Computer Networks

- PALASH BAJPAI

Table Of Contents

Basic

Computer network is a collection of autonomous devices interconnected via a medium. The medium may be a guided medium, a wireless medium or a satellite communication.

1. **Server:-** A server is a physical computer dedicated to run services to serve the needs of other computers. Depending on the service that is running, it could be a file server, database server, home media server, print server, or web server.

2. **Client:-** is a computer hardware device or software that accesses a service made available by a server. The server is often (but not always) located on a separate physical computer.

3. **Host:**-A **host** is a computer, connected to other computers for which it provides data or services over a network.To simplify this, suppose you want to download an image from another computer on your network. That computer is “hosting” the image and therefore, it is the host computer. On the other hand, if that same computer downloads an image from your computer, your computer becomes the host computer.

4. **Protocols:-** A protocol is a set of rules which is used to govern all the aspects of information communication.The main elements of a protocol are:

    ● Syntax: It specifies the structure or format of the data. It also specifies the order in which they are presented.

    ● Semantics: It specifies the meaning of each section of bits.

    ● Timing: Timing specifies two characteristics: When data should be sent and how fast it can be sent.

Network Topology

The physical or logical view of interconnection among devices is known as topology. Ring and mesh topology are examples of peer-to-peer relationship because here all the devices share the link equally. Bus, star and tree topologies are examples of primary–secondary relationship, where one device controls and the other devices have to transmit through it.

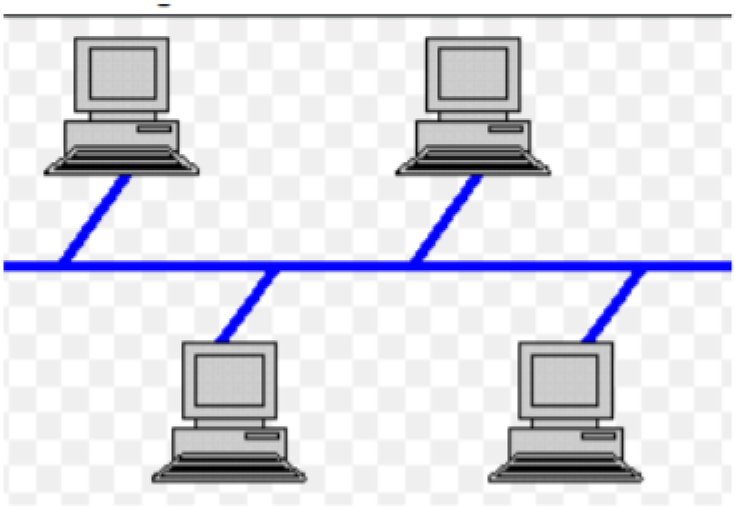
Bus Topology

In a bus network, all the devices are connected with one cable. The major benefit here is, we require less cable length than star topology and expansion is quite easy with the help of repeaters. The issues associated with bus topology are as follows:

1. Only one device can send the data at one time. All the devices will listen at that time.

2. The data communication is only in one direction.

3.In a bus topology, if the network shuts down then there is a problem in identifying the culprit device.

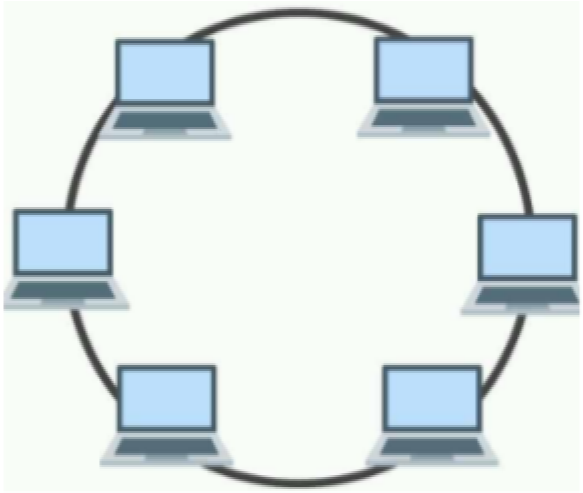


Ring Topology

1. Ring topology is a network topology in which nodes are exactly connected to two or more nodes and thus, forming a single continuous path for the transmission.

2. It does not need any central server to control the connectivity among the nodes.

3. If the single node is damaged, then the whole network fails.



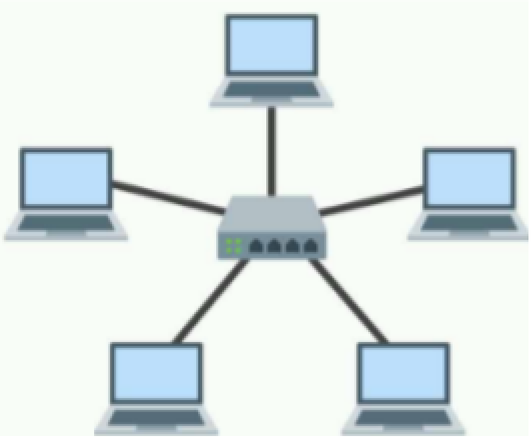
Star Topology

In a star topology, a hub is placed at the central location and all the devices are connected to the hub. All communication is possible through the hub only.. If the hub is active, it may amplify or regenerate the signals. The following are the drawbacks of a star topology:

1. If the central hub fails, no communication is possible.

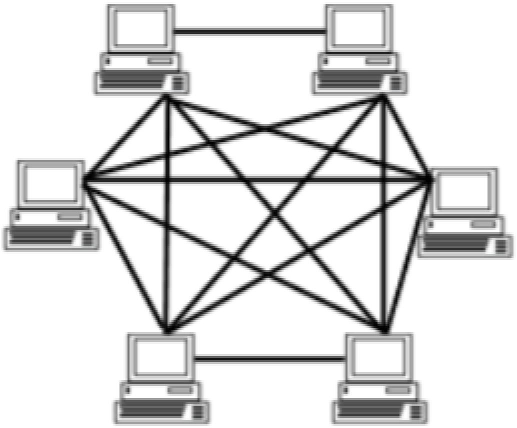
2. Cabling cost is more.

For example, Ethernet 10 base T is a popular example.



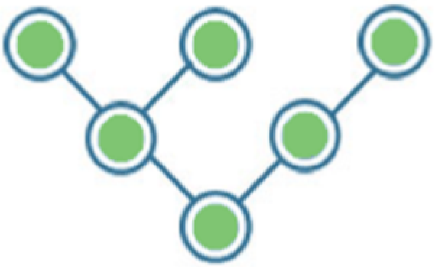
Mesh Topology

All the devices are connected through peer-to-peer links. A fully connected mesh will have n(n−1)/2 physical channels to connect n devices. The advantage of mesh topology is security and privacy. A dedicated link will eliminate traffic problems, and fault diagnosis is easy here. But cabling cost and other hardware required make it difficult to implement in real practice. It is better to use this topology in backbone networks and other topologies for further network configuration.



Tree Topology

A tree topology maintains the devices connected to a central hub as well as to some secondary hubs, which are again connected to the central hub. It allows an isolated network which prioritizes communication from different computers. It also faces the same problem as in a star topology; failure of the central hub will crash the entire network. Also, it has a high cabling cost.



Types of Address

I. IP address

- Every node in the computer network is identified by the help of an IP address.
- Logical address (can change)
- Assigned manually or dynamically

II. MAC address

- Every node in the LAN is identified with the help of MAC address.
- MAC stands for Media Access Control.
- Physical Address / Hardware Address (can't change)
- MAC addresses are only used for communication on Local Area Networks (LANs), so if you want to access a remote network or the Internet, you need an IP address.
- They are 48bit long and consist of 6 blocks of 2 hexadecimal digits 4 bits each.
- Eg: 70-20-84-00-ED-FC

III. Port address

- A port number is the logical address of each application or process that uses a network or the Internet to communicate.
- A port number uniquely identifies a network-based application on a computer.
- Each application/program is allocated a 16-bit integer port number.
- This number is assigned automatically by the OS, manually by the user or is set as a default for some popular applications.

Analogy

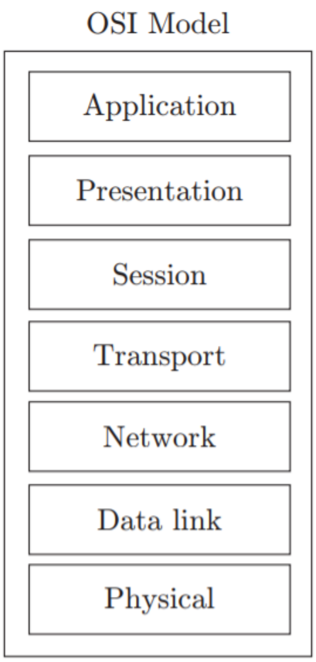
Let's consider a network equivalent to a parcel sent from Delhi to Mumbai.

Reaching our city:- Reaching our network (IP address) (needed by router)

Reaching our apartment :- Reaching our host (MAC address) (used by switch)

Reaching right person:- Reaching right process (Port address) (by OS)

OSI REFERENCE MODEL



- OSI = Open system Interconnection
- It is a model for understanding and designing a network architecture that is flexible, robust and interoperable.
- Developed by ISO.
- The OSI model is not a protocol but only a guideline. And it was never fully implemented.

Working of different layers :-

Let we have to send the data -

7. Application Layer :- abc@123

6. Presentation Layer :- odkf*3daqctv

5. Session Layer :- odkf*3daqctv (creates a session)

4. Transport Layer :- TL INFO- odkf*3daqctv

3. Network Layer :- NL INFO-TL INFO-odkf*3daqctv

2. Data Link Layer :- DL INFO-NL INFO-TL INFO- odkf*3daqctv

1. Physical Layer :- 1010001010010101001010

1. PHYSICAL LAYER

- The major responsibilities of the physical layer are transmission of raw bit stream and to form the physical interface between two communicating devices.
- It is responsible for transmitting bits over a medium.
- The conversion of analog to digital and digital to analog is performed at this layer.
- It is the lowest layer of the OSI reference model.

2. DATA LINK LAYER

- It is responsible for moving data (frames) from one node to another node. (Node to Node / hop to hop delivery)
- It provides communication between machines on the same network.
- Also, it provides frame-level error control and flow control.
- This layer is responsible for encoding and decoding i.e. converting bits to signals at sender site and recovering bits from received signals at receiver side; frame creation i.e. deciding a minimum unit for sending bits; error detection and/or correction of frames through parity or CRC and flow control using ARQ, sliding WINDOW etc.

Functionalities:-

1. Framing: The basic data unit at the data link layer is called a `frame' which is a collection of bits in sequence boundary. In order to mark boundaries of frame starting and ending characters are used.

2. Flow control: It is a mechanism which informs the sender about the amount of data transmission before receiving an acknowledgement from the receiver. As the receiving device has limited speed for processing the incoming data and limited memory to store data, it informs the sending device by sending a few frames and stop. The receiving device has a buffer, a block of memory, for storing extra incoming data before processing.

Some methods of flow control :-

a. Stop and wait :- In this protocol, the sender starts the timer and keeps the copy of the sent frame. If the timer expires and there is no acknowledgement (ACK) for the sent frame, the frame is resent, the copy is held and the timer is restarted.

1. Only 1 frame at a time.
2. Sender Window size = Receiver window size = 1
3. Retransmission = 1

b. Go Back N :- This protocol helps in improving the efficiency of transmission by filling the pipe. It supports multiple frames during wait for acknowledgement. The sequence numbers are modulo 2m, where m is the size of the sequence number field in bits. Sliding window defines the range of sequence numbers related to the sender and receiver. When the timer expires, the sender resends all outstanding frames.

1. Multiple frames are sent.
2. Sender window= 2^k-1
3. Receiver window = 1
4. Retransmission = 2^k -1
5. Cumulative acknowledgement

k= number of bits required to represent window size

c. Selective Repeat :- It is a mechanism which informs the sender about the retransmission of the damaged and lost frames during transmission. It is a method of error detection and error correction.

1. Multiple frames
2. Sender Window = Receiver Window = 2^k-1
3. Retransmission =1
4. Cumulative and Independent acknowledgement

3.Error Control

1. Error detection :- (CRC, checksum,parity bit)
2. Error correction :- (Hamming code)

For error detection send some extra bits, eg sum of digits, or number of occurance of 1 and at receiver end calculate it again, if no change on calculated and end value so no error occurred, else notify the sender.

a.Parity bit :-

Append a single parity bit to a sequence of bits

• If using `odd’ parity, the parity bit is calculated as making the total number of 1’s in the bit sequence odd.

• If using `even’ parity, the parity bit makes the total number of 1’s in the bit sequence even.

b.Cyclic Redundancy Check (CRC) :-

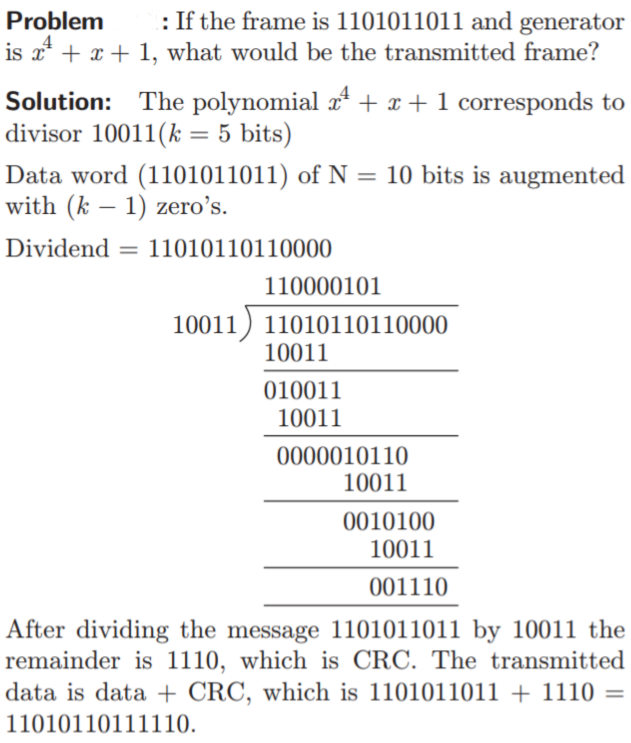
It can detect errors on large chunks of data; has low overhead; is more robust than parity bit; and requires the use of a code polynomial.

Procedure:

• Let r be the degree of the code polynomial. Append r zero bits to the end of the transmitted bit string. Call the entire bit string S(x).

• Divide S(x) by the code polynomial using modulo-2 division

• Subtract the remainder from S(x) using modulo-2 subtraction. The result is the checksummed message



Problem : If the frame is 1101011011 and generator is $x^4 + x + 1$, what would be the transmitted frame?

Solution: The polynomial $x^4 + x + 1$ corresponds to divisor 10011($k = 5$ bits)

Data word (1101011011) of N = 10 bits is augmented with $(k - 1)$ zero's.

Dividend = 11010110110000

```
         110000101
        ______________
10011 ) 11010110110000
        10011
        ______________
        010011
         10011
        ______________
         0000010110
              10011
        ______________
              0010100
                10011
        ______________
                001110
```

After dividing the message 1101011011 by 10011 the remainder is 1110, which is CRC. The transmitted data is data + CRC, which is 1101011011 + 1110 = 11010110111110.

NOTE :-

1. CRC is used in the Data Link layer.
2. Checksum is used in the transport layer (source to destination checking).

c. Hamming code :- Error correction and detection.

Hamming code is a set of error-correction codes that can be

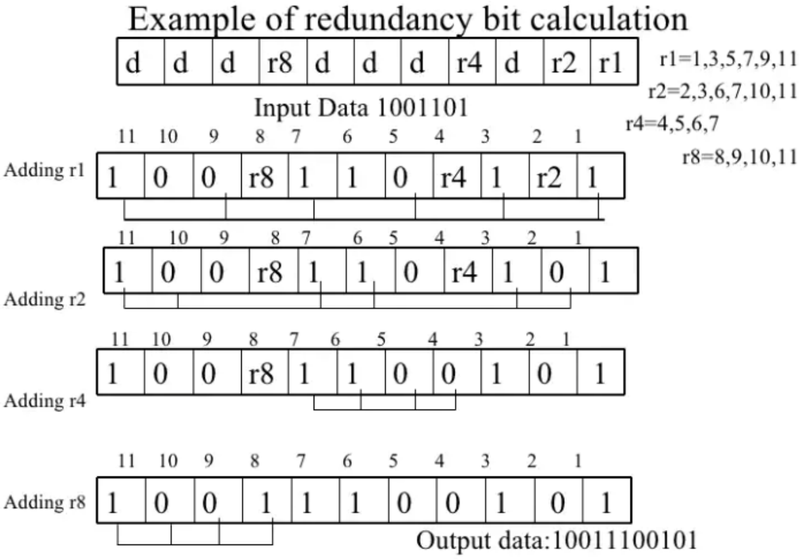
used to detect and correct the errors that can occur when the data is moved or stored from the sender to the receiver

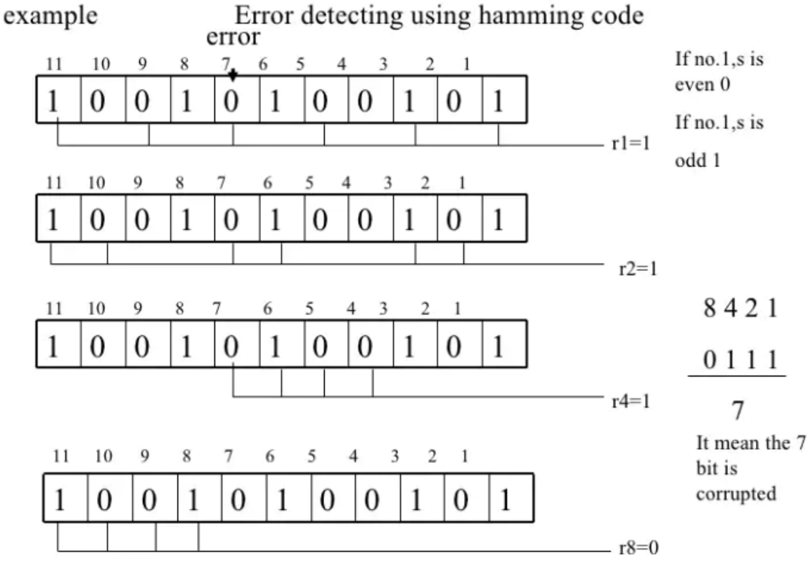
Redundant bits are extra binary bits that are generated and added to the information-carrying bits of data transfer to ensure that no bits were lost during the data transfer.

The number of redundant bits can be calculated using the following formula:

$2^r \geq m + r + 1$
where, r = redundant bit, m = data bit

1001101



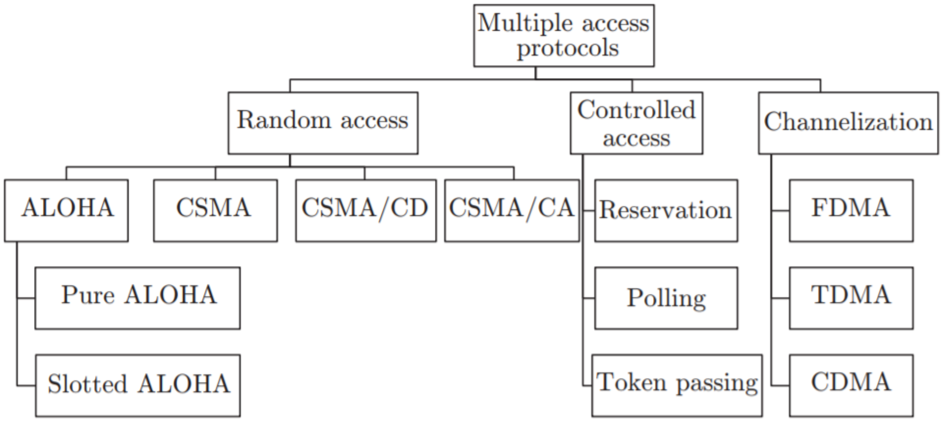


4. Access Control :- it is a mechanism that controls access of stations to a broadcast link.

Data link layer is divided into two sublayers:

1. Multiple access control sublayer: It provides controlled access to shared transmission media.

2. Logical link control sublayer: It is responsible for error and flow control.



Multiple access protocols.

1. **Pure ALOHA:** It says that whenever a station is having the data, they can send it immediately. The time at which the collision occurs is called vulnerable time.

$$\begin{aligned} T_p &= \text{Maximum propagation time} \\ &= \frac{\text{Distance between two stations}}{\text{Velocity}} \end{aligned}$$

Suppose T_{fr} is the average transmission time for a frame, then

$$T_{fr} = \frac{\text{Frame size}}{\text{Bandwidth}} = G$$

$$\text{Throughput } (S) = G \times e^{-2G}$$

$$\text{Vulnerable time} = 2 \times T_{fr}$$

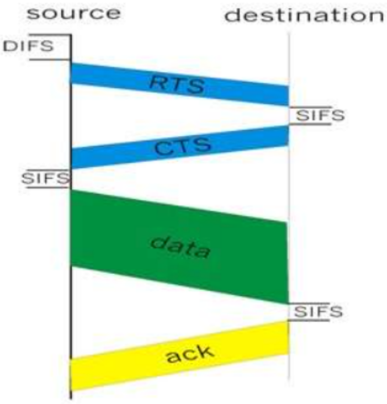
$$S_{\max} = 18.4\%$$

2. **Slotted ALOHA :-** It says that if stations are ready with the data, they have to wait for the required time slot and can transmit data exactly at that time slot.

3. **CSMA (Carrier Sense Multiple Access):** If a station is ready with the data, it senses the channel, and if channel is found idle, data is transmitted, otherwise the station has to wait for a random amount of time.

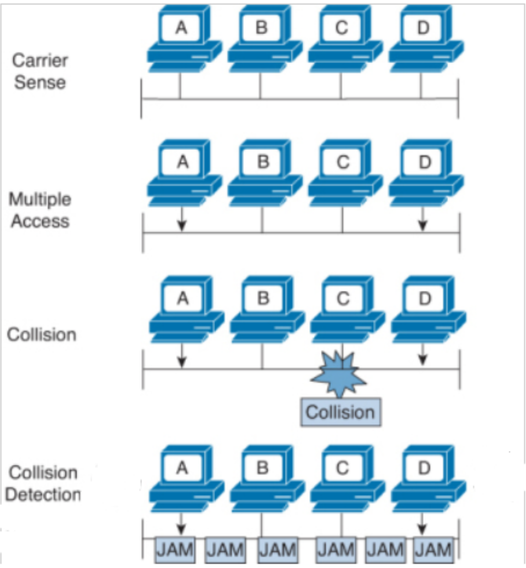
Persistent CSMA :- retry immediately with probability p when channel becomes idle.

Non Persistent CSMA :- retry after random interval.



CSMA-CA

CSMA /CD



3. NETWORK LAYER

The network layer is responsible for host-to-host delivery and path selection between end systems (routing). The fragmentation, reassembly and translation between different network types are also performed at this layer. In other words, communication between nodes is possible in different networks through this layer.

1. Host to host data transfer (from one network to other)
2. Uses IP address (Logical Address)
3. Routing (select path)
4. The network layer receives the data from the upper layer and converts the data into packets. This process is known as packetizing.

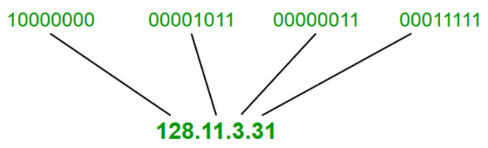
Packet delivery can be accomplished by using either a connection-oriented or a connectionless network service. In a connection-oriented protocol, the connection is established before sending the packets so the route is established before and all the packets have to follow that route. Example: Frame relay and ATM use this service.

In connectionless protocols, the network layer protocol treats each packet independently. The packets in a message may or may not follow the same path to their destination. For example, the Internet uses this type of service.

Classful Addressing of IP Address

IP address is an address having information about how to reach a specific host, especially outside the LAN. An IP address is a 32 bit unique address having an address space of 232.

Generally, there are two notations in which an IP address is written, dotted decimal notation and hexadecimal notation.

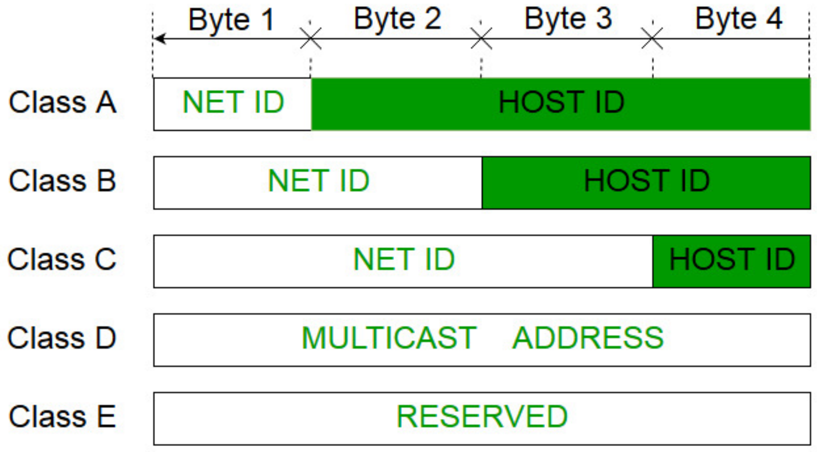


IP ADDRESS

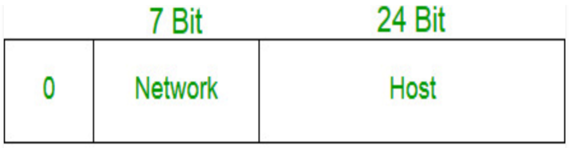
IPv4 address is divided into two parts:

1. Network Id 2. Host Id

The class of IP address is used to determine the bits used for network ID and host ID and the number of total networks and hosts possible in that particular class.



1. **Class A:-**



Network Id :- 7 bit (0 to 127)

Number of networks :- 128 in actual 126
2^7-2= 126 network ID(Here 2 address is subtracted because 0.0.0.0 and 127.x.y.z are special address.)

Number of Host possible :- 2^24

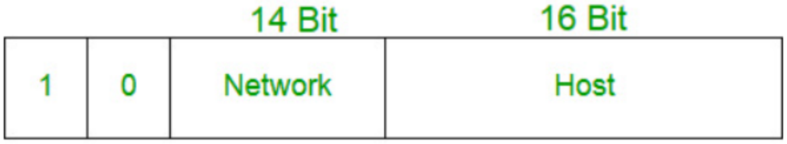
But 64.0.0.0 -> used of representing address of network

64.255.255.255-> used for broadcasting

So in real Host count = 2^24-2

Subnet Mask :- If you want to know to which network this IP address belongs , use the default subnet mask.
Class A default Subnet Mask = 255.0.0.0

2. **Class B:-**



Range = 128 -191

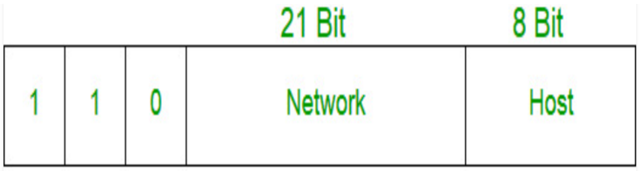
Number of networks= 2^14

Number of hosts = 2^16-2

No of address :- 2^30

Mask =255.255.0.0

3. **Class C:-**



Range = 192-223

Number of networks= 2^21

Number of hosts = 2^8-2

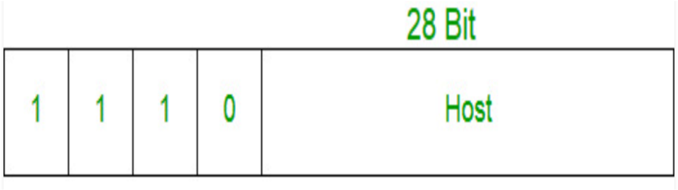
No of address :- 2^29

Mask =255.255.255.0

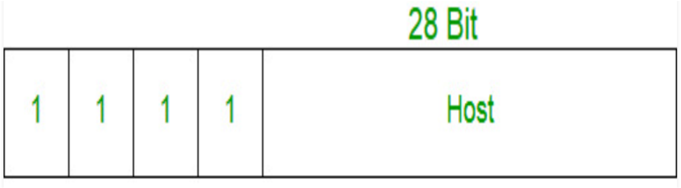
4. **Class D:-**

IP addresses belonging to class D are reserved for multicasting. The higher order bits of the first octet of IP addresses belonging to class D are always set to 1110. The remaining bits are for the address that interested hosts recognize.

Class D does not possess any subnet mask. IP addresses belonging to class D range from 224.0.0.0 – 239.255.255.255.



5. **Class E:-**
   IP addresses belonging to class E are reserved for experimental and research purposes. IP addresses of class E range from 240.0.0.0 – 255.255.255.254. This class doesn’t have any subnet mask. The higher order bits of the first octet of class E are always set to 1111.



Classless Addressing of IP Address

No classes , only blocks

Representation : - x.y.z.w / n

n=mask / number of bit representing network block

Eg :- 200.100.20.40/28

So mask will have 28 1's

mask=11111111.11111111.11111111.11110000

IP=   200   .   100   .20   .00101000 -> (40)

Xor them to get network

Belongs to 200.100.20.32/28 network

Supernetting is a part of classless addressing. In classless addressing, the addresses should be contiguous in a block. The first address should be exactly divisible by the number of addresses in a block. In supernet, bits are borrowed from netid. Rules of supernetting:

1. The number of blocks must be a power of 2.

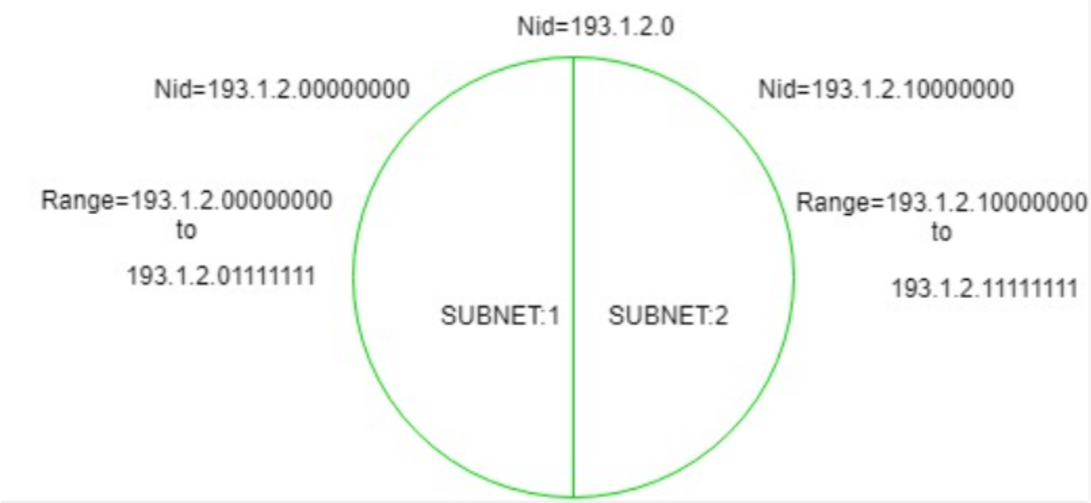
2. The blocks must be continuous in the address space.

3. The third octet of the first address in the superblock must be exactly divisible by the number of blocks.

Subnetting

FOR CLASSFUL ADDRESSING

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.



Basically to divide the network into 2 parts, fix a bit.

For above example:

1. SUBNET 1 :-

Range :- 193.1.2.0 - 193.1.2.127

Valid IP’s :- 126 (since again 2 address are reserved, one to address network and one for broadcast)

Subnet Mask : -255.255.255.0

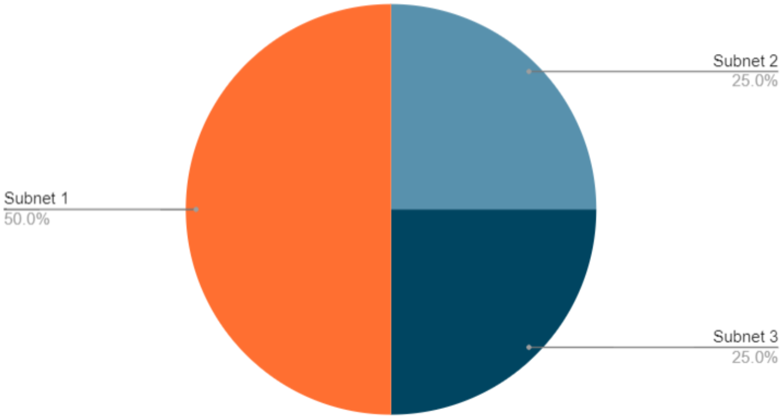
2. SUBNET 2 :-

Range :- 193.1.2.128 - 193.1.2.255

Valid IP’s :- 126

Subnet Mask :- 255.255.255.128

FOR CLASSFUL ADDRESSING (Variable length subnet masking)



Consider network id :- 200.10.20.0 (Class C)

To divide in 2 parts, reserve 1 bit.

Subnet 1:-

200.10.20.0_ _ _ _ _ _ _ (this 0 is fixed)

Range :- 200.10.20.0 to 200.10.20.127

Total usable :- 128-2 =126

Subnet 2:-

200.10.20.10_ _ _ _ _ _ (10 ,2 bits are fixed)

Range :- 200.10.20.128 to 200.10.20.191

Total usable :- 64-2 = 62

Subnet 3:-

200.10.20.11_ _ _ _ _ _ (11, 2 bits are fixed)

Range :- 200.10.20.192 to 200.10.20.255

Total usable :- 64-2 = 62

Subnetting in Classless Interdomain Routing (CIDR)

Step 1:-

If given host Id -> convert to network Id

Eg:- 195.10.20.129/26 -> 195.10.20.128/26 (using subnet mask)

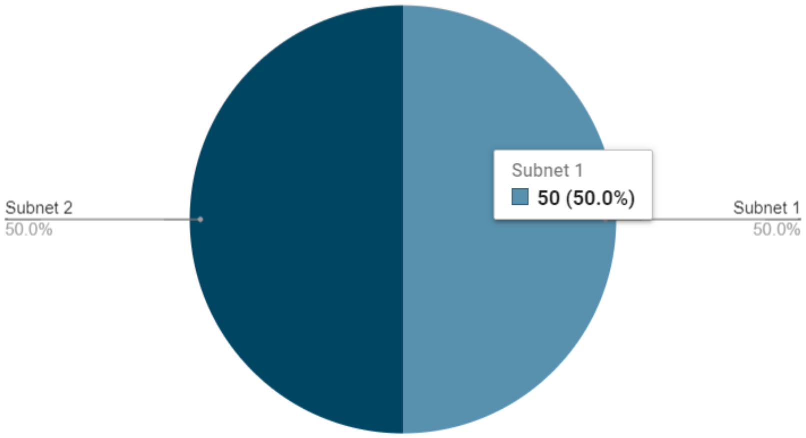
Step 2:-

For subnetting, fix 1+mask bits, fix 1 bit to divide in 2 parts.

Since 26 bits are fixed we get:- 195.10.20.10 000000 (this last 6 bits can vary only)

Step 3:-

Fix one more bit from unfixed bits to divide network in 2 parts



Subnet 1:-

After fixing 1 more bit we get :- 193.10.20.100 00000

Range :- 195.10.20.128 to 195.10.20.159

Subnet 2:-

195.10.20.111 00000

Range :- 195.10.20.160 to 195.10.20.191

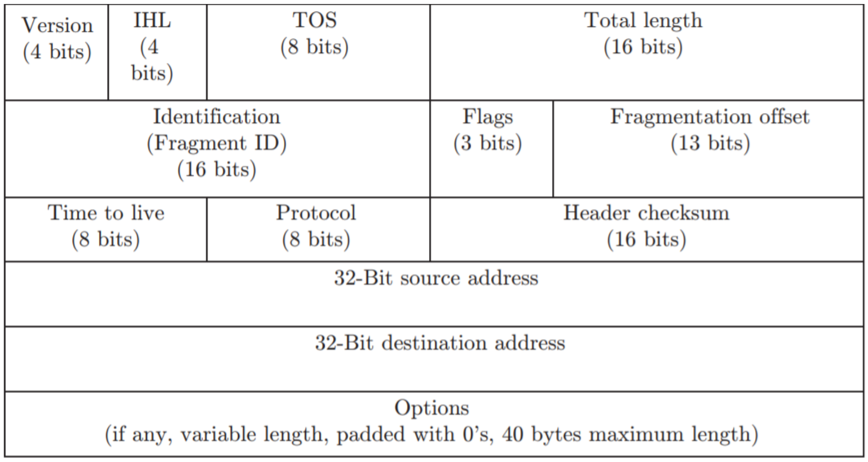
MASK :- 255.255.255.11100000 /27 (Since 27 bits are fixed)

= 255.255.255.224

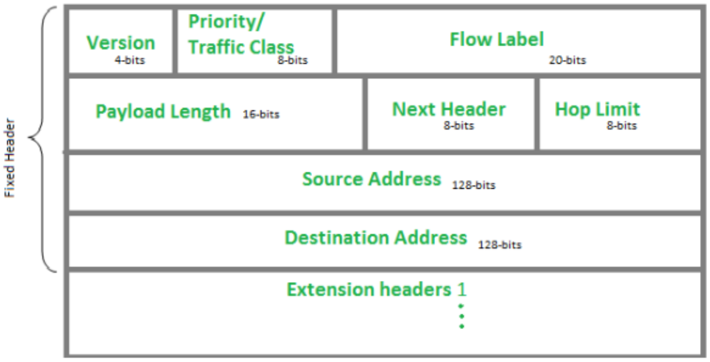
Network layer protocols

In the Internet model, or the TCP/IP suite, there are five main network layer protocols: ARP, RARP, IP, ICMP and IGMP.The main protocol in this layer is IP. It is responsible for host to host delivery of packets from a source to destination. IP needs services of other protocols for better network performance. IP needs ARP to find the MAC address of the next hop. As IP is an unreliable protocol, it needs ICMP (Internet Control Message Protocol) to handle unusual situations and errors. IGMP (Internet Group Message Protocol) is used for multicast delivery.

IPv4 header



<table>
<tr><td>Version
(4 bits)</td><td>IHL
(4
bits)</td><td>TOS
(8 bits)</td><td colspan="2">Total length
(16 bits)</td></tr>
<tr><td colspan="3">Identification
(Fragment ID)
(16 bits)</td><td>Flags
(3 bits)</td><td>Fragmentation offset
(13 bits)</td></tr>
<tr><td colspan="2">Time to live
(8 bits)</td><td>Protocol
(8 bits)</td><td colspan="2">Header checksum
(16 bits)</td></tr>
<tr><td colspan="5">32-Bit source address</td></tr>
<tr><td colspan="5">32-Bit destination address</td></tr>
<tr><td colspan="5">Options
(if any, variable length, padded with 0’s, 40 bytes maximum length)</td></tr>
</table>



<table>
<tr><td>Version
4-bits</td><td>Priority/
Traffic Class
8-bits</td><td colspan="3">Flow Label
20-bits</td></tr>
<tr><td colspan="2">Payload Length 16-bits</td><td>Next Header
8-bits</td><td colspan="2">Hop Limit
8-bits</td></tr>
<tr><td colspan="5">Source Address 128-bits</td></tr>
<tr><td colspan="5">Destination Address 128-bits</td></tr>
<tr><td colspan="5">Extension headers 1
⋮</td></tr>
</table>

. IPv6 Header

4. Transport Layer

Responsible for process to process delivery of the entire message.It delivers the message through the network and provides error checking so that no error occurs during the transfer of data.The standard protocols used by Transport Layer to enhance its functionalities are TCP(Transmission Control Protocol), UDP(User Datagram Protocol), DCCP(Datagram Congestion Control Protocol) etc.

Services :-

1. **Process to process delivery –**Transport Layer requires a Port number to correctly deliver the segments of data to the correct process amongst the multiple processes running on a particular host. A port number is a 16 bit address used to identify any client-server program uniquely.
2. **End-to-end Connection between hosts –**The transport layer is also responsible for creating the end-to-end Connection between hosts for which it mainly uses TCP and UDP. TCP is a secure, connection- orientated protocol which uses a handshake protocol to establish a robust connection between two end- hosts. TCP ensures reliable delivery of messages and is used in various applications. UDP, on the other hand, is a stateless and unreliable protocol which ensures best-effort delivery. It is suitable for the applications which have little concern with flow or error control and requires to send the bulk of data like video conferencing. It is often used in multicasting protocols.
3. **Multiplexing and Demultiplexing –**Multiplexing allows simultaneous use of different applications over a network which is running on a host. The transport layer provides this mechanism which enables us to send packet streams from various applications simultaneously over a network.
4. **Congestion Control –**Congestion is a situation in which too many sources over a network attempt to send data and the router buffers start overflowing due to which loss of packets occur. As a result, retransmission of packets from the sources increases the congestion further.
5. **Data integrity and Error correction –**Transport layer checks for errors in the messages coming from application layer by using error detection codes, computing checksums, it checks whether the received data is not corrupted and uses the ACK and NACK services to inform the sender if the data has arrived or not and checks for the integrity of data.
6. **Flow control –**

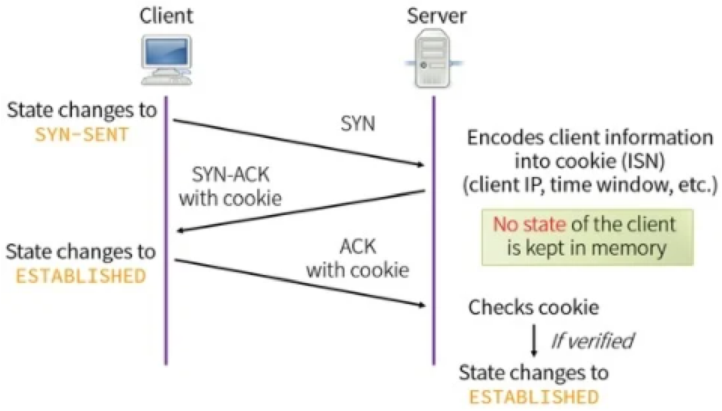
   The transport layer provides a flow control mechanism between the adjacent layers of the TCP/IP model. TCP also prevents data loss due to a fast sender and slow receiver by imposing some flow control techniques. It uses the method of sliding window protocol which is accomplished by the receiver by sending a window back to the sender informing the size of data it can receive.

TCP is a connection-oriented protocol. Connection-orientation means that the communicating devices should establish a connection before transmitting data and should close the connection after transmitting the data.

UDP is the Datagram oriented protocol. This is because there is no overhead for opening a connection, maintaining a connection, and terminating a connection. UDP is efficient for broadcast and multicast type of network transmission.

Three way handshake:-

It is used by TCP to make connections.


Client
Server
State changes to SYN-SENT
SYN
Encodes client information into cookie (ISN) (client IP, time window, etc.)
SYN-ACK with cookie
No state of the client is kept in memory
State changes to ESTABLISHED
ACK with cookie
Checks cookie
If verified
State changes to ESTABLISHED

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.

5. Session Layer

The services provided by session layer are as follows:

1. Establishes, manages and terminates a communication session with remote systems
2. Allows two machines to enter into a dialog (communication may be half duplex or full duplex)
3. Adds checkpoints or synchronisation points to a data stream.
4. Groups several user-level connections into a single `session'.

Some protocol suites do not include the session layer.

Checkpoint: If we need a file of 1000 pages, it is suggested to insert checkpoints after every 100 pages to ensure that each 100-page unit is received and acknowledged independently. Meanwhile, if a crash occurs during the transmission of page 324, the only pages that need to be resent after system recovery are pages 301 to 324. The pages from 1 to 300 need not be resent.

6. Presentation Layer

The following are the major concerns of presentation layer:

1. Syntax and semantics of the information exchanged between two systems.
2. Support to different encoding schemes used by different machines. It converts the sender-dependent format into a common format and the receiver converts it back to the receiver-dependent format.
3. Data encryption–to ensure privacy, sensitive information should be encrypted. Information encrypted to some other form is unreadable to others.
4. Data compression–to reduce the size of information to carry. In the case of multimedia, for example, text, audio and video, compression is a very useful tool.

7. Application Layer

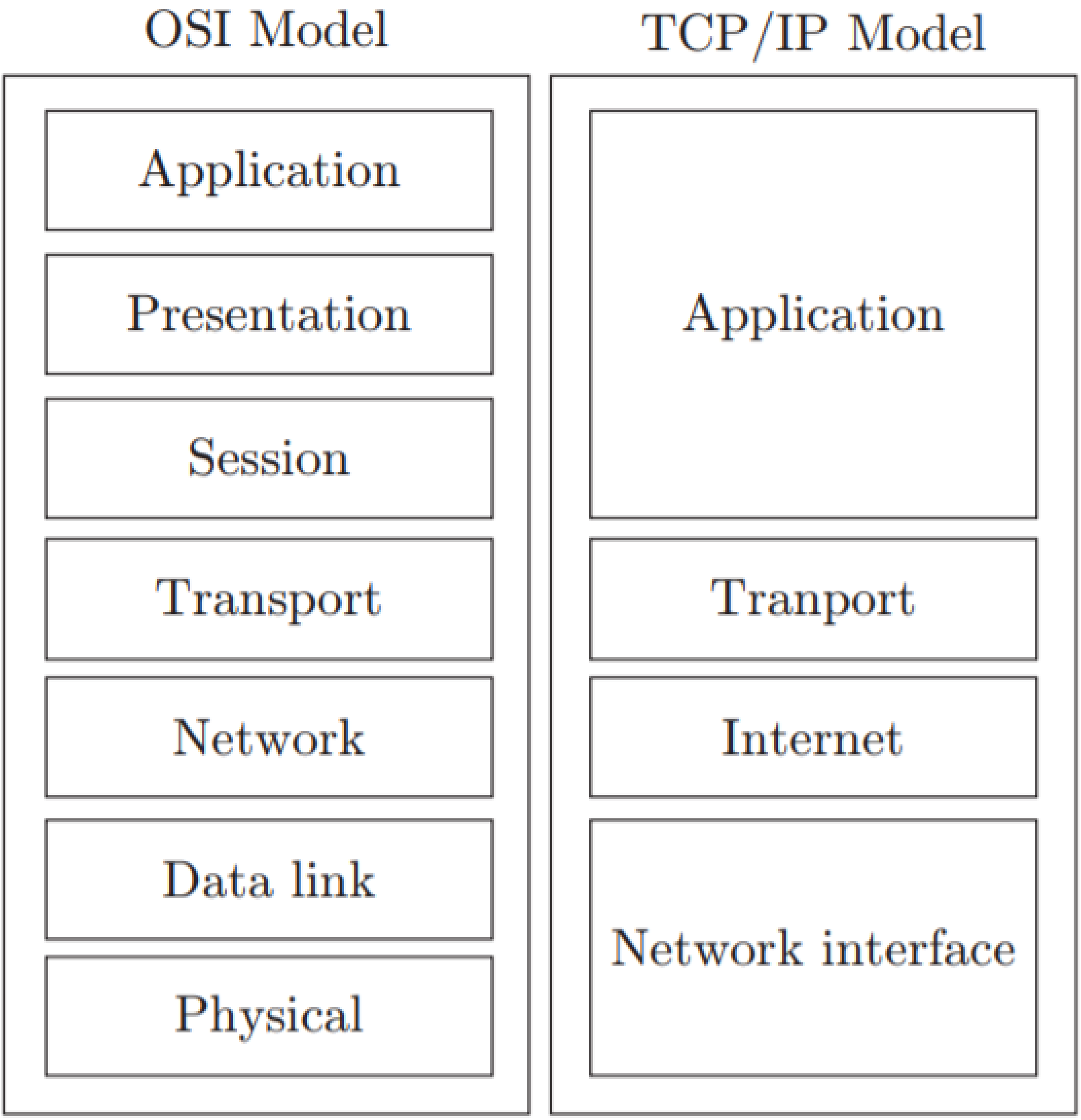
This layer is for applications which are involved in communication systems.

The major responsibility of the application layer is to implement communication between two applications of the same type. There is a common misconception that every user application runs on an application layer, but it runs only on those applications which interact with the communication system. For example, FTP, HTTP, SMTP/ POP3/IMAP (email)are all application layer protocols, but a designing software or text editor cannot be considered as an application layer protocol.

Hypertext Transfer Protocol (HTTP): HTTP is used to access data on the World Wide Web (WWW). It works as a combination of FTP and SMTP. Unlike FTP, HTTP does not have any control connection and uses only one TCP connection. Unlike SMTP, it does not store and then forward the messages. It immediately sends the messages. HTTP uses a TCP **Port 80**.

File Transfer Protocol (FTP): It is used for transferring files from one system to another. FTP establishes two connections between hosts, one for data transfer and the other for control information. FTP uses TCP **Port 21** for the control connection and TCP **Port 20** for the data connection.

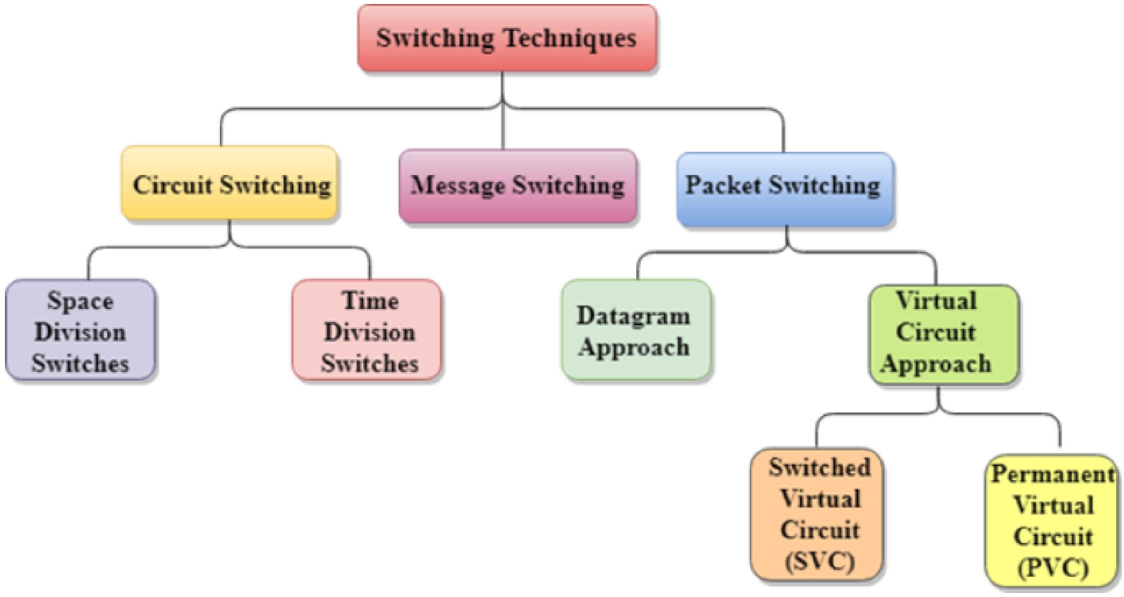
TCP / IP model


OSI Model
TCP/IP Model
Application
Presentation
Session
Transport
Network
Data link
Physical
Application
Tranport
Internet
Network interface

Switching Techniques

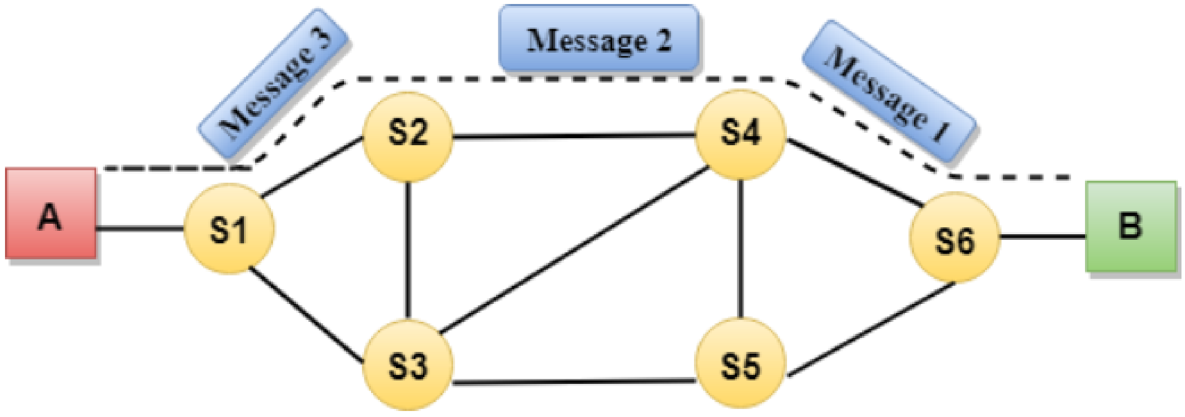
Switching in a computer network helps in deciding the best route for data transmission if there are multiple paths in a larger network.

Classification Of Switching Techniques



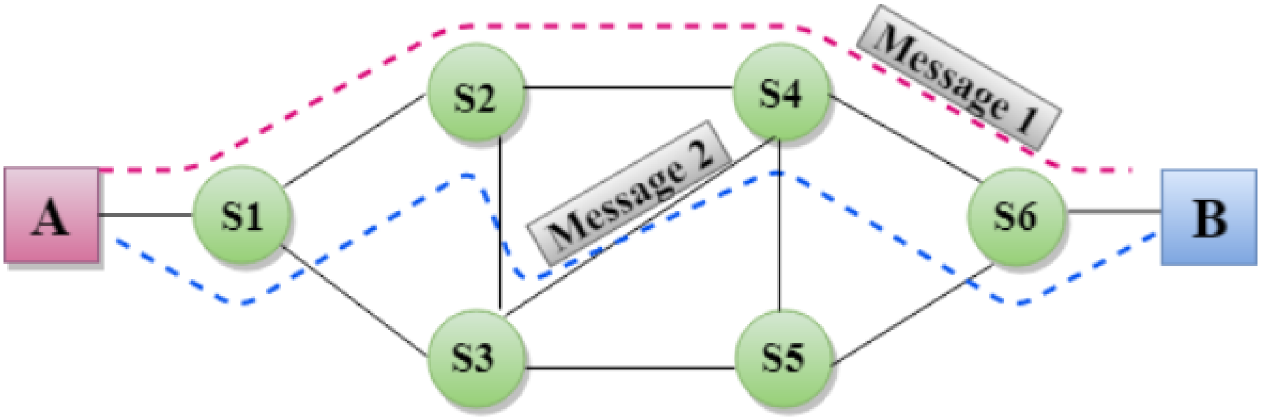
1.Circuit Switching

- A dedicated path is established between sender and receiver.
- Before data transfer, connection will be established first. Eg Telephone network.
- Works in 3 phase 1) connection establishment 2) Data transfer 3)Connection disconnection



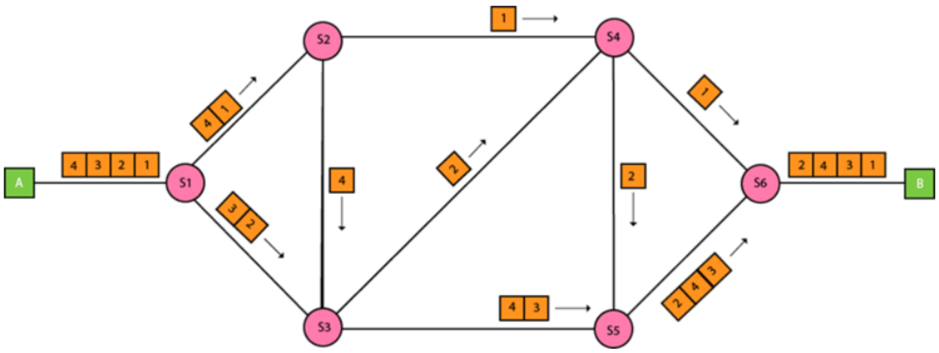
2.Message Switching

- Message Switching is a switching technique in which a message is transferred as a complete unit and routed through intermediate nodes at which it is stored and forwarded.
- In Message Switching technique, there is no establishment of a dedicated path between the sender and receiver.
- The destination address is appended to the message. Message Switching provides a dynamic routing as the message is routed through the intermediate nodes based on the information available in the message
- Each and every node stores the entire message and then forwards it to the next node. This type of network is known as **store and forward network.**
- Message switching treats each message as an independent entity.



3.Packet Switching

- The Internet is a packet switched network.
- Message is broken into individual chunks called packets.
- Each packet is sent individually.
- Every packet contains some information in its headers such as source address, destination address and sequence number.
- Packets are given a unique number (sequence number) to identify their order at the receiving end.



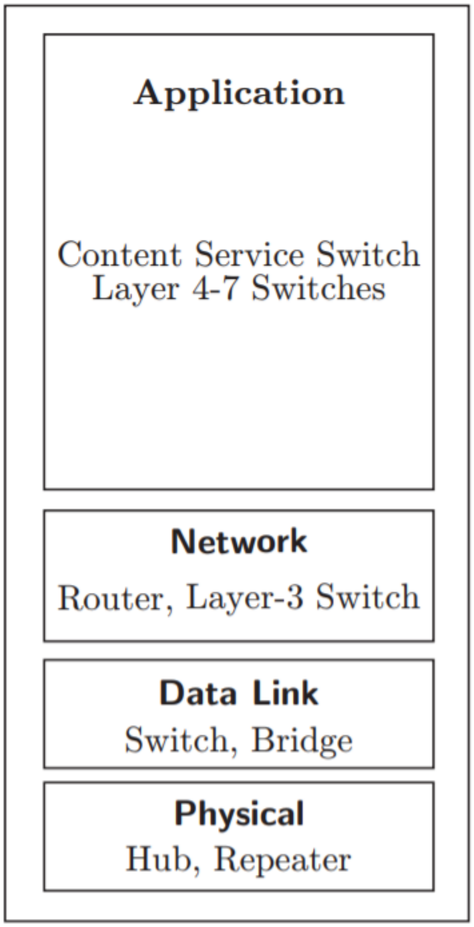
Sequence number will help receiver to

1. Record the packets
2. Detect the missing packets
3. Send Acknowledgements

2 Approaches for packet switching :-

1. **DATAGRAM APPROACH** :- Also known as connectionless switching , each independent entity is called datagram. Datagram contains destination info and intermediary devices uses this info to forward datagrams to the right destination.In datagram packet switching , path is not fixed.
2. **VIRTUAL CIRCUIT APPROACH** :- Also known as connection-oriented switching. A pre-planned route is established before a message is sent. In this approach, the path is fixed for duration of logical connection.

Networking Devices



Cables, repeaters and hubs are just hardware with no software in them. While bridges, switches and routers have software so they can make decisions.

Modem :- used for analog to digital conversion and vice-versa.

1. **Repeaters** :-
    - Operates on a physical layer.
    - Data signals generally become too weak or corrupted if they tend to travel a long distance. Repeaters regenerate signals over the same network.
    - It is pure hardware.
    - It does not amplify the signal.
    - Repeaters can do filter (remove unwanted signals)
    - It is a 2 port device.

2. **Hub :-**
    - Works like multiport repeater, works on physical layer.
    - Used to set up LANs, in star topology
    - When a packet arrives at one port, it is copied to other ports so that all segments of LAN .
3. **Bridges :-**
    - There is a limited number of stations that can be connected with a single LAN. So, a bridge is used to connect multiple LANs of the same type.
    - It operates on a physical layer and data link layer
4. **Switch :-**
    - Switch is a small network device used to connect one or more computers through LAN.
    - Hub is a broadcast device which sends data from one pc to all but switch is a multicast device which sends data to a particular pc you want.
    - Switches and hubs are used in the same network. Hubs increase the network by providing more ports, and switches divide the whole network into smaller networks.
    - Unlike hub, switch has memory. Stores MAC address.
    - Works on data link layer
5. **Router :-**
    - A router is a networking device which takes packets from one network and after analysis sends that packet to another network
    - A router is connected to at least 2 networks, commonly 2 LAN or WAN or LAN and its ISP (internet service provider) network.
    - Stores routing table, store and forward method.
    - Decision taken based on IP address.