# Lab1 Basic Switch management

***Prepared by:***

**Lohan Vaddepally**

## Lab Objectives

1. To gain skills for achieving basic management of a switch.
2. To configure the IP addresses of host computers.
3. To check the status of the interfaces of a switch.
4. To examine the MAC address table entries of a switch before and after running the ARP process.
5. To achieve a basic configuration of a switch.
6. To add security for accessing the configuration of a switch.
7. To enable remote access of a switch configuration within a simple Ethernet LAN.

## Network Topology

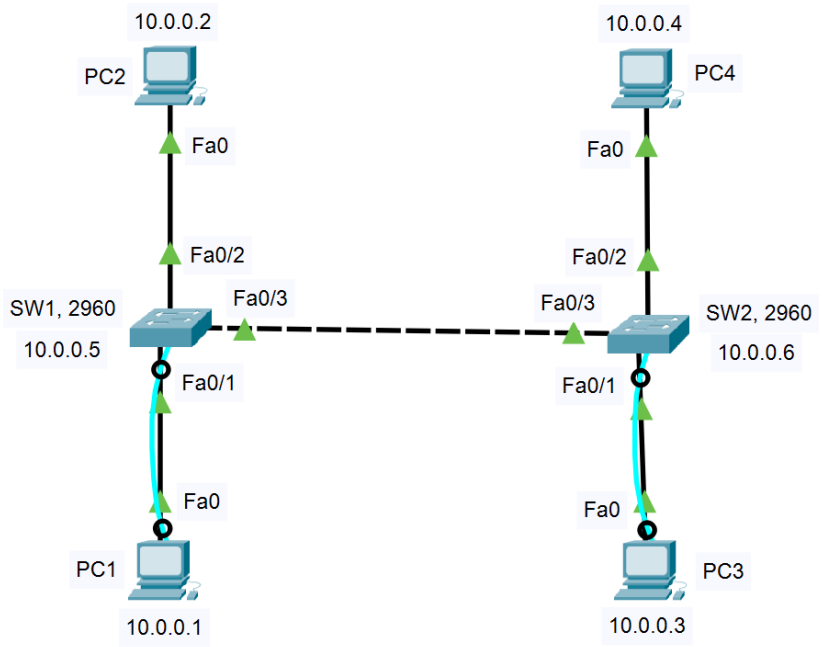



**Figure 1 Topology of the Ethernet LAN network**

Using the devices in the lab, construct the Ethernet LAN network shown in Figure 1. Use the Cisco 2960 model for each of the switches SW1 and SW2. Use copper straight-through cables to connect Fa0 of PC1 to Fa0/1 of SW1, Fa0 of PC2 to Fa0/2 of SW1, Fa0 of PC3 to Fa0/1 of SW2, and Fa0 of PC4 to Fa0/2 of SW2. Note that Fa0 here refers to the FastEthernet port of the NIC of the PC, and Fa0/n (where n is an integer number) is one of the FastEthernet ports of the switch. Also, connect the Fa0/3 ports of SW1 and SW2 using a copper cross-over cable. To console from PC1 to SW1 connect a console cable from the RS232 connector of PC1 to the Console port of SW1. Also to console from PC3 to SW2 connect a console cable from the RS232 connector of PC3 to the Console port of SW2. Notice that the IP address of the NIC of each PC is indicated in the figure. Also, the IP addresses of the administrative VLAN 1 of SW1 and SW2 are indicated in the figure.

## Procedure

1. Access the IPv4 addressing configuration of PC1 in Windows. Enter the IP address 10.0.0.1 of PC1 and notice that the mask will be set to 255.0.0.0. See Figure 2 for the configuration of the IP address of PC1. Repeat the same procedure to configure the IP addresses of each of PC2, PC3, and PC4.

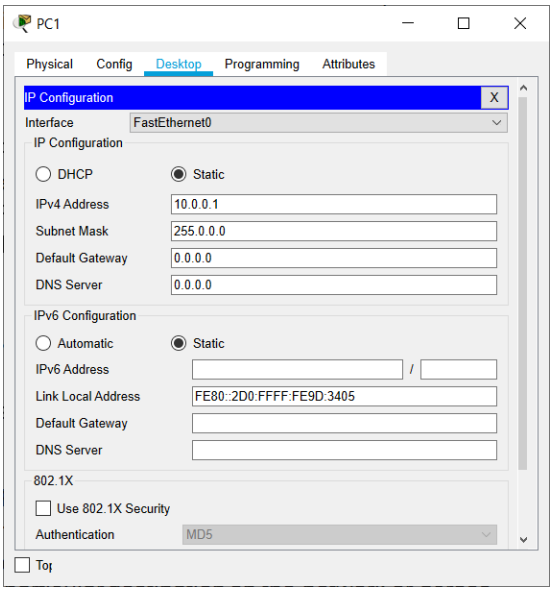



**Figure 2 Configuring the IP address of PC1.**

In Figure 3 below insert an image for the configuration of the IP address of PC4. **[0.5 marks]**

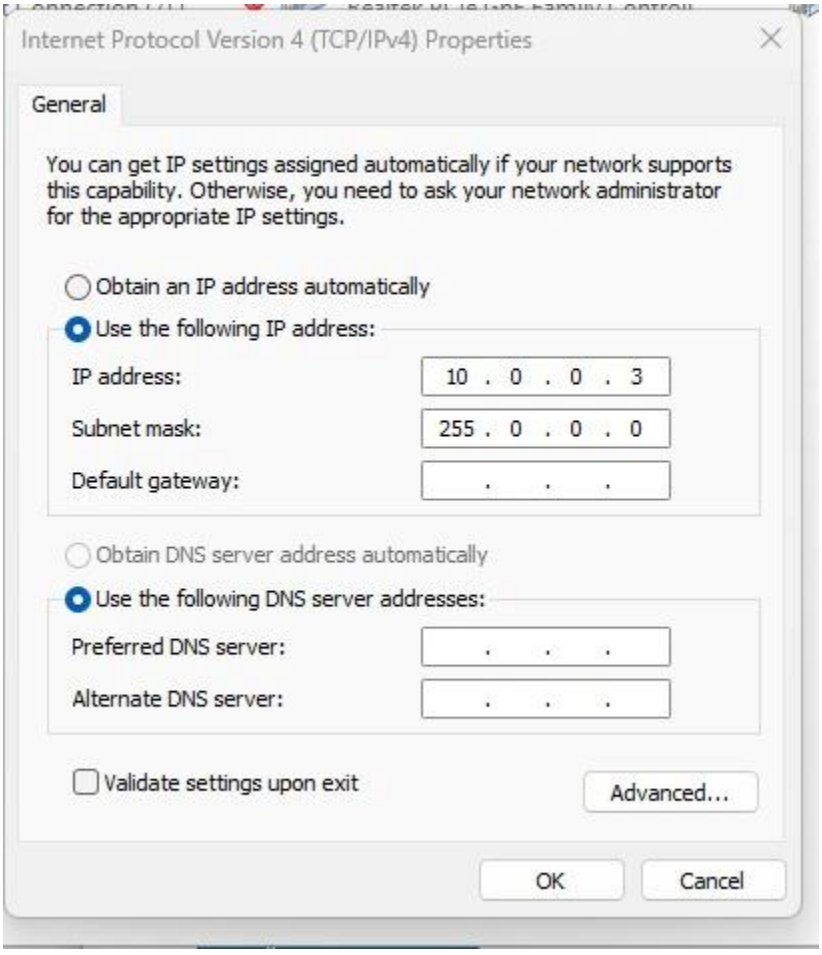



**Figure 3 Configuring the IP address of PC4.**

2. Open the Command Prompt of each PC and execute the command:

   **C:\>ipconfig /all**

   Determine the MAC address (also called the Physical Address) of the NIC (FastEthernet0) of each PC and list the results in Table 1. **[0.5 marks]**

   **Table 1 MAC addresses of FastEthernet0 NIC of the PCs.**

| Host | MAC address of Fa0 |
|---|---|
| PC1 | **00-13-3B-4A-5A-5B** |
| PC2 | **00-13-3B-4A-59-2D** |
| PC3 | **00-13-3B-4A-59-19** |
| PC4 | **00-13-3B-4A-5A-3D** |

3. The command-line interface (CLI) of a switch may be accessed through a PC by connecting the serial port (referred to as the RS232) of the PC to the console port of the switch using a console cable ( a Cisco proprietary cable). A terminal emulation program such as “Putty” is used to enter the console session. This type of access to the CLI of a networking device is referred to as out-of-band access. Open the terminal emulator application on PC1, choose Serial connection type, indicate the COM port associated with your RS232 interface, agree with the default parameters, and click OK to get into the CLI of SW1. Once there, press the Enter key to get started. Notice that the prompt of the switch is at the user exec level:

   **Switch>**

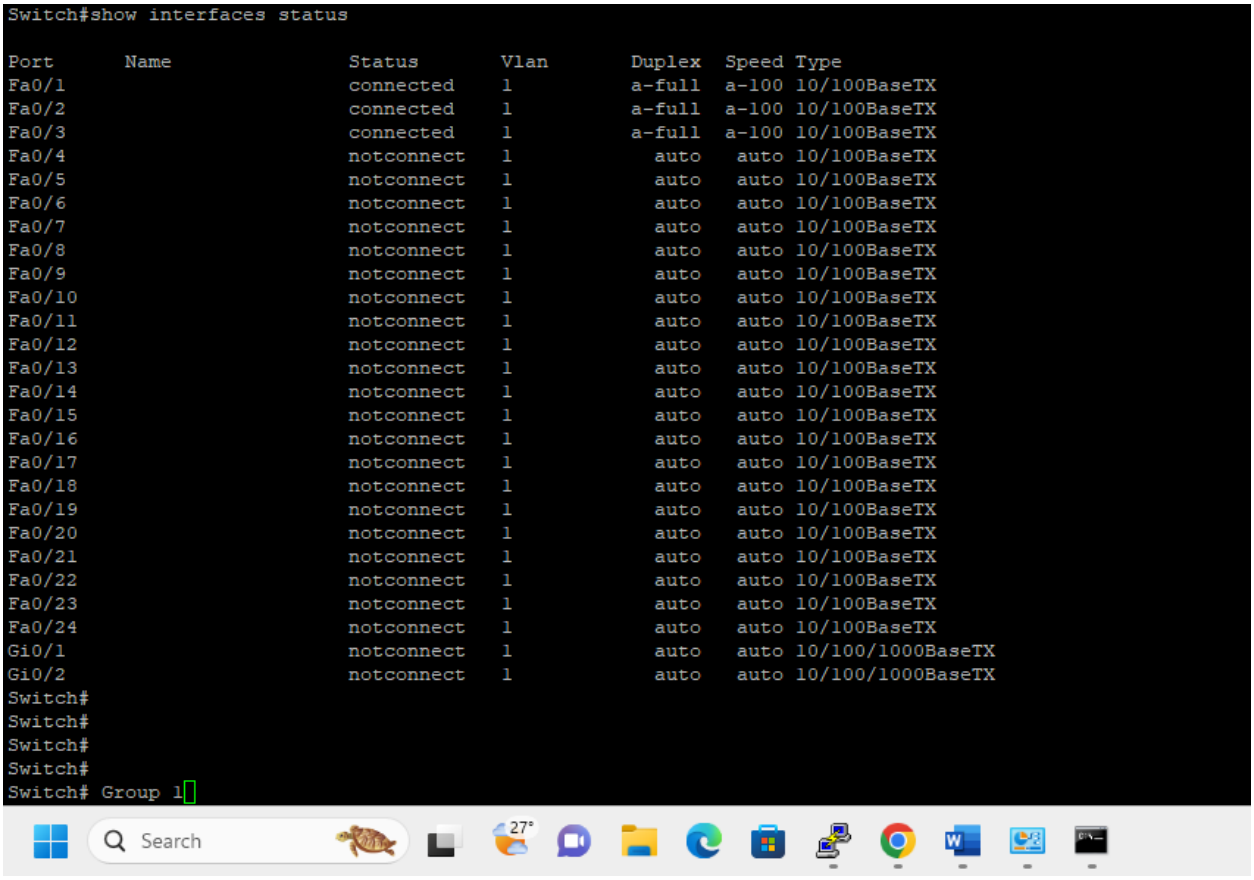
   Enter the command “enable” to elevate the switch prompt to the privileged mode:

   **Switch>enable**
   **Switch#**

   Now use the following command to list the status of all ports of the switch:

   **Switch#show interfaces status**

   Below in Figure 4 insert an image of the output of the above command. Indicate which interfaces of the switch are connected. **Answer: Fa 0/1, Fa 0/2, Fa 0/3**




.....[0.5 marks]

**Figure 4 Status of the Interfaces of SW1.**

Also, check the status of the interfaces of SW2.

4. Display the MAC address table of SW1 using the command:

   **Switch#show mac address-table**

   Insert an image of the output in Figure 5 below.

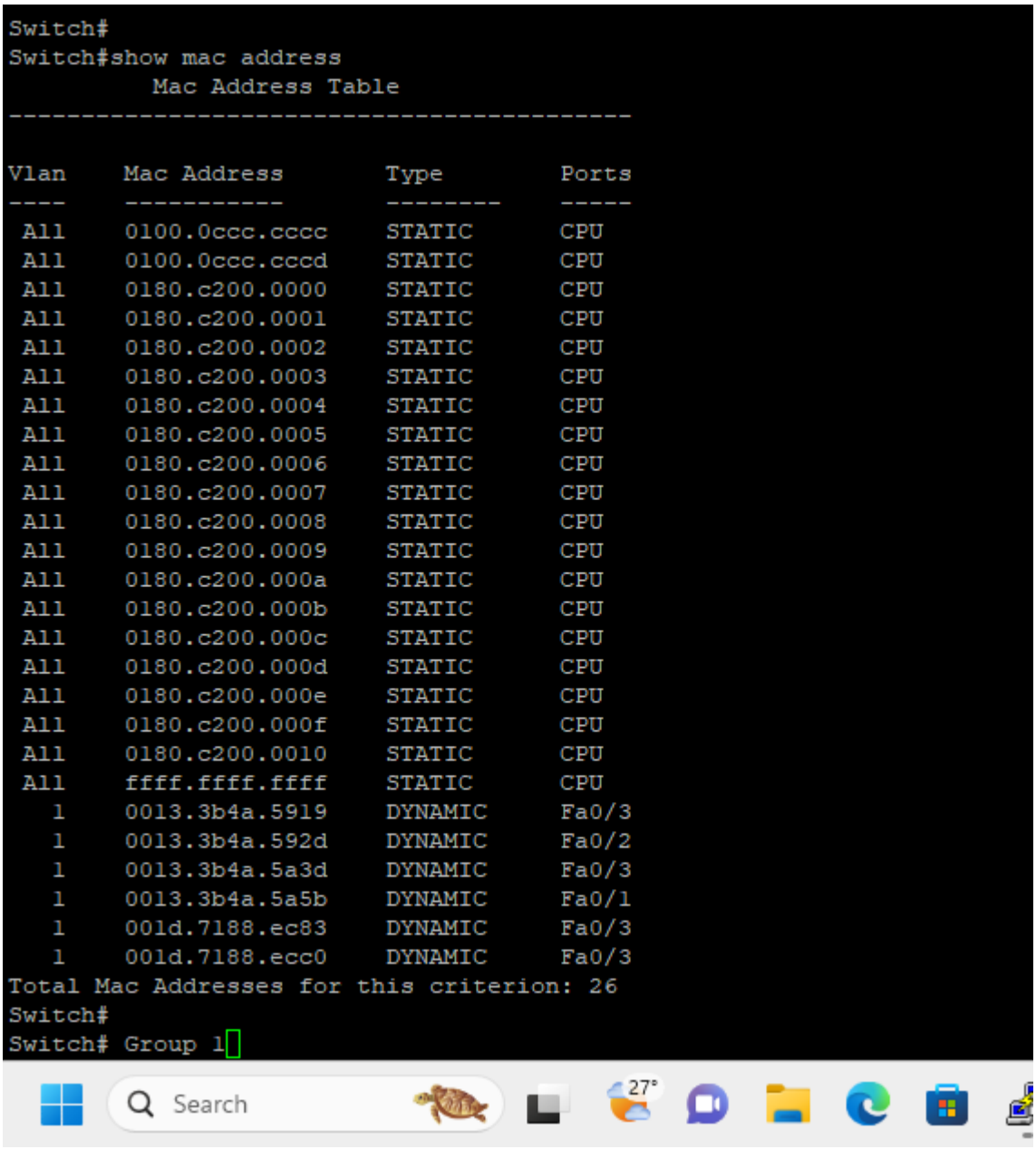



**Figure 5 MAC address table of SW1.**

Notice in this case that the MAC addresses of all PCs are not available in the content addressable memory (CAM) table of the switch yet. Explain why: **[0.5 marks]**
**The MAC addresses of all PCs are not available in the CAM table yet because the switch has not yet received frames from those PCs.**

5. From the Command Prompt of PC1 ping the IP addresses of all the other PCs. Here is the command to ping PC2:

   **C:\>ping 10.0.0.2**

Below in Figure 6 insert an image of the result of the ping operation from PC1 to PC4. **[0.5 marks]**

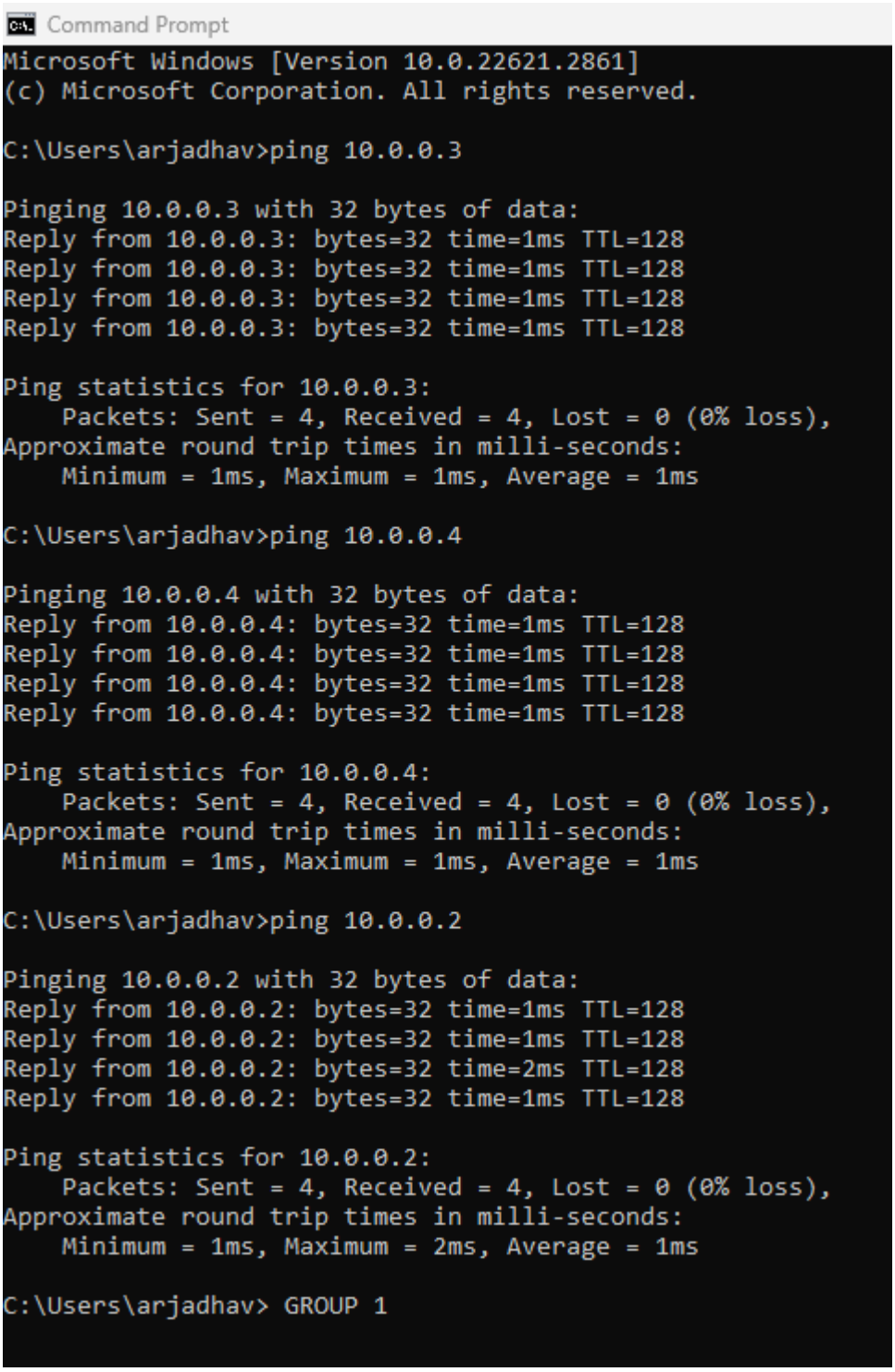



**Figure 6 Ping of PC4 from PC1.**

Immediately after the three ping operations indicated above display the MAC address table of SW1 and insert the image of results in Figure 7.

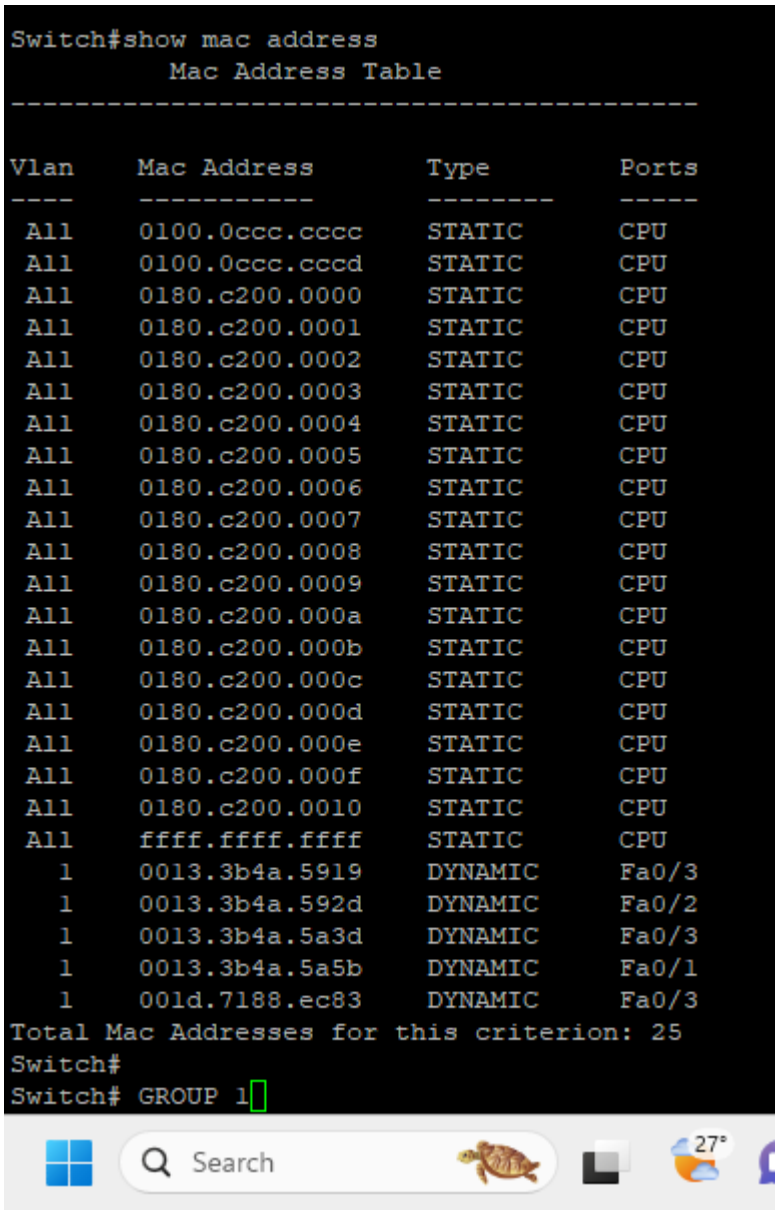



**Figure 7 MAC address table of SW1.**

Also inspect the MAC address table of SW2. Do you see the MAC addresses of the PCs in the CAM tables of SW1 and SW2? **Answer [Yes/No]: YES** **[0.5 marks]**

Briefly explain how the CAM tables of the switches got filled after your attempt to ping between PCs. **[0.5 marks]**

**The CAM tables of the switches got filled as a result of the ARP request and reply packets exchanged during the initial attempt to ping between PCs. Each switch learned the MAC addresses of the PCs by examining the source MAC address of the frames it received and associating these addresses with the corresponding ports. This learning process allows the switches to forward subsequent traffic between the PCs efficiently.**

With which VLAN are the entries of the CAM tables of SW1 and SW2 associated?

**Answer: VLAN1** **[0.5 marks]**

6. In the CLI of SW1 enter the global configuration mode:

**Switch#configure terminal**

Set the hostname of the switch to SW1:

**Switch(config)#hostname SW1**

When you mistype a command in the CLI of a networking device, the DNS name resolution process attempts to resolve a supposed hostname (the mistyped command) into an IP address. This will make you wait for one minute before getting the prompt back. In order to disable the DNS resolution process enter the command:

**SW1(config)#no ip domain-lookup**

Now, configure “cisco” as a plaintext password to restrict access to the privileged mode:

**SW1(config)#enable password cisco**

Enter the command “exit” two times to restart the console session, and notice that you will start from the user exec mode. Enter the command “enable” and notice that you will be prompted to enter a password. In this case, enter the password “cisco” to get into the privileged mode.

Now, configure “class” as the new encrypted password to restrict access to the privileged mode:

**SW1(config)#enable secret class**

Again, enter the command “exit” two times to restart the console session, and notice that you will start from the user exec mode. Enter the command “enable” and notice that you will be prompted to enter a password. In this case, enter the password “class” to get into the privileged mode. So, the new style secret password has overridden the old plain text password.

Now configure a password called “conpass” to restrict access to the console session:

**SW1(config)#line con 0**

**SW1(config-line)#password conpass**

**SW1(config-line)#login**

**SW1(config-line)#exit**

**SW1(config)#**

The login command activates the configured password. Restart the console session as before and notice that you will be prompted to enter the password “conpass” needed to access the console session. As before, to get into the privileged mode you will need to enter the “class” encrypted password.

**User Access Verification**

**Password:**

**SW1>enable**

**Password:**

**SW1#**

The passwords used in this step to limit access to the privileged mode are shared passwords.

7. For SW2 configure a fully qualified domain name (FQDN):

**Switch(config)#hostname SW2**

**SW2(config)#ip domain-name lab1.com**

Now, create RSA encryption keys for the switch.

**SW2(config)#crypto key generate rsa**

The name for the generated public/private keys will be: SW2.lab1.com

Choose the size of the key modulus in the range of 360 to 2048 for your

General Purpose Keys. Generating keys with a key modulus greater than 512 may take a few minutes.

**How many bits in the modulus [512]: 1024**

**% Generating 1024 bit RSA keys, keys will be non-exportable...[OK]**

**SW2(config)#**

Notice that the crypto key command prompts the user for the key modulus. The above commands create a pair of Secure Socket Layer (SSL) encryption keys and enable SSH access.

Use the “login local” command to enable the console to prompt for both username and password:

**SW2(config)#line con 0**

**SW2(config-line)#login local**

**SW2(config-line)#exit**

**SW2(config)#**

Define a local username:

**SW2(config)#username groupX password conpass**

Where X is your group number. Configure the secret password “class” to limit access to the privileged mode for SW2:

**SW2(config)#enable secret class**

Disable the DNS name resolution process on SW2.

Restart the console session of SW2 and test the configured console session access credentials (“groupX” as the user name and “conpass” as the password). Also, test the password “class” to access the privileged mode.

8. In this step, SW1 will be configured for remote access using Telnet.
Configure the IP address for SW1 management VLAN (in this case we will use VLAN1):

**SW1(config)#int vlan 1**
**SW1(config-if)#ip address 10.0.0.5 255.0.0.0**

```
SW1(config-if)#no shutdown

SW1(config-if)#
%LINK-5-CHANGED: Interface Vlan1, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan1, changed state to up

SW1(config-if)#exit
SW1(config)#
```

Configure “telpass” as a password for the telnet session in line vty 0 4:

```
SW1(config)#line vty 0 4
SW1(config-line)#password telpass
SW1(config-line)#login
SW1(config-line)#exit
SW1(config)#
```

Now, from PC4 ping the IP address of VLAN 1 of SW1. Insert the image of the result in Figure 8. **[0.5 marks]**

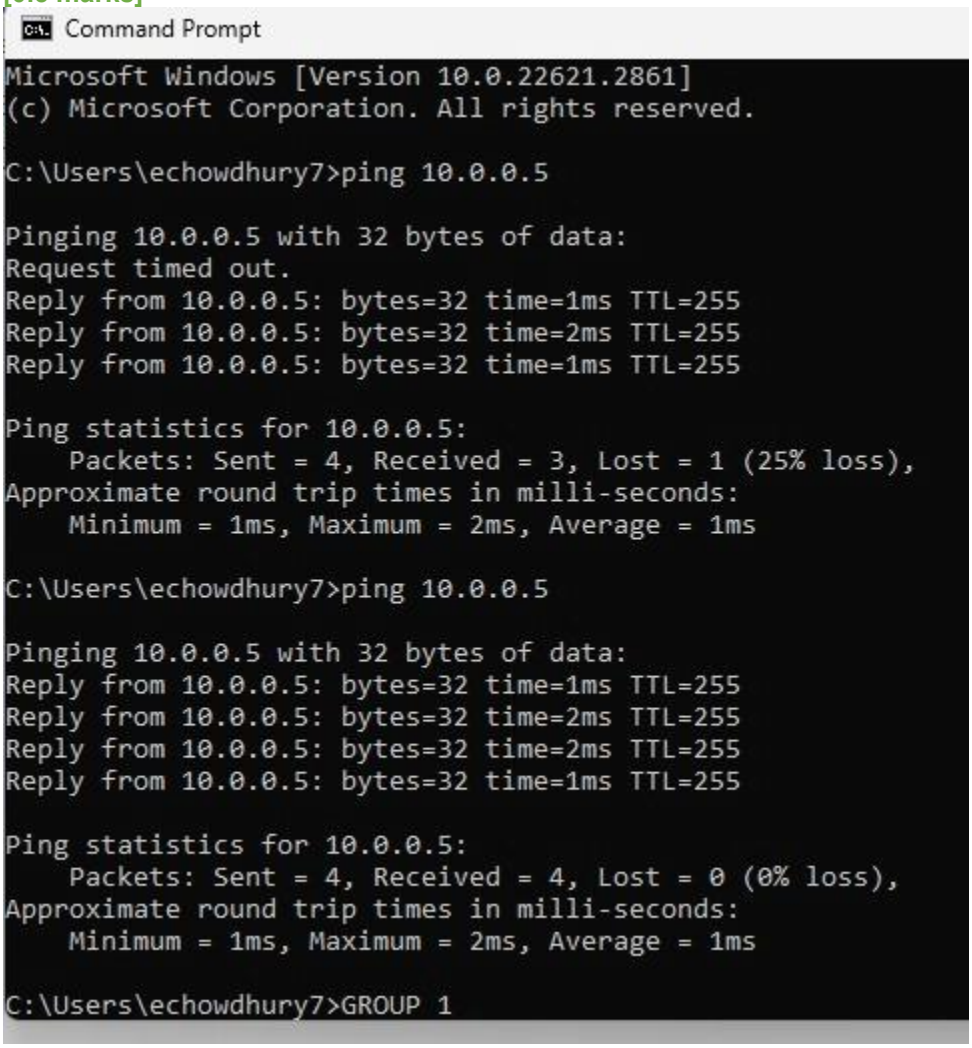



**Figure 8 Output of the ping operation of VLAN 1 from PC4.**

Was the above ping operation successful? **Answer [Yes/No]: YES**

Now, access the CLI of SW1 remotely from PC4:

```
C:\>telnet 10.0.0.5
Trying 10.0.0.5 ...Open


User Access Verification

Password:
SW1>enable
Password:
SW1#
```

Remember the password to enter the telnet session is “telpass” and the password to get into the privileged mode is “class” for SW1. Execute the command “show running-config” from inside the telnet session accessed from PC4 to view the running configuration of SW1:

```
SW1#show running-config
```

Insert the output result in full (you may use more than one image) for this command in Figure 9. **[0.5 marks]**

```
SW1>enable
Password:
SW1#show running-config
Building configuration...

Current configuration : 1462 bytes
!
! Last configuration change at 00:40:48 UTC Mon Mar 1 1993
!
version 15.0
no service pad
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname SW1
!
boot-start-marker
boot-end-marker
!
enable secret 5 $1$5VM7$gzvPRAJen8aM.tw7Ch5CO/
enable password cisco
!
no aaa new-model
system mtu routing 1500
!
!
no ip domain-lookup
!
!
!
!
!
!
!
!
spanning-tree mode pvst
spanning-tree extend system-id
!
vlan internal allocation policy ascending
!
!
!
!
!
!
interface FastEthernet0/1
!
interface FastEthernet0/2
!
interface FastEthernet0/3
!
interface FastEthernet0/4
!
interface FastEthernet0/5
!
```

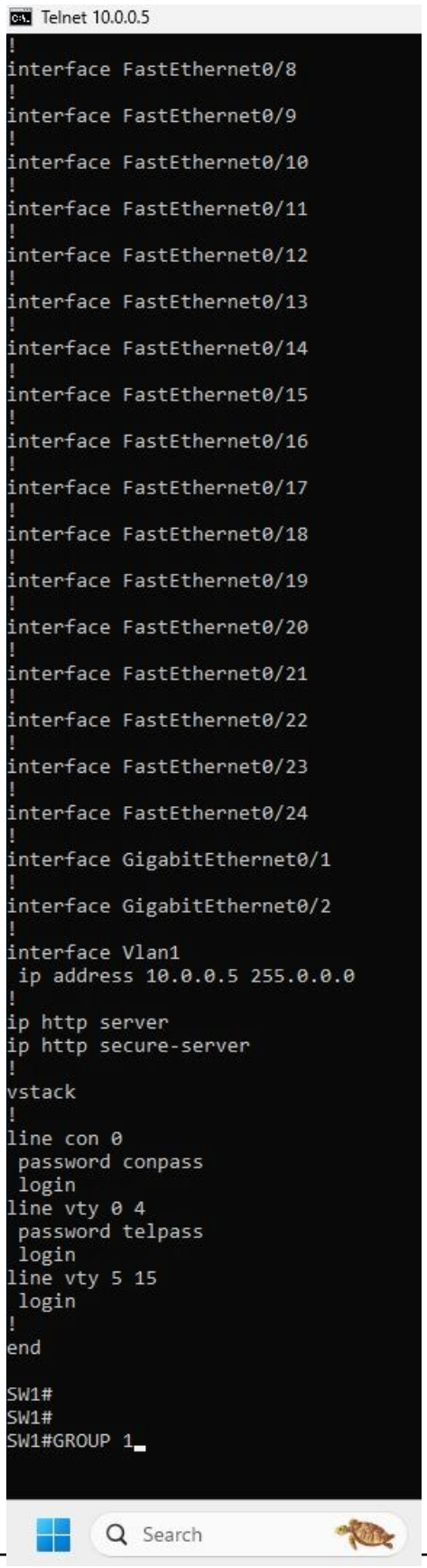
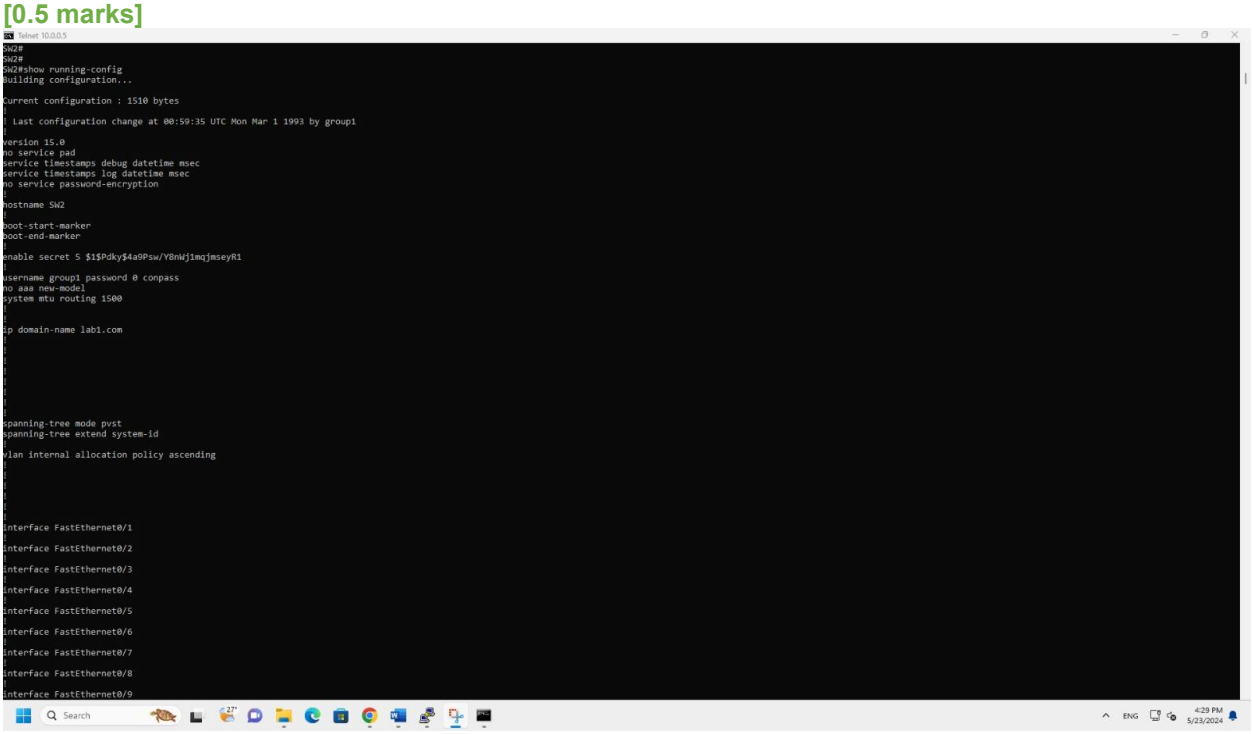

Telnet 10.0.0.5
!
interface FastEthernet0/8
!
interface FastEthernet0/9
!
interface FastEthernet0/10
!
interface FastEthernet0/11
!
interface FastEthernet0/12
!
interface FastEthernet0/13
!
interface FastEthernet0/14
!
interface FastEthernet0/15
!
interface FastEthernet0/16
!
interface FastEthernet0/17
!
interface FastEthernet0/18
!
interface FastEthernet0/19
!
interface FastEthernet0/20
!
interface FastEthernet0/21
!
interface FastEthernet0/22
!
interface FastEthernet0/23
!
interface FastEthernet0/24
!
interface GigabitEthernet0/1
!
interface GigabitEthernet0/2
!
interface Vlan1
 ip address 10.0.0.5 255.0.0.0
!
ip http server
ip http secure-server
!
vstack
!
line con 0
 password conpass
 login
line vty 0 4
 password telpass
 login
line vty 5 15
 login
!
end
SW1#
SW1#
SW1#GROUP 1
Search

**Figure 9 Output of the running configuration file of SW1 within the telnet session.**

9. Execute the “show run” command on SW2 and insert an image for the results in Figure 10 below. **[0.5 marks]**



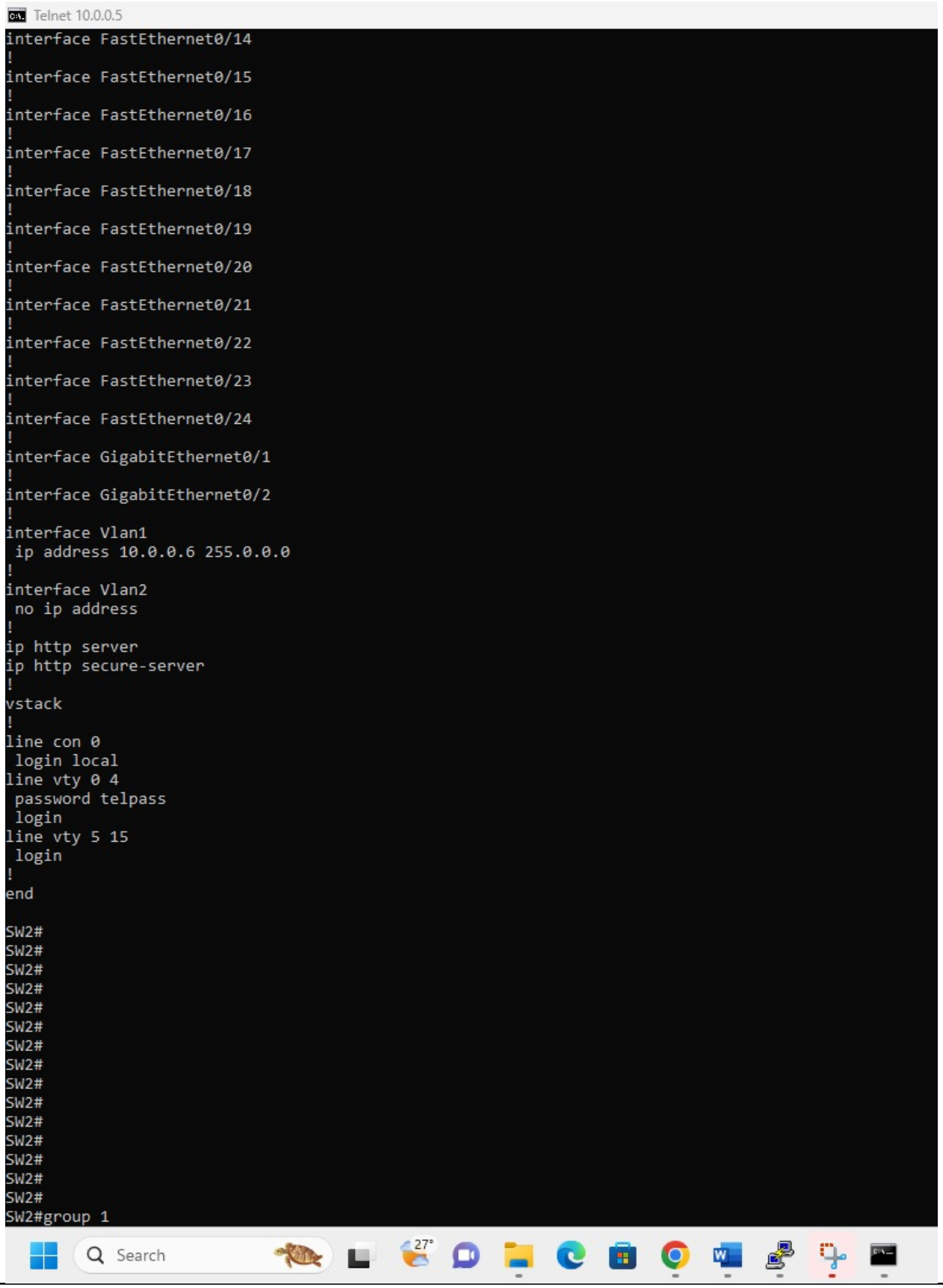

Telnet 10.0.0.5
interface FastEthernet0/14
!
interface FastEthernet0/15
!
interface FastEthernet0/16
!
interface FastEthernet0/17
!
interface FastEthernet0/18
!
interface FastEthernet0/19
!
interface FastEthernet0/20
!
interface FastEthernet0/21
!
interface FastEthernet0/22
!
interface FastEthernet0/23
!
interface FastEthernet0/24
!
interface GigabitEthernet0/1
!
interface GigabitEthernet0/2
!
interface Vlan1
ip address 10.0.0.6 255.0.0.0
!
interface Vlan2
no ip address
!
ip http server
ip http secure-server
!
vstack
!
line con 0
login local
line vty 0 4
password telpass
login
line vty 5 15
login
!
end
SW2#
SW2#
SW2#
SW2#
SW2#
SW2#
SW2#
SW2#
SW2#
SW2#
SW2#
SW2#
SW2#
SW2#
SW2#
SW2#
SW2#group 1
Search
27°

**Figure 10 Output of the running configuration file of SW2 within the telnet session.**

## Discussion

If the Ethernet LAN network of Figure 1 was connected to a default gateway router what extra configuration command(s) would be needed to gain remote Telnet access to the CLI of SW1 from a host located outside the LAN network? **[0.5 marks]**

**Answer:**

**Set the default gateway for the switch so that it can communicate with devices outside its local subnet. This is the IP address of the router interface connected to the LAN.**

**ip default-gateway <10.0.0.1>**