Computer Networks Viva Questions and Answers

What is data communication system

Data Communication is **a process of exchanging data or information**. **In case of computer networks** this exchange is done between two devices over a transmission medium

What is Network Topology?

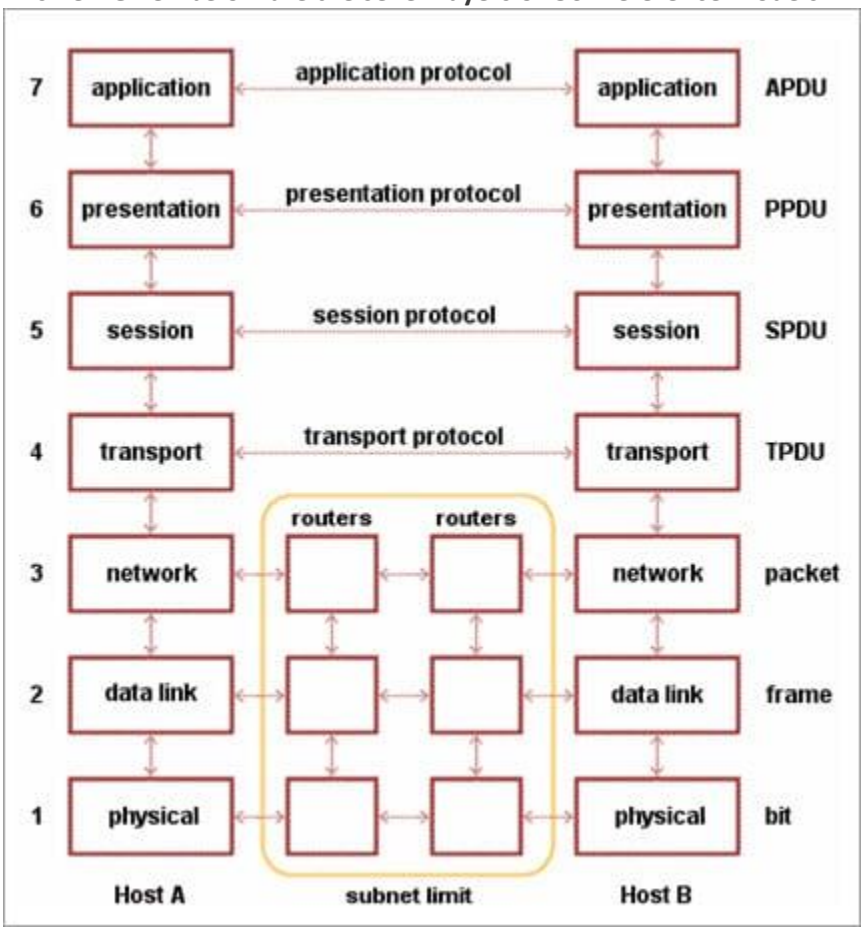
Answer: Network topology is a physical layout of the computer network and it defines how the computers, devices, cables, etc are connected to each other.

What is the OSI reference model?

Answer: Open **S**ystem **I**nterconnection, the name itself suggests that it is a reference model that defines how applications can communicate with each other over a networking system.

What are the layers in OSI Reference Models? Describe each layer briefly.

Answer: Given below are the seven layers of OSI Reference Models:



a) Physical Layer (Layer 1): It converts data bits into electrical impulses or radio signals. **Example:** Ethernet.

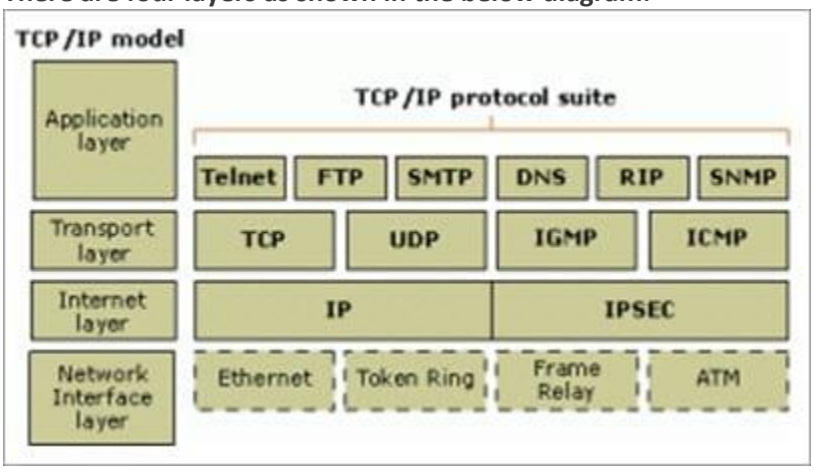
b) Data Link Layer (Layer 2): At the Data Link layer, data packets are encoded and decoded into bits and it provides a node to node data transfer. This layer also detects the errors that occurred at Layer 1.

c) Network Layer (Layer 3): This layer transfers variable length data sequence from one node to another node in the same network. This variable-length data sequence is also known as **"Datagrams"**.
d) Transport Layer (Layer 4): It transfers data between nodes and also provides acknowledgment of successful data transmission. It keeps track of transmission and sends the segments again if the transmission fails.
e) Session Layer (Layer 5): This layer manages and controls the connections between computers. It establishes, coordinates, exchange and terminates the connections between local and remote applications.
f) Presentation Layer (Layer 6): It is also called as "Syntax Layer". Layer 6 transforms the data into the form in which the application layer accepts.
g) Application Layer (Layer 7): This is the last layer of the OSI Reference Model and is the one that is close to the end-user. Both end-user and application layer interacts with the software application. This layer provides services for email, file transfer, etc.

Explain TCP/IP Model

Answer: The most widely used and available protocol is TCP/IP i.e. Transmission Control Protocol and Internet Protocol. TCP/IP specifies how data should be packaged, transmitted and routed in their end to end data communication.

There are four layers as shown in the below diagram:



Given below is a brief explanation of each layer:

- **Application Layer**: This is the top layer in the TCP/IP model. It includes processes that use the Transport Layer Protocol to transmit the data to their destination. There are different Application Layer Protocols such as HTTP, FTP, SMTP, SNMP protocols, etc.
- **Transport Layer**: It receives the data from the Application Layer which is above the Transport Layer. It acts as a backbone between the host's system connected with each other and it mainly concerns about the transmission of data. TCP and UDP are mainly used as Transport Layer protocols.
- **Network or Internet Layer**: This layer sends the packets across the network. Packets mainly contain source & destination IP addresses and actual data to be transmitted.
- **Network Interface Layer**: It is the lowest layer of the TCP/IP model. It transfers the packets between different hosts. It includes encapsulation of IP packets into frames, mapping IP addresses to physical hardware devices, etc.

What is HTTP and what port does it use?

Answer: HTTP is HyperText Transfer Protocol and it is responsible for web content. Many web pages are using HTTP to transmit the web content and allow the display and navigation of HyperText. It is the primary protocol and port used here is TCP port 80.

What is HTTPs and what port does it use?

Answer: HTTPs is a Secure HTTP. HTTPs is used for secure communication over a computer network. HTTPs provides authentication of websites that prevents unwanted attacks.

What are TCP and UDP?

Answer: Common factors in TCP and UDP are:

- TCP and UDP are the most widely used protocols that are built on the top of the IP protocol.
- Both protocols TCP and UDP are used to send bits of data over the Internet, which is also known as 'packets'.
- When packets are transferred using either TCP or UDP, it is sent to an IP address. These packets are traversed through routers to the destination.

The difference between TCP and UDP are enlisted in the below table:

TCP	UDP
TCP stands for Transmission Control Protocol	UDP is stands for User Datagram Protocol or Universal Datag Protocol
Once the connection is setup, data can be sent bi-directional i.e. TCP is a connection oriented protocol	UDP is connectionless, simple protocol. Using UDP, messages as packets
The speed of TCP is slower than UDP	UDP is faster compared to TCP
TCP is used for the application where time is not critical part of data transmission	UDP is suitable for the applications which require fast transm data and time is crucial in this case.
TCP transmission occurs in a sequential manner	UDP transmission also occurs in a sequential manner but it d maintain the same sequence when it reaches the destination
It is heavy weight connection	It is lightweight transport layer
TCP tracks the data sent to ensure no data loss during data transmission	UDP does not ensure whether receiver receives packets are r packets are misses then they are just lost

What is a Firewall?

Answer: Firewall is a network security system that is used to protect computer networks from unauthorized access. It prevents malicious access from outside to the computer network. A firewall can also be built to grant limited access to outside users.

What is DNS?

Answer: Domain Name Server (DNS), in a non-professional language and we can call it an Internet's phone book. All the public IP addresses and their hostnames are stored in the DNS and later it translates into a corresponding IP address.

What is meant by 127.0.0.1 and localhost?

Answer: IP address 127.0.0.1, is reserved for loopback or localhost connections.. To identify any connection issue, the initial step is to ping the server and check if it is responding.

What is NIC?

Answer: NIC stands for Network Interface Card. It is also known as Network Adapter or Ethernet Card. It is in the form of an add-in card and is installed on a computer so that the computer can be connected to a network.
Each NIC has a MAC address which helps in identifying the computer on a network.

What is the difference between the Internet, Intranet, and Extranet?

Answer: The terminologies Internet, Intranet, and Extranet are used to define how the applications in the network can be accessed. They use similar TCP/IP technology but differ in terms of access levels for each user inside the network and outside the network.

- **Internet**: Applications are accessed by anyone from any location using the web.
- **Intranet**: It allows limited access to users in the same organization.
- **Extranet**: External users are allowed or provided with access to use the network application of the organization.

What is a VPN?

- **Answer:** VPN is the Virtual Private Network and is built on the Internet as a private wide area network. Internet-based VPNs are less expensive and can be connected from anywhere in the world.

What are Ipconfig and Ifconfig?

Answer: Ipconfig stands for Internet Protocol Configuration and this command is used on Microsoft Windows to view and configure the network interface.

- **Ifconfig** (Interface Configuration) is a command that is used on Linux, Mac, and UNIX operating systems. It allows you to see the IP addresses of these network interfaces.

What is a subnet mask ?

A method of determining what network devices are local – if all the devices have the same subnet mask, usually 255.255.255.0 , then they are in the same collision domain

Explain DHCP briefly?

Answer: DHCP stands for Dynamic Host Configuration Protocol and it automatically assigns IP addresses to the network devices. It completely removes the process of manual allocation of IP addresses and reduces the errors caused due to this.

What are the different types of a network? Explain each briefly.

Answer: There are 4 major types of networks.
Let's take a look at each of them in detail.

1. **Personal Area Network (PAN)**: It is the smallest and basic network type that is often used at home. It is a connection between the computer and another device such as phone, printer, modem tablets, etc
2. **Local Area Network (LAN)**: LAN is used in small offices and Internet cafes to connect a small group of computers to each other. Usually, they are used to transfer a file or for playing the game in a network.
3. **Metropolitan Area Network (MAN):** It is a powerful network type than LAN. The area covered by MAN is a small town, city, etc. A huge server is used to cover such a large span of area for connection.
4. **Wide Area Network (WAN)**: It is more complex than LAN and covers a large span of the area typically a large physical distance. The Internet is the largest WAN which is spread

across the world. WAN is not owned by any single organization but it has distributed ownership.

Describe the layers of the OSI model?

Answer: OSI model stands for Open System Interconnection It is a framework that guides the applications on how they can communicate in a network.

OSI model has seven layers. They are listed below,

1. **Physical Layer**: Deals with transmission and reception of unstructured data through a physical medium.
2. **Data Link Layer:** Helps in transferring error-free data frames between nodes.
3. **Network Layer:** Decides the physical path that should be taken by the data as per the network conditions.
4. **Transport Layer:** Ensures that the messages are delivered in sequence and without any loss or duplication.
5. **Session Layer:** Helps in establishing a session between processes of different stations.
6. **Presentation Layer:** Formats the data as per the need and presents the same to the Application layer.
7. **Application Layer:** Serves as the mediator between Users and processes of applications.

Define various types of Internet connections?

Answer: There are three types of Internet connections. They are listed below:

1. **Broadband Connection:** This type of connection gives continuous high-speed Internet. In this type, if we log off from the Internet for any reason then there is no need to log in again. **For Example,** Modems of cables, Fibres, wireless connection, satellite connection, etc.
2. **Wi-Fi:** It is a wireless Internet connection between the devices. It uses radio waves to connect to the devices or gadgets.

A few important terminologies we come across networking concepts?

Answer: Below are a few important terms we need to know in networking:

- **Network:** A set of computers or devices connected together with a communication path to share data.
- **Networking:** The design and construction of a network are termed as networking.
- **Link:** The physical medium or the communication path through which the devices are connected in a network is called a Link.
- **Node:** The devices or the computers connected to the links are named as nodes.
- **Router/Gateway:** A device/computer/node that is connected to different networks is termed as a Gateway or Router. The basic difference between these two is that Gateway is used to control the traffic of two contradictory networks whereas the router controls the traffic of similar networks.
- **The router** is a switch that processes the signal/traffic using routing protocols.
- **Protocol:** A set of instructions or rules or guidelines that are used in establishing communications between computers of a network is called Protocol.
- **Unicasting:** When a piece of information or a packet is sent from a particular source to a specified destination then it is called Unicasting.
- **Anycasting:** Sending the datagrams from a source to the nearest device among the group of servers that provide the same service as the source is termed as Anycasting.
- **Multicasting:** Sending one copy of data from a single sender to multiple clients or receivers (selected clients) of the networks which are in need of such data.

- **Broadcasting:** Sending a packet to each device of the network is termed as broadcasting.

How many types of modes are used in data transferring through networks?

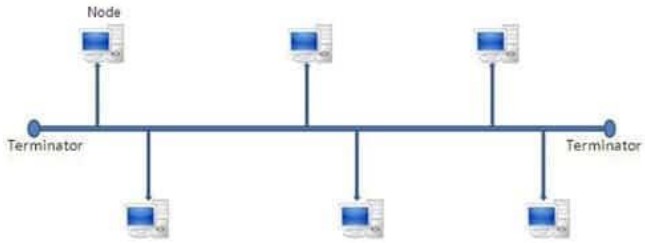
Answer: Data transferring modes in computer networks are of three types. They are listed below,

1. **Simplex:** Data transferring which takes place only in one direction is called Simplex.
2. **Half Duplex:** Data transferring can happen in both directions but not at the same time.
3. **Full Duplex:** Data transferring happens in both directions that too simultaneously. **For**

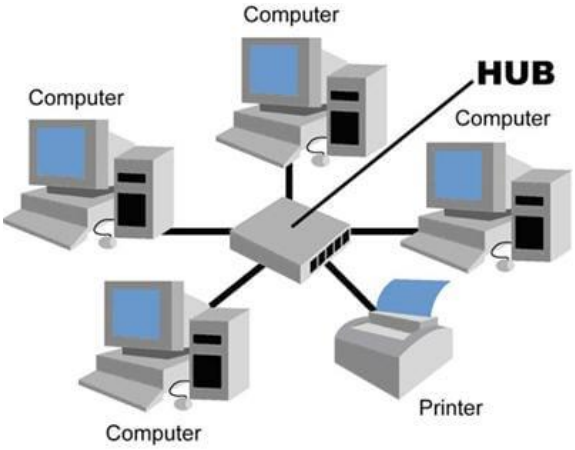
Name the different types of network topologies and brief their advantages?

Answer: Network topologies are classified as below:

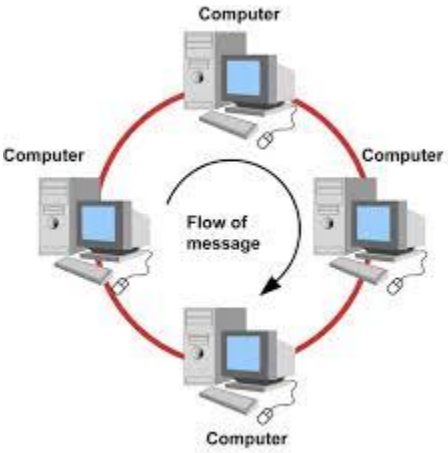
a) Bus Topology: In Bus Topology, all the devices of the network are connected to a common cable (also called as the backbone). As the devices are connected to a single cable, it is also termed as Linear Bus Topology.



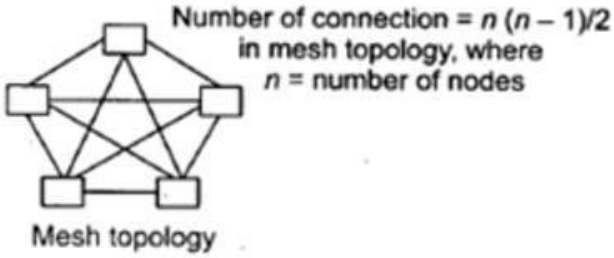
b) Star Topology: In Star Topology, there is a central controller or hub to which every node or device is connected through a cable. In this topology, the devices are not linked to each other. If a device needs to communicate with the other, then it has to send the signal or data to the central hub.



c) Ring Topology: In Ring Topology, each device of the network is connected to two other devices on either side which in turn forms a loop. Data or Signal in ring topology flow only in a single direction from one device to another and reaches the destination node.



d) Mesh Topology: In a Mesh Topology, each device of the network is connected to all other devices of the network. Mesh Topology uses Routing and Flooding techniques for data transmission.



Define Static IP and Dynamic IP?

Answer: When a device or computer is assigned a specified IP address then it is named as Static IP. It is assigned by the Internet Service Provider as a permanent address.

Dynamic IP is the temporary IP address assigned by the network to a computing device. Dynamic IP is automatically assigned by the server to the network device.

What is the use of encryption and decryption?

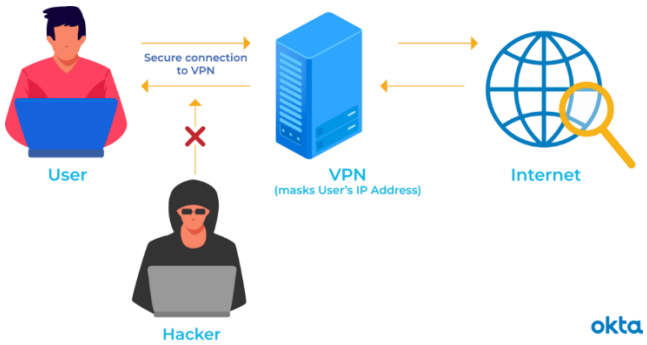
Answer: Encryption is the process of converting the transmission data into another form that is not read by any other device other than the intended receiver.

Decryption is the process of converting back the encrypted data to its normal form. An algorithm called cipher is used in this conversion process.

What is Ethernet?

Answer: Ethernet is a technology that is used to connect computers all over the network to transmit the data between each other.

What is a VPN?



- VPN which stands for a Virtual Private Network.
- It refers to a private WAN (Wide Area Network) that is created on the Internet.
- By using a VPN, a person can connect to an organization's network no matter how far it is present

What is an IPv4 address? What are the different classes of IPv4?

An IP address is a 32-bit dynamic address of a node in the network. An IPv4 address has 4 octets of 8-bit each with each number with a value up to 255.

IPv4 classes are differentiated based on the number of hosts it supports on the network. There are five types of IPv4 classes and are based on the first octet of IP addresses which are classified as Class A, B, C, D, or E.

IPv4 Class	IPv4 Start Address	IPv4 End Address	Usage
A	0.0.0.0	127.255.255.255	Used for Large Network
B	128.0.0.0	191.255.255.255	Used for Medium Size Network
C	192.0.0.0	223.255.255.255	Used for Local Area Network
D	224.0.0.0	239.255.255.255	Reserved for Multicasting
E	240.0.0.0	255.255.255.254	Study and R&D

What is the ICMP protocol?

ICMP is the Internet Control Message Protocol. It is a network layer protocol used for error handling. It is mainly used to check the connectivity/reachability between two systems. It uses port 7 by default

What is the ARP protocol?

ARP is Address Resolution Protocol. It is a network-level protocol used to convert the logical address i.e. IP address to the device's physical address i.e. MAC address. It can also be used to get the MAC address of devices when they are trying to communicate over the local network.

What is the FTP protocol?

FTP is a File Transfer Protocol. It is an application layer protocol used to transfer files and data reliably and efficiently between hosts. It can also be used to download files from remote servers to your computer. It uses port 27 by default

What is the MAC address and how is it related to NIC?

MAC address is the Media Access Control address. It is a 48-bit or 64-bit unique identifier of devices in the network. It is also called the physical address.

What is a subnet?

A subnet is a network inside a network achieved by the process called subnetting which helps divide a network into subnets. It is used for getting a higher routing efficiency and enhances the security of the network. It reduces the time to extract the host address from the routing table.

What happens when you enter google.com in the web browser?

Below are the steps that are being followed:

- Check the browser cache first if the content is fresh and present in cache display the same.
- If not, the OS to do a DNS lookup using UDP to get the corresponding IP address of the URL from the DNS server to establish a new TCP connection.
- A new TCP connection is set between the browser and the server using three-way handshaking.
- An HTTP request is sent to the server using the TCP connection.
- The web servers running on the Servers handle the incoming HTTP request and send the HTTP response.
- The browser process the HTTP response sent by the server and may close the TCP connection or reuse the same for future requests.
- If the response data is cacheable then browsers cache the same.
- Browser decodes the response and renders the content.

Describe Hub, Switch and Router?

Answer:

- **Hub:** Hub will broadcast all data to every port. It has a common connection point for all devices.
- **Switch:** Switch will create the dynamic connection and provide information to the requesting port.
- **Router**: Router is the devices which will be responsible for forwarding data packets.

What is Amplitude shift Keying (ASK) ?

It represent the digital data as variations in amplitudes in carrier wave. i.e '1' represented by transmitting a fixed amplitude carrier wave for the bit duration with constant frequency.

What is Frequency shift keying (FSK) ?

It represent the digital data as variation in frequency in carrier wave, i.e for '1' more than carrier frequency , for '0' less than carrier frequency.

What is Binary Phase shift Keying (BPSK) ?

for each one bit of binary data (0 & 1) carrier phase will be changed (two different shifts: 0, 180)

What do you mean by fiber optic?

A long cylinder or rod of transparent material forming a core surrounded by an external cladding with a slightly different material.

What is Communication System?

Communication system is a data transmitting technique used to transmit data including video, audio, electrons, image etc. An analog signal is a continuous time-varying signal which represents a time-varying quantity

- **Analog Signal** – The value of the amplitude in the analog signal has infinite value.
- **Digital Signal** – The value of the amplitude in the Digital signal can only have finite and discrete values.

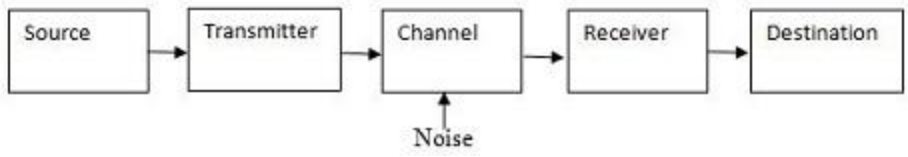
What is bandwidth of a signal?

- **Answer:** Bandwidth is defined as the frequency range over which an information signal is transmitted or in other words we can say that bandwidth is the difference between the upper and lower frequency limits of the signal

What is noise figure?

- **Answer:** The noise figure F is defined as the ratio of the signal-to-noise power supplied to the input terminals of a receiver or amplifier to the signal-to-noise power supplied to the output or load resistor.

Elements of communication system is:



Protocols supported at various levels

Layer	Name	Protocols
Layer 7	Application	SMTP, HTTP, FTP, POP3, SNMP
Layer 6	Presentation	MPEG, ASCH, SSL, TLS

Layer	Name	Protocols
Layer 5	Session	NetBIOS, SAP
Layer 4	Transport	TCP, UDP
Layer 3	Network	IPV5, IPV6, ICMP, IPSEC, ARP, MPLS.
Layer 2	Data Link	RAPA, PPP, Frame Relay, ATM, Fiber Cable, etc.
Layer 1	Physical	RS232, 100BaseTX, ISDN, 11.

What Is Ipv6?

Answer :

IPv6 is the new version of the Internet address protocol that has been developed to supplement (and eventually replace) IPv4, the version that underpins the Internet today.

What is SSH?

SSH stands for **Secure Shell** is a network protocol, used to access remote machine. SSH is Known for its high security. SSH is configured on port 22, by default

SSH or Telnet? Why?

Answer : Both SSH and Telnet are network Protocol. Both the services are used in order to connect and communicate to another machine over Network. SSH uses Port 22 and Telnet uses port 23 by default. Telnet send data in plain text and non-encrypted format everyone can understand whereas SSH sends data in encrypted format. Not to mention SSH is more secure than Telnet and hence SSH is preferred over Telnet.

What does network simulator?

A network simulator is software that **predicts the behavior of a computer network**. Since communication networks have become too complex for traditional analytical methods to provide an accurate understanding of system behavior, network simulators are used

What are protocols?

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

1. **Transmission Control Protocol (TCP):** TCP is a popular communication protocol which is used for communicating over a network. It divides any message into series of packets that are sent from source to destination and there it gets reassembled at the destination.
2. **Internet Protocol (IP):** IP is designed explicitly as addressing protocol. It is mostly used with TCP. The IP addresses in packets help in routing them through different nodes in a network until it reaches the destination system. TCP/IP is the most popular protocol connecting the networks.
3. **User Datagram Protocol (UDP):** UDP is a substitute communication protocol to Transmission Control Protocol implemented primarily for creating loss-tolerating and low-latency linking between different applications.
4. **Post office Protocol (POP):** POP3 is designed for receiving incoming E-mails.
5. **Simple mail transport Protocol (SMTP):** SMTP is designed to send and distribute outgoing E-Mail.
6. **File Transfer Protocol (FTP):** FTP allows users to transfer files from one machine to another. Types of files may include program files, multimedia files, text files, and documents, etc.
7. **Hyper Text Transfer Protocol (HTTP):** HTTP is designed for transferring a hypertext among two or more systems. HTML tags are used for creating links. These links may be in any form like text or images.
8. **Hyper Text Transfer Protocol Secure (HTTPS):** HTTPS is abbreviated as Hyper Text Transfer Protocol Secure is a standard protocol to secure the communication among two computers one using the browser and other fetching data from web server.
9. **Telnet:** Telnet is a set of rules designed for connecting one system with another. The connecting process here is termed as remote login. The system which requests for connection is the local computer, and the system which accepts the connection is the remote computer.
10. **Gopher:** Gopher is a collection of rules implemented for searching, retrieving as well as displaying documents from isolated sites. Gopher also works on the client/server principle.

- ARP (Address Resolution Protocol)
- DHCP (Dynamic Host Configuration Protocol)
- IMAP4 (Internet Message Access Protocol)
- SIP (Session Initiation Protocol)
- RTP (Real-Time Transport Protocol)
- RLP (Resource Location Protocol)
- RAP (Route Access Protocol)
- L2TP (Layer Two Tunnelling Protocol)
- PPTP (Point To Point Tunnelling Protocol)
- SNMP (Simple Network Management Protocol)
- TFTP (Trivial File Transfer Protocol)

- CLI Command line interpreter
- API Application Programming Interface
- ANSI American National Standards Institute
- ACL Access control list
- BGP Border Gateway Protocol (routing protocol)
- DSL Digital subscriber line
- FDDI Fiber Distributed Data Interface
- gbps Gigabit per second
- Mbps Megabits per second
- MAC Media access control
- NAT Network Address Translation
- NIC Network Interface Card
- OSPF Open Shortest Path First (routing protocol)
- PPP Point-to-point Protocol
- RARP Reverse ARP