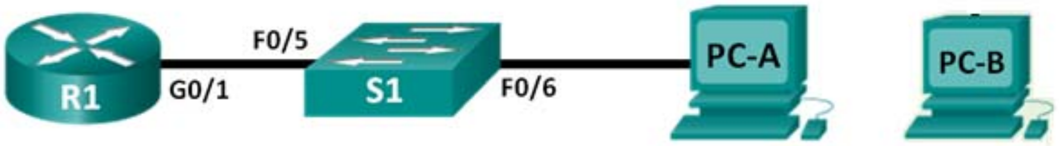
Lab 3 – Managing Switch MAC Addresses and Configuring Security

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 (P-to-p)	172.16.99.22	255.255.255.0	172.16.99.1
PC-B	NIC (P-to-p)	172.16.99.33	255.255.255.0	172.16.99.1

Objectives

Upon completion of this lab, you will be able to:

- Cable a network according to the topology diagram
- Clear an existing configuration on a switch
- Examine and verify the default configuration
- Create a basic switch configuration, including a name and an IP address
- Configure passwords to ensure that access to the CLI is secured
- Configure switch port speed and duplex properties for an interface
- Configure basic switch port security
- Manage the MAC address table
- Assign static MAC addresses
- Add and move hosts on a switch
- Configure SSH access.
- Modify SSH parameters.
- Verify the SSH configuration.
- Configure and verify general security features.
- Configure and verify port security.

Background / Scenario

It is quite common to lock down access and install good 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.

Note: Make sure that the router and switch have been erased and have no startup configurations. If you are unsure, please refer to the previous lab for the procedures to initialize and reload devices.

Task 1: Set Up the Topology and Initialize Devices

In this task, you will set up the network topology and clear any configurations if necessary.

Step 1: Cable a network.

Cable a network that is similar to the one in the topology diagram. Create a console connection to the switch. Connect only PC-A to the switch interface FastEthernet 0/6.

Note: PC-B is not initially connected to the switch. It is only used in Task 5.

Step 2: Clear the configuration on the switch and the router.

Clear the configuration on the switch and the router using the procedure in **the Introductory Lab**. If configuration files were previously saved on the router or switch, initialize and reload these devices back to their basic (default) configurations.

Task 2: Configure Basic Device Settings and Verify Connectivity

In this task, you configure basic settings on the router, switch, and PC. Refer to the Topology and Addressing Table at the beginning of this lab for device names and address information.

Step 1: Configure the IP addressing on PC-A and PC-B.

Remember that PC-B is not initially connected to the switch. It is only used in Task 4.

Step 2: Configure basic settings on R1.

- Configure the device name.
- Disable DNS lookup.
- Configure interface IP address as shown in the Addressing Table.
- Assign **class** as the privileged EXEC mode password.
- Assign **cisco** as the console and vty password and enable login.
- Encrypt plain text passwords.
- Save the running configuration to startup configuration.

Step 3: Configure basic settings on S1.

A good security practice is to assign the management IP address of the switch to a VLAN other than VLAN 1 (or any other data VLAN with end users). In this step, you will create VLAN 99 on the switch and assign it an IP address.

- Configure the device name.
- Disable DNS lookup.
- Assign **class** as the privileged EXEC mode password.
- Assign **cisco** as the console and vty password and then enable login.
- Configure a default gateway for S1 using the IP address of R1.
- Encrypt plain text passwords.
- Save the running configuration to startup configuration.

- 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)#
```

- 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#
```

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

  ....

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

  ....

- 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
```

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

  ....

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

Step 4: Verify connectivity between devices.

- From PC-A, ping the default gateway address on R1. Were your pings successful? ....
- From PC-A, ping the management address of S1. Were your pings successful? ....
- On the command prompt in the PC-A use the command `arp -a` to view the IP/MAC addresses mapping for the IP host configured on the switch (int vlan99).

  IP address…………………………………......... MAC address …………………………………………................

  Verify that these addresses belong to device: ………………………………………………………......................

  Note: The MAC address is usually presented by six fields each of two hexadecimal digits separated by colons (or hyphens), for example: 00:e0:29:17:18:84 (or 00-e0-29-17-18-84). The Cisco IOS will show different presentation of the MAC address. The address will be with three fields each of four hexadecimal digits separated by dots 00e0.2917.1884.

- Show the arp table of the switch interface vlan99 using the command `show arp`.

  ```
  S1#show arp
  ```

  IP address…………………………………......... MAC address …………………………………………….................

  Verify that these addresses belong to device: ………………………………………………………........................

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

- What is the ARP table used for?

  ....

  ....

- From PC-A, open a web browser and go to http://172.16.99.11. If it prompts you for a username and password, leave the username blank and use **class** for the password. If it prompts for secured connection, answer **No**. Were you able to access the web interface on S1? ....

- Close the browser session on PC-A.

Note: The non-secure web interface (HTTP server) on a Cisco 2960 switch is enabled by default. A common security measure is to disable this service, as described in Task 6.

Step 5: Configure the port speed and duplex settings for a FastEthernet interface.

Configure the duplex and speed settings on FastEthernet 0/6. Use the **end** command to return to privileged EXEC mode when finished.

```
S1#configure terminal
S1(config)#interface fastethernet 0/6
S1(config-if)#speed 100
S1(config-if)#duplex full
S1(config-if)#end
```

The line protocol for both interface FastEthernet 0/6 and interface VLAN 99 will temporarily go down.

The default on the Ethernet interface of the switch is auto-sensing and auto-negotiation, so it automatically negotiates optimal settings. You should set duplex and speed manually only if a port must operate at a certain speed and duplex mode. Manually configuring ports can lead to duplex mismatches, which can significantly degrade performance.

Verify the new duplex and speed settings on the FastEthernet interface 0/6.

```
S1#show interface fastethernet 0/6
```

……………………………………………………………………………………………………........................

Check on the switch front panel that this interface is in full duplex mode.

……………………………………………………………………………………………………........................

How would you be able to configure manually the network interface card of PC-A to work in 100Mbps full duplex?

……………………………………………………………………………………………………........................

……………………………………………………………………………………………………........................

Task 3: Managing the MAC Address Table

Step 1: Determine the MAC address of the PC host.

Determine and record the Layer 2 (physical) address of the PC-A network interface card using the command **ipconfig /all** on the command prompt (compare with Step 4, Task 2).

……………………………………………………………………………………………………

Step 2: Determine the MAC addresses that the switch has learned.

Display the MAC addresses using the **show mac address-table** command in privileged EXEC mode.

```
S1#show mac address-table
```

What dynamic addresses are there? ……………………………………………………………

What other addresses are there? ……………………………………………………………

Does any MAC address match the MAC address of PC-A? …………………………………………

What is the MAC address table used for?

……………………………………………………………………………………………………

……………………………………………………………………………………………………

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

```
S1#show mac address-table ?
```

What options are available for the **show mac address-table** command? ………………………………

……………………………………………………………………………………………………

You may show only the MAC addresses that were learned dynamically using the option `dynamic`.

```
S1#show mac address-table dynamic
```

Why are these addresses called dynamic? Explain briefly.

……………………………………………………………………………………………………

……………………………………………………………………………………………………

Step 4: Clearing the MAC address table.

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

```
S1#clear mac address-table dynamic
```

Step 5: Verify the results.

Verify that the MAC address table was cleared.

```
S1#show mac address-table
```

How many static MAC addresses are there? ………………………………………………………

How many dynamic addresses are there? ………………………………………………………

Step 6: Examine the MAC table again.

More than likely, an application running on your PC-A has already sent a frame out the NIC through the switch S1. Look at the MAC address table again in privileged EXEC mode to see if S1 has relearned the MAC address for the PC.

```
S1#show mac address-table
```

Which dynamic addresses are there? ………………………………………………………………………

If S1 has not yet relearned the MAC address for PC-A, ping the VLAN 99 IP address of the switch from PC-A and then repeat Step 6.

Step 7: 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 switchport.

Set up a static MAC address on FastEthernet interface 0/6 using the address that was recorded for PC-A in Step 1 of this task. The MAC address **00e0.2917.1884** is ***the one used here only as an example***. You must use the MAC address of your PC-A, which is different than the one given here as an example.

```
S1(config)#mac address-table static 00e0.2917.1884 vlan 99 interface fastethernet
0/6
```

Step 8: Verify the results.

Verify the MAC address table entries.

```
S1#show mac address-table
```

Which new static MAC address is there? ………………………………………………………………………

Step 9: Remove the static MAC entry.

To complete the next task, it will be necessary to remove the static MAC address table entry. Enter configuration mode and remove the command by putting a **no** in front of the command string.

Note: The MAC address 00e0.2917.1884 is used in the example only. Use the MAC address for your PC1.

```
S1(config)#no mac address-table static 00e0.2917.1884 vlan 99 interface
fastethernet 0/6
```

Step 10: Verify the results.

Verify that the configured static MAC address has been removed from the table.

```
S1#show mac address-table
```

Task 4: Configuring Port Security against Rogue Host

Step 1: Configure a second host.

A second host PC-B is needed for this task. Set the IP address of PC2 to 172.16.99.33, with a subnet mask of 255.255.255.0 and a default gateway of 172.16.99.1**. Do not connect this PC to the switch yet!**

Step 2: Verify connectivity.

Verify that PC-A and the switch are still correctly configured by pinging the IP address of `int vlan99` of the switch from the PC-A host.

Step 3: List the port security options.

Explore the options for setting port security on interface FastEthernet 0/6.

```
S1# configure terminal
S1(config)#interface fastethernet 0/6
S1(config-if)#switchport port-security ?
  aging         Port-security aging commands
  mac-address   Secure mac address
  maximum       Max secure addresses
  violation     Security violation mode
```

Step 4: Configure port security on an access port.

Configure switch port FastEthernet 0/6 to accept only one device, to learn the MAC address of that device dynamically, and to shut down if a violation occurs.

```
S1(config-if)#switchport mode access
S1(config-if)#switchport port-security
S1(config-if)#switchport port-security maximum 1
S1(config-if)#switchport port-security mac-address sticky
S1(config-if)#switchport port-security violation shutdown
S1(config-if)#end
```

Step 5: Verify the results.

Show the port security settings.

```
S1#show port-security
```

How many secure addresses are allowed on FastEthernet 0/6? ………………………………………..........................

What is the security action for this port? …………………………………...

Step 6: Examine the running configuration file.

Ping the VLAN 99 address of the switch from PC-A to verify connectivity and to refresh the MAC address table. You should now see the MAC address for PC-A “stuck” to the running configuration.

```
S1#show running-config
```

What are the statements listed that directly reflect the security implementation of the running configuration?

…………………………………...................……………………………………..

…………………………………...................……………………………………..

Step 7: Introduce a rogue host.

Disconnect PC-A and connect PC-B to port FastEthernet 0/6. Ping the VLAN 99 address 172.16.99.11 from the new host. Wait for the amber link light to turn green. Once it turns green, it should almost immediately turn off.

Record any log messages on the terminal:

…………………………………...................……………………………………..

…………………………………...................……………………………………..

Step 8: Show port configuration information.

To see the configuration information for just FastEthernet port 0/6, issue the following command in privileged EXEC mode:

```
S1#show interface fastethernet 0/6
```

What is the state of this interface?

FastEthernet 0/6 is ……….............................. Line protocol is ……........... (……………………………………)

Step 9: Reactivate the port.

If a security violation occurs and the port is shut down, you can use the **no shutdown** command to reactivate it. However, as long as the rogue host is attached to FastEthernet 0/6, any traffic from the host disables the port. Remove PC-B from the switch and reconnect PC-A to FastEthernet 0/6, and enter the `no shutdown` command on the switch interface. Ping and verify connectivity.

Note: Some IOS version may require a manual **shutdown** command before entering the **no shutdown** command.

Task 5: Configure and Verify SSH Access on S1

Step 1: Configure SSH access on S1.

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

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

- 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
  ```

- 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
  ```

- 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
  ```

- Verify the SSH configuration and answer the questions below.

  ```
  S1# show ip ssh
  ```

  What version of SSH is the switch using? ....

  How many authentication attempts does SSH allow? ....

  What is the default timeout setting for SSH? ....

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? ....

What is the timeout setting for SSH? ....

Step 3: Verify the SSH configuration on S1.

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

  Was the connection successful? ....

  What prompt was displayed on S1? Why?

  ....

  ....

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

Task 6: Configure and Verify More Security Features on S1.

In this task, 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.

- Configure a message of the day (MOTD) banner on S1 with an appropriate security warning message.
- Issue a **show ip interface brief** command on S1. What physical ports are up?

  ....

- 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#
```

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

  ....

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

  What is the HTTP server status? ....

  What server port is the switch using? ....

  What is the HTTP secure server status? ....

What TCP-port is the secure server using? ....

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

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

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

  ………………………………...................………………………………………...

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

  ………………………………...................………………………………………...

- Close the web session on PC-A.

Step 2: Configure and verify port security on S1.

- 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
```

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

- 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: ....

  F0/6 MAC address: ....

- 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 previously in this step.

```
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 (F0/5).

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

- 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? ....

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

```
R1# ping 172.16.99.22
```

- 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
```

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

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

- If possible, have a console connection open on S1 at the same time that you do this step. You will see various messages displayed on the console connection to S1 indicating a security violation. Enable the G0/1 interface on R1.

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

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

....

....

- On the switch, verify port security with the following commands shown below.

```
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
```

- 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
```

- From R1, ping PC-A again at 172.16.99.22. Was the ping successful? ....
- On the Switch, issue the **`show interface f0/5`** command to determine the cause of ping failure. Record your findings.

  ....

  ....
- 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.

- 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
```

- From the R1 command prompt, ping PC-A again. Ping should be now successful.