CSIS 330 – Lab 12 Wireshark – Using Wireshark to Examine Ethernet Frames Answer Template

1. Objectives

Part 1: Examine the Header Fields in an Ethernet II Frame

Part 2: Use Wireshark to Capture and Analyze Ethernet Frames

PLEASE INPUT YOUR RESPONSE IN RED

Part 1: Examine the Header Fields in an Ethernet II Frame

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

**All hosts on the LAN will receive this broadcast frame. The host with the IP address of 192.168.1.1 (default gateway) will send a unicast reply to the source (PC host). This reply contains the MAC address of the NIC of the default gateway.**

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

**Before the PC can send a ping request to a host, it needs to determine the destination MAC address before it can build the frame header for that ping request. The ARP broadcast is used to request the MAC address of the host with the IP address contained in the ARP.**

What is the MAC address of the source in the first frame? **00:1a:73:ea:63:8c**

What is the Vendor ID (OUI) of the Source’s NIC? **GemtekTe**

What portion of the MAC address is the OUI?

**The first 3 octets of the MAC address indicate the OUI.**

What is the Source’s NIC serial number? **ea:63:8c**

Part 2: Use Wireshark to Capture and Analyze Ethernet Frames

**STEP 1:**

What is the IP Address of the PC Default Gateway? **192.168.1.1**

**STEP 2:**

* What is the MAC address of the PC’s NIC? **02:00:00:00:45:00**

What is the default gateway’s MAC address? **00:3c:9f:0c:00:00**

* 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? **0x0800 (IPv4)**
* 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? **127.0.0.1**

What is the destination IP address? **127.0.0.1**

* What do the last two highlighted octets spell? **hi**
* 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?

**The host PC (00:3c:9f:0c:00:00)**

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**: **2600:6c44:5400:1f6:7800:2bc1:b6a7**

**Destination**: **2600:1407:e800:584::b33**

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

**Source**: **192.168.1.1**

**Destination**: **23.13.155.188**

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?

**Layer 2 frames never leave the LAN. When a ping is issued to a remote host, the source will use the default gateway MAC address for the frame destination. The default gateway receives the packet, strips the Layer 2 frame information from the packet and then creates a new frame header with the MAC address of the next hop. This process continues from router to router until the packet reaches its destination IP address.**

1. Reflection

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

**The preamble field contains seven octets of alternating 1010 sequences, and one octet that signals the beginning of the frame, 10101011.**