Lecture Notes For DCCN Prepared By GIRIJA PRASAD SWAIN

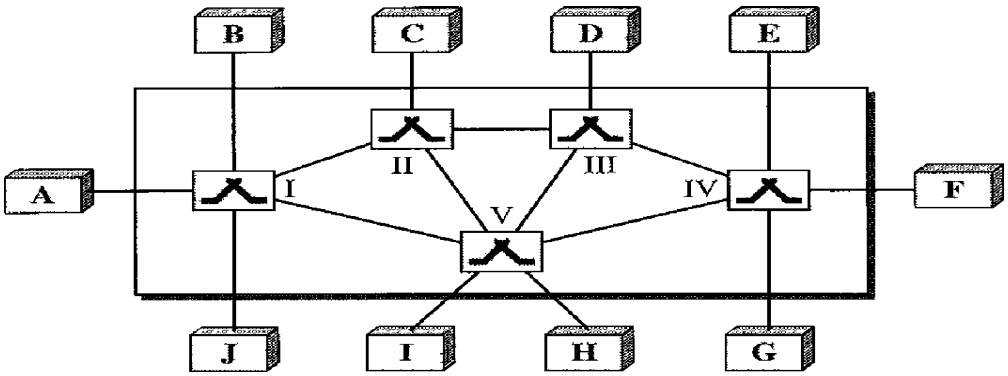
Switching & Routing

Circuit Switching networks
Packet Switching principles
X.25
Routing in Packet switching
Congestion
Effects of congestion, congestion control
Ttraffic Management
Congestion Control in Packet Switching Network.

SWITCHING:

@ A switched network consists of a series of interlinked nodes, called switches. Switchesare 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.



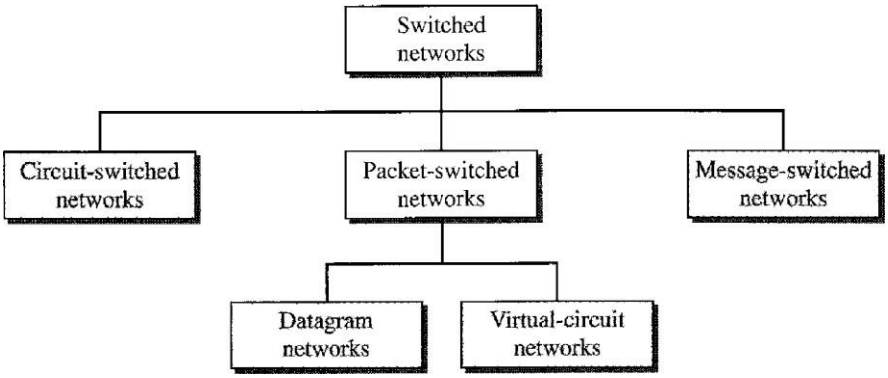
The end systems (communicating devices) are labeled A, B, C, D, and so on, and theswitches are labeled I, II, III, IV, and V. Each switch is connected to multiple links.

TYPES:

1. Circuit switching

2.Packet switching

3.Messageswitching.



CIRCUIT-SWITCHED NETWORKS

1 . A *circuit-switched network consistsof a set of switches connected by physical links.*

2. Aconnection between two stations isa 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 nchannelsby using FDMor TDM.

4. Circuit switching takesplace 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 receive by the destination station, although there may be periodsof silence.

6. There is no addressing involved during data transfer. The switches route the databased on their occupied band (FDM) or time slot (TDM). Of course, there is end- to 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 sy stems are normally connected through dedicated lines to the switches, so connection setup meanscreating dedicated channelsbetween 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 unitscalled aspackets.

1. *The problems associated with circuit switching like non voice and datatransmission problem wassuccessfully overcome in packet switching.*
2. *In packet switching there is no resource allocation for the packets. Theallocation isdone on first come first come basis.*
3. *There are two popular approachesfor packet switching.@*

   Datagram approach

   @ Virtual circuit approach

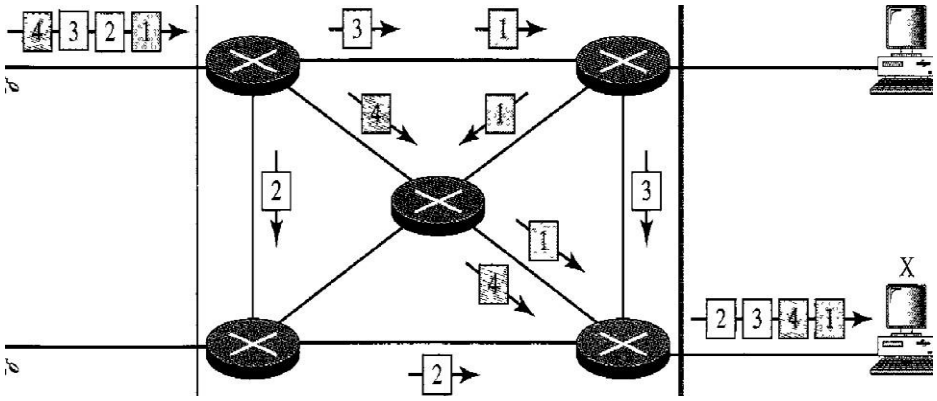
DATAGRAMNETWORKS

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. Packetsin thisapproach are referred to asdata grams.*

2. *Datagram switching isnormally done at the network layer.*

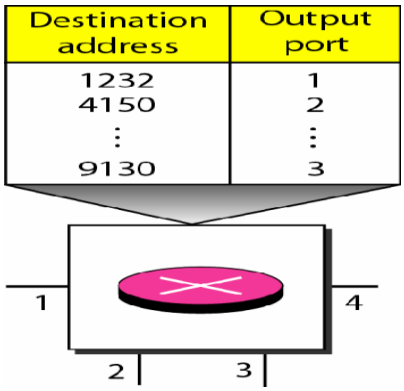
3. *The switches in a datagram network are traditionally referred to asrouters.*

4. *The datagram networks are sometimes referred to as connectionless networks. Theterm* ***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 tablesare 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 remainsthe 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 packetsfrom other sources.*
- *Switching in the Internet is done by using the datagram approach to packet switching at the network layer*

<u>VIRTUAL-CIRCUITNETWORKS</u>

Avirtual- circuit network is a cross between a circuit-switched network and a datagram network. It hassome 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, asin 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- s bwitched network is implemented in the physical layer and a datagram network in the network layer. But thismay change in the future.*

Addressing In a virtual- circuit network,

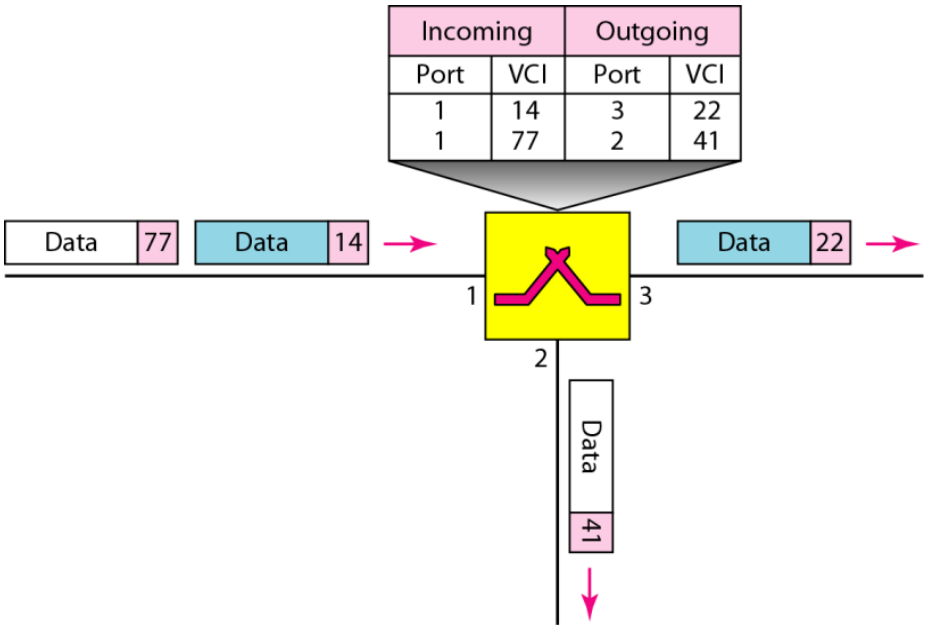
It hastwo typesof addressing are involved: global and local (virtual-circuit identifier).

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 hasa VCI; when it leavesit hasa different VCI.



Three Phases

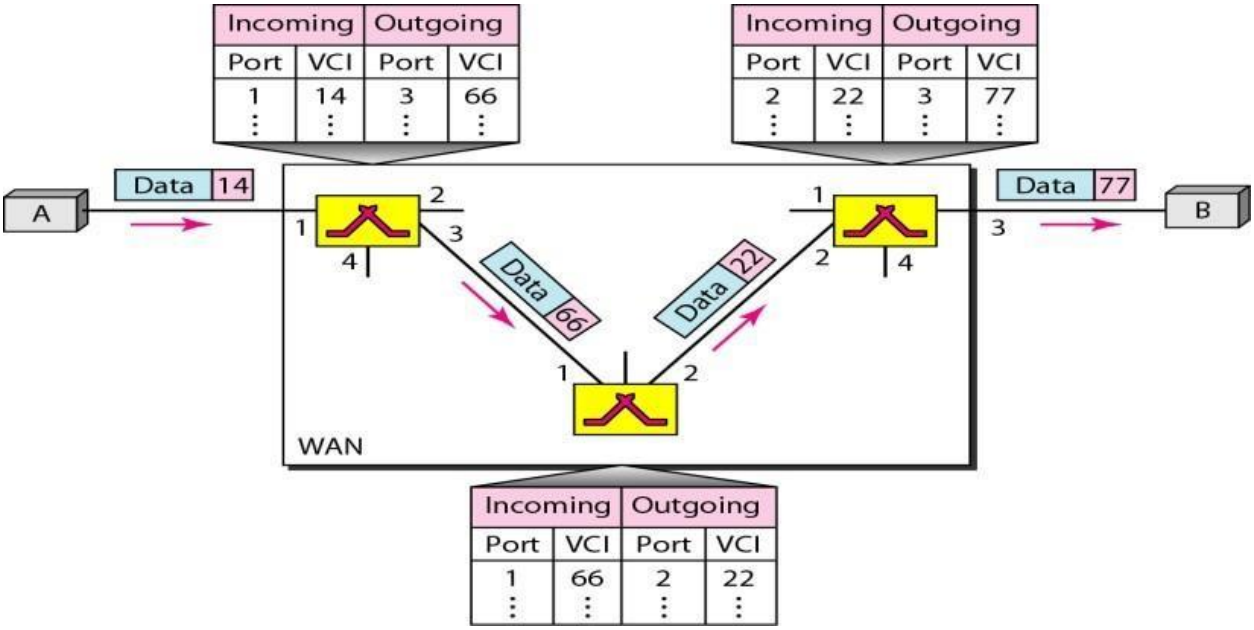
As in a circuit-switched network, a source and destination need to go through three phases in avirtual-circuit network: setup, data transfer, and teardown.

Setup phase

In the setup phase, the source and destination use their global addresses to help switchesmake 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 tableentry for this virtual circuit.*
- *The table, in its simplest form, hasfour columns. This meansthat the switch holdsfourpiecesof information for each virtual circuit that isalready set up.*
- *The data transfer phase isactive until the source sends all its framesto the destination. The process createsa virtual circuit, not a real circuit, between the sourceand destination.*
- *After sending all frames, a special frame is send to end the connection*
- *Destination B responds with a teardown confirmation frame*



Differencesbetween Circuit switching and Packet switching

CIRCUITSWITCHING	***PACKETSWITCHING***
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 unitscalled aspackets.*
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 isneeded*
4. In circuit switching, path is dedicated forthe 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 isold and expensive.	*6. Packet switching ismore modern.*

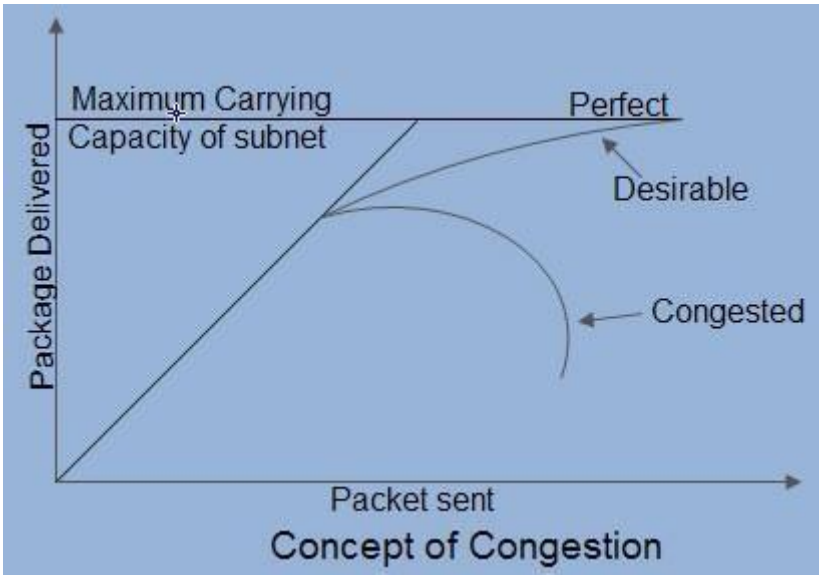
Difference between datagram and virtual circuit approach

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

required	data
Packet containsfull source and destination address	Packet contains short virtual circuit number identifier.
None other than router table containing destination network	Each virtual circuit number entered to table on setup, used forrouting.
Packetsrouted independently	Route established at setup, all packetsfollow same route.
It doesnot affect if any router Fails except those packetslost during crash.	All virtual circuits passing through failed router terminated.
Difficult since all packetsrouted independently router resource requirementscan vary.	Simple by pre-allocating enough buffersto each virtual circuit atsetup, since maximum number of circuits fixed.

Congestion

Congestion isan important issue that can arise in packet switched network. Congestion isa situation in Communication Networks in which too many packetsare present in a part of thesubnet, 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 packetsa network can handle.)

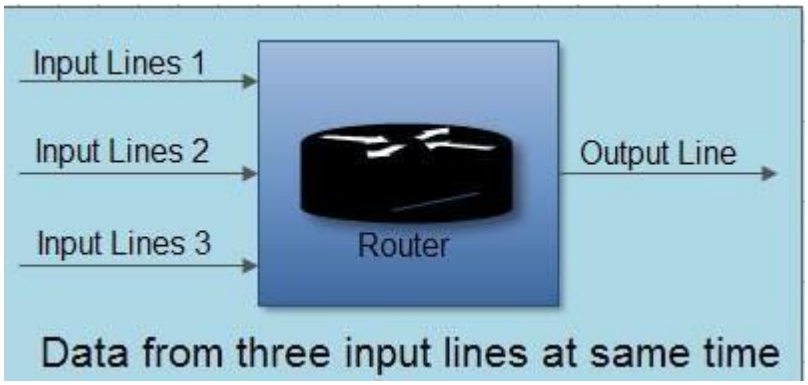


Causing of Congestion:

The variouscauses of congestion in a subnet are

1.The input traffic rate exceedsthe capacity of the output lines. If suddenly, a stream of packet 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 insufficientmemory 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.).

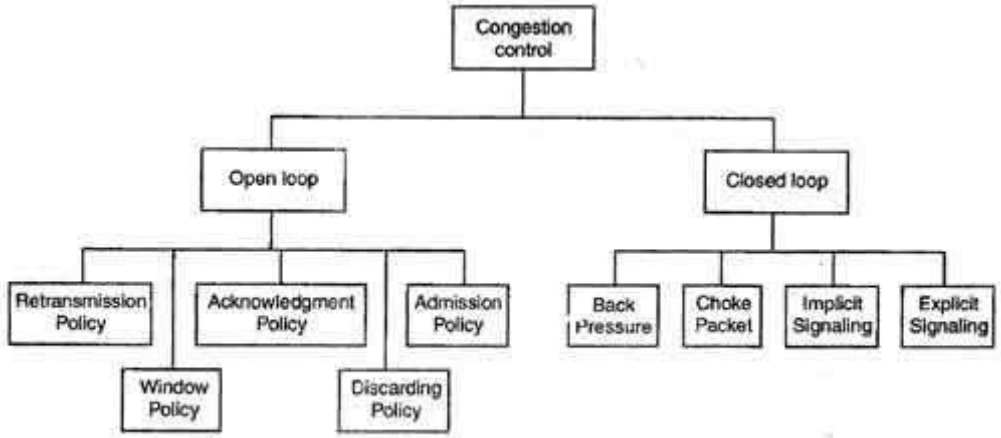
3. The routers' buffer is too limited.

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, queuesare 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 acongestion, 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 removescongestion after it has taken place.



Types of Congestion Control Methods

These two categoriesare:

1. Open loop

2. Closed loop

Open Loop Congestion Control

• In thismethod, policiesare used to prevent the congestion before it happens.

• Congestion control ishandled either by the source or by the destination.

• The variousmethodsused 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. Butwe need to implement good retransmission policy to prevent congestion.

• The retransmission policy and the retransmission timers need to be designed tooptimize 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, thisduplication 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 thesender and help prevent congestion.

• Acknowledgments also add to the traffic load on the network. Thus, by sending fewer acknowledgementswe can reduce load on the network.

• To implement it, several approachescan be used:

1. Areceiver may send an acknowledgement only if it hasa packet to be sent.

2. Areceiver may send an acknowledgement when a timer expires.

3. Areceiver may also decide to acknowledge only Npacketsat a time.

4. Discarding Policy

• Arouter may discard less sensitive packetswhen congestion is likely to happen.

• Such a discarding policy may prevent congestion and at the same time may notharm the integrity of the transmission.

5. Admission Policy

• An admission policy, which is a quality-of-service mechanism, can also preventcongestion in virtual circuit networks.

• Switches in a flow first check the resource requirement of a flow before admitting it tothe network.

• Arouter can deny establishing a virtual circuit connection if there is congestion in the"network or if there isa possibility of future congestion.

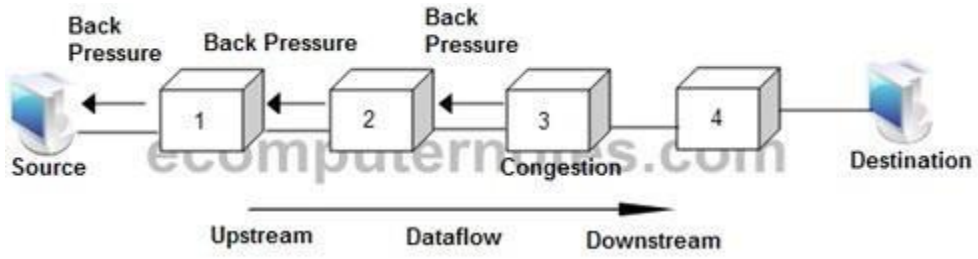
Closed Loop Congestion Control

• Closed loop congestion control mechanisms try to remove the congestion after ithappens.

• The variousmethodsused for closed loop congestion control are:

1. Backpressure

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



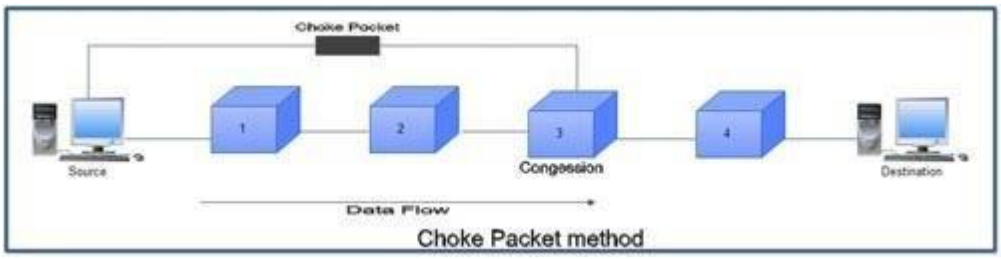
Backpressure Method

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.



Choke Packet method

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 ascongestion in the network.

• On sensing thiscongestion, the source slows down.

• This type of congestion control policy isused 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 packetsthat 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 acknowledgementsto remove the congestion.

Unit- 6.

LAN Technology

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

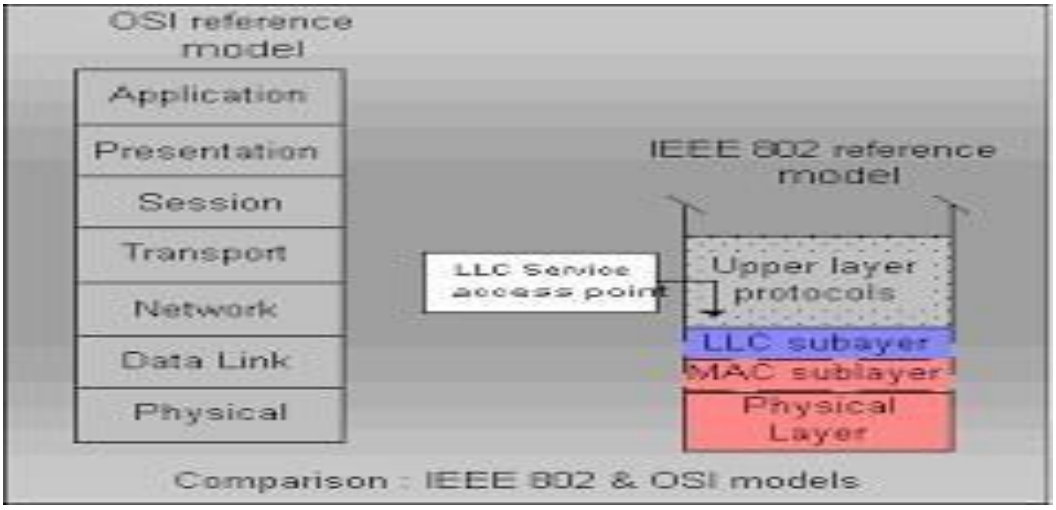
LANprotocol Architecture

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

It isa way of specifying functionsof the physical layer and datalink layer of major LANprotocol.

The LANarchitecture consistsof three layers: Physical, MAC(Medium Access Control) and LLC(Logical Link Control).

- *LLCprovidesconnection management, if needed. (For most applications, it isnot needed.)*
- *MAC isa protocol for accessing high speed physical linksand for transferring data framesfrom one station to another.*
- *Physical layer dealsmainly with actual transmission and reception of bitsover the transmission medium. Its specification dependson the specific physical medium and MAC protocolsitinterfaceswith.*



Physical Lay er

The physical layer isdependent on the implementation and type of physical media used. This layer hasfollowing 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 LANtransmission medium*
- *Interface to higher levelsand performsflow and error control.*
- *The datalink layer in the IEEE standard isdivided into two sublayers: LLCandMAC.*

LLC

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

MAC

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

- ✓ *Centralized control*
- ✓ *Decentralized control*

MACframe format

In Standard Ethernet, the MAC sublay er governsthe operation of the access method. It also framesdata 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 doesnot provide any mechanism for acknowledging received frames, making it what is known asan unreliable medium.*

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

- ***Preamble :****Each frame starts with a preamble of 7 bytes, each byte containing the bitpattern 10101010. Manchester encoding is employed here and thisenablesthe 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 addressesand containsthephysical address of the destination station .*

- ***Source Address :*** *The SA field isalso 6 bytesand containsthe phy sical address of the sender of the frame.*
- ***Length :*** *This field isdefined asa type field or length field. The original Ethernet used this field asthe type field to define the upper-layer protocol using the MAC frame. The IEEE standard used it asthe length field to define the number of bytesin the data field*
- ***Data :****This field carriesdata encapsulated from the upper layer protocol.it isa minimum of 46 and a maximum of 500 bytes.*
- ***Frame Checksum*** *: It isa 32-bit hash code of the data. If some bitsare erroneously received by the destination (due to noise on the cable), the checksum computed by thedestination wouldn't match with the checksum sent and therefore the error will be detected. The checksum algorithm isa cyclic redundancy checksum (CRC) kind. The checksum includesthe packet from Dest. Addressto Data field.*

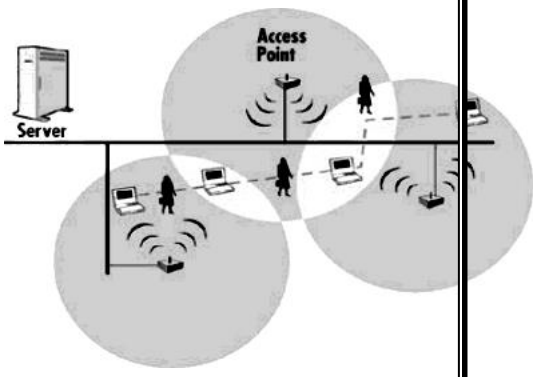
Wireless LAN

- *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.*

- *AWLAN signal can be broadcast to cover an area ranging in size from a small office toa 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 actsasan interface between the computer and the AP.*

WLAN standards

Several standards for WLAN hardware exist:

WLAN	***Pros***	***Cons***

standard		
802.11a	• *Faster data transfer rates (up to 54Mbps)* • *Supports more simultaneous connections* • *Less susceptible to interference*	• *Short range (60-100 feet)* • *Less able to penetrate phy sical barriers*
802.11b	• *Better at penetrating physical barriers* • *Longest range (70-150 feet)* • *Hardware is usually less expensive*	• *Slower data transfer rates (upto 11Mbps)* • *Doesn't support as many simultaneousconnections* • *More susceptible to interference*
802.11g	• *Faster data transfer rates (up to 54Mbps)* • *Better range than 802.11b (65-120 feet)*	• *More susceptible to interference*
802.11n	• *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 ratesup to 600Mbps, and may offer larger ranges.*	

Fibre Channel

- ✓ *Ahigh-speed transmission technology used asa peripheral channel or network backbone.*
- ✓ *Fibre Channel transfers digital data between sources and users of information.*
- ✓ *This digital data represents different typesof information like programs, files,graphics,videosand sound.*
- ✓ *Each having its own structure, protocol, connectivity, measures of performance and reliability requirements.*
- ✓ *Fibre Channel isa switched medium that works similar to a telephone network: any user will have a temporary, direct connection that providesthe option of the full bandwidth of the Fibre Channel aslong asthe connection is established.*
- ✓ *Fibre Channel's acknowledgment and flow control supports connection-less traffic byusing time division multiplexing.*
- ✓ *Fibre Channel isdesigned 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 ratesof Fibre Channel are currently (133 Mbps,266 Mbps,530 Mbps, and 1Gbps). However, data ratesof 2 to 4 Gbpsshould be available soon.*
- ✓ *Fibre Channel will allow simultaneous transmission of different protocolsover a single optical-fiber pair and it can allow a number of existing services, such asnetwork, point-*

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

- ✓ *Fibre Channel also providescontrol and complete error checking.*
- ✓ *The Fibre Channel structure isdefined asa multi-layered stack of functional levels, not unlike those used to represent network protocols, although not mapping directly to OSIlayers.*
- ✓ *The layersof the Fibre channel standard define the physical media and transmission rates, encoding scheme, framing protocol and flow control, common service, and the upper-level applicationsinterfaces. The five layersare: FC-0,FC-1,FC-2,FC-3,FC-4*

Hub

- ✓ *Ahub worksin the physical layer of the OSI model. It isbasically a non-intelligent device, and hasno decision making capability.*
- ✓ *A Hub basically take the input data from one of the portsand broadcast the information to all the portsconnected to the network.*
- ✓ *It used in traditional 10-Mbps Ethernet networksto connect network computersto forma local area network (LAN).*

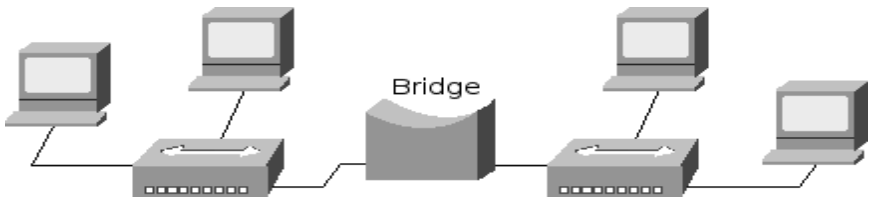
Switch

- ✓ *Aswitch isan intelligent device that worksin the data link layer.*
- ✓ *The term intelligent refers to the decision making capacity of the Switch. Since it worksin the Data link layer, it hasknowledge of the MAC addresses of the portsin the network.*
- ✓ *When a signal entersa port of the switch, the switch looksat the destination address ofthe frame and internally establishes a logical connection with the port connected to the destination node.*
- ✓ *It isalso to be noted that a switch isa secure device, because it sends information only to the desired destinations, and also certain security features such asfirewallscan be implemented in the Switches.*

Switch

Bridge

- ✓ *Bridge operatesin both the physical and data link layer of the OSI model.*
- ✓ *Bridgescan divide a large network into smaller segments.*
- ✓ *Bridgesutilizesthe addressing protocol and can affect the flow control of a single LAN.*
- ✓ *This mechanism helpsto filter the traffic which leadsto control the congestion problemand isolating problem.*
- ✓ *Bridgesalso provide security through thispartitioning of traffic.*
- ✓ *When a frame entersa bridge the bridge not only regeneratesthe signal but checks the address of the destination and forwardsthe new copy only to the segment to whichthe address belongs.*
- ✓ *There are different typesof bridge such as–Simple ,multiport and transparent.*
- ✓

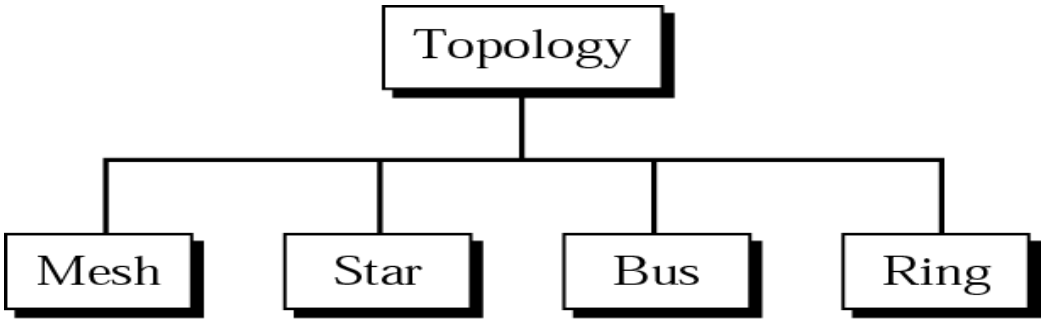


TOPOLOGY:

- ✓ *Topology refersto the way in which a network islaid out physically.*
- ✓ *The topology of a network isthe geometric representation of the relationship of all thelinksand linking devices(usually called nodes) to one another.*

Categories of topology:

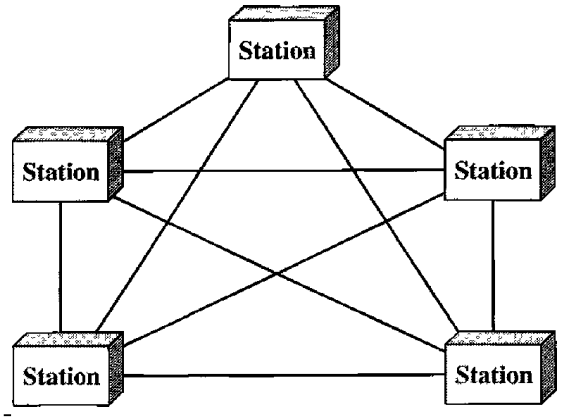
There are four basic topologiespossible.



There are two derived topologies: Tree, Hybrid.

1. Mesh topology:

- ✓ *In a mesh topology, every device hasa dedicated point-to-point link to every otherdevice.*
- ✓ *The term dedicated meansthat the link carries traffic only between the two devicesitconnects.*
- ✓ *Afully connected mesh network therefore hasn(n -1) /2 physical channelslink 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:

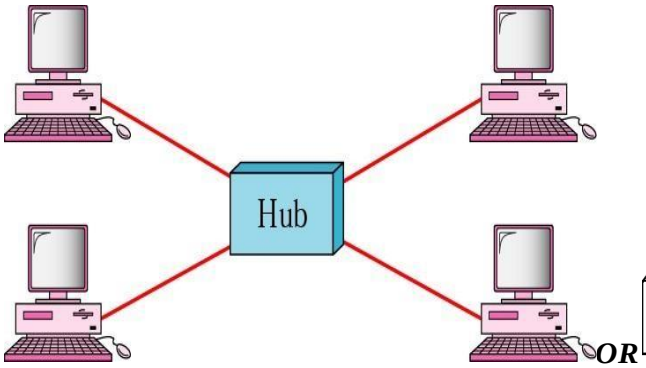
- ✓ *The use of dedicated linksguaranteesthat each connection can carry its own dataload, thuseliminating the traffic problems.*
- ✓ *Amesh topology is robust. If one link becomesunusable, it doesnot hamper the entiresystem.*
- ✓ *There is the advantage of privacy or security.*
- ✓ *Finally, point-to-point linksmake fault identification and fault isolation easy.*

DISADVANTAGES:

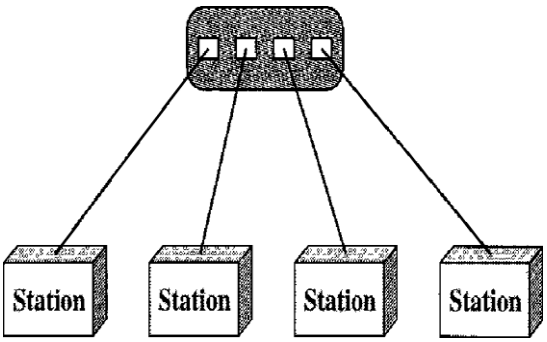
- ✓ *Every device must be connected to every other device, so installation and reconnectionare difficult.*
- ✓ *The sheer bulk of the wiring can be greater than the available space (in walls, ceilings,or floors) can accommodate.*

2. Star Topology :

- ✓ *In a star topology, each device hasa dedicated point-to-point link only to a central controller, usually called a hub.*
- ✓ *The devicesare not directly linked to one another.*
- ✓ *Astar topology doesnot allow direct traffic between devices. The controller actsasan exchange: If one device wantsto send data to another, it sends the data to the controller, which then relaysthe data to the other connected devices.*



OR



ADVANTAGES:

- ✓ *Astar topology islessexpensive than a mesh topology.*
- ✓ *It iseasy to install and reconfigure.*
- ✓ *Other advantagesinclude robustness*
- ✓ *Easy fault identification and fault isolation.*

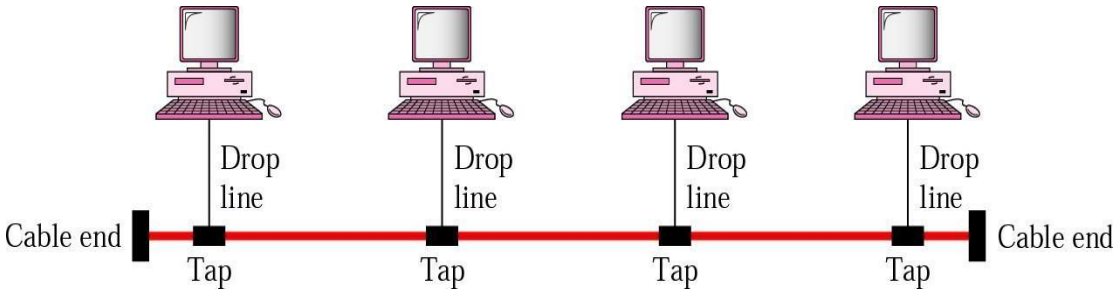
DISADVANTAGE:

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

3. Bus Topology :

- ✓ *Abustopology, on the other hand, ismultipoint. One long cable actsasa backbone tolink all the devicesin a network.*
- ✓ *Nodes are connected to the buscable by drop linesand taps.*

- ✓ *Adrop line isa connection running between the device and the main cable. Atap isa connector that either splices into the main cable or puncturesthe sheathing of a cable to create a contact with the metallic core.*



ADVANTAGES

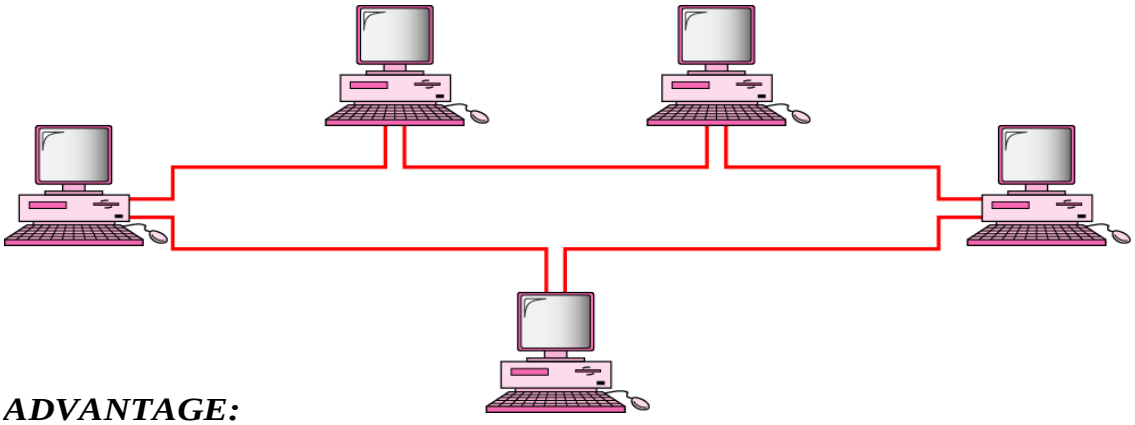
- ✓ *Advantages of a bustopology include ease of installation*
- ✓ *Bususes less cabling.*

DISADVANTAGES:

- ✓ *Difficult reconnection and fault isolation isalso difficult.*
- ✓ *Signal reflection at the tapscan cause degradation in quality.*

4. Ring topology:

- ✓ *In a ring topology, each device hasa dedicated point-to-point connection with onlythe two deviceson either side of it.*
- ✓ *A signal ispassed along the ring in one direction, from device to device, until it reachesits destination.*
- ✓ *Each device in the ring incorporatesa repeater. When a device receivesa signal intended for another device, its repeater regeneratesthe bitsand passes them along.*



ADVANTAGE:

- ✓ *Aring is relatively easy to install and reconfigure.*

- ✓ *Fault isolation is simplified.*

DISADVANTAGE: *Unidirectional traffic can be a disadvantage.*

Tree topology:

- ✓ *Atree topology isa variation of star topology.*
- ✓ *In star, nodesin a tree are linked to a central hub that controlsthe traffic to thenetwork. However, not every device plugsdirectly into the central hub.*
- ✓ *The majority of devicesconnect to a secondary hub that in turn connected to thecentral hub.*
- ✓ *The central hub in the tree isan active hub (i.e. an active hub containsan repeater which regenerates signal.).the secondary hubsmay be active or passive hub(i.e. thepassive hub providesa simple physical connection between the attached devices).*

Advantage

- ✓ *It allowsmore devicesto be attached to a single central hub and can thereforeincrease the distance a signal can travel between devices.*
- ✓ *It allowsthe 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 hubgoesdown, the whole system isdead.

5. Hybrid topology:

Often a network combinesa several topologiesas subnet workslinked together in a larger topology. For example ,one department of a business may have decided to use a bustopology while another department hasa ring . The two can be connected to each other via a central controller in a star topology.

Unit- 7

TCP/I

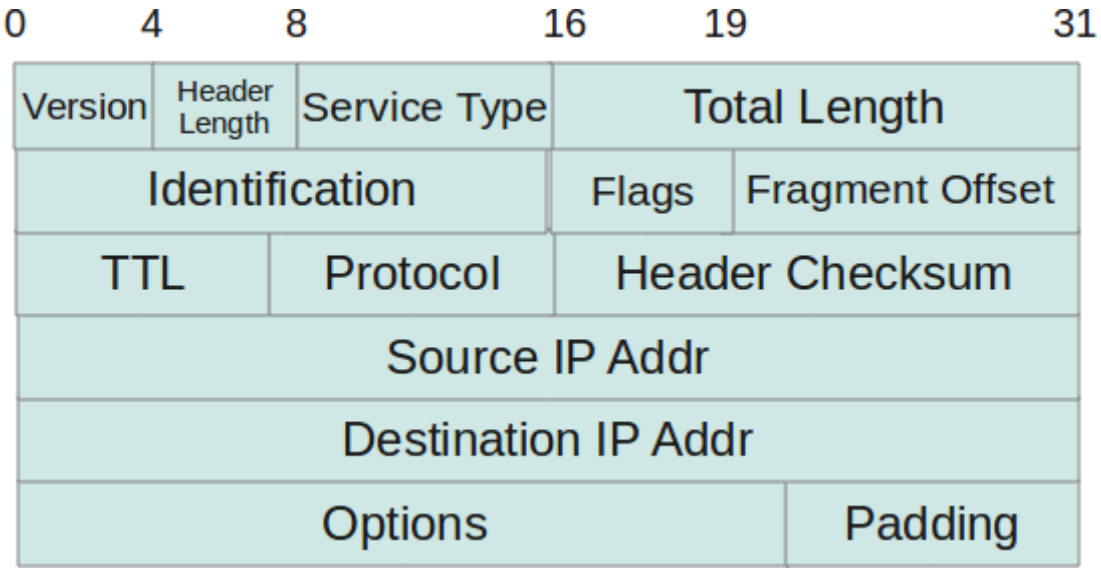
P

TCP/IP Protocol Suite Basic
Protocol functions
Principlesof Internetworking
Internet Protocol operations
Internet Protocol

Internet Protocol

- *IP protocol isone of the main protocolsin the TCP/IP stack.*
- *It is in the form of IP datagramsthat all the TCP, UDP, ICMP and IGMP data travelsover the network.*
- *IP is connection less and unreliable protocol. It is connection less in the sense that no state related to IP datagramsismaintained either on source or destination side and it isunreliable in the sense that it not guaranteed that anIP 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 isgenerally discarded and an ICMP error message is sent back to thesource.*
- *The IP protocol sits at the layer-2 of TCP/IP protocol suite ie the Internet layer .*

IP Header Format



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

occupies 4 bits. This signifies the current IP protocol version being used. Mostcommon version of IP protocol being used is version 4 while version 6 isout inmarket 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 isof 4 bits so the maximum header length allowed is 60 bytes*
- ***Type of Service (8 bits):*** *The first three bitsof this field are known asprecedence bits and are ignored asof 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 isa 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 isused for uniquely identifying the IP datagrams. This value is incremented every-time an IP datagram is sent from source to the destination. This field comesin handy while reassembly of fragmented IP data grams.*
- ***Flags (3 bits):*** *This 3 bit field containsinformation that controlsfragmentation. An application may choose whether to do fragment to datagram or not.*
- ***Fragment Offset (13 bits):*** *In case of fragmented IP data grams, this field contains the offset(in termsof 8 bytesunits) from the start of IP datagram. So again, this field isused in reassembly of fragmented IP datagrams.*
- ***Time to Live (8 bits):*** *Thisvalue representsnumber of hopsthat 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 (lets say) but at every hop over the network this field is decremented by one. When this field becomes zero, the data gram isdiscarded. So,we see that this field literally meansthe effective lifetime for a datagram on network.*
- ***Protocol (8 bits):*** *This field representsthe transport layer protocol that handed over data to IP layer. This field comesin handy when the data isdemultiplex-ed atthe destination asin that case IP would need to know which protocol to hand over the data to.*
- ***Header Checksum (16 bits):*** *This 16 bit field ensure 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 internetheader isprocessed.

- ***Source IP Address, Destination IP Address:*** *These fields store the source and destination address respectively. Since size of these fields is 32 bitseach so an IP address os maximum length of 32 bitscan be used. So we see that this limits the number of IP addresses that can be used. To counter thisproblem, IP V6 hasbeenintroduced which increases thiscapacity.*
- ***Options (Variable length):*** *The optionsmay appear or not in datagrams. They must be implemented by all IP modules (host and gateways). What isoptional 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 maybe 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 addressusesa subnet mask.	*IPv6 usesa prefix length.*
IPv4 haslack of security.	*IPv6 hasa built-in strong security*
ISP(Internet service provider) have IPv4 connectivity or have both IPv4 and IPv6	*Many ISP don't have IPv6 connectivity*

I