Acn Prelim QB

Q1 Attempt any five (2 marks each)

1. State different Agents involved in Mobile IP with their roles.

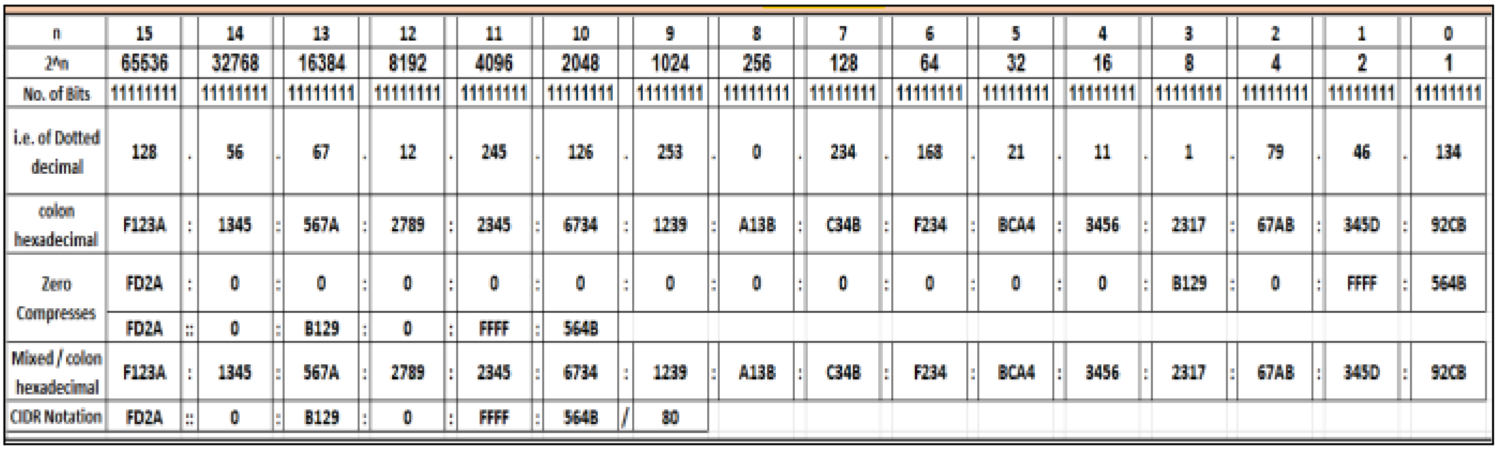
Ans:- There are two agents involved in Mobile Ip they are Home Agent and Foreign Agent.

Home Agent:-The home agent is usually a router attached to the home network of the mobile host. The home agents acts on behalf of the mobile host when a remote host sends a packet to the mobile host.

Foreign Agent:- The foreign agent is usually a router attached to the foreign network. The foreign agent receives and delivers packets sent by the home agent to the mobile host.

2. Give IP address representation notations in IPv6.

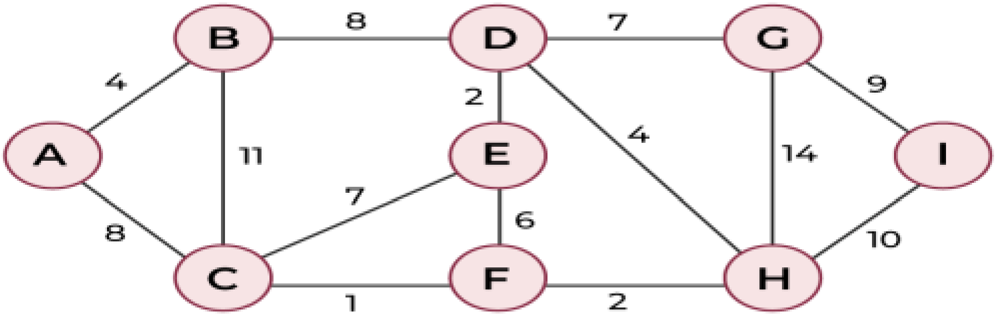
Ans:-



n	15		14		13		12		11		10		9		8		7		6		5		4		3		2		1		0
2^n	65536		32768		16384		8192		4096		2048		1024		256		128		64		32		16		8		4		2		1
No. of Bits	11111111		11111111		11111111		11111111		11111111		11111111		11111111		11111111		11111111		11111111		11111111		11111111		11111111		11111111		11111111		11111111
i.e. of Dotted decimal	128	.	56	.	67	.	12	.	245	.	126	.	253	.	0	.	234	.	168	.	21	.	11	.	1	.	79	.	46	.	134
colon hexadecimal	F123A	:	1345	:	567A	:	2789	:	2345	:	6734	:	1239	:	A13B	:	C34B	:	F234	:	BCA4	:	3456	:	2317	:	67AB	:	345D	:	92CB
Zero Compresses	FD2A	:	0	:	0	:	0	:	0	:	0	:	0	:	0	:	0	:	0	:	0	:	0	:	B129	:	0	:	FFFF	:	564B
	FD2A	::	0	:	B129	:	0	:	FFFF	:	564B																				
Mixed / colon hexadecimal	F123A	:	1345	:	567A	:	2789	:	2345	:	6734	:	1239	:	A13B	:	C34B	:	F234	:	BCA4	:	3456	:	2317	:	67AB	:	345D	:	92CB
CIDR Notation	FD2A	::	0	:	B129	:	0	:	FFFF	:	564B	/	80																		

3. Explain Dijikstra shortest path algorithm.

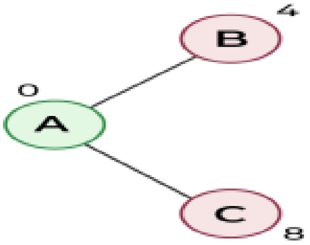
Ans:- **Note**: We use a boolean array sptSet[] to represent the set of vertices included in SPT. If a value sptSet[v] is true, then vertex v is included in SPT, otherwise not. Array dist[] is used to store the shortest distance values of all vertices. Consider the below graph and src = 0.



Shortest Path Calculation – Step 1

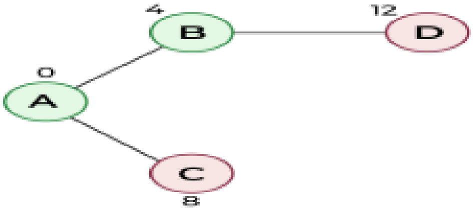
STEP 1: The set sptSet is initially empty and distances assigned to vertices are {0, INF, INF, INF, INF, INF, INF, INF} where INF indicates infinite. Now pick the vertex with a minimum distance value. The vertex 0 is picked and included in sptSet. So sptSet becomes {0}. After including 0 to sptSet, update the distance values of its adjacent vertices. Adjacent vertices of 0 are 1 and 7. The distance values of 1 and 7 are updated as 4 and 8.

The following subgraph shows vertices and their distance values. Vertices included in SPT are included in GREEN color.



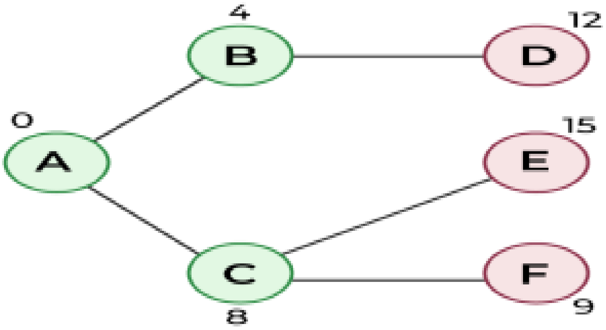
Shortest Path Calculation – Step 2

STEP 2: Pick the vertex with minimum distance value and not already included in SPT (not in sptSET). The vertex 1 is picked and added to sptSet. So sptSet now becomes {0, 1}. Update the distance values of adjacent vertices of 1. The distance value of vertex 2 becomes 12.



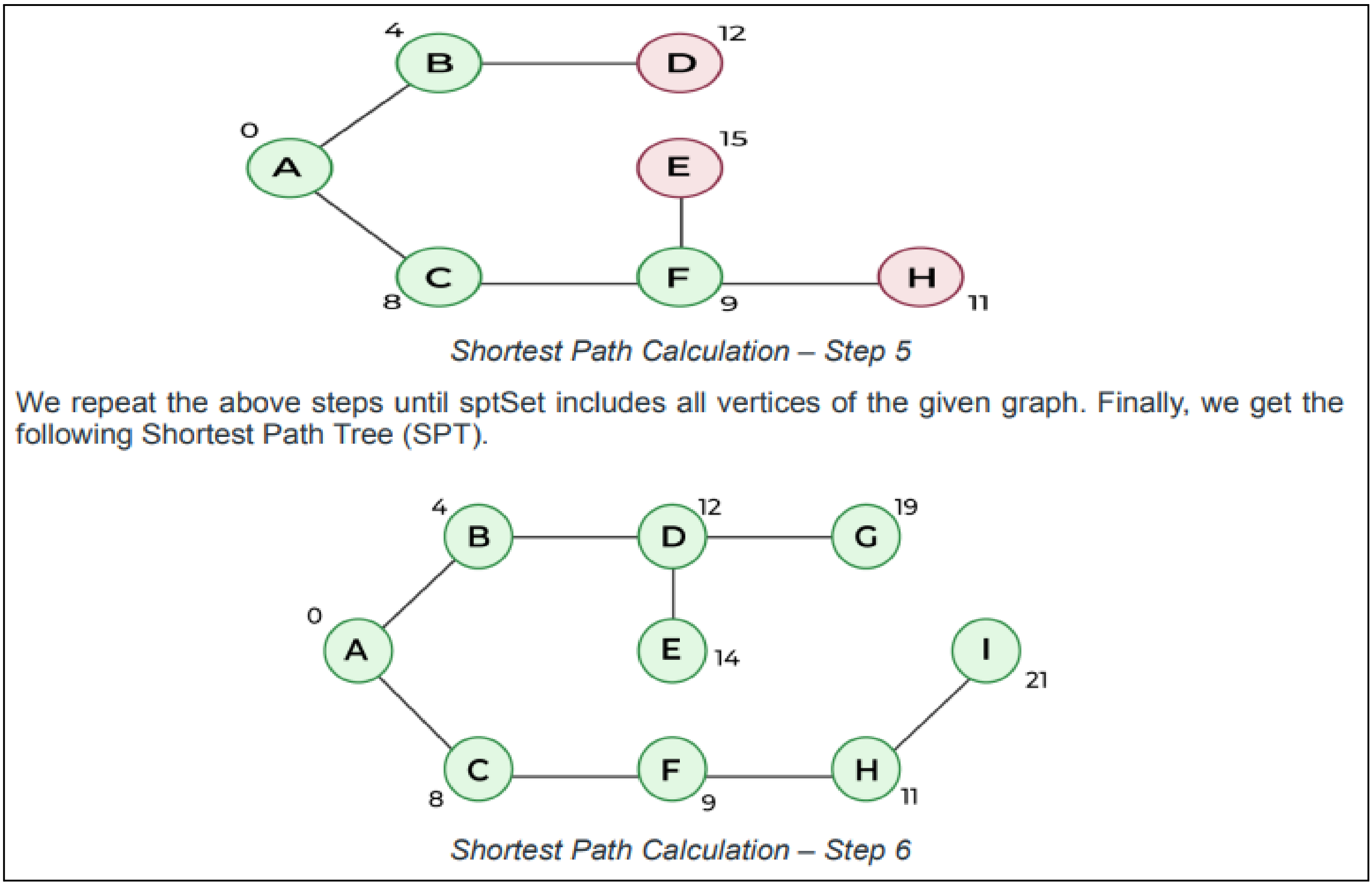
Shortest Path Calculation – Step 3

STEP 3: Pick the vertex with minimum distance value and not already included in SPT (not in sptSET). Vertex 7 is picked. So sptSet now becomes {0, 1, 7}. Update the distance values of adjacent vertices of 7. The distance value of vertex 6 and 8 becomes finite (15 and 9 respectively).



Shortest Path Calculation – Step 4

STEP 4: Pick the vertex with minimum distance value and not already included in SPT (not in sptSET). Vertex 6 is picked. So sptSet now becomes {0, 1, 7, 6}. Update the distance values of adjacent vertices of 6. The distance value of vertex 5 and 8 are updated.



Shortest Path Calculation – Step 5

We repeat the above steps until sptSet includes all vertices of the given graph. Finally, we get the following Shortest Path Tree (SPT).

Shortest Path Calculation – Step 6

4. List four features of TCP

   Ans:- Reliability: ensures data is reliably and accurately transmitted.

   Connection control: establishes a connection before data transfer.

   Flow Control: prevents data congestion using sliding window approach.

   Error Detection: includes error checking mechanism.

5. List any 4 UDP Services explain any one in detail

   Ans:- UDP provides process to process communication using socket addresses a combination of IP addresses and port number.

   Connectionless service / independent datagram.

   NO flow control.

   NO error control.

   Checksum has three sections : pseudo header , UDP header, and data coming from the application layer.

   NO congestion control.

   UDP protocol encapsulates and decapsulates messages.

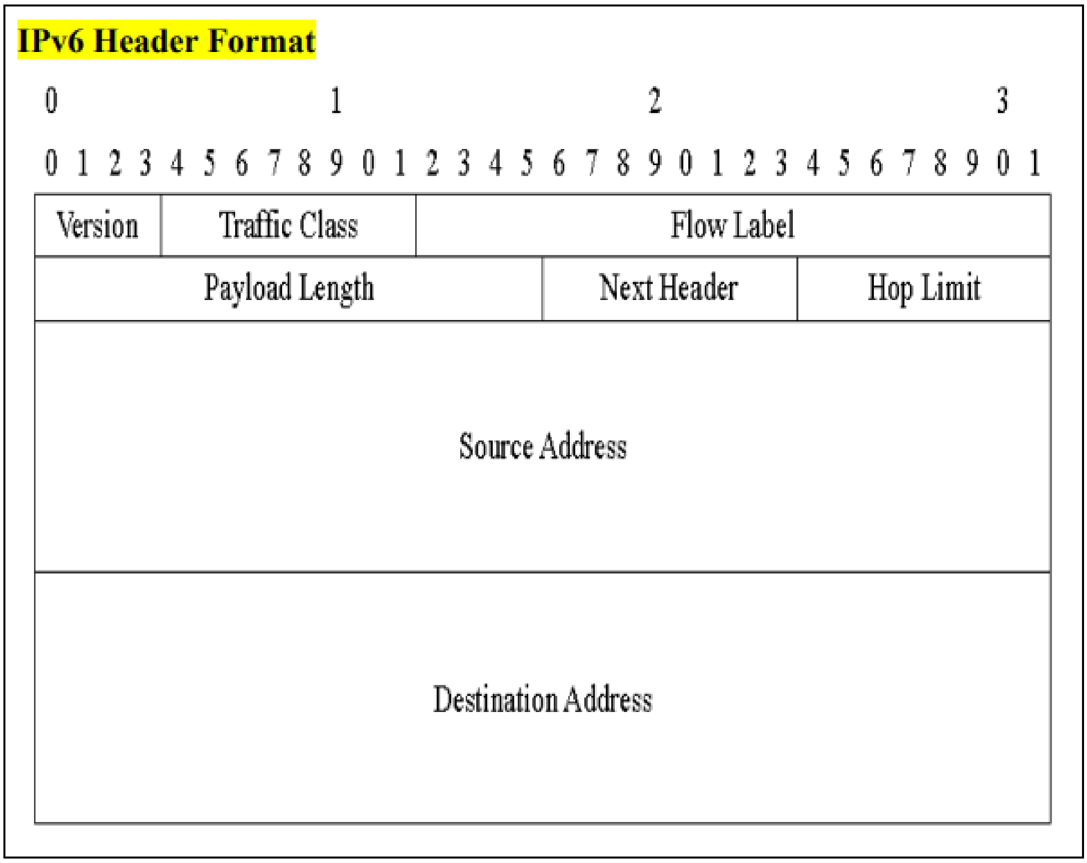
   Queuing is associated with ports.

   Multiplexing and demultiplexing of UDP Processes.

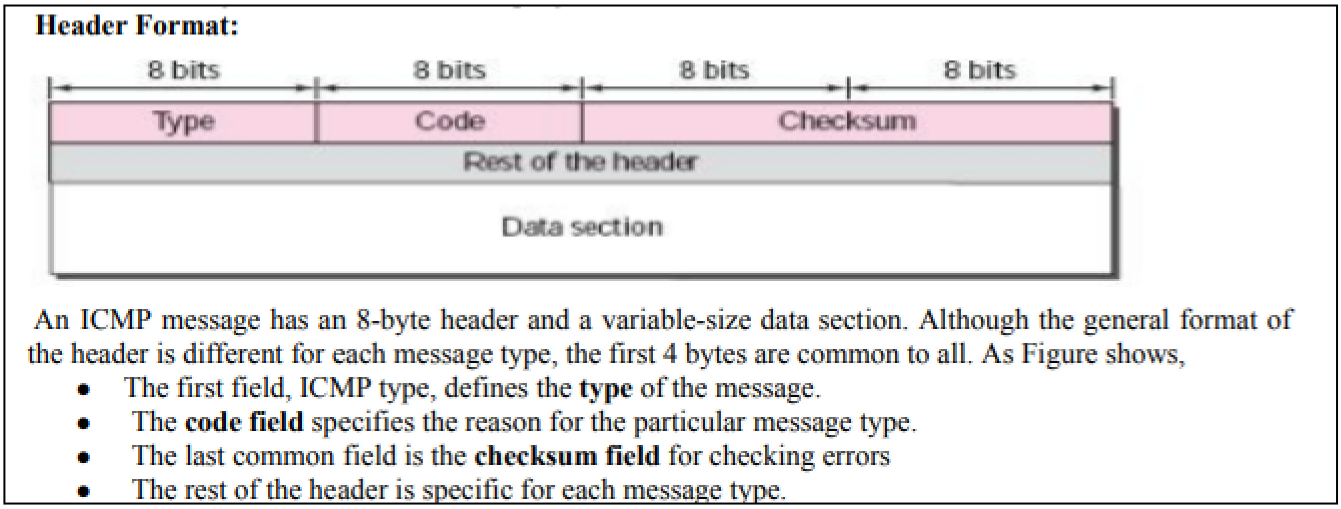
6. Explain significance and syntax of url.
   Ans:- A client that wants to access a web page needs the file name and the address to facilitate the access of documents. The Uniform Resource Locator is standard locator for specifying any kind of information over the internet.
   Syntax:- protocol:// host: port / path

Q2 Attempt any three (4 marks each)

1. Draw IPv6 Header format in detail.
   Ans:-



2. Give significance to ICMP Checksum. Give an example of Checksum Calculation.
   Ans:- ICMP supports the unreliable and connectionless IP. ICMP messages are encapsulated in IP datagrams. There are two categories error-reporting and query message. The error-reporting messages report problems that a router or a host (destination) may encounter when it processes an IP packet. The query messages, which occur in pairs, help a host or a network manager get specific information from a router or another host.



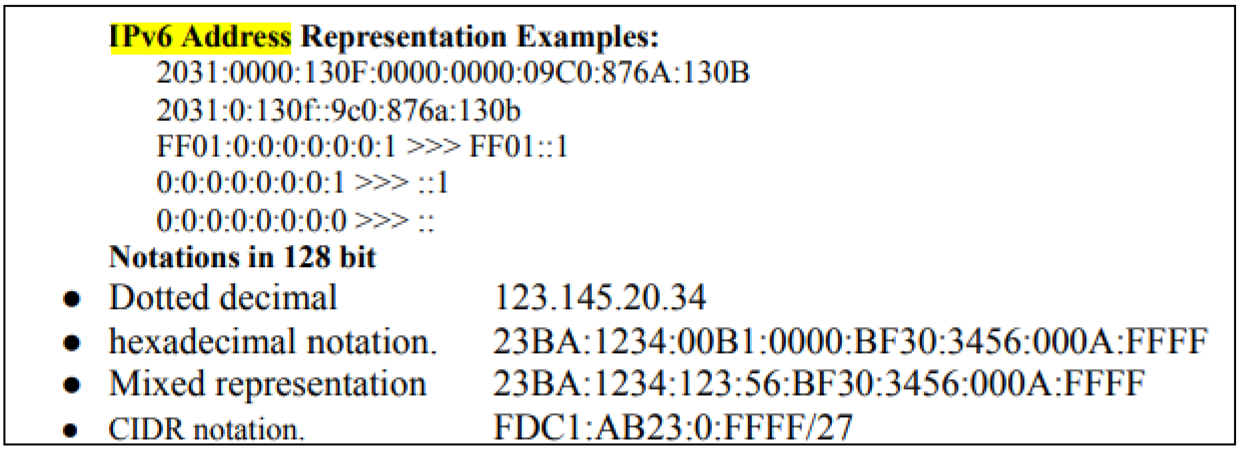
Header Format:

An ICMP message has an 8-byte header and a variable-size data section. Although the general format of the header is different for each message type, the first 4 bytes are common to all. As Figure shows,

- The first field, ICMP type, defines the **type** of the message.
- The **code field** specifies the reason for the particular message type.
- The last common field is the **checksum field** for checking errors
- The rest of the header is specific for each message type.

Calculation

3. Draw IPv6 Address Representation EUI 64- Global and Stateless Auto-configuration.
Ans:-



IPv6 Address Representation Examples:

2031:0000:130F:0000:0000:09C0:876A:130B
2031:0:130f::9c0:876a:130b
FF01:0:0:0:0:0:0:1 >>> FF01::1
0:0:0:0:0:0:0:1 >>> ::1
0:0:0:0:0:0:0:0 >>> ::

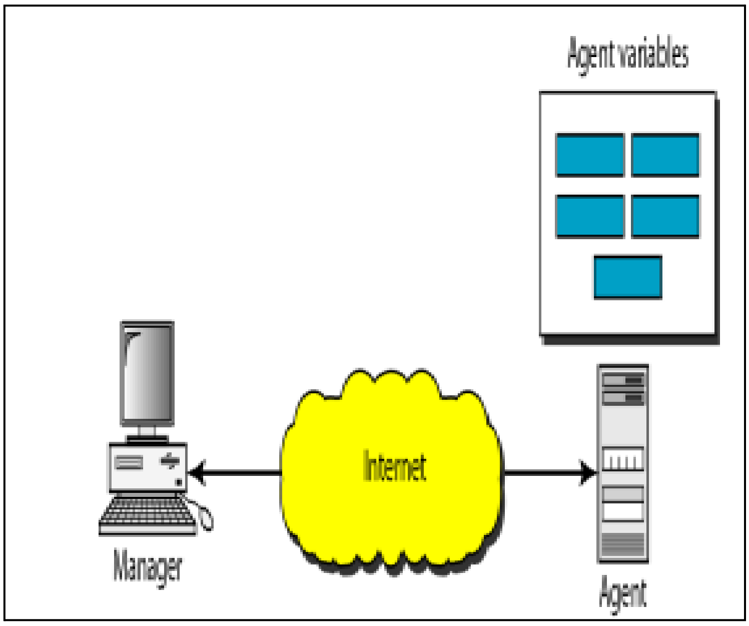
Notations in 128 bit

Dotted decimal	123.145.20.34
hexadecimal notation.	23BA:1234:00B1:0000:BF30:3456:000A:FFFF
Mixed representation	23BA:1234:123:56:BF30:3456:000A:FFFF
CIDR notation.	FDC1:AB23:0:FFFF/27

4. The dump of a UDP header in hexadecimal format is as follows: BC 82000 D 002 B 001 D Obtain the following from it: (i) Source port number (ii) Destination port number (iii) Total length (iv) Length of the data
Ans:- The UDP header has four parts, each of two bytes. That means we get the following interpretation of the header.
i) Source port number = BC8216 = 48258
ii) Destination port number = 000D16= 13
iii) Total length = 002B16 = 43 bytes
iv) Since the header is 8 bytes the data length is 43 − 8 =35 bytes.

5. Explain Simple Network Management Protocol(SNMP) with a diagram.
Ans:- SNMP is an application–layer protocol defined by the Internet Architecture Board (IAB) in RFC1157 for exchanging management information between network devices. It is a part of Transmission Control Protocol⁄ Internet Protocol (TCP⁄IP) protocol suite. SNMP uses a manager/agent architecture/Model. Alarm messages (Traps) are sent by the agent to the manager. SNMP was derived

from its predecessor SGMP (Simple Gateway Management Protocol) Consisting of : a manager, an agent, a database of management information, managed objects and the network protocol. The manager provides the interface between the human network manager and the management system. The agent provides the interface between the manager and the physical device(s) being managed. SNMP defines the format of packets exchanged between a manager and an agent. It reads and changes the status (values) of objects (variables) in SNMP packets.



Q3 Attempt any three (4 marks each)

1. Explain 1)Distance Vector Protocol 2) Link State Protocol.

Ans:- <u>Distance vector Routing Protocol:</u> Current best known cost to reach a destination Idea: exchange vectors among neighbours to learn about lowest cost paths.

Distance vector protocols advertise their routing table to all directly connected neighbours at regular frequent intervals using a lot of bandwidth and are slow to converge.

When a route becomes unavailable, all router tables must be updated with that new information.

The problem is with each router having to advertise that new information to its neighbours, it takes a long time for all routers to have a current accurate view of the network.

Distance vector protocols use fixed length subnet masks which aren't scalable.

<u>Link state Protocol</u>: In link state routing, if each node in the domain has the entire topology of the domain, the node can use Dijkstra's algorithm to build a routing table.

Advertise routing updates only when they occur which uses bandwidth more effectively.

Routers don't advertise the routing table which makes convergence faster.

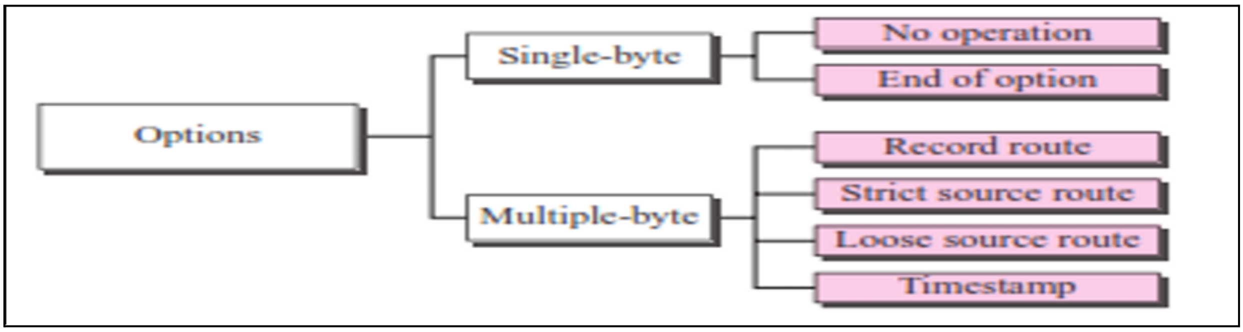
Link state protocols take a different approach to finding the best path in that they share information with other routers in proximity.

The route is calculated based on the speed of the path to the destination and the cost of resources.

One of the key differences to a distance vector protocol is that link state protocols don't send out routing tables; instead, routers notify each other when changes are detected.

2. Enlist types/categories of OPTION.

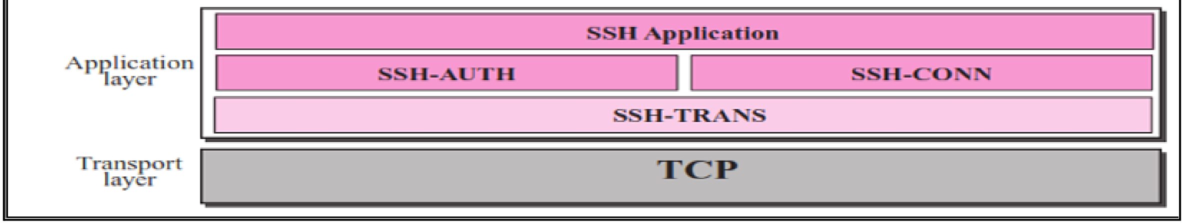
Ans:-



3. Describe components of Secure Shell(SSH).

Ans:-

Figure 20.17 *Components of SSH*



SSH-TRANS: Since TCP is not a secured transport layer protocol, SSH first uses a protocol that creates a secured channel on the top of TCP. This new layer is an independent protocol referred to as SSH-TRANS.

SSH-AUTH: After a secure channel is established between the client and the server and the server is authenticated for the client, SSH can call another software that can authenticate the client for the server.

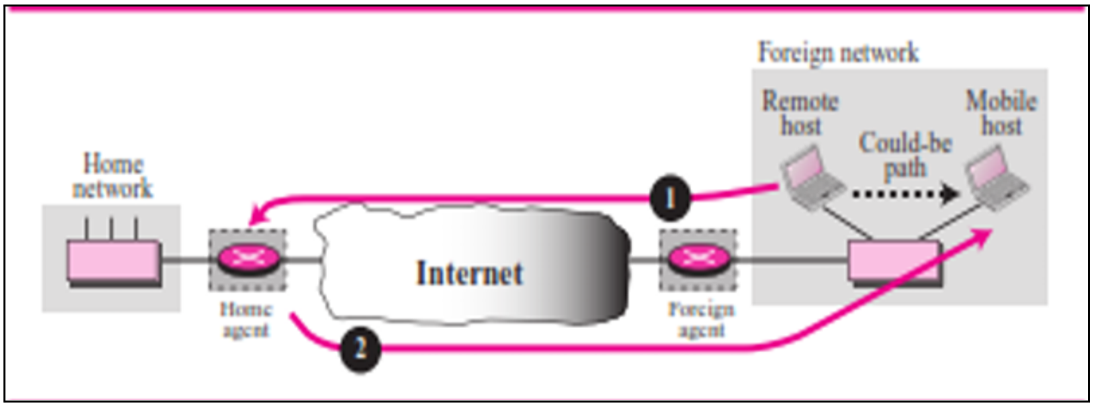
SSH-CONN: After the secured channel is established and both server and client are authenticated for each other, SHH can call a piece of software that implements the third protocol, SSHCONN.

SSH Applications: After the connection phase is completed, SSH allows several application programs to use the connection. Each application can create a logical channel as described above and then benefit from the secured connection.

Port Forwarding: One of the interesting services provided by the SSH protocol is to provide port forwarding. We can use the secured channels available in SSH to access an application program that does not provide security services.

4. Describe any one in detail 1)Triangular Routing 2)Double crossing.

Ans:- Double crossing occurs when a remote host communicates with a mobile host that has moved to the same network (or site) as the remote host.



When the mobile host sends a packet to the remote host, there is no inefficiency; the communication is local. However, when the remote host sends a packet to the mobile host, the packet crosses the Internet twice. Since a computer usually communicates with other local computers (principle of locality), the inefficiency from double crossing is significant.

Q4 Attempt any two (6 marks each)

1. Explain given types of VPN in short: 1) Remote Access VPN 2) Site to Site VPN.
2. Describe duties performed by the transport layer in detail.

Ans:- Packetizing: Packetizing is a process of dividing a long message into smaller ones. These packets are then encapsulated into the data field of the transport layer. The header is added to each packet to allow the transport layer to perform its other functions.

Connection Control: It is further categorised into

Connection oriented delivery: It establishes a connection i.e. virtual path between sender and receiver.

Connectionless delivery: It will treat each packet independently. There is no connection between them. Each packet can take its own different route.

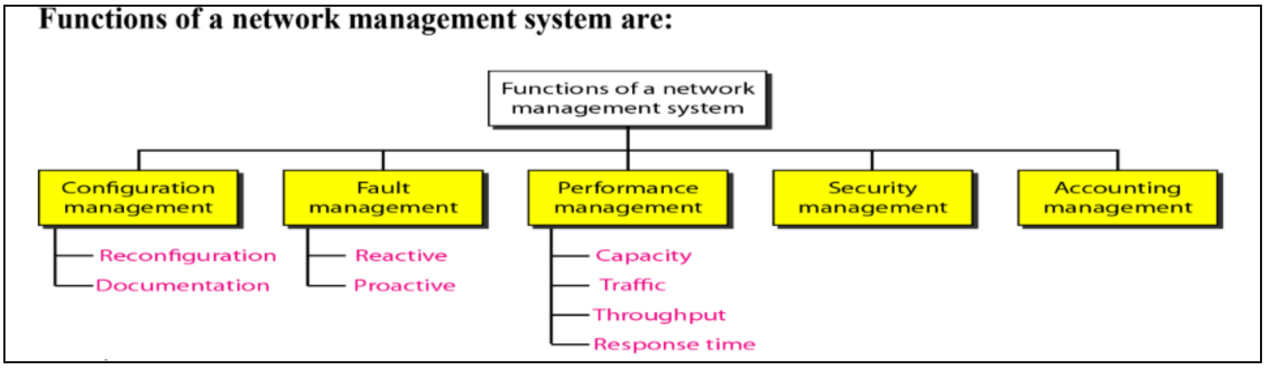
Addressing: The client needs the address of the remote computer it wants to communicate with. Such a remote computer has a unique address so that it can be distinguished from all the other computers.

Flow Control: TCP also provide flow control but this flow control is performed end to end and not across a single link.

Error Control: TCP provide error control as well. Error connection is generally achieved by retransmission of the packets discarded due to errors.

3. State functions of network management systems.

   Ans:-

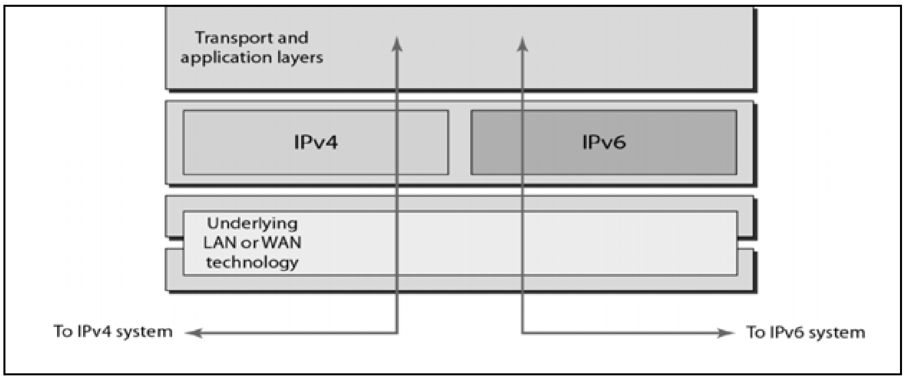


Functions of a network management system are:

Q5 Attempt any two (6 marks each)

1. Explain following strategies of transition with diagram in details

   Ans:- Dual Stack: In this kind of strategy a station has a dual stack of protocols run IPv4 and IPv6 simultaneously. To determine which version to use when sending a packet to a destination, the source host queries the DNS. If the DNS returns an IPv4 address, the source host sends an IPv4 packet. If the DNS returns an IPv6 address, the source host sends an IPv6 packet.

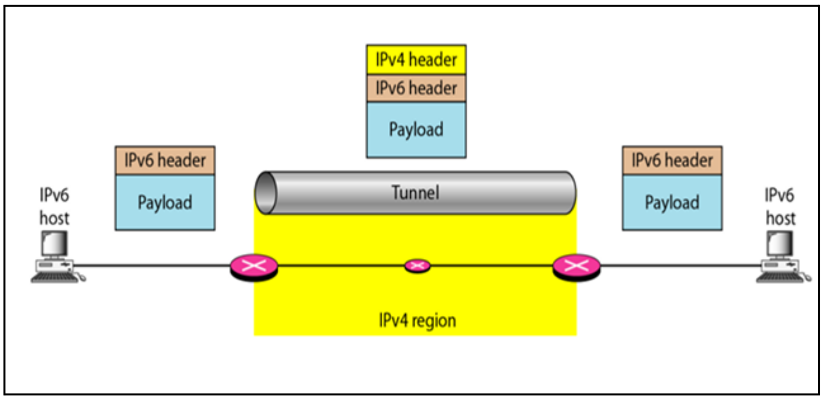


Transport and application layers
IPv4
IPv6
Underlying LAN or WAN technology
To IPv4 system
To IPv6 system

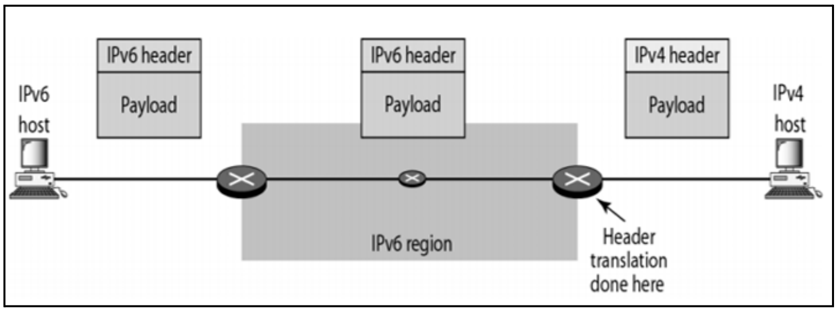
Tunneling: Tunnelling is a strategy used when two computers using IPv6 want to communicate with each other and the packet must pass through a region that uses IPv4.

To pass through this region, the packet must have an IPv4 address. So the IPv6 packet is encapsulated in an IPv4 packet when it enters the region.

To make it clear that the IPv4 packet is carrying an IPv6 packet as data the protocol value is set to 41.



Header Translation: In this case, the header format must be totally changed through header translation. The header of the IPv6 packet is converted to an IPv4 header see figure.



2. State different timers in TCP.

Ans:- **Retransmission Timer** – To retransmit lost segments, TCP uses retransmission timeout (RTO). When TCP sends a segment the timer starts and stops when the acknowledgment is received. If the timer expires timeout occurs and the segment is retransmitted. RTO (retransmission timeout is for 1 RTT) to calculate retransmission timeout we first need to calculate the RTT(round trip time).

Measured RTT(RTTm) – The measured round-trip time for a segment is the time required for the segment to reach the destination and be acknowledged, although the acknowledgement may include other segments.

Persistent Timer – To deal with a zero-window-size deadlock situation, TCP uses a persistence timer. When the sending TCP receives an acknowledgment with a window size of zero, it starts a persistence timer. When the persistence timer goes off, the sending TCP sends a special segment called a probe. This segment contains only 1 byte of new data. It has a sequence number, but its sequence number is never acknowledged; it is even ignored in calculating the sequence number for the rest of the data. The probe causes the receiving TCP to resend the acknowledgment which was lost.

Keep Alive Timer – A keepalive timer is used to prevent a long idle connection between two TCPs. If a client opens a TCP connection to a server transfers some data and becomes silent the client will crash. In this case, the connection remains open forever. So a keepalive timer is used. Each time the server hears from a client, it resets this timer. The time-out is usually 2 hours. If the server does not hear from the client after 2 hours, it sends a probe segment. If there is no response after 10 probes, each of which is 75 s apart, it assumes that the client is down and terminates the connection.

Time Wait Timer – This timer is used during tcp connection termination. The timer starts after sending the last Ack for 2nd FIN and closing the connection.

After a TCP connection is closed, it is possible for datagrams that are still making their way through the network to attempt to access the closed port. The quiet timer is intended to prevent the just-closed port from reopening again quickly and receiving these last datagrams.

3. State need of DNS.

Ans:-Since IP addresses are difficult to remember and names are easier to remember Domain Name System is used and DNS servers are used for converting these names into IP addresses.

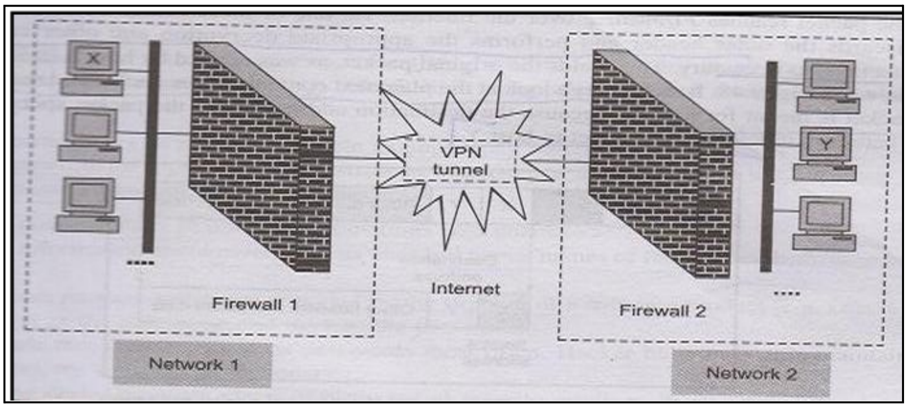
Large number to hosts and servers connected in the internet can be classified using Domain name system so that hierarchical naming system is implemented.

To identify an entity, TCP/IP protocols use the IP address.
An IP is uniquely identifies the connection of a host to internet.
Use for mapping can map a name to an address or an address to a name.

Q6 Attempt any three (4 marks each)

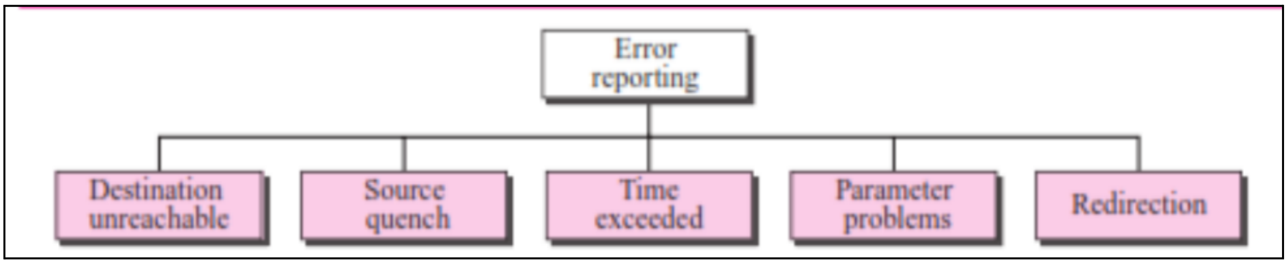
1. Explain Virtual Private Network with proper diagram.

Ans:- Due to internet software, it appears that the internet is a single seamless system of communication to which lots of networks containing a large number of computers are connected.
The internet details of these real or actual networks get hidden when they become a part of the internet.
Every computer connected to the internet has its own unique address assigned to it.
The users of the internet do no have to bother about the internal structure of the physical networks and the details related to them. Thus the user is a part of a virtual network. Internet is thus the best example of virtual network.



2. Explain ICMP messages categories Query, Error reporting with its sub categories in short.

Ans:- **Error Reporting:**



Destination unreachable: When a router cannot route a datagram or a host cannot deliver a datagram, the datagram is discarded and the router or the host sends a destination-unreachable message back to the source host that initiated the datagram.
Source quench: A source quench message informs the source that a datagram has been discarded Due to congestion in a router or the destination host. The source must slow down the sending of Datagrams until the congestion is relieved.
Time exceeded: Whenever a router decrements a datagram with a time to live value to zero, it discards the datagram and sends a time exceeded message to the original source.
When the final destination does not receive all of the fragments in a set time, it discards the received fragments and sends a time exceeded messages to the original source.

Parameter Problems: Any ambiguity in the header part of a datagram can create serious problems as the datagram travels through the Internet. If a router or the destination host discovers an ambiguous or missing value in any field of the datagram, it discards the datagram and sends a Parameter-problem message back to the source.

A parameter-problem message can be created by a router or the destination host.

Redirection: When a router needs to send a packet destined for another network, it must know the IP address of the next appropriate router. The same is true if the sender is a host. Both routers and hosts then must have a routing table to find the address of the router or the next router. Routers take part in the routing update process Routing is dynamic. A host usually starts with a small routing table that is gradually augmented and updated. One of the tools to accomplish this is The redirection message.

Query Messages:-

Echo Request and Reply: The echo-request and echo-reply messages are designed for diagnostic purposes. Network Managers and users utilise this pair of messages to identify network problems. The echo-request and echo-reply messages can be used to determine if there is communication at the IP level. The echo-request and echo-reply messages can also be used by a host to see if another host is Reachable. Echo request, together with echo reply, can determine whether or not a node is functioning properly.

Timestamp Request and Reply: Two machines (hosts or routers) can use the timestamp-request and timestamp-reply messages and to determine the round-trip time needed for an IP datagram to travel between them. It can also be used to synchronise the clocks in two machines. The timestamp request and reply messages can be used to synchronise two clocks in two machine if the exact one way time duration is known.

3. Describe protocols used in transport layer in detail.

Ans:- UDP: UDP is a Transport Layer protocol. UDP is a part of Internet Protocol suite as UDP/IP suite.
Uses a simple connectionless communication model with a minimum of
protocol mechanisms.
One of the core members of the Internet protocol suite.
UDP Protocol no. is 17.
Unlike TCP, it is unreliable and connectionless protocol. So there is no need to establish
connection prior to data transfer.
TCP: TCP as a protocol that is introduced to provide reliable stream delivery service.
TCP Features and compare them with UDP features.
TCP provides a connection-oriented service, and
The segments exchanged during connection establishment and connection termination phases.
It creates a virtual connection between two TCPs to send data.
TCP uses flow and error control mechanisms at the transport level.
The state transition diagram for TCP and discuss some scenarios.
It introduce windows in TCP that are used for flow and error control.

SCTP: SCTP is new transport layer protocol. The multimedia and stream traffic is increasing day by day on the internet. SCTP is a general purpose transport layer protocol which is designed to handle the multimedia and stream traffic.

SCTP is capable of providing the required services with better performance and reliability.

4. Describe the architecture of WWW in short with a diagram.

Ans:- It is a repository of information linked together from points all over the world.

It is a unique combination of :

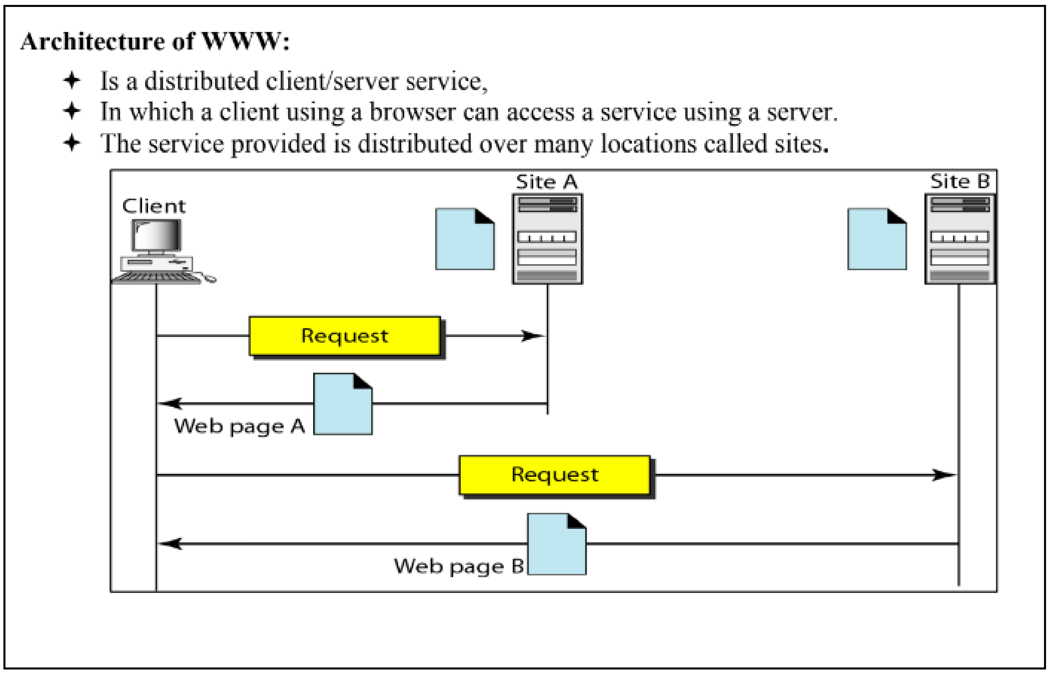
flexibility,

portability, and

user-friendly features that distinguish it from other services provided by the Internet.

It has connected the world in a way that was not possible before and made it much easier for people to get information, share and communicate.

It allowed people to share their work and thoughts through social networking sites, blogs and video sharing. The world wide web made it much easier for people to share information.



Architecture of WWW:

- Is a distributed client/server service,
- In which a client using a browser can access a service using a server.
- The service provided is distributed over many locations called sites.