Define the following

1. NAT

Network Address Translationis designed for IP address conservation. It enables private IP networks that use unregistered IP addresses to connect to the Internet. NAT operates on a router, usually connecting two networks together, and translates the private not globally unique addresses in the internal network into legal addresses, before packets are forwarded to another network

2. FDMA

Frequency-division multiple access is a channel access method used in some multiple-access protocols. allows multiple users to send data through a single communication channel, such as a coaxial cable or microwave beam, by dividing the bandwidth of the channel into separate non-overlapping frequency sub-channels and allocating each sub-channel to a separate user. Users can send data through a subchannel by modulating it on a carrier wave at the subchannels frequency. It is used in satellite communication systems and telephone trunklines.

VLAN

VLAN is a custom network which is created from one or more local area networks. It enables a group of devices available in multiple networks to be combined into one logical network. The result becomes a virtual LAN that is administered like a physical LAN. The full form of VLAN is defined as Virtual Local Area Network.

4. MPLS

The thing about JPLS is that its a technique, not a service so it can deliver anything from IP VPNs to metro Ethernet. Its expensive, so with the advent of SD-WAN enterprises are trying to figure how to optimize its use vs. less expensive connections like the internet.

Q Explain in detail

1. Explain Link state routing algoeithm

Link state routing is a technique in which each router shares the knowledge of its neighborhood with every other router in the internetwork.

Step-1: The node is taken and chosen as a root node of the tree, this creates the tree with a single node, and now set the total cost of each node to some value based on the information in Link State Database

Step-2: Now the node selects one node, among all the nodes not in the tree like structure, which is nearest to the root, and adds this to the tree. The shape of the tree gets changed .

Step-3: After this node is added to the tree, the cost of all the nodes not in the tree needs to be updated because the paths may have been changed.

Step-4: The node repeats the Step 2. and Step 3. until all the nodes are added in the tree

2. Explain dv routing algorithm

A distance-vector routing DVR protocol requires that a router inform its neighbors of topology changes periodically. Historically known as the old ARPANET routing algorithm or known as Bellman-Ford algorithm.

Bellman Ford Basics - Each router maintains a Distance Vector table containing the distance between itself and ALL possible destination nodes. Distances, based on a chosen metric, are computed using information from the neighbors distance vectors.

A router transmits its distance vector to each of its neighbors in a routing packet.

Each router receives and saves the most recently received distance vector from each of its neighbors.

A router recalculates its distance vector when:

It receives a distance vector from a neighbor containing different information than before.

It discovers that a link to a neighbor has gone down.

From time-to-time, each node sends its own distance vector estimate to neighbors.

When a node x receives new DV estimate from any neighbor v, it saves v's distance vector and it updates its own DV using B-F equation

4. ARP and RARp

ARP stands for Address Resolution Protocol.

Whereas RARP stands for Reverse Address Resolution Protocol.

Through ARP, 32-bit IP address mapped into 48-bit MAC address.

Whereas through RARP, 48-bit MAC address of 48 bits mapped into 32-bit IP address.

In ARP, broadcast MAC address is used.

While in RARP, broadcast IP address is used.

- In ARP, ARP table is managed or maintained by local host.

While in RARP, RARP table is managed or maintained by RARP server.

- In Address Resolution Protocol, Receiver's JAC address is fetched.

While in RARP, IP address is fetched.

- In ARP, ARP table uses ARP reply for its updation.

While in RARP, RARP table uses RARP reply for configuration of IP addresses.

- Hosts and routers uses ARP for knowing the JAC address of other hosts and routers in the networks.

While RARP is used by small users having less facilities.

Q. Explain Pakcet Switching Algo

Packet switching allows delivery of variable bit rate data streams, realized as sequences of packets, over a computer network which allocates transmission resources as needed using statistical multiplexing or dynamic bandwidth allocation techniques. As they traverse networking hardware, such as switches and routers, packets are received, buffered, queued, and retransmitted (stored and forwarded), resulting in variable latency and throughput depending on the link capacity and the traffic load on the network. Packets are normally forwarded by intermediate network nodes asynchronously using first-in, first-out buffering, but may be forwarded according to some scheduling discipline for fair queuing, traffic shaping, or for differentiated or guaranteed quality of service, such as weighted fair queuing or leaky bucket.

Packet-based communication may be implemented with or without intermediate forwarding nodes switches and routers. In case of a shared physical medium such as radio or 10BASES, the packets may be delivered according to a multiple access scheme.

Packet switching contrasts with another principal networking paradigm, circuit switching, a method which pre-allocates dedicated network bandwidth specifically for each communication session, each having a constant bit rate and latency between nodes. In cases of billable services, such as cellular communication services, circuit switching is characterized by a fee per unit of connection time, even when no data is transferred, while packet switching may be characterized by a fee per unit of information transmitted, such as characters, packets, or messages.

Q. What is Network layer and Data Link Layer ?

- The network layer

Located at Layer 3 of the Open Systems Interconnection OSI communications model, the primary function of the network layer is to move data into and through other networks. Network layer protocols accomplish this goal by packaging data with correct network address information, selecting the appropriate network routes and forwarding the packaged data up the stack to the transport layer Layer 4.

Data Link Layer

Data Link Layer is second layer of OSI Layered Jodel. This layer is one of the most complicated layers and has complex functionalities and liabilities. Data link layer hides the details of underlying hardware and represents itself to upper layer as the medium to communicate.

Data link layer works between two hosts which are directly connected in some sense. This direct connection could be point to point or broadcast. Systems on broadcast network are said to be on same link. The work of data link layer tends to get more complex when it is dealing with multiple hosts on single collision domain.

Data link layer is responsible for converting data stream to signals bit by bit and to send that over the underlying hardware.

At the receiving end, Data Link layer picks up data from hardware which are in the form of electrical signals, assembles them in a recognizable frame format, and hands over to upper layer.

Q. Error Detection and Correction Techniques

Ans: Error is a condition when the output information does not match with the input information. During transmission, digital signals suffer from noise that can introduce errors in the binary bits travelling from one system to other. That means a 0 bit may change to 1 or a 1 bit may change to 0.

Whenever a message is transmitted, it may get scrambled by noise or data may get corrupted. To avoid this, we use error-detecting codes which are additional data added to a given digital message to help us detect if an error occurred during transmission of the message. A simple example of error-detecting code is parity check.

Along with error-detecting code, we can also pass some data to figure out the original message from the corrupt message that we received. This type of code is called an error-correcting code. Error-correcting codes also deploy the same strategy as error-detecting codes but additionally, such codes also detect the exact location of the corrupt bit.

In error-correcting codes, parity check has a simple way to detect errors along with a sophisticated mechanism to determine the corrupt bit location. Once the corrupt bit is located, its value is reverted (from 0 to 1 or 1 to 0) to get the original message.

It is the simplest technique for detecting and correcting errors. The JSB of an 8-bits word is used as the parity bit and the remaining 7 bits are used as data or message bits. The parity of 8-bits transmitted word can be either even parity or odd parity.

Parity checking at the receiver can detect the presence of an error if the parity of the receiver signal is different from the expected parity. That means, if it is known that the parity of the transmitted signal is always going to be even and if the received signal has an odd parity, then the receiver can conclude that the received signal is not correct. If an error is detected, then the receiver will ignore the received byte and request for retransmission of the same byte to the transmitter.

2 types are:

Even parity - Even parity means the number of 1s in the given word including the parity bit should be even 2,4,6,.. .... .

Odd parity - Odd parity means the number of 1s in the given word including the parity bit should be odd 1,3,5,. . . .

Date : / /

Page No. :

Q7. What is Random Access protocol

Random Access Protocols is a Jultiple access protocol that is divided into four categories which are ALOHA, CSMA, CSMA/CD, and CSMA/CA. In this article, we will cover all of these Random Access Protocols in detail.

The random access protocols consist of the following characteristics:

1. There is no time restriction for sending the data - you can talk to your friend without a time restriction.

2. There is a fixed sequence of stations which are transmitting the data.

As in the above diagram you might have observed that the random-access protocol is further divided into four categories, which are:

ALOHA Random Access Protocol

Teacher's Signature

The ALOHA protocol or also known as the ALOHA method is a simple communication scheme in which every transmitting station or source in a network will send the data whenever a frame is available for transmission. If we succeed and the frame reaches its destination, then the next frame is lined-up for transmission. But remember, if the data frame is not received by the receiver maybe due to collision then the frame is sent again until it successfully reaches the receiver's end.

Whenever we talk about a wireless broadcast system or a half-duplex two-way link, the ALOHA method works efficiently. But as the network becomes more and more complex e.g. the ethernet. Now here in the ethernet, the system involves multiple sources and destinations which share a common data path or channel, then the conflict occurs because data-frames collide, and the information is lost. Following is the flow chart of Pure ALOHA.

CSMA Random Access Protocol

CSMA stands for Carrier Sense Jultiple Access. Till now we have understood that when 2 or more stations start sending data, then a collision occurs, so this CSMA method was developed to decrease the chances of collisions when 2 or more stations start sending their signals over the data link layer. But how do they do it? It makes each station to first check the medium (whether it is busy or not) before sending any data packet.

CSMA/CD means CSMA with Collision Detection.

In this, whenever station transmits data-frame it then monitors the channel or the medium to acknowledge the state of the transmission i.e. successfully transmitted or failed. If the transmission succeeds, then it prepares for the next frame otherwise it resends the previously failed data-frame. The point to remember here is, that the frame transmission time should be at least twice the maximum propagation time, which can be deduced when the distance between the two stations involved in a collision is maximum.

CSMA/CA Random Access Protocol

It means CSMA with collision avoidance.

To detect the possible collisions, the sender receives the acknowledgement and if there is only one acknowledgment present its own then this means that the data-frame has been sent successfully. But, if there are 2 or more acknowledgment signals then this indicates that the collision has occurred.

Q 8 - Explain Ethernet, Switch and VLAN

1. Ethernet is a way of connecting computers together in a local area network or LAN. It has been the most widely used method of linking computers together in LANs since the 1990s. The basic idea of its design is that multiple computers have access to it and can send data at any time.

2. A switch is a device in a computer network that connects other devices together. Jultiple data cables are plugged into a switch to enable communication between different networked devices. ... Switches may also operate at higher layers of the OSI model, including the network layer and above.

3. VLAN is a custom network which is created from one or more local area networks. It enables a group of devices available in multiple networks to be combined into one logical network. The result becomes a virtual LAN that is administered like a physical LAN. The full form of VLAN is defined as Virtual Local Area Network