GATE CSE NOTES

by

UseMyNotes

ISO/OSI Model.

* An internetwork is a collection of individual networks, connected by intermediate networking devices, that functions as a single large network.

* Functions for internetwork -

a) Mandatory : Error control, flow control, access control, multiplexing & demultiplexing, addressing, etc.

b) Optional : Encryption & decryption, check-pointing, routing & so on.

* To implement all the above functionalities there are various reference models which classify all the above functionalities & define what functions are carried out at a particular layer.

✓ Different models -

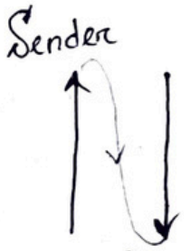
1. ISO-OSI
2. TCP/IP
3. ATM (Asynchronous transfer mode)
4. IEEE (Deals with LAN technologies)
5. X.25

* Open System Interconnection (OSI) Reference Model

Developed by ISO (International organisation of Standardization) in 1984.

It describes how information from a software application in one computer moves through a network medium to a S/W application in another computer. It's a conceptual model composed of 7 layers, each specifying particular N/W functions. It is now considered the primary architectural model for internetworking. The OSI model divides the tasks involved with moving information between networked computers into seven smaller, more manageable task groups. A task or group of tasks is then assigned to each of the seven OSI layer.

→ Layers as defined by the standard in the increasing order of functional complexity:



1. Physical layer (H/W)
2. Data link layer (H/W & S/W)
3. Network layer (complex)

} H/W layers

4. Transport layer (Heart of OSI) Thick layer.
5. Session layer
6. Presentation layer
7. Application layer

} S/W layers. User interaction.

TCP/IP layers
Application
Transport
Internet
Link

→ Advantages of layering:

i) divide & conquer
ii) Encapsulation is possible
iii) Abstraction
iv) Testing made easy

refer RFC (request for comments)

→ Characteristics :

Seven layers can be divided into 2 categories : upper & lower layers.

The upper layers of the model deal with application issues & generally are implemented only in software. The highest layer, the application layer, is closest to the end user. Both users & application layer processes interact with software applications that contain a communications component.

The lower layers handle data transport issues. The physical layer & the data link layer are implemented in H/W & S/W. The physical layer is closest to the physical network medium & is responsible for actually placing information on the medium.

Upper layers	Lower layers
Ap., Pr., Ses.	Tr., Ne., Da., Ph.

→ Protocols

The OSI model provides a conceptual framework for communication between computers, but the model itself is not a method of communication. Actual communication is made possible by using communication protocols. In the context of data networking, a protocol is a formal set of rules & conventions that governs

how computers exchange information over a N/W medium. A protocol implements the functions of one or more of the OSI layers.

Some communication protocols -

a) LAN protocols (physical & DL layer)

b) WAN protocols (lowest 3 layers)

c) Routing protocols (operate at N/W layer)

→ OSI Model & Communication b/w systems.

A given layer in the model generally communicates with 3 other OSI layers - the layer directly above it, below it & its peer layer in other networked computer systems. If system A has information to send to system B, for example, the DL layer of system A communicates with the N/W layer of A, physical layer of A and DL layer of B.

One OSI layer communicates with another layer to make use of the services provided by the 2nd layer. The services provided by adjacent layers help a given OSI layer communicate with its peer layer in other communication systems. Three basic elements are involved in layer services - the service user, the service provider & the service access point (SAP).

The service user is the layer that requests services from an adjacent layer. The service provider is the layer that provides services. OSI layers can provide services to multiple service users. The SAP is a conceptual location at which one OSI layer can request the services of another OSI layer.

Information exchange: Seven OSI layers use various forms of control information to communicate with their peer layers in other computer systems. This control information consists of specific requests & instructions that are exchanged between peer OSI layers. Control information typically takes one of two forms: headers and trailers. Headers are prepended to data that has been passed down from upper layers. Trailers are appended to data that has been passed down from upper layers.

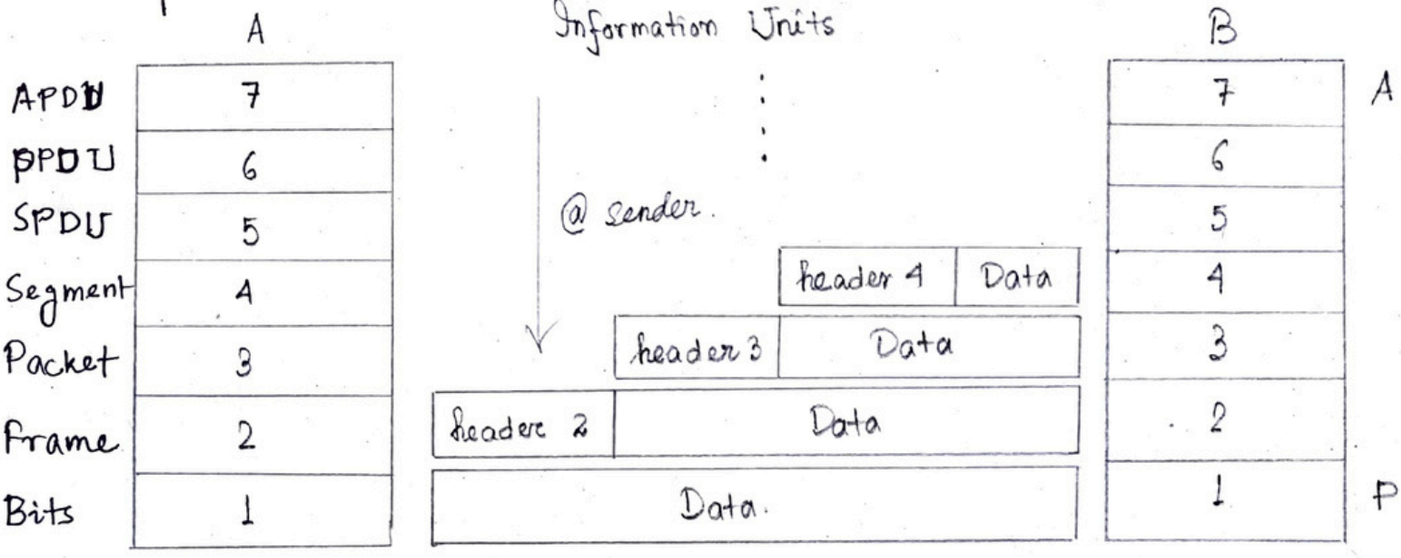
For an OSI layer it is not mandatory to attach a header or a trailer to data from upper layers.

Headers, trailers & data are relative concepts, depending on the layer that analyzes the information unit. At the N/W layer, for example, an information unit consists of a layer 3 header & data. At the data link layer, however, all the information passed down by the N/W layer (layer 3 header & data) is treated as

data.

The data portion of an information unit at a given OSI layer potentially can contain headers, trailers & data from all the higher layers. This is known as encapsulation.

Figure shows how the header & data from one layer are encapsulated into the header of the next lowest layer.



Information exchange: The information exchange process occurs between peer OSI layers. Each layer in the system A (source system) adds control information to data, & each layer in the system B (destination) analyzes & removes the control information from that data.

If system A has data from a S/W application to send to system B, the data is passed to the application layer. The Ap layer in A then communicates any control information required by the Ap layer in system B by prepending a Header to the data. The resulting information unit is passed to the presentation layer, which prepends its

own header containing control information intended for the presentation layer in system B. The information unit grows in size as each layer prepends its own header (in some cases a trailer) that contains control information to be used by its peer layer in system B. At the ph. layer, the entire information unit is placed onto the N/W medium.

The ph. layer in B receives the information unit & passes it to the data link layer. The data link layer in B then reads the control information contained in the header prepended by the data link layer in A. The header is then removed, & the remainder is passed to the N/W layer. Each layer performs the same actions: the layer reads the header from its peer layer, strips it off & passes the remaining information unit to the next highest layer. After the app. layer performs these actions, the data is passed to the recipient software application in B, in exactly the form in which it was transmitted by the application in A.

• Encapsulation: A packet (header & data) at level 7 is encapsulated in a packet at level 6. The whole packet at level 6 is encapsulated in a packet at level 5 & so on.

The data portion of a packet at level N-1 carries the whole packet (data & header) from level N. This is called encapsulation. Level N-1 is not aware of which part of the encapsulated packet is data & which part is the header or trailer. For level N-1, the whole packet coming from level N is treated as one integral unit.

• Physical layer.

→ The physical layer defines the electrical, mechanical, procedural & functional specifications for activating, maintaining & deactivating the physical link between communicating network systems. Physical layer specifications define characteristics such as voltage levels, timing of voltage changes, physical data rates, maximum transmission distances & physical connectors. Physical layer implementations can be categorised as either LAN or WAN specifications.

→ Responsible for the actual physical connection between the devices. The physical layer contains information in the form of bits. It is responsible for transmitting individual bits from one node to other.

While receiving data, this layer will get the signal received & convert it into 0s & 1s & send them to the data link layer, which will put the frame back together.
To be transmitted bits must be encoded into electrical or optical signals.

→ Physical layer is concerned with:

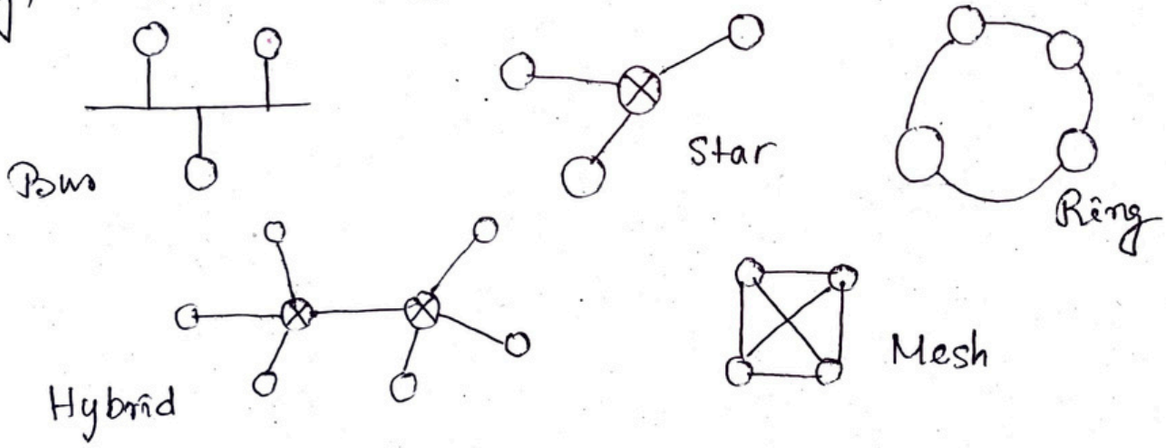
i) Hardware specification: Details of the physical cables, network interface cards, wireless radios etc.

ii) Encoding & Signalling: How are the bits encoded in the medium is decided by this layer. For example, on the copper wire medium, we can use different voltage levels for a certain time interval to represent '0' & '1'. We may use +5mV for 1 nsec to represent '1' & -5 mV for 1 nsec to represent '0'. All the issues with modulation is dealt here, eg. we may use BPSK for representations of 1 & 0 rather than using different voltage levels if we have to transfere in RF waves.

iii) Data transmission & reception: Transfer of each bit of data is the responsibility of this layer. This layer assures the transmission of each bit with a high poob-ability. Transmission of the bits is not completely

reliable as ~~their~~ there is no error correction on this layer.

iv) Topology of Network design : Which part of the N/W is the router going to be placed, where the switches will be used, where we will put the hubs, how many machines is each switch going to handle, what server is going to be placed where, & many such concerns are to be taken care of by the layer. Various kinds of network topologies that we use are ring, bus, star, hybrid.



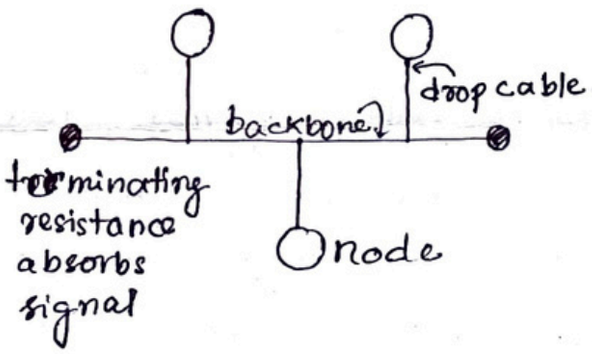
v) Bit synchronisation : By providing a clock. The clock controls both sender & receiver thus providing synchronisation at bit level.

vi) Bit rate control : Defines the transmission rate (# of bits sent per second).

vii) Transmission mode : Simplex, half-duplex or full-duplex.

* Network Topologies.

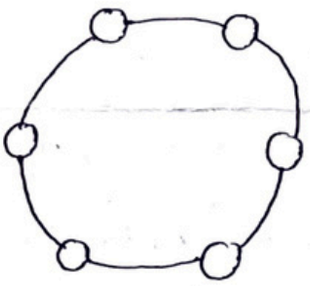
1. Bus topology: All stations are connected through a single cable known as backbone cable. Each node is either connected to the backbone by drop cable or directly connected to the backbone. When a node wants to send a message over the N/W it puts a message over the N/W. All the stations available in the N/W will receive the message whether it has been addressed or not. Mainly used in 802.3 (Ethernet) & 802.4 standard N/Ws. Through backbone msg is broadcasted to all stations. Most common access method for bus topology is CSMA (CSMA/CD & CSMA/CA).



Adv.: i) Low cost cable (as no hubs), ii) moderate data speed (upto 10 Mbps with coaxial or twisted pair), iii) familiar technology, iv) broadcasting, multicasting much simpler, v) N/W is redundant in the sense that failure of one node does not effect the whole N/W. vi) good for smaller N/Ws not requiring very high speed.

Disadv.: i) Extensive cabling, ii) difficult troubleshooting - if any fault occurs in the cable, it would disrupt the comm^n for all nodes, iii) signal interference, iv) adding new devices to the N/W would slow down the N/W. v) attenuation - loss of signal in long distance

2. Ring topology: All nodes are connected in a closed circuit of cable (circular). Messages that are transmitted travel around the ring until they reach the computer that they are addressed to, the signal being refreshed by each node. Transmission is mainly unidirectional, but it can be made bidirectional by having 2 connections between every N/W nodes pair (or by having another ring with the oppositely directed transmission (Dual ring topology). Data transferred bit by bit in a slow orderly fashion. Every node gets a chance to send a packet & it is guaranteed that every node gets to send a packet in a finite amount of time.

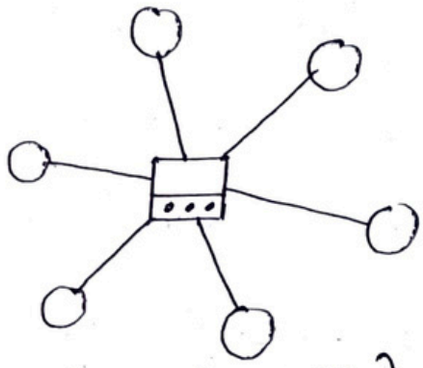


Most common access method for ring topology is token passing.

Adv.: i) N/W mgmt. - faulty devices removed without bringing N/W down. ii) product availaibility - many h/w s/w tools available for operation & monitoring, iii) low installation cost., iv) broadcasting - multicasting is simple, v) very orderly N/W where every device gets chance to transmit & it performs better than a star N/W under heavy load.

Disadv.: i) Breakdown in one station leads to the failure of overall N/W. ii) adding new devices increases the communication delay. iii) Changes of devices can effect N/W. iv) Slower than star topology under normal load.

3. Star topology: Every node connected to a central hub, switch or central computer. Coaxial cable or RJ-45 cables are used to connect these computers. Signals are transmitted & received through the hub. It is the simplest & oldest & all telephone switches are based on this. There exists P2P connection between hosts & hub (central hub). Hub acts as a single point of failure.

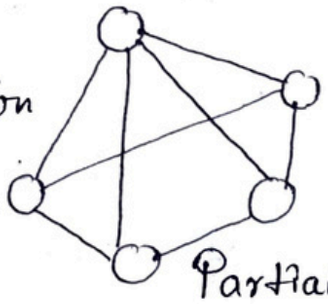


Adv.: i) Efficient troubleshooting (as all are connected to hub, one has to go to the single station to troubleshoot unlike bus topology where we have to check kms of cable), ii) Complex N/W control features can be easily implemented iii) Limited failure – failure in one node does not affect whole N/W., iv) familiar technology, v) easily expandable, vi) cost-effective, vii) high data speed – Ethernet 100BaseT is one of the most popular star N/Ws.

Disadv.: i) Central point of failure, ii) broadcasting & multicasting not easy as extra functionality needed in central hub, iii) installation cost high – each node needs to be connected to central hub.

4. Mesh topology: Computers are connected with each other through various redundant connections. This topology has hosts in P2P with every other host or may also have hosts which are in P2P to few hosts only. → Full mesh – for every

new host $\frac{n(n-1)}{2}$ connections are reqd. Most reliable N/W structure. → Partially mesh - Where we need to provide reliability to selected nodes only. Mesh is used for WAN implementations where failures are a critical concern.

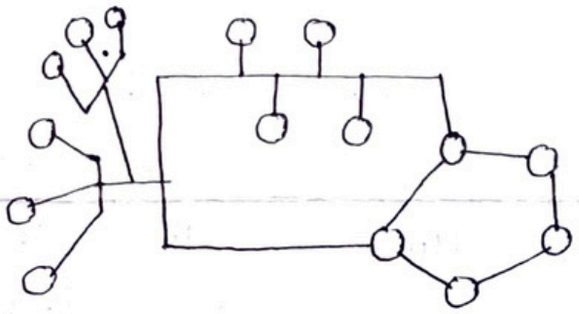

Partially mesh

Adv.: i) reliability ii) fast communication iii) easier reconfiguration - adding new devices is easy.

Disadv.: i) Cost ii) mgmt, iii) efficiency is low as redundant connections are more.

5. Hybrid topology:

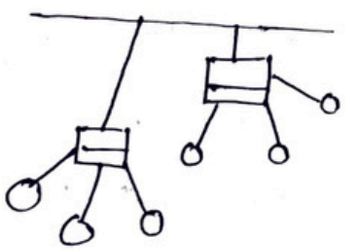
Combination of diff. topologies.



Adv.: reliable, scalable, flexible, effective.

Disadv.: Complex design, costly hubs - hybrid topology hubs are expensive.

6. Tree topology: Combination of bus & star. Parent-child hierarchy. Only one path b/w 2 nodes



adv.: i) support for broadband transmission, ii) easily expandable, iii) easily manageable, iv) error detn easy, v) limited failure.

disadv.: i) difficult troubleshooting, ii) high cost, iii) failure in main bus cable, iv) difficult to reconfigure.

7. Daisy chain topology: Connects all hosts in linear fashion. All connected to 2 hosts except end ones. Each link works as a single point of failure. Every intermediate host works as relay for its immediate hosts.

→ Hub, repeater, modem, cables are physical layer medium devices.

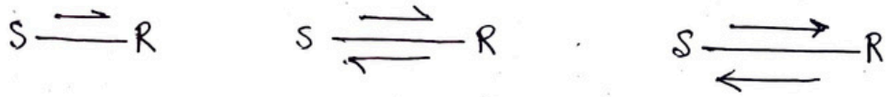
→ Types of medium:

a) Guided media: Signal is guided by the presence of physical media i.e. signal is under control & remains in the physical wire. eg. copper wire.

b) Unguided media: No physical path for the signal to propagate (essentially electromagnetic waves). No control on flow of signal. eg. radio waves.

→ Communication links:

· Communication throug Links classified as — Simplex, half-duplex, full-duplex.



· Links can be classified as —

i) Point to point: Only 2 nodes are connected to each other.

ii) Multipoint: Sharing communication, in which signal can be received by all nodes. (Broadcast)

2 kinds of problem arise in transmission —

✓ i) Attenuation: When a signal transmits in a N/W then the quality of signal degrades as the signal travels longer distances in the wire. To improve quality ~~of~~ amplifiers are used in regular distances.

ii) Noise : In a communication channel many signals are transmitted simultaneously. Certain random signals are also present in the medium. Due to the interference, signals get disrupted.

→ Bandwidth : # of bits that can be transmitted per second in the communication channel.

→ In guided transmission media generally two kinds of materials are used —

1. Copper → Coaxial cable
   → Twisted pair → Unshielded
   → Shielded
2. Optical fiber
   (Light used to send data). - Total internal reflection

Coaxial cable - cable TV

Twisted pair - telephone system

→ Wireless transmission. —

i) Radio transmission (cordless keyboad, wireless LANs, wireless ethernet)

ii) Terrestial microwave (Focused beam between 2 antennas)

iii) Satellite communication (Satellite acts as a switch in the sky. On earth VSAT - very small aperture terminal is used to transmit & receive data from satellite.)

→ Data Encoding :

A) Digital to Analog (Modem → modulator - demodulator used) — ASK, FSK, PSK

B) Digital to Digital C) Analog to digital (PCM, DM)

D) Analog to Analog (AM, FM, PM)

→ Digital to Analog :

i) Amplitude shift keying (Represents digital data as variations in the amplitude of a carriere wave.)

ii) Frequency shift keying (Change of frequency defines different digits)

iii) Phase shift keying (Phase of the carrier is discretely varied in relation either to a reference phase or to the phase of the immediately preceding signal element, in accordance with data being transmitted. Phase of carrier is shifted to represent '0', '1'.

→ Encoding techniques. : Digital to Digital

i) Non return to zero (NRZ)

*Problem with NRZ - Peterson Davie 112

Voltage level is constant during a bit interval. Problem arises when there's a long sequence of 1's or 0's & the voltage level is maintained at the same value for a long time. This creates a problem on the receiving side because now, the clock synchronisation is lost due to lack of any transitions & hence, it is difficult to determine the exact number of 0's & 1's in this sequence.

*Baseline wander, clock recovery problem (clock drift)

Two variations are —

a) NRZ-level : NRZ-L codes ~~shares~~ have the property that the

polarity of the signal changes only when the incoming signal changes from a '1' to a '0' or vice-versa.

b) NRZ-inverted: Transition at the beginning of bit interval = bit 1 and no transition at beginning of bit interval = bit 0 or vice-versa. (Differential encoding)

* NRZ-I has an advantage over NRZ-L. Consider the situation where 2 data wires are wrongly connected in each other's place. In NRZ-L all bit sequences will get reversed (as voltage levels got swapped). Whereas in NRZ-I since bits are recognised by transition, the bits will be correctly interpreted.

A disadvantage in NRZ is that a string of 0's or 1's will prevent synchronisation of transmitter clock with receiver clock & a separate clock line need to be provided.

ii) Biphase encoding: Modulation rate twice that of NRZ & BW correspondingly greater. Since there can be transition at the beginning as well as in the middle of the bit interval the clock operates at twice the data transfer rate.

a) Biphase Manchester / Manchester encoding: Synchronous clock encoding technique.

Baud rate = 2 x Bit rate (Biphase Manchester & Diff. Manchester)

* Clock rate = 2 x Data transfer rate in biphase encoding

If we use 4B/5B or other schemes forcing enough transitions reliable clock recovery is possible.

Characteristics ~

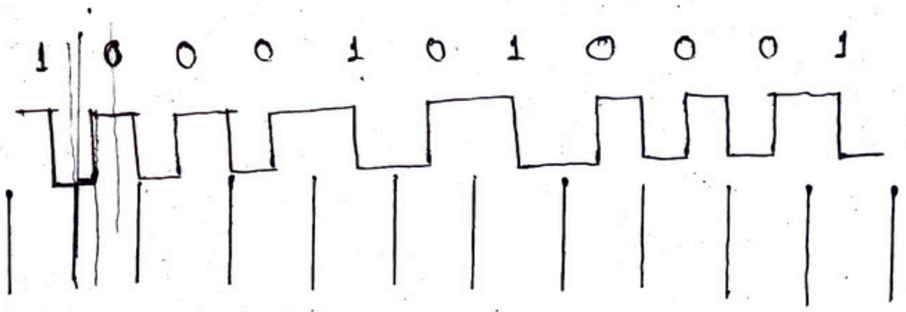
Transition from high to low (⊐) in middle of interval = 1 and transition from low to high in middle of interval (⊏) = 0.

The signal transitions do not always occur at the bit boundary but there is always a transition at the centre of each bit. It is biphase as each bit is encoded by a positive 90 degrees phase transition or by -ve. 90° phase transition.

The manchester encoding consumes twice the bandwidth of the original signal.

Advantages of the encoding is that the DC component of the signal carries no information.

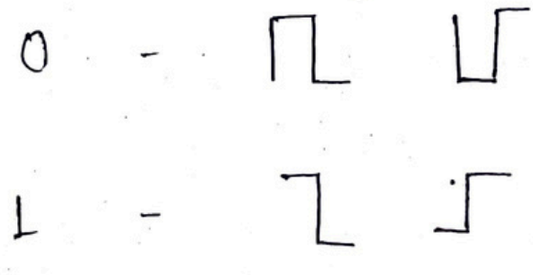
eg.

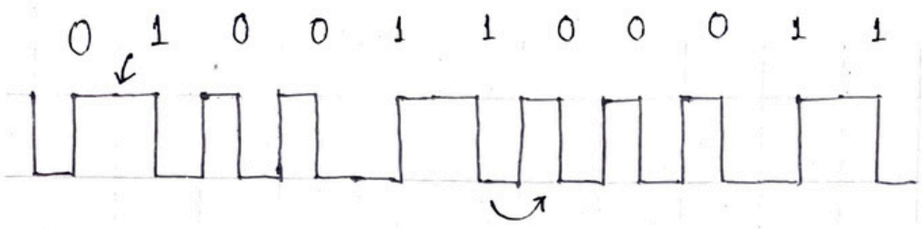


b) Differential Manchester Encoding :

Always a transition in middle of interval.

No transition at beginning of interval = 1 &
transition at beginning of interval = 0.





no transition at beginning as 1

transition at beginning as 0.

iii) 4B5B Encoding: In Manchester encoding, there's a transition after every bit. It means that we must have clocks with double the speed to send same amount of data as in NRZ encoding. We may say that only 50% data is sent. This performance factor can be significantly improved if we use a better encoding scheme. This scheme may have a transition after fixed number of bits instead of every other bit. Like if we have a transition after every 4 bits, then we will be sending 80% data of actual capacity. This is a significant improvement.

Block coding.

In 4B/5B, we convert 4 bits to 5 bits, ensuring at least one transition in them. Basic idea here is that 5 bit code must have at most one leading 0 & no more than two trailing zeros. Thus, it's ensured that we can't have more than 3 consecutive 0s. Now, these 5 bit codes are transmitted using NRZ-I then problem of consecutive 1's is solved.

Should have one leading 0
No more than 2 trailing 0
Words chosen such that 2 transactions take place per block of bits.

→ Analog to digital :

Digitization

$f_s \geq 2 f_{highest}$

i) Pulse code modulation (PCM)

ii) Delta Modulation.

- Data Link Layer (DLL) – Layer 2

→ DLL responsible for the node to node delivery of the message. Main function of this layer is to make sure data transfer is error-free from one node to another, over the physical layer. When a packet arrives in a N/W, it's the responsibility of DLL to transmit it to the host using its MAC address.

→ Packet in DLL is referred as frame. DLL is handled by the NIC & device drivers of host machines. Switch & bridge are DLL devices.

→ The packet received from N/W layer is further divided into frames depending on the frame size of NIC. DLL also encapsulates S's & R's MAC address in the header. The R's MAC address is obtained by placing an ARP (Address Resolution Protocol) request onto the wire asking "Who has that IP address" & the destination host will reply with its MAC address.

→ Responsibilities :

i) Framing : DLL divides the stream of bits received from the N/W layer into manageable data units called frames.

ii) Physical addressing : If frames are to be distributed to different systems on the network, the DLL adds a header to the frame to define the sender and/or receiver of the frame. If the frame is intended for a system outside the sender's network, the receiver address is the address of the device that connects the N/W to the next one.

iii) Flow control : If the rate at which the data are absorbed by the receiver is less than the rate at which data are produced in the sender, the DLL imposes a flow control mechanism to avoid overwhelming the receiver.

iv) Error control : DLL adds reliability to the physical layer by adding mechanisms to detect & retransmit damaged or lost frames. It also uses a mechanism to recognise duplicate frames. Error control is normally achieved through a trailer added to the end of the frame.

v) Access control : When 2 or more devices are connected to the same link, DLL protocols are necessary to determine which device has control over the link at any given time.

→ Data link layer is divided into 2 sublayers -

i) Logical link control (LLC) — EC, FC

ii) Media access control (MAC) - framing, AC, EC, addressing

Framing The LLC manages communications between devices over a single link of a N/W. LLC is defined in the IEEE 802.2 & supports both connectionless and connection-oriented services used by higher layer protocols.

The MAC manages protocol access to the physical N/W medium.

Framing

a) Fixed size framing - No need for defining the boundaries of the frames; the size can be used as a delimeter.

✓ b) Variable size framing - Need a way to define the end of the frame & the beginning of the next.

2 approaches - i) Character oriented & ii) bit oriented.

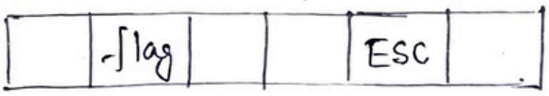
Character oriented protocols. (Byte stuffing)

Data to be carried are 8 bit characters. To separate one frame from the next, an 8-bit flag is added at the beginning & at the end of the frame to signal the start & end of frame.

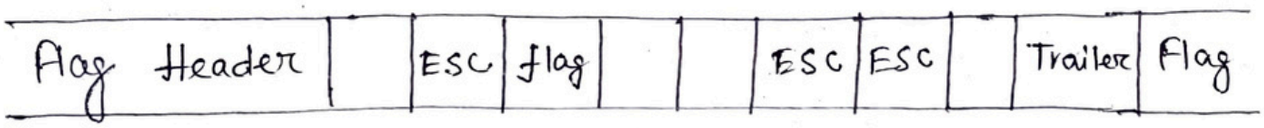
Byte stuffing is the process of adding 1 extra byte if there is a flag or escape character

in the text data itself.

Data from upper layer



Frame sent



→ In variable size framing, we can use length field or end delimeter to define start & end of frame.

→ Length field: We can introduce a length field in the frame to indicate the length of the frame. Used in Ethernet 802.3. Problem is that the length field might get corrupted.

→ End delimeter (ED): We introduce an ED (pattern) to indicate end of the frame. Used in Token ring. Problem with this is that ED can occur in the data. Can be solved by —

A) Character stuffing / Byte stuffing

Used when frames consist of character. If data contains ED then, byte is stuffed into data to differentiate it from ED.

Let ED = '$'. If data contains '$' anywhere, it can be escaped using '\0' character. If data contains '\0' then use \0\0 \0$.

If it is used, the disadvantage is it is very costly & obsolete method.

Each frame starts with DLE STX (Data link escape - start of text) & ends with DLE ETX.

✓ B) Bit stuffing

Let ED = 01111 and if data = 01111, Sender stuffs a bit to break the pattern i.e. appends a 0 in the data 01110 1. Receiver receives the frame. If data contains 01110 1, receiver removes the 0 & reads it.

eg. If data = 0111000 11110 & ED = 01111
↑

then after bit stuffing we have to add a 0 after we see three 1's in the data.

0111 0 000 1110 10

eg. data = 01111, ED = 01111,
↑

we're gonna add 0 after 3 consecutive 1's.

01110 1

eg. ED = 011111 Add 0 after 4 1's
↑

data 011110 011111
↓ ↓
0111100 0111101

Q. G'14. A bit stuffing based framing protocol uses an 8 bit delimeter pattern of 011111 0.
↑
If the o/p bit string after stuffing is 011111 00101, then the i/p string is —

0111110101.

→ In fixed size framing the drawback is it suffers from internal fragmentation if data size is less than the frame size.

Solution to it - use padding (adding dummy bits to data that is less than the frame size).

Physical addressing :

MAC - Local identification
IP - Global identification

2 types of addresses -

a) Physical addresses (static, constant)

b) Logical addresses.

Physical address should be unique within the N/W. Logical address should be unique in the entire world.

IP address - 32 bit no., software no.

(Physical address) MAC address - 48 bit no., hardware no. printed on our NIC → ROM. MAC address is divided into 3 parts -

i) Manufacturer / Vendor ID
ii) Date of manufacture
iii) Serial no. of the device

} Unique globally

** What directs the packet from S to D is the IP address. But, what gets the packet from the S to R_A & then from R_A to R_B & then from R_B to D is the MAC address. MAC address handles the physical connection from computer to computer while IP addresses handle the logical routeable connection from both computer to computer & N/W to N/W.

No 2 devices in a N/W should have same MAC.

→ AppleTalk does not use MAC. It artificially generates a random number & assigns to users.

- Network Layer:

Works for the transmission of data from one host to the other located in different N/Ws. It also takes care of packet routing i.e. selection of the shortest path to transmit the packet, from the number of routes available.

→ If 2 systems are connected to the same link, there's no need for a N/W layer.

→ Main responsibilities:

i) Host to host connectivity

ii) Switching

iii) Routing: Determining how packets will be routed from source to destn. It can be of 3 types - a) static (routes are based on static tables that are wired into the network & are rarely changed), b) dynamic (all packets of one application can follow different routes depending upon the topology of the N/W, the shortest path & the current N/W load), c) semi-dynamic (a route is chosen at the start of each conversation & then all the packets of the application follow the same route).

iv) Congestion control: If all the N/Ws send packets at the same time with maximum rate possible then the router may not be able to handle all the packets & may drop some packets. In this context, the dropping of packets should be minimised & the source whose packet was dropped should be informed. The control of such congestion is also a function of the N/W layer.

Other issues in this layer - transmitting time, delays, jittering.

v) Logical addressing: In order to identify each device on internetwork uniquely, N/W layer defines an addressing scheme. The sender's & receiver's IP address are placed in the header by network layer.

vi) Fragmentation.

→ Services provided by N/W -

i) Connection-less ii) Connection-oriented.

→ N/W layer does not guarantee that the packet will reach its intended destⁿ.

→ Segment in N/W layer is called a packet.

→ Router is a networking device.

(Router has only PL, DL, NL).

- Transport layer :

Responsible for process to process delivery of the entire message. A process is an application program running on a host. Whereas the N/W layer oversees source-to-dest^n delivery of individual packets, it does not recognise any relationship between those packets. It treats each one independently. The transport layer, ensures that the whole message arrives intact & in order. We refer to transport layer packet as a segment.

Main functions –

a) Service point addressing : Transport layer header must include a type of address called service point address (SPA' or port address).

b) Segmentation & reassembly : Data accepted by transport layer from the session layer is split up into smaller units (~~fragmentation~~) if needed & then passed to the N/W layer. The data provided by the N/W layer to the transport layer on the receiving side is reassembled.

c) Connection control : A connectionless transport layer treats each segment as an independent packet & delivers it to the transport layer at the dest^n. A connection oriented transport layer makes

a connection with the transport layer at the dest^n machine first before delivering packets. After all data is transferred, connection is terminated.

d) Flow control (End to end rather than across a single link)

e) Error control (Error correction through retransmission)

f) Multiplexing & demultiplexing

- Session layer: Responsible for dialogue control & synchronisation.

a) Dialogue control: Session layer allows 2 systems to enter into a dialogue. It allows the communication between 2 processes to take place in either half-duplex or full-duplex mode.

b) Synchronization: Allows a process to add checkpoints or sync. points to a stream of data.

- Presentation layer: Concerned with the syntax & semantics of the information transmitted.

a) Translation: Processes in 2 systems are usually exchanging info in the form of character strings, numbers etc. Info must be changed to bit streams before being transmitted.

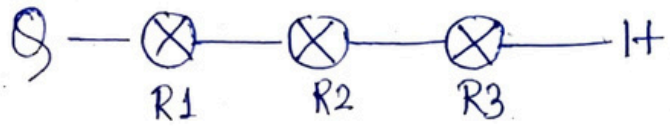
b) Encryption: To carry sensitive data, a system must be able to ensure privacy.

c) Compression: In the transmission of text, audio, video.

- Application Layer:

Enables the user, whether human or software, to access the N/W. Uses protocols like HTTP, FTP, SMTP, DNS etc. Packet of information in this layer is message.

Q. G'14.



S connects to H via HTTP & downloads file.

Session layer encryption is used, with DES as the shared key encryption protocol. Consider these information —

1. URL of the file downloaded by S
2. TCP port no. at S & H
3. IP addresses of S & H
4. Link layer addresses of S & H.

Which of these can an intruder learn through sniffing at R2 alone?

→ Can't learn (1); as URLs & download are functioned at application layer.

✓ Can learn (2) as port no. is encapsulated in the payload field of IP datagram.

Can learn (3), as IP addresses & routers are functioned at N/W layer of OSI model.

Can't learn (4) as it is related to DLL. (Only have MAC addresses of R1 & R3, not B or H)

* A packet is an information unit whose source & destination are network layer entities.

A packet is composed of network layer header (& possibly a trailer) & upper-layer data. The header & trailer contain control information intended for the N/W layer entity in the destination system.

Datagram usually refers to an information unit whose source & destn are N/W layer entities that use connectionless network service.

Segment usually refers to an information unit whose source & destination are transport layer entities.

Message is an information unit whose source & destn entities exist above the N/W layer.

Cell is an information unit of a fixed size whose source & destination are data link layer entities. (Used in switched environments, such as Asynchronous Transfer Mode - ATM & Switched Multimegabit Data Service - SMDS). A cell is composed of the header & payload.

Data unit is a generic term that refers to a variety of information units.

PL: Moves bits b/w devices, specified voltage, rate, pin out cables.

Bit

Protocols – EIA/TIA-232, 100BaseTX, ISDN, 802.11.

DLL: Combines data bytes into frames, perform error detection (not correction) & provides access to media using MAC address, physical addressing, framing

MACL
LLCL
Frame

P - RAPAE, PPP, Frame relay, ATM, fiber cable.

NL: Provisions logical addressing, using which routers route data.

Packet

P- IP, IPX, ICMP, IPSEC, ARP, MPLS.

TL: Provisions con. oriented & -less end-end delivery of segments, error correction

Segment

P- TCP, UDP

SL: Keep different app. data separate & synchronization, dialogue control

P- NETBIOS, SAP

PL: Presents data & handle encryption., translation, compression.

P- MPEG, ASCH, SSL, TLS,

AL: Provides user interface using FTP, HTTP.

P- SMTP, FTP, HTTP, POP3, SNMP.

PL: ISDN (Integrated service digital network), DSL (Digital subscriber line), Ethernet physical layer (10 BASE5, 10BASE-T, 100BASE-T)

DLL: ~~ARP (Addr. resol^n protocol)~~, X
FDDI (Fibre Distributed Data Interface)
HDLC (High level data link control)
VLAN (Virtual LAN)

NLP: ATM (Async. transfer mode), ARP,
SPB (Shortest Path bridging)
IP, ICMP

NL+TR: AppleTalk, IPX (Internetwork packet exchange) / SPX (Sequenced packet exchange), IP suite

TL: TCP, UDP, DCCP (Datagram congestion control protocol),
FCP (Fibre Channel Protocol)

SL: RPC (remote procedure call), H.245, NetBIOS.

PL: TLS (Transport layer security), SSH, Telnet

AL: DHCP (dynamic host config protocol)
DNS, HTTP, HTTPS, POP3, SMTP, TFTP.

Devices.

1. Hubs, repeaters, cables, fibres
2. bridge, modem, network card, 2 layer switch
3. router, brouter (bridge + ..), 3-layer switch
4. gateway, firewall
5. gateway, " , PCs
6. "
7. " phones, servers → User apps

LAN Technologies

* Local area networks (LAN).

Network of computers confined to a small area which may be a room, building or a group of buildings. LAN may be wired, wireless or a combination of both.

* Standard technologies used to build a wired LAN are — ethernet, token ring.

* Ethernet (DLL)

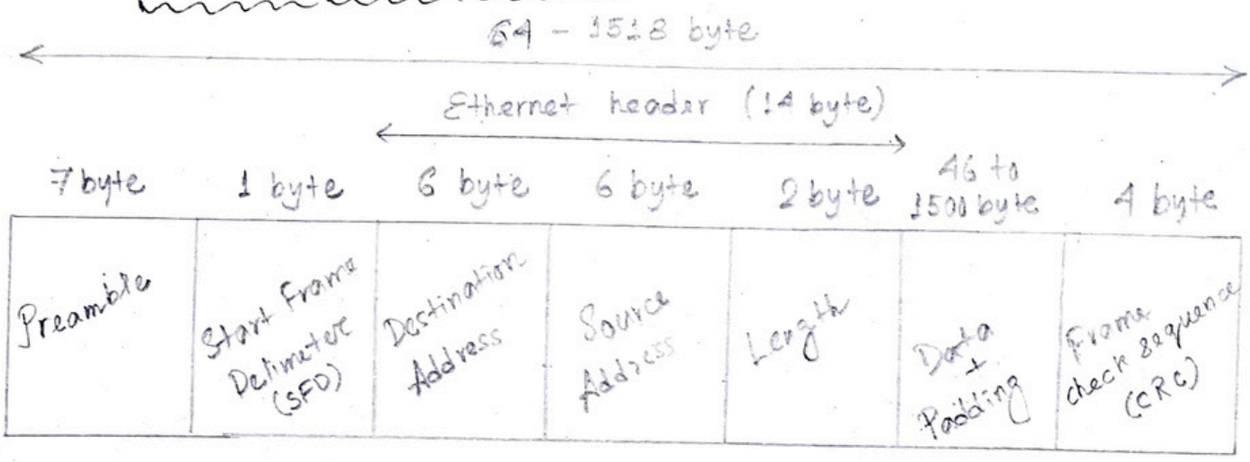
Defined under IEEE 802.3.

→ Characteristics

1. Ethernet uses bus topology.
2. All stations are connected to a single half duplex link.
3. Ethernet uses CSMA/CD as access control method to deal with the collisions.
4. Ethernet uses manchester encoding for converting data bits into signals.
5. Ethernet evolution has four generations -

Standard ethernet	10 Mbps
Fast ethernet	100 Mbps
Gigabit ethernet	1 Gbps
Ten Gigabit ethernet	10 Gbps

→ Ethernet frame format.



1. Preamble : It alerts the stations that a frame is going to start. Also enables the sender & receiver to establish bit synchronisation. It is actually added at the physical layer & is not part of the frame.

2. SFD : Signals the beginning of the frame.

Preamble & SFD are added by the physical layer & represents the physical layer header. Sometimes, SFD is considered to be a part of preamble.

3. DA : MAC address of the dest^n for which data is destined.

4. SA : MAC address of the source that is sending the data.

5. Length: Length of the data field. As ethernet uses variable sized frames, this field is required.

Max value that can be accomodated in this field is $2^{(8+8)} - 1 = 65535$. But, it does not mean max. data that can be sent in one frame is 65535 bytes. Max amount that can be sent is 1500 bytes in a ethernet frame. This is to avoid

the monopoly of any single station.

6. Data: Also called payload field. Length of the field lies in the range [46 bytes, 1500 bytes]. Thus, in an Ethernet frame, min data has to be 46 bytes & max data can be 1500 bytes.

- Minimum length of data field ~

In CSMA/CD (as Ethernet uses it),

min length of data packet $= 2 \times T_p \times B$

$T_t \geq 2T_p$

$L \geq 2T_pB.$

Substituting standard values of Ethernet, it is found the min length of ethernet frame has to be 64 bytes, starting from the destination address field to the CRC field & (72 bytes including preamble & SFD.)

Therefore min length of data field has to be = $64 - (6+6+2+4) = 46$ bytes.

- Maximum length of data field ~ (as per 802.3

max. amount of data that can be sent in a Ethernet frame is 1500 bytes. If Ethernet allows the frames of big sizes, then other stations may not get the fair chance to send their data.

7. Frame check sequence: Contains CRC code for error detection.

→ Advantages of using Ethernet.

i) Simple to understand & implement.

ii) Maintenance easy.

iii) Cheap.

→ Limitations.

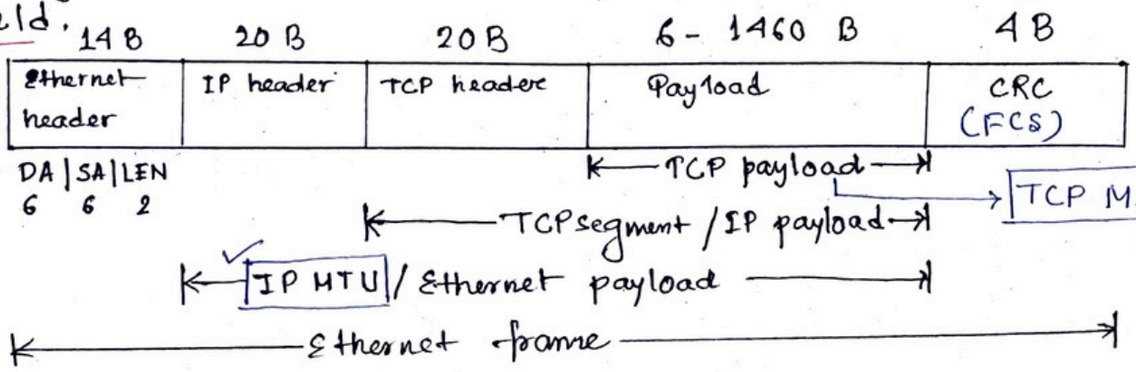
i) It can't be used for real time applications. Real time applications require the delivery of data within some time limit. Ethernet is not reliable for high probability of collisions. High no. of collisions may cause a delay in delivering the data to its destn.

ii) It can't be used for interactive applications. They require the delivery of even very small amount of data (Ethernet min 46 bytes).

iii) Can't be used for client-server applications. They require that server must be given higher priority than clients. Ethernet has no facility to set priorities. (In token ring → prioritization of master node by increased THT)

Token ring overcomes these limitations.

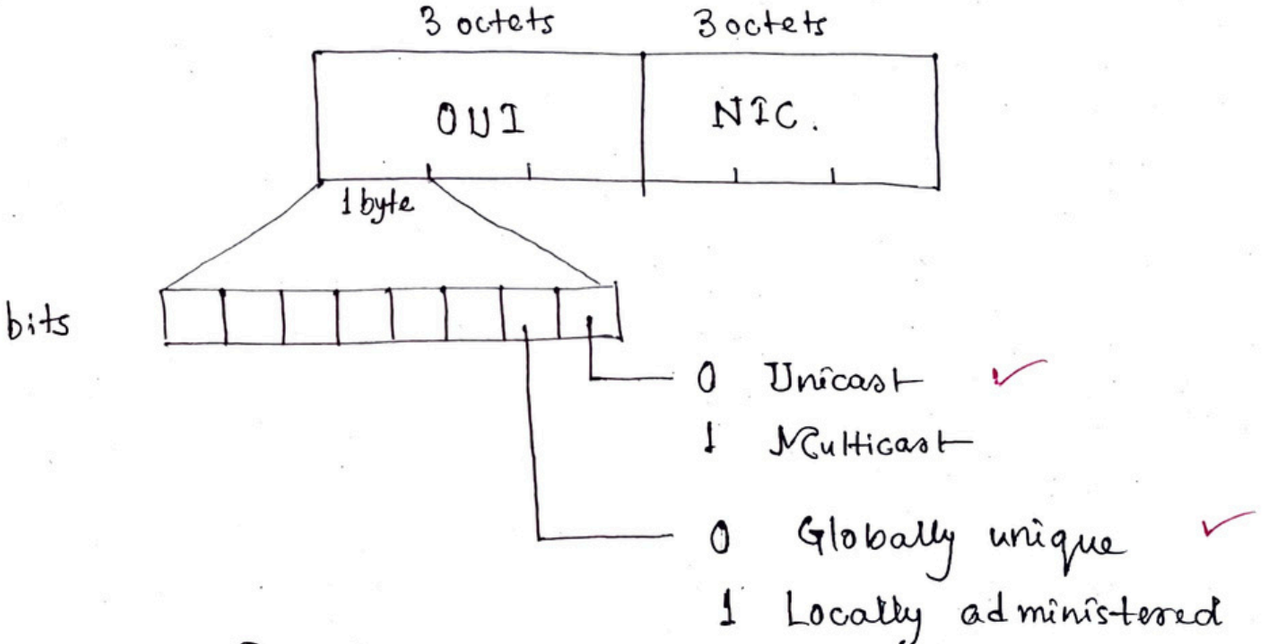
* For data transmission, TCP segment sits inside the IP datagram payload field. IP datagram sits inside the Ethernet payload field.



→ MAC Addressing

Each station on an Ethernet network has its own NIC. The NIC provides the station with a 6 byte physical address.

MAC address is a 12 digit hexadecimal number, represented by colon-Hex notation. First 6 digits identify the manufacturer (Organisational unique identifier). The rightmost 6 digits represent Network interface controller, which is assigned by manufacturer.



Types:

1. Unicast: A unicast addressed frame is only sent out to the interface leading to specific NIC. If the LSB of first octet of an address is set to zero, the frame is meant to reach only one receiving NIC. MAC address of source machine is always unicast.

2. Multicast: Allows the source to send a frame to group of devices. In layer-2 multicast address, LSB of first octet is set to one. IEEE has allocated the address block 01-80-C2-xx-xx-xx for group

addresses for use by standard protocols.

3. Broadcast : Similar to N/W layer, broadcast is also possible on underlying layer (data link layer). Ethernet frames with ones in all bits of the dest^{n} address, referred as broadcast address. Frames which are destined with MAC address FF-FF-FF-FF-FF-FF will reach to every computer belonging to that LAN segment.

eg. AA:30:10:21:10:1A

A = 1010 Hence unicast

eg. 47:20:1B:2E:08:EE

7 = 0111 Hence, multicast

eg. FF:FF:FF:FF:FF:FF

All 1's Hence, broadcast.

Multicast is superset of broadcast.

48 b bin.
↓
12 Hex

8b : ..... : 8b
bin

2dig : ..... : 2dig
Hex

Switching

* Switching : Process of moving the data packets towards their destination by forwarding them from one port to the other port.

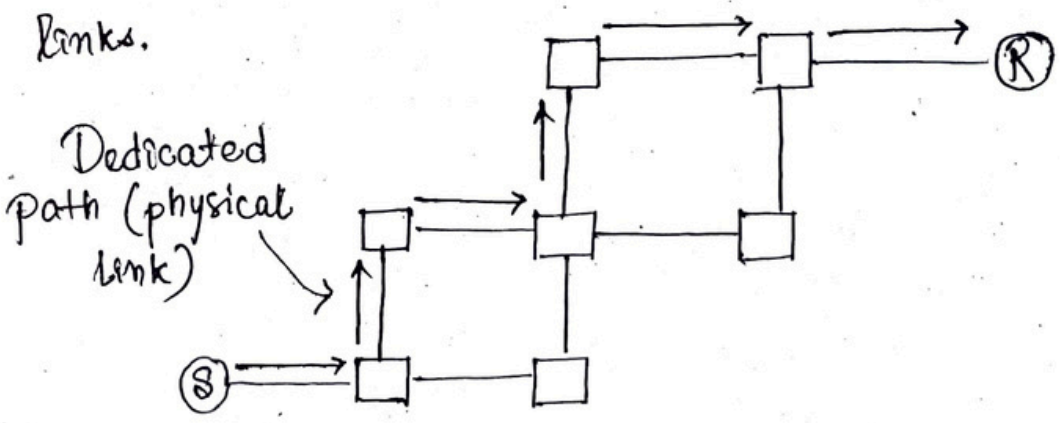
Switching techniques -

1. Circuit switching
2. Message switching
3. Packet switching
   - Datagram switching
   - Virtual circuit switching

* Circuit switching (Implemented at physical layer. Now outdated.)

Operates in 3 phases -

1. Establishing a circuit : A circuit is established between the two ends. Circuit provides a dedicated path for data to travel from one to the other end. Resources are reserved at intermediate switches which are used during the transmission. The intermediate switches are connected by the physical links.



2. Transferring the data. : After the circuit is established, the entire data travels over the dedicated path from one end to the other.

3. Disconnecting the circuit : After the data transfer is completed, the circuit is torn down.

→ Total time :

Time taken to transmit a message in circuit switched N/W =

Connection setup time + T_t + T_p + Tear down time.

→ T_t is independent of the # of links.

Where $T_t = L/B$

$T_p = \frac{\text{\# hops on way} \times \text{distance}}{\text{propagation speed}}$

→ Advantages

i) A well defined & dedicated path exists for the data to travel.

ii) No header overhead.

iii) No waiting time at any switch & the data is transmitted without any delay.

iv) Data always reaches the other end in order.

v) No reordering is required.

→ Disadvantages.

i) Channel is blocked for two ends only.

ii) Inefficient in terms of utilization of system resources.

iii) Time required for establishing the circuit is too long.

iv) Dedicated channels require more bandwidth.

v) More expensive.

vi) Routing decisions cannot be changed once the circuit is established.

Q. Consider all links in the N/W use TDM with 24 slots & have a data rate of 1.536 Mbps. Assume that host A takes 500 msec to establish an end to end circuit with host B before begin to transmit the file. If the file is 512 Kilobytes, then how much time it will take to send the file from host A to B?

→ Bandwidth per user = $\frac{1.536 \text{ Mbps}}{24}$ = 64 Kbps

$T_t = \frac{512 \text{ KB}}{64 \text{ Kbps}}$ = 65536 msec

Time taken to send file = 500 msec + 65536 msec

= 66036 msec.

* Message Switching

No dedicated path to transfer data. The entire message is treated as a single data unit. The message is then forwarded from hop to hop. Store & forward is an important characteristic. The message carries a header that contains the full information about destination. When any intermediate switch receives the message, it stores the entire message. The message is stored until sufficient resources become available to transfer it to the next switch. When resources become available, the switch forwards the message to the next switch.

→ Advantages :

i) It improves the channel efficiency over circuit switched network. In circuit switching, channel is blocked for 2 ends only. But here, more devices can share the channel.

ii) Reduces traffic congestion. The message may be temporarily stored in the route & then forwarded whenever required.

iii) Helpful in setting the message priorities due to store & forward technique.

→ Disadvantages :

i) It requires enough storage at every switch to accomodate the entire message during the transmission.

ii) Extremely slow due to store & forward technique. Also, the message has to wait until sufficient resources become available to transfer it to the next switch.

→ Message switching is replaced by packet switching.

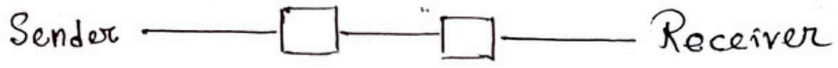
* Packet Switching

→ The entire message to be sent is divided into multiple smaller size packets. This process of dividing a single message into smaller size packets, is called packetization. These smaller packets are sent one after the other. It gives the advantage of pipelining & reduces the total time taken to transmit the message.

→ Optimal packet size :

If the packet size is not chosen wisely, then it may result in adverse effects. It might increase the time taken to transmit the message.

eg. N/W having B = 1 MBps, message size is 1000 B, each packet contains a header of 100 B.



Now, question is, how many packets the message must be divided into to minimise the total time taken to send the message.

We ignore T_p (propagation delay). The reason is in packet switching, T_t dominates over T_p. This is because each packet is transmitted over the link at each hop.

✗ case 1 : Sending in 1 packet only

$$T_t = \frac{(1000 + 100)\ B}{1\ MBps} = 1.1\ msec$$

✓ Time taken = 3 X 1.1 msec = 3.3 msec.
↑ because 3 hops

✗ case 2 : Sending in 5 packets.

Data sent in one packet = $\frac{1000}{5} = 200\ B$

✓ Size of one packet = (200 + 100) = 300 B

✓ $T_t = \frac{300\ B}{1\ MBps} = 0.3\ msec$

Time taken by first packet = 3×0.3 msec
$= 0.9$ msec

Time taken by remaining packets due to pipelining = $4 \times 0.3 = 1.2$ msec.

Total time taken = $0.9 + 1.2 = \underline{2.1 \text{ msec}}$.

After 0.9 ms is over, 2nd by 0.3 ms the receiver will get a packet. 0.3×4 ms

* case-3: Sending in 10 packets

$L = \frac{1000}{10} B + 100 B = 200 B$

$T_t = \frac{200 B}{1 MBps} = 0.2$ msec.

In the beforesaid way, time taken in total =

$(3 \times 0.2 + 9 \times 0.2) = \underline{2.4 \text{ msec}}$.
first other 9

case-4: Sending in 20 packets

$L = \left(\frac{1000}{20} + 100\right) B = 150 B$

$T_t = \frac{150 B}{1 MBps} = 0.15$ msec.

generally,
$t = T_t (\#hops + (n-1))$
↓ for 1 packet ↓ #packets

Total time = $(3 \times 0.15 + 19 \times 0.15) = 3.3$ msec

So, we can conclude –

total time decreas... is reduced but only up to ... after that total time increas...

In the example, ... would be the best choice

Optimal packet size :

$n = \sqrt{\frac{M(\#-1)}{h}}$

packet size = $\left(\frac{M}{n} + h\right)$

M - msg size
- #hops
h - hdr size
n - #packets divided into

In circuit sw^n g, message units don't have to wait at switches, unlike packet switching (where store & forward is used).

In CS → $T_p > T_t$ (have doubt)
In PS → $T_t > T_p$

→ Sending one packet from source to dest^n over a path consisting of N links each of rate R (thus, there are N-1 routers),

$$\text{total delay, } d_{\text{end-to-end}} = N\frac{L}{R}.$$ for one packet

For P packets it will be (as pipelining is used),

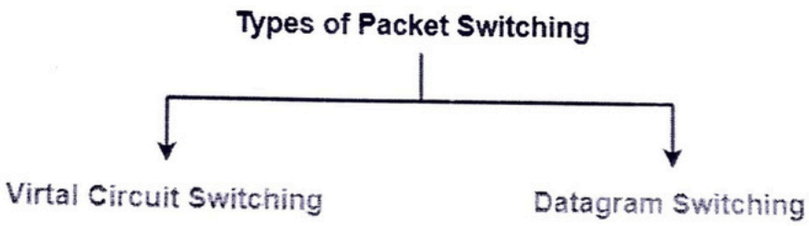
$$d = N\frac{L}{R} + (P-1)\frac{L}{R}.$$

→ Queuing delays & packet loss.

Each packet switch has multiple links attached to it. For each link, the switch has an output buffer / queue, which stores packets that the router is about to send into that link. If an arriving packet needs to be transmitted onto a link but finds the link busy, the arriving packet must wait in the o/p buffer. Thus, in addition to store-and-forward delays, packets suffer o/p buffer queuing delays. These delays are variable & depend on the level of congestion in the N/W. Since, the amount of buffer space is finite, an arriving packet may find that the buffer is full. In this case, packet loss will occur. Either the arriving packet or one of the already queued packets will be dropped (packet dropping).

Types of Packet Switching-

Packet switching may be carried out in the following 2 ways-



1. Virtual Circuit Switching
2. Datagram Switching

Virtual Circuit Switching-

Virtual circuit switching operates in the following three phases-

1. Establishing a circuit
2. Transferring the data
3. Disconnecting the circuit

3. Disconnecting The Circuit-

After the data transfer is completed,

- The connection is disconnected.

Datagram Switching-

In datagram switching,

- There exists no dedicated path for data to travel.
- The header of each packet contains the destination address.
- When any intermediate switch receives the packet, it examines its destination address.
- It then consults the routing table.
- Routing table finds the corresponding port through which the packet should be forwarded.

Virtual Circuit Switching Vs Datagram Switching-

The following table shows a comparison between virtual circuit switching and datagram switching-

Virtual Circuit Switching	Datagram Switching