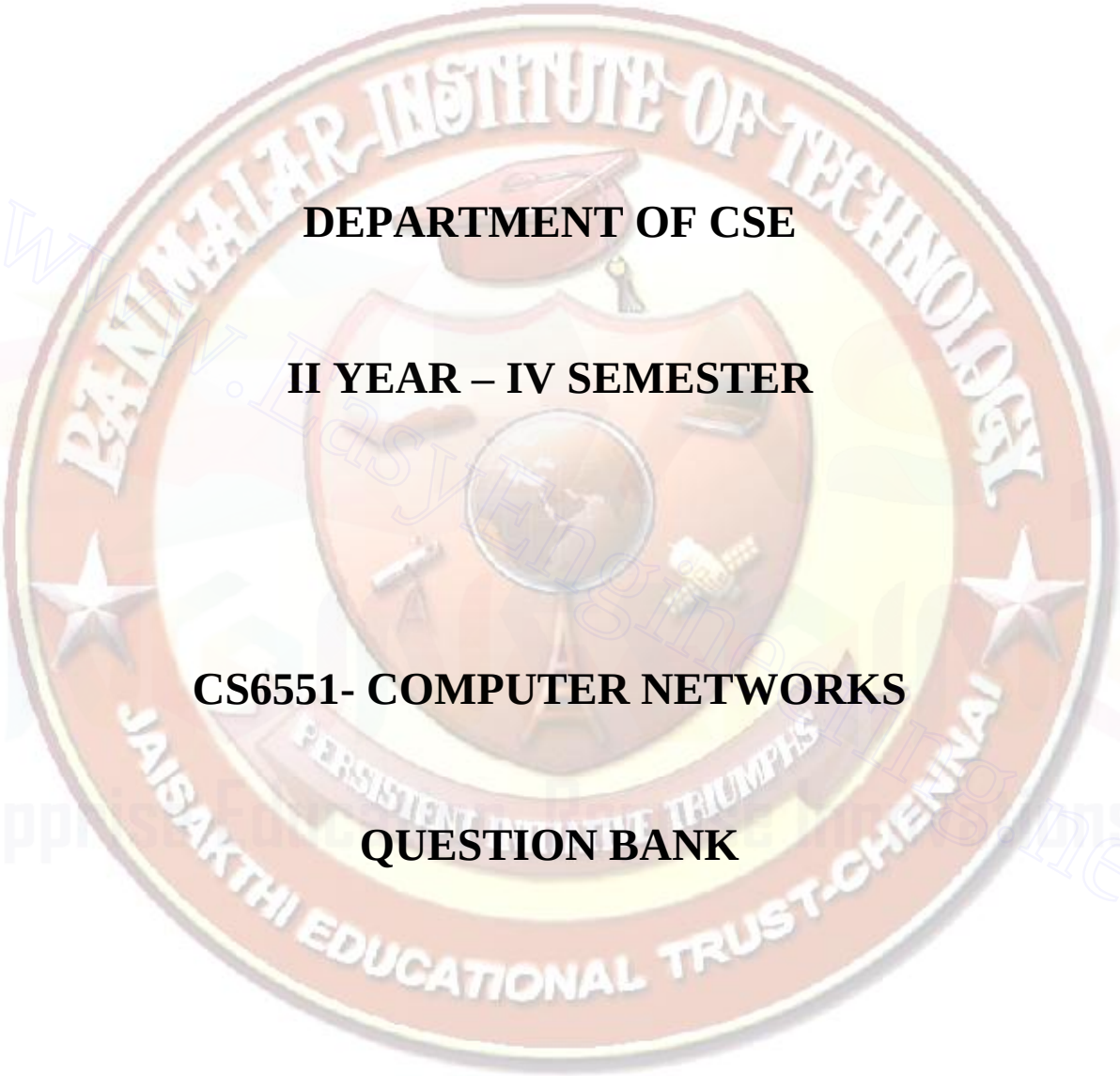


DEPARTMENT OF CSE

II YEAR – IV SEMESTER

CS6551- COMPUTER NETWORKS

QUESTION BANK

CS6551 - COMPUTER NETWORKS

OBJECTIVES: **The student should be made to:**

- Understand the division of network functionalities into layers.
- Be familiar with the components required to build different types of networks
- Be exposed to the required functionality at each layer
- Learn the flow control and congestion control algorithms

UNIT I FUNDAMENTALS & LINK LAYER 9

Building a network – Requirements - Layering and protocols - Internet Architecture – Network software – Performance ; Link layer Services - Framing - Error Detection - Flow control

UNIT II MEDIA ACCESS & INTERNETWORKING 9

Media access control - Ethernet (802.3) - Wireless LANs – 802.11 – Bluetooth - Switching and bridging – Basic Internetworking (IP, CIDR, ARP, DHCP,ICMP)

UNIT III ROUTING 9

Routing (RIP, OSPF, metrics) – Switch basics – Global Internet (Areas, BGP, IPv6), Multicast – addresses – multicast routing (DVMRP, PIM)

UNIT IV TRANSPORT LAYER 9

Overview of Transport layer - UDP - Reliable byte stream (TCP) - Connection management - Flow control - Retransmission – TCP Congestion control - Congestion avoidance (DECbit, RED) – QoS – Application requirements

UNIT V APPLICATION LAYER 9

Traditional applications -Electronic Mail (SMTP, POP3, IMAP, MIME) – HTTP – Web Services – DNS - SNMP

TOTAL: 45 PERIODS

OUTCOMES:

At the end of the course, the student should be able to:

- Identify the components required to build different types of networks
- Choose the required functionality at each layer for given application
- Identify solution for each functionality at each layer
- Trace the flow of information from one node to another node in the network

TEXT BOOK:

1. Larry L. Peterson, Bruce S. Davie, “Computer Networks: A Systems Approach”, Fifth Edition, Morgan Kaufmann Publishers, 2011.

REFERENCES:

1. James F. Kurose, Keith W. Ross, “Computer Networking - A Top-Down Approach Featuring the Internet”, Fifth Edition, Pearson Education, 2009.

2. Nader. F. Mir, “Computer and Communication Networks”, Pearson Prentice Hall Publishers, 2010.

3. Ying-Dar Lin, Ren-Hung Hwang, Fred Baker, "Computer Networks: An Open Source Approach", Mc Graw Hill Publisher, 2011.
4. Behrouz A. Forouzan, "Data communication and Networking", Fourth Edition, Tata McGraw – Hill, 2011.

COURSE OUTCOMES

CO1	An ability to understand the Internet Architecture and apply knowledge of different techniques of error detection methods to detect errors
CO2	An ability to identify the components required to build different types of networks
CO3	An ability to design network routing for internetworks
CO4	An ability to analyze the services and features of the transport layer protocols
CO5	An ability to analyze the features and operations of various application layer protocols such as HTTP, DNS, and SMTP.

UNIT I

FUNDAMENTALS & LINK LAYER

Building a network – Requirements - Layering and protocols - Internet Architecture – Network software – Performance ; Link layer Services - Framing - Error Detection - Flow control

PART A

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

- 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.

2. Group the OSI layers by function? C

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.

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

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.

4. What are the features provided by layering? R

Two features:

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

5. Why are protocols needed? AN

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.

6. What are the two interfaces provided by protocols? R

- 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.

7. Mention the different physical media? R

- 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)

8. Define Signals? R

Signals are actually electromagnetic waves traveling at the speed of light. The speed of light is, however, medium dependent-electromagnetic waves traveling through copper and fiber do so at about two-thirds the speed of light in vacuum.

9. What is wave's wavelength? U

The distance between a pair of adjacent maxima or minima of a wave, typically measured in meters, is called wave's wavelength.

10. Define Modulation? R

Modulation -varying the frequency, amplitude or phase of the signal to effect the transmission of information. A simple example of modulation is to vary the power (amplitude) of a single wavelength.

11. Explain the two types of duplex?U

- 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 CODEC? U

A device that encodes analog voice into a digital ISDN link is called a CODEC, for coder/decoder.

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

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

14. List out the different encoding techniques? R

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

15. How does NRZ-L differ from NRZ-I? AN

In the NRZ-L sequence, positive and negative voltages have specific meanings: positive for 0 and negative for 1. in the NRZ-I sequence, the voltages are meaningless.
Instead, the receiver looks for changes from one level to another as its basis for recognition of 1s.

16. What are the responsibilities of data link layer? R

Specific responsibilities of data link layer include the following. a) Framing b) Physical addressing c) Flow control d) Error control e) Access control.

17. What are the ways to address the framing problem? R

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

18. Distinguish between peer-to-peer relationship and a primary-secondary relationship. AN

peer -to- peer relationship: All the devices share the link equally.
Primary-secondary relationship: One device controls traffic and the others must transmit through it.

19. List out the types of errors and define the terms? R

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.

20. List out the available detection methods. R

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.

21. Write short notes on VRC. C

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.

22. Write short notes on LRC. C

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.

23. Write short notes on CRC. C

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.

24. Write short notes on CRC checker. C

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.

25. Define checksum. R

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

26. What are the steps followed in checksum generator? R

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.

27. List out the types of error correcting methods. R

There are 2 error-correcting methods.

- Single bit error correction
- Burst error correction.

28. Write short notes on error detection and correction? C (Nov/Dec 2011)

Error detection is most commonly realized using a suitable hash function (or checksum algorithm). A hash function adds a fixed-length tag to a message, which enables receivers to verify the delivered message by recomputing the tag and comparing it with the one provided.

Error correction 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.

29. What is the purpose of hamming code? U

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.

30. What is redundancy? U

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.

31. Define flow control? R(Nov/Dec 2011 & April/May 2015) (MAY/JUN 2016)

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

32. Mention the categories of flow control? R

There are 2 methods have been developed to control flow of data across communication links. a) Stop and wait- send one from at a time. b) Sliding window- send several frames at a time.

33. What is a buffer? U

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

34. What are the two types of line configuration? R(Nov/Dec 2010)

A link is a communication medium through which data is communicated between devices. For communication to occur between two devices, they must be connected to the same link at the same time. There are two possible types of line configurations or connections.

1. Point-to-point connection.
2. Multipoint connection.

35. What do you mean by error control? U(Nov/Dec 2010 & April/May 2015)

Error control is the response when a receiver detects an error. The three basic forms of error control are Do nothing, return an error message to transmitter, or correct the error with no further information from transmitter.

36. What are the functions of application layer? U(April/May 2011)

The Application layer supplies network services to end-user applications. Network services are typically protocols that work with user's data. The Application layer provides data to (and obtains data from) the Presentation layer.

37. Define bit stuffing. R (April/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.

38. What is the use of two dimensional parity in error detection? U(Nov/Dec 2012)

Two-dimensional parity check increases the likelihood of detecting burst errors.

39. What are the issues in data link layer? R (Nov/Dec 2012) (Nov/Dec 2015)

- Services provided to the network layer
- Framing
- Error control
- Flow control

40. What are the duties of network layer? R (May/June 2012)

Transport packet from sending to receiving hosts

Three important function:

Path determination: Route taken by packets from source to destination using routing algorithms.

Switching: Move a packet from router's input to appropriate router output.

Call Setup: Some network architectures require router call setup along path before data flows.

41. What are the two different types of errors occurred during data transmission? R (May/June 2012)

Two main types of errors in a transmission .

1. Single Bit Errors
2. Burst Errors

Single Bit Errors : When an error in the transmission changes a 0 to 1 or 1 to 0, it is called single bit error. These are the errors that effect only one bit in the transmission of a data unit.

Burst Errors:When an error in the transmission changes two or more bits in the data unit. It is called as burst error. The burst errors occur more frequently than single bit errors. In burst errors consecutive bits or no conjectured bits can be corrupted.

42. State the purpose of layering. R(May/June 2013)

The purpose of layering is to separate functional components that interact in some sequential and hierarchical way, with each layer usually having an interface only to the layer above it and the layer below it.

43. Mention the advantage and disadvantage of error correction by receiver, as compared to error detection. U (May/June 2013)

Advantage:

- Original data can be obtained through error correction.
- Receiver identifies and corrects the error.

Disadvantage:

- Extra redundant bits are used.
- If the storage is the only source of data (e.g. disk or DRAM)then we want a error-correction to avoid crashing of programs.

44. Define a layer.R (Nov/Dec 2013)

A networking system is simpler, cheaper, and more reliable if it is implemented in terms of layers. Each layer accepts responsibility for a small part of the functionality. Having a clean separation of function between layers means that multiple layers do not need to duplicate functionality. It also means that layers are less likely to interfere with one another.

45. What do you mean by framing? U **(Nov/Dec 2013)**

A point-to-point connection between two computers or devices consists of a wire in which data is transmitted as a stream of bits. However, these bits must be *framed* into discernible blocks of information. Framing is a function of the data link layer which provides a way for a sender to transmit a set of bits that are meaningful to the receivers. Framing separates a message from one source to a destination from other messages.

46. What is the difference between port address, logical address and physical address? U (May/June 2014)

Logical Address:

An IP address of the system is called logical address. This address is the combnation of Net ID and Host ID. This address is used by network layer to identify a particular network (source to destination) among the networks. This address can be changed by changing the host position on the network. So it is called logical address.

Physical address: Each system having a NIC (Network Interface Card) through which two systems physically connected with each other with cables. The address of the NIC is called Physical address or mac address. This is specified by the manufacture company of the card. This address is used by data link layer.
Port Address: There are many applications running on the computer. Each application run with a port no.(logically) on the computer. This port no. is called port address.

47. What will be the maximum number of frames sent but unacknowledged for a sliding window of size n-1 (n is the sequence number)? AP (May/June 2014)

The maximum number of frames sent but unacknowledged for a sliding window of size n-1 is n.

48. Define the term protocol. R (Nov/Dec 2015)

A **communications protocol defines** the rules for sending blocks of **data** (each known as a **Protocol Data** Unit (PDU)) from one node in a network to another node. **Protocols** are normally **defined** in a layered manner and provide all or part of the services specified by a layer of the OSI reference model.

49.Write the parameters used to measure network performance. C (MAY/JUNE 2016)

- Bandwidth
- Latency
- Throughput
- Jitter
- Error rate

PART B

1. Explain in detail the error detection and error corrections**. U(NOV 2010) &(MAY/JUNE 2012)**
2. Discuss in detail about the layers of OSI model. U**(NOV 2010) & (NOV2011) & (MAY/JUNE 2012) (NOV/DEC 2015)**
3. Explain the different types of multiplexing. U**(NOV/DEC 2011)**
4. Discuss in detail about HDLC. U
5. Discuss in detail about SONET.U
6. Explain the different approaches of framing in detail. U
7. Write the Sliding Window Algorithm and explain it in detail.C
8. Compare Stop and Wait ARQ scheme with sliding window ARQ scheme. AP
9. Write in detail about the various flow control mechanisms. **C(NOV/DEC 2015)**

10. Explain in detail about the following U **(APRIL/MAY 2011)**

(i) PPP (5)

(ii) HDLC (5)

(iii) SONET (6)

11. Explain in detail about the network architecture. U **(APRIL/MAY 2011)**

12.Explain the following Error detection mechanism. U **(NOV/DEC 2012)**

(i) Cyclic Redundancy check

(ii) Link Level Control

13.(i) Discuss the framing technique used in HDLC. What is the effect of errors on this Framing? (8) U **(MAY/JUNE 2013)**

(ii) The message 11001001 is to be transmitted, using CRC Error Detection algorithm. Assuming the CRC polynomial to be $x^3 + 1$, determine the message that should be transmitted . If the second left most bit is corrupted, show that it is detected by the receiver. AP (8)

14.(i) Discuss the principle of stop and wait flow control algorithm. Draw time line diagrams and explain how loss of a frame and loss of an ACK are handled. What is the effect of delay-bandwidth product on link utilisation? (8) U**(MAY/JUNE 2013)**

(ii) Assume that a frame consists of 6 characters encoded in 7-bit ASCII. Attach a parity bit for every character to maintain even parity. Also attach a similar parity bit for each bit position across each of the bytes in the frame. Show that such a 2-dimensional parity scheme can detect all 1-bit, 2-bit and 3-bit errors and can correct a single brit error. AP(8)

15.(i) Explain NRZ,NRZI & Manchester encoding schemes with examples.U (8)

(ii) Describe how bit stuffing works in HDLC protocol. (8) U **(NOV/DEC 2013)**

16. (i) Discuss the issues in the data link layer. U (4)

(ii) Suppose we want to transmit the message 11001001 and protect it from errors using the CRC polynomial $x^3 + 1$. Use polynomial long division to determine the message that should be transmitted.(12) AP **(NOV/DEC 2013)**

17. Given a remainder of 111, a data unit of 10110011 and a divisor of 1001,is there an error in the data unit. Justify your answer with necessary principles.AN**(MAY/JUNE 2014)**

18. How is frame order and flow control achieved using the data link layer?AN **(MAY/JUNE 2014)**

19. Discuss in detail about Internet Architecture. (16) U**(APRIL/MAY 2015)**

20. What is the need for error detection? Explain with typical examples. Explain methods used for error detection and error correction. (16) U**(APRIL/MAY 2015)**

21. Explain any two error detection mechanism in detail. **(16) U (MAY/JUN 2016)**

22. Explain in detail about : U **(MAY/JUN 2016)**

i. HDLC (8)
ii. PPP (8)

UNIT II

PART A

1. What are the functions of MAC? R

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 are the functions of LLC? R

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.

3. What is Ethernet? U

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

4. Define the term carrier sense in CSMA/CD? R (Nov/Dec 2011)

All the nodes can distinguish between idle and a busy-link and "collision detect" 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.

5. Define Repeater?R

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.

6. Define collision detection?R

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.

7. Why Ethernet is said to be a I-persistent protocol? AN

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

8. What is exponential back off? U

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.

9. What is token holding time (THT)? U

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.

10. What are the two classes of traffic in FDDI? R

- Synchronous
- Asynchronous

11. What are the four prominent wireless technologies? R

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

12. Define Bluetooth? R

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.

13. What are the four steps involves in scanning?R

1. The node sends a Probe frame.
2. All APs within reach reply with a Probe Response frame.
3. The node selects one of the access points, and sends that AP an Association Request frame.
4. The AP replies with an Association Response frame.

14. Explain the term handoff? U

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.

15. Define satphones? R

Satphones use communication satellites as base stations, communicating on frequency bands that have been reserved internationally for satellite use.

16. How to mediate access to a shared link? AN

Ethernet,token ring, and several wireless protocols. Ethernet and token ring media access protocols have no central arbitrator of access. Media access in wireless networks is made more complicated by the fact that some nodes may be hidden from each other due to range limitations of radio transmission.

17. Define Aggregation points? R

It collects and processes the data they receive from neighboring nodes, and then transmit the processed data. By processing the data incrementally, instead of forwarding all the raw data to the base station, the amount of traffic in the network is reduced.

18. Define Beacons?R

Beacon to determine their own absolute locations based on GPS or manual configuration. The majority of nodes can then derive their absolute location by combining an estimate of their position relative to the beacons with the absolute location information provided by the beacons.

19. What is the use of Switch?U

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.

20. Explain Bridge? U(Nov/Dec 2011)

It is a collection of LANs connected by one or more bridges is usually said to form an extended LAN. In their simplest variants, bridges simply accept LAN frames on their inputs and forward them out on all other outputs.

21. What is Spanning tree?U

It is for the bridges to select the ports over which they will forward frames.

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

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

23. What is broadcast? U

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.

24. What is multicast? U

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

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

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.

26. What are the limitations of bridges? R

- scale
- heterogeneity

27. What are the functions of bridges? R (Nov/Dec 2010 & April/May 2015)

A network bridge, also known as a layer 2 switch, is a hardware device used to create a

connection between two separate computer networks or to divide one network into two. The principal function of a network bridge is to forward data a based on the MAC address of the sending and receiving devices. A network bridge, also known as an Ethernet bridge, connects two segments of a network together. The segments are no independent entities, but are owned and managed by the same organization.

28. What is the advantage of FDDI over a basic token ring? U (Nov/Dec 2010)

Token ring uses priority and reservation bits, but the priority operation of the FDDI ring uses a principle that is based on a parameter known as the Token Rotation Time or TRT. FDDI uses dual rings. When one ring fails, second ring performs data transfer process.

29. Mention some of the physical properties of Ethernet. R(April/May 2011)

Implemented on coaxial cable of up to 500 meters in length

- Hosts connect by "tapping" into it.
  Taps at least 2.5 meters apart
- Transceiver is small device directly attached to tap
  Detects when line is idle and drives signal when host is transmitting
- All protocol logic implemented in the adaptor (not transceiver)

30. What is hop-by-hop flow control? U

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.

31. Explain the term best-effort? U

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

32. What is maximum transmission unit?(May/June 2012)

MTU-Maximum Transmission Unit, which is the largest IP datagram that it can carry in a frame. It is the largest physical packet size, measured in bytes, that a network can transmit. Any messages larger than the MTU are divided into smaller packets before being sent.

33. Define Routing? R

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

34. Define ICMP? R

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.

35. Define Subnetting? R(Nov/Dec 2011) (Nov/Dec 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.

36.What is DHCP? U (Nov/Dec 2012)

The Dynamic Host Configuration Protocol (DHCP) is a network protocol used to configure devices that are connected to a network (known as hosts) so they can communicate on that network using the Internet Protocol (IP). It involves clients and a server operating in a client-server model.

37. Define Source routing. R **(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.

38. What is the need of subnetting? AP(Nov/Dec 2013)

Subnetting changes the subnet mask of the local network number to produce an even number of smaller network numbers, each with a corresponding range of IP addresses. Subnetting is required when one network number needs to be distributed across multiple LAN segments.

39. What is the need for ARP? AP(Nov/Dec 2013) (Nov/Dec 2015)

- The address resolution protocol (arp) is a protocol used by the Internet Protocol (IP), to map IP network addresses to the hardware addresses used by a data link protocol.
- The protocol operates below the network layer as a part of the interface between the OSI network and OSI link layer.
- Address resolution refers to the process of finding an address of a computer in a network.

40. Differentiate fast Ethernet and gigabit. AN (Nov/Dec 2012)

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)

41. What is the difference between switch and Hub? AN (Nov/Dec 2012)

Hub:

Many kinds of nodes can be connected to the hub with networking cable.

- All hubs can be uplinked together, either with straight-through cable or cross-over cable, depending on whether or not the hub has an uplink port.
- Performance will decrease as the number of users is increased.

Switches have many features that make them different than hubs. The most reason to choose a switch rather than a hub is bandwidth. When a 100Mbps hub has five workstations, each receives 20Mbps of bandwidth. When a 10/100Mbps switch is used, each workstation receives 100Mbps of bandwidth, dramatically increasing the speed of the connection.

42. List out any four IEEE 802 standards with its name. R(May/June 2012)

Standard	Description
802.1	Internetworking
802.2	Logical link control
802.3	Ethernet
802.4	Token bus
802.5	Token ring
802.6	Metropolitan area network (MAN)

43. Define Bridge and Switch. R (May/June 2012)

A bridge is a network device that connects more than one network segment. A switch is a small hardware device that joins multiple computers together within one local area network (LAN). Technically, network switches operate at layer two (Data Link Layer) of the OSI model.

44. How is the minimum size of an Ethernet frame determined? AP(May/June 2013)

Minimum Frame Size = 2 * Maximum distance *(data rate / propagation speed)

45. How does an FDDI node determine whether it can send asynchronous traffic and synchronous traffic? AN (May/June 2013)

Synchronous traffic can consume a portion of the 100-Mbps total bandwidth of an FDDI network, while asynchronous traffic can consume the rest. Synchronous bandwidth is allocated to those stations requiring continuous transmission capability. Such capability is useful for transmitting voice and video information. Other stations use the remaining bandwidth asynchronously.

46. List the two main limitations of bridges. R (Nov/Dec 2013)

A bridge is a device to join two network segments. The advantage is it's cheap,easy, doesn't require routing. The disadvantages are it doesn't supportrouting and most bridges don't support any kind of traffic filtering. Bridges aren't much used any more on physical LANS, but are important on virtual LANS and in wireless.

47. **What is the average size of an Ethernet frame? U(May/June 2014)**

The average size of an Ethernet frame is 1000 bytes.

48. What is the access method used by wireless LAN? U(May/June 2014)

- WiMAX(802.16)
- Wi-Fi
- Bluetooth

49. What is the network Address in a class A subnet with the IP address of one of the hosts as 25.34.12.56 and mask 255.255.0.0? AP(May/June 2014)

The network Address in a class A subnet is 25.34.0.0

50. How does a router differ from a bridge? AN (April/May 2015)

S.NO	BRIDGE	ROUTER
1.	Does not block any broadcast or multicast	Block and provide protection against broadcast storms
2.	Transparent bridge and can pass Non-IP protocols	Only IP protocol is supported
3.	PPPOE Protocol Pass through	No PPPOE protocol pass through
4.	Able to transport VLAN tagging	Does not support VLAN
5.	No network segmentation. One broadcast domain	Network Segmentation (Client can be on different IP subnet)
6.	Bridges maintains bridging table(Mac) &STP can be used to avoid loops	No STP features maintains routing table

51. What do you understand by CSMA protocol? U (April/May 2015)

The "carrier sense" in CSMA/CD means that all the nodes can distinguish between an idle and a busy link, and "collision detect" means that all the nodes listens as it transmits and can therefore detect when a frame it is transmitting has interfered (collided) with a frame transmitted by another node.

52. Define hidden node problem. R (MAY/JUN 2016)

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

53. What is Bluetooth? R (MAY/JUN 2016)

Bluetooth is a wireless technology standard for exchanging data over short distances from fixed and mobile devices, and building personal area networks.

PART B

1. Name the four basic network topologies and explain them giving all the relevant features. **(NOV/DEC 2010) U**
2. Explain the functioning of wireless LAN in detail**. U(NOV/DEC 2010)**
3. Explain in detail about token ring and its frame format .U**(NOV/DEC 2011)**
4. Discuss the various, aspects of FDDI in detail. U**(NOV/DEC 2011)**
5. Differentiate FDDI from token ring.AN
6. Write short notes on WI-Fi,Wi-Max. U
7. (i) Explain how bridges run a distributed spanning tree algorithm. U**(APRIL/MAY 2011)**
   (ii) Explain segmentation and reassembly. U
8. Explain CSMA in detail. U**(APRIL/MAY 2011)**

9. Explain the physical properties of Ethernet 802.3 with necessary diagram of Ethernet transceiver and adapter. U **(NOV/DEC 2012)**

10. Write notes on the following U**(NOV/DEC2010)**

(i) Internet protocol. (ii) Routers.

11. Discuss in detail the various aspects of IPV6& its new features. U**(NOV/DEC 2010) & (MAY/JUNE 2012)**

12. Discuss the spanning tree algorithm in detail. What are the limitations of bridges? U

13. Explain in detail about ARP,DHCP,ICMP. U **(NOV/DEC2015)**

14. Write short notes on : U

(i) Ethernet (8)
(ii) Wireless LAN (8)

15. Explain about the physical properties, timed token algorithm, frame format of FDDI. U **(MAY/JUNE 2012)**

16. (i) Explain in detail about Address Resolution Protocol. U **(NOV/DEC 2012)**

(ii) What is subnetting? Explain.U

17. Explain the following: U **(NOV/DEC 2012)**

Error reporting(ICMP)

18. What is the need for ICMP? Mention any four ICMP messages and their purpose. (6) U **(MAY/JUNE 2013)**

19. Discuss the Problems in subnetting. U**(APRIL/MAY 2011)**

20. (i) How does a bridge come to learn on which port the various host reside? Explain with an example. AN **(NOV/DEC 2012)**

(ii) Explain CSMA in detail.U

21. Explain the physical properties and medium access protocol of Ethernet. U **(MAY/JUNE 2012)**

22. (i) An IEEE 802.5 token ring has 5 stations and a total wire length of 230 m. How many bits of delay must the monitor insert into the ring? Calculate this for both 4 Mbps and 16 Mbps rings. The propagation speed may be assumed to be 2.3 X 10^8 m/s. (6) AP **(MAY/JUNE 2013)**

(ii) Discuss the problems encountered in applying CSMA/CD algorithm to wireless LANs. How does 802.11 specification solve these problems. AN (10)

23. (i) Discuss the limitations of bridges. (6) U**(MAY/JUNE 2013)**

(ii) Determine the maximum distance between any pair of stations in a CSMA/CD network with a data rate of 10 Mbps, for the correct operation of collision detection process, assuming the minimum frame size to be 512 bits. What should be the maximum distance if the data rate is increased to 1 Gbps? 2 stations A and B, connected to the opposite ends of a 10-Mbps CSMA/CD network, start transmission of long frames at times $t_1 = 0$ and $t_2 = 3\mu s$ respectively. Determine the instants when A hears the collision and B hears the collision, Signal propagation speed may be assumed as 2×10^8 m/s. AP (10)

24. (i)Describe the transmitter algorithm implemented at the sender side of the Ethernet protocol. Why should Ethernet frame should be 512 bytes long? (10) AN **(NOV/DEC 2013)**

(ii) Explain how the hidden node and exposed node problem is addressed in 802.11? (6) U

25. Describe how MAC protocol operates on a token ring.(16) **(NOV/DEC 2013)**

26. Describe the CSMA/CD protocol and comment on its performance for medium access. **U (MAY/JUNE 2014)**

27. Write short notes on: U **(MAY/JUNE 2014)**

(i) FDDI (8)

(ii) Bridges and Switches (8)

28. (i) Discuss the IP addressing methods. (8) U **(MAY/JUNE 2014)**

(ii) Write short notes on ARP. (8) U

29. Explain in detail about the access method and frame format used in Ethernet and token ring. (16) U **(APRIL/MAY 2015)**

30. (i) Discuss the MAC layer functions of IEEE802.11 (8) **U (APRIL/MAY 2015)**

(iii) Briefly define key requirements of wireless LAN (8)U

31.Give the comparison between different wireless technologies? Enumerate 802.11 protocol stack in detail. **(16) AN (MAY/JUNE 2016)**

32.Write short notes on : U (**MAY/JUNE 2016)**

i. DHCP (8)
ii. ICMP (8)

UNIT III
PART A

1. Define packet switching?R

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? U

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? R

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? U

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? U

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 is VCI?(April/May 2011) U

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.

7. Write the keys for understanding the distance vector routing? U

The three keys for understanding the algorithm are,

- Knowledge about the whole networks
- Routing only to neighbors
- Information sharing at regular intervals

8. Write the keys for understanding the link state routing? U

The three keys for understanding the algorithm are,

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

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

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.

10. Define Reliable flooding? R

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.

11. What are the features in OSPF? R

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

12. What are the different types of AS? R

- Stub AS
- Multi homed AS
- Transit AS

13. What is an Area? U

An Area is a set of routers that are administratively configured to exchange link-state information with each other. There is one special area- the backbone area, also known as area 0.

14. What is Source Specific Multicast? U

SSM , a receiving host specifies both a multicast group and a specific host .the receiving host would then receive multicast addressed to the specified group, but only if they are from the special sender.

15. What is meant by congestion? U

Congestion in a network occurs if user sends data into the network at a rate greater than that allowed by network resources.

16. Why the congestion occurs in network? AN

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

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

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

18. What is LSP? U

In link state routing, a small packet containing routing information sent by a router to all other router by a packet called link state packet.

19. What is meant by circuit switching? U(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.

20. What is multicasting? U (Nov/Dec 2010) & (Nov/Dec 2011)

Multicast is the delivery of a message or information to a group of destination computers simultaneously in a single transmission from the source. Copies are automatically created in other network elements, such as routers, but only when the topology of the network requires it.

21. List the difference between Circuit switching Packet switching (April/May 2011) & May/June 2014) R

1. Circuit switching is done at physical layer whereas datagram switching is generally done at network layer.

2. Circuit switching requires the resources to be reserved before the transmission of data but datagram switching doesn't require such reservation of resources.

3. In circuit switching, whole of the data travels along a single dedicated path between the two terminals whereas in datagram switching data is divided into packets and each of these packets are treated indepently and travel along different paths, source and destination being the same.

22. What are the different kinds of Multicast routing? R (April/May 2011)

- One-to-Many
- Many-to-Many
- Many-to-One

23. What are the applications of Multicasting? R (May/June 2012)

- Teleconferencing
- Video-on-demand

24. Compare circuit switching and virtual circuit based packet switching, in respect of queueing and forwarding delays. AN

Queueing delay of a packet is the waiting time in the output buffers (input queue in some case)

• Circuit-switched networks do not have forward delays or Queuing delays

• In Virtual Circuit networks, Queueing delay is variable, i.e., it depends on the backlog in the node due to other traffic.

• Variable queueing delay is what makes analysis of packet network.

25. Differentiate between connection less operation and connection oriented operation. AN (May/June 2013)

Feature	Connectionless	Connection-oriented
How is data sent?	one packet at a time	as continuous stream of packets
Do packets follow same route?	no	virtual circuit: yes without virtual circuit: no
Are resources reserved in network?	no	virtual circuit: yes without virtual circuit: no
Are resources reserved in communicating hosts?	no	yes
Can data sent can experience variable latency?	yes	yes
Is connection establishment done?	no	yes
Is state information stored at network nodes?	no	virtual circuit: yes without virtual circuit: no
What is impact of node/switch crash?	only packets at node are lost	all virtual circuits through node fail
What addressing information is needed on each packet?	full source and destination address	virtual circuit: a virtual circuit number without virtual circuit: full source and destination address
Is it possible to adapt sending rate to network congestion?	hard to do	virtual circuit: easy if sufficient buffers allocated without virtual

26. What are the salient features of IPV6? R(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

27. What are the metrics used by routing protocols? R(April/May 2015)

Routing use Routers use various metrics and calculations to determine the best route for a packet to reach its final network destination. Each routing protocol uses its own algorithm with varying weights to determine the best possible path

The following are metrics used in determining the best path for a routing protocol:

- **Bandwidth** – Throughput speed in bits per second
- **Cost** – An arbitrary value assigned by an administrator for the intersecting of networks
- **Delay** – Network latency caused by such factors as distance or congestion
- **Hop Count** – The number of routers (hops) a packets passes through to its destination
- **Load** – Measurement of traffic that flows through a router

- **MTU** (Maximum Transmission Unit) – The largest unit size allowed to be transmitted on all routes from source to destination
- **Reliability** – Represents the amount of network downtime, that is, how reliable a network path is)
- **Ticks** – Measurement of delay, where is tick is 1/18 of a second. A tick is used as part of the routing protocol IPX RIP

28. Define routing. R(NOV/DEC 2015)

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

29. Identify the class of the following IP address: R (NOV/DEC 2015)

(a) 110.34.56.45 - Class A
(b) 212.208.63.23 - Class C

30.Write the types of connecting devices in internetworking U (MAY/JUNE 2016)

Connecting devices are:
Repeaters, hubs, bridges, switches, routers and NIC

31.Expand ICMP and write the function. U (MAY/JUNE 2016)

ICMP (Internet Control Message Protocol) is an error-reporting protocol network devices like routers use to generate error messages to the source IP address when network problems prevent delivery of IP packets.

PART-B

1. What are the different approaches in Packet Switching? Explain them in detail. R
2. What is internetworking? Explain its service model, global address and datagram forwarding. U **(APRIL/MAY 2011)**
3. Explain Distance Vector routing in detail with examples. (16) U **(NOV/DEC 2013) (NOV/DEC 2013) (MAY/JUNE 2016)**
4. Explain OSPF & RIP in detail.U **(MAY/JUNE 2012)**
5. Compare circuit switching with **packet switching. AN(NOV/DEC 2011)**
6. Write short notes on Inter Domain Routing. U
7. Write short notes on the following U

   i.Broadcasting

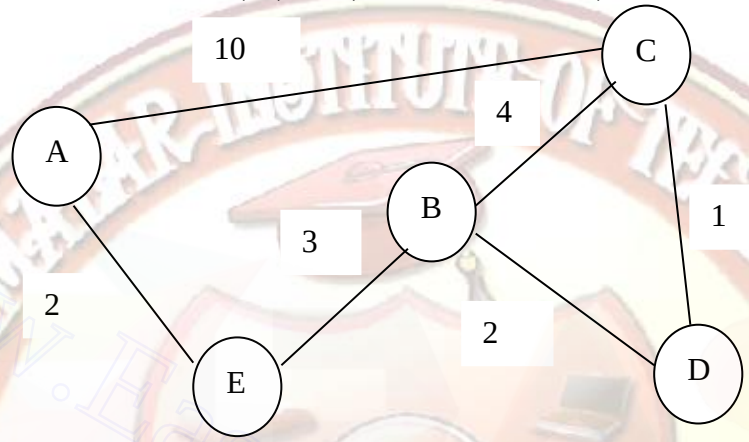
   ii. Multicasting

8. (i) A 4480—byte datagram is to be transmitted through an Ethernet with a maximum data size of 1500 bytes in frames. Show the values of Total Length, M Flag, Identification and

fragment offset fields in each of the fragments created out of the datagram. (10) AP **(MAY/JUNE 2013)**

(ii) Discuss the principles of reliable flooding and its advantages and applications. (6) U

9. (i) For the following network, develop the datagram forwarding table for all the nodes. The links are labeled with relative costs. The tables should forward each packet via the least cost path to destination. (10) AP **(MAY/JUNE 2013)**



10 (i) Suppose hosts A and B have been assigned the same IP address on the same Ethernet, on which ARP is used. B starts up after A. What will happen to A's existing connections? Explain how 'self-ARP' might help with this problem. (4) AN **(NOV/DEC 2013)**

(ii) Describe with example how CIDR addresses the two scaling concerns in the Internet.(12)

11. Explain the RIP algorithm with a simple example of your choice. U**(MAY/JUNE 2014)**

12. Discuss the notation, representation and address space of **IPv6**. U**(NOV/DEC 2011)**

13. Explain the shortest path algorithm with suitable illustrations. (16) U **(APRIL/MAY 2015)**

14. Explain the distance vector routing algorithm. Mention the limitations of the same. (16) **U (APRIL/MAY 2015)**

15. Explain multicast routing in detail. (16) U **(NOV/DEC 2015)**

16. Explain about IPv6? Compare IPv4 and IPv6. **(16) U (MAY/JUNE 2016)**

UNIT IV

TRANSPORT LAYER
PART A

1. Explain the main idea of UDP? U

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.

2. What are the different fields in pseudo header? R

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

3. Define TCP? R(Nov/Dec 2011)

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.

4. Define Congestion Control? R (Nov/Dec 2011)

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.

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

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

6. What is meant by segment? U

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.

7. What is meant by segmentation? U

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.

8. What is meant by Concatenation?U

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.

9. What is rate based design?U

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.

10. Define Gateway. R

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

11. What is meant by quality of service?U

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.

12. What are the two categories of QoS attributes? R

The two main categories are,

- User Oriented
- Network Oriented

13. List out the user related attributes? R

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

14. What are the networks related attributes? R

The network related attributes are, Cell loss ratio (CLR) Cell transfer delay (CTD) Cell delay variation (CDV) Cell error ratio (CER).

15. What is RED? U

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.

16. What are the three events involved in the connection? R

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

17. What is the function of a router? R(Nov/Dec 2010)

A router is a device that forwards data packets between computer networks, creating an overlay internetwork. A router is connected to two or more data lines from different networks. When a data packet comes in one of the lines, the router reads the address information in the packet to determine its ultimate destination.

18. What are the advantages of using UDP over TCP? AN(Nov/Dec 2010)

- No connection establishment
- No connection state
- Small segment header overhead
- Unregulated send rate

19. List the differences between congestion control and flow control? AN (April/May 2011)& (Nov/Dec 2013) (Nov/Dec 2015)

Flow control is a mechanism used in computer networks to control the flow of data between a sender and a receiver, such that a slow receiver will not be outran by a fast sender. Flow control provides methods for the receiver to control the speed of transmission such that the receiver could handle the data transmitted by the sender.

Congestion control is a mechanism that controls data flow when congestion actually occurs. It controls data entering in to a network such that the network can handle the traffic within the network.

20. Give the approaches to improve the QOS. R(April/May 2011)

QoS can be improved with traffic shaping techniques such as packet prioritization, application classification and queuing at congestion points.

21.What is meant by PORT or MAILBOX related with UDP? AN (Nov/Dec 2012)

A Port is a virtual data connection that can be used by programs to exchange data directly, instead of going through a file or other temporary storage location. The most common of these are TCP and UDP ports which are used to exchange data between computers on the Internet. Port 505/udp uses the mailbox-lm protocol for service type mailbox-lm. A malformed request to port 505/udp is known to cause denial of service attacks.

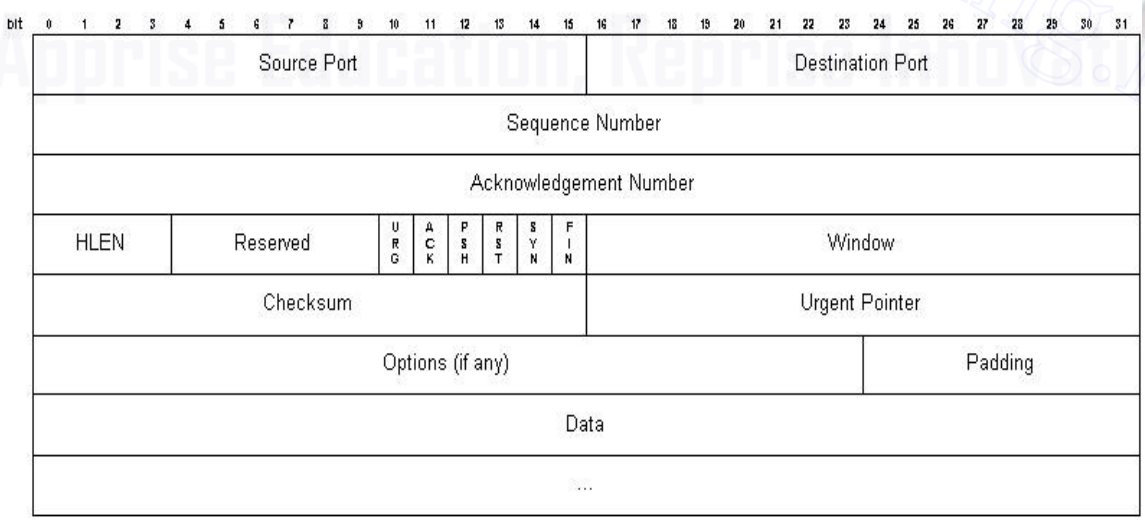
22. List out the various features of sliding window protocol. R(Nov/Dec 2012)

A sliding window protocol is a feature of packet based data transmission protocols. They are used where reliability in order to delivery of packet is required.

Each position of the transmission (packets) is assigned a unique consecutive sequence number and the receiver uses the numbers to place receive packets in correct order.

- Discarding duplicate packets
- Identifying the missing packets

23. Draw the TCP header format. R(May/June 2012)



24. Why is UDP pseudo header included in UDP checksum calculation? What is the effect of an invalid checksum at the receiving UDP? AN (May/June 2013)

In addition to UDP header and data, the UDP checksum includes the source and the destination IP address in order to prevent misrouting. Suppose that the destination IP address in IP header was corrupted, i.e. changed to some other IP address, and that this change wasn't discovered by the IP checksum test. Consequently, the UDP datagram would arrive to the wrong IP address.

Effect of an invalid checksum: The Transport Layer on the other hand, might drop it on receiving this packet because of the wrong check sum.

25. How can the effect of jitter be compensated? What type of applications requires this compensation? AN(May/June 2013)

Jitter is defined as a variation in the delay of received packets.Jitter can be compensated by using play out delay buffers.The play out delay buffer must buffer these packets and then play them out in a steady stream .Application : Real time control systems

25. What do you mean by Qos? U(May/June 2012) (Nov/Dec 2015)

QoS (Quality of Service) is the idea that transmission rates, error rates, and other characteristics can be measured, improved, and, to some extent, guaranteed in advance. QoS is of particular concern for the continuous transmission of high-bandwidth video and multimedia information.

26. Differentiate between delay and Jitter. AN(Nov/Dec 2013)

- End-to-end delay is the time it takes a packet to travel across the network from source to destination.
- Delay jitter is the fluctuation of end-to-end delay from packet to the next packet.

27. Define slow start. R (May/June 2014) May/June 2016)

Slow-start algorithm is part of the congestion control in TCP, designed to avoid sending more data than the network is capable of transmitting. Slow-start algorithm works by increasing the TCP Window by one segment for each acknowledged segment. This behavior effectively doubles the TCP Window size each round trip of the network.

28. When can an application make use of an UDP? AN (May/June 2014)

UDP is suitable for applications that need fast, efficient transmission, such as games. UDP's stateless nature is also useful for servers that answer small queries from huge numbers of clients.

29. How does transport layer perform duplication control? AN(April/May 2015)

It is possible for packets to be duplicated in packet switched network; therefore TCP keeps track of bytes received in order to discard duplicate copies of data that has already been received.

30. List some of the Quality of Service parameters of transport layer. R (April/May 2015)

- Connection establishment delay.

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

31. List the different phases used in TCP connection. R (May/June 2016)

- Connection Establishment
- Data Transfer
- Connection Termination

PART B

1. With neat architecture, explain TCP in detail. U**(NOV/DEC 2010) (Nov/Dec 2015)**

2. Explain adaptive flow control in detail and its uses. U **(NOV/DEC 2010)**

3. With neat architecture, explain UDP and its packet format. U **(NOV/DEC 2011) (MAY/JUNE 2016)**

4. Discuss the different Queuing Discipline in detail.U

5. Explain the TCP Congestion Avoidance techniques in detail. U**(NOV/DEC 2011)**

6. Describe with examples the three mechanism by which Congestion control is achieved in TCP. (16) U (**NOV/DEC 2013) (Nov/Dec 2015) (MAY/JUNE 2016)**

7. Explain how QoS is provided through Integrated Services. AN

8. Explain how QoS is provided through Differentiated Services.AN

9. (i) With the help of a network diagram, Explain how TCP messages a byte stream. Give an example**. AN (NOV/DEC 2012)**

(ii)Explain any one congestion control algorithm.U

10. (i) Explain the Additive increase/multiplicative decrease methods used in TCP for congestion control. U**(NOV/DEC 2012)**

(ii) Give and explain the TCP header format.R

11. Draw and Explain about TCP state transition diagram**. R(MAY/JUNE 2012)**

12. Write short notes on R **(MAY/JUNE 2012)**

i. DECbit

ii. RED

13. (i) Suppose TCP operates over a 1-Gbps link, utilising the full bandwidth continuously. How long will it take for the sequence numbers to wrap around completely? Suppose an added 32—bit timestamp field increments 1000 times during this wrap around time, how long will it take for the timestamp filed to wrap around? (8) AP **(MAY/JUNE 2013)**

(ii) What is the need for Nagle's algorithm? How does it determine when to transmit data? (8) AP

14. (i) A TCP machine is sending full windows of 65,535 bytes over a 1-Gbps network that has a 10-ms one-way delay. What is the throughput achievable? What is the efficiency of transmission? How many bits are needed in the Advertised window field of a proposed reliable byte stream protocol (like TCP) running over the above network, for achieving maximum efficiency? (8) AP **(MAY/JUNE 2013)**

(ii) Illustrate the features of TCP that can be used by the sender to insert record boundaries into the byte stream. Also mention their original purpose. (8) AP

15. (i) Describe how reliable and ordered delivery is achieved through TCP. AN (8)

(ii)Why does TCP uses an adaptive retransmission and describes its mechanism. AN (8) **(NOV/DEC 2013)**

16. Explain the principles of congestion control in TCP**. U(MAY/JUNE 2014)**

17. Discuss the Random Early Detection mechanism and derive the expression for drop probability**.U (MAY/JUNE 2014)**

18. Explain the various fields of the TCP header and the working of the TCP protocol. U (16) **(APRIL/MAY 2015)**

19. (i) Explain the three way handshake protocol to establish the transport level connection.U (8)

(iv)List the various congestion control mechanisms. Explain anyone in detail. R(8) **(APRIL/MAY 2015)**

UNIT V
APPLICATION LAYER
PART A

1. What is the function of SMTP? U (Nov/Dec 2010)

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)? AN

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

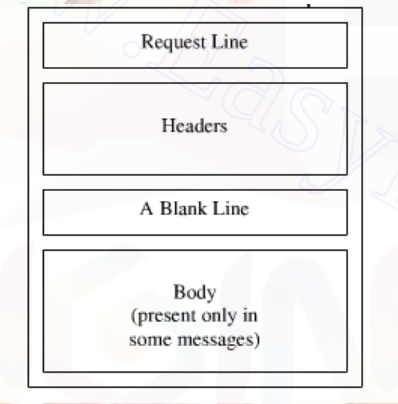
3. How does MIME enhance SMTP? AN

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? AN

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? R



6. What is the purpose of Domain Name System? R

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. U

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. Discuss the TCP connections needed in FTP. U

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.

9. Discuss the basic model of FTP. U

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.

10. Name four factors needed for a secure network. R

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.

11. How is a secret key different from public key? AN

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.

12. What is a digital signature? R

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.

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

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.

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

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.

15. Define permutation. R

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).

16. Define substitution & transposition encryption. R

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.

17. Define CGI. R

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

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

- 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.

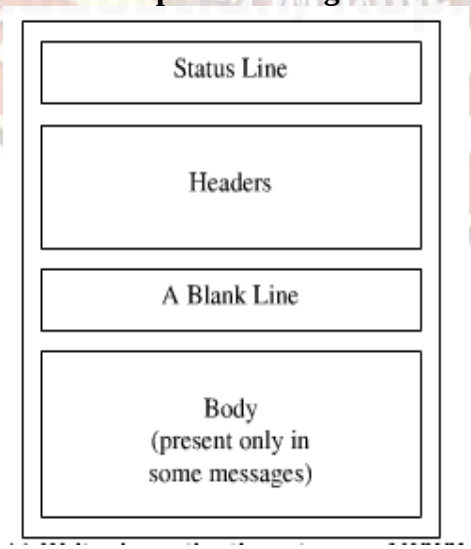
19. Define PGP. R (Nov/Dec 2010)&(May/June 2012) & (May/June 2014)

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

20. Define SSH. R

Secure Shell is used to provide a remote login, and used to remotely execute commands and transfer files and also provide strong client/server authentication / message integrity.

21. Give the format of HTTP response message? R



22. What is Telnet? U(Nov/Dec 2011) & (May/June 2014)

Telnet is a network protocol used on the Internet or local area networks to provide a bidirectional interactive text-oriented communication facility using a virtual terminal connection. User data is interspersed in-band with Telnet control information in an 8-bit byte oriented data connection over the Transmission Control Protocol (TCP).

23. State the purpose of SNMP. R (Nov/Dec 2011)

SNMP is the protocol that allows an SNMP manager (the controller) to control an SNMP agent (the controlee) by exchanging SNMP messages.The main purpose of an SNMP message is to control (set) or monitor (get) parameters on an SNMP agent. In SNMP, a parameter is an instance of a more generic object.

24. What is Simple Mail Transfer Protocol? U (Nov/Dec 2012)

SMTP stands for Simple Mail Transfer Protocol. SMTP is a standard network protocol for transmitting messages to an email server on the Internet.

All modern email client programs support SMTP. Web-based clients embed the address of an SMTP server inside their configuration, while PC clients provide SMTP settings that allow users to specify their own server of choice. Because SMTP handles outgoing messages and not incoming ones, email clients require addresses of both an SMTP server and another server that processes inbound messages (usually, POP or IMAP).

25. Why name services are sometimes called as middleware? AN (Nov/Dec 2012)

Advanced middleware solutions offer centralized naming services with some level of distribution. The issues are the same as those associated with DNS on the Internet or NDS on NetWare. A new frontier in middleware support for naming is in supporting more dynamic configurations, where redundant services must be targeted with load balancing and fault tolerance.

26. List the applications of Telnet. R(April/May 2011)

Telnet provided access to a command-line interface (usually, of an operating system) on a remote host. Most network equipment and operating systems with a TCP/IP stack support a Telnet service for remote configuration

27. List the functions of POP3. R(April/May 2011)

- POP3 is used to receive email messages via a TCP/IP connection; a client establishes a connection with a POP3 server at PORT 110

28. Define SNMP. R(May/June 2012)

Simple Network Management Protocol (SNMP) is an "Internet-standard protocol for managing devices on IP networks". Devices that typically support SNMP include routers, switches, servers, workstations, printers, modem racks, and more.[1] It is used mostly in network management systems to monitor network-attached devices for conditions that warrant administrative attention.

29. What DNS cache issues are involved in changing the IP address of web server host name? AN(Nov/Dec 2013)

it may cause some issues such as some website and web pages not loading or cannot be contacted and connected when browsing, causing by changing of IP address or nameservers that hasn't been reflected and refreshed on local copy.

30. What are the advantages of allowing persistent TCP connections in HTTP? R (May/June 2013)

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.

31. Is a cryptographic hash function, an irreversible mapping? Justify your answer. (May/June 2013) AN

Yes. A hash function is irreversible. Therefore, it can be used to prove knowledge of a secret without revealing it.

30. Differentiate application programs and application protocols. AN (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;
- Application programs use the services of the computer's operating system and other supporting programs.
- An application layer protocol defines how an application processes, running on different end systems, pass messages to each other. Eg :SMTP for electronic mail. HTTP for Web application.

31. Define SMTP. R(April/May 2015) (NOV/DEC 2015)

S*imple* **M***ail* **T***ransfer* **P***rotocol*, a protocol for sending e-mail messages between servers. Most e-mail systems that send mail over the Internet use SMTP to send messages from one server to another; the messages can then be retrieved with an e-mail client using either POP or IMAP. In addition, SMTP is generally used to send messages from a mail client to a mail server. This is why you need to specify both the POP or IMAP server and the SMTP server when you configure your e-mail application.

32. What are the groups of HTTP header? R (April/May 2015)

HTTP header fields provide required information about the request or response, or about the object sent in the message body. There are four types of HTTP message headers:

General-header: These header fields have general applicability for both request and response messages.

33. Mention the types of HTTP messages. R (NOV/DEC 2015)

- HTTP Request : An HTTP client sends an HTTP request to a server in the form of a request message
- HTTP Response : After receiving and interpreting a request message, a server responds with an HTTP response message

34. Define URL. R (MAY/JUNE 2016)

URL is an acronym for *Uniform Resource Locator* and is a reference (an address) to a resource on the Internet.

A URL has two main components:

- Protocol identifier: For the URL http://example.com, the protocol identifier is http.
- Resource name: For the URL http://example.com, the resource name is example.com.

35. Mention the different levels in domain name space. R (MAY/JUNE 2016)

Domain names are organized in subordinate levels (subdomains) of the DNS root domain, which is nameless. The first-level set of domain names are the top-level domains (TLDs), including the generic top-level domains (gTLDs), such as the prominent domains com, info, net, edu, and org, and the country code top-level domains (ccTLDs).

PART B

1. Explain the SMTP and HTTP. Give their uses, state strengths and weaknesses**. U (NOV 2010) (MAY/JUNE 2016)**
2. Explain the role of a DNS on a computer network**. U(NOV 2010) (NOV/DEC 2015)**
3. Explain Email protocols in detail (SMTP,MIME and IMAP). U **(MAY/JUNE 2012)**
4. Discuss FTP in detail. U
5. Discuss in detail about **DNS** and its frame format**. U(NOV/DEC 2011) (NOV/DEC 2015)**
6. Explain **SMTP** in detail.U **(NOV/DEC 2011)**
7. Write short notes on U**(MAY/JUNE 2012)**
   i. PGP
   ii. SSH
8. (i)Explain the various process involved after typing the URL in the task bar. U
   (ii)Write short notes on TELNET. U **(NOV/DEC 2012)**
9. Write short notes on the following U **(NOV/DEC 2012) (NOV/DEC 2015)**
   i. E-mail
   ii. HTTP

10. Discuss the need for name resolution. Illustrate the domain name hierarchy and the steps in resolution. AP **(MAY/JUNE 2013)**

11. (i) lllustrate the features of FTP and its operation. (8) AP**(MAY/JUNE 2013)**

(ii) Illustrate the features of TELNET. What is the need for network virtual terminal? AP(8)

12. Describe the message format and the message transfer and the underlying protocol involved in the working of the electronic mail. (16) U **(NOV/DEC 2013)**

13. Explain with example: U **(NOV/DEC 2013)**

(i) HTTP (8) (ii) RTP(8)

14. Write short notes on **(MAY/JUNE 2014) U**

i. DNS
ii. FTP

15. Discuss SNMP Protocol in detail. U**(MAY/JUNE 2014)**

16. (i) Explain the message transfer using Simple Mail Transfer Protocol.(8) **(APRIL/MAY 2015)U**

(ii) Explain the final delivery of email to the end user using POP3. U(8)

17. Write short notes on U **(APRIL/MAY 2015)**

(i) Web services

(ii) SNMP.

18. Explain in detail about Web service architecture. **(16) U (MAY/JUNE 2016)**