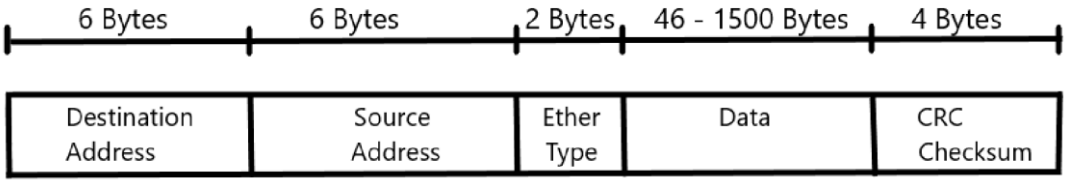
Using Wireshark to View Ethernet Frame Header Information

Introduction

As a member of the IT team at Nerdify Enterprises, you notice an unusual amount of heavy traffic on the network. To make sure that all of the traffic is legitimate, you use a protocol analyzer named Wireshark to capture some random packets for further testing.

The networking protocol used in the most modern computer network is Ethernet. The Ethernet frame format is shown below:



The header consists of the preamble, the start frame delimiter, the destination and source addresses, and the length/type field. Next, is the actual data being transmitted, followed by the pad that is used to bring the total number of bytes up to the minimum of 46 if the data field is less than 46 bytes. The last part of the frame is a 4 byte CRC (cyclic redundancy check) value used for error checking.

Objective

In this lab, the student will use Wireshark to view, examine, and document the fields in an Ethernet Frame.

Resources

- Computer with Internet connection
- Wireshark Protocol Analyzer application installed on the computer

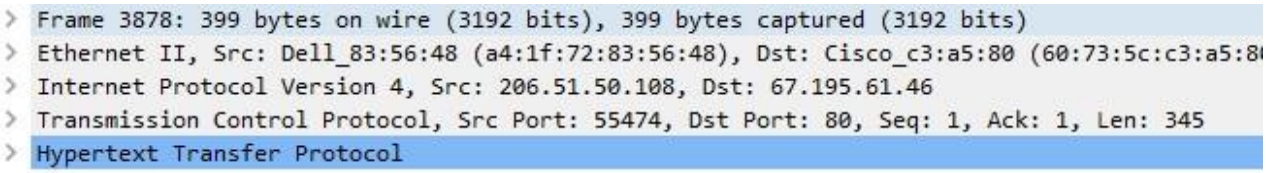
- Ethernet.pcap file downloaded from HERE

Assignment

Estimated Time for Completion: 30 minutes

1. Click the link for the Ethernet.pcap file provided by your instructor. Download, then open the file.

2. In the first column, "No.", scroll down and select packet #3878 to examine. View the details of the packet in the middle pane.



3. Click on the > next to Frame 3878 to open the **frame details**.

    a. What is the length of the frame? 399 bytes

    b. What is the maximum size of an Ethernet frame? 128

4. Observe the frame details.

*Note the **Destination, Source,** and **Type** fields. Recall that each address is **48 bits long**, or 6 bytes, **expressed as 12 hexadecimal digits: 0-9 and A-F**. The first six hex numbers indicate the manufacturer of the network interface card (NIC). The last six hex digits are the NIC identifier.*

*A **Destination Address** may be a Broadcast, which contains all 1's, or Unicast. A **Source Address** is always Unicast.*

5. Record the following information contained about this frame:

    Destination Address

    MAC address:
    60:73:5c:c3:a5:80_____

    NIC manufacturer: Cisco 60:73:5c NIC serial

    number: c3:a5:80_____

Source Address:

MAC address:
a4:1f:72:83:56:48_____

NIC manufacturer: Dell
a4:1f:72_____

NIC serial number:
83:56:48_____

6. The **Type** parameter defines the type of protocol listed inside of the frame. Some examples of values in the type/length field include the following:

   0 - 1500 length field (IEEE 802.3 and/or 802.2)

   0x0800 IP(v4), Internet Protocol version 4

   0x0806 ARP, Address Resolution Protocol

   0x8137 IPX, Internet Packet eXchange (Novell)

   0x86dd IPv6, Internet Protocol version 6

   Record the **Type** of frame being examined. IPV4

   _____

Reflection

1. What other types of packets are located in this pcap file? TCP, UDP
2. How does loading a pcap file differ from live capturing from your PC? The only difference is that you don't have to record.

Rubric

Concerns Working Towards Proficiency	Criteria Standards for This Competency	Accomplished Evidence of Mastering Competency

	Criteria #1: Answers given in lab are appropriate and valid information (11 points for each line)	
	Criteria #2: Correct answer to reflection question 1 (10 points)	

	Criteria #3: Correct answer to reflection question 2 (13 points)	