

EXPERIMENT NO. 9

Aim :- Use Wire shark to understand operation of TCP/IP layers :-

Ethernet Layer :- Frame header, Frame size etc.

DLL :- MAC address, ARP

Network Layer :- IP packet, ICMP

Transport Layer :- TCP Ports, TCP handshake

Theory :-

Using Wireshark, you can gain valuable insights into the operation of TCP/IP layers and examine the various aspects of the network communication. Here's a theoretical overview of how Wireshark can help you understand each of these layers :-

1. Ethernet Layer :-

Wireshark captures Ethernet frames, providing details such as frame header, frame size, source MAC address, and destination one.

You can inspect Ethernet frame headers to understand the physical layer characteristics of data being transmitted on network.

2. Data Link layer :-

Wireshark allows you to view MAC (Media Access Control) addresses within Ethernet frames.

Ethernet Header Format :

Preamble	Start Frame Delimiter	Destination Address	Source Address	Length	Data	Frame Check Sequence (CRC)
7 byte	1 byte	6 byte	6 byte	2 byte	46 to 1500 B	4 byte

TCP Header Format :

Source Port Address 16-bit								Destination Port Address 16-bit							
Sequence Number 32-bit															
Acknowledgement Number 32-bit															
HLEN 4-bit		Reserved 6-bit		U R	A K	P R H	S S I	F Y N	Window Size 16-bit						
Checksum (16-bit)									Urgent Pointer 16-bit						
Options/ Padding 0 to 40 bytes															

UDP Header Format :

Source Port Address 16-bit	Destination Port Address 16-bit
Total length of UDP 16-bit	Checksum 16-bit

IPv4 Header Format :

VER 4-bit	HLEN 4-bit	TYPE OF SERVICE 8-bit	Total length 16-bit			
Identification 16-bit			Res	DF	MF	Fragment offset 13-bit
Time to Live 8-bit		Protocol 8-bit	Header Checksum 16-bit			
Source IP (32-bit)						
Destination IP (32-bit)						
Options + Padding (0-40 bytes)						

IPv6 Header Format:

VER 4-bit	Priority 8-bit	Flow Label 20-bit
Payload Length 16-bit		Next Header 8-bit
Hop Limits 8-bit		
Source IP Address (128-bit)		
Destination IP Address (128-bit)		
Extension Headers		
Data		

3. Network Layer :

Wireshark provides information about IP packets, including the IP header and payload.

You can examine IP packet headers to understand routing, Time-to-live (TTL), and fragmentation. ICMP (Internet Control Message Protocol) packets, such as Ping (Echo Request and Reply) and Traceroute (Time Exceeded), can be observed to diagnose network issues.

4. Transport Layer :

Wireshark captures TCP and UDP packets, allowing you to analyze their characteristics.

For TCP, you can inspect segments, including sequence and acknowledgement numbers.

The TCP handshake (SYN, SYN-ACK, ACK) can be observed, helping you understand how connections are established.

For UDP, you can identify source and destination ports.

Conclusion : - Thus, we implemented operation of TCP/IP layers using the Wireshark software.

~~10/12/23~~

> Ethernet II, Src: Micro-St_c2:99:83 (d8:bb:c1:c2:99:83), Dst: Broadcast (ff:ff:ff:ff:ff:ff)

▼ Address Resolution Protocol (ARP Probe)

Hardware type: Ethernet (1)

Protocol type: IPv4 (0x0800)

Hardware size: 6

Protocol size: 4

Opcode: request (1)

[Is probe: True]

Sender MAC address: Micro-St_c2:99:83 (d8:bb:c1:c2:99:83)

Sender IP address: 0.0.0.0

Target MAC address: 00:00:00_00:00:00 (00:00:00:00:00:00)

Target IP address: 192.168.31.18

> Ethernet II, Src: Micro-ST_e4:eb:d4 (a8:bb:c1:e4:eb:d4), Dst: IPv4mcast_1b (01:00:5e:00:00:1b)

▼ Internet Protocol Version 4, Src: 192.168.31.9, Dst: 224.0.0.22

0100 = Version: 4

.... 0110 = Header Length: 24 bytes (6)

> Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)

Total Length: 40

Identification: 0x4a5b (19035)

> 000. = Flags: 0x0

...0 0000 0000 0000 = Fragment Offset: 0

Time to Live: 1

Protocol: IGMP (2)

Header Checksum: 0x1aad [validation disabled]

[Header checksum status: Unverified]

Source Address: 192.168.31.9

Destination Address: 224.0.0.22

> Options: (4 bytes), Router Alert

▼ Internet Group Management Protocol

< >

```
> User Datagram Protocol, Src Port: 61030, Dst Port: 1900
< Simple Service Discovery Protocol
  < M-SEARCH * HTTP/1.1\r\n
    > [Expert Info (Chat/Sequence): M-SEARCH * HTTP/1.1\r\n]
      Request Method: M-SEARCH
      Request URI: *
      Request Version: HTTP/1.1
    HOST: 239.255.255.250:1900\r\n
    MAN: "ssdp:discover"\r\n
    MX: 1\r\n
    ST: urn:dial-multiscreen-org:service:dial:1\r\n
    USER-AGENT: Google Chrome/117.0.5938.132 Windows\r\n
    \r\n
    [Full request URI: http://239.255.255.250:1900*]
    [HTTP request 1/4]
    [Next request in frame: 51232]
```

▼ Transmission Control Protocol, Src Port: 52187, Dst Port: 443, Seq: 2053, Ack: 1047, Len: 0

Source Port: 52187

Destination Port: 443

[Stream index: 77]

[Conversation completeness: Complete, WITH_DATA (63)]

[TCP Segment Len: 0]

Sequence Number: 2053 (relative sequence number)

Sequence Number (raw): 2527396113

[Next Sequence Number: 2053 (relative sequence number)]

Acknowledgment Number: 1047 (relative ack number)

Acknowledgment number (raw): 1593067049

0101 = Header Length: 20 bytes (5)

> Flags: 0x010 (ACK)

Window: 255

[Calculated window size: 65280]

[Window size scaling factor: 256]

Checksum: 0x2de1 [unverified]

Internet Protocol Version 4, Src: 192.168.31.34, Dst: 239.255.255.250

- 0100 = Version: 4
- 0101 = Header Length: 20 bytes (5)
- > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
- Total Length: 801
- Identification: 0x8672 (34418)
- > 000. = Flags: 0x0
- ...0 0000 0000 0000 = Fragment Offset: 0
- Time to Live: 1
- Protocol: UDP (17)
- Header Checksum: 0x6095 [validation disabled]
- [Header checksum status: Unverified]
- Source Address: 192.168.31.34
- Destination Address: 239.255.255.250
- > User Datagram Protocol, Src Port: 49583, Dst Port: 3702
- > Data (773 bytes)

Internet Protocol Version 4 (IPv4) 20 bytes