[2CEIT503 COMPUTER NETWORKS]

Practical: 10

AIM- To Study About Wire Shark Tool And Ethernet Standard

Ganpat University
॥ विद्यया समाजोत्कर्षः ॥
U.V. Patel College of Engineering

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.

- **Some intended purposes**

  Here are some examples people uses Wireshark for:

  - Network administrators use it to troubleshoot network problems
  - Network security engineers use it to examine security problems
  - Developers use it to debug protocol implementations
  - People use it to learn network protocol internals

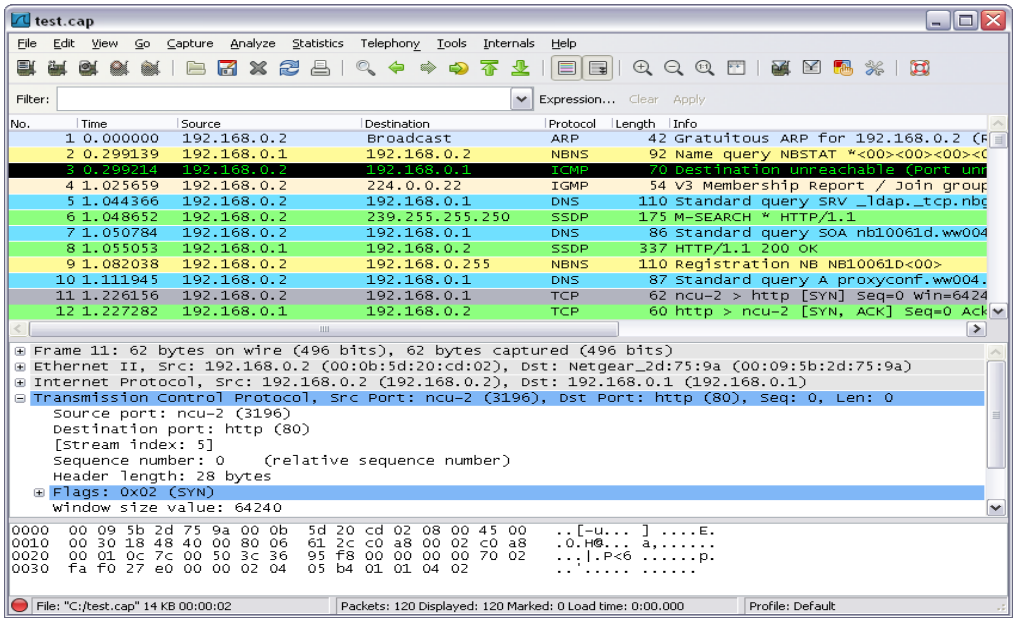
  Beside these examples Wireshark can be helpful in many other situations too.

- **Features**

  The following are some of the many features Wireshark provides:

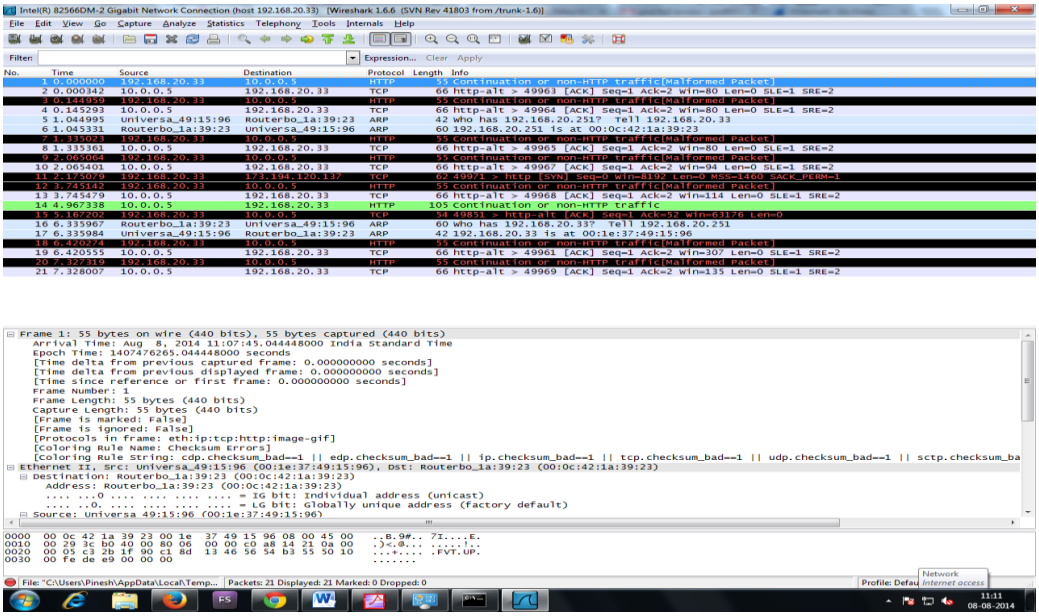
  - Available for UNIX and Windows.
  - Capture live packet data from a network interface.
  - Open files containing packet data captured with tcpdump/WinDump, Wireshark, and a number of other packet capture programs.
  - Import packets from text files containing hex dumps of packet data.
  - Display packets with very detailed protocol information.
  - Save packet data captured.
  - Export some or all packets in a number of capture file formats.
  - Filter packets on many criteria.
  - Search for packets on many criteria.
  - Colorize packet display based on filters.
  - Create various statistics.
  - …and a lot more!

  However, to really appreciate its power you have to start using it.Figure 1.1, "Wireshark captures packets and lets you examine their contents." showsWireshark having captured some packets and waiting for you to examine them.



➢ Capture a Trace

You should see a screen similar to the following



Select any packet in the trace (in the top panel) to see details of its structure (in the middle panel) and the bytes that make up the packet (in the bottom panel). Now we can inspect the details of the packets. In the figure, we have selected the first packet in the trace. Note that we are using the term “packet” in a loose way. Each record captured by Wireshark more correctly corresponds to a single frame in Ether-net format that carries a packet as its payload; Wireshark interprets as much structure as it can.

In the middle panel, expand the Ethernet header fields (using the "+" expander or icon) to see their de-tails. Our interest is the Ethernet header, and you may ignore the higher layer protocols (which are IP and ICMP in this case). Note the following:

- The frames in this trace are DIX Ethernet, called "Ethernet II" in Wireshark.
- There is no preamble in the fields shown in Wireshark. The preamble is a physical layer mecha-nism to help the NIC identify the start of a frame. It carries no useful data and is not received like other fields.
- There is a destination address and a source address. Wireshark is decoding some of these bits in the OUI (Organizationally Unique Identifier) portion of the address to tell us the vendor of the NIC, e.g., Dell for the source address.
- There is a Type field. For the ping messages, the Ethernet type is IP, meaning the Ethernet pay-load carries an IP packet. (There is no Length field as in the IEEE 802.3 format. Instead, the length of a DIX Ethernet frame is determined by the hardware of a receiving computer, which looks for valid frames that start with a preamble and end with a correct checksum, and passed up to higher layers along with the packet.)
- There is no Data field per se – the data starts with the IP header right after the Ethernet header.
- There is no pad. A pad will be present at the end if the frame would otherwise be less than 64 bytes, the minimum Ethernet frame size.
- There is no checksum in most traces, even though it really does exist. Typically, Ethernet hard-ware that is sending or receiving frames computes or checks this field and adds or strips it. Thus it is simply not visible to the OS or Wireshark in most capture setups.
- There are also no VLAN fields. If VLANs are in use, the VLAN tags are normally added and re-moved by switch ports so they will not be visible at host computers using the network.

- **Ethernet Frame Structure**

- Try to understand the Ethernet frame format. Note the range of the Ethernet header and the Ethernet payload. See the frame structure below in Figure 5.
- To work out sizes, observe that when you click on a protocol block in the middle panel (the block itself, not the "+" expander) then Wireshark will highlight the bytes it corresponds to in the packet in the low-er panel and display the length at the bottom of the window.
- You may also use the overall packet size shown in the Length column or Frame detail block.

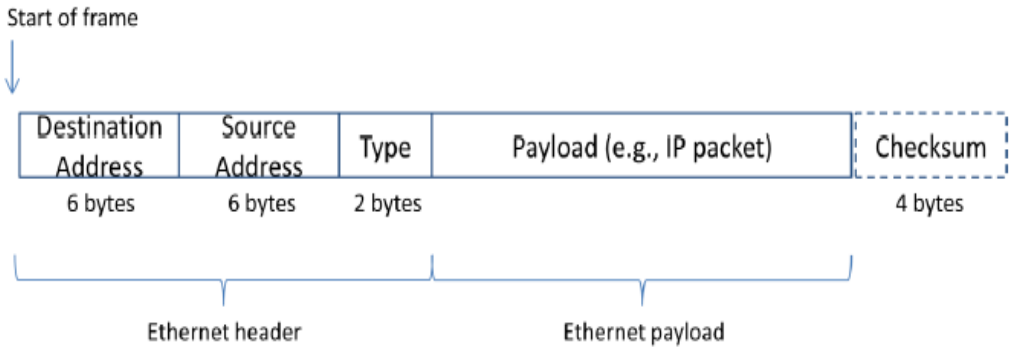


Figure 5: Structure of an Ethernet frame

There are several features to note:

- The destination address comes before the source address.
- The pad is not shown because the packets we examined (ping) are large enough that no pad is needed.
- Unlike many protocols, Ethernet has a trailer (the checksum, and pad if present) as well as a header. The checksum is handled by the hardware and not visible to Wireshark.
- The Ethernet header is 14 bytes long.

➢ **Scope of Ethernet Addresses**

- Each Ethernet frame carries a source and destination address. One of these addresses is that of your computer. It is the source for frames that are sent, and the destination for frames that are received. But what is the other address?
- Assuming you pinged a remote Internet server, it cannot be the Ethernet ad-dress of the remote server because an Ethernet frame is only addressed to go within one LAN.
- Instead, it will be the Ethernet address of the router or default gateway, such as your AP in the case of 802.11. This is the device that connects your LAN to the rest of the Internet.
- In contrast, the IP addresses in the IP block of each packet do indicate the overall source and destination endpoints. They are your computer and the remote server.

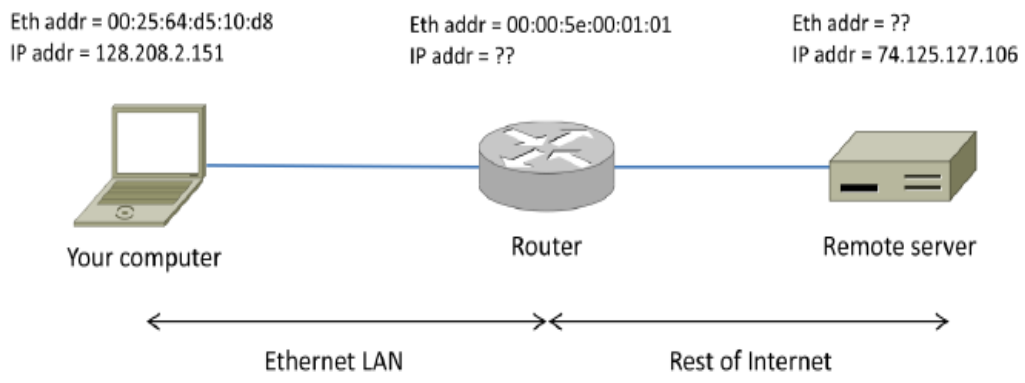


Figure 6: Ethernet and IP addresses of network devices

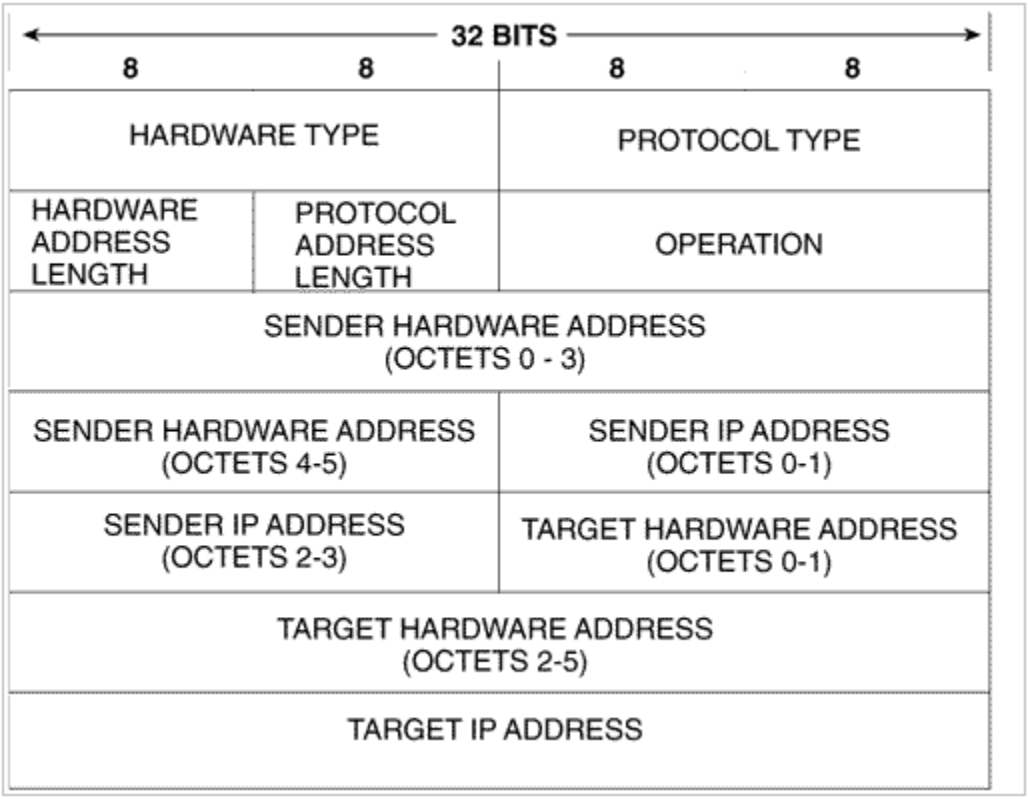
- **Broadcast Frames**

  - The trace that you gathered above captured unicast Ethernet traffic sent between a specific source and destination, e.g., your computer to the router.
  - It is also possible to send multicast or broadcast Ethernet traffic, destined for a group of computers or all computers on the Ethernet, respectively. We can tell from the address whether it is unicast, multicast, or broadcast. Broadcast traffic is sent to a reserved Ethernet address that has all bits set to "1". Multicast traffic is sent to addresses that have a "1" in the first bit sent on the wire; broadcast is a special case of multicast. Broadcast and multicast traffic is widely used for discovery protocols, e.g., a packet sent to everyone in an effort to find the local printer. 1.
  - Start a capture for broadcast and multicast Ethernet frames with a filter of "ether multicast". You do this by selecting Capture in the main menu and then selecting Options. This is not to be confused with the filter box on the live capture page which will not accept the filter expression above.

- **Address Resolution Protocol**

  - The Address Resolution Protocol (ARP) is a telecommunication protocol used for resolution of network layer addresses into link layer addresses, a critical function in multiple-access networks. ARP was defined by RFC 826 in 1982 It is Internet Standard STD 37.
  - It is also the name of the program for manipulating these addresses in most operating systems.
  - The Address Resolution Protocol is a request and reply protocol that runs encapsulated by the line protocol. It is communicated within the boundaries of a single network, never routed across internetwork nodes.

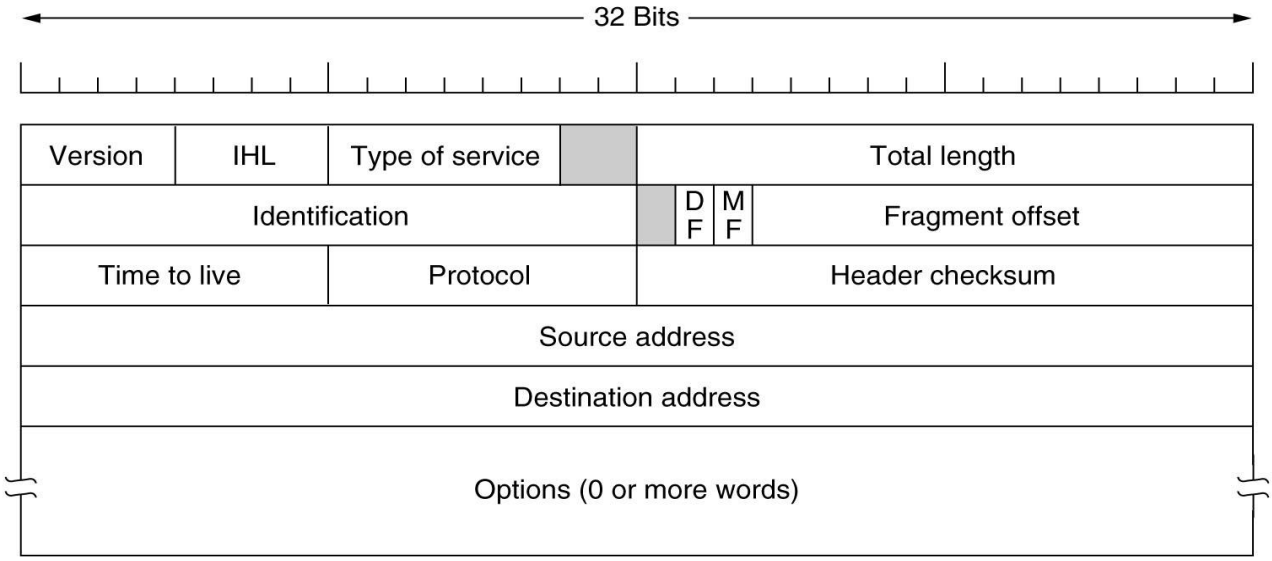
- This property places ARP into the Link Layer of the Internet Protocol Suite, while in the Open Systems Interconnection (OSI) model, it is often described as residing between Layers 2 and 3, being encapsulated by Layer 2 protocols. However, ARP was not developed in the OSI framework.



➢ **IPv4**

- Internet Protocol version 4 (IPv4) is the fourth version in the development of the Internet Protocol (IP) Internet, and routes most traffic on the Internet However, a successor protocol, IPv6, has been defined and is in various stages of production deployment. IPv4 is described in IETF publication replacing an earlier definition.
- IPv4 is a connectionless protocol for use on packet-switched networks. It operates on a best effort deliverymodel, in that it does not guarantee delivery, nor does it assure proper sequencing or avoidance of duplicate delivery. These aspects, including data integrity, are addressed by an upper layer transport protocol, such as the Transmission Control Protocol (TCP).
- IPv4 uses 32-bit (four-byte) addresses, which limits the address space to 4294967296 (232) addresses. As addresses were assigned to users, the number of unassigned addresses decreased. IPv4 address exhaustion occurred on February 3, 2011, although it had been significantly delayed by address changes such as classful network design, Classless Inter-Domain Routing, and network address translation (NAT).

- This limitation of IPv4 stimulated the development of IPv6 in the 1990s, which has been in commercial deployment since 2006.
- IPv4 reserves special address blocks for private networks (~18 million addresses) and multicast addresses (~270 million addresses).



EXERCISE

- **Give answers of following questions.**

1) What is the 48-bit Ethernet address of your computer?

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

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

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

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

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

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

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

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

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.

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.

For example: ping 10.0.0.5 -t

A. What protocol is used by ping?

B. What is full mane of it?

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

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

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

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

G. What is the header length of IPv4 packet?

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

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

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

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

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

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

14) Determine network information.

Host IP Address	
Network Mask	

Find :

Network Address	
Network Broadcast Address	
Total Number of Host Bits	

Number of Hosts	

15) Determine subnet information.

Host IP Address	
Network Mask	
Subnet Mask	

Find :

Number of Bits for subnet address	
Number of Subnets	
Number of Host Bits per Subnet	
Number of Usable Hosts per Subnet	
IP Address for First Host on first Subnet	
IP Address for Last Host on last Subnet	