ABHYASMITRA.IN
COMPREHENSIVE UNIVERSITY STUDY NOTES

NETWORK AND SECURITY

Unit II — Data Link Layer and Network Layer Protocols

Topics Covered in this Unit

Data Link Layer Services, Design Issues & Framing Techniques (Bit/Byte Stuffing)
Error Detection & Correction: Parity, Hamming Code (Math & Derivation) & CRC (Modulo-2 Division)
ARQ Flow Control Protocols: Stop-and-Wait, Go-Back-N, and Selective Repeat (Window Analysis)
Medium Access Control (MAC): ALOHA (Pure/Slotted), CSMA, CSMA/CD (Backoff) & CSMA/CA (RTS/CTS)
LAN & WAN Standards Overview: IEEE 802.3 Ethernet, IEEE 802.11 Wi-Fi, PPP & HDLC Frames
Network Layer Switching: Circuit Switching vs Message Switching vs Packet Switching (Datagram / VC)
IP Addressing & Subnetting: IPv4 Classes, Custom Subnetting Math, CIDR Prefix Notation & IPv6 Structure
Network Address Translation (NAT): Static, Dynamic & PAT (Port Address Translation) Mechanics
Network Layer Protocols: ARP (Address Resolution Protocol) & ICMP (Error Reporting / Ping / Traceroute)
Routing Concepts & Algorithms: Distance Vector (Bellman-Ford) & Link State (Dijkstra's Algorithm)
Internet Routing Protocols: RIP (Hop Count), OSPF (Cost & Areas) & BGP (Path Vector & AS Policies)
Security Integration: Logical Segmentation (VLANs), Controlled Access (NAT) & Secure Routing (RPKI)
High-Yield University Exam Question Bank with Model Answers & Unit Summary

Compiled in a structured, easy-to-understand, textbook style format
Specially curated for B.Tech / B.E. / BCA / MCA / B.Sc Computer Science & IT Students

COURSE SYLLABUS & MAPPING

[UNIT II SYLLABUS — PRESCRIBED UNIVERSITY CURRICULUM]

This section contains the official syllabus for Unit II. Verify with your university curriculum mapping.

Unit II Syllabus Breakdown:

Data Link Layer: Functions and services to Network Layer; framing techniques; error detection and correction (Parity, Hamming Code, CRC); ARQ strategies (Stop-and-Wait, Go-Back-N, Selective Repeat); flow control (Sliding Window); MAC protocols (ALOHA, CSMA/CD, CSMA/CA, Binary Exponential Backoff); overview of IEEE 802.3 and IEEE 802.11 standards; WAN protocols (PPP, HDLC). Network Layer: Functions and switching techniques (Circuit, Message, Packet Switching); IP addressing (IPv4, IPv6, subnetting, CIDR); Network Address Translation (NAT); Network layer protocols (ARP, ICMP); routing concepts (Static and Dynamic Routing, Distance Vector, Link State); routing protocols (RIP, OSPF, BGP – introductory level). Security Integration: Logical network segmentation, controlled access through subnetting/NAT, and secure routing fundamentals.

• Course Code: ____________________ • Semester / Year: ____________________

TABLE OF CONTENTS

2.1 Data Link Layer: Services & Framing Techniques

Definition: Data Link Layer (DLL)

The Data Link Layer (Layer 2 of the OSI Model) transforms a raw, error-prone physical transmission facility into a reliable, error-free communication link. It is responsible for node-to-node (hop-to-hop) frame transfer across a single physical link, providing framing, flow control, error control, and medium access control.

Services Provided to the Network Layer

The principal service of the Data Link Layer is to transfer network layer packets from the source host's network layer to the destination host's network layer across one or more physical links. The DLL offers three distinct types of services:

- **1. Unacknowledged Connectionless Service:** The source machine sends independent frames to the destination machine without the destination acknowledging them. No logical connection is established beforehand. If a frame is lost or damaged due to noise, no recovery is attempted at this layer. Best suited for low error-rate media (Ethernet LANs) and real-time voice/video traffic.
- **2. Acknowledged Connectionless Service:** No logical connection is established, but every transmitted frame is individually acknowledged by the receiver. If a frame is not acknowledged within a timeout interval, it is retransmitted. Highly useful over unreliable, noisy channels such as wireless 802.11 Wi-Fi.
- **3. Acknowledged Connection-Oriented Service:** A formal connection is established between source and destination before data transfer begins. Frames are numbered sequentially, and the layer guarantees that every frame transmitted is received exactly once, without loss, duplication, or reordering (3 phases: Setup, Data Transfer, Teardown).

Framing Techniques

To provide service to the network layer, the Data Link Layer must break the raw bitstream from the Physical layer into discrete units called Frames. Framing marks the beginning and end of each packet. Four standard framing techniques are used:

1. Character Count (Byte Count)

A field in the frame header specifies the total number of characters (bytes) in the frame, including the count field itself. When the destination sees the count, it knows how many bytes follow.

- **Fatal Limitation:** If the character count field itself is corrupted by transmission noise (e.g., a count of 5 flips to 7), the receiver loses frame synchronization completely and cannot locate the start of subsequent frames. Rarely used alone today.

2. Byte Stuffing (Character-Oriented Framing)

Each frame starts and ends with special delimiter bytes called Flag Bytes (often denoted as FLAG = 0x7E). To prevent user data containing the same pattern from accidentally terminating the frame early, Byte Stuffing (Character Stuffing) is employed:

- **Mechanism:** Whenever the sender's data link layer encounters an internal FLAG byte in the user payload, it inserts an Escape Byte (ESC = 0x1B) immediately before it. If an ESC byte appears in the payload, the sender inserts an extra ESC before it. The receiver strips the escape byte, restoring original data.

3. Bit Stuffing (Bit-Oriented Framing - HDLC / SDLC)

Bit stuffing operates at the raw bit level regardless of byte boundaries. Every frame begins and ends with the unique 8-bit flag pattern: 01111110 (six consecutive 1s enclosed by 0s).

- **Sender Rule:** Whenever the sender's data link layer detects FIVE consecutive '1' bits in the user data stream, it automatically inserts ('stuffs') a '0' bit immediately after the fifth '1' bit (producing 0111110...).
- **Receiver Rule:** Whenever the receiver sees five consecutive '1' bits followed by a '0' bit, it automatically deletes (unstuffs) the '0' bit. If it sees five '1' bits followed by a '1' and '0' (01111110), it recognizes the end-of-frame flag delimiter!

BIT STUFFING EXAMPLE

```
Original User Data:      0 1 1 0 1 1 1 1 1 1 0 1 0 1 1 1 1 1 1 1 0
                                 ^^^^^               ^^^^^
Stuffed Transmitted:     0 1 1 0 1 1 1 1 1[0]1 0 1 0 1 1 1 1 1[0]1 1 0
Receiver Unstuffs:       0 1 1 0 1 1 1 1 1 1 0 1 0 1 1 1 1 1 1 1 0 (Original Restored)
```

Figure: Bit stuffing prevents false end-of-frame detection by inserting a 0 after five consecutive 1s

4. Physical Layer Coding Violations

Used in media encoding schemes that contain redundant electrical signal states. In Manchester encoding, bit 1 is High-Low and bit 0 is Low-High. Signals that remain High-High or Low-Low are electrical violations of the code, and are utilized to cleanly delimit frame boundaries without bit stuffing overhead.

2.2 Error Detection and Correction

Transmission impairments (thermal noise, impulse noise, attenuation, crosstalk) introduce bit errors into transmitted data. Error control consists of Error Detection (discovering corrupted bits) and Error Correction (reconstructing the original uncorrupted bit sequence).

1. Parity Check (Simple & 2D Parity)

- **Simple Parity Check:** Appends a single redundant parity bit to each data word. In Even Parity, the bit is set so the total count of 1s in the frame is even; in Odd Parity, the count is made odd. Detects all single-bit errors and odd numbers of errors; completely fails to detect even numbers of flipped bits (e.g., 2-bit flips).
- **Two-Dimensional (2D) Parity:** Arranges data in a matrix (rows and columns). Parity bits are calculated for every row and every column. Can detect multiple bit errors and pinpoint/correct any single-bit error located at the intersection of the corrupted row and column.

2. Hamming Code (Forward Error Correction - FEC)

Developed by Richard Hamming, the Hamming Code is an error-correcting linear block code capable of detecting up to 2-bit errors or correcting single-bit errors without requiring retransmissions.

- **Mathematical Redundancy Condition:** To protect m message bits with r parity (redundant) bits, the total codeword length is n = m + r. The number of parity bits r must satisfy: 2^r >= m + r + 1.
- **Bit Positioning Rules:** Parity bits are placed strictly at bit positions that are powers of 2 (Positions 1, 2, 4, 8, 16, 32...). Message data bits occupy all remaining bit positions (3, 5, 6, 7, 9, 10, 11...).
- **Parity Check Bit Coverage:**
  - Parity Bit P1 (Position 1): Checks bits with a 1 in least significant bit of binary index (Bits 1, 3, 5, 7, 9, 11...).
  - Parity Bit P2 (Position 2): Checks bits with a 1 in 2nd position of binary index (Bits 2, 3, 6, 7, 10, 11...).
  - Parity Bit P4 (Position 4): Checks bits 4, 5, 6, 7, 12, 13, 14, 15...
  - Parity Bit P8 (Position 8): Checks bits 8, 9, 10, 11, 12, 13, 14, 15...
- **Syndrome Word Error Correction:** At the receiver, recalculating parity checks generates a Syndrome Word (C = c4 c2 c1). If Syndrome = 000, no error occurred. If Syndrome != 0, its decimal value gives the EXACT bit position of the inverted bit! Inverting that bit fixes the error.

3. Cyclic Redundancy Check (CRC)

Cyclic Redundancy Check (CRC) is the most powerful and widely implemented polynomial error detection algorithm, utilized in Ethernet (CRC-32), Wi-Fi, and optical links.

- **Modulo-2 Arithmetic:** CRC operates on binary numbers using modulo-2 arithmetic (equivalent to bitwise XOR addition and subtraction without carries or borrows). Example: 1 XOR 1 = 0, 1 XOR 0 = 1, 0 XOR 0 = 0.
- **Step-by-Step CRC Sender Algorithm:**
  - 1. Let data message be M(x) of k bits, and Generator Polynomial be G(x) of degree r (r+1 bits).

- 2. Append r zeros to the lower end of the message: M'(x) = M(x) * 2^r.
- 3. Divide M'(x) by G(x) using binary Modulo-2 division.
- 4. The remainder R(x) (of r bits) is the CRC Checksum (Frame Check Sequence - FCS).
- 5. Transmit the complete Codeword T(x) = M'(x) XOR R(x).

- **Receiver Verification:** The receiver divides the incoming codeword T(x) by the identical generator G(x). If the remainder is strictly ZERO (0), the frame is accepted as error-free; if the remainder is non-zero, an error occurred and the frame is rejected.

2.3 ARQ Strategies & Flow Control

Definition: Automatic Repeat Request (ARQ)
Automatic Repeat Request (ARQ) is an error-control strategy for data transmission that utilizes positive acknowledgments (ACK), negative acknowledgments (NAK), and timeout intervals to achieve reliable, in-order frame delivery over unreliable physical channels.

1. Stop-and-Wait ARQ

The sender transmits a single frame (with a 1-bit sequence number: 0 or 1) and stops, starting a Retransmission Timer. It waits until an acknowledgment (ACK) is received before sending the next frame. If the ACK is lost or the timer expires, the sender retransmits the frame.

- **Link Utilization / Efficiency Formula:** Efficiency (eta) = 1 / (1 + 2a), where a = Tprop / Ttrans (ratio of propagation delay to transmission delay).
- **Drawback:** Extremely inefficient on 'Long Fat Networks' (satellite and fiber links with high bandwidth-delay products) where the pipe remains empty while waiting for ACKs.

2. Go-Back-N (GBN) ARQ (Sliding Window)

Go-Back-N ARQ allows the sender to transmit up to N frames without waiting for an individual ACK, keeping the transmission channel continuously full.

- **Key Operating Rules:**
  - Sender Window Size (Ws): Ws = 2^k - 1 (where k is the number of sequence number bits). If k = 3 bits, Ws = 7.
  - Receiver Window Size (Wr): Strictly equal to 1. The receiver accepts frames in strict sequential order only.
  - Cumulative Acknowledgment: ACK n confirms that all frames up to n-1 have been successfully received.

– Error Recovery (Go-Back-N): If frame i is lost or damaged, the receiver discards all subsequent out-of-order frames (i+1, i+2...). When the sender's timer for frame i expires, the sender must GO BACK and retransmit ALL unacknowledged frames starting from i.

3. Selective Repeat (SR) ARQ

Selective Repeat improves upon GBN by avoiding redundant retransmissions. The receiver accepts and buffers out-of-order frames that arrive without errors.

- **Key Operating Rules:**
  - Sender & Receiver Window Sizes: Ws = Wr = 2^(k - 1). For k = 3 bits, Ws = Wr = 4. (Equal windows prevent sequence number overlap ambiguity).
  - Individual Acknowledgment & NAK: Receiver sends selective ACK for each individual frame and Negative ACK (NAK i) for corrupted frames.
  - Error Recovery: The sender retransmits ONLY the specific lost frame (frame i). Buffered out-of-order frames are retained and delivered to the network layer once frame i arrives.

Comparison Table: ARQ Strategies

Parameter	Stop-and-Wait ARQ	Go-Back-N (GBN) ARQ	Selective Repeat (SR) ARQ
Sender Window (Ws)	1	2^k - 1 (e.g., 7 for 3-bit)	2^(k-1) (e.g., 4 for 3-bit)
Receiver Window (Wr)	1	1 (No out-of-order buffer)	2^(k-1) (Buffers out-of-order)
Acknowledgment Type	Individual (ACK 0 / ACK 1)	Cumulative ACK	Individual / Selective ACK
Retransmission Scope	Single lost frame	Entire window from lost frame	Only the specific lost frame
Channel Efficiency	Lowest (1 / (1 + 2a))	Moderate	Highest (Approaches 100%)
Implementation Complexity	Very Simple	Moderate	High (Complex buffering & logic)

2.4 Medium Access Control (MAC) Protocols

Definition: Medium Access Control (MAC)
Medium Access Control (MAC) protocols are sublayer algorithms governing how multiple communicating nodes share, coordinate, and transmit over a single broadcast communication channel without destructive collision interference.

1. ALOHA Protocols (Pure ALOHA vs Slotted ALOHA)

- **Pure ALOHA (Norman Abramson, 1970):** Stations transmit frames whenever they have data ready. If two transmissions overlap even by 1 bit, a collision occurs and frames are destroyed. Vulnerable Time = 2 * Tframe. Maximum Channel Throughput S_max = 1 / (2e) approx 18.4% at traffic load G = 0.5.
- **Slotted ALOHA (Roberts, 1972):** Time is discretized into discrete time slots equal to frame transmission time (Tframe). Stations are permitted to transmit ONLY at the beginning of a time slot. Vulnerable Time is halved to Tframe. Maximum Channel Throughput S_max = 1 / e approx 36.8% at traffic load G = 1.0 (doubles Pure ALOHA efficiency!).

2. CSMA (Carrier Sense Multiple Access)

CSMA improves efficiency based on the principle of 'Listen Before Talk'. Stations sense the shared channel carrier before attempting to transmit:

- **1-Persistent CSMA:** Senses channel. If busy, continuously listens until channel is idle, then immediately transmits with probability 1. High collision rate if multiple stations are waiting simultaneously.
- **Non-Persistent CSMA:** Senses channel. If busy, waits for a random backoff interval before sensing again. Reduces collisions but introduces idle channel delay.
- **p-Persistent CSMA:** Used in slotted channels. Senses channel. If idle, transmits with probability p, and defers to next slot with probability (1 - p).

3. CSMA/CD (Collision Detection - IEEE 802.3 Ethernet)

CSMA/CD ('Listen While Talk') senses the medium while transmitting. If an electrical collision occurs, transmission is aborted immediately, a 32-bit Jamming Signal is broadcast to notify all nodes, and the station waits for a random backoff period.

- **Minimum Frame Size Condition (Crucial Exam Concept):** To guarantee that a transmitting station detects a collision before completing its transmission, the Frame Transmission Time (Ttrans) must be at least twice the Maximum Propagation Delay (Tprop): Ttrans >= 2 * Tprop, which means Minimum Frame Length L_min = 2 * Tprop * Bandwidth (For standard 10 Mbps Ethernet over 2.5 km, L_min = 64 bytes / 512 bits).

- **Binary Exponential Backoff Algorithm:** After collision attempt n (where n = 1 to 16): Backoff multiplier k = min(n, 10). The station picks a random integer R uniformly from range [0, 2^k - 1] and waits R * Slot Time (512 bit times). If n reaches 16, the transmission is aborted with an error.

4. CSMA/CA (Collision Avoidance - IEEE 802.11 Wi-Fi)

Wireless transceivers cannot detect collisions while transmitting because their own outbound radio transmission overwhelms incoming signals (CSMA/CD is impossible). Hence, Wi-Fi uses Collision Avoidance (CSMA/CA):

- **Mechanisms:**
  - Interframe Space (IFS): Stations wait for a quiet period before transmitting (SIFS for high-priority ACKs, DIFS for standard data frames).
  - RTS / CTS Handshake: Solves the Hidden Terminal Problem. Sender transmits a short Request-to-Send (RTS) frame. The Access Point responds with a Clear-to-Send (CTS) broadcast, reserving the wireless medium (Network Allocation Vector - NAV) for the sender.

2.5 LAN and WAN Protocols: 802.3, 802.11, PPP, HDLC

1. IEEE 802.3 Ethernet Frame Structure

IEEE 802.3 ETHERNET FRAME FORMAT

```
+----------+-----+------------+------------+------+--------------+-----+
| Preamble | SFD | Dest MAC   | Source MAC | Type | Payload Data | FCS |
| (7 Bytes)| (1B)| (6 Bytes)  | (6 Bytes)  | (2B) | (46-1500 B)  | (4B)|
+----------+-----+------------+------------+------+--------------+-----+
  10101010  10101011 [48-bit Hex] [48-bit Hex]  IPv4/ARP (IP Packet)   CRC-32
```

Figure: Standard Ethernet Frame (Total Min Size: 64 Bytes, Max MTU: 1518 Bytes)

2. WAN Protocols: HDLC and PPP

- **HDLC (High-Level Data Link Control):** ISO standard bit-oriented protocol using bit stuffing (01111110 flags). Supports three frame types: (1) Information Frames (I-frames) for user data, (2) Supervisory Frames (S-frames) for flow/error control (RR, RNR, REJ), and (3) Unnumbered Frames (U-frames) for link management (SABM, DISC).
- **PPP (Point-to-Point Protocol):** The universal byte-oriented protocol for direct point-to-point links (broadband DSL, dial-up, serial lines). Comprises: (1) LCP (Link Control Protocol) for link establishment and authentication (PAP, CHAP), and (2) NCP (Network Control Protocol) for negotiating network-layer protocols (IPCP for IPv4).

2.6 Network Layer: Switching Techniques

Definition: Switching

Switching is the process of forwarding data packets arriving on an incoming transmission link to a specific outgoing transmission link that leads toward the destination across intermediate network nodes.

Comparison of the Three Switching Techniques

- **1. Circuit Switching:** A dedicated physical transmission path is established between sender and receiver before communication begins. Operates in 3 phases: (a) Circuit Setup, (b) Data Transmission, (c) Circuit Teardown. Constant data rate, guaranteed bandwidth, zero queuing delay. Inefficient for bursty traffic because channel capacity remains reserved even when idle (Traditional PSTN telephone network).
- **2. Message Switching (Store-and-Forward):** The entire message is treated as a single block and forwarded hop-by-hop through intermediate switches. Each switch buffers the complete message on disk before forwarding. Incurs massive storage overhead and variable propagation delay; obsolete in modern real-time networks.
- **3. Packet Switching:** Data is broken down into small, standardized chunks called Packets (typically 1500 bytes). Packets travel independently through the network. Two distinct approaches:
  - • **Datagram Packet Switching (Connectionless):** Each packet is treated independently with its own destination IP. Packets may take different paths and arrive out of order. No setup delay. (The Internet model).
  - • **Virtual Circuit Packet Switching (Connection-Oriented):** A predetermined logical route is established before transmission. All packets carry a small Virtual Circuit Identifier (VCI) and follow the identical path in sequential order (e.g., ATM, Frame Relay, MPLS).

Comparison Parameter	Circuit Switching	Message Switching	Packet Switching (Datagram)
Dedicated Path	Yes (Physical connection)	No (Dynamic hop-by-hop)	No (Independent routing)
Store-and-Forward	No (Real-time transmission)	Yes (Full message buffered)	Yes (Individual small packets)
Setup Delay	High (Connection setup phase)	None	None
Bandwidth Utilization	Low (Wasted during idle periods)	High	Maximum (Statistical multiplexing)

Comparison Parameter	Circuit Switching	Message Switching	Packet Switching (Datagram)
Best Application	Analog voice telephony	Telegraph, historical email	Internet, web browsing, cloud

2.7 IP Addressing, Subnetting & CIDR

1. IPv4 Addressing & Classful Architecture

An IPv4 address is a 32-bit binary number uniquely identifying a host's network connection. It is represented in Dotted-Decimal notation (e.g., 192.168.10.1), dividing 32 bits into 4 octets of 8 bits each.

Class	Leading Bits	Network ID / Host ID Bits	First Octet Range	Default Subnet Mask	Number of Valid Hosts / Network
Class A	0	8 Net bits / 24 Host bits	1 to 126 (0 & 127 reserved)	255.0.0.0 (/8)	2^24 - 2 = 16,777,214
Class B	10	16 Net bits / 16 Host bits	128 to 191	255.255.0.0 (/16)	2^16 - 2 = 65,534
Class C	110	24 Net bits / 8 Host bits	192 to 223	255.255.255.0 (/24)	2^8 - 2 = 254
Class D	1110	Multicast Group ID (28 bits)	224 to 239	N/A (Multicasting)	N/A
Class E	1111	Experimental / Reserved	240 to 255	N/A (Research)	N/A

2. Subnetting & Mathematical Calculation

Subnetting is the practice of dividing a single large network into two or more smaller logical sub-networks (subnets) by borrowing host bits to create subnet bits.

- **Subnetting Formulas:**
  - Number of Subnets created = 2^s (where s is the number of borrowed bits).
  - Number of Usable Hosts per Subnet = 2^h - 2 (where h is the remaining host bits; 2 addresses are subtracted for Network ID and Broadcast ID).
  - Subnet Block Size (Increment) = 256 - Value of the interesting octet in the subnet mask.

- **Classless Inter-Domain Routing (CIDR):** Replaces classful addressing with Slash Notation (/n), where n represents the exact prefix length of network bits (e.g., 192.168.1.0/26 has 26 network bits and 6 host bits, yielding 4 subnets with 62 usable hosts each).

3. IPv6 Addressing

IPv6 expands the address space to 128 bits (producing 3.4 x 10^38 unique addresses), written as 8 groups of 4 hexadecimal digits separated by colons (e.g., 2001:0db8:85a3:0000:0000:8a2e:0370:7334).

- **Zero Compression Rules:** Leading zeros in a group can be omitted (e.g., 0db8 -> db8). One contiguous block of consecutive all-zero groups can be replaced with double colons '::' once per address (e.g., 2001:db8:85a3::8a2e:370:7334).
- **Advantages over IPv4:** Virtually limitless address pool; no broadcast storms (replaced by Anycast & Multicast); built-in mandatory IPsec cryptographic security; simplified 40-byte fixed header for faster router processing; eliminates need for NAT.

2.8 NAT, ARP, and ICMP Protocols

1. Network Address Translation (NAT)

NAT (RFC 1631) conserves public IPv4 addresses by allowing an entire private LAN (using private RFC 1918 ranges: 10.0.0.0/8, 172.16.0.0/12, 192.168.0.0/16) to access the Internet through a single registered public IP address.

- **Types of NAT:**
  - Static NAT: Maps 1 private IP to 1 dedicated public IP (used for hosting internal web servers).
  - Dynamic NAT: Maps an internal private IP to a public IP chosen dynamically from an ISP address pool.
  - Port Address Translation (PAT / NAT Overload): Maps thousands of internal private IP addresses to a SINGLE public IP by appending unique Layer 4 TCP/UDP Port Numbers (e.g., 192.168.1.5:4500 -> 203.0.113.1:50001). Standard in all home routers.

2. Address Resolution Protocol (ARP)

ARP dynamically resolves a known 32-bit Logical IP Address into its corresponding 48-bit Physical MAC Address on a local network segment.

- **Working Mechanism:**
  - 1. ARP Request: Host A broadcasts an Ethernet frame (Dest MAC: FF:FF:FF:FF:FF:FF) asking 'Who has IP 192.168.1.10? Tell 192.168.1.5'.

- 2. ARP Reply: Host B (matching the IP) replies with a direct Unicast frame stating '192.168.1.10 is at MAC 00:1A:2B:3C:4D:5E'.
- 3. ARP Cache: Host A caches the IP-MAC mapping in its RAM table to avoid repeating broadcasts.

3. Internet Control Message Protocol (ICMP)

ICMP is a companion network layer protocol used by routers and hosts for diagnostic queries and error reporting. ICMP packets are encapsulated directly within IP datagrams.

- **Key ICMP Message Types:**
  - Echo Request (Type 8) & Echo Reply (Type 0): Used by the `ping` utility to test end-to-end host reachability and round-trip time.
  - Destination Unreachable (Type 3): Generated when a router cannot route a packet (network down, host unreachable, port closed).
  - Time Exceeded (Type 11): Generated when a packet's TTL (Time-to-Live) field reaches zero. Utilized by the `traceroute` utility to map hop-by-hop internet paths!

2.9 Routing Concepts & Protocols (RIP, OSPF, BGP)

1. Distance Vector Routing (Bellman-Ford Algorithm)

In Distance Vector routing, each router maintains a vector (table) of minimum distances to all network destinations. Routers periodically transmit their entire routing table to their directly connected immediate neighbors.

- **Mathematical Update Equation:** Distance to Destination D via neighbor v is: D(x, y) = min_v { c(x, v) + D(v, y) }.
- **Count-to-Infinity Problem:** Good news (link restoration) propagates rapidly, but bad news (link failure) propagates slowly through neighbor gossip, causing routing loops where metric values increment toward infinity. Solved using Split Horizon (never advertise a route back out of the interface it was learned from) and Poison Reverse (advertise dead links with infinite metric 16).

2. Link State Routing (Dijkstra's Shortest Path Algorithm)

In Link State routing, every router discovers its direct neighbors, measures link costs, constructs a Link State Advertisement (LSA) packet, and floods the LSA to ALL routers in the entire network. Every router builds an identical Link State Database (LSDB) map and independently runs Dijkstra's algorithm to compute the Shortest Path Tree (SPT).

3. Overview of Internet Routing Protocols

Routing Protocol	Algorithm Family	Metric Used	Routing Domain (IGP / EGP)	Convergence Speed & Max Limit
RIP (Routing Information Protocol)	Distance Vector	Hop Count (Max 15 hops; 16 = Infinity)	Interior Gateway Protocol (Small LANs)	Slow; periodic 30-second full table broadcast
OSPF (Open Shortest Path First)	Link State (Dijkstra)	Cost = 10^8 / Bandwidth (bps)	Interior Gateway Protocol (Large Enterprise)	Fast; event-triggered LSAs; hierarchical Areas
BGP (Border Gateway Protocol)	Path Vector	AS-Path, Local Pref, Multi-Exit Discriminator	Exterior Gateway Protocol (Global Internet)	Policy-based; inter-connects Autonomous Systems

2.10 Security Integration in Layers 2 & 3

- **1. Logical Network Segmentation (VLANs - IEEE 802.1Q):** Partitions a physical switch into isolated logical broadcast domains. Prevents unauthorized lateral movement and confines ARP broadcast storms. Inter-VLAN traffic must pass through a firewall router.
- **2. Controlled Access through Subnetting & NAT:** Private IP addressing hides internal host topology from the public Internet. Firewall access control lists (ACLs) filter packets based on source/dest IP subnets and TCP ports at boundary routers.
- **3. Secure Routing Fundamentals:** Protects routing infrastructure against route spoofing and BGP hijacking: (a) Cryptographic route authentication (MD5/SHA-256 neighbor peering in OSPF/BGP), (b) BGP Route Filtering, and (c) Resource Public Key Infrastructure (RPKI) validating Route Origin Authorizations (ROA).

2.11 High-Yield University Exam Question Bank

Part A: Short Answer Questions (2 to 5 Marks)

Q1. Explain bit stuffing with an example. [3 Marks]

- **Answer:** In HDLC framing, whenever the sender detects five consecutive 1s in user data, it inserts a 0 bit immediately after. The receiver deletes any 0 appearing after five 1s. This prevents user payload from mimicking the 01111110 flag.

Q2. Why is the minimum frame size in Ethernet 64 bytes? [3 Marks]

- **Answer:** For CSMA/CD to detect collisions reliably before transmission ends, Ttrans >= 2 * Tprop. For standard 10 Mbps Ethernet over a 2.5 km collision domain, minimum frame size is L = 2 * (25.6 microsec) * 10 Mbps = 512 bits = 64 bytes.

Q3. Differentiate between IPv4 and IPv6. [4 Marks]

- **Answer:** IPv4 has 32-bit addresses (dotted decimal, ~4.3 billion pool), uses broadcast/ARP, variable header (20-60B), requires NAT. IPv6 has 128-bit addresses (hexadecimal colon notation, virtually infinite pool), uses multicast/anycast, fixed 40B header, built-in IPsec, no NAT required.

Q4. Explain the Count-to-Infinity problem and its solutions. [4 Marks]

- **Answer:** In Distance Vector routing, when a link fails, neighbors continue updating each other with slowly incrementing hop counts until reaching infinity (16 in RIP). Solved via Split Horizon (do not advertise route back to source) and Poison Reverse (advertise failed link with infinity metric).

Part B: Long Answer Questions (10 to 15 Marks Outline Guides)

- **Q5. Explain Sliding Window Flow Control protocols (Stop-and-Wait, Go-Back-N, Selective Repeat) with window diagrams and efficiency formulas. [15 Marks]**
- **Q6. Explain Cyclic Redundancy Check (CRC). Given data M = 1101011011 and generator polynomial G(x) = x^4 + x + 1, calculate the transmitted codeword and verify receiver operation. [10 Marks]**
- **Q7. Discuss IP addressing, classful architecture, and solve a numerical on subnetting a /24 network into 4 subnets with valid host ranges. [10 Marks]**
- **Q8. Compare Distance Vector (RIP) vs Link State (OSPF) vs Path Vector (BGP) routing algorithms. [12 Marks]**

2.12 Unit Summary & Key Takeaways

- Data Link Layer provides framing (bit/byte stuffing), error control (CRC, Hamming code), flow control (ARQ), and MAC.
- Hamming code corrects 1-bit errors via 2^r >= m + r + 1; CRC detects burst errors using modulo-2 polynomial division.
- ARQ Protocols: Stop-and-Wait (Ws=1, Wr=1), Go-Back-N (Ws=2^k-1, Wr=1, cumulative ACK), Selective Repeat (Ws=Wr=2^(k-1), selective ACK).

- MAC protocols include Pure ALOHA (18.4%), Slotted ALOHA (36.8%), CSMA/CD (Ethernet: min 64B frame, backoff), and CSMA/CA (Wi-Fi: RTS/CTS, NAV).
- Network layer provides packet switching (Datagram vs Virtual Circuit), IP addressing (IPv4/IPv6), subnetting, and NAT.
- Routing algorithms: Distance Vector (Bellman-Ford / RIP) vs Link State (Dijkstra / OSPF) vs Path Vector (BGP).
- Security integration leverages VLAN segmentation, NAT boundary isolation, and RPKI/BGP cryptographic route authentication.