

Name: Raj Koyani

Reg no: 21MIS1017

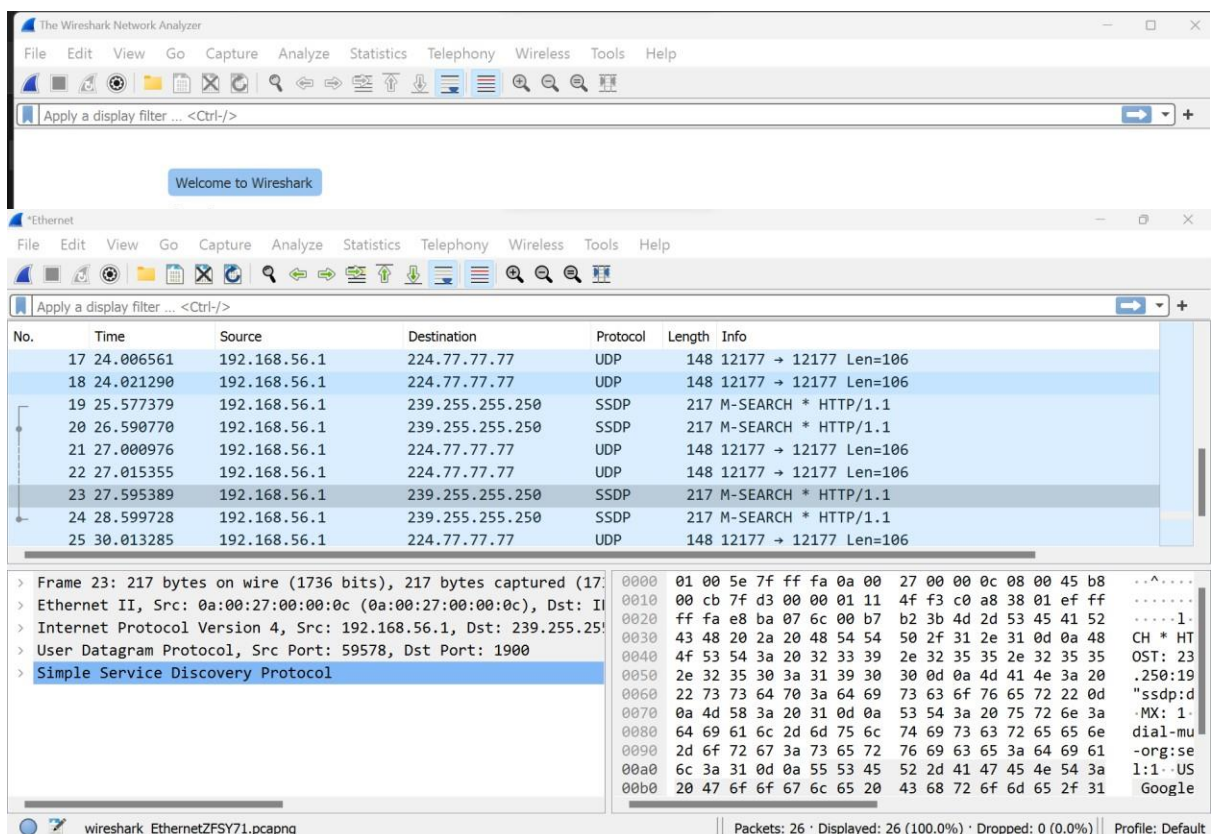
CN:6

(a) Establish a wired network for your startup concern and configure it with a suitable protocol and measure the performance.

Algorithm:

1. Set up the physical network infrastructure: This includes connecting Ethernet cables from each device to a central network switch or router. Ensure that the cables are properly plugged in and the network devices are powered on.
2. Choose a suitable network protocol: Commonly used wired network protocols include Ethernet (e.g., Ethernet 802.3), Fast Ethernet, Gigabit Ethernet, and 10 Gigabit Ethernet. Select a protocol that meets the bandwidth and performance requirements of your startup concern.
3. Configure IP addresses: Assign IP addresses to each device on the network. You can use either static IP addressing or dynamic IP addressing with DHCP (Dynamic Host Configuration Protocol). Configure the IP addresses based on your network's requirements and ensure they are unique for each device.
4. Configure the network devices: Configure the network as UDP TCP etc

Using Wireshark:



The screenshot displays the Wireshark Network Analyzer interface. The top menu bar includes File, Edit, View, Go, Capture, Analyze, Statistics, Telephony, Wireless, Tools, and Help. The toolbar contains various icons for file operations, capture control, and analysis. The display filter bar shows "Apply a display filter ... <Ctrl-/>".

The packet list pane shows a table of captured packets:

No.	Time	Source	Destination	Protocol	Length	Info
17	24.006561	192.168.56.1	224.77.77.77	UDP	148	12177 → 12177 Len=106
18	24.021290	192.168.56.1	224.77.77.77	UDP	148	12177 → 12177 Len=106
19	25.577379	192.168.56.1	239.255.255.250	SSDP	217	M-SEARCH * HTTP/1.1
20	26.590770	192.168.56.1	239.255.255.250	SSDP	217	M-SEARCH * HTTP/1.1
21	27.000976	192.168.56.1	224.77.77.77	UDP	148	12177 → 12177 Len=106
22	27.015355	192.168.56.1	224.77.77.77	UDP	148	12177 → 12177 Len=106
23	27.595389	192.168.56.1	239.255.255.250	SSDP	217	M-SEARCH * HTTP/1.1
24	28.599728	192.168.56.1	239.255.255.250	SSDP	217	M-SEARCH * HTTP/1.1
25	30.013285	192.168.56.1	224.77.77.77	UDP	148	12177 → 12177 Len=106

The packet details pane for the selected packet (No. 23) shows the following structure:

- Frame 23: 217 bytes on wire (1736 bits), 217 bytes captured (1736 bits) on interface 0
- Ethernet II, Src: 0a:00:27:00:00:0c (0a:00:27:00:00:0c), Dst: 01:00:5e:7f:ff:fa
- Internet Protocol Version 4, Src: 192.168.56.1, Dst: 239.255.255.250
- User Datagram Protocol, Src Port: 59578, Dst Port: 1900
- Simple Service Discovery Protocol

The packet bytes pane shows the raw data in hexadecimal and ASCII:

```
0000 01 00 5e 7f ff fa 0a 00 27 00 00 0c 08 00 45 b8  ..^....  
0010 00 cb 7f d3 00 00 01 11 4f f3 c0 a8 38 01 ef ff  ....  
0020 ff fa e8 ba 07 6c 00 b7 b2 3b 4d 2d 53 45 41 52  ....1.  
0030 43 48 20 2a 20 48 54 54 50 2f 31 2e 31 0d 0a 48  CH * HT  
0040 4f 53 54 3a 20 32 33 39 2e 32 35 35 2e 32 35 35  OST: 23  
0050 2e 32 35 30 3a 31 39 30 30 0d 0a 4d 41 4e 3a 20  .250:19  
0060 22 73 73 64 70 3a 64 69 73 63 6f 76 65 72 22 0d  "ssdp:d  
0070 0a 4d 58 3a 20 31 0d 0a 53 54 3a 20 75 72 6e 3a  .MX: 1.  
0080 64 69 61 6c 2d 6d 75 6c 74 69 73 63 72 65 65 6e  dial-mu  
0090 2d 6f 72 67 3a 73 65 72 76 69 63 65 3a 64 69 61  -org:se  
00a0 6c 3a 31 0d 0a 55 53 45 52 2d 41 47 45 4e 54 3a  1:1..US  
00b0 20 47 6f 6f 67 6c 65 20 43 68 72 6f 6d 65 2f 31  Google
```

Ethernet

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

ip.addr == 192.168.56.1 && ip.addr == 224.77.77.77

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	192.168.56.1	224.77.77.77	UDP	148	12177 → 12177 Len=106
2	0.015145	192.168.56.1	224.77.77.77	UDP	148	12177 → 12177 Len=106
3	3.002167	192.168.56.1	224.77.77.77	UDP	148	12177 → 12177 Len=106
4	3.017336	192.168.56.1	224.77.77.77	UDP	148	12177 → 12177 Len=106
5	6.012524	192.168.56.1	224.77.77.77	UDP	148	12177 → 12177 Len=106
6	6.026926	192.168.56.1	224.77.77.77	UDP	148	12177 → 12177 Len=106
7	9.008582	192.168.56.1	224.77.77.77	UDP	148	12177 → 12177 Len=106
8	9.023161	192.168.56.1	224.77.77.77	UDP	148	12177 → 12177 Len=106
9	12.001884	192.168.56.1	224.77.77.77	UDP	148	12177 → 12177 Len=106
10	12.016364	192.168.56.1	224.77.77.77	UDP	148	12177 → 12177 Len=106
11	14.997741	192.168.56.1	224.77.77.77	UDP	148	12177 → 12177 Len=106
12	15.012536	192.168.56.1	224.77.77.77	UDP	148	12177 → 12177 Len=106
13	18.000179	192.168.56.1	224.77.77.77	UDP	148	12177 → 12177 Len=106

> Frame 1: 148 bytes on wire (1184 bits), 148 bytes captured (1184 bits) on interface 0
> Ethernet II, Src: 0a:00:27:00:00:0c (0a:00:27:00:00:0c), Dst: 01:00:5e:4d:4d:0a (01:00:5e:4d:4d:0a)
> Internet Protocol Version 4, Src: 192.168.56.1, Dst: 224.77.77.77
> User Datagram Protocol, Src Port: 12177, Dst Port: 12177
> Data (106 bytes)

Internet Protocol Version 4 (ip), 20 bytes

Packets: 566 · Displayed: 534 (94.3%)

Profile: Default

Ethernet

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

ssdp

No.	Time	Source	Destination	Protocol	Length	Info
49	70.565701	192.168.56.1	239.255.255.250	SSDP	217	M-SEARCH * HTTP/1.1
50	71.574768	192.168.56.1	239.255.255.250	SSDP	217	M-SEARCH * HTTP/1.1
53	72.578407	192.168.56.1	239.255.255.250	SSDP	217	M-SEARCH * HTTP/1.1
54	73.582614	192.168.56.1	239.255.255.250	SSDP	217	M-SEARCH * HTTP/1.1
133	190.573869	192.168.56.1	239.255.255.250	SSDP	217	M-SEARCH * HTTP/1.1
134	191.574540	192.168.56.1	239.255.255.250	SSDP	217	M-SEARCH * HTTP/1.1
137	192.578686	192.168.56.1	239.255.255.250	SSDP	217	M-SEARCH * HTTP/1.1
138	193.582588	192.168.56.1	239.255.255.250	SSDP	217	M-SEARCH * HTTP/1.1
217	310.589796	192.168.56.1	239.255.255.250	SSDP	217	M-SEARCH * HTTP/1.1
218	311.605474	192.168.56.1	239.255.255.250	SSDP	217	M-SEARCH * HTTP/1.1
221	312.610256	192.168.56.1	239.255.255.250	SSDP	217	M-SEARCH * HTTP/1.1
222	313.615008	192.168.56.1	239.255.255.250	SSDP	217	M-SEARCH * HTTP/1.1
301	430.593231	192.168.56.1	239.255.255.250	SSDP	217	M-SEARCH * HTTP/1.1

> Frame 49: 217 bytes on wire (1736 bits), 217 bytes captured (1736 bits) on interface 0
> Ethernet II, Src: 0a:00:27:00:00:0c (0a:00:27:00:00:0c), Dst: 01:00:5e:4d:4d:0a (01:00:5e:4d:4d:0a)
> Internet Protocol Version 4, Src: 192.168.56.1, Dst: 239.255.255.250
> User Datagram Protocol, Src Port: 61820, Dst Port: 1900
> Simple Service Discovery Protocol

Simple Service Discovery Protocol: Protocol

Packets: 588 · Displayed: 31 (5.3%)

Profile: Default

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	192.168.56.1	224.77.77.77	UDP	148	12177 → 12177 Len=106
2	0.015145	192.168.56.1	224.77.77.77	UDP	148	12177 → 12177 Len=106
3	3.002167	192.168.56.1	224.77.77.77	UDP	148	12177 → 12177 Len=106
4	3.017336	192.168.56.1	224.77.77.77	UDP	148	12177 → 12177 Len=106
5	6.012524	192.168.56.1	224.77.77.77	UDP	148	12177 → 12177 Len=106
6	6.026926	192.168.56.1	224.77.77.77	UDP	148	12177 → 12177 Len=106
7	9.008582	192.168.56.1	224.77.77.77	UDP	148	12177 → 12177 Len=106
8	9.023161	192.168.56.1	224.77.77.77	UDP	148	12177 → 12177 Len=106
9	12.001884	192.168.56.1	224.77.77.77	UDP	148	12177 → 12177 Len=106
10	12.016364	192.168.56.1	224.77.77.77	UDP	148	12177 → 12177 Len=106
11	14.997741	192.168.56.1	224.77.77.77	UDP	148	12177 → 12177 Len=106
12	15.012536	192.168.56.1	224.77.77.77	UDP	148	12177 → 12177 Len=106
13	18.000179	192.168.56.1	224.77.77.77	UDP	148	12177 → 12177 Len=106

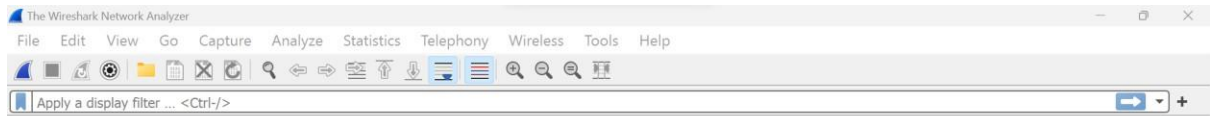
Frame 49: 217 bytes on wire (1736 bits), 217 bytes captured (1736 bits) on interface 0	Details	Bytes	ASCII
Ethernet II, Src: 0a:00:27:00:00:0c (0a:00:27:00:00:0c), Dst: 01:00:5e:7f:ff:fa	0000 01 00 5e 7f ff fa 0a 00 27 00 00 0c 08 00 45 b8	..^....	
Internet Protocol Version 4, Src: 192.168.56.1, Dst: 224.77.77.77	0010 00 cb 7f dc 00 00 01 11 4f ea c0 a8 38 01 ef ff	
User Datagram Protocol, Src Port: 61820, Dst Port: 1900	0020 ff fa f1 7c 07 6c 00 b7 a9 79 4d 2d 53 45 41 521.	
Simple Service Discovery Protocol	0030 43 48 20 2a 20 48 54 54 50 2f 31 2e 31 0d 0a 48	CH * HT	
	0040 4f 53 54 3a 20 32 33 39 2e 32 35 35 2e 32 35 35	OST: 23	
	0050 2e 32 35 30 3a 31 39 30 30 0d 0a 4d 41 4e 3a 20	.250:19	
	0060 72 73 73 64 70 3a 64 60 73 63 6f 76 65 72 72 0d	"e d n d	

(b) Establish a wireless network for your startup concern and configure it with a suitable protocol and measure the performance.

Algorithm:

1. Start a Capture: Open Wireshark and start a new capture. Choose the network adapter that's connected to the network you want to monitor.
2. Analyze the Data: Wireshark will capture all the data that passes through the network adapter. You can analyze this data to measure the performance of your network. Look for things like the amount of data being transferred, the speed of transfers, and any errors that occur.
3. Use Filters: Wireshark allows you to use filters to focus on specific types of data. For example, you can filter by protocol to see only data related to the wireless protocol you're using.
4. Stop the Capture: When you're done analyzing, stop the capture. You can save the capture file for later analysis if you want.

Using Wireshark

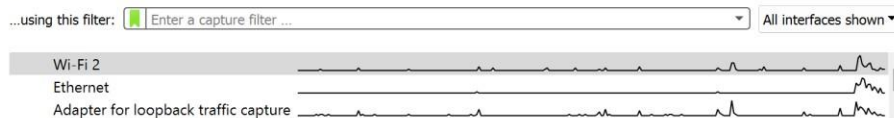


Welcome to Wireshark

Open

C:\Users\Asus\OneDrive\Desktop\CN Lab\Wireshark\Wired.pcapng (147 KB)

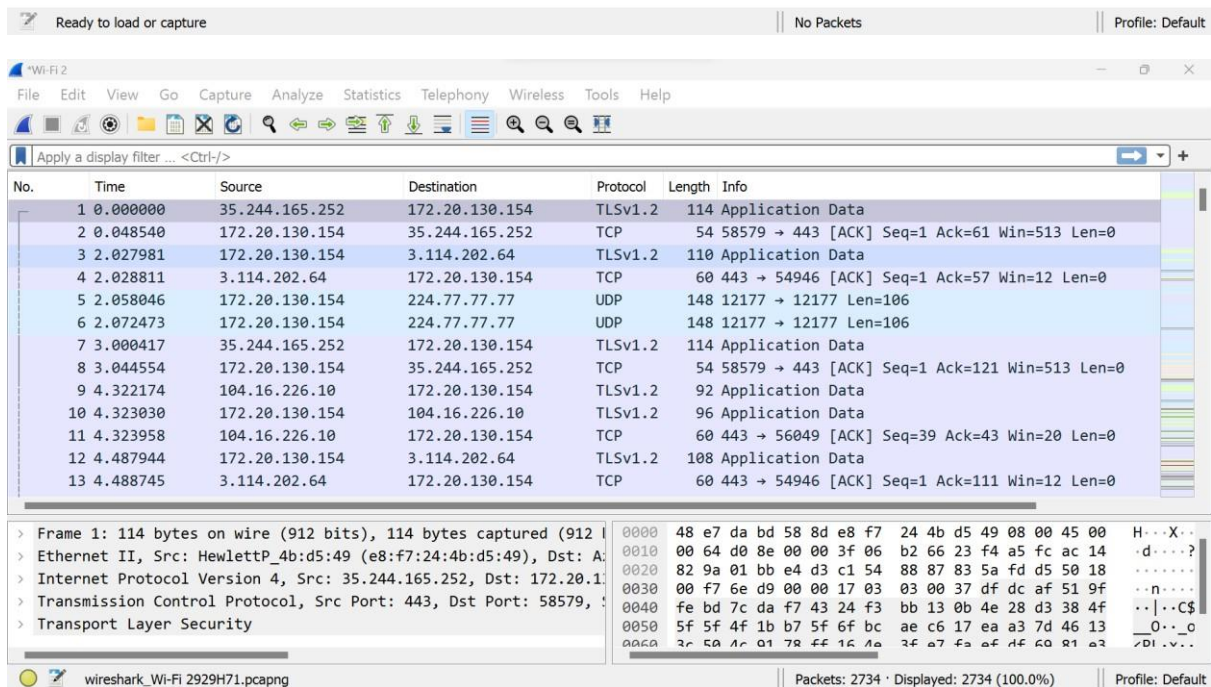
Capture



Learn

[User's Guide](#) · [Wiki](#) · [Questions and Answers](#) · [Mailing Lists](#) · [SharkFest](#) · [Wireshark Discord](#) · [Donate](#)

You are running Wireshark 4.0.6 (v4.0.6-0-gac2f5a01286a). You receive automatic updates.



Wi-Fi 2

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

ip.addr == 35.244.165.252 && ip.addr == 172.20.130.154

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	35.244.165.252	172.20.130.154	TLSv1.2	114	Application Data
2	0.048540	172.20.130.154	35.244.165.252	TCP	54	58579 → 443 [ACK] Seq=1 Ack=61 Win=513 Len=0
7	3.000417	35.244.165.252	172.20.130.154	TLSv1.2	114	Application Data
8	3.044554	172.20.130.154	35.244.165.252	TCP	54	58579 → 443 [ACK] Seq=1 Ack=121 Win=513 Len=0
27	6.000977	35.244.165.252	172.20.130.154	TLSv1.2	114	Application Data
28	6.056570	172.20.130.154	35.244.165.252	TCP	54	58579 → 443 [ACK] Seq=1 Ack=181 Win=513 Len=0
53	9.001764	35.244.165.252	172.20.130.154	TLSv1.2	114	Application Data
54	9.053329	172.20.130.154	35.244.165.252	TCP	54	58579 → 443 [ACK] Seq=1 Ack=241 Win=512 Len=0
66	12.002428	35.244.165.252	172.20.130.154	TLSv1.2	114	Application Data
67	12.046352	172.20.130.154	35.244.165.252	TCP	54	58579 → 443 [ACK] Seq=1 Ack=301 Win=512 Len=0
74	15.002726	35.244.165.252	172.20.130.154	TLSv1.2	114	Application Data
75	15.058080	172.20.130.154	35.244.165.252	TCP	54	58579 → 443 [ACK] Seq=1 Ack=361 Win=512 Len=0
99	18.003127	35.244.165.252	172.20.130.154	TLSv1.2	114	Application Data

> Frame 1: 114 bytes on wire (912 bits), 114 bytes captured (912) on interface 0
 > Ethernet II, Src: HewlettP_4b:d5:49 (e8:f7:24:4b:d5:49), Dst: A
 > Internet Protocol Version 4, Src: 35.244.165.252, Dst: 172.20.130.154
 > Transmission Control Protocol, Src Port: 443, Dst Port: 58579, Seq=1, Win=513, Len=0
 > Transport Layer Security

wireshark_Wi-Fi 2929H71.pcapng

Packets: 2734 · Displayed: 96 (3.5%) · Dropped: 0 (0.0%) Profile: Default

Wi-Fi 2

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

http

No.	Time	Source	Destination	Protocol	Length	Info
36	7.304931	172.20.130.154	23.205.118.16	HTTP	208	GET /connecttest.txt HTTP/1.1
38	7.313060	23.205.118.16	172.20.130.154	HTTP	241	HTTP/1.1 200 OK (text/plain)
141	20.680640	172.20.130.154	91.108.23.100	HTTP	154	POST /api HTTP/1.1 (application/x-www-form-urlencoded)
170	20.708105	91.108.23.100	172.20.130.154	HTTP	313	HTTP/1.1 200 OK
343	21.204069	172.20.130.154	23.205.118.16	HTTP	165	GET /connecttest.txt HTTP/1.1
345	21.211568	23.205.118.16	172.20.130.154	HTTP	241	HTTP/1.1 200 OK (text/plain)
415	21.653663	172.20.130.154	91.108.23.100	HTTP	290	POST /api HTTP/1.1 (application/x-www-form-urlencoded)
416	21.653678	172.20.130.154	91.108.56.120	HTTP	222	POST /api HTTP/1.1 (application/x-www-form-urlencoded)
417	21.653689	172.20.130.154	91.108.23.100	HTTP	326	POST /api HTTP/1.1 (application/x-www-form-urlencoded)
460	21.685053	91.108.23.100	172.20.130.154	HTTP	349	HTTP/1.1 200 OK
467	21.687308	91.108.23.100	172.20.130.154	HTTP	317	HTTP/1.1 200 OK
1699	55.345634	172.20.130.154	23.205.118.154	HTTP	208	GET /connecttest.txt HTTP/1.1
1701	55.361554	23.205.118.154	172.20.130.154	HTTP	241	HTTP/1.1 200 OK (text/plain)

> Frame 36: 208 bytes on wire (1664 bits), 208 bytes captured (1664) on interface 0
 > Ethernet II, Src: AzureWav_bd:58:8d (48:e7:da:bd:58:8d), Dst: I
 > Internet Protocol Version 4, Src: 172.20.130.154, Dst: 23.205.118.16
 > Transmission Control Protocol, Src Port: 59113, Dst Port: 80, Seq=1, Win=0, Len=0
 > Hypertext Transfer Protocol

Hypertext Transfer Protocol: Protocol

Packets: 2734 · Displayed: 17 (0.6%) · Dropped: 0 (0.0%) Profile: Default

No.	Time	Source	Destination	Protocol	Length	Info
121	20.632779	AzureWav_bd:58:8d	Broadcast	ARP	42	Who has 172.20.128.1? Tell 172.20.130.154
124	20.639646	IETF-VRRP-VRID_0e	AzureWav_bd:58:8d	ARP	60	172.20.128.1 is at 00:00:5e:00:01:0e
125	20.639646	IntelCor_e3:95:1d	AzureWav_bd:58:8d	ARP	56	172.20.130.97 is at f4:c8:8a:e3:95:1d
168	20.703352	IntelCor_e2:07:d9	AzureWav_bd:58:8d	ARP	56	172.20.131.6 is at 2c:db:07:e2:07:d9
169	20.703448	5e:7d:97:ba:aa:31	AzureWav_bd:58:8d	ARP	56	172.20.129.116 is at 5e:7d:97:ba:aa:31
179	20.717973	IntelCor_fa:28:a5	AzureWav_bd:58:8d	ARP	56	172.20.128.66 is at 7c:50:79:fa:28:a5
290	20.914693	AzureWav_bd:58:8d	Broadcast	ARP	42	Who has 172.20.128.1? Tell 172.20.130.154
291	20.917304	IETF-VRRP-VRID_0e	AzureWav_bd:58:8d	ARP	60	172.20.128.1 is at 00:00:5e:00:01:0e
292	20.920863	IntelCor_fa:28:a5	AzureWav_bd:58:8d	ARP	56	172.20.128.66 is at 7c:50:79:fa:28:a5
301	20.936960	IntelCor_e3:95:1d	AzureWav_bd:58:8d	ARP	56	172.20.130.97 is at f4:c8:8a:e3:95:1d
302	20.942242	IntelCor_ee:7c:49	AzureWav_bd:58:8d	ARP	56	172.20.129.28 is at f0:77:c3:ee:7c:49
303	20.945239	IntelCor_fa:96:73	AzureWav_bd:58:8d	ARP	56	172.20.128.242 is at dc:21:48:fa:96:73
308	20.956579	IntelCor_f3:2f:a5	AzureWav_bd:58:8d	ARP	56	172.20.131.91 is at 60:dd:8e:f3:2f:a5

Frame 121: 42 bytes on wire (336 bits), 42 bytes captured (336) on interface 0	0000	ff ff ff ff ff ff 48 e7 da bd 58 8d 08 06 00 01H-
Ethernet II, Src: AzureWav_bd:58:8d (48:e7:da:bd:58:8d), Dst: Broadcast	0010	08 00 06 04 00 01 48 e7 da bd 58 8d ac 14 82 9aH-
Address Resolution Protocol (request)	0020	00 00 00 00 00 00 ac 14 80 01H-

Address Resolution Protocol: Protocol | Packets: 2734 · Displayed: 454 (16.6%) · Dropped: 0 (0.0%) | Profile: Default

(c) Compare the performance of the above two scenarios.

Algorithm:

As packets are captured, Wireshark displays them in the main window. Expand each captured packet to view detailed information about the wireless communication, such as source and destination MAC addresses, signal strength, data rate, and other relevant fields. Look for patterns or anomalies in the packet data that might indicate performance issues, such as high packet loss, low signal strength, or excessive retransmissions.

Performance Metrics:

Wireshark provides various performance metrics to assess the wireless network's performance. You can use features like **"Statistics" -> "Conversations"** to view statistics about packet exchanges between devices, including packet counts, data volume, and average packet sizes. Analyze **"Statistics" -> "IO Graphs"** to generate graphs showing metrics like packet rate, data rate, or signal strength over time.

Wireless.pcapng

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Apply a display filter ... <Ctrl-/>

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	35.244.165.252	172.20.130.154	TLSv1.2	114	Application Data
2	0.048540	172.20.130.154	35.244.165.252	TCP	54	58579 → 443 [ACK] Seq=1 Ack=61 Win=513 Len=0
3	2.027981	172.20.130.154	3.114.202.64	TLSv1.2	110	Application Data
4	2.028811	3.114.202.64	172.20.130.154	TCP	60	443 → 54946 [ACK] Seq=1 Ack=57 Win=12 Len=0
5	2.058046	172.20.130.154	224.77.77.77	UDP	148	12177 → 12177 Len=106
6	2.072473	172.20.130.154	224.77.77.77	UDP	148	12177 → 12177 Len=106
7	3.000417	35.244.165.252	172.20.130.154	TLSv1.2	114	Application Data
8	3.044554	172.20.130.154	35.244.165.252	TCP	54	58579 → 443 [ACK] Seq=1 Ack=121 Win=513 Len=0
9	4.322174	104.16.226.10	172.20.130.154	TLSv1.2	92	Application Data
10	4.323030	172.20.130.154	104.16.226.10	TLSv1.2	96	Application Data

> Frame 3: 110 bytes on wire (880 bits), 110 bytes captured (880 bits) on interface 0
> Ethernet II, Src: AzureWav_bd:58:8d (48:e7:da:bd:58:8d), Dst: Intel_Ethernet_E7:9B:34:43:10:00 (08:00:00:00:00:00)
> Internet Protocol Version 4, Src: 172.20.130.154, Dst: 3.114.202.64
> Transmission Control Protocol, Src Port: 54946, Dst Port: 443, Seq: 1, Len: 0
> Transport Layer Security

0000 00 00 5e 00 01 0e 48 e7 da bd 58 8d 08 00 45 b8 ...H...
0010 00 60 3b 6b 40 00 80 06 c2 13 ac 14 82 9a 03 72 ...;k@...
0020 ca 40 d6 a2 01 bb 93 57 24 20 78 1b 74 2b 50 18 ...@.....W
0030 10 00 4b ac 00 00 17 03 03 00 33 ee 54 f9 43 5f ...K.....
0040 d1 22 02 2c 5a 4b 06 67 f7 30 2c 8d 9a 1e 41 2e ...".,ZK.g
0050 fd ed aa e7 8f 4c 83 0d 7e 40 f5 7e 00 1e 0d 5bL..
0060 76 91 95 ea d8 84 27 2b ea 02 1e dd 70 a0 v.....'+

Wireless.pcapng Packets: 2734 · Displayed: 2734 (100.0%) · Dropped: 0 (0.0%) Profile: Default

Wireshark · Conversations · Wireless.pcapng

Conversation Settings

- ☐ Name resolution
- ☐ Absolute start time
- ☐ Limit to display filter

Copy

Follow Stream...

Graph...

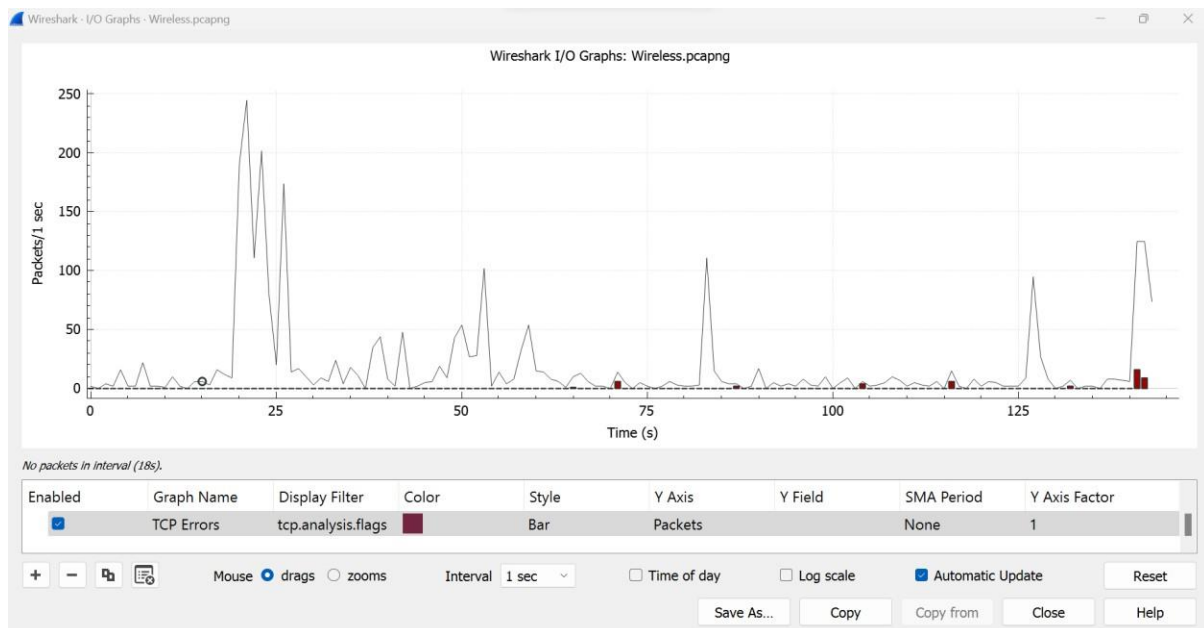
Protocol

- ☐ Bluetooth
- ☐ DCCP
- ☒ Ethernet
- ☐ FC
- ☐ FDDI
- ☐ IEEE 802.11
- ☐ IEEE 802.15.4
- ☒ IPv4
- ☐ IPv6

Filter list for specific type

Ethernet · 28		IPv4 · 41		IPv6 · 7		TCP · 68		UDP · 76	
Address A	Address B	Packets	Bytes	Packets A → B	Bytes A → B	Packets B → A	Bytes B → A	Rel Start	
2c:db:07:e2:07:d9	48:e7:da:bd:58:8d	8	448 bytes	8	448 bytes	0	0 bytes	20.703352	
48:e7:da:bd:58:8d	00:00:5e:00:01:0e	951	220.762 KiB	947	220.527 KiB	4	240 bytes	0.048540	
48:e7:da:bd:58:8d	01:00:5e:00:00:16	11	618 bytes	11	618 bytes	0	0 bytes	21.006983	
48:e7:da:bd:58:8d	01:00:5e:00:00:fb	68	10.401 KiB	68	10.401 KiB	0	0 bytes	10.372046	
48:e7:da:bd:58:8d	01:00:5e:00:00:fc	13	834 bytes	13	834 bytes	0	0 bytes	22.667204	
48:e7:da:bd:58:8d	01:00:5e:4d:4d:4d	94	13.586 KiB	94	13.586 KiB	0	0 bytes	2.058046	
48:e7:da:bd:58:8d	01:00:5e:7f:ff:fa	23	4.614 KiB	23	4.614 KiB	0	0 bytes	21.103924	
48:e7:da:bd:58:8d	33:33:00:00:00:01	1	86 bytes	1	86 bytes	0	0 bytes	22.008550	
48:e7:da:bd:58:8d	33:33:00:00:00:02	4	264 bytes	4	264 bytes	0	0 bytes	21.007142	
48:e7:da:bd:58:8d	33:33:00:00:00:16	16	1.523 KiB	16	1.523 KiB	0	0 bytes	21.007180	
48:e7:da:bd:58:8d	33:33:00:00:00:fb	49	4.664 KiB	49	4.664 KiB	0	0 bytes	22.096352	
48:e7:da:bd:58:8d	33:33:00:01:00:02	10	1.445 KiB	10	1.445 KiB	0	0 bytes	4.691587	
48:e7:da:bd:58:8d	33:33:00:01:00:03	13	1.068 KiB	13	1.068 KiB	0	0 bytes	22.667141	
48:e7:da:bd:58:8d	33:33:ff:b7:1b:a9	2	156 bytes	2	156 bytes	0	0 bytes	21.007114	
48:e7:da:bd:58:8d	ff:ff:ff:ff:ff:ff	21	1.854 KiB	21	1.854 KiB	0	0 bytes	20.628031	
5c:8a:38:b9:04:2b	ff:ff:ff:ff:ff:ff	123	7.688 KiB	123	7.688 KiB	0	0 bytes	23.087986	
5c:8a:38:b9:04:36	48:e7:da:bd:58:8d	54	7.966 KiB	52	7.884 KiB	2	84 bytes	7.303465	
5e:7d:97:ba:aa:31	48:e7:da:bd:58:8d	8	448 bytes	8	448 bytes	0	0 bytes	20.703448	
60:dd:8e:f3:2f:a5	48:e7:da:bd:58:8d	8	448 bytes	8	448 bytes	0	0 bytes	20.956579	
70:3a:0e:fe:85:10	48:e7:da:bd:58:8d	151	164.412 KiB	151	164.412 KiB	0	0 bytes	20.696535	
70:3a:0e:fe:85:10	48:e7:da:bd:58:8d	5	717 bytes	5	717 bytes	0	0 bytes	1.027715	

Close Help



1. Wired Network Performance Measurement:

- **Bandwidth:** Measure the maximum data transfer rate supported by the wired network using tools like iPerf or speedtest.net.
- **Latency:** Measure the round-trip time (RTT) using tools like ping or traceroute to assess the delay in communication.
- **Throughput:** Measure the data transfer rate over a specific period of time using tools like iPerf or network monitoring software.
- **Packet Loss:** Measure the percentage of lost packets during transmission using tools like ping or network monitoring software.
- **Network Efficiency:** Monitor network utilization, traffic patterns, bottlenecks, and congestion using network monitoring software.

2. Wireless Network Performance Measurement:

- **Signal Strength:** Measure the strength of the wireless signal using tools like NetSpot or insider to identify areas with weak coverage.
- **Signal-to-Noise Ratio (SNR):** Measure the ratio of the signal strength to the background noise level to assess the quality of the wireless signal.
- **Throughput:** Measure the data transfer rate over the wireless network using tools like iPerf or network monitoring software.
- **Latency:** Measure the round-trip time (RTT) using tools like ping or traceroute to assess the delay in communication.
- **Packet Loss:** Measure the percentage of lost packets during wireless transmission using tools like ping or network monitoring software.
- **Network Efficiency:** Monitor network utilization, traffic patterns, and potential interference sources (e.g., overlapping channels) using network monitoring software.

d) Using Wireshark, Capture, Filter and inspect the packets for the above network.

Wired Network:

The screenshot shows the Wireshark interface with a capture filter set to 'udp'. The packet list displays 13 packets, all of which are UDP datagrams from source 192.168.56.1 to destination 224.77.77.77. The packet details pane for packet 49 is expanded, showing the following layers:

- Frame 49: 217 bytes on wire (1736 bits), 217 bytes captured (1736 bits) on interface 0
- Ethernet II, Src: 0a:00:27:00:00:0c (0a:00:27:00:00:0c), Dst: 01:00:5e:7f:ff:fa (01:00:5e:7f:ff:fa)
- Internet Protocol Version 4, Src: 192.168.56.1, Dst: 224.77.77.77
- User Datagram Protocol, Src Port: 61820, Dst Port: 1900
- Simple Service Discovery Protocol

The packet bytes pane shows the raw data in hexadecimal and ASCII. The status bar at the bottom indicates 611 packets displayed (100.0%) and the profile is set to Default.

Wireless Network:

The screenshot shows the Wireshark interface with a capture filter set to 'arp'. The packet list displays 13 packets, all of which are ARP requests from various sources to destination 172.20.128.1. The packet details pane for packet 121 is expanded, showing the following layers:

- Frame 121: 42 bytes on wire (336 bits), 42 bytes captured (336 bits) on interface 0
- Ethernet II, Src: AzureWav_bd:58:8d (48:e7:da:bd:58:8d), Dst: Broadcast
- Address Resolution Protocol (request)

The packet bytes pane shows the raw data in hexadecimal and ASCII. The status bar at the bottom indicates 2734 packets displayed (16.6%) and 0 packets dropped (0.0%), with the profile set to Default.

CPT Model Algorithm

1. Select the network interface: Choose the network interface that corresponds to the wired or wireless network you want to capture packets from. Click on "Capture Options" or select the desired interface from the drop-down menu.

2. Start packet capture: Click on the "Start" or "Capture" button to begin capturing packets on the selected interface.

3. Apply filters: Use Wireshark's filtering capabilities to focus on specific packets you want to inspect. Some commonly used filters include:

- "tcp": Captures only TCP packets.
- "arp": Captures only ARP packets.
- "ip.src == [source IP] && ip.dst == [destination IP]": Filters packets based on specific source and destination IP addresses.

4. Analyze captured packets: As packets are captured, Wireshark will display a list of captured packets in the main window. You can click on individual packets to inspect their details in the packet details pane.

Wireshark provides extensive packet analysis features, including packet decoding, source and destination addresses, protocols used, packet length, and more. You can expand each packet to explore the layers and fields within.

5. Save captured packets: If you want to save the captured packets for further analysis or reference, go to "File" and select "Save As" to save the packet capture in a suitable format, such as a .pcap file.

Stop packet capture: When you have captured the desired packets or completed your analysis, click on the "Stop" or "Capture" button in Wireshark to end the packet capture.

