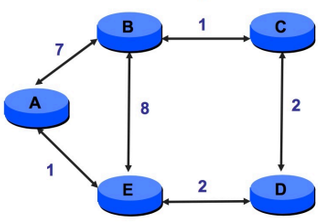
CN Assignment IV

1. **Explain Distance Vector Routing algorithm with an example.**

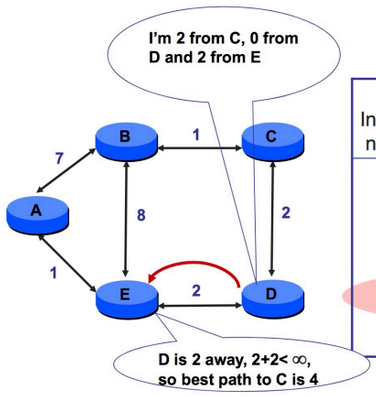
- Define distances at each node X
  - $d_x(y)$ = cost of least cost path from X to Y
- Update distances based on neighbors
  - $d_x(y) = \min \{ d_x(y), c(x, v) + d_v(y) \}$ over all neighbors V
- c(x, v) = cost for direct link from x to v
  - Node x maintains a list of all costs of direct links c(x, v)
- $D_x(y)$ = estimate of least cost from x to y
  - Node x maintains a list its of distance vectors D_x.
- Each node periodically sends D_v to neighbors and they update their own distance vectors.
  - $Dx(y) = \min \{ d_x(y), c(x, v) + d_v(y) \}$

Example:

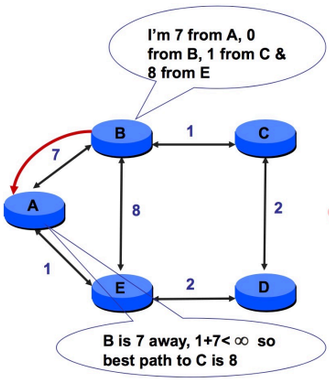
Initially



Info at node	Distance to Node				
	A	B	C	D	E
A	0	7	∞	∞	1
B	7	0	1	∞	8
C	∞	1	0	2	∞
D	∞	∞	2	0	2
E	1	8	∞	2	0

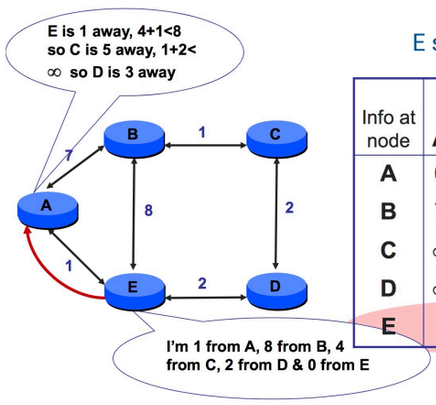


Info at node	Distance to Node				
	A	B	C	D	E
A	0	7	∞	∞	1
B	7	0	1	∞	8
C	∞	1	0	2	∞
D	∞	∞	2	0	2
E	1	8	**4**	2	0



B sends vector to A

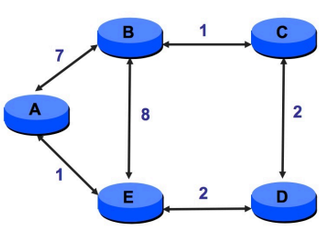
Info at node	Distance to Node				
	A	B	C	D	E
A	0	7	**8**	∞	1
B	7	0	1	∞	8
C	∞	1	0	2	∞
D	∞	∞	2	0	2
E	1	8	4	2	0



E sends vector to A

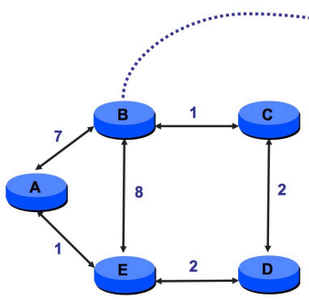
Info at node	Distance to Node				
	A	B	C	D	E
A	0	7	**5**	**3**	1
B	7	0	1	∞	8
C	∞	1	0	2	∞
D	∞	∞	2	0	2
E	1	8	4	2	0

Until Convergence



Info at node	Distance to Node				
	A	B	C	D	E
A	0	6	5	3	1
B	6	0	1	3	5
C	5	1	0	2	4
D	3	3	2	0	2
E	1	5	4	2	0

Node B's distance vectors



Dest	Next hop		
	A	E	C
A	7	9	**6**
C	12	12	**1**
D	10	10	**3**
E	8	8	**5**

2. **Explain with necessary diagrams, Internet Group Management Protocol (IGMP).**

The **Internet Group Management Protocol** (**IGMP**) is a communications protocol used by hosts and adjacent routers on IPv4 networks to establish multicast group memberships. IGMP is an integral part of IP multicast.

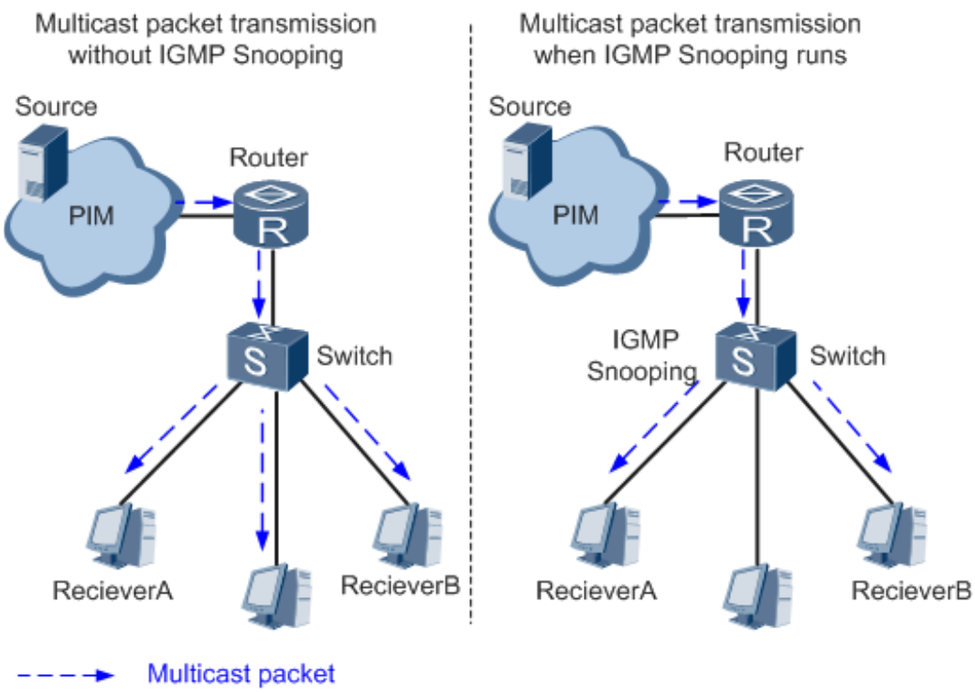
IGMP can be used for one-to-many networking applications such as online streaming video and gaming, and allows more efficient use of resources when supporting these types of applications.

In general, IGMP supports two principal operations:

- Hosts send messages to routers to subscribe to and unsubscribe from a multi-cast group defined by a given multicast address.
- Routers periodically check which multicast groups are of interest to which hosts.

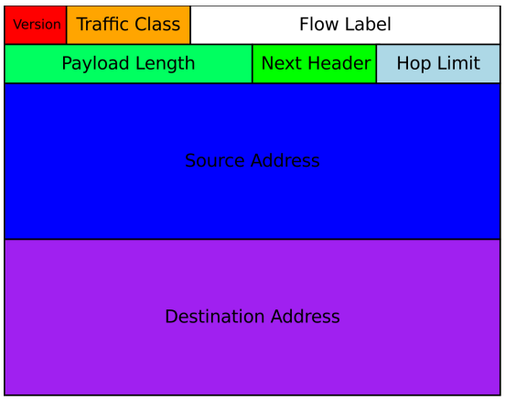
The objective of each host in using IGMP is to make itself known as a member of a group with a given multicast address to other hosts on the LAN and to all routers on the LAN.

To join a group, a host sends an IGMP membership report message, in which the group address field is the multicast address of the group.



3. **Describe Base Header fields used in IPv6 packet.**

The fixed header of an IPv6 packet consists of its first 40 octets (320 bits).



Version (4 bits)
The constant 6 (bit sequence `0110`).

Traffic Class (8 bits)
The bits of this field hold two values. The 6 most-significant bits are used for differentiated services, which is used to classify packets. The remaining two bits are used for ECN; priority values subdivide into ranges: traffic where the source provides congestion control and non-congestion control traffic.

Flow Label (20 bits)
Originally created for giving real-time applications special service. The flow label when set to a non-zero value now serves as a hint to routers and switches with multiple outbound paths that these packets should stay on the same path so that they will not be reordered. It has further been suggested that the flow label be used to help detect spoofed packets.

Payload Length (16 bits)
The size of the payload in octets, including any extension headers. The length is set to zero when a *Hop-by-Hop* extension header carries a Jumbo Payload option.

Next Header (8 bits)
Specifies the type of the next header. This field usually specifies the transport layer protocol used by a packet's payload. When extension headers are present in the packet this field indicates which extension header follows. The values are shared with those used for the IPv4 protocol field, as both fields have the same function (see List of IP protocol numbers).

Hop Limit (8 bits)
Replaces the time to live field of IPv4. This value is decremented by one at each intermediate node visited by the packet. When the counter reaches 0 the packet is discarded.

Source Address (128 bits)
The IPv6 address of the sending node.

Destination Address (128 bits)
The IPv6 address of the destination node(s).

4. Explain character oriented framing with neat diagrams.

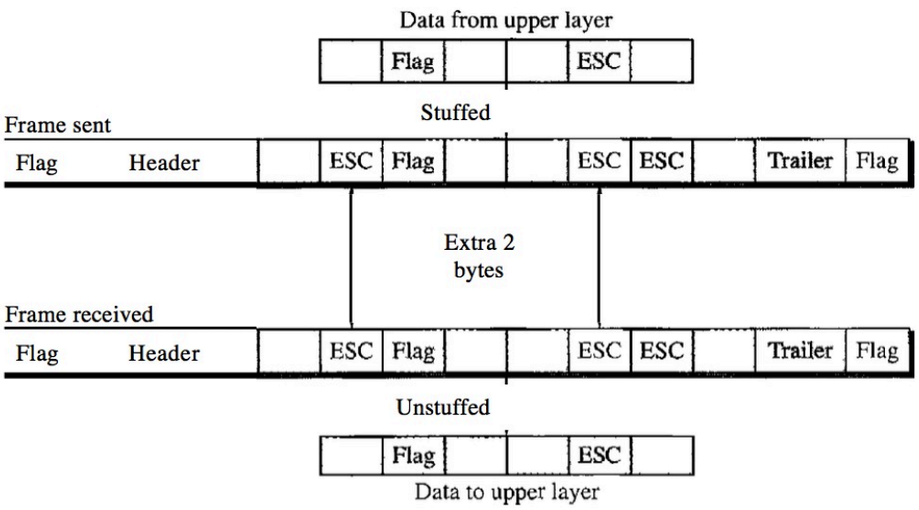
In a character-oriented protocol, data to be carried are 8-bit characters from a coding system. The header, which normally carries the source and destination addresses and other control information, and the trailer, which carries error detection or error correction redundant bits, are also multiples of 8 bits.

To separate one frame from the next, an 8-bit (I-byte) flag is added at the beginning and the end of a frame. The flag, composed of protocol-dependent special characters, signals the start or end of a frame.

The flag could be selected to be any character not used for text communication.

In byte stuffing (or character stuffing), a special byte is added to the data section of the frame when there is a character with the same pattern as the flag. The data section is stuffed with an extra byte. This byte is usually called the escape character (ESC), which has a predefined bit pattern. Whenever the receiver encounters the ESC character, it removes it from the data section and treats the next character as data, not a delimiting flag.

The escape characters that are part of the text must also be marked by another escape character i.e. if the escape character is part of the text, an extra one is added to show that the second one is part of the text.



5. **Explain the procedure to calculate the traditional checksum at Sender and Receiver ends in Internet.**

Traditionally, the Internet has been using a 16-bit checksum. The sender calculates the checksum by following these steps:

Sender site:

1. The message is divided into 16-bit words.
2. The value of the checksum word is set to 0.
3. All words including the checksum are added using one's complement addition.
4. The sum is complemented and becomes the checksum.
5. The checksum is sent with the data.

The receiver uses the following steps for error detection.

Receiver site:

1. The message (including checksum) is divided into 16-bit words.
2. All words are added using one's complement addition.
3. The sum is complemented and becomes the new checksum.
4. If the value of checksum is 0, the message is accepted; otherwise, it is rejected.