

LECTURE NOTES ON

DATA COMMUNICATION AND COMPUTER NETWORK

4TH SEMESTER E&TC



Prepared by:NUSHRAT BARI

GOVERNMENT POLYTECHNIC, DHENKANAL

DEPARTMENT OF ELCTRONICS AND TELECOMMUNICATION ENGINEERING

Switching & Routing

Circuit Switching networks

Packet Switching principles

X.25

Routing in Packet switching

Congestion

Effects of congestion, congestion control

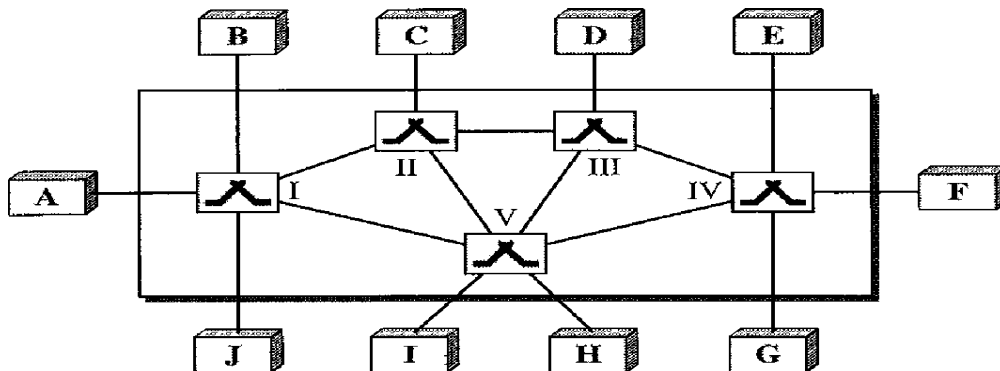
Traffic Management

Congestion Control in Packet Switching Network.

SWITCHING:

@ A switched network consists of a series of interlinked nodes, called switches. Switches are devices capable of creating temporary connections between two or more devices linked to the switch.

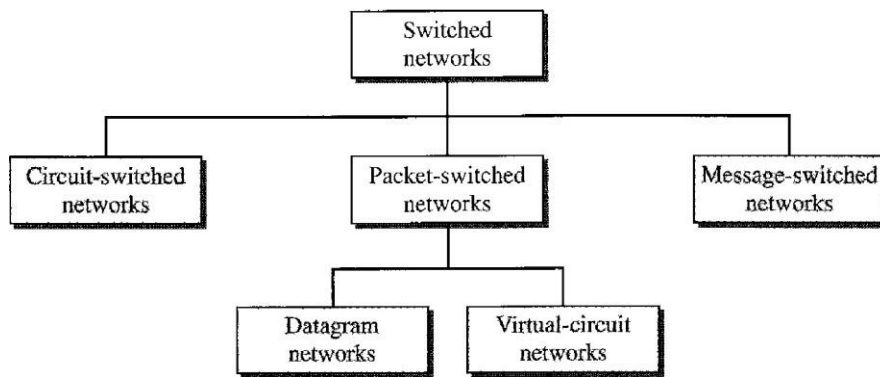
@ The process by which data are transmitted from one node to the other via a switched network is called switching.



The end systems (communicating devices) are labeled A, B, C, D, and so on, and the switches are labeled I, II, III, IV, and V. Each switch is connected to multiple links.

TYPES:

1. Circuit switching
2. Packet switching
3. Message switching.



CIRCUIT-SWITCHED NETWORKS

- 1. A circuit-switched network consists of a set of switches connected by physical links.*
- 2. A connection between two stations is a dedicated path made of one or more links.*
- 3. However, each connection uses only one dedicated channel on each link. Each link is normally divided into n channels by using FDM or TDM.*
- 4. Circuit switching takes place at the physical layer.*
- 5. Data transferred between the two stations are not packetized (physical layer transfer of the signal). The data are a continuous flow sent by the source station and received by the destination station, although there may be periods of silence.*
- 6. There is no addressing involved during data transfer. The switches route the data based on their occupied band (FDM) or time slot (TDM). Of course, there is end-to-end addressing used.*

Three Phases

The actual communication in a circuit-switched network requires three phases: connection setup, data transfer, and connection teardown.

Setup Phase

Before the two parties (or multiple parties in a conference call) can communicate, a dedicated circuit (combination of channels in links) needs to be established. The end systems are normally connected through dedicated lines to the switches, so connection setup means creating dedicated channels between the switches.

Data Transfer Phase

After the establishment of the dedicated circuit (channels), the two parties can transfer data.

Teardown Phase

When one of the parties needs to disconnect, a signal is sent to each switch to release the resources.

PACKETSWITCHED NETWORK

In this switching network data are transmitted in discrete units called packets.

- 1. The problems associated with circuit switching like non voice and data transmission problem were successfully overcome in packet switching.*
- 2. In packet switching there is no resource allocation for the packets. The allocation is done on first come first serve basis.*
- 3. There are two popular approaches for packet switching.*

Datagram approach

@ Virtual circuit approach

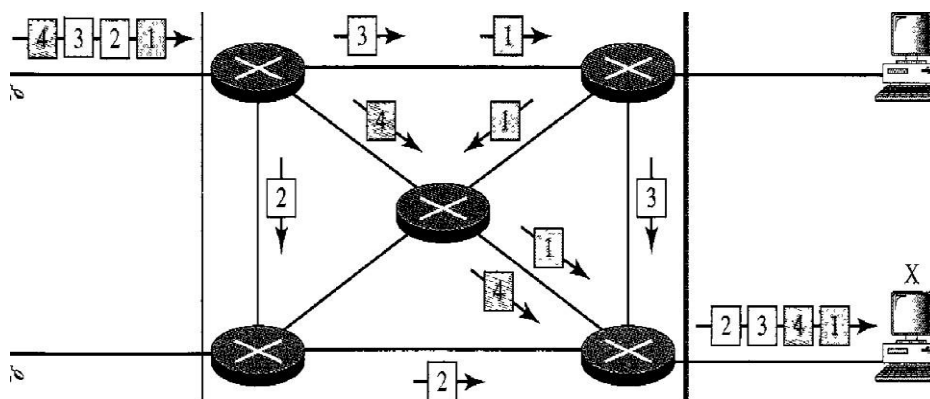
DATAGRAM NETWORKS

1. In a datagram network, each packet is treated independently of all others. Even if a packet is part of a multipacket transmission, the network treats it as though it existed alone. Packets in this approach are referred to as datagrams.

2. Datagram switching is normally done at the network layer.

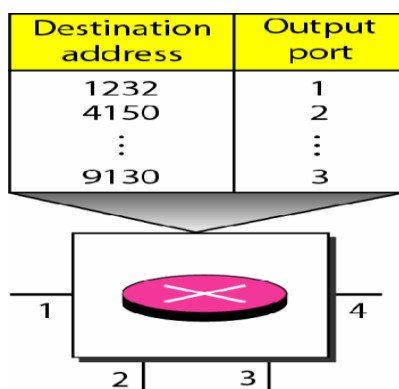
3. The switches in a datagram network are traditionally referred to as routers.

4. The datagram networks are sometimes referred to as connectionless networks. The term ~~connectionless~~ here means that the switch (packet switch) does not keep information about the connection state. There are no setup or teardown phases. Each packet is treated the same by a switch regardless of its source or destination.



Routing Table

- Each packet switch has a routing table which is based on the destination address.
- The routing tables are dynamic and are updated periodically.
- The destination addresses and the corresponding forwarding output ports are recorded in the tables.
- The destination address in the header of a packet in a datagram network remains the same during the entire journey of the packet.
- When the switch receives the packet, this destination address is examined; the routing table is consulted to find the corresponding port through which the packet should be forwarded.



Efficiency

- Better than that of a circuit-switched network.
- Resources are allocated only when there are packets to be transferred. If a source sends a packet and there is a delay of a few minutes before another packet can be sent, the resources can be reallocated during these minutes for other packets from other sources.
- Switching in the Internet is done by using the datagram approach to packet switching at the network layer

VIRTUAL-CIRCUIT NETWORKS

A virtual-circuit network is a cross between a circuit-switched network and a datagram network. It has some characteristics of both.

- 1. As in a circuit-switched network, there are setup and teardown phases in addition to the data transfer phase.*
- 2. Resources can be allocated during the setup phase, as in a circuit-switched network, or on demand, as in a datagram network.*
- 4. As in a circuit-switched network, all packets follow the same path established during the connection.*
- 5. A virtual-circuit network is normally implemented in the data link layer, while a circuit-switched network is implemented in the physical layer and a datagram network in the network layer. But this may change in the future.*

Addressing In a virtual-circuit network,

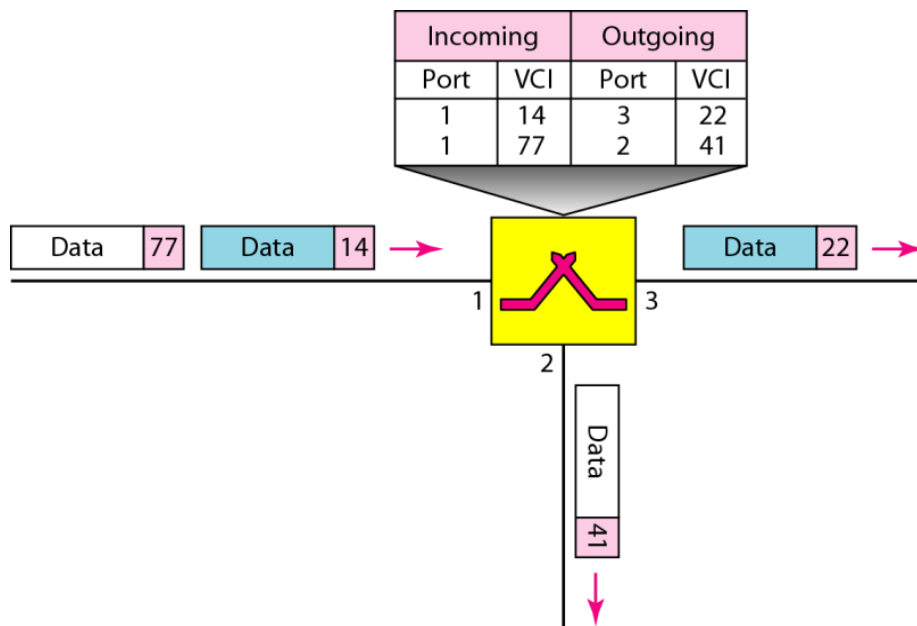
It has two types of addressing are involved: global and local (virtual-circuit identifier).

Global Addressing:

A source or a destination needs to have a global address, an address that can be unique in the scope of the network or internationally if the network is part of an international network.

Virtual-Circuit Identifier:

The identifier that is actually used for data transfer is called the virtual-circuit identifier (VCI). A VCI, unlike a global address, is a small number that has only switch scope; it is used by a frame between two switches. When a frame arrives at a switch, it has a VCI; when it leaves it has a different VCI.



Three Phases

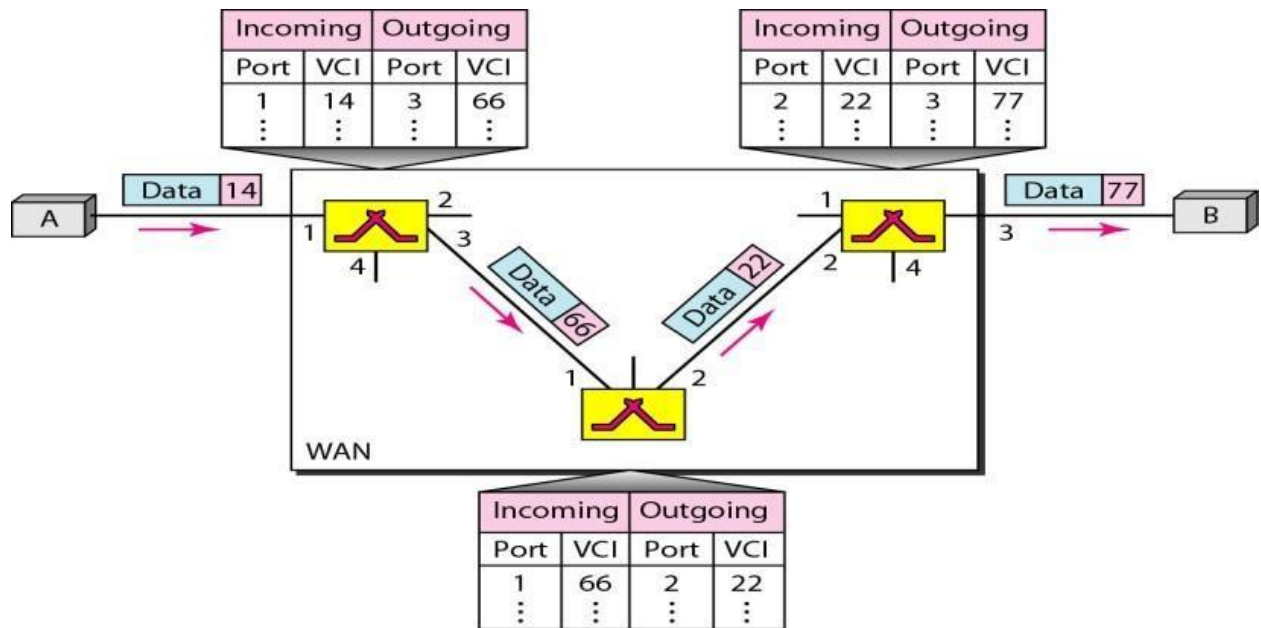
As in a circuit-switched network, a source and destination need to go through three phases in a virtual-circuit network: setup, data transfer, and teardown.

Setup phase

In the setup phase, the source and destination use their global addresses to help switches make table entries for the connection.

Data Transfer Phase and teardown phase

- To transfer a frame from a source to its destination, all switches need to have a table entry for this virtual circuit.
- The table, in its simplest form, has four columns. This means that the switch holds four pieces of information for each virtual circuit that is already set up.
- The data transfer phase is active until the source sends all its frames to the destination. The process creates a virtual circuit, not a real circuit, between the source and destination.
- After sending all frames, a special frame is sent to end the connection.
- Destination B responds with a teardown confirmation frame.



Differences between Circuit switching and Packet switching

CIRCUIT SWITCHING	PACKET SWITCHING
1. In circuit switching a message path or data communication path or channel or circuit is dedicated to an entire message .	1. In this switching network data are transmitted in discrete units called as packets.
2. Circuit-switching is more reliable than packet-switching	2. Packet-switching is less reliable than circuit-switching
3. circuit switching statically reserves the required bandwidth	3. packet switching acquires & releases it as it is needed
4. In circuit switching, path is dedicated for the transmission.	4. In packet switching, route can be shared for different transmission.
5. With circuit switching any unused bandwidth on a allocated circuit is just wasted.	5. with packet switching any unused bandwidth may be utilized by other packets
6. Circuit switching is old and expensive.	6. Packet switching is more modern.

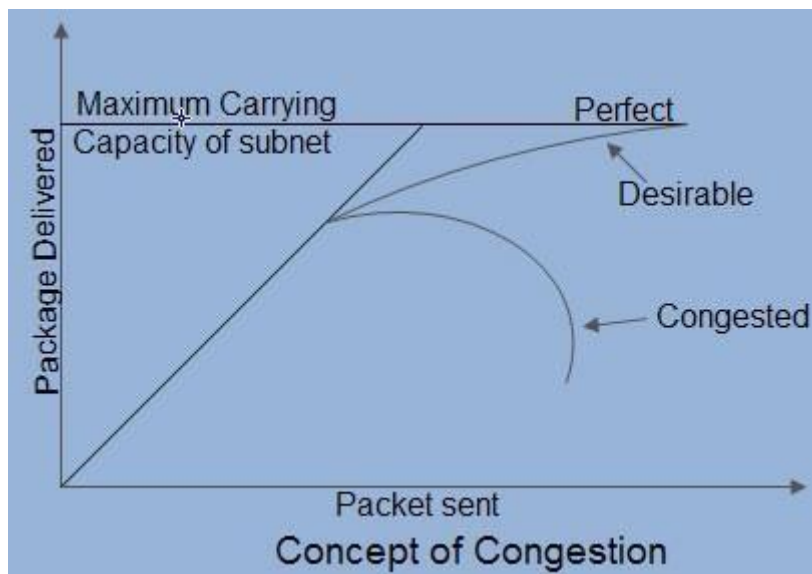
Difference between datagram and virtual circuit approach

Datagram	Virtual circuit
Connection setup is not	Connection setup is initially required prior to sending

<i>required</i>	<i>data</i>
<i>Packet contains full source and destination address</i>	<i>Packet contains short virtual circuit number identifier.</i>
<i>None other than router table containing destination network</i>	<i>Each virtual circuit number entered to table on setup, used for routing.</i>
<i>Packets routed independently</i>	<i>Route established at setup, all packets follow same route.</i>
<i>It does not affect if any router fails except those packets lost during crash.</i>	<i>All virtual circuits passing through failed router terminated.</i>
<i>Difficult since all packets routed independently router resource requirements can vary.</i>	<i>Simple by pre-allocating enough buffers to each virtual circuit at setup, since maximum number of circuits fixed.</i>

Congestion

Congestion is an important issue that can arise in packet switched network. Congestion is a situation in Communication Networks in which too many packets are present in a part of the subnet, performance degrades. Congestion in a network may occur when the load on the network (the number of packets sent to the network) is greater than the capacity of the network (i.e. the number of packets a network can handle.)

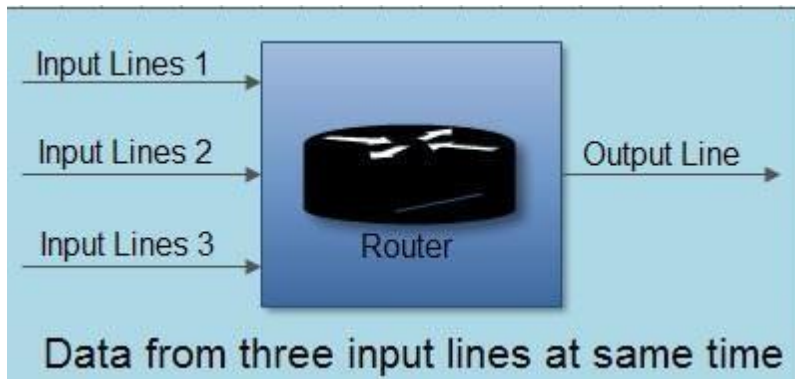


Causing of Congestion:

The various causes of congestion in a subnet are

1. The input traffic rate exceeds the capacity of the output lines. If suddenly, a stream of packets start arriving on three or four input lines and all need the same output line. In this case, a queue will be built up. If there is insufficient memory to hold all the packets, the packet will be lost. Increasing the memory to unlimited size does not solve the

problem.



2. The routers are too slow to perform bookkeeping tasks (queuing buffers, updating tables, etc.).

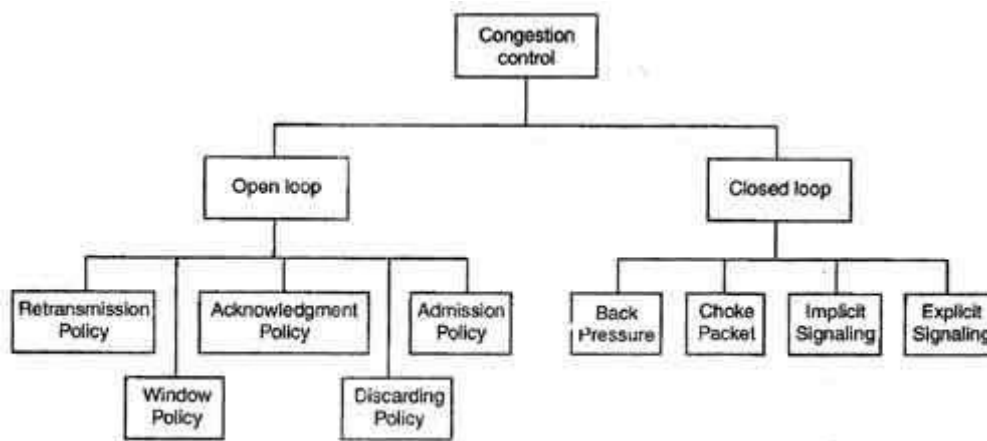
3. The routers' buffer is too limited.

4. Congestion in a subnet can occur if the processors are slow. Slow speed CPU at routers will perform the routine tasks such as queuing buffers, updating table etc slowly. As a result of this, queues are built up even though there is excess line capacity.

5. Congestion is also caused by slow links. This problem will be solved when high speed links are used. But it is not always the case. Sometimes increase in link bandwidth can further deteriorate the congestion problem as higher speed links may make the network more unbalanced. Congestion can make itself worse.

Congestion Control Technique

Congestion Control refers to techniques and mechanisms that can either prevent a congestion, before it happens, or remove congestion, after it has happened. Congestion control mechanisms are divided into two categories, one category prevents the congestion from happening and the other category removes congestion after it has taken place.



Types of Congestion Control Methods

These two categories are:

1. Open loop
2. Closed loop

Open Loop Congestion Control

- In this method, policies are used to prevent the congestion before it happens.
- Congestion control is handled either by the source or by the destination.
- The various methods used for open loop congestion control are:

1. Retransmission Policy

- The sender retransmits a packet, if it feels that the packet it has sent is lost or corrupted.
- However retransmission in general may increase the congestion in the network. But we need to implement good retransmission policy to prevent congestion.
- The retransmission policy and the retransmission timers need to be designed to optimize efficiency and at the same time prevent the congestion.

2. Window Policy

- To implement window policy, selective reject window method is used for congestion control.
- Selective Reject method is preferred over Go- back- n window as in Go- back- n method, when timer for a packet times out, several packets are resent, although some may have arrived safely at the receiver. Thus, this duplication may make congestion worse.
- Selective reject method sends only the specific lost or damaged packets.

3. Acknowledgement Policy

- *The acknowledgement policy imposed by the receiver may also affect congestion.*
- *If the receiver does not acknowledge every packet it receives it may slow down the sender and help prevent congestion.*
- *Acknowledgments also add to the traffic load on the network. Thus, by sending fewer acknowledgments we can reduce load on the network.*
- *To implement it, several approaches can be used:*

1. *A receiver may send an acknowledgement only if it has a packet to be sent.*
2. *A receiver may send an acknowledgement when a timer expires.*
3. *A receiver may also decide to acknowledge only N packets at a time.*

4. Discarding Policy

- *A router may discard less sensitive packets when congestion is likely to happen.*
- *Such a discarding policy may prevent congestion and at the same time may not harm the integrity of the transmission.*

5. Admission Policy

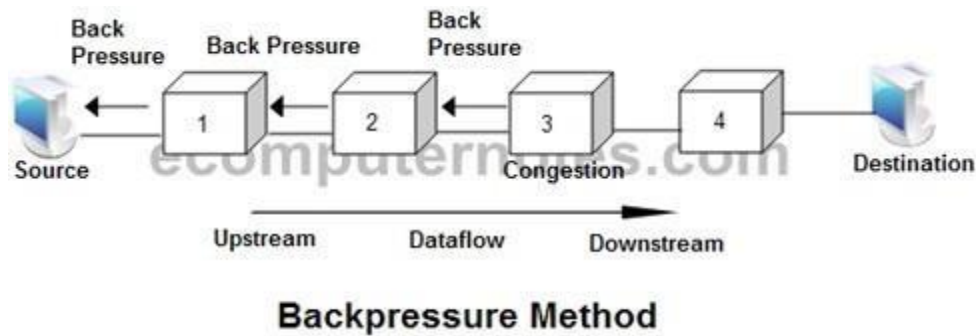
- *An admission policy, which is a quality-of-service mechanism, can also prevent congestion in virtual circuit networks.*
- *Switches in a flow first check the resource requirement of a flow before admitting it to the network.*
- *A router can deny establishing a virtual circuit connection if there is congestion in the network or if there is a possibility of future congestion.*

Closed Loop Congestion Control

- *Closed loop congestion control mechanisms try to remove the congestion after it happens.*
- *The various methods used for closed loop congestion control are:*

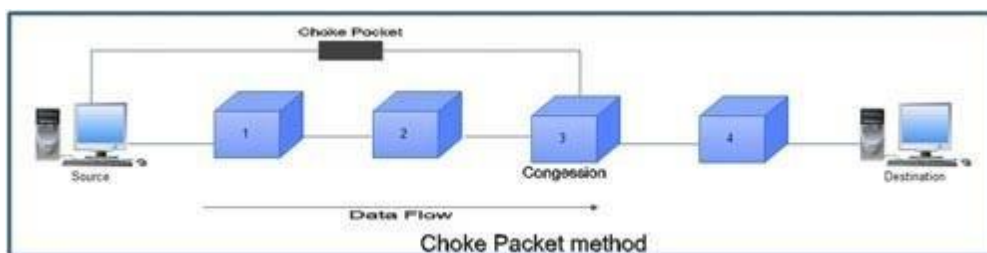
1. Backpressure

- *Backpressure is a node-to-node congestion control that starts with a node and propagates, in the opposite direction of data flow.*



2. Choke Packet

- In this method of congestion control, congested router or node sends a special type of packet called choke packet to the source to inform it about the congestion.
- Here, congested node does not inform its upstream node about the congestion as in backpressure method.
- In choke packet method, congested node sends a warning directly to the source station i.e. the intermediate nodes through which the packet has traveled are not warned.



3. Implicit Signaling

- In implicit signaling, there is no communication between the congested node or nodes and the source.
- The source guesses that there is congestion somewhere in the network when it does not receive any acknowledgment. Therefore the delay in receiving an acknowledgment is interpreted as congestion in the network.
- On sensing this congestion, the source slows down.
- This type of congestion control policy is used by TCP.

4. Explicit Signaling

- In this method, the congested nodes explicitly send a signal to the source or destination to inform about the congestion.

- *Explicit signaling is different from the choke packet method. In choke packed method, a separate packet is used for this purpose whereas in explicit signaling method, the signal is included in the packets that carry data .*
- *Explicit signaling can occur in either the forward direction or the backward direction .*
- *In backward signaling, a bit is set in a packet moving in the direction opposite to the congestion. This bit warns the source about the congestion and informs the source to slowdown.*
- *In forward signaling, a bit is set in a packet moving in the direction of congestion. This bit warns the destination about the congestion. The receiver in this case uses policies such as slowing down the acknowledgements to remove the congestion.*

Unit- 6.

LAN Technology

Topology and Transmission Media
LAN protocol architecture Medium
Access control
Bridges, Hub, Switch
Ethernet (CSMA/CD), Fibre Channel
Wireless LAN Technology..

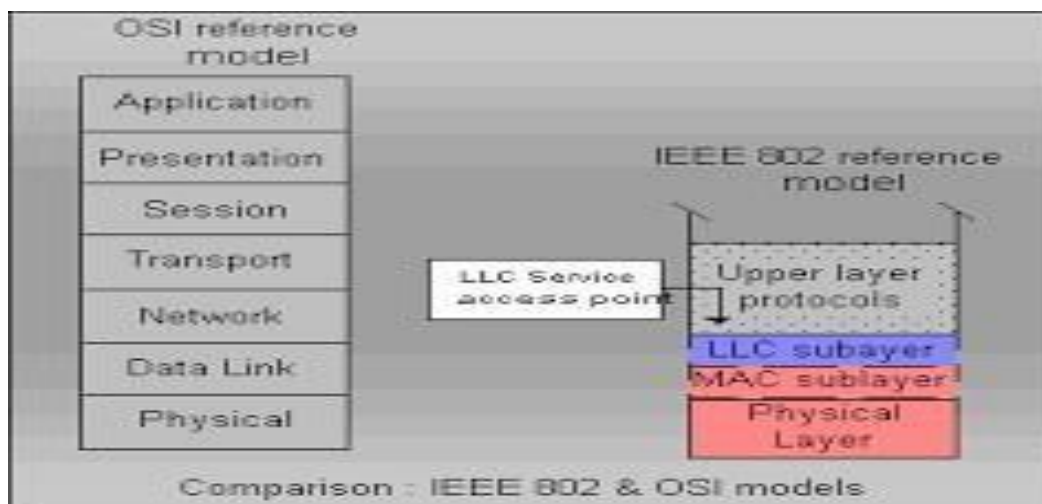
LAN protocol Architecture

In 1985 the computer society of the IEEE started a project 802 ,to set the standards to enable intercommunication.

It is a way of specifying functions of the physical layer and data link layer of major LAN protocol.

The LAN architecture consists of three layers: Physical, MAC (Medium Access Control) and LLC (Logical Link Control).

- o LLC provides connection management, if needed. (For most applications, it is not needed.)*
- o MAC is a protocol for accessing high speed physical links and for transferring data frames from one station to another.*
- o Physical layer deals mainly with actual transmission and reception of bits over the transmission medium. Its specification depends on the specific physical medium and MAC protocols it interfaces with.*



Physical Layer

The physical layer is dependent on the implementation and type of physical media used.
This layer has following functions.

- Encoding and decoding of signals
- Preamble generation and removal (for synchronization)
- Bit transmission and reception

Data link layer

- Assemble data into a frame with address and error-detection fields
- Disassemble frame and perform address recognition and error detection
- Govern access to the LAN transmission medium
- Interface to higher levels and performs flow and error control.
- The data link layer in the IEEE standard is divided into two sublayers: LLC and MAC.

LLC

- LLC is concerned with transmission of link-level PDU (protocol data unit) between two stations
- LLC is meant for error control, flow control and part of the framing duties message sequencing and message acknowledgement.

MAC

The MAC (Media Access Control) is a protocol which controls the access to the transmission medium for an orderly and efficient use of the transmission capacity of the network. Such a control can be exercised in two different ways:

- ✓ Centralized control
- ✓ Decentralized control

MAC frame format

In Standard Ethernet, the MAC sublayer governs the operation of the access method. It also frames data received from the upper layer and passes them to the physical layer. **Frame Format**
The Ethernet frame contains seven fields: preamble, SFD, DA, SA, length or type of protocol data unit (PDU), upper-layer data, and the CRC. Ethernet does not provide any mechanism for acknowledging received frames, making it what is known as an unreliable medium.

Preamble (7 bytes)	Start of Frame Delimiter (1 byte)	Dest. Address (6 bytes)	Source Address (6 bytes)	Length (2 bytes)	Header+Data^a	Frame Checksum (4 bytes)

- **Preamble** : Each frame starts with a preamble of 7 bytes, each byte containing the bit pattern 10101010. Manchester encoding is employed here and this enables the receiver's clock to synchronize with the sender's and initialise itself.
- **Start of Frame Delimiter** : This field containing a byte sequence 10101011 denotes

the start of the frame itself.

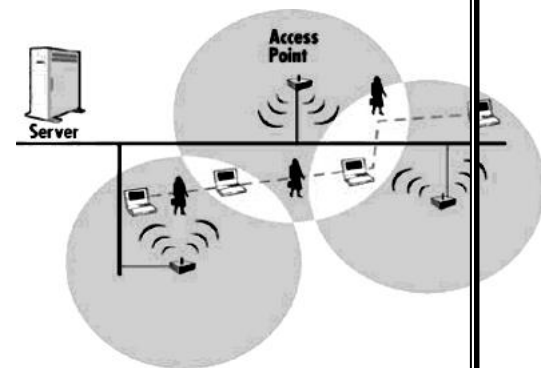
- **Dest. Address :** The destination address field is 6-byte addresses and contains the physical address of the destination station .
- **Source Address :** The SA field is also 6 bytes and contains the physical address of the sender of the frame.
- **Length :** This field is defined as a type field or length field. The original Ethernet used this field as the type field to define the upper-layer protocol using the MAC frame. The IEEE standard used it as the length field to define the number of bytes in the data field
- **Data :** This field carries data encapsulated from the upper layer protocol. It is a minimum of 46 and a maximum of 500 bytes.
- **Frame Checksum :** It is a 32-bit hash code of the data. If some bits are erroneously received by the destination (due to noise on the cable), the checksum computed by the destination wouldn't match with the checksum sent and therefore the error will be detected. The checksum algorithm is a cyclic redundancy checksum (CRC) kind. The checksum includes the packet from Dest. Address to Data field.

Wireless LAN

- A wireless LAN (WLAN) is a flexible data communication system implemented as either extension or alternative of a wired LAN within a building or campus. So it combines data connectivity with user mobility.
- A WLAN is a local area network that doesn't rely on wired Ethernet connections. It uses electromagnetic waves for data transmission. It has data transfer speeds of up to 54Mbps.
- A WLAN signal can be broadcast to cover an area ranging in size from a small office to a large campus. Commonly, a WLAN access point provides access within a radius of 65 to 300 feet.

How WLANs Work

- In a typical WLAN configuration, a transmitter/receiver (transceiver) device, called an access point, connects to the wired network from a fixed location using standard Ethernet cable.
- Each access point receives, buffers, and transmits data between the WLAN and the wired network infrastructure.
- A single access point can support a small group of users and can function within a range of several hundred feet.
- The client computer or USER access the WLAN through wireless LAN adapters, which are installed in the PC or LAPTOP.
- The WLAN adapter acts as an interface between the computer and the AP.



WLAN standards

Several standards for WLAN hardware exist:

WLAN	Pros	Cons
------	------	------

<i>standard</i>		
802.11a	<ul style="list-style-type: none"> • <i>Faster data transfer rates (up to 54Mbps)</i> • <i>Supports more simultaneous connections</i> • <i>Less susceptible to interference</i> 	<ul style="list-style-type: none"> • <i>Short range (60-100 feet)</i> • <i>Less able to penetrate physical barriers</i>
802.11b	<ul style="list-style-type: none"> • <i>Better at penetrating physical barriers</i> • <i>Longest range (70-150 feet)</i> • <i>Hardware is usually less expensive</i> 	<ul style="list-style-type: none"> • <i>Slower data transfer rates (up to 11Mbps)</i> • <i>Doesn't support as many simultaneous connections</i> • <i>More susceptible to interference</i>
802.11g	<ul style="list-style-type: none"> • <i>Faster data transfer rates (up to 54Mbps)</i> • <i>Better range than 802.11b (65-120 feet)</i> 	<ul style="list-style-type: none"> • <i>More susceptible to interference</i>
802.11n	<ul style="list-style-type: none"> • <i>The 802.11n standard is recently certified by the Institute of Electrical and Electronics Engineers (IEEE), as compared to the previous three standards. Though specifications may change, it is expected to allow data transfer rates up to 600Mbps, and may offer larger ranges.</i> 	

Fibre Channel

- ✓ *A high-speed transmission technology used as a peripheral channel or network backbone.*
- ✓ *Fibre Channel transfers digital data between sources and users of information.*
- ✓ *This digital data represents different types of information like programs, files, graphics, videos and sound.*
- ✓ *Each having its own structure, protocol, connectivity, measures of performance and reliability requirements.*
- ✓ *Fibre Channel is a switched medium that works similar to a telephone network: any user will have a temporary, direct connection that provides the option of the full bandwidth of the Fibre Channel as long as the connection is established.*
- ✓ *Fibre Channel's acknowledgment and flow control supports connection-less traffic by using time division multiplexing.*
- ✓ *Fibre Channel is designed to transport many protocols, such as FDDI, serial HIPPI, SCSI, IPI, and many more that will be listed in the section describing the FC-4 layer.*
- ✓ *The transfer rates of Fibre Channel are currently (133 Mbps, 266 Mbps, 530 Mbps, and 1 Gbps). However, data rates of 2 to 4 Gbps should be available soon.*
- ✓ *Fibre Channel will allow simultaneous transmission of different protocols over a single optical-fiber pair and it can allow a number of existing services, such as network, point-*

to- point, and peripheral interfaces, to be accessed over a single medium using the same hardware connection.

- ✓ Fibre Channel also provides control and complete error checking.
- ✓ The Fibre Channel structure is defined as a multi-layered stack of functional levels, not unlike those used to represent network protocols, although not mapping directly to OSI layers.
- ✓ The layers of the Fibre channel standard define the physical media and transmission rates, encoding scheme, framing protocol and flow control, common service, and the upper-level applications interfaces. The five layers are: FC-0, FC-1, FC-2, FC-3, FC-4

Hub

- ✓ A hub works in the physical layer of the OSI model. It is basically a non-intelligent device, and has no decision making capability.
- ✓ A Hub basically takes the input data from one of the ports and broadcasts the information to all the ports connected to the network.
- ✓ It is used in traditional 10-Mbps Ethernet networks to connect network computers to form a local area network (LAN).



Switch

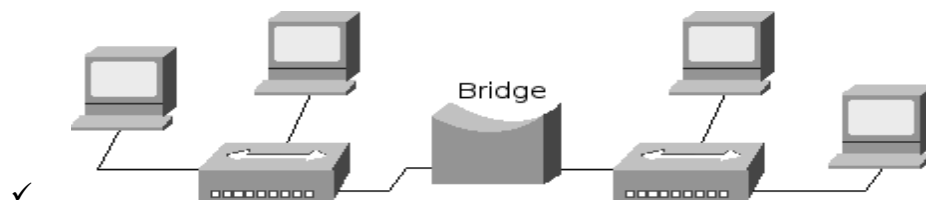
- ✓ A switch is an intelligent device that works in the data link layer.
- ✓ The term intelligent refers to the decision making capacity of the Switch. Since it works in the Data link layer, it has knowledge of the MAC addresses of the ports in the network.
- ✓ When a signal enters a port of the switch, the switch looks at the destination address of the frame and internally establishes a logical connection with the port connected to the destination node.
- ✓ It is also to be noted that a switch is a secure device, because it sends information only to the desired destinations, and also certain security features such as a firewall can be implemented in the Switches.



Switch

Bridge

- ✓ Bridge operates in both the physical and data link layer of the OSI model.
- ✓ Bridge can divide a large network into smaller segments.
- ✓ Bridge utilizes the addressing protocol and can affect the flow control of a single LAN.
- ✓ This mechanism helps to filter the traffic which leads to control the congestion problem and isolating problem.
- ✓ Bridge also provides security through this partitioning of traffic.
- ✓ When a frame enters a bridge, the bridge not only regenerates the signal but checks the address of the destination and forwards the new copy only to the segment to which the address belongs.
- ✓ There are different types of bridge such as—Simple, multiport and transparent.

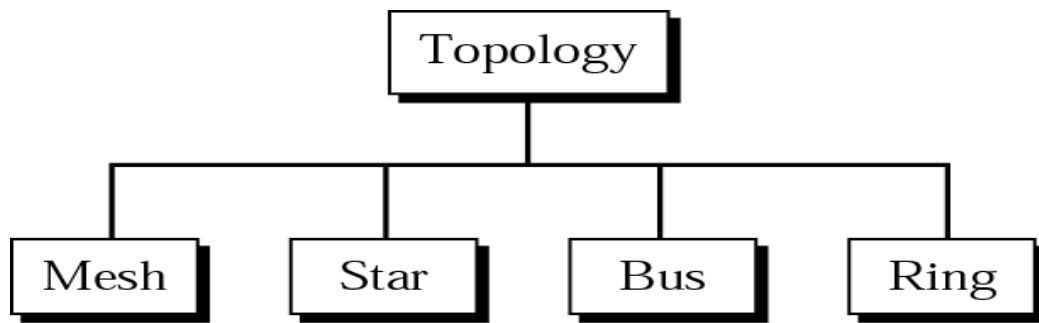


TOPOLOGY:

- ✓ Topology refers to the way in which a network is laid out physically.
- ✓ The topology of a network is the geometric representation of the relationship of all the links and linking devices (usually called nodes) to one another.

Categories of topology:

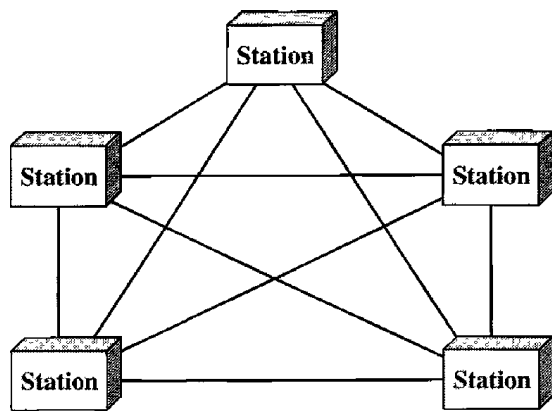
There are four basic topologies possible.



There are two derived topologies: Tree, Hybrid.

1. Mesh topology:

- ✓ *In a mesh topology, every device has a dedicated point-to-point link to every other device.*
- ✓ *The term dedicated means that the link carries traffic only between the two devices it connects.*
- ✓ *A fully connected mesh network therefore has $\frac{n(n-1)}{2}$ physical channels/link n devices.*
- ✓ *To accommodate that many links, every device on the network must have $n - 1$ input/output (I/O) ports to be connected to the other $n - 1$ stations.*



ADVANTAGES:

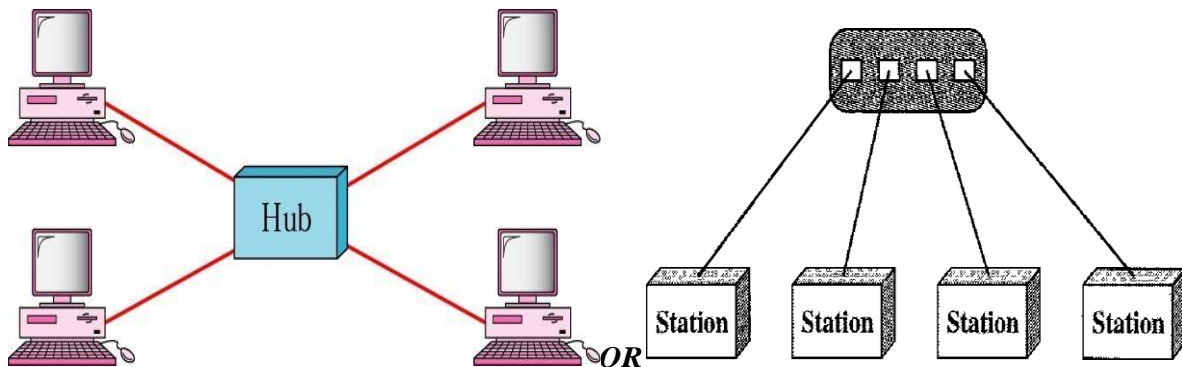
- ✓ *The use of dedicated links guarantees that each connection can carry its own data load, thus eliminating the traffic problems.*
- ✓ *A mesh topology is robust. If one link becomes unusable, it does not hamper the entire system.*
- ✓ *There is the advantage of privacy or security.*
- ✓ *Finally, point-to-point links make fault identification and fault isolation easy.*

DISADVANTAGES:

- ✓ Every device must be connected to every other device, so installation and reconnection are difficult.
- ✓ The sheer bulk of the wiring can be greater than the available space (in walls, ceilings, or floors) can accommodate.

2. Star Topology :

- ✓ In a star topology, each device has a dedicated point-to-point link only to a central controller, usually called a hub.
- ✓ The devices are not directly linked to one another.
- ✓ A star topology does not allow direct traffic between devices. The controller acts as an exchange: If one device wants to send data to another, it sends the data to the controller, which then relays the data to the other connected devices.



ADVANTAGES:

- ✓ A star topology is less expensive than a mesh topology.
- ✓ It is easy to install and reconfigure.
- ✓ Other advantages include robustness.
- ✓ Easy fault identification and fault isolation.

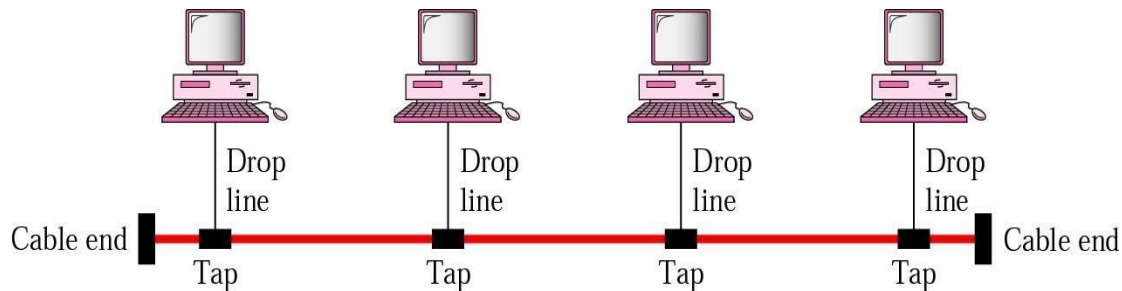
DISADVANTAGE:

The dependency of the whole topology on one single point, the hub. If the hub goes down, the whole system is dead.

3. Bus Topology :

- ✓ A bus topology, on the other hand, is multipoint. One long cable acts as a backbone to link all the devices in a network.
- ✓ Nodes are connected to the bus cable by drop lines and taps.

- ✓ A drop line is a connection running between the device and the main cable. A tap is a connector that either splices into the main cable or punctures the sheathing of a cable to create a contact with the metallic core.



ADVANTAGES

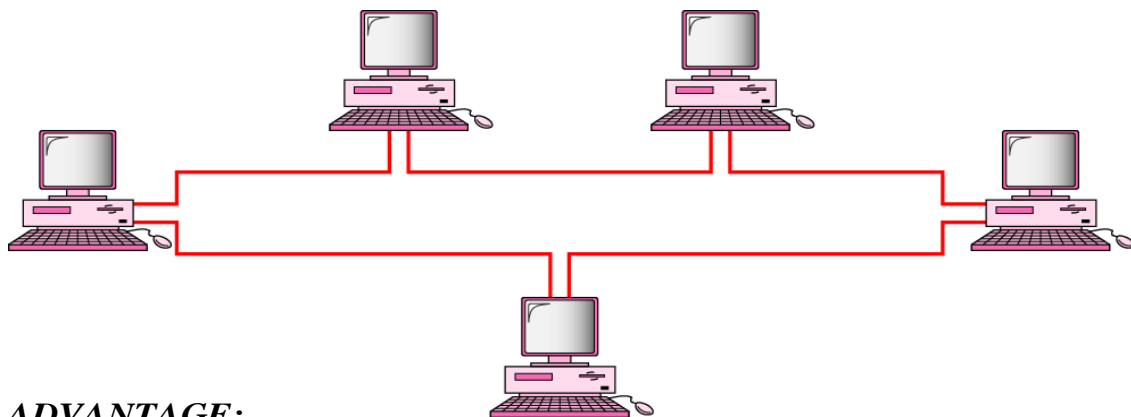
- ✓ Advantages of a bus topology include ease of installation
- ✓ Uses less cabling.

DISADVANTAGES:

- ✓ Difficult reconnection and fault isolation is also difficult.
- ✓ Signal reflection at the taps can cause degradation in quality.

4. Ring topology:

- ✓ In a ring topology, each device has a dedicated point-to-point connection with only the two devices on either side of it.
- ✓ A signal is passed along the ring in one direction, from device to device, until it reaches its destination.
- ✓ Each device in the ring incorporates a repeater. When a device receives a signal intended for another device, its repeater regenerates the bits and passes them along.



ADVANTAGE:

- ✓ A ring is relatively easy to install and reconfigure.

- ✓ *Fault isolation is simplified.*

DISADVANTAGE: *Unidirectional traffic can be a disadvantage.*

Tree topology:

- ✓ *A tree topology is a variation of star topology.*
- ✓ *In star, nodes in a tree are linked to a central hub that controls the traffic to the network. However, not every device plugs directly into the central hub.*
- ✓ *The majority of devices connect to a secondary hub that in turn is connected to the central hub.*
- ✓ *The central hub in the tree is an active hub (i.e. an active hub contains a repeater which regenerates signal.). the secondary hubs may be active or passive hub (i.e. the passive hub provides a simple physical connection between the attached devices).*

Advantage

- ✓ *It allows more devices to be attached to a single central hub and can therefore increase the distance a signal can travel between devices.*
- ✓ *It allows the network to isolate and prioritize communication from different computers.*

Disadvantage

The dependency of the whole topology on one single point, the central hub. If the central hub goes down, the whole system is dead.

5. Hybrid topology:

Often a network combines several topologies as subnet works linked together in a larger topology. For example, one department of a business may have decided to use a bus topology while another department has a ring. The two can be connected to each other via a central controller in a star topology.

Unit- 7

TCP/I

P

TCP/IP Protocol Suite Basic

Protocol functions

Principles of Internetworking

Internet Protocol operations

Internet Protocol

Internet Protocol

- IP protocol is one of the main protocols in the TCP/IP stack.
- It is in the form of IP datagrams that all the TCP, UDP, ICMP and IGMP data travel over the network.
- IP is connection less and unreliable protocol. It is connection less in the sense that no state related to IP datagrams is maintained either on source or destination side and it is unreliable in the sense that it is not guaranteed that an IP data gram will get delivered to the destination or not.
- If an IP datagram encounters some error at the destination or at some intermediate host (while traveling from source to destination) then the IP datagram is generally discarded and an ICMP error message is sent back to the source.
- The IP protocol sits at the layer-2 of TCP/IP protocol suite i.e. the Internet layer .

IP Header Format

0	4	8	16	19	31
Version	Header Length	Service Type	Total Length		
Identification			Flags	Fragment Offset	
TTL	Protocol		Header Checksum		
Source IP Addr					
Destination IP Addr					
Options				Padding	

- **Header Version (4b):** This is the first field in the protocol header. This field

occupies 4 bits. This signifies the current IP protocol version being used. Most common version of IP protocol being used is version 4 while version 6 is out in market and fast gaining popularity.

- **Header Length (4 bits):** This field provides the length of the IP header. The length of the header is represented in 32 bit words. This length also includes IP options (if any). Since this field is of 4 bits so the maximum header length allowed is 60 bytes.
- **Type of Service (8 bits):** The first three bits of this field are known as precedence bits and are ignored as of today. The next 4 bits represent type of service and the last bit is left unused. The 4 bits that represent TOS are: minimize delay, maximize throughput, maximize reliability and minimize monetary cost.
- **Total Length (16 bits):** This represents the total IP datagram length in bytes. Since the header length (described above) gives the length of header and this field gives total length so the length of data and its starting point can easily be calculated using these two fields. Since this is a 16 bit field and it represents length of IP datagram so the maximum size of IP datagram can be 65535 bytes.
- **Identification (16 bits):** This field is used for uniquely identifying the IP datagrams. This value is incremented every-time an IP datagram is sent from source to the destination. This field comes in handy while reassembly of fragmented IP datagrams.
- **Flags (3 bits):** This 3 bit field contains information that controls fragmentation. An application may choose whether to do fragment to datagram or not.
- **Fragment Offset (13 bits):** In case of fragmented IP datagrams, this field contains the offset (in terms of 8 byte units) from the start of IP datagram. So again, this field is used in reassembly of fragmented IP datagrams.
- **Time to Live (8 bits):** This value represents number of hops that the IP datagram will go through before being discarded. The value of this field in the beginning is set to be around 32 or 64 (let's say) but at every hop over the network this field is decremented by one. When this field becomes zero, the data gram is discarded. So, we see that this field literally means the effective lifetime for a datagram on network.
- **Protocol (8 bits):** This field represents the transport layer protocol that handed over data to IP layer. This field comes in handy when the data is demultiplexed at the destination as in that case IP would need to know which protocol to hand over the data to.
- **Header Checksum (16 bits):** This 16 bit field ensures the integrity of header value. A checksum on the header only. Since some header fields change (e.g., time

to live), this is recomputed and verified at each point that the internet header is processed.

- ~~Source and Destination IP Address~~ These fields store the source and destination address respectively. Since size of these fields is 32 bits each so an IP address of maximum length of 32 bits can be used. So we see that this limits the number of IP addresses that can be used. To counter this problem, IP V6 has been introduced which increases this capacity.
- ~~Options~~ The options may appear or not in datagrams. They must be implemented by all IP modules (host and gateways). What is optional is their transmission in any particular datagram, not their implementation. In some environments the security option may be required in all datagrams. The option field is variable in length. There may be zero or more options

Difference between IPv4 and IPv6

IPv4	IPv6
The size of an address in IPv4 is 32 bits	The size of an address in IPv6 is 128 bits
Address Shortages: IPv4 supports 4.3×10^9 (4.3 billion) addresses, which is inadequate to give one (or more if they possess more than one device) to every living person.	Larger address space: IPv6 supports 3.4×10^{38} addresses, or 5×10^{28} (50 octillion) for each of the roughly 6.5 billion people alive today. ^{33(*)}
IPv4 header has 20 bytes	IPv6 header is the double, it has 40 bytes
IPv4 is subdivided into classes <A-E>.	IPv6 is classless.
IPv4 address uses a subnet mask.	IPv6 uses a prefix length.
IPv4 has lack of security.	IPv6 has a built-in strong security
ISP (Internet service provider) have IPv4 connectivity or have both IPv4 and IPv6	Many ISP don't have IPv6 connectivity