Q1.a) Describe the different guided transmission medias used in the network.

Ans. (2 marks for theory+3marks for diagram).

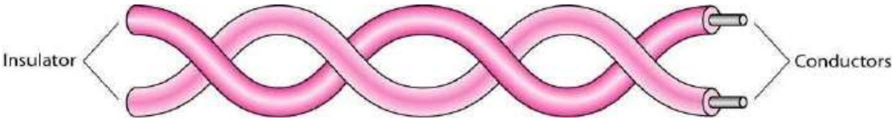
Guided transmission media consists of physical connection between source and destination through a wire or a cable.

There are three basic types of guided media which are as follows −

- Twisted pair cable
- Co-axial cable
- Fiber-optic cable

1) Twisted-pair cable

- A twisted pair consists of two conductors
- Basically, copper based
- With its own plastic insulation, twisted together



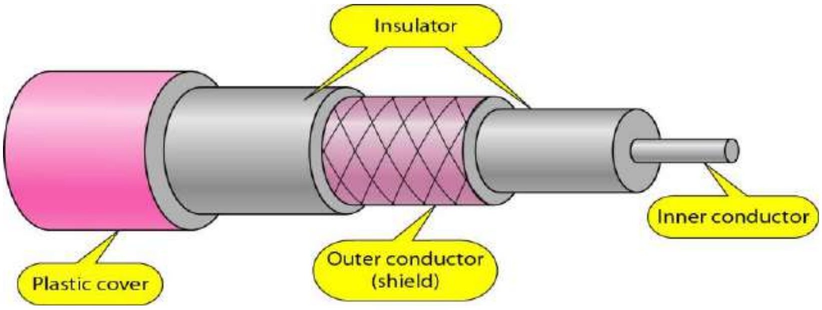
- Provide protection against cross talk or interference(noise)
- One wire use to carry signals to the receiver, second wire used as a ground reference for twisting, after receiving the signal remains same.
- Therefore, number of twists per unit length, determines the quality of cable.

Types of Twisted Pair

- ➢ STP (shielded twisted pair): The pair is wrapped with metallic foil or braid to insulate the pair from electromagnetic interference.
- ➢ UTP (unshielded twisted pair): Each wire is insulated with plastic wrap, but the pair is encased in an outer covering

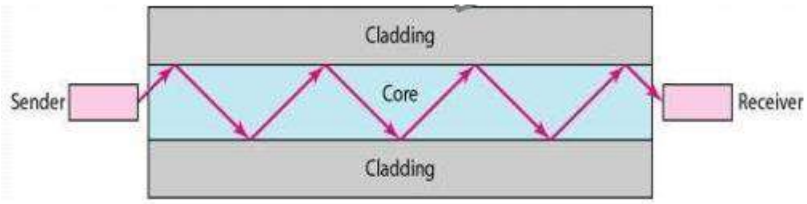
2) Coaxial Cable (or Coax)

- Used for cable television, LANs, telephony
- Has an inner conductor surrounded by a braided mesh
- Both conductors share a common centre axial, hence the term “co-axial”



3) Optical Fiber

- An optical fiber is a transparent thin fibre, usually made of glass or plastic, for transmitting light.
- This optical fiber can be used as a medium for telecommunication and networking because it is flexible and can be bundled as cables.
  The light transmitted through the fiber is confined due to total internal reflection within the material.
- Cladding is of less dense glass or plastic surrounded
- An optical fiber cable has a cylindrical shape and consists of three concentric sections: the core, the cladding, and the jacket (outer part of the cable).



Q1.b) Explain Repeater, Hub, Bridge, Switch & Routers.
Ans. (Each topic carries 1 mark)

Repeater – A repeater operates at the physical layer. Its job is to regenerate the signal over the same network before the signal becomes too weak or corrupted to extend the length to which the signal can be transmitted over the same network. An important point to be noted about repeaters is that they not only amplify the signal but also regenerate it. When the signal becomes weak, they copy it bit by bit and regenerate it at its star topology connectors connecting following the original strength. It is a 2-port device.

Hub – A hub is a basically multi-port 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, the collision domain of all hosts connected through Hub remains one. Also, they do not have the intelligence to find out the best path for data packets which leads to inefficiencies and wastage.

Bridge – A bridge operates at the data link layer. A bridge is a repeater, with add on the functionality of filtering content by reading the MAC addresses of the 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.

Switch – A switch is a multiport bridge with a buffer and a design that can boost its efficiency (a large number of ports imply less traffic) and performance. A switch is a data link layer device. The switch can perform error checking before forwarding data, which makes it very efficient as it does not forward packets that have errors and forward good packets selectively to the correct port only. In other words, the switch divides the collision domain of hosts, but the broadcast domain remains the same.

Routers – A router is a device like a switch that routes data packets based on their IP addresses. The router is mainly a Network Layer device. Routers normally connect LANs and WANs and have a dynamically updating routing table based on which they make decisions on routing the data packets. The router divides the broadcast domains of hosts connected through it.

Q1.c) Enumerate the main responsibilities of the DLL
Ans. (Min 5 responsibilities for 5 marks).

- **Framing & Link access:** Data Link Layer protocols encapsulate each network frame within a Link layer frame before the transmission across the link. A frame consists of a data field in which network layer datagram is inserted and a number of data fields. It specifies the structure of the frame as well as a channel access protocol by which frame is to be transmitted over the link.
- **Reliable delivery:** Data Link Layer provides a reliable delivery service, i.e., transmits the network layer datagram without any error. A reliable delivery service is accomplished with transmissions and acknowledgements. A data link layer mainly provides the reliable delivery service over the links as they have higher error rates and they can be corrected locally, link at which an error occurs rather than forcing to retransmit the data.
- **Flow control:** A receiving node can receive the frames at a faster rate than it can process the frame. Without flow control, the receiver's buffer can overflow, and frames can get lost. To overcome this problem, the data link layer uses the flow control to prevent the sending node on one side of the link from overwhelming the receiving node on another side of the link.
- **Error detection:** Errors can be introduced by signal attenuation and noise. Data Link Layer protocol provides a mechanism to detect one or more errors. This is achieved by adding error detection bits in the frame and then receiving node can perform an error check.
- **Access control**: When more than two or two devices are connected to the common link, data link layer protocols are necessary to determine which device has control over the link at any point of time.

Q1.d) Differentiate between TCP and UDP
Ans. (min 5 differences-5marks)

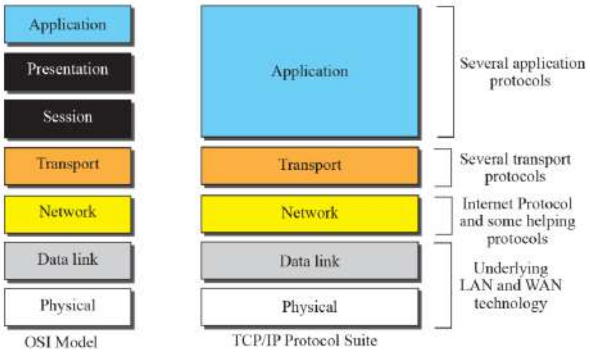
	TCP	UDP
Type of connection	It is a connection-oriented protocol, which means that the connection needs to be established before the data is transmitted over the network.	It is a connectionless protocol, which means that it sends the data without checking whether the system is ready to receive or not.

Reliable	TCP is a reliable protocol as it provides assurance for the delivery of data packets.	UDP is an unreliable protocol as it does not take the guarantee for the delivery of packets.
Speed	TCP is slower than UDP as it performs error checking, flow control, and provides assurance for the delivery of	UDP is faster than TCP as it does not guarantee the delivery of data packets.
Header size	The size of TCP is 20 bytes.	The size of the UDP is 8 bytes.
Acknowledgment	TCP uses the three-way-handshake concept. In this concept, if the sender receives the ACK, then the sender will send the data. TCP also has the ability to resend the lost data.	UDP does not wait for any acknowledgment; it just sends the data.
Flow control mechanism	It follows the flow control mechanism in which too many packets cannot be sent to the receiver at the same time.	This protocol follows no such mechanism.
Error checking	TCP performs error checking by using a checksum. When the data is corrected, then the data is retransmitted to the receiver.	It does not perform any error checking, and also does not resend the lost data packets.
Applications	This protocol is mainly used where a secure and reliable communication process is required, like military services, web browsing, and e-mail.	This protocol is used where fast communication is required and does not care about the reliability like VoIP, game streaming, video and music streaming, etc.

Q2.a) Explain TCP/IP reference model & compare it with OSI reference model.

Ans.5 marks for TCP/IP(2 marks for theory+3 marks diagram) + 5 marks for comparison(any 5 point)

The layers in the TCP/IP protocol suite do not exactly match those in the OSI model. The original TCP/IP protocol suite was defined as having four layers: host-tonetwork, internet, transport, and application. However, when TCP/IP is compared to OSI, we can say that the TCP/IP protocol suite is made of five layers: physical, data link, network, transport, and application.



TCP/IP support the Internet Protocol IP (unreliable). IP is a host-to-host protocol.
Supporting protocols:

- Address Resolution Protocol (ARP)
- Reverse Address Resolution Protocol (RARP)
- Internet Control Massage Protocol (ICMP)
- Internet Group Massage Protocol (IGMP)

OSI	TCP/IP
OSI represents Open System Interconnection.	TCP/IP model represents the Transmission Control Protocol / Internet Protocol
OSI is a generic, protocol independent standard. It is acting as an interaction gateway between the network and the final-user	TCP/IP model depends on standard protocols about which the computer network has created. It is a connection protocol that assigns the network of hosts over the internet.
The OSI model was developed first, and then protocols were created to fit the network architecture's needs	The protocols were created first and then built the TCP/IP model
It provides quality services	It does not provide quality services
The OSI model represents defines administration, interfaces and conventions. It describes clearly which layer provides services	It does not mention the services, interfaces, and protocols
The protocols of the OSI model are better unseen and can be returned with another appropriate protocol quickly	The TCP/IP model protocols are not hidden, and we cannot fit a new protocol stack in it.
It is difficult as distinguished to TCP/IP	It is simpler than OSI
It provides both connection and connectionless oriented transmission in the network layer; however, only connection-oriented transmission in the transport layer	It provides connectionless transmission in the network layer and supports connecting and connectionless-oriented transmission in the transport layer
It uses a vertical approach	It uses a horizontal approach
The smallest size of the OSI header is 5 bytes	The smallest size of the TCP/IP header is 20 bytes.

Protocols are unknown in the OSI model and are returned while the technology modifies	In TCP/IP, returning protocol is not difficult

Q2.b) With the help of suitable example explain sliding window protocol using Go-Back-N technique.

Ans. (example 5 marks (diagram+thoery)+ concept of go back n 5 marks.

In the Go-Back-N Protocol, the sequence numbers are modulo 2m, where m is the size of the sequence number field in bits.

Send window for Go-Back-N ARQ

The send window is an abstract concept defining an imaginary box of size 2m − 1 with three variables: Sf, Sn, and Ssize.The send window can slide one or more slots when a valid acknowledgment arrives.

Receive window for Go-Back-N ARQ

The receive window is an abstract concept defining an imaginary box of size 1 with one single variable Rn.The window slides when a correct frame has arrived; sliding occurs one slot at a time.

In Go-Back-N ARQ, the size of the send window must be less than 2m; the size of the receiver window is always 1.

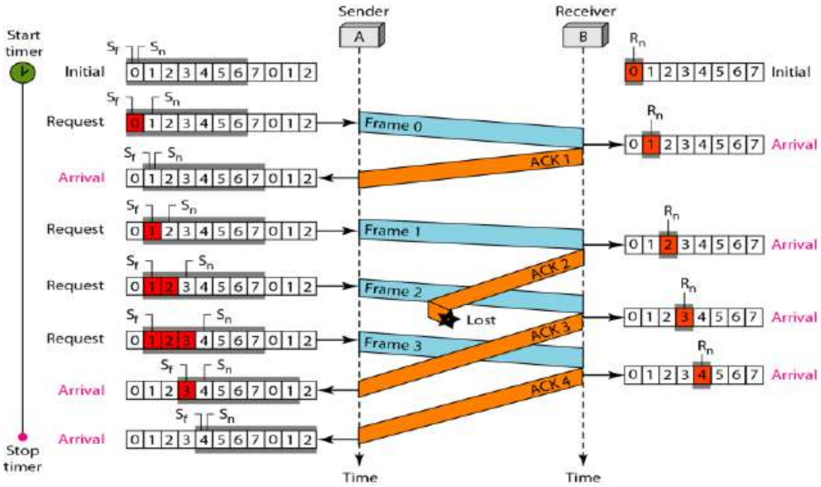


Figure shows an example of Go-Back-N. This is an example of a case where the forward channel is reliable, but the reverse is not. No data frames are lost, but some ACKs are delayed and one is lost. The example also shows how cumulative acknowledgments can help if acknowledgments are delayed or lost. After initialization, there are seven sender events. There is no time-out event here because all outstanding frames are acknowledged before the timer expires. Note that although ACK 2 is lost, ACK 3 serves as both ACK 2 and ACK 3.

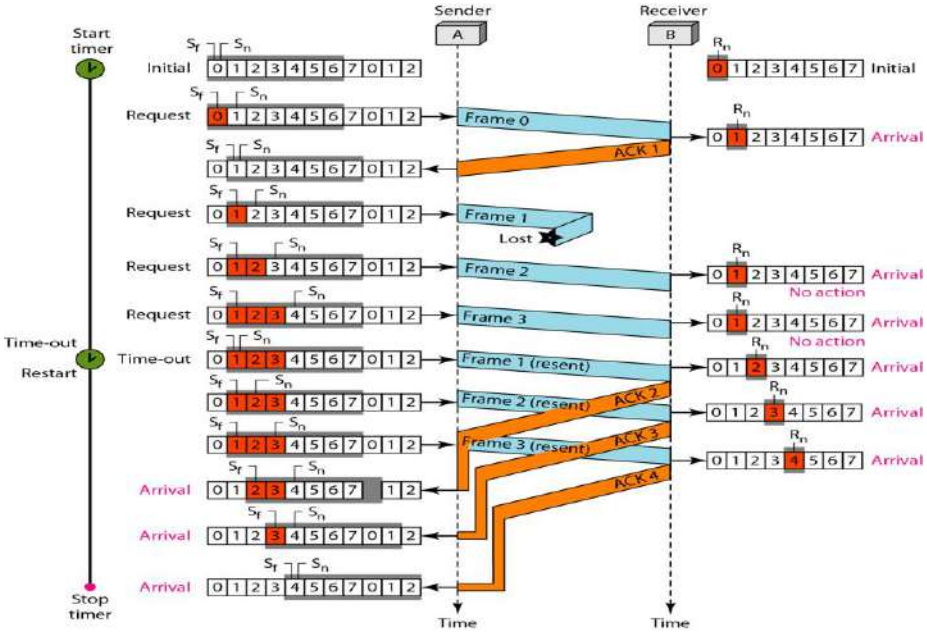


Figure shows what happens when a frame is lost. Frames 0, 1, 2, and 3 are sent. However, frame 1 is lost. The receiver receives frames 2 and 3, but they are discarded because they are received out of order. The sender receives no acknowledgment about frames 1, 2, or 3. Its timer finally expires. The sender sends all outstanding frames (1, 2, and 3) because it does not know what is wrong. Note that the resending of frames 1, 2, and 3 is the response to one single event. When the sender is responding to this event, it cannot accept the triggering of other events. This means that when ACK 2 arrives, the sender is still busy with sending frame 3.

Before the second timer expires, all outstanding frames have been sent and the timer is stopped.

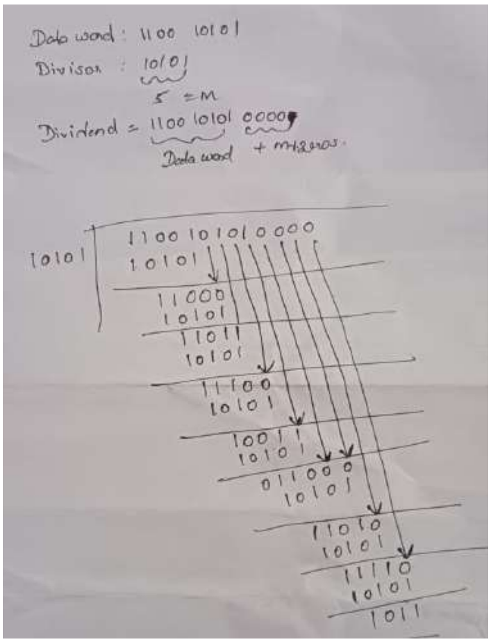
Q3. a) Consider an error detecting CRC With the generator10101

i) Compute the transmitted bit sequence for the data bit sequence 110010101

ii) The string of bits 110011001100 is received. Check whether there are errors in the received code word.

Ans. (part1 -5 marks+part 2- 5marks)

i)



Data word : 1100 10101

Divisor : 10101

5 = M

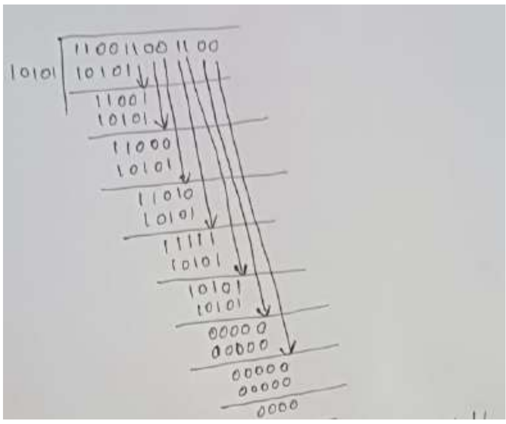
Dividend = 1100 10101 0000

Data word + m-1 zeros.

```
10101 | 1100101010000
        10101
        -----
         11000
         10101
         -----
          11011
          10101
          -----
           11100
           10101
           -----
            10011
            10101
            -----
             011000
              10101
              -----
               11010
               10101
               -----
                11110
                10101
                -----
                 1011
```

The remainder is 1011.
So the transmitted sequence is 011011011011

ii)



```
10101 | 110011001100
        10101
        -----
         11001
         10101
         -----
          11000
          10101
          -----
           11010
           10101
           -----
            11111
            10101
            -----
             10101
             10101
             -----
              00000
              00000
              -----
               00000
               00000
               -----
                0000
```

It is acceptable because the remainder is 0000.

Q3. b) What is routing? What are desirable characteristics of routing algorithm? Explain Dijkstra’s algorithm as shortest path routing with suitable example.

Ans. Routing-1mark, charachteristics-4marks,dijkstra’s algm-5 marks(2marks concept+3marks example)

Routing is a process of selecting path along which the data can be transferred from source to the destination. Routing is performed by a special device known as a router.

The routing algorithms are used for routing the packets. The routing algorithm is nothing but a software responsible for deciding the optimal path through which packet can be transmitted.

The routing protocols use the metric to determine the best path for the packet delivery.

Desirable characteristics of routing algorithms

1. Correctness: The routing algorithm should be correct enough to deliver the right packet to the right destination.

2. Simplicity: It should be simple enough to implement and also to manipulate.

3. Robustness: It should be robust enough to adapt to the situation in which the desired path is congested or a router in the path is under maintenance or they may be topological changes in the network.

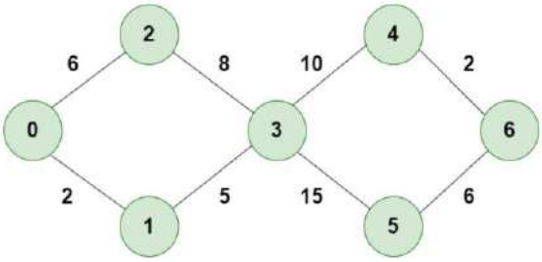
4. Stability: The routing algorithm should come to equilibrium after running a certain amount of time and after accommodating the changes in the network.

5. Fairness: The routing algorithm should be fair to all the hosts in delivering the data sent by them. Although some situations may require non-fairness to implement optimality.

6. Optimality: To achieve efficient routing one or more of the metrics should be optimized. The metric may be the number of hops, delay bandwidth etc.

Dijkstra's algorithm

Consider the below graph:



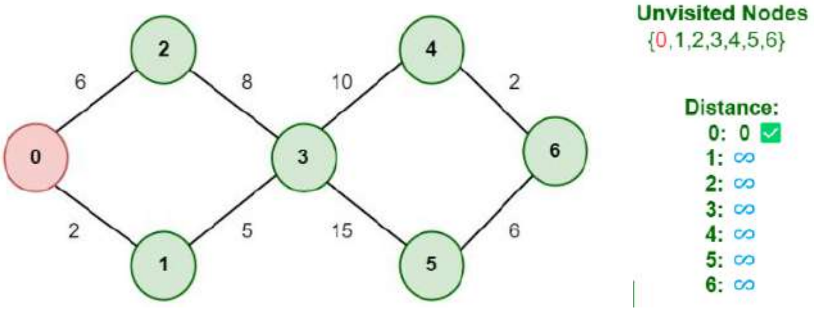
The algorithm will generate the shortest path from node 0 to all the other nodes in the graph.
For this graph, we will assume that the weight of the edges represents the distance between two nodes.

As, we can see we have the shortest path from,
Node 0 to Node 1, from
Node 0 to Node 2, from
Node 0 to Node 3, from
Node 0 to Node 4, from
Node 0 to Node 6.

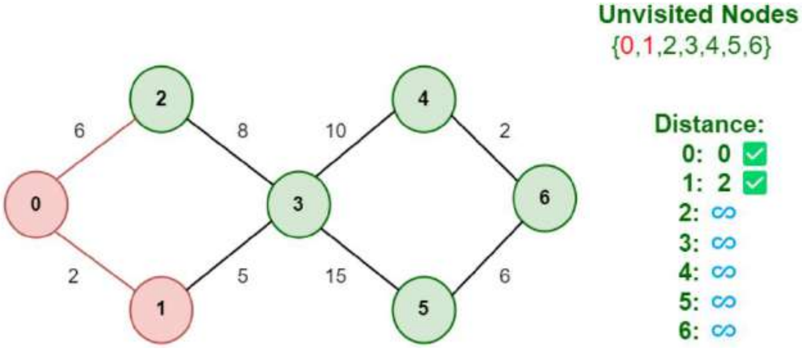
Initially we have a set of resources given below :

- The Distance from the source node to itself is 0. In this example the source node is 0.
- The distance from the source node to all other node is unknown so we mark all of them as infinity.
- we'll also have an array of unvisited elements that will keep track of unvisited or unmarked Nodes.
- Algorithm will complete when all the nodes marked as visited and the distance between them added to the path. Unvisited Nodes:- 0 1 2 3 4 5 6.

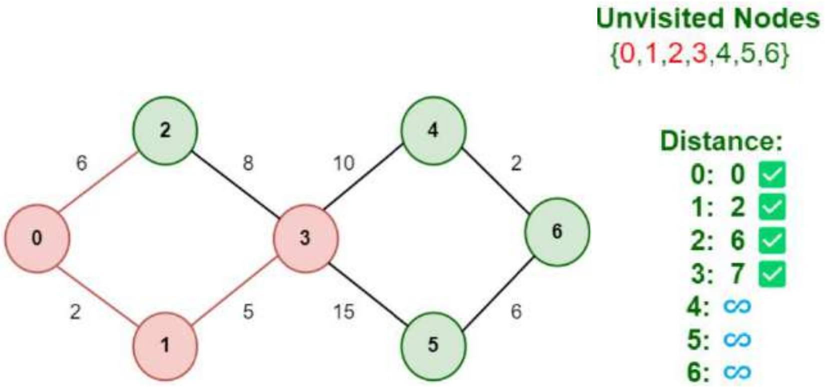
Step 1:
Start from Node 0 and mark Node as visited. Visited Node is marked red.



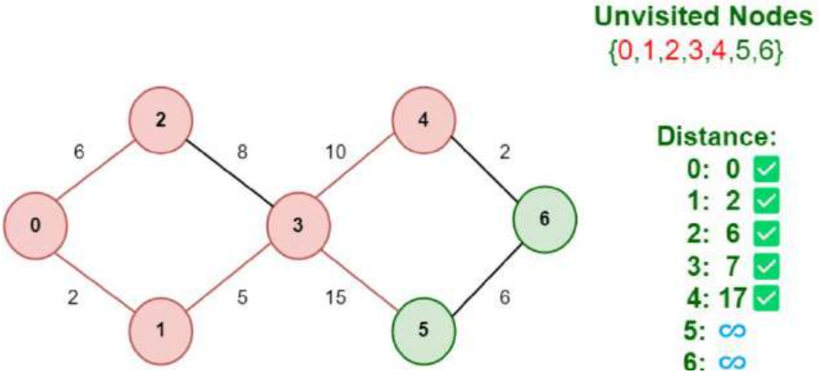
Step 2:
Check for adjacent Nodes, Now we have two choices (Either choose Node1 with distance 2 or either choose Node 2 with distance 6) and choose Node with minimum distance. In this step Node 1 is Minimum distance adjacent Node, so marked it as visited and add up the distance.



Step 3: Then Move Forward and check for adjacent Node which is Node 3, so marked it as visited and add up the distance, Now the distance will be:

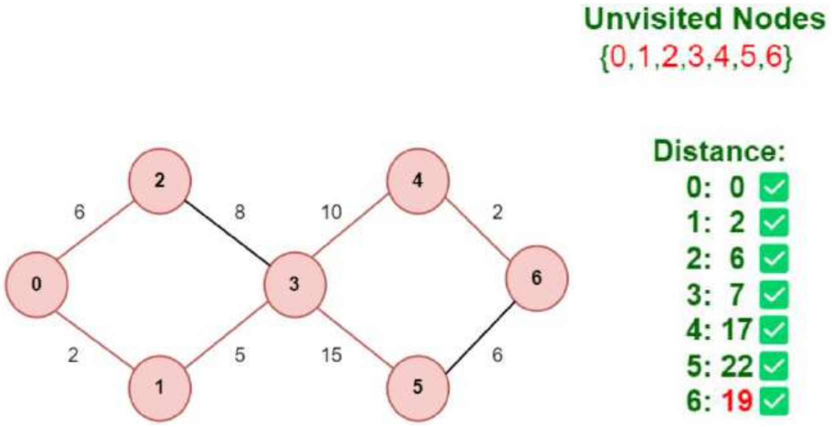


Step 4:
Again we have two choices for adjacent Nodes (Either we can choose Node 4 with distance 10 or either we can choose Node 5 with distance 15) so choose Node with minimum distance. In this step Node 4 is Minimum distance adjacent Node, so marked it as visited and add up the distance.



Step 5:

Again, Move Forward and check for adjacent Node which is Node 6, so marked it as visited and add up the distance, Now the distance will be:



So, the Shortest Distance from the Source Vertex is 19 which is optimal one.

Q4. a) What is subnetting? Given the class C network 192.168.10.0 use the subnet mask

255.255.255.192 to create subnets and answer the following:

(i) What is the number of subnets created?

(ii) How many hosts per subnet?

(iii) Calculate the IP address of the first host, the last host and the broadcast address ofeach subnet

Ans. Subnetting – 1 mark, each part carry 3 marks.

Subnetting is the process of dividing a network into smaller subnetworks, each with its own range of IP addresses and subnet mask. Subnetting can improve network performance, security, and efficiency by reducing the size and scope of broadcast domains.

Given the class C network 192.168.10.0 and the subnet mask 255.255.255.192, we can answer the following questions:

(i) The number of subnets created is equal to the number of bits borrowed from the host portion of the IP address. In this case, we have borrowed 2 bits (since 192 in binary is 11000000), so the number of subnets is 2^2 = 4.

(ii) The number of hosts per subnet is equal to the number of remaining bits in the host portion of the IP address, minus 2 (one for the network address and one for the broadcast address). In this case, we have 6 remaining bits (since 192 in binary is 11000000), so the number of hosts per subnet is 2^6 - 2 = 62.

(iii) To calculate the IP address of the first host, the last host and the broadcast address of each subnet, we need to find the subnet ID of each subnet first. The subnet ID is obtained by setting the borrowed bits to 0, 1, 2, or 3 (in binary) and leaving the rest of the bits unchanged. For example, the subnet ID of the first subnet is 192.168.10.0, since we set the borrowed bits to 00 and leave the rest unchanged. The subnet ID of the second subnet is 192.168.10.64, since we set the borrowed bits to 01 and leave the rest unchanged. Similarly, the subnet ID of the third subnet is 192.168.10.128, and the subnet ID of the fourth subnet is 192.168.10.192.

The IP address of the first host of each subnet is obtained by adding 1 to the subnet ID. For example, the IP address of the first host of the first subnet is 192.168.10.1, since we add 1 to 192.168.10.0. The IP address of the first host of the second subnet is 192.168.10.65, since we add 1 to 192.168.10.64. Similarly, the IP address of the first host of the third subnet is 192.168.10.129, and the IP address of the first host of the fourth subnet is 192.168.10.193.

The IP address of the last host of each subnet is obtained by subtracting 1 from the broadcast address of each subnet. The broadcast address of each subnet is obtained by setting the remaining bits in the host portion to 1. For example, the broadcast address of the first subnet is 192.168.10.63, since we set the remaining bits to 111111. The IP address of the last host of the first subnet is 192.168.10.62, since we subtract 1 from 192.168.10.63. The broadcast address of the second subnet is 192.168.10.127, since we set the remaining bits to 111111. The IP address of the last host of the second subnet is 192.168.10.126, since we subtract 1 from 192.168.10.127. Similarly, the broadcast address of the third subnet is 192.168.10.191, and the IP address of the last host of the third subnet is 192.168.10.190. The broadcast address of the fourth subnet is 192.168.10.255, and the IP address of the last host of the fourth subnet is 192.168.10.254.

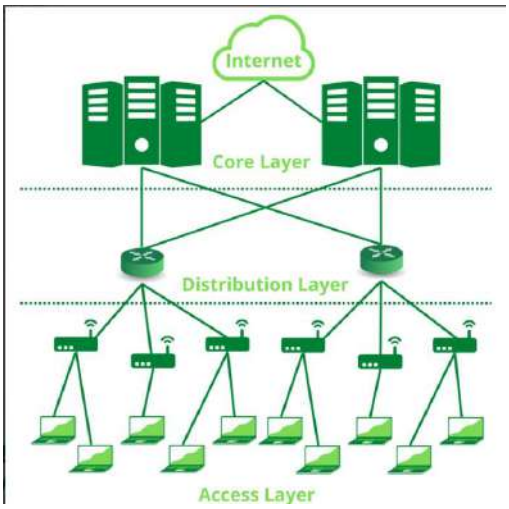
The following table summarizes the results:

Subnet ID	First Host	Last Host	Broadcast Address
192.168.10.0	192.168.10.1	192.168.10.62	192.168.10.63
192.168.10.64	192.168.10.65	192.168.10.126	192.168.10.127
192.168.10.128	192.168.10.129	192.168.10.190	192.168.10.191
192.168.10.192	192.168.10.193	192.168.10.254	192.168.10.255

Q4. b) Explain in brief classic three-layer Hierarchical model for network design by Cisco.

Ans. Theory -6(each layer 2)+diagram -4

The Cisco three-layer hierarchical model is a set of recommendations that describe how a campus LAN network should be designed. This model suggests that instead of designing a flat campus LAN network, an administrator should design a hierarchical campus LAN network. A hierarchical network is easier to manage and troubleshoot than a flat network. The Cisco three-layer hierarchical model contains three layers: core, distribution, and access. The core layer is the backbone of the network. It provides a high-speed connection between different distribution layer devices. The distribution layer connects the access layer to the core layer. The access layer provides initial connections to end users.



Access Layer:

The Access Layer is the part of the network which enables the users to connect to the wired Ethernet Network. It enables the users to share data and resources on the local network. The devices used in this layer include Ethernet Switches and Hubs.

Hubs are basically multiport repeaters. They are devices that cannot decode the data packets received by them because they lack circuitry and logic to decode the data packets. Hubs cannot determine which host must receive the data packet. They simply repeat the electronic signals received on one interface to all other interfaces on the hub, thus all the hosts connected to the hub receive the data packet. Hubs have a fatal issue of collision. if two hosts transmit data packets at the same time, they would "collide" and be rendered useless. The hosts must retransmit the packets again.

Another device used in the Access Layer is the Ethernet Switch. An Ethernet Switch is far more capable than hubs. They can decode the data packets and determine the interface to which the data packet must be forwarded. they use the MAC address, also known as the Physical Address, assigned to the host to forward the data packets. This reduces the issue of collision faced while using hubs. The development of Switches has rendered Hubs obsolete. Devices like Cisco 2390XR are used at this layer.

Distribution Layer:

When a network grows beyond a certain size, it must be divided into multiple local (Access Layer) networks. the distribution layer connects these networks together. It ensures that local traffic remains confined to local networks and governs traffic control between these networks.

This layer uses Routers to connect multiple networks together. Routers and other devices on this layer are meant to connect multiple networks together, and not individual hosts. In order to navigate traffic between hosts on different networks, IP Address, also known as Logical Address, is used. The Router maintains a Routing Table to determine the interface on which to forward the received data packet.

This layer also acts as an intermediary between the Access Layer and the Core Layer. Devices like the Cisco C9300 are used at this layer.

Core Layer:

This layer is considered the backbone of a network, as it is used to connect multiple Distribution Layer devices together. This layer uses the most powerful devices to manage the traffic between the networks. The speed at which data flows in this layer is upwards of 10 Gigabit Ethernet. This layer has the maximum number of redundant connections (Redundancy is the process of introducing extra connections between the same network points to ensure reliable data transfer even if one of the connections is down) in order to ensure reliable connectivity.

Devices like Cisco Catalyst 9600 are used at this layer with high-speed and high-bandwidth transmission media like optical fibre cable.

Advantages:

Larger, more complex networks are divided into smaller, manageable subnetworks.

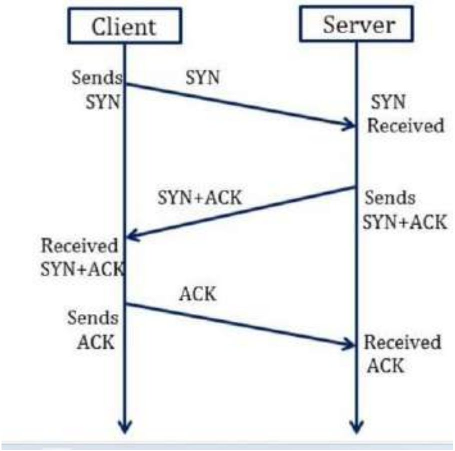
Local traffic remains local, which increases network efficiency.

Makes the network scalable. The addition of new networks does not affect the performance of existing ones.

Q. 5 a) Explain with the help of suitable diagram TCP connection management

and release?

Ans. Diagram-4,theory-6



Synchronization Sequence Number (SYN) − The client sends the SYN to the server

- When the client wants to connect to the server, then it sends the message to the server by setting the SYN flag as 1.
- The message carries some additional information like the sequence number (32-bit random number).

- The ACK is set to 0. The maximum segment size and the window size are also set. For example, if the window size is 1000 bits and the maximum segment size is 100 bits, then a maximum of 10 data segments can be transmitted in the connection by dividing (1000/100=10).

Synchronization and Acknowledgement (SYN-ACK) to the client

- The server acknowledges the client request by setting the ACK flag to 1.
- The ACK indicates the response of the segment it received and SYN indicates with what sequence number it will start the segments.
- For example, if the client has sent the SYN with sequence number = 500, then the server will send the ACK using acknowledgment number = 5001.
- The server will set the SYN flag to '1' and send it to the client if the server also wants to establish the connection.
- The sequence number used for SYN will be different from the client's SYN.
- The server also advertises its window size and maximum segment size to the client. And, the connection is established from the client-side to the server-side.

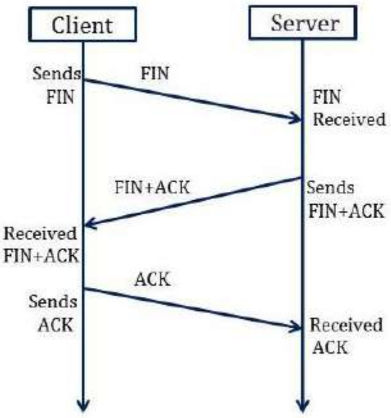
Acknowledgment (ACK) to the server

- The client sends the acknowledgment (ACK) to the server after receiving the synchronization (SYN) from the server.
- After getting the (ACK) from the client, the connection is established between the client and the server.
- Now the data can be transmitted between the client and server sides.

3 -Way Handshake Closing Connection Process

To close a 3-way handshake connection,

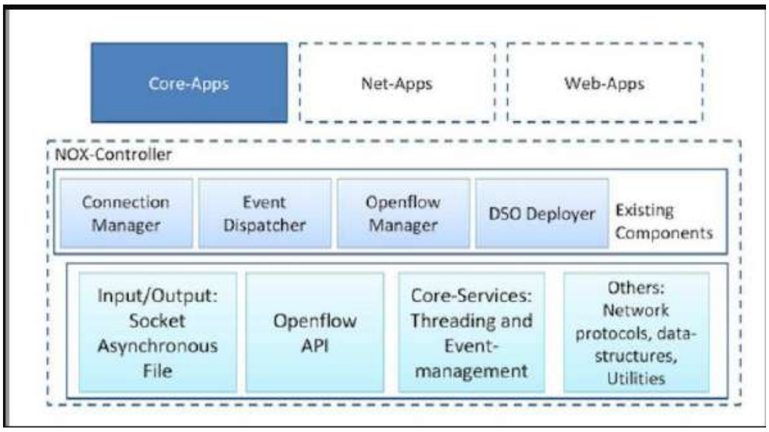
- First, the client requests the server to terminate the established connection by sending FIN.
- After receiving the client request, the server sends back the FIN and ACK request to the client.
- After receiving the FIN + ACK from the server, the client confirms by sending an ACK to the server.



Q.5. b) Elaborate the architecture of Nox and Pox controller of SDN with their comparison.

Ans. NOX-5(2+3),POX-5 (2+3)

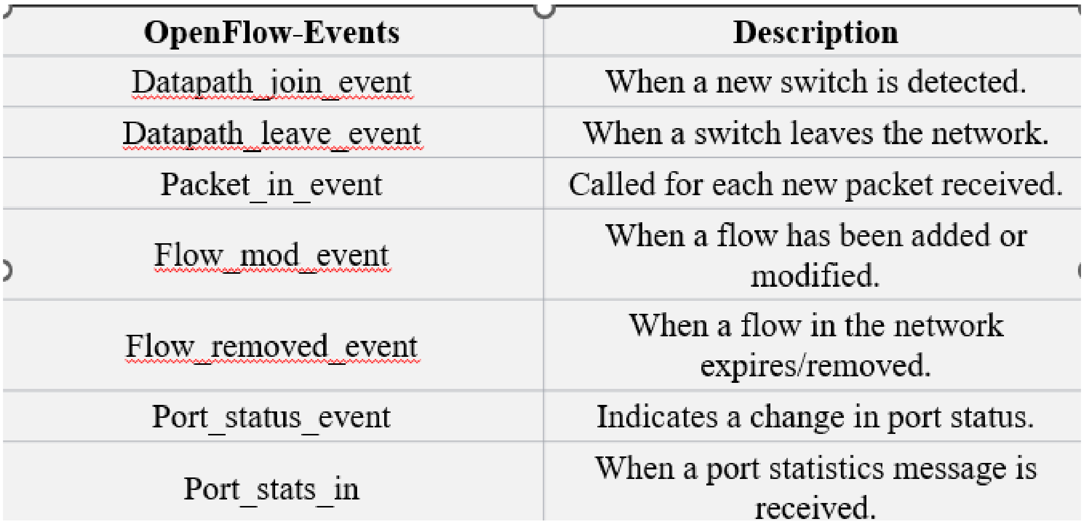
NOX Architecture


Core-Apps
Net-Apps
Web-Apps
NOX-Controller
Connection Manager
Event Dispatcher
Openflow Manager
DSO Deployer
Existing Components
Input/Output: Socket Asynchronous File
Openflow API
Core-Services: Threading and Event-management
Others: Network protocols, data-structures, Utilities

- NOX is the original OpenFlow controller.
- It serves as a network control platform, that provides a high level programmatic interface for management and the development of network control applications.
- Its system-wide abstractions turn networking into a software problem.
- NOX versions:
  1. NOX classic: This is the version that has been available under the GPL since 2009.
  2. NOX: The “new NOX.” Only contains support for C++ and has lesser applications than the classic; however, this version is faster and has better codebase.
  3. POX: Typically termed as NOX’s sibling. Provides Python support.

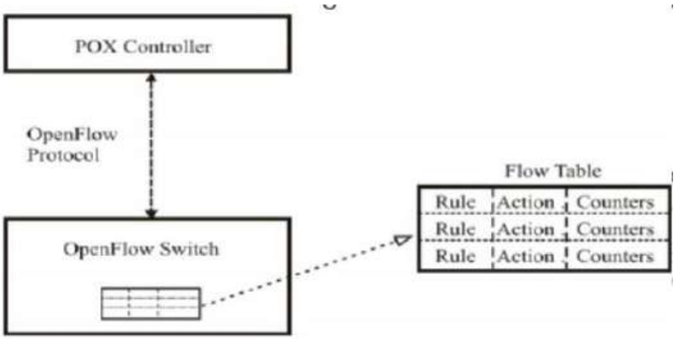
- The NOX core provides helper methods, such as network packet process, threading and event engine, in addition to OpenFlow APIs for interacting with OpenFlow switches, and I/O operations support.

- At the top, we have applications: Core, Net and Web.
- However, with the current NOX version, there are only two core applications: OpenFlow and switch, and both network and web applications are missing.
- The middle layer shows the in-built components of NOX. The connection manager, event dispatcher and OpenFlow manager are self-explanatory, whereas the dynamic shared object (DSO) deployer basically scans the directory structure for any components being implemented as DSOs.
- All the applications can be viewed as components.
- All applications inherit from the component class. Hence, NOX applications are generally composed of cooperating components that provide the required functionality. In short, a component encapsulates specific functionality that is made available to NOX.
- An event represents a low-level or high-level event in the network.
- Typically the event only provides the information, and processing of that information is deferred to handlers.
- Many events roughly correlate to something which happens on the network that may be of interest to a NOX component.
- These components, typically, consists a set of event handlers. In this sense, events drive all execution in NOX.



OpenFlow-Events	Description
Datapath_join_event	When a new switch is detected.
Datapath_leave_event	When a switch leaves the network.
Packet_in_event	Called for each new packet received.
Flow_mod_event	When a flow has been added or modified.
Flow_removed_event	When a flow in the network expires/removed.
Port_status_event	Indicates a change in port status.
Port_stats_in	When a port statistics message is received.

POX Architecture



- POX is an open source development platform for Python-based software-defined networking (SDN) control applications, such as OpenFlow SDN controllers.
- POX, which enables rapid development and prototyping, is becoming more commonly used than NOX.

  POX, is to allow users to write their own applications that use the controller as an intermediary — or abstraction layer — between network applications and the network equipment

- POX controller provides an efficient way to implement the OpenFlow protocol which is the communication protocol between the controllers and the switches.
- Using POX controller you can run different applications like hub, switch, load balancer, and firewall.
- Tcp dump packet capture tool can be used to capture and see the packets flowing between POX controller and OpenFlow devices.
- Communication between the controller and the switches is carried by communication protocol. OpenFlow is the most popular standard protocol used in SDN.
- OpenFlow switches behave as dumb forwarding devices. They are unable to perform any actions without programmed by the controller.
- When a switch is powered on, it will immediately connect to an OpenFlow controller.
- Initially, the flow table of the switches is empty.
- When a packet arrives at a switch, it does not know, how this packet is to be handled.
- Then it send packet-in message to the controller.
- To handle the packet, controller inserts a flow entries in flow table of switch.
- Flow entry in flow table contains three parts, rule(match field), action, counters.
- For each packet, that has to pass through a switch, a flow entry will have to be installed so that the switch can forward this traffic without further intervention of the controller .
- Flow modification messages are sent to the switches to install the flow entries in flow table.

- Once these are installed, traffic belonging to this flow will be handled by the switches themselves.

Q. 6 Write a short note on:

a) DNS

b) SDN

c) PPDIOO Network design Methodology.

d) NAT

ANS. 2.5 marks for each topic.

DNS

An application layer protocol defines how the application processes running on different systems, pass the messages to each other.

- DNS stands for Domain Name System.
- DNS is a directory service that provides a mapping between the name of a host on the network and its numerical address.
- DNS is required for the functioning of the internet.
- Each node in a tree has a domain name, and a full domain name is a sequence of symbols specified by dots.
- DNS is a service that translates the domain name into IP addresses. This allows the users of networks to utilize user-friendly names when looking for other hosts instead of remembering the IP addresses.
- For example, suppose the FTP site at EduSoft had an IP address of 132.147.165.50, most people would reach this site by specifying ftp.EduSoft.com. Therefore, the domain name is more reliable than IP address.

SDN

- Software-defined networking (SDN) is a new networking paradigm that separates the network's control and data planes**.** The traditional networking architecture has a tightly coupled relationship between the data and control planes. This means that network devices, such as routers and switches, are responsible for forwarding packets and determining how the network should operate.

- With SDN, the control plane is decoupled from the data plane and implemented in software, allowing for centralized network control. The control plane, also called the network controller, is responsible for making decisions about how traffic should be forwarded, based on the overall network policy. The data plane, on the other hand, is responsible for forwarding traffic based on the decisions made by the control plane.
- In SDN, network devices are called switches, and they are typically simple, low-cost devices that forward traffic based on the instructions received from the network controller. The controller communicates with the switches using a standard protocol, such as OpenFlow, which allows the controller to program the switches to forward traffic in a particular way.

PPDIOO

The PPDIOO phases are as follows:

- **Prepare:** Involves establishing the organizational requirements, developing a network strategy, and proposing a high-level conceptual architecture identifying technologies that can best support the architecture. The prepare phase can establish a financial justification for network strategy by assessing the business case for the proposed architecture.
- **Plan:** Involves identifying initial network requirements based on goals, facilities, user needs, and so on. The plan phase involves characterizing sites and assessing any existing networks and performing a gap analysis to determine whether the existing system infrastructure, sites, and the operational environment can support the proposed system. A project plan is useful for helping manage the tasks, responsibilities, critical milestones, and resources required to implement changes to the network. The project plan should align with the scope, cost, and resource parameters established in the original business requirements.
- **Design:** The initial requirements that were derived in the planning phase drive the activities of the network design specialists. The network design specification is a comprehensive detailed design that meets current business and technical requirements, and incorporates specifications to support availability, reliability, security, scalability, and performance. The design specification is the basis for the implementation activities.
- **Implement:** The network is built or additional components are incorporated according to the design specifications, with the goal of integrating devices without disrupting the existing network or creating points of vulnerability.
- **Operate:** Operation is the final test of the appropriateness of the design. The operational phase involves maintaining network health through day-to-day operations, including maintaining high availability and reducing expenses. The fault detection, correction, and performance monitoring that occur in daily operations provide the initial data for the optimization phase.
- **Optimize:** Involves proactive management of the network. The goal of proactive management is to identify and resolve issues before they affect the organization. Reactive fault detection and correction (troubleshooting) is needed when proactive management cannot predict and mitigate failures. In the PPDIOO process, the optimization phase can prompt a network redesign if too many network problems and errors arise, if performance does not meet expectations, or if new applications are identified to support organizational and technical requirements.

NAT

To access the Internet, one public IP address is needed, but we can use a private IP address in our private network. The idea of NAT is to allow multiple devices to access the Internet through a single public address. To achieve this, the translation of a private IP address to a public IP address is required. Network Address Translation (NAT) is a process in which one or more local IP address is translated into one or more Global IP address and vice versa in order to provide Internet access to the local hosts. Also, it does the translation of port numbers i.e. masks the port number of the host with another port number, in the packet that will be routed to the destination. It then makes the corresponding entries of IP address and port number in the NAT table. NAT generally operates on a router or firewall.

NAT working

Generally, the border router is configured for NAT i.e the router which has one interface in the local (inside) network and one interface in the global (outside) network. When a packet traverse outside the local (inside) network, then NAT converts that local (private) IP address to a global (public) IP address. When a packet enters the local network, the global (public) IP address is converted to a local (private) IP address.

If NAT runs out of addresses, i.e., no address is left in the pool configured then the packets will be dropped and an Internet Control Message Protocol (ICMP) host unreachable packet to the destination is sent.