Practical – Week 3

Objectives:

The aim of this week's practical includes:

- To improve skills in building and configuring simple networks
- To display and analyse Ethernet MAC addresses, and examine switch MAC address table
- To examine and understand Ethernet frames

Tasks:

Accordingly, you will need to complete the following two labs in this week's practical class:

a. View Device MAC Addresses and Switch MAC Address Table
b. Examine Ethernet frames

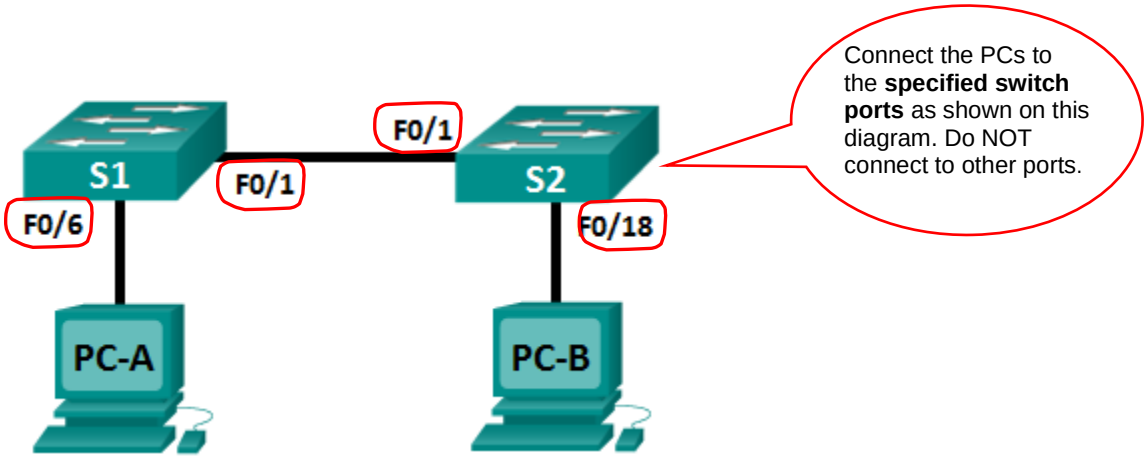
Instructions of the tasks are given on the next pages.

Assessment:

This week's Practical is assessed in class, and it is worth 3% of the total score of the course.

Lab – Viewing Device MAC Addresses and Switch MAC Address Table

Topology



Addressing Table

Device	Interface	IP Address	Subnet Mask	Default Gateway
S1	VLAN 1	192.168.1.11	255.255.255.0	N/A
S2	VLAN 1	192.168.1.12	255.255.255.0	N/A
PC-A	NIC	192.168.1.2	255.255.255.0	N/A
PC-B	NIC	192.168.1.3	255.255.255.0	N/A

Objectives

Part 1: Build and Configure the Network

Part 2: Display, Describe, and Analyze Ethernet MAC Addresses

Part 3: Examine the Switch MAC Address Table

Background / Scenario

In Part 1 of this lab, you will cable the equipment as shown in the topology. You will configure the switches and PCs to match the addressing table. You will verify your configurations by testing for network connectivity.

In Part 2 of this lab, you will view the MAC addresses of the devices (PCs and Switches). Every Network Interface Card (NIC) of a device on an Ethernet LAN is identified by a Layer 2 MAC address. This address is assigned by the manufacturer and stored in the firmware of the NIC. You will explore and analyze the components that make up a MAC address, and how you can find this information on a switch and a PC.

In Part 3 of the lab, you will examine the **MAC address tables** of switches. Each entry of the MAC address table of a switch is a mapping between a port number of the switch and the MAC address of the NIC of the device (e.g. the Ethernet NIC of a PC) attached to the port. Switches are used to interconnect and deliver information to computers on local area networks. Switches deliver Ethernet frames to host devices identified by NIC MAC addresses. A switch learns MAC addresses of the NICs of the devices attached to its ports, and builds the MAC address table, as network devices initiate communication on the network.

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 15.0(2) lanbasek9 image or comparable)
- 2 PCs 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.

Part 1: Build and Configure the Network

Step 1: Cable the network according to the topology. Use the switch interfaces as indicated in the topology.

Step 2: Configure the IPv4 address for PC-A and PC-B

Note: Please **do NOT** configure the switches at this stage. **Only configure the two PCs in this step**.

a. Configure the IPv4 address and subnet mask for PC-A as per the above Addressing Table

b. Configure the IPv4 address and subnet mask for PC-B as per the above Addressing Table

c. From the command prompt on **PC-A**, ping switch **S1** and switch **S2**, respectively.

Were the pings successful?. _____ Explain why/why not_____

d. From the command prompt on **PC-B**, ping switch **S1** and switch **S2**, respectively.

Were the pings successful?. _____ Explain why/why not_____

e. From the command prompt on **PC-A**, ping **PC-B**'s address

Were the pings successful?. _____ Explain why/why not_____

f. From the command prompt on **PC-B**, ping **PC-A**'s address

Were the pings successful?. _____ Explain why/why not_____

The pings of step 2e. and 2f. should be successful. If not, check your cable connections and PC IP address configurations.

Step 3: Configure basic settings for switch S1.

In this step, you will configure the device name and the IP address, and disable DNS lookup on the switch.

a. Console into switch S1 from PC-A

b. Remember to press ENTER after the Tera Term window opens.

i) If your switch shows `switch>`, then move to **step 3c** below (i.e. Enter global configuration mode)

ii) If your switch asks for a password, try the password cisco or class. If not working, ask your instructor for assistance.

c. Enter global configuration mode.

```
Switch> enable
Switch# configure terminal
Enter configuration commands, one per line.     End with CNTL/Z.
Switch(config)#
```

d. Assign a hostname to the switch based on the Addressing Table.

```
Switch(config)# hostname S1
```

e. Disable DNS lookup.

```
S1(config)# no ip domain-lookup
```

f. Configure and enable the SVI interface for VLAN 1.

```
S1(config)# interface vlan 1
S1(config-if)# ip address 192.168.1.11 255.255.255.0
S1(config-if)# no shutdown
S1(config-if)# end
 *Mar  1 00:07:59.048: %SYS-5-CONFIG_I: Configured from console by console
```

Step 4: Configure basic settings for switch S2.

Repeat Steps 3a. to 3f. to configure basic settings for Switch S2, via the console connection from PC-B.

Note: When you configure switch S2, remember to use hostname "S2" and the IP addressing information of S2 as shown in the Addressing Table on page 1.

Step 5: Verify network connectivity.

a. Ping each of the switches from PC-A. Were the pings successful?_____

b. Ping each of the switches from PC-B. Were the pings successful?_____

All pings to the switches should be successful now. If not, check your switch configurations.

Checkpoint: Keep the Command Prompt Window on PC-A and PC-B open, then ask your practical supervisor to check your work of Part 1

Part 2: Display, Describe, and Analyze Ethernet MAC Addresses

Every NIC of a device on an Ethernet LAN has a MAC address that is assigned by the manufacturer and stored in the firmware of the NIC. Ethernet MAC addresses are 48-bits long. They are displayed using six sets of hexadecimal digits that are usually separated by dashes, colons, or periods. The following example shows the same MAC address using the three different notation methods:

00-05-9A-3C-78-00 00:05:9A:3C:78:00 0005.9A3C.7800

MAC addresses are also called physical addresses, hardware addresses, or Ethernet hardware addresses.You will issue commands to display the MAC addresses on a PC and a switch, and you will analyze the properties of each one.

Step 1: Analyze the MAC address for the PCs' NICs.

Before you analyze the MAC address on PC-A and PC-B, look at the following example from the NIC of a different PC. You can issue the **ipconfig /all** command to view the MAC address of your NIC. An example screen output is shown below.

```
Ethernet adapter Local Area Connection:

   Connection-specific DNS Suffix  . :
   Description . . . . . . . . . . . : Intel(R) 82577LM Gigabit Network Connection
   Physical Address. . . . . . . . . : 5C-26-0A-24-2A-60
   DHCP Enabled. . . . . . . . . . . : No
   Autoconfiguration Enabled . . . . : Yes
   Link-local IPv6 Address . . . . . : fe80::b875:731b:3c7b:c0b1%10(Preferred)
   IPv4 Address. . . . . . . . . . . : 192.168.1.3(Preferred)
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 192.168.1.1
   DHCPv6 IAID . . . . . . . . . . . : 240920024
```

When using the **ipconfig /all** command, notice that MAC addresses are referred to as **physical addresses**. Reading the MAC address from left to right, the **first six hex digits** (3 bytes) refer to the vendor (manufacturer) of this device and they are also known as the **organizationally unique identifier (OUI)**. This 3-byte code is

assigned to the vendor by the IEEE organization. The last six digits are the **NIC serial number** assigned by the manufacturer. To find the manufacturer, you can use a tool like www.macvendorlookup.com or go to the IEEE web site to find the registered OUI vendor codes. The IEEE web site address for OUI information is http://standards.ieee.org/develop/regauth/oui/public.html.

a. Using **the above example screen output** (result of the **ipconfig /all** command), answer the following questions.

i) What is the OUI portion of the MAC address for this device?

_____

ii) What is the serial number portion of the MAC address for this device?

_____

b. From the command prompt on **PC-A**, issue the **ipconfig /all** command and identify the OUI portion of the MAC address for the NIC of PC-A, and write the information in the table below.

c. From the command prompt on **PC-B**, issue the **ipconfig /all** command and identify the OUI portion of the MAC address for the NIC of PC-B.

	PC-A NIC	PC-B NIC
OUI portion		
Serial number portion		

Step 2. Analyze the MAC address for the S1 F0/6 interface.

a. Use the **show interfaces** command for interface F0/6 of S1 to display MAC address information. A sample is shown below. Use output generated by your switch to answer the questions.

```
S1> show interfaces f0/6
FastEthernet0/6 is up, line protocol is up (connected)
  Hardware is Fast Ethernet, address is 0cd9.96e8.7285 (bia 0cd9.96e8.7285) MTU
  1500 bytes, BW 100000 Kbit, DLY 100 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA, loopback not set
  Keepalive set (10 sec)
  Full-duplex, 100Mb/s, media type is 10/100BaseTX
  input flow-control is off, output flow-control is unsupported ARP
  type: ARPA, ARP Timeout 04:00:00
  Last input 00:00:45, output 00:00:00, output hang never Last
  clearing of "show interface" counters never
  Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0 Queueing
  strategy: fifo
  Output queue: 0/40 (size/max)
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec 3362
     packets input, 302915 bytes, 0 no buffer Received
     265 broadcasts (241 multicasts)
     0 runts, 0 giants, 0 throttles
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored
     0 watchdog, 241 multicast, 0 pause input
     0 input packets with dribble condition detected 38967
     packets output, 2657748 bytes, 0 underruns
     0 output errors, 0 collisions, 1 interface resets
     0 babbles, 0 late collision, 0 deferred
     0 lost carrier, 0 no carrier, 0 PAUSE output
     0 output buffer failures, 0 output buffers swapped out
```

b. What is the MAC address for F0/6 on S1? _____

c. What is the MAC serial number for F0/6? _____

d. What is the OUI for F0/6? _____

e. Why does the output show the same MAC address twice? (Note: "bia" in the output above means "burned in address")_____

_____

Step 4. Analyze the MAC address for the S2 F0/18 interface.

You can use a variety of commands to display MAC addresses on the switch.

a. Use the **show interfaces** command for interface F0/18 of S2 to display MAC address information. A sample is shown below. Use output generated by your switch to answer the questions.

```
S2> show interfaces f0/18
FastEthernet0/18 is up, line protocol is up (connected)
  Hardware is Fast Ethernet, address is 0cd9.96e8.7285 (bia 0cd9.96e8.7285) MTU
  1500 bytes, BW 100000 Kbit, DLY 100 usec,


     reliability 255/255, txload 1/255, rxload 1/255
    Encapsulation ARPA, loopback not set
    Keepalive set (10 sec)
    Full-duplex, 100Mb/s, media type is 10/100BaseTX
    input flow-control is off, output flow-control is unsupported ARP
    type: ARPA, ARP Timeout 04:00:00
    Last input 00:00:45, output 00:00:00, output hang never
    Last clearing of "show interface" counters never
    Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0 Queueing
  strategy: fifo
    Output queue: 0/40 (size/max)
    5 minute input rate 0 bits/sec, 0 packets/sec
    5 minute output rate 0 bits/sec, 0 packets/sec 3362
     packets input, 302915 bytes, 0 no buffer Received
     265 broadcasts (241 multicasts)
     0 runts, 0 giants, 0 throttles
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored
     0 watchdog, 241 multicast, 0 pause input
     0 input packets with dribble condition detected
     38967 packets output, 2657748 bytes, 0 underruns
     0 output errors, 0 collisions, 1 interface resets
     0 babbles, 0 late collision, 0 deferred
     0 lost carrier, 0 no carrier, 0 PAUSE output
     0 output buffer failures, 0 output buffers swapped out
```

b. What is the MAC address for F0/18 on S2? _____

c. What is the MAC serial number for F0/18? _____

d. What is the OUI for F0/18? _____

_____

Part 3: Examine the Switch MAC Address Table

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.

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. Issue the **show interface F0/1** command on each switch's console session window. On the second line of command output, what is the hardware addresses (or burned-in address [bia])?

S1 F0/1 MAC Address:_____ S2 F 0/1 MAC Address: _____

c. Issue the **show interface vlan 1** command on each switch's console session window. On the second line of command output, what is the hardware addresses (or burned-in address [bia])?

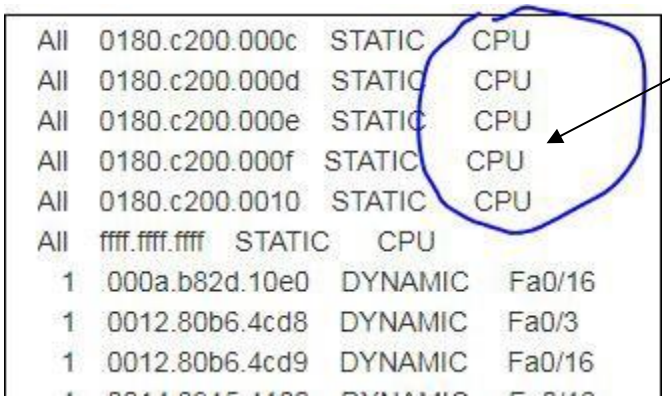
S1 VLAN 1 MAC Address:_____ S2 VLAN 1 MAC Address: _____

Step 2: Display each switch's MAC address table.

a. On each switch, in privileged EXEC mode, type the **show mac address-table** command and press Enter. To see ALL of the information available, press the SPACE bar.

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

b. Are there any MAC addresses recorded in the MAC address table? _____



c. Ignoring any MAC addresses that are mapped to the CPU (if any), record the MAC addresses in the table and the switch ports that they are mapped to. Also write in the third column what devices the ports belong to.

MAC address	switch port	device

d. 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 each switch's MAC address table and display the MAC address table again.

Note: Read the instructions of the following steps (a and b) BEFORE starting doing them.

This part of the exercise works best if you **follow the instructions below** to **clear**, and then "**very quickly**" type the given commands.

a. On **each** switch, in privileged EXEC mode, type the **clear mac address-table dynamic** command and press **Enter**.

```
S2# clear mac address-table dynamic
```

b. **Very quickly** type the **show mac address-table** command again (instead of typing the command again, you can use the up-arrow key on keyboard to find the **show mac address-table** you typed in previously).

Does the MAC address table have any addresses in it for VLAN 1? _____

Wait 10 seconds or longer, 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 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.

_____

b. On 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 _____

c. On S1, 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 _____

Appendix: Initializing and Reloading a Switch

Step 1: Connect to the switch.

Console into the switch and enter privileged EXEC mode.

```
Switch> enable
Switch#
```

Step 2: Determine if there have been any virtual local-area networks (VLANs) created.

Use the **show flash** command to determine if any VLANs have been created on the switch.

```
Switch# show flash
Directory of flash:/
    2  -rwx        1919   Mar 1 1993 00:06:33 +00:00  private-config.text
    3  -rwx        1632   Mar 1 1993 00:06:33 +00:00  config.text
    4  -rwx       13336   Mar 1 1993 00:06:33 +00:00  multiple-fs
    5  -rwx    11607161   Mar 1 1993 02:37:06 +00:00  c2960-lanbasek9-mz.150-2.SE.bin
    6  -rwx         616   Mar 1 1993 00:07:13 +00:00  vlan.dat
32514048 bytes total (20886528 bytes free)
Switch#
```

NOTE: this may not appear in YOUR switch.

Step 3: Delete the VLAN file.

a. If the **vlan.dat** file was found in flash, then delete this file.

```
Switch# delete vlan.dat
Delete filename [vlan.dat]?
```

You will be prompted to verify the file name. At this point, you can change the file name or just press Enter if you have entered the name correctly.

b. When you are prompted to delete this file, press Enter to confirm the deletion. (Pressing any other key will abort the deletion.)

```
Delete flash:/vlan.dat? [confirm]
Switch#
```

Step 4: Erase the startup configuration file.

Use the **erase startup-config** command to erase the startup configuration file from NVRAM. When you are prompted to remove the configuration file, press Enter to confirm the erase. (Pressing any other key will abort the operation.)

```
Switch# erase startup-config
Erasing the nvram filesystem will remove all configuration files! Continue? [confirm] [OK]
Erase of nvram: complete
Switch#
```

Step 5: Reload the switch.

Reload the switch to remove any old configuration information from memory. When you are prompted to reload the switch, press Enter to proceed with the reload. (Pressing any other key will abort the reload.)

```
Switch# reload
Proceed with reload? [confirm]
```

Note: You may receive a prompt to save the running configuration prior to reloading the switch. Type **no** and press Enter.

```
System configuration has been modified. Save? [yes/no]: no
```

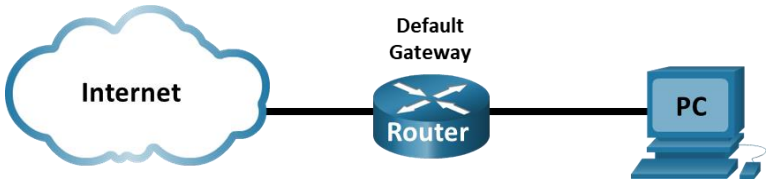
Step 6: Bypass the initial configuration dialog.

After the switch reloads, you should see a prompt to enter the initial configuration dialog. Type **no** at the prompt and press Enter.

```
Would you like to enter the initial configuration dialog? [yes/no]: no
Switch>
```

Lab - Examine Ethernet Frames

Topology



Objectives

Examine the Header Fields in an Ethernet Frame

Background / Scenario

When upper layer protocols communicate with each other, data flows down the Open Systems Interconnection (OSI) layers and is encapsulated into a Layer 2 frame. The frame composition is dependent on the media access type. For example, if the upper layer protocols are TCP and IP and the media access is Ethernet, then the Layer 2 frame encapsulation will be Ethernet II. This is typical for a LAN environment.

When learning about Layer 2 concepts, it is helpful to analyze frame header information. In this lab, you will review the fields contained in an Ethernet frame.

Part 1: Examine the Header Fields in an Ethernet Frame

In Part 1, you will examine the header fields and content in an Ethernet frame. A Wireshark capture will be used to examine the contents in those fields.

Step 1: Review the Ethernet header field descriptions and lengths.

Preamble	Destination Address	Source Address	Frame Type	Data	FCS
8 Bytes	6 Bytes	6 Bytes	2 Bytes	46 – 1500 Bytes	4 Bytes

Step 2: Examine the network configuration and the MAC address of the PC.

Refer to the following screen output of the `ipconfig /all` command, answer the following questions:

a. What is this PC's IP address? _____

b. What is this PC's default gateway address? _____

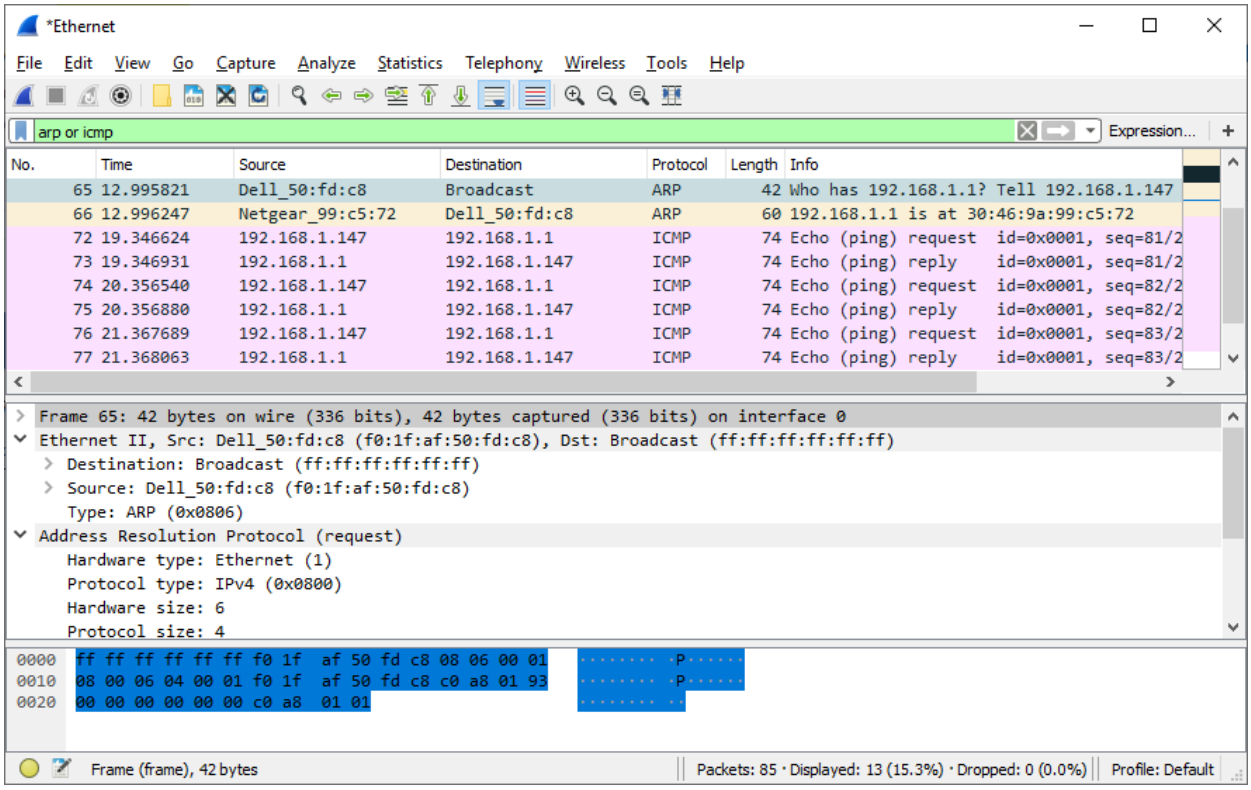
c. What is this PC's MAC address? _____

```
C:\> ipconfig /all
Ethernet adapter Ethernet:
   Connection-specific DNS Suffix  . :
   Description . . . . . . . . . . . : Intel(R) 82579LM Gigabit Network Connection
   Physical Address. . . . . . . . . : F0-1F-AF-50-FD-C8
   DHCP Enabled. . . . . . . . . . . : Yes
   Autoconfiguration Enabled . . . . : Yes
   Link-local IPv6 Address . . . . . : fe80::58c5:45f2:7e5e:29c2%11(Preferred)
   IPv4 Address. . . . . . . . . . . : 192.168.1.147(Preferred)
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Lease Obtained. . . . . . . . . . : Friday, September 6, 2019 11:08:36 AM
   Lease Expires . . . . . . . . . . : Saturday, September 7, 2019 11:08:36 AM
   Default Gateway . . . . . . . . . : 192.168.1.1
   DHCP Server . . . . . . . . . . . : 192.168.1.1
<output omitted>
```

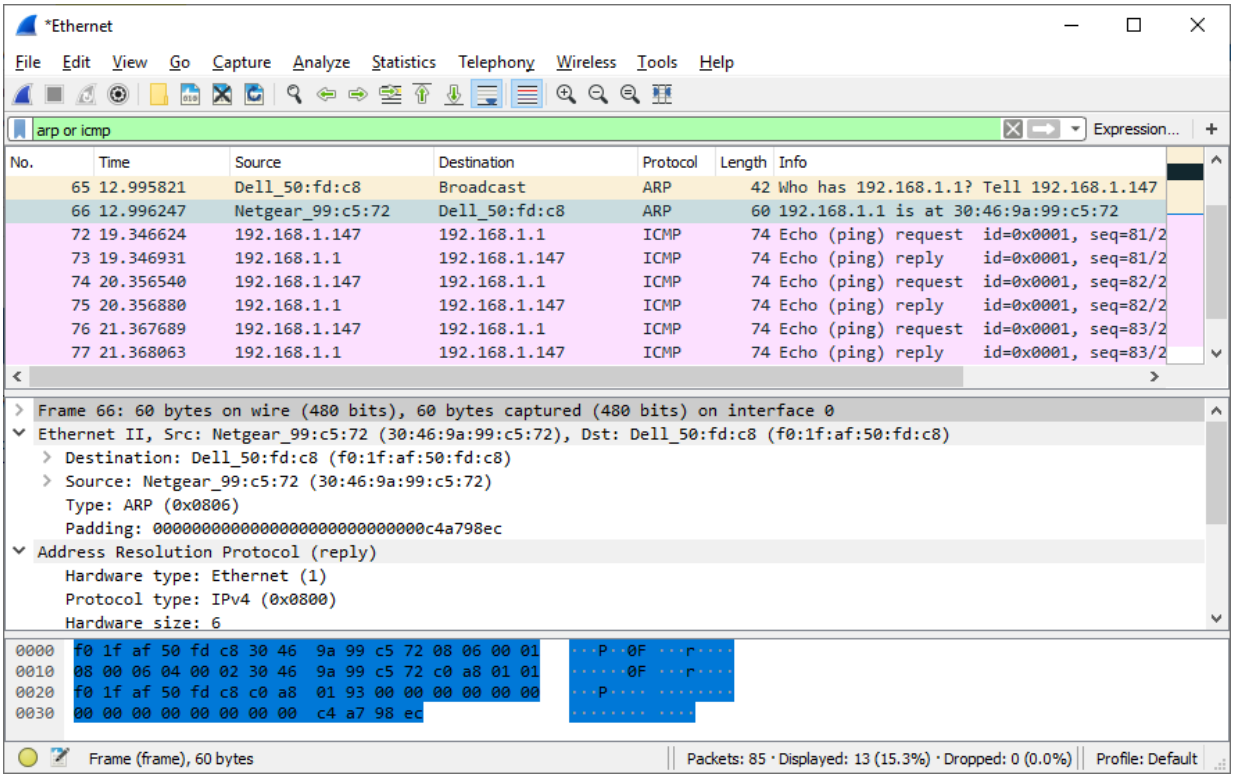
Step 3: Examine Ethernet frames in a Wireshark capture.

The screenshots of the Wireshark capture below shows the packets generated by a ping being issued from a PC host to its default gateway. A filter has been applied to Wireshark to view the ARP and ICMP protocols only. ARP stands for address resolution protocol. ARP is a communication protocol that is used for determining the MAC address that is associated with the IP address. The session begins with an ARP query and reply for the MAC address of the gateway router, followed by four ping requests and replies.

This screenshot highlights the frame details for an ARP request (line # 65).



This screenshot highlights the frame details for an ARP reply (line # 66).



Step 4: Examine the Ethernet header contents of an ARP request.

The following table takes the first frame in the Wireshark capture (line # 65).and displays the data in the Ethernet header fields. Read the information in the table carefully (and refer to the screenshot of the ARP request to see if you can find the **Values** of the **Fields** shown in this table)

Field	Value	Description
Preamble	Not shown in capture	This field contains synchronizing bits, processed by the NIC hardware.
Destination Address	Broadcast (ff:ff:ff:ff:ff:ff)	Layer 2 addresses for the frame. Each address is 48 bits long, or 6 octets, expressed as 12 hexadecimal digits, `0-9,A-F`. A common format is `12:34:56:78:9A:BC`. The first six hex numbers indicate the manufacturer of the network interface card (NIC), the last six hex numbers are the serial number of the NIC. The destination address may be a broadcast, which contains all ones, or a unicast. The source address is always unicast.
Source Address	Dell_50:fd:c8 (f0:1f:af:50:fd:c8)	
Frame Type	0x0806	For Ethernet II frames, this field contains a hexadecimal value that is used to indicate the type of upper-layer protocol in the data field. There are numerous upper-layer protocols supported by Ethernet II. Two common frame types are these: Value Description `0x0800` IPv4 Protocol `0x0806` Address Resolution Protocol (ARP)
Data	ARP	Contains the encapsulated upper-level protocol. The data field is between 46 – 1,500 bytes.
FCS	Not shown in capture	Frame Check Sequence, used by the NIC to identify errors during transmission. The value is computed by the sending device, encompassing frame addresses, type, and data field. It is verified by the receiver.

a. What is significant about the **Value** of the **Destination Address** field? _____

b. Why does the PC send out a broadcast ARP prior to sending the first ping request? _____

c. What is the MAC address of the source in this frame of the ARP request ?_____

d. What is the Vendor ID (OUI) of the Source NIC in this request frame?_____

e. What portion of a MAC address is the OUI? _____

f. What is the NIC serial number of the source MAC address in this request frame? _____