CS8591 - COMPUTER NETWORKS

UNIT I INTRODUCTION AND PHYSICAL LAYER 9

Networks – Network Types – Protocol Layering – TCP/IP Protocol suite – OSI Model – Physical Layer: Performance – Transmission media – Switching – Circuit-switched Networks – Packet Switching.

2 Marks

1. list the requirements to building a network

- Scalable Connectivity
- Cost-Effective Resource Sharing
- Support for Common Services
- Manageability

2. What is network software?

A general phrase for software that is designed to help set up, manage, and/or monitor computer networks. Networking software applications are available to manage and monitor networks of all sizes, from the smallest home networks to the largest enterprise networks

3. Write the parameters used to measure network performance (May 2016)

- Bandwidth and Latency
- Delay × Bandwidth Product
- High-Speed Networks
- Application Performance Needs

4. Define API

Application Programming Interface (Sockets)

The place to start when implementing a network application is the interface exported by the network. Since most network protocols are implemented in software, and nearly all computer systems implement their network protocols as part of the operating system, when we refer to the interface "exported by the network," we are generally referring to the interface that the OS provides to its networking subsystem. This interface is often called the network *application programming interface* (API)

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

The most important criteria are

- Performance
- Reliability
- Security.

Performance of the network depends on number of users, type of transmission medium, and the capabilities of the connected h/w and the efficiency of the s/w. *Reliability* is measured by frequency of failure, the time it takes a link to recover from the failure and the network's robustness in a catastrophe. *Security* issues include protecting data from unauthorized access and viruses.

6. Group the OSI layers by 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.*

7. What are the features provided by layering? (May2013) Two features:

- It decomposes the problem of building a network into more manageable components.
- It provides a more modular design.

8. Why are protocols needed?

In networks, communication occurs between the entities in different systems. Two entities cannot just send bit streams to each other and expect to be understood. For communication, the entities must agree on a protocol. A protocol is a set of rules that govern data communication.

9. What are the two interfaces provided by protocols?

- Service interface
- Peer interface

Service interface- defines the operations that local objects can perform on the protocol. Peer interface- defines the form and meaning of messages exchanged between protocol peers to implement the communication service.

10. Mention the different physical media?

- Twisted pair (the wire that your phone connects to)
- Coaxial cable (the wire that your TV connects to)
- Optical fiber (the medium most commonly used for high-bandwidth, long-distance links)

- Space (the stuff that radio waves, microwaves and infra red beams propagate through)

11. Explain the two types of duplex?

- *Full duplex*-two bit streams can be simultaneously transmitted over the links at the same time, one going in each direction.
- *Half duplex*-it supports data flowing in only one direction at a time.

12. What is spread spectrum and explain the two types of spread spectrum?

Spread spectrum is to spread the signal over a wider frequency band than normal in such a way as to minimize the impact of interference from other devices.

- Frequency Hopping
- Direct sequence

13. What are the different encoding techniques?

- NRZ
- NRZI
- Manchester
- 4B/5B

14. What are the responsibilities of data link layer?

Specific responsibilities of data link layer include the following.

a) Framing b) Physical addressing c) Flow control d) Error control e) Access control.

15. What are the ways to address the framing problem?

- Byte-Oriented Protocols(PPP)
- Bit-Oriented Protocols(HDLC)
- Clock-Based Framing(SONET)

16. Mention the types of errors and define the terms? (MAY 2012)

There are 2 types of errors

- Single-bit error.
- Burst-bit error.

Single bit error: The term single bit error means that only one bit of a given data unit (such as byte character/data unit or packet) is changed from 1 to 0 or from 0 to 1.

Burst error: Means that 2 or more bits in the data unit have changed from 1 to 0 from 0 to 1.

17. List out the available detection methods.

There are 4 types of redundancy checks are used in data communication.

- Vertical redundancy checks (VRC).
- Longitudinal redundancy checks (LRC).

- Cyclic redundancy checks (CRC).
- Checksum.

18. Write short notes on VRC.

The most common and least expensive mechanism for error detection is the vertical redundancy check (VRC) often called a parity check. In this technique a redundant bit called a parity bit, is appended to every data unit so, that the total number of 0"s in the unit (including the parity bit) becomes even.

19. Write short notes on LRC.

In longitudinal redundancy check (LRC), a block of bits is divided into rows and a redundant row of bits is added to the whole block.

20. Write short notes on CRC.

The third and most powerful of the redundancy checking techniques is the cyclic redundancy checks (CRC) CRC is based on binary division. Here a sequence of redundant bits, called the CRC remainder is appended to the end of data unit.

21. Write short notes on CRC checker.

A CRC checker functions exactly like a generator. After receiving the data appended with the CRC it does the same modulo-2 division. If the remainder is all 0"s the CRC is dropped and the data accepted. Otherwise, the received stream of bits is discarded and the dates are resent.

22. Define checksum.

The error detection method used by the higher layer protocol is called checksum. Checksum is based on the concept of redundancy.

23. What are the steps followed in checksum generator?

The sender follows these steps a) the units are divided into k sections each of n bits. b) All sections are added together using 2"s complement to get the sum. c) The sum is complemented and become the checksum. d) The checksum is sent with the data.

24. Write short notes on error correction? (NOV 2011)

It is the mechanism to correct the errors and it can be handled in 2 ways.

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

25. What is the purpose of hamming code?

A hamming code can be designed to correct burst errors of certain lengths. So the simple strategy used by the hamming code to correct single bit errors must be redesigned to be applicable for multiple bit correction.

26. What is redundancy?

It is the error detecting mechanism, which means a shorter group of bits or extra bits may be appended at the destination of each unit.

27. Define flow control? (NOV 2011)(May 2015) (May 2016)

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

28. Mention the categories of flow control?

There are 2 methods have been developed to control flow of data across communication links.

- Stop and wait - send one from at a time.
- Sliding window - send several frames at a time.

29. What is a buffer?

Each receiving device has a block of memory called a buffer, reserved for storing incoming data until they are processed.

30. What is the difference between a passive and an active hub?

An active hub contains a repeater that regenerates the received bit patterns before sending them out. A passive hub provides a simple physical connection between the attached devices.

31. For n devices in a network, what is the number of cable links required for a mesh and ring topology?

- Mesh topology – n (n-1)/2
- Ring topology – n

32. List the Channelization Protocols

- Frequency Division Multiple Access (FDMA)
  - The total bandwidth is divided into channels.
- Time Division Multiple Access (TDMA)
  - The band is divided into one channel that is time shared
- Code Division Multiple Access (CDMA)
  - One channel carries all transmission simultaneously

33. What are the two types of line configuration? (NOV 2010)

Point-to-point & Multipoint

34. What do you meant by error control? (NOV 2010)(May 2015)

Error control is used for detecting and retransmitting damaged or lost frames and to prevent duplication of frames. This is achieved through a trailer added at the end of the frame.

35. Define Error detection (NOV 2011)

Data can be corrupted during transmission. For reliable communication, errors must be detected and corrected Types of error:

- Single bit error Burst error
- The three error detecting techniques are: Parity check
- Check sum algorithm Cyclic Redundancy Check

36. What is the use of two dimensional parity in error detection? (NOV 2012)

It is based on simple parity.

It performs calculation for each bit position across each byte in the frame.

This adds extra parity byte for entire frame, in addition to a parity bit for each byte.

37. What are the issues (Services) in data link layer? (NOV 2012) (May 2016) (Nov 2016)

- Services Provided to the Network Layer
- Framing
- Error Control
- Flow Control

38. Define network and computer network

A **network** is any collection of independent computers that communicate with one another over a shared network medium. A **computer network** is a collection of two or more connected computers. When these computers are joined in a network, people can share files and peripherals such as modems, printers, tape backup drives, or CD-ROM drives.

39. List the components of data communication

Message Sender Receiver Medium Protocol

40. Define bit stuffing (MAY 2011)

Bit stuffing is the insertion of one or more bits into a transmission unit as a way to provide signaling information to a receiver. The receiver knows how to detect and remove or disregard the stuffed bits.

41. What are the major duties of network layer? (MAY 2012)

Logical addressing - If a packet passes the n/w boundary, we need another addressing system for source and destination called logical address.

Routing – The devices which connects various networks called routers are responsible for delivering packets to final destination.

42. What are the functions of application layer? (MAY 2011)

- **FTAM (file transfer, access, mgmt)** - Allows user to access files in a remote host.
- **Mail services** - Provides email forwarding and storage.
- **Directory services** - Provides database sources to access information about various sources and objects.

43. Define a layer. (Nov/Dec 2013)

The OSI (Open System Interconnection) Model breaks the various aspects of a computer network into seven distinct layers. Each successive layer envelops the layer beneath it, hiding its details from the levels above.

44. What do you mean by framing? (Nov/Dec 2013) (Nov/Dec 2014)

Frames are the small data units created by data link layer and the process of creating frames by the data link layer is known as framing What is protocol? What are its key elements? (NOV/DEC 2007) (May 2016)

Set of rules that govern the data communication is protocol. The key elements are
i) Syntax ii) Semantics iii) Timing

45. Define (or) mechanism of stop and wait protocol (Nov 2016)

The idea of stop-and-wait is straightforward: After transmitting one frame, the sender waits for an acknowledgment before transmitting the next frame. If the acknowledgment does not arrive after a certain period of time, the sender times out and retransmit the original frame.

46. Define sliding window algorithm

The sender can transmit several frames before needing an acknowledgement. Frames can be sent one right after another meaning that the link can carry several frames at once and its capacity can be used efficiently. The receiver acknowledges only some of the frames, using a single ACK to confirm the receipt of multiple data frames

47. Define character stuffing

The problem with the sentinel approach is that the ETX character might appear in the data portion of the frame. BISYNC overcomes this problem by "escaping" the ETX character by preceding it with a DLE (data-link-escape) character whenever it appears in the body of a frame; the DLE character is also escaped (by preceding it with an extra DLE) in the frame body. This approach is called character stuffing.

48. List the 7 OSI layers

- Physical Layer.
- Data link Layer.
- Network Layer.
- Transport Layer.
- Session Layer.
- Presentation Layer.
- Application Layer

49. Define hamming distance (Nov/Dec 2014)

Hamming distance = the number of bit positions in which two code-words differ. Eg. How to calculate ?(Exclusive OR=XOR):

10001001

10110001

00111000=> the number of 1"s give the number of different bits

16 – MARKS

1. Explain about Network Architecture with neat sketch on it.
2. Explain about OSI Architecture with neat sketch on it.
3. Explain about Internet Architecture with neat sketch on it.
4. Explain about Network software.
5. Explain about Performance of computer network.
6. Explain about Framing and its types.
7. Explain about Error Detection.
8. Explain about Reliable transmission or Flow Control.
9. Explain about requirement of building a network.
10. Problems on Bandwidth and Latency.

UNIT II DATA-LINK LAYER & MEDIA ACCESS

Introduction – Link-Layer Addressing – DLC Services – Data-Link Layer Protocols – HDLC – PPP - Media Access Control - Wired LANs: Ethernet - Wireless LANs – Introduction – IEEE 802.11, Bluetooth – Connecting Devices.

2-Marks

1. What are the functions of MAC?

MAC sub layer resolves the contention for the shared media. It contains synchronization, flag, flow and error control specifications 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.

2. What is Ethernet?

Ethernet is a multiple-access network, meaning that a set of nodes send and receive frames over a shared link.

3. Define Repeater?

A repeater is a device that forwards digital signals, much like an amplifier forwards analog signals. However, no more than four repeaters may be positioned between any pairs of hosts, meaning that an Ethernet has a total reach of only 2,500m.

4. Why Ethernet is said to be a I-*persistent* protocol?

An adaptor with a frame to send transmits with probability ,,1 ,,whenever a busy line goes idle.

5. What is exponential back off? (Nov 2016)

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.

6. What are the four prominent wireless technologies?

Bluetooth Wi-Fi (formally known as 802.11) WiMAX (802.16) Third generation or 3G cellular wireless.

7. Define Bluetooth? (May 2016)

Bluetooth fills the niche of very short-range communication between mobile phones, PDAs, notebook computers, and other personal or peripheral devices. For example, Bluetooth can be used to connect mobile phones to a headset, or a notebook computer to a printer.

8. Explain the term handoff?

If the phone is involved in a call at the time, the call must be transferred to the new base station in what is called a hand off.

9. What is the use of Switch?

It is used to forward the packets between shared media LANs such as Ethernet. Such switches are sometimes known by the obvious name of LAN switches.

10. What is meant by circuit switching? (NOV/DEC 2010)

Circuit switching is a process that establishes connections on demand and permits exclusive use of those connections until released.

11. What is Spanning tree?

It is for the bridges to select the ports over which they will forward frames. A spanning tree is a sub graph of this graph that covers (spans) all the vertices but contains no cycles. That is, a spanning tree keeps all of the vertices of the original graph but throws out some of the edges

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

- 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.

13. What is broadcast?

Broadcast is simple – each bridge forwards a frame with a destination broadcast address out on each active (selected) port other than the one on which the frame was received.

14. What is multicast?

It can be implemented with each host deciding for it whether or not to accept the message.

15. How does a given bridge learn whether it should forward a multicast frame over a given port?

It learns exactly the same way that a bridge learns whether it should forward a unicast frame over a particular port- by observing the source addresses that it receives over that port.

16. Differentiate fast Ethernet and gigabit Ethernet. (NOV/DEC 2012)

Fast Ethernet cards connect to networks at a rate of 100 Mbps while Gigabit network cards can connect at speeds up to 1000mb/s. The main difference between the two is speed. A fast Ethernet card can run on bandwidths at 100mb/s while a gigabit Ethernet can run at ten times that speed. However, the existence of FDDIs around made this technology more like a stepping stone to something better – enter the gigabit card. Gigabit networks are made to run the best at Layer
3 switching meaning it have more route functionality than the 100mbs fast Ethernet.

17. What is Transceiver?

Transceiver is a device which connects host adaptor to Ethernet Cable. It receives and sends signal

18. What is the difference between switch and bridge? (NOV/DEC 2012)

Bridge	Switch
A bridge is device which operates at the data link layer. It may be used to join two LAN segment(A,B),Constructing a larger LAN	A bridge with more than two interfaces (Ports) is also known as a switch.
Bridges receive Ethernet frames then forward all frames, like a repeater	A switch, on the other hand, forward the frame to only the required interfaces
Bridges learns the association between the system MAC addresses and the interface ports.	The switch reduces the number of packets on the other LAN segments, by sending the packet only where it need to go.

19. Define bridge and switch. (NOV/DEC 2012)

- Bridges are software based ,while switches are hardware based
- Bridges can only have one spanning –tree instance per bridge, while switches can have many
- Bridges can only have up to 16 ports, whereas a switch can have hundreds.

20. State the difference between token ring and FDDI? (NOV/DEC 2010)

Token ring	FDDI
It uses shielded twisted pair cables It uses Manchester encoding It supports data rate upto 16Mbps It is implemented as a ring, switch or multi-station access unit	It uses fibre optic cables. It uses 4B/5B before NRZ-1 for encoding It supports data rate upto100 Mpbs It is implemented as dual ring, nodes with single attachment station and dual attachment station with concentrator.

21. Define a Bridge. (NOV/DEC 2010)

A network bridge is an abstract device that connects multiple network segments along the data link layer. A concrete example of a bridge in a computer network is the network switch.

22. A network with bandwidth of 10 Mbps can pass only an average of 12,000 frames per minute with each frame carrying an average of 10,000 bits. What is the throughput of this network? (APRIL/MAY 2011)

Throughput= (12,000*10,000)/60=2Mb

ps. It is 1/5 of bandwidth.

23. What is the role of VCI?

A virtual channel identifier (VCI) distinguishes virtual channels (also known as circuits) created in a packet/cell switched network. A VCI has multiple circuits per communication channel and is primarily used for managing the unique identification of each created circuit.

A VCI is also known as a virtual circuit identifier (VCI).

24. List the two main limitations of bridges. Nov/Dec 2013

- Limited scalability to O(1,000) hosts not to global networks
- Not heterogeneous no translation between frame formats
-

25. Define source routing. Nov/Dec 2013

Source routing allows a sender of a packet to partially or completely specify the route the packet takes through the network.

Source routing allows easier troubleshooting, improved trace route, and enables a node to discover all the possible routes to a host. It does not allow a source to directly manage network performance by forcing packets to travel over one path to prevent congestion on another.

26. Why should Ethernet frame should be 512 bytes long?

A Valid collision can only happen within the first 512 bits of frame transmission. The 512 bits include 12 bytes of addresses, plus 2 bytes used in the type/length field, plus 46 bytes of data, plus 4 bytes of FCS. The preamble is not considered part of the actual frame in these calculations.

27. Define ICMP? (Or) Expand ICMP and write the function (May 2016)

Internet Control Message Protocol is a collection of error messages that are sent back to the source host whenever a router or host is unable to process an IP datagram successfully

28. Define Subnetting? (Nov 2015)

Subnetting provides an elegantly simple way to reduce the total number of network numbers that are assigned. The idea is to take a single IP network number and allocate the IP address with that network to several physical networks, which are now referred to as subnets.

29. What is CIDR? (MAY/JUNE2007)

Classless Inter-Domain Routing (CIDR) is a methodology of allocating and routing packets. It was introduced in 1993 to replace the prior addressing architecture of design in the with the goal to slow the growth of routing tables on routers across the Internet, and to help slow the rapid of addresses, uses a syntax of specifying IP addresses for IPv4 and IPv6, using the base address of the network followed by a slash and the size of the routing prefix, e.g., 192.168.0.0/16 (IPv4), and 2001:db8:: /32 (IPv6).

30. What is (Differ) ARP and RARP? (MAY/JUNE 2009)

ARP stands for Address Resolution Protocol. It is used to convert IP address to Physical address RARP stands for Reverse Address Resolution Protocol. It is used to convert Physical address into IP address.

31. What is DHCP? (NOV/DEC 2012)

Dynamic Host Configuration Protocol (DHCP) is a protocol designed to provide information dynamically.
It is a client-server program.
DHCP is used to assign addresses to a host dynamically. Basically, DHCP server has two databases.
The first database is addresses to IP addresses.

32. What are the salient features of IPV6? (NOV/DEC 2012)

- New Packet Format and Header
- Large Address Space
- State full and Stateless IPv6 address
- Multicast
- Integrated

33. Give the CIDR notation for class A, B and C. APR/MAY 2011)

Class	Binary	Dotted-Decimal	CIDR
A	11111111 00000000 00000000	255.0.0.0	/ 8
B	00000000	255.255.0.0	/ 16
C	11111111 11111111 00000000	255.255.255.0	/ 24

	00000000 11111111 11111111 11111111 00000000		

34. What is IP addressing?

Internet address or IP address is 32 bit identifier that uniquely and universally defines a host or router connected to the internet.

35. What is the need of subnetting (NOV/DEC 2013)

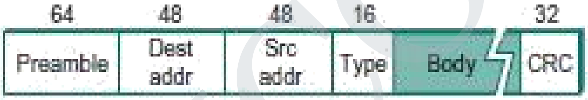
Subnetting is the technique used to break down networks into subnets. With the advent of internet, IP based networks become hugely popular. Due to this available IP addresses depleted at huge rate. To overcome this shortage concept of subnetting was introduced. Subnetting removes the classification of IP addresses according to classes and helps in creating further subnetworks from existing range of a IP network range.

For e.g A class B IP address can be broken down into further smaller networks.

36. What is the need for ARP? (NOV/DEC 2013) (Nov 2015)

Address Resolution Protocol (ARP) is a protocol for mapping an Internet Protocol

37. Draw Ethernet frame format



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. (The physical machine address is also known as a Media Access Control or MAC address.) A table, usually called the ARP cache, is used to maintain a correlation between each MAC address and its corresponding IP address. ARP provides the protocol rules for making this correlation and providing address conversion in both directions.

38. Define collision detection?

In Ethernet, all these hosts are competing for access to the same link, and as a consequence, they are said to be in the same collision detection.

39. What are the four steps involves in scanning?

The technique for selecting an AP is called *scanning* and involves the following four steps:

The node sends a Probe frame.

All APs within reach reply with a Probe Response frame.

The node selects one of the access points, and sends that AP an Association Request frame.

The AP replies with an Association Response frame.

40. Define Piconet

The basic Bluetooth network configuration, called a *piconet*, consists of a master device and up to seven slave devices

41. Differentiate persistent and non persistent CSMA (Nov/Dec 2014) In 1-persistent CSMA if the medium is busy, the channel will be sensed until it is idle, then it will transmit immediately. This means that collisions are almost guaranteed to occur.

In non-persistent CSMA if the medium is busy, there will be a random delay for retransmission. This reduces the probability of collisions, but wastes the capacity.

42. State the uses of valid transmission timer (Nov/Dec 2014)

The Valid Transmission Timer (TVX) times the period between correct frame transmissions, therefore is a check for faults on the ring. If it expires then a new claim process begins

43. What do you understand by CSMA protocol? (May 2015)

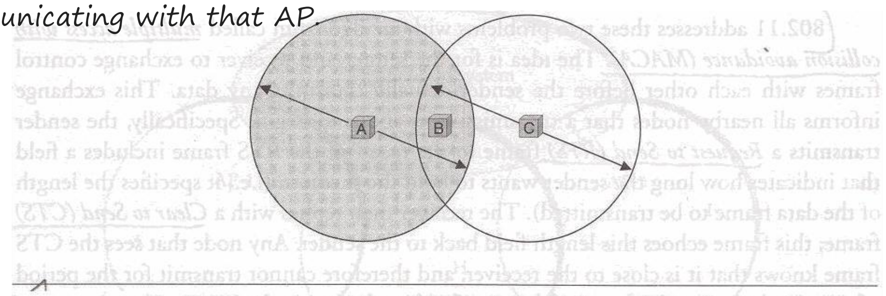
Carrier Sense Multiple Access is a probabilistic Media Access control (MAC) protocol in which a node verifies the absence of other traffic before transmitting on a shared transmission medium, such as an electrical bus

44. List the functions of bridges (May 2015)

35. Pass data frames between networks using MAC address
36. Break up collision domains
37. Forwards all broadcast messages

45. Define hidden node problem (May 2016)

In wireless networking, the hidden node problem or hidden terminal problem occurs when a node is visible from a wireless access point (AP), but not from other nodes communicating with that AP.



The hidden node problem. Although A and C are hidden from each other, their signals can collide at B. (B's reach is not shown.)

46. What is scatternet? (Nov 2016)

The bluetooth network consisting of one or more piconets is known as scatternet. The devices in one piconet type may function as master or slave in another piconet type of the same scatternet

47. Identify the class of the following IP address: (a) 110.34.56.45 (b) 212.208.63.23 (Nov 2015)

110.34.56.45 - Class A
212.208.63.23 - Class C

48. What is fragmentation and reassembly?

IP fragmentation is an Internet Protocol (IP) process that breaks datagrams into smaller pieces (fragments), so that packets may be formed that can pass through a link with a smaller maximum transaction unit (MTU) than the original datagram size. The fragments are reassembled by the receiving host.

16 – MARKS

1 .Explain about Ethernet (802.3).

2. Explain about Wi- Fi (802.11).

3. Explain about Bluetooth with its architecture.

4. Explain about Switching and Bridging.

5. Explain about Internet Protocol.

6. Explain about ARP.

7. Explain about CIDR.

8. Explain about DHCP.

9. Explain about ICMP.

10. Problems about Ethernet LAN.

UNIT III NETWORK LAYER 9

Network Layer Services – Packet switching – Performance – IPV4 Addresses – Forwarding of IP Packets - Network Layer Protocols: IP, ICMP v4 – Unicast Routing Algorithms – Protocols – Multicasting Basics – IPV6 Addressing – IPV6 Protocol.

2 Marks

1. **Define packet switching?**

A packet switch is a device with several inputs and outputs leading to and from the hosts that the switch interconnects.

2. **What is a virtual circuit?**

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.

3. **What are data grams?**

In datagram approach, each packet is treated independently from all others. Even when one packet represents just a place of a multi packet transmission, the network treats it although it existed alone. Packets in this technology are referred to as datagram.

4. **What is meant by switched virtual circuit?**

Switched virtual circuit format is comparable conceptually to dial-up line in circuit switching. In this method, a virtual circuit is created whenever it is needed and exits only for the duration of specific exchange.

5. **What is meant by Permanent virtual circuit?**

Permanent virtual circuits are comparable to leased lines in circuit switching. In this method, the same virtual circuit is provided between two uses on a continuous basis. The circuit is dedicated to the specific uses.

6. **What are the properties in star topology?**

- Even though a switch has a fixed number of inputs and outputs, which limits the number of hosts that can be connected to a single switch , large networks can be built by interconnecting a number of switches.
- We can connect switches to each other and to hosts using point-to point links, which typically means that we can build networks of large geographic scope.

7. **What is VCI? (Nov 2016)**

A Virtual Circuit Identifier that uniquely identifies the connection at this switch, and which will be carried inside the header of the packets that belongs to this connection

8. What is hop-by-hop flow control?

Each node is ensured of having the buffers it needs to queue the packets that arrive on that circuit. This basic strategy is usually called hop-by-hop flow control.

9. Define Reliable flooding?

It is the process of making sure that all the nodes participating in the routing protocol get a copy of the link state information from all the other nodes.

10. What are the different types of AS?

- Stub AS
- Multi homed AS
- Transit AS

11. Compare circuit switching and virtual circuit based packet Switching, in respect of queuing and forwarding delays. (MAY/JUNE 2013)

Circuit Switching

- In circuit switching dedicated communication path is available between two stations. It is easier to double the capacity of a packet switched network than a circuit network. A circuit network is heavily dependent on the number of channel available.
- Packet switching
- More security
- Bandwidth used to full potential
- Devices of different speeds can communicate Not affected by line failure(redirects signal)

12. Differentiate between connection less operation and connection oriented operation. (MAY/JUNE 2013)

Connection-oriented communication includes the steps of setting up a call from one computer to another, transmitting/receiving data, and then releasing the call, just like a voice phone call.

Connectionless communication is just packet switching where no call establishment and release occur. A message is broken into packets, and each packet is transferred separately.

13. What are the different routing techniques available to manage routing table entries?

- Next hop routing.
- Network specific routing
- Host specific routing
- Default routing

14. What is meant by router?

Router is network node connected to two or more networks that forwards packets from one network to another.

15. Give the types of routing table?

There are two types of routing table. They are,

Static routing table: The entries are created or update manually by an administrator. **Dynamic routing table:** The entries are updated automatically by dynamic routing protocols such as RIP, OSPF or BGP.

16. Define routing protocol.

Routing protocols is defined as "a combination of rules and procedures, which allows routers to share whatever they know about the internet or their neighborhood. It also includes procedures for combining information received from other routers".

17. Mention the types of routing protocol.

There are two basic categories of routing. They are,

- Intradomain routing, and Interdomain routing

18. Distinguish between Intradomain and Interdomain routing protocol.

Intradomain Routing	**Interdomain Routing**
It is defined as routing inside an AS.	It is defined as routing between AS.
It is classified as, 1.Distance Vector, 2.Link State	The path vector is of type interdomain.
RIP (Routing Information Protocol) Is an implementation of the distance vector protocol and OSPF (Open shortest path first) is an implementation of link state protocol.	BGP (Border Gateway Protocol) is an implementation of the path vector protocol.

19. Define AS.

A group of networks and routers under the authority of single administration is called as Autonomous System (AS).

20. Define RIP (or) Express the purpose of RIP?

Routing information protocol (RIP) is a simple protocol intradomain routing protocol used inside and Autonomous System(AS) based distance vector routing algorithm, in which each router shares, at regular intervals, its knowledge about the entire AS with its neighbors.

21. Mention the advantages of RIP over OSPF.

(i) RIP for IP is easy to implement. In its simplest default configuration, RIP for IP is as easy as configuring IP addresses and subnet masks for each router interface and then turning on the router.

(ii) RIP for IP has a large installed base consisting of small and medium- sized IP internetworks that do not wish to bear the design and configuration burden of OSPF.

22. What is Link state routing (LSR)?

It is a lowest-cost algorithm used in routing. The information on directly connected neighbors and current link costs are flooded to all routers; each router uses this information to build a view of the network which is the base to make forwarding decisions.

23. What do you meant by flooding?

Flooding means that a router sends all its link-state information about in neighbors, then the neighbors forward this information to in neighbors and so on. Thereby, every router receives the copy of the same information. This process continues until the information has reached all the nodes in the network.

24. Elaborate OSPF.

Open shortest path first (OSPF) is protocol widely used for intra-AS routing in the internet. It is the popular intradomain routing protocol based on link state routing that uses flooding of link-state information and a Dijkstra least- cost path algorithm.

25. Mention the advantages of OSPF.

OSPF has the following advantages

- Authentication
- Support for hierarchy within a single routing domain
- Multiple same-cost paths and
- Integrated support for unicast and multicast routing.

26. Compare distance vector routing with link state routing.

Distance vector routing(DVR)	Link state routing(LSR)
In DVR, each router periodically shares its knowledge about the entire network with its neighbours.	In LSR, each router shares its knowledge of its neighborhood with all routers in the internetwork.

The three important keys are, Knowledge about the whole network. Routing only to neighbors Information sharing at regular intervals.	The three important keys are, Knowledge about the neighborhood. Routing to all routers Information sharing when there is a change.

27. Define the term latency.

The term latency is a measure of how long a single bit takes to propagate from one end of a link or channel to the other. It is measured strictly in terms of time.

28. Define switches.

Switches are devices capable of creating temporary connections between two or more devices linked to the switch.

29. Give the comparison between router and switch.

Parameter	Router	Switch
Layer	Network layer(Layer 3devic	Data link layer. Network switche operates at layer 2 of the model.

Data transmission	Packet	Frame(L2 switch)
		Packet(L3 switch)

Transmission mode	Full duplex	Full duplex
Used in	LAN,WAN	LAN
Speed	1-10 Mbps 100 Mbps(wired)	10/100 Mbps, 1Gbps
Used for	Connecting two or more networks	Connecting two or more nodes the same network or different netwo
Address used	Uses IP address	Used MAC address.

30. A switch can process 2 million packets each second and each packet contains average of 64 bytes, then find out the throughput of the switch.

Solution:

Packet per second (pps) =2million packets=2x10^6

Throughput = pps x (bits per packet)

= 2 x 10^6 x 64 x 8

= 1024 x 10^6

= 1 Gbps

31. A 640-Gbps switch can handle a steady stream of 64-byte packets then what is pps rate? Solution:

Packet per second (pps) rate =Throughput

Bits per packet

= 640 x 10^9

64 x 8

= 10 x 10^9

8

= 1.25 x 10^9 pps

32. Define an area.

The link-state routing protocols such as OSPF and IS-IS can be used to partition a routing domain(AS) into subdomains called areas, to improve scalability, which is a set of adjacent routers that administratively configured to exchange full routing information with each other.

33. Define BGP. (NOV/DEC 2014)

The Border Gateway Protocol (BGP) is an interdomain routing protocol based on path vector routing by which different autonomous system (ASs) exchange reachability information.

34. Mention the names of two interdomain routing protocols.

There have been two major interdomain routing protocols in the history of the Internet.

(i) Exterior Gateway Protocol (EGP) and

(ii) Border Gateway Protocol (BGP).

35. What is EGP? Mention its drawbacks.

Exterior gateway protocol (EGP) is an interdomain routing protocol of the internet, which was used by exterior gateway (routers) of autonomous systems to exchange routing information with other autonomous systems, which had a number of limitations.

EGP was designed when the Internet had a tree like topology, and did not allow for the topology to become more general and autonomous systems are connected only as parents and children and not a peers. The replacement for EGP is the Border Gateway Protocol (BGP).

36. Define an IGP.

Interior Gateway Protocol (IGP) is a routing protocol used to exchange routing information among routers within a single autonomous system.

37. Write the functions of BGP. BGP provides each AS:

(i) Obtain subnet reachability information from neighboring Ass

(ii) Propagate the reachability information to all routers internal to the AS.

(iii) Determine "good" routes to subnets based on the reachability information and on AS policy.

38. Mention the drawbacks of IPV4.

- It provides a very limited number if host and network addresses. For example, if an organization chooses class C only 256 IP addresses are available to it, it's a very little number.
- Since the IP address is 32 bits long, the space of the IP address will be exhausted soon. This space growth won't match with the user's growth in t internet.
- The IPv4 doesn't provide real-time audio and video support, which is needed by the modern internet applications.

39. List the advantages of IPv6 over IPv4.

The advantages of Next generation IP or IPv6 over IPv4 are,

- Larger address space
- Better header format
- New options
- Support for real-time services
- Support for resource allocation
- Support for more security
- Auto –configuration
- Enhanced routing functionality, including support for mobile hosts.

40. The extension headers in IPv6 are equivalent to what in IPv4?

The length of the base header is of about 40 bytes in length. The base header can be followed by six extension headers, in order to give more functionality to the IPv6 datagram. The extension headers here are equivalent to the options in IPv4.

41. What is multicast?

Multicast is a special form of broadcast in which a single source transmits the packets and they are delivered to specified subgroup of network hosts (one- to-many).

42. Give the comparison of unicast, multicast and broadcast Routing. (Nov 2016)

Unicasting	Multicasting	Broadcasting
One source and one destination	One source and a group of destinations.	One source and all destinations.
Relationship is one-to-one	Relationship is one-to-many	Relationship is one-to-all
Both source and destination addresses are unicast addresses	The source address is unicast address, but the destination address is a group address	Both source andDestination addresses are broadcast addresses
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 its interfaces.

43. Expand DVMRP.

Distance Vector Multicast Routing Protocol (DVMRP) is a multicast distance vector routing uses the source-based least cost trees, but the router never actually makes a routing table.

44. Name the strategies used in multicast DVR protocol.

The multicast DVR algorithm uses a process based on four decision-making strategies.

Each strategy is built on its predecessor.

- Flooding,
- Reverse Path Forwarding(RPF),
- Reverse Path Broadcasting(RPB), and
- Reverse Path Multicasting(RPM)

45. What do you meant by PIM?

Protocol independent multicast (PIM) is a multicasting protocol family with two independent multicast routing protocols such as:

- PIM-DM (Dense Mode) and
- PIM-SM (Spare Mode)

Both protocols are unicast-protocol dependent.

46. Define the terms PIM-DM & PIM-SM.

Protocol independent multicast- Dense Mode (PIM-DM) is used in a dense multicast environment, such as a LAN. It is a source-based tree routing protocol that uses RPF and pruning and grafting strategies for multicasting.

Protocol independent multicasting-Spare Mode (PIM-SM)

Is used in a spares multicast environment such as a WAN. PIM-SM is group- shared tree routing protocol that has a rendezvous point (RP) as the source of the tree. PIM-SM is similar to CBT but uses a simpler procedure.

47. Write down any two differences between circuit switching and packet switching (Nov/Dec 2014)

Circuit switching

In circuit switching network dedicated channel has to be established before the call is made between users. The channel is reserved between the users till the connection is active

Packet switching

- In packet switching network unlike CS network, it is not required to establish the connection initially
- The connection/channel is available to use by many users.

48. How does a router differ from a bridge? (May 2015)

A **bridge** is a product that connects a local area network (LAN) to another local area network that uses the same protocol (for example, Ethernet or Token Ring). You can envision a bridge as being a device that decides whether a message from you to someone else is going to the local area network in your building or to someone on the local area network in the building across the street.

A **router** is a device or, in some cases, software in a computer, that determines the next network point to which a packet should be forwarded toward its destination. The router is connected to at least two networks and decides which way to send each information packet based on its current understanding of the state of the networks it is connected to. A router is located at any gateway (where one network meets another), including each point-of-presence on the Internet. A router is often included as part of a network switch.

49. What are the metrics used by routing protocols? (May 2015)

Router metrics can contain any number of values that help the router determine the best route among multiple routes to a destination. A router metric typically based on information like path length, bandwidth, load, hop count, path cost, delay, Maximum Transmission Unit (MTU), reliability and communications cost.

50. Define routing (Nov 2015)

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

16 – MARKS

1. Explain about Switching and Forwarding.
2. Explain about RIP.
3. Explain about OSPF.
4. Explain about BGP.
5. Explain about Routing areas.
6. Explain about IPv6.
7. Explain about Multicast.
8. Explain about DVMRP.
9. Explain about PIM.
10. Explain about Multicast address.

UNIT IV TRANSPORT LAYER 9

Introduction – Transport Layer Protocols – Services – Port Numbers – User Datagram Protocol – Transmission Control Protocol – SCTP.

2 Marks

1) *List the duties of Transport Layer (TL)*

- Packetizing
- Connection Control
- Addressing
- Providing reliability

2) *What is the difference between TCP & UDP? (NOV 2014 & 2016)*

TCP	UDP
Connection Oriented Service	Connection less Service
Reliable	Not much reliable
Not suitable for multimedia, real time applications	used for multimedia and multicasting applications

3) *What is socket? Define socket address.*

Socket is the end point of a bi-directional communication flow across IP based network (Internet)

Socket address is the combination of an IP address (location of computer) and a port (application program process) into a single entity.

4) *What is congestion? How to control congestion?*

Congestion in network is the network is the situation in which an increase in data transmission results in a reduction in the throughput.

Throughput-amount of data passes through network congestion can be controlled using two techniques.

- Open-loop congestion control (prevention)
- Closed-loop congestion control(removal)

5) *Define jitter*

Jitter is the variation in delay for packets belonging to the same flow.

Example: 2ms delay for 1 packet
60ms delay for second packet.

6) *What is the use of integrated services?*

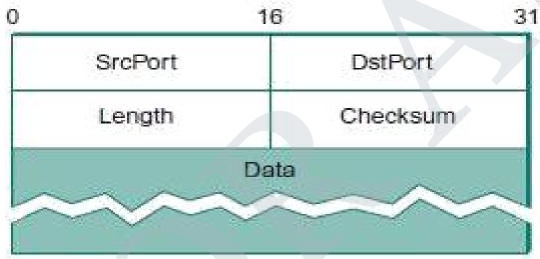
Integrated services (Instserv) are a followed based QoS model where the user creates a flow from source to direction and inform all the routers of the source requirement.

7). Differentiate between delay and jitter.

Voice over IP (VoIP) is susceptible to network behaviors, referred to as delay and jitter, which can degrade the voice application to the point of being unacceptable to the average user. Delay is the time taken from point-to-point in a network. Delay can be measured in either one-way or round-trip delay.

Jitter is the VARIATION in delay over time from point-to-point. If the delay of transmissions varies too widely in a VoIP call, the call quality is greatly degraded. The amount of jitter tolerable on the network is affected by the depth of the jitter buffer on the network equipment in the voice path. The more jitter buffer available, the more the network can reduce the effects of jitter.

8) Draw UDP header format



9) What is traffic shaping?

Traffic shaping is a mechanism to control the amount and rate of traffic sent to the network.

10) What is the unit of data transfer in UDP and TCP? In UDP, the Unit of data transfer is called datagram. In TCP, Unit of data transfer is called segments.

11) List the timers used by TCP.

- Retransmission timer
- Persistence timer
- Keep alive timer
- Time waited timer

12) Define Sill window syndrome.

Sending less amount of Data (Ex. 1 byte) which is lesser than header size (20 bytes of TCP header +20 bytes of IP header) is called silly window syndrome. Here the capacity of network is used inefficiently.

13. Explain the main idea of UDP? Or Simple Demultiplexer

The basic idea is for a source process to send a message to a port and for the destination process to receive the message from a port.

14. What are the different fields in pseudo header?

- Protocol number
- Source IP address
- Destination IP addresses.

15. Define TCP? Or Reliable byte stream

TCP guarantees the reliable, in order delivery of a stream of bytes. It is a full-duplex protocol, meaning that each TCP connection supports a pair of byte streams, one flowing in each direction.

16. Define Congestion Control?

It involves preventing too much data from being injected into the network, thereby causing switches or links to become overloaded. Thus flow control is an end to an end issue, while congestion control is concerned with how hosts and networks interact.

17. State the two kinds of events trigger a state transition?

- A segment arrives from the peer.
- The local application process invokes an operation on TCP.

18. What is meant by segment?

At the sending and receiving end of the transmission, TCP divides long transmissions into smaller data units and packages each into a frame called a segment.

19. What is meant by 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.

20. What is meant by 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.

21. What is rate based design?

Rate- based design, in which the receiver tells the sender the rate-expressed in either bytes or packets per second – at which it is willing to accept incoming data.

22. Define Gateway.

A device used to connect two separate networks that use different communication protocols.

23. What are the two categories of QoS attributes? The two main categories are,

- User Oriented
- Network Oriented

24. What is RED?

Random Early Detection in each router is programmed to monitor its own queue length and when it detects that congestion is imminent, to notify the source to adjust its congestion window.

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

For security, the transport layer may create a connection between the two end ports. A connection is a single logical path between the source and destination that is associated with all packets in a message. Creating a connection involves three steps:

- Connection establishment
- Data transfer
- Connection release

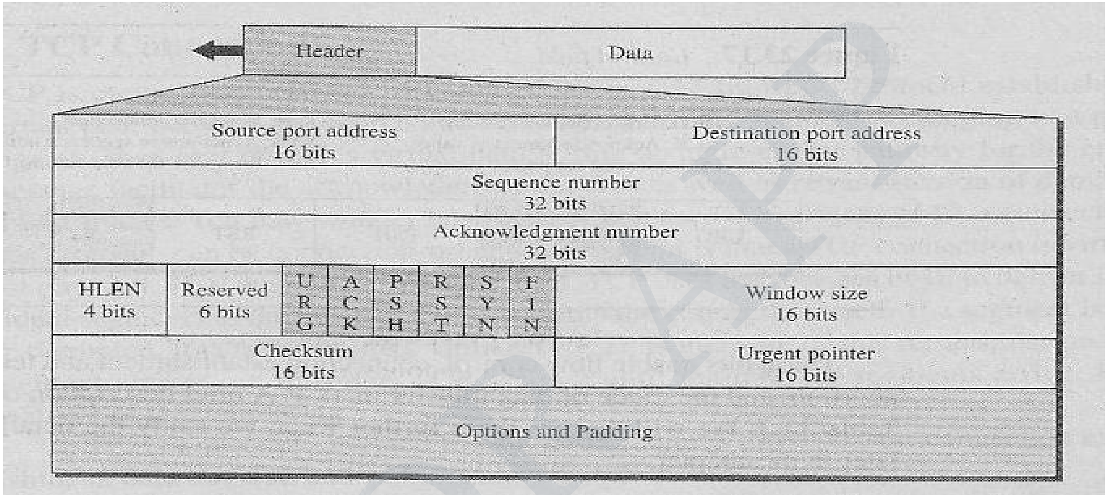
26. What is the difference between service point address, logical address and physical address?

Service point addressing	Logical addressing	Physical addressing
The transport layer header includes a type of address called a service point address or port address, which makes a data delivery from a specific process on one computer to a specific process on another computer.	If a packet passes the network boundary we need another addressing to differentiate the source and destination systems. The network layer adds a header, which indicate the logical address of the sender and receiver.	If the frames are to be distributed to different systems on the network, the data link layer adds the header, which defines the source machine‟ s address and the destination Machine‟ s address.

27. Give the approaches to improve the QoS Four common techniques are:

Scheduling
- Traffic shaping
- Admission control
- Resource reservation

28. Draw TCP header format



29. How will the congestion be avoided?

The congestion may be avoided by two bits BECN - Backward Explicit Congestion Notification FECN - Forward Explicit Congestion Notification

30. What is the function of BECN BIT?

The BECN bit warns the sender of congestion in network. The sender can respond to this warning by simply reducing the data rate.

31. What is the function of FECN?

The FECN bit is used to warn the receiver of congestion in the network. The sender and receiver are communicating with each other and are using some types of flow control at a higher level.

32. What is meant by quality of service or QoS? (NOV 2014 & 2015)

The quality of service 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.

33. List out the user related attributes?

User related attributes are SCR – Sustainable Cell rate PCR – Peak Cell Rate MCR- Minimum Cell Rate

CVDT – Cell Variation Delay Tolerance

34. 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)

35. Why is UDP pseudo header included in UDP checksum calculation? What is the effect of an invalid checksum at the receiving UDP?

The UDP checksum is performed over the entire payload, *and* the other fields in the header, *and* some fields from the IP header. A pseudo-header is constructed from the IP header in order to perform the calculation (which is done over this pseudo-header, the UDP header and the payload). The reason the pseudo-header is included is to catch packets that have been routed to the wrong IP address.

If the checksum validation is enabled and it detected an invalid checksum, features like packet reassembling won't be processed.

36. How can the effect of jitter be compensated? What type of application require for this compensation?

Jitter is an undesirable effect caused by the inherent tendencies of TCP/IP networks and components.

Jitter is defined as a variation in the delay of received packets. The sending side transmits \ packets in a continuous stream and spaces them evenly apart. Because of network congestion, improper queuing, or configuration errors, the delay between packets can vary instead of remaining constant. This variation causes problems for audio playback at the receiving end. Playback may experience gaps while waiting for the arrival of variable delayed packets.

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 play out delay buffer is also referred to as the dejitter buffer.

37. What is meant by PORT or MAILBOX related with UDP?
Form of address used to identify the target process:

Process can directly identify each other with an OS-assigned process ID(pid) More commonly-processes indirectly identify each other using a port or mailbox Source sends a message to a port and destination receives the message from the port UDP port is 16 bits, so there are 64K possible ports- not enough for all Internet hosts Process is identified as a port on a particular host – a (port, host) pair.

To send a message the process learns the port in the following way:
A client initiates a message exchange with a server process. The server knows the client"s port (contained in message header and can reply to it. Server accepts messages at a well known port. Examples: DNS at port 53, mail at port 25

38. List out the various features of sliding window protocol.
The key feature of the sliding window protocol is that it permits pipelined communication. In contrast, with a simple stop-and-wait protocol, the sender waits for an acknowledgment after transmitting every frame. As a result, there is at most a single outstanding frame on the channel at any given time, which may be far less than the channel's capacity. For maximum throughput, the amount of data in transit at any given time should be equal to (channel bandwidth) X (channel delay).

39. What is the function of a router?

•Connect network segment together

•Router forwards the packet to the right path

40. What is the advantage of using UDP over TCP?
- UDP can send data in a faster way than TCP
- UDP is suitable for sending multicasting and multimedia applications

41. What is the difference between congestion control and flow control? (Nov 2015) Congestion control
It involves preventing too much data from being injected into the network, thereby causing switches or links to become overloaded. Thus flow control is an end to an end issue, while congestion control is concerned with how hosts and networks interact.

Flow control

The amount of data flowed from source to destination should be restricted. The source can send one byte at a time, but it will take long time to transmit n bytes.

42. List the mechanisms used in TCP congestion control mechanism

- Additive Increase/Multiplicative Decrease
- Slow Start
- Fast Retransmit and Fast Recovery

43. List the mechanisms used in TCP congestion avoidance

- DEC bit
- RED (Random Early Detection)
- Source-based Congestion Avoidance

44. Define DEC bit

Each router monitors the load it is experiencing and explicitly notifies the end nodes when congestion is about to occur. This notification is implemented by setting a binary congestion bit in the packets that flow through the router, hence the name *DEC bit.*

45. What is meant by Source-Based Congestion Avoidance?

The general idea of these techniques is to watch for some sign from the network that some router‟s queue is building up and that congestion will happen soon if nothing is done about it

46. List the approaches to QoS support

***Fine-grained* approaches**, which provide QoS to individual applications or flows ***Coarse-grained* approaches**, which provide QoS to large classes of data or aggregated traffic

47. List the types of application requirements in QoS

- Real-time
- Non-real-time

48. List some of the Quality of service parameters of transport layer (May 2015)

- Reliability
- Delay
- Jitter
- Bandwidth

49. How does transport layer perform duplication control? (May 2015)

Duplication can be controlled by the use of sequence number & acknowledgment number

50. What do you mean by slow start in TCP congestion? (May 2016)

The sender starts with a very slow rate of transmission but increases the rate rapidly to reach a threshold

51. List the different phases used in TCP connection

Connection establishment and Data transfer Connection termination

16 – MARKS

1. Explain about the operation of TCP with neat sketch on it.

2. Explain about the concept of sliding window protocol.

3. Explain about UDP with neat sketch on it.

4. (i). Difference between UDP and TCP. (ii). Discuss flow control with an example.

5. Explain about the three way handshake protocol for connection establishment in TCP.

6. Explain about the TCP congestion control.

7. Explain about the RED algorithm.

8. Explain about the concept of congestion avoidance in TCP?

9. Explain about the RSVP protocol with neat sketch.

10. Explain about the differentiated services.

UNIT V APPLICATION LAYER 9

WWW and HTTP – FTP – Email –Telnet –SSH – DNS – SNMP.

2 MARKS

1. What is the function (Define) of SMTP? (May & Nov 2015)

The TCP/IP protocol supports electronic mail on the Internet is called Simple Mail Transfer (SMTP). It is a system for sending messages to other computer users based on e-mail addresses. SMTP provides mail exchange between users on the same or different computers.

2. 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.

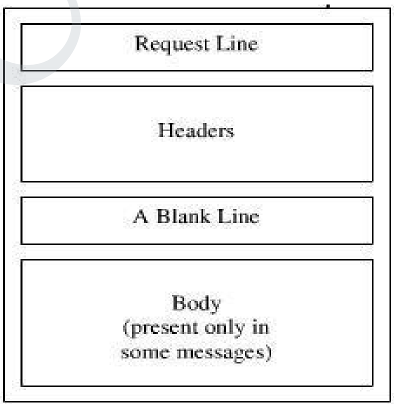
3. How does MIME (Differ) enhance SMTP? (Nov/Dec 2007) (Or) State the difference between SMTP and MIME (NOV/DEC 2014)

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 deliverers 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.

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

Workstations interact with the SMTP host, which receives the mail on behalf of every host in the organization, to retrieve messages by using a client-server protocol such as Post Office Protocol, version 3(POP3). Although POP3 is used to download messages from the server, the SMTP client still needed on the desktop to forward messages from the workstation user to its SMTP mail server.

5. Give the format of HTTP request message?



6. What is the purpose of Domain Name System?

Domain Name System can map a name to an address and conversely an address to name.

7. 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.

8. Define CGI?

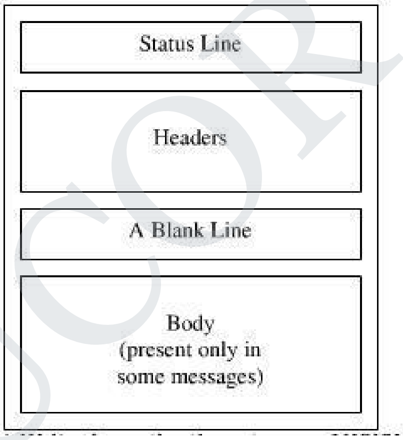
CGI is a standard for communication between HTTP servers and executable programs. It is used in crating dynamic documents.

9. What are the requests messages support SNMP and explain it?

- GET
- SET

The former is used to retrieve a piece of state from some node and the latter is used to store a new piece of state in some node.

10. Give the format of HTTP response message?



11. Why name services are sometimes called as middleware?

Name services are sometimes called middleware because they fill a gap between applications and the underlying network

12. What are the types of DNS Message

Two types of messages

Query: header and question records
Response: Header, question records, answer records, authoritative records, and additional records.

13. What is POP3? (Nov 2016)

POP3 (Post Office Protocol 3) is the most recent version of a standard protocol for receiving e-mail. POP3 is a client/server protocol in which e-mail is received and held for you by your Internet server. POP and IMAP deal with the receiving of e-mail and are not to be confused with the Simple Mail Transfer Protocol (SMTP), a protocol for transferring e-mail across the Internet.

14. What is IMAP4? (Nov 2016)

IMAP (Internet Message Access Protocol) is a standard protocol for accessing e-mail from your local server. IMAP (the latest version is IMAP Version 4) is a client/server protocol in which e-mail is received and held for you by your Internet server. IMAP can be thought of as a remote file server. POP3 can be thought of as a "store-and-forward" service.

15. What is DNS? (Apr /May 2010)

The **DNS** translates Internet domain and host names to IP addresses. DNS automatically converts the names we type in our Web browser address bar to the IP addresses of Web servers hosting those sites.

16. What is persistent HTTP? What are the advantages of allowing persistent TCP Connections in HTTP? (May 2013) (Nov 2016)

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.

Persistent HTTP connections have a number of advantages:

By opening and closing fewer TCP connections, CPU time is saved in routers and hosts (clients, servers, proxies, gateways, tunnels, or caches), and memory used for TCP protocol control blocks can be saved in hosts.

HTTP requests and responses can be pipelined on a connection. Pipelining allows a client to make multiple requests without waiting for each response, allowing a single TCP connection to be used much more efficiently, with much lower elapsed time.

Network congestion is reduced by reducing the number of packets caused by TCP opens, and by allowing TCP sufficient time to determine the congestion state of the network.

Latency on subsequent requests is reduced since there is no time spent in TCP's connection opening handshake.

HTTP can evolve more gracefully, since errors can be reported without the penalty of closing the TCP connection. Clients using future versions of HTTP might optimistically try a new feature, but if communicating with an older server, retry

with old semantics after an error is reported.
HTTP implementations SHOULD implement persistent connections.

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

It is really, really hard to infer the input from the hash **because there are an infinite amount of input strings that will generate the same output** (irreversible property). However, ***finding*** even a single instance of multiple input strings that generate the same output is also really, really hard (collision resistant property).

18. Define SNMP?
SNMP is a frame work for managing devices in an internet using TCP/IP suite. It provides fundamental operations for monitoring and maintaining an internet.

19. What DNS cache issues are involved in changing the IP address of a web Server host name? Nov/Dec 2013

The Domain Name System supports DNS cache servers which store DNS query results for a period of time determined in the configuration (time-to-live) of the domain name record in question. Typically, such caching DNS servers, also called DNS caches, also implement the recursive algorithm necessary to resolve a given name starting with the DNS root through to the authoritative name servers of the queried domain. With this function implemented in the name server, user applications gain efficiency in design and operation.

20. Differentiate application programs and application protocols. Nov/Dec 2013

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. Examples of application programs include word processors; database programs; Web browsers; development tools; drawing, paint, and image editing programs; and communication programs. Application programs use the services of the computer's operating system and other supporting programs.

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.

37. What are the two mainly used application protocols

Simple Mail Transfer Protocol (SMTP) is used to exchange electronic mail.
Hypertext Transport Protocol (HTTP) is used to communicate between web browsers and web servers.

38. Define HTTP protocol (WWW)

HTTP PROTOCOL Protocol for transfer of data between Web servers and Web clients (browsers).
"The Hypertext Transfer Protocol (HTTP) is an **application-level protocol** for **distributed**, collaborative, hypermedia information systems.
Popular Web servers:
Apache HTTPD, JBoss and Tomcat
Popular Web clients:
Firefox and Opera

38. Define web services

The term *Web services* describes a standardized way of integrating Web-based applications using the XML, SOAP, WSDL and UDDI open standards over an Internet protocol backbone. XML is used to tag the data, SOAP is used to transfer the data, WSDL is used for describing the services available and UDDI is used for listing what services are available. Used primarily as a means for businesses to communicate with each other and with clients, Web services allow organizations to communicate data without intimate knowledge of each other's IT systems behind the firewall.

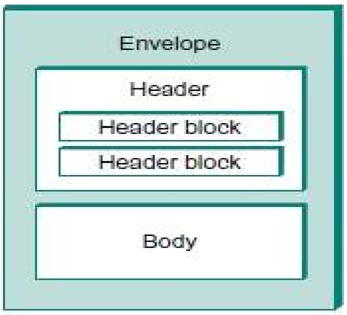
42. What is SOAP?

- SOAP stands for Simple Object Access Protocol
- SOAP is a communication protocol
- SOAP is for communication between applications
- SOAP is a format for sending messages
- SOAP communicates via Internet
- SOAP is platform independent
- SOAP is language independent
- SOAP is based on XML
- SOAP is simple and extensible
- SOAP allows you to get around firewalls
- SOAP is a W3C recommendation

25. What is WSDL?

The Web Services Description Language (WSDL) is an XML-based language used to describe the services a business offers and to provide a way for individuals and other businesses to access those services electronically.

26. Draw SOAP message structure



27. Define MIME

MIME, an acronym for Multipurpose Internet Mail Extensions, specifies how messages must be formatted so that they can be exchanged between different email systems. MIME is a very flexible format, permitting one to include virtually any type of file or document in an email message. MIME messages can contain text, images, audio, video, or other application-specific data.

28. List down the key lengths supported by PGP (NOV/DEC 2014)

The "length" is a formal characterization of one of the mathematical values that constitute the *key pair*. Thus, the public and the private key don't have independent lengths per se; the private/public key pair has a length, which, by extension, is also said to be the length of the public key *and* of the private key.

The length is not the actual bit length of the encoding of either the public or private key, although there are correlations

29. What are the groups of HTTP header? (May 2015)

Accept HTTP_User - Agent

Content-Language Content-Length Content-Type Date

Expires: Host Location Retry-After

30 . Define URL (May 2016)

A URL (Uniform Resource Locator), as the name suggests, provides a way to locate a resource on the web, the hypertext system that operates over the internet. The URL contains the name of the protocol to be used to access the resource and a resource name. The first part of a URL identifies what protocol to use. The second part identifies the IP address or domain name where the resource is located.

31. Mention the different levels in domain name space (May 2016)

Top Level Domains
Third Level Domains

32. Mention the types of HTTP messages

HTTP request message
HTTP response message

16 – MARKS

1. Explain about the Traditional applications.

2. Explain about the WSDL in web services.

3. Explain about the SOAP.

4. Explain about the SMTP.

5. Explain about the DNS.

6. Explain about the SNMP.

7. Explain about the MIME.

8. Explain about the POP3.

9. Explain about the IMAP.

10. Explain about the HTTP.