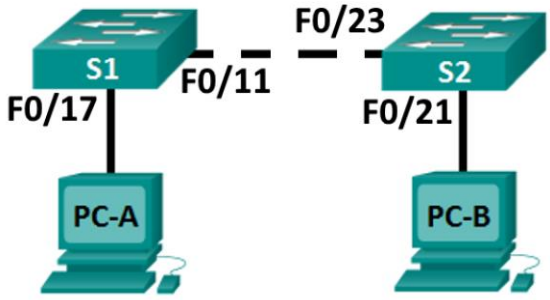
Lab 4 Activity 4.1 – View the Switch MAC Address Table

Topology ON-CAMPUS VERSION



Addressing Table

Device	Interface	IP Address	Subnet Mask	Default Gateway
S1	VLAN 1	192.168.11.111	255.255.255.0	N/A
S2	VLAN 1	192.168.11.112	255.255.255.0	N/A
PC-A	NIC	192.168.11.72	255.255.255.0	N/A
PC-B	NIC	192.168.11.74	255.255.255.0	N/A

Objectives

Part 1: Build and Configure the Network

Part 2: Examine the Switch MAC Address Table

Background / Scenario

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. The way a switch operates has implications for network administrators whose job it is to ensure secure and consistent network communication.

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.

In Part 1, you will build a multi-switch topology with a trunk (cable between two switches) linking the two switches. In Part 2, you will ping various devices and observe how the two switches build their MAC address tables.

Required Resources

- 2 Switches
- 2 PCs

Part 1: Build and Configure the Network

Step 1: Cable the network according to the topology.

a. Add a console cable from PC-A to S1.

b. Add a console cable from PC-B to S2.

Step 2: Configure PC hosts.

Use the information shown in the topology.

Step 3: Configure basic settings for each switch.

a. Configure device name as shown in the topology.

b. Disable DNS lookup to prevent the router from attempting to translate incorrectly entered commands as though they were host names.

c. Configure IP address as listed in Addressing Table.

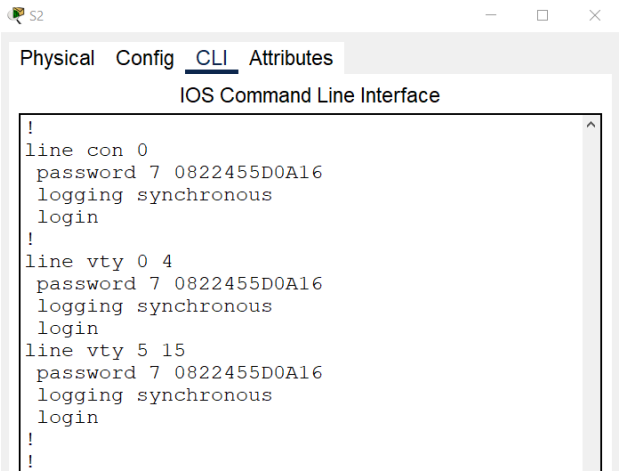
d. Assign **cisco** as the console and vty passwords. Enable login and logging synchronous for both.

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

f. Encrypt the clear text passwords (ie. cisco). The command for this is:

service password-encryption

Once you have done this, the console and vty passwords will show as encrypted when viewing the running-configuration file:



g. Create a banner that warns anyone accessing the device that unauthorized access is prohibited. Use the following text:

Unauthorised access is strictly prohibited and will be prosecuted.

Part 2: 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: _____

PC-B MAC Address: _____

b. Console into switch S1, navigate to the correct mode, and type the **show interface F0/11** command. Interface f0/11 is the link that connects S1 to S2.

On the second line of command output, what is the hardware addresses (or burned-in address [bia])?

S1 Fast Ethernet 0/11 MAC Address: _____

c. Console into switch S2, navigate to the correct mode, and type the **show interface F0/23** command. Interface f0/23 is the link that connects S2 to S1.

On the second line of command output, what is the hardware addresses (or burned-in address [bia])?

S2 Fast Ethernet 0/23 MAC Address: _____

Step 2: Display the switch MAC address table.

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?

_____

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

_____

_____

_____

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?

_____

_____

_____

_____

Step 3: 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?

_____

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

Step 4: From PC-B, ping the devices on the network and observe the switch MAC address table.

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

_____

_____

b. 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?

_____

_____

Reflection

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?

_____