

CS8591 – COMPUTER NETWORKS

UNIT I : INTRODUCTION AND PHYSICAL LAYER

PART – A (2 Marks)

1. Define – Data Communication (or) What is meant by data communication?

Data communication is defined as the exchange of data between two devices via some form of transmission medium in whatever form that is agreed upon by the parties creating and using the data.

2. What are the three criteria necessary for an effective and efficient network?

The three criteria necessary for the effective and efficient networks are

- a. Performance
- b. Reliability
- c. Security

3. What are the fundamental characteristics that determine the effectiveness of the data communication system?

The fundamental characteristics that determines the effectiveness of data communication system are

- a. Delivery
- b. Accuracy
- c. Timeliness
- d. Jitter

4. What are the advantages of distributed processing?

The advantages of the distributed processing are

- a. Security
- b. Encapsulation
- c. Distributed databases
- d. Faster problem solving
- e. Security through redundancy
- f. Collaborative processing

5. Define – Protocol

A protocol is a set of rules that govern data communication. It represents an agreement between the communicating devices. Without a protocol, two devices may be connected but not communicating with each other.

6. What are the five important component of the data communication? (or) Name the various components of data communication system.

The five important components of the data communication are

- a. Message
- b. Sender
- c. Receiver
- d. Transmission Medium
- e. Protocol

7. Name the four topologies used in the network.

The four topologies of a network are

- a. Ring
- b. Star
- c. Mesh
- d. Bus

8. Define – Computer network (or) Define – Network

A computer network is group of devices referred to as nodes connected by communication links. A node can be a computer, printer, or any other device capable of sending and/or receiving data generated by other nodes on the network.

9. What are the criteria to evaluate the transmission medium?

The criteria used to evaluate transmission medium are

- a. Throughput

- b. Propagation Speed
- c. Propagation Time
- d. Wavelength

10. What are the key elements of a protocol?

The Key elements of a protocol are

- a. Syntax
- b. Semantics
- c. Timing

11. Define – Link

Link is a physical medium that transfers data from one device to another

12 List the types of Link. (or)

What are the two types of line configuration?

The types of link or line configuration are

- a. Point to Point
 - i. Dedicated link between two devices
 - ii. Capacity reserved for two nodes
- b. Multipoint (or) multidrop
 - i. More than two devices connected
 - ii. Link and Capacity shared either spatially or temporally

13. Define – Flow control.

Flow Control refers to a set of procedures which is used to restrict the flow of data that the sender can send before waiting for acknowledgment.

14. Define – Error control.

Error control in the data link layer refers primarily to methods of error detection and retransmission and is based on automatic repeat request, which is the retransmission of data.

15. The transport layer creates a communication between the source and destination. What are the three events involved in the connection?

The three events involved in connection between the source and destination are

- a. Connection Establishment
- b. Data Transfer
- c. Connection Release

16. What are the modes for propagating light along optical channels?

There are two modes for propagating light along optical channels, multimode and single mode.

Multimode: Multiple beams from a light source move through the core in different paths.

Single mode: Fiber with extremely small diameter that limits beams to a few angles, resulting in an almost horizontal

17. What is the main function of physical layer?

The main functions of physical layer are

- a. Physical characteristics of interfaces and media
- b. Representation of bits
- c. Data rate
- d. Synchronization of bits
- e. Line configuration
- f. Physical topology
- g. Transmission mode

18. What is TCP/IP?

TCP/IP is a five-layer hierarchical protocol suite made up of interactive modules, developed before the OSI model. It is the internet model. The five layers are

- a. Physical
- b. data link (Host to network)
- c. Network (Internet)
- d. Transport

e. Application (session, presentation and application)

19. What is meant by circuit switching?

A circuit switched network is made of a set of switches connected by physical links, in which each link is divided into n channels. Circuit switching takes place at the physical layer. In circuit switching, the resources need to be reserved during the setup phase. The resources remain dedicated for the entire duration of data transfer phase until the teardown phase.

20. What is the role of DSL modem?

The role of Digital Subscriber Line (DSL) modem, is to provide high speed access to the Internet over the existing local loops. DSL technology is a set of technologies, each differing in the first letter (ADSL, VDSL, HDSL, and SDSL).

PART – B (16 Marks)

1. Explain in detail, the OSI-ISO reference model of a computer with neat diagram. (13)
2. Explain the TCP/IP reference model with neat sketch. (13)
3. Explain the different types of switching networks and list out its advantages and disadvantages. (13)
4. Explain the four basic network topologies and explain with its relevant features. (13)
5. Distinguish between point-to-point links and multi-point links with relevant diagram(13).
6. i) Compare connection oriented service with connection less service. (8)
ii) Compare the performance of TCP/IP (Internet model) with ISO/OSI reference model.(8)
7. i) Differentiate guided media from unguided media. (8)
ii) How is cable TV used for data transfer? Explain in detail. (8)
8. What are the different types of transmission media available? Explain the various standards of guided and unguided media. (13)

UNIT II : DATA LINK LAYER AND MEDIA ACCESS

PART – A (2 Marks)

1. What are the responsibilities of the Data Link Layer?

The responsibilities of data link layer are

- a. Framing
- b. Physical Addressing
- c. Flow Control
- d. Error Control
- e. Access Control

2. Write short notes on error correction.

Error correction is the mechanism used to correct the error and it can be handled in two ways

- a. When an error is discovered, the receiver can have the sender to retransmit the entire data unit.
- b. A receiver can use an error correcting code, which automatically corrects certain error.

3. Define – Flow control.

Flow Control refers to a set of procedures which is used to restrict the flow of data that the sender can send before waiting for acknowledgment.

4. Define Error control.

Error control in the data link layer refers primarily to methods of error detection and retransmission and is based on automatic repeat request, which is the retransmission of data.

5. What is a buffer?

Buffer is a device which has a block of memory, reserved for storing incoming data until they are processed.

6. What are the categories of flow control?

The two categories of flow control are

- a. Stop and Wait
- b. Sliding Window

7. What is the function of stop and wait protocol?

The function of stop and wait protocol is to transmit frame and wait for the acknowledgement before sending the next frame.

8. What is selective reject ARQ?

In selective reject ARQ only specific damaged or lost frame is transmitted. If a frame is corrupted in transit, a NAK (Negative Acknowledgement) is returned and the frame is resent out of sequence.

9. Define Automatic Repeat Request(ARQ).

Error Control in the data link layer is based on the Automatic Repeat Request, which means retransmission of data in three cases.

- a. Damaged Frame
- b. Lost Frame
- c. Lost Acknowledgement

10. What is the function of go-back N ARQ?

The function of go-back-N ARQ is to control the error in the continuous transmission.

11. Define HDLC (or) What is HDLC?

HDLC is a bit oriented protocol designed to support both half duplex and full duplex communication over point to point and multipoint links.

12. List the types of stations in HDLC.

The types of stations present in the HDLC are

- a. Primary
- b. Secondary
- c. Combined

13. Why Ethernet is said to be an I-persistent protocol?

Ethernet uses I-persistent protocol as the access method. In the I-persistent method, after the station finds the line idle, it sends its frame immediately with probability 1. This method has the highest chance of collision because two or more stations may find the line idle and send their frames immediately.

(or)

The Ethernet is said to be I-persistent protocol because a station with a frame to send transmits with probability 1 whenever a busy line goes idle.

14. What is CSMA/CD?

Carrier Sense Multiple Access with Collision Detection (CSMA/CD) augments the algorithm to handle the collision. In this method, a station monitors the medium after it sends a frame to see if the transmission was successful. If so, the station is finished. If there is a collision, the frame is sent again.

15. What are the differences between fast Ethernet and gigabit Ethernet?

Fast Ethernet	Gigabit Ethernet
---------------	------------------

Fast Ethernet is an improvement of Ethernet, which Gigabit Ethernet Network is an upgrade on Fast provides 100Mbps speed Ethernet.	Gigabit Ethernet provides 1000Mbps transmission in full-duplex and half-duplex.
Speed improvement over Ethernet is achieved by reducing the bit time (time taken to transmit one bit) to 0.01 microseconds	Although Gigabit Ethernet uses the same CSMA/CD and Ethernet framing format, it shows significant differences like slot time.
The physical media specifications are 100Base-T4, 100Base-TX, 100Base-FX.	The physical media specifications are 1000Base-LX, 1000Base-CX, 1000Base-TX

16. Define – Bluetooth

Bluetooth is a wireless LAN technology designed to connect devices of different functions such as telephones, notebooks, computers (desktop and laptop), cameras, printers etc. A Bluetooth LAN is an ad hoc network. Bluetooth communicates over short distance of 10m.

17. Define – Error detection and correction

Error detection and error correction are mechanisms of Error control. Error detection is a mechanism for detecting corrupted segments, lost segments, out-of-order segments, and duplicated segments. Error control also includes a mechanism for correcting errors after they are detected. Error detection and correction is achieved through the use of three simple tools: checksum, acknowledgment, and time-out.

18. What is the purpose of Network Interface Card?

A network interface controller (NIC, also known as a network interface card, network adapter, LAN adapter) is a computer hardware component that connects a computer to a computer network. Every network controller for an IEEE 802 network such as Ethernet, Wi-Fi, or Token Ring, and every FDDI network controller, has a unique 48-bit serial number called a MAC address, which is stored in read-only memory.

19. What are Virtual LANs?

Virtual local area network (VLAN) is a local area network configured by software, not by physical wiring. VLANs group stations belonging to one or more physical LANs into broadcast domains. The stations in a VLAN communicate with one another as though they belonged to a physical segment.

20. What are the different communication modes in HDLC?

The different communication modes in HDLC are

- a. Normal Response Mode (NRM)
- b. Asynchronous Response Mode (ARM)
- c. Asynchronous Balanced Mode (ABM)

21. List the types of frames in HDLC.

The types of frames available in HDLC are

- a. Information Frames (I-Frames)
- b. Supervisory Frames (S-Frames)
- c. Unnumbered Frames (U-Frames)

22. What are the uses of I, S and U frames?

The uses of I, S and U frames are

I frames: used to transport user data and control information relating to user data.

S frames: used only to transport control information, primarily data link layer and error controls.

U frames: reserved for systems management.

23. What is meant by bit stuffing?

Bit stuffing is the process of adding one extra 0 whenever there are 5 consecutive ones in the data so that the receiver doesn't mistake data for a flag.

24. Define – LAN

A Local Area Network (LAN) is a data communication system that allows a number of independent devices to communicate directly with each other in a limited geographic area.

25. List the types of architecture in a LAN.

The various LAN architectures are:

- a. Ethernet
- b. Token Bus
- c. Token Ring
- d. Fiber Distributed Data Interface (FDDI)

26. List the types of Ethernet Networks.

The types of Ethernet Networks are

- a. Switched Ethernet
- b. Fast Ethernet
- c. Gigabit Ethernet

27. What is piggy backing?

Piggybacking means, combining data to be sent and acknowledgement of the frame to be received in one single frame. It can save bandwidth because the overhead from a data frame and an ACK frame can be combined into just one frame.

28. Name the four types of S-frames.

The four types of S-frames are

- a. Receive Ready (RR)
- b. Receive Not Ready (RNR)
- c. Reject (REJ)
- d. Selective Reject (SREJ)

29. Name the five categories of U-frame.

The five categories of the U-frame are

- a. Mode Setting
- b. Unnumbered Exchange
- c. Disconnection
- d. Initialization Mode
- e. Miscellaneous Mode

30. What are the functions of bridges? or What is meant by bridge?

A bridge is a device that can connect segments of a network. A bridge operates in both the physical and the data link layer. The functions of bridges are:

- a. As a physical layer device, it regenerates the signal it receives.
- b. As a data link layer device, the bridge check the physical (MAC) addresses (source and destination) contained in the frame.

31. What are the functions of MAC?

The functions of MAC layer are

- a. It resolves the contention for the shared media.
- b. It contains the synchronization, flag, flow and error control specification necessary to move information from one place to another, as well as the physical address of the next station to receive and route a packet.

PART – B (16 Marks)

1. Explain the functioning of Wireless LANs in detail.(13)
2. List out the types of Ethernet. Explain in detail standard Ethernet and fast Ethernet in detail. (13)
3. Explain the flow and error control mechanisms in data link control. (13)
4. i) Explain the stop and wait protocol with a neat diagram. (7)
ii) Write short notes on Bluetooth technology. (7)
5. Explain DLC Services. (13)
6. Explain Data Link Layer Protocols (13)
7. Explain in detail about HDLC (13)

8. Explain MAC in detail (13)

UNIT - III : NETWORK LAYER

PART – A (2 Marks)

1. What are network support layers and user support layers?

Network Support Layers: The network support layers are Physical, Data Link and Network Layers. These layers deal with the electrical specifications, physical connection, transport timing and reliability.

User Support Layers: The user support layers are Session, Presentation and Application Layers. These allow interoperability among the unrelated software systems.

2. State the goals of Network layer (Or) What are the responsibilities of the network layer.

The Network Layer is responsible for the source to destination delivery of packet across multiple network links. The specific responsibilities of network layer includes

- a. Logical Addressing
- b. Routing

3. Define ICMP.

ICMP is a mechanism used by host and gateways to send query and error messages to the source of the datagram.

4. What is internetworking?

Internetworking is the process or technique of connecting different networks by using intermediary devices such as routers or gateway devices.

5. What is datagram approach?

In datagram approach, each packet is treated independently from all others. Even when a packet represents part of a multipacket transmission, the network treats it as if it exists alone. The individual packets travel different path. Packets in this technology are referred as datagram.

6. What is a router? (Or) What is the function or role of a router?

A router is a three layer device that routes packets based on their logical addresses i.e. host to host addressing. A router normally connects LANs and WANs in the internet and has a routing table that is used for making decisions about the route.

The function of a router is to

- a. Find a path between nodes in a network
- b. Route the packets across the path to their final destination

c. router that connects to the internet uses one private address and one global address.

7. Why is IPV6 preferred than IPV4?

IPV6 is preferred than IPV4 due to some deficiencies in IPV4 which becomes unsuitable for fast growing internet

The deficiencies in IPv4 are

- a. Address depletion is a long term problem in the internet.
- b. Lack of accommodation for real-time audio and video transmission.
- c. Lack of encryption and authentication of data for some application

8. What is IPV6?

IPv6 is the second network layer standard protocol that follows IPv4 for computer communications across the Internet and other computer networks. IPv6 offers several compelling functions that IPv4 cannot provide.

9. What is the use of Network Address Translation?

NAT (Network Address Translation) enables a user to have a large set of addresses internally and one address, or a small set of addresses, externally (public network). The traffic inside can use the large set, the traffic outside can use the small set.

10. What is meant by hop count?

Hop count is defined as the pathway requiring the smallest number of relays, in which every link is considered to be of equal length and give the value one.

11. How can a routing be classified?

The routing can be classified into two types

- a. Adaptive Routing
- b. Non Adaptive Routing

12. What is the time-to-live (TTL) or packet life time?

The time-to-live determines the life time of a packet. The time-to-live field of each such packet is marked with a life time. It is usually the number of hops that are allowed before a packet is considered lost and accordingly, destroyed.

13. Write the keys for understanding the distance vector routing.

The keys for understanding the algorithm are

- a. Knowledge about the neighbourhood.
- b. Routing only to immediate neighbours.
- c. Information (routing table) sharing at regular intervals.
- d. The shortest route is the route with minimum hop count. (N/D – 12 R08)

14. Write the keys to understand the link state routing.

The keys for understanding algorithm are:

- a. Knowledge about the whole networks.
- b. Routing to all neighbours.
- c. Information sharing where there is a change.
- d. The shortest route is the route with minimum cost metric.

15. How is the packet cost referred in distance vector and link state routing?

In distance vector routing, cost refer to the hop count while in the case of link state routing, cost is a weighted value based on a variety of factors such as security levels, traffic or the state of link.

16. How do routers get the information about the neighbours?

A router gets its information about the neighbours by periodically sending them short gesturing packets. If the neighbourhood responds to the greeting as expected, it is assumed to be alive and functioning. If it does not, a change is assumed to have occurred and the sending router alerts the rest of the network in its next LSP (Link State Packet).

17. What are the four internetworking device?

The four internetworking devices are

- a. Repeaters
- b. Bridges
- c. Routers
- d. Gateway

18. Define – IP address

IP address is a unique global logical address in the network. It is a 4-digit (32 bit in IPV4) number representing a host or a system in the network. One portion of the IP address indicates a networking and other represents the host in the network.

19. Define – Masking

Masking is the process that extracts the address of the physical network from an IP address.

20. Define – Gateway

Gateway is defined as a device used to connect two separate networks that use different communication protocols.

21. What is LSP?

Link State Packet (LSP) is a small packet containing routing information sent by a router to all other router in a link state routing.

22. What is meant by multicasting?

Multicasting is the delivery of a message or information to a group of destination computers simultaneously in a single transmission from the source. It is communication between one source and many destinations.

23. Define – Subnetting

Subnetting is dividing the large block of addresses into several contiguous groups and assigning each group to smaller networks called subnets. Subnetting increases the number of 1's in the mask.

24. What is multitasking?

The simultaneous execution of multiple tasks i.e. programs under the control of an interrupt driven operating system is called multitasking.

PART – B (16 Marks)

1. Write short notes on the following:
 - (i) Multicast routing(8)
 - (ii) Multicast routing protocol (7)
2. a) Explain the different classes of IP addressing (10)
b) What is the need for an IP address? (3)
3. Explain in detail the IPV6 addressing schemes, notation, representation and address space in detail. (13)
4. Explain in detail the ICMP message format and error reporting in detail. (13)
5. Draw the IPV4 header format and explain the various components and its role in that format. (13)
6. Explain in detail any one routing algorithm. (13)

UNIT - IV : TRANSPORT LAYER

PART – A (2 Marks)

1. What is function of transport layer?

The functions of transport layer protocols are

- a. It takes care of the delivery of data from one application program (service) on one device to an application program on another device.
- b. They act as a link between the upper layer protocols and the services provided by the lower layer.

2. What are the duties of the transport layer?

The duties of the transport layer are

- a. End (Process) -to - end delivery
- b. Port Addressing
- c. Reliable delivery
- d. Flow control
- e. Multiplexing
- f. Segmentation and Reassembly

3. What are the four aspects related to the reliable delivery of data?

The four aspects related to the reliable delivery of the data are

- a. Error control
- b. Sequence control
- c. Loss control
- d. Duplication control

4. What is a segment?

TCP divides long transmissions into smaller data units. It packages each into a frame called a segment.

When 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.

5. What is UDP?

User Datagram Protocol (UDP) is a connectionless, unreliable transport protocol. It does not add anything to the IP services. It provides process-to-process communication and performs limited error checking.

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

The advantages of using UDP over TCP are

- a. UDP is a very simple protocol using a minimum overhead.
- b. UDP is used to send a small message without reliability.
- c. UDP has less interaction between the sender and receiver while sending small messages, than using TCP or SCTP.

7. What is TCP?

TCP is a connection-oriented, reliable protocol. It creates a virtual connection between two TCP's to send data. TCP uses flow and error control mechanisms at the transport level.

8. List the services of TCP from the application program point of view.

The services of TCP from the application program point of view are

- a. Process-to-process communication
- b. Stream delivery service
- c. Sending and receiving buffers
- d. Segments
- e. Full-duplex communication

9. What is segmentation?

When 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.

10. What is Concatenation?

The size of the data unit belonging to a single session 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.

11. What are the types of multiplexing?

The types of multiplexing are

- a. Upward multiplexing
- b. Downward multiplexing

12. What are the two possible transport services?

Two basic types of transport services are

- a. Connection service
- b. Connectionless services

13. The transport layer creates the connection between source and destination. What are the three events involved in the connection?

The three events involved in the connection are

- a. Connection establishment
- b. Data transfer
- c. Connection release

14. What are the techniques used in multiplexing?

The three basic techniques of multiplexing are

- a. Frequency-division multiplexing
- b. Time-division multiplexing
- c. Wave-division multiplexing

15. What is meant by congestion? (Or) Define – Congestion

Congestion is the blockage in the network which reduces the throughput. Congestion in a network occurs if load on the network is greater than the capacity of the network.

16. Why does congestion occur in network?

Congestion occurs because the switches in a network have a limited buffer size to store arrived packets before and after processing.

17. How can the congestion be avoided?

The congestion can be avoided by two bits. The two bits are

- a. BECN - Backward Explicit Congestion Notification
- b. FECN - Forward Explicit Congestion Notification

18. What is Quality of Service (QoS)?

The Quality of Service (QoS) defines a set of attributes related to the performance of the connection. For each connection, the user can request a particular attribute; each service class is associated with a set of attributes. The attributes are

- a. Reliability
- b. Delay
- c. Jitter
- d. Bandwidth

19. Name the parameters of Quality of Service (QoS) in a network.

The parameters of Quality of Service (QoS) in a network are

- a. Reliability
- b. Delay
- c. Jitter
- d. Bandwidth

20. What are the two categories of QoS attributes?

The two main categories of QoS are

- a. User Oriented
- b. Network Oriented

21. What is queuing?

Packets from different flows arrive at a switch or router for processing. The routers and switches have queues (buffers) that hold the packets before and after processing. The scheduling method of processing the packets waiting in a queue is called as queuing.

Three types of queuing are FIFO queuing, priority queuing, and weighted fair queuing.

22. What are the techniques used to improve QoS in process-to-process delivery?

The techniques used to improve QoS are

- a. Scheduling
- b. Traffic shaping
- c. Admission control
- d. Resource reservation

23. What is a frame?

One complete cycle of time slots, including one or more slot dedicated to each sending device is known as frame.

24. What is interleaving?

Interleaving is the process in which the switch moves from device to device at a constant rate and fixed order.

25. What is framing bits?

One or more synchronization bits are usually added to the beginning of each frame. These bits are called framing bits.

PART – B (16 Marks)

1. Explain the segment formats for TCP and UDP. (13)
2. How is connection established and released in TCP? Explain with neat sketch. (13)
3. Explain the congestion control mechanism and transmission control protocol with neat sketches. (13)
4. Explain in detail, the TCP congestion avoidance algorithm. (13)
5. Explain the default timer mechanism followed in TCP. (13)
6. Explain in detail the user datagram protocol (UDP) in detail. (13)
7. Explain in detail, the transmission control protocol. (13)
8. Explain SCTP in detail (13).

UNIT - V : APPLICATION LAYER

PART – A (2 Marks)

1. What is the purpose of Domain Name System? (Or) State the role of DNS.

Domain Name System maps a name to an address (IP address) and conversely an address to name.

2. What is cryptanalysis?

Cryptanalysis refers to the science and art of breaking ciphers to gain as much information as possible about the original messages.

3. Define – Cryptography

Cryptography refers to the science and art of transforming messages to make them secure and immune to attack.

4. What is PGP?

Pretty Good Privacy (PGP) protocol provides security at the application layer. PGP is designed to create authenticated and confidential e-mails.

5. What is HTTP?

Hyper Text Transfer Protocol (HTTP) is a protocol which is used to access data on the World Wide Web (WWW). It functions as a combination of File transfer protocol (FTP) and Simple mail transfer protocol (SMTP).

6. List the multimedia applications.

The multimedia applications are

- a. Streaming stored audio/video
- b. Streaming live audio/video
- c. Real time interactive audio/video

7. What is TELNET?

TErminaLNEtwork (TELNET) is the standard TCP/IP protocol for virtual terminal service as proposed by ISO. TELNET is a general-purpose client/server application program. It enables the establishment of a connection to a remote system in such a way that the local terminal appears to be a terminal at the remote system.

8. What are the functionalities of TELNET? (N/D – 11 MCA) (Or) Name the function of TELNET.

TELNET enables the establishment of a connection to a remote system in such a way that the local terminal appears to be a terminal at the remote system.

9. State the purpose of SNMP.

Simple Network Management Protocol (SNMP) is a framework used for managing devices in an internet using the TCP/IP protocol suite. It provides a set of fundamental operations for monitoring and maintaining an internet.

10. Why is POP3 or IMAP4 needed for E-mail?

POP3 or IMAP4 is a client-server protocol. POP3 or IMAP4 for E-mail is needed by the client to pull messages i.e. retrieve messages from the server. The direction of the bulk data is from the server to the client. The POP3 or IMAP4 are message access agent protocols.

11. What is SMTP?

Simple Mail Transfer Protocol (SMTP) is a system for sending messages to other computer users based on e-mail addresses. It provides mail exchange between users on the same or different computers. Simple Mail Transfer Protocol (SMTP) is a formal protocol that defines the Message Transfer Agent (MTA) client and server in the internet. The mail transfer is done through MTA.

12. What are the three main division of the domain name space?

Three main division of the domain name space are generic domains, country domains and inverse domain.

a. **Generic domain:** Define registered hosts according to their generic behaviour, uses generic suffixes.

b. **Country domain:** Uses two characters to identify a country as the last suffix.

c. **Inverse domain:** Finds the domain name given the IP address.

13. Explain the TCP connections needed in FTP.

FTP establishes two connections between the hosts. One connection is used for data transfer, the other for control information. The control connection uses very simple rules of communication. The data connection needs more complex rules due to the variety of data types transferred.

14. What is the difference between a user agent (UA) and a mail transfer agent (MTA)?

The UA prepares the message, creates the envelope, and puts the message in the envelope. The MTA transfers the mail across the Internet.

15. How does MIME enhance SMTP?

MIME is a supplementary protocol that allows non-ASCII data to be sent through SMTP. MIME transforms non-ASCII data at the sender site to NVT ASCII data and delivers it to the client SMTP to be sent through the Internet. The server SMTP at the receiving side receives the NVT ASCII data and delivers it to MIME to be transformed back to the original data.

16. What is the purpose of HTML?

HTML (Hyper Text Markup Language) is a computer language for creating web pages. It specifies the contents and format of a web document. It allows additional text to include codes that define fonts, layouts, embedded graphics and hypertext links.

17. Define – CGI (Common Gateway Interface)

CGI is a set of standard that defines how a dynamic document is written, how data are input to the program, and how the output result is used. It is used for communication between HTTP servers and executable programs. It is used in creating dynamic documents.

18. Name four factors needed for a secure network.

The four factor that are needed for the secure network are

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

19. How is a secret key (symmetric) different from public key?

In **secret (symmetric) key**, the same key is used by both parties. The sender uses this key and an encryption algorithm to encrypt data. The receiver uses the same key and the corresponding decryption algorithm to decrypt the data.

In **public key**, there are two keys, a private key and a public key. The private key is kept by the receiver. The public key is announced to the public.

20. What is a digital signature?

Digital signature is a method to authenticate the sender of a message. Digital signature is a signature on a document, when verified, is a sign of sender.

PART – B (16 Marks)

1. Explain in detail, DNS and its frame format. (8)
2. What is the role of the local name server and the authoritative name server in DNS? What is the resource record maintained in each of them? (13)
3. Explain the SNMP. List out its uses, state strengths and weakness. (13)
4. Explain in detail, the HTTP and FTP with neat sketches. (13)
5. Explain e-mail in detail.(13)
6. Draw the architecture of WWW and explain in detail the various blocks. (13)