

what is networking ?

- **Networking** is the process of connecting two or more computers or devices so they can communicate, share data, and use resources like the internet, files, printers, and applications.
- Example:
When your phone connects to Wi-Fi and opens a website, it is using networking to send and receive data.
- **IP Address (Internet Protocol Address)**
An IP address is a unique numerical label assigned to a device on a network to identify it and enable communication between devices over the internet or a local network.
- **MAC Address (Media Access Control Address)**
A MAC address is a permanent, unique hardware identifier assigned to a network interface card (NIC) by the manufacturer to identify a device within a local network.
- **DNS (Domain Name System)**
DNS is a system that translates human-readable domain names (like websites) into IP addresses so that computers can locate and communicate with each other on the internet.
- **TCP (Transmission Control Protocol)**
TCP is a connection-oriented communication protocol that ensures reliable, ordered, and error-free delivery of data between devices.
- **UDP (User Datagram Protocol)**
UDP is a connectionless communication protocol that sends data without guaranteeing delivery, order, or error checking, prioritizing speed over reliability.

1. Filter packets by protocol (HTTP, DNS, TCP).

➤ TCP:

➤ DNS:

➤ HTTP:

```

http
No. Time Source Destination Protocol Length Info
+ 126 19.7.933980 10.6.13.133 23.192.223.206 HTTP/1.1
  133 19.7.933980 10.6.13.133 23.192.223.206 HTTP/1.1
  468 18.932658 10.6.13.133 217.20.51.22 HTTP/1.1
  464 18.965580 217.20.51.22 10.6.13.133 HTTP/1.1
  466 19.881288 10.6.13.133 217.20.51.22 HTTP/1.1
  467 19.115178 217.20.51.22 10.6.13.133 HTTP/1.1
  5979 26.252259 10.6.13.133 10.6.13.133 HTTP/X...
  5982 26.254088 10.6.13.133 10.6.13.133 HTTP/X...
  6642 11.3.131635 10.6.13.133 104.21.24.186 HTTP/1.1
  6654 11.3.323933 104.21.24.186 10.6.13.133 HTTP/1.1
  6699 12.774462 10.6.13.133 104.21.112.1 HTTP/1.1
  8561 149.326987 104.21.112.1 10.6.13.133 HTTP/1.1
  44292 209.7.130387 10.6.13.133 104.21.16.1 HTTP/1.1
  44436 239.182819 10.6.13.133 104.21.16.1 HTTP/1.1
  44495 269.891374 10.6.13.133 104.21.16.1 HTTP/1.1
  44502 10.6.13.133 104.16.130.132 HTTP/1.1
  44693 336.100565 10.6.13.133 104.21.16.1 HTTP/1.1
  47756 36.282282 10.6.13.133 104.21.16.1 HTTP/1.1
  48416 390.364199 10.6.13.133 104.16.230.132 HTTP/1.1
  48468 420.467370 10.6.13.133 104.21.16.1 HTTP/1.1
  49029 450.562340 10.6.13.133 104.16.130.132 HTTP/1.1

Frame 126: Packet, 165 bytes on wire (1320 bits), 165 bytes captured (1320 bits)
Ethernet II, Src: Intel_ac:97:df (24:77:03:ac:97:df), Dst: Cisco_54:95:22 (00:02:ba:54:95:22)
Internet Protocol Version 4, Src: 10.6.13.133, Dst: 23.192.223.206
Transmission Control Protocol, Src Port: 52431, Dst Port: 80, Seq: 1, Ack: 1, Len: 111
Hypertext Transfer Protocol

 0000  00 02 da 54 95 22 44 77 03 ac 97 df 08 45 00 ...-T~w-----E:
 0010  00 07 f7 a3 00 80 06 f3 a3 0a 06 d5 17 c0 ...@-----P...
 0020  d7 cc cc cf 00 44 bd 0d 68 1a 08 fc 50 18 ...P-----P...
 0030  00 00 00 00 00 00 47 45 5d 28 2f 63 0e 66 69 ...-----P...
 0040  00 00 00 00 00 00 78 00 00 00 00 00 00 00 00 00 ...-----P...
 0050  31 2e 31 0d 0e 43 f6 6e 65 65 7d 74 09 ff 6e 3a 1. Con nection:
 0060  20 43 6c 73 65 0d 55 65 73 65 72 2d 41 67 65 ...Close User-Age
 0070  6e 7a 3a 20 4d 69 63 72 f6 73 6f 66 74 20 4e 43 ...nt: Microsoft NC
 0080  53 49 0d 08 4f 6f 74 3a 20 27 77 77 2e 6d 73 SI Host: www.ms
 0090  66 74 63 6f 6e 65 65 74 74 65 73 74 2e 63 6f ftconnect ttest.co
 00a0  6d 0d 00 00 00 ...m...
```

➤ TLS:

No.	Time	Source	Destination	Protocol	Length Info
95	8.3.74958	173.222.52.33	10.6.13.133	TLSv1.2	344 bytes Session Ticket, Change Cipher Spec, Encrypted Handshake Message
96	8.3.74970	10.6.13.133	173.222.52.33	TLSv1.2	388 Application Data
98	8.4.176431	173.222.52.33	10.6.13.133	TLSv1.2	60 Application Data
105	8.4.548457	10.6.13.133	52.156.123.84	TLSv1.2	260 Client Hello (SNI=geo.prod.do.dsp.mp.microsoft.com)
107	8.4.637310	52.156.123.84	10.6.13.133	TLSv1.2	1110 Server Hello, Certificate, Server Key Exchange, Server Hello Done
109	8.4.639153	10.6.13.133	52.156.123.84	TLSv1.2	212 Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
116	8.4.727252	52.156.123.84	10.6.13.133	TLSv1.2	105 Change Cipher Spec, Encrypted Handshake Message
117	8.4.727253	52.156.123.84	10.6.13.133	TLSv1.2	123 Application Data
119	8.4.728072	10.6.13.133	52.156.123.84	TLSv1.2	141 Application Data
120	8.4.728073	10.6.13.133	52.156.123.84	TLSv1.2	228 Application Data
121	8.4.728074	10.6.13.133	52.156.123.84	TLSv1.2	92 Application Data
127	8.4.808776	52.156.123.84	10.6.13.133	TLSv1.2	92 Application Data
129	8.4.808776	52.156.123.84	10.6.13.133	TLSv1.2	631 Application Data
148	8.5.540678	10.6.13.133	104.208.203.90	TLSv1.2	232 Client Hello (SNI=client.wms.windows.com)
150	8.5.540678	104.208.203.90	10.6.13.133	TLSv1.2	138 Client Hello, Certificate, Server Key Exchange, Server Hello Done
153	8.5.663197	10.6.13.133	104.208.203.90	TLSv1.2	212 Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
157	8.5.735236	104.208.203.90	10.6.13.133	TLSv1.2	105 Change Cipher Spec, Encrypted Handshake Message
158	8.5.738184	10.6.13.133	104.208.203.90	TLSv1.2	414 Application Data
160	8.5.738188	10.6.13.133	104.208.203.90	TLSv1.2	71 Application Data
161	8.5.738189	10.6.13.133	104.208.203.90	TLSv1.2	381 Application Data
162	8.5.820338	104.208.203.90	10.6.13.133	TLSv1.2	331 Application Data

Frame 121: Packet, 92 bytes on wire (736 bits), 92 bytes captured (736 bits)
Ethernet II, Src: Intel_ae:97:df (24:77:03:a6:97:df), Dst: Cisco_54:95:22 (00:02:ba:54:95:22)
Internet Protocol Version 4, Src: 10.6.13.133, Dst: 52.156.123.84
Transmission Control Protocol, Src Port: 52450, Dst Port: 443, Seq: 635, Ack: 2553, Len: 38
Transport Layer Security

0000 00 02 ba 54 95 22 24 77 03 ac 97 df 08 00 45 00 ... T "\$w" E
0010 00 04 82 1a 00 80 06 b1 14 0a 06 0d 85 34 9c N @ 4
0020 00 00 cc 00 00 00 00 00 00 00 00 00 00 00 00 00 T [GGP
0030 00 ff 00 7a 00 00 17 a3 00 00 00 00 00 00 00 00 00 T - t -
0040 00 00 03 5f 84 07 9d 0d 91 f0 3c 3f ca 73 08 03 ? sh
0050 03 2e d5 6c 2a 81 b1 f7 85 9d aa 8b . 1* ..

➤ TCP 3-Way Handshake:

No.	Time	Source	Destination	Protocol	Length Info
28	0.156966	10.6.13.133	10.6.13.3	TCP	66 52427 + 389 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM
29	0.156969	10.6.13.3	10.6.13.133	TCP	66 389 + 52427 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM
35	0.159844	10.6.13.133	10.6.13.3	TCP	66 52428 + 88 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM
36	0.159846	10.6.13.3	10.6.13.133	TCP	66 88 + 52428 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM
80	0.227463	10.6.13.133	10.6.13.133	TCP	66 52429 + 443 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM
81	0.227469	173.222.52.33	10.6.13.133	TCP	66 0 + 52429 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM
107	0.5460312	10.6.13.133	52.156.123.84	TCP	66 52430 + 443 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM
103	0.547295	52.156.123.84	10.6.13.133	TCP	66 443 + 52430 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1396 WS=256 SACK_PERM
123	4.7.576187	10.6.13.133	23.192.223.206	TCP	66 52431 + 88 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM
124	4.7.576188	23.192.223.206	10.6.13.133	TCP	66 80 + 52431 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1396 SACK_PERM WS=128
145	5.5.134947	10.6.13.133	104.208.203.90	TCP	66 52432 + 443 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM
146	5.5.889189	104.208.203.90	10.6.13.133	TCP	66 443 + 52432 [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0 MSS=1396 WS=1 SACK_PERM
196	14.222837	10.6.13.133	10.6.13.3	TCP	66 52433 + 88 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM
197	14.222840	10.6.13.3	10.6.13.133	TCP	66 88 + 52433 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM
204	14.232483	10.6.13.133	10.6.13.3	TCP	66 52434 + 88 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM
205	14.232485	10.6.13.3	10.6.13.133	TCP	66 88 + 52434 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM
214	14.235093	10.6.13.133	10.6.13.3	TCP	66 52435 + 88 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM
215	14.235099	10.6.13.3	10.6.13.133	TCP	66 88 + 52435 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM
231	14.434042	10.6.13.133	10.6.13.3	TCP	66 52436 + 445 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM
232	14.434044	10.6.13.3	10.6.13.133	TCP	66 445 + 52436 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM
274	14.435377	10.6.13.133	10.6.13.3	TCP	66 52437 + 135 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM

Frame 103: Packet, 66 bytes on wire (528 bits), 66 bytes captured (528 bits)
Ethernet II, Src: Cisco_54:95:22 (00:02:ba:54:95:22), Dst: Intel_ae:97:df (24:77:03:a6:97:df)
Internet Protocol Version 4, Src: 10.6.13.133, Dst: 52.156.123.84
Transmission Control Protocol, Src Port: 443, Dst Port: 52430, Seq: 0, Ack: 1, Len: 0

0000 24 77 03 ac 97 df 00 02 ba 54 95 22 08 00 45 00 Sw T "-" E
0010 00 34 53 29 40 00 66 00 fa 1f 34 9c 7b 54 0a 06 45)@ f 4 (T
0020 00 85 01 bb cc ce 87 47 35 f4 5b 4b fe cd 80 12 G 5 [K
0030 ff ff c1 ee 00 00 02 04 05 74 01 03 08 01 01 t t
0040 04 02 ..