Name: Sayma Akter Shumi

ID: IT-18032

Subject: computer Network

course code: ICT- 3207

Set-1

(a) What do you mean by Data Link Layer?

(b) What are the protocols of data link layer?

(c) What are the types of data link layer?

(d) What is link layer frame? Discuss the functionality of Data-link Layer details?

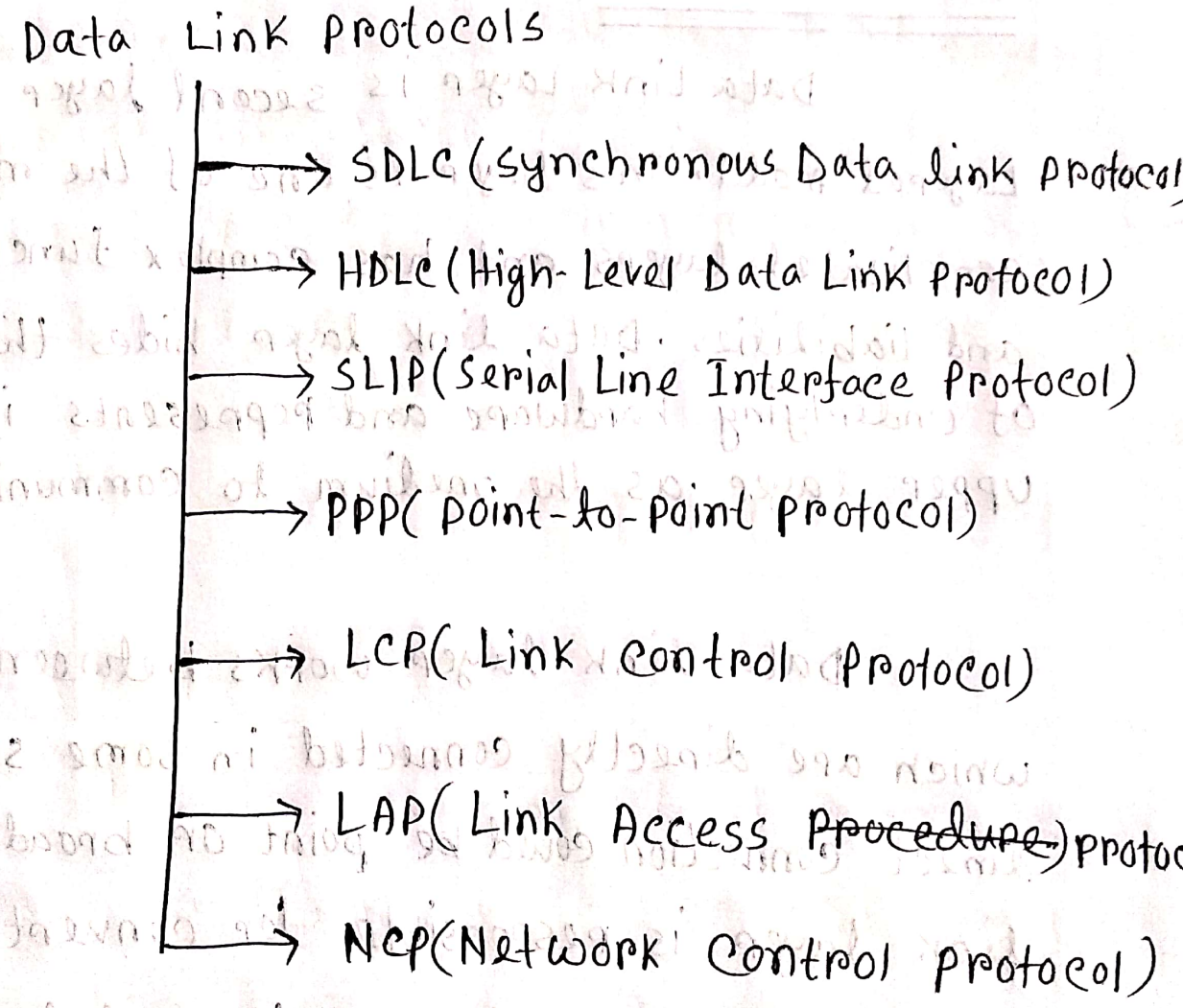
Ans to the question No: 1 (a)

Data-link Layer:

Data Link Layer is second layer of OSI Layered model. This layer is one of the most complicated layers and has complex functionalities and liabilities. Data link layer hides the details of underlying hardware and represents itself to upper layer as the medium to communicate.

Data link layer works between two hosts which are directly connected in some sense. This direct connection could be point or broadcast. Data link layer is responsible for converting data stream to signals bit by bit and to send that over the underlying hardware.

Ans to the question No: 1 (b)



Ans to the question No: 1(c)

The data link layer has two sublayer:

Logical link control (LLC):

The uppermost sublayer, LLC, multiplexes protocols running at the top of the data link layer, and optionally provides flow control, acknowledgement and error notification. The LLC provides addressing and control of the data link. It specifies which mechanisms are to be used for addressing station over the transmission medium and for controlling the data exchanged between the originator and recipient machines.

media access control (MAC):

MAC may refer to the sublayer that determines who is allowed to access the

media at any one time. Other times it refers to a frame structure delivered based on MAC addresses inside. There are generally two forms of media access control: distributed and centralized. Both of these may be compared to communication between people.

Ans to the question No: 1(d)

Link layer frame:

In the OSI model of computer networking, a frame is the protocol data unit at the data link layer. A frame is the unit of transmission in a link layer protocol and consists of a link layer header followed by a packet. Each frame is separated from the next by an interframe gap.

Functionality of Data-link Layer:

Data link layer does many tasks on behalf of upper layer. These are:

Framing:

Data link layer takes packets from Network Layer and encapsulates them into frames. Then it sends each frame bit-by-bit on the hardware. A receiver end data link layer picks up signals from hardware and assembles them into frame.

Addressing:

Data link layer provides layer-2 hardwar addressing mechanism. Hardware address is assumed to be unique on the link. It is encoded into hardware at the time of manufacturing.

Synchronization:

When data frames are sent on the link, both machines must be synchronized in order to transfer to take place.

Error control:

Sometimes signals may have encountered problem in transition and the bits are flipped. These errors are detected and attempted to recover actual data bits. It also provides error reporting mechanism to the sender.

Flow control:

Stations on same link may have different speed or capacity. Data link layer ensures flow control that

enables both machine to exchange data on same speed.

Multi-Access:

When host on the shared link tries to transfer the data, it has a high probability of collision. Data-link layer provides mechanism such as CSMA/CD to equip capability of accessing a shared media among multiple systems.

Set - 2

(a) What is flow control in data link layer? What types of mechanisms are used to control the flow in data link layer?

(b) What is Error control in data link layer? Mention all the mechanisms are required in Error control?

(c) What is ARQ in computer network? Discuss the types of ARQ Protocols?

Ans to the question No: 2 (a)

Flow control:

When a data frame is sent from one host to another over a single medium, it is required that the sender and receiver should work at the same speed. That is, sender sends at a speed on which the receiver can process and accept the data. If sender is sending too fast the receiver may be overloaded, data may be lost.

Two types of mechanisms can be deployed the flow:

- Stop and Wait:

This flow control mechanism forces the sender after transmitting a data

frame to stop and wait until the acknowledgement of the data-frame sent is received.

Sliding Window:

In this flow control mechanism, both sender and receiver agree on the number of data-frames after which the acknowlegement should be sent. As we learnt, stop and wait flow control mechanism wastes resources, this protocol tries to make use of underlying resources as much as possible

Ans to the question No: 2(b)

Error control:

When data-frame is transmitted, there is a probability that data-frame may be lost in the transit or it is received corrupted. In both cases, the receiver does not receive the correct data-frame and sender does not know anything about any loss. In such case, both sender and receiver are equipped with some protocols which helps them to detect transit errors such as loss of data-frame. Hence, either the sender retransmits the data-frame or the receiver may request to resend the previous data-frame.

Requirements for error control mechanism:

Error detection:

The sender and receiver, either both or any, must ascertain that there is some error in the transit.

positive ACK:

When the receiver receives a correct frame, it should ~~ackno~~ acknowledge it.

Negative ACK:

When the receiver receives a damaged frame or a duplicate frame, it sends a NACK back to the sender and the sender must retransmit the correct frame.

Retransmission:

The sender maintains a clock

and sets a timeout period. If can acknowledgement of a data-frame previously transmitted does not arrive before the timeout the sender retransmits the frame, thinking that the frame or its acknowledgement is lost in transit.

Ans to the question NO: 2(c)

Automatic Repeat Request (ARQ):

ARQ is a group of error-control protocols for transmission of data over noisy or unreliable communication network. These protocols reside in the data Link layer and in the transport layer of the OSI model. They

are named so because they provide for automatic retransmission of frames that are corrupted or lost during transmission. ARQ is also called positive Acknowledgement with Retransmission (PAR)

Types of ARQ Protocols:

There are three types of ARQ Protocols in the data link layer.

Stop and wait ARQ:

Stop and wait ARQ provides unidirectional data transmission with flow control and error control mechanism, appropriate

for noisy channels. The sender keeps a copy of the sent frame. It then waits for a finite time to receive a positive acknowledgement from receiver. If the timer expires, the frame is retransmitted. If a positive acknowlegement is received then the next frame is sent.

Go-Back-N ARQ:

Go-Back-N ARQ provides for sending multiple frames before receiving the acknowledgement for the first frame. It uses the concept of sliding window and so is also called sliding window protocol The frames are sequentially numbered and a finite number of frames are sent. If the acknowledgement of a frame is not received within the time period, all the frames starting from that frame

are retransmitted.

Selective Repat ARQ:

This protocol also provides for sending multiple frames before receiving the acknowledgement for the first frame. However, here only the erroneous or lost frames are retransmitted, while the good frames are ~~see~~ received and buffered.

Set-3

(a) What do you mean by error? Discuss the types of error?

(b) What do you mean by error detection? What are the types of error detection?

(c) What is CRC? Give example?

(d) What is parity check? How ~~is CRC used in error detection~~? What are the different types of errors detected by parity check?

Ans to the question No: 3(a)

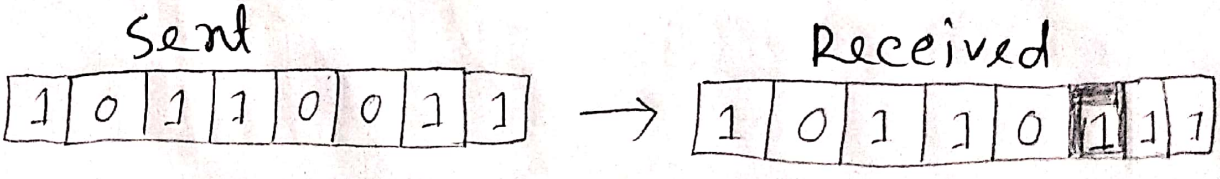
Error:

Error is a situation when the sender's data does not match the data at the receiver's end. When an error is detected then we need to retransmit the data. So there are various techniques of error control in computer networks.

Types of error:

There are three types of error-

Single bit error:



In a frame, there is only one bit, anywhere though, which is corrupt.

Multiple bits error:

Frame is received with more than one bits in corrupted state.

Burst error:

Ans to the Question NO: 3(b)

Error detection:

Error detection is the process of detecting the errors that are present in the data transmitted from transmitter to receiver, in a communication system. we use some redundancy codes to detect these errors, by adding to the data while it is transmitted from source.

Types of error detection:

* Parity checking
* Cyclic Redundancy check (CRC)
* Longitudinal Redundancy check (LRC)
* Check sum.

Ans to the question NO: 3(c)

CRC:

A cyclic redundancy check (CRC) is an error detecting code commonly used in digital networks and storage devices to detect accidental changes to raw data. Blocks of data entering these systems get a short check value attached, based on the remainder of a polynomials division of their contents.

Example:

CRC uses Generator polynomial which is available on both sender and receiver side. An example generator polynomial is of the form like x^3+x+1.

Ans to the question No: 3(d)

Parity check:

A parity check is the process that ensures accurate data transmission between nodes during communication. A parity bit is appended to the original data bits to create an even or odd bit number, the number of bits with value one.

If one bit (or odd number of bits) get inverted during transmission, then parity check will detect an error. In other words, only odd numbers of errors are detected by parity check.

set- 4

(a) What do you mean by Error correction? How error correction can be handled?

(b) Difference between error detection and error correction?

(c) what is Network layer? Write down its all functionalities?

Ans to the question No: 4(a)

Error correction:

Error correction codes are used to detect and correct the errors when data is transmitted from the sender to the receiver.

Error correction can be handled in two ways:

Backward error correction:

Once the error is discovered the receiver requests the sender to retransmit the entire data unit.

Forward error correction:

In this case, the receiver uses the error-correcting code which automatically corrects the errors.

Ans to the question NO: 4(b)

Difference between error detection and error correction -

Error detection	Error correction
Error detection is the detection of errors caused by noise or other impairments during transmission from transmitter to the receiver	Error correction is the detection of errors and reconstruction of the original, error-free data
Adding some Extra bits to detect Occurance of error	Adding enough redundant bits to deduce what the corred bits are
Request retransmission	correct the error
Error detection is easy	Error correction is hard
Less expensive	more expensive

Ans to the question No: 1 (c)

Network layer:

Layer-3 is the OSI model is called Network layer. Network layer manages options pertaining to host and network addressing, managing sub-networks, and internetworking.

Network layer takes the responsibility for routing packets from source to destination within or outside a subnet.

Functionalities of Network layer:

- Addressing devices and networks
- Populating routing tables or static routes
- Queuing incoming and outgoing data and then forwarding them according to quality of service constraints set for those packets
- Internetworking between two different subnets.

- Delivering packets to destination with best efforts.
- Provides connection oriented and connection less mechanism.

Set - 5

(a) What is Internet Protocol? Write down all features of network layer?

(b) What is network ~~address~~ address? Writedown types of network address?

(c) What is IP address? What are the types of IP address? How an IP address works?

Ans to the question NO: 5(a)

Internet Protocol:

Internet Protocol is widely respected and deployed Network layer protocol which helps to communicate end to end devices over the internet.

Network layer features:

withits standard functionalities, layer 3 can provide various features are:

- Quality of service management
- Load balancing and link management
- Security
- Interrelation of different Protocols and subnets with different schema
- Different logical network design over the physical network design
- L3 VPN and tunnels can be used to provide end to end dedicated connectivity.

Ans to the question No: 5(b)

Network address:

A network address is an identifier for a node or host on a telecommunications network. Network addresses are designed to be unique identifiers across the network, although some networks allow for local, private addresses, or locally administered addresses that may not be unique.

There are different kinds of network addresses in existence—

- IP
- IPX
- AppleTalk.

Ans to the question No: 5(c)

IP Address:

IP address stands for internet protocol address; it is an identifying number that is associated with a specific computer or computer network. When connected to the internet, the IP address allows the computers to send and receive information.

There are four types of IP addresses:

- Private
- Public
- Static
- Dynamic.

IP address works as -

An IP address allows computer to send and receive data over the internet most IP addresses are purely numerical, but as internet usage grows, letters have been added to some addresses.

Set-6

(a) What do you mean by routing? Write down the types of routing?

(b) Brifly discuss difference between static routing and dynamic routing?

(c) What is default routing? Why is Routing so important? Discuss

Ans to the question No: 6(a)

Routing:

Routing is a process which is performe by layer 3 devices in order to deliver th packet by choosing an optimal path fr one network to another.

Types of routing:

There are 3 types of routing

1. Static routing
2. Default routing
3. Dynamic routing

Ans to the question No: 6(b)

Difference between Static and dynamic routing -

Static routing	Dynamic routing
A form of routing that occurs when a router uses a manually-configured routing entry rather than information from a dynamic routing traffic.	A process where a router can forward data via a different route or given destination based on the current conditions of the communication circuits within a network
It is also called non-adaptive routing	It is also called adaptive routing
The network administrator manually adds the routes in the routing table	The routes are found automatically according to the changes in the network
Requires less Bandwidth	Requires more bandwidth
Configuration is difficult	Configuration is easy
More secure	Less secure

Ans to the question No: 6 (c)

Default routing:

This is the method where the router is configured to send all packet towards a single router. It doesn't matter to which network the packet belong, it is forwarded out to router which is configured for default routing. It is generally used with stub routers. A stub router is a router which has only one route to reach all other networks.

Importance of routing:

Routing is the hub around which all of IP connectivity revolves. At the simplest level, routing establishes basic internetwork communications, implements an addressing structure that uniquely identifies each device and organizes individual devices into a hierarchical network structure. Traditionally routers have also served as the media adapters that have connected remote offices to the headquarters via a WAN. The most recent trend, though, is to see routers as the integration platforms for a wide variety of network enchancements such as security, policy, and services that extend the capabilities of IP to support

Telephony, video, legacy service integration, and other applications over a converged network.

Set-7

(a) What is router? How router can make decision?

(b) Brifly discuss Unicast routing, Broadcast routing and multicast routing, anycast routing.

(c) What is routing Algorithm? Discuss difference between routing and Flooding

Ans to the question No: 7(a)

Router:

A router is a networking device that forwards data packets between computer networks. Routers platform the traffic directing functions on the internet. Then using information in its routing table, it directs the packet to the next network on it's ~~Joun~~ Journey.

Router can make decision based on the following information:

- Hop count
- Bandwidth
- Metric
- Prefix-length
- Delay

Ans to the question No: 7 (b)

Unicast routing:

Unicast routing is the process of forwarding Unicasted traffic ~~for~~ from a source to a destination on an internetwork. Unicasted traffic is destined for a unique address. The Internet Protocol and the internetwork Packet Exchange protocol are used as the example protocol where appropriate.

Broadcast routing:

In Broadcast routing, Packets are sent to all nodes even if they do not want it. ~~But~~ Routers create broadcast domains. But it can be configured to forward broadcast in some special cases. A broadcast message is destined to all network devices.

Multicast routing:

Multicast routing is a network-layer function that constructs paths along which data packet from a source are distributed to each many, but not all, destination in a communication network.

Anycast routing:

Anycast is a traffic routing algorithm used for the speedy delivery of website content that advertises individual IP addresses on multiple nodes. User requests are directed to specific nodes based on such factors as the capacity and health of your server, as well as the distance between it and the website visitor.

Ans to the Question No: 7(c)

Routing Algorithm:

A routing algorithm is a set of step-by step operations used to direct internet traffic efficiently. When a packet of data leaves its source, there are many different paths it can take to its destination. The routing algorithm is used to determine mathematically the best path to take.

Difference between routing and Flooding.

Routing	Flooding
Routing table is required	No routing table is required
May give shortest path	Always gives shortest path
Less reliable	more reliable
Traffic is less	Traffic is high
No duplicate packet	Duplicate packets are present

Set - 8

(a) Discuss Flooding and Shortest path in Routing Algorithm

(b) What is Internetworking ? What is the fundamental difference between Data link layer and network layer?

(c) What is Tunneling in computer network? What is ARP, Iemp in networking ?

Ans to the question No: 8(a)

Flooding:

Flooding is simplest method packet forwarding. when a packet is received, the routers send it to all the interfaces except the one on which it was received. This creates too much burden on the network and lots of duplicate packets wandering in the network. Time to Live can be used to avoid infinite looping of packets. There exists another approach for flooding which is called selective flooding to reduce the overhead on the network. In this method, the router does not flood out on all the interfaces, but selective ones.

Shortest Path:

Routing decision in network, are mostly taken on the basis of cost between source and destination. Hop count plays major role here

Shortest path is a technique which uses various algorithms to decide a path with minimum number of hops.

common shortest path algorithm are

→ Dijkstra's algorithm

→ Bellman Ford algorithm

→ Floyd warshall algorithm

Ans to the Question No: 8(b)

Internetworking:

In real world scenario, networks under same administration are generally scattered geographically. There are exist requirement of connecting two different networks of same kind as well as of different kinds. Routing between two networks is called internetworking

Fundamental difference between network layer and data link layer:

Data link layer only deals with efficient transmission of information between adjacent machines in the network that are directly connected to each other.

Network layer, which employs the services of the data link layer, provides end-to-end connectivity between machines that are not necessarily directly connected.

Ans to the question NO: 8(c)

Tunneling:

In computer networks, a tunneling protocol is a communications protocol that allows for the movement of data from one network to another. It involves allowing private network communicatio to be sent across a public network through a process called encapsulation.

ARP:

The Address Resolution Protocol (ARP) is a communication protocol used for discovering the link layer address, such as a MAC address, associated with a given internet layer address, typically an IPV4 address. This mapping is a critical function in the internet protocol suite.

Icmp:

Icmp is a transport level protocol within Tcp/Ip which communicates information about network connectivity issues back to the source of the compromised transmission. It sends control messages such as destination network unreachable, source route failed and source quench.