Arunai Engineering College
Tiruvannamalai

DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING

CS8591– COMPUTER NETWORKS
PART A- 2 MARKS

CS8591 COMPUTER NETWORKS

UNIT I INTRODUCTION AND PHYSICAL LAYER

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

UNIT II DATA-LINK LAYER & MEDIA ACCESS

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

UNIT III NETWORK LAYER

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

UNIT IV TRANSPORT LAYER

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

UNIT V APPLICATION LAYER

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

TOTAL : 45 PERIODS

UNIT 1

FUNDAMENTALS AND LINK LAYER

PART - A

1. What do you mean by error control? [APR/MAY-2015]

Error control is the process of detecting and correcting both the bit level and packet level errors.

Types of Errors

***Single Bit Error**

Single bit error means that only one bit of the data unit was changed from 1 to 0 and 0 to 1.

***Burst Error**

Burst error means that two or more bits in the data unit were changed. Burst error is also called packet level error, where errors like packet loss, duplication, reordering.

2.Define flow control [APR/MAY-2015, NOV/DEC-2011, MAY/JUNE-2016]

It refers to a set of procedures used to restrict the amount of data flow between sending and receiving stations. It tells the sender how much data it can transmit before it must wait for an acknowledgement from the receiver.

There are two methods are used. They are,

- Stop and wait
- Sliding window

3.Define Layer [NOV/DEC – 2013]

Each layer of a specific network model may be responsible for a different function of the network. Each layer will pass information up and down to the next subsequent layer as data is processed.

4.What do you mean by framing? [NOV/DEC -2014, NOV/DEC – 2013]

The stream of bits are divided into manageable bit units called frames.

5. Give the purpose of layering. [MAY/JUNE – 2013]

- To reduce the design complexity, most of the networks are organized as a series of layers or levels, each one build upon one below it.
- The basic idea of a layered architecture is to divide the design into small pieces.
- It decomposes the problem of building a network into more manageable components.
- Layering provides a more modular design.

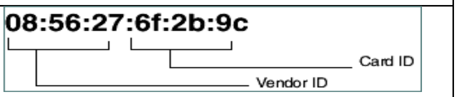
6. Mention the advantage and disadvantage of error correction by receiver, as compared to error detection. [MAY/JUNE – 2013]

Detecting errors is only one part of the problem. The other part is correcting errors once detected

Advantages of error correction compared to error detection:

Error correction is the additional ability to reconstruct the original, error-free data.

7.What is the difference between port address, logical address and physical address? [MAY/JUNE – 2014]

S.N	Port Address	Logical Address	Physical Address
1	The port address (service-point) identifies the application process on the station.	The logical address defines the sender and receiver at the network layer and is used to deliver messages across multiple networks	The physical address is the local address of a node; it is used by the data link layer to deliver data from one node to another within the same network.
2	Each application runs with a port no. on the computer. The no. for application is decided by the Kernel of the OS. The port no. is called port address.	An IP address of the system is called logical address. This address is the combination of Net ID and Host ID.	The address of the NIC(Network Interface Card) is called Physical address or MAC address.
3	Example: 0 to 65535	Example: 130.57.64.11	

8.Define hamming distance [NOV/DEC -2014]

Hamming code is a linear error-correcting code

The Hamming code can:

- Detect *and* correct all 1 bit errors
- Detect most 2 bit errors, but does not detect all 2 bit errors

9. What are the major duties of Network Layer? [MAY/JUNE -2012]

The major duties of Network Layer are,

a. Logical Addressing

If a packet passes the network boundary, another addressing system is needed to distinguish between source and destination systems. The network layer adds a header to the packet coming from the upper layer that includes logical address of the sender and receiver.

b.Routing

When more than one networks are connected to create internetworks, the connecting devices route the packet to its final destination. Network layer provides this mechanism.

10. What is the use of two dimensional parity in error detection? [NOV/DEC 12]

- Two dimensional parity increases the overhead in data transmission, but provides correction of ONE error and detection of MULTIPLE errors (All 1,2,3 & most 4 bits).
- It provides stronger protection against common errors than the repetition code

11.What are the issues in data link Layer? [NOV/DEC – 2012]

Recognizing exactly what set of bits constitute a frame, that is determining where the frame begins and ends is the central challenge (issue) faced by the adaptor.

There are several ways to address the framing problem:

- Byte Oriented Protocols
- Bit Oriented Protocols
- Clock Based Protocols

12. Define Bit stuffing. [MAY/JUNE -2011,17]

At the start end of each frame is a flag byte consisting of the special bit pattern 01111110 Whenever the sender's data link layer encounters five consecutive 1s in the data, it automatically stuffs a zero bit into the outgoing bit stream. This technique is called bit stuffing. When the receiver sees five consecutive 1s in the incoming data stream, followed by a zero bit, it automatically de-stuffs the 0 bit. The boundary between two frames can be determined by locating the flag pattern.

13. What are the functions of application Layer? [MAY/JUNE -2011]

- This layer supports application and end-user processes.
- Communication partners are identified, quality of service is identified, user authentication and privacy are considered, and any constraints on data syntax are identified.
- This layer provides application services for file transfers, e-mail, and other network software services.
- Telnet and FTP are applications that exist entirely in the application level.

14.Write the parameters used to measure Network performance.

[MAY/JUNE-2016]

- **Bandwidth** commonly measured in bits/second is the maximum rate that information can be transferred
- **Throughput** is the actual rate that information is transferred

- **Latency** the delay between the sender and the receiver decoding it, this is mainly a function of the signals travel time, and processing time at any nodes the information traverses
- **Jitter** variation in packet delay at the receiver of the information
- **Error rate** the number of corrupted bits expressed as a percentage or fraction of the total sent

15. Define the term protocol. **[NOV/DEC-2015]**

When computers communicate with each other, there needs to be a common set of rules and instructions that each computer follows. A specific set of communication rules is called a protocol

UNIT 2

MEDIA ACCESS AND INTERNETWORKING

PART – A

1. List the functions & limitations of bridges [APR/MAY 15,17,NOV/DEC-10]

Functions of Bridges:

A bridge device filters data traffic at a network boundary. Bridges reduce the amount of traffic on a local area network (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.

Limitations of bridges:

A network bridge does not incur any communication between network path and the physical hosts of the data. The data packets are not guided as through which path to travel along. Therefore a network data packet is sent to every network terminal.

2.What do you understand by CSMA protocol? [APR/MAY-2015]

What is CSMA/CD? [NOV/DEC-2011]

CSMA/CD (Carrier Sense, Multiple Access with Collision Detect):

Carrier sense multiple access means that multiple stations can listen to the link and detect when it is in use or idle; —collision detect‖ indicates that, if two or more stations are transmitting on the link simultaneously, they will detect the collision of their signals. Ethernet is the best-known technology that uses CSMA/CD.

3. What is the average size of an Ethernet frame? [MAY/JUNE-2014]

The original Ethernet IEEE 802.3 standard defined the minimum Ethernet frame size as 64 bytes and the maximum as 1518 bytes. The maximum was later increased to 1522 bytes to allow for VLAN tagging.

4. What is the access method used by wireless LAN? [MAY/JUNE-2014]

IEEE 802.11 defines the physical layer (PHY) and MAC (Media Access Control) layers based on **CSMA/CA (Carrier Sense Multiple Access with Collision Avoidance) access method**. The 802.11 specification includes provisions designed to minimize collisions, because two mobile units may both be in range of a common access point, but out of range of each other.

5. Define source routing [NOV/DEC-2013]

source routing, also called path addressing, allows a sender of a packet to partially or completely specify the **route** the packet takes through the network. In contrast, in non-**source routing** protocols, routers in the network determine the path based on the packet's destination

6. **What is subnetting and what is the need for subnetting?[NOV/DEC-2013,2015]**

Subnetting is breaking up a single network into smaller networks. To do this, you add more bits (more numbers) to the **subnet** mask. Traditionally, we are used to seeing **subnet** masks that look like 255.0.0.0, 255.255.0.0, or 255.255.255.0.

Four of the major reasons for subnetting or segmenting your network

- To divide a large network into smaller segments to reduce traffic and speed up the sections of your network.
- To connect networks across geographical areas.
- To connect different topologies such as Ethernet, Token Ring, and FDDI together via routers.
- To avoid physical limitations such as maximum cable lengths or exceeding the maximum number of computers on a segment.

7. **How does a router & switch differ from a bridge?[APR/MAY-2015] & [NOV/DEC-2012]**

Router	**Switch**	**Bridge**
A device that forwards data packets along networks. A router is connected to at least two networks, commonly two LANs or WANs	In networks, a device that filters and forwards packets between LAN segments which selects a path or circuit for sending a unit of data to its next destination.	A bridge is a product that connects a local area network (LAN) to another local area network that uses the same protocol
Routers are located at gateways, the places where two or more networks connect.	Switches operate at the data link layer (layer 2) and sometimes at the network layer (layer 3)	A bridge examines each message on a LAN. Messages are sent out to every address on the network and accepted only by the intended destination node.
Routers use headers and forwarding tables to determine the best path for forwarding the packets	LANs that use switches to join segments are called switched LANs	Bridges learn which addresses are on which network and develop a learning table so that subsequent messages can be forwarded to the right network.

8. What is the need for ARP? [NOV/DEC-2013,2015]

ARP – –**Address Resolution Protoco**l‖, is used to map IP Network addresses to the hardware (Media Access Control sub layer) addresses used by the data link protocol. The ARP protocol operates between the network layer and the data link layer in the Open System Interconnection (OSI) model.

ARP is used in four cases of two hosts communicating:

- When two hosts are on the same network and one desires to send a packet to the other
- When two hosts are on different networks and must use a gateway/router to reach the other host
- When a router needs to forward a packet for one host through another router
- When a router needs to forward a packet from one host to the destination host on the same network

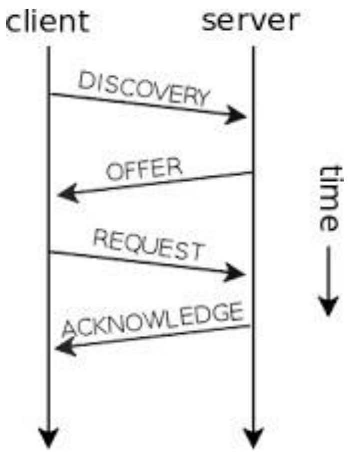
9. How is the minimum size of an Ethernet frame determined? [MAY/JUNE-2013]

What is the average size of an Ethernet frame? [MAY/JUNE-2014]

The original Ethernet IEEE 802.3 standard defined the minimum Ethernet frame size as **64 bytes** and the maximum as **1518 bytes**. The reason for this minimum frame size is that the frame must be long enough to detect a collision. The maximum was later increased to **1522 bytes** to allow for VLAN tagging. The minimum size of an Ethernet frame that carries an ICMP packet is 74 bytes.

10. What is DHCP? [NOV/DEC-2012]

The **Dynamic Host Configuration Protocol** (**DHCP**) is a standardized network protocol used on Internet Protocol (IP) networks for dynamically distributing network configuration parameters, such as IP addresses for interfaces and services.



11. Differentiate circuit and packet switched networks.

[MAY/JUNE-14,17] , [MAY/JUNE-2013] & [NOV/DEC-2014]

Circuit Switching	**Packet switching**
Source and destination host are physically connected	No such physical connection exits
Switching takes place at the physical layer	Switching takes place at network (datagram) or data link layer (VCN)
Resources such as bandwidth, switch buffer & processing time are allocated in advance	Resources are allocated on demand
Resources remain allocated for the entire duration of data communication	Resources can be reallocated when idle
There is no delay during data transfer	Delay exists at each switch during data transfer
Data transferred between the two stations is a continuous flow of signal	Data is transferred as discrete packets
Example : Telephony	Example: Internet

12. 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 255.255.0.0? [MAY/JUNE- 2014]

Subnet address = IP address of system logical and with subnet mask
Given IP address is 25.34.12.56 and subnet mask is 255.255.0.0
Then subnet address is calculated by

	Decimal format	**Binary format**
IP Address	25.34.12.56	00011001.00100010.00001100.00111000
Subnet mask	255.255.0.0	11111111.11111111.00000000.00000000
Do Logical bitwise AND		00011001.00100010.00000000.00000000
The result is subnet address		25.34.0.0

13. Define hidden node problem? [MAY/JUNE-2016]

In a wireless network, it is likely that the node at the far edge of the access point's range, which is known as **A**, can see the access point, but it is unlikely that the same node can see a node on the opposite end of the access point's range, **C**. These nodes are known as hidden. The problem is when nodes **A** and **C** start to send packets simultaneously to the access point **B**. Because the nodes **A** and **C** are out of range of each other and so cannot detect a collision while transmitting, Carrier sense multiple access with collision detection (CSMA/CD) does not work, and collisions occur, which then corrupt the data received by the access point called hidden node problem

14. What is bluetooth? [MAY/JUNE-2016]

Bluetooth is a wireless technology standard for exchanging data over short distances (using short-wavelength UHF radio waves in the ISM band from 2.4 to 2.485 GHz) from fixed and mobile devices, and building personal area networks (PANs)

15. What is meant by exponential back off and scatter net? [Nov 16]

In a variety of computer networks, binary **exponential backoff** or truncated binary exponential backoff refers to an algorithm used to space out repeated retransmissions of the same block of data, often as part of network congestion avoidance.

A **scatternet** is a type of network that is formed between two or more Bluetooth-enabled devices, such as smartphones and newer home appliances. A scatternet is made up of at least two piconets. Bluetooth devices are peer units that act as slaves or masters. Scatternets are formed when a device in a piconet, whether a master or a slave, decides to participate as a slave to the master of another piconet. This device then becomes the bridge between the two piconets, connecting both networks.

UNIT 3

ROUTING

PART- A

1. Define BGP and VCI. [NOV/DEC-2014,16].

Border Gateway Protocol (BGP) is an inter domain routing protocol using path vector routing traffic on the internet can be classified into two types:

- Local traffic that starts/ends on nodes within an AS
- Transit traffic that passes through an AS

Virtual Channel Identifier: The **VCI**, used in conjunction with the VPI (virtual path indicator), indicates where an ATM cell is to travel over a **network**. ATM, or asynchronous transfer mode, is a method that many ISPs (Internet Service Providers) use to transfer data to client computers.

2. What are the salient features of IPV6? [NOV/DEC-2012]

- Support for real time services
- Security support auto configuration
- Enhanced routing functionality, including support for mobile hosts

- 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 neighbouring node interaction
- Extensibility

3. What is multicasting? [NOV/DEC – 2010], [NOV/DEC-2011]

A host places a multicast address in the destination address field to send packets to a set of hosts belonging to a group. Internet multicast can be implemented on physical networks that support broadcasting by extending forwarding functions.

4. What are the functions of a router? [NOV/DEC – 2010]

- It is layer 3 device.
- Used to communicate among different networks.
- Forwards packet on the basis of routed protocol. Such as IP, IPv6, IPX etc.
- It has main three functions: **Packet Forwarding, Packet switching and Packet filtering**.
- Every interface is single broadcast domain.

- Every interface with Ethernet is single collision domain.
- It creates routing table and maintain possible network to be reached.
- It chooses best path, if multiple path is exist.

5. What are the different kinds of multicast routing? [MAY/JUNE – 2011]

The various kinds of multicast routing are:

- Link State Multicast
- Distance Vector Multicast
- Protocol Independent Multicast (PIM)

6. Mention any 4 applications of multicasting. [MAY/JUNE-2012]

- Audio-video distribution (1-to-many) and symmetric (all-to-all)
- Distributed simulation (war gaming)
- Resource discovery
- File distribution (stock market quotes, new software.

7. What are the metrics used by routing protocols? [APR/MAY-2015]

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

8. What is an autonomous system?

Internet is so large that no one routing protocol can handle the task of updating the routing tables of all routers. Internet is divided into autonomous systems. An autonomous system is a group of networks and routers under the authority of a single administration.

- Routing inside an autonomous system is referred to as intra domain routing.

- Routing between autonomous systems is referred to as inter domain routing.

9. What are routing areas? [Regulation 2013]

Link-state routing protocols (such as OSPF and IS-IS) can be used to partition a routing domain into subdomains called *areas*. 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.

10. 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

11. Identify the classes of following IP address. [Nov/Dec – 2015]

110.34.56.45	**- class A**
212.208.63.23	**- class C**

12. Expand ICMP and write the function. [MAY/JUNE-2016,17]

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. ICMP creates and sends messages to the source IP address indicating that a gateway to the Internet that a router, service or host cannot be reached for packet delivery. Any IP network device has the capability to send, receive or process ICMP messages.

13.Write the types of connecting device in internet working.[MAY/JUNE-2016]

- hub
- ethernet hubs
- switches
- bridges
- routers
- brouters

14. How does a router differ from a bridge? [APRIL / MAY – 2015]

Bridge – It is used to connect a LAN to another LAN that used same protocol.

Router - A **router** is a device that forwards data packets along networks. A **router** is connected to at least two networks, commonly two LANs or WANs or a LAN and its ISP's network. **Routers** are located at gateways, the places where two or more networks connect.

15. Define routing. [Nov/Dec – 15]

The process by which nodes exchange topological information to build correct forwarding tables are said to be *routing*.

UNIT 4

TRANSPORT LAYER

PART A

1. List out the various features of Sliding Window Protocol. [NOV/DEC 2012]

A Sliding window protocols are used where reliable in-order delivery of packets is required. A sliding window protocol allows an unlimited number of packets to be communicated using fixed-size sequence numbers. The term "window" on the transmitter side represents the logical boundary of the total number of packets yet to be acknowledged by the receiver. The receiver informs the transmitter in each acknowledgment packet the current maximum receiver buffer size (window boundary).

2. Differentiate delay and jitter. [NOV/DEC 2013]

Delay: is the amount of time data (signal) takes to reach the destination. A higher delay generally means congestion of some sort of breaking of the communication link.

Jitter: is the variation of delay time. eg. Video Streaming suffers from jitter a lot because the size of data transferred is quite large

3. Define slow start. [MAY/JUNE 2014], [MAY/JUNE-2016]

Slow-start is part of the congestion control strategy used by TCP. **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.

4. When can an application make use of UDP? [MAY /JUNE 2014]

UDP uses a simple connectionless transmission model with a minimum of protocol mechanism. It has no handshaking dialogues. There is no guarantee of delivery, ordering, or duplicate protection. UDP provides checksums for data integrity, and port numbers for addressing different functions at the source and destination of the datagram.

5. Difference between connections oriented service and Connectionless service.

[MAY/JUNE 2013,16]

In connection oriented service authentication is needed while connectionless service does not need any authentication.

- Connection oriented protocol makes a connection and checks whether message is received or not and sends again if an error occurs connectionless service protocol does not guarantees a delivery.
- Connection oriented service is more reliable than connectionless service.

- Connection oriented service interface is stream based and connectionless is message based

6. What is function of transport layer?

The protocol in the transport layer takes care in the delivery of data from one application program on one device to an application program on another device. They act as a link between the upper layer protocols and the services provided by the lower layer

7. What are the duties of the transport layer? [APR/MAY-2015]

The services provided by the transport layer End-to-end delivery

- Addressing
- Reliable delivery
- Flow control
- Multiplexing

8. Differentiate TCP and UDP . [NOV/DEC 2014,16]

TCP	UDP
Reliability: TCP is connection-oriented protocol. When a file or message send it will get delivered unless connections fails. If connection lost, the server will request the lost part. There is no corruption while transferring a message.	*Reliability*: UDP is connectionless protocol. When you a send a data or message, you don't know if it'll get there, it could get lost on the way. There may be corruption while transferring a message.
Ordered: If you send two messages along a connection, one after the other, you know the first message will get there first. You don't have to worry about data arriving in the wrong order.	*Ordered*: If you send two messages out, you don't know what order they'll arrive in i.e. **no ordered**
Heavyweight: **-** when the low level parts of the TCP "stream" arrive in the wrong order, resend requests have to be sent, and all the out of sequence parts have to be put back together, so requires a bit of work to piece together.	*Lightweight*: No ordering of messages, no tracking connections, This means it's a lot quicker, and the network card / OS have to do very little work to translate the data back from the packets.
Streaming: Data is read as a "stream," with nothing distinguishing where one packet ends and another begins. There may be multiple packets per read call.	*Datagrams*: Packets are sent individually and are guaranteed to be whole if they arrive. One packet per one read call.
Examples: World Wide Web (Apache TCP port 80), e-mail (SMTP TCP port 25 Postfix MTA),	*Examples*: Domain Name System (DNS UDP port 53), streaming media applications

File Transfer Protocol (FTP port 21) and Secure Shell (OpenSSH port 22) etc.	such as IPTV or movies, Voice over IP (VoIP), Trivial File Transfer Protocol (TFTP) and online multiplayer games etc

9. How does transport layer perform duplication control? [APRIL/MAY -15]

Duplication control is important to consider as well because as the speed of networks continue to increase, it becomes possible for different messages to be identified as duplicated and discarded. Similarly, if a packet can become corrupted or erroneous, it is possible then for the sequence number of a real message to be incorrect and cause a duplicate. Also it is entirely possible for a duplicate message to be sent by the sender itself, and therefore this duplicate should be detected to avoid errors.

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

The four aspects are,

- Error control
- Sequence control
- Loss control,
- Duplication control

11. What is the difference between congestion control and flow control?
[Nov/Dec15]

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.

12. What is meant by congestion?

Congestion in a network occurs if user sends data into the network at a rate greater than that allowed by network resources. Congestion occurs because the switches in a network have a limited buffer size to store arrived packets

13. What is QoS?What are the two categories of QoS attributes? [Nov/Dec-15]

Quality of Service (QoS) refers to the capability of a network to provide better service to selected network traffic over various technologies

The two main categories of QoS attributes are:

- User Oriented
- Network Oriented

14. List some of the QoS parameters of transport layer.[APRIL / MAY – 2015]

- Throughput
- Priority
- Resilence
- Transit delay

15. List the different phases used in TCP connection. [MAY/JUNE-2016]

- Connection establishment
- Data transfer
- Termination

16. Compare Unicast, multicast and broadcast. [Nov – 16]

Unicast: Unicast is the term used to describe communication where a piece of information is sent from one point to another point. In this case there is just one sender, and one receiver.
Broadcast: Broadcast is the term used to describe communication where a piece of information is sent from one point to all other points. In this case there is just one sender, but the information is sent to all connected receivers.
Multicast: Multicast is the term used to describe communication where a piece of information is sent from one or more points to a set of other points. In this case there is may be one or more senders, and the information is distributed to a set of receivers (theer may be no receivers, or any other number of receivers).

UNIT 5

APPLICATION LAYER

PART – A

1. Define SMTP. [APR/MAY-2015,17], [NOV/DEC-2015], [NOV/DEC-2010]

SMTP (Simple Mail Transfer Protocol) is a TCP/IP protocol used in sending and receiving e-mail. However, since it is limited in its ability to queue messages at the receiving end, it is usually used with one of two other protocols, POP3 or IMAP

In other words, users typically use a program that uses SMTP for sending e-mail and either POP3 or IMAP for receiving e-mail. On Unix-based systems, send mail is the most widely-used SMTP server for e-mail

2. What DNS cache issues are involved in changing the IP address of a Web server host name? How might these be minimized? [NOV 13, April - 17]

This is an example where using an obsolete entry can be a serious problem, since you might get served the wrong page if you contact the "old" owner of a given name. This problem might be minimized by providing a mechanism for sending "DNS update" messages to inform hosts that their entries have gone bad.

3. State the difference between SMTP and MIME. [NOV/DEC-14,APR - 15]

SMTP	**MIME**
Simple Mail Transfer Protocol (SMTP) is an Internet standard for electronic mail (email) transmission.	Multipurpose Internet Mail Extensions (MIME) is an Internet standard that extends the format of email

SMTP is a set of commands that authenticate and direct the transfer of electronic mail. When configuring the settings for your e-mail program, you usually need to set the SMTP server to your local Internet Service Provider's SMTP settings However, the incoming mail server should be set to your mail account's server which may be different than the SMTP	It supports: • Text in character sets other than ASCII • Non-text attachments: audio, video, images, application programs etc. • Message bodies with multiple parts • Header information in non-ASCII character sets

4. Why name services are sometimes called as middleware [NOV/DEC-2012]

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

5. List the functions of POP3 **[APR/MAY-2011]**

POP3 stands for Post Office Protocol. POP3 allows an email client to download an email from an email server. The POP3 protocol is simple and does not offer many features except for download. Its design assumes that the email client downloads all available email from the server, deletes them from the server and then disconnects. POP3 normally uses port 110.

6. State the purpose of SNMP. **[NOV/DEC-2011]**

Simple Network Management Protocol (**SNMP**)

It is a popular protocol for network management. It is used for collecting information from, and configuring, network devices, such as servers, printers, hubs, switches, and routers on an Internet Protocol (IP) network.

7. How would you define the term SOAP **[Regulation 2013]**

- SOAP- Simple Object Access Protocol
- SOAP uses many of the same strategies as WSDL, including message formats defined using XML Schema, bindings to underlying protocols, MEPs, and reusable specification elements identified using XML namespaces.
- SOAP is used to define transport protocols with exactly the features needed to support a particular application protocol.
- SOAP aims to make it feasible to define many such protocols by using reusable components

8. What is URI **[Regulation 2013]**

URI-Uniform Resource Identifiers

The URLs that HTTP uses as addresses are one type of *Uniform Resource Identifier* (URI). A URI is a character string that identifies a resource, where a resource can be anything that has identity, such as a document, an image, or a service.

The first part of a URI is a *scheme* that names a particular way of identifying a certain kind of resource, such as mail to for email addresses or file for file names.

The second part of a URI, separated from the first part by a colon, is the *scheme-specific part*.

9. Define Hypertext links.

Web browser has some way in which you can recognize URLs (often by highlighting or underlining some text) and then you can ask the browser to open them. These embedded URLs are called *hypertext links*.

10. What is IMAP? **[REGULATION-2013]**

IMAP stands for, **Internet Message Access Protocol**

It is an Internet standard protocol used by e-mail clients to retrieve e-mail messages from a mail server over a TCP/IP connection.

IMAP4 has several distinct advantages:

- Stronger authentication

- Support for multiple mailboxes
- Greater support for online, offline, or disconnected modes of operation

10. Define URL [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, Resource Name

11. Mention the different levels in domain name space. [MAY/JUNE-2016]

- Top level
- Second level
- Lower level

12. Mention the types of HTTP messages. [NOV/DEC-15]

HTTP messages consist of requests from client to server and responses from server to client.

HTTP-message = Request | Response ; HTTP/1.1 messages

13. What are the groups of HTTP header? [April / may 2015]

- General Header
- Request Header
- Response Header
- Entity Header

14. Expand POP3 and IMAP4. [Nov 16]

- **POP -** Post Office Protocol
- **IMAP4 -** Internet Message Access Protocol

15. What is persistant HTTP and get in HTTP? [Nov 16]

HTTP persistent connection, also called **HTTP** keep-alive, or **HTTP** connection reuse, is the idea of using a single TCP connection to send and receive multiple **HTTP** requests/responses, as opposed to opening a new connection for every single request/response pair.

GET: The GET method is used to retrieve information from the given server using a given URI. Requests using GET should only retrieve data and should have no other effect on the data.