|  |  |
| --- | --- |
| **Operating System &Networking Fundamentals**  Diploma in CSF/IT  Year 1 (2021/22) Semester 2 | Week **16** |
| Practical |
| **TCP/IP Protocol Suite** | |

**A. Objectives**

At the end of this practical, students would be able to use a protocol analyzer such as Wireshark to:

1. Identify and examine the protocol layers in a HTTP frame;

2. Identify broadcast frames and understand how ARP works;

3. Examine the protocol layers in a DNS frame;

4. Determine what happens when the ping command is executed.

**B. Resources**

1. Windows PC
2. Wireshark Application

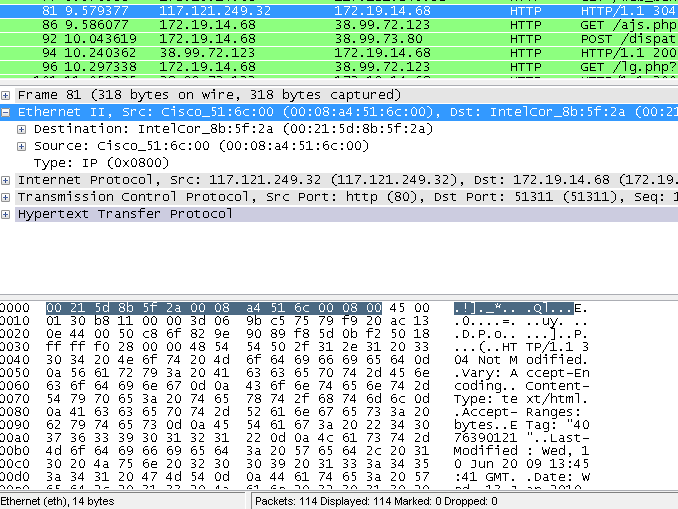
**C. Capturing Ethernet Frames Using Wireshark**

## 1. Capturing HTTP Frames

1. Launch the Wireshark application on a PC in the lab.
2. Select the “Interface” with network traffic.
3. Click ***Start*** to capture packets.

Try to browse some web pages so that Wireshark will capture some HTTP frames.

1. Click ***Stop*** to stop capturing packets and Wireshark will automatically display the results.
2. Select a frame carrying HTTP **(**Hypertext Transfer Protocol). [Note: You can type in “HTTP” in the **Filter**: textbox, click **Apply** to view only HTTP frames captured.]
3. Answer the following questions based on the HTTP frame captured:



Sample frame captured for your explanation to students. Students may capture different HTTP frames. Answers below are based on the sample frame captured.

1. Identify the protocols used in each of the following layers:

|  |  |
| --- | --- |
| **Layers** | **Protocols** |
| Data Link | Ethernet II |
| Internet | IP – Internet Protocol |
| Transport | TCP – Transmission Control Protocol |
| Application | HTTP – Hypertext Transfer Protocol |

1. What is the length of the Ethernet header?

|  |
| --- |
| 14 bytes (Ethernet header length is always 14 bytes for any frame capture):   * Destination MAC 12 Hexadecimal digits (6bytes) * Source MAC 12 hesxadecimal digits (6bytes) * Type 4 hexadecimal digits (2bytes) |

1. What is the length of the frame (from Destination MAC Address Field to the FCS field)?

|  |
| --- |
| 318 Bytes + 4 bytes = 322 bytes. We add 4 bytes because wireshark does not capture the 4 bytes of the FCS field |

1. Does this frame require padding?

|  |
| --- |
| No.  Padding is only required if the length of the (destination MAC address Field to the FCS field) is less than 64 bytes. In this particular case the length of the fram is 322 bytes. |

1. Identify the source and destination Ethernet address/MAC address in the Ethernet header.

|  |  |
| --- | --- |
| **Destination MAC Address** | 00:1c:7f:a1:02:19 |
| **Source MAC Address** | 00:08:a4:51:6c:00 |

1. Identify the source and destination IP address in the Internet Protocol header.

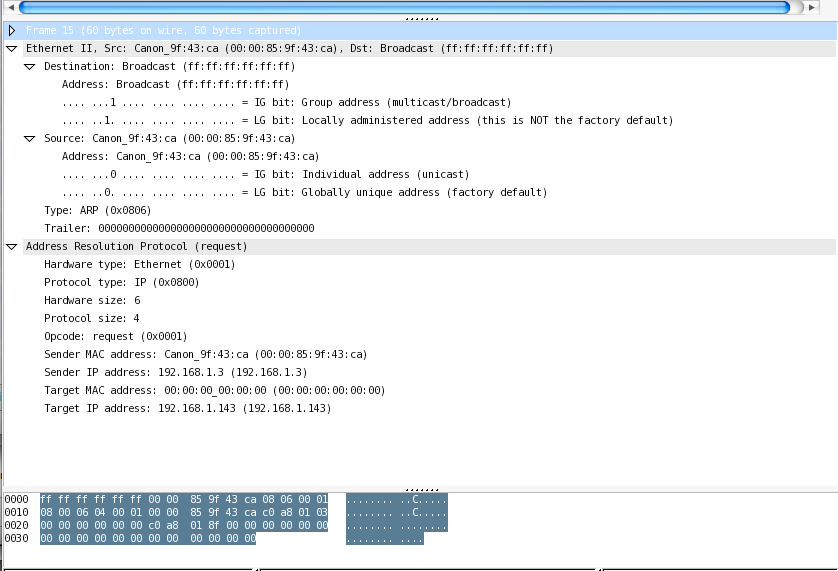
|  |  |
| --- | --- |
| **Source IP Address** | Src: xxx.xxx.xxx.xxx |
| **Destination IP Address** | Dst: xxx.xxx.xxx.xxx |

1. Identify the port number used by HTTP in the Transmission Control Protocol (TCP) header.

|  |
| --- |
| http (80) indicates that TCP port 80 (well known port) is used by HTTP Application Layer Protocol |

2. Broadcast Frames and Understanding How ARP Works

1. Select a frame carrying **ARP** protocol. A sample of the ARP Request packet is shown in Figure below.



ARP Request Frame Captured

1. Answer the following questions based on the ARP frame captured.
2. What is the Destination MAC address when the ARP is invoked?

|  |
| --- |
| ff:ff:ff:ff:ff:ff |

1. What is the term given to this special address?

|  |
| --- |
| Broadcast address on a MAC frame. |

1. Which host(s) on this Ethernet Network will process the ARP frame and respond to the source host?

|  |
| --- |
| All hosts on the same LAN will process the frame (de-encapsulation of MAC header and trailer) to get the ARP Request, but only the host with the IP address that matches with the “Target UP address” would reply. |

1. What is the value (in hex) of the Type field in the Ethernet II Header for the ARP?

If an IP packet were to be encapsulated in the frame instead of the ARP packet, what will be the value of the Type field?

|  |
| --- |
| ARP packet: Hex 0806  IP packet: Hex 0800 |

1. Explain the function and purpose of the ARP.

|  |
| --- |
|  |

1. Domain Name Service
2. Select a frame carrying DNS **(**Domain Name Service).
3. Identify the protocols used in each of the following layers:

|  |  |
| --- | --- |
| **Layers** | **Protocols** |
| Data Link | Ethernet II |
| Internet | IP |
| Transport | UDP – User protocol |
| Application | DNS – Domain name service |

1. What type of Transport Layer service does DNS **(**Domain Name Service) uses? Connection-oriented or Connectionless?

|  |
| --- |
| DNS uses UDP which is conntecionless TLS  Notes; HTTP uses TCP which is a connection oriented service |

1. The ‘ping’ command
2. Click Capture > Start to start the capturing process one more time.
3. From the PC, at the command prompt, ping the server, www.ict.np.edu.sg.
4. Click Capture > Stop to stop capturing.
5. Apply filter so that only ICMP (Internet Control Message Protocol) packets are displayed.
6. Answer the following questions based on the ICMP packets captured.
7. When you activated the ping command, how many echo (requests) and echo (replies) are generated?

|  |
| --- |
| 4 echo (requests) and 4 echo (replies) |

1. Which protocols are required for each echo (request) or echo (reply). (Your answer should include those protocols at the Internet and Data Link layers).

|  |
| --- |
| Two internet (layer 3) protocol  Internet layer: IP  Internet LayerL ICMP (internet control messsag protocl)  Datalink: Ethernet II |