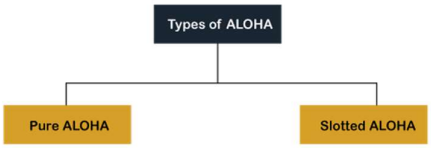
ALOHA Random Access Protocol

It is designed for wireless LAN (Local Area Network) but can also be used in a shared medium to transmit data. Using this method, any station can transmit data across a network simultaneously when a data frameset is available for transmission.

Aloha Rules

1. Any station can transmit data to a channel at any time.
2. It does not require any carrier sensing.
3. Collision and data frames may be lost during the transmission of data through multiple stations.
4. Acknowledgment of the frames exists in Aloha. Hence, there is no collision detection.
5. It requires retransmission of data after some random amount of time.



Pure Aloha

Whenever data is available for sending over a channel at stations, we use Pure Aloha. In pure Aloha, when each station transmits data to a channel without checking whether the channel is idle or not, the chances of collision may occur, and the data frame can be lost. When any station transmits the data frame to a channel, the pure Aloha waits for the receiver's acknowledgment. If it does not acknowledge the receiver end within the specified time, the station waits for a random amount of time, called the backoff time (Tb). And the station may assume the frame has been lost or destroyed. Therefore, it retransmits the frame until all the data are successfully transmitted to the receiver.

1. The total vulnerable time of pure Aloha is 2 * Tfr.
2. Maximum throughput occurs when G = 1/ 2 that is 18.4%.
3. Successful transmission of data frame is S = G * e ^ - 2 G.

Slotted Aloha

The slotted Aloha is designed to overcome the pure Aloha's efficiency because pure Aloha has a very high possibility of frame hitting. In slotted Aloha, the shared channel is divided into a fixed time interval called **slots**. So that, if a station wants to send a frame to a shared channel, the frame can only be sent at the beginning of the slot, and only one frame is allowed to be sent to each slot. And if the stations are unable to send data to the beginning of the slot, the station will have to wait

until the beginning of the slot for the next time. However, the possibility of a collision remains when trying to send a frame at the beginning of two or more station time slot.

1. Maximum throughput occurs in the slotted Aloha when G = 1 that is 37%.
2. The probability of successfully transmitting the data frame in the slotted Aloha is S = G * e ^ - 2 G.
3. The total vulnerable time required in slotted Aloha is Tfr.
4. we shall see the difference between these Protocols:

S.NO	Pure Aloha	Slotted Aloha
1.	In this aloha, any station can transmit the data at any time.	In this, any station can transmit the data at the beginning of any time slot.
2.	In this, The time is continuous and not globally synchronized.	In this, The time is discrete and globally synchronized.
3.	Vulnerable time for pure aloha = 2 x Tt	Vulnerable time for Slotted aloha = Tt
4.	In Pure Aloha, Probability of successful transmission of data packet = $G \times e^{-2G}$	In Slotted Aloha, Probability of successful transmission of data packet = $G \times e^{-G}$
5.	In pure aloha, Maximum efficiency = 18.4%	In slotted aloha, Maximum efficiency = 36.8%
6.	Pure aloha doesn't reduces the number of collisions to half.	Slotted aloha reduces the number of collisions to half and doubles the efficiency of pure aloha.

Network Interface Card (NIC)

Network Interface Card (NIC) is a **hardware component** that is present on the computer. It is used to **connect different networking devices** such as computers and servers to share data over the connected network. It provides functionality such as support for I/O interrupt, Direct Memory Access (DMA) interfaces, partitioning, and data transmission.

NIC is important for us to establish a wired or wireless connection over the network.

Network Interface Card is also known as **Network Interface Controller, Network Adapter, Ethernet card, Connection card**, and **LAN (Local Area Network) Adapter.**

Functions of the Network Interface Card

A list of functions of the Network Interface Card is given below -

1. NIC is used to convert data into a digital signal.
2. In the OSI model, NIC uses the physical layer to transmit signals and the network layer to transmit data packets.

3. NIC offers both wired (using cables) and wireless (using Wi-Fi) data communication techniques.
4. NIC is a middleware between a computer/server and a data network.
5. NIC operates on both physical as well as the data link layer of the OSI model.

Types of Network Interface Cards

There are the following two types of NICs -

1. Ethernet NIC

Ethernet NIC was developed by **Robert Metcalf in 1980**. It is made by ethernet cables. This type of NIC is most widely used in the LAN, MAN, and WAN networks.

Example: TP-LINK TG-3468 Gigabit PCI Express Network Adapter.

2. Wireless Networks NIC

It is a wireless network that allows us to connect the devices without using the cables. These types of NICs are used to design a Wi-Fi connection.

Example: Intel 3160 Dual-Band Wireless Adapter

Advantages of NIC

A list of advantages of NIC is given below -

1. As compared to the wireless network card, NIC provides a secure, faster, and more reliable connection.
2. NIC allows us to share bulk data among many users.
3. It helps us to connect peripheral devices using many ports of NIC.
4. Communication speed is high.
5. Network Interface cards are not expensive.
6. NICs are easy to troubleshoot.

Disadvantages of NIC

A list of disadvantages of NIC is given below -

1. NIC is inconvenient as compared to the wireless card.
2. For wired NIC, a hard-wired connection is required.
3. NIC needs a proper configuration to work efficiently.
4. NIC cards are not secure, so the data inside NIC is not safe.

TCP 3-Way Handshake Process

This could also be seen as a way of how TCP connection is established.

TCP stands for **Transmission Control Protocol** which indicates that it does something to control the transmission of the data in a reliable way.

The process of communication between devices over the internet happens according to the current **TCP/IP** suite model(stripped out version of OSI reference model). The Application layer is a top pile of stack of TCP/IP model from where network referenced application like web browser on the client side establish connection with the server. From the application layer,the information is transferred to the transport layer where our topic comes into picture. The two important protocols of this layer are – TCP, **UDP(User Datagram Protocol)** out of which TCP is prevalent(since it provides reliability for the connection established). However you can find application of UDP in querying the DNS server to get the binary equivalent of the Domain Name used for the website.

TCP provides reliable communication with something called **Positive Acknowledgement with Re-transmission(PAR)**. The Protocol Data Unit(PDU) of the transport layer is called segment. Now a device using PAR resend the data unit until it receives an acknowledgement. If the data unit received at the receiver's end is damaged(It checks the data with checksum functionality of the transport layer that is used for Error Detection), then receiver discards the segment. So the sender has to resend the data unit for which positive acknowledgement is not received. You can realize from above mechanism that three segments are exchanged between sender(client) and receiver(server) for a reliable TCP connection to get established. Let us delve how this mechanism works :

- **Step 1 (SYN) :** In the first step, client wants to establish a connection with server, so it sends a segment with SYN(Synchronize Sequence Number) which informs server that 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 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 server and they both establish a reliable connection with which they will start the actual data transfer The steps 1, 2 establish the connection parameter (sequence number) for one direction and it is acknowledged. The steps 2, 3 establish the connection parameter (sequence number) for the other direction and it is acknowledged. With these, a full-duplex communication is established.

Leaky Bucket Algorithm

Suppose we have a bucket in which we are pouring water in a random order but we have to get water in a fixed rate, for this we will make a hole at the bottom of the bucket. It will ensure that water coming out is in a some fixed rate, and also if bucket will full we will stop pouring in it.

The input rate can vary, but the output rate remains constant. Similarly, in networking, a technique called leaky bucket can smooth out bursty traffic. Bursty chunks are stored in the bucket and sent out at an average rate.

A simple leaky bucket algorithm can be implemented using FIFO queue. A FIFO queue holds the packets. If the traffic consists of fixed-size packets (e.g., cells in ATM networks), the process removes a fixed number of packets from the queue at each tick of the clock. If the traffic consists of variable-length packets, the fixed output rate must be based on the number of bytes or bits.

The following is an algorithm for variable-length packets:

1. Initialize a counter to n at the tick of the clock.
2. If n is greater than the size of the packet, send the packet and decrement the counter by the packet size. Repeat this step until n is smaller than the packet size.
3. Reset the counter and go to step 1.

Token bucket Algorithm

Need of token bucket Algorithm:-
The leaky bucket algorithm enforces output pattern at the average rate, no matter how bursty the traffic is. So in order to deal with the bursty traffic we need a flexible algorithm so that the data is not lost. One such algorithm is token bucket algorithm.

Steps of this algorithm can be described as follows:

1. In regular intervals tokens are thrown into the bucket. ƒ
2. The bucket has a maximum capacity. ƒ
3. If there is a ready packet, a token is removed from the bucket, and the packet is sent.
4. If there is no token in the bucket, the packet cannot be sent.

Some advantage of token Bucket over leaky bucket –

- If bucket is full in token Bucket , tokens are discard not packets. While in leaky bucket, packets are discarded.
- Token Bucket can send Large bursts at a faster rate while leaky bucket always sends packets at constant rate.

Difference between Leaky and Token buckets –

Leaky Bucket	Token Bucket
When the host has to send a packet , packet is thrown in bucket.	In this leaky bucket holds tokens generated at regular intervals of time.
Bucket leaks at constant rate	Bucket has maximum capacity.
Bursty traffic is converted into uniform traffic by leaky bucket.	If there is a ready packet , a token is removed from Bucket and packet is send.
In practice bucket is a finite queue outputs at finite rate	If there is a no token in bucket, packet can not be send.

Token Ring

Token ring (IEEE 802.5) is a communication protocol in a local area network (LAN) where all stations are connected in a ring topology and pass one or more tokens for channel acquisition. A token is a special frame of 3 bytes that circulates along the ring of stations. A station can send data frames only if it holds a token. The tokens are released on successful receipt of the data frame.

Token Bus

Token Bus (IEEE 802.4) is a standard for implementing token ring over virtual ring in LANs. The physical media has a bus or a tree topology and uses coaxial cables. A virtual ring is created with the nodes/stations and the token is passed from one node to the next in a sequence along this virtual ring. Each node knows the address of its preceding station and its succeeding station. A station can only transmit data when it has the token. The working principle of token bus is similar to Token Ring.

Differences between Token Ring and Token Bus

Token Ring	Token Bus
The token is passed over the physical ring formed by the stations and the coaxial cable network.	The token is passed along the virtual ring of stations connected to a LAN.
The stations are connected by ring topology, or sometimes star topology.	The underlying topology that connects the stations is either bus or tree topology.

Token Ring	Token Bus
It is defined by IEEE 802.5 standard.	It is defined by IEEE 802.4 standard.
The maximum time for a token to reach a station can be calculated here.	It is not feasible to calculate the time for token transfer.

Class ranges of IP A B C

Internet Protocol hierarchy contains several classes of IP Addresses to be used efficiently in various situations as per the requirement of hosts per network. Broadly, the IPv4 Addressing system is divided into five classes of IP Addresses. All the five classes are identified by the first octet of IP Address.

Class A Address

The first bit of the first octet is always set to 0 (zero). Thus the first octet ranges from 1 – 127, i.e.

```
00000001 - 01111111
       1 - 127
```

Class A addresses only include IP starting from 1.x.x.x to 126.x.x.x only. The IP range 127.x.x.x is reserved for loopback IP addresses.

The default subnet mask for Class A IP address is 255.0.0.0 which implies that Class A addressing can have 126 networks (2^7-2) and 16777214 hosts (2^{24}-2).

Class A IP address format is thus: **0NNNNNNN**.HHHHHHHH.HHHHHHHH.HHHHHHHH

Class B Address

An IP address which belongs to class B has the first two bits in the first octet set to 10, i.e.

```
10000000 - 10111111
     128 - 191
```

Class B IP Addresses range from 128.0.x.x to 191.255.x.x. The default subnet mask for Class B is 255.255.x.x.

Class B has 16384 (2^{14}) Network addresses and 65534 (2^{16}-2) Host addresses.

Class B IP address format is: **10NNNNNN.NNNNNNNN**.HHHHHHHH.HHHHHHHH

Class C Address

The first octet of Class C IP address has its first 3 bits set to 110, that is –

```
11000000 - 11011111
     192 - 223
```

Class C IP addresses range from 192.0.0.x to 223.255.255.x. The default subnet mask for Class C is 255.255.255.x.

Class C gives 2097152 (2^{21}) Network addresses and 254 (2^8-2) Host addresses.

Class C IP address format is: **110NNNNN.NNNNNNNN.NNNNNNNN**.HHHHHHHH

Class D Address

Very first four bits of the first octet in Class D IP addresses are set to 1110, giving a range of –

```
11100000 - 11101111
     224 - 239
```

Class D has IP address range from 224.0.0.0 to 239.255.255.255. Class D is reserved for Multicasting. In multicasting data is not destined for a particular host, that is why there is no need to extract host address from the IP address, and Class D does not have any subnet mask.

Class E Address

This IP Class is reserved for experimental purposes only for R&D or Study. IP addresses in this class ranges from 240.0.0.0 to 255.255.255.254. Like Class D, this class too is not equipped with any subnet mask.

Difference Between IPv4 and IPv6:

IPV4	IPV6
Ipv4 has 32-bit address length	IPv6 has 128-bit address length
It supports manual and dhcp address configuration	It supports Auto and renumbering address configuration
In ipv4 end to end connection integrity is unachievable	In IPv6 end to end connection integrity is Achievable
It can generate 4.29×10^9 address space	Address space of IPv6 is quite large it can produce 3.4×10^{38} address space
Security feature is dependent on application	IPSEC is inbuilt security feature in the IPv6 protocol
Address representation of ipv4 is in decimal	Address Representation of IPv6 is in hexadecimal
Fragmentation performed by sender and forwarding routers	In IPv6 fragmentation performed only by sender
In ipv4 packet flow identification is not available	In IPv6 packetflow identification are Available and uses flow label field in the header
In ipv4 checksumfield is available	In IPv6 checksumfield is not available
It has broadcast message transmission scheme	In IPv6 multicast and any cast message transmission scheme is available
In ipv4 encryption and authentication facility not provided	In IPv6 Encryption and Authentication are provided
Ipv4 has header of 20-60 bytes.	IPv6 has header of 40 bytes fixed

---

TELNET

TELNET stands for **TE**rmina**L NET**work. It is a type of protocol that enables one computer to connect to local computer. It is a used as a standard TCP/IP protocol for virtual terminal service which is given by ISO. Computer which starts connection known as the **local computer**. Computer which is being connected to i.e. which accepts the connection known as **remote computer**. When the connection is established between local and remote computer. During telnet operation whatever that is performing on the remote computer will be displayed by local computer. Telnet operates on client/server principle. Local computer uses telnet client program and the remote computers uses telnet server program.

Non return to Zero (NRZ)

In telecommunication, a **non-return-to-zero** (**NRZ**) line code is a binary code in which ones are represented by one significant condition, usually a positive voltage, while zeros are represented by some other significant condition, usually a negative voltage, with no other neutral or rest condition. The pulses in NRZ have more energy than a return-to-zero (RZ) code, which also has an additional rest state beside the conditions for ones and zeros. NRZ is not inherently a self-clocking signal, so some additional synchronization technique must be used for avoiding bit slips; examples of such techniques are a run-length-limited constraint and a parallel synchronization signal.

For a given data signaling rate, i.e., bit rate, the NRZ code requires only half the baseband bandwidth required by the Manchester code (the passband bandwidth is the same). When used to represent data in an asynchronous communication scheme, the absence of a neutral state requires other mechanisms for bit synchronization when a separate clock signal is not available.

Difference between Hub and Switch:

S.NO	HUB	SWITCH
1.	Hub is operated on **Physical layer**.	While switch is operated on **Data link layer**.
2.	Hub is a broadcast type transmission.	While switch is a Unicast, multicast and broadcast type transmission.
3.	Hub have maximum 4 ports.	While switch can have 24 to 28 ports.
4.	In hub, there is only one collision domain.	While in switch, different ports have own collision domain.
5.	Hub is a half duplex transmission mode.	While switch is a full duplex transmission mode.
6.	In hub, Packet filtering is not provided.	While in switch, Packet filtering is provided.

7.	Hub cannot be used as a repeater.	While switch can be used as a repeater.
8.	Hub is not an intelligent device hence it is comparatively inexpensive.	While switch is an intelligent device so it is expensive.
9.	Hub is simply old type of device and is not generally used.	While switch is very sophisticated device and widely used.
10.	Hacking of systems attached to hub is complex.	Hacking of systems attached to switch is little easy.

---

difference between Fast Ethernet and Gigabit Ethernet:

S.NO	FAST ETHERNET	GIGABIT ETHERNET
1.	Fast Ethernet provides 100 Mbps speed.	Gigabit Ethernet offers 1 Gbps speed.
2.	Fast Ethernet is simple configured.	While Gigabit Ethernet is more complicated than Fast Ethernet.
3.	Fast Ethernet generate more delay comparatively.	Gigabit Ethernet generate less delay than Fast Ethernet.
4.	The coverage limit of Fast Ethernet is up to 10 km.	While the coverage limit of Gigabit Ethernet is up to 70 km.
5.	The round-trip delay in Fast Ethernet is 100 to 500 bit times.	While the round-trip delay in Gigabit Ethernet is 4000 bit times.
6.	Fast Ethernet is the Successor of 10-Base-T Ethernet.	While Gigabit Ethernet is the successor of Fast Ethernet.

FTP

- FTP stands for File transfer protocol.
- FTP is a standard internet protocol provided by TCP/IP used for transmitting the files from one host to another.
- It is mainly used for transferring the web page files from their creator to the computer that acts as a server for other computers on the internet.
- It is also used for downloading the files to computer from other servers.

Objectives of FTP

- It provides the sharing of files.
- It is used to encourage the use of remote computers.
- It transfers the data more reliably and efficiently.

Why FTP?

Although transferring files from one system to another is very simple and straightforward, but sometimes it can cause problems. For example, two systems may have different file conventions. Two systems may have different ways to represent text and data. Two systems may have different directory structures. FTP protocol overcomes these problems by establishing two connections

between hosts. One connection is used for data transfer, and another connection is used for the control connection.

Advantages of FTP:

- **Speed:** One of the biggest advantages of FTP is speed. The FTP is one of the fastest way to transfer the files from one computer to another computer.
- **Efficient:** It is more efficient as we do not need to complete all the operations to get the entire file.
- **Security:** To access the FTP server, we need to login with the username and password. Therefore, we can say that FTP is more secure.
- **Back & forth movement:** FTP allows us to transfer the files back and forth. Suppose you are a manager of the company, you send some information to all the employees, and they all send information back on the same server.

Disadvantages of FTP:

- The standard requirement of the industry is that all the FTP transmissions should be encrypted. However, not all the FTP providers are equal and not all the providers offer encryption. So, we will have to look out for the FTP providers that provides encryption.
- FTP serves two operations, i.e., to send and receive large files on a network. However, the size limit of the file is 2GB that can be sent. It also doesn't allow you to run simultaneous transfers to multiple receivers.
- Passwords and file contents are sent in clear text that allows unwanted eavesdropping. So, it is quite possible that attackers can carry out the brute force attack by trying to guess the FTP password.
- It is not compatible with every system.

MAC

The medium access control (MAC) is a sublayer of the data link layer of the open system interconnections (OSI) reference model for data transmission. It is responsible for flow control and multiplexing for transmission medium. It controls the transmission of data packets via remotely shared channels. It sends data over the network interface card.

Functions of MAC Layer

- It provides an abstraction of the physical layer to the LLC and upper layers of the OSI network.
- It is responsible for encapsulating frames so that they are suitable for transmission via the physical medium.

- It resolves the addressing of source station as well as the destination station, or groups of destination stations.
- It performs multiple access resolutions when more than one data frame is to be transmitted. It determines the channel access methods for transmission.
- It also performs collision resolution and initiating retransmission in case of collisions.
- It generates the frame check sequences and thus contributes to protection against transmission errors.

LLC

The logical link control (LLC) is the upper sublayer of the data link layer of the open system interconnections (OSI) reference model for data transmission. It acts act an interface between the network layer and the medium access control (MAC) sublayer of the data link layer.

The LLC sublayer is mainly used for its multiplexing property. It allows several network protocols to operate simultaneously within a multipoint network over the same network medium.

Functions of LLC Sublayer

- The primary function of LLC is to multiplex protocols over the MAC layer while transmitting and likewise to de-multiplex the protocols while receiving.
- LLC provides hop-to-hop flow and error control.
- It allows multipoint communication over computer network.
- Frame Sequence Numbers are assigned by LLC.
- In case of acknowledged services, it tracks acknowledgements

---

TCP/ IP layers

The layers are:

1. Process/Application Layer
2. Host-to-Host/Transport Layer
3. Internet Layer
4. Network Access/Link Layer

1. Network Access Layer –

This layer corresponds to the combination of Data Link Layer and Physical Layer of the OSI model. It looks out for hardware addressing and the protocols present in this layer allows for the physical transmission of data.
We just talked about ARP being a protocol of Internet layer, but there is a conflict about declaring it as a protocol of Internet Layer or Network access layer. It is described as residing in layer 3, being encapsulated by layer 2 protocols.

2. Internet Layer –

This layer parallels the functions of OSI's Network layer. It defines the protocols which are responsible for logical transmission of data over the entire network. The main protocols residing at this layer are :

1. **IP –** stands for Internet Protocol and it is responsible for delivering packets from the source host to the destination host by looking at the IP addresses in the packet headers. IP has 2 versions:
   IPv4 and IPv6. IPv4 is the one that most of the websites are using currently. But IPv6 is growing as the number of IPv4 addresses are limited in number when compared to the number of users.
2. **ICMP –** stands for Internet Control Message Protocol. It is encapsulated within IP datagrams and is responsible for providing hosts with information about network problems.
3. **ARP –** stands for Address Resolution Protocol. Its job is to find the hardware address of a host from a known IP address. ARP has several types: Reverse ARP, Proxy ARP, Gratuitous ARP and Inverse ARP.

3. Host-to-Host Layer –

This layer is analogous to the transport layer of the OSI model. It is responsible for end-to-end communication and error-free delivery of data. It shields the upper-layer applications from the complexities of data. The two main protocols present in this layer are :

1. **Transmission Control Protocol (TCP) –** It is known to provide reliable and error-free communication between end systems. It performs sequencing and segmentation of data. It also has acknowledgment feature and controls the flow of the data through flow control mechanism. It is a very effective protocol but has a lot of overhead due to such features. Increased overhead leads to increased cost.
2. **User Datagram Protocol (UDP) –** On the other hand does not provide any such features. It is the go-to protocol if your application does not require reliable transport as it is very cost-effective. Unlike TCP, which is connection-oriented protocol, UDP is connectionless.

4. Application Layer –

This layer performs the functions of top three layers of the OSI model: Application, Presentation and Session Layer. It is responsible for node-to-node communication and controls user-interface specifications. Some of the protocols present in this layer are: HTTP, HTTPS, FTP, TFTP, Telnet, SSH, SMTP, SNMP, NTP, DNS, DHCP, NFS, X Window, LPD. Have a look at Protocols in Application Layer for some information about these protocols. Protocols other than those present in the linked article are :

1. **HTTP and HTTPS –** HTTP stands for Hypertext transfer protocol. It is used by the World Wide Web to manage communications between

web browsers and servers. HTTPS stands for HTTP-Secure. It is a combination of HTTP with SSL(Secure Socket Layer). It is efficient in cases where the browser need to fill out forms, sign in, authenticate and carry out bank transactions.

2. **SSH –** SSH stands for Secure Shell. It is a terminal emulations software similar to Telnet. The reason SSH is more preferred is because of its ability to maintain the encrypted connection. It sets up a secure session over a TCP/IP connection.
3. **NTP –** NTP stands for Network Time Protocol. It is used to synchronize the clocks on our computer to one standard time source. It is very useful in situations like bank transactions. Assume the following situation without the presence of NTP. Suppose you carry out a transaction, where your computer reads the time at 2:30 PM while the server records it at 2:28 PM. The server can crash very badly if it's out of sync.

Difference between TCP/IP and OSI Model:

TCP/IP	OSI
TCP refers to Transmission Control Protocol.	OSI refers to Open Systems Interconnection.
TCP/IP has 4 layers.	OSI has 7 layers.
TCP/IP is more reliable	OSI is less reliable
TCP/IP does not have very strict boundaries.	OSI has strict boundaries
TCP/IP follow a horizontal approach.	OSI follows a vertical approach.
TCP/IP uses both session and presentation layer in the application layer itself.	OSI uses different session and presentation layers.
TCP/IP developed protocols then model.	OSI developed model then protocol.
Transport layer in TCP/IP does not provide assurance delivery of packets.	In OSI model, transport layer provides assurance delivery of packets.
TCP/IP model network layer only provides connection less services.	Connection less and connection oriented both services are provided by network layer in OSI model.
Protocols cannot be replaced easily in TCP/IP model.	While in OSI model, Protocols are better covered and is easy to replace with the change in technology.

DNS

DNS is a host name to IP address translation service. DNS is a distributed database implemented in a hierarchy of name servers. It is an application layer protocol for message exchange between clients and servers.

Requirement

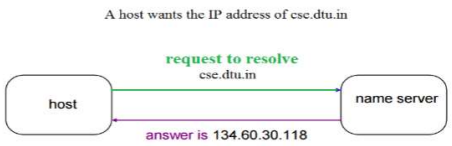
Every host is identified by the IP address but remembering numbers is very difficult for the people and also the IP addresses are not static therefore a mapping is required to change the domain name to IP address. So DNS is used to convert the domain name of the websites to their numerical IP address.

Domain :

There are various kinds of DOMAIN :

1. Generic domain : .com(commercial) .edu(educational) .mil(military) .org(non profit organization) .net(similar to commercial) all these are generic domain.
2. Country domain .in (india) .us .uk
3. Inverse domain if we want to know what is the domain name of the website. Ip to domain name mapping.So DNS can provide both the mapping for example to find the ip addresses of geeksforgeeks.org then we have to type nslookup www.geeksforgeeks.org.
4. **DNS record** – Domain name, ip address what is the validity?? what is the time to live ?? and all the information related to that domain name. These records are stored in tree like structure.
5.
6. **Namespace** – Set of possible names, flat or hierarchical . Naming system maintains a collection of bindings of names to values – given a name, a resolution mechanism returns the corresponding value –
7. **Name server** – It is an implementation of the resolution mechanism.. DNS (Domain Name System) = Name service in Internet – Zone is an administrative unit, domain is a subtree.

Name to Address Resolution



The host request the DNS name server to resolve the domain name. And the name server returns the IP address corresponding to that domain name to the host so that the host can future connect to that IP address.

Frequency Division Multiplexing (FDM) –

In this, a number of signals are transmitted at the same time, and each source transfers its signals in the allotted frequency range. There is a suitable frequency gap between the 2 adjacent signals to avoid over-lapping. Since the signals are transmitted in the allotted frequencies so this decreases the probability of collision. The frequency spectrum is divided into several logical channels, in which every user feels that they possess a particular bandwidth. A number of signals are sent simultaneously at the same time allocating separate frequency bands or channels to each signal. It is used in radio and TV transmission. Therefore to avoid interference between two successive channels **Guard bands** are used.

Time Division Multiplexing (TDM) –

This happens when data transmission rate of media is greater than that of the source, and each signal is allotted a definite amount of time. These slots are so small that all transmissions appear to be parallel. In frequency division multiplexing all the signals operate at the same time with different frequencies, but in time division multiplexing all the signals operate with same frequency at different times.

It is of the following types:

1. **Synchronous TDM –**
   The time slots are pre-assigned and fixed. This slot is even given if the source is not ready with data at this time. In this case, the slot is transmitted empty. It is used for multiplexing digitized voice streams.
2. **Asynchronous (or statistical) TDM –**

The slots are allocated dynamically depending on the speed of the source or their ready state. It dynamically allocates the time slots according to different input channel's needs, thus saving the channel capacity.

A **web browser and web** server are software applications and considered part of the application **layer**.

Transport Layer Protocols

The transport layer is represented by two protocols: TCP and UDP.

UDP

- UDP stands for **User Datagram Protocol**.
- UDP is a simple protocol and it provides nonsequenced transport functionality.
- UDP is a connectionless protocol.
- This type of protocol is used when reliability and security are less important than speed and size.

- UDP is an end-to-end transport level protocol that adds transport-level addresses, checksum error control, and length information to the data from the upper layer.
- The packet produced by the UDP protocol is known as a user datagram.

Disadvantages of UDP protocol

- UDP provides basic functions needed for the end-to-end delivery of a transmission.
- It does not provide any sequencing or reordering functions and does not specify the damaged packet when reporting an error.
- UDP can discover that an error has occurred, but it does not specify which packet has been lost as it does not contain an ID or sequencing number of a particular data segment.

TCP

- TCP stands for Transmission Control Protocol.
- It provides full transport layer services to applications.
- It is a connection-oriented protocol means the connection established between both the ends of the transmission. For creating the connection, TCP generates a virtual circuit between sender and receiver for the duration of a transmission.

Features Of TCP protocol

- **Stream data transfer:** TCP protocol transfers the data in the form of contiguous stream of bytes. TCP group the bytes in the form of TCP segments and then passed it to the IP layer for transmission to the destination. TCP itself segments the data and forward to the IP.
- **Reliability:** TCP assigns a sequence number to each byte transmitted and expects a positive acknowledgement from the receiving TCP. If ACK is not received within a timeout interval, then the data is retransmitted to the destination.
  The receiving TCP uses the sequence number to reassemble the segments if they arrive out of order or to eliminate the duplicate segments.
- **Flow Control:** When receiving TCP sends an acknowledgement back to the sender indicating the number the bytes it can receive without overflowing its internal buffer. The number of bytes is sent in ACK in the form of the highest sequence number that it can receive without any problem. This mechanism is also referred to as a window mechanism.
- **Multiplexing:** Multiplexing is a process of accepting the data from different applications and forwarding to the different applications on different computers. At the receiving end, the data is forwarded to the correct application. This process is known as demultiplexing. TCP transmits the packet to the correct application by using the logical channels known as ports.

- **Logical Connections:** The combination of sockets, sequence numbers, and window sizes, is called a logical connection. Each connection is identified by the pair of sockets used by sending and receiving processes.
- **Full Duplex:** TCP provides Full Duplex service, i.e., the data flow in both the directions at the same time. To achieve Full Duplex service, each TCP should have sending and receiving buffers so that the segments can flow in both the directions. TCP is a connection-oriented protocol. Suppose the process A wants to send and receive the data from process B. The following steps occur:
  - Establish a connection between two TCPs.
  - Data is exchanged in both the directions.
  - The Connection is terminated.

Differences b/w TCP & UDP

Basis for Comparison	TCP	UDP
Definition	TCP establishes a virtual circuit before transmitting the data.	UDP transmits the data directly to the destination computer without verifying whether the receiver is ready to receive or not.
Connection Type	It is a Connection-Oriented protocol	It is a Connectionless protocol
Speed	slow	high
Reliability	It is a reliable protocol.	It is an unreliable protocol.
Header size	20 bytes	8 bytes
acknowledgement	It waits for the acknowledgement of data and has the ability to resend the lost packets.	It neither takes the acknowledgement, nor it retransmits the damaged frame.

Sampling –

The first step in PCM is sampling. Sampling is a process of measuring the amplitude of a continuous-time signal at discrete instants, converting the continuous signal into a discrete signal. There are three sampling methods:

(i) Ideal Sampling: In ideal Sampling also known as Instantaneous sampling pulses from the analog signal are sampled. This is an ideal sampling method and cannot be easily implemented.

(ii) Natural Sampling: Natural Sampling is a practical method of sampling in which pulse have finite width equal to T.The result is a sequence of samples that retain the shape of the analog signal.

(iii) Flat top sampling: In comparison to natural sampling flat top sampling can be easily obtained. In this sampling technique, the top of the samples remains constant by using a circuit. This is the most common sampling method used.

Nyquist Theorem:

One important consideration is the sampling rate or frequency. According to the Nyquist theorem, the sampling rate must be at least 2 times the highest frequency contained in the signal. It is also known as the minimum sampling rate and given by:

Fs =2*fh

Subnet

A subnet, or subnetwork, is a network inside a network. Subnets make networks more efficient. Through subnetting, network traffic can travel a shorter distance without passing through unnecessary routers to reach its destination.

When a bigger network is divided into smaller networks, in order to maintain security, then that is known as Subnetting. so, maintenance is easier for smaller networks.

Subnet Mask

A **subnet mask** is a 32-bit number which is used to identify the subnet of an IP address. The subnet mask is combination of 1's and 0's. 1's represents network and subnet ID while 0's represents the host ID. For this case, subnet mask is,

So in order to get the network which the destination address belongs to we have to **bitwise &** with subnet mask.

```
    11111111.11111111.11111111.11000000
&&  11001000.00000001.00000010.00010100
-----------------------------------------------------
    11001000.00000001.00000010.00000000
```

The address belongs to,

```
11001000.00000001.00000010.00000000
```

or

200.1.2.0

Gateway

A gateway is a network node that forms a passage between two networks operating with different transmission protocols. The most common type of gateways, the network gateway operates at layer 3, i.e. network layer of the OSI (open systems interconnection) model. However, depending upon the functionality, a gateway can operate at any of the seven layers of OSI model. It acts as the entry – exit point for a network since all traffic that flows across the networks should pass through the gateway. Only the internal traffic between the nodes of a LAN does not pass through the gateway.

Features of Gateways

- Gateway is located at the boundary of a network and manages all data that inflows or outflows from that network.
- It forms a passage between two different networks operating with different transmission protocols.
- A gateway operates as a protocol converter, providing compatibility between the different protocols used in the two different networks.
- The feature that differentiates a gateway from other network devices is that it can operate at any layer of the OSI model.
- It also stores information about the routing paths of the communicating networks.
- When used in enterprise scenario, a gateway node may be supplemented as proxy server or firewall.
- A gateway is generally implemented as a node with multiple NICs (network interface cards) connected to different networks. However, it can also be configured using software.
- It uses packet switching technique to transmit data across the networks.

A **default gateway** is the node in a computer network using the internet protocol suite that serves as the forwarding host (router) to other networks when no other route specification matches the destination IP address of a packet.

A **data breach** is the intentional or unintentional release of secure or private/confidential information to an untrusted environment. Other terms for this phenomenon include **unintentional information disclosure**, **data leak**, information leakage and also **data spill**. Incidents range from concerted attacks by black hats, or individuals who hack for some kind of personal gain, associated with organized crime, political activist or national governments to careless disposal of used computer equipment or data storage media and unhackable source.

Definition: "A data breach is a security violation in which sensitive, protected or confidential data is copied, transmitted, viewed, stolen or used by an individual unauthorized to do so."[1] Data breaches may involve financial information such as credit card or bank details, personal health information (PHI), Personally identifiable information (PII), trade secrets of corporations or intellectual property. Most data breaches involve overexposed and vulnerable unstructured data – files, documents, and sensitive information.

OSI Model Layers

1. Physical **Layer**.
2. Data Link **Layer**. ...
3. Network **Layer**. ...
4. Transport **Layer**. ...
5. Session **Layer**. ...
6. Presentation **Layer**.
7. Application **Layer**.

Optical fibre vs coaxial fibre

Twisted pair cable	Co-axial cable	Optical fiber
1. Transmission of signals takes place in the electrical form over the metallic conducting wires.	1. Transmission of signals takes place in the electrical form over the inner conductor of the cable.	1. Signal transmission takes place in an optical forms over a glass fiber.
2. In this medium the noise immunity is low.	2. Coaxial having higher noise immunity than twisted pair cable.	2. Optical fiber has highest noise immunity as the light rays are unaffected by the electrical noise.
3. Twisted pair cable can be affected due to external magnetic field.	3. Coaxial cable is less affected due to external magnetic field.	3. Not affected by the external magnetic field.
4. Cheapest medium.	4. Moderate Expensive.	4. Expensive
5. Low Bandwidth.	5. Moderately high bandwidth.	5. Very high bandwidth
6. Attenuation is very high.	6. Attenuation is low.	6. Attenuation is very low.
7. Installation is easy.	7. Installation is fairly easy.	7. Installation is difficult.

Optical Fiber

• Fiber-optic cable or optical fiber consists of thin glass fibers that can carry information in the form of visible light. The typical optical fiber consists of a very narrow strand of glass or plastic called the ***core***.

• Around the core is a concentric layer of less dense glass or plastic called the ***cladding***, whose refractive index is less than that of the core. The outer most layer of the cable is known as the jacket, which shields the cladding and the core from moisture, crushing and abrasion.