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 - IEEE 802.2		
	MAC	Ethernet IEEE 802.3	WLAN 802.11	WPAN 802.15
Physical		Fast ethernet OR "	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 /

Four basic 2 layer functions : (performed by Router)

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.

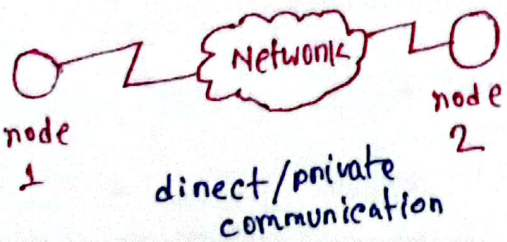
2 type

1) Physical
- shows physical interconnection between devices

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

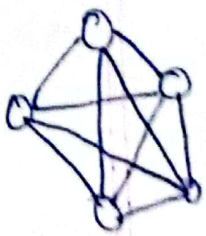
3 common physical WAN topologies

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



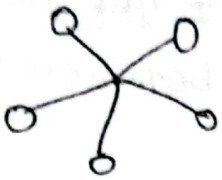
Hub and spoke
- similar to star
- a central site interconnects branch

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



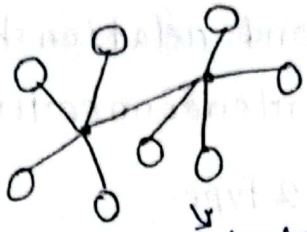
ISO - International Organizations for Standardization
ANSI - American National Standards Institute

LAN Topologies (4)

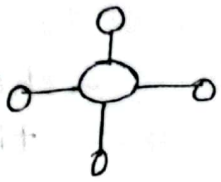


Star

- easy to install
- easy to troubleshoot
- scalable

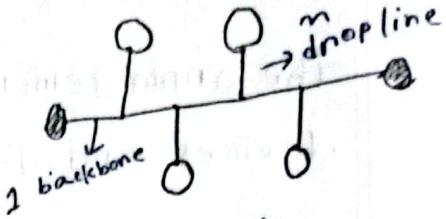


Extended star



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 - Cannier Sense multiple Access with Collision Avoidance

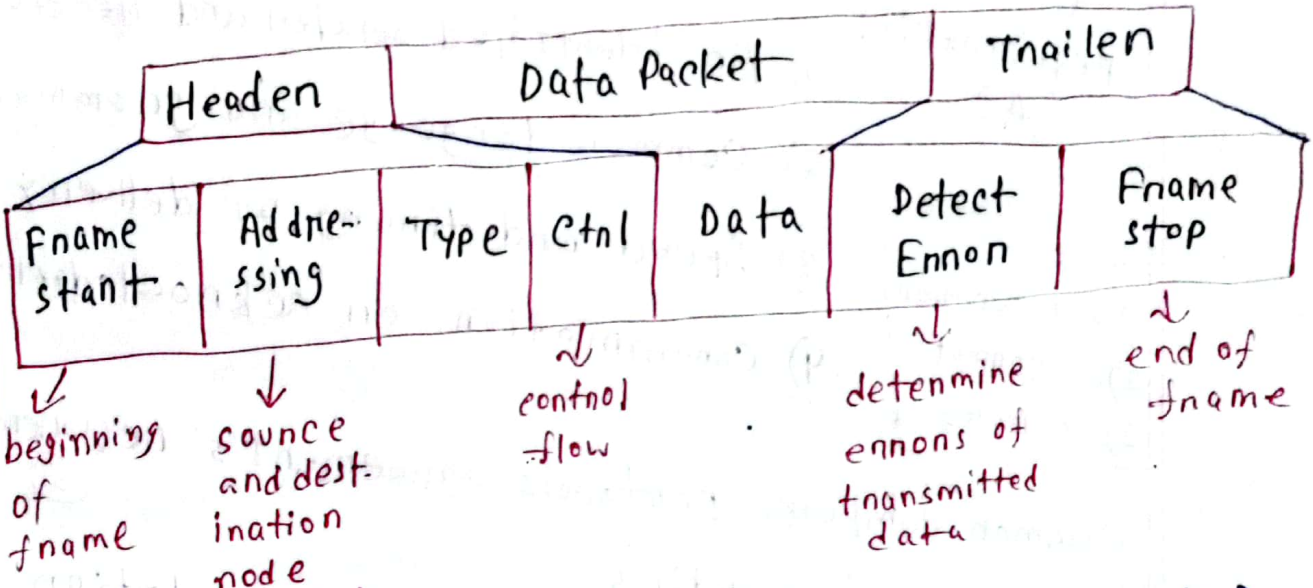
CSMA/CA — " Detection

* Data — encapsulated by DLL
— form a frame

Data Link Fname

3 parts

Headen Trailen Data



Protocols used (5)

1) Ethennet
2) 802.11 Wineless
3) PPP (point to point)
4) HDLC (High level data link control)
5) Fname relay

Access Ctnl Methods (2)

1) Contention based access
2) Controlled access
→ 2 types:
1) CSMA/CA
2) CSMA/CD

Routing: When router receives an IP packet on one interface, it determines which interface to use to forward the packet to the destination.

- use it IP routing table to determine path.

Best path (longest match)

	Dest IP address	Binary
	192.168.2.82	11000000.10101000.00000010.01010010
Prefix:	192.168.2.80	11000000.10101000.00000010.01000000

How Router building routing table?

→ 1) Directly connected networks

2) Remote Networks → not directly connected with router
   - static
   - dynamic

Default routing ..../0
no bits to match the dest. IP address for this route entry to be used

→ using protocol : static and dynamic

Static	Dynamic
manually configure the routing table on each router	automate the process of building and maintaing routing table by allowing routers to exchange routing info.
manually enters the routes and associated next hop info.	complexity doesn't depend on size.
complexity: increases with net. size.	automatically adapts to change.
when topology changes, administraton intervention needed.	more scalable large network
less scalable small network	use cpu, memory and link b/w
no. additional resource needed	auto. determine best path.
explicitly defined by administraton	

Routing Table Entries:

1) Route source
2) destination network
3) administrative distance
4) metric
5) next hop
6) route timestamp
7) exit interface

Default routing? specify a next hop en route to use routing table doesn't contain a specific route. that matches dest. IP add.

— dynamic / static

IPv4 route entry: 0.0.0.0/0

IPv6 : ::/0

Lecture - 10

* TCP servers processes are assigned port numbers. A server can't have 2 services assigned to the same port number within the same transport layer services

* TCP connection Establishment

1) client requests a client-to-server communication session with the server.
2) server acknowledges and request
3) client acknowledges

* TCP connection termination:

1) when the client has no more data to send in the stream, it sends a segment with FIN (finish) flag set.
2) the server sends an ACK to acknowledge the receipt of FIN and terminate session from client to server.
3) the server sends a FIN
4) The client responds with ACK

* TCP 3-way handshake:
— establish reliable connection between client and server.

3 steps: 1) client sends (SYN) to server to initiate the connection
2) server receives SYN and sends SYN-ACK
3) client sends ACK to complete the handshake

* TCP reliability and flow control.
1) provides guaranteed and ordered delivery of data
2) uses sequence numbers to ensure correct order of data segments.
→ UDP not track sequence number

* Q.S:
— set of techniques used to prioritize and manage network traffic.
— maintain reliability and performance
— voice, video, data traffic has diff. requirements and priorities.

VLAN

- logical groups of devices in the same broadcast domain
- acts as a subgroup of the switch ports in an Ethernet LAN.
- spread across multiple switches
- acts like a physical LAN.

Why VLAN's used? → provide logical separation of device

- increase the no. of broadcast domains, but decrease their size
- keep hosts that hold sensitive data on a separate VLAN to improve security.
- enable flexible network designs, not limited by physical location.
- easier to manage / maintenance
- scalability → no need of rewiring connection, simply configure a port on the switch to belong to a different VLAN

- high performance - low latency
- less cost - less complex

Ranges:

0 and 4095 — not used / not seen

1 — default, use / ~~delete~~, ~~edit~~

2 - 1001 : create, edit, delete

1002 - 1005 → ~~delete~~

1006 - 4094 - extended range

How VLAN works?

- id assign
- port assign
- inter-VLAN communication by VLAN trunking
- VLAN tagging is used to identify which VLAN the data belongs to.
  - when traffic passes through a trunk port between switches

Types: (3)

1) Port based 2) Protocol based 3) MAC based

LAN	VLAN
- group of devices connected in a limited area	- custom network created from one or more LAN
- Local Area Network	- virtual Local Area Nw.
- latency high	- latecy low
- cost high	- cost low
- packet is delivered to each device	- delivered to only a specific broadcast domain
- uses FDDI as a protocol	- ISP and VTP as a protocol

FDDI - Fiber Distributed Data Interface

→ 2 or 3 devices

Purpose: a) when lot of traffic on LAN

b) a group of users need more security on being slow down by many broadcasts

c) when users not on 1 broadcast domain.

d) make a single switch into multiple switche

Cons: a) if attackers gain access to a VLAN, affect the entire VLAN

b) message packet can be mistakely forwarded to another VLAN

c) if large networks with multiple VLANs, for routing between VLANs, routers or layer 3 switch is needed.

d) interoperability challenges

e) limited inter-VLAN traffic forwanding

f) if a single device malware infected → affect the whole VLAN.