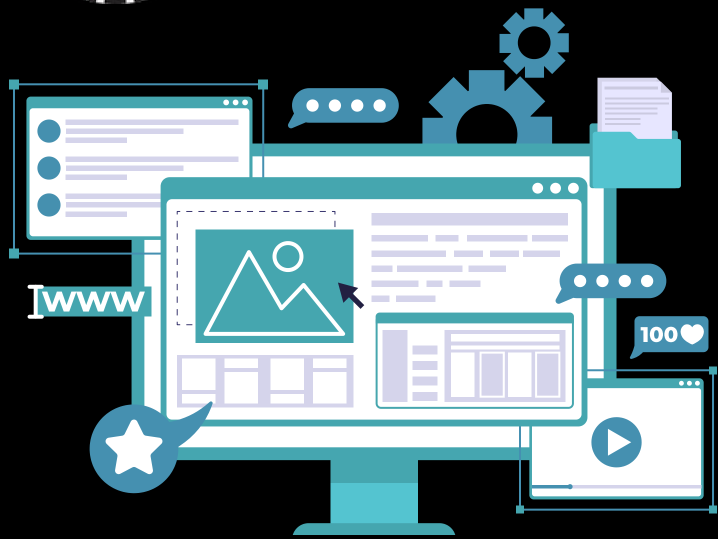
noteswithlove ❤

COMPUTER NETWORKS - II

HANDWRITTEN NOTES

X noteswithlove



These Storage Networks notes are curated as per the upcoming semester exam syllabus and cover all key topics for quick revision. Specially prepared by seniors for Graphic Era students, they are ideal for last-minute preparation. Go through them carefully.
All the best for your exam!

JOIN US FOR MORE NOTES

CLICK HERE TO JOIN TELEGRAM

CLICK HERE TO JOIN WHATSAPP

Unit-2

Introduction to link layer

The link layer or (Data link layer) is the 2nd layer of the OSI model.

Its primary function is to enable reliable communication between directly connected devices (neighbor-to-neighbor) over a physical medium (wired or wireless).

Main Responsibilities of Link Layer.

- Framing – dividing data into manageable units.
- Error detection and handling.
- Flow control – Ensure sender does not overload receiver.
- Media Access Control → Ensure & control which device can transmit when device share link.
- Ensure Integrity – Ensures frames are delivered without loss / duplication.

Services Provided by Link Layer

1) Framing – A frame contains header + playload + trailer
The receiver extracts playload (packet) from frame

2) Error detection and Checking – during transmission, bits may get corrupted due to noise
Link layer detects Error through –
   - CRC
   - Checksum
   - Parity Bits

Some technology support error correction → ARQ in WiFi

3) Flow control → Ensure that sender does not transmit faster than user can process.
Techniques used → Stop and wait, Sliding Window

4) MAC - Determines which device can transmit at a given time when multiple device share a communication.
Prevents collisions and Confusion → CSMA/CD
CSMA/CA

5) Reliable Delivery
Some link technologies retransmit lost or corrupted frames to ensure reliability.
More important in wireless networks

Where link layer is Implemented?

Area of Implementation	Examples
• Inside NIC (Network Interface Card)	Ethernet NIC WIFI Card
• In device drivers	OS Network drivers
• In Hardware	Switches, Bridges
• In wireless Network and wired	Bluetooth, WiFi, Ethernet

* The link layer is implemented at the boundary of network devices, where frames are transmitted physically across the link.

MAC address
A MAC address is a unique hardware identifier assigned to every NIC for communication with LAN. It helps devices identify each other.

Characterstics
Length - 48 bits (6 bytes)
Representation - 12 hexadecimal digits
Format - Example → 08:4F:A2:65:1B:3C
Uniqueness - different for every device
Layer - data link layer
Purpose - for local addressing.

MAC → divided into
- OUI (Organizationall unique Identifier) — First 24 bits
- NIC Specific (Last 24 bits)

Purpose –
- to provide correct ethernet / wifi frame to devices inside LAN. Used in APR, wi-fi Access Control.

MAC Address	IP address
• Hardware address	• Logical Address
• Assigned by manufactorer	• Assigned by network admin
• Link Layer	• Network Layer
• Permanent	• Changable

$\boxed{\text{ARP}}$

ARP (Address Resolution Protocol) is a protocol used to map an IP address to a MAC address within a LAN.

Since devices, IP works at Network layer and MAC works at Link Layer, to send a data inside a LAN, an IP packet must be encapsoldte inside frame containing a MAC address

Therefore ARP act as a bridge between IP and MAC

Example – A PC A (IP: 192.168.1.10) sends data to PC B (IP: 192.168.1.20)

- A sends ARP Req. – broadcast
- B reply with ARP reply – Unicast
- A can now send data to B.

ARP cache – temporary storage of recently learned IP–MAC mappings

Types of ARP

- ARP
- RARP (Reverse ARP)
- Proxy ARP

Ethernet

Ethernet is the most widely used wired LAN
It operates at link layer and Physical layer
of OSI model used to transmit data in
form of frames using fibre cables.

Key features

- Based on IEEE 802.3 Standards.
- Support unicast, multicast, broadcast
- Use MAC address for device identification
- Very reliable and Fast

* Ethernet frame format

| Preamble | Dest. MAC | Source MAC | Type / Length | Playload | FCS |

Early Ethernet	Modern Ethernet
Bus topology	Star topology
Collision common	Collision - free
Hubs Used	Switches used

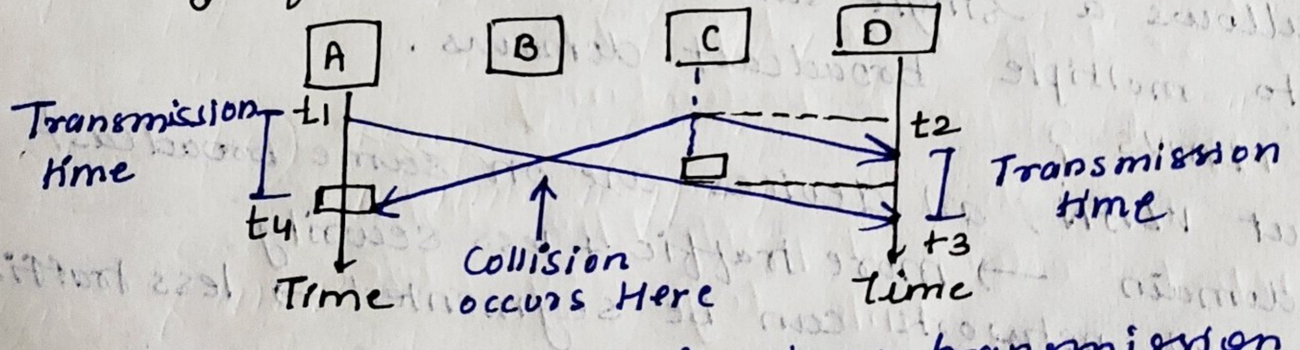
Ethernet Technologies

Technology	Speed	Medium	Note
10 Base-5 / 10 Base-T	10 mbps	Coax	First Ethernet
Fast Ethernet	100 mbps	UTP	10x faster
Gigabit Ethernet	1Gbps	UTP	Common in LAN
10G ethernet	10Gbps	Fibre/copper	Data Centres
40G / 100G Ethernet	40-400 Gbps	Fiber	Cloud
Switched Ethernet	Varies	Switch + Fiber	Remove Collisions

- Low Installation cost and High speed.

# CSMA / CD	CSMA / CA
• Carries sense Multiple Access with collision Detection.	• Carrier sense multiple Access with collision Avoidance.
• Used in wired Ethernet (LAN).	• Used in wireless Network (WiFi), WLAN.
• device detects collision after it occurs then stop and retransmit.	• device tries to avoid collision before transmission.
	• Transmit only when collision probability is minimum.
• Collision can occur but can be detected	• Collisions are avoided.
• Suitable for wired Networks where collision detection is easy.	• Suitable for wireless Networks where collision detection is difficult
• works only in Half duplex Ethernet.	• works in half & full duplex WIFI
• Now Replaced by the switches.	• still used in IEEE 802.11
• Efficient only in Low traffic.	• Efficient even in high traffic wireless conditions

• Working of CMA/CD



If a collision occurs, it stops transmission sends a gamming signal waits a random backoff time and then retransmits.

Switch | Routers

Switch	Routers
• Operates at Layer 2 (data link layer)	• Operates at Layer 3 (Network Layer)
• Use MAC address for forwarding frames.	• Use IP address for forwarding ~~frames~~ packets.
• data unit = Frame	• data unit = packet
• Connects devices inside a LAN and forward frames.	• Connects multiple Networks and forward packets
• Faster	• Slower
• Basic LAN-level security	• Strong Network-level security
• supports VLAN	• does not support VLAN
• eg - Connecting PC, printers, mobiles within an office.	• eg - connecting office LAN to the Internet.

VLAN's (Virtual Local Area Network)

A VLAN is a local grouping of devices in a LAN regardless of physical location.

It allows a single switch network to be divided into multiple broadcast domains.

Why VLANS ?

Without VLAN, all devices are on same broadcast domain → more traffic + less security

With LAN, network can be segmented → less traffic + improved security + better performance.

Benefits

- Security - device in diff VLAN's can't communicate without a router
- Reduced broadcast traffic

Example of VLAN →

A company can divide departments using VLANs

VLAN 10 = HR department

VLAN 20 = finance dept

VLAN 30 = IT dept

Even if computers are physically mixed, VLAN seperate their traffic logically.

Gateway | Bridge

Gateway	Bridge
• Connects two ~~similar~~ different networks	• Connects two similar networks
• works at Layer higher.	• work at Layer-2.
• Address used → IP /Port	• Address used - MAC
• data → packets / Message	• data - Frames
• Connect LAN to Internet	• Connect two Ethernet LAN

Link Layer Switches

- A Link Layer Switch is a Layer-2 device that forwards Ethernet frames based on MAC
- Provide point-to-point communication inside an LAN.

Types of Link Layer Switching

1) Store and forward Switching
   Switch receives the entire frame, checks for error and the forward. Reliable but Higher Delay
2) Cut-through Switching
   Switch reads only the destination MAC address and immediately forward frame. Fast, can't detect Error
3) Fragment-free switching
   Switch first wait for 64 bytes before forwarding
   Avoid collision but can't check Errors

Properties of Link Layer Switching

- Forwarding and filtering frames only to intended destination port, filters out unnecessary transmission.
- Full-Duplex transmission – sender, Receiver can transmit simultaneously
- Allow broadcast + multicast
- Support for VLAN
- High throughput

Problems Associated with Switched LAN

Main problem — Switching loops
When multiple switches are connected loops may form. This leads to
- Duplicate frames.
- Network Failure

Methods to overcome –

Spanning Tree Protocol (STP)

STP is a switching protocol that automatically prevents loops in a switched LAN.
It prevents broadcast storms.
Ensure loop free topology
Support network Redundancy

How STP works

- detect redundant path b/w switches
- disable some links logically while keeping one active
- If active links fail
  ↓
  STP reactivates disable link

Provide redundancy without loops

— with Love
Nikhil Saxena

Important topics

Multiple Access Protocols

Multiple Access Protocols are rules the follow multiple users / nodes to share, a common communication channel without interference

They are used in Link Layer / MAC.

- Channel Partioning Protocols
- Random Access Protocols
- Taking Turns protocols

(1) Channel Partioning protocols

The channel bandwidth is divided among all users so everyone get a fixed share of medium

Techniques

- TDMA (Time Division Multiple Access)
  time is divided into slots, each user get slot.
- FDMA (frequency division multiple Access)
  channel bandwidth is divided into frequency
- CDMA (code division multiple access)

  All users transmit through simultaneously but with unique codes.

Features -

- No Collisions
- Fair to all Users
- High efficiency at High Load

(2) Random Access Protocols

In Random Access Protocols Nodes transmits whenever they have data. Collision may occur but recovery techniques are used.

- Pure ALOHA
- slotted ALOHA
- CSMA (Already covered)

Pure ALOHA

- Original ALOHA protocol developed at University of Hawaii.
- Transmit data anytime.
- Continuous time division.
- Collision probability is very high.
- 2 x Frame time
- Max. throughput = 18.4%
  and G = 0.5 for maximum
- Simple Structure
- Formula for throughput

  $$S = G e^{-2G}$$

  G = offered Load

  S = throughput
- More efficient in low load.
- Eg – Used in Early wireless network

Slotted ALOHA

- Improved version of pure ALOHA.
- Transmit only at the begin
- Time divided into equal slots.
- Collision probability is low
- 1 x frame time
- Max throughput = 36.8%
  almost double
- Complex structure
- Formula for throughput

  $$S = G e^{-G}$$
- More efficient for high load
- Used in
  Satelline Communication System
  TDMA based system.

Taking turns

The key idea of Taking turns is each device gets a turn to send data. Only the device whose turn it is can transmit and other must wait.

Example –

- polling – A central controller control each node. Like wired / wireless LAN.
- Token passing – A special token is passed b/w nodes send data → having token.

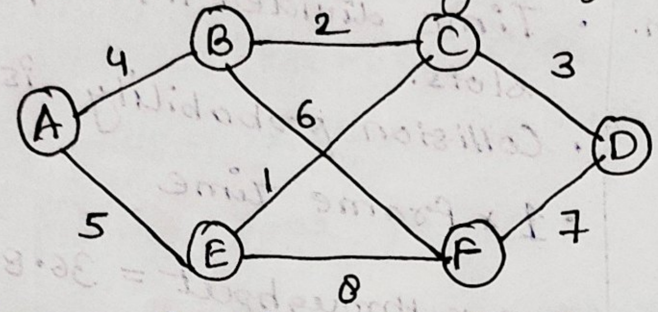
Taking turns are used in wifi power saving mode.

ARP	RARP
• Address Resolution Protocol	• Reverse Address Resolution Protocol.
• IP → MAC Mapping	• MAC → IP mapping
• Output → MAC Address	• output → IP address
• Used by normal Routers.	. Used by diskless workstation
• ARP table maintained locally	• Require RARP server
• Still used widely	• Replace by DHCP.

Advantages

- No collisions
- more efficient when traffic is high
- But token failure can stop network

Link State Routing Algorithm



Draw Routing table for all the Alphabets

A

Seq	
Age	
B	4
E	5

B

Seq	
Age	
A	4
C	2
F	6

C

Seq	
Age	
B	2
E	1
D	3

D

Seq	
Age	
C	3
F	7

E

Seq	
Age	
A	5
C	1
F	8

F

Seq	
Age	
E	8
B	6
D	7

this routing table consist which alphabet or node is connected to a node and its cost.

Dijkstra Algorithm — to find Shortest path.

Let A be source node.

	B	C	D	E	F
A	4	∞	∞	5	∞
AB	4	6	∞	$\boxed{5}$	10
ABE	4	6	∞	$\boxed{5}$	10
ABEC	4	6	9	5	10
ABECD	4	6	9	5	10

- (from A to nodes write cost if connected otherwise use ∞)
- Now choose the smallest Number and Add its path & don't repeat the choosen cost

ABECDF → possible shortest path to cover all nodes.

From A → B = 4

A → C = 6

A → D = 9

A → E = 5

A → F = 10

For Distance Vector you have to apply Bellman ford

— with Love
Nikhil Saxena

Numerical part

Error Detection and Correction

Error detection and correction are techniques which alters, modify the data at the time of transmission.

101 → 100
5 data altered 4

Types of Error —

→ Single bit Error
Error accured in single bit only / Change of single bit
Eg → 100 ⟶ 101

→ Burst Error
Error occured due to change in more than on bit.
Eg → 101010 ⟶ 111011

Error Detection techniques —
- Simple parity (Even, odd)
- 2D parity check
- Checksum
- CRC (Cyclic Redundancy checks)

Correction
- through Hamming

Parity Checks

Sender ~~checks~~ Sends → 1001001 0011
⇓
We Add 1 to check for Error — 1001 0011 0011 1 ↗ parity
⇓
Network

Transmission without Error	Transmission with Single-bit Error	Transmission with multiple-bit Error
Receiver Receives = 100100100111	100110100111	010100100111
No. of 1 = even	No. of 1 = odd	No. of 1 = Even
Even Parity	odd parity	Even parity
Parity is 0	Parity is 1	No error detect X
Error is not detected	Error detected	

• Parity checks only detects error of single-bit.

Checksum

Used to detect error.

10011001 | 11100010 | 00100100 | 10000100

$\boxed{\begin{matrix} n=4 \\ m=8 \end{matrix}}$ (no. of frames)
(no. of bits)

sender ⟶ receiver

Add first two frames then the remaining frames and if carry occurs add it again.

```
 ① 10011001
  + 11100010
  ----------
    01111011
          +1
  ----------
    01111100
  + 00100100
  ----------
 ① 10100000
  + 10000100
  ----------
    00100100
          +1
```

$\boxed{00100101}$ → Remainder

- Last step remainder + checksum

checksum is compliment of Remainder.

```
   00100101  → Remainder
 + 11011010  → Checksum
 ----------
   11111111
      ↓
  complement
 ----------
   00000000
```

- If we got all 0 at the end → Message Accepted Error-free.

CRC (cyclic Redundancy check)

Used to detect the Error.

Given frame = 11010110 11

Generator or divisor ⇒ 10011 or polynomial.

for example → $\boxed{x^3 + x + 1}$

→ $x^3 \; x^2 \; x^1 \; x^0$

binary conversion $\boxed{1 \; 0 \; 1 \; 1}$

As x^2 is not present in eqn we place 0.

PYQ on CRC

frame: 1101011011

Generator or divisor = 10011 (n=5)

Step 1 → ~~Add zero~~ In order to add Zero in ~~[illegible]~~ Frame.

no. of zeros add = $\boxed{n-1}$ wher n = length of generator

= 5 − 1

= 4 add 4 zeros.

Sender's Side

Use XOR operations

```
10011 ) 11010110110000
        ⊕ 10011
          010011
        ⊕ 10011
          00000 10110
              ⊕ 10011
                0010000
                ⊕ 10011
                  001110 → Remainder
```

Receiver Side

```
10011 ) 11010110111110
        ⊕ 10011
          010011
        ⊕ 10011
          00000 10111
              ⊕ 10011
                0010011
                ⊕ 10011
                  000000
                    ⇓
              Remainder of Receiver      Remainder
```

∴ As 4 bit no. is not divided by 5 bit no.

If Remainder of Receiver is 0 the message is accepted.

PYQ on ALOHA

Q An Aloha network uses 19.2 kbps channel for sending message packets of 100-bit long size. Calculat max throughput?

Ans Given, Channel Rate R = 19.2 kbps = 19200 bps

Packet Length L = 100 bits

For pure Aloha $\boxed{S = Ge^{-2G}}$

max occurs at $\boxed{G = 0.5}$ → It is standard for max. throughput

$S_{max} = Ge^{-2G} = 0.5 \times e^{-2 \times 0.5}$

$= 0.5 \times e^{-\cancel{2} \times \frac{1}{\cancel{2}}}$

$\Rightarrow 0.5 \times e^{-1} = 0.5 \times 0.3679 \approx 0.184$

Max throughput ⇒ 0.184

~~PYQ~~ PYQ

Q. A slotted ALOHA transmit on a shared channel of 400-bit frame size and 400 kbps. What is throughput if

(i) 1000 frames per second

(ii) 500 frames per second

For 1000 frames per sec,

$S = Ge^{-2G} \Rightarrow$ we need G

Given → frame size = 400 bits

Channel Rate = 400 Kbps

Frame Time ⇒ $\frac{\text{frame Size}}{\text{Frame Rate}} \Rightarrow \frac{400 \text{ b}}{400{,}000 \text{ bps}}$

$\Rightarrow 0.001 \text{ sec} = \boxed{1ms}$

→ For 1000 frames,

calculate G = Frame generation rate X Frametime

$G \Rightarrow 1000 \times 0.001 \Rightarrow 1$

$S \Rightarrow Ge^{-G} \Rightarrow 1e^{-1} = 0.3679$ → Throughput

→ For 500 frames

G = frame Generation Rate x Frame time

$G \Rightarrow 500 \times 0.001 \Rightarrow 0.5$

$S \Rightarrow Ge^{-G} \Rightarrow 0.5\, e^{-1 \times 0.5} \Rightarrow 0.5 \times e^{-0.5} \Rightarrow 0.3039$