Lab1A Basic Switch management

Prepared by:

Ali Abdulsattar Hussein
Majid Shahravan
Nagham Kubba

[redacted]

[redacted]

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.

Lab Instructions

1. Type your name, student ID
2. Launch Packet Tracer and perform the lab
3. Follow the procedure of the lab and fulfill all requirements.
4. Answer all questions in the provided spaces (preferably in the red-bold font).
5. Add all required screenshots into corresponding spaces
6. Save the file again as a " .pdf " file
7. Submit the PDF file and the packet tracer file in Blackboard by the due date.

Network Topology

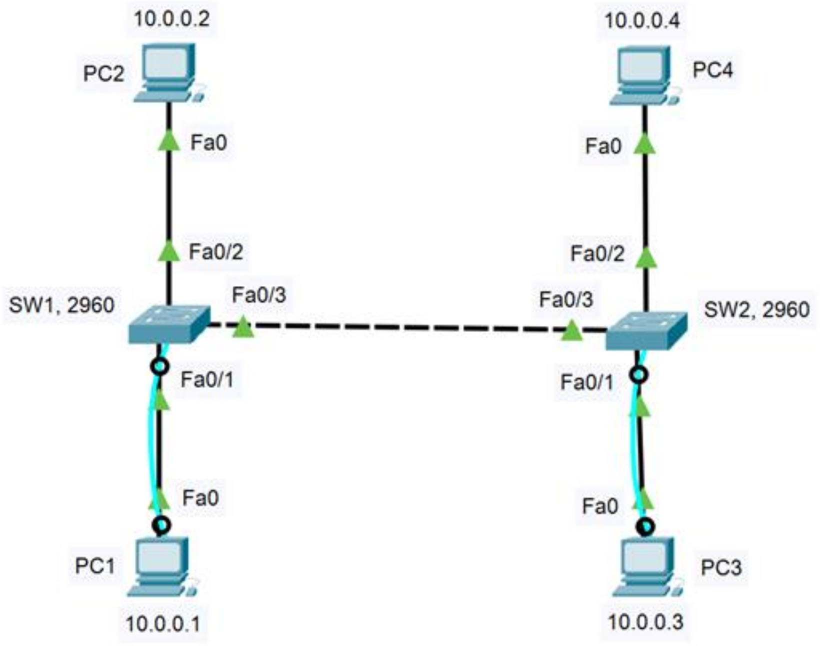


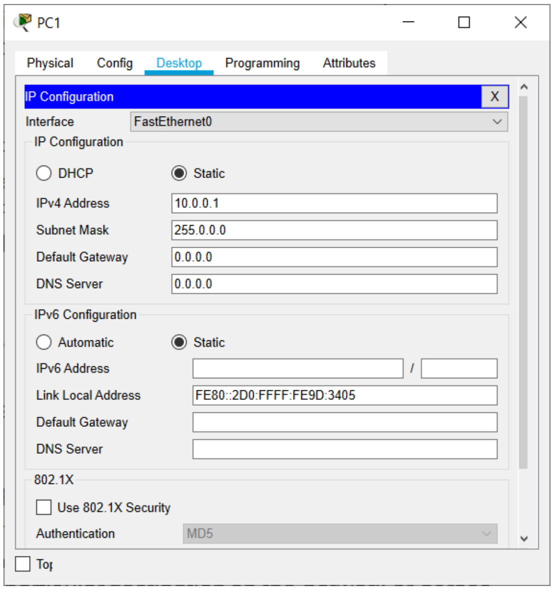
Figure 1 Topology of the Ethernet LAN network

Procedure

1. In packet tracer construct the Ethernet LAN network shown in Figure 1.
2. Use the Cisco 2960 module for each of switches SW1 and SW2.
3. 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.
4. 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.
5. Connect the Fa0/3 ports of SW1 and SW2 using a copper cross-over cable.
6. To console from PC1 to SW1 connect a console cable from the RS232 connector of PC1 to the Console port of SW1.
7. To console from PC3 to SW2 connect a console cable from the RS232 connector of PC3 to the Console port of SW2.
8. Notice that the IP address of the NIC of each PC is indicated in the figure.
9. Also, the IP addresses of the administrative VLAN 1 of SW1 and SW2 are indicated in the figure.

Configuring the devices

1. Click on **PC1** and in the **Desktop** tab open the **IP Configuration** application.
2. Make sure that the **Static** IP address is chosen.
3. Enter the IP address **10.0.0.1 of PC1** and notice that the mask will be set to **255.0.0.0.** (Figure 2)
4. You can change the Display Name of the PC in the **Config** tab.
5. **Repeat** the same procedure to configure the IP addresses of PC2, PC3, and PC4.
6. Make sure that the display name of each PC **matches** Fig. 1



IP Configuration

Interface: FastEthernet0

IP Configuration

○ DHCP ● Static

IPv4 Address: 10.0.0.1

Subnet Mask: 255.0.0.0

Default Gateway: 0.0.0.0

DNS Server: 0.0.0.0

IPv6 Configuration

○ Automatic ● Static

IPv6 Address: /

Link Local Address: FE80::2D0:FFFF:FE9D:3405

Default Gateway:

DNS Server:

802.1X

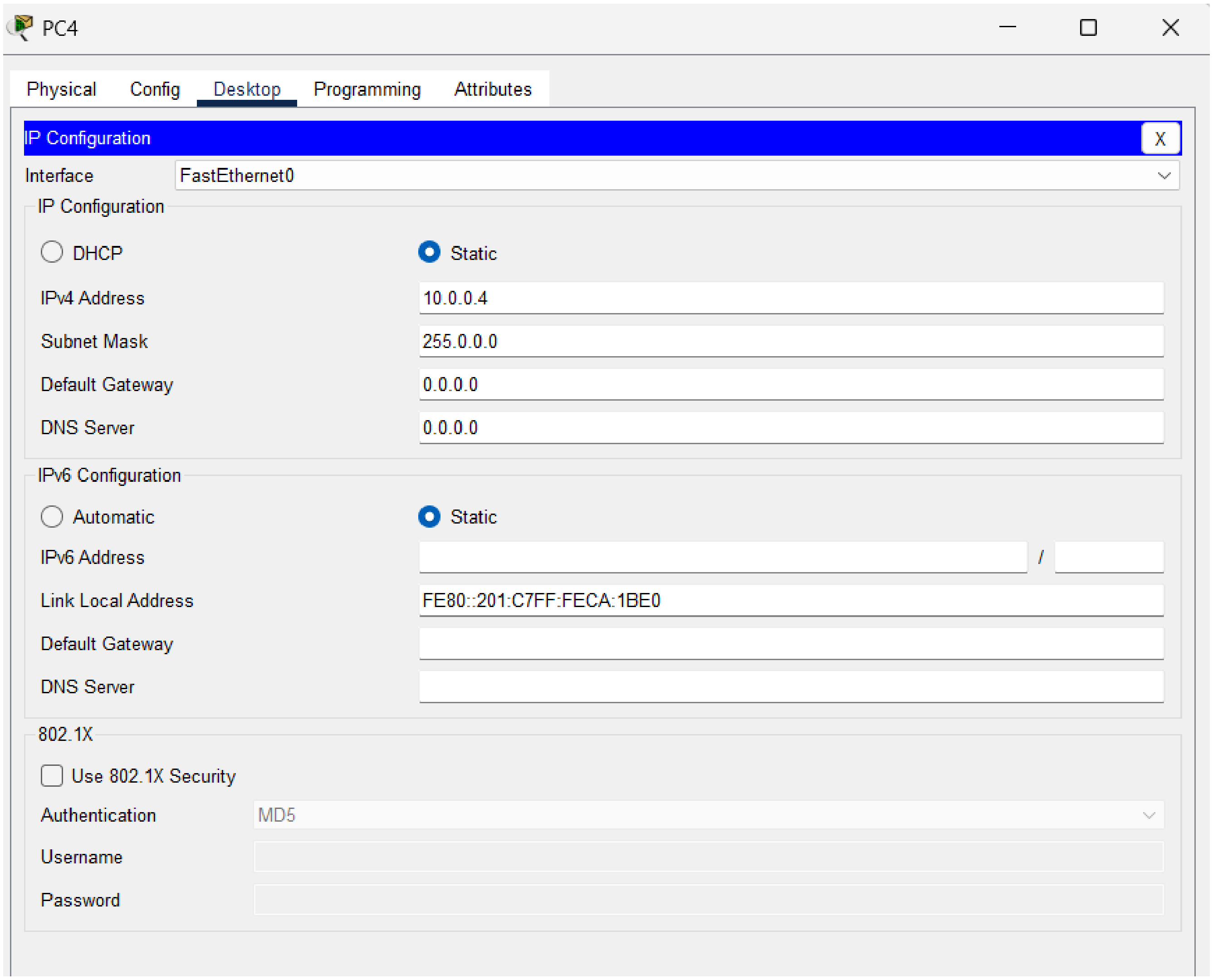
□ Use 802.1X Security

Authentication: MD5

□ Top

Figure 2 Configuring the IP address of PC1.

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



Interface: FastEthernet0

IP Configuration

○ DHCP ● Static

IPv4 Address	10.0.0.4
Subnet Mask	255.0.0.0
Default Gateway	0.0.0.0
DNS Server	0.0.0.0

IPv6 Configuration

○ Automatic ● Static

IPv6 Address	/
Link Local Address	FE80::201:C7FF:FECA:1BE0
Default Gateway	
DNS Server	

802.1X

□ Use 802.1X Security

Authentication	MD5
Username	
Password	

Figure 3 Configuring the IP address of PC4.

7. Click on each **switch**, then the Config Tab, you will see:
   i. Display Name
   ii. Host name
8. Change the Display Name of the switches into SW1 and SW2 as shown in Fig.1 (note that the **display name** is the one that is shown on **packet tracer** while the ***Hostname*** is the one used with the ***CLI*** commands)
9. Open the Command Prompt under Desktop of each PC and execute the command:

```
C:\>ipconfig /all
```

Figure out the MAC address (also called the Physical Address) of the NIC (FastEthernet0) of each PC and list the results in Table 1.

Table 1 MAC addresses of FastEthernet0 NIC of the PCs.

Host	MAC address of Fa0
PC1	**0050.0F72.285A**
PC2	**000C.CFE1.385A**
PC3	**00D0.9789.C268**
PC4	**0001.C7CA.1BE0**

Command-Line Interface (CLI) of CISCO devices

The command-line interface (CLI) of a switch may be accessed on Packet Tracer in two ways:

- Through the **CLI** Tab of the CISCO device (switch or router)
- Through a PC by connecting the serial port (referred to as the **RS232**) of the PC to the **console** port of the CISCO device using a console cable (a Cisco proprietary cable).

In real physical devices, we have only **one option**, that is through the console cable but on packet tracer, we have three ways to configure devices:

1. The **Config** Tab.
2. The **CLI** Tab.
3. The **Console** port when connected to any PC.

When using the Console port, a **terminal emulation program** such as “Tera Term” or “PuTTY” must be used to start the console session. This type of access to the CLI of a networking device is referred to as **out-of-band access**.

Procedure of using the Console Port

1. On PC1, click on Desktop then **Terminal**.
2. Keep the default parameters, click OK, this will take you to the user execute level of the Switch. Press Enter to get started

```
Switch>
```

a) Enter the command “enable” to alleviate the switch prompt to the privileged mode:

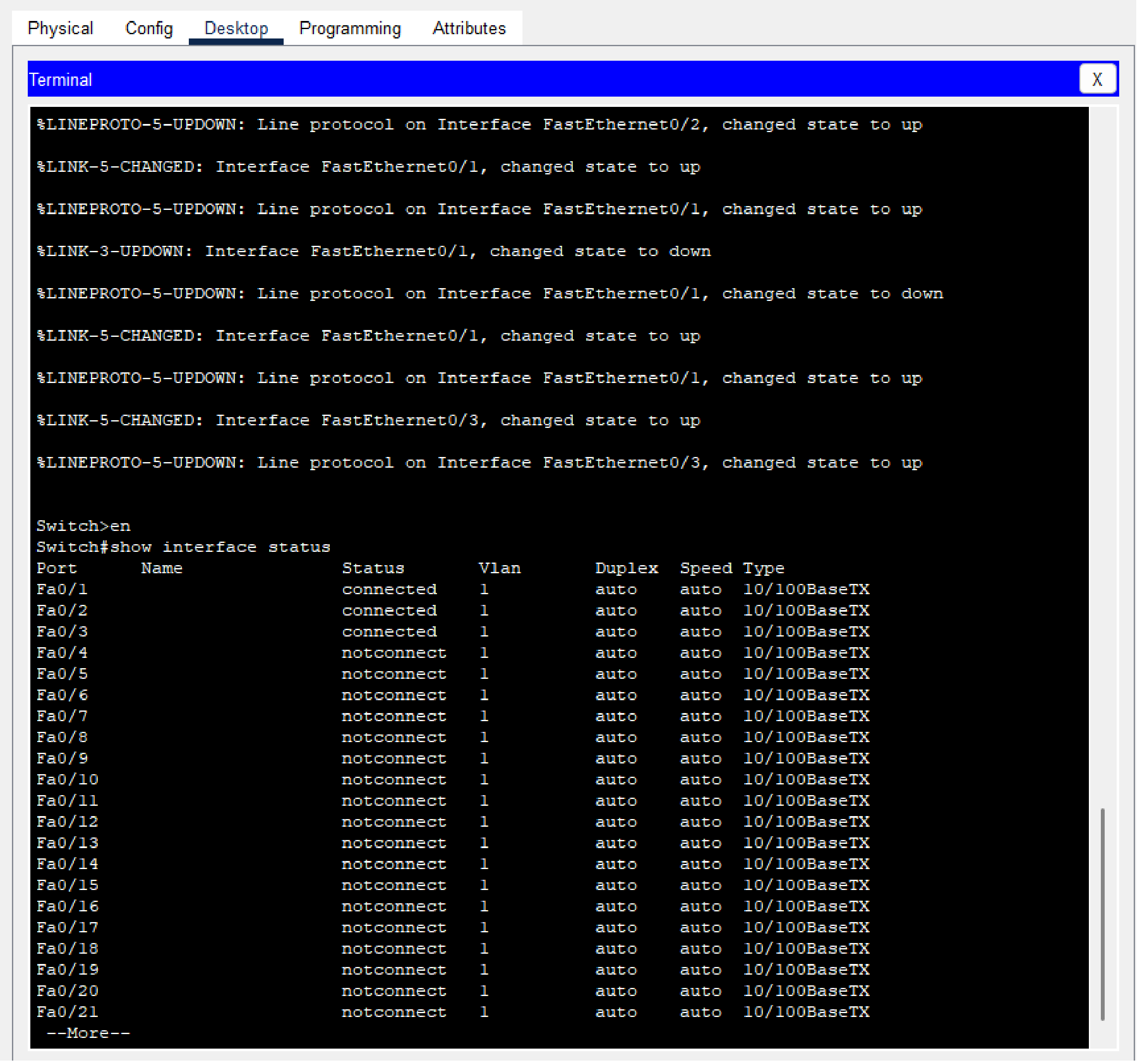
```
Switch>enable
Switch#
```

b) 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 for the output of the above command. Indicate (in red) which interfaces of the switch are connected.

Answer: Fa0/1, Fa0/2, Fa0/3.



```
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/2, changed state to up

%LINK-5-CHANGED: Interface FastEthernet0/1, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed state to up

%LINK-3-UPDOWN: Interface FastEthernet0/1, changed state to down

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed state to down

%LINK-5-CHANGED: Interface FastEthernet0/1, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed state to up

%LINK-5-CHANGED: Interface FastEthernet0/3, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/3, changed state to up


Switch>en
Switch#show interface status
Port      Name               Status       Vlan       Duplex  Speed Type
Fa0/1                        connected    1          auto    auto  10/100BaseTX
Fa0/2                        connected    1          auto    auto  10/100BaseTX
Fa0/3                        connected    1          auto    auto  10/100BaseTX
Fa0/4                        notconnect   1          auto    auto  10/100BaseTX
Fa0/5                        notconnect   1          auto    auto  10/100BaseTX
Fa0/6                        notconnect   1          auto    auto  10/100BaseTX
Fa0/7                        notconnect   1          auto    auto  10/100BaseTX
Fa0/8                        notconnect   1          auto    auto  10/100BaseTX
Fa0/9                        notconnect   1          auto    auto  10/100BaseTX
Fa0/10                       notconnect   1          auto    auto  10/100BaseTX
Fa0/11                       notconnect   1          auto    auto  10/100BaseTX
Fa0/12                       notconnect   1          auto    auto  10/100BaseTX
Fa0/13                       notconnect   1          auto    auto  10/100BaseTX
Fa0/14                       notconnect   1          auto    auto  10/100BaseTX
Fa0/15                       notconnect   1          auto    auto  10/100BaseTX
Fa0/16                       notconnect   1          auto    auto  10/100BaseTX
Fa0/17                       notconnect   1          auto    auto  10/100BaseTX
Fa0/18                       notconnect   1          auto    auto  10/100BaseTX
Fa0/19                       notconnect   1          auto    auto  10/100BaseTX
Fa0/20                       notconnect   1          auto    auto  10/100BaseTX
Fa0/21                       notconnect   1          auto    auto  10/100BaseTX
 --More--
```

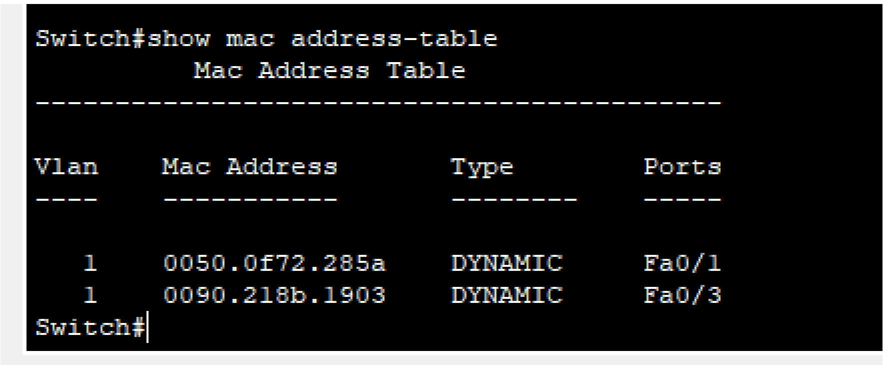
Figure 4 Status of the Interfaces of SW1.

Also, check the status of the interfaces of SW2.

c) 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.



```
Switch#show mac address-table
          Mac Address Table
-------------------------------------------

Vlan    Mac Address       Type        Ports
----    -----------       --------    -----

   1    0050.0f72.285a    DYNAMIC     Fa0/1
   1    0090.218b.1903    DYNAMIC     Fa0/3
Switch#
```

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 (in red) why:

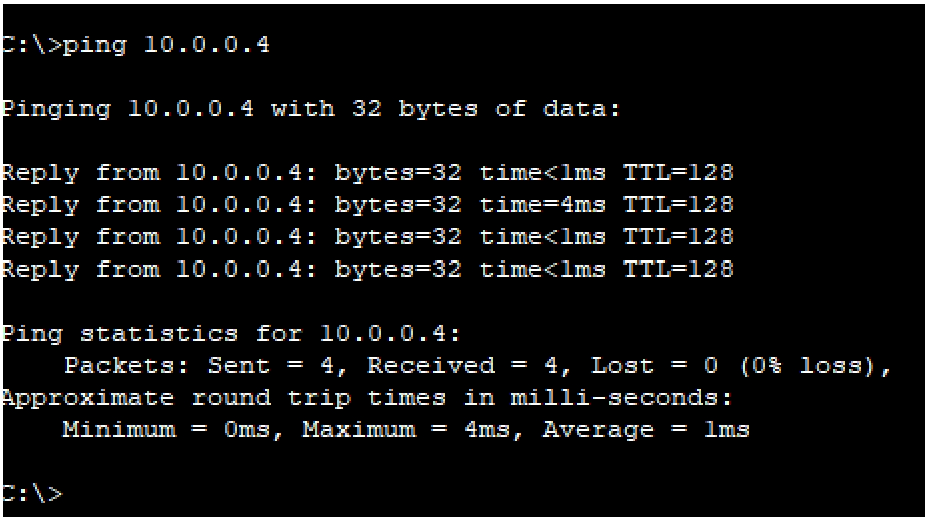
Answer: This is because, we did not test the connection(ping with other PCs), therefore, for MAC address of a computer to be determined or found there must be packets sent between the compiuters, or in case of traffic of the packets

Also, repeat the same practice of this step to SW2.

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

C:\>ping 10.0.0.2

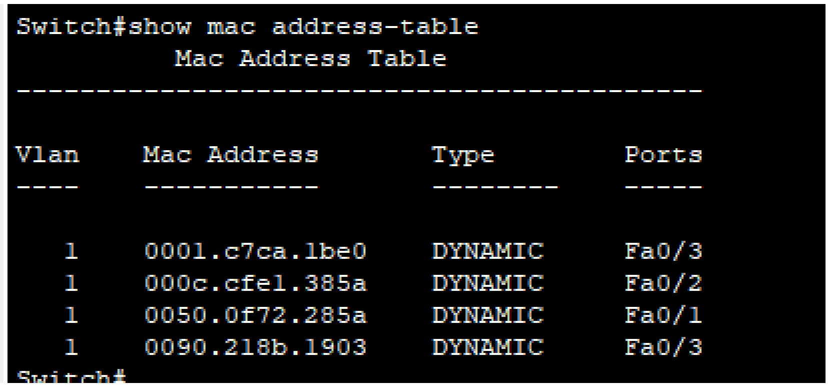
Below in Figure 6 insert an image for the result of the ping operation from PC1 to PC4.



```
C:\>ping 10.0.0.4

Pinging 10.0.0.4 with 32 bytes of data:

Reply from 10.0.0.4: bytes=32 time<1ms TTL=128
Reply from 10.0.0.4: bytes=32 time=4ms TTL=128
Reply from 10.0.0.4: bytes=32 time<1ms TTL=128
Reply from 10.0.0.4: bytes=32 time<1ms TTL=128

Ping statistics for 10.0.0.4:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 4ms, Average = 1ms

C:\>
```

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.



```
Switch#show mac address-table
          Mac Address Table
-------------------------------------------

Vlan    Mac Address       Type        Ports
----    -----------       --------    -----

   1    0001.c7ca.1be0    DYNAMIC     Fa0/3
   1    000c.cfe1.385a    DYNAMIC     Fa0/2
   1    0050.0f72.285a    DYNAMIC     Fa0/1
   1    0090.218b.1903    DYNAMIC     Fa0/3
Switch#
```

Figure 7 MAC address table of SW1.

Also inspect the MAC address table of SW2. Are the MAC addresses of the PCs in the CAM tables of SW1 and SW2 identical to those in Table 1?

Answer [Yes/No]: No

Briefly explain (in red) below what happened in terms of the address resolution protocol (ARP) that yield giving the entries of the MAC addresses of the host computers associated with the port labels of the two switches:

Answer: Each time you ping from one computer to another, the MAC addresses changes, therefore MAC addresses being different.

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

Answer: VLAN 1

e) In the CLI of SW1 enter into the global configuration mode:

```
Switch#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#
```

f) Set the hostname of the switch to SW1:

```
Switch(config)#hostname SW1
SW1(config)#
```

When you mistype a command in the CLI of a networking device the DNS name resolution process attempts to resolve the hostname which is the mistyped command into an IP address. This will make you wait for a minute of delay due to the error.

g) Therefore, to disable the DNS resolution process enter the command:

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

h) Configure "**cisco**" as the old plain text password to limit 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 execute mode.

i) Enter the command "enable" and notice that you will be prompted to enter the password. In this case, enter the password "**cisco**" to get into the privileged mode.

j) Configure "**class**" as the new encrypted password to limit 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 execute mode.

k) Enter the command “enable” and notice that you will be prompted to enter the 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.

l) Configure a password called “**conpass**” to limit 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. Also to get into the privileged mode you will need to enter the “class” encrypted password as before.

m) To see all these details, display the running configuration of the switch

```
SW1# show run
Building configuration...

Current configuration : 1151 bytes (vary depending on device)
!
version 15.0
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
!
hostname SW1
!
enable secret 5 $1$mERr$9cTjUIEqNGurQiFU.ZeCi1
enable password cisco
!
!
!
!
Other lines omitted
```

Notice that the enable password is shown as **cisco** while the secret password is **encrypted**. When you have both passwords, the secret password will overwrite the enabled password.

n) Run the show run command again and keep clicking on the space bar until you reach the end of the running configuration.

```
SW1# show run
!
!
interface Vlan1
no ip address
shutdown
!
!
!
!
line con 0
password conpass
login
!
line vty 0 4
login
line vty 5 15
login
!
!
!
!
end
```

Notice the line **console** password shown at the end of the running configuration.

Deleting and Modifying Passwords

To change any password on CISCO switches and routers, you must delete the old one and then create a new one.

1. Delete the enable plain text password as follows:

```
SW1(config)#no enable password
```

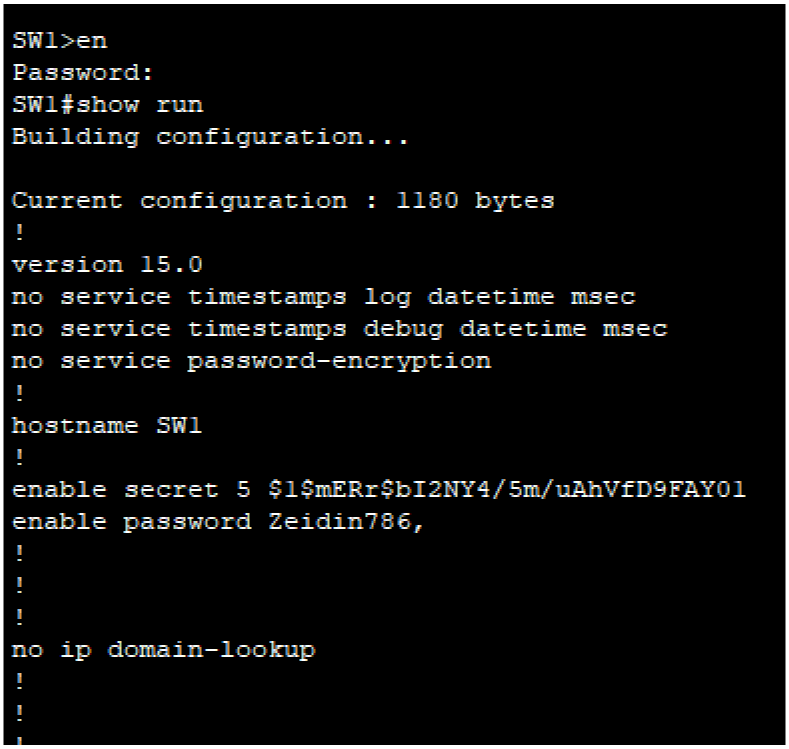
2. Delete the enable encrypted password as follows:

SW1(config)#no enable secret

3. Delete the Console password as follows:

   SW1(config)#line con 0
   SW1(config-line)#no password
   SW1(config-line)#exit

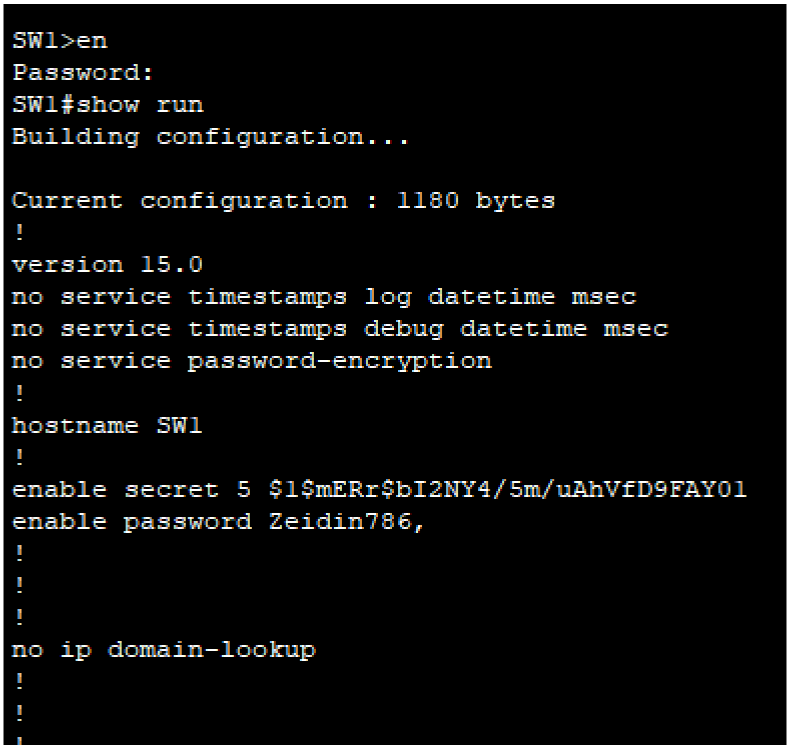
4. Create a **plain** text password to limit access to the privileged mode, let it be after your **first** name.
5. Create a **console** password to limit access to the console session, let it be after your **last** name.
6. Apply the show running configuration command
7. Take a screenshot of the part showing the privileged mode password and insert it in Fig. 8 below:



```
SW1>en
Password:
SW1#show run
Building configuration...

Current configuration : 1180 bytes
!
version 15.0
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
!
hostname SW1
!
enable secret 5 $1$mERr$bI2NY4/5m/uAhVfD9FAY01
enable password Zeidin786,
!
!
!
no ip domain-lookup
!
!
```

Figure 8 Running Configuration of SW1 showing plain text PWD.

8. Take a screenshot of the part showing the console session password and insert it in Fig. 9 below:



```
SW1>en
Password:
SW1#show run
Building configuration...

Current configuration : 1180 bytes
!
version 15.0
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
!
hostname SW1
!
enable secret 5 $1$mERr$bI2NY4/5m/uAhVfD9FAY01
enable password Zeidin786,
!
!
!
no ip domain-lookup
!
!
```

Figure 9 Running Configuration of SW1 showing console PWD.