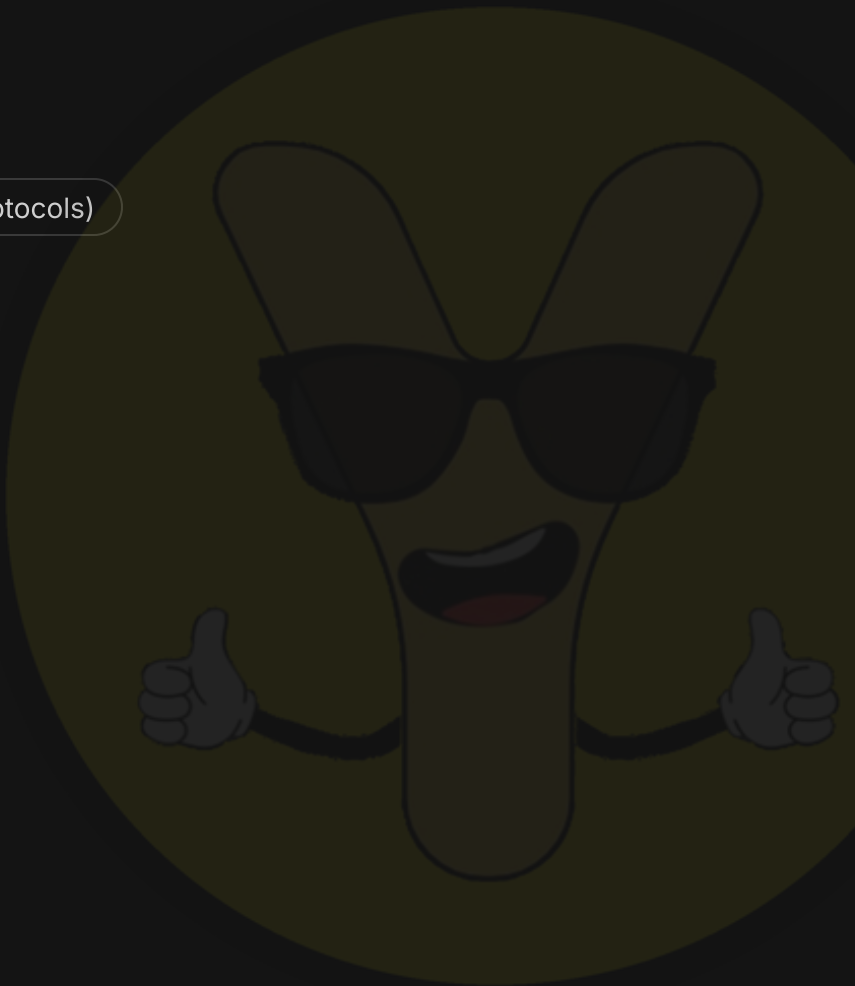
AKTU · 3RD YEAR · SEMESTER 6 · BCS603

Computer Networks

Unit 2 — Link Layer and Medium Access Control

- Framing
- Error Detection and Correction
- Flow control (Elementary Data Link Protocols, Sliding Window protocols)
- Channel allocation
- Multiple access protocols
- LAN standards
- Link layer switches & bridges (learning bridge and spanning tree algorithms)



DECODED BY

Chirag Jain

Founder, Ycotes · Gold Medalist in Artificial Intelligence, IIT Madras · taught 10,000+ students

theycotes.com

Data Link Layer & Framing Overview

FRAMING

Framing is a data link layer function that divides raw bit streams from the physical layer into discrete, manageable units called frames, containing control information like source/destination addresses and error-checking fields.

- Converts unreliable physical bit transmission into structured frames.
- Adds header (MAC addresses, control info) and trailer (CRC/FCS).
- Allows receiver to recognize frame boundaries and bit patterns.

Framing Methods

Framing techniques ensure the receiver correctly identifies frame starts and ends.

- Character Count: Header specifies frame length; vulnerable if count field corrupts.
- Byte Stuffing: Uses ESC (Escape) bytes to differentiate data bytes from FLAG delimiters.
- Bit Stuffing: Inserts a 0 after five consecutive 1s in data to prevent misinterpreting 01111110 flag.
- Physical Layer Coding Violations: Uses unused signals (e.g., Manchester encoding high-high) as frame delimiters.

Bit Stuffing Worked Example

Given the data bit stream 01111111001111101, perform bit stuffing for frame transmission with FLAG string 01111110.

1. Scan data from left to right for consecutive 1s.
2. After five consecutive 1s, insert a '0' bit regardless of the next bit.
3. Input data: 01111111001111101
4. First block: 011111 → insert '0' → 0111110011001111101
5. Second block: ...11111 → insert '0' → ...11111001
6. Stuffed payload: 01111101100111111001
7. Enclose payload with FLAG (01111110) at both ends.

Transmitted Frame: 01111110 01111101100111111001 01111110

Error Detection and Correction Methods

ERROR CONTROL

Error control techniques at the data link layer detect and correct bit errors introduced by channel noise during transmission.

- Parity Check: Single-bit parity (VRC) or 2D parity (LRC) detects odd number of errors.
- Checksum: Sums data blocks using 1's complement addition; commonly used in upper layers.
- Cyclic Redundancy Check (CRC): Polynomial division based robust error detection mechanism.
- Hamming Code: Forward Error Correction (FEC) mechanism capable of detecting 2-bit errors and correcting 1-bit errors.

Cyclic Redundancy Check (CRC) Calculation

Calculate the CRC frame trailer (FCS) for message polynomial $M(x) = 110101$ using generator polynomial $G(x) = 1001$ ($x^3 + 1$).

1. Determine generator degree $k = 3$ (number of bits in G minus 1).
2. Append $k = 3$ zeros to message: $M' = 110101000$.
3. Perform modulo-2 binary division of 110101000 by 1001.
4. Division remainder obtained after XOR operations: 011.
5. Append remainder (FCS = 011) to original message M.

Transmitted frame payload: 110101011

Hamming Code Error Correction Example

Encode 4-bit data $D = 1011$ into a 7-bit Hamming code $(7, 4)$ using even parity.

1. Bit positions: 1, 2, 4 are Parity bits (P_1, P_2, P_4); 3, 5, 6, 7 are Data bits ($D_3, D_5, D_6, D_7 = 1, 0, 1, 1$).
2. Position setup: $P_1, P_2, 1, P_4, 0, 1, 1$.
3. Calculate P_1 (positions 1,3,5,7): $P_1 \oplus 1 \oplus 0 \oplus 1 = 0 \Rightarrow P_1 = 0$.
4. Calculate P_2 (positions 2,3,6,7): $P_2 \oplus 1 \oplus 1 \oplus 1 = 0 \Rightarrow P_2 = 1$.
5. Calculate P_4 (positions 4,5,6,7): $P_4 \oplus 0 \oplus 1 \oplus 1 = 0 \Rightarrow P_4 = 0$.

Encoded 7-bit Hamming code: 0110011

Flow Control & Elementary Data Link Protocols

Flow control prevents a fast sender from overwhelming a slow receiver.

- Unrestricted Simplex Protocol: Ideal protocol assuming infinite buffer space and error-free channel.
- Simplex Stop-and-Wait Protocol: Sender sends one frame and waits for receiver ACK before sending next.
- Efficiency Formula: Efficiency $\eta = \frac{1}{1+2a}$, where $a = \frac{T_p}{T_t}$.
- Propagation Delay (T_p): Time taken for a bit to travel from sender to receiver.
- Transmission Delay (T_t): Time taken to push frame bits onto medium ($\text{Length}/\text{Bandwidth}$).

Sliding Window Protocols

SLIDING WINDOW

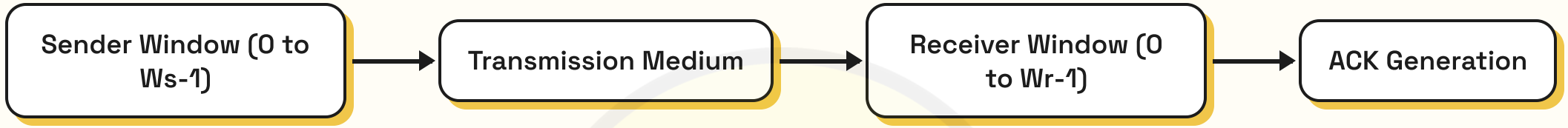
A flow control mechanism where both sender and receiver maintain a range of sequence numbers (window) allowing multiple unacknowledged frames in transit.

- Sender Window: Holds sequence numbers of frames sent but not yet acknowledged.
- Receiver Window: Holds sequence numbers of acceptable incoming frames.
- Increases link utilization significantly compared to Stop-and-Wait when bandwidth-delay product is high.
- Utilizes sequence numbers of size m bits, calculated modulo 2^m.

Go-Back-N ARQ vs Selective Repeat ARQ

Feature	Go-Back-N ARQ	Selective Repeat ARQ
Sender Window Size (W_s)	$2^m - 1$	2^{m-1}
Receiver Window Size (W_r)	1	2^{m-1}
Out-of-Order Frames	Discarded by receiver	Buffered by receiver
Re-transmission	Retransmits frame N and all subsequent frames	Retransmits only the specific corrupted frame
ACK Type	Cumulative ACK	Individual / Selective ACK
Complexity & Buffer	Low hardware complexity, minimal buffer	Higher complexity, memory buffers at receiver

Sliding Window Protocol Architecture

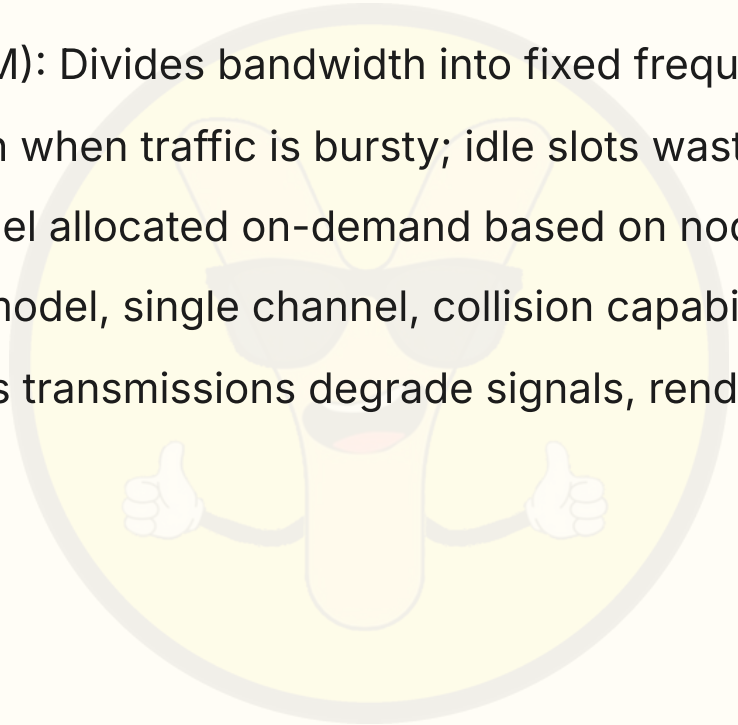


Continuous frame flow controlled by sliding window boundaries and ACKs.

Channel Allocation Problem

Determines how a single shared broadcast channel is allocated among multiple competing nodes.

- Static Channel Allocation (FDM/TDM): Divides bandwidth into fixed frequency or time slots.
- Inefficiency of Static: Low utilization when traffic is bursty; idle slots wasted.
- Dynamic Channel Allocation: Channel allocated on-demand based on node activity.
- Assumptions for Dynamic: Station model, single channel, collision capability, continuous/slotted time.
- Collision: Two or more simultaneous transmissions degrade signals, rendering data unreadable.



Random Access Protocols: ALOHA

Nodes transmit at will without prior coordination, handling collisions post-facto.

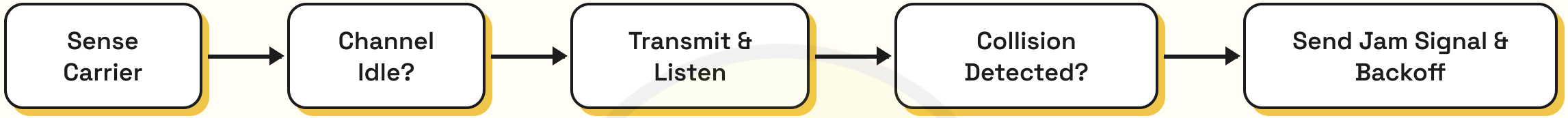
- Pure ALOHA: Nodes transmit immediately whenever data is ready.
- Vulnerable Time (Pure): $2 \times T_{frame}$.
- Pure ALOHA Throughput: $S = G \cdot e^{-2G}$; Maximum throughput = 18.4% at $G = 0.5$.
- Slotted ALOHA: Time is divided into discrete slots; nodes transmit only at slot boundaries.
- Vulnerable Time (Slotted): $1 \times T_{frame}$.
- Slotted ALOHA Throughput: $S = G \cdot e^{-G}$; Maximum throughput = 36.8% at $G = 1.0$.

CSMA Protocols (Carrier Sense Multiple Access)

Nodes listen to channel (carrier sensing) before transmitting to reduce collisions.

- 1-Persistent CSMA: If idle, transmit immediately with probability 1; if busy, sense continuously.
- Non-Persistent CSMA: If idle, transmit; if busy, wait a random time before sensing again.
- p-Persistent CSMA: Used in slotted channels; if idle, transmit with probability p, wait next slot with $1 - p$.
- CSMA/CD: CSMA with Collision Detection; aborts transmission immediately upon collision detection.
- CSMA/CA: CSMA with Collision Avoidance; uses RTS/CTS frames and random backoff (used in Wi-Fi).

CSMA/CD Operation Flowchart



Logic flow for Carrier Sense Multiple Access with Collision Detection.

Comparison of Multiple Access Protocols

Protocol Type	Collision Occurrence	Channel Utilization	Key Characteristic
Pure ALOHA	High	18.4% max	Transmit anytime without sensing
Slotted ALOHA	Moderate	36.8% max	Transmit only at slot boundaries
CSMA/CD	Low	Up to 80-90%	Carrier sense + Collision abort
Bit-Map Protocol	None	High at heavy load	Reservation phase prior to transmission
Token Ring (802.5)	None	High under heavy load	Token passing permission ring

IEEE 802 LAN Standards

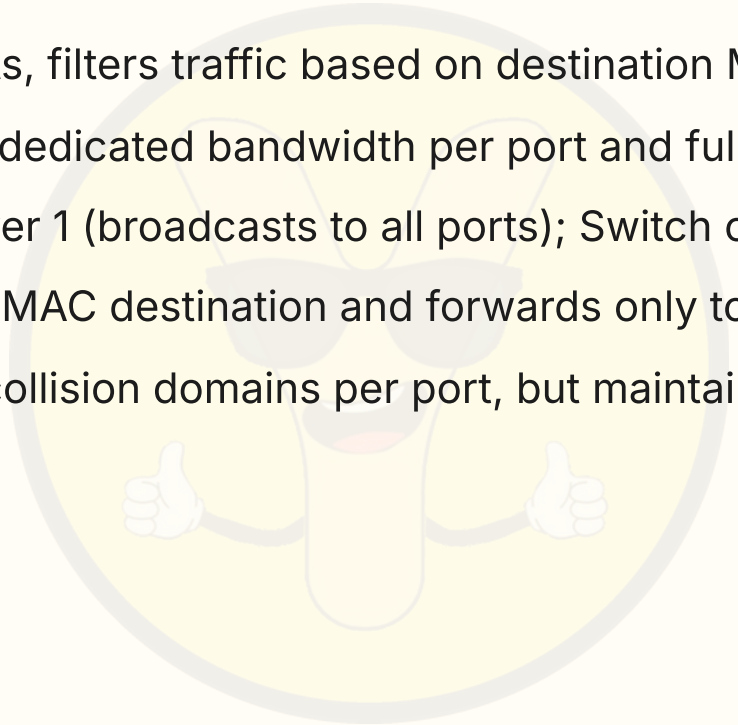
Standardized physical and data link layer specifications for local area networks.

- IEEE 802.3 (Ethernet): CSMA/CD based medium access over coaxial/UTP cabling.
- Ethernet Frame Format: Preamble (7B), SFD (1B), Dest MAC (6B), Src MAC (6B), Type (2B), Data (46-1500B), FCS (4B).
- Minimum Ethernet Frame Size: 64 bytes to ensure collision detection before frame transmission finishes.
- IEEE 802.11 (Wi-Fi): Wireless LAN standard using CSMA/CA and hidden/exposed terminal handling.
- IEEE 802.15 (Bluetooth): Wireless Personal Area Network (WPAN) standard.

Link Layer Switches & Bridges

Devices operating at Data Link Layer (Layer 2) to interconnect network segments.

- Bridge: Connects two LAN segments, filters traffic based on destination MAC address.
- Switch: Multi-port bridge providing dedicated bandwidth per port and full-duplex communication.
- Hub vs Switch: Hub operates at Layer 1 (broadcasts to all ports); Switch operates at Layer 2 (unicasts).
- Filtering and Forwarding: Examines MAC destination and forwards only to target port segment.
- Collision Domains: Switch isolates collision domains per port, but maintains single broadcast domain.

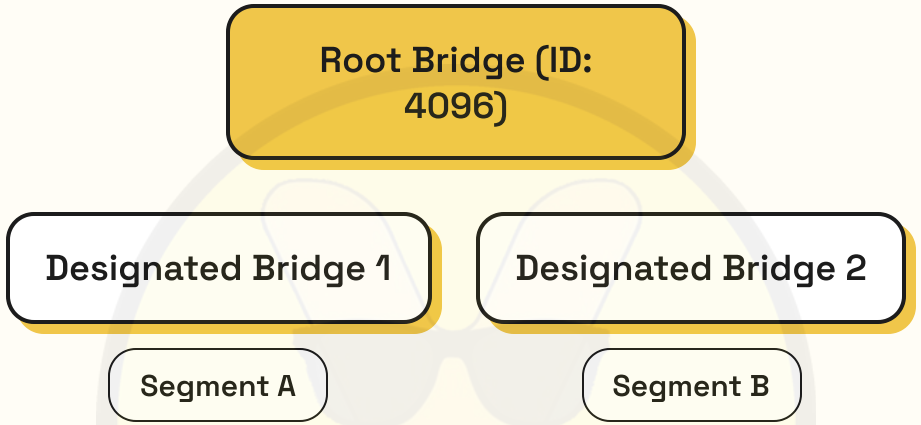


Backward Learning Algorithm (Transparent Bridge)

Enables bridges to dynamically build MAC address tables without manual configuration.

- Initial State: Bridge table is completely empty.
- Frame Arrival: Bridge receives a frame on Port X with Source MAC A and Destination MAC B.
- Learning Phase: Record mapping A → Port X with a timestamp in table.
- Forwarding Decision: Look up destination MAC B in bridge table.
- If B found on Port Y (Y != X): Forward frame to Port Y.
- If B found on Port X: Drop frame (filter). If B not found: Flood frame to all ports except X.

Spanning Tree Protocol (STP) Topology



Loop-free logical tree structure constructed by IEEE 802.1D Spanning Tree Algorithm.

Exam Corner - Likely AKTU Questions

Q1 Explain bit stuffing and byte stuffing with suitable examples. Why is bit stuffing preferred?

Q2 Differentiate between Go-Back-N ARQ and Selective Repeat ARQ protocols with neat diagrams.

Q3 Given data 100100 and generator 1101, calculate the transmitted CRC bit sequence.

Q4 Derive the maximum efficiency of Pure ALOHA and Slotted ALOHA protocols.

Q5 Explain the working of CSMA/CD protocol. Why is minimum frame size required in Ethernet?

Q6 How does a transparent bridge learn host locations using backward learning algorithm? Explain flooding, filtering, and forwarding.

Q7 Describe the Spanning Tree Algorithm (IEEE 802.1D) used to eliminate loops in switched network topologies.

Unit 2 done. You are exam-ready.

Revise the Exam corner once more, then open Unit 3 on theycotes.com. Every AKTU subject, unit by unit, free. Notes by Chirag Jain, Ycotes.

