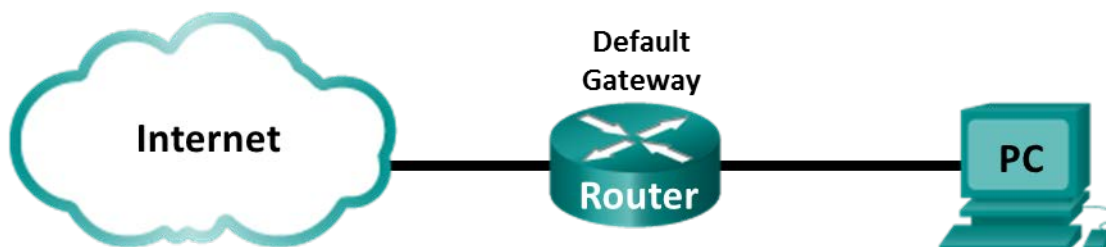


Lab – Using Wireshark to Examine Ethernet Frames

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.

Required Resources

- 1 PC (Windows 7, 8, or 10 with internet access with Wireshark installed)

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.

This PC host IP address is 192.168.1.147 and the default gateway has an IP address of 192.168.1.1.

```
Microsoft Windows [Version 10.0.16299.64]
(c) 2017 Microsoft Corporation. All rights reserved.

C:\> ipconfig /all

Windows IP Configuration

    Host Name . . . . . : DESKTOP-C73CB0M
    Primary Dns Suffix . . . . . :
    Node Type . . . . . : Hybrid
    IP Routing Enabled. . . . . : No
    WINS Proxy Enabled. . . . . : No

Ethernet adapter Ethernet:

    Connection-specific DNS Suffix . :
    Description . . . . . : Intel(R) 82577LM Gigabit Network Connection
    Physical Address. . . . . : 00-26-B9-DD-00-91
    DHCP Enabled. . . . . : Yes
    Autoconfiguration Enabled . . . . : Yes
    Link-local IPv6 Address . . . . . : fe80::d009:d939:110f:1b7f%20 (Preferred)
    IPv4 Address. . . . . : 192.168.1.147 (Preferred)
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 192.168.1.1
    DHCP Server . . . . . : 192.168.1.1
```

Step 3: Examine Ethernet frames in a Wireshark capture.

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. The

Lab – Using Wireshark to Examine Ethernet Frames

session begins with an ARP query for the MAC address of the gateway router, followed by four ping requests and replies.

The image shows a Wireshark packet capture window titled "*Ethernet". The filter bar at the top is set to "arp or icmp". The packet list shows several packets, with packet 25 selected. The packet details pane shows the structure of the selected packet: Ethernet II, Src: BelkinIn_9f:6b:8c (14:91:82:9f:6b:8c), Dst: Dell_dd:00:91 (00:26:b9:dd:00:91), and Address Resolution Protocol (request). The packet bytes pane shows the raw data in hexadecimal and ASCII.

No.	Time	Source	Destination	Protocol	Length	Info
25	30.848323	BelkinIn_9f:6b:8c	Dell_dd:00:91	ARP	60	Who has 192.168.1.147? ...
26	30.848365	Dell_dd:00:91	BelkinIn_9f:6b:8c	ARP	42	192.168.1.147 is at 00:...
30	45.346129	192.168.1.147	192.168.1.1	ICMP	74	Echo (ping) request id...
31	45.346432	192.168.1.1	192.168.1.147	ICMP	74	Echo (ping) reply id...
32	46.359847	192.168.1.147	192.168.1.1	ICMP	74	Echo (ping) request id...
33	46.360272	192.168.1.1	192.168.1.147	ICMP	74	Echo (ping) reply id...
34	47.375524	192.168.1.147	192.168.1.1	ICMP	74	Echo (ping) request id...
35	47.375919	192.168.1.1	192.168.1.147	ICMP	74	Echo (ping) reply id...

Frame 25: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface 0
Ethernet II, Src: BelkinIn_9f:6b:8c (14:91:82:9f:6b:8c), Dst: Dell_dd:00:91 (00:26:b9:dd:00:91)
Address Resolution Protocol (request)

```
0000  00 26 b9 dd 00 91 14 91 82 9f 6b 8c 08 06 00 01  .&.....k....
0010  08 00 06 04 00 01 14 91 82 9f 6b 8c c0 a8 01 01  .....k....
0020  00 00 00 00 00 00 c0 a8 01 93 00 00 00 00 00 00  .....
0030  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  .....
```

Frame (frame), 60 bytes | Packets: 48 · Displayed: 12 (25.0%) | Profile: Default

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	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	BelkinIn_9f:6b:8c (14:91:82:9f:6b:8c)							
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: <table><tr><td>Value</td><td>Description</td></tr><tr><td>0x0800</td><td>IPv4 Protocol</td></tr><tr><td>0x0806</td><td>Address Resolution Protocol (ARP)</td></tr></table>	Value	Description	0x0800	IPv4 Protocol	0x0806	Address Resolution Protocol (ARP)
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 machine, encompassing frame addresses, type, and data field. It is verified by the receiver.						

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

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

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

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

What portion of the MAC address is the OUI?

What is the NIC serial number of the source?

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.

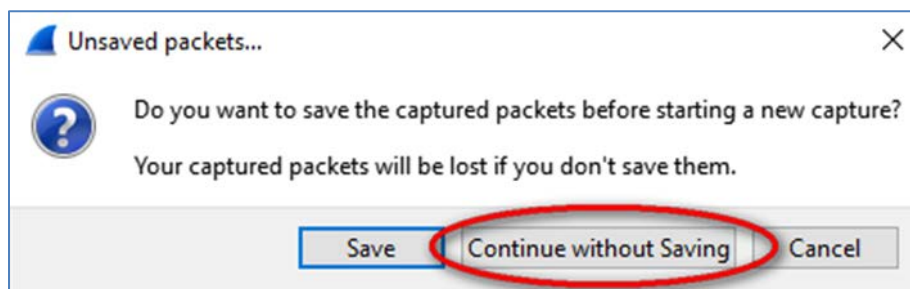
Step 1: Determine the IP address of the default gateway on your PC.

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

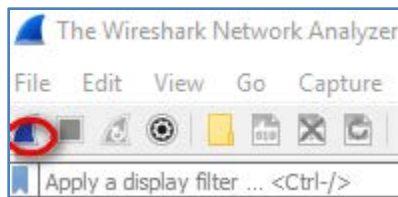
What is the IP address of the PC default gateway?

Step 2: Start capturing traffic on your PC NIC.

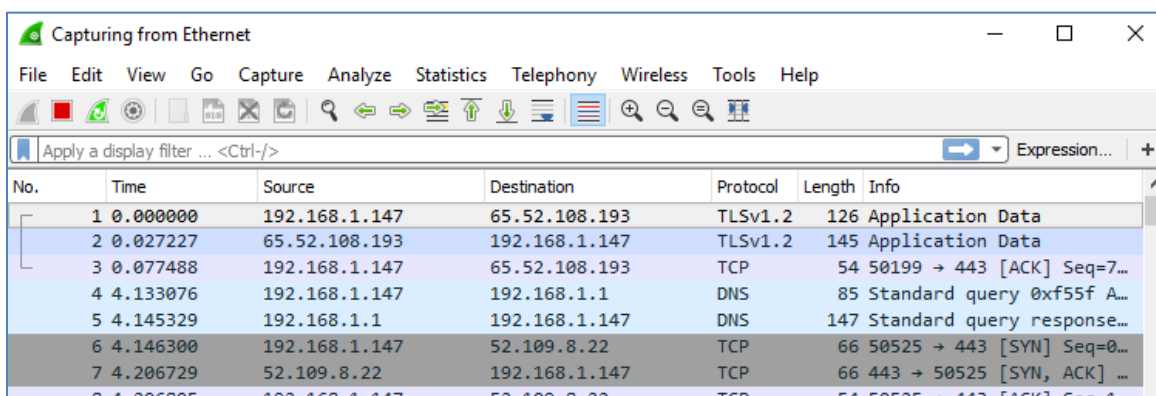
- a. Close Wireshark. No need to save the captured data.



- b. Open Wireshark, start data capture.



- c. Observe the traffic that appears in the packet list window.



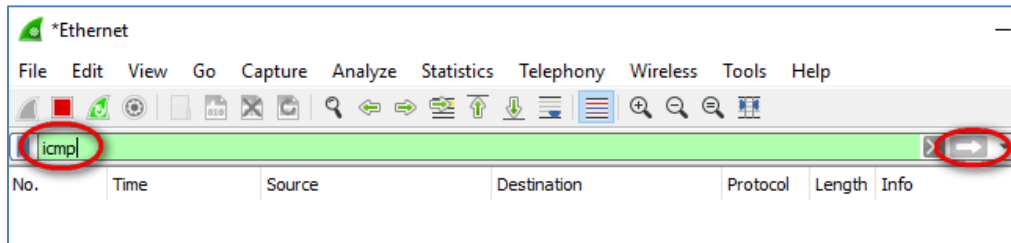
No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	192.168.1.147	65.52.108.193	TLSv1.2	126	Application Data
2	0.027227	65.52.108.193	192.168.1.147	TLSv1.2	145	Application Data
3	0.077488	192.168.1.147	65.52.108.193	TCP	54	50199 → 443 [ACK] Seq=7...
4	4.133076	192.168.1.147	192.168.1.1	DNS	85	Standard query 0xf55f A...
5	4.145329	192.168.1.1	192.168.1.147	DNS	147	Standard query response...
6	4.146300	192.168.1.147	52.109.8.22	TCP	66	50525 → 443 [SYN] Seq=0...
7	4.206729	52.109.8.22	192.168.1.147	TCP	66	443 → 50525 [SYN, ACK] ...
8	4.206805	192.168.1.147	52.109.8.22	TCP	54	50525 → 443 [ACK] Seq=1...

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 to display on the screen. For now, only ICMP traffic is to be displayed.

Lab – Using Wireshark to Examine Ethernet Frames

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.

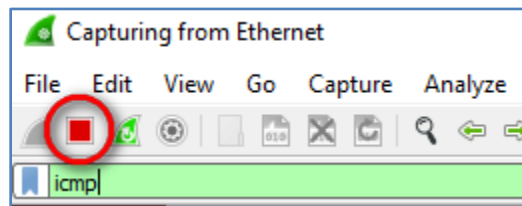


Step 4: From the command prompt window, ping the default gateway of your PC.

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 Capture** icon to stop capturing traffic.

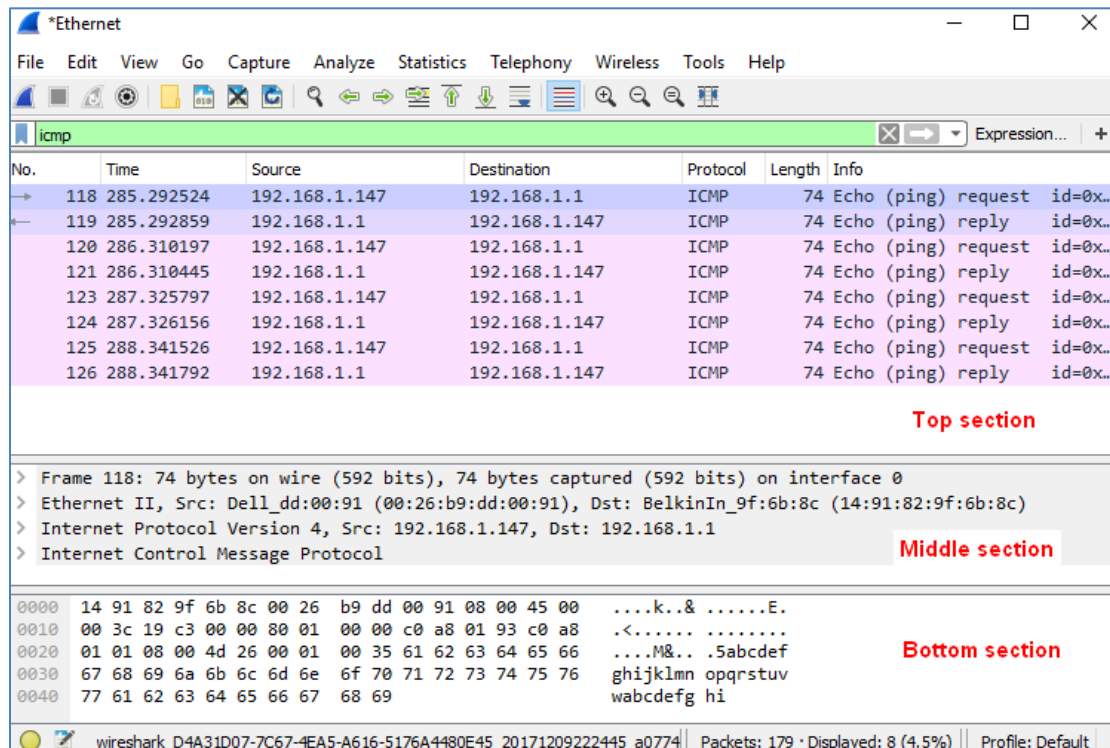


Step 6: Examine the first Echo (ping) request in Wireshark.

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 in

Lab – Using Wireshark to Examine Ethernet Frames

Step 3, Wireshark should display the ICMP information in the packet list pane of Wireshark, similar to the following example.



- In the packet list pane (top section), click the first frame listed. You should see **Echo (ping) request** under the **Info** heading. This should highlight the line blue.
- Examine the first line in the packet details pane (middle section). This line displays the length of the frame; 74 bytes in this example.

- 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?

What is the default gateway's MAC address?

- You can click the plus (+) sign at the beginning of the second line to obtain more information about the Ethernet II frame. Notice that the plus sign changes to a minus (-) sign.

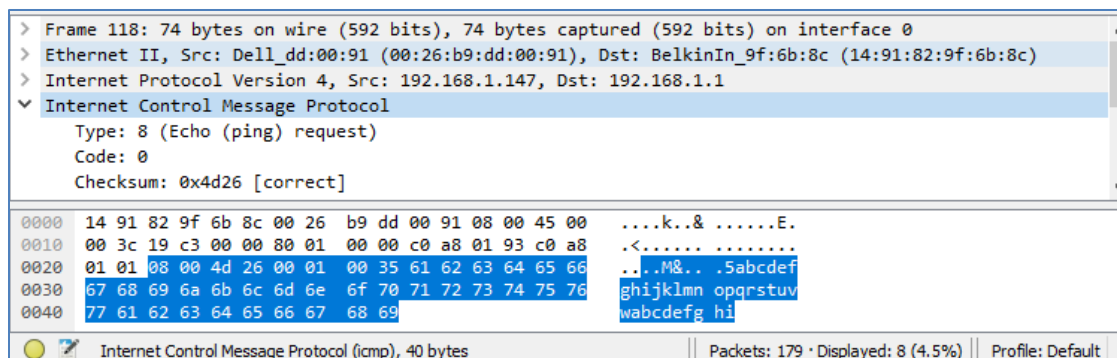
What type of frame is displayed?

- 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?

What is the destination IP address?

- 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.



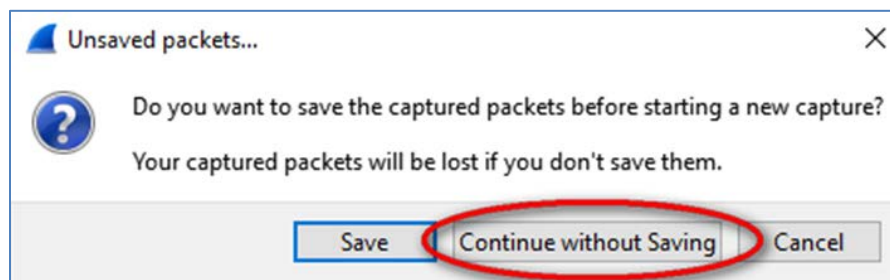
What do the last two highlighted octets spell?

- 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?

Step 7: Restart packet capture in Wireshark.

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**.



Step 8: In the command prompt window, ping www.cisco.com.

Step 9: Stop capturing packets.

Step 10: 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:

Destination:

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

Source:

Destination:

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?

Reflection

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