Network: It refers to a collection of interconnected devices that can communicate and share resources with each other.

The first network ARPANET is made.

Internet: The internet is a global network of networks. It's a massive interconnected system of various networks worldwide that enables communication and resource sharing on a global scale.

Internet uses a packet switching technique to transmit the data. Thus, the data to be sent is divided into packets and the data is sent in the form of packets only. Each packet of data contains various information like the address of the destination, error control information, etc. Internet majorly uses protocols called Internet Protocol also simply called protocol (IP) and Transmission Control Protocol (TCP) to transmit data from one computer to another.

Protocol: a set of rules and conventions that govern how data is exchanged between devices or systems in a network or communication environment.

TCP - data is not corrupted and 100% data has reached the destination.

UDP - some data may be lost. video call.

HTTP - used by web browsers. format of data transfered in the servers contains all the rules.

Also, there are several other protocols that are used by the internet for different purposes. For example, it uses Simple Mail Transfer Protocol (SMTP) to send mail from one client to another, it uses File Transfer Protocol (FTP) to transfer files over the internet, it uses Hypertext Transfer Protocol (HTTP) through which a browser (client) can interact with the internet server.

To know the IP address of the internet provider - $ curl if config.me -s. some of the ports are reserved. 0 - 1023 are reserved.

> IP address is used to identify the device and port is used to identify to identify application.

> 1mbps = 1000000 bits/second.

WWW - world wide web (Tim Berners Lee).

What happens when we surf the Internet?

1. Extracting IP address of a URL (Uniform Resource Locator) In our browser, we enter the URL (Uniform Resource Locator) address of the website we want to visit. Once we enter the URL address of the website, the browser with the help of the DNS (Domain Name System) extracts the

IP address corresponding to the URL address that is entered. The DNS (Domain Name System) contains the mapping of the URLs along with their corresponding IP addresses.

2. Sending request to the server to access the webpage and receiving response Once we get the IP address of the website we want to access using DNS, the browser sends an HTTP (Hypertext Transfer Protocol) request to the server to extract the HTM (Hypertext Markup Language)L webpage corresponding to the IP address. This request is sent over PORT 80 using TCP (Transmission Control Protocol). Once the server receives this HTTP request, it responds back with an HTTP response. This HTTP response consists of the information related to the HTML page corresponding to the IP address of the website.
3. Receiving HTTP response and displaying the webpage The browser receives the HTML (Hypertext Markup Language) information for the website along with the response and hence, it processes and displays the HTML page on the browser. Finally, the users can see an HTML page for the URL that they entered.

What is Circuit Switching?
In circuit switching, a dedicated communication channel is set up between the sender and the receiver. Due to the dedicated circuit, there is extremely little chance of data loss or error but a lot of bandwidth is lost because other senders cannot utilize the same channel when a transmission is going on.
example - Traditional Telephone calls, Emergency services.

What is packet swithching?
In packet switching, the message is first divided into data packets and then transmitted individually over the network, and each packet can take a different route to reach its destination. It is connectionless, as it doesn't require a dedicated communication channel. These data packets are then grouped at the receiver's end to obtain the actual data or message.
example - Internet Browsing, streaming communication, email communication.

NIC (Network Interface Card) : A NIC is a hardware component that allows a computer or other device to physically connect to a network and communicate with other devices over that network.

Hub: A hub is a basic networking device that operates at the physical layer of the OSI model. It simply receives data packets from one device and broadcasts them to all other devices connected to the hub. Flooding is a simple computer network routing technique in which a source or node sends packets through every outgoing link. The flooding algorithm is easy to implement. The hubs use the flooding algorithm to forward data.

Switch: A switch is a more advanced networking device that operates at the data link layer of the OSI model. Unlike hubs, switches are intelligent and can learn the MAC addresses of devices connected to them. They use this information to forward data only to the specific device for which the data is intended. This significantly reduces unnecessary network traffic and improves overall network

performance. When a data frame arrives at any network switch port, it evaluates the destination address(destination MAC address), performs the necessary checks, and sends the frame to the associated device.

Router: A router is a networking device that operates at the network layer (Layer 3) of the OSI (Open Systems Interconnection) model. Its primary function is to route data packets between different networks. Routers make decisions based on IP addresses and are responsible for determining the best path for data to travel from the source to the destination across multiple networks.

Bridge : A bridge is a device or software component that operates at the data link layer (Layer 2) of the OSI model. Its primary function is to connect and filter traffic between two or more network segments, making them function as a single network.

bridge vs gateway?

modem : A modem is a network device that modulates and demodulates analog carrier signals (known as sine waves) to encode and decode digital data for processing. Because modems perform both of these tasks simultaneously, the term modem is a combination of "modulate" and "demodulate".

Repeater : A repeater is a two-port device that operates at the physical layer . It is used to regenerate the signal over the same network before it becomes too weak or corrupted, allowing the signal to be transmitted for a longer distance over the same network. It is important to understand that repeaters do not amplify the signal. When the signal weakens, repeaters copy it bit by bit and regenerate it at its original strength.

modem vs router?
Hub vs Switch?
Bridge vs Repeater?

Types of Network:
LAN: Local Area Network - offices, buildings.
WAN: Wide Area Network - across the countries.
MAN: Metropoliton Area Network - across the cities.
PAN: Personal Area Network - personal bluetooth, hotstop.

Network Topology - It defines the structure of the network of how all the components are interconnected to each other. There are two types of topology: physical and logical topology.
Physical topology is the geometric representation of all the nodes in a network.
Bus Topology - designed in such a way that all the stations are connected through a single cable known as a backbone cable. only one person can send data at one time.
Ring Topology - like a bus topology, but with connected ends.The data in a ring topology flow in a

clockwise direction.
Tree Topology - a type of structure in which all the computers are connected with each other in hierarchical fashion.There is only one path exists between two nodes for the data transmission. Thus, it forms a parent-child hierarchy. it can also be said as combination of many star topology.
Star Topology - an arrangement of the network in which every node is connected to the central hub, switch or a central computer.
if central device fails sysytem won't work.
Mesh Topology - an arrangement of the network in which computers are interconnected with each other through various redundant connections.
Full Mesh Topology: In a full mesh topology, each computer is connected to all the computers available in the network.
Partial Mesh Topology: In a partial mesh topology, not all but certain computers are connected to those computers with which they communicate frequently.
Hybrid Topology - The combination of various different topologies.

Transmission modes
The way in which data is transmitted from one device to another device is known as transmission mode.
Simplex Mode: the communication is unidirectional, i.e., the data flow in one direction. A device can only send the data but cannot receive it or it can receive the data but cannot send the data. e.g - keyword, monitor, Radio, TV
Half-Duplex Mode: Messages flow in both the directions, but not at the same time. e.g - walkies talkies, Railway Track
Full-duplex mode: The communication is bi-directional, i.e., the data flow in both the directions. Both the stations can send and receive the message simultaneously. e.g - Telephone Network.

OSI Model:
OSI stands for Open System Interconnection is a reference model that describes how information from a software application in one computer moves through a physical medium to the software application in another computer.
OSI consists of seven layers, and each layer performs a particular network function.

Physical, data link, network layer - Responsibilty of the network also called lower layer.
Transport, Session, Presentation, Application - Resposibility of the host also called upper layer.
Transport Layer is heart of OSI model.
physical, data link, network layer - Hardware Layers.
Application, Presentation, Session layer - software layers.

benefits of osi model:
The change in one layer does not affect the other layers.
The layered architecture reduces the complexity by dividing the task in a manageable way.
The layered architecture provides abstraction from other layers.
Each layer can be changed, tested, and analyzed independently.

Physical Layer: Lowermost Layer of the OSI Model.
This layer deals with the physical transmission of data over the network medium.
Functions:
Defines the hardware characteristics of the network, including cables, connectors, voltage levels, and transmission speeds.
Converts digital data into signals suitable for transmission.
It deals with the type of network topology.
It also deals with the type of transmission - simplex, half-duplex, full-duplex.
Bits synchronization :
Example: Ethernet cables, fiber optics, wireless radio waves.
The various protocols used in the physical layer are :
Digital Subscriber Line.
Integrated Services Digital Network.
Ethernet, etc.
The various devices used in the physical layer are :
Network adapters,
Hubs,
Cables,
Repeaters,
Modem, etc.

point to point configuration : It provides a dedicated linking or the cabling between two devices. The entire capacity of the link is reserved for the data transmission between those two devices. It is the simplest and the most efficient point of connection topology between the devices.

Network devices are physical devices that enable communication and interaction between hardware on a computer network. e.g - hub, bridge, repeater, modem, router, gateway, etc.

Reasons to Have Both IP and MAC Addresses:
Every MAC address assigned to the NIC of a physical device that aids in network device identification is the solution to this question.
On the internet, a response is sent to our IP address when we ask for a page to load.
The internet protocol suite has different layers on which MAC and IP addresses work. The layer 2

MAC address identifies the devices connected to the same broadcast network (such as the router). On the other hand, layer 3 uses IP addresses to aid distinguish between devices on various networks. The MAC address is still required to locate the devices on the same network even when we have the IP address to identify the device over other networks.
IP addresses manage the logical routable connection from computer to computer AND network to network while MAC addresses manage the actual connection between computers.

Bandwidth : Bandwidth in computer networks refers to the maximum data transfer rate or capacity of a network channel or communication link. It represents the amount of data that can be transmitted in a given time frame.

Data Link Layer:
This layer focuses on creating a reliable link between two directly connected nodes and managing data frames.
Functions:
Framing : It is the technique in which the data is divided into streams of bits (called frames) received from the network layer. Along with the conversion of data into frames, the data link layer adds a header and trailer to the frames. The header (present at the starting of the frame) contains the hardware's physical address of source and destination. The trailer (present at the end of the frame) contains the error detection and correction bits.
Physical addressing: Adds MAC addresses to frames for addressing.
Flow control: Ensures data flows at a rate both sender and receiver can handle.
Error detection and correction: Detects and handles errors in transmitted data.
Example: Ethernet frames, Wi-Fi frames.
The various protocols used in this layer are :
PPP (Point-to-Point Protocol),
Frame Relay,
ATM (The asynchronous transfer mode protocol), etc.
The various devices used in this layer are :
Bridges,
Switches,
NIC cards (Network Interface Cards), etc.
Ethernet?

What is Flow Control in Data Link Layer ?
Flow control is a set of procedures that restrict the amount of data a sender should send before it waits for some acknowledgment from the receiver.
Methods of Flow Control are Stop-and-wait and Sliding window.
Buffers are blocks in the memory that store data until it is processed. If the buffer is overloaded and

there is more incoming data, then the receiver will start losing frames.Thus, flow control is the method of controlling the rate of transmission of data to a value that the receiver can handle.

ACK (Acknowledgment): This bit is set to indicate that the receiver has successfully received the data or frame. It serves as a positive acknowledgment to the sender, indicating that the data was received without errors.
NACK (Negative Acknowledgment): In some protocols, a NACK bit is used to indicate that the receiver encountered errors or issues while trying to receive the data. A NACK is a negative acknowledgment, indicating that the data transmission was not successful.

Stop-and-wait Protocol
Stop-and-wait protocol works under the assumption that the communication channel is noiseless and transmissions are error-free.
Working :
The sender sends data to the receiver.
The sender stops and waits for the acknowledgment.
The receiver receives the data and processes it.
The receiver sends an acknowledgment for the above data to the sender.
The sender sends data to the receiver after receiving the acknowledgment of previously sent data.
The process is unidirectional and continues until the sender sends the End of Transmission (EoT) frame.
It is secure.
Problems Occur Due to Lost Data - Infinite waiting time.
Problems Occur Due to Lost Acknowledgment

Stop-and-Wait ARQ (Automatic Repeat Request)
Initially, the sender sends one frame as the window size is 1. The receiver on the other end receives the frame and sends the ACK for the correctly received frame. The sender waits for the ACK until the timer expires. If the sender does not receive the ACK within the timer limit, it re-transmits the frame for which the ACK has not been received.
Problem of Lost Data Packet
Problem of Lost/ Delayed Acknowledgement - To overcome this type of problem, the sender uses sequence numbering. When the sender sends the data packet, it attaches a certain sequence number which helps the receiver identify the data packet. If the timer goes off before receiving the acknowledgment from the receiver, the sender retransmits the same data packet. But in this case, the receiver already has the data packet, so it discards the data and sends it back an acknowledgment.
Problem of Damaged Packet
The window size of the sender and the receiver is only 1. So, only one frame can be sent at a time.

There is no negative acknowledgment for the lost or damaged frames. So, there is no NACK (negative acknowledgment) in case of stop and wait ARQ.

Go-Back-N ARQ Protocol

Go Back N ARQ is a sliding window protocol which is used for flow control purposes. Multiple frames present in a single window are sent together from sender to receiver.

Pipelining is allowed in the Go Back N ARQ protocol. Pipelining means sending a frame before receiving the acknowledgment for the previously sent frame.

The size of the sender window in Go Back N ARQ is equal to N.

The size of the receiver window in Go Back N ARQ is equal to 1.

When the acknowledgment for one frame is not received by the sender or the frames received by the receiver are out of order, then the whole window starting from the corrupted frame is retransmitted.

Retransmission of all the frames on detecting a corrupted frame increases channel congestion and also increases the bandwidth requirement.

Selective Repreat ARQ

In selective repeat ARQ, the sender sets a timer for each frame so whenever the timer is over and the sender has not received any acknowledgment for the frame or receiver sends NACK, then the sender knows that the particular frame is either lost or damaged. So, the sender sends back the lost or damaged frame once the timer is out. The ACK and the NACK have the sequence number of the frame that helps the sender to identify the lost frame.

As the receiver may receive the frames in a different order, the receiver has the capability of sorting the frames present in the memory buffer using the sequence numbers. On the other hand, the sender must be capable enough to search for the lost frame for which the NACK has been received. So searching at the sender's end and sorting at the receiver's are two minor drawbacks of the selective repeat ARQ.

Error Detection Techniques

Three methods are used to detect an error in frames: Parity check, Checksum, and Cyclic Redundancy Check (CRC).

1. Parity Check The parity check is performed by adding an extra bit to the data known as the parity bit, which results in a number of 1s that are either even in the case of even parity or odd in the case of odd parity. The parity check is only useful for detecting single-bit errors.
   The sender counts the amount of 1s in the frame and adds the parity bit in the following manner:
   Even parity: If the number of 1s is even, the parity bit value will be 0. The parity bit value will be 1 if the number of 1s is odd.
   Odd parity: If the number of 1s is odd, the parity bit value will be 0. The parity bit value will be 1 if the number of 1s is even.

2. Cyclic Redundancy Check(CRC) : In the sender part, we have appended n bits (all zeroes) to the data part, and then we divide the total data part (data + appended bits) with the divisor (generated from the generator polynomial). Now we get n CRC bits as the remainder. We append the CRC bits to the data part and send it to the receiver.
   On the receiver side, we divide the received data with the same divisor. If the receiver gets the remainder value as 0, then the received data is totally correct, or else the received data has some error.
3. CheckSum : The sender divides data into blocks of equal size and then adds the data of every block using 1’s complement arithmetic to get the sum. It then complements the sum to get the Checksum and sends it along with the data frames.
   The receiver receives data + Checksum and passes it to the checksum validator.
   Then do the same process as it is done at the sender's end. If we got a result that contains only 0, then ACCEPT the data, otherwise, REJECT the data.

IEEE - It stands for the Institute of Electrical and Electronics Engineers. IEEE is a professional association that develops and publishes technical standards for various fields, including computer networking.
Compatibility: Standards ensure that devices and technologies developed by various vendors are compatible with each other. This allows organizations to build heterogeneous networks composed of components from different manufacturers.
Innovation: IEEE standards are regularly updated and improved to accommodate technological advancements and innovations. This encourages the development of new networking technologies and features while maintaining compatibility with existing infrastructure.
Global Adoption: IEEE standards are internationally recognized and adopted, making them a basis for networking technologies used worldwide. This global acceptance helps in achieving uniformity in network communication.

Network Layer:
There are two primary purposes of the network layer.
The first one is to divide segments into network packets and then reassemble them on the receiving end.
Another is to route packets across a physical network by determining the optimum path.
Logical addressing: Assigns IP addresses to devices for identification.
Routing: Determines the best path for data packets to travel between networks.
Subnetting: Divides networks into smaller segments for efficient routing.
Example: IP (Internet Protocol), routers.
The various protocols used in this layer are :
IPv4 (Internet Protocol version 4),
IPv6 (Internet Protocol version 6),

ICMP (Internet Control Message Protocol),
IPSEC (IP Security),
ARP (Address Resolution Protocol),
MPLS (Multiprotocol Label Switching), etc.
The various devices used in this layer are :
Routers,
Brouters, etc.

Functions of Network Layer
The network provides the following functionalities.
Host-to-Host data delivery
Network layer is responsible for delivering data packets from source to destination. This layer provides the service that ensures the packet will reach its intended destination.
Logical Addressing
The network layer defines an addressing scheme to uniquely identify each device on the network. The network layer places the IP addresses of the sender and receiver in the header. Such an address distinguishes each device uniquely and universally. The header contains the network ID and the host ID of the network, which describes which device of the given network is the receiver.
Routing and Forwarding
Routing decides which route from source to destination is most appropriate. It chooses the shortest root between sender and receiver to forward data packets. Some widely used routing protocols are distance vector routing, link-state routing, and path vector.
Fragmentation
The network layer fragments the extensive data in fragments to forward from source to destination. It is done because each receiving node has some fixed capacity to accept data.
Congestion Control
When the data packets are flooded into the network in tremendous amounts, and the router is unable to route them properly, it causes aggregation of data packets into the network, which is referred to as congestion. The network layer is also responsible for controlling the congestion in the network and manipulating the flow of the network.
In-Order packets:- This service guarantees that the packets arrive at their destination in the same sequence as they were sent.

The various network layer protocols are

ARP
Address resolution protocol converts a logical address(IP address) to a physical address(MAC address). If a host on its network wants to know the physical address of another host on the network, it sends an ARP query packet with the IP address and MAC address of the source host and IP address

of the destination host and broadcasts it over the network. The ARP packet is received and processed by every host on the network, but only the intended recipient recognizes its own IP address in the request address and responds with the physical address.

ICMP

It relays messages from the receiver to the sender about the data that was supposed to arrive. ICMP protocol notifies the sender if the data is not received by the receiver or received in the wrong order. Thus, ICMP is a protocol for communicating information about data, but it does not manage the data itself.

ICMP stands for Internet Control Message Protocol. It is a network diagnostic and error reporting protocol. ICMP is a protocol that is part of the IP protocol suite that employs IP as a carrier protocol because the ICMP packet is enclosed in an IP packet after it is constructed.

Any network feedback is returned to the original host. If an error occurs on the network, it is reported using ICMP. There are dozens of diagnostic and error-reporting messages in the ICMP protocol. An IP datagram comprises the source and destination addresses, but it does not know the address of the last router it travelled through. As a result, ICMP can only deliver messages to the source, not to the routers in the immediate vicinity.

https://www.scaler.com/topics/computer-network/internet-control-message-protocol-icmp/

IPv4

https://www.scaler.com/topics/computer-network/ipv4-address/

Internet Protocol Version 4 is a network layer protocol that addresses and controls information and is used to transport packets in a network. To transport data packets across a network, IP and TCP work together. Each host is given a 32-bit IP address consisting of the network and host ID. The host number identifies a host on the network, assigned by a network administrator, whereas the network number identifies a network and is assigned by the internet. The IP is only responsible for delivering the packets, and TCP(a transport layer protocol) helps put them back in the correct order.

Types of IPv4 - classful and classless.

IPv6

https://www.scaler.com/topics/computer-network/ipv6-address/

Internet Protocol Version 6 is the latest version of the Internet Protocol. It is a network layer protocol containing addressing and control information for packet routing. IPv6 was established to address the exhaustion of IPv4. To accommodate more levels of addressing, it raises the IP address size from 32 bits to 128 bits.

IPv4 vs IPv6

https://www.scaler.com/topics/computer-network/ipv4-vs-ipv6/

IGMP

It stands for Internet group message protocol. IGMP is a multicasting communication protocol that uses resources efficiently to broadcast message/data packets. Hosts and nearby routers use it for multicasting communication with IP networks. IGMP can be utilized in streaming media, games, or web conferencing tools since multicast communication can have multiple senders and receivers.

Introduction to Port

https://scaler.com/topics/images/different-port-numbers.webp

The Internet Assigned Numbers Authority (IANA) is an organization that maintains the list of all port numbers.

In a computer network, a Port is a logical address which is assigned to each application on the computer that utilizes the internet for communication.

Port is an address of a 16-bit unsigned integer number which ranges from 0 to 65535.

The primary application of a port number is to transmit the data between a Computer Network and an Application.

Port is just a unique number assigned to every application of a computer.

However, the operating system can automatically assign a port number to the application running on the computer.

Port allows the computer to differentiate between all coming traffic such as email going to different ports and web pages going to different ports.

After seeing what is the port number now let us see different ranges of port numbers.

The ports 0 to 1023 are called well-known ports or system ports, these ports are especially associated with particular services.

The ports from 1024 to 49151 are called registered ports and this range port can be registered with the Internet Assigned Numbers Authority for a specific use.

The ports from 49152 to 65535 are unassigned ports, called dynamic or ephemeral ports and can be utilized for any type of service.

Subnetting :

https://www.scaler.com/topics/computer-network/subnetting/

Public and Private IP Address :

https://www.scaler.com/topics/computer-network/public-and-private-ip-address/

Network Address Translation (NAT) :

https://www.scaler.com/topics/computer-network/nat/

Quality Of Services :

https://www.scaler.com/topics/computer-network/qos/

> Routing can be static or dynamic or default.

Routing Protocol :
The Routing protocol is used to determine the path between one or more networks and store the information in the routing table.
The routing protocol is a process where the router connects with other routers in order to share information about the most cost-effective path and status of the network. The routing process selects the best path on the basis of the reachability information and stores it in a router table.

Routing Tables :
https://www.scaler.com/topics/computer-network/routing-table/

Intradomain and Interdomain Routing
https://scaler.com/topics/images/reference-link.webp

Intradomain Routing
Intradomain Routing is the routing protocol that operates only within a domain. In other words, intradomain routing protocols are used to route packets within a specific domain, such as within an institutional network for e-mail or web browsing. Unlike interdomain routing protocols, it doesn't communicate with other domains.

1. Distance Vector Routing : https://www.scaler.com/topics/computer-network/distance-vector-routing-algorithm/
2. Link State Routing : https://www.scaler.com/topics/computer-network/link-state-routing-algorithm/

Interdomain Routing
Interdomain Routing is the protocol in which the routing algorithm works both within and between domains. Domains must be connected in some way, for hosts inside one domain to exchange data with hosts in other domains. This connection within domains is governed by the interdomain routing protocols. This is often done using the Border Gateway Protocol (BGP). It is used in Path Vector Routing using which interdomain routing is performed. In path vector routing, the routing depends on the analysis of the path from the nodes in the current domain to the node in the other domain, and not on the distance between nodes.

1. Path Vector Routing : https://www.scaler.com/topics/computer-network/intradomain-and-interdomain-routing/

SDN?

Transport Layer:
This layer ensures end-to-end communication, reliability, and data integrity between devices on

different networks.
It is an end to end layer which is used to deliver message to a host.
It is responsible for the process to process delivery of data. The main aim of the transport layer is to maintain the order so that the data must be received in the same sequence as it was sent by the sender.
Functions:
The transport layer maintains the order of data.
It receives the data from the upper layer and converts it into smaller parts known as segments.
One of the major tasks of the transport layer is to add the port addressing (addition of a port number to the header of the data). The port number is added so that the data can be sent at the respective process only.
The transport layer on the receiver's end reassembles the segments to form the actual data.
Flow control: Manages data flow to prevent congestion.
Error detection and correction: Ensures data integrity.
Example: TCP (Transmission Control Protocol), UDP (User Datagram Protocol).
The various protocols used in this layer are :
TCP (Transmission Control Protocol),
UDP (User Datagram Protocol), etc.
The various devices used in this layer are :
Segments,
Load Balancers/Firewalls, etc.

what is present in the header?

Functions:

1. Process to Process Communication - It uses a port number to deliver the segmented data to the correct process amongst the multiple processes that are running on a particular host
2. Muliplexing and Demultiplexing
3. Flow Control
4. Data integrity
5. Congestion avoidance

Transmission Control Protocol:

What is a TCP 3-way Handshake?
The 3-Way handshake is a TCP/IP network connection mechanism that connects the server and client. Before the real data communication process begins, both the client and server must exchange synchronization and acknowledgment packets.

Working of TCP:
Step 1: Establishing the connection Whenever two computer systems want to exchange data using the transmission control protocol, they first establish a three-way handshake connection. The three-way handshake connection is used to create a connection between the host or client and the server. As the name suggests, it is a three-step process in which first the client (wants to establish a connection) sends an SYN segment (Synchronize Sequence Number segment) which tells the server that the client wants to start the communication. In the second step, the server responds with an SYN-ACK signal (SYN Acknowledgement). The SYN-ACK signifies the server has received the client's request of establishing the connection. In the third and the last step, the client again sends the ACK signal to the server and they both establish a reliable connection that will be used to transfer the data packets. The three-way handshake is also known as SYN-SYN-ACK. Refer to the diagram below for more clarity.
Step 2: Sending of data packets In the second step, the data packets along with the sequence number are sent from the first computer system (client). The second computer (server) responds to these sent packets by sending an acknowledgment or ACK. This acknowledgment bit keeps on increasing with the number of packets sent. This ACK bit helps to keep track of three things:
the successfully received packets,
the lost packets, and
the packets which were accidentally sent twice.
Step 3: Closing the connection As we have discussed that the client initiates the connection with the server by sending a SYN. But in case of closing the connection, either server or the client can close the connection. The first computer system (either server or the client) initiates the closing of the connection by sending a packet with a FIN bit or finish bit attached to it. The other computer sends back or responds with an ACK bit. Finally, the first computer sends an ACK bit back to the second computer and the connection gets closed.

Features of TCP:
Connection-oriented
Reliable
Flow Control
Error Control
Sequencing of packets
Congestion Control
Stream-oriented data transfer
Full duplex

TCP: https://scaler.com/topics/images/tcp-segment-format.webp
Source port address is a 16 bit field that defines port number of application program that is sending the segment.

Destination port address is a 16 bit field that defines port number of application program that is receiving the segment.
Sequence number is a field of 32 bit that will define the number assigned to data first byte contained in segment.
Acknowledgement number is a 32 bit field that describe the next byte that receiver is looking forward to receive next from sender.
Header Length (HLEN) is a field of 4 bit that specify the number of 4 byte words in TCP header. The header length of TCP header can be between 20 to 60 bytes.
Reserved is a field 6 bit that are reserved for future use.
Control bits are 6 different independent control bits or flags in this field.
There are six in control field:
URG: Urgent pointer
ACK: Acknowledgement number
PSH: Push request
RST: Reset connection
SYN: Sequence number Synchronization
FIN: Connection termination
Window Size is a 16-bit field that defines the size of the window of sending TCP in bytes.
Checksum, 16-bit field contains checksum and used for error detection.
Urgent pointer is a 16 bit field .This flag is set when there is urgent data in the data segment.
Options and padding can be upto 40 bytes field for optional information in TCP header.

User Datagram Protocol:
Features of UDP protocol
Transport layer protocol
User Datagram Protocol is a transport layer protocol.
UDP is considered as an unreliable and connection-less protocol
Connectioness
UDP protocol is a connectionless protocol, so it does not establish any virtual path before transmitting the data.
Since it is connectionless, so packets are sent from different paths between sender and receiver.
Ordered delivery of data is not guaranteed.
UDP does not guarantee the order of the datagram. A datagram can be received in any order
The UDP protocol utilizes different port numbers for transmitting data to the correct destination.
The port numbers are defined between 0 - 1023.
Faster transmission
UDP provides us a faster service of data transmission as there is no prior connection establishment before transmitting the data.

UDP does not require any virtual path for data transmission.
Acknowledgment mechanism
There is no acknowledgment mechanism provided by UDP as UDP protocol is a connection-less protocol, so there is no handshaking.
Segments are handled independently.
Every segment in UDP takes a different path to reach the destination. So, every UDP packet is handled independent of other UDP packets.
Stateless
UDP protocol is a stateless protocol which means that the sender does not wait for an acknowledgment after sending the packet.

UDP: https://scaler.com/topics/images/format-of-user-datagram.webp
UDP header + UDP data
User datagram have a fixed size header of 8 bytes which is divided into four parts -
Source port address: It defines source port number and it is of 16 bits.
Destination port address: It defines destination port number and it is of 16 bits.
Total length: This field is used to define the total length of the user datagram which is sum of header and data length in bytes. It is a 16-bit field.
Checksum: Checksum is also 16 bit field to carry the optional error detection data.

SCTP
SCTP stands for Stream Control Transmission Protocol.
SCTP is one of the connection oriented tranport layer protocols.
It allows transmitting of data between sender and receiver in full duplex mode.

TCP vs UDP : https://www.scaler.com/topics/computer-network/tcp-vs-udp/

The TCP protocol is a connection-oriented protocol, whereas the UDP protocol is a connectionless protocol.
TCP guarantees that a stream of bytes is sent in a reliable and orderly manner from the user to the server or vice versa. UDP isn't designed for end-to-end communication, and it doesn't confirm the receiver's readiness.
TCP's speed is slower, whereas UDP's speed is faster.
TCP performs error checking as well as error recovery, whereas UDP does error checking but discards erroneous packets.
TCP contains acknowledgment segments, whereas UDP does not have any.
TCP employs handshake protocols such as SYN, SYN-ACK, and ACK, but UDP employs no handshake protocols.
Overall, UDP is a much quicker, simpler, and more efficient protocol, nonetheless, only TCP allows for

the retransmission of lost data packets.
When comparing the TCP and UDP protocols, TCP is heavier while UDP is lighter.

TCP congestion :
Congestion is an important factor in packet switched network. It refers to the state of a network where the message traffic becomes so heavy that the network response time slows down leading to the failure of the packet. It leads to packet loss. Due to this, it is necessary to control the congestion in the network, however, it cannot be avoided.
When congestion takes place in the network, TCP handles it by reducing the size of the sender's window. The window size of the sender is determined by the following two factors:
Receiver window size - The sender should not send data greater than that of the size of receiver window.
Congestion window size - To calculate the size of the congestion window, different variants of TCP and methods are used.

Approaches for Congestion Control :
Congestion in TCP is handled by using these three phases:

1. Slow Start
2. Congestion Avoidance
3. Congestion Detection

// To study in detail...

How does Flow Control in TCP Work?
The sender writes the data to a socket and sends it to the transport layer which is TCP in this case. The transport layer will then wrap this data and will send it to the network layer which will route it to the receiving node.
The TCP stores the data that needs to be sent in the send buffer and the data to be received in the receive buffer. Flow control makes sure that no more packets are sent by the sender once the receiver's buffer is full as the messages will be dropped and the receiver won't be able to handle them. In order to control the amount of data sent by the TCP, the receiver will create a buffer which is also known as Receive Window.
In order to solve deadlock condition problem, whenever the TCP receives the zero window message, it starts a persist timer that will send small packets to the receiver periodically. This is also called WindowProbe.

Session Layer:
This layer manages the establishment, maintenance, and termination of communication sessions between two devices.

The session layer is responsible to create a dialog box which allows two systems to enter into a dialog and transmit the data in either half-duplex or full-duplex mode.
The session layer is also responsible t adding synchronization bits or checkpoints into the stream of data. These checkpoints help to detect any kind of error that may have occurred during the data transmission. So, if an error has occurred in between the transmission then the re-transmission will take place from the last checkpoint only.
Functions:
Session establishment, maintenance, and termination.
Synchronization of data exchange.
Example: NetBIOS, RPC (Remote Procedure Call).
The various protocols used in this layer are :
PAP (Password Authentication Protocol)
PPTP (Point-to-Point Tunneling Protocol)
RPC (Remote Procedure Call Protocol)
RTCP (Real-time Transport Control Protocol), etc.
The various devices used in this layer are :
Gateway, etc.

Presentation Layer:
This layer deals with data format conversion, encryption, and compression to ensure compatibility between different devices and systems. Since different computer systems use different encoding systems so the presentation layer must translate the data into a computer-dependent format.
Functions:
Data translation: Converts data between different formats.
Encryption and decryption: Secures data during transmission.
Data compression: Reduces the size of data for efficient transmission.
Example: SSL/TLS, JPEG, GIF.
The various protocols used in this layer are:
AFP (Apple Filing Protocol),
ICA (Independent Computing Architecture),
Citrix system core protocol,
LPP (Lightweight Presentation Protocol),
NCP (NetWare Core Protocol),
NDR (Network Data Representation),
Tox protocol, etc.

Application Layer:
This is the top layer that directly interacts with user applications and provides network services. Application layers allow users to access and share files, access and send emails, access webpages

(via the world wide web), etc.
Functions:
Application protocols: Support specific services for users and applications.
User interfaces and APIs: Provide interfaces for application communication.
Example: HTTP, FTP, SMTP, DNS.
The various protocols used in this layer are:
DNS (Domain Name System),
SMTP (Simple Mail Transfer Protocol),
FTP (File Transfer Protocol),
POP (Post Office Protocol),
HTTP (HyperText Transfer Protocol), etc.
The various devices used in this layer are:
PC's (Personal Computer),
Phones,
Servers,
Firewalls, etc.

Functions of the Application Layer
The application layer provides the following functions.
The Application Layer provides protocols that allow the software to communicate and receive data and finally present it to users in a meaningful way.
This layer allows users to log on as a remote host.
The Application Layer provides various facilities for users to forward multiple emails and a storage facility.
This layer acts as a window via which users and application processes can access network resources.
This layer provides services such as email, file transfer, results distribution, directory services, network resources, etc.
The application layer communicates with the operating system and guarantees that data is properly saved.
This layer allows users to interact with other software applications.
This application layer generally performs host initialization followed by remote login to hosts.

HTTP
Hypertext transfer protocol enables us to access data via the internet. It sends data in plain text, audio, and video formats. Client and servers exchange resources over the internet using the HTTP protocol. Client devices request servers for the resources required to load a web page, and the servers respond by sending responses to the client.
https://www.scaler.com/topics/computer-network/hypertext-transfer-protocol/

SMTP

The SMTP (Simple Mail Transfer Protocol) is the TCP/IP protocol that handles email. The data is sent to another email address using this protocol. SMTP uses a procedure known as "store and forward" to transmit user emails on and across networks. It works with the Mail Transfer Agent to ensure that your message is sent to the correct computer and email mailbox. The port number for SMTP is 25.
https://www.scaler.com/topics/computer-network/smtp-protocol/

DNS

DNS stand for (Domain Name System). Similar to how a phone's contacts list matches names to numbers, the domain name system is a naming database that locates and translates internet domain names to their unique IP addresses. DNS was created because it is more difficult for humans to recall numerical numbers than alphabetic names. DNS is used in a variety of internet activities to swiftly discover an IP address to connect to and access content.

DHCP

The Dynamic Host Configuration Protocol is a network management protocol that dynamically allocates a unique IP address to any device or node on a network so that they can communicate using IP. DHCP is used to automate and maintain these setups from a central location. There is no need to manually assign IP addresses to new devices. As a result, connecting to a DHCP-based network requires no user configuration.

FTP

The FTP (File Transfer Protocol) is a standard internet protocol for transferring data from one computer to another. FTP uses TCP to transmit data because TCP provides reliability and error-free data transmission. It facilitates file sharing via remote computer devices while ensuring dependable and efficient data delivery. For data control, FTP utilizes port 21, and for data access, it uses port 20.
https://www.scaler.com/topics/computer-network/file-transfer-protocol/

TFTP

The TFTP (Trivial File Transfer Protocol) is a simple file transfer protocol. The TFTP uses User Datagram Protocol (UDP) to transmit data from one end to the other. While transmitting files, TFTP does not provide any authentication or security. As a result, it's commonly used to transfer boot files or configuration information between workstations in a local setup.

NFS

It's known as a NFS (network file system). It enables remote computers to mount file systems over a network and interact with them as if they were mounted locally. System administrators can combine resources on the network's centralized servers as a result of this. Port number for the NFS is 2049.

TELNET
Telnet, short for "Telecommunication Network," is both a protocol and an application that allows users to establish a remote terminal session with another computer or device over a network, typically the internet. Telnet enables users to access the command-line interface (CLI) or shell of a remote system and interact with it as if they were physically present at that system

> A Client is a computer system that accesses the services provided by a server.

> A Server is a powerful centralized hub that stores various information and handles the requests of the client(s).

client to server architecture:
In the client-server network, the files are not stored on the hard drive of each computer system. Instead, the files are centrally stored and backed up on a specialized computer known as a server. Here, a server is designed to efficiently provide data to a remote client. On a large-scale network, there can be more than one server.
social media, streaming services, online shoping.

Peer to peer architecture:
Peer-to-peer has decentralized the simplest form of network architecture where every computer system (node) can communicate with every other computer system (node). There is no use of a centralized server as every computer system can communicate with every other computer system directly.
Every device can act as a Server as well as Client.
Some online gaming platforms also use the peer-to-peer network model.
The peer-to-peer network architecture is also used in the field of blockchain.

Domain Name System (DNS) :
It is a naming database that locates and translates internet domain names to their unique IP addresses.

1. Recursive DNS Service
   In this type, if the DNS resolver only communicates to the root servers and the remaining servers were communicated recursively by the root server. The root server sends the output (IP in this case) to the DNS resolver.
   https://scaler.com/topics/images/recursive-dns-service.webp
2. Iterative DNS Service
   In this type, the DNS resolver can directly communicate and receive input from the servers at different levels.
   https://scaler.com/topics/images/iterative-dns-service.webp

There are four types of DNS servers.
DNS Resolver
Root Name Server
Top-Level Domain Server
Authoritative name server

How does DNS work?
DNS is concerned with translating a domain name into an IP address.
If you type scaler.com into a web browser, the query is transmitted over the Internet and received by a DNS resolver.
The DNS resolver then queries a DNS root nameserver.
After then, the root server responds to the DNS resolver with the address of a TLD DNS server (such as .com or .net), which keeps the information for the resolver's domains. Our request for scaler.com is directed to the .com top-level domain (TLD).
The DNS resolver then requests the .com TLD after receiving the address of the TLD by the root server.
The IP address of the domain nameserver, scaler.com, is then returned by the TLD server.
Finally, the DNS resolver sends a query to the domain's nameserver.
The nameserver returns the IP address, for scaler.com, to the resolver.
The DNS resolver then returns the IP address of the domain that was requested originally to the web browser.
An HTTP request is sent to the IP address by the browser.
The server returns the webpage to be rendered in the browser at that IP.
Finally, after all the processes mentioned above, the user can now view the web page on their machine.

Domain Name System Security
Along with the various features and reliability the DNS provides, it also has some vulnerabilities. Two of the major vulnerabilities are

1. Cache Poisoning
   DNS cache poisoning is a misleading assault that diverts traffic away from authorized websites and puts users at risk of malware infestations and data theft. An attacker uses a web server and cache to serve a malicious Hypertext Transfer Protocol (HTTP) response to users in web cache poisoning. DNS resolvers cannot validate the data in their caches, which implies that inaccurate data will remain in the cache until the issue is manually fixed or TTL(time to live) expires.
2. Phishing
   It is done to get users’ data by creating a false website of a well-known website with an utterly

unauthorized backend. Phishing causes user privacy and financial status as it is intended to harm the end-user.

World Wide Web : The World Wide Web popularly known as WWW, W3, or the Web is an interconnected system of public webpages accessible through the Internet. The working of the World Wide Web is based on the client-server model. A web server is software and hardware that uses HTTP (Hypertext Transfer Protocol) and other protocols to respond to client requests made over the World Wide Web.
A web server is used to store data or information and this data is transferred to the computer of the user when a user on the same network requests data or information. The computer system of the user that is requesting this data is known as a client. This exchange of data is usually carried out by the browser present on our computer systems. It allows us to access the retrieved data in the form of documents from the web.

> TCP / IP model.
> Internet Protocol suite.
> Layers 5 - application, transport, network, datalink, physical.

repeater.
active and passive hub.
bridge.
transparent
source routing
switch.
router
gateway
Brouter

Physical Layer:
Multiplexing is a technique used to combine and send the multiple data streams over a single medium. The process of combining the data streams is known as multiplexing and hardware used for multiplexing is known as a multiplexer.

Multiplexing is achieved by using a device called Multiplexer (MUX) that combines n input lines to generate a single output line. Multiplexing follows many-to-one, i.e., n input lines and one output line.

More than one signal can be sent over a single medium.
The bandwidth of a medium can be utilized effectively.

Demultiplexing is achieved by using a device called Demultiplexer (DEMUX) available at the receiving end. DEMUX separates a signal into its component signals (one input and n outputs). Therefore, we can say that demultiplexing follows the one-to-many approach

protocols:
web protocols -
TCP / IP : HTTP, DHCP, FTP, SMTP, POP3 & IMAC, SSH, VNC
Telnet : port-23
UDP: stateless connection, data may be lost.
threads - a process can have multiple threads. thread can do only one operations at a time.
a process can have multiple threads.

sockets :

Ports : Port tells us which application should data be sent.
Ephemeral port : used to identify the threads.

HTTP - hyper text transfer protocol. application layer protocols. it has get, post requests. It uses TCP in tranport layer. It is a stateless protocols.

status codes:
100 - informational
200 - success status
300 - redirecting
400 - client error
500 - server error

cookies - unique string stored in the browser.
Third Party cookies - cookies which set for the url which was not visited.

SMTP - uses TCP.
if sender and receiver are not using the same email then
sender->Sender's SMTP server->Receiver's SMTP server->Receiver.
else direct sent.

we can receive the email using pop with the help of pop server.
using this it will be available only on that devices.

If done using IMAP it will be available on all the devices where that email has been logged.

DNS - Domain Name System. convert the url to ip address.
divided in different databases.

mail.google.com
mail - sub-domain, google - second-level domain, com - top-level domain.
root dns server: .io, .com, .org ans so on.
second level domain: google.com, student.io and so on.
first search in device then local dns server - isp(internet service provider) then root dns server.
domain name can not be bought. it can only be rented.

Transport Layer:
from the network to application and vice versa. It works within the device only.
TCP (Transmission Control Protocol): connection protocol. application layer send a lot of raw data, tcp divides it into segments and add headers and do check sums.
congestion control- takes care of when the data arrived and maintain the order of data.
features: connection oriented. error control, congestion control, full duplex.
one tcp connection is only between two devices.
Three-Way Handshakes. sequence no are random for the security purposes.
UDP(User Datagram Protocol): data may not get delivered, data may not be in order, may detoriate. It is connectionless protocol.
UDP Packets: source port no and destination port no, length of data, check sum, data.
data - non header. 2^16 - 8.
remianing - header 8 bytes
It is faster.video call, gaming.
Multiplexer:
Demultiplexer:
socket attaches the port no in this layer.
it controls the congestion which happens due to difference in flow speed at sender and receiver end.
congestion control algorithms:
check sum:
Timers:

Transport - segments.
Network - packets.
data link - frames.

Network Layer:
Routing Table is used to find the best route to reach the destination.
Control plan: It is used to create the routing table.
static routing.
dynamic routing.
IP (Internet Protocol):

IPV4 - 32 bits, 4 words.
IPV6 - 128 bits.
classes in IP addresses.
subnet:
Resevered address and loopback addresses.

> In general the first address is the network identification and the last one is the broadcast, they cannot be used as regular addresses.

packets : Header is of 20 bytes.

IPV4 vs IPV6

Middle Boxes:
firewall:
framing:
Error Detection:

VPN?