Alan Palayil
ECE 407

ECE 407

Introduction to Computer Networks Laboratory

Practice 4 – Switching table and Switch Security

Objectives

The goal of this experiment is to:

1. Familiarize students with switching and switching table learning algorithms.
2. Familiarize students with switch security features.

Background

Every device on an Ethernet LAN is identified by a Layer 2 MAC address. This address is assigned by the manufacturer and stored in the firmware of the NIC. The purpose of a Layer 2 LAN switch is to deliver Ethernet frames to host devices on the local network. The switch records host MAC addresses that are visible on the network, and maps those MAC addresses to its own Ethernet switch ports. This process is called building the MAC address table. When a switch receives a frame from a PC, it examines the frame's source and destination MAC addresses. The source MAC address is recorded and mapped to the switch port from which it arrived. Then the destination MAC address is looked up in the MAC address table. If the destination MAC address is a known address, then the frame is forwarded out of the corresponding switch port associated with that MAC address. If the MAC address is unknown, then the frame is broadcasted out of all switch ports, except the one from which it came. It is important to observe and understand the function of a switch and how it delivers data on the network. Switches are used to interconnect and deliver information to computers on local area networks. Switches deliver Ethernet frames to host devices identified by network interface card MAC addresses. The way a switch operates has implications for network administrators whose job it is to ensure secure and consistent network communication.

Cisco switches can be configured with a special IP address known as the switch virtual interface (SVI). The SVI, or management address, can be used for remote access to the switch to display or configure settings. If the VLAN 1 SVI is assigned an IP address, by default all ports in VLAN 1 have access to the SVI IP address.

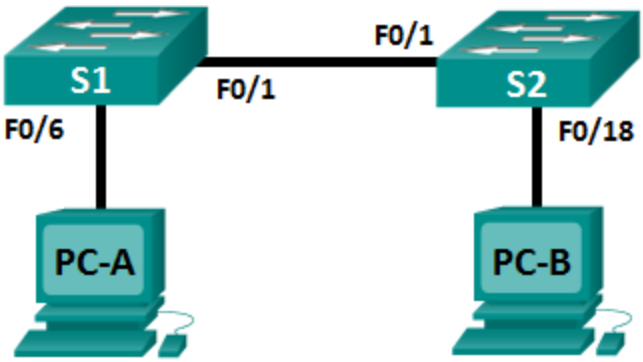
Exercises in this experiment are based on Cisco NetAcad Labs

It is quite common to lock down access and install strong security features on PCs and servers. It is important that your network infrastructure devices, such as switches and routers, are also configured with security features.

In this lab, you will follow some best practices for configuring security features on LAN switches. You will only allow SSH and secure HTTPS sessions. You will also configure and verify port security to lock out any device with a MAC address not recognized by the switch.

Exercise 1: The switch MAC address table (5.2.1.7)

Topology



Addressing Table

Device	Interface	IP Address	Subnet Mask
SVI-1	VLAN 1	192.168.1.11	255.255.255.0
SVI-2	VLAN 1	192.168.1.12	255.255.255.0
PC-A	NIC	192.168.1.3	255.255.255.0
PC-B	NIC	192.168.1.2	255.255.255.0

A. Build and configure the above network using Cisco Packet Tracer

Step 1: Cable the network according to the topology. Make sure to choose the correct cable type (straight-through/crossover).

Step 2: Configure PC hosts with the above IP addresses and subnet mask.

Step 3: Configure basic settings for each switch.

a. Configure device name as shown in the topology.

b. Configure IP address as listed in Addressing Table.

c. Assign **cisco** as the console and vty passwords.

d. Assign **class** as the privileged EXEC password.

B. Display, Describe, and Analyze Ethernet MAC Addresses

Every device on an Ethernet LAN has a MAC address that is assigned by the manufacturer and stored in the firmware of the NIC. Ethernet MAC addresses are 48-bits long. They are displayed using six sets of hexadecimal digits that are usually separated by dashes, colons, or periods. The following example shows the same MAC address using the three different notation methods:

00-05-9A-3C-78-00 00:05:9A:3C:78:00 0005.9A3C.7800

Note: MAC addresses are also called physical addresses, hardware addresses, or Ethernet hardware addresses.

You will issue commands to display the MAC addresses on a PC and a switch, and you will analyze the properties of each one.

Step 1: Analyze the MAC address for the PC-A NIC.

Before you analyze the MAC address on PC-A, look at an example from a different PC NIC. You can issue the **ipconfig /all** command to view the MAC address of your NIC. An example screen output is shown below. When using the **ipconfig /all** command, notice that MAC addresses are referred to as physical addresses. Reading the MAC address from left to right, the first six hex digits refer to the vendor (manufacturer) of this device. These first six hex digits (3 bytes) are also known as the organizationally unique identifier (OUI). This 3-byte code is assigned to the vendor by the IEEE organization. To find the manufacturer, you can use a tool like www.macvendorlookup.com or go to the IEEE web site to find the registered OUI vendor codes. The IEEE web site address for OUI information is http://standards.ieee.org/develop/regauth/oui/public.html. The last six digits are the NIC serial number assigned by the manufacturer.

a. Using the output from the **ipconfig /all** command, answer the following questions.

```
Ethernet adapter Local Area Connection:

   Connection-specific DNS Suffix  . :
   Description . . . . . . . . . . . : Intel(R) 82577LM Gigabit Network Connection
   Physical Address. . . . . . . . . : 5C-26-0A-24-2A-60
   DHCP Enabled. . . . . . . . . . . : No
   Autoconfiguration Enabled . . . . : Yes
   Link-local IPv6 Address . . . . . : fe80::b875:731b:3c7b:c0b1%10(Preferred)
   IPv4 Address. . . . . . . . . . . : 192.168.1.3(Preferred)
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 192.168.1.1
   DHCPv6 IAID . . . . . . . . . . . : 240920024
```

What is the OUI portion of the MAC address for this device?

5C-26-0A

What is the serial number portion of the MAC address for this device?

24-2A-60

Using the example above, find the name of the vendor that manufactured this NIC.

Dell Inc.

b. From the command prompt on PC-A, issue the **ipconfig /all** command and identify the OUI portion of the MAC address for the NIC of PC-A.

A8-A1-59

Identify the serial number portion of the MAC address for the NIC of PC-A.

53-97-34

Identify the name of the vendor that manufactured the NIC of PC-A.

ASRock Inc.

Step 2: Analyze the MAC address for the S1 F0/6 interface.

You can use a variety of commands to display MAC addresses on the switch.

a. Console into S1 and use the **show interfaces vlan 1** command to find the MAC address information. A sample is shown below. Use output generated by your switch to answer the questions.

S1# **show interfaces vlan 1**

Vlan1 is up, line protocol is up
Hardware is EtherSVI, address is 001b.0c6d.8f40 (bia 001b.0c6d.8f40)
Internet address is 192.168.1.1/24
MTU 1500 bytes, BW 1000000 Kbit/sec, DLY 10 usec,
reliability 255/255, txload 1/255, rxload 1/255
Encapsulation ARPA, loopback not set
Keepalive not supported
ARP type: ARPA, ARP Timeout 04:00:00
Last input never, output 00:14:51, output hang never
Last clearing of "show interface" counters never
Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0
Queueing strategy: fifo
Output queue: 0/40 (size/max)
5 minute input rate 0 bits/sec, 0 packets/sec
5 minute output rate 0 bits/sec, 0 packets/sec
0 packets input, 0 bytes, 0 no buffer
Received 0 broadcasts (0 IP multicasts)
0 runts, 0 giants, 0 throttles
0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored

34 packets output, 11119 bytes, 0 underruns

0 output errors, 2 interface resets

0 unknown protocol drops

0 output buffer failures, 0 output buffers swapped out

What is the MAC address for VLAN 1 on S1?

001b.0c6d.8f40

What is the MAC serial number for VLAN 1?

6d.8f40

What is the OUI for VLAN 1?

001b.0c

Based on this OUI, what is the name of the vendor?

Cisco Systems

What does bia stand for?

Burned in Address

Why does the output show the same MAC address twice?

It may change through a command within software. The original will stay stated in ().

b. Another way to display the MAC address on the switch is to use the **show arp** command. Use the **show arp** command to display MAC address information. This command maps the Layer 2 address to its corresponding Layer 3 address. A sample is shown below. Use output generated by your switch to answer the questions.

S1# **show arp**

Protocol	Address	Age (min)	Hardware Addr	Type	Interface
Internet	192.168.1.1	-	001b.0c6d.8f40	ARPA	Vlan1
Internet	192.168.1.3	0	5c26.0a24.2a60	ARPA	Vlan1

What Layer 2 addresses are displayed on S1?

S1 VLAN 1 and PC-A MAC Addresses

What Layer 3 addresses are displayed on S1?

S1 and PC-A IP Addresses.

C. Examine the Switch MAC Address Table

A switch learns MAC addresses and builds the MAC address table, as network devices initiate communication on the network.

Step 1: Record network device MAC addresses.

a. Open a command prompt on PC-A and PC-B and type **ipconfig /all**. What are the Ethernet adapter physical addresses?

PC-A MAC Address: 0060.5C59.4027

PC-B MAC Address: 00E0.8F08.B343

b. Console into switch S1 and S2 and type the **show interface F0/1** command on each switch. On the second line of command output, what are the hardware addresses (or burned-in address [bia])?

S-1 Fast Ethernet 0/1 MAC Address: 0cd9.96d2.3d81

S-2 Fast Ethernet 0/1 MAC Address: 0cd9.96d2.4581

Step 2: Display the switch MAC address table.

The goal is to console into switch S2 and view the MAC address table, both before and after running network communication tests with ping.

a. Establish a console connection to S2 and enter privileged EXEC mode.

b. In privileged EXEC mode, type the **show mac address-table** command and press Enter.

S2# **show mac address-table**

Even though there has been no network communication initiated across the network (i.e., no use of ping), it is possible that the switch has learned MAC addresses from its connection to the PC and the other switch.

Are there any MAC addresses recorded in the MAC address table?

Yes there is more than one recorded into the table.

What MAC addresses are recorded in the table? To which switch ports are they mapped and to which devices do they belong? Ignore MAC addresses that are mapped to the CPU.

0180.c200.0002, 0180.c200.0004, etc. They are MAC addresses learned through the first switched F0/1 port. The S1 F0/1 address and PC-A-MAC address are mapped to S2 F0/1.

If you had not previously recorded MAC addresses of network devices in Step 1, how could you tell which devices the MAC addresses belong to, using only the output from the **show mac address-table** command? Does it work in all scenarios?

This command shows the port that the MAC was learned on, it would work in most cases but not all. It can work in cases which identify which network device the MAC address belongs to, except in the case of multiple MAC which belong from the same port, this may happen within a switch-to-switch connection in which case all the MAC addresses are shared between the two.

How many dynamic addresses are there? 1

How many MAC addresses are there in total? 24

Does the dynamic MAC address match the MAC address of PC-B? Yes

Step 3: List the show mac address-table options.

a. Display the MAC address table options.

S2# **show mac address-table ?**

How many options are available for the **show mac address-table** command? 12

b. Issue the **show mac address-table dynamic** command to display only the MAC addresses that were learned dynamically.

S2# **show mac address-table dynamic**

How many dynamic addresses are there? 1

c. View the MAC address entry for PC-B. The MAC address formatting for the command is xxxx.xxxx.xxxx.

S2# **show mac address-table address <PC-A MAC here>**

Step 4: Clear the S2 MAC address table and display the MAC address table again.

a. In privileged EXEC mode, type the **clear mac address-table dynamic** command and press **Enter**.

S2# **clear mac address-table dynamic**

b. Quickly type the **show mac address-table** command again. Does the MAC address table have any addresses in it for VLAN 1? Are there other MAC addresses listed?

Wait 10 seconds, type the **show mac address-table** command, and press Enter. Are there new addresses in the MAC address table? More than 20 addresses.

Step 5: From PC-B, ping the devices on the network and observe the switch MAC address table.

a. From PC-B, open a command prompt and type **arp -a**. Not including multicast or broadcast addresses, how many device IP-to-MAC address pairs have been learned by ARP?

It has no devices.

b. From the PC-B command prompt, ping PC-A, S1, and S2. Did all devices have successful replies? If not, check your cabling and IP configurations.

Yes

c. From a console connection to S2, enter the **show mac address-table** command. Has the switch added additional MAC addresses to the MAC address table? If so, which addresses and devices?

Yes there was one MAC address from the PC-A

From PC-B, open a command prompt and retype **arp -a**. Does the PC-B ARP cache have additional entries for all network devices that were sent pings?

Yes

Step 6: Set up a static MAC address.

a. Clear the MAC address table.

To remove the existing MAC addresses, use the **clear mac address-table dynamic** command in privileged EXEC mode.

S2# **clear mac address-table dynamic**

b. Verify that the MAC address table was cleared.

S2# **show mac address-table**

How many static MAC addresses are there? 11

How many dynamic addresses are there? 2

c. Set up a static MAC address.

To specify which ports a host can connect to, one option is to create a static mapping of the host MAC address to a port.

Set up a static MAC address on F0/6 using the address that was recorded for PC-B. The MAC address 0050.56BE.6C89 is used as an example only. You must use the MAC address of PC-A, which is different from the one given here as an example.

S1(config)# **mac address-table static 0050.56BE.6C89 vlan 1 interface fastethernet 0/6**

d. Verify the MAC address table entries.

S1# **show mac address-table**

How many total MAC addresses are there? 1

How many static addresses are there? 0

e. Remove the static MAC entry. Enter global configuration mode and remove the command by putting a **no** in front of the command string.

Note: The MAC address 0050.56BE.6C89 is used in the example only. Use the MAC address for PC-A.

S1(config)# **no mac address-table static 0050.56BE.6C89 vlan 1 interface fastethernet 0/6**

f. Verify that the static MAC address has been cleared.

S1# **show mac address-table**

How many total static MAC addresses are there? 0

Reflection

1. Why should you configure the vty password for the switch?

   It is for remote login of the switch

2. Can you have broadcasts at the Layer 2 level? If so, what would the MAC address be?

Yes you can, the default MAC is FFFF.FFFF.FFFF

3. Why would you need to know the MAC address of a device?

   With the MAC address you may check the manufacturer using the OUI which can allow you to find the exact device through the burned in address.

4. On Ethernet networks, data is delivered to devices by their MAC addresses. For this to happen, switches and PCs dynamically build ARP caches and MAC address tables. With only a few computers on the network this process seems fairly easy. What might be some of the challenges on larger networks?

   Within larger networks it is hard to have security on ARP caches and MAC address tables do not authenticate entries. Through this spoofing may occur.

5. Why configure a static MAC address on a port interface?

   It sets it apart from dynamic addresses so you can clear all the caches that are dynamic while keeping the static ones present. Along with that the MAC address may be added to the cache of the ARP which allows it to be found on the MAC address table, trusting the device.

Exercise 2: Configuring Switch Security Features (5.2.2.9)

Topology

Addressing Table

Device	Interface	IP Address	Subnet Mask	Default Gateway
R1	G0/1	172.16.99.1	255.255.255.0	N/A
S1	VLAN 99	172.16.99.11	255.255.255.0	172.16.99.1
PC-A	NIC	172.16.99.3	255.255.255.0	172.16.99.1

A. Set Up the Topology using Cisco Packet Tracer

B. Configure Basic Device Settings and Verify Connectivity

Step 1: Configure an IP address on PC-A.

Refer to the Addressing Table for the IP Address information.

Step 2: Configure basic settings on R1.

a. Console into R1 and enter global configuration mode.

b. Copy the following basic configuration and paste it to running-configuration on R1.

```
no ip domain-lookup
hostname R1
service password-encryption
enable secret class
banner motd #
Unauthorized access is strictly prohibited. #
line con 0
password cisco
login
logging synchronous
```

line vty 0 4

password cisco

login

interface g0/1

ip address 172.16.99.1 255.255.255.0

no shutdown

end

c. Save the running configuration to startup configuration.

Step 3: Configure basic settings on S1.

a. Console into S1 and enter global configuration mode.

b. Copy the following basic configuration and paste it to running-configuration on S1.

no ip domain-lookup

hostname S1

service password-encryption

enable secret class

banner motd #

Unauthorized access is strictly prohibited. #

line con 0

password cisco

login

logging synchronous

line vty 0 15

password cisco

login

exit

c. Create VLAN 99 on the switch and name it **Management**.

S1(config)# **vlan 99**

S1(config-vlan)# **name Management**

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

S1(config)#

d. Configure the VLAN 99 management interface IP address, as shown in the Addressing Table, and enable the interface.

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

S1(config-if)# **ip address 172.16.99.11 255.255.255.0**

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

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

S1#

e. Issue the **show vlan** command on S1. What is the status of VLAN 99?

Active.

f. Issue the **show ip interface brief** command on S1. What is the status and protocol for management interface VLAN 99?

Manual up and protocol is down.

Why is the protocol down, even though you issued the **no shutdown** command for interface VLAN 99?

No physical ports are assigned to VLAN99.

g. Assign ports F0/5 and F0/6 to VLAN 99 on the switch.

S1# **config t**

S1(config)# **interface f0/5**

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

S1(config-if)# **switchport access vlan 99**

S1(config-if)# **interface f0/6**

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

S1(config-if)# **switchport access vlan 99**

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

h. Save the running configuration to startup configuration.

i. Issue the **show ip interface brief** command on S1. What is the status and protocol showing for interface VLAN 99?

Now the protocol is up along with the status.

Note: There may be a delay while the port states converge.

Step 4: Verify connectivity between devices.

a. From PC-A, ping the default gateway address on R1. Were your pings successful?

Yes

b. From PC-A, ping the management address of S1. Were your pings successful?

Yes

c. From S1, ping the default gateway address on R1. Were your pings successful?

Yes

C. Configure and Verify SSH Access on S1

Step 1: Configure SSH access on S1.

a. Enable SSH on S1. From global configuration mode, create a domain name of **CCNA-Lab.com**.

S1(config)# **ip domain-name CCNA-Lab.com**

b. Create a local user database entry for use when connecting to the switch via SSH. The user should have administrative level access.

Note: The password used here is NOT a strong password. It is merely being used for lab purposes.

S1(config)# **username admin privilege 15 secret sshadmin**

c. Configure the transport input for the vty lines to allow SSH connections only, and use the local database for authentication.

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

S1(config-line)# **transport input ssh**

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

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

d. Generate an RSA crypto key using a modulus of 1024 bits.

S1(config)# **crypto key generate rsa modulus 1024**

The name for the keys will be: S1.CCNA-Lab.com

% The key modulus size is 1024 bits

% Generating 1024 bit RSA keys, keys will be non-exportable...

[OK] (elapsed time was 3 seconds)

S1(config)#

S1(config)# **end**

e. Verify the SSH configuration.

S1# **show ip ssh**

What version of SSH is the switch using? 1.99

How many authentication attempts does SSH allow? 3 retries

What is the default timeout setting for SSH? 2 minutes

Step 2: Modify the SSH configuration on S1.

Modify the default SSH configuration.

S1# **config t**

S1(config)# **ip ssh time-out 75**

S1(config)# **ip ssh authentication-retries 2**

How many authentication attempts does SSH allow? 2

What is the timeout setting for SSH? 75 seconds

Verify the SSH configuration on S1.

a. Using the SSH client software on PC-A (such as Tera Term), open an SSH connection to S1. If you receive a message on your SSH client regarding the host key, accept it. Login with **admin** for username and **ssh admin** for the password.

   Was the connection successful? Yes

   What prompt was displayed on S1? Why?

   No unauthorized access is prohibited because this is the MOTD which prompts a user attempting to log in.

b. Type **exit** to end the SSH session on S1.

D. Configure and Verify Security Features on S1

In Part 4, you will shut down unused ports, turn off certain services running on the switch, and configure port security based on MAC addresses. Switches can be subject to MAC address table overflow attacks, MAC spoofing attacks, and unauthorized connections to switch ports. You will configure port security to limit the number of MAC addresses that can be learned on a switch port and disable the port if that number is exceeded.

Step 1: Configure general security features on S1.

a. Change the message of the day (MOTD) banner on S1 to, "Unauthorized access is strictly prohibited. Violators will be prosecuted to the full extent of the law."

b. Issue a **show ip interface brief** command on S1. What physical ports are up?

   F0/5 and F0/6

c. Shut down all unused physical ports on the switch. Use the **interface range** command.

   S1(config)# **interface range f0/1 – 4**

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

   S1(config-if-range)# **interface range f0/7 – 24**

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

   S1(config-if-range)# **interface range g0/1 – 2**

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

   S1(config-if-range)# **end**

   S1#

d. Issue the **show ip interface brief** command on S1. What is the status of ports F0/1 to F0/4?

Administratively down

e. Issue the **show ip http server status** command.

What is the HTTP server status? enabled

What server port is it using? 80

What is the HTTP secure server status? enabled

What secure server port is it using? 443

f. HTTP sessions send everything in plain text. You will disable the HTTP service running on S1.

S1(config)# **no ip http server**

g. From PC-A, open a web browser and go to http://172.16.99.11. What was your result?

It couldn't as HTTP connections are not allowed by S1 anymore.

h. From PC-A, open a web browser and go to https://172.16.99.11. Accept the certificate. Log in with no username and a password of **class**. What was your result?

It went through as we used https instead of http.

i. Close the web browser.

Step 2: Configure and verify port security on S1.

a. Record the R1 G0/1 MAC address. From the R1 CLI, use the **show interface g0/1** command and record the MAC address of the interface.

R1# **show interface g0/1**

GigabitEthernet0/1 is up, line protocol is up

Hardware is CN Gigabit Ethernet, address is 30f7.0da3.1821 (bia 3047.0da3.1821)

What is the MAC address of the R1 G0/1 interface?

0090.210b.db02

b. From the S1 CLI, issue a **show mac address-table** command from privileged EXEC mode. Find the dynamic entries for ports F0/5 and F0/6. Record them below.

F0/5 MAC address: 0090.210b.db02

F0/6 MAC address: 00D0.D32E.9D54

c. Configure basic port security.

Note: This procedure would normally be performed on all access ports on the switch. F0/5 is shown here as an example.

1) From the S1 CLI, enter interface configuration mode for the port that connects to R1.

S1(config)# **interface f0/5**

2) Shut down the port.

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

3) Enable port security on F0/5.

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

Note: Entering the **switchport port-security** command sets the maximum MAC addresses to 1 and the violation action to shutdown. The **switchport port-security maximum** and **switchport port-security violation** commands can be used to change the default behavior.

4) Configure a static entry for the MAC address of R1 G0/1 interface recorded in Step 2a.

S1(config-if)# switchport port-security mac-address xxxx.xxxx.xxxx

(xxxx.xxxx.xxxx is the actual MAC address of the router G0/1 interface)

Note: Optionally, you can use the **switchport port-security mac-address sticky** command to add all the secure MAC addresses that are dynamically learned on a port (up to the maximum set) to the switch running configuration.

5) Enable the switch port.

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

d. Verify port security on S1 F0/5 by issuing a **show port-security interface** command.

S1# **show port-security interface f0/5**

Port Security : Enabled
Port Status : Secure-up
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 : 0000.0000.0000:0
Security Violation Count : 0

What is the port status of F0/5?

Secure-up

e. From the R1 command prompt, ping PC-A to verify connectivity.

R1# **ping 172.16.99.3**

f. You will now violate security by changing the MAC address on the router interface. Enter interface configuration mode for G0/1 and shut it down.

R1# **config t**

R1(config)# **interface g0/1**

R1(config-if)# **shutdown**

g. Configure a new MAC address for the interface, using **aaaa.bbbb.cccc** as the address.

R1(config-if)# **mac-address aaaa.bbbb.cccc**

h. If possible, have a console connection open on S1 at the same time that you do the next two steps. You will eventually see messages displayed on the console connection to S1 indicating a security violation. Enable the G0/1 interface on R1.

R1(config-if)# **no shutdown**

i. From R1 privileged EXEC mode, ping PC-A. Was the ping successful? Why or why not?

It was not because the port F0/5 was shut down on S1 due to security violation from attempting to change the MAC.

j. On the switch, verify port security with the following commands.

S1# **show port-security**

```
Secure Port MaxSecureAddr CurrentAddr SecurityViolation Security Action
            (Count)       (Count)       (Count)
---------------------------------------------------------------------
    Fa0/5         1          1              1        Shutdown
---------------------------------------------------------------------
Total Addresses in System (excluding one mac per port)     :0
Max Addresses limit in System (excluding one mac per port) :8192
```

S1# **show port-security interface f0/5**

```
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 : aaaa.bbbb.cccc:99

Security Violation Count : 1

S1# **show interface f0/5**

FastEthernet0/5 is down, line protocol is down (err-disabled)

Hardware is Fast Ethernet, address is 0cd9.96e2.3d05 (bia 0cd9.96e2.3d05)

MTU 1500 bytes, BW 10000 Kbit/sec, DLY 1000 usec,

reliability 255/255, txload 1/255, rxload 1/255

<output omitted>

S1# **show port-security address**

Secure Mac Address Table

Vlan	Mac Address	Type	Ports	Remaining Age (mins)
99	30f7.0da3.1821	SecureConfigured	Fa0/5	-

Total Addresses in System (excluding one mac per port) :0

Max Addresses limit in System (excluding one mac per port) :8192

k. On the router, shut down the G0/1 interface, remove the hard-coded MAC address from the router, and re-enable the G0/1 interface.

R1(config-if)# **shutdown**

R1(config-if)# **no mac-address aaaa.bbbb.cccc**

R1(config-if)# **no shutdown**

R1(config-if)# **end**

l. From R1, ping PC-A again at 172.16.99.3. Was the ping successful? No

m. On the switch, issue the **show interface f0/5** command to determine the cause of ping failure. Record your findings.

The line protocol is down because F0/5 is down as stated: FastEthernet0/5 is down, line protocol is down (err-disabled).

n. Clear the S1 F0/5 error disabled status.

S1# **config t**

S1(config)# **interface f0/5**

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

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

Note: There may be a delay while the port states converge.

o. Issue the **show interface f0/5** command on S1 to verify F0/5 is no longer in error disabled mode.

S1# **show interface f0/5**

FastEthernet0/5 is up, line protocol is up (connected)

Hardware is Fast Ethernet, address is 0023.5d59.9185 (bia 0023.5d59.9185)

MTU 1500 bytes, BW 100000 Kbit/sec, DLY 100 usec,

reliability 255/255, txload 1/255, rxload 1/255

p. From the R1 command prompt, ping PC-A again. The ping should be successful.

Reflection

1. Why would you enable port security on a switch?

   This makes sure that unauthorized devices do not access your network. It is simple cybersecurity as we are keeping unwanted visitors out of the network.

2. Why should unused ports on a switch be disabled?

   If we leave them open then they are susceptible to being attacked although if we close off the unused ports then we are only keeping open what we use, along with port security then it makes it much harder for unauthorized users.