configuration mode.

“copy running-config startup-config” command that saves the running configuration to non-volatile memory, ensuring it persists after a reboot.