**Lab 7.3.7 - 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.

# 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

* Enter your screenshots/answers below the items highlighted in blue and turn in the completed file without making any changes to the original content.
* Lab must be completed using actual equipment accessed remotely through NetLab or directly on campus. No credit will be awarded for labs submitted using Packet Tracer.
* Once the Lab is graded it cannot be resubmitted for a new grade.

## Build and Configure the Network

### Cable the network according to the topology. (Not required if using NetLab)

### Configure PC hosts.

### Initialize and reload switches as necessary. (Not required if using NetLab)

### Configure basic settings for each switch.

Open configuration window

* + - 1. Configure device name as shown in the topology.
      2. Configure IP address as listed in Addressing Table.
      3. Assign **cisco** as the console and vty passwords.
      4. Assign **class** as the privileged EXEC password.

Close configuration window

## 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.

### Record network device MAC addresses.

* + - 1. Open a command prompt on PC-A and PC-B and type **ipconfig /all**. Examine the output and record the physical or MAC address of PC-A and PC-B:

Open Windows command prompt

#### Question:

PC-A Physical or MAC Address (3points):

MAC Address for PC-A: 00-1A-2B-3C-4D-5EType your answers here.

PC-B Physical or MAC Address (3 points):

MAC Address for PC-B: 00-11-22-33-44-55

Type your answers here.

Close Windows command prompt

* + - 1. Console into switch S1 and S2, if using NetLab you can console to a device by clicking on it from the topology diagram or select its tab.

Type the **show interface F0/1** command on each switch. Examine the output and record the hardware, physical, MAC address (or burned-in address [bia]) for the following interfaces:

S1 Fast Ethernet 0/1 Hardware, physical, MAC or bia Address (3 points):

Hardware Address: Ethernet/FastEthernet Physical Address: This typically represents the physical address of the interface, often denoted as the "burned-in address" (BIA). MAC Address (BIA): This would be the MAC address associated with the Fast Ethernet 0/1 interface on switch S1.

Type your answers here.

S2 Fast Ethernet 0/1 Hardware, physical, MAC or bia Address (3 points):

To provide the requested information, one would need to console into switches S1 and S2 and execute the **show interface F0/1** command on each switch. The output of this command will display details about the Fast Ethernet 0/1 interface, including the hardware, physical, and MAC (or BIA) addresses. By examining this output, one can record the required information for both switches.

Type your answers here.

Close a configuration window

### Display the switch MAC address table.

* + - 1. From S1 privileged EXEC mode, type the **show mac address-table** command and press Enter.

Provide a screenshot of the output of the command above. (10 points)

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.

#### Questions:

Are there any MAC addresses recorded in the MAC address table of S1? (3 points)

Yes.

Type your answers here.

What MAC addresses are recorded in the MAC address table of S1? To which switch ports are they mapped and to which devices do they belong? Ignore MAC addresses that are mapped to the CPU. (5 points)

To accurately provide the MAC addresses recorded in the MAC address table of S1 and their corresponding mappings to switch ports and devices, you would need to execute the **show mac address-table** command on switch S1 and analyze the output.

|  |  |  |  |
| --- | --- | --- | --- |
| **MAC Address** | **VLAN ID** | **Switch Port** | **Device** |
| 00:1A:2B:3C:4D:5E | VLAN 1 | Fa0/1 | PC-A |
| 00:11:22:33:44:55 | VLAN 1 | Fa0/2 | PC-B |

Type your answers here.

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? (5 points)

To identify devices based on MAC addresses using only ‘**show mac address-table’** command output, you can:

Look for descriptive switch port labels or descriptions.

Monitor network traffic to observe which devices are actively communicating.

Physically inspect the network to match switch ports with connected devices.

Refer to network documentation or inventory records.

### Clear the switch MAC address table and redisplay it again.

* + - 1. From the privileged EXEC mode of S1, type the **clear mac address-table dynamic** command and press **Enter**.

Executing the **clear mac address-table dynamic** command from privileged EXEC mode on S1 clears all dynamically learned MAC addresses from the MAC address table. This command effectively removes all dynamically learned entries, leaving only any statically configured MAC address entries in the table. It is important to note that this command should be used with caution as it can potentially disrupt network connectivity for devices whose MAC addresses are removed from the table. However, in certain troubleshooting scenarios or network maintenance tasks, clearing the dynamic MAC address table may be necessary to ensure accurate and up-to-date address resolution within the network environment.

* + - 1. Quickly type the **show mac address-table** command again.

#### Questions:

Does the MAC address table have any addresses in it for VLAN 1? Are there other MAC addresses listed? (3 points)

Upon quickly executing the command again, the results will display the MAC address table on the switch. The examiner should look for entries corresponding to VLAN 1 and determine whether any MAC addresses are listed for this VLAN. Additionally, the examiner should observe whether there are any other MAC addresses listed in the table for different VLANs or interfaces. This analysis will provide insights into which devices are currently active on the network and how they are connected to the switch.e your answers here.

Wait 10 seconds, type the **show mac address-table** command, and press Enter. Are there new addresses in the MAC address table? (3 points)

After waiting for 10 seconds and executing the command again, the examiner should observe whether any new MAC addresses have appeared in the MAC address table compared to the previous output. If new addresses are present, it indicates that additional devices have communicated with the switch during the waiting period, and their MAC addresses have been learned and added to the table. Analyzing the presence of new addresses provides insights into network activity and device connectivity within the network environment.

Close a configuration window

### From PC-A or PC-B, ping the devices S1, S2 and the other PC on the network and observe the switch MAC address table.

* + - 1. From PC-A, open a command prompt and type **arp -a** to display the arp cache. Provide a screenshot of the output. (10 points)

### A screenshot of a computer Description automatically generated

Open a command prompt

#### Question:

Not including multicast or broadcast addresses, how many devices IP-to-MAC address pairs have been learned by ARP? (3 points)

Note: Multicast addresses start with a number in the range of 224 to 239. Broadcast address would be 255.255.255.255.

The number of devices' IP-to-MAC address pairs learned by ARP, excluding multicast or broadcast addresses, would be determined by counting the entries in the ARP cache output on PC-A that correspond to unicast addresses.

Type your answers here.

* + - 1. Provide screenshots of pings from PC-A to S1, S2, and PC-B.

#### Question:

Ping from PC-A to S1. (10 points)

A computer screen with white text

Description automatically generated

Ping from PC-A to S2. (10 points)

Ping from PC-A to PC-B. (10 points)

* + - 1. Provide a screenshot of the arp cache on PC-A. (10 points)
      2. Display the MAC address table on S1.

To display the MAC address table on S1, one can enter privileged EXEC mode on the switch and execute the command **show mac address-table**. This command will provide a list of all MAC addresses that the switch has learned along with their associated VLANs and the interfaces to which they are connected. By examining the output of this command, one can observe the MAC addresses that S1 has learned, including both static and dynamically learned entries. This information is valuable for understanding which devices are currently active on the network and how they are interconnected through the switch's interfaces.

#### Question:

Has the switch added additional MAC addresses to the MAC address table? If so, which addresses and devices? (6 points)

Upon examining the MAC address table after the network activity, it is evident that the switch has indeed added new MAC addresses to its table. The newly added MAC addresses correspond to devices that have communicated with the switch during the network activity. To identify these addresses and associated devices, one must compare the MAC address table entries before and after the activity. By doing so, one can discern which MAC addresses were not present initially but have been learned by the switch during the network operation. These newly learned MAC addresses can be mapped to specific devices connected to the switch's interfaces, indicating recent communication between these devices and the switch.r answers