STUCOR APP - EC8551 - COMMUNICATION NETWORKS

DEPARTMENT OF ELECTRONICS AND COMMUNICATION ENGINEERING

UNIT-I FUNDAMENTALS & LINK LAYER
PART-A

1. **Write down the requirements to build a computer network.**

   The following are the requirements to build a computer network. Computers, Network interfaces, Switches, Hub, Routers and cables . All these components work together to create a functioning network.

2. **List the metrics that influence the performance of computer networks.**

   Network performance is measured by reviewing the statistics and metrics from the following network components:
   - Network bandwidth or capacity - Available data transfer.
   - Network throughput - Amount of data successfully transferred over the network in a given time.
   - Network delay, latency and jittering - Any network issue causing packet transfer to be slower than usual.
   - Data loss and network errors - Packets dropped or lost in transmission and delivery.

3. **Define the terms: Bandwidth and Latency.**

   Bandwidth
   - Amount of data that can be transmitted per time unit
     ⇨ transmitted = put into the pipe (wire)
   - Example: 10Mbps (10 million bits per second)

   Latency
   - Time it takes to send a message from point A to point B
   - Components of latency
     Latency = Propagation + Transmit + Queuing
     Propagation = Distance / Speed-of-Light
     Transmit = Packet-Size / Bandwidth

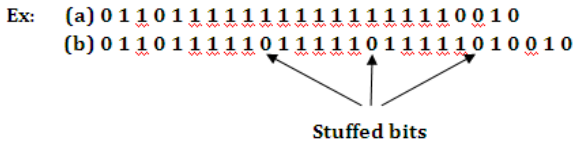
4. **Compare Byte-oriented versus Bit-oriented protocol.**

   Byte-oriented protocol
   - In a byte-oriented protocol, data to be carried are 8-bit characters from a coding system.
   - Character-oriented protocols were popular when only text was exchanged by the data link layers.

   Bit-oriented protocol
   - In a bit-oriented protocol, the data section of a frame is a sequence of bits.
   - Bit-oriented protocols are more popular today because we need to send text, graphic, audio, and video which can be better represented by a bit pattern than a sequence of characters

5. **What is meant by bit stuffing? Give an example.**

   Bit stuffing is the process of adding one extra 0 whenever there are five consecutive 1s in the data, so that the receiver does not mistake the data for a flag (01111110).



6. Distinguish between packet switched and circuit switched networks.

The differences between packet switched and circuit switched networks are as follows.

S.No.	Circuit switched networks.	Packet switched networks
1.	Dedicated transmission path	No dedicated transmission path
2.	All packets use same path	All packets use different path
3.	Busy signal is introduced if called party is busy.	No busy signal here.
4.	Messages are not stored	Packets may be stored until delivered
5.	Fixed Bandwidth transmission	Dynamic use of Bandwidth

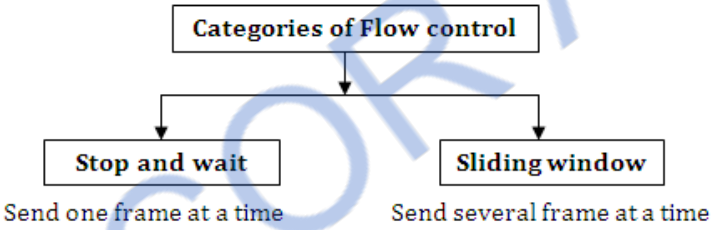
7. List the services provided by data link layer.

The services provided by data link layer are

- Framing and link access
- Reliable delivery
- Flow control
- Error detection
- Error correction and
- Half-Duplex and Full-Duplex

8. Define flow control.

- Flow control refers to a set of procedures used to restrict the amount of data that the sender can send before receiving an acknowledgement from the receiver.



9. Write the parameters used to measure network performance.

The parameters used to measure network performance are:

- Bandwidth commonly measured in bits/second is the maximum rate that information can be transferred.
- Throughput is the actual rate that information is transferred.
- Latency is the delay between the sender and the receiver decoding it, this is mainly a function of the signals travel time, and processing time at any nodes the information traverses.
- Jitter variation is the packet delay at the receiver of the information.
- Error rate is the number of corrupted bits expressed as a percentage.

10. Define the term protocol.

- A network protocol defines rules and conventions for communication between network devices.
- Protocols for computer networking generally use packet switching techniques to send and receive messages in the form of packets.

11. State the issues of data link layer.

The main job of the data link layer is to make the communication on the physical link reliable and efficient. The major issues of DLL are,

- Provide interface to the network layer services.
- Framing
- Error Control
- Flow control
- Synchronization , Link configuration control

12. What do you mean by error control?

- The term error control is defined as the process of identification or correction of error occurred in the transmitted data.
- The purpose of error control is to ensure that the information received by the receiver is exactly the information transmitted by the sender.
- There are two types of error control mechanisms. They are:
    1. Forward error control:
    2. Feedback or (backward) error control:

13. What is meant by framing?

- Framing is a function of the data link layer. It provides a way for a sender to transmit a set of bits that are meaningful to the receiver. Framing are categorized into two types. They are
    a) Fixed size framing
    b) Variable size framing.

14. Define Hamming distance.

- The Hamming distance is a number used to denote the difference between two binary strings.
- It is a small portion in a broader set of formulas used in information analysis.
- Specifically, Hamming formulas allow computers to detect and correct error on their own.

15. What is meant by port address, logical address and physical address?

- **Port Address**
    - ✓ There are many applications running on the computer. Each application run with a port number (logically) on the computer. This port number for application is decided by the Kernel of the OS. This port number is called port address.
- **Logical Address**
    - ✓ An IP address of the system is called logical address. This address is the combination of Net ID and Host ID. This address is used by network layer to identify a particular network (source to destination) among the networks. This address can be changed by changing the host position on the network. So it is called logical address.
- **Physical Address**
    - ✓ Each system having a NIC (Network Interface Card) through which two systems physically connected with each other with cables. The address of the NIC is called Physical address or MAC address. This is specified by the manufacture company of the card. This address is used by data link layer.

16. **What will be the maximum number of frames sent but unacknowledged for a sliding Window of size n-1(n is the sequence number)?**
    - Sliding windows, a technique also known as windowing, is used by the Internet's Transmission Control Protocol (TCP) as a method of controlling the flow of packets between two computers or network hosts.
    - The window can hold n-1 frames at either end; therefore, a maximum of n-1 frames may be sent before an acknowledgement is required.

17. **Give the purpose of layering.**
    The purpose of the OSI reference model is to make networks more manageable and to aid the problem of moving data between computers.
    - Allow manufactures of different systems to interconnect their equipment through standard interfaces.
    - Allow software and hardware to integration well and be portable on differing systems.
    - Create a model which all the countries of the world use.
    - The model divides the problem of moving data between computers into seven smaller, more manageable tasks, which equate to the seven layers of the OSI reference model.

18. **Mention the advantage and disadvantage of error correction by receiver, as compared to error detection.**
    Advantages and disadvantages of error correction by receivers are,
    - Error correcting codes are more sophisticated than error detection codes
    - It requires more redundancy bits.
    - The number of bits required for correcting a multiple-bit.
    - Burst error is so high that in most cases it is inefficient to do so.

19. **What do you mean by framing?**
    The data link layer divides the stream of bits and computes the checksum for each frame received from the network layer into manageable data units called frames. At the destination the checksum is recomputed.
    The framing methods are
    - Character count ,Starting and ending characters with character stuffing
    - Starting and ending flags with bit stuffing.

20. **What are the two different types of errors occurred during data transmission?**
    The two different types of Errors that occur during data transmission are
    - **Single Bit Error :** The term single bit error means that only one bit of the data unit was changed from 1 to 0 and 0 to 1.
    - **Burst Error :** The term burst error means that two or more bits in the data unit were changed. Burst error is also called packet level error, where errors like packet loss, duplication, reordering.

21. **What are the major duties of network layer?**
    The network layer is responsible for the source to destination delivery of a packet across multiple networks .The major duties are
    - Routing
    - Frame fragmentation
    - Logical-physical address mapping

22. What are the three fundamentals characteristics does the effectiveness of a data communications system depends upon?

The effectiveness of a data communications system depends upon the 3 fundamental characteristics such as

- **Delivery** : The system must deliver data to the correct destination.
- **Accuracy** : The system must deliver data accurately.
- **Timeliness** : The system must deliver data in a timely manner.

23. Define Error detection and correction.

- **Error Detection**

  Error detection is the process of detecting the error during the transmission between the sender and the receiver.

  - **Types of error detection**
    - ✓ Parity checking
    - ✓ Cyclic Redundancy Check (CRC)
    - ✓ Checksum
- **Error Correction**

  This type of error control allows a receiver to reconstruct the original information when it has been corrupted during transmission.
    - ✓ Hamming Code

24. **What are the two types of line configuration?**

- Line configuration refers to the way two or more communication devices attach to a link. Line configuration is also referred to as connection.
- A link is a communication medium through which data is communicated between devices. For communication to occur between two devices, they must be connected to the same link at the same time.

  There are two possible types of line configurations or connections. They are,

  1. Point-to-point connection – Dedicated link between two devices
  2. Multipoint connection – More than two devices share a single link.

25. **Define Full Duplex and simplex transmission system.**

- **Full duplex:** In full duplex or duplex communication mode, both the devices can transmit and receive the data at the same time. Example: Telephone conversation.
- **Simplex** : In this mode of transmission, the information is communicated in only one direction (unidirectional), that is, always from source to destination. Example: Transfer of data from computer to a printer.

26. **How does NRZ-L differ from NRZ-I?**

- "Non return-to-zero-level (NRZ-L) is a data encoding scheme in which a negative voltage is used to represent binary one and a positive voltage is used to represent binary zero.
- As with NRZ-L, "Non return-to-zero-level (NRZ-I) maintains a constant voltage pulse for the duration of a bit time. The data themselves are encoded as the presence or absence of a signal transition at the beginning of the bit time. A transition (low to high or high to low) at the beginning of a bit time denotes a binary 1 for that bit time; no transition indicates a binary 0."

27. Name some services provided by the application layer.

Some services of the application layer are:

- Network Virtual Terminal (NVT)
- File transfer, access and management
- Mail services
- Directory services

28. Group the OSI layers by its function.

The seven layers of the OSI model belonging to three subgroups.

- Physical, data link and network layers are the network support layers; they deal with the physical aspects of moving data from one device to another.
- Session, presentation and application layers are the user support layers; they allow interoperability among unrelated software systems.
- The transport layer ensures end-to-end reliable data transmission.

29. What are the steps followed in checksum generator?

The sender follows these steps in checksum generator,

- The units are divided into k sections each of n bits.
- All sections are added together using 2's complement to get the sum.
- The sum is complemented and become the checksum.
- The checksum is sent with the data.

30. Define Unicast and Multicast.

Unicast: Unicast is the term used to describe communication where a piece of information is sent from one point to another point. In this case there is just one sender, and one receiver.
EX: All LANs (e.g. Ethernet) and IP networks support the unicast transfer mode.

Multicast: Multicast is the term used to describe communication where a piece of information is sent from one or more points to a set of other points. In this case there is may be one or more senders, and the information is distributed to a set of receivers (there may be no receivers, or any other number of receivers).
Ex: One example of an application which may use multicast is a video server sending out networked TV channels

PART-B

1. With a neat sketch, explain the function of OSI network architecture. **(13)**

2. Discuss the different ways to address the framing problem. **(13)**

3. With a neat sketch, explain the architecture of an OSI seven layer model **(13)**

4. Discuss the approaches used for error detection in networking. **(13)**

5. i) Obtain the 4-bit CRC code for the data bit sequence 10011011100 using the polynomial $x^4 + x^2 + 1$. **(03)**

ii) Explain the challenges faced in building a network. **(10)**

6. i) With a protocol graph, explain the architecture of internet. **(07)**

ii) Consider a bus LAN with a number of equally spaced stations with a data rate of 9 Mbps and a bus length of 1 km. What is the mean time to send a frame of 500 bits to another station, measured from the beginning of transmission to the end of reception? Assume a propagation speed of 150 m/s. If two stations begin to monitor and transmit at the same time, how long does it need to wait before an interference is noticed? **(06)**

7. Draw the OSI network architecture and explain the functionalities of each layer in detail. **(13)**
8. i) Discuss in detail about the network performance measures. **(08)**
   ii) Explain selective-repeat ARQ flow control method. **(08)**
9. Explain any two error detection mechanism in detail. **(13)**
10. Explain in detail about i) HDLC ii) PPP. **(13)**
11. Explain the various flow control mechanisms. **(13)**
12. What is the need for error detection? Explain with typical examples. Explain methods used for error detection and error correction. **(13)**
13. Explain in detail the error-detection codes. **(13)**
14. Given a remainder of 111, a data unit of 10110011 and a divisor of 1001, is there an error in the data unit. Justify your with necessary principles. **(13)**
15. How frame order and flow control is achieved using the data link layer. **(13)**
16. i) Explain NRZ, NRZI and Manchester encoding schemes with examples.
    ii) Describe how bit stuffing works in HDLC protocol. **(13)**
17. i) Discuss the issues in the data link layer. **(13)**
    ii) Suppose we want to transmit the message 11001001 and protect it from errors using the CRC polynomial X^3+1. Use polynomial long division to determine the message that should be transmitted. **(06)**
18. (i) Discuss the framing technique used in HDLC. What is the effect of errors on this framing?
    (ii) The message 11001001 is to be transmitted, using CRC error deduction algorithm. Assuming the CRC polynomial to be X^3+1, determine the message that should be transmitted. If the second left most bit is corrupted, show that it is deducted by the receiver. **(13)**
19. (i) Discuss the principle of stop and wait flow control algorithm. Draw time line diagrams and explain how loss of a frame and loss of an ACK are handled. What is the effect of delay-bandwidth Product on link utilization? **(08)**
    (ii) Assume that a frame consists of 6 character encoded in 7 bit ASCII. Attach a parity bit of every character to maintain even parity. Also attach a similar parity bit for each bit position across each of the byte in the frame. Show that such a 2-dimensional parity scheme can deduct all 1 bit, 2-bit and 3-bit errors and can correct a single bit error. **(08)**
20. Explain with examples the two classes of transmission media. **(13)**
21. Describe with a neat diagram the layered architecture of the OSI model. **(13)**

UNIT II - MEDIA ACCESS & INTERNETWORKING

PART-A

1. **Define 802.11.**
   - 802.11 is an evolving family of specifications for wireless local area networks (WLANs) developed by a working group of the Institute of Electrical and Electronics Engineers (IEEE).
   - There are several specifications in the 802.11 family:
     802.11, 802.11a ,802.11b ,802.11e ,802.11g ,802.11n ,802.11ac ,802.11ac,802.11ad , 802.11ah,802.11r ,802.1X

2. **Define sub-netting in MAC layer.**
   - A sub network or subnet is a logical subdivision of an IP network. The practice of dividing a network into two or more networks is called sub netting.

3. Show the Ethernet frame format.

Ethernet Frame

62 bits	Preamble used for bit synchronization
2 bits	Start of Frame Delimiter
48 bits	Destination Ethernet Address
48 bits	Source Ethernet Address
16 bits	Length or Type
46 -1500 bytes	Data
32 bits	Frame Check Sequence

4. Highlight the characteristics of datagram networks.

- A host can send a packet anywhere at any time
- When a host sends a packet, it has no way of knowing if the network is capable of delivering it or if the destination host is even up and running
- Each packet is forwarded independently-two packets from host A to host B may follow different paths (due to a change in the forwarding table at some switch)
- A switch or link failure would not have any serious effect on communication if it is possible to find an alternate route around the failure and update the forwarding table accordingly

5. State the function of bridges.

The functions of Bridges are as follows.

- Bridges operate in both the physical and data link layers of the OSI model.
- Bridges can divide a large network into smaller segments.
- Bridges can also relay frames between two originally separate LANs.
- Bridges contain logic that allows them to keep the traffic for each segment separate.

6. What is meant by exponential backoff?

- Once an adaptor has detected a collision and stopped its transmission, it waits a certain amount of time and tries again.
- Each time it tries to transmit but fails, the adaptor doubles the amount of time it waits before trying again.
- This strategy of doubling the delay interval between each transmission attempt is a general technique known as exponential back off.

7. When is ICMP redirect message used?

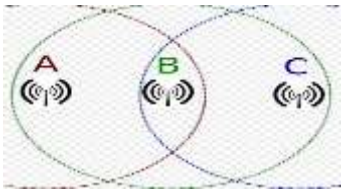
- ICMP – Internet Control Message Protocol.
- ICMP redirect is a mechanism for routers to convey routing information to hosts.
- The message informs a host to update its routing information (to send packets on an alternative route).
- If a host tries to send data through a router (R1) and R1 sends the data on another router (R2) and a direct path from the host to R2 is available (that is, the host and R2 are on the same Ethernet segment), then R1 will send a redirect message to inform the host that the best route for the destination is via R2.
- The host should then send packets for the destination directly to R2.

8. What is scatternet?

- A scatternet is a type of network that is formed between two or more Bluetooth-enabled devices, such as smartphones and newer home appliances. A scatternet is made up of at least two piconets.
- One Bluetooth devices can operate simultaneously on two piconets, acting as a bridge between the two. A conglomeration of two or more piconets is called a scatternet.

9. Define Hidden Node Problem.

- In wireless networks, when two terminals are not within the radio range to each other then they cannot transmit directly. This is called hidden terminal problem or hidden node problem.



- **Example:** Station A can communicate with Station B. Station C can also communicate with Station B. However, Stations A and C cannot communicate with each other since they cannot sense each other on the network, because they are out of range of each other.

10. What is Bluetooth?

- Bluetooth is a wireless technology standard for exchanging data over short distances (using short-wavelength UHF radio waves in the ISM band from 2.4 to 2.485 GHz) from fixed and mobile devices, and building Personal Area Networks (PANs).

11. What is the need for ARP?

- Address Resolution Protocol (ARP) is a protocol for mapping an Internet Protocol address (IP address) to a physical machine address that is recognized in the local network.
- For example, in IP Version 4, the most common level of IP in use today, an address is 32 bits long. In an Ethernet local area network, however, addresses for attached devices are 48 bits long.

12. What do you understand by CSMA protocol?

- Carrier Sense Multiple Access (CSMA): CSMA is a network access method used on shared network topologies such as Ethernet to control access to the network.
- Devices attached to the network cable listen (carrier sense) before transmitting.
- If the channel is in use, devices wait before transmitting. MA (Multiple Access) indicates that many devices can connect to and share the same network. All devices have equal access to use the network when it is clear.

13. What is the need of FH-SS in Bluetooth?

- The transmitted data are divided into packets.
- During each time slot, a sender transmits a packet on one of 79 channels based on pseudo-random manner from slot to slot.
- This form of channel hopping, known as Frequency Hopping – Spread Spectrum.

14. What is the access method used by wireless LAN?

- A Wireless Local Area Network (WLAN) is a wireless computer network that links two or more devices using a wireless distribution method (often spread-spectrum or OFDM radio) within a limited area such as a home, school, computer laboratory, or office building.
- This gives users the ability to move around within a local coverage area and still be connected to the network, and can provide a connection to the wider Internet. Most modern WLANs are based on IEEE 802.11 standards, marketed under the Wi-Fi brand name.
- The access methods used by wireless LANs are:
  - ✓ Frequency Hopping Spread Spectrum (FHSS)
  - ✓ Direct sequence Spread Spectrum (DSSS)

15. What is the average size of Ethernet frame?

- The original Ethernet IEEE 802.3 standard defined the minimum Ethernet frame size as 64 bytes and the maximum as 1518 bytes.
- The maximum was later increased to 1522 bytes to allow for VLAN tagging.
- The minimum size of an Ethernet frame that carries an ICMP packet is 74 bytes.

16. How is the minimum size of an Ethernet frame determined?

By defining the minimum Ethernet frame size, we ensure that all necessary information is being transferred at each transmission. The minimum frame size breaks down like this: Size is 64 bytes:

- Destination Address (6 bytes)
- Source Address (6 bytes)
- Frame Type (2 bytes)
- Data (46 bytes)
- CRC Checksum (4 bytes)
- 46 bytes must be transmitted at a minimum,
- It is additional pad bytes added to meet frame requirements

17. How does an FDDI node determine whether it can send asynchronous traffic?

- It allows each node to transmit a given amount of synchronous traffic each time it gets the token, and transmit some asynchronous traffic if there is any "time left over".
- Asynchronous bandwidth is allocated using an eight-level priority scheme. Each station is assigned an asynchronous priority level. FDDI (Fiber Distributed Data Interface) also permits extended dialogues, where stations may temporarily use all asynchronous bandwidth.
- The FDDI priority mechanism can essentially lock out stations that cannot use synchronous bandwidth and have too low an asynchronous priority. FDDI specifies the use of dual rings. Traffic on these rings travels in opposite directions. Physically, the rings consist of two or more point-to-point connections between adjacent stations. One of the two FDDI rings is called the primary ring; the other is called the secondary ring.

18. List the main limitations of bridges.

The main limitations of bridges are,

- First of all bridges are unable to read specific IP address; they are more concerned with the MAC addresses.
- Bridges cannot help to build a communication network between the networks of different architectures.
- Bridges transfer all types of broadcast messages, thus bridges are unable to limit the sco pe of these messages.
- Extremely large networks cannot rely on bridges; therefore the large networks as WAN which are IP address specific cannot make use of it.
- Bridges are expensive if we compare the prices of repeaters and hubs to it. Bridging is most suitable to be used for LAN network traffic data load.
- It is unable to handle more complex and variable data load such as occurring from WAN.

19. Define source routing.

- Source routing also called path addressing.
- This is a method that can be used to specify the route that a packet should take through the network.
- In source routing the path through the network is set by the source or a device that tells the network source the desired path.

20. List out the IEEE 802 standards with its name.

The IEEE 802 standards are,

- IEEE 802.1(LAN)
- IEEE 802.2(Logical Link Control)
- IEEE 802.3 (Ethernet)
- IEEE 802.4(Token bus)
- IEEE 802.5(Token Ring)
- IEEE 802.11(Wireless LAN)

21. How a single bit error does differ from a burst error?

Single bit error	Burst error
It means only one bit of data unit is changed from 1 to 0 or from 0 to 1	It means two or more bits in data unit are changed from 1 to 0 from 0 to 1
Single bit error can happen in parallel transmission where all the data bits are transmitted using separate wires.	Burst error is most likely to occur in a serial transmission.
The noise occurring for a longer duration affects only the single bit.	The noise occurring for a longer duration affects multiple bits. The number of bits affected depends on the data rate & duration of noise.
One bit error will occur per data unit	Two or more errors will occur per data unit

22. Define Bridge and Switch.

- A network bridge is a network device that connects multiple network segments. In the OSI model, bridging is performed in the first two layers, below the network layer. There are four types of network bridging technologies:
  - ✓ simple bridging,
  - ✓ Multiport bridging,
  - ✓ Learning or transparent bridging and
  - ✓ Source route bridging.
- A network switch (also called switching hub, bridging hub, officially MAC Bridge) is a computer networking device that connects devices together on a computer network, by using packet switching to receive, process and forward data to the destination device.

23. What is CSMA/CD?

- The Carrier Sense Multiple Access/Collision Detection, CSMA/CD is a Media Access Control (MAC) protocol that defines how network devices respond when two devices attempt to use a data channel simultaneously and encounter a data collision.
- The CSMA/CD rules define how long the device should wait if a collision occurs. The medium is often used by multiple data nodes, so each data node receives transmissions from each of the other nodes on the medium.

24. What are the advantages of FDDI over a basic Token Ring?

The advantages of FDDI over a basic Token Ring as,

- The Fiber Distributed Data Interface (FDDI) provides high-speed network backbones that can be used to connect and extend LANs.
- Like token ring, FDDI also has error-detection and correction capabilities. In a normally operating Fiber Distributed Data Interface (FDDI) ring, the token passes by each network device fast.
- If the token is not seen within the maximum amount of time that it takes to circulate the largest ring, it indicates a network problem.
- Fiber-optic cable such as the cable used with Fiber Distributed Data Interface (FDDI) can support very large volumes of data over large distances.

25. What is meant by ICMP and IGMP?

- The Internet Control Message Protocol (ICMP) is a mechanism used by hosts and routers to send notification of datagram problems back to the sender.
- The Internet Group Message Protocol (IGMP) has been designed to help a multicast router identify the hosts in a LAN that are members of a multicast group.

26. What are the uses of Bluetooth?

The uses of Bluetooth are,

- Bluetooth can be used to connect a mobile phone to a headset or a notebook computer to a keyboard.
- Bluetooth is a more convenient alternative to connecting two devices with a wire.
- Bluetooth links have typical bandwidths around 1 to 3 Mbps and a range of about 10 m.

27. What are the functions of MAC?

The functions of MAC layer are as follows.

- Frame delimiting and recognition.
- Addressing of destination stations (both as individual stations and as groups of stations)
- Conveyance of source-station addressing information.
- Transparent data transfer of LLC PDUs, or of equivalent information in the Ethernet sub layer.
- Protection against errors, generally by means of generating and checking frame check sequences.
- Control of access to the physical transmission medium.

28. What are the functions of LLC layer?

The functions of LLC are as follows.

- Protocol multiplexing
- Flow control
- Detection
- Error control through a retransmission of dropped packets when indicated.

29. What are the three pieces of information in the configuration messages?

The three pieces of information in the configuration messages are,

- The ID for the bridge that is sending the message.
- The ID for what the sending bridge believes to the root bridge.
- The distance, measured in hops, from the sending bridge to the root bridge.

30. Define Beacons.

- Beacons are small, often inexpensive devices that enable more accurate location within a narrow range than GPS, cell tower triangulation and Wi-Fi proximity.
- Beacons transmit small amounts of data via Bluetooth Low Energy (BLE) up to 50 meters, and as a result are often used for indoor location technology, although beacons can be used outside as well.
- Beacons are typically powered by small batteries, but they can be plugged into an outlet or USB port instead to maintain consistent power.
- In addition to standalone beacon devices, mobile phones, tablets and PCs with BLE support can all function as beacons, with the ability to both emit and receive beacon signals.

31. What is Broadcast?

- Broadcast is the term used to describe communication where a piece of information is sent from one point to all other points. In this case there is just one sender, but the information is sent to all connected receivers.
- Broadcast transmission is supported on most LANs (e.g. Ethernet), and may be used to send the same message to all computers on the LAN (e.g. the Address Resolution Protocol (ARP) uses this to send an address resolution query to all computers on a LAN).

PART B

1. i) Show and explain the Ethernet frame format. **(07)**

ii)Highlight the characteristics of connectionless networks. **(06)**

2. i)Write an algorithm for datagram forwarding in IP. **(07)**

ii) Show the ARP packet format. **(06)**

3. Explain the functions of Wi-Fi and Bluetooth in detail. **(13)**

4. Explain the datagram forwarding in IP. **(07)**

5. Show and explain the ARP packet format for mapping IP addresses into

6. Ethernet addresses. **(06)**

7. i) Draw the format of TCP packet header and explain each of its field. **(13)**

ii) Specify the justification for having variable field lengths for the fields in the TCP header. **(05)**

8. i) Discuss the working of CSMA/CD protocol. **(06)**

ii) Explain the functions of MAC layer present in IEEE 802.11 with necessary diagrams. **(07)**

9. i) Consider sending a 3500-byte datagram that has arrived at a router R_1 that needs to be sent over a link that has an MTU size of 1000 bytes to R_2. Then it has to traverse a link with an MTU of 600 bytes. Let the identification number of the original datagram be 465. How many fragments are delivered at the destination? Show the parameters associated with each of these fragments. **(06)**

ii) Explain the working of DHCP protocol with its header format. **(07)**

10. Explain the physical properties of Ethernet 802.3 with necessary diagram of Ethernet transceiver and adapter. **(13)**

11. With a neat sketch explain about IP service model, packet format, fragmentation and reassembly. **(13)**

12. Give the comparison between different wireless technologies? Enumerate 802.11 protocol stack in detail. **(13)**

13. Write short notes on Ethernet and wireless LAN. **(13)**

14. Explain in detail ARP,DHCP and ICMP. **(13)**

15. Explain in detail about the access method and frame format used in Ethernet and token ring. **(13)**

16. Briefly define key requirements of wireless LAN. **(08)**

17. Explain and differentiate FDDI and Ethernet. **(13)**

18. Write short notes on

i) Transparent bridges ii) MACA and MACAW **(13)**

19. Write short notes on:

i) FDDI ii) Bridges and Switches **(8+8)**

20. i) Describe the transmitter algorithm implemented at the sender side of the Ethernet Protocol. Why should Ethernet frame be 512 bytes long? **(08)**

ii) Explain how the hidden node exposed problem is addressed in 802.11? **(08)**

21. Describe how MAC protocol operates on a token ring. **(13)**

22. i) An IEEE 802.5 token ring has 5 stations and a total wire length of 230 m. How many bits of delay must the monitor insert into the ring? Calculate this for both 4 Mbps and 16 Mbps rings. The propagation speed may be assumed to be 2.3×10^8 m/s. **(08)**

ii)Discuss the problems encountered in applying CSMA/CD algorithm to wireless LANs. How do 802.11 specifications solve these problems? **(08)**

23. i) Discuss the limitations of bridges. **(08)**

ii) Determine the maximum distance between any of pair of stations in a CSMA/CD network with a data rate of 10 Mbps , for the correct operation of collision deduction process, assuming the minimum distance if the data rate is increased to 1 Gbps? 2 stations A and B, connected to opposite ends of a 10-Mbps CSMA/CD network, start transmission of long

frames at times t_1=0 and t_2=3ms respectively. Determine the instants when A hears the collision and B hears the collision. Signal propagation speed may be assumed as $2x10^8$ m/s. **(08)**

24. Define flow control and error control. Explain with illustrations the two mechanisms of flow control. **(13)**

25. Discuss about physical properties, and medium access protocol of Ethernet. **(13)**

26. Explain about physical properties, timed token algorithm, frame format of FDDI **(13)**

UNIT III ROUTING

PART-A

1. What are the benefits of Open Shortest Path First (OSPF) protocol?

- OSPF is a true LOOP- FREE (route-free loop) routing protocol. It is derived from the merits of the algorithm itself.
- Fast convergence of OSPF: The route changes can be transmitted to the entire autonomous system in the shortest time.
- The concept of area division is proposed. After the autonomous system is divided into different regions, the summary of routing information between the regions is adopted, which greatly reduces the quantity of routing information to be transmitted. It also makes routing information not expand rapidly as the network scale increases.

2. What is multicast routing?

- A multicast routing protocol is one type of service provider that functions as a client within the framework of the router architecture.
- The routing architecture is designed to be extended by such router client modules.
- A multicast routing protocol manages group membership and controls the path that multicast data takes over the network.
- Examples: Protocol Independent Multicast (PIM), Multicast Open Shortest Path First (MOSPF)

3. Differentiate between forwarding table and routing table.

- A routing table uses a packet's destination IP address to determine which IP address should next receive the packet, that is, the "next hop" IP address.
- A forwarding table uses the "next hop" IP address to determine which interface should deliver the packet to that next hop, and which layer 2 address (e.g., MAC address) should receive the packet on multipoint interfaces like Ethernet or Wi-Fi.

4. Define BGP.

- Border Gateway Protocol (BGP) is a routing protocol used to transfer data and information between different host gateways, the Internet or autonomous systems.
- BGP is a Path Vector Protocol (PVP), which maintains paths to different hosts, networks and gateway routers and determines the routing decision based on that.

5. How do routers differentiate the incoming unicast, multicast and broadcast IP Packets?

Routers will differentiate the incoming unicast, multicast and broadcast IP Packets based on the IP addresses.

Unicast: Both source and destination addresses are unicast addresses.

Multicast: The source and destination addresses are multicast addresses.

Broadcast: Both source and destination addresses are broadcast addresses.

6. Why is IPv4 to IPv6 transition required?

IPV4 is having the following drawbacks,

- It provides a very limited number of host and network addresses.
- The IP address is 32 bits long, the space of the IP address will be exhausted soon.
- The internet security issues won't be addressed by the IPV4 addresses.
- The IPV4 doesn't provide real time audio and video support, which is needed by the modern internet applications.

By considering these drawbacks, IPV6 was developed. So, the transition was required from IPV4 to IPV6.

7. Define VCI.

- Virtual Circuit Identifier (VCI) uniquely identifies the connection link at the switch and is carried inside the header of the packets that belong to this connection.
- It is a small number in a data frame changes from one switch to another switch used for data transfer.

8. What is fragmentation and reassembly?

- Fragmentation is the division of a datagram into smaller units to accommodate the Maximum Transmission Unit (MTU) of a data link protocol.
- The transport layer breaks a message into transmittable segments, numbers them by adding sequence numbers at the source and uses the sequence numbers at the destination to reassemble the original message.

9. Expand ICMP and write the function.

- The Internet Control Message Protocol (ICMP) is a supporting protocol in the Internet protocol suite.
- It is used by network devices, like routers, to send error messages operational information indicating, for example, that a requested service is not available or that a host or router could not be reached.

10. Write the types of connecting devices in internetworking.

The different types of connecting devices in internetworking are

- Network Interface Card (NIC)
- CSU/DSU (Channel Service Unit/Data Service Unit)
- Gateway
- Proxy
- Modem
- HUB
- Bridge
- Switch
- Router
- Brouters

11. Identify the class of the following IP address .

a) 110.34.56.45 - The Class A ranges from 0.0.0.0 to 127.255.255.255. This IP falls in Class A.

b) 212.208.63.23 - The Class C ranges from 128.0.0.0 to 223.255.255.255. This IP falls in Class C.

12. Define routing.

- Routing is the process of moving packets across a network from one host to another host. It is usually performed by dedicated devices called routers.

13. How does router differ from bridge?

- A router essentially determines which way is the shortest or fastest in a network, and routes packets accordingly. It works at layer 3 of the OSI model, moving packets from one port to another based on L3 addresses - ie. IP addresses, IPX addresses, etc.
- A bridge connects one point to another in a network. It works at layer 1 and 2 of the OSI model. It only connects two segments of the network.

14. What are the metrics used by routing protocol?

- Metrics are cost values used by routers to determine the best path to a destination network.
- The most common metric values are hop, bandwidth, delay, reliability, load, and cost.

15. Write the differences between circuit switching and packet switching.

The differences between circuit switching and packet switching are as follows.

S.No.	Circuit switching	Packet switching
1.	It involves dedicated transmission path	No dedicated transmission path
2.	Messages not stored here	Store and forward procedure is followed here
3.	Busy signal is introduced if called party is busy.	No busy signal here
4.	Blocking may occur	Blocking won't occur.
5.	No speed or code conversion.	Speed and code conversion will takes place here.
6.	Fixed bandwidth transmission.	Dynamic use of bandwidth.

16. What is the network address in a class A subnet with the IP address of one of the hosts as 25.34.12.56 and mask 255.255.0.0)?

The network address in a class A subnet with the IP address of one of the hosts as,

- Mask Address : 255.255.0.0
- IP Address : 25.34.12.56
- Network Address : 25.34.0.0

17. Compare circuit switching and virtual circuit based packet switching in respect of queuing and forwarding delays?

- In circuit switching, a dedicated path is established. Data transmission is fast and interactive. Nodes need not have storage facility. However, there is a call setup delay. In overload condition, it may block the call setup. It has fixed bandwidth from source to destination and no overhead after the call setup.
- In virtual-circuit packet switching, there is no dedicated path. It requires storage facility and involves packet transmission delay. It can use different speed of transmission and encoding techniques at different segments of the route.

18. What is the need of sub netting?

- Sub netting is used to partition a single physical network into more than one smaller logical sub-network (subnets). An IP address includes a network segment and a host segment.
- Subnets are designed by accepting bits from the IP addresses host part and using these bits to assign a number of smaller sub-networks inside the original network. Sub netting allows an organization to add sub-networks without the need to acquire a new network number via the Internet Service Provider (ISP).

19. What is the need for ARP?

- ARP is abbreviated as Address Resolution Protocol. This is used to find the physical address of the node when its Internet address is known.
- Anytime a host on its network, it formats an ARP query packet that includes the IP address and broadcasts it over the network.
- Every host on the network receives and processes the ARP packet, but only the intended recipient recognizes its internet address and sends back its physical address.

20. Expand and define MTU.

A Maximum Transmission Unit (MTU) is the largest size packet or frame, specified in octets (eight-bit bytes), that can be sent in a packet- or frame-based network such as the Internet. The Internet's Transmission Control Protocol (TCP) uses the MTU to determine the maximum size of each packet in any transmission.

21. Mention any four application of multicasting.

The main applications of multicasting are,

- Video server sending out networked TV channel
- Sending an e-mail message to a mailing list
- Videoconferencing
- Teleconferencing

22. Define internetworking.

- The Internetworking is the process or technique of connecting different networks by using intermediary devices such as routers or gateway devices.
- Internetworking ensures data communication among networks owned and operated by different entities using a common data communication and the Internet Routing Protocol.

23. Define sub netting.

- A subnetwork or subnet is a logical subdivision of an IP network. The practice of dividing a network into two or more networks is called subnetting.
- Computers that belong to a subnet are addressed with a common, identical, most-significant bit-group in their IP address.

24. What is meant by circuit switching?

- Circuit switching is a method of implementing a telecommunications network in which two network nodes establish a dedicated communications channel (circuit) through the network before the nodes may communicate.
- The defining example of a circuit-switched network is the early analog telephone network.

25. What is multicasting?

- A transmission method that allows copies of a single packet to be sent to a selected group of receivers.
- It is similar to broadcasting, but, where broadcasting requires that a packet be passed to all possible definitions.
- In computer networking, multicast (one-to-many or many-to-many distribution) is group communication where information is addressed to a group of destination computers simultaneously.
- Multicast should not be confused with physical layer point-to-multipoint communication.

26. What is the function of a router?

- Routers relay packets among multiple interconnected networks. They route packets from one network to any of a number of potential destination networks on the internet.
- A packet sent from a station on one network to a station on the neighboring network goes first to the jointly held router, which switches it over to the destination network.

27. What is the function of a gateway?

- A gateway can accept a packet formatted for one protocol and convert it to a packet formatted for another protocol before forwarding it. The gateway understands the protocols used by each network linked into the router and is therefore able to translate from one to another.
- While forwarding an IP packet to another network, the gateway might or might not perform Network Address Translation. A gateway is an essential feature of most routers, although other devices (such as any PC or server) can function as a gateway.

28. What is the router's role in controlling the packet lifetime?

- Each packet is marked with a lifetime as Time to Life (TTL) field; usually the number of hops that are allowed before a packet is considered lost and destroyed.
- Each router to encounter the packet subtracts 1 from the total before passing it on. When the lifetime total reaches 0, the packet is destroyed.

29. What is meant by flooding?

- In a network, flooding is the forwarding by a router of a packet from any node to every other node attached to the router except the node from which the packet arrived. Flooding is a way to distribute routing information updates quickly to every node in a large network.
- Flooding means that a router sends its information to all of its neighbors. Each neighbor sends the packet to all of neighbors and so on. Every router that receives the packet sends copies to all of its neighbors.

30. What are the rules of non-boundary-level masking?

- The bytes in the IP address that corresponds to 255 in the mask will be repeated in the sub network address.
- The bytes in the IP address that corresponds to 0 in the mask will change to 0 in the sub network address
- For other bytes, use the bit-wise AND operator.

31. What is a virtual circuit?

- A Virtual Circuit (VC) is a means of transporting data over a packet switched computer network in such a way that it appears as though there is a dedicated physical layer link between the source and destination end systems of this data.
- A logical circuit made between the sending and receiving computers.
- The connection is made after both computers do handshaking.
- After the connection, all packets follow the same route and arrive in sequence.

32. What is LSP?

- A Label Switched Path (LSP) is a path through an MPLS network, set up by a signaling protocol such as LDP, RSVP-TE, BGP or CR-LDP. The path is set up based on criteria in the FEC.
- The path begins at a [Label Edge Router] (LER), which makes a decision on which label to prefix to a packet, based on the appropriate FEC.
- In link state routing, a small packet containing routing information sent by a router to all other router by a packet called link state packet.

33. Specify the purpose of ICMP.

- The Internet Control Message Protocol (ICMP) is one of the core protocols of the Internet Protocol Suite.
- It is chiefly used by the operating systems of networked computers to send error messages – indicating, for instance, that a requested service is not available or that a host or router could not be reached.

PART-B

1. i) Explain the function of Routing Information Protocol(RIP) **(07)**
   ii) Draw the IPv6 packet header format. **(06)**
2. i) Explain the operation of Protocol-Independent Multicast (PIM) **(07)**
   ii)Out line the need of Distance Vector Multicast Routing Protocol(DVMRP). **(06)**
3. Outline the steps involved in building a computer network. Give the detailed description for each step. **(15)**
4. b) For the network given in Figure 1, give global distance - vector tables when
   (i) Each node knows only the distances to its immediate neighbors. **(05)**
   (ii) Each node has reported the information it had in the preceding step to its immediate neighbors. **(05)**
   (iii) Step (ii) happens a second time. **(05)**

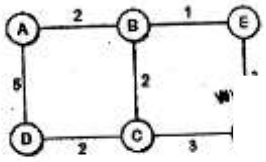


Figure 1

5. Elaborate on multicast routing protocols. **(13)**
6. With an example, explain the function of link state routing protocol. **(13)**
7. Explain in detail the operation of OSPF protocol by considering a suitable network. **(13)**

8. Explain the working of Protocol Independent Multicast (PIM) in detail. **(13)**

9. Discuss in detail about open source shortest path routing with neat diagrams. **(13)**

10. Discuss in detail about multicast routing with neat sketches. **(13)**

11. With a neat diagram explain Distance vector routing protocol. **(13)**

12. Explain about IPv6? Compare IPv4 and IPv6. **(13)**

13. i) Differentiate ARP and RARP. **(08)**

14. i) What is internet multicast? Explain in detail **(08)**

ii) Show the IPv6 header details and explain them. **(08)**

15. Explain the RIP algorithm with a simple example of your choice. **(16)**

16. i) Discuss the IP addressing methods. **(08)**

ii) Write short notes on ARP. **(08)**

17. i) Suppose hosts A and B have been assigned the same IP address on the same Ethernet, on Which ARP is used? B starts up after A. what will happen to A's existing connections? Explain how 'Self-ARP' might help with this problem. **(06)**

ii) Describe with example how CIDR addresses the two scaling concerns in the interact. **(13)**

18. i) A 4480-byte datagram is to be transmitted through an Ethernet with a maximum data size of 1500 bytes in frames. Show the values of Total Length, M flag, identification and fragment offset fields in each of the fragments created out of the datagram. **(06)**

ii) Discuss the principles of reliable flooding and its advantage and applications. **(13)**

19. i) For the following network, develop the datagram forwarding table for all the Nodes. The links are labeled with relative costs. The tables should forward each packet via the least cost path to destination. **(13)**

ii) What is the needed for ICMP? Mention any four ICMP messages and their purpose. **(06)**

20. What the algorithm does link state routing use to calculate the routing tables? Describe with example the link state routing algorithm. **(13)**

21. What are the three main elements of distance vector routing? Describe with example the distance vector routing algorithm. **(13)**

UNIT IV TRANSPORT LAYER

PART-A

1. What are the services provided by Transport layer protocol?

- The two major services provided at the transport layer are TCP and UDP.
- The TCP service provides reliability between sending and receiving, flow control, congestion control and is connection oriented.
- The UDP service does not provide reliable data transfer, flow control and is not connection-oriented, this allows it to have less overhead that a TCP connections

2. Define congestion control.

Congestion control refers to the techniques used to control or prevent congestion. Congestion control techniques can be broadly classified into two categories:

Types

- Open Loop Congestion Control
- Closed Loop Congestion Control

3. Compare flow control versus congestion control.

Basis for Comparison	Flow Control	Congestion Control
Basic	It controls the traffic from a particular sender to a receiver.	It controls the traffic entering the network.
Purpose	It prevents the receiver from being overwhelmed by the data.	It prevents the network from getting congested.
Responsibility	Flow control is the responsibility handled by data link layer and the transport layer.	Congestion Control is the responsibility handled by network layer and transport layer.
Responsible	The sender is responsible for transmitting extra traffic at receivers side.	The transport layer is responsible transmitting extra traffic into the network.
Preventive measures	The sender transmits the data slowly to the receiver.	Transport layer transmits the data into the network slowly.
Methods	Feedback-based flow control and Rate-based flow control	Provisioning, traffic-aware routing and admission control

4. What are the approaches used to provide a range of Quality of Service (QoS) ?

QoS is a collection of technologies which allows applications to request and receive predictable service levels in terms of data throughput capacity (bandwidth), latency variations (jitter), and delay. In particular, QoS features provide better and more predictable network service by the following methods:

- Supporting dedicated bandwidth.
- Improving loss characteristics.
- Avoiding and managing network congestion.
- Shaping network traffic.
- Setting traffic priorities across the network

5. List the advantages of connection oriented services and connectionless services.

Advantages of connection-oriented services:

- In connection-oriented virtual circuits, buffers can be reserved in advance.
- Sequencing can be guaranteed.
- Short-headers can be used.
- Troubles caused by delayed duplicate packets can be avoided.

Advantages of connectionless services:

- It can be used over subnets that do not use virtual circuit inside.
- No circuit set-up time required.
- It is highly robust in the face of router failures.
- It is best for connectionless transport protocols because it does not impose unnecessary overhead.

6. How do fast retransmit mechanism of TCP works?

The fast retransmit mechanism of TCP works as follows:

- If a TCP sender receives a specified number of acknowledgements which is usually set to three duplicate acknowledgements with the same acknowledge number (that is, a total of four acknowledgements with the same acknowledgement number), the sender can be reasonably confident that the segment with the next higher sequence number was dropped, and will not arrive out of order.
- The sender will then retransmit the packet that was presumed dropped before waiting for its timeout.

7. Differentiate between TCP and UDP.

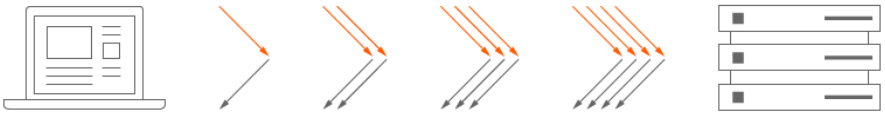
S.No	TCP –Transmission Control Protocol	UDP- User Datagram Protocol
1.	It is a connection oriented protocol.	It is a connection less protocol.
2.	It provides reliable delivery	It provides unreliable service.
3.	These are heavy weight	These are light weight.
4.	Sockets in TCP is usually identified by means of 4-tuple. 1. Source IP address 2. Source port number 3. Destination IP address 4. Destination port number	UDP socket is identified by means of two tuple are, 1. IP address (destination) 2. Port number (destination)

8. Give the comparison of unicast, multicast and broadcast routing.

S.NO	Unicasting	Multicasting	Broadcasting
1.	One source and one destination	One source and a group of destinations.	One source and all destination.
2.	Relationship is one- to-one	Relationship is one- to-many	Relationship is one- to- all.
3.	Both source and destination addresses are unicast addresses.	The source and destination addresses are multicast addresses.	Both source and destination addresses are broadcast addresses.
4.	In unicasting, the router forwards the received packet through only one of its interface.	In multicasting, the router forwards the received packet through several of its interfaces.	In broadcasting, the router forwards the received packet through all of its interfaces.

9. What do you mean by slow start in TCP congestion?

- TCP slow start is an algorithm which balances the speed of a network connection. TCP slow start is one of the first steps in the congestion control process.
- It balances the amount of data a sender can transmit (known as the congestion window) with the amount of data the receiver can accept (known as the receiver window).
- The lower of the two values becomes the maximum amount of data that the sender is allowed to transmit before receiving an acknowledgment from the receiver.
- Slow start gradually increases the amount of data transmitted until it finds the network's maximum carrying capacity.



10. List the different phases used in TCP connection.

The different phases used in TCP connection are,

- Connection Establishment
- Data Transfer
- Connection Termination

11. What do you mean by QOS?

- Quality of Service (QoS) refers to a network's ability to achieve maximum bandwidth and deal with other network performance elements like latency, error rate and uptime.
- Quality of service also involves controlling and managing network resources by setting priorities for specific types of data (video, audio, files) on the network.
- QoS is exclusively applied to network traffic generated for video on demand, IPTV, VoIP, streaming media, videoconferencing and online gaming.

12. What is the difference between congestion and flow control?

S.NO	Basis for Comparison	Flow Control	Congestion control
1.	Basic	It controls the traffic from a particular sender to a receiver.	It controls the traffic entering the network.
2.	Purpose	It prevents the receiver from being overwhelmed by the data.	It prevents the network from getting congested.
3.	Responsibility	Flow control is the responsibility handled by data link layer and the transport layer.	Congestion Control is the responsibility handled by network layer and transport layer.
4.	Responsible	The sender is responsible for transmitting extra traffic at receiver's side.	The transport layer is responsible transmitting extra traffic into the network.
5.	Preventive measures	The sender transmits the data slowly to the receiver.	Transport layer transmits the data into the network slowly.
6.	Methods	Feedback-based flow control and Rate-based flow control	Provisioning, traffic-aware routing and admission control

13. List some of the QOS parameters of transport layer.

The QOS parameters of transport layer are,

- Connection Establishment delay
- Connection establishment failure probability
- Throughput
- Transit delay
- Residual error ratio
- Protection , Priority , Resilience

14. Define slow start.

- Slow-start is part of the congestion control strategy used by TCP, the data transmission protocol used by many Internet applications.

- Slow-start is used in conjunction with other algorithms to avoid sending more data than the network is capable of transmitting, that is, to avoid causing network congestion.

15. How does transport layer perform duplication control?

- Sequence numbers help to uncover the duplication problems.
- The sender needs sequence numbers so that the receiver can tell if a data packet is a duplicate of an already received data packet.
- In the case of ACKs, the sender does not need this info (i.e., a sequence number on an ACK) to tell detect a duplicate ACK.
- A duplicate ACK is obvious to the receiver, since when it has received the original ACK it transitioned to the next state. The duplicate ACK is not the ACK that the sender needs and hence is ignored by the sender.

16. When can an application make use of UDP?

- Tunneling/VPN (lost packets are ok - the tunneled protocol takes care of it)
- Media streaming (lost frames are ok)
- Games that don't care if you get every update
- Local broadcast mechanisms (same application running on different machines "discovering" each other)
- UDP is suitable for purposes where error checking and correction is either not neces sary or is performed in the application, avoiding the overhead of such processing at the network interface level.

17. Define delay and Jitter.

- Delay: Is the amount of time data (signal) takes to reach the destination. Now a higher delay generally means congestion of some sort of breaking of the communication link.
- Jitter: Is the variation of delay time. This happens when a system is not in deterministic state eg. Video Streaming suffers from jitter a lot because the size of data transferred is quite large and hence no way of saying how long it might take to transfer.

18. Why UDP pseudo header is includes in UDP checksum calculation? What is the effect of an checksum at the receiving UDP

- The basic idea is that the UDP (User Datagram Protocol) checksum is a complement of a 16-bit one's complement sum calculated over an IP "pseudo-header" and the actual UDP data. The IP pseudo-header is the source address, destination address, protocol (padded with a zero byte) and UDP length.
- Example of this short packet is the source IP address is 152.1.51.27, and the destination IP address is 152.14.94.75. Divided into 16-bit quantities, these are 0x9801, 0x331b and 0x980e, 0x5e4b. If we add those together using two's complement (e.g. with Windows calculator), we get 0x1c175.

19. How can the effect of jitter be compensated? What type of application requires this compensation?

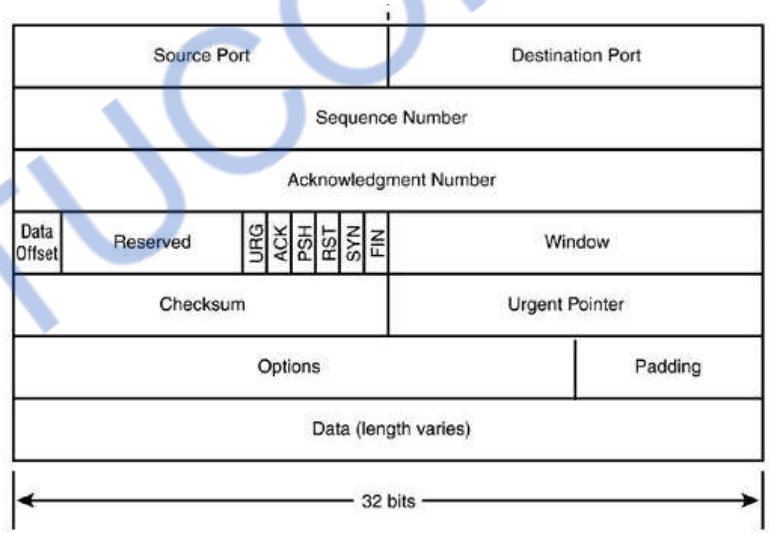
- When a router receives an audio stream for VoIP, it must compensate for any jitter that it detects. The playout delay buffer mechanism handles this function.
- Playout delay is the amount of time that elapses between the time a voice packet is received at the jitter buffer on the DSP and the time a voice packet is played out to the codec.

- The playout delay buffer must buffer these packets and then play them out in a steady stream to the DSPs.
- The DSPs then convert the packets back into an analog audio stream. The playout delay buffer is also referred to as the dejitter buffer.

20. What is the difference between end-to-end delivery in the transport layer and end-to-end delivery in the network layer?

S.No	Transport Layer	Network Layer
1.	Logical communication between processes.	Logical communication between hosts.
2.	Responsible for checking that data available in session layer are error free.	Responsible for logical addressing and translating logical addresses (ex. amazon.com) into physical addresses (ex. 180.215.206.136)
3.	Protocols used at this layer are : ➢ TCP(Transmission Control Protocol) ➢ UDP(User Datagram Protocol) ➢ SCTP(Stream Control Transmission Protocol)	Protocols used at this layer are : ➢ IP(Internet Protocol) ➢ ICMP(Internet Control Message Protocol) ➢ IGMP(Internet Group Message Protocol) ➢ RARP(Reverse Address Resolution Protocol) ➢ ARP(Address Resolution Protocol)
4.	This layer ensures that the protocols operated at this layer provide reliable end-to-end flow and error control.	This layer controls routing of data from source to destination plus the building and dismantling data packets.

21. Draw the TCP header format.



22. What is TCP?

- The reliable but complex transport layer protocol in the internet is called Transmission Control Protocol.
- It is a connection oriented protocol. TCP enables two hosts to establish a connection and exchange streams of data.
- TCP guarantees delivery of data and also guarantees that packets will be delivered in the same order in which they were sent.

23. Define Congestion.

- Congestion in a network occurs if user sends data into the network at a rate greater than that allowed by network resources.
- Congestion occurs because the switches in a network have a limited buffer size to store arrived packets.
- Network congestion is the situation in which an increase in data transmissions results in a proportionately smaller increase, or even a reduction, in throughput.

24. What are the advantages of using UDP over TCP?

The advantages of using UDP over TCP are,

- UDP does not need the overhead required to detect reliability.
- It does not need to maintain the unexpected deception of a data flow.
- UDP requires less processing at the transmitting and receiving of hosts
- It is simple to use for a network.
- Not need to maintain UDP connections information.

25. What factors determine the reliability of a delivery?

The factors determine the reliability of a delivery systems are,

- Error Control
- Sequence Control
- Loss Control
- Duplication Control

26. What are the five main categories of transport layer services?

They are the five main categories of transport layer services are,

- End to End Delivery
- Addressing
- Reliable Delivery
- Flow Control and
- Multiplexing

27. What are the fields in the TPDU?

The fields in the TPDU are,

- Length
- Fixed Parameters
- Variable Parameters and
- Data

28. Why there is a need for sequence control?

- On the sending node, the transport layer is responsible for ensuring that data units received from the upper layers are usable by lower layers.
- On the receiving end, it is responsible for ensuring that the various pieces of a transmission are correctly reassembled.

29. What is meant by segmentation and Concatenation?

- **Segmentation:** The size of the data unit received from the upper layer is too long for the network layer datagram or data link layer frame to handle, the transport protocol divides it into smaller usable blocks. The dividing process is called segmentation.

- **Concatenation**: The size of the data unit belonging to single sessions are so small that several can fit together into a single datagram or frame, the transport protocol combines them into a single data unit. The combining process is called concatenation.

30. What are the three events involved in the connection?

The three events involved in the connection are:

- Connection establishment
- Data transfer
- Connection release

31. List out the user related attributes.

There are different user related attributes. They are

- User related attributes are SCR
- Sustainable Cell Rate PCR
- Peak Cell Rate MCR
- Minimum Cell Rate CVDT
- Cell Variation Delay Tolerance.

32. What are the networks related attributes?

The network related attributes are,

- Cell loss ratio (CLR)
- Cell transfer delay (CTD)
- Cell delay variation (CDV)
- Cell error ratio (CER).

33. What is Silly Window Syndrome?

- If the sender or the receiver application program processes slowly and can send only 1 byte of data at a time, then the overhead is high.
- This is because to send one byte of data, 20 bytes of TCP header and 20 bytes of IP header are sent. This is called as silly window syndrome.

PART-B

1. Analyze various error detection techniques in transmission of data. **(15)**
2. Elaborate on TCp congestion control mechanisms. Differentiate these mechanisms. **(15)**
3. i)Explain how TCP manages a byte stream. **(07)**
   ii)Identify and explain the states involved in TCP. **(06)**
4. i)Explain any one TCP congestion avoidance mechanism. **(07)**
   ii)Brief about the approaches used to provide QoS support. **(06)**
5. i) Draw a TCP state transition diagram for connection management. **(07)**
   ii)Brief about approaches used for TCP congestion control. **(06)**
6. Write a detaled note on congestion avoidance mechanisms used in TCP. **(13)**
7. i) Explain the adaptive flow control and retransmission techniques used in TCP. **(08)**
   ii) With TCPs slow start and AIMD for congestion control, show how the window size will vary for a transmission where every 5th packet is lost. Assume an advertised window size of 50 MSS. **(05)**
8. i) Explain congestion avoidance using random early detection in transport layer with an example. **(07)**
   ii) Explain the differentiated services operation of QoS in detail. **(06)**

9. Explain various fields of the TCP header and the working of the TCP protocol. **(13)**

10. How is congestion controlled? Explain in detail about congestion control techniques in transport layer. **(13)**

11. Define UDP. Discuss the operations of UDP. Explain UDP checksum with one example. **(13)**

12. Explain in detail the various TCP congestion control mechanisms. **(13)**

13. With a neat architecture, explain TCP in detail. **(13)**

14. i) Explain the three way handshake protocol to establish the transport level connection. **(08)**

ii) List the various congestion control mechanisms and explain any one in detail. **(08)**

15. Explain the principles of congestion control in TCP. **(13)**

16. Discuss the Random Early Detection mechanism and derive the expression for drop probability. **(13)**

17. i) Describe how reliable and ordered delivery is achieved through TCP. **(08)**

ii) Why does TCP uses an adaptive retransmission and describes its mechanism. **(08)**

18. Describe with examples the three mechanisms by which congestion control is achieved in TCP. **(13)**

19. Suppose TCP operates over a 1-Gbps link, utilizing the full bandwidth continuously. How long will it take for the sequence numbers to wrap around completely? Suppose an added 32-bit timestamp field increments 1000 times during this wrap around time, how long will take for the timestamp filed to wrap around? **(13)**

20. What is the needed for Nagle's algorithm? How does it determine when to transmit data? **(13)**

21. A TCP machine is sending full windows of 65,535 bytes over a 1-Gbps network that has a 10-ms one –day delay. What is the throughput achievable? What is the efficiency of transmission? How many bits are needed in the Advertised window field of a proposed reliable byte stream protocol (like TCP) running over the above network, for achieving maximum efficiency? **(13)**

22. Illustrate the features of TCP that can be used by the sender to insert record boundaries into the bytes stream. Also mention their original purpose. **(13)**

23. What is the relationship between the ISDN layers and the OSI model layers? Explain with a neat diagram the layers of ISDN. **(13)**

24. Draw and Explain about TCP state transition diagram. **(13)**

25. Explain the following: i) DEC bit ii) RED **(13)**

UNIT V - APPLICATION LAYER

PART-A

1. Write the use of Hyper Text Transfer Protocol (HTTP).

- HTTP is a protocol designed to transfer information between computers over WWW (World Wide Web). Simply, HTTP (Hyper Text Transfer Protocol),
- It is used for transferring information like document, file, image, video between computers over internet.

2. What is DNS.

- The domain name system (DNS) is the way that internet domain names are located and translated into internet protocol (IP) addresses.
- The domain name system maps the name people use to locate a website to the IP address that a computer uses to locate a website.
- For example, if someone types TechTarget.com into a web browser, a server behind the scenes

will map that name to the IP address 206.19.49.149.

3. **What do you mean by web services Description Language (WSDL)?)**
   - WSDL stands for Web Services Description Language. It is a document written in XML. The document describes a Web service.
   - It specifies the location of the service and the operations (or methods) the service exposes. It contains set of definitions to describe a Web service.

4. **State the usage of conditional get in HTTP.**
   - The HTTP version 1.0 allows only three types of methods namely GET, POST and HEAD. But HTTP 1.1 specification allows for several additional methods including PUT and DELETE. The usual form of GET is

     GET filename HTTP / 1.1

     Where, **filename** names the **resource (file)** to be fetched.

5. **Present the information contained in a DNS resource record.**

   The information contained in a DNS resource record are as follows.
   - Each domain name is associated with resource record which contains set of information and server database also consists of resource record.
   - Each name server implements the zone information as a collection of RRs.
   - Domain name tells the domain to which this record applies.
   - Type and value field
   - Class field which identifies the protocol family
   - Time to live field which shows the valid time of resource record.

6. **Expand POP3 and IMAP4.**
   - **POP3:Post Office Protocol, Version 3:**

     POP3 is an extremely simple mail access protocol. It is defined in RFC 1939, which is short and quite readable and limited in functionality.
   - **IMAP4: Internet Mail Access Protocol, Version 4:**

     IMAP4 is another mail access protocol, which is defined in RFC 2060 and is more powerful and more complex. It assumes that all the e-mail will remain on the server indefinitely in multiple mail boxes.

7. **What is persistent HTTP?**
   - HTTP persistent connection, also called HTTP keep-alive, or HTTP connection reuse, is the idea of using a single TCP connection to send and receive multiple HTTP requests/ responses, as opposed to opening a new connection for every single request/response pair.

8. **Mention the different levels in domain name space (DNS).**

   The different levels in domain name space are
   - Domain name syntax
   - Top-level domains
   - Second-level and lower level domains

9. **Define URL**

- A URL (Uniform Resource Locator), is a text string used to identify the location of Internet resources. A typical URL looks like:

  http://www.annauniv.edu/index.html

In this URL, http is the protocol used to access the resource located on host www.annauniv.edu and immediately retrieve and display the file called index.html. These embedded URLs are called hypertext links.

10. Mention the types of HTTP message.

The four types of Hyper Text Transfer Protocol (HTTP) message headers are

- General-header: These header fields have general applicability for both request and response messages.
- Request-header: These header fields have applicability only for request messages.
- Response-header: These header fields have applicability only for response messages.
- Entity-header: These header fields define meta information about the entity-body or, if nobody is present, about the resource identified by the request.

11. What is SMTP?

- SMTP (Simple Mail Transfer Protocol) is a TCP/IP protocol used in sending and receiving e-mail. However, since it is limited in its ability to queue messages at the receiving end, it is usually used with one of two other protocols, POP3 or IMAP that let the user save messages in a server mailbox and download them periodically from the server.

12. What are the groups of HTTP header?

The groups of HTTP header are

- General format
- Field names
- Field values
- Size limits
- Request fields
- Response fields

13. State the difference between REST/HTTP and WSDL/SOAP.

The difference between REST/HTTP and WSDL/SOAP are a follows.

S.No	REST/HTTP REST – Representational State Transfer. HTTP – Hyper Text Transfer Protocol	WSDL/SOAP SOAP – Simple Object Access Protocol. WSDL – Web Service Description Language
1.	In the REST architecture, the protocol is always HTTP, so that source of interoperability problems is eliminated.	In the SOAP architecture, interoperability additionally depends on agreement on the protocol.
2.	HTTP has only a small set of methods, some of which are frequently blocked by firewalls.	WSDL has user defined operations.
3.	HTTP's own extensibility takes the form of headers, new methods, and new content types.	Protocol designers using WSDL/SOAP need to design such extensibility into each of their custom protocols.

14. List down the key lengths supported by PGP.

- Pretty Good Privacy (PGP) gives us choices for RSA and DSA key size ranging from 512 to 2048 or even 4096 bits.
- The larger the key, the more secure the RSA/DSA portion of the encryption.
- The only place where the key size makes a large change in the running time of the program is during key generation.

15. What is PGP?

- Pretty Good Privacy (PGP) is a popular program used to encrypt and decrypt email over the Internet, as well as authenticate messages with digital signatures and encrypted stored files.
- Pretty Good Privacy is a security protocol, which was invented by Phil Zimmermann to provide email with privacy, integrity, and authentication. PGP can be used to create secure e-mail messages.

16. What do you mean by TELNET?

- The word TELNET is derived by combining the Telecommunication and Network. Telnet is a protocol which provides the capability to log on to the remote computer. Hence it is called remote login. Telnet is a user command and an underlying TCP/IP protocol for accessing remote computers.
- Through Telnet, an administrator or another user can access someone else's computer remotely. On the Web, HTTP and FTP protocols allow you to request specific files from remote computers, but not to actually be logged on as a user of that computer.

17. What DNS cache issues are involved in changing the IP address of a web server host name?

- A DNS cache contains entries that translate Internet domain names to IP addresses. A DNS cache becomes poisoned (sometimes also called polluted) when unauthorized domain names or IP addresses are inserted into it.
- Occasionally, a cache may become corrupted due to technical glitches or administrative accidents, but DNS cache poisoning is typically associated with computer viruses or other attacks that insert invalid entries which redirect clients to malicious Web sites or other Internet servers.

18. Differentiate application programs and application protocols.

- AP: An application program (sometimes shortened to application) is any program designed to perform a specific function directly for the user or, in some cases, for another application program.
- Protocols: Communication on the Internet network is governed by various protocols. These protocols, or rules, spell out how the participants in various network processes should behave. Application protocol is one such protocol. Application protocols govern various processes, such as the process for downloading a web page, or for sending e-mail. The application protocol directs how these processes are done.

19. What are the advantages of allowing persistent TCP connection in HTTP?

The following are the advantages of allowing persistent TCP connection in HTTP,

- Lower CPU and memory usage (because fewer connections are open simultaneously).

- Enables HTTP pipelining of requests and responses.
- Reduced network congestion (fewer TCP connections).
- Reduced latency in subsequent requests (no handshaking).
- Errors can be reported without the penalty of closing the TCP connection.
- These advantages are even more important for secure HTTPS connections, because establishing a secure connection needs much more CPU time and network round-trips.

20. Is a cryptographic hash function, an irreversible mapping? Justify your answer.

- Yes, cryptographic hash function is an irreversible mapping.
- Cryptographic hash function is a combination of several components including a compression function which is made up of a few underlying elements such as Boolean functions and permutation. Some properties of Boolean functions are very helpful for determining sufficient conditions used in modern attack for hash functions.
- Two main cryptographic properties are studied for both elements namely Strict Avalanche Criterion (SAC) and randomness.

21. Compare and contrast the three types of www documents.

- **Static Documents** are fixed content documents that are created and stored in a server. The client can get only a copy of the document.
- **Dynamic Documents** do not exist in a predefined format. A dynamic document is created by a web server whenever a browser requests the document.
- **An active document** in the server is stored in the form of binary code. An active document is transported from the server to the client in binary form.

22. Why is an application such as POP needed for electronic messaging?

POP follows the simplistic idea that only one client requires access to mail on the server and that mails are best stored locally. This leads to the following advantages:

- Mail stored locally, i.e. always accessible, even without internet connection.
- Internet connection needed only for sending and receiving mail.
- Saves server storage space.
- Option to leave copy of mail on server.
- Consolidate multiple email accounts and servers into one inbox.

23. Define SNMP.

- SNMP (Simple Network Management Protocol) is an application-layer protocol that facilitates the exchange of management information between network devices. It is part of the Transmission Control Protocol/Internet Protocol (TCP/IP) suite.
- SNMP enables network administrators to manage network performance, find and solve network problems, and plan for network growth. SNMP plays an important role in managing networks.

24. State the purpose of SNMP.

- Simple Network Management Protocol (SNMP) is a popular protocol for network management. It is used for collecting information from, and configuring, network devices, such as servers, printers, hubs, switches, and routers on an Internet Protocol (IP) network.

Using SNMP, you can monitor network performance, audit network usage, detect network faults or inappropriate access, and in some cases configure remote devices.

- SNMP is designed to be deployed on the largest possible number of network devices, to have minimal impact on the managed nodes, to have minimal transport requirements, and to continue working when most other network applications fail.

25. What is the purpose of the Domain Name System?

- The Domain Name System (aka DNS) is used to resolve human-readable hostnames like www.Dyn.com into machine-readable IP addresses like 204.13.248.115.
- DNS also provides other information about domain names, such as mail services.

26. How does MIME enhance SMTP?

- MIME (Multipurpose Internet Mail Extensions) supplements SMTP and allows the encapsulation of multimedia (non-text) messages inside of a standard SMTP message. MIME uses Base64 encoding to convert complex files into ASCII.
- MIME is a relatively new standard, and although it is supported by almost all UA applications at this time, there might be a chance that our e-mail application does not support MIME. If that is the case, we will likely use one of the other encoding methods (Bin Hex or uuencode).MIME is described in RFCs 2045–2049.

27. Discuss the three main division of the domain name space.

- Domain name space is divided into three different sections: generic domains, country domains & inverse domain.
- **Generic domain:** Define registered hosts according to their generic behavior, uses generic suffixes.
- **Country domain:** Uses two characters to identify a country as the last suffix.
- **Inverse domain:** Finds the domain name given the IP address

28. Name the four factors needed for a secure network.

The four factors needed for a secure network are

- **Privacy:** The sender and the receiver expect confidentiality.
- **Authentication:** The receiver is sure of the sender's identity and that an imposter has not sent the message.
- **Integrity:** The data must arrive at the receiver exactly as it was sent.
- **Non-Reputation:** The receiver must able to prove that a received message came from a specific sender.

29. What are the advantages & disadvantages of public key encryption?

Advantages

- Remove the restriction of a shared secret key between two entities. Here each entity can create a pair of keys, keep the private one, and publicly distribute the other one.
- The no. of keys needed is reduced tremendously. For one million users to communicate, only two million keys are needed.

Disadvantage :

- If we use large numbers the method to be effective. Calculating the cipher text using the long keys takes a lot of time. So it is not recommended for large amounts of text.

30. What is a digital signature?

- Digital signature is a method to authenticate the sender of a message. It is similar to that of signing transactions documents when you do business with a bank.
- In network transactions, you can create an equivalent of an electronic or digital signature by the way you send data.

PART-B

1. Discuss the working of Email in detail. **(13)**

2. i) Tabulate the various HTTP request operations. **(07)**
ii)Draw the IMAP state transition diagram. **(06)**

3. i) Explain the function of Internet Message Access Protocol with a state diagram. **(08)**
ii) List and e>rplain the various HTTP request operations. **(05)**

4. What is Domain Name System (DNS) ? Explain. **(08)**
ii) Briefaboutthe importance of Simple Network Management ProtocoI (SNMP). **(05)**

5. Illustrate the sequence of events and the respective protocols involved while accessing a web page from a machine when it is connected with internet for first time. **(15)**

6. i) Describe how SMTP transfers message from one host to another with suitable illustration. **(06)**
ii) Explain IMAP with its state transition diagram. **(07)**

7. i) Explain in detail about SNMP messages. **(08)**
ii) Illustrate the role of POP3 in Electronic mail applications. **(08)**

8. Explain in detail about Web service architecture. **(13)**

9. Explain in detail about domain name system. **(13)**

10. Write short notes on Email and Web services. **(13)**

11. Explain the final delivery of email to the end user using POP3. **(08)**

12. Write notes on URLs. **(13)**

13. Describe the message format and the message transfer and the underlying protocol involved in the working of the electronic mail. **(13)**

14. Discuss the needed for name resolution. Illustrate the domain name hierarchy and the steps in resolution. **(13)**

15. i) Illustrate the features of FTP and its operation. **(08)**
ii) Illustrate the feature of TELNET. What is the needed for network virtual terminal? **(08)**

16. Discuss the importance of UAs, MTAs and relay MTAs in exchanging mail between users on the same or different computers. **(13)**

17. Explain the following **(13)**
(i) DNS (ii) FTP (iii) HTTP (iv) RTP

18. Discuss briefly about electronic Mail(SMTP, MIME and IMAP) **(4+4+5)**

19. Explain the following **(7+6)**
(i)PGP (ii) SSH

