Chapter 1

Q / What Is an Internetwork?

collection of individual networks, connected by intermediate networking devices, that functions as a single large network. Internetworking refers to the industry, products, and procedures that meet the challenge of creating and administering internetworks

Q/ Internetwork evolved as solution for what?

1. Isolated LANs made electronic communication between different offices or departments impossible.
2. Duplication of resources meant that the same hardware and software had to be supplied to each office or department as did separate support staff.
3. lack of network management meant that no centralized method of managing and troubleshooting networks existed.

Q/WHAT Internetworking Challenges?

1. **(connectivity)** connecting various systems is to support communication among disparate technologies.
2. **(reliability)** companies rely heavily on data communication, internetworks must provide a certain level of reliability.
3. **(network management)** network management must provide centralized support and troubleshooting capabilities in an internetwork. Configuration, security, performance, and other issues.
4. **(Security)** protect the network from internal AND external attacks.
5. **(flexibility)** internetworks must be flexible enough to change with new demands.

Q/ WHAT IS OSI MODEL?

The OSI reference model is a conceptual model composed of seven layers, each specifying network functions, The OSI model divides the tasks involved with moving information between networked computers into seven smaller, more manageable task groups. A task or group of tasks is then assigned to each of the seven OSI layers. These layers are divided in two categories

-UPPER LAYER (Application / Presentation/ Session)

The upper layers of the OSI model deal with application issues and generally are implemented only in software.

-LOWER LAYER (Transport / Network / Data link / Physical)

The lower layers of the OSI model handle data transport issues. The physical layer and the data link layer are implemented in hardware and software.

Q/ WHAT IS OSI LAYER AND WHAT IT IS PRIMARY FUNCTIONS OF EACH ONE?

1. **OSI Model Physical Layer**
   - Define electrical, mechanical, procedural, and functional specification for activating, maintaining, deactivating the physical link between sender and receiver.
   - Define characteristic such as timing of voltage levels, voltage levels, data rate, transmission distance, physical connectors.
2. **OSI Model Data Link Layer**
   - provides reliable transit of data across a physical network link.
   - Define network and protocol characteristics, including physical addressing, network topology, error notification, sequencing of frames, and flow control.

DATA LINK SUBLAYERS IS

- Logical Link Control (LLC): sublayer of the data link layer manages communications between

devices over a single link of a network. also supports both connectionless and connection-oriented services used by higher-layer protocols.

-Media Access Control(MAC): Manages protocol access to the physical network medium. Also define mac addresses.

3. **OSI Model Network Layer**
   - Define network address(IP)
   - defines the logical network layout
   - routers can use this layer to determine how to forward packets.
4. **OSI Model Transport Layer**
   - Accept data from session layer and segment it to be transport across network
   - Define error control mechanism which guarantee that received data is free of error and in proper sequence.
   - Define flow control mechanism which manage data rates between sender and receiver.
   - Manage multiplexing, virtual circuits.
   - Define protocols used on the Internet TCP and UDP
5. **OSI Model Session Layer**
   - establishes, manages, and terminates communication sessions
   - Communication sessions consist of service requests and service responses that occur between applications located in different network devices. These requests and responses are coordinated by protocols implemented at the session layer.
6. **OSI Model Presentation Layer**
   - provides a variety of coding and conversion functions that are applied to application layer data that ensure that information sent from the application layer of one system would be readable by the application layer of another system
     these function is
     - common data representation formats enable interchange of data between different computer systems

- Conversion schemes are used to exchange information with systems by using different text and data representations, such as EBCDIC and ASCII.
- Standard data compression schemes enable data that is compressed at the source device to be properly decompressed at the destination
- Standard data encryption schemes enable data encrypted at the source device to be properly deciphered at the destination.

7. **OSI Model Application Layer**
    - Closest to the end user which mean application layer and end user interact directly with software application (browsers, chat and others)
    - (communication partners): determines the identity and availability of communication partners for an application with data to transmit.
    - (determining resource availability): decide whether sufficient network resources for the requested communication exist
    - (synchronizing communication) all communication between applications requires cooperation that is managed by the application

Q / WHAT IS PROTOCOL AND WHAT IS ITS TYPES?

It is a formal set of rules and conventions that governs how computers exchange information over a network medium. A protocol implements the functions of one or more of the OSI layers.

1. **LAN PROTOCOLS:** operate at the physical and data link layers of the OSI model and define communication over the various LAN media.
2. **WAN PROTOCOLS**: operate at the lowest three layers of the OSI model and define communication over the various wide-area media.
3. **ROUTING PROTOCOLS**: network layer protocols that are responsible for exchanging information between routers so that the routers can select the proper path for network traffic.
4. **NETWORK PROTOCOLS**: various upper-layer protocols that exist in a given protocol suite

NOTE: DIFFERENT PROTOCOLS CAN INTERACT WITH EACH OTHER.

Q / WHAT OSI LAYER SERVICES AND WHAT IS ITS ELEMNTS?

At source side One OSI layer communicate with adjacent layers to use services provided by second layer, these services allow first layer to communicate with peer layer in the destination side. This provided using following elements:

1. Service user (first layer)
2. Service provider (second layer)
3. Service access point (SAP): conceptual location where first layer request service from second layer.

Q / WHAT IS CONTROL INFORMATION IN OSI MODEL?

It consists of specific requests and instruction that is exchanged between peer layers.

Control information has two types:

1.**headers** (prepended to data passed from upper layers)

2.**trailers** (appended to data passed from upper layers)

Q/WHAT IS INFORMATION FORAMT (OR FORMS) AT DIFFERENT OSI LAYERS?

- AT DATA LINK LAYER
    1. **FRAME** (in normal environment):it is composed of the data link layer header (and possibly a trailer) and upper-layer data.
    2. **Cell** (in switched environments) an information unit of a fixed size whose source and destination are data link layer.
- AT NETWORK LAYER
    1. **PACKET** (Connection-Oriented network service): information unit of whose source and destination are NETWORK layer.
    2. **DATAGRAM** (connectionless network service) information unit whose source and destination are network layer entities
- AT TRANSPORT LAYER
    1. **SEGMENT**: information unit whose source and destination are transport layer entities.
- AT UPPER LAYER
    1. **MESSAGE**: information unit whose source and destination entities exist above the network layer (often at the application layer).

NOTE: **Data unit** is a generic term that refers to a variety of information units. Some common data units are service data units (SDUs), protocol data units, and bridge protocol data units (BPDUs). SDUs are information units from upper-layer protocols that define a service request to a lower-layer protocol. PDU is OSI terminology for a packet. BPDUs are used by the spanning-tree algorithm as hello messages.

Q / WHAT IS ISO HIERARCHY OF NETWORKS AND HOW ITS DEFINED

It is a hierarchical organization provides such advantages as ease of management, flexibility, and a reduction in unnecessary and has three networks levels:

1. **ES:** network device that does not perform routing or other traffic forwarding functions. Typical ESs include such devices as terminals, personal computers, and printers.
2. **IS:** is a network device that performs routing or traffic-forwarding functions, ISs include such devices as routers, switches, and bridges .IS has two types:
   -intradomain IS communicates within a single autonomous system.
   -interdomain IS communicates within and between autonomous systems.
3. **AREA:** logical group of network segments and their attached devices. Areas are subdivisions of autonomous systems (AS's).
4. **AS:** collection of networks under a common administration that share a common routing strategy. Autonomous systems are subdivided into areas, and an AS is sometimes called a domain.

Q / WHAT IS Connection-Oriented and Connectionless Network Services

1. **Connection-Oriented**
   - must first establish a connection with the desired service before passing any data SO there will be three phases: connection establishment, data transfer, and connection termination,
   - connection-oriented services provide some level of delivery guarantee, whereas connectionless services do not.
   - Connection-oriented network services have more overhead than connectionless ones.
2. **Connectionless Network Services**
   - send the data without any need to establish a connection first.
   - transfer can simply send the data without the added overhead of creating and tearing down a connection.

Q/ WHAT IS DIFFERENCE BETWEEN HIERARCHICAL AND FLAT ADDRESS SPACE?

HIERARCHICAL	FLAT
1. organized into numerous subgroups, each successively narrowing an address until it points to a single device. 2. offers certain advantages over flat-addressing schemes (Address sorting and recall is simplified using comparison operations)	1. organized into a single group

Q / WHAT IS INTERNETWORK ADDRESSING:

Internetwork addresses identify devices separately or as members of a group. Addressing

schemes vary depending on the protocol family and the OSI layer

DATA LINK LAYER ADDRESS	MAC	IP(NETWORK LAYER ADDRESS)
1. uniquely identifies each physical network connection of a network devices 2. exist within a flat address space 3. have a pre-established and typically fixed relationship to a specific device 4. End systems generally have only one physical network connection and thus have only one datalink address 5. Routers and other internetworking devices typically have multiple physical network connections and therefore have multiple data-link addresses 6. Sometimes called physical or hardware addresses	1. identify network entities in LANs. 2. consist of a subset of data link layer addresses. 3. MAC addresses are unique for each LAN interface 4. MAC addresses are 48 bits in length and are expressed as 12 hexadecimal digits 5. The first 6 hexadecimal digits identify the manufacturer or vendor 6. The last 6 hexadecimal digits comprise the interface serial number 7. sometimes are called burned-in addresses (BIAs)	1. Identify entity at the network layer of the OSI layers. 2. exist within a hierarchical address space 3. The relationship between a network address and a device is logical and unfixed; 4. End systems require one network layer address for each network layer protocol that they support 5. Routers and other internetworking devices require one network layer address per physical network connection for each network layer protocol supported. 6. sometimes are called virtual or logical addresses

Q / WHAT IS MAPPING AND ITS METHODS?

it is technique that allow map network addresses to MAC addresses, SO When the network layer has determined the destination station's network address, it must forward the information over a physical network using a MAC address. IT HAS THREE METHODS:

1. **Address Resolution Protocol (ARP):** method used in the TCP/IP suite, First, the sending station will check its ARP table to see if it has already discovered this destination station's MAC address. If it has not, it will send a broadcast on the network with the destination station's IP address contained in the broadcast. Every station on the network receives the broadcast and compares the embedded IP address to its own. Only the station with the matching IP address replies to the sending station with a packet containing the MAC address for the station. The first station then adds this information to its ARP table for future reference and proceeds to transfer the data. When the destination device lies on a remote network, one beyond a router, the process is the same except that the sending station sends the ARP request for the MAC address of its default gateway. It then forwards the information to that device. The default gateway will then forward the information over whatever networks necessary to deliver the packet to the network on which the destination device resides. The router on the destination device's network then uses ARP to obtain the MAC of the actual destination device and delivers the packet
2. **Hello protocol:** network layer protocol that enables network devices to identify one another and indicate that they are still functional, when a new end system powers up, for example, it broadcasts hello messages onto the network. Devices on the network then return hello replies, and hello messages are also sent at specific intervals to indicate that they are still functional. Network devices can learn the MAC addresses of other devices by examining Hello protocol packets.
3. **predictable MAC addresses**: Three protocols make MAC addresses are predictable because the network layer either
   -embeds the MAC address in the network layer address
   -or uses an algorithm to determine the MAC address.
   The three protocols are Xerox Network Systems (XNS), Novell Internetwork Packet Exchange (IPX), and DECnet Phase IV.

Q/ WHAT IS DIFFERENCE BETWEEN STATIC AND DYNAMIC ADDRESS ASSIGNMENTS

STATIC	DYNAMIC
1. assigned by a network administrator according to a preconceived internetwork addressing plan. 2. does not change until the network administrator manually changes it	1. obtained by devices when they attach to a network 2. device has different address each time it connects to network. 3. May defined using server, and theses server has recycle address and reuse it when device disconnected

Q / EXPLAIN NAMES AND ADDRESSES IN INTERNETWORK THEN EXPLAIN DNS?

Internetwork devices usually have both a name and an address associated with them

1. **names:** typically, are location-independent and remain associated with a device wherever that device moves
2. **addresses:** usually are location-dependent and change when a device is moved (MAC addresses are an exception to this rule).
3. **Domain Name System (DNS):** map the name of a device to its IP address

Q/ WHAT IS FLOW CONTROL AND WHAT IS ITS TECHNIQUE?

function that prevents network congestion by ensuring that transmitting devices

do not overwhelm receiving devices with data, AND has following technique

1. **Buffering:** used by network devices to temporarily store bursts of excess data in memory until they can be processed.
2. **Source-quench messages:** used by receiving devices to help prevent their buffers from overflowing. The receiving device sends source-quench messages to request that the source reduce its current rate of data transmission,
   - First, the receiving device begins discarding received data due to overflowing buffers.
   - Second, the receiving device begins sending source quench messages to the transmitting device at the rate of one message for each packet dropped
   -third, the source device receives the source-quench messages and lowers the data rate until it stops receiving the messages
   -fourth, source device then gradually increases the data rate if no further source-quench requests are received.
3. **Windowing:** source device requires an acknowledgment from the destination after a certain number of packets have been transmitted.

Q/EXPLAIN ERROR-CHECKING BASICS AND WHAT IS CRC?

determine whether transmitted data has become corrupt or otherwise damaged while traveling from the source to the destination. Error checking is implemented at several of the OSI layers.

CRC(cyclic redundancy check):

A CRC is a value generated by a calculation that is performed at the source device. The destination device compares this value to its own calculation to determine whether errors occurred during transmission. If the values are equal, the packet is considered valid. If the values are unequal, the packet contains errors and is discarded.

Q/ EXPLAIN MULTIPLEXING AND ITS METHOD IN DATA AND WHAT IS MULTIPLEXER?

- **MULTIPLEXING**: process in which multiple data channels are combined into a single data or physical channel at the source. Multiplexing can be implemented at any of the OSI layers, demultiplexing is the process of separating multiplexed data channels at the destination.
- **MULTIPLEXER**: physical layer device that combines multiple data streams into one or more output channels at the source. Multiplexers demultiplex the channels into multiple data streams at the remote end and thus maximize the use of the bandwidth of the physical medium by enabling it to be shared by multiple traffic sources.

PHYSICAL LAYER MULTIPLEXING METHODS:

1. **TDM:** information from each data channel is allocated bandwidth based on preassigned time slots, regardless of whether there is data to transmit.
2. **ATDM**: information from data channels is allocated bandwidth as needed by using dynamically assigned time slots.
3. **FDM**: information from each data channel is allocated bandwidth based on the signal frequency of the traffic.
4. **statistical multiplexing**: bandwidth is dynamically allocated to any data channels that have information to transmit

CHAPTER 2:

Q/ What Is a LAN?

a high-speed data network that covers a relatively small geographic area. It typically connects workstations, personal computers, printers, servers, and other devices, LANs offer computer users many advantages

- including shared access to devices and applications

-file exchange between connected users

- communication between users via electronic mail and other applications.

Q / EXPLAIN LAN MEDIA-ACCESS METHODS.

It is methods that must be used to allow one device access to the network media at a time

carrier sense multiple access collision detects (CSMA/CD):	**token-passing networks**
1.when device has data to send first listens to see if any other device is currently using the network.	1. a special network packet called a token is passed around the network from device to device.

2.If not, it starts sending its data 3.After finishing its transmission, it listens again to see if a collision occurred 4.When a collision happens, each device waits a random length of time before resending its data. 5. creating smaller collision domains, the performance of a network can be increased significantly without requiring addressing changes. 6. CSMA/CD networks are half-duplex	2. When a device has data to send, it must wait until it has the token and then sends its data 3.When finish the token is released so that other devices may use the network media 4. The main advantage of token-passing networks is easy to calculate the maximum time that will pass before a device can send data.

Q / EXPLAIN LAN TRANSMISSION METHODS

1. unicast transmission: a single packet is sent from the source to a destination on a network
2. multicast transmission: consists of a single data packet that is copied and sent to a specific subset of nodes on the network.
3. broadcast transmission consists of a single data packet that is copied and sent to all nodes on the network.

Q/ EXPLAIN LAN TOPOLOGIES.

define the way that network devices are organized, these topologies are logical architectures, but the actual devices need not be physically organized in these configurations.

BUS	RING	STAR	TREE
Linear LAN architecture in which transmissions from network stations propagate the length of the medium and are received by all other stations	LAN architecture that consists of a series of devices connected to one another by unidirectional transmission links to form a single closed loop	LAN architecture in which the endpoints on a network are connected to a common central hub, or switch, by dedicated links. Logical bus and ring topologies are often implemented physically in a star topology	LAN architecture that is identical to the bus topology, except that branches with multiple nodes are possible in this case

Q / EXPLAIN LAN DEVICES

1.**REPEATER:** physical layer device used to interconnect the media segments of an extended network. A repeater essentially enables a series of cable segments to be treated as a single cable. Repeaters receive signals from one network segment and amplify, retime, and retransmit those signals to another network segment, all electrical signals, including electrical disturbances and other errors, are repeated and amplified. The total number of repeaters and network segments that can be connected is limited due to timing and other issues.

2. **hub** is a physical layer device that connects multiple user stations, each via a dedicated cable. Electrical interconnections are established inside the hub. Hubs are used to create a physical star network while maintaining the logical bus or ring configuration of the LAN.

3. **A LAN extender:** is a remote-access multilayer switch that connects to a host router. LAN extenders forward traffic from all the standard network layer protocols and filter traffic based on the MAC address

or network layer protocol type. LAN extenders are not capable of segmenting traffic or creating security firewalls.

Q / WHICH IS BEST TOKEN RING AND FDDI?

FDDI is the best because it has two tracks to transmit data one always available and the other as a backup track, so this will provide reliability in the network.

Q / EXPLAIN MODULATION IN NETWORK

modulation is the process of converting a digital signal (sender side) into an analog signal (so that it can be transmitted as electrical pulses). on the receiver side we have demodulation, which takes an analog signal and converts it back into a digital signal that can be read by the receiving computer. This process done usually by NIC attached to computer.

Q/WHAT IS DIFFERENCE BETWEEN ROUTER AND BRIDGES

ROUTER	BRIDGES
1. determine the best path for sending data and filtering broadcast traffic to the local segment 2. Routers work at the Network layer of the OSI model 3. Routers have access to more information in packets than Bridges 4. Routers can share status and routing information with one another and use this information to bypass slow or malfunctioning connections 5. Routers will only pass the information if the network address is known This made routers use links more efficiently than Bridge	1. A Bridge can join segments or workgroup LANs 2. Bridges work at the Data Link Layer of the OSI 3. do not distinguish between one protocol and another 4. bridge forwards the packets based on the address of the destination node

Some important notes:

- **encapsulation**: means that the a given layer "adding" protocol information to the next layer, from Layer 7 straight down to Layer 1 in purpose of transmitting data from one device to another device correctly
- **burned-in addresses (BIAs):** It is term called to MAC addresses because they are burned into read only memory (ROM) and are copied into random-access memory (RAM) when NIC initialized.
- **A collision**: occurs when two devices send data simultaneously