Computer Network

Data-Link Layer

Lecture : 7

Gaurav Raj

TCP/IP

TCP/IP Layer	Hardware	Software/Protocols
Application	None	HTTP, FTP, SMTP, POP3, IMAP, DNS, SSH
Transport	None	TCP, UDP
Internet	Routers	IP (IPv4/v6), ICMP, IGMP, ARP, RARP Routing(DVR(RIP), LSR(OSPF), BGP)
Data Link	Switches, Bridges, NICs	Ethernet (MAC framing), Wi-Fi (802.11 MAC), PPP, Frame Relay, HDLC
Physical	Cables (fiber, coaxial, twisted pair), Hubs, Repeaters, Connectors (RJ-45), Amplifier	ONLY physical standards (IEEE 802.3 for wiring, IEEE 802.11 PHY for Wi-Fi)

Data-Link Layer

Responsibility
Framing
Error Detection
Error Recovery
Flow Control
Access Control
Addressing
Link Management
Framing and Encapsulation

Number Systems

Number Systems

Data Link Layer: Error Control

Parity, Checksum, CRC, Hamming Distance

Data Link Layer: Error Control

Checksum : Error Control

1. **Purpose:**

To detect accidental errors in transmitted messages.

2. Working Principle:

1. Divide the message into **k-bit blocks** (commonly 8, 16, or 32 bits).

2. Add all k-bit blocks using **1's complement arithmetic**.

3. If there's a **carry/overflow**, wrap it around and add it to the result.

4. Take 1's complement of the final sum — this is the **checksum**.

5. Transmit the message along with this checksum.

6. The receiver **repeats the same process** (including the checksum):
   1. If the final sum (including checksum) is **all 1s** → No error.
   2. If **not all 1s** → Error detected.

Checksum : Error Control

Suppose three 16-bit words are transmitted:

Word 1	**1100110011001100**
Word 2	1111000011110000
Word 3	0000111100001111

Checksum : Error Control

Three 8-bit words are to be sent: 01100110, 01010101, 10001111. Compute the 8-bit checksum.

Cyclic Redundancy Check : Error Control

What is CRC?

CRC (Cyclic Redundancy Check) is an **error-detecting code** used to detect **accidental** changes to raw data in digital networks and storage devices.

Where is CRC used?

- Data Link Layer (e.g., Ethernet, PPP)
- Storage (e.g., hard disks, CDs)
- Checksums in file downloads

Cyclic Redundancy Check : Error Control

Term	Meaning
Data/Message	Binary string to be transmitted
Generator (G)	A predetermined binary number (like a polynomial)
Divisor	Same as generator
CRC or Remainder	The extra bits added to message for error detection
Transmitted Frame	Message + CRC

Cyclic Redundancy Check : Error Control

Conceptual Steps in CRC

1. **Append (n−1) Zeros** to the data, where n = length of the generator.

2. **Divide** the new data by the generator using **modulo-2 division** (XOR instead of subtraction).

3. The **remainder** becomes the **CRC**.

4. The sender **appends** this CRC to the original data.

5. The receiver **divides** the received data (message + CRC) by the same generator.

    1. If remainder = 0 ⇒ **No Error**
    2. Else ⇒ **Error Detected**

Cyclic Redundancy Check : Error Control

Message (M): 101100
Generator (G): 1101 (Polynomial of degree 3 ⇒ append 3 zeros)

Cyclic Redundancy Check : Error Control

Can Two Different Messages Have the Same CRC?

Cyclic Redundancy Check : Error Control

It means the CRC **failed to detect the error**.

This is **rare but possible**.

No error detection scheme is perfect.

CRCs are **not cryptographic hashes**. They're **fast error-checking tools**, not meant for security or uniqueness.

Gate Qn: Consider the cyclic redundancy check (CRC) based error detecting scheme having the generator polynomial X3+X+1.

Suppose the message m4m3m2m1m0=11000 is to be transmitted. Check bits c2c1c0 are appended at the end of the message by the transmitter using the above CRC scheme. The transmitted bit string is denoted by m4m3m2m1m0c2c1c0. The value of the check-bit sequence c2c1c0 is

Data Link Layer: Error Control

Data Link Layer: Error Control

Thank You