COMPUTER NETWORKS

COMPUTER NETWORKS

OSI Model

PDNTSPAN → Network Security

Physical layer

Datalink

Network

Transport

Presentation

Application

Session

PHYSICAL LAYER

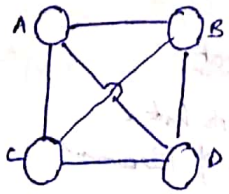
→ provides functionality to data link layer.

functionalities (deals with hardware)

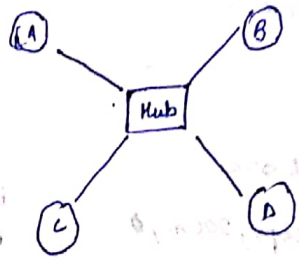
- Cables & Connectors
- physical topology (star, mesh, bus, point to point) (LAN)
- Hardware (Repeater, Hubs)
  - Attenuation components
  - Multiport connectors.
- Transmission mode
- Multiplexing (wavelength division)
- Encoding (analog / noise / digital)

① Mesh

→ Security is high

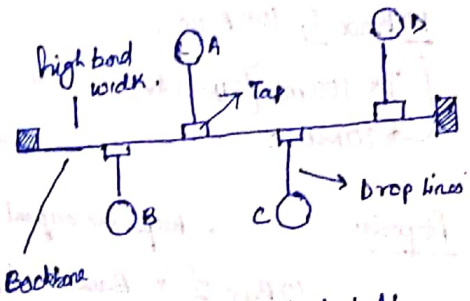


② Star/Hub (Multiport device)



→ No Reliability
No Security.

③ Bus Topology:

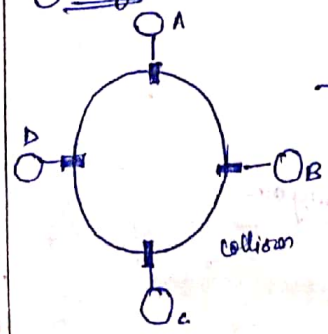


→ No Reliability is checked by Single point of failure = 0

→ Security is less.

(high bandwidth: range of frequencies with a given band, in particular that is used for transmitting signal)

④ Ring



→ Reliability and security is low

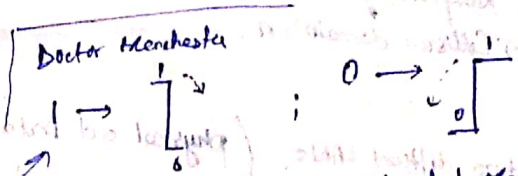
→ Unidirectional ring.

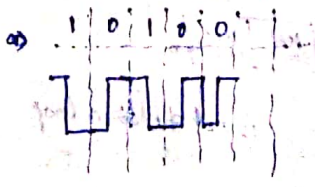
→ Token to Reduce collision.

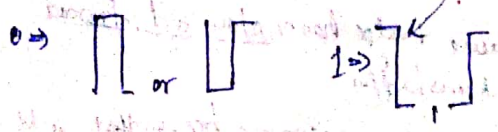
Data Encoding

① Manchester Encoding.

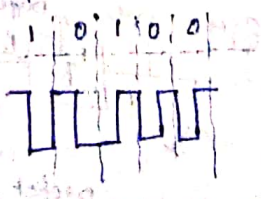
Doctor Manchester







② Differential Manchester Decoding



Various Networking Devices in Computer Networks

1) Cables
2) Hub
3) Switches
4) Gateway
5) Firewall
6) Repeaters
7) Bridges
8) Routers
9) IDS
10) Modem.

Hub.

Security.

Intrusion detection sensors

↳ Modulator / demodulator.

Cables

(i) if n devices are connected over a base band, n collisions can happen.

Max Collision domain : n

(ii) Does not filter data

Base band - At a time only one signal can transmit

Broad band - Many signal.

Types

Unshielded twisted pair Cable (Used in Ethernet LAN).

10 Base T, 100 Base T

T3 100 mts (attenuation)

↳ 10 Mbps.

Coaxial

10 Base 2

10 Base 3

Fibre optics

100 Base FX

(2 km Attenuation)

Repeater

↗ keeps the original strength same

10 Base 2 : Base band, 10 Mbps, 200 m, 0

(i) Forwarding

(ii) No filtering

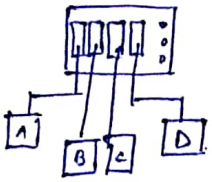
(iii) Collision domain : n (inside the device).

Subnet

interconnected host.

Made up of telecommunication lines.

Hub (same LAN)



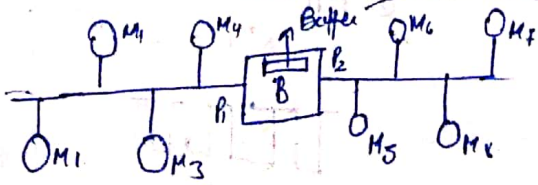
(i) Multiport Repeater

(ii) forwarded and broadcasted — packet goes to everyone

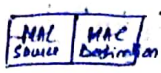
(iv) No filtering

(iv) Collision domain : n.

Bridges : to connect two different LANs. (physical and Data link layer).



MAC



(i) Forwarding : if bridge has a packet, it forwards it

(ii) filtering : filters for two different LAN's.

(iii) Collision domain : Collision not occur, because bridge has a store and forward strategy. Bridge maintains buffer.

(iv) Use data Unit protocol : They make a Minimum spanning tree, so that packet is not stuck in a loop.

Type of addressing

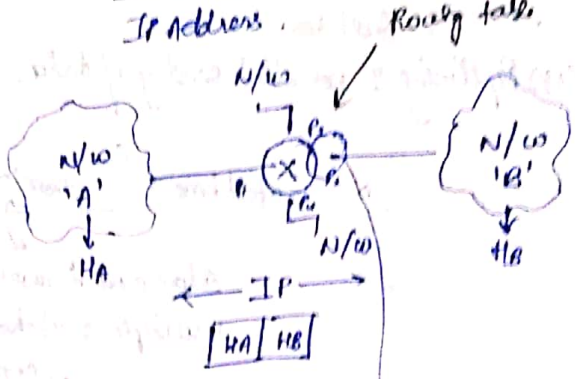
Static (Entered manually)

MAC	Port
M_1	P_1
M_2	P_1
M_5	P_2
M_8	P_2
⋮	⋮

Dynamic or Transparent
- Learn themselves
- Store addresses, by backward learning things first time.
- The machines have to acknowledge message passing or receiving.

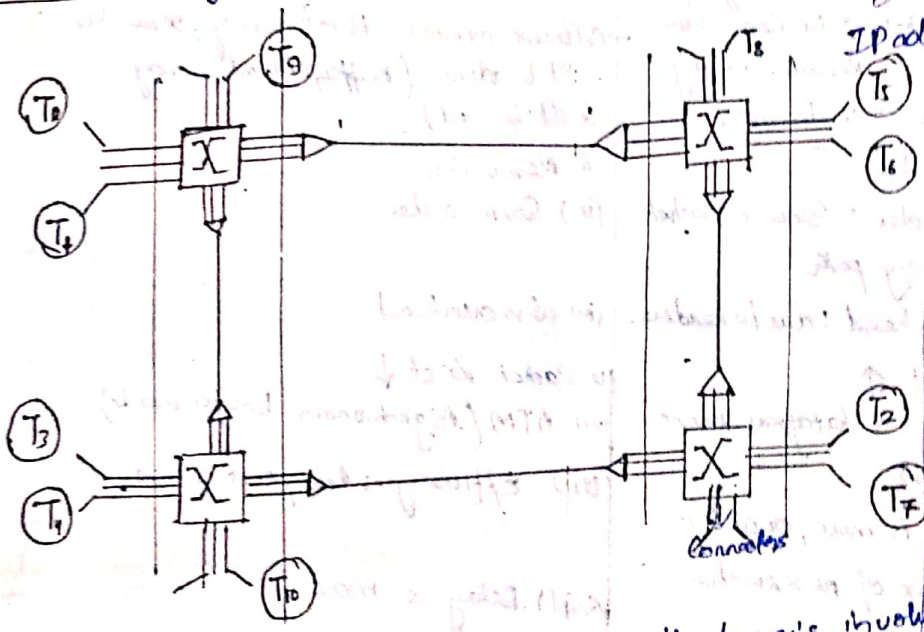
Routers (Internet) (Connects Physical, Data link, Network layer)
(WAN) - Wide Area Network.

- forwarding: Router using Routing table
- flooding: To broadcast the package in all direction
- filtering: Using its Routing table
- Collision Domain: No, Store and forward method is used.



- MAP address is used in local Area Network
- ARP: Used to Request MAC address

Circuit Switching



IP address from Network B.

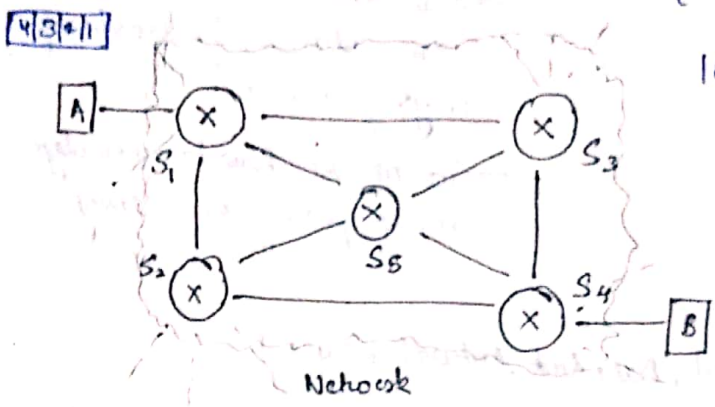
Maximum data transfer rate of a network.

Totat (i) Physical layer: No other layer's involved. Circuit switching used a dedicated path to communicate
(ii) Contiguous flow: data flows continuously.
(iii) No Headers: No Headers like MAC address, IP address.
(iv) Efficiency: Low, due to Resource fixing.
(v) Delay less: No delay in communication., No store and forward.

Total time = Setup Time + Transmission (Message / Bandwidth) + Propagation Delay (D/S) + Teardown

Packet Switching → Datagram Service (works on Network layer)
→ Virtual Circuit (works on Data link layer)

Packet



S: Switches

(i) Store & Forward: Switches store data in buffer, and take decision on the path of data.

(ii) Efficiency is high.

(iii) Delay is more than circuit switching, due to buffer time.

(iv) Pipelining: parallel sending of data.

Total time = (Transmission Time) + PD (propagation delay)

↓
Store and forward through multiple switches.

n(T.T)

↓
no of switches

Datagram Switching Vs. Virtual Switched Circuit.

Datagram Switching	Virtual Circuit
(i) Connection less – No Reservation. No Resource & Reserved. Everything will be allocated on demand.	→ Collection oriented – Before sending, reservation will be done (Buffer, CPU and memory will be used).
(ii) No Reservation	(ii) Reservation
(iii) Out of Order: Every packet can follow any path	(iv) Same order.
(iv) High Overhead: due to headers.	(iv) less overhead
(v) Packet Lost ↑	(v) Packet Lost ↓
(v) Internet uses a datagram service - IP network.	(vi) ATM (Asynchronous transfer mode)
(vii) Efficiency is more, or cost is less, because of no reservation	(vii) Efficiency is less, cost is more.
(viii) Delay is more	(viii) Delay is more.

CN : Noor Academy

Simulation

(i) CISCO packet Network :

Introduction

→ A computer network is a set of nodes connected by communication links. Mainly used for Resource Sharing.

- A node can be a computer, ports or any other device capable of sending / receiving data generated by other nodes in the network.

OSI Model — Layers — Network Security, Application, Presentation, Transport, Session, Network, Data link, Physical

- A communication link can be wired link or wireless link. Link carries the information.
- End device : They are either the starting point or end point in the communication.

Basic Characteristics

Basic Characteristics — Fault tolerance, Scalability, Security, Quality of Service (QoS)

(i) Fault tolerance
ability to :
- Continue working despite failures
- Ensure no loss of service.

(ii) Scalability (Eg: Internet)
ability to :
- Grow based on the needs
- Have good performance after growth

(iii) Quality of Service (QoS)
ability to :
- Set Priorities
- Manage data traffic to reduce data loss, delay etc.

(iv) Security
ability to provide :
- Unauthorized access
- Misuse
- forgery

ability to prevent :
- Confidentiality
- Integrity
- Availability.

Network Protocol & Communication

(i) SIMPLEX
- Communication is always unidirectional
- One device can transmit and the other device will receive.

(ii) HALF DUPLEX.
- Communication is in both directions but not at the same time.
- If one device is sending, the other can only receive and vice versa.

(iii) DUPLEX / FULL DUPLEX
- Communication is in both direction simultaneously.

Types of data flow

(iii) **PROTOCOLS** → Rules governing all methods of communication.

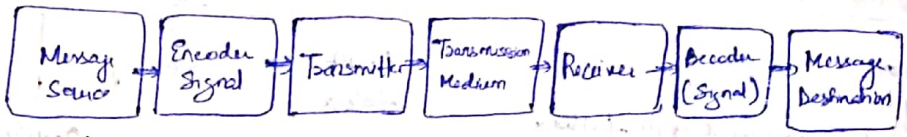
All communication schemes will have following things in common:

* Source or sender
* Destination or receiver
* Channel or media.

Protocols define (OR) Elements of a Protocol.

- Message encoding
- Message formatting & encapsulation.
- Message timing
- Message size (breaking of message into packets)
- Message delivery options.

Message Encoding →



(in forms of waves)

Message formating & encapsulation →
- Agreed format
- Encapsulate the information to identify the sender and the receiver rightly.

Message timing →
- Flow Control (speed synchronization)
- Response Timeout (Synchronization and Acknowledgement)

Message Delivery options →
- Unicast (Sender sending to exactly one destination)
- Multicast (Sending to set of receiver, but not to all)
- Broadcast (to all participants in network).

IP address is added to the data to be send.
- Every computer in the network is identified by its IP address.
- Data contains both source and destination IP address.
- Acknowledgment, if not done → receiver has to resend the package.
- Message packets are ensured to ensured synchronized receiving and avoid message loss.

PEER TO PEER NETWORK →
- No centralized administration
- All peers are equal
- Simple sharing applications
- Not Scalable (new devices can be added to the network)
  - ↳ due to port limitation

Client Server Network →
- Central administration
- Request - Response model
- Scalable
- Server may be overloaded.

Components of a Computer Network

Components → · Nodes
· Media
· Services

Nodes → · End nodes (End devices)
· Intermediary nodes

End nodes → · Computer, Network printers, VOIP phones, Telepresence endpoints, Security cameras, Mobile handheld services

Intermediary Nodes → Switches, WAP (wireless Access point), Routers, Security Devices (Firewall), Bridges, Hubs, Repeaters, Cell tower.

Media → Wired Medium (Guided Medium) / Unguided - Wireless medium

WIRED MEDIUM

- Ethernet straight Through cable / Twisted pair Cable
  - To connect devices of same type - data in form of electrical signals.
- Ethernet Crossover cable
  - Different type of devices
- Fiber Optic Cable
  - Light wave (Fastest Medium of Wired comm.)
- Coaxial Cable
  - Audio/Video Communication.
- USB cable
  - Computer to a passes.

Wireless Media. → · Infrared · Eg: short range communication - TV remote control.
- Radio · Eg: Bluetooth, Wi-Fi
· Microwaves · Eg: Cellular System
· Satellite · Eg: GPS (Long Range communication)

RMILUVXU.

Services → : e-mail, Storage Services, Online Game, Voice over IP, Television, Videoteleplony, Instant messaging, World Wide Web.

Voice over IP is an Intermediary Node ex.

Classification of Computer Networks - LAN, MAN, WAN.

LAN → · Interconnects with a Limited Area
· Connected using switch.
· Mayne Wired (Hub, Switch) Ethernet, Wireless (Wi-Fi)

MAN → Interconnects users with computer resources in a geographic region of the size of a city
· Devices — Switches / Hub → for LAN
Routers / Bridges → for MAN to connect two switches or Hubs.

WAN → · Extends over large geographical Area. - Telecommunication Network

· Devices : End devices and Intermediary devices

Internet → · Wide WAN.

Cloud Computing → · On-demand availability of computer system resources, especially data storage and computing power, without direct active management by the user.

Network Topology : Arrangement of nodes of a compute network

physical topology
· placement of various nodes,

Logical Topology
· Deals with the data flow in the networks.

→ Bus, Ary, Star, Mesh, Hybrid.

Bus → · Common transmission medium
· Bidirectional communication
· Suited for tempory Network
· One node does not affect other

· No fault tolerant
· No redendancy
· No security

Ring → · Bus topology in a closed loop
· PEER-to-PEER LAN topology
· Unidirectional communication.
· Sending and receiving data taken place with the help of a token.
· Can cause bottleneck due to weak links
· No Security
· ~~Unidirect~~ Single point of failure
· High load, low performance

· Closed circuit (for 2 node - 2 cable)

Star → · Centralized Management - hub or switch
· All traffics passes through hub or switch.
· Scalable
· Single point of network ——— point of congestion.
· Bottlenecks due to overloaded switch / Hub.
· Repeaters connect two or more star topology.

Mesh → · 100% fault tolerance and Reliable
· Each nod is interconnected
· Issues with broadcast message
· Expensive

No traffic problem in mesh topology only.

Basics of IP addressing

IP address → . Internet protocol - Every node in the computer network is identified with the help of IP addr

IPv4 → . logical address - Can be changed based on logic or location of devices
. Assigned by manually or dynamically
. Represented in decimal and it has 4 octets (x.x.x.x) // 32 bits
0.0.0.0 to 255.255.255.255
1 byte 1 byte 1 byte 1 byte

ipconfig gives IP address of the computer.

Basics of MAC Addressing

MAC address → . Media Access Control. - Used to identify node in LAN network
- IP address = Location of a person — may change
- MAC address = Name of a person — will not change
MAC address = Name of the person
. Routers need IP address (used by MAN/WAN)
MAC address is used by switches. (used by LAN)
. physical Address - unique, and cannot be changed. - Assigned by the manufacturer.
represented in hexadecimal.
. Example : 48 bits (70.-20-84-00-EO-FC) 6×8 bit = 48 bit
1 byte
(-, :)
dash. dot colon

ipconfig/all - to see MAC address details.

IP address
↓
MAC address
↓
Port address

Basics of Port Addressing

→ Port - Communication endpoint.
. Unique for every process
. Fixed port number and dynamic port number (0 - 65535) (2^16 or (2^3)^5 × 2)
615 381
= 2 * (8)^3
= 2^19 bits 8 byte

Use Resource Monitor to check port number.

Switching Techniques - Route for multiple connection

Circuit Switching
Message Switching
Packet Switching
Datagram approach
Virtual Circuit approach

Circuit Switching → . dedicated path between sender & Receiver
. Before data transfer, connection will be established first
. Eg : Telephone network
. phases — Connection establishment
— Data transfer
— Connection disconnection.

Message Switching
- Store and forward mechanism.
- Intermediary node is first storage and then forwarded.
- Not suited for real time application

Packet Switching
- Each packet is sent individually. Each packet has source and destination IP address with sequence number.
  - Sequence number — Reorder the packets
  - Detect missing packets
  - Send Acknowledgement

Datagram Approach (Connectionless switching)
- Each independent entity is called as datagram
- Path is not fixed.
- Intermediary nodes take routing decision.

Virtual Circuit Switching (connection oriented)
- A preplanned route is established.
- Call request and call accept packets are used to establish the connection between sender and receiver.
- path is fixed for the duration of a logical connection.

Layering in Computer Networks

Layering
- Decomposing problem into more manageable components (layers).
- Advantages
  - Modular Design
  - Easy to trouble shoot.

Protocols
- Protocols in each layer govern the communication in that layer.

OSI Model
- OSI : Open system Interconnection
- Model for understanding and designing a network architecture that is flexible, robust, and interoperable.
- OSI is only a guidance, only a reference model.
- purpose is to show how to facilitate communicate between different system without requiring changes to the logic of the underlying hardware and software.

TCP/IP Model
- TCP : Transmission Control Protocol
  IP : Internet Protocol
- Hierarchical protocol made up of interactive modules, each of which provide specific functionality

Every layer in both of the communicating nodes.

The OSI Model

Layering → Layering means decomposing the problem of building a network into more manageable layers.

Purpose → Communicate between different systems without requiring changes to the logic of underlying hardware and software.

Layers - PDNTSPA — Application, Presentation, Session } Network Security.

Physical Layer, Data link, Network, Transport

Intermediary Nodes operate on Network, Datalink and physical layers only.

Application Layer
- Enables user to access the network Resources
  - → Ux file transfer and Access Management (FTAM)
  - → Mail Services
  - → Directory Services

Presentation
- Concerned with the syntax and semantics of the information exchanged between two systems.
  - → Translation : Converting data into a common format
  - → Encryption : Protect data from unathorized access
  - → Compression : to send multimedia (Reduce ~~matt~~ bits)

Session Layer
- Maintains, synchronizes the interaction among communicating devices.
  - → Dialog Control : Determines data flow - simplex, duplex, half duplex
  - → Synchronization : Checkpoint synchronization

Transport layer
- Responsible for process to process delivery of the entire message.
  - → Port Addressing : handling data to right process.
  - → Segmentation and Reassembly
  - → Connection Control : Wireless no n wireless connection establishment
  - → End to End flow control : between end to end devices
  - → Error control.

Network Layer → Responsible for delivery of data from the original source to the destination network
  - → Logical Addressing (IP Address)
  - → Routing : finding best Routes.

Data Link Layer → Responsible for moving data (frames) from one node to another node
  - → Framing (grouping of bits 0's and 1's)
  - → physical Addressing (MAC addressing)
  - → flow control, Error Control
  - → Access Control : If two or more devices are connected to the same link, to determine which device has access.

Physical layer → • Responsible for transmitting bits over a medium. provides electrical and mechanical specifications.
↳ wired or wireless

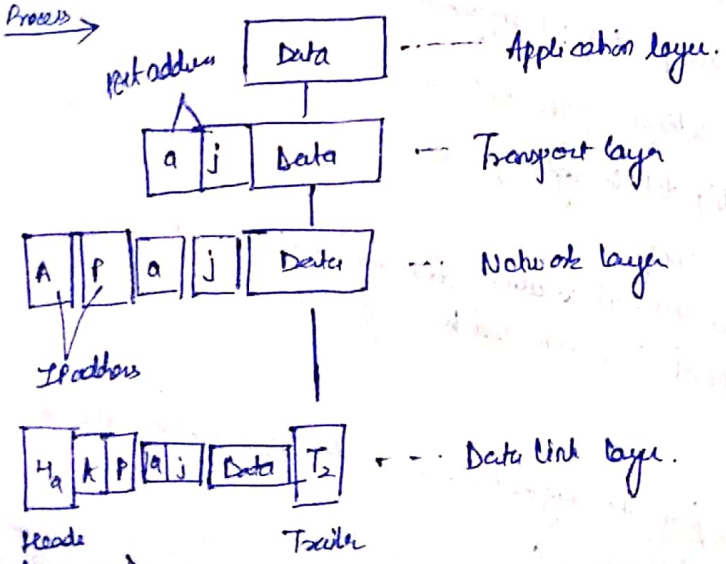
↳ signal conversion.
↳ Representation of bits : encoding (how 0 and 1s are converted to signals)
↳ Data rate
↳ Synchronization of bits
↳ Line Configuration (point to point communication or multipoint layer).
↳ physical topology.
↳ Transmission mode / Data flow.

Addressing in Network

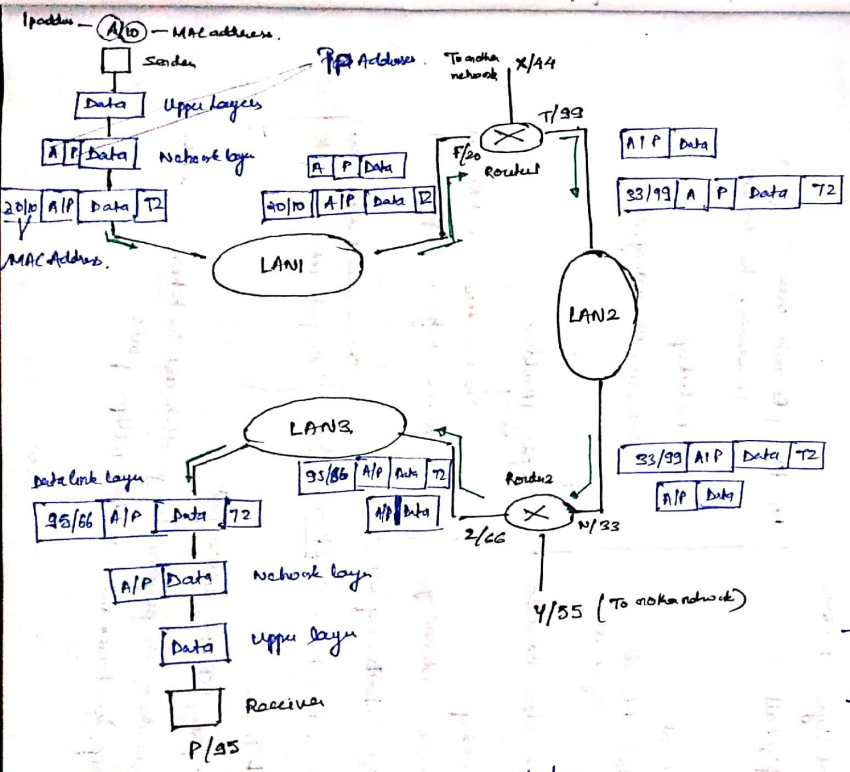
Port Addressing & IP addressing
- Port addressing handled by Transport layer
- IP addressing by network layer.

General
- Source and destination port no. : 16 bits
- IP address IpV4 : 32 bits
- IpV6 : 128 bits

IP Addressing & MAC address.
- Mac Addresses are of 48 bits.
- Routers take decision based on IP addresses.
- Every node has a Address (MAC or IP).



90 / 20
- Original MAC address is never given to access network
- In a Router every port has IP address and MAC address



Note (i) Port and IP-Address remains constant

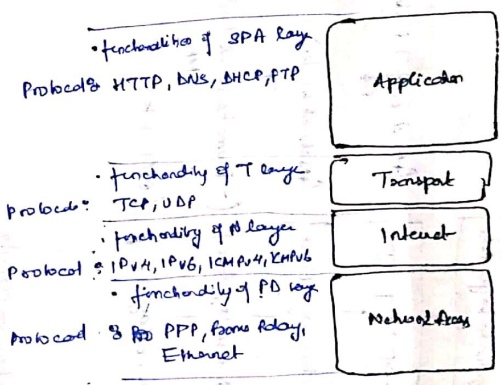
(ii) MAC address changes during physical transportation.

→ Intermediary devices can access Physical layer, Datalink layer, Network layer.

TCP/IP protocol

OSI Ref

TCP/IP



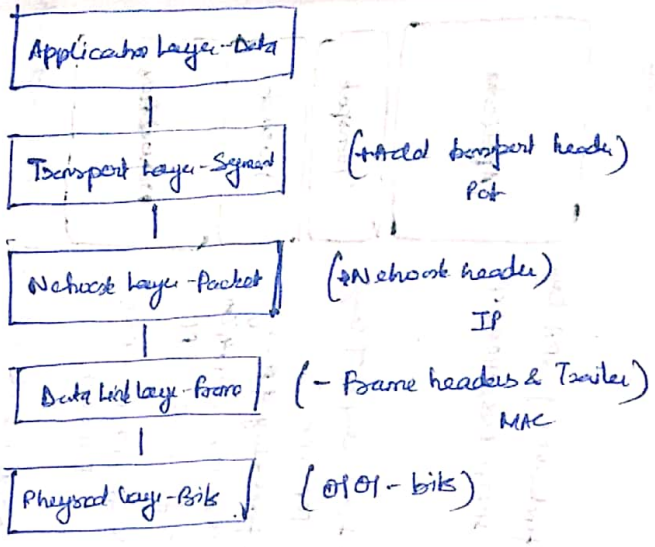
→ Network Access: Control hardware devices and media that make up the network

→ Internet: Determines best path through the network

→ Transport: Supports communication between devices across diverse networks

→ Application: Represents data to the user, plus encoding and dialog control.

Protocol Data Unit : Data, Segment, packet, frame and bits



Basic Networking Commands

(i) ipconfig :- gives us IP configuration details.
- Every IP address is complemented by a subnet mask
- Default gateway is Router's IP address

Layer 3 information
ie Network layer - IP Address.

(ii) ipconfig/all :

Layer 2 information
ie Data Link - MAC address
(Physical address)

(iii) cls : clear the screen.

(iv) DNS (Domain name sever gives IP address for the domain)

cmd > nslookup
> www.nsacademy.org

(v) ping
> ping IP address.
Check whether its reachable or not
(receives acknowledgements on packets sent)

(vi) > nslookup
> www.nsacademy
> ^C (aborts any operation)
> bacert (baceroot) IP address — Shows several details that the path taken by the pkts

Cisco Packet Tracer

i) Serial ports, USB port, Ethernet port

(ii) Hub works in the physical layer. Hubs and switches are used to setup local area network. Has multiple ports

Hub / Network Hub

- Used to set up LAN
- Has multiple ports
- Follows star topology.
- Cable: Straight through ethernet cable

PROS
- Cheaper than switches
- Works good for small networks

CONS
- Issues with load
- Not secure

Switch

- Switch has memory. Can store MAC Address in memory. (In conjunction with interface / port)
- It is a layer 2 device.

Router

- A Networking device that forwards packets between computer networks.
- Connected to at least two networks, commonly two LANs or WANs or a LAN and its ISP's network.
- Operates in Network layer. Stores routing table in memory. The interfaces of a router are part of a LAN.
- Default Gateway information is stored with All devices. This is the IP address of the interface in Router.

Repeater

- physical layer device
- A two port device
- Repeater just regenerates the signal.

Bridge

- Bridge = Repeater + functionality of reading MAC address.
- It is a layer 2 device.
- Used for interconnecting two LANs on the same protocol.
- A two port device

Source Routing Bridges

- Routing is performed by source station and the frame specifies which route to follow.

Transparent Bridges

- These are the bridge in which the stations are completely unaware of the bridge's existence
- Reconfiguration of the stations is unnecessary even if bridge is added or removed from network.

Multi-layer Switch

- Can act as Switch and a Router

Router

- Act as a layer-2 bridge & a router

Modem

- Modulates and demodulates information

Firewall

- Security Device
- filters incoming and outgoing device.

NIC (Network Interface Card) : Connects PC to Network Device.

PHYSICAL LAYER AND MEDIA

(i) Wired Media → Copper Cable (Ethernet cable)
- Unshielded Twisted Pair (UTP) → Copper coaxial cable / Fiber optic cable
- Shielded Twisted Pair (STP) → shielding from signal interference.

Use shielding to counter the effects of EMI & RFI.

(ii) Wireless media

Concerns: (i) Coverage area
(ii) Interference
(iii) Security.

LINE CONFIGURATION

→ Line configuration is called connection.
↳ Types: point-to-point connection, Multidrop/Broadcast/multipoint connection.

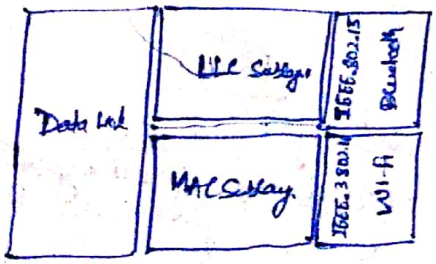
Data Link Layer Services / Link Layer

(i) Services
- framing
- Access Control
- physical Addressing
- Flow Control
- Error Control

→ Add Header (MAC address) and trailer.
- Envelope serves as the delimiter. It's called a frame
- A frame is the encapsulation of the header and trailer information with the packet.
- In the header source and destination MAC addresses are dealt

→ Flow control is one of the duties of data link control sublayer.
- Speed matching mechanism.
→ Media Access Control.
- protecting frame
- Error Detection
- Error Correction

Sub-layer of DL Layer



→ Logical link Control (LLC) or Data Link Control (DLC) sublayer.
- takes the network protocol data and adds control information to help deliver the packet to the destination (flow control).

→ MAC sublayer

- Implemented by hardware, typically in the computer NIC.
- Two primary responsibilities:

→ Data Encapsulation

- Frame assembly and frame disassembly.
- Add header and trailer to the network layer PDU.

→ Media Access control

- Responsible for the placement of frames on the media and the removal of frames from the media.

- Functions:
  - framing
  - Physical addressing or MAC addressing
  - Error control.

FRAMING

i). frames are packets of 0's and 1's.

- The start and end of the frame is set by a protocol. (boundary bits)
- frame = Header + Network Layer PDU + Trailer.

Protocol Data Unit

Types of framing

Fixed Size framing

- Size of frame is fixed and so the frame length acts as delimiter of the frame
- Consequently, does not require additional boundary bits to identify the start & end of the frame.

Variable-size framing

- Size of each frame to be transmitted may be different.

(ii) Framing Approaches

Bit Oriented

- Frame is viewed as a collection of bits.
- Protocol: HDLC (High Level Data Link control)

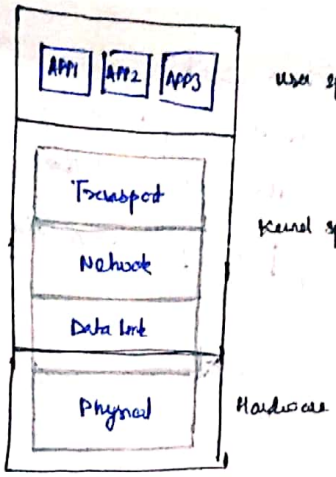
Clock Based framing

- Eg: SONET → Synchronous Optical Network.

Byte Oriented.

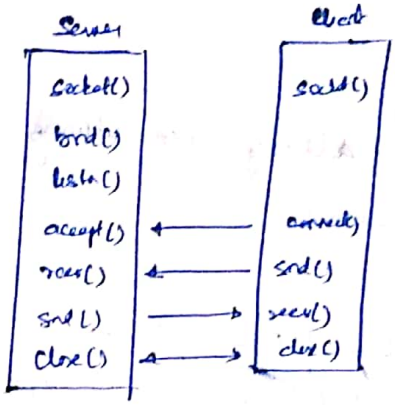
- Each frame viewed as a collection of bytes (characters) rather than bits.
- Protocol: BSCP / BISYNC: binary synchronous Communication protocol
  DDCMP: Digital Data Communication Message protocol
  PPP: Point to point protocol.

Socket Programming



→ the logical pipe between two objects is called Socket. Form end to end connection in TCP, and end-to-end semantics in case of UDP.

→ A set of system calls to get the services from TCP/IP protocol stack (not modules in the OS kernel)



→ i) Socket Programming framework/API:

→ Server() announces a port and client needs to make a connection to that particular port.

- This will create the server side opening of the logical pipe and it will bind the socket with your TCP/IP protocol stack.

→ Bind() function: with the port number you are specifying, it will bind that port number with that socket.

→ listen() function: help you to make the server go to the listening state,

→ connect(): to initiate a connect call: Client sends a SYN packet, Server sends an ACK packet.

→ snd(): send the data

receive(): to receive data.

→ close(): close the corresponding connection.

(i) Socket Type

- TCP is Reliable whereas UDP is Unreliable
- Types of sockets: — Stream Socket (SOCK_STREAM) — Reliable, connection oriented
  — Datagram Socket (SOCK_DGRAM) — Unreliable, connectionless
- Raw Socket – helps in directly interacting with IP layer.

(iii) Socket API

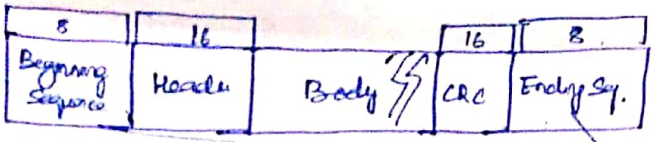
- int s = socket(domain, type, protocol); - Create a socket
  - domain : Communication domain, typically used AF_INET (IPv4 Protocol)
  - type : Type of the socket - SOCK_STREAM & SOCK_DGRAM
  - Protocol : Specifies protocols - usually set to 0 - Explore!
- int status = bind(sockid, &addrport, size); - Reserves a port for the socket
  - sockid : Socket identifier
  - addrport : struct sockaddr_in - the (IP) address and port of the machine (address usually set to INADDR_ANY chooses a local address)
  - size : Size of the sockaddr structure.

High-level Data Link Control (HDLC)

i) BIT ORIENTED APPROACH.

- Simply views the frame as a collection of bits.
- HDLC : High level Data Link Control.

(ii) HDLC - Frame format.



- This sequence is also transmitted during any time that the link is idle so that the sender and receiver can keep their clock synchronized.
- Beg and ending seq : 01111110.
- Header : Address and Control field.

  Body : Payload (Variable size)

  CRC : Cyclic Redundancy check - Error detection.

(iii) Types of HDLC Field. (In control field)

I-Frame
- Information frame
- 1st bit is 0 i.e, this frame is carrying information

S-Frame
- Supervisory frame
- 1st two bit is 10 for flow and error control mechanism

U-Frame
- Un-numbered frame.
- 1st two bits is 11. Doing link management and miscellaneous activities

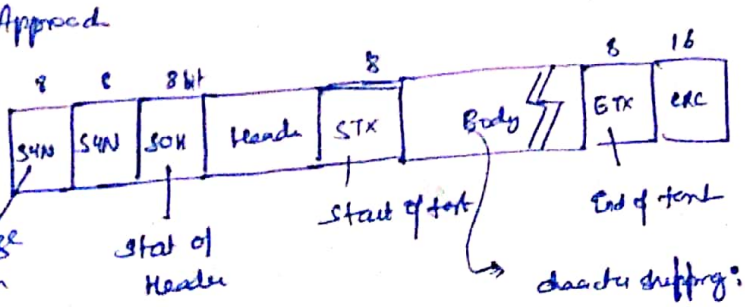
Bit Stuffing

- A Bit is stuff to properly distinguish frame Sequence.

BISYNC : Binary Synchronous communications protocol (BSC)

- A Sentinel Approach

body & guard



Character stuffing: whenever a flag or escape character appears in the body.

PPP Protocol

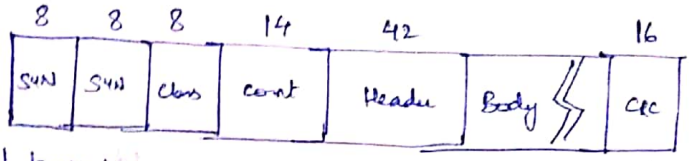
- A WAN protocol run over Internet links used in broadband communications having heavy loads and high speed
- Character stuffing is done using DLE: Data Link escape protocol.
- PPP

- Flag is 01111110 : marks the beginning and the end of the frame.
- Address is set to 11111111 in case of broadcast.
- Control field : Control set at 1100,0000
- Protocol : 1 or 2 bytes that define the type of data contained in the payload field.
- Payload : This carries the data from the network layer.. Maximum length of the payload field is 1500 bytes . this may be negotiated between the endpoints of communication.

→ Character stuffing : An earlier style of framing is called.

DDCMP : Digital Data Communication Message Protocol

→ • Uses a byte counting approach.
- Count field determines how many bytes are contained in the frame body.



- Danger : if transmission error could corrupt the count field, then the end of the frame would not be correctly detected by the receiver.

ERROR DETECTION

- Data can be corrupted during transmission.
- For reliable communication, errors must be detected and corrected.
- Error detection and correction are implemented either at the data link layer or the transport layer of OSI model.

Types of Error.

BIT Error

- only 1 bit in the data unit has been changed.

BURST Error.

- 2 or more bits in data unit have changed.

- Error detection is done by the Receiver. To detect or correct error, we need to send some extra bits with the data. These bits are called redundant bit.

A Generating function is used for redundancy check.

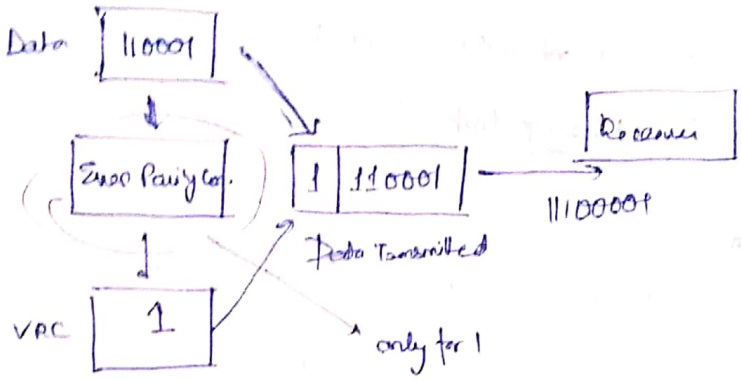
A Checking function is used for checking consistency.

- Error Correction → (i) Receiver can have the sender retransmit entire data unit
  → (ii) Use an error-correcting code, automatically correct certain errors.

Error Detection Techniques

1. VRC : Vertical Redundancy Check
2. LRC : Longitudinal Redundancy check (LRC)
3. Check sum
4. CRC : Cyclic Redundancy check (CRC)

Vertical Redundancy Check (Parity Check)



performance

- Can detect single bit error
- can detect burst errors only if the no. of errors is odd.

Longitudinal Redundancy Check (Two dimensional parity)

- In LRC, a block of bits is organized in rows and columns.
- parity bit is calculated for each column and sent along with the data.
- Block of parity add as redundant bit.
- At last LRC is added.
  ↳ row.

Checksum

Checksum = check + sum

Checksum Analog : Sender side

Checksum Validation : Receive side..

- Break the original message into 'k' number of blocks with 'n' bits in each block.
- Sum all the 'k' data blocks
- Add the carry to the sum, if any
- Do 1's complement to the sum = Checksum (n bits)

For Receive : The Result of all blocks including parity block, sum must be 11111.

98
-47
51

50
+33
+07
90 = 3011

Checksum Protocols.