**ITFN 2512: Intermediate Networking and Security**

**LAB EXERCISE**

**Lab 02: Use Wireshark to View Protocol Stack and Examine Ethernet Frames**

Through this lab you will learn how network packets from upper layer of the TCP/IP stack are encapsulated in a packet at the lower layer. You will also be able capture and examine Ethernet frame and how a frame is formatted.

**Background:**

When upper layer protocols communicate with each other, data flows down the Open Systems Interconnection (OSI) layers and is encapsulated into a Layer 2 (Datalink layer) 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 Layer2 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:**

A PC or a Laptop (Windows OS with Internet access and Wireshark installed).

**Lab Activities:**

**Part I:**

In Part I, you will examine the header fields and content in an Ethernet II Frame. A Wireshark capture will be needed to examine the contents in those fields.

**Steps:**

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 |

1. **Examine the network configuration of the PC.**

Identify the IP address of your laptop and the default gateway by typing ipconfig/all at the command prompt of your laptop. Record your findings:

|  |  |  |  |
| --- | --- | --- | --- |
| **IP address (IPv4)** | **Subnet Mask** | **MAC Address** | **Default Gateway** |
| 192.168.1.254 | 255.255.255.0 | 8C-3B-AD-19-19-5D | fe80::3a3b:c8ff:fe1a:9d85%2 |

1. **Examine Ethernet frames in a Wireshark capture.**

Apply filter to view the ARP and ICMP protocols only by typing: **arp or icmp** at the Filter textbox.

1. **Examine the Ethernet II header contents of an ARP request.**

Take the first frame in the Wireshark capture and record 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 | ff:ff:ff:ff:ff:ff | Layer 2 addresses for the frame. Each address is 48 bits long.or (ff:ff:ff:ff:ff:ff) 6 octets, expressed as 12 hexadecimal digits, 0-9,A-F.  Source Address Dell 24:2a:60 A common format is B4-B6-76-21-FF-02. (B4:B6:76:21:FF:02) 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 | 2wire\_1a:9d:85 |
| Frame Type | 0x0806 | Contain a hexadecimal value. This frame type of a upper-layer protocol. Supported by ethernet two. 0x0806 is a address resolution protocol. |
| Data | ARP | Is the upper level protocol that is encapsulated. |
| FCS | Not shown | FCFS is used to detect error during a transmission. |

**Answer the following:**

1. What is significant about the contents of the destination address field? Contain nothing but   
   “f” as the broadcast address. That address sis used to send to all the devices in the network
2. Why does the PC send out a broadcast ARP prior to sending the first ping request? To first pint request so that it can know the physical address of all the host so that it can have the other MAC address in its ARP cache.
3. What is the MAC address of the source in the first frame? 1c:1b:0d:1e:af:45
4. What is the Vendor ID (OUI) of the Source's NIC? 2wire
5. What portion of the MAC address is the QUI? The first 6 number of the mac
6. What is the Source's NIC serial number? 1a:9d:85

**Part2: 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.

**Steps:**

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

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? 192.168.1.254

1. **Start capturing traffic on your PC's NIC.**
2. **Filter Wireshark to display only ICMP traffic.**
3. **From the command prompt window, ping the default gateway of your PC.**
4. **Stop capturing traffic on the NIC.**
5. **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 Step 3, Wireshark should display the ICMP information in the Packet List pane of Wireshark.

* 1. 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.
  2. Examine the first line in the Packet Details pane (middle section). This line displays the length of the frame.
  3. The second line in the Packet Details pane should 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's NIC? 8c:3b:ad:19:5d
  4. What is the default gateway's MAC address? 38:3b:c8:1a:9d”85
  5. 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.
  6. What type of frame is displayed?unicast frame
  7. 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? 192.168.1.74

What is the destination IP address? 192.168.1.254

* 1. 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.
  2. 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 reply to the first ping.

What device and MAC address is displayed as the destination address? the destination address :192.168.1.254

|  |
| --- |
| Mac address: 8c:3b:ad:19:19:5d |
|  |

1. **Restart packet capture in Wireshark.**
2. **In the command prompt window, ping** [**www.google.com**](http://www.google.com)**.**
3. **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: 8c:3c:ad:19:19:5d

Destination: 2wire\_la:9d:85

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

Source: 192.168.1.74

Destination: 192.168.1.130

Compare these addresses to the addresses you received in Step (g). 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?

The IP address changed while the destination address remained the same because a ping is issued to a remote host. The source uses the remote default gateway to get the packet, then create a new frame header to the next mac address. This process is called hop to hop since the packet will hop to another router until it reaches its destination.