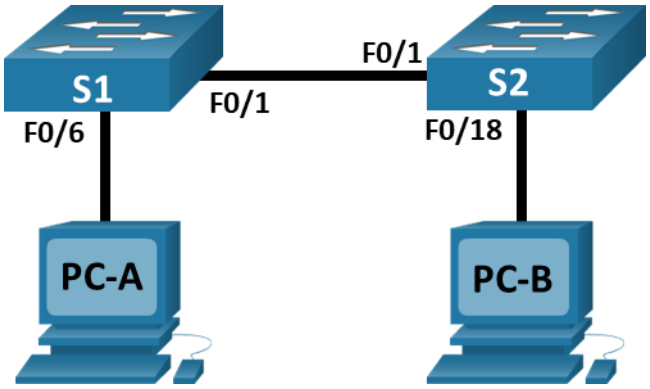
Lab - View the Switch MAC Address Table

Topology



Addressing Table

Device	Interface	IP Address	Subnet Mask
S1	VLAN 1	192.168.1.11	255.255.255.0
S2	VLAN 1	192.168.1.12	255.255.255.0
PC-A	NIC	192.168.1.1	255.255.255.0
PC-B	NIC	192.168.1.2	255.255.255.0

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 linking the two switches. In Part 2, you will ping various devices and observe how the two switches build their MAC address tables.

Note: The switches used are Cisco Catalyst 2960s with Cisco IOS Release 15.2(2) (lanbasek9 image). Other switches and Cisco IOS versions can be used. Depending on the model and Cisco IOS version, the commands available and output produced might vary from what is shown in the labs.

Note: Make sure that the switches have been erased and have no startup configurations. If you are unsure contact your instructor.

Required Resources

- 2 Switches (Cisco 2960 with Cisco IOS Release 15.2(2) lanbasek9 image or comparable)
- 2 PCs (Windows with terminal emulation program, such as Tera Term)
- Console cables to configure the Cisco IOS devices via the console ports
- Ethernet cables as shown in the topology

Note: The Fast Ethernet interfaces on Cisco 2960 switches are autosensing and an Ethernet straight-through cable may be used between switches S1 and S2. If using another model Cisco switch, it may be necessary to use an Ethernet crossover cable.

Instructions

Part 1: Build and Configure the Network

Step 1: Cable the network according to the topology.

Step 2: Configure PC hosts.

Step 3: Initialize and reload switches as necessary.

Step 4: 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.

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: 00D0.D39C.E781

PC-B MAC Address: 0002.4A9C.81C9

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 is the hardware addresses (or burned-in address [bia])?

S1 Fast Ethernet 0/1 MAC Address: 000c.8578.5401

S2 Fast Ethernet 0/1 MAC Address: 0001.64d7.c301

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?

yes

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.

they are mapped to port 0/1

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?

the output command shows the port that the mac address was learned on

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 for VLAN 1? Are there other MAC addresses listed?

yes, it has one

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

yes, there is one more, now there are 2 addresses

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 and type **arp -a**.

Not including multicast or broadcast addresses, how many device IP-to-MAC address pairs have been learned by ARP?

No ARP Entries Found

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.

its ok

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?

it added the address of 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

Reflection Question

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?

ARP broadcasts could cause broadcast storms. Because ARP and switch MAC tables do not authenticate or validate the IP addresses to MAC addresses it would be easy to spoof a device on the network.