Computer Networks (18IT405) :: Short Answer Questions

UNIT-I

1. Define Network?

A network is a set of devices connected by physical media links. A network is recursively is a connection of two or more nodes by a physical link or two or more networks connected by one or more nodes.

2. What is point-point link?

If the physical links are limited to a pair of nodes it is said to be point-point link.

3. What is Multiple Accesses?

If the physical links are shared by more than two nodes, it is said to be Multiple Access.

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

a. Performance

It can be measured in many ways, including transmit time and response time.

b. Reliability

It is measured by frequency of failure, the time it takes a link to recover from a failure, and the network's robustness.

c. Security

Security issues include protecting data from unauthorized access and virus.

5. Name the factors that affect the performance of the network?

a. Number of Users

b. Type of transmission medium

c. Hardware

d. Software

6. Name the factors that affect the reliability of the network?

a. Frequency of failure

b. Recovery time of a network after a failure

7. What is Protocol?

A protocol is a set of rules that govern all aspects of information communication.

8. What are the key elements of protocols?

The key elements of protocols are

a. Syntax

It refers to the structure or format of the data, that is the order in which they

are presented.

b. Semantics

It refers to the meaning of each section of bits.

c. Timing

Timing refers to two characteristics: When data should be sent and how fast they can be sent.

9. What are the key design issues of a computer Network?

a. Connectivity

b. Cost-effective Resource Sharing

c. Support for common Services

d. Performance

10. What are the possible ways of data exchange?

(i) Simplex (ii) Half-duplex (iii) Full-duplex.

11. What are the important topologies for networks?

1. **BUS topology**: In this each computer is directly connected to primary network cable in a single line.

Advantages: Inexpensive, easy to install, simple to understand, easy to extend.

2. **STAR topology**: In this all computers are connected using a central hub.

Advantages: Can be inexpensive, easy to install and reconfigure and easy to trouble shoot physical problems.

3. **RING topology**: In this all computers are connected in loop.

Advantages: All computers have equal access to network media, installation can be simple, and signal does not degrade as much as in

other topologies because each computer regenerates it.

12. Define Bandwidth and Latency?

Network performance is measured in Bandwidth (throughput) and Latency (Delay). Bandwidth of a network is given by the number of bits that can be transmitted over the network in a certain period of time.

Latency corresponds to how long it takes a message to travel from one end off a network to the other. It is strictly measured in terms of time.

13. List the layers of OSI

a. Physical Layer

b. Data Link Layer

c. Network Layer

d. Transport Layer

e. Session Layer

f. Presentation Layer

g. Application Layer

14. Which layers are network support layers?

a. Physical Layer

b. Data link Layer and

c. Network Layers

15. Which layers are user support layers?

a. Session Layer

b. Presentation Layer and

c. Application Layer

16. Which layer links the network support layers and user support layers?

The Transport layer links the network support layers and user support layers.

17. What are the concerns of the Physical Layer?

Physical layer coordinates the functions required to transmit a bit stream over a physical medium.

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 are the responsibilities of Data Link Layer?

The Data Link Layer transforms the physical layer, a raw transmission facility, to a reliable link and is responsible for node-node delivery.

a. Framing

b. Physical Addressing

c. Flow Control

d. Error Control

e. Access Control

19. What are the responsibilities of Network Layer?

The Network Layer is responsible for the source-to-destination delivery of packet possibly across multiple networks (links).

a. Logical Addressing

b. Routing

20. What are the responsibilities of Transport Layer?

The Transport Layer is responsible for source-to-destination delivery of the entire message.

a. Service-point Addressing

b. Segmentation and reassembly

c. Connection Control

d. Flow Control

e. Error Control

21. What are the responsibilities of Session Layer?

The Session layer is the network dialog Controller. It establishes, maintains and synchronizes the interaction between the communicating systems.

a. Dialog control b. Synchronization

22. What are the responsibilities of Presentation Layer?

The Presentation layer is concerned with the syntax and semantics of the information exchanged between two systems.

a. Translation

b. Encryption

c. Compression

23. What are the responsibilities of Application Layer?

The Application Layer enables the user, whether human or software, to access the network. It provides user interfaces and support for services such as e-mail, shared database management and other types of distributed information services.

a. Network virtual Terminal

b. File transfer, access and Management (FTAM)

c. Mail services

d. Directory Services

24. What are the two classes of hardware building blocks?

Nodes and Links.

25. What are the categories of Transmission media?

a. Guided Media- i. Twisted - Pair cable

1. Shielded TP
2. Unshielded TP

ii. Coaxial Cable

iii. Fiber-optic cable

b. Unguided Media

i. Terrestrial microwave

ii. Satellite Communication

26. What are the types of errors?

a. Single-Bit error

In a single-bit error, only one bit in the data unit has changed

b. Burst Error

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

27. What is Error Detection? What are its methods?

Data can be corrupted during transmission. For reliable communication errors must be deducted and corrected. Error Detection uses the concept of redundancy, which means adding extra bits for detecting errors at the destination. The common Error Detection methods are

a. Vertical Redundancy Check (VRC)

b. Longitudinal Redundancy Check (VRC)

c. Cyclic Redundancy Check (VRC)

d. Checksum

28. What is Redundancy?

The concept of including extra information in the transmission solely for the purpose of comparison. This technique is called redundancy.

29. What is CRC?

CRC, is the most powerful of the redundancy checking techniques, is based on binary division.

30. What is Checksum?

Checksum is used by the higher layer protocols (TCP/IP) for error detection

31. What are the Data link protocols?

Data link protocols are sets of specifications used to implement the data link layer. The categories of Data Link protocols are

1. Asynchronous Protocols
2. Synchronous Protocols
    a. Character Oriented Protocols
    b. Bit Oriented protocols

32. Compare Error Detection and Error Correction:

The correction of errors is more difficult than the detection. In error detection, checks only any error has occurred. In error correction, the exact number of bits that are corrupted and location in the message are known. The number of the errors and the size of the message are important factors.

33. What is Forward Error Correction?

Forward error correction is the process in which the receiver tries to guess the message by using redundant bits.

34. Define Retransmission?

Retransmission is a technique in which the receiver detects the occurrence of an error and asks the sender to resend the message. Resending is repeated until a message arrives that the receiver believes is error-freed.

35. What is framing?

Framing in the data link layer separates a message from one source to a destination, or from other messages to other destinations, by adding a sender address and a destination address. The destination address defines where the packet has to go and the sender address helps the recipient acknowledge the receipt.

36. Define Character Stuffing?

In byte stuffing (or character stuffing), a special byte is added to the data section of the frame when there is a character with the same pattern as the flag. The data section is stuffed with an extra byte. This byte is usually called the escape character (ESC), which has a predefined bit pattern. Whenever the receiver encounters the ESC character, it removes it from the data section and treats the next character as data, not a delimiting flag.

37. What is Bit Stuffing?

Bit stuffing is the process of adding one extra 0 whenever five consecutive Is follow a 0 in the data, so that the receiver does not mistake the pattern 0111110 for a flag.

38. What is Flow Control?

Flow control refers to a set of procedures used to restrict the amount of data that the sender can send before waiting for acknowledgment.

39. What is Error Control?

Error control is both error detection and error correction. It allows the receiver to inform the sender of any frames lost or damaged in transmission and coordinates the retransmission of those frames by the sender. In the data link layer, the term error control refers primarily to methods of error detection and retransmission.

40. What Automatic Repeat Request (ARQ)?

Error control is both error detection and error correction. It allows the receiver to inform the sender of any frames lost or damaged in transmission and coordinates the retransmission of those frames by the sender. In the data link layer, the term error control refers primarily to methods of error detection and retransmission. Error control in the data link layer is often implemented simply: Any time an error is detected in an exchange, specified frames are retransmitted. This process is called Automatic repeat request (ARQ).

41. What is Stop-and-Wait Protocol?

In Stop and wait protocol, sender sends one frame, waits until it receives confirmation from the receiver (okay to go ahead), and then sends the next frame.

42. What is Sliding Window?

The sliding window is an abstract concept that defines the range of sequence numbers that is the concern of the sender and receiver. In other words, he sender and receiver need to deal with only part of the possible sequence numbers.

43. What is Stop-and-Wait Automatic Repeat Request?

Error correction in Stop-and-Wait ARQ is done by keeping a copy of the sent frame and retransmitting of the frame when the timer expires.

44. Difference between bit rate and baud rate.

Bit rate is the number of bits transmitted during one second whereas baud rate refers to the number of signal units per second that are required to represent those bits.

baud rate = (bit rate / N)

where N is no-of-bits represented by each signal shift.

45. What is MAC address?

The address for a device as it is identified at the Media Access Control (MAC) layer in the network architecture. MAC address is usually stored in ROM on the network adapter card and is unique.

UNIT-II

1. What is task of the network layer?

The network layer deals with end-to-end transmission.

2. What is Datagram?

Definition: A datagram is an independent, self-contained message sent over the network whose arrival, arrival time, and content are not guaranteed.

3. What is Bandwidth?

Every line has an upper limit and a lower limit on the frequency of signals it can carry. This limited range is called the bandwidth.

4. Define Routing?

The process of determining systematically hoe to forward messages toward the destination nodes based on its address is called routing.

5. What is a gateway or Router?

A node that is connected to two or more networks is commonly called as router or Gateway. It generally forwards message from one network to another.

6. What is a peer-peer process?

The processes on each machine that communicate at a given layer are called peer-peer process.

7. Define flooding.

Flooding means every incoming packet is sent out on every outgoing line except the one it arrived on.

8. Define the terms Unicasting, Multicasting and Broadcasting?

If the message is sent from a source to a single destination node, it is called Unicasting.

If the message is sent to some subset of other nodes, it is called Multicasting.

If the message is sent to all the m nodes in the network it is called Broadcasting.

9. What is multicast routing?

Sending a message to a group is called multicasting, and its routing algorithm is called multicast routing.

10. Define Congestion.

When too many packets are present in the subnet, performance degrades. This situation is called congestion.

11. Define Jitter.

The variation (i.e., standard deviation) in the packet arrival times is called **jitter**.

12. What is choke packet?

Choke packet technique is applicable to both virtual networks as well as datagram subnets. A **choke packet is a packet** sent by a node to the source to inform it of congestion. When the source host gets the choke packet, it is required to reduce the traffic sent to the specified destination by *X* percent.

13. What is load shedding?

Load shedding is a fancy way of saying that when routers are being overwhelmed by packets that they cannot handle, they just throw them away.

Old packets are better than new is often called **wine** and new packets are better than old is often called **milk**.

14. What is traffic shaping?

One of the main causes of **congestion** is that traffic is often busy. If hosts could be made to transmit at a uniform rate, congestion would be less common. Another open loop method to help manage congestion is forcing the packet to be transmitted at a more predictable rate. This is called traffic shaping.

15. What is ICMP?

ICMP is Internet Control Message Protocol, a network layer protocol of the TCP/IP suite used by hosts and gateways to send notification of datagram problems back to the sender. It uses the echo test / reply to test whether a destination is reachable and responding. It also handles both control and error messages.

16. What is difference between ARP and RARP?

The address resolution protocol (ARP) is used to associate the 32 bit IP address with the 48 bit physical address, used by a host or a router to find the physical address of another host on its network by sending a ARP query packet that includes the IP address of the receiver.

The reverse address resolution protocol (RARP) allows a host to discover its Internet address when it knows only its physical address.

17. What is the minimum and maximum length of the header in the TCP segment and IP datagram?

The header should have a minimum length of 20 bytes and can have a maximum length of 60 bytes.

18. What is the range of addresses in the classes of internet addresses?

Class A - 0.0.0.0 - 127.255.255.255

Class B - 128.0.0.0 - 191.255.255.255

Class C - 192.0.0.0 - 223.255.255.255

Class D - 224.0.0.0 - 239.255.255.255

Class E - 240.0.0.0 - 247.255.255.255

19. What is subnet?

A generic term for section of a large networks usually separated by a bridge or router.

UNIT-III

1. What is the task of the transport layer?

Its task is to provide reliable, cost-effective data transport from process to process communication.

2. What is SAP?

Series of interface points that allow other computers to communicate with the other layers of network protocol stack.

3. What is three-way hand shake method?

THREE-WAY HANDSHAKE or a TCP **3-way handshake** is a process which is used in a TCP/IP **network** to make a connection between the server and client. It is a **three**-step process that requires both the client and server to exchange synchronization and acknowledgment packets before the real data communication process starts

4. What is Round Trip Time?

The duration of time it takes to send a message from one end of a network to the other and back, is called RTT.

5. What is Multiplexing?

Multiplexing is the set of techniques that allows the simultaneous transmission of multiple signals across a single data link.

6. What is usage of Sequence Number in Reliable Transmission?

The protocol specifies that frames need to be numbered. This is done by using sequence numbers. A field is added to the data frame to hold the sequence number of that frame. Since we want to minimize the frame size, the smallest range that provides unambiguous communication. The sequence numbers can wrap around.

7. What are the data units at different layers of the TCP / IP protocol suite?

The data unit created at the **application layer** is called a message,

at the **transport layer** the data unit created is called either a segment or an user datagram,

at the **network layer** the data unit created is called the datagram,

at the **data link layer** the datagram is encapsulated in to a frame and finally transmitted as signals along the transmission media.

8. What are the uses of UDP?

UDP is widely used in the following

1. Remote Procedure Call (RPC)
2. Real Time Transport Protocol (RTP).
3. Domain Name System (DNS)

9. Define a Port.

A **port** is a communication endpoint. Each socket has a socket number (address) consisting of the IP address of the host and a 16-bit number local to that host, called a **port**.

10. What is silly window syndrome?

It is a problem that can ruin TCP performance. This problem occurs when data are passed to the sending TCP entity in large blocks, but an interactive application on the receiving side reads 1 byte at a time.

UNIT-IV

1. What is the function of DNS?

Domain Name Service (DNS) is the service used to convert human readable names of hosts to IP addresses.

2. Define Resource Record in DNS.

A resource record is a five tuple. Resource records are presented as ASCII text, one line per resource record. The format we will use is as follows:

Domain_name Time_to_live Class Type Value

3. Define MIME Protocol.

MIME is a kind of *add on or a supplementary protocol* which allows non-ASCII data to be sent through SMTP. It allows the users to exchange different kinds of data files on the Internet: audio, video, images, application programs as well.

4. Define SMTP Protocol.

Most of the internet systems use SMTP as a method to transfer mail from one user to another. SMTP is a push protocol and is used to send the mail.

5. Define POP3 Protocol.

Post Office Protocol version 3 (**POP3**) is a standard mail protocol used to receive emails from a remote server to a local email client. **POP3** allows you to download email messages on your local computer and read them even when you are offline.

6. Define IMAP Protocol.

IMAP (Internet Message Access Protocol) is a standard email protocol that stores email messages on a mail server, but allows the end user to view and manipulate the messages as though they were stored locally on the end user's computing device.

7. Write about WWW?

The World Wide Web (WWW) is a collection of documents and other web resources which are identified by URLs, interlinked by hypertext links, and can be accessed and searched by browsers via the Internet.

8. What is URL?

A Uniform Resource Locator (**URL**) is a reference to a web resource that specifies its location on a **computer network** and a mechanism for retrieving it.

9. Define HTTP Protocol.

Hyper Text Transfer Protocol -The communications protocol used to connect to Web servers on the Internet or on a local network (intranet). Its **primary function** is to establish a connection with the server and send HTML pages back to the user's browser.

10. Define FTP Protocol.

FTP stands for **File transfer protocol**. FTP is a standard internet protocol provided by TCP/IP used for transmitting the files from one host to another.

11. What is the difference between TFTP and FTP application layer protocols?

The Trivial File Transfer Protocol (TFTP) allows a local host to obtain files from a remote host but does not provide reliability or security. It uses the fundamental packet delivery services offered by UDP.

The File Transfer Protocol (FTP) is the standard mechanism provided by TCP / IP for copying a file from one host to another. It uses the services offer by TCP and so is reliable and secure. It establishes two connections (virtual circuits) between the hosts, one for data transfer and another for control information.

12. What is NVT (Network Virtual Terminal)?

It is a set of rules defining a very simple virtual terminal interaction. The NVT is used in the start of a Telnet session.