



VETRI VINAYAHA COLLEGE OF ENGINEERING AND TECHNOLOGY
DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING

CS6551 COMPUTER NETWORKS

II year/ IV sem CSE

(Regulation 2013)



UNIT 1-FUNDAMENTALS AND LINK LAYER

PART A

1. State the major functions performed by the presentation layer of the ISO OSI model.(Nov Dec 2006)

Presentation layer is concerned with the format of data exchanged between peers, for example, whether an integer is 16, 32, or 64 bits long and whether the most significant bit is transmitted first or last, or how a video stream is formatted.

2. A sine wave has a frequency of 6 Hz. What is its period?(Nov Dec 2006)

Frequency is indirectly proportional to time. Consider the time T and frequency f . Then, the formula is, $T=1/freq = 1/6Hz=0.17$ seconds.

3. Define the term Protocol and give its key elements. (Nov Dec 2007)

Protocol is used for communications between entities in a system and must speak the same language. Protocol is the set of rules governing the exchange of data between 2 entities. It defines what is communicated, how it is communicated, when it is communicated

Key elements of Protocol:

Syntax – It refers to the structure or format of data meaning the order in which they are presented.

Semantics – It refers to the meaning of each section of bit. How to do interpretation.

Timing – When data should be sent and how fast they can be sent.

4. State the purpose of layering in networks?(May Jun 2007)

A layer is a collection of related functions that provides services to the layer above it and receives services from the layer below it.

To execute the functions by each layer is independent.

5. At which level of OSI model does repeaters, bridges, routers and gateways operate?(May Jun 2007)

DEVICES	LAYERS
Repeater	Physical
Bridge	Physical, Datalink
Router	Physical, Datalink and Network
Gateway	All 7 layers

6. For n devices in a network, what is the number of cable links required for a mesh, ring, bus and star topology?(Nov Dec 2008)

Cable links required to make communication between n network devices.

Links required for mesh topology = $n(n-1)/2$

Links required for ring topology = $n-1$

Links required for star topology = n

Links required for bus topology = one backbone and n drop lines

7. What are the two types of line configuration? (Nov Dec 2010)

Point to point line configuration and multipoint line configuration.

Point to point:

It provides a dedicated link between 2 devices.

Entire capacity of the link is reserved for transmission between 3 devices only

Eg: connection between remote control and TV's control system

Multipoint:

Also called as multi drop connection

Here the channel capacity is shared

If many devices share the link simultaneously it is called spatially shared connection.

8. What do you mean by error control? (Nov Dec 2010)

Error control refers to mechanism to detect and correct errors that occur in the transmission of frames.

9. What is flow control? (Nov Dec 2011)

Flow control is a technique for assuring that a transmitting entity does not overwhelm a receiving entity with data. *Flow control*—a feedback mechanism by which the receiver is able to throttle the sender. Such a mechanism is used to keep the sender from overrunning the receiver, i.e., from transmitting more data than the receiver is able to process.

10. Define Error detection and correction. (Nov Dec 2011)

Error detection: Sender transmits every data unit twice. Receiver performs bit-by-bit comparison between those two versions of data. Any mismatch would indicate an error, which needs error correction.

11. What are the issues in data link layer? (Nov Dec 2012)

The Data Link Layer is the protocol layer which transfers data between adjacent network nodes in a wide area network or between nodes on the same local area network segment. The Data Link Layer provides the functional and procedural means to transfer data between network entities and might provide the means to detect and possibly correct errors that may occur in the Physical Layer. Examples of data link protocols are Ethernet for local area networks (multi-node), the Point-to-Point Protocol (PPP), HDLC and ADCCP for point-to-point (dual-node) connections.

12. What is ARQ? (Dec 10)

Automatic repeat request (ARQ). In error control mechanism when an error is detected in an exchange, specified frames are retransmitted. This process is called ARQ.

13. What are the functions of application layer? (May 11)

User access information on the network through the application layer. This layer is the main interface for the user to interact with the application.

14. Define bit stuffing. (May 11)

Each frame begins and ends with a special bit pattern called flag byte. Whenever sender data link layer encounters five consecutive ones in the data stream, it automatically stuffs a 0 bit into the outgoing stream.

15. Difference between circuit switching and packet switching. (May 11)

Circuit switching	Packet switching
Physical connection b/w sender and receiver	No Physical connection b/w sender and receiver
All packet use same path	All packet use different path
Waste of bandwidth is possible	Waste of bandwidth is not possible
Congestion occurs for per minute	Congestion occurs for per packet

16. What is HDLC? (May 12)

It is a protocol that implements ARQ mechanisms. It supports communication over point – to – point or point – to – multipoint links.

17. Define a layer. (Dec 13)

A layer is a collection of related functions that provides services to the layer above it and receives services from the layer below it. To executed the functions by each layer is independent.

18. What do you mean by framing? (Dec-13)

The DLL translates the physical layers raw bit stream into discrete units called frames. Framing in DLL separates messages from one source to a destination, or from other messages to other destination, by adding sender and receiver address.

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

The most important criteria are performance, reliability and 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.

20. 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.

21. What are header and trailers and how do they get added and removed?

Each layer in the sending machine adds its own information to the message it receives from the layer just above it and passes the whole package to the layer just below it. This information is added in the form of headers or trailers. Headers are added to the message at the layers 6,5,4,3, and 2. A trailer is added at layer2. At the receiving machine, the headers or trailers attached to the data unit at the corresponding sending layers are removed, and actions appropriate to that layer are taken.

22. What are the features provided by layering?

Two features:

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

23. 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.

24. 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.

25. 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 highbandwidth,long-distance links)

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

PART B

1. Explain the ISO-OSI model of computer network with a neat diagram.
2. Discuss the major functions performed by the Presentation layer and Application layer of the ISO OSI model.
3. Explain the methods used for error detection and error correction.
4. Explain various flow control mechanisms.
5. Write a note on network hardware.
6. Explain various Network topologies.
7. Explain Transport Layer and Physical Layer.
8. What are the major components of an optical communication system? Discuss.
9. Distinguish between point to point links and multi point links. Give relevant diagrams.
10. Explain Data Link Layer and Network Layer.
11. Compare Connection oriented and connectionless service.
12. Discuss the principles of stop and wait flow control algorithm.

PART C

1. Problems solving in Cyclic Redundancy Check
2. Problems solving in Sliding window protocol
3. Problems solving in ARQ Protocol
4. Hamming distance calculation
5. Programs using socket API

UNIT 2-MEDIA ACCESS & INTERNETWORKING

PART A

1. What is CSMA/CD? (Nov Dec 2011)

Carrier sense multiple access with collision detection (CSMA/CD) is a Media Access Control method,

a carrier sensing scheme is used.

a transmitting data station that detects another signal while transmitting a frame, stops transmitting that frame, transmits a jam signal, and then waits for a random time interval before trying to resend the frame.

2. What is meant by bridge? .(Nov Dec 2011)

A network bridge connects multiple network segments (network domains) along the data link layer. It is sometimes called a network switch, and it works by using bridging. Traffic from one network is forwarded through it to another network. The bridge simply does what its name entails, by connecting two sides from adjacent networks.

3. Differentiate fast Ethernet and gigabit Ethernet. .(Nov Dec 2012)

The 'Ether' part of Ethernet denotes that the system is not meant to be restricted for use on only one medium type, copper cables, fiber cables and even radio waves can be used. Fast Ethernet Network was developed as an upgrade to traditional Ethernet Networking. Fast Ethernet improved traditional Ethernet by increasing transfer rates 10 times, from 10 Megabit to 100 Megabit speed. Gigabit Ethernet Network is an upgrade on Fast Ethernet Network equivalent to Fast Ethernet Networks improvement over Fast Ethernet Network, offering speeds of 1000 Megabits (1 Gigabit).

4. What is the difference between switch and bridge? .(Nov Dec 2012)

The difference between switch and bridge are,

1. Bridge is device which divides a network into two. Switch connects multiple networks.
2. Bridge is software based and switch is a hardware based.
3. Bridge can have upto 16 ports while switch can handle many ports.
4. Bridge is rarely used. Switches are frequently used.

5. Compare a piconet and a scatter net. .(Nov Dec 2008)

A piconet is the type of connection that is formed between two or more Bluetooth enabled devices, one device takes the role of 'master', and all other devices assume a 'slave' role for synchronization reasons. Scatternet is a number of interconnected piconets that supports communication between more than 8 devices. Scatternet can be formed when a member of one piconet elects to participate as a slave in a second, separate piconet.

6. What are the functions of Bridges? (Nov Dec 2010)

A bridge device filters data traffic at a network boundary. Bridges reduce the amount of traffic on a LAN by dividing it into two segments.

Bridges operate at the data link layer (Layer 2) of the OSI model. Bridges inspect incoming traffic and decide whether to forward or discard it. An Ethernet bridge, for example, inspects each incoming Ethernet frame - including the source and destination MAC addresses, and sometimes the frame size - in making individual forwarding decisions.

7. Which class does the following IP address belong to? (Nov Dec 2006)

(a) 157.143.252.207 (b) 93.31.1.245

- a. This IP address comes under Class B.
- b. This IP address comes under Class A.

8. Is the size of the ARP packet fixed? Explain.(Nov Dec 2008)

The ARP packet size must vary because it contains 2 Hardware/MAC addresses in it and 2 different protocol addresses in it. Depending on the datalink and network protocol used the size addresses vary.

9. What is DHCP? .(Nov Dec 2012)

Dynamic Host Configuration Protocol (DHCP) is a client/server protocol that automatically provides an Internet Protocol (IP) host with its IP address and other related configuration information such as the subnet mask and default gateway.

10. What is meant by circuit switching? (Nov Dec 2010)

Circuit switching is a methodology of implementing a telecommunications network in which two network nodes establish a dedicated communications channel (circuit) through the network before the nodes may communicate. The circuit guarantees the full bandwidth of the channel and remains connected for the duration of the communication session. The circuit functions as if the nodes were physically connected as with an electrical circuit.

11. List the two forms in which virtual circuit packet switching is implemented.(Nov Dec 2006)

Two forms of virtual circuit packet switching implementations are,
Switched Virtual Circuit (SVC)
Permanent Virtual Circuit (PVC)

*PVC makes permanent virtual connection between two specific nodes.

12. Define subnetting. (Nov Dec 2011)

Subnetting divides a network into several subnetworks (or subnets). All systems (for example, workstations, printers, server, and routers) that exist in the subnet have common network and subnet values, but each must have a unique interface portion of their logical or IP address.

13. What is the data rate of fast ethernet? (May 11)

100 Mbits/sec

14. What is Bluetooth standard? (May 11)

CLASS	POWER	RANGE
Class 3	1 MW	10M
Class 2	2.5 MN	20M
Class 1	100 MN	100M

15. What is meant by bridge? .(Dec 11)

Connects two similar and dissimilar networks.

It filters the traffic based on destination address of the frame.

16. 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.

17. What are the functions of LLC?

The IEEE project 802 models take the structure of an HDLC frame and divides it into 2 sets of functions. One set contains the end user portion of the HDLC frame – the logical address,

control information, and data. These functions are handled by the IEEE 802.2 logical link control (LLC) protocol.

18. What is Ethernet?

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

19. Define the term carrier sense in CSMA/CD?

All the nodes can distinguish between idle and a busy-link and —collision detectll means that a node listens as it transmits and can therefore detect when a frame it is transmitting has interfered (collided) with a frame transmitted by another node.

20. 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.

21. 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.

22. 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.

23. What is exponential back off?

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.

24. What is token holding time (THT)?

It defines that how much data a given node is allowed to transmit each time it possesses the token or equivalently, how long a given node is allowed to hold the token.

25. What are the two classes of traffic in FDDI?

Synchronous
Asynchronous

26. What are the four prominent wireless technologies?

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

PART B

1. Explain in detail about the access method and frame format used in Ethernet and token ring.
2. Discuss the MAC layer functions of IEEE 802.11.
3. Briefly define key requirement of wireless LAN.

4. Write short notes on Ethernet and Wireless LAN.
5. Explain in detail ARP, DHCP, ICMP.
6. Write short notes on Random Access.
7. Describe CSMA/CD protocol and comment on its performance for medium access.
8. Explain in detail about the token ring.
9. Explain FDDI in detail.
10. Explain and differentiate Ethernet and FDDI in detail.
11. Write short notes on MACA and MACAW.
12. Explain the MAC layer functions of IEEE 802.11.
13. Discuss the problems encountered in applying CSMA/CD algorithm to wireless LANs. How do 802.11 specifications solve these problems?
14. Explain in detail about SONET.
15. What is internetworking? Explain its service model, global address and datagram forwarding in detail.
16. Write short notes on Classful and Classless Addressing.
17. Write short notes on Bridges and Switches.

PART C

1. Problems on subnetting.
2. Problems on class of Addressing
3. Problems on CSMA/CD
4. Throughput calculations on Aloha, Slotted Aloha
5. Efficiency calculation on FDDI.
6. ICMP Timestamp protocol problems.

UNIT 3-ROUTING

PART A

1. **What kind of routing information do routers exchange among themselves while running distance vector algorithm? In particular, briefly describe the format of the routing information that it exchanged. (May Jun 2007)**

In distance vector algorithm, the routers exchange their routing table with other neighbor routers.

The routing table consist information's on Network ID, Cost and Next Hop for the neighbours.

2. **Identify the class/specialty of the following IP addresses: (May 2009)**

a)110.34.56.45 b)127.1.1.1 c)212.208.63.23 d)255.255.255.255

a)110.34.56.45 - Class A

b)127.1.1.1 - Loop back address

c)212.208.63.23 - Class C d)255.255.255.255 –
Broadcast address

3. **What is the purpose of Address Resolution Protocol(ARP)? (May 2009)**

ARP is a dynamic mapping method that finds a physical address for a given logical address. i.e. mapping IP address to physical address.

4. **What is multicasting? .(Nov Dec 2010)&(Nov Dec 2011)**

Multicasting is a technical term that means that you can send a piece of data (a *packet*) to multiple sites at the same time. (How big a packet is depends on the protocols involved-it may

range from a few bytes to a few thousand.) The usual way of moving information around the Internet is by using *unicast* protocols -- tools that send packets to one site at a time.

5. What are the different kinds of multicast routing? (May 2011)

Different kinds of multicast routing are reverse path multicasting and reverse path broadcasting.

6. Define subnetting. (May 2011)

Subnetting is a technique that allows a network administrator to divide one physical network into smaller logical networks and thus, control the flow of traffic for security or efficiency reasons.

7. What is multicast? What is the motivation for developing multicast? (May 2011)

Multicasting means delivering the same packet simultaneously to a group of clients. Motivation for developing multicast is that there are applications that want to send a packet to more than one destination hosts.

8. Expand and define MTU. (May 2012)

Maximum Transmission Unit. MTU is a networking term defines the largest packet size that can be sent over a network connection.

9. What are the salient features of IPV6? .(Nov Dec 2012)

The following are the features of the IPV6 protocol:

- New header format
- Large Address space
- Efficient and hierarchical addressing and routing infrastructure
- Stateless and stateful address configuration
- Built-in security
- Better support for quality of service (QoS)
- New protocol for neighboring node interaction
- Extensibility

10. Define source routing. (Dec 2013)

All the information about the network topology is required to switch a packet across the network is provided by the source host. For switching that uses neither virtual circuits nor conventional datagrams is known as source routing.

11. What is the need of subnetting? (Dec 2013)

Subnetting divides one large network into several smaller ones. Subnetting adds an intermediate level of hierarchy in IP addressing.

12. Define packet switching?

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

13. 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.

14. 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.

15. 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 exists only for the duration of specific exchange.

16. 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 users on a continuous basis. The circuit is dedicated to the specific uses.

17. 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.

18. What is VCI?

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.

19. 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.

20. Explain the term best-effort?

If something goes wrong and the packet gets lost, corrupted, misdelivered, or in any way fails to reach its intended destination, the network does nothing.

21. What is maximum transmission unit?

MTU- which is the largest IP datagram that it can carry in a frame .

22. Define Routing?

It is the process of building up the tables that allow the collect output for a packet to be determined.

23. Define ICMP?

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

24. Write the keys for understanding the distance vector routing?

The three keys for understanding the algorithm are,

Knowledge about the whole networks

Routing only to neighbors

Information sharing at regular intervals

25. Write the keys for understanding the link state routing?

The three keys for understanding the algorithm are,

- Knowledge about the neighborhood.
- Routing to all neighbors.
- Information sharing when there is a range.

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

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

27. 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.

28. What are the features in OSPF?

- Authentication of routing Messages.
- Additional hierarchy.
- Load balancing.

PART B

1. Explain in detail Unicast routing protocol.
2. Explain Interdomain routing.
3. Explain the RIP algorithm with a simple example.
4. Describe the distance vector routing protocol with examples.
5. Discuss briefly about OSPF.
6. Explain the shortest path algorithm with suitable illustrations.
7. Explain multicast routing in detail.
8. Discuss in detail the various aspects of IPv6.

PART C

1. Problems on Distance vector routing.
2. Problems on RIP.
3. Problems on shortest path routing.
4. Case study on IPv6.
5. Problems on Multicast Addressing.

UNIT 4-TRANSPORT LAYER

PART A

1. What are the advantages of using UDP over TCP? (Dec-10)

TCP always guarantees three things - your data reaches its destination, it reaches there in time and it reaches there without duplication.

In TCP, since all the work is done by the operating system, so you just need to sit back and watch the show. Even the debugging is taken care of by your OS.

It automatically breaks up data into packets for you.

It is slower in functioning than UDP.

2. Give the approaches to improve the QoS. (May-11)

Fine granted approaches: Provide QoS to individual applications or flows.

Coarse granted approaches: Provide QoS to large classes of data.

3. What is TCP? (Dec-11)

The Transmission Control Protocol (TCP) is one of the two original core protocols of the Internet protocol suite (IP) and is so common that the entire suite is often called *TCP/IP*.

TCP provides a connection oriented, reliable byte stream services.

The term connection oriented means the two applications using TCP must establish a TCP connection with each other before they can exchange data.

4. Define congestion.(Dec-11)

A state occurring in part of a network when the message traffic is so heavy that it slows down network response time.

5. Draw TCP header format. (May 12)

0	4	10	16	32
SOURCE PORT		DESTINATION PORT		
SEQUENCE NUMBER				
ACKNOWLEDGEMENT				
HdrLen	0	FLAGS	ADVERTISED WINDOW	
CHECKSUM		UrgPtr		
OPTIONS (VARIABLE)				
DATA				

6. Explain how TCP flow control works. (May /Jun 2007)

TCP flow control mechanism achieve using Sliding window mechanism that generates that the receive buffer does not overflow. To avoid congestion, TCP uses the Additive Increase and Multiple Decrease (AIMD) concepts.

The TCP sender is not allowed to send more data than the receiver can receive.

Because TCP connections are full duplex, this happens in both directions.

7. What do you mean by Qos? (May-12)

Quality of service is used in some organizations to help provide an optimal end-user experience for audio and video communications.

QoS is most commonly used on networks where bandwidth is limited.

8. Differentiate between delay and jitter. (Dec 13)

Delay: It is the time taken by a packet to travel across the network from source to destination.

Jitter: It is an unwanted variation of one or more characteristics of a periodic signal in electronics and telecommunications. Jitter may be seen in characteristic such as the interval between successive pulses, or the amplitude, frequency, or phase of successive cycles. Jitter is a significant factor in the design of almost all communications links.

9. What is the difference between congestion control and flow control? (May 11)

FLOW CONTROL	CONGESTION CONTROL
Done by server machine	Done by Router

Cannot block the bandwidth of the medium	Block the bandwidth of the medium
Affect less on network performance	Affects on network performance
Use buffering	Does not use buffering

10. Define slow start.(May-14)

Slow-start is part of the congestion control strategy used by TCP, the data transmission protocol used by many Internet applications. *Slow-start* is used in conjunction with other algorithms to avoid sending more data than the network is capable of transmitting, that is, to avoid causing network congestion.

11. When can application make use of UDP? (May-14)

Fast data transmission & multicast operation

12. Explain the main idea of UDP?

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.

13. What are the different fields in pseudo header?

Protocol number Source IP address
Destination IP addresses.

14. Define TCP?

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.

15. 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.

16. 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.

17. 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.

18. 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.

19. 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.

20. 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.

21. Define Gateway.

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

22. What is meant by quality of service?

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.

23. What are the two categories of QoS attributes?

The two main categories are,
User Oriented
Network Oriented

24. 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.

25. 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).

26. 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.

27. 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

28. What is Silly Window Syndrome?

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

PART B

1. Explain in detail about the simple demultiplexing and reliable byte stream.
2. Explain the three way handshake protocol.
3. Write a detailed note on: i)RPC ii) RTP.
4. Illustrate and explain UDP and its packet format.

5. With neat architecture explain TCP in detail.
6. Give and explain the TCP header format.
7. What is need for Nagle's algorithm? How does it determine when to transmit data?
8. Explain the additive increase/multiplicative decrease methods used in TCP for congestion control.
9. Explain the adaptive flow control.
10. Explain the principles of congestion control in TCP.

PART C

1. Problems on TCP sliding window protocol
2. Case study on TCP and UDP protocol
3. Token bucket algorithm problems.
4. Case study on Qos parameters

UNIT 5-APPLICATION LAYER

PART A

1. What is a Domain Name Service? .(Nov Dec 2006)

The Domain Name System (DNS) is a hierarchical distributed naming system for computers, services, or any resource connected to the Internet or a private network. It associates various information with domain names assigned to each of the participating entities. Most prominently, it translates easily memorized domain names to the numerical IP addresses needed for the purpose of locating computer services and devices worldwide. By providing a worldwide, distributed keyword-based redirection service, the Domain Name System is an essential component of the functionality of the Internet.

2. What is MIME? .(Nov Dec 2007)

MIME stands for Multi-purpose Internet Mail Extensions. MIME types form a standard way of classifying file types on the Internet. Internet programs such as Web servers and browsers A MIME type has two parts: a type and a subtype.

3. Why is DNS necessary? State it significance. (May Jun 2007)

For unique client/server identification in the network, the DNS is necessary. It provides two addressing scheme number-based Internet Protocol addresses and text-based Domain Name System (DNS) names. A domain name is a textual address for a location on the Internet.

4. What is Security Parameter Index? (May Jun 2007)

The Security Parameter Index (SPI) is an identification tag added to the header while using IPsec for tunneling the IP traffic. This tag helps the kernel discern between two traffic streams where different encryption rules and algorithms may be in use. The SPI is an essential part of an IPsec Security Association (SA) because it enables the receiving system to select the SA under which a received packet will be processed.

5. What are the two main categories of DNS messages? (Nov Dec 2008)

DNS has two types of messages: Query and response.

Query: header and question records

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

6. How is HTTP similar to SMTP? (Nov Dec 2008)

HTTP is like SMTP because the data transferred between the client and server are similar in appearance to SMTP messages. Also, the format of the messages is controlled by MIME-like headers

7. What is SMTP? (Dec-10)

The protocol that supports email on the Internet is called Simple Mail Transfer Protocol. SMTP is part of the TCP/IP protocol suite SMTP consists of two parts: A local part and a domain name separated by an @ sign Local Part @ Domain Name.

8. What is Telnet? (Dec-11)

Telnet is the standard TCP/IP protocol for virtual terminal service. It enables the establishment of a connection to a remote s/m in such a way that the local terminal appears to be a terminal at remote system.

9. State the purpose of SNMP. (Dec-11)

Simple Network Management Protocol (SNMP) is a standard internet protocol enabling certain nodes in a network (the management stations or managing nodes) to query other network components or applications for information about their status and activities. Such a query is known as an SNMP poll.

10. Define SNMP. (May-12)

Refer 5.A.9

11. Why email security is necessary? (Dec-11)

It is the process of using email encryption to send messages that can only be opened by the intended recipient. Secure email encryption protects both your online data and customers sensitive information.

12. What is SMTP? (Dec-10)

Refer 5.A.7

13. What are the advantages of allowing persistent TCP connection in HTTP? (Dec-11)

HTTP requests and responses can be pipelined on a connection

Network congestion is reduced by reducing the no. of packets caused by TCP opens.

Latency on subsequent requests is reduced.

14. What do you mean by TELNET? (May-14)

Refer 5.A.8

15. What is the function of SMTP?

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.

16. 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.

17. How does MIME enhance SMTP?

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

18. 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.

19. What is the purpose of Domain Name System?

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

20. 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.

21. Discuss the TCP connections needed in FTP.

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

22. Discuss the basic model of FTP.

The client has three components: the user interface, the client control process, and the client data transfer process. The server has two components: the server control process and the server data transfer process. The control connection is made between the control processes. The data connection is made between the data transfer processes.

23. Name four factors needed for a secure network?

Privacy: The sender and the receiver expect confidentiality.

Authentication: The receiver is sure of the sender's identity and that an imposter has not sent the message.

Integrity: The data must arrive at the receiver exactly as it was sent.

Non-Reputation: The receiver must able to prove that a received message came from a specific sender.

24. How is a secret key different from public key?

In secret key, the same key is used by both parties. The sender uses this key and an encryption algorithm to encrypt data; the receiver uses the same key and the corresponding decryption algorithm to decrypt the data. In public key, there are two keys: a private key and a public key. The private key is kept by the receiver. The public key is announced to the public.

25. What is a digital signature?

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

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

Advantages:

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

Disadvantage:

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

27. What are the advantages & disadvantages of secret key encryption?

Advantage:

Secret Key algorithms are efficient: it takes less time to encrypt a message. The reason is that the key is usually smaller. So it is used to encrypt or decrypt long messages.

Disadvantages:

- a) Each pair of users must have a secret key. If N people in world want to use this method, there needs to be $N(N-1)/2$ secret keys. For one million people to communicate, a half-billion secret keys are needed.
- b) The distribution of the keys between two parties can be difficult.

28. Define permutation.

Permutation is transposition in bit level. Straight permutation: The no. of bits in the input and output are preserved.

Compressed permutation: The no. of bits is reduced (some of the bits are dropped).

Expanded permutation: The no. of bits is increased (some bits are repeated).

29. Define substitution & transposition encryption?

Substitution: A character level encryption in which each character is replaced by another character in the set.

Transposition: A Character level encryption in which the characters retain their plaintext but the position of the character changes.

30. Define CGI?

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

31. 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.

32. Define PGP?

Pretty Good Privacy is used to provide security for electronic mail. It provides authentication, confidentiality, data integrity, and non repudiation.

33. What is IMAP?

IMAP (Internet Message Access Protocol) is a standard protocol for accessing email 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.

34. What is SSH?

(Secure Shell) A security protocol for logging into a remote server. SSH provides an encrypted session for transferring files and executing server programs. Also serving as a secure client/server connection for applications such as database access and e-mail SSH supports a variety of authentication methods.

PART B

1. Explain in detail about the SMTP protocol
2. Explain in detail Write short note on E-mail
3. Explain the final delivery of email to the end user using POP3
4. Explain the HTTP. Give their uses, state strengths an weakness.
5. Explain with example: RTP
6. Write short notes on DNS
7. Write the short notes on web services.
8. Explain in detail about name services.
9. Discuss the advantages of DNS.
10. Discuss in detail about the WWW in detail.

PART C

1. Case study on WWW
2. Case study on XML and XSL
3. Case study on SNMP,TFTP,FTP
4. Case study on TELNET.