Chapter 1

Introduction to Computer Network

- **Computer Network:**
  - Collection of autonomous computers interconnected by a technology is known as computer Networks
  - The merging of computers and communication has had a profound influence on the way computer system are organized. Large number of separate but interconnected computers do the job
  - Two computers are said to be interconnected if they are able to exchange information. The connection need not via a copper wire; infrarred, fiberoptic, microwaves and communication satellite can also be used.
  - Although it may sound strange but internet and world wide web are not a computer Network. The internet is not a single network but a network of ~~inte~~ network and web is distributed system that runs on top of the internet.
  - Distributed system: A collection of independent computers appears to its users as a single coherent system. Eg: WWW

- **Merits of Computer Network**

  It's now worth to point out why people are interested in computer network and what they can be used for:

  a. Network for companies
  - i) Resource sharing
    ii) High reliability
    iii) Saving money: Small computer have a much better price/performance ratio than large ones. 'File server' 'client-server' model.
    iv) Scalability: new client can be added as need

v. powerful communication medium

b. Network for people
   i. Access to remote information (BBC online)
   ii. Person to person communication (Skype)
   iii. Interactive entertainment (Eg: Youtube)

c. Social Networking (Eg: facebook)

d. Core banking system (Eg: Temenos T24)

- Better communication
  Better connectivity
  Better sharing of resources
  Bring people together

· **Demerits**
  - Increased cost
  - Security
  - Unavailability of information in case of Network failure.

· **A Communication model**

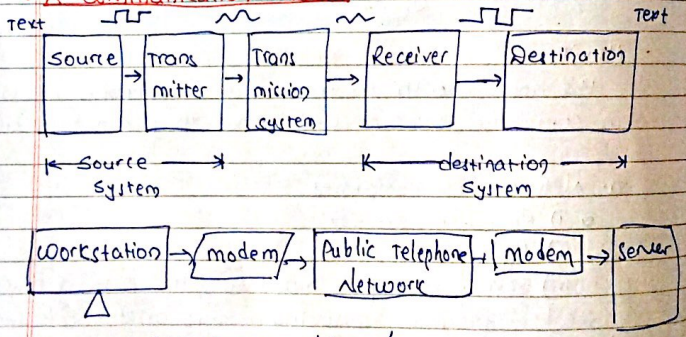


fig: General block diagram
fig: Example of communication model.

Source: Generates data to be transmitted.
Transmiter: Convert data into transmitable signals.
Transmission system: carries data.
Receiver: Converts recived signal into data.
Destination: Takes incoming data.

· **Direction of data flow:** Multiplexing

i) Simplex: only one way communication at any instant. Eg: TV, radio

ii) Half Duplex: either one of the direction of data flow at a time Eg: Police radio, walkie-talkie

iii) Full duplex: both way communication at a time
Eg: Telephone communication

— **Types of communication service** (Nlw hardware) (Transmission Technology)
- Point to point (unicast)

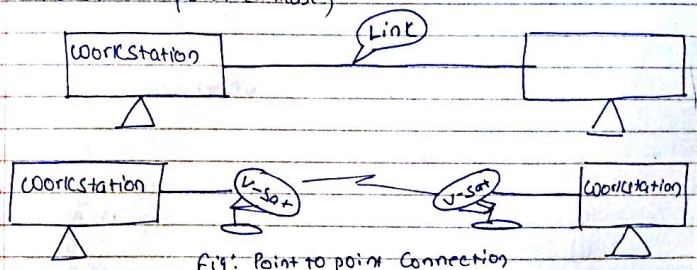


fig: Point to point Connection

(Broadcast) Multipoint

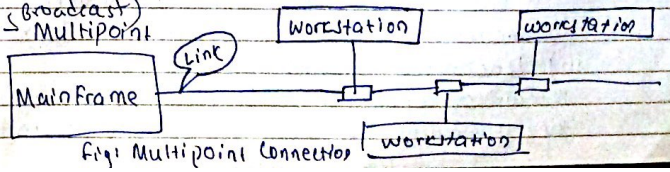
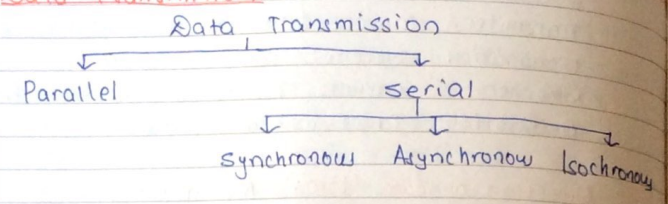


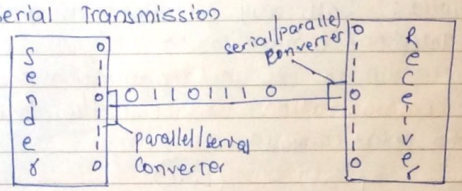
fig: Multipoint Connection

Data Transmition



a. Parallel Transmission

b. Serial Transmission



8 bits are sent one after another

i) Asynchronous Transmission
It can occur at any time with an arbitary delay between the transmision of two data item : email, blog

ii) Synchronous Transmission
It occurs continously with no gap between the transmision of two data item : chat room, calls

iii) Isochronous Transmition
It occurs at regular interval with a fixed gap between the transmission of two data item : video conferensing

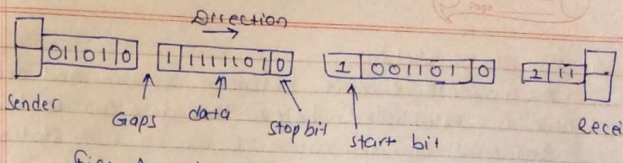
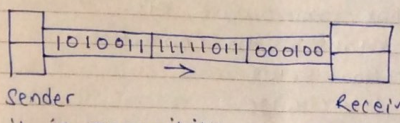


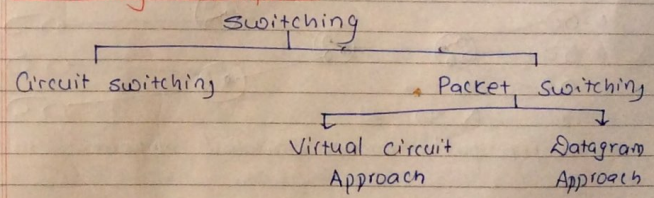
Fig: Asynchronous



it is responsibility of receiver to group Isort the bit.
fig: Synchronous

In Isochronous :
- Fast steady and uninterrupted data stream
- Necessary for Multimedia application
- JIT (Just in Time) delievery
- It is designed to accept and send data rate at a fixed rate ℓ
- Provides each stream a gaurenteed time slot of 125 μs

Switching Techniques



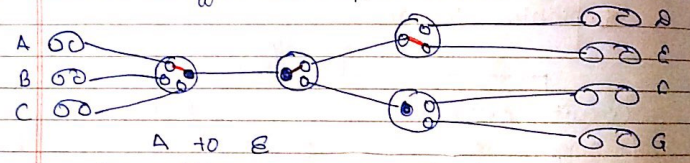
a. Circuit switching:

- A complete circuit between source and destination node is established before the data can be transmitted
- Dedicated communication between two stations
- Communication link: Telephone line, Coaxial cable, Satellite link, microwave etc.
- Steps to establish the connection:
  1. Connection setup
  2. Data interchange
  3. Connection Termination

Problems

1. Inefficient
   - Channel dedicated for the duration of connection
   - If no data, capacity is wasted
2. Setup connection takes time
3. Once connected, transfer is transparent
4. Developed for voice traffic
5. Ckt switching usually uses fixed rate (64Kbps) and is difficult to support variable data rate

eg:



A to E

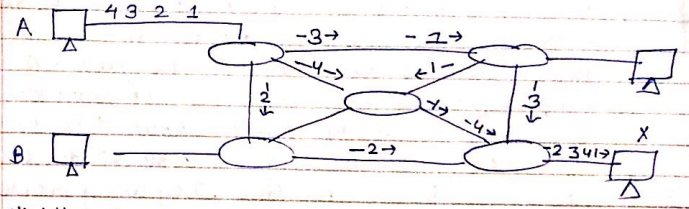
Fig: public circuit switched Network

b. Packet switching

- Data transmitted in small packets
- Each packet contains user data plus control information
- Control information contain Routing information

(i) Datagram Packet switching

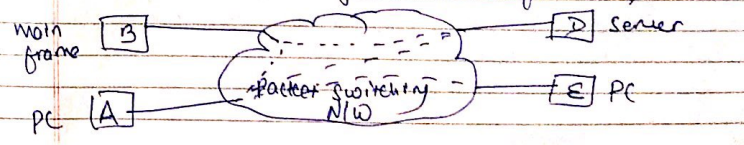
- No need to establish the connection between the source and destination
- Route choosen on packet by packet basis
- Packet may be stored until delievered (store & forward)
- Different packets may follow different routes
- Packets may arrive out of order at the destination



(ii) Virtual Circuit switching

- Route is choosen at the start of session and it is only a logical connection
- All packets associated with a session follow the same path.
- Packets are labeled with a VC# designated the route
- The VC number must be unique on a given link.
- Packets are forwarded more quickly (no routing decision)

Example: ATM (Asynchronous Transfer Mode)



Network Hardware

There are two types of transmission technology that are in widespread use. They are as follows:

1. Broadcast links
2. point to point links

a. Broadcast links:

It have a single communication channel that is shared by all the machines on the nlw. short messages called packets in certain contexts, sent by any machine are received by all the others. An address field within the packet specifies the intended recipent. Upon receiving a packet, machine checks the address field, if the packet is intended for the receiving machine, that machine processes the packet. If the packet is intended for some other machine it just ignore it

Eg: A person at the hotel shout "Watson! come here! I want you". Although the packet (voice) may be received (heard) by many people. only watson responds. The other just ignore it. This is called broadcasting.

b. Point to point

Point to point Nlw consist of many connection between individual pairs of machine. To go from the source to the destination, a packet on this type of network may have to first visit one or more intermediate machine. Point to point transmission with one sender and one receiver is called unicasting

→ we classify multiple processor systems by their physical size.

- Personal Area Network, networks that are meant for one person Eg: wireless nlw connecting a computer with its mouse.

- The connection of two or more networks is called an internetwork. Eg: world wide internet

InterProcessor distance	Processors located in same	Example
1 m	Sq. meter	Personal Area Nlw
10 m	Room	Local Area Network
100 m	Building	
1000 m = 1km	Campus	
10 km	City	Metropolitan Area Network
100 km	country	Wide Area Network
1000 km	continent	
10,000 km	Planet	The internet

* Physical Topologies

- Physical layout of the Network
- It is a geometric representation of the relationships of all the links and linking devices
- Linking device are called Nodes
- Four Basic possible Topologies are:
  - Bus Topology
  - Star Topology
  - Mesh Topology
  - Ring Topology

Network categories

- Local Area Network (LAN)
- Metropolitan Area Network (MAN)
- Wide Area Network (WAN)
- Campus Area Network (CAN)*
- Country Area Network (CAN)**
- Personal Area Network (PAN)
- Global Area Network (GAN)

LAN	WAN
- Connects host within a relatively small geographical area · Same building · Same room	- Hosts may be widely dispersed • Accross campuses • Across cities/countries
- Faster, cheaper	- slower, expensive
- under a control of single ownership	- Not under a control of a single person
- Typical speed: 10MBps to 10 Gbps	- Typical speed: 64 Kbps to 8 Mbps

Modes of Communication

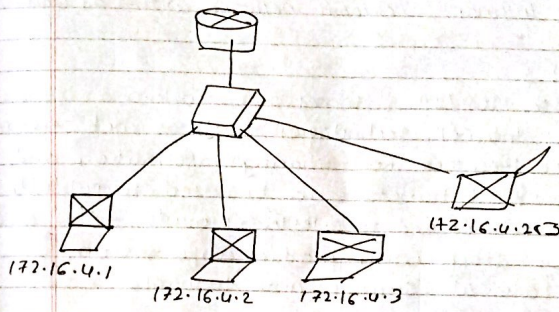
In an IPv4 network, the host can communicate one of three different ways

1. Unicast :- The process of sending a packet from one host to an individual host.
2. Broadcast : the process of sending a packet from one host to all hosts in the network.
3. Multicast : the process of sending a packet from one host to a selected group of hosts.

1. Unicast Transmission

Source 172.16.4.1

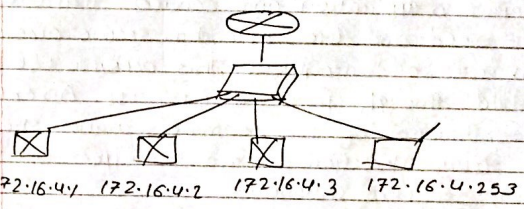
Destination: 172.16.4.253



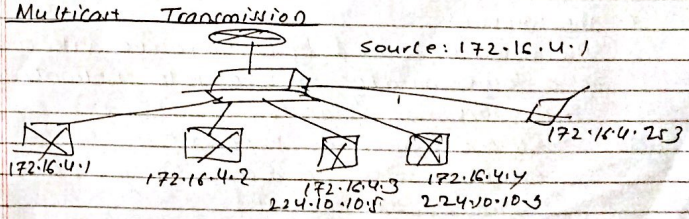
2. Broadcast transmission

Source: 172.16.4.1

Destination: 255.255.255.255



3. Multicast Transmission



Inter - Networking

- Intra Net : Network within an Org.
- Internet : Network bet^{n} diff other org.
- The Internet : Global network within an Universe

A. Intranet :

A private TCP/IP internetwork within an organization that uses Internet technologies such as web servers and web browsers for sharing information and collaborating. Intranets can be used to publish company policies and newsletter, provide sales and marketing staff with product information, provide technical support and tutorials

- Intranet VPN
- Extranet VPN

B. Extranet

It refers to application and services that are intranet based and use extended, secure access to external user or enterprises. This access is usually accomplished through password, user IDs. An Extranet is the extension of two or more intranet strategy with a secure interaction between participant enterprises and their respective intranets.

C. The Internet

The network formed by co-operative interconnection of a large number of Computer networks.

- Network of Networks
- No one owns the Internet
- Everyperson who makes a connection owns the slice of the Internet
- There is no central administration of the Internet

Topology :

1. physical topology :

The way in which a network is laid out physically. The actual layout of the wire or media. Two or more devices connect to a link : two or more links form a topology.

- Bus topology
- Ring topology
- Star topology
- Extended star topology
- Mesh topology
- Extended Star topology

2. logical topology

It defines how the hosts access the media to send data. shows the flow of data on a network.

types :

(i) broadcast topology indicates that each host send its data to all other hosts on the network medium.

(ii) token passing

An electronic token is passed sequentially to each host. When host receives the token, the host can send data on the network

Example : Token Ring
: Fiber Distributed Data Interface (FDDI)

Network Model / Architecture

1. Peer to Peer Model
2. Client-server Model

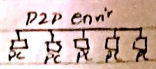
A. Peer to Peer Model :

- No use of dedicated servers

As in P2P, network computers act as equal partners, or peers. As peers, each computer can take on the client function or the server function.
Example: Computer 'A' may request for a file from computer 'B', which then sends file to 'A'. Computer 'A' acts like the client and computer 'B' acts like the server. At a later time, Computer A and B can reverse the role.

In P2P Nlw, individual users control their own resources
- user may decide to share certain files with others
- user may also require passwords.
- P2P nlw works well with ten or fewer computers.
- P2P donot scale well, their efficiency decreases rapidly as the computer increases.

Client-server model or network can be used to overcome the limitations of P2P network.



B. Client-Server Model :

Client/server describes the relationship between two computer programs in which one program, the client makes a service request from another program, the server, which fulfil the request. client/server model provides a convenient way to interconnect programs that are distributed efficiently across different location.

Example: To check your bank account from your computer, a client-program in your computer forwards your request to a server program of the bank.

Client-Server Vs Peer-to-Peer Network

Peer to Peer	Client-Server
Advantage	**Advantage**
- less expensive to implement - doesnot require network administrative softwares - Doesnot require a dedicated network administrator	- Provides a better security - Easier to administer because administration is centralized - All data can be backed up on one central location
DisAdvantage	**DisAdvantage**
- Does not scale well to large nlw and administration is unmanageable. - less secure - All machine sharing the resources negatively impact the Performance - Each user must be trained to perform administrative works	- Requires expensive, specialized network administrative and operational software. - Requires a professional Administrator - Has a single point of failure ~~each~~ user data is unavailable if the server is down. - Requires more expensive, powerful h/w for server machine

chapter 2

Reference Model

* Network Software :

Network software is a set of primitives that define the protocol between two machines. The nlw software resolves an ambiguity among different types of network making it possible for all the machines in the network to connect and communicate with one another and share information.

Network software is used to efficiently share information among computers. It encloses the information to be sent in a 'package' that contain a 'header' and a 'trailer'. The header and trailer contain information for the receiving computer, such as the address of that computer and how the information package is coded.

* Protocols :

- A protocol is set of rules that governs the data and communication
- For communication to occur, the entities must agree on a protocol
- The key elements of a protocols are
  1. Syntax : Structure / format of data.
  2. Semantics : Meanings of each data
  3. Timing : how fast and when data should be sent

"French scientist cannot communicate with Japanese scientist without any protocol"

* Standards

- It provides a guidelines to Manufacturers for interoperability.
- Creates open and competitive market for manufacturers
- Data communication standards falls into two categories
  1. De-facto
  2. De-jure
- De-facto standards have not been approved by organization
- Standards through wide spread use are De-facto standards
- De-jure standards have been legalized by an org.

Standard organization :
ISO : International organization of standardization
ITU : International Telecommunication Union
ANSI : American National Standards Institute
IEEE : Institute of Electrical and Electronics Engineer
EIA : Electronic Industries Association

Extra: Network software : Protocol Hierarchies
- Stack of layer → Protocol stack / Protocal Suite
- Each layer provides service to layer above it.
- No direct data transfer from layer n on one machine to other.
- Through physical Medium actual communication occurs.
- layer n on one machine carries a conversation with layer n on another machine. The rules and conventions used in this convention is known as layer n Protocol.

- To reduce their design complexity, most network are organized as a stack of layers or levels, each one built upon the one below it. The number of layers, contents of each layer, function of layers differ from network to network.
- In a sense, each ~~kin~~ layer is a kind of Virtual machine, offering certain services to the layer above it.
- Through Physical Medium actual communication occurs.

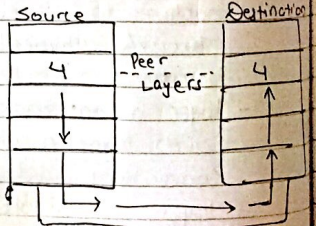
Layer Communication

- In order of data packets to travel from a source to a destination on a network, it is important that all devices on the network speak the same language or protocol
- A protocol is a set of rules that make communication on a network more efficient.

Example: While flying an aeroplane, pilots obey very specific rules for communication with other aeroplanes and with air control

Data Communication protocol is a set of rules or an agreement that determines the format and transmission of data.

A protocol in one layer perform a certain set of operation on data as it prepares the data to be sent over the network. The data is then passed



to the next layer where another protocol performs a different set of operations.

- Once the packet has been sent to the destination, the protocols undo the construction of the packet that was done on the source ~~code~~ side. This is done in reverse order.
- The protocols for each layer on the destination return the information to its original form so the application can properly read the data.

* Design Issues for the layer

- Some form of addressing is needed in order to specify a specific destination.
- Concern ~~for~~ the rules of data transfer ie. data in one direction and data in two direction.
- Error control is an important issue. Many error detecting and correcting codes are known.
- Receiver must have some way of telling to sender which data correctly received and which
- Issues with fast sender with slow receiver. Flow control should maintained.
- When multiple paths between source and destination, routing should be done

or: # (I) Addressing (II) Segmentation and Reassembly (III) Encapsulation (IV) Flow control (V) Error Control (VI) Multiplexing and Demultiplexing (VII) Routing (VIII) Connection Control
- Connection oriented Service
- Connectionless service.

OSI Reference Model

- The protocols associated with OSI model are rarely used anymore, the model itself is actually quite general and still valid, and the features discussed at each layer are still very important.
- The model proposed by ISO.
- ISO (open system interconnection) because it deals with connecting open systems.
- It has seven layers
- A theoretical system delievered too late

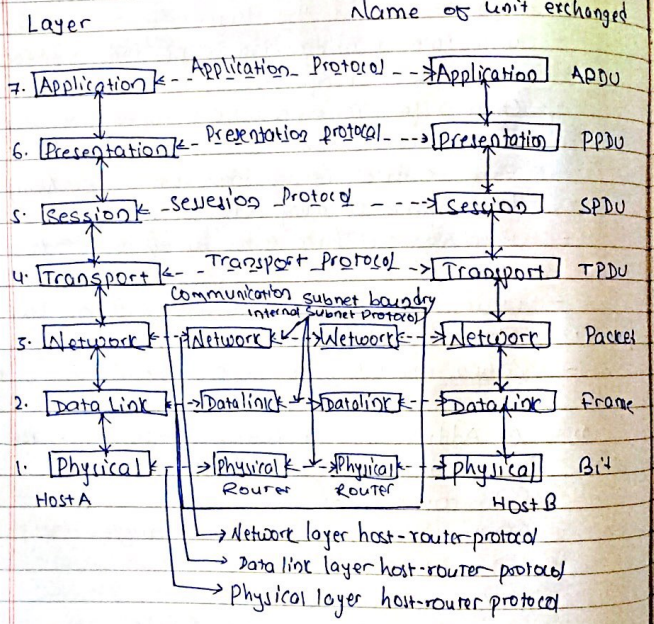


Fig: OSI reference Model

Function of OSI layers

(i) Physical Layer

- Concerned with transmitting individual bits over a communication channel
- Deals with physical characteristics of interfaces and Medias [electrical and mechanical, and timing]
- questions like how many volt used to represent a 1
- whether transmission proceed in two direction
- how initial connection established

(ii) Data link layer

- Enable node to node communication
- The main task is to transform a raw transmission facility into a line that appears free of undetected error to network layer
- break up the input data into data frames and transmit the frames sequentially.
- Receiver sends back an acknowledgement frame.
- keep a fast transmitter from drowning a slow reciever (traffic regulation mechanism is needed)
- Broadcast networks : how to control access to shared channel [CSMA/CD]

(iii) Network Layer

- how packets are routed from source to destination
- Route can be ~~stat~~ based on static table (determined at start of each conversation
- They can be highly dynamic
- quality of service is a network layer issue
- if too many packets, they will get in one's another way, forming bottle neck.

- The addressing used by second nlw may different
- Packet could be too large
- Protocol may differ
- In broadcast nlw, the routing problem is simple so the nlw layer is often thin or even non-existent.

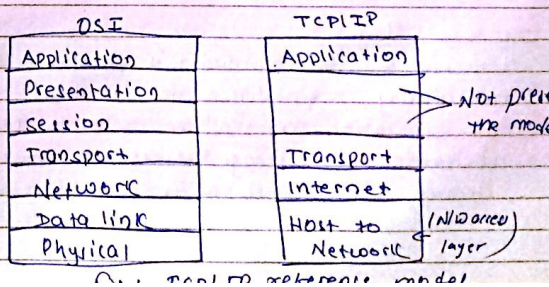
4. Transport layer
- Accept data from above, split it up into smaller unit if need be, pass these to nlw layer and ensure that the pieces arrive correctly.
- determines what types of service to provide to the session layer and ultimately users.
- The most popular type of transport connection is an error free point to point channel and delievers message or bytes in order in which they were sent
- Transport layer is true end-to-end layer, all the way from source to destination. (One machine conversation with another machine using the message header and control messages.
- In lower layer, protocols are between each machine or immediate neighbours.
- layer 1-2-3 are chained, layer 4,5,6,7 are end to end.

5. Session layer
- it allows users on different machines to establish sessions between them.
- session offer service like
  - dialog control (keeping track of whose turn it is)
  - token mgmt
  - synchronization
- Dialogue Discipline → half duplex / full duplex

6. The Presentation Layer
- lower layer move bits
- It concerned with syntax and semantics of the information transmitted
- Different computer use different data representation, it provide an abstract, standard encoding
- Data Formats, Data Compression, Encryption

7. Application Layer
- Responsible for providing service to end users.
- Contains a variety of protocols commonly used by user
- Mail transfer service
- file Transfer Service

TCP/IP Reference model
- ARPANET was a research nlw sponsored by DOD (US Department of defence). It eventually connects hundreds of universities and government, using telephone lines.
- when sattelite and radio nlw were added, existing protocols had trouble interworking with them.
- "The ability to connect multiple networks in a seamless way was one of the major design goals from very beginning". This architecture called TCP/IP ref. model



1. TCP/IP means Transmission Control protocol and Internet protocol (DOD). it was developed because:
- supports for a flexible architecture. (adding more machines)
- Network was robust,
- The ov allow one application on one computer to communicate to another application running on different computer.

2. Host to Network layer
- lowest layer
- to connect to the host, so that packets can be sent over it
- varies from host-to-host and n/w-to-n/w.

2. Internet Layer:
- Selection of packet switching n/w which is based on connectionless Internetwork layer is called Internet layer
- It is the layer which holds the whole architecture together.
- It helps the packet to travel independently to dest^n.
- Order of receive is diff than way they are sent
- IP (Internet protocol) is used in this layer.

3. Transport Layer
- It decides if data transmission is parallel or serial trans^n
- multiplexing, segmenting or data is done.
- The application can read or write to Transport layer.
- It breaks the message (data) into small units
- Arrange the packets to be sent, in sequence.

4. Application Layer
The TCP/IP described a lot of application that were at the top of protocol stack. Some of them are
- TELNET: two-way communication protocol which allows connecting to remote machine
- FTP (File Transport protocol): allows file transfer
- SMTP (Simple mail Transfer protocol): allows electronic mail
- DNS (Domain Name Server): resolves an IP address into a textual address for hosts connected over a network.

Merits of TCP/IP model:
- It operated independently.
- Scalable,
- client/server architecture
- supports a no. of routing protocol (SMTP, FTP)
- can be used to establish a connection bet^n two computer

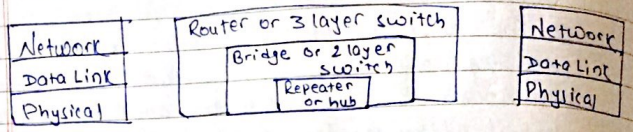
DeMerits of TCP/IP
- Transport layer doesnot gaurantee delievery of packets
- The model cannot be used in any other application
- Replacing protocol is not easy.
- not clearly separated its service, interfaces and protocol

OSI	TCP/IP
1. guarantees the delievery of Packets	1. doesnot
2. less eligible 7 layer	2. more, 5 layer
3. follows vertical approach	3. follows horizontal approach.
4. OSI is a reference model, from which other built.	4. Implementation of OSI
5. N/w layer provides both connectionless or connection oriented service.	5. Provides connectionless service

~~6. It fits on any protocol~~

Networking Hardware

Hub and Repeaters



① Repeater
- Repeater forwards each frame
- It has no filtering capability
- Repeater is a regenerator Not an Amplifier
- Operater as a physical layer
- regenererate the signal before signal gone weak.
- Copy the signal bit by bit
- It is a 2 port device

② Hub
- multiport repeater
- Connects multiple wires coming from different branches
- cannot filter data, datapackets are sent to all connected device, collision domains of all host connected through Hub remains one.
- donot have intelligence to find out best path for data packets which leads to inefficience and wastage.

③ Bridge
- It operates a data link layer
- is a repeater, with add on functionality of filtering content by reading the MAC address of source dest.
- Used to connect two LANS working on same protocol.
- It has single dlp, single ilp port, hence 2 port device.

④ Switch:
- is a multiport bridge with a buffer and a design that can boost its efficiency (large no. of ports → less traffic)
- is a data link layer device.
- perform error checking before forwarding data, that makes it very efficient as it doesnot forward packets that have error
- divides collision domain of host but broadcast domain remains same

⑤ Router:
- device like switch that routes data packets based on their IP addresses.
- mainly a nlw layer device
- connects LANs and WANs together & have dynamically updating routing table base on which make decisions on routing the data packets.
- Router divide broadcast domains of hosts connected through it.

⑥ Gateway:
- is a passage to connect two networks together that may work upon different nlwing models.
- works as a messenger agent, takes data from one system, interpret it, transfer to another system.
- also called protocol converters
- can operate on any nlw layer
- more complex than switch or router.

① Twisted pair cable
- most common, cheaper, lightweight
- easily installed, supportive, availability
- frequency range 0 to 3.5 kHz
- typical attenuation : 0.2 dB/km @ 1 kHz
- Typical delay is 50 μs/km
- Repeater spacing is 2km

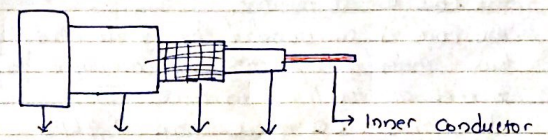
types
ⓘ Unshielded twisted pair (UTP)
ⓘⓘ Shielded twisted pair (STP)
- cable connector → RJ45 and RJ11

STP:
- metal foil covered, which encases each pair of insulated conductors
- electromagnetic noise penetration is prevented by metal coring.
- Same attenuation as unshielded twisted pair
- more expensive than UTP
- can be used for digital or analog
- heavy

UTP
- Common types, consist two conductor, each with its own color plastic insulator
- Color → identification easy
- 100 m limit
- used in ethernet
- bandwidth lower

ⓘⓘ Co-axial cable
- Contain 2 conductor that are parallel to each other
- copper is used in this as centre conductor which can be a solid wire a standard one

-surrounded by PVC installation, a sheath which is encased in an outer conductor of metal foil, braid or both.
- it can span longer distance with higher rates
- metallic coupling act as a shield against coupling

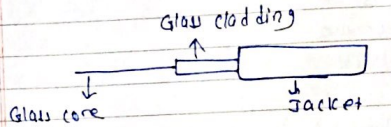


Baseband:
This is 50 ohm (Ω) coaxial cable which is used for digital transmission. It is mostly used for LANs Baseband transmits a single signal at a time with very high speed. The major drawback is that it needs amplification after every 1000 feet

Broad band:
- This uses analog transmission on standard cable tv cabling. It transmits several simultaneous signal using different frequencies.
- Covers large area than baseband

• Expensive, difficult to install, long distance, high bandwidth
- transmits digital signals at a very high rate of 10Mbps

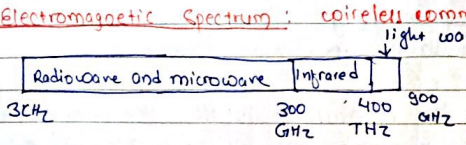
(iii) fiber optic cable
- Similar to coaxial, uses electric signals to transmit data,
- At the centre is the glass core through which light propagates.
- the core is 50 microns,
- The core is surrounded by glass cladding with lower index of refraction as compared to core to keep all the light in core.
- bandwidth : 60 more than 2 gbps



Advantage: high quality transmission at high speed
- not affected by electromagnetic interference so noise and distortion is very less
- used for both analog and digital signal
- lower attenuation

Disadvantage: expensive, difficult to install.
- donot allow complete routing of light signals.

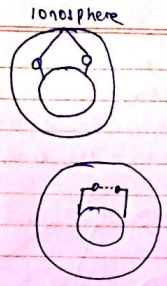
* Electromagnetic Spectrum : coireless communication



① Propagation method

a.) 

Ground propagation below 2MHz



b. Sky Propagation 2-30 MHz

c. Line-of-sight propagation above 30 MHz

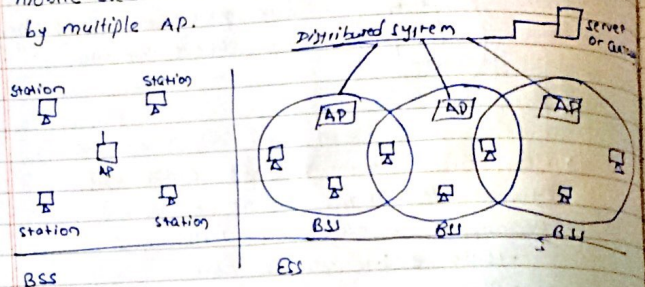
* Wireless Communication (WLAN): Architecture
- Growing technologies, found everywhere
- Promising wireless LAN Technologies
  - IEEE 802.11 wireless LAN
  - Bluetooth
- IEEE 802.11 wireless LAN is also referred as wireless ethernet
- A Bluetooth LAN is an ad hoc Network.
- The gadgets find each other and make a nlw called piconet
- Bluetooth is defined by IEEE 802.15 standard.
- It defines wireless PAN operable in an area of room.

ESS: Extended service set
Bss : Basic service set
AP: Access point
SSID: Service set ID

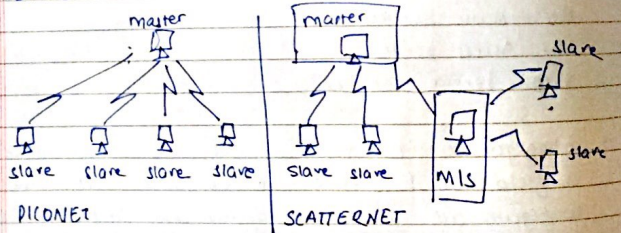
- When you configure your wireless access device, you notice a field called service set ID (SSID). You must configure all connecting devices and APs in a service set to use the same SSID.
- two type: BSS and ESS

① BSS consist of a group of computers and one AP which links to a wired LAN.

② ESS consists of more than one AP. An ESS lets mobile users roam anywhere within the area covered by multiple AP.



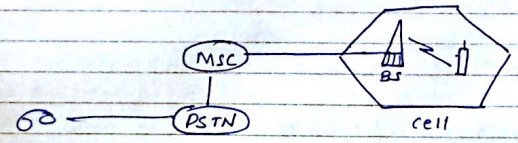
+ PICONET	Scatternet
- In this nlw, device can function either as master or slave	- In this nlw, device can function as master or slave
- It serves smaller coverage	- large coverage
- Connect maximum 8 node	- more than 8 nodes
- It allows less efficient use of available bluetooth channel bandwidth	- It allows more ~~two~~ efficient use of available bluetooth channel bandwidth



+ Cellular System
- Partitioned the region into smaller regions called cells.
- Each cell gets atleast one Base station (BS) or tower
- Users within a cell talks to the tower.
- How can we divide the region
- cellular structure

Advantage: more capacity due to frequency reusage
less transmission power needed
more robust, tolerate failures

Frequency reuse factor
- available channel
- N adjacent cells (cluster), system has M clusters (N cells ~~set~~ share S channels)
- Each cells get K channel
$S = KN$
- capacity of system $C = MKN$
- Frequency reuse factor is $1/N$



MSC: mobile switching center
PSTN: public switched telephone Network

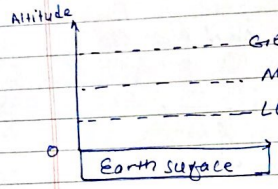
Satellite categories

Satellites

GEO (Geo-Stationary earth orbit) | MEO (Medium) | LEO (Low)

A communication satellite is a station in space that receives microwave signals from on earth based stations, amplifies the signals and broadcast the signal back over a wide area to many earth-based stations.

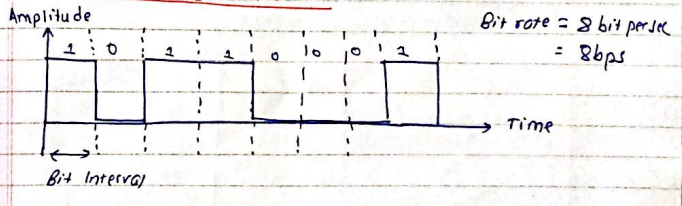
Application:
- tv and radio, weather forecast
- Videoconferencing
- Global positioning system (GPS)



* Geosynchronous orbit (GSO)
- is an orbit around Earth of a satellite with an orbital period that matches Earth's rotation on its axis.
- takes sidereal day (23H, 56m, 45)

* Bandwidth
- property of medium
- difference bet^n highest and lowest frequencies that the medium can satisfactorily pass.
- Bit rate and Bandwidth are proportional to each other.

* Bit rate and Bit Interval



- Bit interval is the inverse of Bit rate.
- Analog bandwidth in Hz, digital bits per second

* Baud Rate vs. Bit rate
- Baud rate of a data communication system is the no. of symbols per second transferred.
- Symbol may have more than two states
  Bit rate = Baud per second x No. of bits per baud
- Bit rate is 6 times the Baud rate
  Passenger in a Highway Bus.

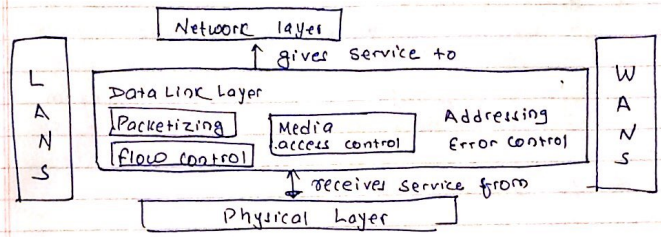
Throughput : is the number of bits passing through this coail in a second.

Bandwidth delay product refers to the product of a data link's capacity and its round-trip delay time
↳ in bits per second ↳ in seconds.

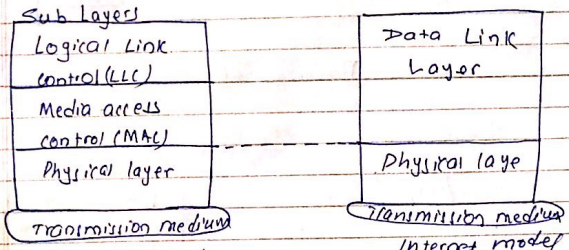
* Jitter:
- The internet makes no guarantee about time of delievery of a packet
- Consider an IP telephony session
- A packet pair's jitter is the difference between the transmission time gap and receive time gap.

Chapter 4

Data Link layer



Duties of Data Link Layer:
1. Packetizing
2. Addressing
3. Error Control
4. Flow control
5. Access Control

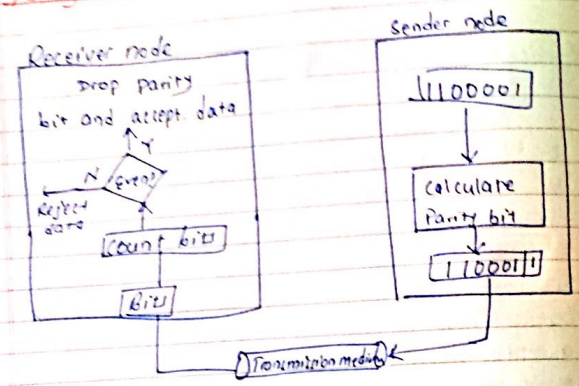


Error Detection

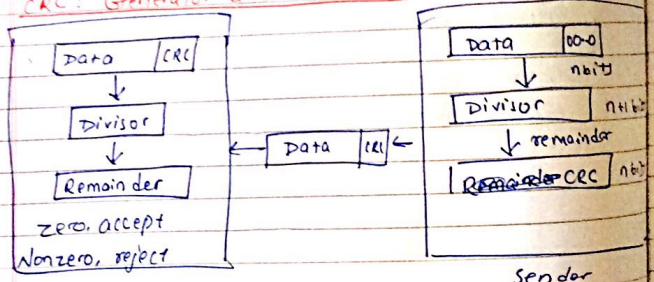
Detection methods

Parity check | cyclic redundancy check | Checksum

① Parity check



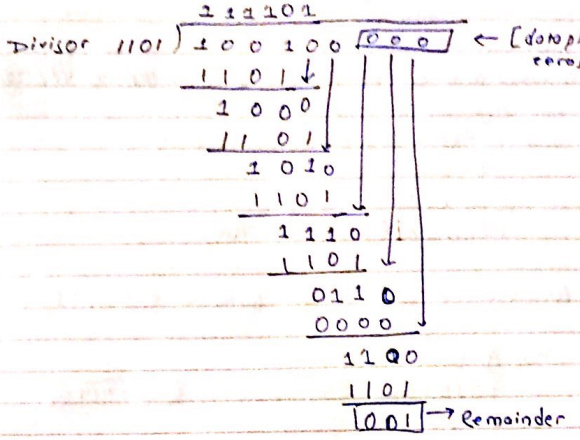
* CRC : Generator and Checker



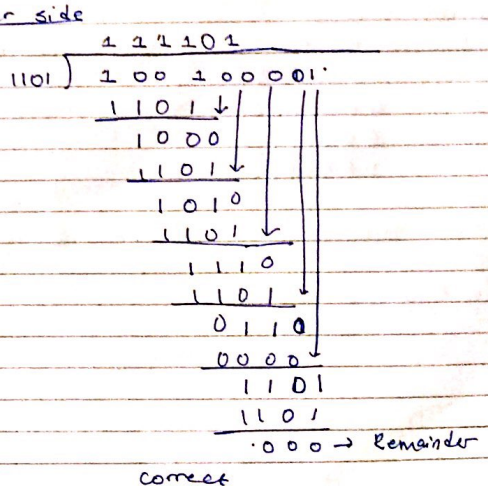
: Receiver — cyclic Redundancy check (CRC)

Sender side :

• When the leftmost bit of the remainder is zero, we must use 0000 instead of the original divisor.



Receiver side



correct

* Checksum

Receiver: If the result is 0, keep else discard

Qn. checksum example

Suppose the block of 16 bits is to be sent using a checksum of 8 bits [10101001 00111001]

→ Sender side

step1: two 8 bit no. are added

```
  10101001
+ 00111001
  11100010   ← Sum
```

Complement's by 1 of sum = 00011101

The pattern sent is

10101001 00111001 **00011101**

→ Receiver side is

The received data along with checksum is added

```
  10101001
  00111001
  00011101
  11111111
```

Compute one's complement of Sum = 00000000

No error in transmission

* Error correction by Retransmission
  - Stop and wait ARQ
  - Go Back N ARQ
  - Selective repeat ARQ

ARQ = Automatic repeat request

Error correction by forward error control
✓ Hamming code.

Hamming Code

- Given by R.W. Hamming
- Easy to implement
- 7 bit hamming code is used commonly

→ data bits - 4 , parity bit - 3 → $2^n \geq n+1, n$

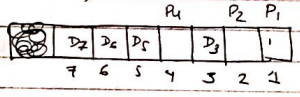
For Place of parity (for n = 7)

$2^0 = 1 \rightarrow P_1$

$2^1 = 2 \rightarrow P_2$

$2^2 = 4 \rightarrow P_4$

$2^3 = 8 \rightarrow$ out of range



$P_1 \rightarrow D_3\ D_5\ D_7$

$P_2 \rightarrow D_3\ D_6\ D_7$

$P_4 \rightarrow D_5\ D_6\ D_7$

1	001	P_1
2	010	P_2
3	011	$\{P_2, P_2\}$
4	100	P_4
5	101	$\{P_1, P_4\}$
6	110	$\{P_2, P_4\}$
7	111	$\{P_1, P_2, P_4\}$

Example

Data : 1011

P_4	P_2	P_1
1	0	1	0	1	0	1
D_1	D_2	D_3	D_4

P_1 = D_3 D_5 D_7 : 1 1 1 (1) for even parity

P_2 = D_3 D_6 D_7 : 1 0 1 (0)

P_4 = D_5 D_6 D_7 : 1 0 1 (0)

→ 1 0 1 0 1 0 1

Receiver checks the parity

* Stop and wait ARQ: See notes 4- 21p to 24p
* ~~big~~ piggybacking : See notes 25p
* Go Back N ARQ:
* Selective Repeat ARQ

Multiple Access protocol

- Random Access Protocol
  - MA (Multiple Access)
  - CSMA (Carreer sense multiple
  - CSMA/CD (with collisiondetect
- Controlled Access Protocol
  - Reservation
  - Polling
  - Token Passing
- Channelization Protocol
  - FDMA
  - TDMA
  - CDMA

Aloha :

- If you have a packet, just send it.
- If multiple people try it and so there is collision, try resending it later.

Multiple access links

- two types of link
  - point to point
    - → PPP for dial up access
    - → Point to point link betn ethernet and host.
    - → point to points are those in which, when a msg is sent from one comp to another, it usually has to be sent via other computers in nlw.

- Broadcast Network (shared wire or medium)
  - → Old-fashioned Ethernet
  - → 802.11 wireless LAN
  - → Broadcast nlw have a single communication channel that is shared by all the machines on the network

- single shared broadcast channel
- two or more simultaneous transmission by nodes: Interference
  - Collision: If node receives two or more signals at same time

~~Need~~ issues in multiple of

- who is going to use the channel
- when and for how much, the channel is going to be used

1. Random access
- Single channel shared by large no. of hos
- No coordination between hosts
- Control is completely distributed
Example, Aloha, CSMA, CSMA/CD

a. Aloha: allows multiple access (MA) to the shared medium. There are potential collisions in this arrangement. when a station send data, another station may attempt to do so at the same time. The data from two station collide and become garbled.

b. CSMA: to minimize collisions and increase the performance CSMA was developed. The chance of collision can be reduced if a station senses the medium before trying to use it. CSMA requires that each ~~collision~~ station first listen to the medium before sending

c. CSMA/CD: augment the CSMA algorithm to detect the collision. a station monitors the medium after it sends a frame to see if the transmission was successful. if so, the station is finished. if however, there is a collision, the frame is sent again

To avoid collisions on wireless nlw, CSMA with collision avoidance (CSMA/CA) was invented. collisions are avoided through the use three strategies: interframe space, the contention window, and acknowledgm

2. Controlled Access:
The station consult one another to find out which has right to send. A station cannot send unless it has been authorized by other station

a. Reserving (Reservation access method): a station needs to make a reservation before sending data. Time is divided into intervals. in each interval, a reservation fram precedes the data frames sent in that interval.
b. Polling method, all data exchanges must be made through the primary device even when the ultimate destination is a secondary device. The primary device controls the ~~device~~ link; the secondary device follow its instruction
c. token passing method: the stations in a nlw are organized in a local ring. Each station has a predecessor and a successor. A special packet called a token circulates through the link

3. Channelization: is a multiple-access method in which the available bandwidth of a link is shared at a time, frequency or through code, between different station.

a. FDMA: In frequency-division multiple access, the available bandwidth is divided into frequency bands. Each station is allocated a band to send its data. In other words, each band is reserved for a specific station, and it belongs to the station all the time.

TDMA (Time-division multiple access): The stations share the bandwidth of time. each station is allocated a time slot during which it can send data. Each station transmits its data in its assigned time slot.

CDMA: (code-division multiple access), the stations use different codes to achieve multiple access. CDMA is based on coding theory and uses sequences of number called chips. The sequences are generated using orthogonal codes such the walsh tables.

Data Link protocols

① High level Data Link Control (HDLC)

- HDLC is a transmission protocol used at the data link layer of OSI model for data communications. The HDLC protocol embeds information in a data frame that allows devices to control data flow and correct error
- HDLC is a bit oriented protocols, support half and full duplex communication over point to point and multipoint link.
- HDLCs can provide both connection-oriented and connectionless services.
- Data in HDLC is organized into unit called frames
- Each piece of data is encapsulated in an HDLC frame by adding a trailer and header. The header contains HDLC address, too and an HDLC control field. The trailer contain CRC.
-

- modes of transmission
  - NRM (Normal response mode)
  - ABM (Asynchronous Balanced mode
  - ARM (Asynchronous Response mode)

NRM: A secondary station running in an unbic communications environment may communicate when signalled to do so by a primary.

ABM: when in a bic comm, either combined station may initiate comm. (LAPB mode on combided stations)

ARM: when in a unbic env, secondary may transmit on will, however primary is still responsible for error detection, line and flow control.

frame format:

only in I- and U- frame

| Flag | Address | control | information | FCS | Flag |

frame type:

① I-frames: (User data): Information frames, transport user data from nlw layer. They also include flow and error control information piggybacked on data.

② S-frames (control)
supervisory are used for flow and error control wherever piggybacking is impossible, such as when a station doesnot have data to send. S-frames do not have information fields.

③ U-frame (un-numbered frame)
supplementry link control. used in link setup and do not contain ACK.

HDLC frames: See notes (47)

PPP (point to point protocol)
- byte oriented protocol operates at layer 2 & layer 3. It uses HDLC frame format at layer-2 and uses IPV4 and IPV6 format at layer-3
- It has CRC-16 field in the
- PPP defines the format of frame to be exchanged betn the devices
- This protocol offer the services that were not present in SLIP.
- It defines how nlw layer data are encapsulated in data link frame.
- It provides error detection
- Unlike SLIP that support IP, PPP support multiple protocol
- PPP allows IP address to be assigned at the connection time ie. dynamically. Thus a temporary IP address can be assigned to each host.
- PPP provides multiple nlw layer services supporting a variety of nlw layer protocol. For this PPP uses a protocol called NCP (Network Control protocol)
- It also defines how two def device can authenticate each other.

Frame Format:
The frame format of PPP resemble HDLC formats. It:

Flag	Address	Control	Protocol	Data	FCS	Flag
01111110	11111111	00000011				01111110
1 byte	1 byte	1 byte	1 or 2 bytes	variable	2 or 4 byte	

Flag field: Flag field marks the begining and end of PPP frame. Flag byte is 1 byte. (01111110)

Address field: is 1 byte and always 11111111. This address is a broadcast address ie: all the station accept this frame.
Control field: is 1 byte. This field uses the format of the U-frame (unnumbered) in HDLC. The value is always 00000001 to show that the frame doesnot contain any sequence of numbers and there is no flow control or error control.
Protocol field: This field specifies the kind of packet in the data field ie what is being carried in data field.
Data field: Its length is variable. If the length is not negotiated using LCP during line set up, a default length of 1500 bytes is used. It carries user data.
FCS field: (frame checks sequence). It is either of 2 bytes or 4 bytes. It contains the checksum.

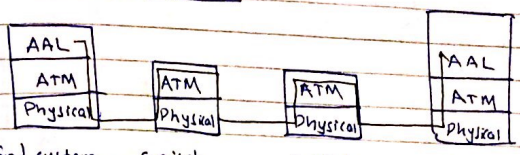
- PPP is a protocol most widely used by Internet service providers (ISPs) to enable dial up connections to the Internet
- PPP facillates the transmission of data packets betn point to point
- PPP can be encapsulated in a no. of datalink layer protocols, including ethernet (PPPoE) and ATM (PPPoA)

* SLIP: Serial Line Internet protocol
- older protocol used by PCs to connect to internet via modem
- SLIP is a TCP/IP protocol used for communication betn two machines that are previously configured for communication with each other.
- PPP replace SLIP protocol of choice for p2p connection

- SLIP is still used today and is supported by IBM operating system
- SLIP has no support for system authentication, while PPP has 2-way authentication
- SLIP has no support for error detection or error compression but is implemented in PPP
- SLIP has no standard way to define IP addressing between two hosts.
- Relies on hlw for error checking and correction.

* ATM: Asynchronous Transfer mode:
- 1990s standard for High speed for broadband integrated service digital nlw architecture.
- Goal: Integrated voice, video and data transport
- Its a high speed nlwing standard designed to support voice, video and data communications and to improve utilization and quality of service (QOS) on high traffic nlw.
- ATM is normally utilized by ISPs on their private long-distance nlws. ATM operates in datalink layer over either fiber or twisted pair cable.
- Although it's fading in favour of the NGN (next gen. nlw) this protocol is critical to SONET/SDH backbone, the PSTN (public switched telephone nlw) and ISDN (Integrated services digital nlw).
- is a dedicated connection switching technology that organizes digital data into 53 byte cell units and transmits them over a physical medium using digital signal technology.
- ATM is switching technique used by telecommunication nlw that uses asynchronous time-division multiplexing to encode

ATM: Architecture ??



AAL (ATM adaptation Layer)
- used only at edge of ATM nlw.
- Data segmentation Reassembly
- Analogous to Internet transport Layer

ATM Layer
- analogous to Internet nlw layer
- cell switching and routing.

Physical Layer
- analogous to Internet physical layer

* Frame relay
- Speed 1.54 mbps at physical & data link layer
- can be used as backbone nlw.

5

Nlw layer

* **IP address : Representation in dotted decimal notation**
- is a numerical label assigned to each device connected to a computer nlw that uses the Internet protocol for communication.

10000000.00001011.00000011.00011111
128.11.3.31

IPv4 supports 3 different types of addressing modes :

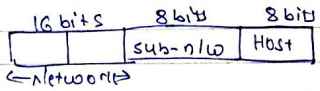
unicast : - data is sent only to one destined host
- 32 bit IP address of destination

broadcast : packet is addressed to all hosts in a nlw segment. The dest^n address field contains a special broadcast address.

multicast : mix mode, neither single host nor the all host on segment.

* **Hierarchichal addressing scheme**

IPv4 uses hierarchichal addressing scheme. An IP addres which is 32 bit in length is divided into two or 3 parts as



A single ip address can contain information about nlw, its Sub network and host.

* **Subnet mask**

router use subnet mask, which is as long as the size of nlw address in IP address. Subnet mask is also 32 bit long. If IP address in binary is ANDed with its subnet mask, the result yields the Nlw address

IPv4 : Address classes :

- 5 classes are identified by first octet of IP address.

no. of nlw = $2^{\text{nlw bit}}$

no. of usable host = $2^{\text{host bit}} - 2$

- first IP address is network number
last IP address : Broadcast IP

Class-A :

- first 0 bits in first octet set to 0, ie first octet ranges from 1-127 ie
00000001 - 01111111

default subnet mask : 255.0.0.0

networks = $2^7 - 2 = 126$

hosts = $2^{24} - 2 = 16777214$

Class-B

- first 2 bits in first octet set to 10 ie
10000000 - 10111111
(128 - 191)

network address = $2^{14} = 16384$

host addresses = $2^{16} - 2 = 65534$

Class-C

- first 3 bits set to 110 that is
192 - 223 (11000000 - 11011111

class c gives = 2^{21} nlw addresses

one host address = $2^8 - 2$ (host address

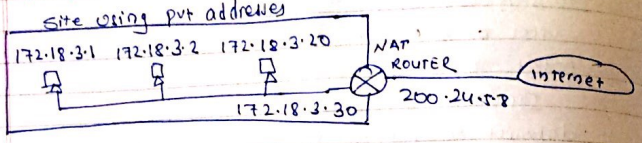
Class-D

- first 4 bits of first octet set to 1110 (224-2
1110 0000 - 1110 1111
- reserved for multicasting.
- doesnot have any subnet mask

Class-E : 240.0.0.0 - 255.255.255.254,
no subnet mask.

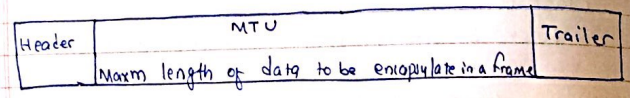
Class	First byte	default subnet	Subnet mask	total host in Subnet n mask	Range
A	0	/8	255.0.0.0	2^{24}	10.0.0.0 - 10.255.255.25
B	10	/16	255.255.0.0	2^{20}	172.16.0.0 - 172.31.255.25
C	110	/24	255.255.255.0	2^{16}	192.168.0.0 - 192.168.255.25
D	1110	-	-	-	-
E	1111	-	-	-	-

* NAT (Network address Translation)



* MTU: Maximum Transmission Unit

IP datagram



IPV4 :

- 32 bit long
- Part of an IP address identifies which local nlw, host on that local nlw.
- IPV4 provides no error control or flow control

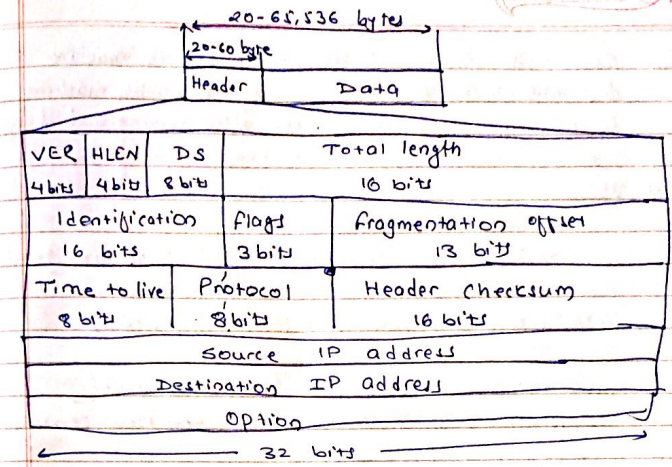


fig: IPV4 frame format (Datagram format)

VER : Defines the version of IP
HLEN : Header length
DS : Differentiated service. Defines the class of packet for QoS.
Total length : length of data ⇒ Total length - header length
Identification :
- when datagram is fragmented ⇒ Identification copied to a
- All fragments have same identification.
- Helps in re-assembling the datagram.

Flags :
3 bit → reserved, MF and DF
DF → don't fragment MF ⇒ More fragment

Fragmentation offset : offset value of fragment
TTL : If TTL=0, packet is discard
Checksum : Compute Checksum

Source IP address: IP address of source machine
destination IP address: IP address of destination machine
Option: Optional field used for n/w testing and debugging

* IPV6 :
- Internet protocol version 6
- It is known as Internetworking Protocol next gen. (IPng)
- It is suitable for fast growing internet
- It is also suitable for NGN (next gen n/w)

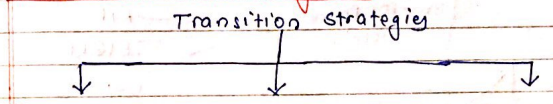
Features
- larger address space (128 bit address space)
- supports resource allocation via flow control field
- supports more security.
- Better header format [Base and Extension header]

128 bit addressing scheme
Unabbreviated
FDEC:BA98:0074:3210:000F:BBFF:0000:FFFF
Abbreviated
FDEC:BA98:74:3210:F:BBFF:0:FFFF
more abbreviate
FDEC:0:0:0:BBFF:0:FFFF → FDEC::BBF:0:FFFF
Header format: (Base + Extension)

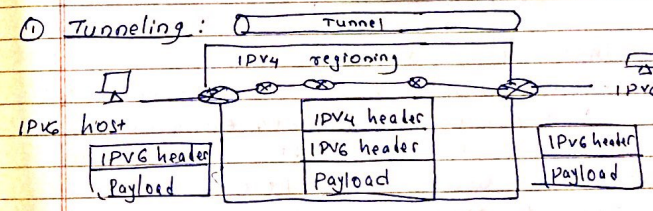
VER	PRI	Flow Label
Payload length	Next header	Hop Limit
Source Address		
Destination Address		
Payload		
extension headers		
+		
Data Packets from upper Layer		

VER: 4 bits, version of IPV6
pri: 4bit, priority of packets
flow label: 24 bits, used for resource reservation
payload length: 16 bits; total length of IP datagram excluding base header
next header: 8 bits, provides info about extension header.
Hop Limit: Same as TTL in IPV4 (8bits)
Source address: 128 bit source IPV6 address.
dest^n address: 128 bits dest^n of IPV6 address.

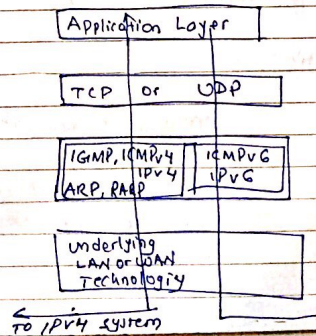
* IPV6 Transition Strategies



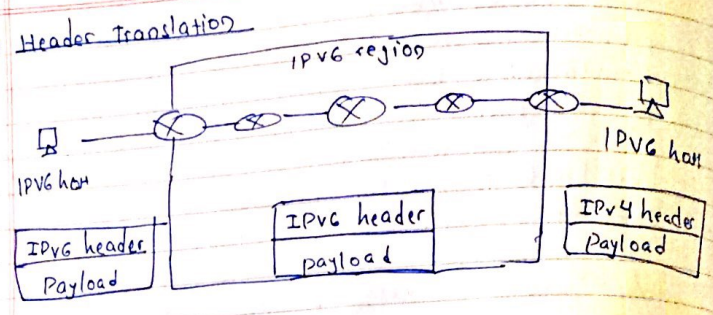
① Tunneling:



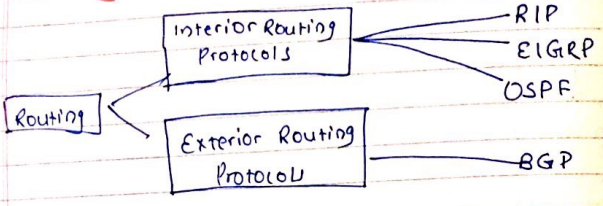
② Dual stack



Header Translation



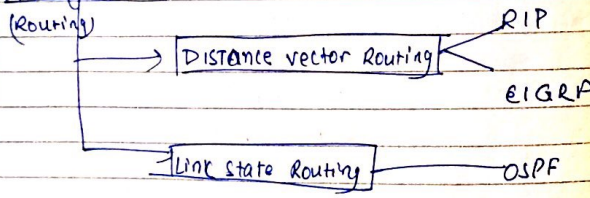
Routing Protocols



a. Interior gateway routing Protocols
- used for routing inside an Autonomous System (AS)
AS ⇒ Network under Common Administration
Examples : RIP, EIGRP, OSPF

b. Exterior Gateway routing protocols
- used for routing betn AS

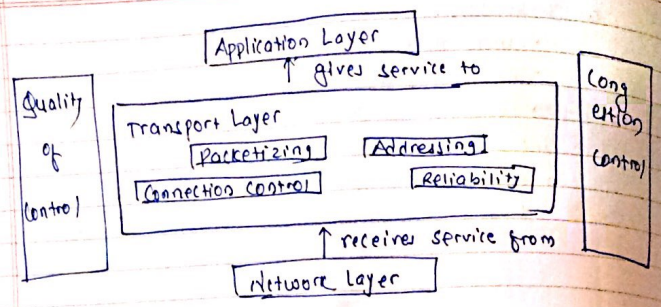
classification (Routing)



a. Distance :
- ✓ incomplete view of topology
- ✓ Routes are advertised as vectors of distance & direction
- ✓ Generally periodic Updates

b. Link State :
- ✓ Complete view of Nlw topology
- ✓ Updates are not periodic (triggered or bounded updates)

6 Transport Layer



node to node : data link layer
host to host : Nlw layer
process to process : Transport layer

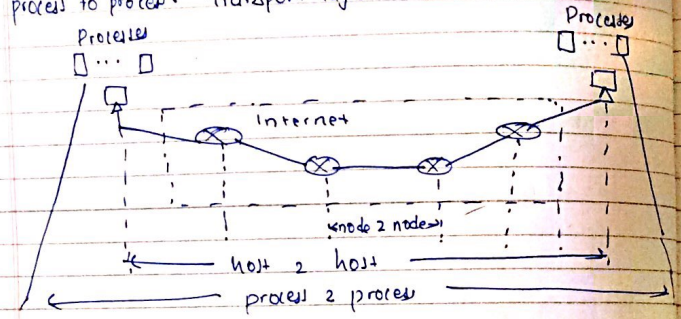


fig. types of data delievers

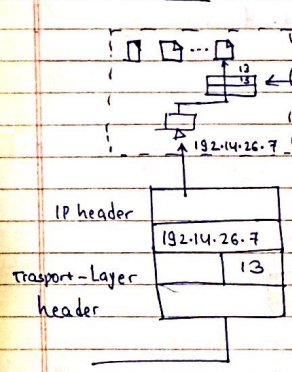
Port Numbers

A port number is a way to identify a specific process to which an internet or other nlw message is to be forwarded when it arrives at a server.
for TCP or UDP, it is 16 bit integer that is put in header append to a msg unit. The port number is passed logically betn client and server transport layers and physically betn transport layer and Internet protocol layer.

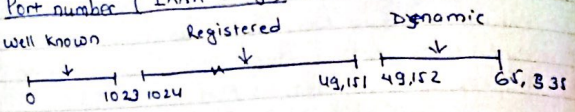
- Some services or processes have assigned permanent port addr known as well-known port numbers. others called ephemeral port number
HTTP = 80, Telnet = 23

Functions of Transport Layer:
- Service point addressing
- Segmentation and reseambling
- Connection control
- Flow control
- Error control
- The aim is to be delievered the entire msg from src to destn.
- Transport layer ensures whole msg arrives intact, inorder ensuring both error control and flow control
- It decides if data transmission should be on parallel path or single path.

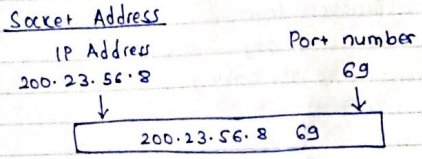
Port vs IP



* Port number (IANA range)



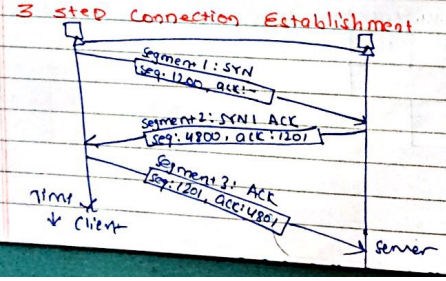
* Socket Address



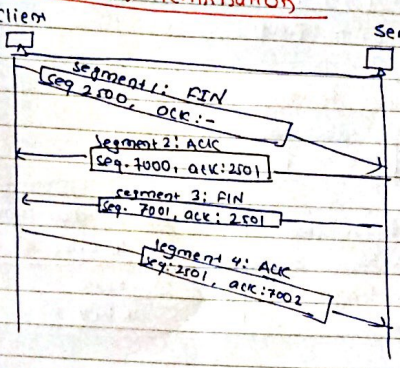
* Multiplexing and Demultiplexing
- Gathering data from multiple application processes of sender, enveloping that data with header and sending them as a whole to the intended receiver is called multiplexing. — multiplexing
- Delievering received segments at receiver side to the correct app layerprocesses is called as demultiplexing
- Connectionless multiplexing & demultiplexing
- Connection Oriented

How it is done :
- To send data, sender must know IP address of receiver
- [geeks for geek]

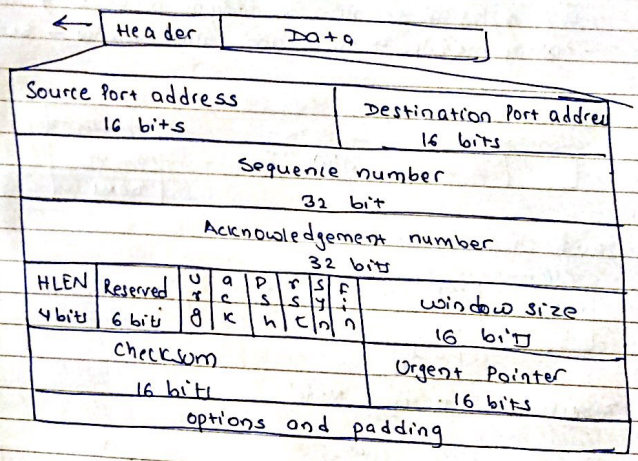
* 3 step Connection Establishment



four step Connection termination



* Transport Layer: TCP Segment Format :

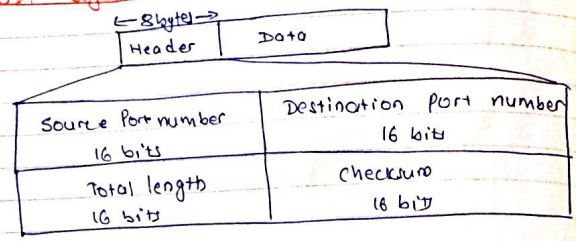


URG: Urgent pointer is valid
ACK: Acknowledgement is valid
PSH: Request for Push
SYN: Synchronize sequence number
FIN: Terminate the connec

URG	ACK	PSH	RST	SYN	FIN

Fig: Control fields

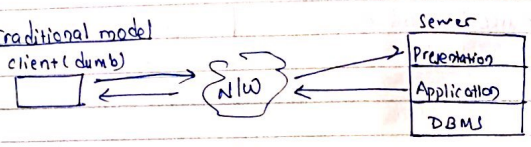
* UDP Segment Format



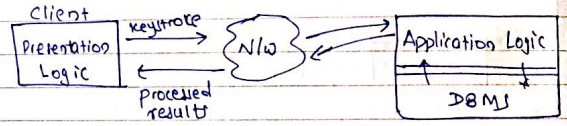
* Client Server Computing

- It is a logical extension of modular programing
- calling modules → client and called modules → Server

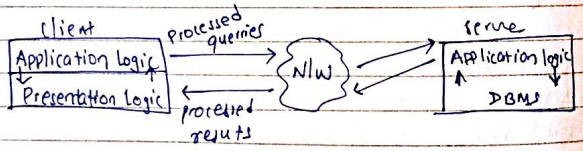
Traditional model



True client server Model

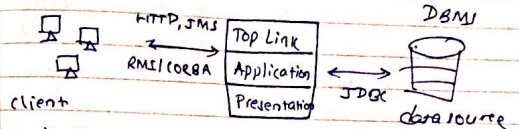


Distributed client server Model

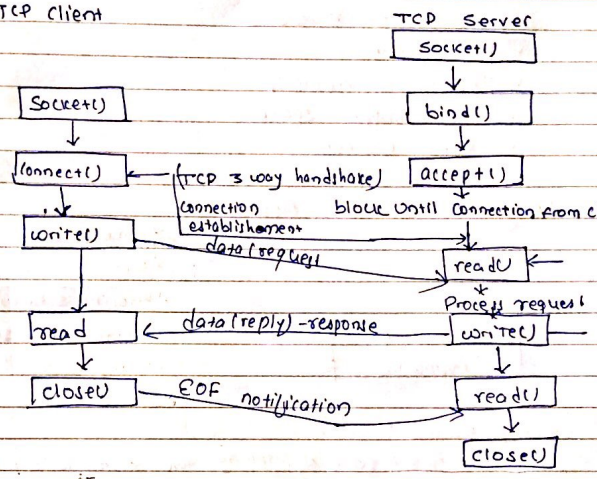


* Distributed Applications:

- Three-Tier Architecture



* flow diagram of TCP server and client:



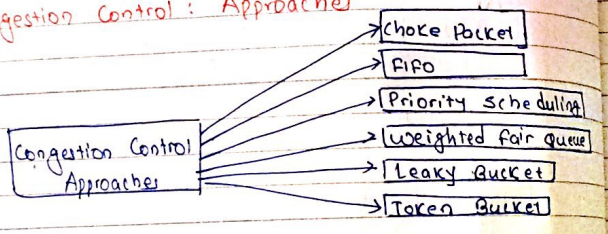
Network Congestion

- The situation in which an increase in data transmissions results in reduction of throughput.
- Congestion occurs when no. of packets being transmitted through the nlw approaches the packet handling capacity of the network.
- Congestion Control types
  - open Loop (prevent congestion occuring by good design)
  - closed Loop (detect ⇒ Feedback ⇒ Correct)

* why Congestion occur ?

- ✓ heavy traffic
- ✓ Insufficient memory
- ✓ Low buffer space
- ✓ Low processor

* Congestion Control : Approaches

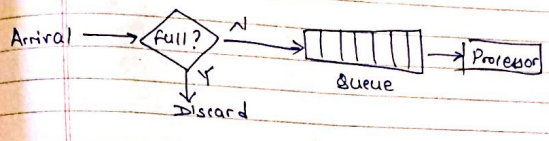


Choke packet :

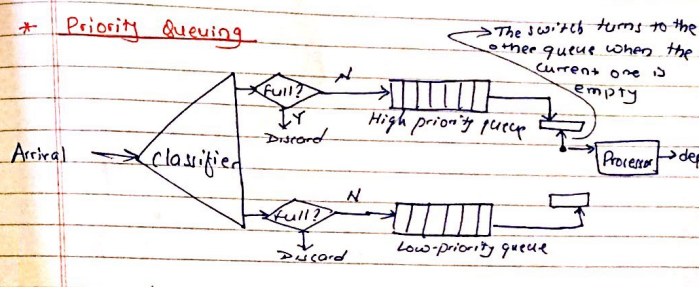
- A more direct way of telling the source to slow down
- choke packet is a control packet generate at Congested node
- It is then transmitted to source.
- The source on receiving the choke packet must reduce its transmission rate.
- Hop by Hop choke packet is more efficient than choke packet.

It enables each Hop to reduce its transmission rate even before choke packet receives at source

* FIFO Queue



* Priority Queuing



* Weighed Fair Queuing

see note