Lab-9: Objective:

Part-A: Configure Port Security on Layer 2 switch.

Part B: Configure Switch Security on given network.

Lab-9
Port Security& Switch Security

Part-A: Configure Port Security on Layer 2 switch for this given network in figure 20.All the attached users are secured while any unauthorized users should be restricted to enter in network. What do you see when you use the command Show Port-Security and Show Port-Security Interface fa 0/1 (as an example)?

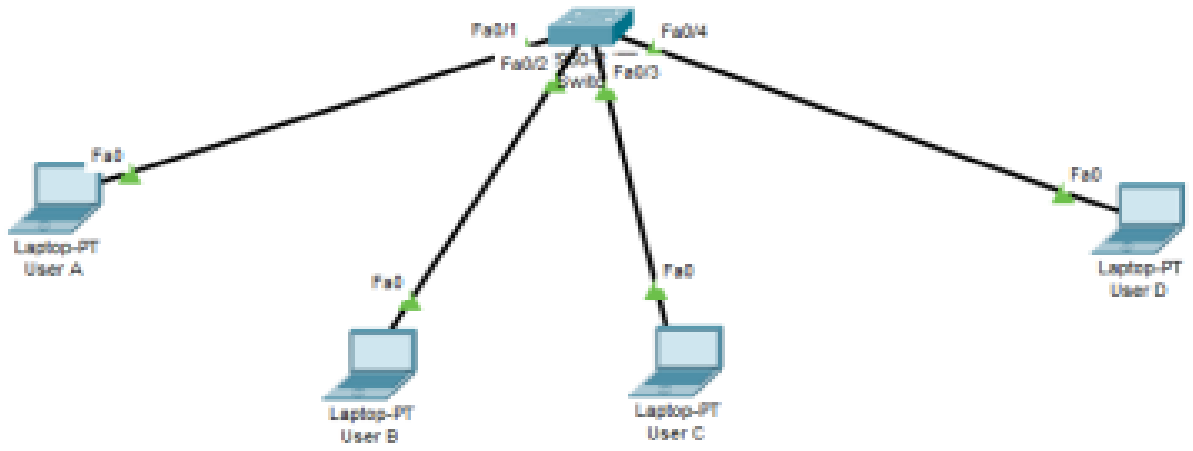

Figure 20

Port Security

Attacker's task is comparatively very easy when they can enter the network they want to attack. Ethernet LANs are very much vulnerable to attack as the switch ports are open to use by

default. Various attacks such as Dos attack at layer 2, address spoofing can take place. If the administrator has control over the network then obviously the network is safe. To take total control over the switch ports, user can use feature called port-security. If somehow prevent an unauthorized user to use these ports, then the security will increase up to a great extent at layer 2.

User can secure a port in two steps:

1. Limiting the number of MAC addresses to a single switch port, i.e if more than the limits, Mac addresses are learned from a single port then appropriate action will be taken.
2. If an unauthorized access is observed, the traffic should be discarded by using any of the options or more appropriate, user should generate a log message so that unauthorized access can be easily observed.

Switches learn MAC addresses when the frame is forwarded through a switch port. By using port security, user can limit the number of MAC addresses that can be learned to a port, set static MAC addresses and set penalties for that port if it is used by an unauthorized user. User can either use restrict, shut down or protect port-security commands.

Task 1, Configure Port Securityon Layer 2 switch

Switch>enable

Switch# configure terminal

Switch (config)#interface range fa 0/1-4

Switch (config-if-range)# switchport mode access

Switch (config-if-range)# switchport port-security

Switch (config-if-range)# switchport port-security maximum 1

Switch (config-if-range)# switchport port-security mac-address sticky

Switch (config-if-range)# switchport port-security violation shutdown

Switch (config-if-range)#exit

Task 2, Tables before violation by any unauthorized user

(Refer Figure 21, 22):

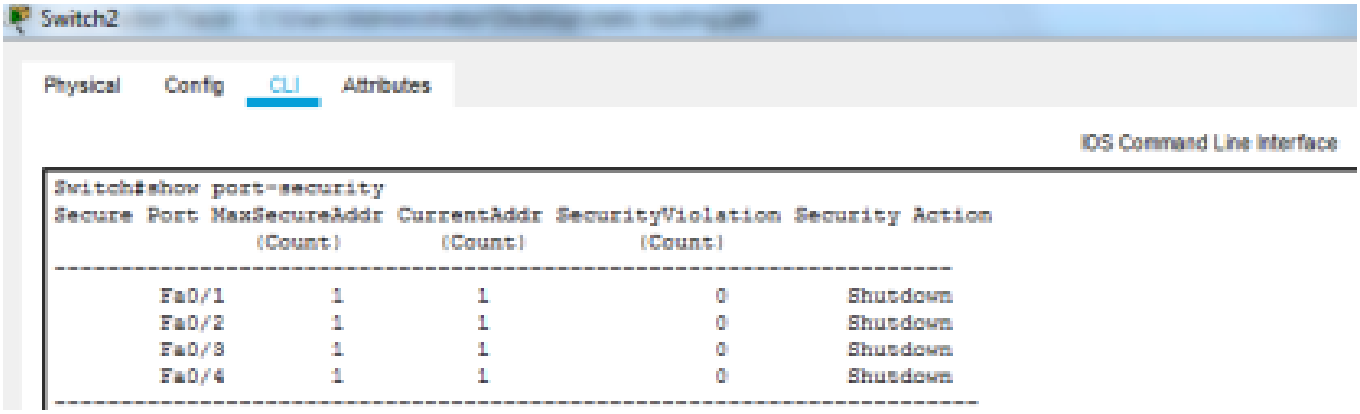

Figure 21

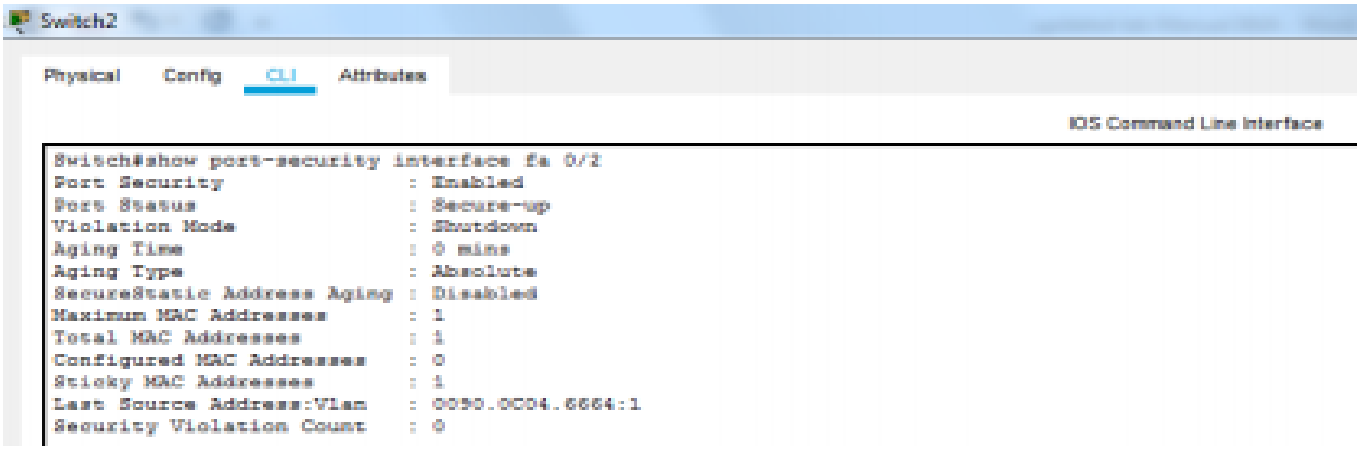

Figure 22

After violation by unauthorized user

(Refer Figure 23, 24, 25):

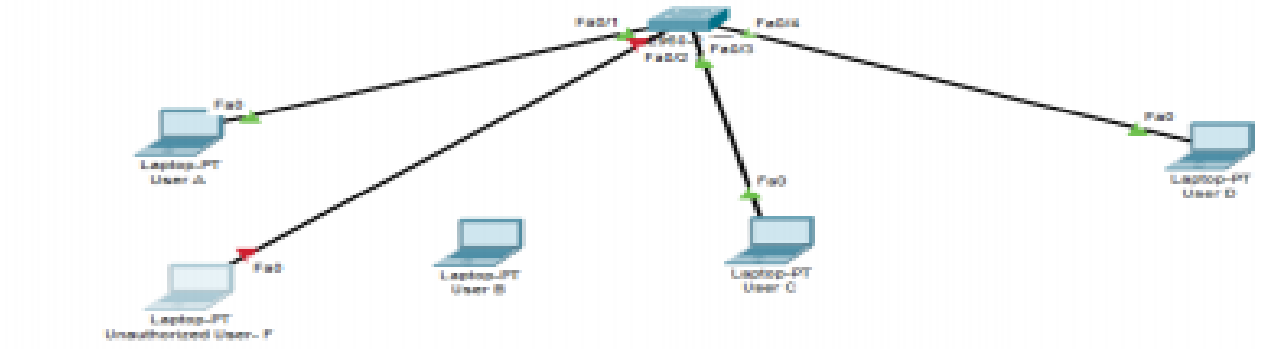

Figure 23

Tables after violation by unauthorized user F on Fast Ethernet 0/2:

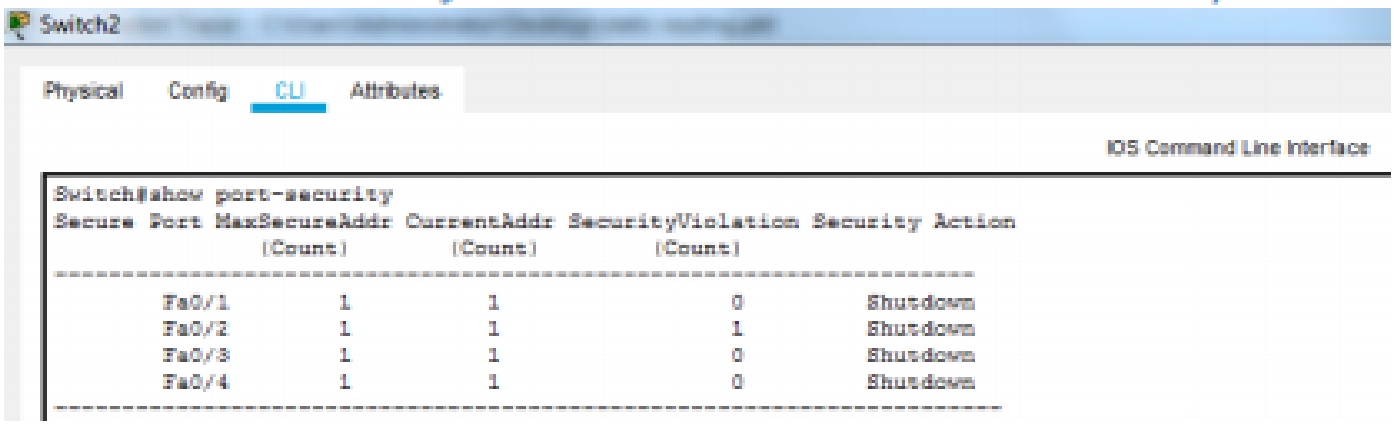

Figure 24

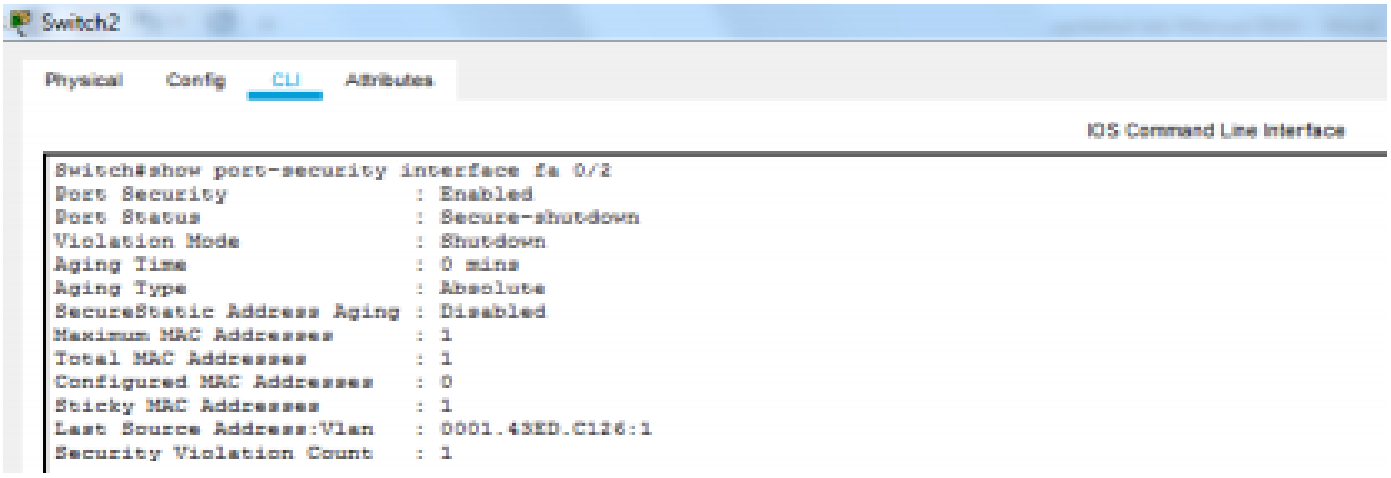

Figure 25

Switch Security

Part B: Configure Switch Security on given network in figure 26, at the end of the configuration, all the unused ports should be secured from any unauthorized access.

Addressing Table

Device	Interface	IP Address	Subnet Mask
S1	VLAN99	172.17.99.11	255.255.255.0
PC1	NIC	172.17.99.21	255.255.255.0
PC2	NIC	172.17.99.32	255.255.255.0

Learning Objectives

- Configure basic switch management
- Configure dynamic port security
- Test dynamic port security
- Secure unused ports

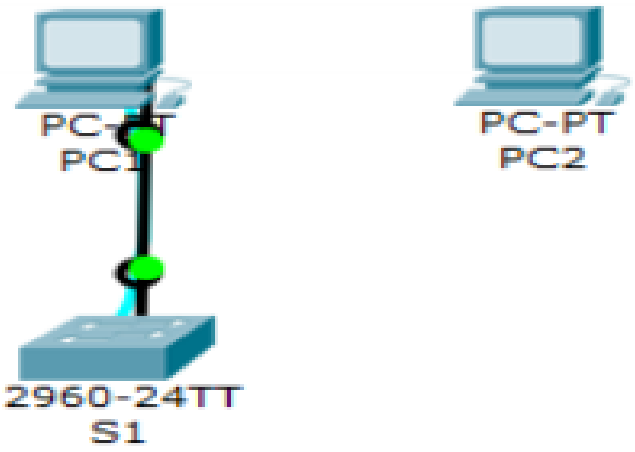

Figure 26

Switch Security

When you take a new switch out of the box, the first thing the network engineer does is secure the switch and assign it an IP address, subnet mask, and default gateway so the switch can be managed from a remote location.

Secure Remote Access

There are different methods that can be used to secure a switch including Telnet and SSH. Telnet has already been covered, but SSH is a much better method used to securely manage the switch from a remote location.

SSH Operation

Secure Shell (SSH) is a protocol that provides a secure (encrypted) management connection to a remote device. SSH should replace Telnet for management connections. Telnet is an older protocol that uses insecure plaintext transmission of both the login authentication (username and password) and the data transmitted between the communicating devices. SSH provides security for remote connections by providing strong encryption when a device is authenticated (username and password) and also for the transmitted data between the communicating devices. SSH is assigned to TCP port 22. Telnet is assigned to TCP port 23.

Task 1, Configure Basic Switch Management

Step 1. From PC1, access the console connection to S1.

- Click PC1 and then the Desktop tab. Select Terminal in the Desktop tab.
- Keep these default settings for Terminal Configuration and then click OK:
  - Bits Per Second = 9600
  - Data Bits = 8
  - Parity = None
  - Stop Bits = 1
  - Flow Control = None
- You are now consoled into S1. Press Enter to get the Switch prompt.

Step 2. Change to privileged EXEC mode.

To access privileged EXEC mode, type the **enable** command.

S1>**enable**

S1#

Notice how you were able to enter privileged EXEC mode without providing a password. Why is the lack of a privileged EXEC mode password a security threat?

Step 3. Change to global configuration mode and configure the privileged EXEC password.

- While in privileged EXEC mode, you can access global configuration mode by using the **configure terminal** command.
- Use the **enable secret** command to set the password. For this activity, set the password to **class**.

S1#**configure terminal**

Enter configuration commands, one per line. End with CNTL/Z.

S1(config)#**enable secret class**

S1(config)#

Note: PT will not grade the **enable secret** command.

Step 4. Configure virtual terminal and console passwords and require users to login.

A password should be required to access the console line. Even the basic user EXEC mode can provide significant information to a malicious user. In addition, the vty lines must have a password before users can access the switch remotely.

- Access the console prompt using the **line console 0** command.
- Use the **password** command to configure the console and vty lines with **cisco** as the password. Note: PT will not grade the **password cisco** command in this case.
- Then enter the **login** command, which requires users to enter a password before gaining access to user EXEC mode.
- Repeat the process with the vty lines. Use the **line vty 0 15** command to access the correct prompt.
- Type the **exit** command to return to the global configuration prompt.

S1(config)#**line console 0**

S1(config-line)#**password cisco**

S1(config-line)#**login**

S1(config-line)#**line vty 0 15**

S1(config-line)#**password cisco**

S1(config-line)#**login**

S1(config-line)#**exit**

S1(config)#

Step 5. Configure password encryption.

The privileged EXEC password is already encrypted. To encrypt the line passwords that you just configured, enter the **service password-encryption** command in global configuration mode.

S1(config)#**service password-encryption**

S1(config)#

Step 6. Configure and test the MOTD banner.

Configure the message-of-the-day (MOTD) using **Authorized Access Only** as the text. The banner text is case sensitive. Make sure you do not add any spaces before or after the banner text. Use a delimiting character before and after the banner text to indicate where the text

begins and ends. The delimiting character used in the example below is **&**, but you can use any character that is not used in the banner text. After you have configured the MOTD, log out of the switch to verify that the banner displays when you log back in.

S1(config)#**banner motd&Authorized Access Only&**

S1(config)#**end[**or **exit]**

S1#**exit**

S1 con0 is now available

Press RETURN to get started.

[Enter]

Authorized Access Only

User Access Verification

Password:

- The password prompt now requires a password to enter user EXEC mode. Enter the password **cisco**.
- Enter privileged EXEC mode with the password **class** and return to global configuration mode with the **configure terminal** command.

Password: **[cisco]** !Note: Password does not display as you type.

S1>**enable**

Password: **[class]** !Note: Password does not display as you type.

S1#**configure terminal**

Enter configuration commands, one per line. End with CNTL/Z.

S1(config)#

Step 7. Check results.

Your completion percentage should be 40%. If not, click **Check Results** to see which required components are not yet completed.

Task 2, Configure Dynamic Port Security

Step 1. Enable VLAN99.

Packet Tracer opens with the VLAN 99 interface in the down state, which is not how an actual switch operates. You must enable VLAN 99 with the **no shutdown**command before the interface becomes active in Packet Tracer.

S1(config)**#interface vlan 99**

S1(config-if)**#no shutdown**

Step 2. Enter interface configuration mode for FastEthernet 0/18 and enable port security.

Before any other port security commands can be configured on the interface, port security must be enabled.

S1(config-if)**#interface fa0/18**

S1(config-if)**#switchport access Vlan99**

S1(config-if)**#switchport mode access**

S1(config-if)**#switchport port-security**

Notice that you do not have to exit back to global configuration mode before entering interface configuration mode for fa0/18.

Step 3. Configure the maximum number of MAC addresses.

To configure the port to learn only one MAC address, set the **maximum** to **1**:

S1(config-if)**#switchport port-security maximum 1**

Note: PT does not grade the **switchport port-security maximum 1** command, however this command is vital in configuringport security.

Step 4. Configure the port to add the MAC address to the running configuration.

The MAC address learned on the port can be added to ("stick" to) the running configuration for that port.

S1(config-if)**#switchport port-security mac-address sticky**

Note: PT does not grade the **switchport port-security mac-address sticky** command, however this command is vital in configuring port security.

Step 5. Configure the port to automatically shut down if port security is violated.

If you do not configure the following command, S1 only logs the violation in the port security statistics but does not shut down the port.

S1(config-if)**#switchport port-security violation shutdown**

Note: PT does not grade the **switchport port-security violation shutdown** command, however this command is vital in configuring port security.

Step 6. Confirm that S1 has learned the MAC address for PC1.

Ping from PC1 to S1.

Confirm that S1 now has static MAC address entry for PC1 in the MAC table:

S1#show mac-address-table

Mac Address Table

Vlan	Mac Address	Type	Ports
99	0060.5c5b.cd23	STATIC	Fa0/18

The MAC address is now "stuck" to the running configuration.

S1#show running-config

<output omitted>
interface FastEthernet0/18
switchport access vlan 99
switchport mode access
switchport port-security
switchport port-security mac-address sticky
switchport port-security mac-address sticky 0060.5C5B.CD23
<output omitted>
S1#

Step 7. Check results.

Your completion percentage should be 70%. If not, click **Check Results** to see which required components are not yet completed.

Task 3, Test Dynamic Port Security

Step 1. Remove the connection between PC1 and S1 and connect PC2 to S1.

- To test port security, delete the Ethernet connection between PC1 and S1. If you accidentally delete the console cable connection, simply reconnect it.
- Connect PC2 to Fa0/18 on S1. Wait for the amber link light to turn green and then ping from PC2 to S1. The port should then automatically shut down.

Step 2. Verify that port security is the reason the port is shut down.

To verify that port security has shut the port down, enter the command **show interface fa0/18**.

S1#show interface fa0/18

FastEthernet0/18 is down, line protocol is down (err-disabled)

Hardware is Lance, address is 0090.213e.5712 (bia 0090.213e.5712)

<output omitted>

The line protocol is down because of an error (**err**) of accepting a frame with a different MAC address than the learned MAC address, so the Cisco IOS software shut down (**disabled**) the port.

You can also verify a security violation with the **show port-security interface fa0/18** command.

```
S1#show port-security interface fa0/18
Port Security              : Enabled
Port Status                : Secure-shutdown
Violation Mode             : Shutdown
Aging Time                 : 0 mins
Aging Type                 : Absolute
SecureStatic Address Aging : Disabled
Maximum MAC Addresses      : 1
Total MAC Addresses        : 1
Configured MAC Addresses   : 1
Sticky MAC Addresses       : 0
Last Source Address:Vlan   : 00E0.F7B0.086E:99
Security Violation Count   : 1
```

Notice that the Port Status is **secure-shutdown**, and the security violation count is **1**.

Step 3. Restore the connection between PC1 and S1 and reset port security.

Remove the connection between PC2 and S1. Reconnect PC1 to the Fa0/18 port on S1. Notice that the port is still down even though you reconnected the PC that is allowed on the port. A port that is in the down state because of a security violation must be manually reactivated. Shut down the port and then activate it with **no shutdown**.

```
S1#config t

Enter configuration commands, one per line.  End with CNTL/Z.

S1(config)#interface fa0/18

S1(config-if)#shutdown

%LINK-5-CHANGED: Interface FastEthernet0/18, changed state to administratively down

S1(config-if)#no shutdown

%LINK-5-CHANGED: Interface FastEthernet0/18, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/18, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan99, changed state to up

S1(config-if)#exit
```

S1(config)#

Step 4. Test connectivity by pinging S1 from PC1.

The ping from PC1 to S1 should be successful.

Your completion percentage should still be 70% at the end of this task.

Task 4, Secure Unused Ports

A simple method many administrators use to help secure their network from unauthorized access is to disable all unused ports on a network switch.

Step 1. Disable interface Fa0/17 on S1.

Enter interface configuration mode for FastEthernet 0/17 and shut down the port.

S1(config)**#interface fa0/17**

S1(config-if)**#shutdown**

Step 2. Test the port by connecting PC2 to Fa0/17 on S1.

Connect PC2 to the Fa0/17 interface on S1. Notice that the link lights are red. PC2 does not have access to the network.

Lab-9 Exercise:

Configure Port Security on Layer 2 switch. You have to attach 8 users with this switch. Any unauthorized user should be restricted to enter the network. What do you see when you use the command Show Port-Security and Show Port-Security on specific interfaces? How can you save unused ports in this environment?