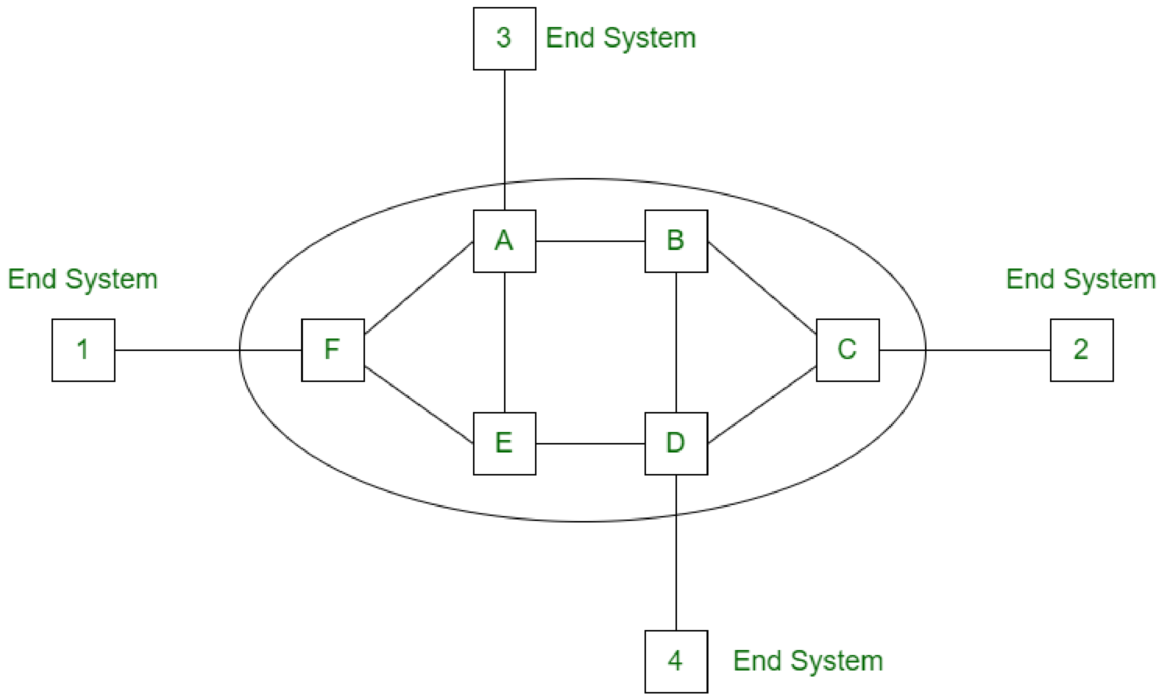
Part-A

1.How Virtual circuits woks in Network Layer.

Virtual Circuit is the computer network providing connection-oriented service. It is a connection-oriented network. In virtual circuit resource are reserve for the time interval of data transmission between two nodes. This network is a highly reliable medium of transfer. Virtual circuits are costly to implement.



Working of Virtual Circuit:

- In the first step a medium is set up between the two end nodes.
- Resources are reserved for the transmission of packets.
- Then a signal is sent to sender to tell the medium is set up and transmission can be started.
- It ensures the transmission of all packets.
- A global header is used in the first packet of the connection.
- Whenever data is to be transmitted a new connection is set up.

2.Explain how checksum works.

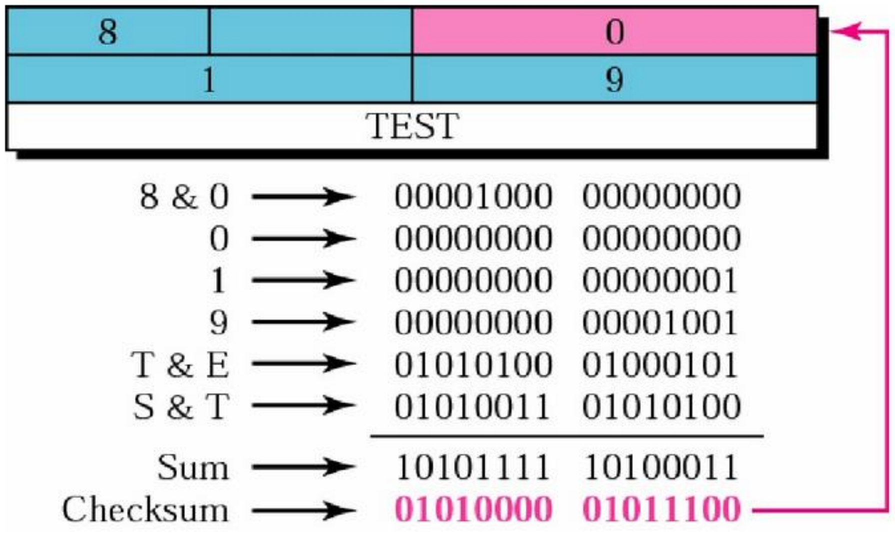
A checksum is the outcome of running an algorithm, called a cryptographic hash function, on a piece of data, usually a single file. Comparing the checksum that can generate from the version of the file, with the one provided by the source of the file, helps ensure that the copy of the file is genuine and error free.

A checksum is also sometimes called a *hash sum* and less often a *hash value*, *hash code*, or simply a *hash*.

The idea of a checksum or a cryptographic hash function might seem complicated and not possibly worth the effort, but we'd like to convince you otherwise! Checksums really aren't that hard to understand or create.

Checksums are used to ensure the integrity of a file after it has been transmitted from one storage device to another. This can be across the Internet or simply between two computers on the same network.

Figure 9.19 Example of checksum calculation



```
    8 & 0  ──→  00001000  00000000
        0  ──→  00000000  00000000
        1  ──→  00000000  00000001
        9  ──→  00000000  00001001
    T & E  ──→  01010100  01000101
    S & T  ──→  01010011  01010100
                ──────────────────
      Sum  ──→  10101111  10100011
 Checksum  ──→  01010000  01011100
```

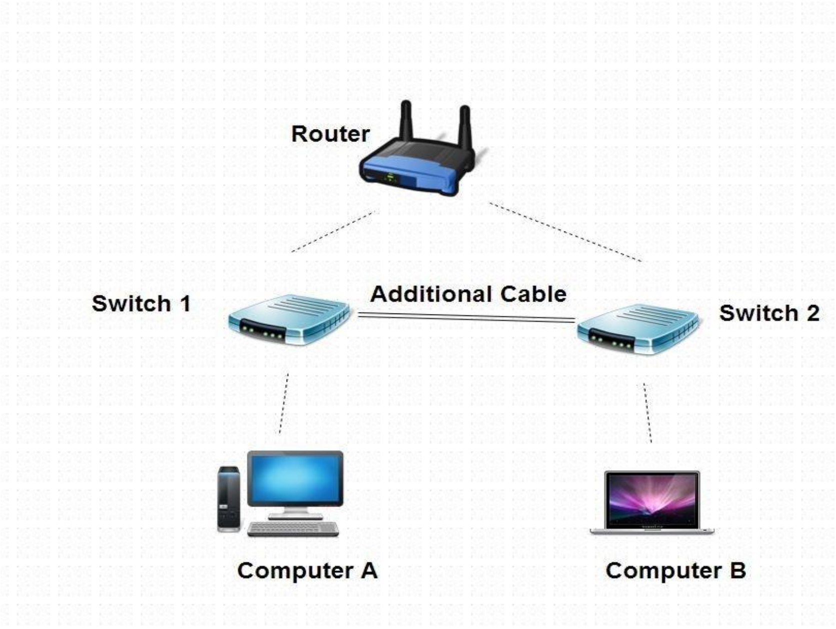
Checksum calculators are the tools used to compute checksums. There are plenty of checksum calculators out there, each supporting a different set of cryptographic hash functions.

3.Explain how Switching implemented in networking with neat sketch.

- When a user accesses the internet or another computer network outside their immediate location, messages are sent through the network of transmission media. This technique of transferring the information from one computer network to another network is known as **switching**.
- Switching in a computer network is achieved by using switches. A switch is a small hardware device which is used to join multiple computers together with one local area network (LAN).
- Network switches operate at layer 2 (Data link layer) in the OSI model.
- Switching is transparent to the user and does not require any configuration in the home network.
- Switches are used to forward the packets based on MAC addresses.
- A Switch is used to transfer the data only to the device that has been addressed. It verifies the destination address to route the packet appropriately.
- It is operated in full duplex mode.
- Packet collision is minimum as it directly communicates between source and destination.
- It does not broadcast the message as it works with limited bandwidth.

Switching concept is developed because of the following reasons:

- **Bandwidth:** It is defined as the maximum transfer rate of a cable. It is a very critical and expensive resource. Therefore, switching techniques are used for the effective utilization of the bandwidth of a network.
- **Collision:** Collision is the effect that occurs when more than one device transmits the message over the same physical media, and they collide with each other. To overcome this problem, switching technology is implemented so that packets do not collide with each other.



Advantages of Switching:

- Switch increases the bandwidth of the network.
- It reduces the workload on individual PCs as it sends the information to only that device which has been addressed.
- It increases the overall performance of the network by reducing the traffic on the network.
- There will be less frame collision as switch creates the collision domain for each connection.

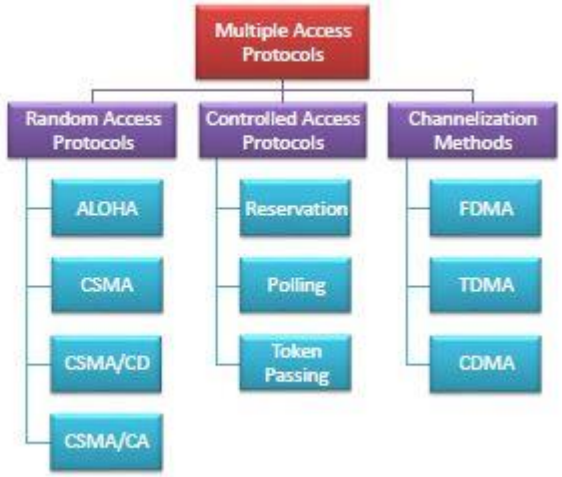
4.Various types of Multiple access protocols.

Multiple access protocols are a set of protocols operating in the Medium Access Control sublayer (MAC sublayer) of the Open Systems Interconnection (OSI) model. These protocols allow a number of nodes or users to access a shared network channel. Several data streams originating from several nodes are transferred through the multi-point transmission channel.

The objectives of multiple access protocols are optimization of transmission time, minimization of collisions and avoidance of crosstalks.

Categories of Multiple Access Protocols

Multiple access protocols can be broadly classified into three categories - random access protocols, controlled access protocols and channelization protocols.



Random Access Protocols

Random access protocols assign uniform priority to all connected nodes. Any node can send data if the transmission channel is idle. No fixed time or fixed sequence is given for data transmission.

The four random access protocols are−

- ALOHA
- Carrier sense multiple access (CMSA)
- Carrier sense multiple access with collision detection (CMSA/CD)
- Carrier sense multiple access with collision avoidance (CMSA/CA)

Controlled Access Protocols

Controlled access protocols allow only one node to send data at a given time.Before initiating transmission, a node seeks information from other nodes to determine which station has the right to send. This avoids collision of messages on the shared channel.

The station can be assigned the right to send by the following three methods−

- Reservation
- Polling
- Token Passing

Channelization

Channelization are a set of methods by which the available bandwidth is divided among the different nodes for simultaneous data transfer.

The three channelization methods are−

- Frequency division multiple access (FDMA)
- Time division multiple access (TDMA)

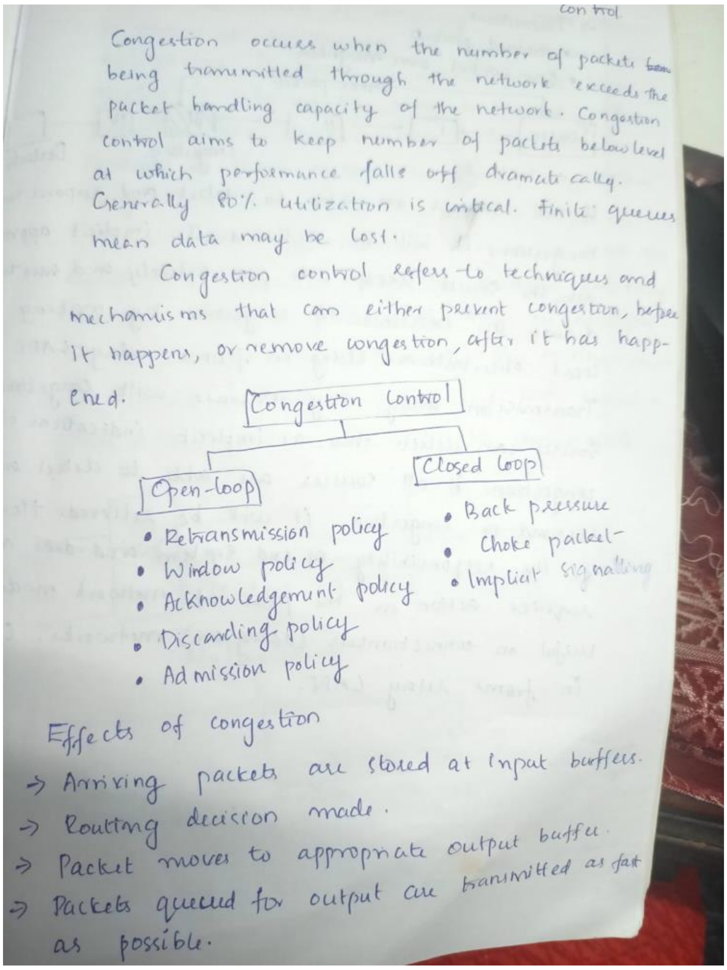
- Code division multiple access (CDMA)

5.Explain Principles of congestion control.

A state occurring in network layer when the message traffic is so heavy that it slows down network response time.

Effects of Congestion

- As delay increases, performance decreases.
- If delay increases, retransmission occurs, making situation worse.



control

Congestion occures when the number of packets ~~been~~ being transmitted through the network exceeds the packet handling capacity of the network. Congestion control aims to keep number of packets below level at which performance falls off dramatically. Generally 80% utilization is critical. Finite queues mean data may be lost.

Congestion control refers to techniques and mechanisms that can either prevent congestion, before it happens, or remove congestion, after it has happened.

Congestion control

Open-loop

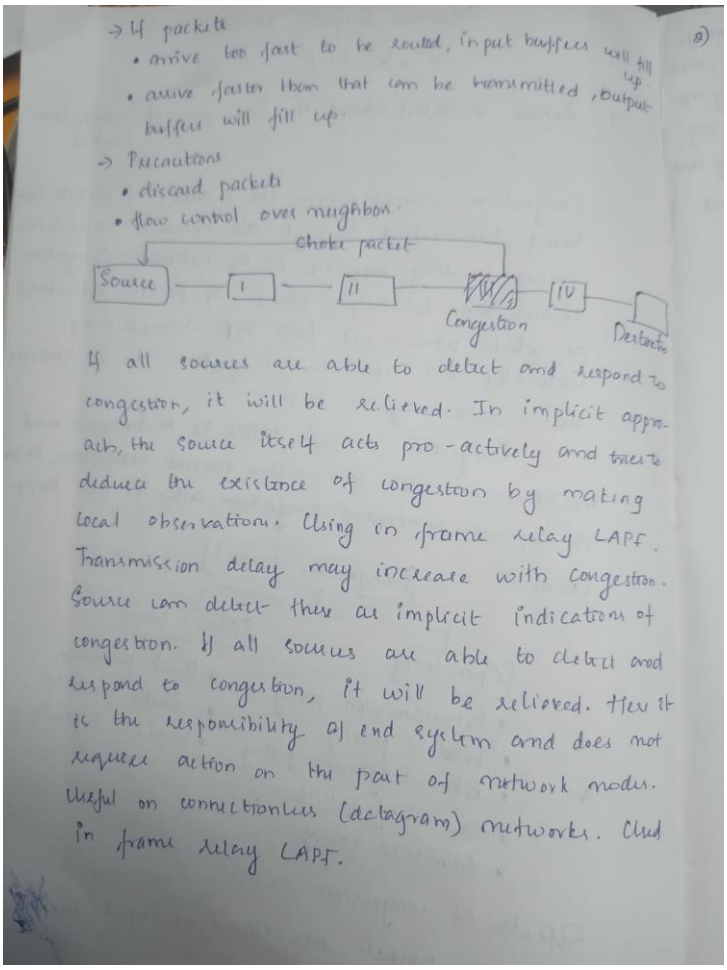
- Retransmission policy
- Window policy
- Acknowledgement policy
- Discarding policy
- Admission policy

Closed loop

- Back pressure
- Choke packet
- Implicit signalling

Effects of congestion

→ Arriving packets are stored at input buffers.
→ Routing decision made.
→ Packet moves to appropriate output buffer.
→ Packets queued for output are transmitted as fast as possible.



2)

→ If packets
- arrive too fast to be routed, input buffers will fill up.
- arrive faster than that can be transmitted, output buffers will fill up.

→ Precautions
- discard packets
- flow control over neighbor.

Choke packet
Source
I
II
III
IV
Congestion
Destinatn

If all sources are able to detect and respond to congestion, it will be relieved. In implicit approach, the source itself acts pro-actively and tries to deduce the existence of congestion by making local observations. Using in frame relay LAPF. Transmission delay may increase with congestion. Source can detect these as implicit indications of congestion. If all sources are able to detect and respond to congestion, it will be relieved. Here it is the responsibility of end system and does not require action on the part of network nodes. Useful on connectionless (datagram) networks. Used in frame relay LAPF.

6.Explain software defined networks implemented in Network Layer.

Software-defined networking (SDN) is a new emerging technology for networking in which control is Decoupled a hardware and given to software part called a controller. When a packet arrives at a switch in a foreseeable network rule built into the switch patented firmware tell the switch where to forward the packet. The switch sends every packet going to the same destination along the same path and treats all the packets the exact same way. In the campus network, smart switches designed with application-specific integrated circuits (ASICs) are Refined enough to recognize different types of packets and treat them differently, but such switches can be quite expensive.

Software-defined networking architecture layers consist of 3 layers.

a) an infrastructure layer
b) a control layer and
c) an application layer.

The Application Layer

The application layer contains programs that explicitly and programmatically communicate their desired network behavior and network requirements to the SDN Controller.

The Control Layer

The SDN Controller is the mid-layer that connects the application layer and infrastructure layer- Northbound interface is the connection between the controller and applications while the southbound interface is the connection between the controller and the infrastructure layer.

The Infrastructure Layer

This consists of networking devices that control the forwarding and data processing capabilities for the network.

The devices are responsible for handling packets based on the rules provided by a controller.

It is the physical layer responsible for collecting the network statuses such as traffic statistics, network topology, network usage, etc. and send them to the control layer.

Part-B

7.Explain how distance vector routing with a neat diagram.

- **The Distance vector algorithm is iterative, asynchronous and distributed.**
    - **Distributed:** It is distributed in that each node receives information from one or more of its directly attached neighbors, performs calculation and then distributes the result back to its neighbors.
    - **Iterative:** It is iterative in that its process continues until no more information is available to be exchanged between neighbors.
    - **Asynchronous:** It does not require that all of its nodes operate in the lock step with each other.
- The Distance vector algorithm is a dynamic algorithm.
- It is mainly used in ARPANET, and RIP.
- Each router maintains a distance table known as **Vector**.

Three Keys to understand the working of Distance Vector Routing Algorithm:

- **Knowledge about the whole network:** Each router shares its knowledge through the entire network. The Router sends its collected knowledge about the network to its neighbors.
- **Routing only to neighbors:** The router sends its knowledge about the network to only those routers which have direct links. The router sends whatever it has about the network through the ports. The information is received by the router and uses the information to update its own routing table.
- **Information sharing at regular intervals:** Within 30 seconds, the router sends the information to the neighboring routers.

Distance Vector Routing Algorithm

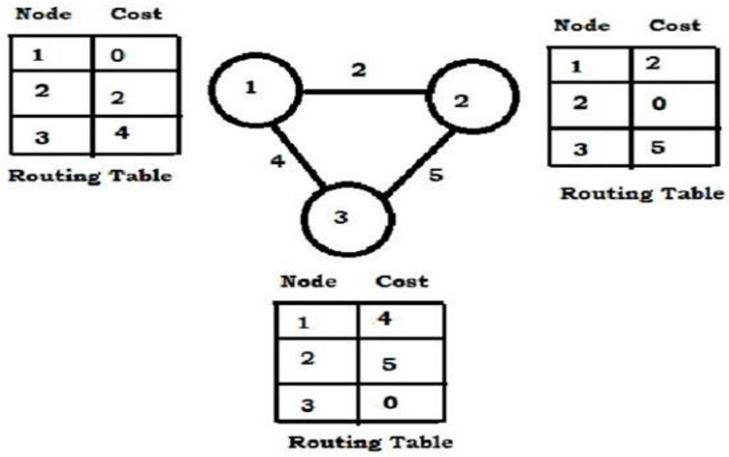
Let $d_x(y)$ be the cost of the least-cost path from node x to node y. The least costs are related by Bellman-Ford equation,

$$d_x(y) = \min_v\{c(x,v) + d_v(y)\}$$

Where the minv is the equation taken for all x neighbors. After traveling from x to v, if we consider the least-cost path from v to y, the path cost will be $c(x,v)+d_v(y)$. The least cost from x to y is the minimum of $c(x,v)+d_v(y)$ taken over all neighbors.

Distance vector routing is an asynchronous algorithm in which node x sends the copy of its distance vector to all its neighbors. When node x receives the new distance vector from one of its neighboring vector, v, it saves the distance vector of v and uses the Bellman-Ford equation to update its own distance vector.

$$d_x(y) = \min_v\{ c(x,v) + d_v(y)\} \quad \text{for each node y in N}$$



Node	Cost
1	0
2	2
3	4

Routing Table

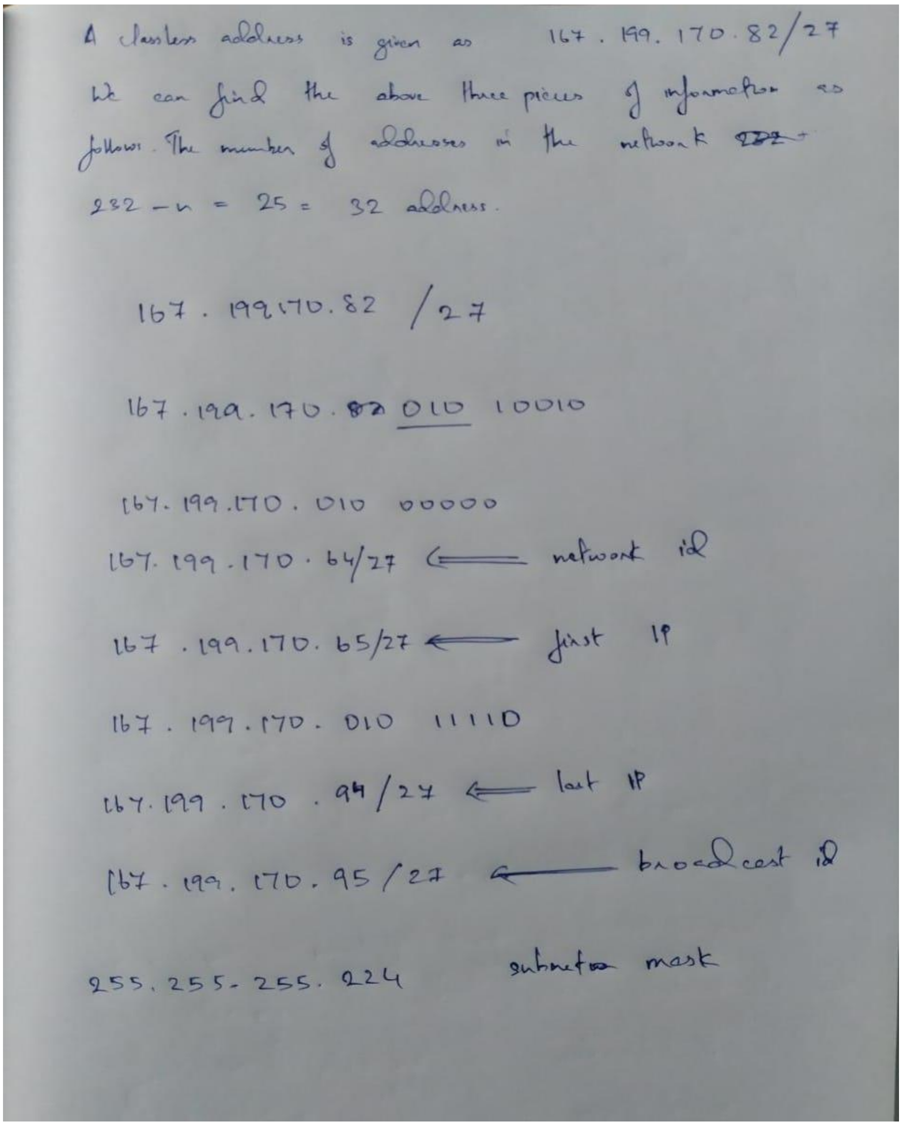
Node	Cost
1	2
2	0
3	5

Routing Table

Node	Cost
1	4
2	5
3	0

Routing Table

8.A classless address is given as 167.199.170.82/27. We can find the above three pieces of information as follows. The number of addresses in the network is 232 − n = 25 = 32 addresses.



A classless address is given as 167 . 199. 170 . 82/27
We can find the above three pieces of information as follows. The number of addresses in the network ~~232~~
232 − n = 25 = 32 address.

167 . 199170. 82 /27

167 . 199 . 170 . ~~82~~ 010 10010

167. 199 .170 . 010 00000

167. 199 . 170 . 64/27 ⟸ network id

167 . 199. 170. 65/27 ⟵ first IP

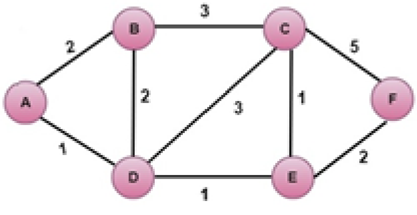
167 . 199 . 170 . 010 11110

167. 199 . 170 . 94/27 ⟸ last IP

167 . 199. 170. 95/27 ⟵ broadcast id

255. 255. 255. 224 subnet mask

9.Explain in detail about Link-state with given example.



10.Explain in detail how OSPF and BGP is implemented with neat diagrams.

OSPF

The OSPF stands for **Open Shortest Path First**. It is a widely used and supported routing protocol. It is an intradomain protocol, which means that it is used within an area or a network. It is an interior gateway protocol that has been designed within a single autonomous system. It is based on a link-state routing algorithm in which each router contains the information of every domain, and based on this information, it determines the shortest path. The goal of routing is to learn routes. The OSPF achieves by learning about every router and subnet within the entire network. Every router contains the same information about the network. The way the router learns this information by sending LSA (Link State Advertisements). These LSAs contain information about every router, subnet, and other networking information. Once the LSAs have been flooded, the OSPF stores the information in a link-state database known as LSDB. The main goal is to have the same information about every router in an LSDBs.

There are three steps that can explain the working of OSPF:

Step 1: The first step is to become OSPF neighbors. The two connecting routers running OSPF on the same link creates a neighbor relationship.

Step 2: The second step is to exchange database information. After becoming the neighbors, the two routers exchange the LSDB information with each other.

Step 3: The third step is to choose the best route. Once the LSDB information has been exchanged with each other, the router chooses the best route to be added to a routing table based on the calculation of SPF.

The following are the fields in an OSPF message format:

BGP

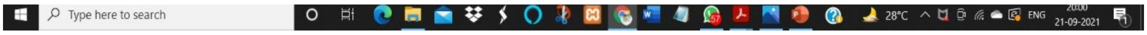
BGP stands for Border Gateway Protocol.

It is an interdomain routing protocol, and it uses the path-vector routing. It is a gateway protocol that is used to exchange routing information among the autonomous system on the internet.

The main difference between OSPF (Open Shortest Path First) and BGP (Border Gateway Protocol) is that, Open Shortest Path First is an **intra-domain** routing protocol while, Border Gateway Protocol is the **inter-domain** routing protocol.

An autonomous system is a collection of networks that comes under the single common administrative domain. Or we can say that it is a collection of routers under the single administrative domain. For example, an organization can contain multiple routers having different locations, but the single autonomous number system will recognize them. Within the same autonomous system or same organization, we generally use IGP (Interior Gateway Protocol) protocols like RIP, IGRP, EIGRP, OSPF. Suppose we want to communicate between two autonomous systems. In that case, we use EGP (Exterior Gateway Protocols). The protocol that is running on the internet or used to communicate between two different autonomous number systems is known as BGP (Border Gateway Protocol). The BGP is the only protocol that is running on the internet backbone or used to exchange the routes between two different autonomous number systems. Internet service providers use the BGP protocol to control all the routing information.

11.Explain how collision based multiple access protocols applied in network with real time example.



12.Explain how CRC is applied to detect errors?

CRC or Cyclic Redundancy Check is a method of detecting accidental changes/errors in the communication channel.
CRC uses **Generator Polynomial** which is available on both sender and receiver side. An example generator polynomial is of the form like $x^3 + x + 1$. This generator polynomial represents key 1011. Another example is $x^2 + 1$ that represents key 101.

n : Number of bits in data to be sent from sender side. k : Number of bits in the key obtained from generator polynomial.

Sender Side (Generation of Encoded Data from Data and Generator Polynomial (or Key)):

1. The binary data is first augmented by adding k-1 zeros in the end of the data
2. Use ***modulo-2 binary division*** to divide binary data by the key and store remainder of division.
3. Append the remainder at the end of the data to form the encoded data and send the same.

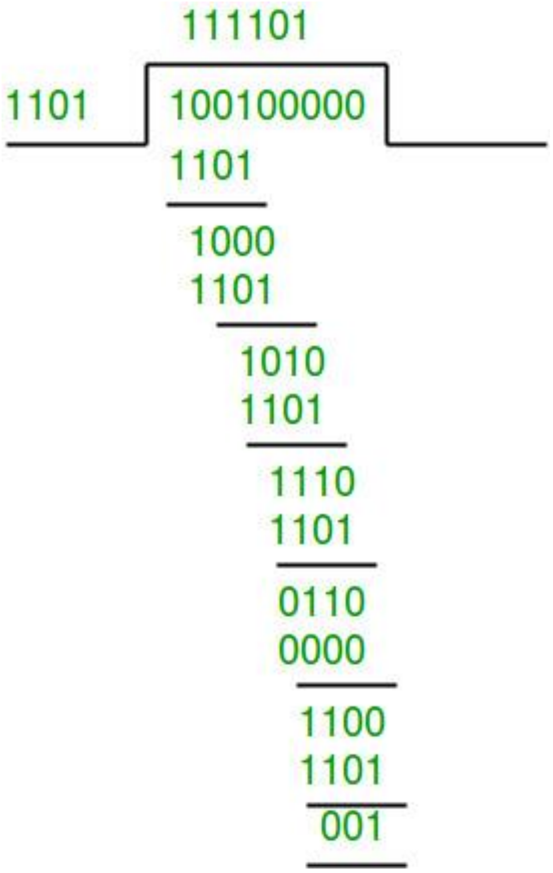
Receiver Side (Check if there are errors introduced in transmission)
Perform modulo-2 division again and if the remainder is 0, then there are no errors.

Modulo 2 Division:
The process of modulo-2 binary division is the same as the familiar division process we use for decimal numbers. Just that instead of subtraction, we use XOR here.

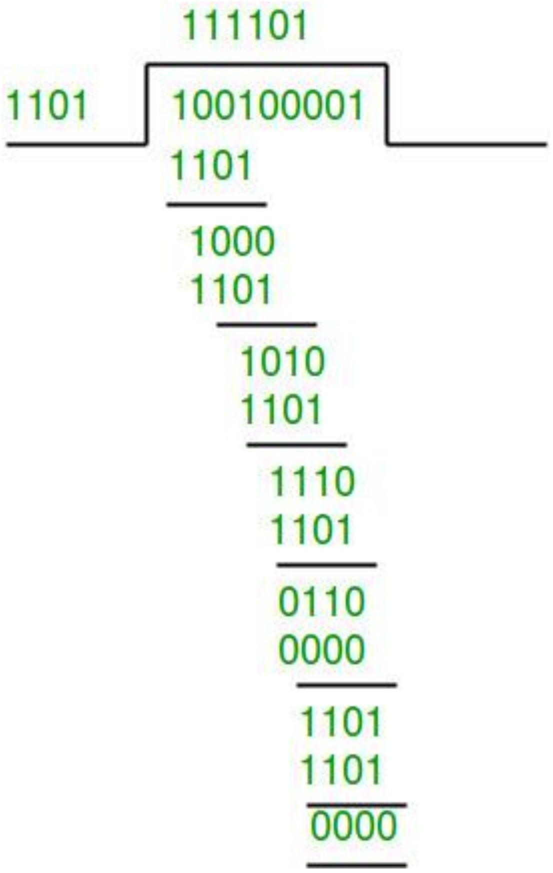
- In each step, a copy of the divisor (or data) is XORed with the k bits of the dividend (or key).
- The result of the XOR operation (remainder) is (n-1) bits, which is used for the next step after 1 extra bit is pulled down to make it n bits long.
- When there are no bits left to pull down, we have a result. The (n-1)-bit remainder which is appended at the sender side.

Example:

Data word to be sent - 100100Key - 1101 [Or generator polynomial x^3 + x^2 + 1]Sender Side:



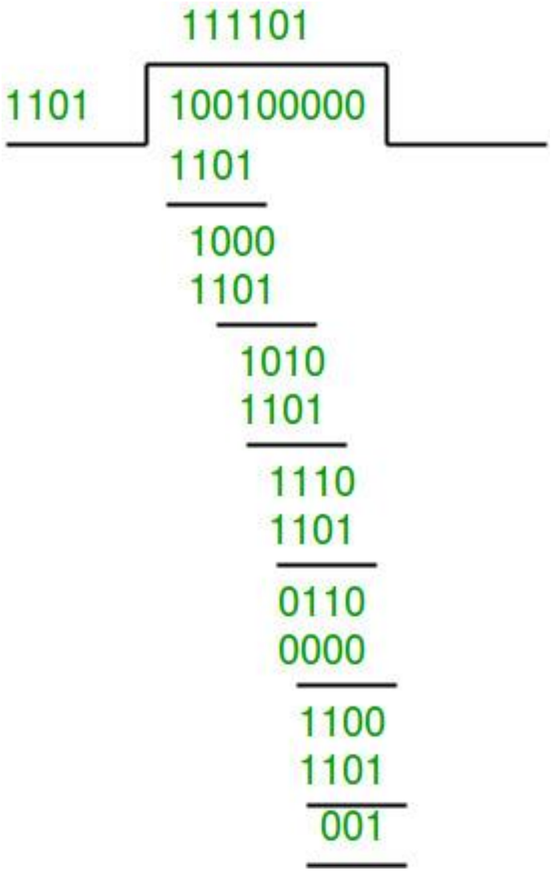
Therefore, the remainder is 001 and hence the encoded data sent is 100100001.Receiver Side:Code word received at the receiver side 100100001



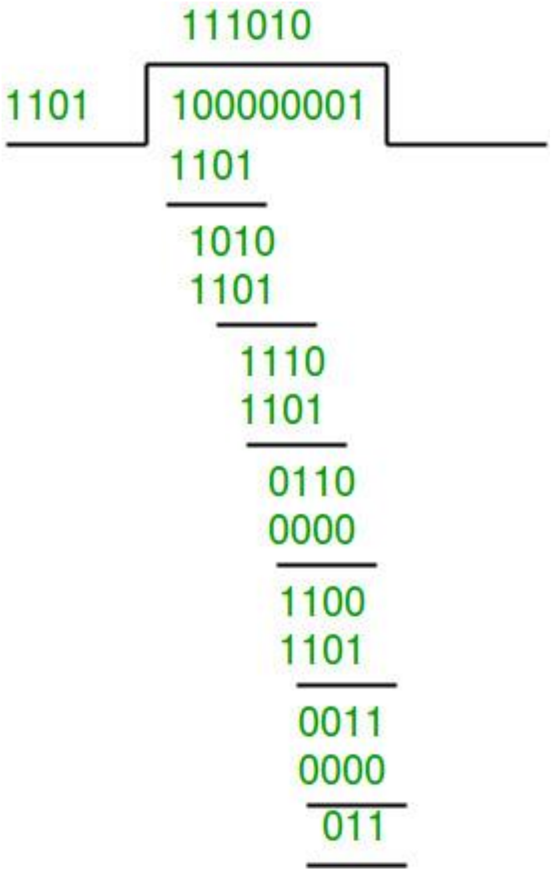
Therefore, the remainder is all zeros. Hence, thedata received has no error.

Example 2: (Error in transmission)

Data word to be sent - 100100Key - 1101Sender Side:



Therefore, the remainder is 001 and hence the code word sent is 100100001.Receiver SideLet there be an error in transmission mediaCode word received at the receiver side - 100000001



Since the remainder is not all zeroes, the error is detected at the receiver side.

13.Explain the Procedure for pure ALOHA protocol?

ALOHA

ALOHA, the earliest random access method, was developed at the University of Hawaii

in early 1970. It was designed for a radio (wireless) LAN, but it can be used on any

shared medium.

It is obvious that there are potential collisions in this arrangement. The medium is

shared between the stations. When a station sends data, another station may attempt to

do so at the same time. The data from the two stations collide and become garbled.

Pure ALOHA

The original ALOHA protocol is called pure ALOHA. This is a simple but elegant

protocol. The idea is that each station sends a frame whenever it has a frame to send

(multiple access). However, since there is only one channel to share, there is the possibility of collision between frames from different stations. Figure 5.29 shows an example

of frame collisions in pure ALOHA are a total of eight frames on the shared medium. Some of these frames collide because multiple frames are in contention for the shared channel. Figure 5.29 shows that only two frames survive: one frame from station 1 and one frame from station 3. We need to mention that even if one bit of a frame coexists on the channel with one bit from another frame, there is a collision and both will be destroyed. It is obvious that we need to resend the frames that have been destroyed during transmission.

The pure ALOHA protocol relies on acknowledgments from the receiver. When a station sends a frame, it expects the receiver to send an acknowledgment. If the acknowledgment does not arrive after a time-out period, the station assumes that the frame (or the acknowledgment) has been destroyed and resends the frame.

A collision involves two or more stations. If all these stations try to resend their frames after the time-out, the frames will collide again. Pure ALOHA dictates that when the time-out period passes, each station waits a random amount of time before resending its frame. The randomness will help avoid more collisions. We call this time the back-off time TB.

Pure ALOHA has a second method to prevent congesting the channel with retransmitted frames. After a maximum number of retransmission attempts Kmax, a station

must give up and try later

14.Explain in detail about Standard Ethernet.

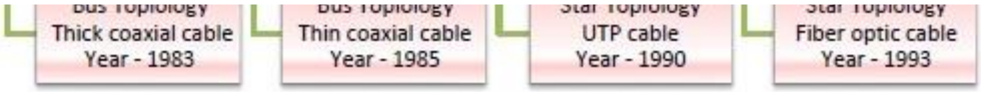
Ethernet is a set of technologies and protocols that are used primarily in LANs. It was first standardized in 1980s by IEEE 802.3 standard. IEEE 802.3 defines the physical layer and the medium access control (MAC) sub-layer of the data link layer for wired Ethernet networks. Ethernet is classified into two categories: classic Ethernet and switched Ethernet.

Classic Ethernet is the original form of Ethernet that provides data rates between 3 to 10 Mbps. The varieties are commonly referred as 10BASE-X. Here, 10 is the maximum throughput, i.e. 10 Mbps, BASE denoted use of baseband transmission, and X is the type of medium used. Most varieties of classic Ethernet have become obsolete in present communication scenario.

A switched Ethernet uses switches to connect to the stations in the LAN. It replaces the repeaters used in classic Ethernet and allows full bandwidth utilization.

IEEE 802.3 Popular Versions

There are a number of versions of IEEE 802.3 protocol. The most popular ones are -

- **IEEE 802.3**: This was the original standard given for 10BASE-5. It used a thick single coaxial cable into which a connection can be tapped by drilling into the cable to the core. Here, 10 is the maximum throughput, i.e. 10 Mbps, BASE denoted use of baseband transmission, and 5 refers to the maximum segment length of 500m.
- **IEEE 802.3a**: This gave the standard for thin coax (10BASE-2), which is a thinner variety where the segments of coaxial cables are connected by BNC connectors. The 2 refers to the maximum segment length of about 200m (185m to be precise).
- **IEEE 802.3i**: This gave the standard for twisted pair (10BASE-T) that uses unshielded twisted pair (UTP) copper wires as physical layer medium. The further variations were given by IEEE 802.3u for 100BASE-TX, 100BASE-T4 and 100BASE-FX.
- 

that ion.

Frame Format of Classic Ethernet and IEEE 802.3

The main fields of a frame of classic Ethernet are -

- **Preamble**: It is the starting field that provides alert and timing pulse for transmission. In case of classic Ethernet it is an 8 byte field and in case of IEEE 802.3 it is of 7 bytes.
- **Start of Frame Delimiter**: It is a 1 byte field in a IEEE 802.3 frame that contains an alternating pattern of ones and zeros ending with two ones.
- **Destination Address**: It is a 6 byte field containing physical address of destination stations.
- **Source Address**: It is a 6 byte field containing the physical address of the sending station.
- **Length**: It a 7 bytes field that stores the number of bytes in the data field.
- **Data**: This is a variable sized field carries the data from the upper layers. The maximum size of data field is 1500 bytes.
- **Padding**: This is added to the data to bring its length to the minimum requirement of 46 bytes.
- **CRC**: CRC stands for cyclic redundancy check. It contains the error detection information.

15.Explain about Multicast routing.

□ multicast service, in which a multicast packet is delivered to only a subset of network nodes.

□ A number of emerging network applications require the delivery of packets from one or more senders to a group of receivers

⍰ bulk data transfer (for example, the transfer of a software upgrade from the software developer to users needing the upgrade),

⍰ streaming continuous media (for example, the transfer of the audio, video, and text of a live lecture to a set of distributed lecture participants)

, ⍰ shared data applications (for example, a whiteboard or teleconferencing application that is shared among many distributed participants),

⍰ data feeds (for example, stock quotes),

⍰ Web cache updating, and interactive gaming ⍰ In multicast communication, we are faced with two problems—

⍰ how to identify the receivers of a multicast packet and how to address a packet sent to these receivers.

⍰ In the case of unicast communication, the IP address of the

⍰ receiver (destination) is carried in each IP unicast datagram and identifies the single recipient; ⍰ in the case of broadcast, all nodes need to receive the broadcast packet, so no destination addresses are needed.

⍰ Multicast packet is addressed using address indirection.

⍰ That is, a single identifier is used for the group of receivers, and a copy of the packet that is addressed to the group using this single identifier is delivered to all of the multicast receivers associated with that group. ⍰ In the Internet, the single identifier that represents a group of receivers is a class D multicast IP address.

⍰ The group of receivers associated with a class D address is referred to as a multicast group