* Why need networking ?
- World without boundaries
- Global communities
- human network.

* Networking : Networking refers to the practice of connecting multiple devices and systems together to enable communication, resource sharing and collaboration.

Host : Every computer (device) on a network

End device : An end device specifically refers to the devices at the edge of a network that interact directly with users.

- Data originate
- flows through network
- Data recieve

Ex: Router, switch → host but not end device

All end device → host

not all host → end device

Server : Computers that provide info to end devices.

3 types:
1) Email
2) web
3) ~~Server~~ File

Senven type	What senven uses	what client use	Access what
Email	email senven s/w	client s/w	Email
Web	web senven s/w	browsen s/w	web pages
File	stones componate and usen file	componate and usen file	files

- **Clients**: computons that send neqvests to the senvens to netrieve infonmation.

- **Peen-to-peen Netwonk (P2P)**: P2P netwonk is a distributed netwonk anchitecture in which participants (often nefenned to as peens) communicate and shane nesounces directly with each othen without the need for a centna-lized senven on authonity.

Pros:

- Easy to set up
- Less complex
- Lower cost
- used for simple tasks
  - transfer file
  - share prints

Cons

- no centralized administration
- not secured
- not scalable
- slower performance

Intermediary Device: interconnects end devices.

- regenerate and retransmit data signals.
- maintain info about existing pathways
- notify other device about errors / communication failures.

Ex: Router, LAN switch, multilayer switch, firewall appliance, Router

(5)

Network media: allows message to travel from source to destination

- carries communication

ISOC – Internet Society

IRTF – Internet Research Task Force

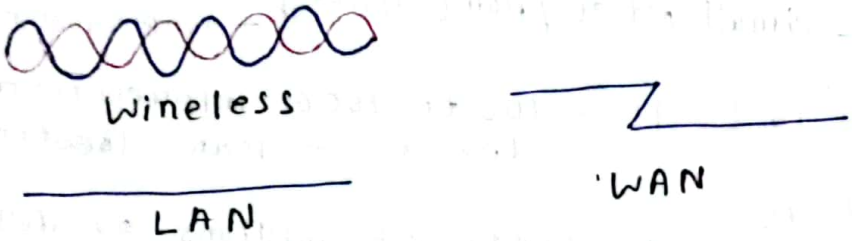
IANA – Internet Assigned Numbers Authority manages → IP Address, Domain Name, TCP/UDP Port Number

(3) types of Network media

Cables (Copper) → Metal wire — Electrical impulses

Fiber optic cable — light

Wireless — specific frequencies of electromagnetic waves



Network / Topology Diagram: use symbols to represent devices within network.

NIC (Network Interface Card): hardware component that enables a computer to connect to a network.

- provide necessary interface between computer and network medium
- establish and maintain network communication

Physical port: physical connecton on a device

Interface: connection point between device and network / another device

Networks types (based on size) — (4)

1) Small home — few computers and internet
2) SOHO - [Small office / Home office] - remote office - corporate network
3) Medium to Large — 100 to 1000 interconnected devices — many locations
4) World Wide — hundreds of millions of devices

* Network infrastructe depends on / vary in terms of:

1) Size of the area covered
2) No. of connected users
3) No. and types of available services
4) Area of responsibility.

EIA - Electronic Industries Alliance
TIA - Telecommunications Industry Association

* Types of Networks (based on area) - (2)

LAN → Network Infrastructure ← WAN

Local Area Network	Wide Area Network
- spans a small geographical area	- spans a wide geographical area
- interconnect end devices in a limited area	- interconnect LANs over wide geo. areas
- administrated by a single org. / individuals	- administrated by 1 or more service providers.
- provide high-speed bandwidth to internal devices	- provide slower speed links between LANs

Internet: worldwide ~~conn~~ collection of interconnected LANs and WANs.

LANs use WANs
WANs use copper wires / Fiber optic cable / wireless transmissions

to connect with each other.

IETF - Internet Engineering Task force
ICANN - Internet Corporation for Assigned Names and Numbers
IAB - Internet Architecture Board
→ maintain structure of internet

collection of LANs and WANs

Intranet: private network accessible only to authonized individuals within an org. (only company)

Extranet: accessible to

- authonized individuals within an org.
- company
- suppliens
- collaborators
- customens can access
- external users outside org.
  - Limited permission of access

Home and Small office (SOHO) Internet Connections

1) **Cable:**
   - high bandwidth
   - always on
   - provided by cable tv service provider

2) **DSL** (broad band digital subscriber Line)
   - high bandwidth
   - always on
   - runs over a telephone line

3) **cellular**
   - use cell phone network

4) **Satelite**
   - no internet service providers needed
   - rural areas

ITU-T → International Telecommunications Union Telecommunication Standardization Sector

5) Dial-up telephone (modem)
   - low bandwidth
   - not expensive

Business internet connections
- higher bandwidth
- dedicated connection
- managed services needed

1) Dedicated Leased Line
2) Ethernet WAN
3) DSL (Ex: SDSL (Symmetric))
4) Satellite

Converged networks: deliver data/voice/video over the same network infrastructure
- uses same set of rules and standards

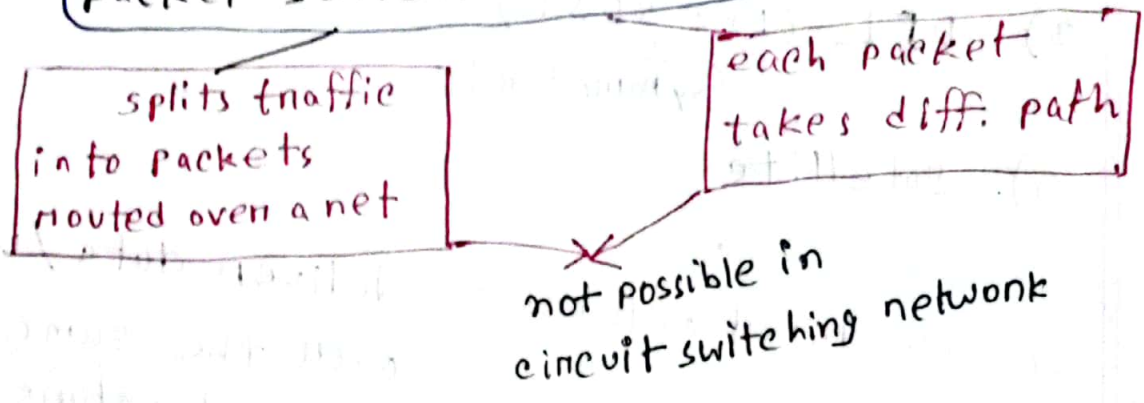
Network Architecture: refers to the technologies that support the infrastructure that moves data across the network.

* characteristics of Reliable Network (4)
1) Fault tolerance
2) Scalability
3) QoS (Quality of Service)
4) Security

1) Fault tolerance: refers to the network's ability to limit the impact of a failure by limiting the number of affected devices.

how works? – multiple paths needed

– provide redundancy by implementing a packet switched network



why redundancy needed?

→ when a link/device fails

→ allow alternative path

→ unaffected network

2) Scalability: - expand networks quickly
- support additional devices to be connected to network
- doesn't affect performance of services
- follow accepted standards/protocols

3) QoS: primary mechanism used to ensure reliable delivery of content for all users
- managed by routers
- set priorities — web page - lower priority
voice over call - higher priority
- need smooth/uninterrupted service

Ex: Live video - pause and break continuously
- bandwidth demand > available
- QoS not configured

4) Network security : (2 types)

Network infrastructure security	Information security
– security of network devices	– protect info.
– prevent unauthorized access to device	

3 goals: 1 Confidentiality 2 Integrity 3 Availability

* Network Trends (4)

1) BYOD – Bring Your Own Device

allows end users to use their own devices which give them more opportunities and greater flexibility to access information.

2) Online Collaboration: work with others over network

Tool: Cisco WebEx Teams

– joint project

send msg post image etc

3) Video Communication:

Tool: Cisco TelePnesence Powens

4) Cloud Computing:

- stone pensonal files / backup data on senvens oven intennet
- smallen companies
  - not affond own data centen
  - lease senven and stonage from langen data centen ong.

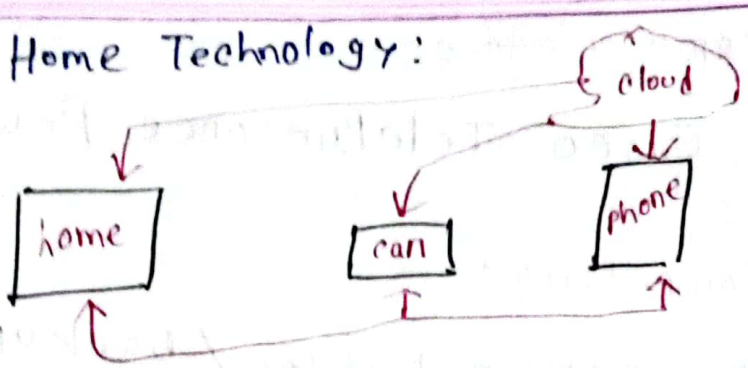
(4) types

1) Public: available to public
   - paid on free
2) Pnivate: fon specific ong
3) Hybnid: combo of 2 on mone types of clouds
   - some pant custom
   - " " public

Each pant ~~अलग~~, but connected using the same anchitecture

4) Custom: built fon specific ong.

Smart Home Technology:



Powerline Networking:

- when wireless communication not possible
- device connect to LAN
- use standard powerline adapter.

Wireless Broadband: home / small business use

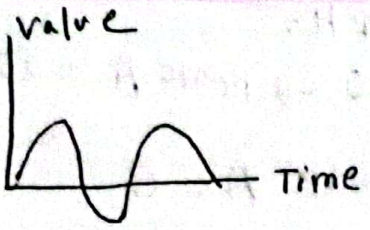
- antenna is installed

WISP — Wireless Internet Service Provider

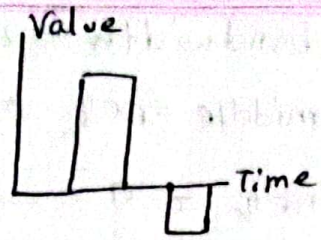
- is an ISP that connects user to designated access points or hotspots.

1 character — 8 bit

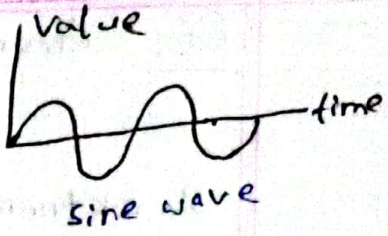
Chap — 3



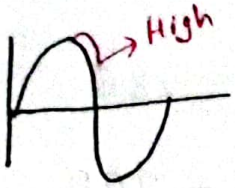
Analog Signal

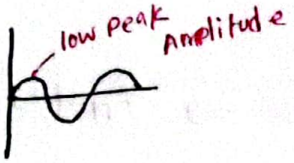


Digital signal



sine wave



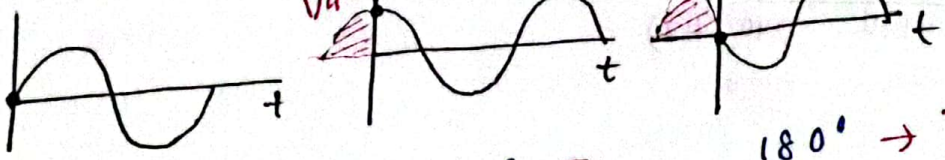


Period, $T = \frac{1}{f}$ → Frequency
(s) (Hz)

Wavelength, $\lambda = vT$
(m) $= \frac{v}{f}$

v → propagation speed

Phase: (same amplitude and f) with



phase = 0° → T=0

0 amplitude
↓
increase

not shifted

90° → T/4

peak amplitude
↓
decrease

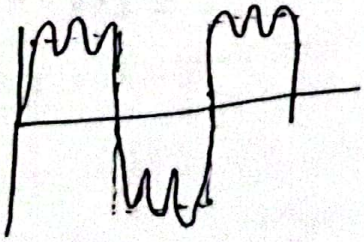
shifted to left by 1/4 cycle

180° → T/2

0 amplitude
↓
decrease

shifted to left by 1/2 cycle

Composite signal.



* Bandwidth, $B = f_H - f_L$
* Medium frequency, $f_0 = \frac{f_H + f_L}{2}$
* No. of bits per level $= \log_2$ (no. of levels)
* Bit rate = amount of data / time

Ex: Given, bandwidth = 200 kHz

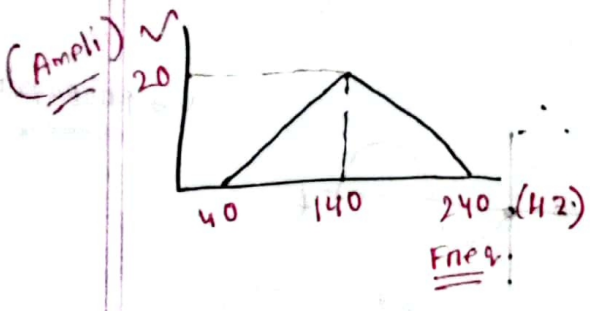
middle freq = 140 → peak A = 20 V

2 extreme freq = ? → peak A = 0.

(both low and high) Find freq of them.

Soln: $\frac{f_H + f_L}{2} = 140 \rightarrow f_H + f_L = 280$

Again, $f_H - f_L = 200$



$\therefore f_H = 240, f_L = 40$ Hz

Ex: download text document at the rate of 100 pages per minute, where

1 page → 24 line

1 line → 80 chars.

Soln:

bit rate = (100 × 24 × 80 × 8)

= 1536000 bps

= 1.536 mbps

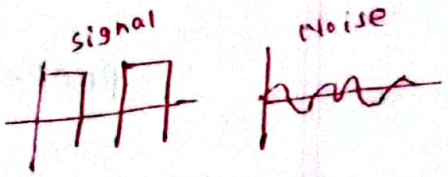
For noiseless channel,

* Bit rate = 2 × bandwidth × $\log_2$(level) → Nyquist theonem
* Bit length = propagation speed × bit duration
* Bandwidth (Hz or bps): $B = \frac{f}{2}$ (Harmonic 1st)

$B = \frac{3f}{2}$ (3rd harmonic)

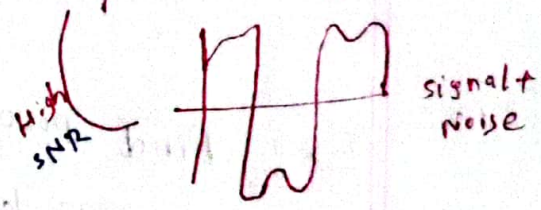
$B = \frac{5f}{2}$ (5^{th})

* decibel: $dB = 10 \log_{10} \frac{P2}{P_1}$
* Signal to Noise Ratio: $SNR = \frac{\text{avg. signal power}}{\text{avg. noise power}}$



* $SNR_{dB} = 10 \log_{10}(SNR)$

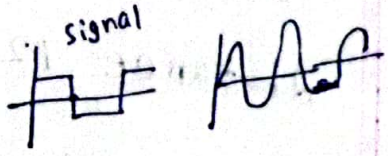
high low



* when noiseless → ideal/ not possible in real

$SNR = \frac{\text{signal power}}{0} = \infty$

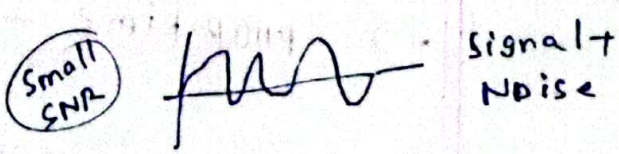
$SNR_{dB} = 10 \log_{10}(\infty) = \infty$



* For noisy channel (Shannon capacity)

$C = B \log_2(1 + SNR)$

$= B \times \frac{SNR_{dB}}{3}$



* Transmission time (s) = $\frac{\text{packet length (bits)}}{\text{Bandwidth (bps)}}$ (message size)

* Latency (s) = processing time + queuing time + transmission time + propagation time

$t = \frac{s}{v} = \frac{\text{dist.}}{\text{prop. speed}}$

* Throughput = am. of data / time

* bit length = $v \times$ bit duration

$= \frac{s}{t} \times$ bit u

s → distance

t → propagation time

$\therefore$ prop. time = $\frac{s \times \text{bit duration}}{\text{bit length}}$

Ex: Find propagation time and transmission time for a 2.5 kbyte message, bandwidth = 1 Gbps, distance 12000 km, speed = 2.4×10^8 m/s

→ prop time = $\frac{\text{dist.}}{\text{prop. speed}} = \frac{12000 \times 10^3}{2.4 \times 10^8} =$ s

trans. time = $\frac{\text{message size}}{B} = \frac{2.5 \times 10^3 \times 8 \text{ bits}}{1 \times 10^9 \text{ bps}} =$ s

Analog signal: continuous waveforms where the signal's amplitude, frequency and phase can take on any value within a given range.

Digital signal: a signal that represents data as a sequence of discrete values.

Periodic signal: a signal that repeats its waveform over time at regular intervals. (T fixed)

Non-periodic signal: a signal that doesn't repeat its waveform over time in a regular interval.

Peak amplitude: The peak amplitude of a signal is the absolute value of its highest ~~ent~~ intensity, proportional to the energy it carries.

Period: refers to the amount of time, a signal needs to complete 1 cycle.

Frequency: refers to the no. of periods in 1 s.

Phase: describes the position of the waveform relative to time 0.

Wavelength: refers to the distance between two consecutive points of the same phase on a wave.

Single frequency sine wave → make sound
→ not send data

Composite signal: A signal made of many simple sine waves with diffenent f, A and phases.

periodic/non periodic
T → same or diff.

periodic composite signal —decomposition→ discrete frequency (series of signals)

non-periodic → continuous frequency (combo of sine waves)

Bandwidth: range of frequencies contained in a composite signal.

Bit rate: no. of bits sent in 1 s.

Bit length: distance one bit occupies on the transmission medium.

Broadband Transmission/ modulation: digital signal → analog

Decibel: measures the relative strengths of 2 signals on 1 signal at 2 different points.

→ energy loss
negative → signal decreases (attenuated)
positive → " amplified → energy gain

Distortion: means that the signal changes its form/shape.

condition
- composite signal
- different f

Impairment: the signal beginning of medium ≠ " end " "

3 cause
- Distortion (form change)
- Attenuation (energy loss)
- Noise

Throughput: how fast send data (bps)

Delay: refers to the time it takes for a packet to travel from source to destination

Transmission time: time to transmit a data packet over a network link.

Propagation time: refers to time it takes for a signal to propagate through a physical medium.

Queuing/waiting time: time a packet spends in a queue before it can be transmitted.

Processing time: time needed by network devices to process and handle packets.

DLL (3)

Data Link Layer: responsible for communication between end-device NIC.

5 tasks

(1) Framing
- encapsulate network layer packets into frames
  - 2 parts: header, trailer

(2) Physical Addressing
- assign unique MAC address to each device
- used to identify device (LAN)

(3) Media Access Control (MAC)
- control access to physical transmission medium (LAN)

(4) Error Detect and Reject
- if a frame is corrupted, reject it; not forward to upper layers

(5) Access control
- manage access to physical transmission medium
- manage data transfer

2 sublayer of DLL:

1) LLC
Logical Link Control
- acts as an interface between Network layer and MAC sublayer.
- error check
- control flow
- frame synchronize

2) MAC
Media Access Control
- encapsulate data
- media access ctrl

Network	Network Layer protocol			
Data link	LLC	LLC - IEE 802.2		
	MAC	Ethernet IEEE 802.3	WLAN 802.11	WPAN 802.15
Physical		Fast ethernet GB "	wireless	blue-tooth

IEEE 802 LAN/MAN

MAN – Metropolitan Area Network
WLAN – Wireless LAN
WPAN – wireless personal area network

* How provide access to media? /
Packet exchange between nodes /
(performed by router)

Four basic 2 layer functions :

1) Accepts a frame from network medium
   – via ethernet or wireless connection
   → encapsulated data packet

2) De-encapsulates the received frame
   – to extract the original packet
   – remove header and trailer
     ↓
     added at the prev. hop

3) Re-encapsulates the packet into new frame
   – examine packet header (to determine destination)
   – add new header and trailer
     ↓
     appropriate for next hop

4) Forwards the new frame on the medium of next network segment.

hop – movement of data packets device to device

IEEE - Institute for Electrical and Electronic Engineers
ITE - International Telecommunications Union

** Topology: The topology of the network is the arrangement and relationship of the network devices and the interconnections between them.

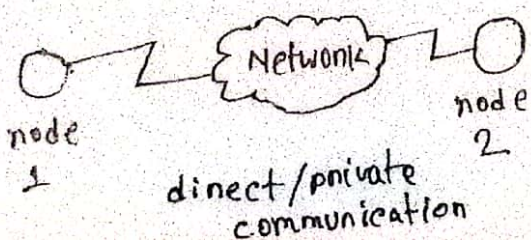
2 type

1) Physical
- shows physical interconnection between devices

2) Logical
- shows virtual connection
- use device interface and IP addressing schemes

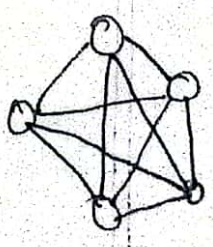
3 common physical WAN topologies

Point to point
- permanent link between to endpoints
- nodes may not share media with other hosts
- simplest



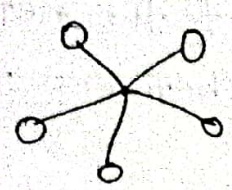
Hub and spoke
- similar to star
- a central site interconnects branch

mesh
- needs every end users to be connected to each other
- highly available



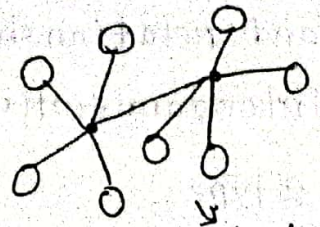
ISO - International Organizations for Standardization
ANSI - American National Standards Institute

LAN Topologies (4)

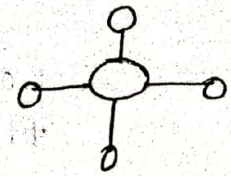


Star

- easy to install
- easy to troubleshoot
- scalable

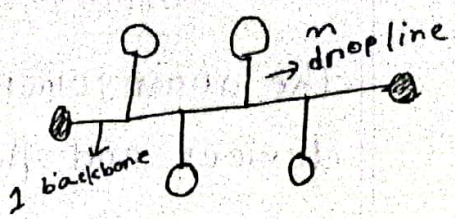


Extended star



Ring

- each end device connected to neighbours
- form a ring



Bus

- all end device chained together
- terminates on each end

Half-duplex

only 1 device is allowed to send and receive at a time

Ex: WLAN, legacy bus topology with ethernet hubs

Full-duplex

- allows both devices for simaltaneous data transmission

Ex: ethernet switch

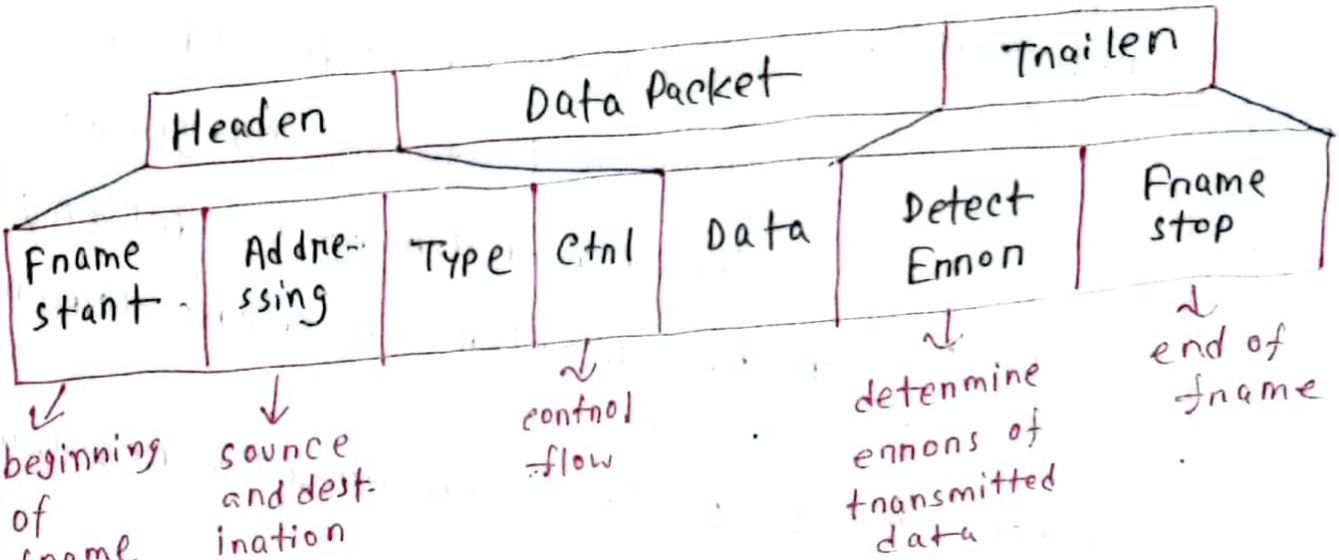
CSMA/CA - Cannien Sense Multiple Access with Collision Avoidance

CSMA/CA — " Detection

* Data — encapsulated by DLL
— fonm a frame

Data Link Fname
3 pants

Headen Trailen Data



Protocols used (5)

1) Ethennet
2) 802.11 Wineless
3) PPP (Point to point)
4) HDLC (High level data link Contnol)
5) Fname nelay

Access Ctnl Methods (2)

1) Contention based access
2) Controlled access

2 types:
1) CSMA/CA
2) CSMA/CD

Communication Elements: [3]

1) senden
2) Receiven
3) media

Protocols: nules that communication follows.

↳ Requinements: (4)

1) An identified senden and neceiven
2) common language and gnamman
3) Speed and timing of deliveny.
4) confinmation on acknowledgement

have –
1) own function
2) " fonmat
3) " nules

Common computen protocols agneement's nequinements: (5)

1) message encoding
2) message fonmatting and encapsulation
3) " size
4) " timing
5) " delivery options (3)

- Flow ctnl – nate of data transmission / speed / how much info
- Response timeout – how long wait when no neply neceived
- Access method – determines when msg send

Message has specific fonmat
depends on
– type of msg
– deliveny channel

Unicast – 1 to 1 | Mulicast – 1 to many | Bnoad – 1 to all
IPV4 network

message → (converted) bits → (encoded) light/ sound/ electnical impulse → (decode signals) destination

lossy
interprete msg

Collission: more than on device send traffic at the same time → message conupted

reverse

Encoding: process of converting information into another acceptable form for submission

Decoding: process of interpreting and extracting meaningful information from encoded data.

More about protocols:

Protocol Data Unit (PDU) → steps

Data segment packet ↓ Frame Bits ↓ (All 5 are top to bottom)

Types: (4)

1) Network communication: how many device communicate
2) " Security: secure data, authentication, integrity encryption
3) Routing: (exchange route info → compare path info → select best path
4) Service Discovery: auto detect service

6 functions:

1) Addressing - identify senden and receiven
2) Reliability - guaranteed delivery
3) Flow Control - ensure data flow at efficient rate
4) Sequencing - uniquely labels each transmitted segment of data
5) Error Detection - determines if data corrupted
6) Application Interface - p2p communication
   ↓
   Process to process

4 Layers of TCP/IP

diffenent protocols: (message delivery format)

* HTTP — web server → web client → App layer
* TCP — individually handle → Transport layer
* IP — sender → receiver (globally) → Internet layer
* Ethernet — NIC → NIC (same LAN) → Network Access Layer

2 layers: - Higher
- Lower → move data
→ provide service to higher layers

Protocol suite: set of ~~procols~~ protocols that work together to provide network communication and services.

* TCP/IP — most common
— maintained by IETF
* OSI — developed by ISO and ITU
* Apple Talk — developed by Apple Inc. released
* Novell Netware — developed by Novell Inc

middle ↗

OSI Model Layer (7)	TCP/IP Protocol suit	TCP/IP Model Layer (5)
7. Application – contains Protocols used for P2P communication		
6. Presentation	HTTP/DNS/ DHCP/FTP	Application
5. Session		
4. Transport	TCP/UDP	Transport
3. Network	IPv4/IPv6/ ICMPv4/ICMPv4	Internet / Network
2. Data Link – exchange data frame method	Ethernet/WLAN/ SONET/SDH	Network Access
1. Physical		

Right sign ekhn

TCP - connection oriented
UDP - connectionless

~~Data Bits (0+1)~~ Physical, Data Link

* Segmenting: process of breaking up messages into smaller units

2 pros →
1) speed increase
2) Efficiency ↑

* multiplexing: process of taking multiple streams of segmented data and interleaving them together.

* Sequencing: process of numbering the segments so that the message may be reassembled at the destination.

TCP does this

আবার একত্রিত করা

* 6 benefits of using layered model:
1) modular design 2) Interoperability 3) Abstraction 4) Easy troubleshooting
5) standardization and compatibility 6) Easy implementation

Application → Data

Transport → Segment Header | Data

Internet → Packet Header | Seg Header | Data

Data Link → Fname Header | Pack Head | Seg Hea | Data | Fname trailer

Physical → Data (0 and 1 only)

Left ⇒ TCP/IP

Right ⇒ Data Encapsulate and De-encapsulate

উপর থেকে নিচে → Encapsulate

নিচ থেকে উপরে → De-encapsulate