Data Link Layer

PANA ACADEMY

Services of Data Link Layer

1.Framing and Link Access

2. Flow Control

3. Error detection

4. Error correction

Framing

The Data Link Layer divides the stream of bits received from the Physical Layer into manageable data units called frames. These frames include a header and a trailer, which contain control information for error detection, flow control, and addressing.

Frame Header: It contains the source and the destination addresses of the frame and the control bytes.

Payload field: It contains the message to be delivered.

Trailer: It contains the error detection and error correction bits. It is also called a Frame Check Sequence (FCS).

Flag: Two flag at the two ends mark the beginning and the end of the frame.

Description of parameters inside the frame

Flag: It is of 1 byte that with bit pattern 01111110.

Address: 1 byte which is set to 11111111 in case of the broadcast.

Control: 1 byte set to a constant value of 11000000.

Protocol: 1 or 2 bytes that define the type of data contained in the payload field.

Payload: This carries the data from the network layer. The maximum length of the payload field is 1500 bytes.

FCS: It is a 2 byte or 4 bytes frame check sequence for error detection. The standard code used is CRC (cyclic redundancy code).

Data Link Layer Protocols

Point – to – Point Protocol

Point – to – Point Protocol (PPP) is a communication protocol of the data link layer that is used to transmit multiprotocol data between two directly connected (point-to-point) computers.

PPP is a byte-oriented protocol.

High-level Data Link Control

HDLC is a bit-oriented protocol,

- PPP: PPP is primarily used for establishing a direct connection between two nodes over serial links. It's commonly used for dial-up connections, DSL, and other point-to-point connections.
- HDLC: HDLC is a bit-oriented synchronous data link layer protocol used for communication over both point-to-point and multipoint links. It's often used in wide area networks (WANs) and is the basis for several other data link layer protocols, including SDLC (Synchronous Data Link Control).

Error detection and correction

In case of transmission of data from one node to another node, it is not guaranteed whether the data received by the device is identical to the data transmitted by another device.

Error: **is a situation when the message received at the receiver end is not identical to the message transmitted from the sender.**

Errors can be classified into two categories:

1.Single-Bit Error

2. Burst Error

Single Bit Error

single bit error

The only one bit of a given data unit is changed from 1 to 0 or from 0 to 1.

00001010 ------------------> 00000010

Single-Bit Error mainly occurs in Parallel Data Transmission. For example, if eight wires are used to send the eight bits of a byte, if one of the wire is noisy, then single-bit is corrupted per byte.

Burst Error

The two or more bits are changed from 0 to 1 or from 1 to 0 is known as Burst Error.

Burst Errors are most likely to occur in Serial Data Transmission.

Error Detection Techniques

Single parity check

Checksum (uses one's complement arithmetic)

Cyclic redundancy check (uses modulo-2 division/ XOR division)

Single Bit Parity Checking

single parity checking

In this technique, a redundant bit is also known as a parity bit which is added at the end of the data unit so that the number of 1s becomes even.

Therefore, the total number of transmitted bits would be 9 bits.

If the number of 1s bits is odd, then parity bit 1 is appended and if the number of 1s bits is even, then parity bit 0 is appended at the end of the data unit.

At the receiving end, the parity bit is calculated from the received data bits and compared with the received parity bit.

This technique generates the total number of 1s even, so it is known as even-parity checking.

Limitations

If two bits are interchanged, then it cannot detect the errors.

CRC (Cyclic Redundancy Check)

cyclic redundancy check

A CRC generator uses a modulo-2 division. (Modulo-2 division, also known as polynomial division over a binary field or XOR division)

Firstly, L -1 zeroes are appended at the end of the data as the length of the divisor is L and we know that the length of the string 0s to be appended is always one less than the length of the divisor where L is the length of the divisor.

The remainder generated from the binary division is known as CRC remainder.

CRC remainder replaces the appended string of 0s at the end of the data unit, and the final string will be sent across the network.

CRC checker

The functionality of the CRC checker is similar to the CRC generator.

When the string of bits is received at the receiving end, then CRC checker performs the modulo-2 division.

A string is divided by the same divisor..

In this case when CRC checker generates the remainder of zero , the data is accepted otherwise rejected,

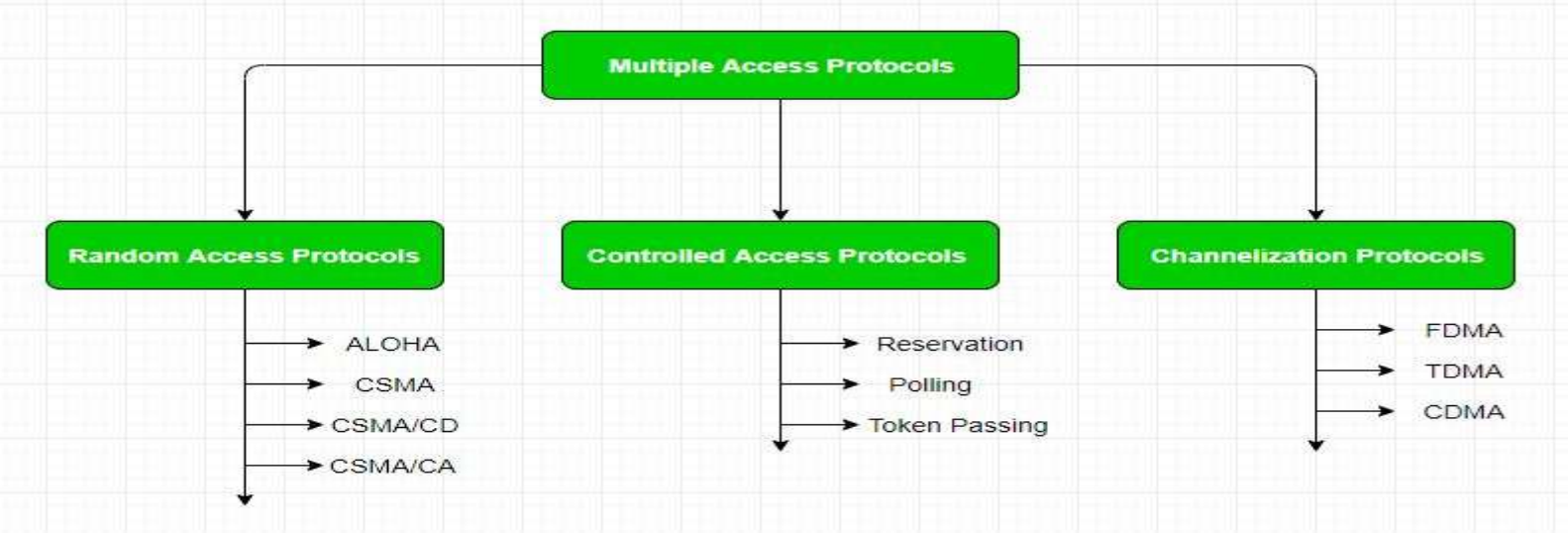
Error Correction

Difference between two methods

Automatic Repeat reQuest (ARQ)	Forward Error Correction (FEC)
ARQ is a method where the receiver detects errors in received frames and requests the sender to retransmit those frames.	FEC is a technique where the sender adds redundant information (error-correcting codes) to the data before transmission.
It operates based on acknowledgments (ACKs) and negative acknowledgments (NAKs) sent by the receiver to the sender.	This redundant information allows the receiver to detect and correct errors without the need for retransmission requests.

Multiple Access Protocol

If there is a dedicated link between the sender and the receiver then data link control layer is sufficient, however if there is no dedicated link present then multiple stations can access the channel simultaneously. Hence multiple access protocols are required to decrease collision and avoid crosstalk.



ALOHA vs Slotted ALOHA

Pure Aloha	Slotted Aloha
In this Aloha, any station can transmit the data at any time.	In this, any station can transmit the data at the beginning of any time slot.
In this, The time is continuous and not globally synchronized.	In this, The time is discrete and globally synchronized.
Vulnerable time for Pure Aloha = 2 × Tt	Vulnerable time for Slotted Aloha = Tt
In Pure Aloha, the Probability of successful transmission of the data packet $= G \times e^{-2G}$	In Slotted Aloha, the Probability of successful transmission of the data packet $= G \times e^{-G}$
In Pure Aloha, Maximum efficiency = 18.4%	In Slotted Aloha, Maximum efficiency = 36.8%
Pure Aloha doesn't reduce the number of collisions to half.	Slotted Aloha reduces the number of collisions to half and doubles the efficiency of Pure Aloha.

CSMA

CSMA – Carrier Sense Multiple Access ensures fewer collisions as the station is required to first sense the medium (for idle or busy) before transmitting data. If it is idle then it sends data, otherwise it waits till the channel becomes idle. However there is still chance of collision in CSMA due to propagation delay. For example, if station A wants to send data, it will first sense the medium.If it finds the channel idle, it will start sending data. However, by the time the first bit of data is transmitted (delayed due to propagation delay) from station A, if station B requests to send data and senses the medium it will also find it idle and will also send data. This will result in collision of data from station A and B.

CSMA

CSMA access modes-

- **1-persistent:** The node senses the channel, if idle it sends the data, otherwise it continuously keeps on checking the medium for being idle and transmits unconditionally(with 1 probability) as soon as the channel gets idle.
- **Non-Persistent:** The node senses the channel, if idle it sends the data, otherwise it checks the medium after a random amount of time (not continuously) and transmits when found idle.
- **P-persistent:** The node senses the medium, if idle it sends the data with p probability. If the data is not transmitted ((1-p) probability) then it waits for some time and checks the medium again, now if it is found idle then it send with p probability. This repeat continues until the frame is sent. It is used in Wifi and packet radio systems.
- **O-persistent:** Superiority of nodes is decided beforehand and transmission occurs in that order. If the medium is idle, node waits for its time slot to send data.

Channelization

Channelization:
In this, the available bandwidth of the link is shared in time, frequency and code to multiple stations to access channel simultaneously.

- **Frequency Division Multiple Access (FDMA) –** The available bandwidth is divided into equal bands so that each station can be allocated its own band. Guard bands are also added so that no two bands overlap to avoid crosstalk and noise.
- **Time Division Multiple Access (TDMA) –** In this, the bandwidth is shared between multiple stations. To avoid collision time is divided into slots and stations are allotted these slots to transmit data. However there is a overhead of synchronization as each station needs to know its time slot. This is resolved by adding synchronization bits to each slot. Another issue with TDMA is propagation delay which is resolved by addition of guard bands.
  For more details refer – Circuit Switching
- **Code Division Multiple Access (CDMA) –** One channel carries all transmissions simultaneously. There is neither division of bandwidth nor division of time. For example, if there are many people in a room all speaking at the same time, then also perfect reception of data is possible if only two person speak the same language. Similarly, data from different stations can be transmitted simultaneously in different code languages.

PPP protocol

Data Link Layer Protocol

Transmit **multiprotocol** data between two directly connected (point-to-point) computers.

Point-to-Point Protocol (PPP) is used in various networking scenarios, primarily for establishing direct connections between two network nodes over serial links.

byte - oriented protocol

Point - to - Point Protocol is a layered protocol having three components –

Encapsulation Component – It encapsulates the datagram so that it can be transmitted over the specified physical layer.

Link Control Protocol (LCP) – It is responsible for establishing, configuring, testing, maintaining and terminating links for transmission. It also imparts negotiation for set up of options and use of features by the two endpoints of the links.

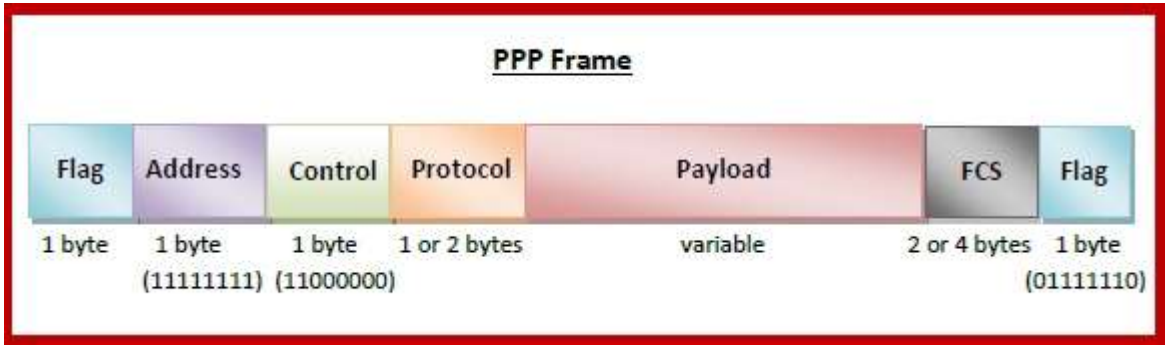
Authentication Protocols (AP) – These protocols authenticate endpoints for use of services. The two authentication protocols of PPP are –

- Password Authentication Protocol (PAP)
- Challenge Handshake Authentication Protocol (CHAP)

Network Control Protocols (NCPs) – These protocols are used for negotiating the parameters and facilities for the network layer. For every higher-layer protocol supported by PPP, one NCP is there. Some of the NCPs of PPP are –

- Internet Protocol Control Protocol (IPCP)
- OSI Network Layer Control Protocol (OSINLCP)
- Internetwork Packet Exchange Control Protocol (IPXCP)
- DECnet Phase IV Control Protocol (DNCP)
- NetBIOS Frames Control Protocol (NBFCP)
- IPv6 Control Protocol (IPV6CP)

PPP Frame


PPP Frame
Flag
Address
Control
Protocol
Payload
FCS
Flag
1 byte
1 byte
(11111111)
1 byte
(11000000)
1 or 2 bytes
variable
2 or 4 bytes
1 byte
(01111110)

HDLC VS PPP

HDLC is a bit-oriented protocol , whereas PPP is a byte-oriented protocol.

HDLC is implemented by Point-to-point link configuration and also multi-point link configurations whereas

PPP is implemented by Point-to-Point configuration only.

HDLC does not offer error detection whereas PPP provides the feature of error detection using FCS (Frame Check Sequence) while transmitting data.

HDLC does not provide link authentication whereas PPP provides link authentication using protocols like PAP (Password Authentication Protocol) and CHAP (Challenge Handshake Authentication Protocol).

Token Bus (IEEE 802.4)

The token is passed from one user to another in a sequence.

A station can only transmit data when it has the token.

The physical medium has a bus architecture.

The tokens are released on successful receipt of the data frame.

A token is a small message that circulates among the stations of a computer network providing permission to the stations for transmission.

Ethernet

Ethernet is the most widely used LAN technology and is defined under IEEE standards 802.3

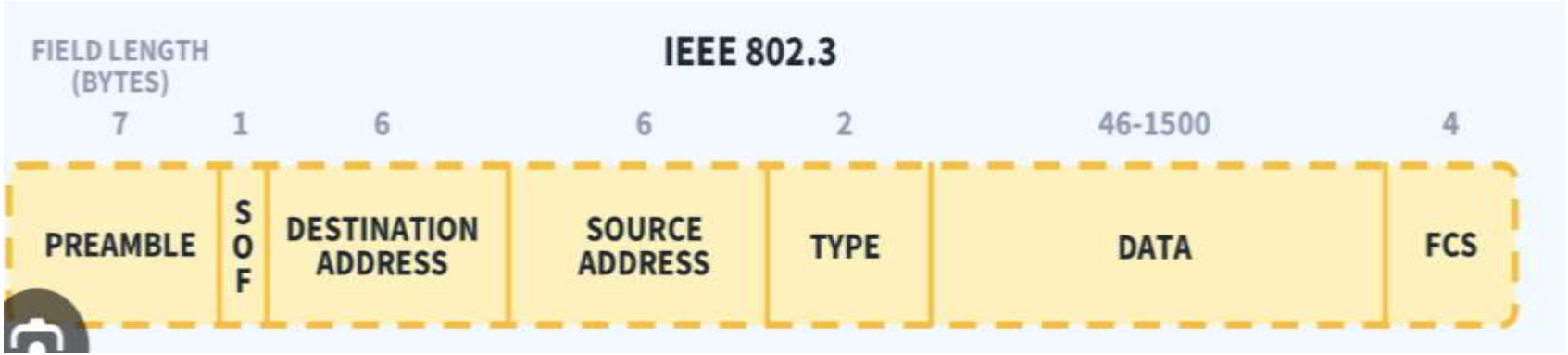
Media Access Control (MAC):

- Ethernet uses the MAC protocol to control access to the shared medium.
- It operates using Carrier Sense Multiple Access with Collision Detection (CSMA/CD):
  - **Carrier Sense**: Devices listen to the network before transmitting.
  - **Multiple Access**: Multiple devices can access the network.
  - **Collision Detection**: Devices detect collisions and retransmit after a random delay.

Ethernet Frame has following fields:

- **Preamble**: 7 bytes used for synchronization, The preamble helps the receiver synchronize its clock with the sender's clock.
- **SFD (Start Frame Delimiter)**: 1 byte indicating the start of the frame.
- **Destination MAC Address**: 6 bytes identifying the recipient.
- **Source MAC Address**: 6 bytes identifying the sender.
- **Length/Type**: 2 bytes indicating the frame length or protocol type.
- **Data and Padding**: Payload data (46 to 1500 bytes), padded if necessary to meet the minimum length.
- **FCS (Frame Check Sequence)**: 4 bytes for error detection using CRC.

Ethernet Frame structure



Revision for Yesterday

The arrangement of a network that comprises nodes and connecting lines via sender and receiver is referred to as **Network Topology**. The various network topologies are:

- Mesh Topology - every device is connected to another device via a particular channel.
- Star Topology - all the devices are connected to a single central node through a cable
- Bus Topology - is a network type in which every computer and network device is connected to a single cable.
- Ring Topology - It forms a ring connecting devices with exactly two neighboring devices.
- Hybrid Topology - This topological technology is the combination of all the various types of topologies we have studied above.

MCQ practice for data link layer

1.which error detection method uses one's complement airthemetic?

a.simple parity check

b.two dimensional parity check

c.CRC

d.checksum

ans: d

2.which error detection method consists of just one redundant bit per data unit?

a.simple parity check

b.two dimensional parity check

c.CRC

d.checksum

ans: a

3.In cyclic redundancy checking, what is the CRC?

a.the divisor

b.the quotient

c.the dividend

d.the remainder

ans : d

4.in the cyclic redundancy checking the divisor is ..... than the CRC

a.the same size as

b.one bit less than

c.one bit more than

d.none of the above

ans : b

5.A ..... error means that two or more bits in the data unit have changed.

a.double-bit
b.burst
c.single-bit
d.none of the above
ans: b

6.In ..... error correction, the receiver corrects error without requesting re-transmissions?
a.backward
b.onward
c.forward
d.none of the above
ans: c

7.In ..... error correction the receiver asks the sender to send the data again.
a.backward
b.retransmissions
c.forward
d.none of the above
ans: a

8.we can divide coding schemes into two broad categories:
a.block;linear
b.linear;nonlinear
c.block;convolution
d.none of the above
ans: c

9.In modulo-2 airthemetic ..... give the same results
a.addition and multiplication
b.addition and division
c.addition and substraction
d.none of the above
ans : c

10.we add r redundant bits to each block to make the length n = K + r . the resulting n-bit blocks
are called
a. data word
b. blockword
c. codewords
d. none of the above
ans : c

11.The ..... between two words is the number of difference between corresponding bits.
a.hamming code
b.hamming distance
c.hamming rule
d.none of the above
ans : b

12.the ..... of errors is more difficult than the .....
a. correction;detection
b. detection;correction
c. creation;correction
d. creation;detection
ans: a

13. The data link layer takes the packets from _____ and encapsulates them into frames for transmission.
a) network layer
b) physical layer
c) transport layer
d) application layer
ans: a

14. Which of the following tasks is not done by data link layer?
a) framing
b) error control

c) flow control
d) channel coding
ans : d

15. Which sublayer of the data link layer performs data link functions that depend upon the type of medium?
a) logical link control sublayer
b) media access control sublayer
c) network interface control sublayer
d) error control sublayer
ans: b

16. Automatic repeat request error management mechanism is provided by _____
a) logical link control sublayer
b) media access control sublayer
c) network interface control sublayer
d) application access control sublayer
ans: a

17. Which of the following is a data link protocol?
a) ethernet
b) point to point protocol
c) hdlc
d) all of the mentioned
ans: d

18. Which of the following is the multiple access protocol for channel access control?
a) CSMA/CD
b) CSMA/CA
c) Both CSMA/CD & CSMA/CA
d) HDLC
ans: c