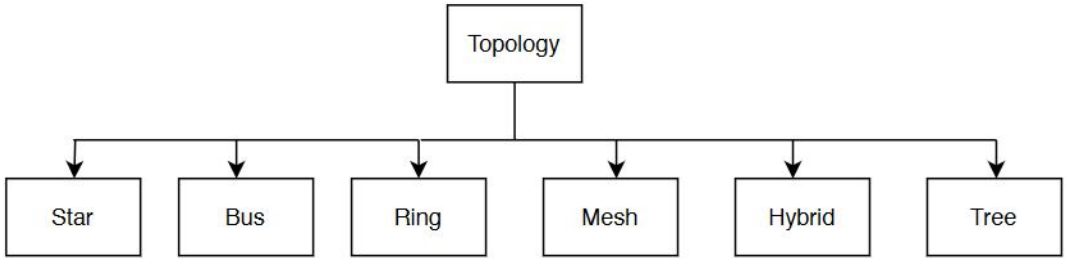
Computer Networking

Computer Network:
Computer network is the collection of two or more computers that are interconnected with each other to perform data communication using the data communication protocol through communications media (wired and wireless). So these computers can share information, data, programs, and use of hardware together. Data communications that can be done include text data, images , video and sound. There are different networks:
1. LAN
2. MAN
3. WAN

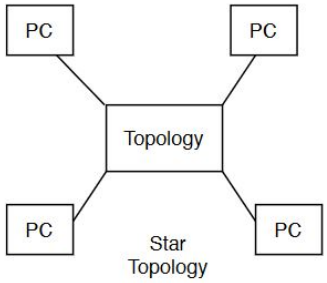
LAN
A Local Area Network (LAN) is a network that is confined to a relatively small area. It is generally limited to a geographic area such as a lab, school, or building. LAN Computers rarely span more than a mile apart.
In a typical LAN configuration, one computer is designated as the file server. It stores all the software that controls the network, as well as the software that can be shared by the computers attached to the network. Computers connected to the file server are called workstations. The workstations can be less powerful than the file server, and they may have additional software on their hard drives. On many LANs, cables are used to connect the network interface cards in each computer. However, one LAN can be connected to other LANs over any distance via telephone lines and radio waves. Most LANs connect workstations and personal computers.
Each node (individual computer) in a LAN has its own CPU which executes programs and it is also able to access data and devices anywhere on the LAN. This means that many users can share expensive devices, such as laser printers, as well as data. Users can also use LAN to communicate with each other, by sending e-mail or engaging in chat sessions.

Three characteristic features of LAN
1. The size of a LAN network.
2. The topology of the local area network.
3. The technology used for transmission.
In simple LAN configuration, a single cable runs through the entire set up and the peripherals and computers are attached to the cable. Traditional **LAN speeds are 10 Mbps to 100 Mbps**. Modern LAN cables are capable of much higher data transfer per second.
In case two or more systems need to use the LAN at the same time, then an arbitration mechanism is deployed to resolve the conflict. A first come first serve policy or a prioritized approach may be chosen.

LAN topologies:



Star Topology: Each device has a dedicated point-to-point link to a central controller called a hub. Most used LAN topology.
If one device wants to send data to another, it sends the data to the controller, which then relays the data to the other connected devices.



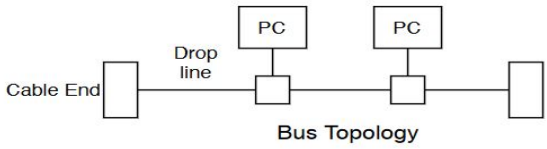
Advantages

- ✓ Robust, if one link fails, only that link is affected. All other links remain active.
- ✓ As long as the hub is working, it can monitor link problems and bypass defective links.

Disadvantages

- ✓ If the hub goes down, the whole system dies.
- ✓ More cabling is required in a star than ring or bus.

Bus Topology: A bus topology is multipoint. One long cable acts as a backbone to link all the devices in a network. Carrier Sense Multiple Access/Collision Detection (CSMA/CD) is the accessing technique used. The traffic can go in either direction, i.e., it is bidirectional.
Nodes are connected to the bus cable by drop lines.



Bus Topology

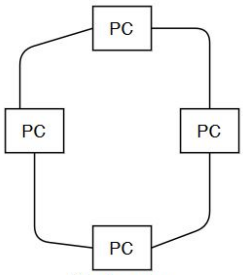
Advantages

- ✓ Ease of installation.
- ✓ Require less cabling than mesh or star topologies.

Disadvantages

- ✓ Difficult to add new devices.
- ✓ A fault in the bus cable stops all transmission. The damaged area reflects signals back in the direction of origin, creating noise in both directions.

Ring Topology: Each device has a dedicated point-to-point connection with only the two devices on either side of it. Each device in the ring incorporates a repeater; when a device receives a signal intended for another device, its repeater regenerates the bits and passes them along.



Ring topology

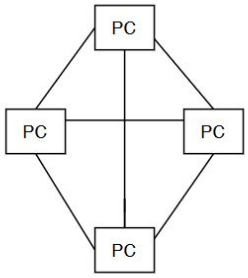
Advantages

- ✓ Easy to install and reconfigure
- ✓ Fault isolation is simplified as it issues alarm which alerts the network operator to the problem and its location.

Disadvantages

- ✓ A break in the ring can disable the entire network.
- ✓ It is not relevant for higher-speed LANs.

Mesh topology: Every station is interconnected to every other station as shown in the figure.



Mesh Topology

n(n - 1)/2 (duplex mode) links are required for communication in both directions. Each device on the network must have (n-1) I/O ports to be connected to the other (n-1) stations.

Advantages

- ✓ The use of dedicated links guarantees that each connection can carry its own data load, thus eliminating traffic problems.
- ✓ 2 This topology is robust. If one link becomes unusable, it does not incapacitate the entire system.
- ✓ There is an advantage of security, only the intended recipient sees the message on the dedicated line.
- ✓ Fault identification and fault isolation is easy because of point-to-point links.

Disadvantages

- ✓ As the hardware(cables) required for connection is more, it is expensive.
- ✓ Installation and reconnection are difficult.
- ✓ The sheer bulk of the wiring can be greater than the available space.

Hybrid Topology: More than one topology in a network.

Advantage:

- ✓ 1.Fault detection is easier
- ✓ 2.We can add new stations without affecting the orginal architecture.

Disadvantages

- ✓ As different topologies are combined so complexity of design increases. Very less practical implementation
- ✓ The hub which is used to connect different topologies is very costly. Moreover the cost of whole infrastructure is very high.

Tree Topology: The topology uses the combination of star and bus topology.

Advantages

- ✓ Expansion is easier, one can add new stations easily.
- ✓ Errors can be easily detected.
- ✓ Robust, if one link fails the remaining system is in communication

Disadvantages

- ✓ With the increase in the number of nodes, complexity and maintenance become difficult.

Examples: The most common type of local area network is an Ethernet LAN. The smallest home LAN can have exactly two computers; a large LAN can accommodate thousands of computers. Many LANs are divided into logical groups called subnets. An internet protocol Class A LAN can in theory accomodate more than 16 million devices organized into subnets.

MAN

A metropolitan area network is a computer network that usually spans a city or a large campus.A man usually interconnects a number of local area networks(LANs) using a high capacity backbone technology, such as fiber optical links, and provides up links services to wide area networks and the internet.

WAN

Wide area networks connect larger geographic areas, such as Bangladesh, US or the world. A WAN connects several LANs, and may be limited to an enterprise (a corporation or an organization) or accessible to the public. The technology is high speed and relatively expensive. The Internet is an example of a worldwide public WAN.

What type of network provides access to the regional service providers and typically span distances greater than 100 miles? *[probashi kallyan bank(P)-2019]*

a) LAN b) MAN c) WAN d) WLAN Ans.c

Other Types of Networks

Apart from above mentioned here, are some other important types of networks:

- ✓ WLAN (Wireless Local Area Network)
- ✓ Storage Area Network
- ✓ System Area Network
- ✓ Home Area Network
- ✓ POLAN- Passive Optical LAN
- ✓ Enterprise private network
- ✓ Campus Area Network
- ✓ Virtual Area Network

Extranet allows-*[SBL JBL- SO(IT/ICT)-2018]*

a) insiders only b) authorized outsides only

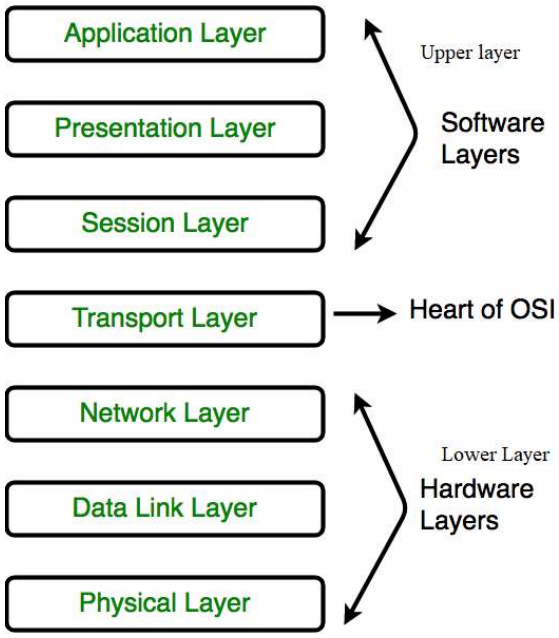
c) all outside d) both inside and authentic outsides **Ans. d**

OSI Model

- ✓ OSI stands for **Open System Interconnection** is a reference model that describes how information from a software application in one computer moves through a physical medium to the software application in another computer.
- ✓ OSI consists of seven layers, and each layer performs a particular network function.
- ✓ OSI model was developed by the International Organization for Standardization (ISO) in 1984, and it is now considered as an architectural model for the inter-computer communications.
- ✓ OSI model divides the whole task into seven smaller and manageable tasks. Each layer is assigned a particular task.
- ✓ Each layer is self-contained, so that task assigned to each layer can be performed independently.

OSI reference model is a logical framework for standards for the network communication. OSI reference model is now considered as a primary standard for internetworking and inter computing. Today many network communication protocols are based on the standards of OSI model.

- ✓ Layer 1, 2 and 3 i.e. physical, data link, and network are network support layers.
- ✓ Layer 4, Transport layer provides end to end reliable data transmission.
- ✓ Layer 5, 6 and 7 i.e. Session, Presentation, and Application layer are user support layers.



In TCP/IP model which one is not a valid layer? *[JBL-AEO(IT)-2015]*

a) Application Layer b)Internet Layer

c) Transport Layer d) Physical Layer **Ans.b**

Responsibility of Application layer:

- ✓ **File transfer, access, and management (FTAM):** An application layer allows a user to access the files in a remote computer, to retrieve the files from a computer and to manage the files in a remote computer.
- ✓ **Mail services:** An application layer provides the facility for email forwarding and storage.
- ✓ Directory services: An application provides the distributed database sources and is used to provide that global information about various objects.
- ✓ This layer provides network services to the end-users like Mail, ftp, telnet, DNS.

Email is a protocol of the following layer? *[SBL-AE-2016]*

a) PhysicalLayer b)Data Link Layer c) Application Layer d) TCP layer **Ans. c**

Responsibility of Presentation layer:

- ✓ **Translation:** The processes in two systems exchange the information in the form of character strings, numbers and so on.
- ✓ **Encryption:** Encryption is needed to maintain privacy. Encryption is a process of converting the sender-transmitted information into another form and sends the resulting message over the network.
- ✓ **Compression:** Data compression is a process of compressing the data, i.e., it reduces the number of bits to be transmitted. Data compression is very important in multimedia such as text, audio, video.
- ✓ **Data conversion:** bit order, CR-CR/LF, integer-floating point, and so on.

Responsibility of Session layer:

The session protocol defines the **format of the data** sent over the connections. Session layer **establish and manages the session** between the two users at different ends in a network. Session layer also manages who can transfer the data in a certain amount of time and for how long.

- ✓ **Dialog control:** Session layer acts as a dialog controller that creates a dialog between two processes or we can say that it allows the communication between two processes which can be either half-duplex or full-duplex.
- ✓ **Synchronization:** Session layer adds some checkpoints when transmitting the data in a sequence. If some error occurs in the middle of the transmission of data, then the transmission will take place again from the checkpoint. This process is known as Synchronization and recovery.
- ✓ **Protocols:** The protocols that work on the session layer are **NetBIOS, Mail Slots, Names Pipes, and RPC.**

Responsibility of Transport Layer:

- ✓ **Service-point addressing:** Computers run several programs simultaneously due to this reason, the transmission of data from source to the destination not only from one computer to another computer but also from one process to another process. The transport layer adds the header that contains the address known as a service-point address or port address. The responsibility of the network layer is to transmit the data from one computer to another computer and the responsibility of the transport layer is to transmit the message to the correct process.
- ✓ **Segmentation and reassembly:** When the transport layer receives the message from the upper layer, it divides the message into multiple segments, and each segment is assigned with a sequence number that uniquely identifies each segment. When the message has arrived at the destination, then the transport layer reassembles the message based on their sequence numbers.
- ✓ **Connection control:** Transport layer provides two services Connection-oriented service and connectionless service. A connectionless service treats each segment as an individual packet, and they all travel in different routes to reach the destination. A connection-oriented service makes a connection with the transport layer at the destination machine before delivering the packets. In connection-oriented service, all the packets travel in the single route.
- ✓ **Flow control:** The transport layer also responsible for flow control but it is performed end-to-end rather than across a single link.
- ✓ **Error control:** The transport layer is also responsible for Error control. Error control is performed end-to-end rather than across the single link. The sender transport layer ensures that message reach at the destination without any error.
- ✓ **Protocols:** TCP, UDP, NETBIOS, ATP and NWLINK.

Responsibility of Network Layer:

This layer is **incharge of packet addressing** , converting **logical addresses into physical addresses**. It is responsible for the source-to-destination delivery of a packet across multiple networks (links). **This layer is also incharge of setting the routing.** The packets will use to arrive at their destination, based on factors like traffic and priorities. **The network layer determines that how data transmits between the network devices**.

- ✓ **Internetworking:** An internetworking is the main responsibility of the network layer. It provides a logical connection between different devices.
- ✓ **Addressing:** A Network layer adds the source and destination address to the header of the frame. Addressing is used to identify the device on the internet.
- ✓ **Routing:** Routing is the major component of the network layer, and it determines the best optimal path out of the multiple paths from source to the destination.
- ✓ **Packetizing:** A Network Layer receives the packets from the upper layer and converts them into packets. This process is known as Packetizing. It is achieved by internet protocol (IP).
- ✓ **Fragmentation:** Fragmentation means dividing the larger packets into small fragments.

Which one is a layer 3 (Network Layer) protocol? *[SBL-SO(IT)-2013]*

a) UDP b) DNS c) TCP d)IP **Ans.d**

Responsibility of the Data-link layer

- ✓ **Framing:** The data link layer translates the physical's raw bit stream into packets known as Frames. The Data link layer adds the header and trailer to the frame. The header which is added to the frame contains the hardware destination and source address.

- ✓ **Physical Addressing:** The Data link layer adds a header to the frame that contains a destination address. The frame is transmitted to the destination address mentioned in the header.
- ✓ **Flow Control:** Flow control is the main functionality of the Data-link layer. It is the technique through which the constant data rate is maintained on both the sides so that no data get corrupted. It ensures that the transmitting station such as a server with higher processing speed does not exceed the receiving station, with lower processing speed.
- ✓ **Error Control:** Error control is achieved by adding a calculated value CRC (Cyclic Redundancy Check) that is placed to the Data link layer's trailer which is added to the message frame before it is sent to the physical layer. If any error seems to occurr, then the receiver sends the acknowledgment for the retransmission of the corrupted frames.
- ✓ **Access Control:** When two or more devices are connected to the same communication channel, then the data link layer protocols are used to determine which device has control over the link at a given time.

Which does not work on the Data link layer? *[BB AP-2016]*

a) error control b) adding MAC address c) cabling d) None Ans.c

Functions of a Physical layer:

- ✓ **Line Configuration:** It defines the way how two or more devices can be connected physically.
- ✓ **Data Transmission:** It defines the transmission mode whether it is simplex, half-duplex or full-duplex mode between the two devices on the network.
- ✓ **Topology:** It defines the way how network devices are arranged.
- ✓ **Signals:** It determines the type of the signal used for transmitting the information
- ✓ **Bit rate control:** Physical layer defines the transmission rate *i.e.* the number of bits sent in one second. Therefore it defines the duration of a bit.
- ✓ **Multiplexing**: Physical layer can use different techniques of multiplexing, in order to improve the channel efficiency.

- ✓ **Circuit switching**: Physical layer also provides the circuit switching to interconnect different networks.

Physical Layer

Physical layer is concerned with transmitting raw bits over a communication channel. The design issue has to do with making sure that when one side sends a 1-bit, it received by the other side as 1- bit and not as 0 bit. In physical layer we deal with the communication medium used for transmission.

Types of Medium

Medium can be classified into two categories:

- ✓ **Guided Media:** Guided media means that signals are guided by the presence of physical media i.e., signals are under control and remains in the physical wire. For example, copper wire.
- ✓ **Unguided Media:** Unguided media means that there is no physical path for the signal to propagate. Unguided media has essentially electromagnetic waves. There is no control on flow of signal. For example, radio waves.

Transmission media:

In Guided transmission media, generally two kinds of materials are used.

1. Copper: Coaxial cable,Twisted pair
2. Optical Fiber

Coaxial cable

Coaxial cable consists of an inner conductor and an outer conductor which are separated by an insulator. The inner conductor is usually copper.The outer conductor is covered by a plastic jacket.

Twisted pair

A twisted pair consists of two insulated copper wires, typically 1mm thick. The wires are twisted together in a helical form, the purpose of twisting is to reduce crosstalk interference between several pairs. Twisted pair is much cheaper than coaxial cable but it is susceptible to noise and electromagnetic interference and attenuation is large.

Optical fiber

In optical Fiber light is used to send data. In general terms the presence of light is taken as bit-1 and its absence as bit o.Optical fiber consists of either glass or plastic core which is surrounded by cladding of the same material but of different refractive index. This cladding is surrounded by a plastic jacket which prevents optical fiber from electromagnetic interference and harsh environments.

Communication Link:

In a network nodes are connected through links. The communication through links are classified as

Simplex: Communication can be take plaace in one direction. Example TV broadcasting.

Half Duplex: Communication can take place in one direction at a time. Example walkie-talkies.

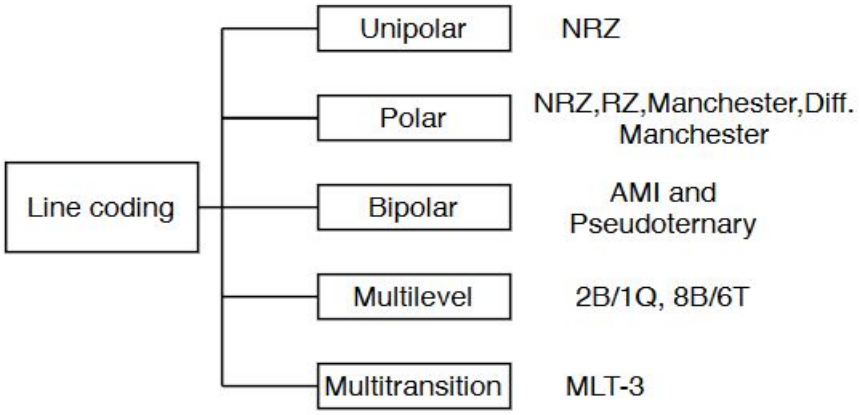
Full Duplex: Communication can take place simultaneously in both direction. Example Telephone networks.

Point-to-Point: In this communication only two nodes are connected to each other.When a node sends a packet then it can be received only by the node on the other side.

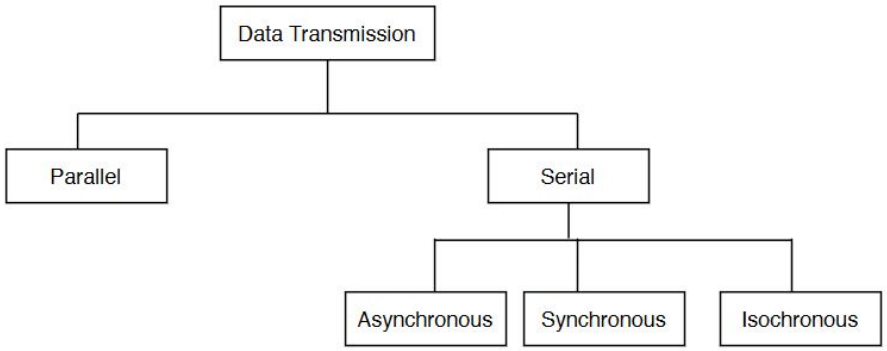
Multi-Point: It is a kind o sharing communication in which signal can be received by all nodes. This is also called broadcast.

Digital data to digital signals:

A digital signal is sequence of discreate, discontinuous voltage pulse. Each pulse is a signal element. Encoding scheme is an important factor in knowing that how successfully the receiver interprets the incoming signal.



Digital data Communication Technique: For two devices linked by a transmission medium to exchange data, a high degree of co operation is required.



Data transmission and mode

Data Link Layer

Data link layer provides interface to the network layer, determines the number of bits of the physical layer to be grouped into frames, detects transmission error and regulates the flow frames,

Function of data link layer:

- ✓ Framing
- ✓ Physical addressing
- ✓ Flow control
- ✓ Error control
- ✓ Access control

Various methods of Framing are

- ✓ Time gaps

- ✓ Character Count
- ✓ Starting and ending character, with character stuffing
- ✓ Starting and ending flags, with bit stuffing
- ✓ Physical layer coding violations

Flow Control

It regulates the flow of frames so that slow receivers are not affected by the fast sender or vice versa. It tells the sender how much data it should transmit before it waits for an acknowledgement from the receiver. Flow control refers to a set of procedures used to restrict the amount of data that the sender can send before waiting for acknowledgement.

Error control in the data link layer is often implemented simply. Any time an error is detected in an exchange, specified frames are retransmitted. This process is called automatic repeat request (ARQ).

What type of architecture does Skype use while conversation? *[JBL-AEO(IT)-2015]*

a) Client Server Architecture b)Peer To Peer Architecture

c) Service oriented architecture d) MVC architecture **Ans.b**

MEDIUM ACCESS CONTROL SUBLAYER

Multiplexing

When two communicating nodes are connected through a media, it generally happens that bandwidth of media is several times greater than that of the communicating nodes.

Transferring of a single signal at a time is both slow and expensive. The whole capacity of the link is not utilized in this case. This link can be further exploited by sending several signals combined into one. This combining of signals into one is called multiplexing.

Frequency Division Multiplexing (FDM)

This is possible in the case where transmission media has a bandwidth higher than the required bandwidth of signals to be transmitted. A number of signals can be transmitted at the same time. Each source is allotted a frequency range in which it can transfer its signals, and a suitable frequency gap is given between two adjacent signals to avoid overlapping. This type of multiplexing is commonly seen in the cable TV networks.

Time Division Multiplexing (TDM)

This is possible when the data transmission rate of the media is much higher than that of the data rate of the source. Multiple signals can be transmitted if each signal is allowed to be transmitted for a definite amount of time. These time slots are so small that all transmissions appear to be in parallel

Synchronous TDM Time slots are pre. Assigned and are fixed. Each source is given it's time slot at every turn due to it. This turn may be once per cycle or several turns per cycle, if it has a high data transfer rate, or maybe once in a number of cycles if it is slow. This slot is given even if the source is not ready with data. So this slot is transmitted empty.

Routing Algorithms

The main function of network layer is routing packets from the source machine to the destination macine. The routing algorithms are part of the network layer software, responsible for deciding which output line an incoming packet should be transmitted on.

Routing algorithms can be grouped into two major classes: Non-adaptive and Adaptive.

1. Non-adaptive algorithms do not base their routing decisions on measurements or estimates of the current traffic and topology. Instead, the choice of the route to use is downloaded to the routers when the network is booted. This procedure is called static routing.
2. Adaptive algorithms, in contrast, change their routing decisions to reflect changes in the topology, and the traffic as well.

Store and forward packet switching

In this technique, the data packet will be storeed at the node and it is forwarded to its next appropriate intermediate node. The next intermediate node will first store the packet in the buffer, based on the router decision, it selects an interface, and forwards to receiver. The technique is most suitable for the networks with unsteady connectivitys.

The length of the packet we take shows effect on the file transfer, if the data packet is small, in the store the forward, delay will be less at each node, but causes extra overhead with headers.So, the packet size selection should be done appropriately.

Some Routing Algorithms:

- ✓ Multipath routing
- ✓ Distance Vector Routing
- ✓ Link State Routing
- ✓ Open Shortest path first(OSPF)

TRANSPORT LAYER

Real communication takes place between two applications programs i.e processes. For this process-to-process delivery is needed. A mechanism is required in order to deliver data from one of these processes running on the source host to the corresponding process running on the destination host.

The transport layer is responsible for process-to-process delivery.

Addressing in Transport Layer

Port addresses

- ✓ A transport layer address is a port number,
- ✓ The destination port number is needed for delivery and the source port number is needed for reply.
- ✓ The port numbers are 16-bit integers ranging from 0 to 65535,

The IANA (Internet Assigned Number Authority) has divided the port numbers as:

- ✓ Well-known ports (0 to 1023)
- ✓ Registered ports (1024 to 49151)
- ✓ Dynamic or private or ephemeral ports (49,152 to 65,535)

Socket address

Process to process delivery needs two identifiers, IP address and port address at each end to make a connection.

The combination of an IP address and a port number is socket address.
Lets: IP address---192.53.52.1 Port Number 59
So Socket Address is: 192.53.52.1 59

Protocols at transport layer:

- ✓ UDP
- ✓ TCP
- ✓ SCTP

USER DATAGRAM PROTOCOL (UDP)

UDP is **connectionless** protocol.

- ✓ There is no mechanism for connection establishment or connection termination.
- ✓ The packets may be delayed or lost or may arrive out of sequence, i.e., there is no acknowledgement.
- ✓ Each user datagram sent by UDP is an independent program. Even if the user datagram are coming from the same source program and going to the same destination process, there is no relationship between the different datagrams.Thus, user datagrams can travel on a different path.
- ✓ Multicasting capability is embedded in UDP.
- ✓ It is a simple, unreliable transport protocol.
- ✓ There is no flow control, no window mechanism.
- ✓ There is no error control as well except for the checksum. The sender does not know if a message has been lost or duplicated. When the receiver detects an error through the checksum, the datagram is discarded silently.
- ✓ It is used in real-time applications.
- ✓ The header length is fixed, of 8 bytes. Real time applications require a constant flow of data. Moreover, the unreliability (fast and less complex service) of UDP aids in real-time applications like voice over IP, online games etc.
- ✓ It encapsulates and decapsulates messages in an IP datagram.

TCP/IP

- ✓ TCP stands for Transmission Control Protocol,
- ✓ It is **connection-oriented** protocol.
- ✓ TCP has 5 layer.
- ✓ It creates a virtual connection between two TCPs to send data then data is transferred and at the end the connection is released.
- ✓ There is an acknowledgement mechanism for safe and sound arrival of data.
- ✓ It is a reliable transport protocol.
- ✓ Uses flow and error control.
- ✓ Slower and more complex service.
- ✓ Duplicate segments are detected, lost segments are resent, the bytes are delivered to the end process in order.
- ✓ It is a stream-oriented protocol.

- ✓ TCP offers **full duplex** services data can flow in both directions at the same time.
- ✓ Each TCP has a sending and receiving buffer.

----Provides a connection- oriented reliable service for sending message. *[probashi kallyan bank(P)-2019]*

a)TCP b) IP c) UDP d) None of these Ans.: a

APPLICATION LAYER

An interface between the networks is called application. This section introduces two important concepts:

- ✓ Application Layer: The application layer of the OSI model provides the first step of getting data onto the network.
- ✓ Application Software: Applications are the softwere programs used by people to communicate over the network. Examples of application software, includes HTTP, FTP,e-mail, and others, used to explain the differences between these two concepts.

TCP/IP Application Layer Protocol

The most widely known TCP/IP application layer protocols are those that provide the exchange of user information. These protocols specify the format and control information necessary for many of the common internet communication functions. Among these, TCP/IP protocols are the following

- ✓ Domain name system (DNS) is used to resolve internet names to IP addresses.
- ✓ Hypertext transfer protocol (HTTP) is used to transfer files that make up the web pages of the world wide web.
- ✓ Simple mail transfer protocol (SMTP) is used for the transfer of mail messages and attachments.
- ✓ Telnet, a terminal emulation protocol, is used to provide remote access to servers and networking devices.
- ✓ File transfer protocol (FTP) is used for interactive file transfers between systems.

SMTP

- ✓ SMTP stands for simple mail transfer protocol.
- ✓ It uses the services of TCP on port number 25.
- ✓ It is a push protocol. Even when the destination is not interested to receive the message this push approach of the SMTP makes the receiver receive the message.

POP3

- ✓ It is a pull protocol
- ✓ It uses the services of TCP on port number 110

HTTP

- ✓ HTTP stands for Hyper Text Transfer Protocol.
- ✓ It uses the services of TCP on well known port 80
- ✓ It is a protocol mainly used to access data on the world Wide Web(www).
- ✓ HTTP functions as a combination of FTP and SMTP.
- ✓ It uses only one TCP connection; there is no separate control connection.
- ✓ It works on two commands request ans reply.

FTP

- ✓ FTP uses the services of TCP
- ✓ Its needs two TCP connections. Port 21 for the control connection and port 20 for the data connection.

DNS

- ✓ Stands for Domain name System.
- ✓ The DNS is a client/server application that identifies each host on the internet with a unique
- ✓ User-friendly name i.e it is used to map an uniform Resource Locator (URL) to an IP address.
- ✓ DNS can use the services of UDP or TCP wing the well known port 53
- ✓ If the size of the response mense is more than 512 bytes, it uses the TCP connection,
- ✓ When the size of the response message is less than 512 bytes, UDP connection is used. Even though the of message is not known then also the UDP can be used.

What does the DNS database contain? *[JBL-AEO(IT)-2015]*

a) Name server Records b) Hostname-to-address records

c) Hostname Aliase d) All of these **Ans.: d**

Which of the following protocols uses both TCP and UDP ports? *[SBL-AP-2016]*

a) SMTP b)telnet c) FTP d)DNS **Ans.d**

Networking Devices

Repeater

In digital communication systems, a repeater is a device that receives a digital signal on an electromagnetic or optical transmission medium and regenerates the signal. Repeaters remove the unwanted noise in an incoming signal. Unlike an analog signal, the original digital signal, even if weak or distorted, can be clearly perceived and restored. With analog transmission, signals are strengthened with amplifiers which unfortunately also amplify noise as well as information.

Hub

A hub is basically a multiport repeater. A hub connects multiple wires coming from different branches, for example, the connector in star topology which connects different stations. Hubs cannot filter data, so data packets are sent to all connected devices. In other words, collision domain of all hosts connected through Hub remains one. Also, they do not have intelligence to find out best path for data packets which leads to inefficiencies and wastage.

Switch

In a telecommunications network, a switch is a device that channels incoming data from any of multiple input ports to the specific output port that will take the data towards its intended destination. In the traditional circuit-switched telephone network, one or more switches are used to set up a dedicated though temporary connection or circuit for an exchange between two or more parties.

In the open systems Interconnection (OST) communications model, a switch performs the Layer 2 or Data-link layer function

Bridge

A bridge operates at data link layer. A bridge is a repeater, with add on the functionality of filtering content by reading the MAC addresses of source and destination. It is also used for interconnecting two LANs working on the same protocol. It has a single input and single output port, thus making it a 2 port device.

Router:

A router is a three-layer device that routes packets based on their logical addresses (host-to-host addressing). A router normally connects LANs and WANs in the Internet and has a routing table that is used for making decisions about the route. The routing tables are normally dynamic and are updated using routing protocols. Data is grouped into packets, or blocks of data. Each packet has a physical device address as well as logical network address. The network address allows routers to calculate the optimal path to a workstation or computer.

Gateway:

A gateway is normally a computer that operates in all five layers of the Internet or seven layers of OSI model. A gateway takes an application message, reads it, and interprets it. This means that it can be used as a connecting device between two internetworks that use different models.

IPV4 ADDRESSES

Each machine on the internet has a unique identification number, called an IP address. An IPv4 address is a 32-bit address that uniquely and universally defines the connection of a host or a router to the Internet. The IP address is the address of the connection, not the host or the router, because if the device is moved to another network, the IP address may be changed. IPv4 addresses are unique in the sense that each address defines one, and only one, connection to the Internet. If a device has two connections to the Internet, via two networks, it has two IPv4 addresses

Address Space

A protocol like IPv4 that defines addresses has an address space. An **address space** is the total number of addresses used by the protocol. If a protocol uses *b* bits to define an address, the address space is 2*b* because each bit can have two different values (0 or 1). IPv4 uses 32-bit addresses, which means that the address space is 232 or 4,294,967,296 (more than four billion). If there were no restrictions, more than 4 billion devices could be connected to the Internet.

IPv4 Address Classes

As explained in the previous section, the 32-bit IPv4 addressing scheme allows a large number of host addresses to be defined. However, the link-based addressing scheme adopted by IP requires network links to be associated with groups of addresses from which the connected hosts are assigned specific addresses. These address groups, described also as address prefixes, and are referred to in classical IP terminology as IP network numbers.

Address Class	Bit Pattern of First Byte	First Byte Decimal Range	Host Assignment Range in Dotted Decimal
A	0xxxxxxx	1 to 127	1.0.0.1 to 126.255.255.254
B	10xxxxxx	128 to 191	128.0.0.1 to 191.255.255.254
C	110xxxxx	192 to 223	192.0.0.1 to 223.255.255.254
D	1110xxxx	224 to 239	224.0.0.1 to 239.255.255.254
E	11110xxx	240 to 255	240.0.0.1 to 255.255.255.255

- ✓ Classes A-C: unicast addresses
- ✓ Class D: multicast addresses
- ✓ Class E: reserved for future use

ClassA

In a class A address, the first bit of the first octet is always '0'. Thus, class A addresses range from 0.0.0.0 to 127.255.255.255(as 01111111 in binary converts to 127 in decimal). The first 8 bits or the first octet denote the network portion and the rest 24 bits or the 3 octets belong to the host portion.

Example: 10.1.1.1

- ✓ 127.X.X.X is reserved for loopback
- ✓ 0.X.X.X is reserved for default network
- ✓ Therefore, the actual range of class A addresses is: 1.0.0.0 to 126.255.255.255

Class B

In a class B address, the first octet would always start with '10'. Thus, class B addresses range from 128.0.0.0 to 191.255.255.255. The first 16 bits or the first two octets denote the network portion and the remaining 16 bits or two octets belong to the host portion.

Example: 172.16.1.1

Class C

In a class C address, the first octet would always start with '110'. Thus, class C addresses range from 192.0.0.0 to 223.255.255.255. The first 24 bits or the first three octets denote the network portion and the rest 8 bits or the remaining one octet belong to the host portion.

Example: 192.168.1.1

Class D

Class D is used for multicast addressing and in a class D address the first octet would always start with '1110'. Thus, class D addresses range from 224.0.0.0 to 239.255.255.255.
Example: 239.2.2.2

- ✓ Class D addresses are used by routing protocols like OSPF, RIP, etc.

Class E

Class E addresses are reserved for research purposes and future use. The first octet in a class E address starts with '1111'. Thus, class E addresses range from 240.0.0.0 to 255.255.255.255.

IPV 6

- ✓ IPv6 is the next generation Internet Protocol designed as a successor to the IP version 4.
- ✓ IPv6 was designed to enable high performance, scalable internet.
- ✓ This was achieved by overcoming many of the weaknesses of IPv4 protocol and by adding several new features.
- ✓ In IPv6, there are 2128 possible ways (about 3.4 x 1038 addresses).
- ✓ IPv6 is written in hexadecimal and consists of 8 groups, containing 4 hexadecimal digits or 8 groups of 16 bits each.
- ✓ The IPv6 header is a static header of 40 bytes in length and has only 8 fields. Option information is carried by the extension header which is placed after the IPv6 header.
- ✓ IPv6 has no header checksum because checksums are for example above the TCP/IP protocol suite and above the Token Ring, Ethernet etc.
- ✓ The IPv6 header contains an 8 bit field called the Traffic Class Field. This field allows the traffic source to identify the desired delivery priority of its packets.
- ✓ The IPv6 has both a stateful and stateless address auto-configuration mechanism.
- ✓ IPv6 has been designed to satisfy the growing and expanded need for network security.
- ✓ Source and destination addresses are 128 bits (16 bytes) in length.
- ✓ Packet flow identification for QoS handling by routers is included in the IPv6 header using the Flow Label Field.
- ✓ ARP request frames are replaced with multicast neighbour solicitation messages.
- ✓ ICMP router discovery is replaced with ICMPv6 router solicitation and router advertisement messages are required.
- ✓ IPv6 has three different types of addresses.

Unicast: A unicast address defines a single computer. A packet sent to a unicast address is delivered to that specific computer.

Anycast: This is a type of address that defines a group of computers with addresses which have the same prefix. A packet sent to an anycast address must be delivered to exactly one of the members of the group which is closest or the most easily accessible.
Multicast: A multicast address defines a group of computers which may or may not share the same prefix and may or may not be connected to the same physical network. A packet sent to a multicast address must be delivered to each member of the set.

Advantages of IPv6:

Larger address space: IPv6 has 128 bit address space which is 4 times wider in bits compared to IPv4's 32 bit address space. So there is a huge increase in the address space.

Better header format: IPv6 uses a better header format. In its header format the option are separated from the base header. The options are inserted when needed between the base header and upper layer data. This helps in speeding up the routing process.

New options: New options have been added in IPv6 to increase the functionality.

Possibility of extension: IPv6 has been designed in such a way that there is a possibility of extension of protocol if required.

More security: IPv6 includes security in the basic specification. It includes encryption of packets (ESP: Encapsulated Security Protocol) and authentication of the sender of packets (AH: Authentication Header)

Support to resource allocation: To implement better support for real time traffic (such as video conference), IPv6 includes flow label in the specification. With flow label mechanism, routers can recognize to which end-to-end flow the packets belongs.

Plug and play: IPv6 includes plug and play in the standard specification. It therefore must be easier for novice users to connect their machines to the network, it will be done automatically.

Clearer specification and optimization: IPv6 follows good practices of IPv4 and rejects minor flaws/obsolete items of IPv4.

What is not the advantage of IPV6 over IPV4? *[probashi kallyan bank(P)-2019]*

a)longer address b) Classification of traffic

c) More real IP addresses d) Jumbo Payload Ans.a

Some Important Abbreviation

Sort	Abbreviation
CDMA	Code Division Multiple Access
GSM	Global System for Mobiles Communication
GPRS	General Packet Radio Services
GPS	Global Positioning System
LCD	Liquid crystal display
LED	Light-emitting diode
CRT	Cathode ray tube
DVD	Digital versatile disc/ Digital video disc
FAT	File Allocation Table
WAR	Web Application Resource/ Web Application Archive
WAP	Wireless application Protocol
DLL	Dynamic Link Library
HDTV	High Definition Television
HTML	Hypertext Markup Language
EDGE	Enhanced Data for GSM Evolution
XML	Extensible Markup Language
RAID	Redundant array of independent disks
DAT	Digital Audio Tape/ Dynamic Address Translation
NTFS	New Technology for File System
JAR	Java Archive
ERP	Enterprise resource planning
APK	Android Application package
UTF	Unicode Transformation Format

Some Important Protocol:

Protocol	Abbreviation	Description
IP	Internet Protocol	The principal communications protocol in the Internet protocol suite for relaying datagram's across network boundaries. Its routing function enables internetworking, and essentially establishes the Internet
UDP	User Datagram Protocol	which acts as an alternative communication protocol to TCP and is used to establish low-

		latency and loss-tolerating connections between applications and the Internet.
RTPS	Real-Time Publish Subscribe	
FTP	File Transfer Protocol	used for the transfer of computer files between a client and server on a computer network
SMTP	Simple Mail Transfer Protocol	an Internet standard for electronic mail (email) transmission
TCP	Transmission Control Protocol	is one of the main protocols of the Internet protocol suite. It originated in the initial network implementation in which it complemented the Internet Protocol (IP). Therefore, the entire suite is commonly referred to as TCP/IP.
Telnet	Teletype Network	allows you to connect to remote computers (called hosts) over a TCP/IP network (such as the Internet)
HTTP	Hypertext Transfer Protocol	Hypertext is structured text that uses logical links (hyperlinks) between nodes containing text
HTTPS	Hyper Text Transfer Protocol Secure	It means all communications between your browser and the website are encrypted.
POP	Post Office Protocol	an application-layer Internet standard protocol used by local e-mail clients to retrieve e-mail from a remote server over a TCP/IP connection
HTCPCP	Hyper Text Coffee Pot Control Protocol	
SSL	Secure Sockets Layer	provides a secure channel between two machines operating over the Internet or an internal network
TLS	Transport Layer Security	its predecessor, Secure Sockets Layer (SSL), both frequently referred to as "SSL", are cryptographic protocols that provide communications security over a computer network
IMAP	Internet Message Access Protocol	is a standard email protocol that stores email messages on a mail server, but allows the end user to view and manipulate the messages as though they were stored locally on the end user's computing device(s)
PPP	Point-to-Point Protocol	used to establish a direct connection between two nodes
QOTD	Quote of the Day	the QOTD concept predated the specification, when QOTD was used by mainframe

		sysadmins to broadcast a daily quote on request by a user
NNTP	Network News Transfer Protocol	protocol used for transporting Usenet news articles (Netnews) between news servers and for reading and posting articles by end user client applications
NTP	Network Time Protocol	is a networking protocol for clock synchronization between computer systems over packet-switched, variable-latency data networks
SMTP	Simple main transport Protocol	which is used to send and distribute outgoing e-mails.

Internet Protocol - TCP, UDP, HTTP, and FTP
Wireless Network Protocols - Wi-Fi, Bluetooth, and LTE,
Network Routing Protocols- EIGRP, OSPF, and BGP.

Which of the following is not a standard synchronous communication protocol? *[Com. bank(officer)-2019]*

a) PAS b) SDLC c) SLIP d) SMTP Ans. a

Which of the standard protocol for network management features? *[Com. bank(officer)-2019]*

a) FTP b) SNA c) SNMP d) SMTP Ans. c

POP3 is a protocol for- [Com. bank(officer)-2019]

a) Email Sending b) Email Composing c) Email Receiving d) Email Storing Ans. c

Some Protocol and there port number

Protocol Name	Port Number
FTP	20,21
Telnet	23
SMTP	25
DNS	53
HTTP	80
POP3	110
HTTPS	443

Cryptography:

Cryptography is associated with the process of converting ordinary plain text into unintelligible text and vice-versa. It is a method of storing and transmitting data in a particular form so that only those for whom it is intended can read and process it. Cryptography not only protects data from theft or alteration, but can also be used for user authentication.

Modern cryptography concerns with:

- ✓ Confidentiality - Information cannot be understood by anyone
- ✓ Integrity - Information cannot be altered.
- ✓ Non-repudiation - Sender cannot deny his/her intentions in the transmission of the information at a later stage
- ✓ Authentication - Sender and receiver can confirm each

Uses of Cryptography: banking transactions cards, computer passwords, and e- commerce transactions etc.

Types of Cryptography techniques: Three types of cryptographic techniq used in general.

- ✓ Symmetric-key cryptography
- ✓ Hash functions.
- ✓ Public-key cryptography

Symmetric-key Cryptography: Both the sender and receiver share a single key. The sender uses this key to encrypt plaintext and send the cipher text to the receiver. On the other side the receiver applies the same key to decrypt the message and recover the plain text. AES, RC4, DES, 3DES, RC5, RC6, etc. Out of these algorithms, DES and AES algorithms are the best known.

Public-Key Cryptography: This is the most revolutionary concept in the **last 300-400** years. A public key, which everyone knows, and a private key, which only you know. To encrypt, the public key is applied to the target information, using a predefined operation (several times), to produce a pseudo-random number. To decrypt, the private key is applied to the pseudo-random number, using a different predefined operation (several times), to get the target information back.
Example: RSA

Hash Functions: No key is used in this algorithm. A fixed-length hash value is computed as per the plain text that makes it impossible for the contents of the plain text to be recovered. Hash functions are also used by many operating systems to encrypt passwords. For example, bitcoin, the original and largest cryptocurrency, uses the SHA-256 cryptographic hash function in its algorithm. Similarly, IOTA, a platform for the Internet of Things, has its own cryptographic hash function, called Curl.

Common Encryption Algorithms

Name	Type	Comment
Triple DES	Symmetric algorithm	Triple DES uses three individual keys with 56 bits each. The total key length adds up to 168 bits, but experts would argue that 112-bits
RSA	public-key encryption	
Blowfish		This symmetric cipher splits messages into blocks of 64 bits and encrypts them individually.

AES	Advanced Encryption Standard (AES)	AES also uses keys of 192 and 256 bits for heavy duty encryption purposes.

Networking

1. Which does not work on the Data link layer? [BB AP-2016]

a) error control b) adding MAC address c) cabling d) None Ans.c

1. Which of the following is not a standard synchronous communication protocol? [Com. bank(officer)-2019]

a) PAS b) SDLC c) SLIP d) SMTP Ans. a

2. Which of the standard protocol for network management features? [Com. bank(officer)-2019]

a) FTP b) SNA c) SNMP d) SMTP Ans. c

3. How many pairs of stations can simultaneously communicate on Ethernet LAN? [Com. bank(officer)-2019]

a) 1 b) 2 c)3 d) Multiple Ans. a

Explanation: only 1 pair of stations can communicate on Ethernet LAN. LAN is defined as local area network. It is used for short distances.

4. A path for carrying signals between a source and a destination is known as - [Com. bank(officer)-2019]

a) Router b) Channel c) Link d) Block Ans. b

1. POP3 is a protocol for- [Com. bank(officer)-2019]

a) Email Sending b) Email Composing c) Email Receiving d) Email Storing Ans. c

1. What is not the advantage of IPV6 over IPV4?**[probashi kallyan bank(P)-2019]**

a)longer address b) Classification of traffic

c) More real IP addresses d) Jumbo Payload Ans.a

1. What type of network provides access to the regional service providers and typically span distances greater than 100 miles? **[probashi kallyan bank(P)-2019]**

a) LAN b) MAN c) WAN d) WLAN Ans.c

2. ----Provides a connection- oriented reliable service for sending message. **[probashi kallyan bank(P)-2019]**

a)TCP b) IP c) UDP d) None of these Ans.: a

1. A device that allows one of several analog or digital input signals which are to be selected and transmits input that is selected into a single medium is called **[probashi kallyan bank(P)-2019]**

a) signal changer b)multiplexer c) demultiplexer d) digital transmitter Ans. b

1. Any hardware or software which is used to connect two devices by enabling them to communicate is claşsified as [probashi kallyan bank(P)-2019]

a) analogue modem b) digital modem c) analogue interface d) interface Ans. d

1. Issuance of cash through terminal outside bank is an example of[probashi kallyan bank(P)-2019]

a) terminals b) interfaces c) hardware devices d) telecommunication Ans. a

1. A path for carrying signals between a source and a destination is known as[probashi kallyan bank(AP)-2019]

a)Router b)Channel c) Link d) Block Ans.b

1. Which of the standard protocol for network management features?[probashi kallyan bank(AP)-2019]

a)SNMP b)SNA c)FTP d)SMTP Ans.a

1. Which of the following is not a standard synchronous communication protocol?[probashi kallyan bank(AP)-2019]

a)SDLC b)SNA c)FTP d)SMTP Ans.c

1. What can greatly reduce TCP/IP configuration problem?[BREB-(AJE)-2019]

a)WINS Server b)WINS Power c)DHCP Server d)PDC

1. Which one is used in FTP protocol?[BPSC(ANE)-2019]

a)IP b)TCP c)UDP d)SMTP

Which one is working IP-mapping from domain name? [BPSC(ANE)-2019]

a. HTTP b) SMTP c) DNS d) Telnet Ans.: c

Congestion control occur in which layer [BPSC(ANE)-2019]

a. Physical b) data link c) Network d) Transport

1. Which of the following defines the addressing capabilities of the networking? [Com bank- SO(IT/ICT)-2018]

a) OSL b) NAT c) TCP d) UDP **Ans.b**

1. How many layers are there in the software part of networking framework? [Com bank- SO(IT/ICT)-2018]

a) Three b) Sever c) Four d) Five **Ans. b**

1. **A host machine is unable to communicate with google server. Which command is the most appropriate to run at host machine to determine which intermediary device is responsible for this failure? [Com bank- AME-2018]**

a) telnet 192.168.1.1 b) ping 192.168.1.1

c) tracert 192.168.1.1 d) ftp 192.168.1.1 **Ans. c**

1. **Which of the following protocols uses both TCP and UDP ports? [Com bank- AME-2018]**

a)SMTP b) Telnet c) FTP d) DNS **Ans.d**

1. **To divide a class C network into a maximum of 14 subnets- each capable of having up to 14 hosts. The subnet mask used should be ---------- [Com bank- AME-2018]**

a)255.255.255.240 b) 255.255.255.192 c)255.255.255.78 d) 255.255.255.0 **Ans. a**

1. **Email is a protocol of following layer----------[Com bank- AME-2018]**

a)Physical layer b) Data Link Layer c) Application layer d) TCP layer **Ans. c**

1. **Which protocol is used for secure web browsing? [Com bank- AME-2018]**

a)WWW b) RSA c) ftp d)https **Ans. d**

1. **How many layer internet protocol suites? [Com bank- AME-2018]**

a)7 b) 5 c) 3 d) 4 **Ans. d**

1. **Which of the following sends data packets over unprotected system [Com bank- AP-2018]**

a)OSL b) NAT c) TCP d) UDP **Ans. d**

1. **Extranet allows-[SBL JBL- SO(IT/ICT)-2018]**

a) insiders only b) authorized outsides only
c) all outside d) both inside and authentic outsides **Ans. d**

1. **Which of the following protocols uses both TCP and UDP ports?[ICB-AP-2017]**

a) SMTP b) Telnet c) FTP d)DNS **Ans. d**

1. **Which of the following TCP/IP addresses constitute the loopback address? [ICB-AP-2017]**

a) 1.1.1.1 b)255.255.255.255 c) 127.0.0.0 d) 127.0.0.1 **Ans.d**

1. **Which protocol can cause overload on a managed device? [ICB-AP-2017]**

a) Netflow b)WCCP c) IP SLA d) SNMP **Ans. d**

1. **To divide a class C network into a maximum of 14 subnets – each capable of having up to 14 hosts, the subnet mask use should be [SBL-AE-2016]**

a) 255.255.255.0 b)255.255.255.192
c) 255.255.255.78 d) 255.255.255.240 **Ans.d**

1. **Email is a protocol of the following layer? [SBL-AE-2016]**

a) PhysicalLayer b)Data Link Layer c) Application Layer d) TCP layer **Ans. c**

1. **Which of the following protocols uses both TCP and UDP ports? [SBL-AP-2016]**

a) SMTP b)telnet c) FTP d)DNS **Ans.d**

1. **Which of the following TCP/IP addresses constitute the loopback address? [SBL-AP-2016]**

a) 1.1.1.1 b)255.255.255.0 c) 127.0.0.0 d) 127.0.0.1 **Ans.d**

1. **In TCP/IP model which one is not a valid layer? [JBL-AEO(IT)-2015]**

a) Application Layer b)Internet Layer

c) Transport Layer d) Physical Layer **Ans.b**

1. **What type of architecture does Skype use while conversation? [JBL-AEO(IT)-2015]**

a) Client Server Architecture b)Peer To Peer Architecture

c) Service oriented architecture d) MVC architecture **Ans.b**

1. **What does the DNS database contain? [JBL-AEO(IT)-2015]**

a) Name server Records b) Hostname-to-address records

c) Hostname Aliase d) All of these **Ans.d**

1. Which one is a layer 3 (Network Layer) protocol? [SBL-SO(IT)-2013]

a) UDP b) DNS c) TCP d)IP **Ans.d**

1. In an email address "aaa@bbb.ccc", the portion "bbb" indicates? [SBL-SO(IT)-2013]

a) Domain name b) TCP/IP Layer name c) Domain type d) Protocol name **Ans. a**

1. The type of internet connection might be compared to regular telephone call, in a term of its duration: [SBL-SO(IT)-2013]

a) Baseband b) Broadband c) Dial up d) Satellite **Ans.c**