CMR INSTITUTE OF TECHNOLOGY	USN										

Internal Assesment Test – II Answer Key

Subject : Computer Networks				Code : 18MCA24
Date : 14/05/2019	Duration : 90 mins	Max Marks : 50	Sem : II	Branch : MCA

Answer ANY FIVE FULL Questions	Marks	OBE CO	OBE RBT
1. Explain WI-FI(802.11) Architecture.	[10]	CO2	L1

Wireless LANs are most important access networks technologies in the Internet

 Most popular is the IEEE 802.11 wireless LAN, known also as Wi-Fi

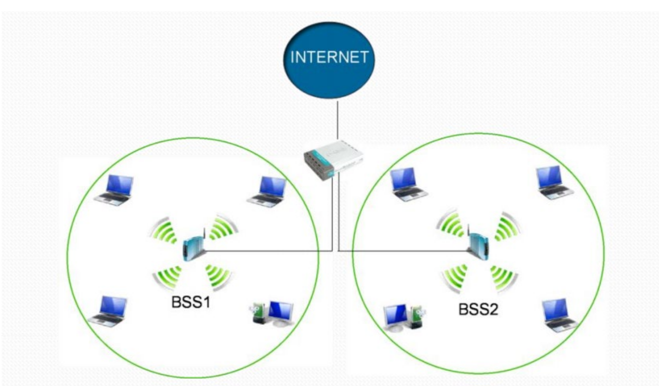
 There are several standards for wireless LAN technology.

The IEEE 802.11 Architecture

 Basic Service Set (BSS) is the fundamental building block of the architecture. It can contain one or more wireless stations and one central base station, also known as Access Point (AP).

 Typical architecture consist of few BSSs connected to some interconnection device like hub or switch which lead to the Internet.

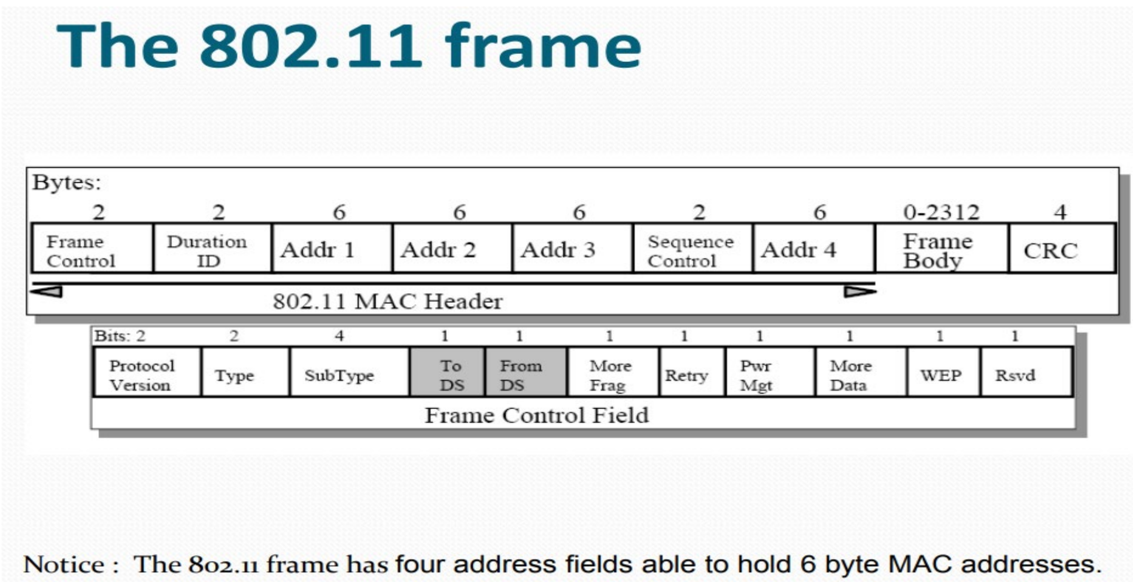
The IEEE 802.11 LAN Architecture:-



Infrastructure wireless LAN is a term often referred to wireless LANs that deploy AP, with the infrastructure being the APs along with wired Ethernet infrastructure that connects APs and router, hub or switch

 IEEE 802.11 stations can also group together and form ad hoc type network with no connection to internet

❖ The 802.11 frame:-



For 802.11 network it is necessary to use three address fields for moving datagram from a wireless station through the Access Point to a router.

The forth address is used in ad hoc networks

. □ Address 1 field holds the MAC address of the station that is suppose to receive the frame.

□ Address 2 field holds the MAC address of station that sends data.

□ Address field 3 contains the MAC address of the router to which AP is connected.

Sequence number helps to distinguishing between a newly transmitted frame and the retransmission of a previous frame. □ The duration value field is used when transmitting station reserves the channel for the time to transmit data frame and ACK.

□ Frame control fields type and subtype are used to distinguish the association , RTS, CTS, ACK, and data frames.

□ The to and from fields are used to define the meaning of the address fields which meanings change depending whether it is an ad hoc or infrastructure network.

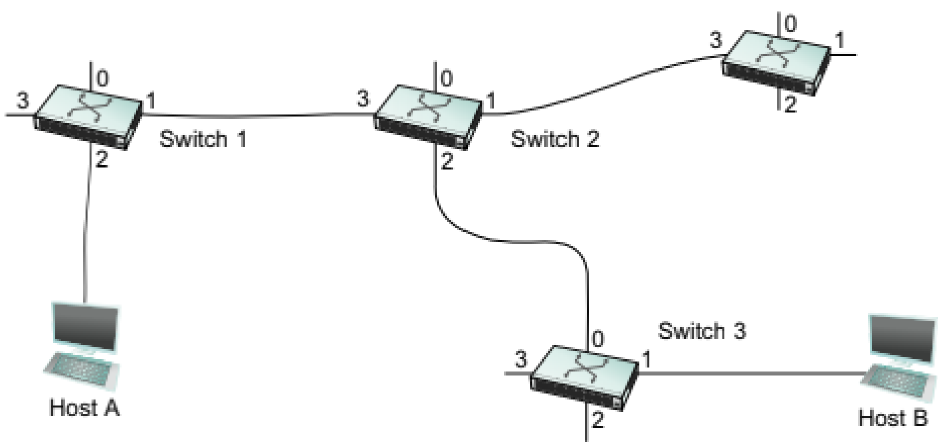
□ The WEP field specifies if encryption is being used or not.

More Frag field specifies that more fragments will come

□ Retry bit indicates retransmission of a frame sent earlier □ Pwr Mgt field is used by the base station to put the reciever into sleep state or take it out of sleep □ More Data indicates that sender has more frames for the reciever □ Rsvd bit tell the reciever that a sequence of frames with this bit must be processed strictly in order			
2. Explain Interdomain routing(BGP) Protocol.	[10]	CO3	L2
3. What is Switching? Explain Virtual Circuit Switching.	[10]	CO3	L2

A second technique for packet switching, which differs significantly from the datagram model, uses the concept of a virtual circuit (VC).

Virtual Circuit Switching also referred to as a connection-oriented model, requires setting up a virtual connection from the source host to the destination host before any data is sent.



■ FIGURE 3.3 An example of a virtual circuit network.

- In Figure, where host A again wants to send packets to host B. We can think of this as a two-stage process. The first stage is "connection setup." The second is data transfer.
- In the connection setup phase, it is necessary to establish a "connection state" in each of the switches between the source and destination hosts.
- The connection state for a single connection consists of an entry in a "VC table" in each switch through which the connection passes.
- **One entry in the VC table on a single switch contains:**

  ■ A virtual circuit identifier (VCI) that uniquely identifies the connection at this switch and which will be carried inside the header of the packets that belong to this connection

■ An incoming interface on which packets for this VC arrive at the switch

■ An outgoing interface in which packets for this VC leave the switch

■ A potentially different VCI that will be used for outgoing packets

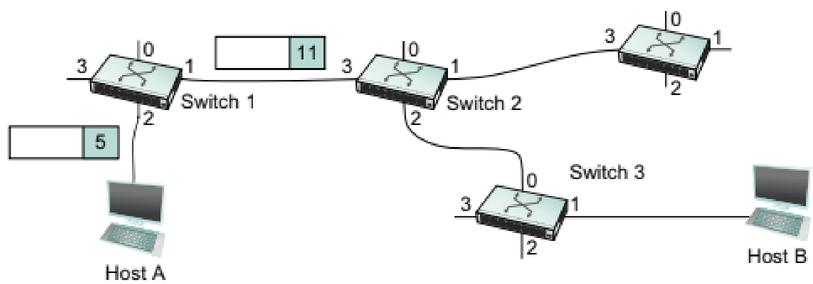
Let's assume that a network administrator wants to manually create a new virtual connection from host A to host B. First, the administrator needs to identify a path through the network from A to B.

In the example network of Figure 3.3, there is only one such path, but in general this may not be the case. The administrator then picks a VCI value that is currently unused on each link for the connection.

For the purposes of our example, let's suppose that the VCI value 5 is chosen for the link from host A to switch 1, and that 11 is chosen for the link from switch 1 to switch 2. In that case, switch 1 needs to have an entry in its VC table configured as shown in Table 3.2.

Table 3.2 Virtual Circuit Table Entry for Switch 1

Incoming Interface	Incoming VCI	Outgoing Interface	Outgoing VCI
2	5	1	11



■ FIGURE 3.4 A packet is sent into a virtual circuit network.

suppose that the VCI of 7 is chosen to identify this connection on the link from switch 2 to switch 3 and that a VCI of 4 is chosen for the link from switch 3 to host B. In that case, switches 2 and 3 need to be configured with VC table entries as shown in Table 3.3. Note that the "outgoing" VCI value at one switch is the "incoming" VCI value at the next switch.

Table 3.3 Virtual Circuit Table Entries for Switches 2 and 3

VC Table Entry at Switch 2			
Incoming Interface	Incoming VCI	Outgoing Interface	Outgoing VCI
3	11	2	7
VC Table Entry at Switch 3			
Incoming Interface	Incoming VCI	Outgoing Interface	Outgoing VCI
0	7	1	4

There are several things to note about virtual circuit switching:

■ Since host A has to wait for the connection request to reach the far side of the network and return before it can send its first data packet, there is at least one round-trip time (RTT) of delay before data is sent.3

■ While the connection request contains the full address for host B (which might be quite large, being a global identifier on the network), each data packet contains only a small identifier, which is only unique on one link. Thus, the per-packet overhead caused by the header is reduced relative to the datagram model.

■ If a switch or a link in a connection fails, the connection is broken and a new one will need to be established. Also, the old one needs to be torn down to free up table storage space in the switches.

■ The issue of how a switch decides which link to forward the connection request on has been glossed over. In essence, this

is the same problem as building up the forwarding table for datagram forwarding, which requires some sort of routing algorithm. Routing is described in Section 3.3, and the algorithms described there are generally applicable to routing setup requests as well as datagrams.

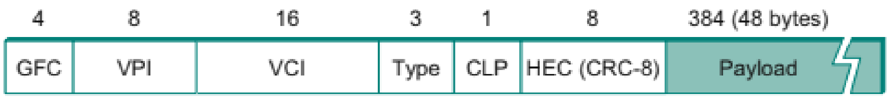
Asynchronous Transfer Mode (ATM)

Asynchronous Transfer Mode (ATM) is probably the most well-known virtual circuit-based networking technology, although it is now somewhat past its peak in terms of deployment.

ATM became an important technology in the 1980s and early 1990s for a variety of reasons, not the least of which is that it was embraced by the telephone industry, which had historically been less than active in data communications past its peak in terms of deployment.

ATM also happened to be in the right place at the right time, as a high-speed switching technology that appeared on the scene just when shared media like Ethernet and token rings were starting to look a bit too slow for many users of computer networks. In some ways ATM was a competing technology with Ethernet switching, and it was seen by many as a competitor to IP as well.

There are a few aspects of ATM that are worth examining. The picture of the ATM packet format—more commonly called an ATM cell in Figure will illustrate the main points.



■ FIGURE 3.6 ATM cell format at the UNI.

the generic flow control (GFC) bits, which never saw much use.

start with the 24 bits that are labelled VPI (virtual path identifier—8 bits)

VCI (virtual circuitidentifier—16 bits).

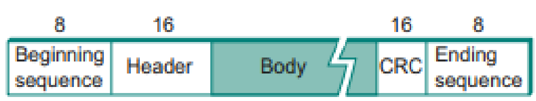
CLP-priority of the cells

we find an 8-bit cyclic redundancy check (CRC), known as the header error check (HEC).

4. What is Framing? Explain Bit-Oriented Protocols.

[10] CO2 L3

The Synchronous Data Link Getting connected (SDLC) protocol developed by IBM is an example of a bit-oriented protocol; SDLC was later standardized by the ISO as the High-Level Data Link Control (HDLC) protocol.



■ FIGURE 2.10 HDLC frame format.

HDLC denotes both the beginning and the end of a frame with the distinguished bit sequence 01111110. This sequence is also transmitted during any times that the link is idle so that the sender and receiver can keep their clocks synchronized.

In this way, both protocols essentially use the sentinel approach. Because this sequence might appear anywhere in the body of the frame—in fact, the bits 01111110 might cross byte boundaries—bit-oriented protocols use the analog of the DLE character, a technique known as bit stuffing.

Bit stuffing in the HDLC protocol works as follows. On the sending side, any time five consecutive

1s have been transmitted from the body of the message (i.e., excluding when the sender is trying to transmit the distinguished 01111110 sequence), the sender inserts a 0 before transmitting the next bit. On the receiving side, should five consecutive 1s arrive, the receiver makes its decision based on the next bit it sees (i.e., the bit following the five 1s). If the next bit is a 0, it must have been stuffed, and so the receiver removes it. If the next bit is a 1, then one of two things is true: Either this is the end-of-frame marker or an error has been introduced into the bit stream. By looking at the next bit, the receiver can distinguish between these two cases. If it sees a 0 (i.e., the last 8 bits it has looked at are 01111110), then it is the end-of-frame marker; if it sees a 1 (i.e., the last 8 bits it has looked at are 01111111), then there must have been an error and the whole frame is discarded.			
5. Explain Bluetooth(802.15) Architecture.	[10]	CO2	L4

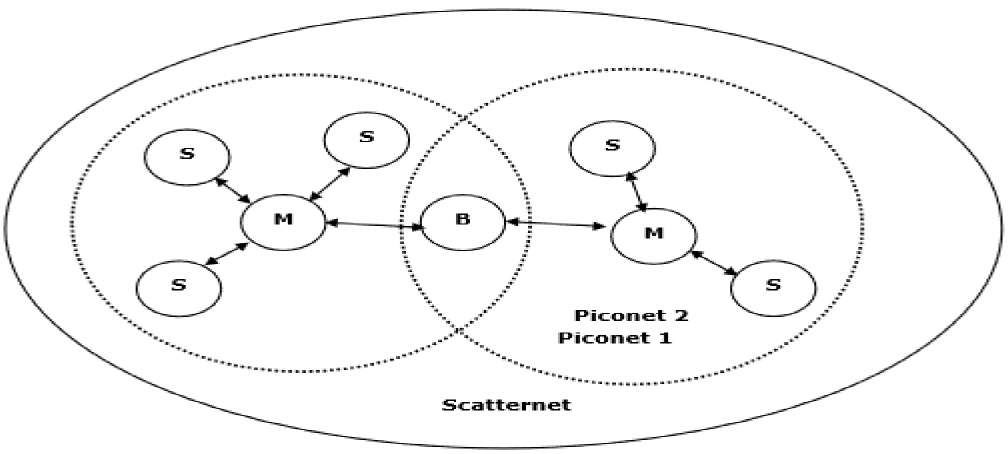
WLAN technology enables device connectivity to infrastructure based services through a wireless carrier provider. The need for personal devices to communicate wirelessly with one another without an established infrastructure has led to the emergence of **Personal Area Networks (PANs)**.

- Ericsson's Bluetooth project in 1994 defines the standard for PANs to enable communication between mobile phones using low power and low cost radio interfaces.
- In May 1988, Companies such as IBM, Intel, Nokia and Toshiba joined Ericsson to form the Bluetooth Special Interest Group (SIG) whose aim was to develop a defacto standard for PANs.
- IEEE has approved a Bluetooth based standard named IEEE 802.15.1 for Wireless Personal Area Networks (WPANs). IEEE standard covers MAC and Physical layer applications

The usage of Bluetooth has widely increased for its special features.

- Bluetooth offers a uniform structure for a wide range of devices to connect and communicate with each other.
- Bluetooth technology has achieved global acceptance such that any Bluetooth enabled device, almost everywhere in the world, can be connected with Bluetooth enabled devices.
- Low power consumption of Bluetooth technology and an offered range of up to ten meters has paved the way for several usage models.
- Bluetooth offers interactive conference by establishing an adhoc network of laptops.
- Bluetooth usage model includes cordless computer, intercom, cordless phone and mobile phones

- # Piconets and Scatternets
- Bluetooth enabled electronic devices connect and communicate wirelessly through shortrange devices known as **Piconets**. Bluetooth devices exist in small ad-hoc configurations with the ability to act either as master or slave the specification allows a mechanism for **master** and **slave** to switch their roles. Point to point configuration with one master and one slave is the simplest configuration.
- When more than two Bluetooth devices communicate with one another, this is called a **PICONET**. A Piconet can contain up to seven slaves clustered around a single master. The device that initializes establishment of the Piconet becomes the **master**.
- The master is responsible for transmission control by dividing the network into a series of time slots amongst the network members, as a part of **time division multiplexing** scheme which is shown below.



- Figure: Piconets and Scatternets
-

The features of Piconets are as follows −

- Within a Piconet, the timing of various devices and the frequency hopping sequence of individual devices is determined by the clock and unique **48-bit address** of master.
- Each device can communicate simultaneously with up to seven other devices within a single Piconet.
- Each device can communicate with several piconets simultaneously.
- Piconets are established dynamically and automatically as Bluetooth enabled devices enter and leave piconets.
- There is no direct connection between the slaves and all the connections are essentially master-to-slave or slave-to-master.
- Slaves are allowed to transmit once these have been polled by the master.

<table>
<tr><td>

Transmission starts in the slave-to-master time slot immediately following a polling packet from the master.
A device can be a member of two or more piconets, jumping from one piconet to another by adjusting the transmission regime-timing and frequency hopping sequence dictated by the master device of the second piconet.
It can be a slave in one piconet and master in another. It however cannot be a master in more than once piconet.
Devices resident in adjacent piconets provide a bridge to support inner-piconet connections, allowing assemblies of linked piconets to form a physically extensible communication infrastructure known as Scatternet.

<h2>Range</h2>
Bluetooth operating range depends on the device Class 3 radios have a range of up to 1 meter or 3 feet Class 2 radios are most commonly found in mobile devices have a range of 10 meters or 30 feet Class 1 radios are used primarily in industrial use cases have a range of 100 meters or 300 feet.
<h2>Data rate</h2>
Bluetooth supports 1Mbps data rate for version 1.2 and 3Mbps data rate for Version 2.0 combined with Error Data Rate.
</td><td></td><td></td><td></td></tr>
<tr><td>6. Write a short note on:-
(a) ARP
(b)DHCP</td><td>[10]</td><td>CO3</td><td>L 3</td></tr>
<tr><td>7. Explain Virtual Networks and Tunnels.</td><td>[10]</td><td>CO3</td><td>L 3</td></tr>
<tr><td>8. Explain the distance vector router algorithm.
Each node constructs a one-dimensional array (a vector) containing the “distances” (costs) to all other nodes and distributes that vector to its immediate neighbors.
for distance-vector routing is that each node knows the cost of the link to each of its directly connected neighbors. These costs may be provided when the router is configured by a network manager.
</td><td>[10]</td><td>CO3</td><td>L 4</td></tr>
</table>

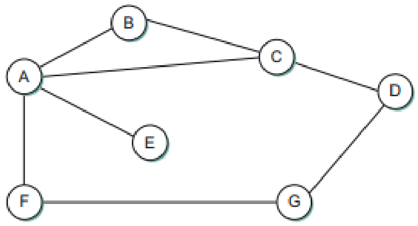


FIGURE 3.29 Distance-vector routing: an example network.

Table 3.10 Initial Distances Stored at Each Node (Global View)

Information Stored at Node	Distance to Reach Node						
	A	B	C	D	E	F	G
A	0	1	1	∞	1	1	∞
B	1	0	1	∞	∞	∞	∞
C	1	1	0	1	∞	∞	∞
D	∞	∞	1	0	∞	∞	1
E	1	∞	∞	∞	0	∞	∞
F	1	∞	∞	∞	∞	0	1
G	∞	∞	∞	1	∞	1	0

In this example, the cost of each link is set to 1, so that a least-cost path is simply the one with the fewest hops.

each node sets a cost of 1 to its directly connected neighbors and ∞ to all other nodes. Thus, A initially believes that it can reach B in one hop and that D is unreachable.

Table 3.11 Initial Routing Table at Node A

Destination	Cost	NextHop
B	1	B
C	1	C
D	∞	—
E	1	E
F	1	F
G	∞	—

The next step in distance-vector routing is that every node sends a message to its directly connected neighbors containing its personal list of distances.

For example, node F tells node A that it can reach node G at a cost of 1; A also knows it can reach F at a cost of 1, so it adds these costs to get the cost of reaching G by means of F. This total cost of 2 is less than the current cost of infinity, so A records that it can reach G at a cost of 2 by going through F.

Table 3.12 Final Routing Table at Node A		
Destination	Cost	NextHop
B	1	B
C	1	C
D	2	C
E	1	E
F	1	F
G	2	F

The process of getting consistent routing information to all the nodes is called convergence. Table 3.13 shows the final set of costs from each node to all other nodes when routing has converged. We must stress that there is no one node in the network that has all the information in this table—each node only knows about the contents of its own routing table.

Routing Information Protocol (RIP)

Rip is a distance vector routing protocol. Routing protocols in internetworks differ very slightly from the idealized graph model described.

In an internetwork, the goal of the routers is to learn how to forward packets to various networks. rather than advertising the cost of reaching other routers, the routers advertise the cost of reaching networks.

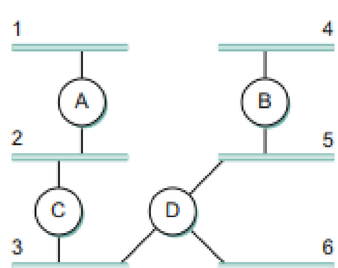


FIGURE 3.30 Example network running RIP.

For example, in Figure , router C would advertise to router A the fact that it can reach networks 2 and 3 (to which it is directly connected) at a cost of 0, networks 5 and 6 at cost 1, and network 4 at cost 2.

Routing Information Protocol (RIP) is a dynamic routing protocol which uses hop count as a routing metric to find the best path between the source and the destination network. It is a distance vector routing protocol which has AD value 120 and works on the application layer of OSI model. RIP uses port number 520.

HopCount:

Hop count is the number of routers occurring in between the source and destination network. The path with the lowest hop count is considered as the best route to reach a network and therefore placed in the routing table. RIP prevents routing loops by limiting the number of hopes allowed in a path from source and destination. The maximum hop count allowed for RIP is 15 and hop count of 16 is considered as network unreachable.

Features of RIP :

1. Updates of the network are exchanged periodically.
2. Updates (routing information) are always broadcast.
3. Full routing tables are sent in updates.
4. Routers always trust on routing information received from neighbor routers. This is also known as *Routing.*

RIP versions :

There are three vesions of routing information protocol – **RIP Version1**, **RIP Version2** and **RIPng**.

RIP v1 is known as *Classful* Routing Protocol because it doesn’t send information of subnet mask in its routing update.

RIP v2 is known as *Classless* Routing Protocol because it sends information of subnet mask in its routing update.

RIP 2 Message Format:-

Command	**Version**	**Must be zero**
Family of Network 1 (AFI)		**Route Tag**
IP Address of Network 1		
Subnet mask for Network 1		
Next hop Field		
Distance to Network 1 (Metric)		
Family of Network 2		**Route Tag**
IP Address of Network 2		
Subnet mask for Network 2		
Next hop Field		
Distance to Network 2 (Metric)		

Command—Indicates whether the packet is a request or a response. The request asks that a router send all or a part of its routing table. The response can be an unsolicited regular routing update or a reply to a request. Responses contain routing table entries.

Multiple RIP packets are used to convey information from large routing tables. **Version**—Specifies the RIP version used. In a RIP packet implementing any of the RIP 2 fields or using authentication, this value is set to 2. **Address-family identifier (AFI)—**Specifies the address family used. RIPv2's AFI field functions identically to RIP's AFI field, with one exception: If the AFI for the first entry in the message is 0xFFFF, the remainder of the entry contains authentication information. Currently, the only authentication type is simple password. **Route tag**—Provides a method for distinguishing between internal routes (learned by RIP) and external routes (learned from other protocols). **IP address**—Specifies the IP address for the entry. **Subnet mask**—Contains the subnet mask for the entry. If this field is zero, no subnet mask has been specified for the entry. **Next hop**—Indicates the IP address of the next hop to which packets for the entry should be forwarded. **Metric**—Indicates how many internetwork hops (routers) have been traversed in the trip to the destination. This value is between 1 and 15 for a valid route, or 16 for an unreachable route.			
9. Explain IPV6 header format with diagram.	[10]	CO3	L4
10. Explain Link State (OSPF) Algorithm.	[10]	CO3	L4