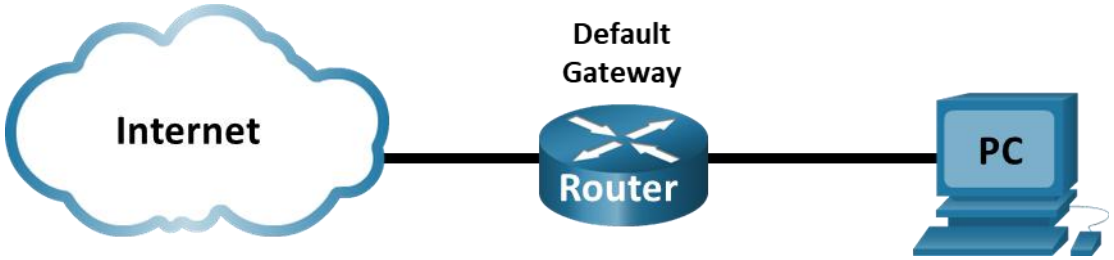
Lab - Use Wireshark to Examine Ethernet Frames

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 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 (lengkapi tabel di bawah ini).

Preamble	Destination Address	Source Address	Frame Type	Data	FCS

© 2013 - 2026 Cisco and/or its affiliates. All rights reserved. Cisco Public

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    (tambahkan screenshot dari komputer anda)

Ethernet adapter Ethernet:

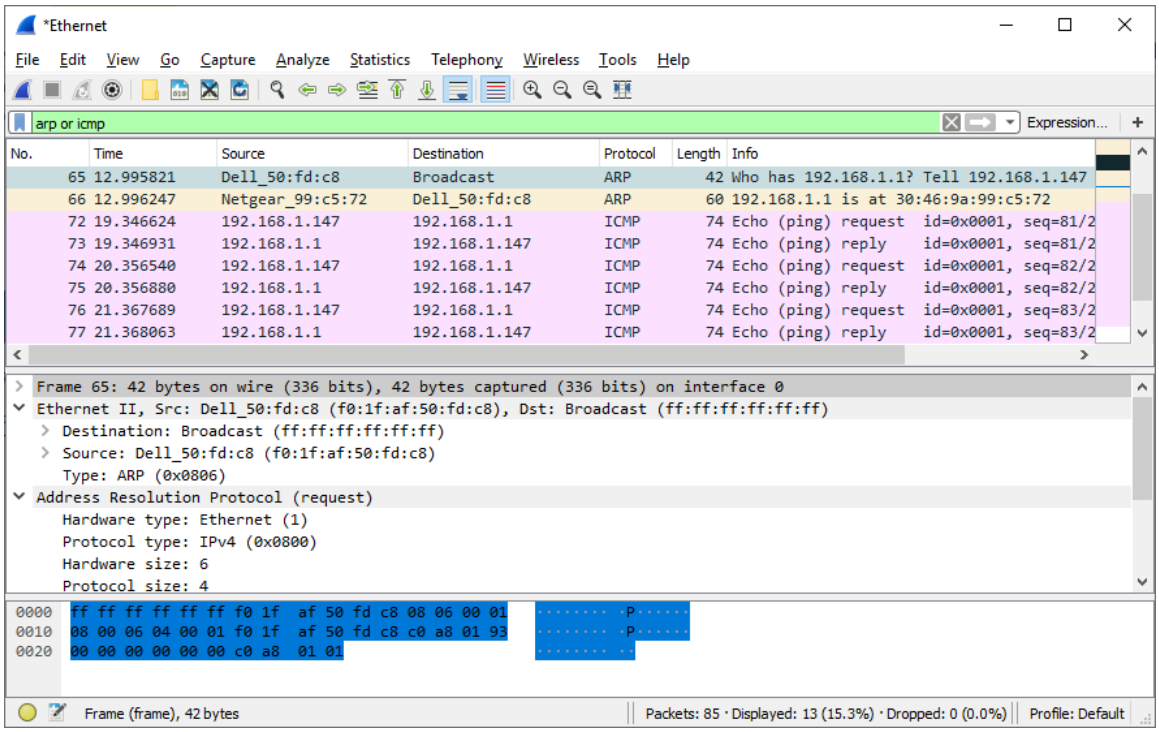
   Connection-specific DNS Suffix  . :
   Description . . . . . . . . . . . : Intel(R) 82579LM Gigabit Network Connection
   Physical Address. . . . . . . . . : F0-1F-AF-50-FD-C8
   DHCP Enabled. . . . . . . . . . . : Yes
   Autoconfiguration Enabled . . . . : Yes
   Link-local IPv6 Address . . . . . : 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.

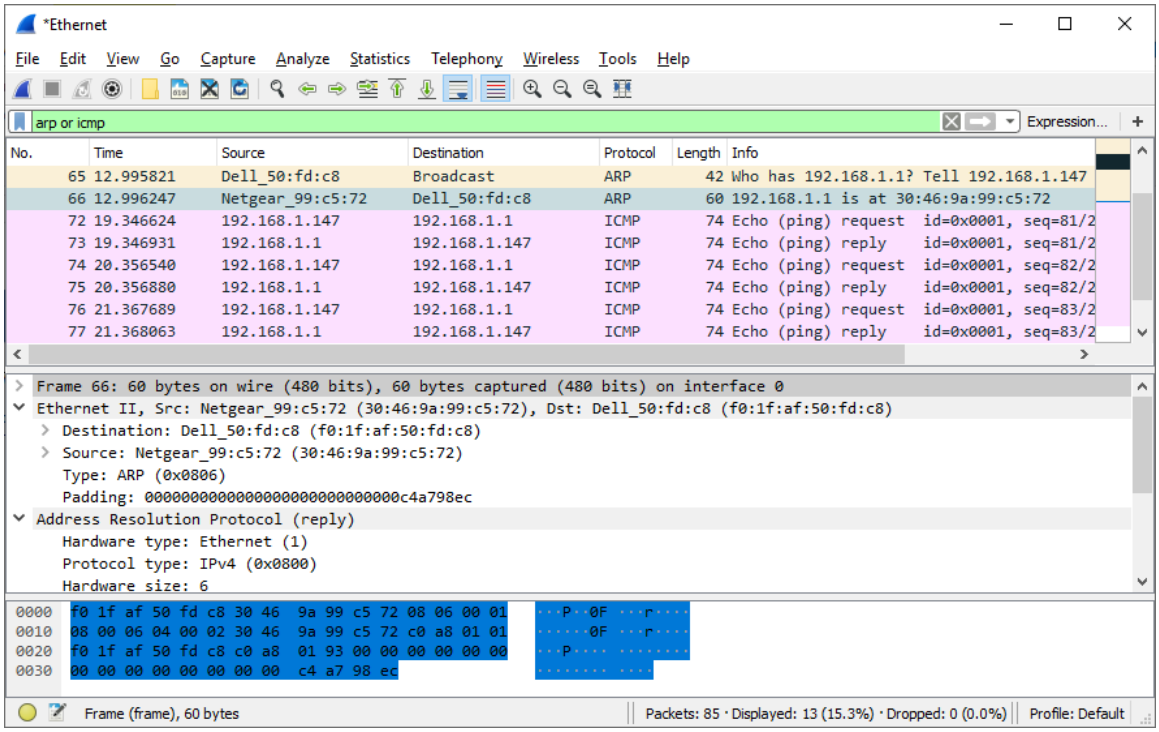
The screenshots of the Wireshark capture below shows the packets generated by a ping being issued from a PC host to its default gateway. A filter has been applied to Wireshark to view the ARP and ICMP protocols only. ARP stands for address resolution protocol. ARP is a communication protocol that is 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.

© 2013 - 2026 Cisco and/or its affiliates. All rights reserved. Cisco Public

This screenshot highlights the frame details for an ARP request (sesuaikan dengan tangkapan anda sendiri).



This screenshot highlights the frame details for an ARP reply (sesuaikan dengan tangkapan anda sendiri).



© 2013 - 2026 Cisco and/or its affiliates. All rights reserved. Cisco Public

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. Lengkapi tabel berikut ini.

Field	Value	Description
Preamble		
Destination Address Source Address		
Frame Type		
Data		
FCS		

Jawablah pertanyaan berikut ini :

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 in the ARP reply?

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.

© 2013 - 2026 Cisco and/or its affiliates. All rights reserved. Cisco Public

What is the IP address of the PC default gateway?

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?

What is the default gateway's MAC address?

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?

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?

What is the destination IP address?

© 2013 - 2026 Cisco and/or its affiliates. All rights reserved. Cisco Public

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: 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:

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?

© 2013 - 2026 Cisco and/or its affiliates. All rights reserved. Cisco Public