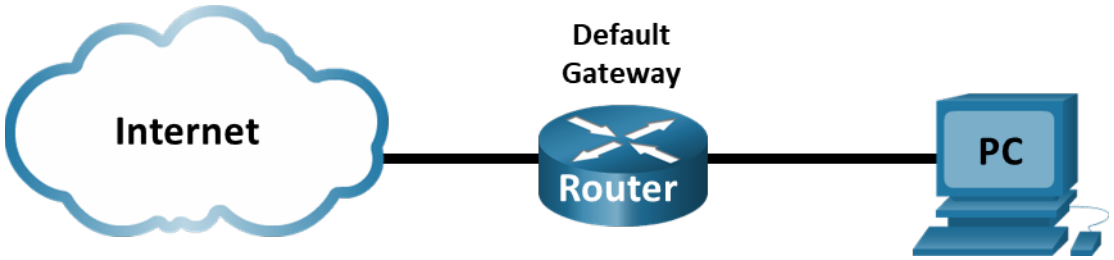
Lab - Use Wireshark to Examine Ethernet Frames (Instructor Version)

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

Topology



Objectives

Part 1: Examine the Header Fields in an Ethernet II Frame

Part 2: Use Wireshark to Capture and Analyze Ethernet Frames

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 the first part of this lab, you will review the fields contained in an Ethernet II frame. In Part 2, you will use Wireshark to capture and analyze Ethernet II frame header fields for local and remote traffic.

Instructor Note: This lab assumes that the student is using a PC with internet access. It also assumes that Wireshark has been pre-installed on the PC. The screenshots in this lab were taken from Wireshark v2.4.3 for Windows 10 (64bit).

Required Resources

- 1 PC (Windows with internet access and with Wireshark installed)

Instructions

Part 1: Examine the Header Fields in an Ethernet II Frame

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

Step 1: Review the Ethernet II 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 of the PC.

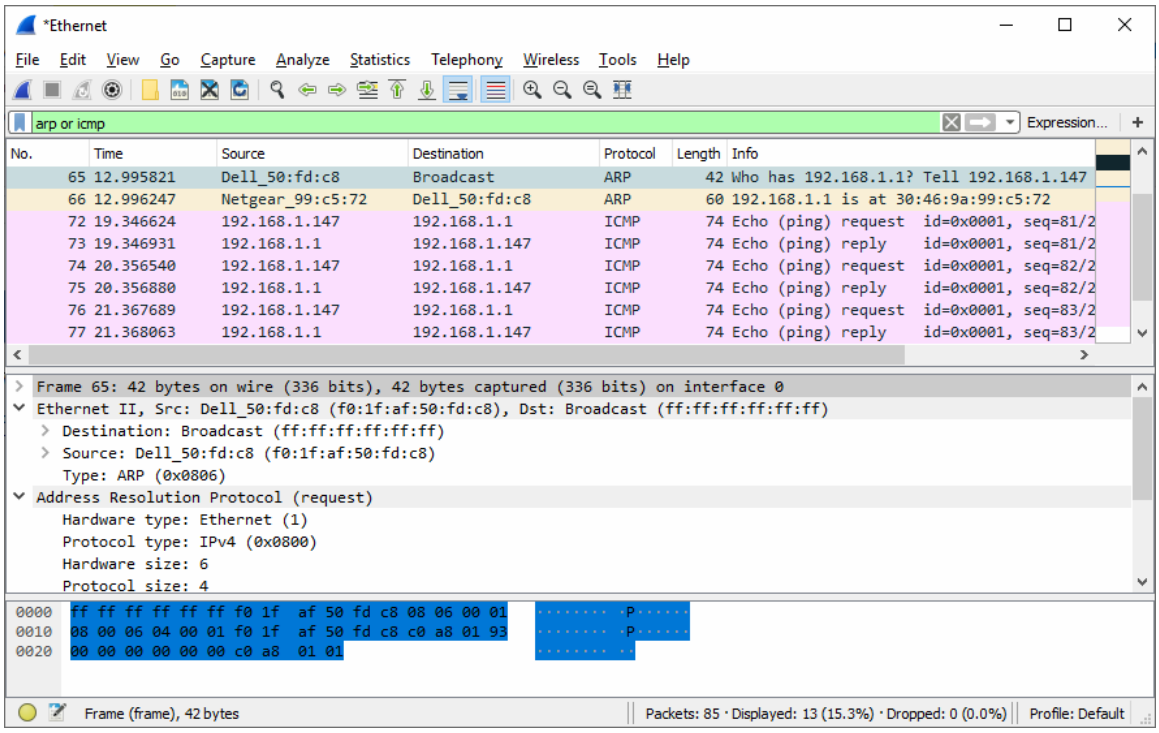
In this example, this PC host IP address is 192.168.1.147 and the default gateway has an IP address of 192.168.1.1.

```
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>
```

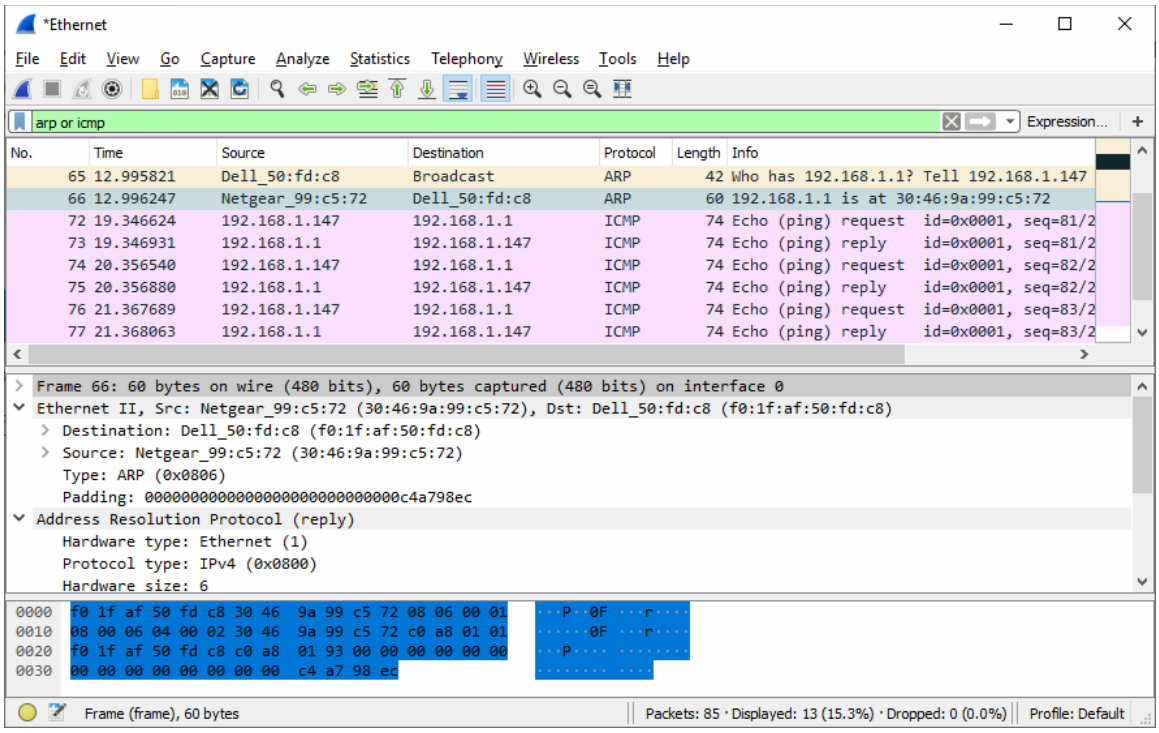
Step 3: Examine Ethernet frames in a Wireshark capture.

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.



This screenshot highlights the frame details for an ARP reply.



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

The following table takes the first frame in the Wireshark capture and displays the data in the Ethernet II header fields.

Field	Value	Description
Preamble	Not shown in capture	This field contains synchronizing bits, processed by the NIC hardware.
Destination Address Source Address	Broadcast (ff:ff:ff:ff:ff:ff) Netgear_99:c5:72 (30:46:9a:99:c5:72)	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.
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.

What is significant about the contents of the destination address field?

All hosts on the LAN will receive this broadcast frame. The host with the IP address of 192.168.1.1 (default gateway) will send a unicast reply to the source (PC host). This reply contains the MAC address of the NIC of the default gateway.

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

The PC cannot send a ping request to a host until it determines the destination MAC address, so that it can build the frame header for that ping request. The ARP broadcast is used to request the MAC address of the host with the IP address contained in the ARP.

What is the MAC address of the source in the first frame?

It varies; in this case, it is f0:1f:af:50:fd:c8.

What is the Vendor ID (OUI) of the Source NIC in the ARP reply?

It varies, in this case, it is Netgear.

What portion of the MAC address is the OUI?

The first 3 octets of the MAC address indicate the OUI.

What is the NIC serial number of the source?

It may vary, it is 99:c5:72 in this case.

Part 2: Use Wireshark to Capture and Analyze Ethernet Frames

In Part 2, you will use Wireshark to capture local and remote Ethernet frames. You will then examine the information that is contained in the frame header fields.

Step 1: Determine the IP address of the default gateway on your PC.

Open a command prompt window and issue the **ipconfig** command.

What is the IP address of the PC default gateway?

Answers will vary.

Step 2: Start capturing traffic on your PC NIC.

a. Open Wireshark to start data capture.

b. Observe the traffic that appears in the packet list window.

Step 3: Filter Wireshark to display only ICMP traffic.

You can use the filter in Wireshark to block visibility of unwanted traffic. The filter does not block the capture of unwanted data; it only filters what you want to display on the screen. For now, only ICMP traffic is to be displayed.

In the Wireshark **Filter** box, type **icmp**. The box should turn green if you typed the filter correctly. If the box is green, click **Apply** (the right arrow) to apply the filter.

Step 4: From the command prompt window, ping the default gateway of your PC.

From the command window, ping the default gateway using the IP address that you recorded in Step 1.

Step 5: Stop capturing traffic on the NIC.

Click the **Stop Capturing Packets** icon to stop capturing traffic.

Step 6: Examine the first Echo (ping) request in Wireshark.

The Wireshark main window is divided into three sections: the packet list pane (top), the **Packet Details** pane (middle), and the **Packet Bytes** pane (bottom). If you selected the correct interface for packet capturing previously, Wireshark should display the ICMP information in the packet list pane of Wireshark.

a. In the packet list pane (top section), click the first frame listed. You should see **Echo (ping) request** under the **Info** heading. The line should now be highlighted.

b. Examine the first line in the packet details pane (middle section). This line displays the length of the frame.

c. The second line in the packet details pane shows that it is an Ethernet II frame. The source and destination MAC addresses are also displayed.

What is the MAC address of the PC NIC?

Your answers will vary.

What is the default gateway's MAC address?

Your answers will vary.

d. You can click the greater than (>) sign at the beginning of the second line to obtain more information about the Ethernet II frame.

What type of frame is displayed?

0x0800 or an IPv4 frame type.

e. The last two lines displayed in the middle section provide information about the data field of the frame. Notice that the data contains the source and destination IPv4 address information.

What is the source IP address?

Your answers will vary.

What is the destination IP address?

Your answers will vary.

f. You can click any line in the middle section to highlight that part of the frame (hex and ASCII) in the **Packet Bytes** pane (bottom section). Click the **Internet Control Message Protocol** line in the middle section and examine what is highlighted in the **Packet Bytes** pane.

What do the last two highlighted octets spell?

hi

g. Click the next frame in the top section and examine an Echo reply frame. Notice that the source and destination MAC addresses have reversed, because this frame was sent from the default gateway router as a reply to the first ping.

What device and MAC address is displayed as the destination address?

Your answers will vary.

Step 7: Capture packets for a remote host.

a. Click the **Start Capture** icon to start a new Wireshark capture. You will receive a popup window asking if you would like to save the previous captured packets to a file before starting a new capture. Click **Continue without Saving**.

b. In a command prompt window, ping www.cisco.com.

c. Stop capturing packets.

d. Examine the new data in the packet list pane of Wireshark.

In the first echo (ping) request frame, what are the source and destination MAC addresses?

Source:

This should be the MAC address of the PC.

Destination:

This should be the MAC address of the Default Gateway.

What are the source and destination IP addresses contained in the data field of the frame?

Source:

This is still the IP address of the PC.

Destination:

This is the address of the server at www.cisco.com.

Compare these addresses to the addresses you received in Step 6. The only address that changed is the destination IP address. Why has the destination IP address changed, while the destination MAC address remained the same?

Layer 2 frames never leave the LAN. When a ping is issued to a remote host, the source will use the default gateway MAC address for the frame destination. The default gateway receives the packet, strips the Layer 2 frame information from the packet and then creates a new frame header with the MAC address of the next hop. This process continues from router to router until the packet reaches its destination IP address.

Reflection Question

Wireshark does not display the preamble field of a frame header. What does the preamble contain?

The preamble field contains seven octets of alternating 1010 sequences, and one octet that signals the beginning of the frame, 10101011.