Computer Networking

1. **Network** -> Computers connected together is a network.
2. **Internet** -> Collection of computer network connected to each other on a global scale is called internet.
3. **Protocol** -> A protocol is a set of rules and guidelines for communicating data. Rules are defined for each step and process during communication between two or more computers. Networks have to follow these rules to successfully transmit data.
4. **World wide web (www)** -> The World Wide Web (WWW) is a network of online content that is formatted in HTML and accessed via HTTP. The term refers to all the interlinked HTML pages that can be accessed over the Internet.
5. Internet Society creates protocols for communicating data.
6. When we type google.com on our local machine (client) , it sends the request to the google server, google server send back the response to our local machine(client) with all the required web page and google web page opens on our local machine.
7. **TCP** -> TCP stands for transmission control protocol. It is a type of protocol. TCP makes sure your data reaches its destination in complete format , without data been corrupted.
8. **UDP** -> UDP stands for User Datagram Protocol. It is a type of protocol. The UDP helps to establish low-latency and loss-tolerating connections establish over the network.When we do not care whether 100 percent data is reaching to the destination. example - Video conferencing.
9. **HTTP** -> HTTP stands for hyper text transfer protocol. It is a type of protocol. It defines the format of the data that is transferred between clients and server.
10. Data is transferred in the form of packets.
11. **IP address** -> IP (Internet Protocol) addresses are used to identify hardware devices on a network. The addresses allow these devices to connect to one another and transfer data on a local network or over the internet.
12. IP address format x . x . x . x , where every x can range from 0-255. When we type google.com it resolves to a particular IP address.
13. **curl ifconfig.me -s** -> Check IP address of our own computer given by internet provider.
14. We have Internet service provider (ISP) . ISP gives us a router. Router is going to have a global IP address. The devices connected to the router have the local IP address given by the router. Router assigns the local IP address to the device connected to it using **DHCP protocol**. DHCP stands for dynamic host configuration protocol. If you make a request to google.com from your device, the google server will see the global IP address of the router and not your device local IP address.
15. When the response comes from google server to the router through ISP, the router will check which device requested for the google page using **Network address Translation(NAT).**
16. But which application in the device made the request ? -> We can know that using **Port.** IP address decides which device to send the data and port decide which application to send the data in that device.
17. **Port** -> Port are 16 bit number. 65000 port number are available. Every application in a device

have a port number and they are running on that specific port.

18. HTTP -> Port 80. MongoDB -> Port 27017.
19. Ports from 0 to 1023 are reserved ports.
20. Ports from 1024 to 49152 are registered for specific applications. example - mongodb , mysql. SQL server -> port 1433. Remaining ports we can use.
21. 1 Mbps -> 10^6 bits per second. 1 Gbps -> 10^9 bits per second. 1Kbps -> 10^3 bits per second.
22. **Upload speed** -> Speed with which you are sending the data from your computer to the other computer via internet.
23. **Download speed** -> Speed with which you are downloading the data on your computer, send by some other computer via internet.
24. **Local Area Network (LAN)** -> A local area network (LAN) is a collection of devices connected together in one physical location, such as a building, office, or home. A LAN can be small or large, ranging from a home network with one user to an enterprise network with thousands of users and devices in an office or school.
25. **Metropolitan Area Network (MAN)** -> A metropolitan area network (MAN) is a computer network that connects computers within a metropolitan area, which could be a single large city, multiple cities and towns, or any given large area with multiple buildings.
26. **Wide Area Network (WAN)** -> A wide area network (WAN) is a large computer network that connects groups of computers over large distances(country) using optical fibre cables.
27. **Modem** -> Modem is used to convert the digital signals to analog signals and vice versa. The digital data from your computer,modem can convert it into electrical signals so that you can transfer it via telephone lines.
28. **Router** -> Router is a device that routes the data packet based on their IP address.
29. **Topology** -> Topology defines the structure of the network of how all the components are interconnected to each other.
30. **Bus topology** -> The bus topology is designed in such a way that all the stations are connected through a single cable known as a backbone cable.If the backbone cable gets broken entire network is spoiled. Only one person can send the data over particular time.
31. **Ring topology** -> Computers are connected in a ring with one another. If one of the cable breaks you cannot transmit the data.Unnecessary lot of calls are made.
32. **Star topology** -> One central device that is connected to all computers. If computer A wants to communicate with computer B it will communicate via Central Device. If central device fails, your network will go down.
33. **Tree topology** -> Combination of bus and star topology. Many central devices are connected in bus sort of a way.Many computers are connected to the central devices. has more fault tolerance.
34. **Mesh topology** -> Every single computer is connected to every single computer. It is expensive(many wires). Scalability issues.
35. **OSI Model** -> OSI stands for open system interconnection model. It is a standard about how two devices interconnect with each other. There are 7 layers in OSI model. Application layer, Presentation layer, Session layer, Transport layer, Network layer,Data link layer, Physical layer.
36. **Abstract of OSI model** -> Application layer consist of the application with which user is interacting.Then the data is send from application layer to presentation layer.The data from the

application layer is in words,characters,numbers etc, that data will be converted to machine understandable binary format by presentation layer. Data is also compressed and encrypted. Data is then send to session layer. This layer allows users on different machines to establish active communications sessions between them. It is responsible for establishing, maintaining, synchronizing, terminating sessions between end-user applications. Then data is transferred from session layer to transport layer. This layer has its own protocol about how the data is transferred. It does in 3 ways. **Segmentation** - Data which is received from session layer that data is divided into various segments. Every segment will contain source port no, destination port no and sequence no. **Flow control** - Transport layer controls the amount of data been transferred. **Error control** - Deals with lost or corrupted data, it adds checksum to every data segments to see whether the data received is good or not. In network layer, transmission of received data segments from one computer to another is located in different networks.Router lives in network layer. The main function of network layer is to provide the source and destination IP address to the data segments and form am IP packet,so that every data packet can reach it's correct destination. It also performs routing and load balancing. Data link layer adds the MAC addresses to the data packet.Physical layer receives the signal converts the signal into bits and pass it into data link layer as a frame.

37. **TCP/IP model** -> It is known as internet protocol suit.5 layers. Application, Transport, network, data link, physical layer.
38. **Application layer** -> This is the layer where the users interact with. It consist of application. eg - Whatsapp,Facebook,Browser etc. Application lie on devices.
39. **Client-Server Architecture** -> Client sends the request,Server sends the response. There are multiple servers in data centres. Collection of huge no of computers having static IP addresses, very good internet connection and high upload speed.
40. **Peer to Peer Architecture** -> Various application running on different computers,and these computers are interconnected to each other.There is no one dedicated server or data centre. Every computer can act as a client or a server. We can scale it very rapidly. It is kind of a decentralized network. Eg- Bit Torrent.
41. **Repeater** -> A repeater operates at the physical layer. When the signal becomes weak, they copy the signal bit by bit and regenerate it at the original strength. It is a 2 port device.
42. **Hub** -> Hub is a multi port repeater. There are 2 types of hub - active and passive hub.
43. **Bridge** -> Bridge operates at data link layer. A bridge is a repeater, with add on functionality of filtering content by reading the MAC addresses of source and destination.
44. **Switch** -> Switch is a data link layer device. Switch can perform error checking before forwarding data, that makes it very efficient as it does not forward packets that have errors and forward good packets to selectively ports only.
45. **Gateway** -> Gateway is a passage to connect two networks together that may work upon different networking models.
46. **Brouter** -> Combines the feature of both bridge and router. It can work at either data link layer or network layer.Working as a router, it is capable of routing packets across networks and working as bridge, it is capable of filtering local area network traffic.
47. **TCP/IP protocol** -> 1.) **HTTP** -> how the data is transferred over web browser.full form is hyper

text transfer protocol. 2.) **DHCP** -> DHCP stands for dynamic host control protocol.DHCP is used to assign the local IP addresses to the devices connected to the router. 3.) **SMTP** -> SMTP stands for simple mail transfer protocol. It is used while sending email. 4.) **POP3 and IMAC** -> These are used to receive emails. 5.) **SSH** - SSH stands for secure shell. It is a method for secure remote login from one computer to another. 6.) **Telnet** -> Telnet is an application protocol that helps users communicate with a remote system.SSH is more secured than telnet as it encrypts the data.

48. **Socket** -> Sockets allow communication between two different processes on the same or different machines.
49. **HTTP in detail** -> It is a client server protocol and it tells us how you request the data from server and how the server will send back the data to the client. Application layer protocol also requires transport layer protocol. HTTP uses TCP. It is stateless protocol.
50. **HTTP method** -> 1. **GET** -> Requesting some data from server 2. **POST** -> Client giving something to the server. example - username,password. 3. **PUT** -> Puts data at a specific location. 4. **DELETE** -> delete data from the server, you will send the delete request.
51. **Status Codes** -> 1. **200** -> Request was successful. 2. **404** -> Server cannot find the requested resource. 3. **400** -> Bad Request.400 Bad Request response status code indicates that the server cannot or will not process the request due to something that is perceived to be a client error 4. **500** -> Internal Server error. This error is usually returned by the server when no other error code is suitable. It is generic error response.
52. **Status codes** -> 1. **1xx range** -> informational category 2.**2xx range** -> success codes 3. **3xx range** -> Redirecting 4.**4xx range** -> client error 5..**5xx range** -> server error.
53. **Cookies** -> Cookie is a unique string. It is stored on the client browser. When we visit the website for the first time,cookie is set. And after that whenever you make a new request,in that request header,cookie will be sent.Then the server will know that the request is coming from the this specific person, the server will check the database and it will find the state for that.
54. **Third party cookies** -> A third-party cookie is placed on a website by someone other than the owner (a third party) and collects user data for the third party. For example, a user visits a website called news.com. Cookies placed on this domain by news.com are first-party cookies. A cookie placed by any other site, such as an advertiser or social media site, is a third-party cookie.
55. **How Email Works** -> Simple mail transfer protocol (SMTP) is used to send email to the other person. And POP3 to receive email. This is on the application layer protocol. Email uses TCP as a transport layer protocol. If a person is sending an email from yahoo.com to gmail.com account. How does is work? -> Firstly sender sends the email to sender's SMTP server.Senders SMTP sever then makes the connection with Receivers SMTP server.And then the email is transferred to the receiver SMTP server.When the receiver logs into the email client,it downloads the email from the server and it is visible to the receiver.
56. **nslookup -type=mx gmail.com** -> Name and IP address of SMTP server for gmail.
57. **POP** -> POP stands for post office protocol. It is used to receive emails. First the client connects to the pop server using TCP port 110. Then the client asks the pop server to give all the emails.Client authorizes the pop server and pop server transact the emails to client.

58. **IMAP** -> It is also used to get emails. It stands for internet message access protocol. It allows to view your emails on multiple devices.
59. **Domain Name System (DNS)** -> Domain names are mapped to IP addresses. When we type google.com http protocol will use DNS to find the IP address of google server. It is difficult to remember the IP address therefore we use domain name. DNS is a directory database of url and ip address. Directory is divided into various classes of domains. In mail.google.com mail is **sub-domain**,google is **second level domain**, .com is **top level domain**. There are multiple databases for these 3 categories. Top one is known as **Root DNS server**. They have top level domain. eg- .io , .org, .com. These themselves have commclassroom.org , google.com etc. These are second level domains. Top level domains are managed by ICANN.
60. **What happens when you hit url in browser** -> Person enters a url into the browser and hits enter. URL stands for universal resource locator.URL has 4 components. eg- http://example.com/product/electric/phone. http is a scheme. It tells the browser to connect to the server using http protocol. Another one is https which means that connection is encrypted. example.com is a domain name of the site. product/electric is a path. /phone is a resource. Browser needs to know how to reach to the server, in this case example.com. This is done with a process called as DNS lookup. It is kind of phone book to the internet. DNS translates domain name to ip addresses so browser can know the resources. To make lookup process fast DNS info is heavily cached. First the Browser looks up IP in cache. If it is not in the browser cache the browser asks the OS for it. OS also has it's own cache which it keeps for certain period of time. If the OS doesn't have the IP, it makes the query out to the internet to the DNS resolver. It makes a chain of request until the IP address is resolved. Now finally the browser has the IP address of the server, in our case example.com. Then the browser establishes a TCP connection with the server using the IP address it got for it. Now the browser sends an HTTP request to the server over the established TCP connection. The server process the request and sends back a response. The browser receives the response and renders the content.
61. **dig google.com** -> to check messages received by the DNS server. It is a DNS lookup utility.
62. **Transport Layer** -> Role of transport layer is to take the information(message), from the network to the application and vice versa. If the data needs to transferred from one network to another it is done by network layer. Suppose you are sending message,files and video call simultaneously to your friend. Transport layer has a multiplexer which receives all the 3 items.(message,file and video call). This will pass it to the demultiplexer and demultiplexer will send it to your friend application. If the message application wants to send something to other application it will give it to sockets. These sockets have port numbers. Data travels in packets. Transport layer will attach these socket port numbers. Therefore it knows from which application the data is coming and to which application data needs to send. Transport layer also takes care of congestion control. While sending the data, data might be corrupted or lost. To deal with this transport layer has something called as checksums.
63. **Checksum** -> When you are sending some data to your friend. Using this data a particular string value is calculated using some algorithm.Then that data and value is send to your friend. The receiver side will also calculate a checksum and generate a random string value based on the data received.Then both the string value are matched. If both are same then data received is

correct and complete.If not then something is wrong.

64. **Timers** -> Suppose you are sending data packets to the friend. When you send a particular data packet a timer starts. When receiver sends a confirmation that packet is received the timer stops.Suppose you send a packet number 2 and the timer starts.But the receiver didn't received the data then the timer expires. Then you know that packet 2 was not send.There can be another case where you are sending data packet 2 and the timer starts. Friend receives the data packet 2 but while sending back the response it didn't reach the sender and the timer expires. Now the sender will think that data packet 2 was not send successfully and it will resend it. Now the person has 2 duplicate packets. This problem is solved using sequence number.
65. **User datagram protocol(UDP)** -> It is a transport layer protocol. But here your data may or may not be delivered fully. Data may change. Data may not be in order. It is a connection less protocol. UDP uses checksum. It will tell whether data is corrupted or not but UDP will not do anything. UDP packet will consist of Data,Source port no,Destination port no,Length of datagram and checksum. UDP is faster.
66. **Use cases of UDP** -> 1. It is very fast 2. Video Conferencing app. 3. DNS uses UDP 4. Gaming
67. Transmission Control Protocol(TCP) -> It is a transport layer protocol. Application layer sends lot of raw data and TCP segments the data (divide in chunks). It provides congestion control. Takes care of when data does not arrive and maintains the order of data using sequence number.
68. **Features of TCP** -> 1.Connection oriented 2.Error control 3.Congestion control 4.Bidirectional(full duplex) 5. One tcp connection only between two computer.
69. **3 way handshake** -> **Step 1 (SYN):** In the first step, the client wants to establish a connection with a server, so it sends a segment with SYN(Synchronize Sequence Number) which informs the server that the client is likely to start communication and with what sequence number it starts segments with. **Step 2 (SYN + ACK):** Server responds to the client request with SYN-ACK signal bits set. Acknowledgement(ACK) signifies the response of the segment it received and SYN signifies with what sequence number it is likely to start the segments with. **Step 3 (ACK):** In the final part client acknowledges the response of the server and they both establish a reliable connection with which they will start the actual data transfer.
70. **Network Layer** -> Here we work with routers. There can be many routers between source and destination connected to each other. Every router has its own network address. Whenever the data packet reaches the router it checks in the forwarding table where to route the data packet. This is known as hop-by-hop forwarding where the data packet is transferred to many routers until it reaches its destination. In 192.168.2.30 , 192.168.2 is a network address and .30 is a device address.
71. **Control Plane** -> Control plane is used to build these routing tables.Every router is a node in a graph and connection between the router is the edges.There are two types of routing used to create tables. First is static routing in which addresses are added manually. It is not adaptive. Second is dynamic routing. In this if there is change in network it will evolve accordingly. Algorithms used to create these are bellman-ford, Dijkstra etc.
72. **Internet Protocol(IP)** -> Internet Protocol is network layer protocol. IP address is used to uniquely identify a device from one another. IPv4 is a 32 bit,4 words.IPv6 is 128 bit numbers.Every number in a IP address is of 8 bit.There are 4 number so 8*4=32 bit. **Subnet** -> A

subnetwork or subnet is a logical subdivision of an IP network. The practice of dividing a network into two or more networks is called subnetting. Computers that belong to the same subnet are addressed with an identical most-significant bit-group in their IP addresses. In 192.168.2.30 , 198.168.2 is a subnet id and .30 is a host id. This increases the routing efficiency.

73. **Packets** -> Header is of 20 bytes. It contains ip version,length,identification number,flags,protocols,checksum,addresses, TTL etc. TTL stands for time to live. Time to live (TTL) refers to the amount of time or “hops” that a packet is set to exist inside a network before being discarded by a router.
74. **IPv4 vs IPv6** -> IPv4 is 32 bit. 2^32 unique ip address can be created. Ipv6 is 4 times larger than IPv4. 2^128 unique ip address can be created. But it is not backward compatible.
75. **Middle Boxes** -> Extra devices which also interact with ip packet.Found in network or transport layer. Firewall is a middle box. 1. **Firewall** -> There are two types of firewall,one connected to the global internet and other to your trusted network. Firewall filters out the IP packets based on various roles. eg -based on ip address,modify packet, based on port nos,set flags,protocols etc. There are two types of firewall, Stateless and Statefull firewalls. Stateless packet do not maintain the state and stateful packet maintains the state, it stores in cache memory. It is more efficient.
76. **Network Address Translation(NAT)** -> It is also a middle box. The idea of NAT is to allow multiple devices to access the Internet through a single public address. To achieve this, the translation of a private IP address to a public IP address is required. Your laptop private ip address is replaced by the ip of the router while accessing something from internet. Example -> When a device from a LAN request the facebook page, suppose our laptop ip address is (10.5.1.2) wants to access the fb page. Then that request first reaches our router. The router changes the source of IP address, here (10.5.1.2) to its own IP say (56.1.5.4) and sends that request to the fb server. fb server sends back response back to the router (56.1.5.4) and router sends it back to our private laptop which requested the fb page(10.5.1.2) . Through NAT, devices within LAN are secured and protected.
77. **Data Link Layer** -> Data link layer is responsible for sending the packet from network layer to Physical layer. Whenever a new device is added to the router,new device is connected to the DHCP server. DHCP server will allocate a new IP address to the new device. Data link layer communicate with each other using Data link layer address. Data link layer transfers in frame. Frame contains data link layer address of sender, and IP address of destination. Data link layer works closely with physical layer.

Created By -

Yash Patil.