Ans -(1) =

The Application layer serves as the window for users and application process to access the network services.

=> The Application layer contains a variety of commonly needed functions: -

(1) Network Virtual Terminal
(2) Remote File Access and Resource Management
(3) Electronic messaging
(4) Inter-Process Communication
(5) Directory services
(6) Addressing and Authentication

* Authentication *

=> This layer provides authentication to occur between the devices.

=> This functionality provides an extra layer of security

=> It authenticates both sender and receiver's message

* Directory Services *

=> A database is contained by an application that provides access to global information about various services, etc.

* Mail Services *

=> Application layer provides mail services for email forwarding and storage.

* File transfer, Access and management :-

=> This functionality is also called FTAM.

=> It allows users to access files in a remote computer, to retrive files from computer and to manage files in remote computers.

* Network Virtual Terminal *

=> It provides software version of physical terminal.

=> It also permits users for logging into remote host.

* Addressing *

=> To achieve communication between client and server, there is need for addressing.

=> Request is sent to server from client and server answers the request.

=> It happens with the help of address.

=> DNS is common example.

Ans-

(2) Data Encapsulation is the process of adding additional information when the data is traveling in OSI or TCP/IP model.

=> The addition information is added on the sender's side

=> The addition of information starts from Application layer and continues till physical layer

* Working of Encapsulation *

=> NO additional information is added in the data in the Application layer of TCP/IP or in Application, Presentation and Session layer of OSI model.

=> The Session layer sends data to transport layer.

=> In transport layer, data is broken into different pieces.

=> Transport layer adds header in each of the broken data.

=> This header contains information like source and destination port, sequence number, etc.

=> Everything is combined.

=> The encapsulated data in the transport layer is called Segments.

=> Here, transmission using TCP, then it is called Segments.

=> If transmission using UDP then, datagrams.

=> Data comes to network network layer.

=> Here, layer 3 header is added which contains source IP, destination IP, and other information.

=> The data is again combined.

=> The encapsulated data in network layer is called Packets.

=> The data comes to data-link layer.

=> Here, header and trailer are added.

=> It contains info. like source MAC address, destination MAC address, etc.

=> The trailer is used for error checking

=> The encapsulated data is called Frames.

=) In Physical layer, encapsulated data is called Bits.

=) The encapsulated data is called by different names in the layers.

=) These names are called Protocol Data Units (PDU)

=)

Application, Presentation, Session	Data
Transport	Segment / Datagram
Network	Packets
Datalink	Frames
Physical	Bits.

Ans -(3)

Static Routing	Dynamic Routing
=> Routing routes are user defined	=> Routes are updated according to changes in topology.
=> It does not use complex routing algorithms	=> It uses complex routing algorithms.
=> The routing is manual	=> The routing is automated
=> Implemented in small network	=> Implemented in large networks
=> Provides high security	=> Provides low security.

=> Suppose, if we want to connect three networks with static routing.

=> Suppose, we connect networks with the help of 3 routers: Router A, B, C.

=> In static routing, I will have to provide Routing information for /in all the routers connected in the network manually.

=> Any changes will not be reflected so, we need to do modifications manually.

=> while, this is eliminated in Dynamic Routing, where we can use RIP or OSPF protocols.

Page: WALES
Date:

Ans -(4) => An Access Network is a type of network which physically connects an end system to the immediate router.

=> This connection forms on a path from the end system to any other distant end system.

* Types of Access Networks:-
  (1) Ethernet
  (2) DSL
  (3) FTTH
  (4) Wireless LAN.
  (5) LTE

* Ethernet:-

=> It is the common installed wired LAN technology.

=> It provides services on physical layer and data link layer.

=> Ethernet lan uses coaxial cable or twisted pair wires.

* DSL :-

=> DSL stands for Digital Subscriber Line.

=> It brings connection to home through telephone lines and a DSL line carries both data and voice signals.

=> Here, the data part of the line is continuously connected.

=> DSL modem uses telephone lines to exchange data with DSLAMs.

* FTTH :-

=> It stands for Fibre to the home.

=> It uses optical fibre from a central office to buildings.

=> It provides high speed internet access among all.

=> It is the most expensive and future proof option among all.

(3) 19DCS0018

Page: WALES
Date:

* Wireless LANS *

=> It links two or more devices using wireless communication

=> This connection is within range.

=> It uses high-frequency radio waves.

=> It often include an access point for connecting to the internet

Ans- (5) CSMA/CD stands for Cassier Sense Multiple Access/ collision Detection.

=) It is made up of two words : (1) CSMA
(2) CD

=) The protocols in which the stations listen for a cassier for transmission and act accordingly are called cassier sense protocol.

=) CSMA/CD is one of such protocols.

=) The working is as follow:-

=) If two stations sense the ~~cast~~ channel to be idle and begin data transmission simultaneously., then collision might occur.

=) Here, the stations will detect the collision almost immediately.

=) Rather than finish transmitting their frames, which are gasbled anyway and data loss will occur, they abruptly stop transmission.

=) Data transmission stops as soon as collision is detected.

=) This protocol is called CSMA/CD.

=) It is widely used on LANs in the MAC sublayer.

=> Here, collision are detected by looking at the power of 1 or pulse width of the received signal.

=> This signal is compared with the transmitted signal.

=> After a station detects a collision, it aborts the transmission

=> The station waits for a random period of time and then tries again.

=> This model consists of alternating contention and transmission periods, with idle periods occuring when all the stations are quiet.

=> This protocol detects the collision, but it does not reduce the number of collisions.

=> This protocol is not appropriate for large networks.

(1) 19DCS098

Ans-
(7) =

=) Packet switching is a connection less network switching technique.

=) Here, message is divided and grouped into number of units called packets.

=) There is no need to establish a dedicated circuit for communication.

=) It was designed to provide a more efficient facility than circuit switching.

=) A station transmit data in small blocks called packets.

=) At each node, packets are received, stored briefly and passed on the next node.

=) It is called Store and forward mechanism.

=) A key element of packet switching network is whether the internal operation is datagram or virtual circuit.

=) with internal VCs, a route is defined between two endpoints and all the packets for that VC follow same route.

=) with internal datagram, each packet is treated independently.

=> Examples are X.25, Frame Relay, ATM, etc.

* Datagram:-

=> Each packet treated independently

=> Packets can take any route

=> Packets may arrive out of order

=> Packets may go missing

=> Receiver will re-order packets.

* Virtual Circuit :-

=> Pre-planned Route is established.

=> All the packets will follow the same route through the network

=> Call request and accept packets to establish connection

=> Each packet contains a VC identifier.

=> No routing decisions for each packet

=> Clear Request to drop circuit.

Ans-

(8) Basically, congestion control is a method used for monitoring the process of regulating the total amount of data entering the network so as to keep the traffic level at an acceptable value.

=) It also refers to techniques that can:-

(1) Either remove congestion after it has happened

(2) Prevent congestion before it happens.

=> Congestion control Types:-
(1) Open Loop
(2) Closed Loop

=> Open Loop Congestion control policies are applied to prevent congestion before it happens.

=> The congestion control is held by source or destination

=> Policies adopted by open loop:-

(1) Retransmission Policy
(2) Window Policy
(3) Discarding Policy
(4) Acknowledgement Policy
(5) Admission Policy

=> Closed loop Congestion control Policies are used to treat congestion after it happens.

=> (1) Back pressure
(2) Choke Packet
(3) Implicit Signalling
(4) Explicit Signalling

(1). 19DCS092

Ans
-(a) Network infrastructure refers to all of the Resources of a network that make network or internet connectivity, management, business operation, and communication possible.

=> Network infrastructure allows for effective communication and service between users, applications, services, devices, etc.

=> There are number of challenges in regards to running a network infrastructure.

=> Some challenges are:-

(1) Centralizing Traffic:-

=> Centralized management of network allows for a strategic network design and architecture that can be readily optimized for performance, availability and security.

=> Certain best practice like highly sensitive data and traffic should be isolated through virtual LAN or firewall.

(2) Dealing with duplicate Data :-

=) Duplicate data can sometimes compromise 50-60% of network traffic

=) Removing duplicate data is critical.

=) It is also necessary for network security.

=) More amount of duplicate data causes less effectiveness in detecting threats.

(3) Sending Right Data to Right Tool :-

=) Many companies uses a number of different cyber tools.

=) Sending Right type of data to right tool is a critical aspect of network infrastructure management.

=) It should be cost effective.

WAVES
Page:
Date:

Ans- (10) Both TCP and UDP perform multiplexing and demultiplexing.

=> The job is done by including two fields in the segment header:-

(1) Source port number
(2) Destination port number

* Multiplexing:-

=> Gathering data from multiple application processes of the sender, enveloping that data with header, and sending them as a whole to the intended receiver is called Multiplexing.

* Demultiplexing :-

=> Delivering received segments at the receiver side to correct app layer processes is called demultiplexing.

=> Multiplexing and De-multiplexing takes place at transport layer

=> There are 2 types :-

(1) Connectionless multiplexing and Demultiplexing

(2) Connection oriented multiplexing and De-multiplexing

=> For sending data from an application on sender side to receiver side, sender must know IP address of destination and also Port number.

=> Suppose, A is sender and B is Receiver.

=> A wants to send messages to B in 2 applications.

=> SO, A must mention IP address of B and destination port number of both applications.

=> Now, messages from both apps are wrapped up with some headers and sent as single message

=> This process is called multiplexing.

=> At destination, the received message is unwrapped and individual messages are sent to appropriate application.

=> This is done with the help of Port number

=> This process is called demultiplexing

Ans -(11)

Define the following terms:-

(1) Processing delay :-

=> The time required to examine and process the ~~packet is~~ header of the packet in order to determine where to direct it is called Processing Delay

(2) Queing Delay :-

=> Queuing Delay refers to the time that a packet spends in the waiting for being processed in Queue.

(3) Transmission Delay

=> Transmission Delay is the time taken for packet to be transmitted to the outgoing link.

(4) Propagation Delay

=> Propagation delay is the time taken by packet to reach from one end of the link to other

Ans -(12)

E-mail is an asynchronous communication medium in which people can send and read the messages when it is convenient for them, without having to coordinate with other peoples schedules.

=> Email has 3 major components:-

(1) User Agents
(2) Mail Servers
(3) Mail Transfer Agents

* User Agents *

=> Basically, user agent allows user to read, reply, forward, save and compose messages.

=> Normally, it is a program which is used to send and receive mails.

=> It is also called as Mail Reader

=> Examples are microsoft outlook, G-mail, etc.

* Mail Servers *

=> Mail Servers forms the core of E-mail infrastructure.

=> Mail Server contains two parts:-

(1) Mail Box
(2) Message Queue

=> Mail Box contains the incoming messages
=> Normally, messages that are yet to be read by users are displayed first.

=> Message Queue contains the outgoing mail messages.

=> It contains the mails to be sent.

=> Normally, mail server containing the mail box is used for authentication.

=> If a mail server cannot deliver a message/mail, then it holds the message in message Queue and attempts to transfer the message later.

=> Message Queue is also known as Spool file.

* Mail Transfer Agent *

=> MTA is actually responsible for transfer of mail from one system to another.

=> To Send a mail, a system must have client mail transfer agent and a system mail transfer agent.

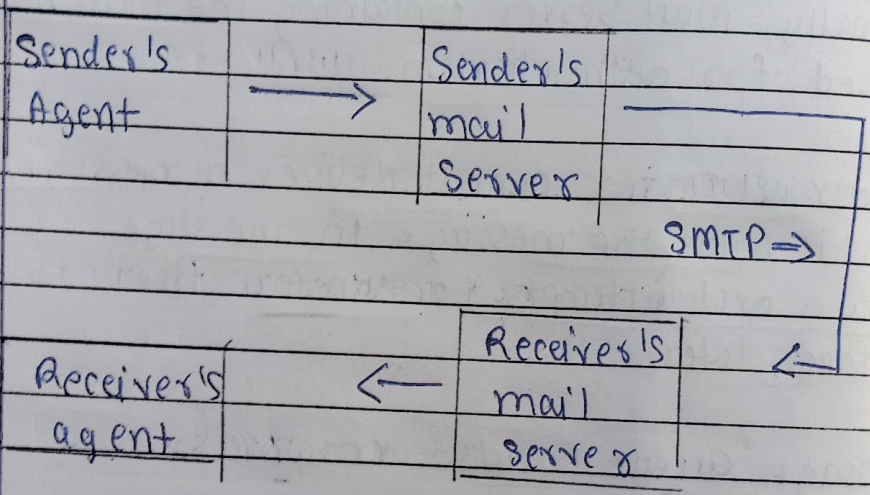
=> It transfer mail to mail boxes of recipients.

⇒ The delivery of email is done by a protocol.

⇒ The protocol is : SMTP.

⇒ SMTP stands for simple mail Transfer Protocol.

⇒ SMTP transfers messages from sender's mail servers to recipient's mail server.



⇒ mail server will contain message Queue and User mailbox.