

## **EXPERIMENT NO. 4**

**AIM:** Using wireshark understand the operations of TCP/IP layers:

Ethernet Layer: Frame header, Frame size etc.

Data Link Layer: MAC address, ARP.

Network Layer: IP packet (Header, fragmentation, ICMP).

Transport Layer: TCP Ports, TCP handshake segments etc.

Application Layer: FTP, DHCP, HTTP header formats

### **Theory:**

Wireshark, a network analysis tool formerly known as Ethereal, captures packets in real time and displays them in human-readable format. Wireshark includes filters, color coding, and other features that let you dig deep into network traffic and inspect individual packets.

Wireshark is a network or protocol analyzer (also known as a network sniffer) available for free at the Wireshark website. It is used to analyze the structure of different network protocols and has the ability to demonstrate encapsulation. The analyzer operates on Unix, Linux and Microsoft Windows operating systems, and employs the GTK+ widget toolkit and pcap for packet capturing. Wireshark and other terminal-based free software versions like Tshark are released under the GNU General Public License.

Wireshark shares many characteristics with tcpdump. The difference is that it supports a graphical user interface (GUI) and has information filtering features. In addition, Wireshark permits the user to see all the traffic being passed over the network.

### **Features of Wireshark include:**

- Data is analyzed either from the wire over the network connection or from data files that have already captured data packets.
- Supports live data reading and analysis for a wide range of networks (including Ethernet, IEEE 802.11, point-to-point Protocol (PPP) and loopback).
- With the help of GUI or other versions, users can browse captured data networks.
- For programmatically editing and converting the captured files to the editcap application, users can use command line switches.
- Display filters are used to filter and organize the data display.
- New protocols can be scrutinized by creating plug-ins.
- Captured traffic can also trace Voice over Internet (VoIP) calls over the network.
- When using Linux, it is also possible to capture raw USB traffic.

Capturing from eth0

Filter: Expression... Clear Apply Save

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000000	192.168.211.72	239.255.255.250	SSDP	214	M-SEARCH * HTTP/1.1
2	0.077095414	HewlettP 8c:83:22	Spanning-tree-(for-bri	STP	60	RST. Root = 32768/0/20:e5:2a:68:a2:5a Cost = 1060 Port = 0x8029
3	1.001184282	192.168.211.72	239.255.255.250	SSDP	214	M-SEARCH * HTTP/1.1
4	1.952134611	fe80::ca1f:66ff:fe2b:c	ff02::fb	MDNS	199	Standard query 0x0000 PTR _ipp_tcp.local, "QM" question PTR _ipps_tc
5	1.952176092	192.168.211.28	224.0.0.251	MDNS	179	Standard query 0x0000 PTR _ipp_tcp.local, "QM" question PTR _ipps_tc
6	2.002072361	192.168.211.72	239.255.255.250	SSDP	214	M-SEARCH * HTTP/1.1
7	2.076993858	HewlettP 8c:83:22	Spanning-tree-(for-bri	STP	60	RST. Root = 32768/0/20:e5:2a:68:a2:5a Cost = 1060 Port = 0x8029
8	3.002178385	192.168.211.72	239.255.255.250	SSDP	214	M-SEARCH * HTTP/1.1
9	3.569997497	fe80::6600:6aff:fe18:a	ff02::fb	MDNS	225	Standard query 0x0000 ANY 8.6.c.a.8.1.e.f.f.a.6.0.0.6.6.0.0.0.0.0.
10	3.570032037	192.168.211.225	224.0.0.251	MDNS	205	Standard query 0x0000 ANY 8.6.c.a.8.1.e.f.f.a.6.0.0.6.6.0.0.0.0.0.
11	3.571041000	fe80::6600:6aff:fe19:4	ff02::fb	MDNS	152	Standard query response 0x0000 AAAA, cache flush fe80::6600:6aff:fe19:
12	3.571063752	192.168.211.132	224.0.0.251	MDNS	148	Standard query response 0x0000 AAAA, cache flush fe80::6600:6aff:fe19:

Frame 1: 214 bytes on wire (1712 bits), 214 bytes captured (1712 bits) on interface 0

Ethernet II, Src: Dell\_19:45:1c (64:00:6a:19:45:1c), Dst: IPv4mcast 7f:ff:fa (01:00:5e:7f:ff:fa)

Internet Protocol Version 4, Src: 192.168.211.72, Dst: 239.255.255.250

User Datagram Protocol, Src Port: 53578, Dst Port: 1900

Simple Service Discovery Protocol

```

0000  01 00 5e 7f ff fa 64 00 6a 19 45 1c 08 00 45 00  ..^...d. j.E...E.
0010  00 c8 d7 e2 40 00 01 11 1d 57 c0 a8 d3 48 ef ff  ...@... .W...H..
0020  ff fa d1 4a 07 6c 00 b4 03 aa 4d 2d 53 45 41 52  ...J.L...M-SEAR
0030  43 48 20 2a 20 48 54 54 50 2f 31 2e 31 0d 0a 48  CH * HTTP/1.1.H
0040  4f 53 54 3a 20 32 33 39 2e 32 35 35 2e 32 35 35  OST: 239 .255.255
0050  2e 32 35 30 3a 31 39 30 30 0d 0a 4d 41 4e 3a 20  .250:190 0..MAN:
0060  22 73 73 64 70 3a 64 69 73 63 6f 76 65 72 22 0d  "ssdp:discover".
0070  0a 4d 58 3a 20 31 0d 0a 53 54 3a 20 75 72 6e 3a  .MX: 1..ST: urn:
0080  64 69 61 6c 2d 6d 75 6c 74 69 73 63 72 65 65 6e  dial-multiscreen
0090  2d 6f 72 67 3a 73 65 72 76 69 63 65 3a 64 69 61  -org:service:dia
00a0  6c 3a 31 0d 0a 55 53 45 52 2d 41 47 45 4e 54 3a  l:1..USER-AGENT:
00b0  2d 47 6f 6f 67 6c 65 20 43 68 72 6f 6d 65 2f 37  Google Chrome/7
00c0  35 2e 30 2e 33 37 37 30 2e 31 34 32 20 4c 69 6e  5.0.3770 .142 Lin
00d0  75 78 0d 0a 0d 0a                                     ux....

```

eth0: <live capture in progress> ... Packets: 12 · Displayed: 12 (100.0%) Profile: Default

## Ethernet Layer :

Ethernet layer is very simple. It contains a destination address and a source address. The data link layer is relatively simple in that it is only concerned with getting a frame to the next adjacent node on the physical medium.

Capturing from eth0

Filter: Expression... Clear Apply Save

No.	Time	Source	Destination	Protocol	Length	Info
229	32.296533271	192.168.211.91	224.0.0.251	MDNS	148	Standard query response 0x0000 AAAA, cache flush fe80::6600:6aff:fe1
230	32.522822239	HewlettP 8c:89:50	HewlettP 8c:93:d0	ARP	60	Who has 192.168.211.33? Tell 192.168.211.69
231	32.523270698	HewlettP 8c:89:50	HewlettP 8c:90:50	ARP	60	Who has 192.168.211.88? Tell 192.168.211.69
232	32.523490722	HewlettP 8c:89:50	HewlettP 8c:f1:38	ARP	60	Who has 192.168.211.85? Tell 192.168.211.69
233	32.605940704	192.168.211.98	192.168.211.255	BROWSER	282	Host Announcement COMPUTER-DESKT0, Workstation, Server, Print Queue
234	32.605979602	192.168.211.71	192.168.211.255	NBNS	92	Name query NB WORKGROUP<Id>
235	32.606759612	192.168.211.153	192.168.211.255	BROWSER	282	Host Announcement COMPUTER-DESKT0, Workstation, Server, Print Queue
236	32.815590197	192.168.211.185	224.0.0.251	MDNS	82	Standard query 0x0000 PTR _googlecast._tcp.local, "QM" question
237	32.815670392	192.168.211.185	224.0.0.251	MDNS	82	Standard query 0x0000 PTR _googlecast._tcp.local, "QM" question
238	33.803993065	0.0.0.0	255.255.255.255	DHCP	590	DHCP Discover - Transaction ID 0x682bcdad
239	33.804035042	192.168.211.253	255.255.255.255	DHCP	350	DHCP Offer - Transaction ID 0x682bcdad
240	33.913577656	fe80::6600:6aff:fe18::e	ff02::fb	MDNS	199	Standard query 0x0000 PTR _ipps._tcp.local, "QM" question PTR _ipp...
241	34.075556036	HewlettP 8c:83:22	Spanning-tree-(for-bri	STP	60	RST. Root = 32768/0/20:e5:2a:68:a2:5a Cost = 1060 Port = 0x8029
242	34.191450666	192.168.211.54	239.255.255.250	SSDP	214	M-SEARCH * HTTP/1.1

[Time delta from previous captured frame: 0.000000000 seconds]  
[Time delta from previous displayed frame: 0.000000000 seconds]  
[Time since reference or first frame: 0.000000000 seconds]  
Frame Number: 1  
Frame Length: 214 bytes (1712 bits)  
Capture Length: 214 bytes (1712 bits)  
[Frame is marked: False]  
[Frame is ignored: False]  
[Protocols in frame: eth:ethertype:ip:udp:ssdp]

▼ Ethernet II, Src: Dell 19:45:1c (64:00:6a:19:45:1c), Dst: IPv4mcast 7f:ff:fa (01:00:5e:7f:ff:fa)  
► Destination: IPv4mcast 7f:ff:fa (01:00:5e:7f:ff:fa)  
► Source: Dell 19:45:1c (64:00:6a:19:45:1c)  
Type: IPv4 (0x0800)  
► Internet Protocol Version 4, Src: 192.168.211.72, Dst: 239.255.255.250  
► User Datagram Protocol, Src Port: 53578, Dst Port: 1900  
► Simple Service Discovery Protocol

```

0000  01 00 5e 7f ff fa 64 00 6a 19 45 1c 08 00 45 00  ..^..d..j.E...E.
0010  00 c8 d7 e2 40 00 01 11 1d 57 c0 a8 d3 48 ef ff  ....@... .W...H..
0020  ff fa d1 4a 07 6c 00 b4 03 aa 4d 2d 53 45 41 52  ...J.L...M-SEAR
0030  43 48 20 2a 20 48 54 54 50 2f 31 2e 31 0d 0a 48  CH * HTTP/1.1..H
0040  4f 53 54 3a 20 32 33 39 2e 32 35 35 2e 32 35 35  OST: 239 .255.255
0050  2e 32 35 30 3a 31 39 30 30 0d 0a 4d 41 4e 3a 20  .250:190 0..MAN:
0060  22 73 73 64 70 3a 64 69 73 63 6f 76 65 72 22 0d  "ssdp:discover".
0070  0a 4d 58 3a 20 31 0d 0a 53 54 3a 20 75 72 6e 3a  .MX: 1..ST: urn:
0080  64 69 61 6c 2d 6d 75 6c 74 69 73 63 72 65 65 6e  dial-multiscreen
0090  2d 6f 72 67 3a 73 65 72 76 69 63 65 3a 64 69 61  -org:service:dia
00a0  6c 3a 31 0d 0a 55 53 45 52 2d 41 47 45 4e 54 3a  l:1..USER-AGENT:
00b0  20 47 6f 6f 67 6c 65 20 43 68 72 6f 6d 65 2f 37  Google Chrome/7
00c0  35 2e 30 2e 33 37 37 30 2e 31 34 32 20 4c 69 6e  5.0.3770 .142 Lin
00d0  75 78 0d 0a 0d 0a                                     ux....

```

Ethernet (eth), 14 bytes      Packets: 242 · Displayed: 242 (100.0%)      Profile: Default

## Network Layer:

The Ethernet layer is concerned with node to node. The IP layer is concerned with moving between networks, hence the original meaning of the term internetwork, from whence Internet was derived. Highlighting the network layer shows more details. From Figure C, we can see the source and destination IP addresses as well as the IP header length (20 bytes in this case). We can also see the Differentiated Services (DiffServ) area. This would be where extra information relating to the packet's type of service goes. For most packets on a LAN this is set to zero, which means best effort.

Capturing from eth0

Filter: Expression... Clear Apply Save

No.	Time	Source	Destination	Protocol	Length	Info
265	42.075189056	HewlettP_8c:83:22	Spanning-tree-(for-bri	STP	60	RST. Root = 32768/0/20:e5:2a:68:a2:5a Cost = 1060 Port = 0x8029
266	43.077806052	HewlettP_8c:83:22	LLDP Multicast	LLDP	319	TTL = 120 System Name = HP 1920G Switch System Description = 1920-48
267	43.427647931	fe80::6600:6aff:fe18:aff02::fb	224.0.0.251	MDNS	225	Standard query 0x0000 ANY 8.6.c.a.8.1.e.f.f.a.6.0.0.6.6.0.0.0.0.0.
268	43.427688815	192.168.211.225	224.0.0.251	MDNS	205	Standard query 0x0000 ANY 8.6.c.a.8.1.e.f.f.a.6.0.0.6.6.0.0.0.0.0.
269	43.428427576	fe80::6600:6aff:fe18:aff02::fb	224.0.0.251	MDNS	152	Standard query response 0x0000 AAAA, cache flush fe80::6600:6aff:fe1
270	43.428456799	192.168.211.91	224.0.0.251	MDNS	148	Standard query response 0x0000 AAAA, cache flush fe80::6600:6aff:fe1
271	44.075087635	HewlettP_8c:83:22	Spanning-tree-(for-bri	STP	60	RST. Root = 32768/0/20:e5:2a:68:a2:5a Cost = 1060 Port = 0x8029
272	45.871015979	169.254.143.1	255.255.255.255	DHCP	383	DHCP Discover - Transaction ID 0x25d09f47
273	46.075018049	HewlettP_8c:83:22	Spanning-tree-(for-bri	STP	60	RST. Root = 32768/0/20:e5:2a:68:a2:5a Cost = 1060 Port = 0x8029
274	46.179960282	fe80::calf:66ff:fe2b:cf02::fb	224.0.0.251	MDNS	225	Standard query 0x0000 ANY 6.f.e.c.b.2.e.f.f.f.6.6.f.1.a.c.0.0.0.0.0.
275	46.179995279	192.168.211.28	224.0.0.251	MDNS	205	Standard query 0x0000 ANY 6.f.e.c.b.2.e.f.f.f.6.6.f.1.a.c.0.0.0.0.0.
276	46.181009479	fe80::calf:66ff:fe2b:cf02::fb	224.0.0.251	MDNS	152	Standard query response 0x0000 AAAA, cache flush fe80::calf:66ff:fe2
277	46.181034813	192.168.211.125	224.0.0.251	MDNS	148	Standard query response 0x0000 AAAA, cache flush fe80::calf:66ff:fe2
278	46.594936891	192.168.211.181	239.255.255.250	SSDP	214	M-SEARCH * HTTP/1.1

Type: IPv4 (0x0000)

Internet Protocol Version 4, Src: 192.168.211.72, 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: 200  
 Identification: 0xd7e2 (55266)  
 ►Flags: 0x4000, Don't fragment  
 Time to live: 1  
 Protocol: UDP (17)  
 Header checksum: 0xd57 [validation disabled]  
 [Header checksum status: Unverified]  
 Source: 192.168.211.72  
 Destination: 239.255.255.250

►User Datagram Protocol, Src Port: 53578, Dst Port: 1900

►Simple Service Discovery Protocol

```

0000 01 00 5e 7f ff fa 64 00 6a 19 45 1c 08 00 45 00  ..^...d. j.E...E
0010 00 c8 d7 e2 40 00 01 11 1d 57 c0 a8 d3 48 ef ff  ...@...W...H.
0020 ff fa d1 4a 07 6c 00 b4 03 aa 4d 2d 53 45 41 52  .J.L...M-SEAR
0030 43 48 20 2a 20 48 54 54 50 2f 31 2e 31 0d 0a 48  CH * HTTP/1.1.H
0040 4f 53 54 3a 20 32 33 39 2e 32 35 35 2e 32 35 35  OST: 239 .255.255
0050 2e 32 35 30 3a 31 39 30 30 0d 0a 4d 41 4e 3a 20  .250:190 0..MAN:
0060 22 73 73 64 70 3a 64 69 73 63 6f 76 65 72 22 0d  "ssdp:discover".
0070 0a 4d 58 3a 20 31 0d 0a 53 54 3a 20 75 72 6e 3a  .MX: 1..ST: urn:
0080 64 69 61 6c 2d 6d 75 6c 74 69 73 63 72 65 65 6e  dial-multiscreen
0090 2d 6f 72 67 3a 73 65 72 76 69 63 65 3a 64 69 61  -org:service:dia
00a0 6c 3a 31 0d 0a 55 53 45 52 2d 41 47 45 4e 54 3a  l:1..USER-AGENT:
00b0 20 47 6f 6f 67 6c 65 20 43 68 72 6f 6d 65 2f 37  Google Chrome/7
00c0 35 2e 30 2e 33 37 37 30 2e 31 34 32 20 4c 69 6e  5.0.3770 .142 Lin
00d0 75 78 0d 0a 0d 0a                                ux....
  
```

Internet Protocol Version 4 (ip),... Packets: 278 · Displayed: 278 (100.0%) Profile: Default

## Transport Layer:

The transport layer is where applications communicate via the use of ports. Figure 4 will show the source port i.e 40519 and the destination port i.e 5001. The header length (32 bytes in this case) and the sequence number are displayed. The sequence number generally will change for each packet.



Capturing from eth0

Filter: Expression... Clear Apply Save

No.	Time	Source	Destination	Protocol	Length	Info
343	52.627834871	192.168.211.60	192.168.211.255	BROWSER	241	Browser Election Request
344	52.627838706	192.168.211.74	192.168.211.255	BROWSER	241	Browser Election Request
345	52.627843766	192.168.211.119	192.168.211.255	BROWSER	241	Browser Election Request
346	53.589883643	192.168.211.98	239.255.255.250	SSDP	213	M-SEARCH * HTTP/1.1
347	53.888346877	192.168.211.125	239.255.255.250	SSDP	214	M-SEARCH * HTTP/1.1
348	54.074659291	HewlettP 8c:83:22	Spanning-tree-(for-bri	STP	60	RST. Root = 32768/0/20:e5:2a:68:a2:5a Cost = 1060 Port = 0x8029
349	54.590375847	192.168.211.98	239.255.255.250	SSDP	213	M-SEARCH * HTTP/1.1
350	54.630590792	192.168.211.115	192.168.211.255	BROWSER	232	Browser Election Request
351	54.630631978	192.168.211.122	192.168.211.255	BROWSER	241	Browser Election Request
352	54.630639101	192.168.211.60	192.168.211.255	BROWSER	241	Browser Election Request
353	54.880967689	192.168.211.125	239.255.255.250	SSDP	214	M-SEARCH * HTTP/1.1
354	55.889330324	192.168.211.125	239.255.255.250	SSDP	214	M-SEARCH * HTTP/1.1
355	56.074535861	HewlettP 8c:83:22	Spanning-tree-(for-bri	STP	60	RST. Root = 32768/0/20:e5:2a:68:a2:5a Cost = 1060 Port = 0x8029
356	56.210863052	192.168.211.185	224.0.0.251	MDNS	179	Standard query 0x0000 PTR _ipps_tcp.local, "QM" question PTR _ipp.

Identification: 0x0/e2 (53200)

Flags: 0x4000, Don't fragment

Time to live: 1

Protocol: UDP (17)

Header checksum: 0x1d57 [validation disabled]

[Header checksum status: Unverified]

Source: 192.168.211.72

Destination: 239.255.255.250

User Datagram Protocol, Src Port: 53578, Dst Port: 1900

Source Port: 53578

Destination Port: 1900

Length: 180

Checksum: 0x03aa [unverified]

[Checksum Status: Unverified]

[Stream index: 0]

Simple Service Discovery Protocol

```

0000 01 00 5e 7f ff fa 64 00 6a 19 45 1c 08 00 45 00  ..^...d. j.E...E.
0010 00 c8 d7 e2 40 00 01 11 1d 57 c0 a8 d3 48 ef ff  ....@... .W...H..
0020 ff fa d1 4a 07 6c 00 b4 03 aa 4d 2d 53 45 41 52  ..J.l...M-SEAR
0030 43 48 20 2a 20 48 54 54 50 2f 31 2e 31 0d 0a 48  CH * HTTP/1.1..H
0040 4f 53 54 3a 20 32 33 39 2e 32 35 35 2e 32 35 35  OST: 239 .255.255
0050 2e 32 35 30 3a 31 39 30 30 0d 0a 4d 41 4e 3a 20  .250:190 0..MAN:
0060 22 73 73 64 70 3a 64 69 73 63 6f 76 65 72 22 0d  "ssdp:discover".
0070 0a 4d 58 3a 20 31 0d 0a 53 54 3a 20 75 72 6e 3a  .MX: 1.. ST: urn:
0080 64 69 61 6c 2d 6d 75 6c 74 69 73 63 72 65 65 6e  dial-multiscreen
0090 2d 6f 72 67 3a 73 65 72 76 69 63 65 3a 64 69 61  -org:service:dia
00a0 6c 3a 31 0d 0a 55 53 45 52 2d 41 47 45 4e 54 3a  l:1..USER-AGENT:
00b0 20 47 6f 6f 67 6c 65 20 43 68 72 6f 6d 65 2f 37  Google Chrome/7
00c0 35 2e 30 2e 33 37 37 30 2e 31 34 32 20 4c 69 6e  5.0.3770 .142 Lin
00d0 75 78 0d 0a 0d 0a                                ux....

```

User Datagram Protocol (udp), ... Packets: 356 - Displayed: 356 (100.0%) Profile: Default

## Application layer (FTP header):

FTP stands for File transfer protocol, which is used to transfer files from one host to other. It makes use of two separate connections (Control and Data connections) before transferring files. It uses TCP as its underlying network.

