[2CEIT503 COMPUTER NETWORKS]

Practical: 10

AIM- To Study About Wire Shark Tool And Ethernet Standard

By – 21012021003_AMIT GOSWAMI

Department of Computer Engineering/Information Technology

What is Wire shark?

- Wire shark is a network packet analyzer. A network packet analyzer will try to capture. network packets and tries to display that packet data as detailed as possible.
- You could think of a network packet analyzer as a measuring device used to examine

  what's going on inside a network cable, just like a voltmeter is used by an electrician

  to examine what's going on inside an electric cable (but at a higher level, of course).

Wire shark is perhaps one of the best open source packet analyzers available today

EXERCISE ❖

Give answers of following questions.

1) What is the 48-bit Ethernet address of your computer? 08-ED-B9-A9F2-6B

2) Select any frame, and find, what is the highest level protocol that is carried in this frame?

Frame summary:

870 16.901103 192.168.63.51 142.251.42.99 ICMP 74 Echo (ping) request id=0x0001, seq=1437/86794

In the ping request frame for google server, the highest level protocol used is **ICMP.**

3) Select any frame, and find, which field in frame identifies type of packet that this protocol message is encapsulated in?

a. Give the EtherType value (in Hex) that identifies this protocol?

Type: IPv4 (0x0800)

b. Give the decimal value for the two-byte Frame type field.

2048

4) What is the broadcast Ethernet address, written in standard form as Wireshark displays it?

ff.ff.ff.ff.ff.ff

5) Which bit of the Ethernet address is used to determine whether it is unicast or multicast/broadcast?

The least significant bit of the first byte of the MAC address is used to determine whether the address is meant for unicast or multicast/broadcast transmission. If the least significant bit of the first byte is set to 0, the address is interpreted as a unicast address. On the other hand, if this bit is set to 1, the address is considered either a multicast or a broadcast address.

6) How long are the combined IEEE 802.3 and LLC headers compared to the DIX Ethernet headers?

The IEEE 802.3 header is 14 bytes, the same as DIX Ethernet. (Both also have a trailer with a checksum and padding if needed.) LLC adds another 3 bytes of headers for a total of 17 bytes of headers.

7) How does the receiving computer know whether the frame is DIX Ethernet or IEEE 802.3?

The DIX Ethernet Type field and IEEE 802.3 Length field are in the same position. If the value is less than 0x600 (1536) then it is interpreted as a frame length. If the value is larger than 0x600 (1536) then it is interpreted as a Type value.

8) If IEEE 802.3 has no Type field, then how is the next higher layer determined? Use Wireshark to look for the demultiplexing key. IEEE 802.3 adds the LLC header immediately after the IEEE 802.3 header to convey the next higher layer protocol. LLC uses a single initial byte called the DSAP (destination service access point) rather than the two bytes in the Type field.

9) From the command line of the computer, ping the IP address of another network connected. You can, for example, ping the default gateway of your PC 10.10.0.101, or another PC connected to the network. After receiving the successful replies to the ping in the command line window, stop the packet capture.

A. What protocol is used by ping?

ICMP protocol is used by ping. **B.**

What is full name of it?

Internet Control Message Protocol

C. What are the names of the two ping messages?

One ping message from source to destination is **Echo ping Request** message.

Second ping message from destination to source is **Echo ping Reply** message.

D. Are the listed source and destination IP addresses what you expected?Yes/No Yes

E. What is the length of first echo request packet?

length of first echo request packet is **32 bytes**.

F.Which field of IPv4 packet will identifies that this packet is of type ICMP? What is the value of it?

The protocol field will identifies that this packet is of type ICMP. Value is 01 in hexadecimal.

G. What is the header length of IPv4 packet?

20 Bytes.

H. What is the value of TTL field in IPv4? What happens when value of TTL reaches to zero?

116 . It indicates that the packet has been in the network for too long or has encountered an unexpected loop. In this case, the router typically sends an ICMP Time Exceeded message back to the source IP address to inform the sender that the packet was discarded due to the TTL reaching zero.

I. What is the value of type field of ICMP message for echo request andecho reply?

The value of type field of ICMP message for echo request is 8 (Echo (ping) request).

The value of type field of ICMP message for echo reply is 0(Echo (ping) reply.

10) What is the average packet size of our captured trace? 54 bytes is the average packet size of our captured trace.

11) What is the average data rate (in Mbps) of your captured trace?

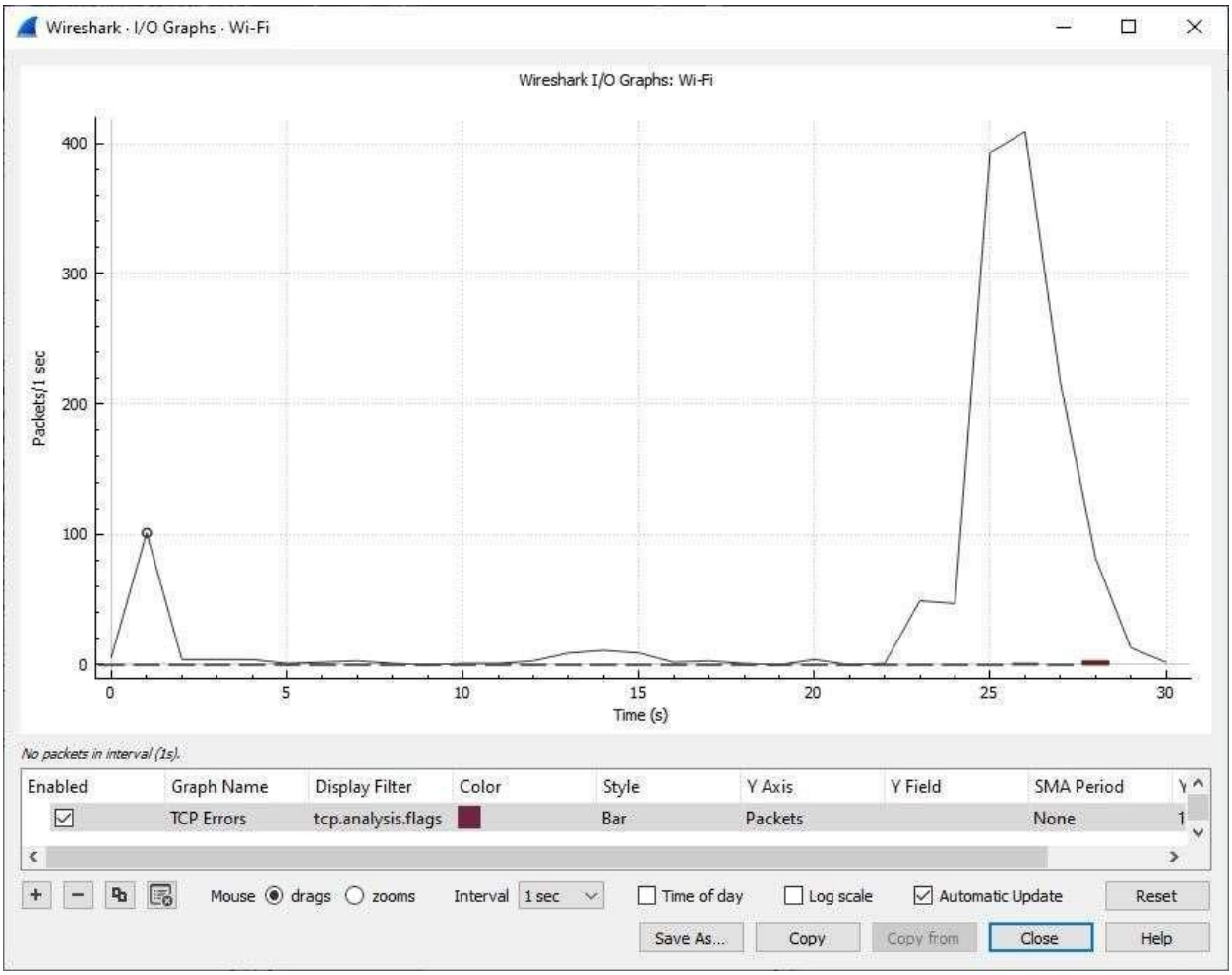
1231/1000000 = 0.001231Mbps

12) How many percent of captured packets are of IPv4 for your captured trace?

1. Click on the Statistics menu item and select Protocol Hierarchy.
2. In the Protocol Hierarchy window, expand the IPv4 node.

98.9% are IPv4 packets.

13) Give graph for IPv4 vs. TCP packets per second for your captured trace?



14) Determine network information.

Host IP Address	192.168.63.51
Network Mask	255.255.252.0

Find :

Network Address	192.168.60.0
Network Broadcast Address	192.168.63.255
Total Number of Host Bits	8
Number of Hosts	1024

15) Determine subnet information.

Host IP Address	192.168.63.51
Network Mask	255.255.252.0
Subnet Mask	255.255.252.0

Find :

Number of Bits for subnet address	2
Number of Subnets	
Number of Host Bits per Subnet	1024
Number of Usable Hosts per Subnet	1022
IP Address for First Host on first Subnet	192.168.60.1
IP Address for Last Host on last Subnet	192.168.63.254