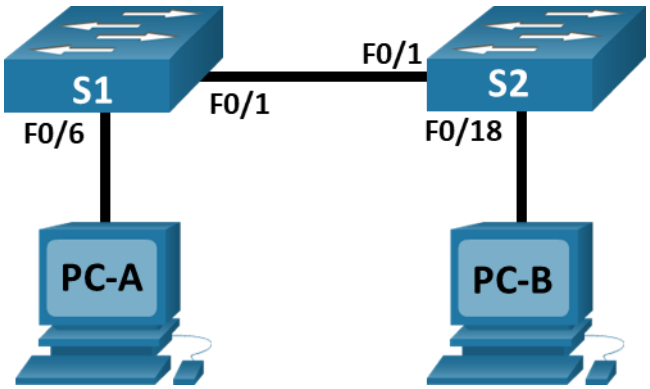
# Lab - View the Switch MAC Address Table (Instructor Version)

**Instructor Note**: Red font color or gray highlights indicate text that appears in the instructor copy only.

## 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.

**Instructor Note**: Refer to the Instructor Lab Manual for the procedures to initialize and reload devices.

### 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:

**Answers will vary. The MAC address in this example is 00-50-56-B3-27-D6.**

PC-B MAC Address:

**Answers will vary. The MAC address in this example is 00-50-56-B3-FF-54.**

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:

**Answers will vary. From the example output below, the S1 F0/1 MAC address is 0cd9.96e2.3d01.**

S2 Fast Ethernet 0/1 MAC Address:

**Answers will vary. From the example output below, the S2 F0/1 MAC address is 0cd9.96d2.3f81.**

```
S1# show interface f0/1
FastEthernet0/1 is up, line protocol is up (connected)
  Hardware is Fast Ethernet, address is 001a.e3cf.b883 (bia 001a.e3cf.b883)
  MTU 1500 bytes, BW 100000 Kbit, DLY 100 usec,
<output omitted>

S2# show interface f0/1
FastEthernet0/1 is up, line protocol is up (connected)
  Hardware is Fast Ethernet, address is 0025.83e6.9081 (bia 0025.83e6.9081)
  MTU 1500 bytes, BW 100000 Kbit/sec, DLY 100 usec,
<output omitted>
```

## 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?

**The switch may have one or more MAC addresses in its table, based on whether or not the students entered a ping command when configuring the network. The switch will most likely have learned MAC addresses through S1's F0/1 switch port. The switch will record multiple MAC addresses of hosts learned through the connection to the other switch on F0/1.**

```
S2# show mac address-table
          Mac Address Table
-------------------------------------------
```

```
Vlan    Mac Address       Type        Ports
----    -----------       --------    -----
 All    0100.0ccc.cccc    STATIC      CPU
 All    0100.0ccc.cccd    STATIC      CPU
 All    0180.c200.0000    STATIC      CPU
 All    0180.c200.0001    STATIC      CPU
 All    0180.c200.0002    STATIC      CPU
 All    0180.c200.0003    STATIC      CPU
 All    0180.c200.0004    STATIC      CPU
 All    0180.c200.0005    STATIC      CPU
 All    0180.c200.0006    STATIC      CPU
 All    0180.c200.0007    STATIC      CPU
 All    0180.c200.0008    STATIC      CPU
 All    0180.c200.0009    STATIC      CPU
 All    0180.c200.000a    STATIC      CPU
 All    0180.c200.000b    STATIC      CPU
 All    0180.c200.000c    STATIC      CPU
 All    0180.c200.000d    STATIC      CPU
 All    0180.c200.000e    STATIC      CPU
 All    0180.c200.000f    STATIC      CPU
 All    0180.c200.0010    STATIC      CPU
 All    ffff.ffff.ffff    STATIC      CPU
   1    001a.e3cf.b883    DYNAMIC     Fa0/1
Total Mac Addresses for this criterion: 21
```

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.

**There may be multiple MAC addresses recorded in the MAC address table, especially MAC addresses learned through S1's F0/1 switch port. In the example output above, the S1 F0/1 MAC 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?

**The output of the show mac address-table command shows the port that the MAC address was learned on. In most cases this would identify which network device the MAC address belongs to, except in the case of multiple MAC addresses associated to the same port. This happens when switches are connected to other switches and record all of the MAC addresses for devices connected to the other switch.**

### 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?

**No. The student will most likely discover that the MAC address for the other switch's F0/1 switch port has been quickly reinserted in the MAC address table.**

```
S2# show mac address-table
          Mac Address Table
-------------------------------------------

Vlan    Mac Address       Type        Ports
----    -----------       --------    -----
 All    0100.0ccc.cccc    STATIC      CPU
 All    0100.0ccc.cccd    STATIC      CPU
 All    0180.c200.0000    STATIC      CPU
 All    0180.c200.0001    STATIC      CPU
 All    0180.c200.0002    STATIC      CPU
 All    0180.c200.0003    STATIC      CPU
 All    0180.c200.0004    STATIC      CPU
 All    0180.c200.0005    STATIC      CPU
 All    0180.c200.0006    STATIC      CPU
 All    0180.c200.0007    STATIC      CPU
 All    0180.c200.0008    STATIC      CPU
 All    0180.c200.0009    STATIC      CPU
 All    0180.c200.000a    STATIC      CPU
 All    0180.c200.000b    STATIC      CPU
 All    0180.c200.000c    STATIC      CPU
 All    0180.c200.000d    STATIC      CPU
 All    0180.c200.000e    STATIC      CPU
 All    0180.c200.000f    STATIC      CPU
 All    0180.c200.0010    STATIC      CPU
 All    ffff.ffff.ffff    STATIC      CPU
   1    001a.e3cf.b883    DYNAMIC     Fa0/1
Total Mac Addresses for this criterion: 21
```

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

**Answers will vary. There may be more MAC addresses in the 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 and type **arp -a**.

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

**Answers will vary. The ARP cache may have no entries in it, or it may have the gateway IP address to MAC address mapping.**

```
C:\Users\PC-B> arp -a
<output omitted>
Interface: 192.168.1.2 --- 0x6
```

```
  Internet Address      Physical Address      Type
  192.168.1.255         ff-ff-ff-ff-ff-ff     static
  224.0.0.22            01-00-5e-00-00-16     static
  224.0.0.252           01-00-5e-00-00-fc     static
  255.255.255.255       ff-ff-ff-ff-ff-ff     static
```

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.

**If the network was cabled and configured correctly the answer should be 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?

**There may only be one additional MAC address mapping added to the table, most likely the MAC address of PC-A.**

```
S2# show mac address-table
          Mac Address Table
-------------------------------------------

Vlan    Mac Address       Type        Ports
----    -----------       --------    -----
 All    0100.0ccc.cccc    STATIC      CPU
 All    0100.0ccc.cccd    STATIC      CPU
 All    0180.c200.0000    STATIC      CPU
 All    0180.c200.0001    STATIC      CPU
 All    0180.c200.0002    STATIC      CPU
 All    0180.c200.0003    STATIC      CPU
 All    0180.c200.0004    STATIC      CPU
 All    0180.c200.0005    STATIC      CPU
 All    0180.c200.0006    STATIC      CPU
 All    0180.c200.0007    STATIC      CPU
 All    0180.c200.0008    STATIC      CPU
 All    0180.c200.0009    STATIC      CPU
 All    0180.c200.000a    STATIC      CPU
 All    0180.c200.000b    STATIC      CPU
 All    0180.c200.000c    STATIC      CPU
 All    0180.c200.000d    STATIC      CPU
 All    0180.c200.000e    STATIC      CPU
 All    0180.c200.000f    STATIC      CPU
 All    0180.c200.0010    STATIC      CPU
 All    ffff.ffff.ffff    STATIC      CPU
   1    001a.e3cf.b883    DYNAMIC     Fa0/1
   1    001a.e3cf.b8c0    DYNAMIC     Fa0/1
   1    0050.56b3.27d6    DYNAMIC     Fa0/1
   1    0050.56b3.ff54    DYNAMIC     Fa0/18
```

```
Total Mac Addresses for this criterion: 24
```

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?

**Answers may vary, but the ARP cache on PC-B should have more entries.**

```
C:\Users\PC-B> arp -a
<output omitted>
Interface: 192.168.1.2 --- 0x6
  Internet Address      Physical Address      Type
  192.168.1.1           00-50-56-b3-27-d6     dynamic
  192.168.1.11          00-1a-e3-cf-b8-c0     dynamic
  192.168.1.12          00-25-83-e6-90-c0     dynamic
  192.168.1.255         ff-ff-ff-ff-ff-ff     static
  224.0.0.22            01-00-5e-00-00-16     static
  224.0.0.252           01-00-5e-00-00-fc     static
  239.255.255.250       01-00-5e-7f-ff-fa     static
```

## 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.**

## Device Configs

## Switch S1

```
S1# show running-config
Building configuration...

version 15.0
no service pad
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname S1
!
boot-start-marker
boot-end-marker
!
enable secret 5 $1$lRkm$DFlxhlhb6FCHl4J.ux4Fb/
!
```

```
no aaa new-model
system mtu routing 1500
!
spanning-tree mode pvst
spanning-tree extend system-id
!
vlan internal allocation policy ascending
!
!
!
interface FastEthernet0/1
!
interface FastEthernet0/2
!
interface FastEthernet0/3
!
interface FastEthernet0/4
!
interface FastEthernet0/5
!
interface FastEthernet0/6
!
interface FastEthernet0/7
!
interface FastEthernet0/8
!
interface FastEthernet0/9
!
interface FastEthernet0/10
!
interface FastEthernet0/11
!
interface FastEthernet0/12
!
interface FastEthernet0/13
!
interface FastEthernet0/14
!
interface FastEthernet0/15
!
interface FastEthernet0/16
!
interface FastEthernet0/17
!
interface FastEthernet0/18
!
interface FastEthernet0/19
!
interface FastEthernet0/20
!
```

```
interface FastEthernet0/21
!
interface FastEthernet0/22
!
interface FastEthernet0/23
!
interface FastEthernet0/24
!
interface GigabitEthernet0/1
!
interface GigabitEthernet0/2
!
interface Vlan1
 ip address 192.168.1.11 255.255.255.0
!
ip http server
ip http secure-server
!
line con 0
line vty 0 4
 password cisco
 login
line vty 5 15
 login
!
end
```

### Switch S2

```
S2#show running-config
Building configuration...

version 15.0
no service pad
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname S2
!
boot-start-marker
boot-end-marker
!
enable secret 5 $1$lRkm$DFlxhlhb6FCHl4J.ux4Fb/
!
no aaa new-model
system mtu routing 1500
!
spanning-tree mode pvst
spanning-tree extend system-id
```

```
!
vlan internal allocation policy ascending
!
interface FastEthernet0/1
!
interface FastEthernet0/2
!
interface FastEthernet0/3
!
interface FastEthernet0/4
!
interface FastEthernet0/5
!
interface FastEthernet0/6
!
interface FastEthernet0/7
!
interface FastEthernet0/8
!
interface FastEthernet0/9
!
interface FastEthernet0/10
!
interface FastEthernet0/11
!
interface FastEthernet0/12
!
interface FastEthernet0/13
!
interface FastEthernet0/14
!
interface FastEthernet0/15
!
interface FastEthernet0/16
!
interface FastEthernet0/17
!
interface FastEthernet0/18
!
interface FastEthernet0/19
!
interface FastEthernet0/20
!
interface FastEthernet0/21
!
interface FastEthernet0/22
!
interface FastEthernet0/23
!
interface FastEthernet0/24
```

```
!
interface GigabitEthernet0/1
!
interface GigabitEthernet0/2
!
interface Vlan1
 ip address 192.168.1.12 255.255.255.0
!
ip http server
ip http secure-server
!
line con 0
line vty 0 4
 password cisco
 login
line vty 5 15
 login
!
end
```