V2V EDTECH LLP

Online Coaching at an Affordable Price.

OUR SERVICES:

- Diploma in All Branches, All Subjects
- Degree in All Branches, All Subjects
- BSCIT / CS
- Professional Courses

+91 93260 50669

v2vedtech.com

V2V EdTech LLP

v2vedtech

WINTER – 2019 EXAMINATION
MODEL ANSWER

Subject: Advanced Computer Network **Subject Code: 22520**

Important Instructions to examiners:

1) The answers should be examined by key words and not as word-to-word as given in the model answer scheme.
2) The model answer and the answer written by candidate may vary but the examiner may try to assess the understanding level of the candidate.
3) The language errors such as grammatical, spelling errors should not be given more Importance (Not applicable for subject English and Communication Skills).
4) While assessing figures, examiner may give credit for principal components indicated in the figure. The figures drawn by candidate and model answer may vary. The examiner may give credit for any equivalent figure drawn.
5) Credits may be given step wise for numerical problems. In some cases, the assumed constant values may vary and there may be some difference in the candidate's answers and model answer.
6) In case of some questions credit may be given by judgement on part of examiner of relevant answer based on candidate's understanding.
7) For programming language papers, credit may be given to any other program based on equivalent concept.

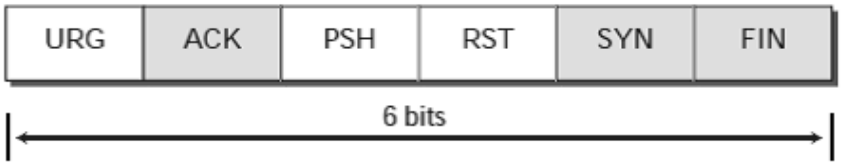
<table>
<tr><th>Q. No.</th><th>Sub Q.N.</th><th>Answer</th><th>Marking Scheme</th></tr>
<tr><td>1.</td><td>(a) Ans.</td><td>Attempt any FIVE of the following:
Differentiate between IPv4 and IPv6. (any two)
<table>
<tr><th>Sr. No.</th><th>IPv4</th><th>IPv6</th></tr>
<tr><td>1</td><td>IPv4 addresses are 32 bits i.e. 4 bytes length</td><td>IPv6 addresses are 128 bits i.e. 16 bytes length</td></tr>
<tr><td>2</td><td>Header length is 20 bytes</td><td>Header length is 40 bytes</td></tr>
<tr><td>3</td><td>Checksum is available in header</td><td>No Checksum in header</td></tr>
<tr><td>4</td><td>IPv4 allows 5 different classes of IP address</td><td>IPv6 allows storing an unlimited of IP address</td></tr>
<tr><td>5</td><td>No packet flow identification</td><td>Packet flow identification is available</td></tr>
<tr><td>6</td><td>Limited addresses</td><td>Larger address space</td></tr>
</table></td><td>10
2M

Any two points 1M each</td></tr>
<tr><td></td><td>(b) Ans.</td><td>State the four advantages of IPv6.</td><td>2M</td></tr>
</table>

WINTER – 2019 EXAMINATION
MODEL ANSWER

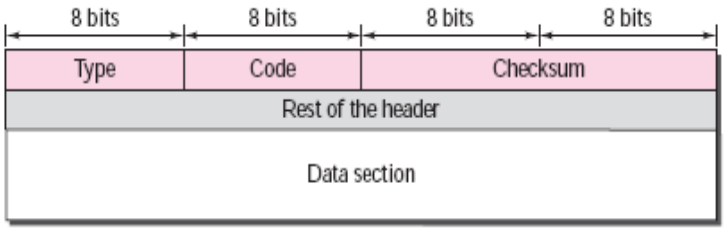
Subject: Advanced Computer Network **Subject Code: 22520**

		Advantages of IPv6: • Larger address space. • Better header format. • New options for additional functionalities. • Allowance for extension. • Support for more security. • More efficient routing • More efficient packet processing • Directed data flows • Simplified Network configuration • Support for new services • Support for Security • Auto configuration	***Any four advantages ½M each***
	(c) Ans.	**State the need of domain name system.** **Need of domain name system:** • 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.	**2M** ***Any one Need 2M***
	(d) Ans.	**State the use of 6 flags in TCP header.** There are 6, 1-bit control bits that control connection establishment, termination, abortion, flow control etc.. URG | ACK | PSH | RST | SYN | FIN 1) URG: Urgent pointer If this bit field is set the receiving TCP should interpret the urgent pointer field. 2) ACK: Acknowledgement If this bit field is set the ACK field described earlier is valid. 3) PSH: Push function Request for push 4) RST: Reset the connection If this bit is present it signals the receiver that sender is aborting the	**2M** ***Correct use 2M***

		connection i.e. Reset the connection. 5) SYN: Synchronize When this bit field in present then the sender is attempting to 'synchronize' sequence numbers 6) FIN: No more data from sender. If this bit is set then it terminates the connection. **OR** URG: Urgent pointer is valid RST: Reset the connection ACK: Acknowledgment is valid SYN: Synchronize sequence numbers PSH: Request for push FIN: Terminate the connection 	
	(e) Ans.	**List two advantages of using UDP over TCP.** **Advantages of using UDP over TCP:** 1) UDP is connection less and unreliable transport layer protocol. i.e. It does not require to maintain a connection. 2) UDP is transaction oriented and suitable for simple query response protocols. 3) UDP is faster since it does not require acknowledgment. 4) Useful when time sensitivity is more important	**2M** ***Any two advantages 1M each***
	(f) Ans.	**State the transmission modes of FTP.** **Transmission modes of FTP:** 1. Stream mode 2. Block mode 3. Compressed mode	**2M** ***Correct modes 2M***
	(g) Ans.	**State the concept of fragmentation in IPv4.** Fragmentation: When the maximum size of datagram is greater than maximum size of data that can be held a frame then the network layer divides the datagram received from x-port layer into fragments. OR Fragmentation is the division of a IP datagram into smaller units. After fragmentation, each fragment will have its own header with few fields changed and few fields remaining same. OR	**2M** ***Fragmentation definition 1M***

		In fragmentation, a datagram is divided into smaller units. Most of the fields of the original header are copied into the fragment header. The three fields Flags, Fragmentation offset and Total length are altered.	***Concept 1M***
2.	**(a) Ans.**	**Attempt any THREE of the following:** **Compare TCP and UDP (any four points).**	**12** **4M** ***Any four points 1M each***

Characteristics	TCP	UDP
Connection	TCP is connection oriented Protocol	UDP is connection less Protocol
Reliability	It provides reliable delivery of messages	It provides unreliable delivery of messages
Error Handling	TCP makes checks for errors and reporting	UDP does error checking but no reporting.
Flow controlling	TCP has flow control	UDP has no flow control
Data transmission order	TCP gives guarantee that the order of the data at the receiving end is the same as the sending end	No guarantee of the data transmission order
Header Size	20 bytes	8 bytes
Acknowledgment	TCP acknowledges the data reception	UDP has no acknowledgment Section
Use	Used where reliability is important	Used where time sensitivity is more important.
Data Interface to application	Stream-based: No particular structure for data	Message based data: Data sent in discrete packages by application
Overhead	Low	Very low
Speed	High	Very high
Application	FTP, Telnet, SMTP, DNS, HTTP, POP	DNS, BOOTP, DHCP, TFTP, RIP

	(b) Ans.	**Explain ICMP protocol. Describe the header format of ICMP.** The Internet Control Message Protocol (ICMP) supports the unreliable and connectionless Internet Protocol (IP). • ICMP messages are encapsulated in IP datagrams. There are two categories of ICMP messages: error-reporting and query messages. 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. • The checksum for ICMP is calculated using both the header and the data fields of the ICMP message. • There are several tools that can be used in the Internet for debugging. We can find if a host or router is alive and running. Two of these tools are ping and traceroute. **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. • The data section in error messages carries information for finding the original packet that had the error. In query messages, the data section carries extra information based on the type of the query.	**4M** ***Explanation 2M*** ***Format 1M*** ***Description 1M***

WINTER – 2019 EXAMINATION
MODEL ANSWER

Subject: Advanced Computer Network **Subject Code: 22520**

	(c) **Ans.**	**Explain working of WWW.** ***(Note: Description explaining the concept shall be considered).*** The Web is a repository of information in which the documents, called **web pages,** are distributed all over the world and related documents are linked together. The WWW today 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.* Each site holds one or more web pages. Each web page can contain some links to other web pages in the same or other sites. • Simple web page has no links to other web pages. • Composite web page has one or more links to other web pages. Each web page is a file with a name and address. The web page is stored at the web server. Each time a request arrives, the corresponding document is sent to the client.	**4M** ***Explanation 4M***
	(d) **Ans.**	**Describe the sub-network address if the destination address is 200.45.34.56 and the subnet mask is 255.255.240.0** To find the subnet address we have to AND the IP address and the subnet mask as shown below: 200.45.34.56 **Destination address:** 11001000 . 00101101 . 00100010.00111000 255.255.240.0 **AND** Subnet mask **11111111 . 11111111 . 1111**0000.00000000 ANDing 200.45.32.0 Subnet address **11001000 . 00101101 . 0010**0000.00000000 Thus subnet address is **200.45.32.0** **OR** To find the subnet address, keep the network bits in the IP address as it is, and make all host bits as 0's.:	**4M** ***Identifying subnet mask/ netid and host id 2M*** ***Correct Answer 2M***

200.45.34.56
Destination address 11001000 . 00101101 . 00100010.00111000

With subnet mask as 255.255.240.0, network bits are **20** and host bits are **12.**
Keeping first 20 bits as it is, and making host bits as 0, the subnet address is obtained as given below.
Subnet address **11001000 . 00101101 . 0010**0000.00000000

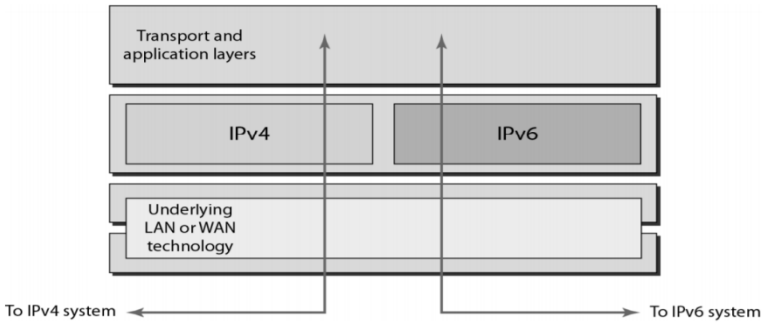
Thus subnet address is **200.45.32.0**

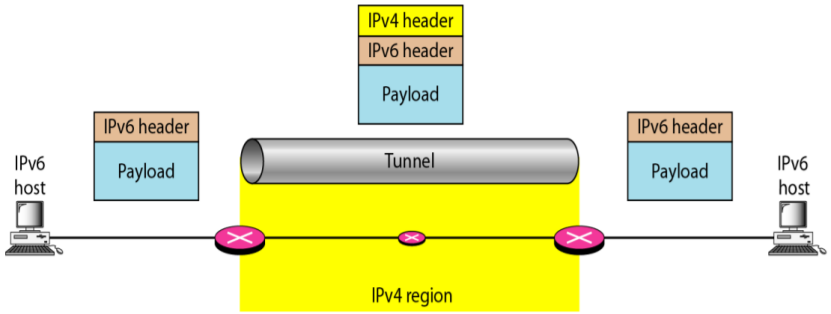
3. **(a)** **Ans.** **Attempt any THREE of the following:** **12**

Explain difference between distance vector and link state routing. (Any four points). **4M**

Sr. No.	Distance Vector Routing	Link State Routing
1	Routing tables are updated by exchanging information with the neighbours.	Complete topology is distributed to every router to update a routing table.
2	It update full routing table.	It updates only link states.
3	It uses Bellman-Ford algorithm	It uses Dijkstra algorithm.
4	Distance Vector routing doesn't have any hierarchical structure.	Link state routing works best for hierarchical routing design.
5	CPU and memory utilization is lower than Link state routing.	Higher utilization of CPU and memory than distance vector routing.
6	Bandwidth required is less due to local sharing, small packets and no flooding.	Bandwidth required is more due to flooding and sending of large link state packets.
7	Example protocols are RIP and IGRP.	Example protocols are OSPF and IS-IS.
8	Slow convergence.	Fast convergence.
9	Summarization is automatic	Summarization is manual.
10	Easier to configure	Harder to configure
11	Count to infinity problem	No count to infinity problem

Any four points 1M each

	(b) Ans.	**Explain different transition method of IPv4 to IPv6.** Three Transition from IPv4 to IPv6 strategies are 1. Dual Stack 2. Tunnelling 3. Header Translation **1. 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.  **Fig. Dual Stack** **2. Tunnelling** 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.	**4M** ***List 1M*** ***1M for each transition method***



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.

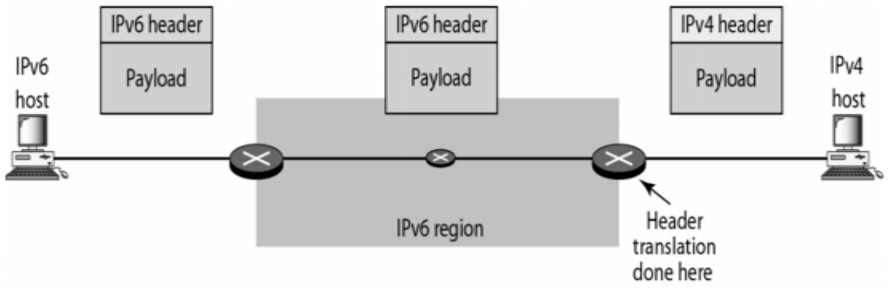
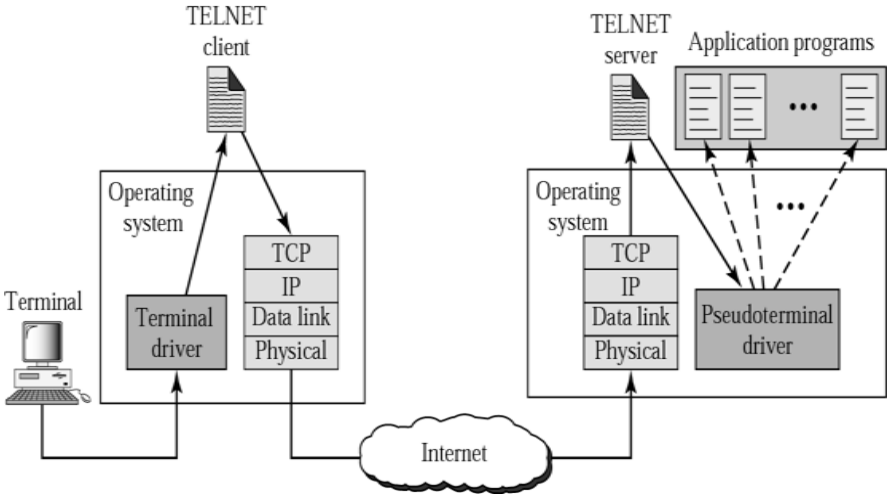
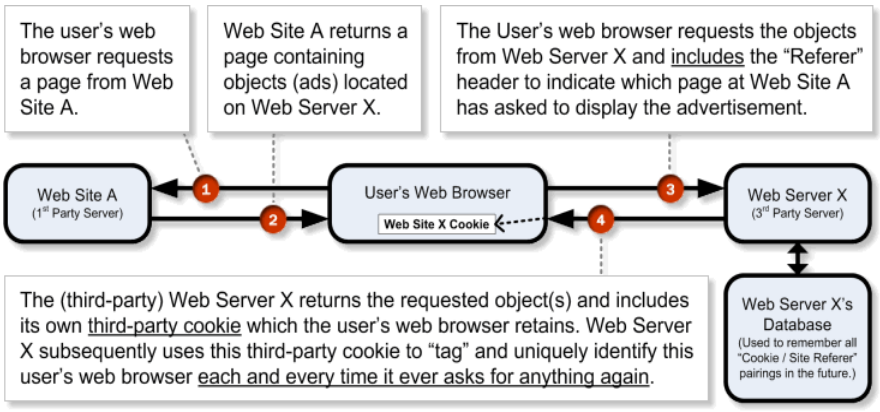
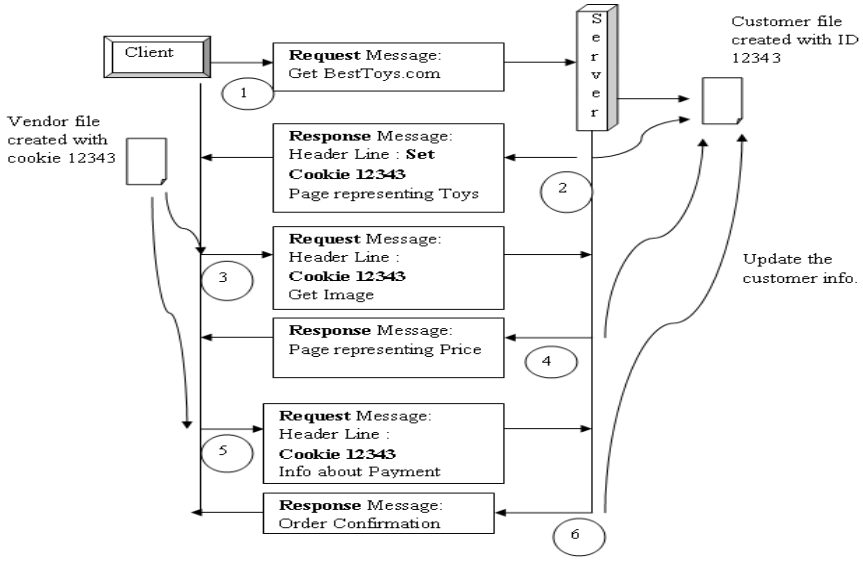


Fig. Header Translation

	(c) Ans.	**Explain the working of TELNET.** **TELNET:** TELNET is an abbreviation for TErminaLNETwork. It is the standard TCP/IP protocol for virtual terminal service. **TELNET Working:** • TELNET is a client-server application that allows a user to log on to a remote machine, giving the user access to the remote system. • The user sends the keystrokes to the terminal driver, where the local operating system accepts the characters but does not interpret them. • A terminal driver correctly interprets the keystrokes on the local terminal or terminal emulator. • The characters are sent to the TELNET client, which transforms	**4M** ***Working descripti on 2M***

		the characters to a universal character set called network virtual terminal (NVT) characters and delivers them to the local TCP/IP protocol stack. • The commands or text, in NVT form, travel through the Internet and arrive at the TCP/IP stack at the remote machine. • Here the characters are delivered to the operating system and passed to the TELNET server, which changes the characters to the corresponding characters understandable by the remote computer. • However, the characters cannot be passed directly to the operating system because the remote operating system is not designed to receive characters from a TELNET server: It is designed to receive characters from a terminal driver. • A piece of software called a pseudo terminal driver is added which pretends that the characters are coming from a terminal. • The operating system then passes the characters to the appropriate application program.  **Fig. Working of TELNET**	***Working diagram 2M***
	(d)	**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**	**4M**

	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 = **$BC82_{16}$ = 48258** ii) Destination port number = **$000D_{16}$= 13** iii) Total length = **$002B_{16}$ = 43 bytes** iv) Since the header is 8 bytes the data length is **43 − 8 =35 bytes**.	***Each correct answer carries 1M***
4.	**(a)** **Ans.**	**Attempt any THREE of the following:** **Construct a diagram to show the application of cookies in a scenario in which the server uses cookies for advertisement.** ***(Note: Any other diagram shall be considered)*** **Use of Cookies for advertisements:** A cookie is also used by advertising agencies. An advertising agency can place banner ads on some main website that is often visited by users. The advertising agency supplies only a URL that gives the banner address instead of the banner itself. When a user visits the main website and clicks on the icon of an advertised corporation, a request is sent to the advertising agency. The advertising agency sends the banner, a GIF file, for example, but it also includes a cookie with the ill of the user. Any future use of the banners adds to the database that profiles the Web behaviour of the user. The advertising agency has compiled the interests of the user and can sell this information to other parties. This use of cookies has made them very controversial. Hopefully, some new regulations will be devised to preserve the privacy of users.  **Fig. Use of Cookies in advertisement** **OR**	**12** **4M** ***Use 1M***

		• Figure below shows a scenario in which an electronic store can benefit from the use of cookies. • A shopper wants to buy a toy from an electronic store named BestToys.com. • The Server sends the Webpage, but it also includes a cookie with the ID 12343. • Using this a file is created such that the information clicked by the user is sent and stored in the file, which are used by the server.  	***Diagram 3M***
	(b) Ans.	**Describe the RIP message format.** **RIP(Routing Information Protocol) message format** • RIP is routing protocol based on Distance Vector Routing algorithm which is an intradomain (interior) routing protocol used inside an autonomous system. • The metric used by RIP is the distance which is defined as the number of links (networks) that have to be used to reach the destination. For this reason, the metric in RIP is called a hop count. • Infinity is defined as 16, which means that any route in an autonomous system using RIP cannot have more than 15 hops. • The next node column defines the address of the router to which the packet is to be sent to reach its destination.	**4M** ***Description 2M***

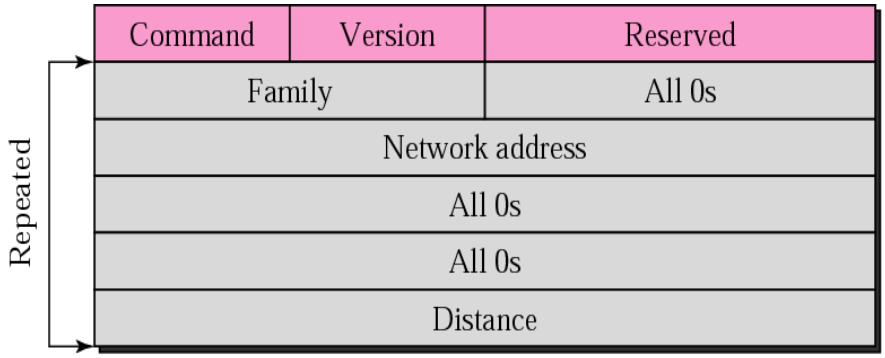


Fig. RIP message format

Message format diagram 2M

- **Command**: 8-bit
  - The type of message: request (1) or response (2)
- **Version:** 8-bit
  - Define the RIP version
- **All 0s**
  - This field is not actually used by RFC 1058 RIP; it was added solely to provide backward compatibility with pre-standard varieties of RIP. Its name comes from its defaulted value, zero.
- **Family:**
  - 16-bit field defines the family of the protocol used. For TCP/IP, value is 2
- **IP Address Network Address:**
  - 14 bytes n Defines the address of the destination network and 14 bytes for this field to be applicable to any protocol. However, IP currently uses only 4 bytes, the rest are all 0s
- **Distance:**
  - 32-bit field defines the hop count from the advertising router to the destination network

(c) **Describe the HTTP response message format.** **4M**

(Note: Any other diagram showing the actual contents of the format shall be considered).

Ans.

Status Line

Status line shows status for the response it indicates response status using a code as well as a status phrase.

The status-Line begins with a protocol version, then status code and status phrase.

Description 2M

E.g: HTTP/1.1 200 OK

Headers

Three types of headers are present HTTP Response message which are as follows.

General Header

The general header gives general information about the message and can be present in both a request and a response.

e.g. Date: Mon, 27 Jul 2009 12:28:53 GMT

Response Header

The response header can be present only in a response message. It specifies the server's configuration and special information about the request.

e.g. Server: Apache/2.2.14 (Win32)

Entity Header

The entity header gives information about the body of the document.

e.g. Content-Length: 88

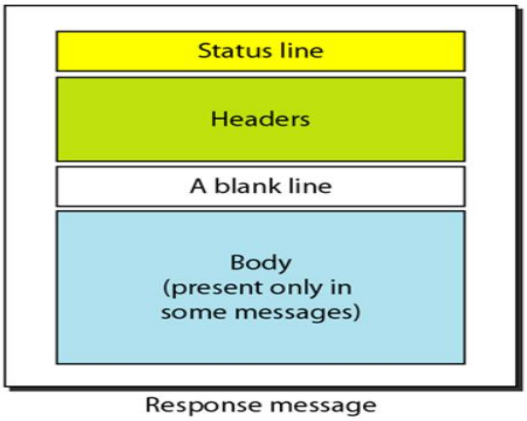
e.g. Content-Type: text/html

Blank Line

An empty line (i.e., a line with nothing preceding the CRLF) indicating the end of the header fields

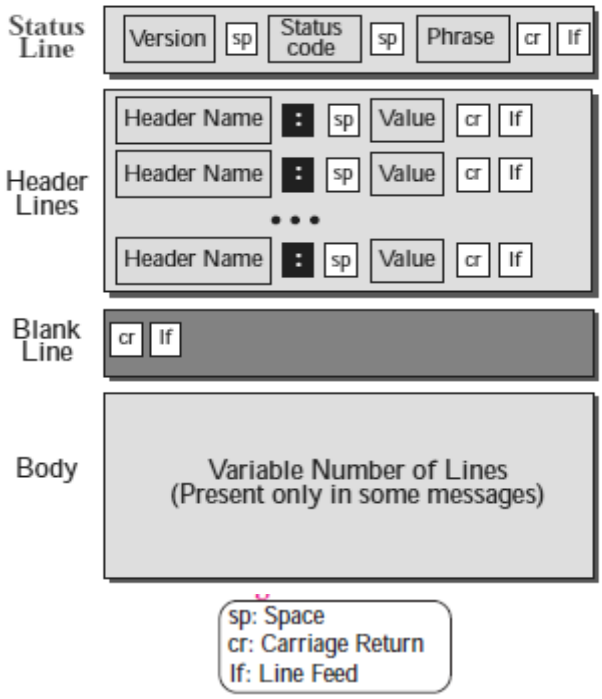
Body

It contains actual content. This part is optional.



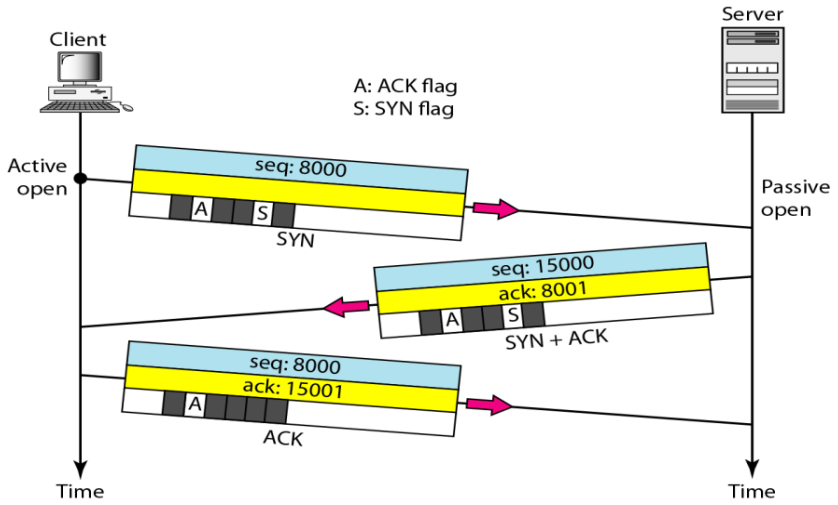
Response message

Diagram 2M

		OR  	
	(d) **Ans.**	**Explain the TCP connection establishment using a three way handshake mechanism.** **Connection Establishment** TCP uses a Three way handshaking mechanism to establish a connection between client and server machines. The three steps in three way handshaking mechanism are as follows. **SYN:** The client sends the first segment, a SYN segment, in which only the SYN flag is set. This segment is for synchronization of sequence numbers. **SYN + ACK** The server sends the second segment, a SYN +ACK segment, with 2 flag bits set. **ACK** The client sends the third segment. This is just an ACK segment. It guarantees the completion of three way handshaking.	**4M** ***Each step description carries 1M***

WINTER – 2019 EXAMINATION
MODEL ANSWER

Subject: Advanced Computer Network **Subject Code: 22520**

		 **Fig. TCP Connection Establishment : Three way Handshaking**	***Diagram 1M***
	(e) **Ans.**	**Explain about standard and non standard protocols at the application layer.** ***(Note: Any other protocol shall be considered).*** **HTTP** • The Hypertext Transfer Protocol (HTTP) is a Application layer protocol used mainly to access data on the World Wide Web. • HTTP uses the services of TCP on well-known port 80. **FTP** • FTP (File Transfer Protocol) is standard TCP/IP protocol to transfer files. • It uses the services of TCP. It needs two TCP connections. • The well-known port 21 is used for the control connection and the well-known port 20 for the data connection. **SMTP** • It stands for Simple Mail Transfer Protocol. It is a part of the TCP/IP standard protocol. • Using a process called "store and forward," SMTP moves your email on and across networks. • It works closely with something called the Mail Transfer Agent (MTA) to send your communication to the right computer and email inbox. • Port number for SMTP is 25.	**4M** ***Any 4 protocol description 1M each***

		TELNET • TELNET is an abbreviation for TErminaLNETwork. It is the standard TCP/IP protocol for virtual terminal service • TELNET enables the establishment of a connection to a remote system in such a way that the local terminal appears to be a terminal at the remote system. • There are two parties involved TELNET Client and TELNET server. **DNS** • It stands for Domain Name Service. Every time you use a domain name, therefore, a DNS service must translate the name into the corresponding IP address. • For example, the domain name www.abc.com might translate to 198.105.232.4. • Port number for DNS is 53. **DHCP** • It stands for Dynamic Host Configuration Protocol (DHCP). It gives IP addresses to hosts. • There is a lot of information a DHCP server can provide to a host when the host is registering for an IP address with the DHCP server. • Port number for DHCP is 67, 68. **POP3** • Post Office Protocol, version 3 (POP3) is simple and limited in functionality. • POP works as a Message Access Agent. • The client POP3 software is installed on the recipient computer; the server POP3 software is installed on the mail server. • Mail access starts with the client when the user needs to download e-mail from the mailbox on the mail server.	
5.		**Attempt any TWO of the following:**	**12**
	(a)	**Explain how TCP connections are established using the 3 way handshake. What happens when 2 hosts simultaneously try to establish a connection?** ***(Note: Any other explanation of the concept shall be considered).***	**6M**
	Ans.		

Connection Establishment

TCP uses a Three way handshaking mechanism to establish a connection between client and server machines.

The three steps in three way handshaking mechanism are as follows.

SYN:

The client sends the first segment, a SYN segment, in which only the SYN flag is set. This segment is for synchronization of sequence numbers.

SYN + ACK

The server sends the second segment, a SYN +ACK segment, with 2 flag bits set.

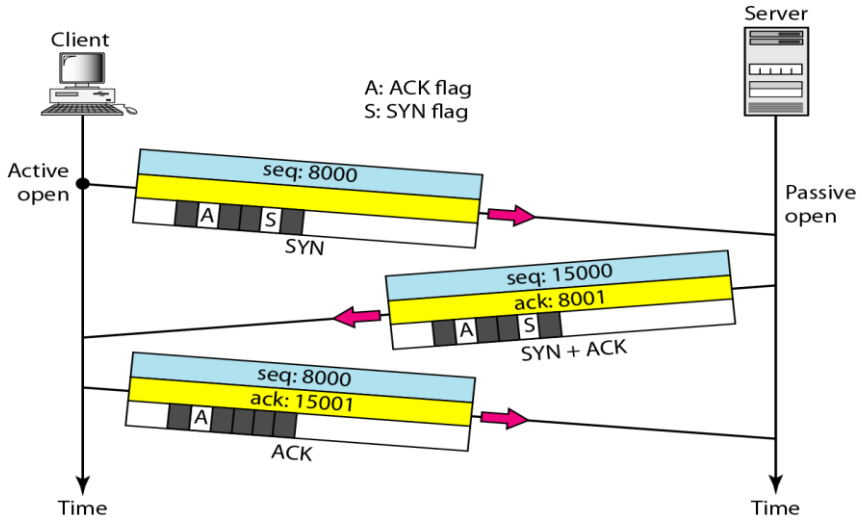
ACK

The client sends the third segment. This is just an ACK segment. It guarantees the completion of three way handshaking.

1M Diagram

3M Steps

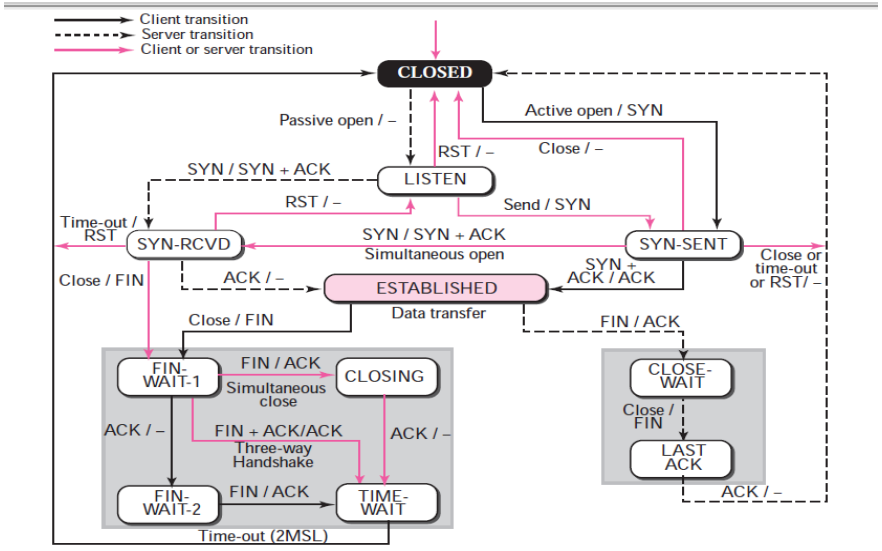
2M for simultaneous connection



If 2 host Simultaneously try to establish connection:

Simultaneous Open:

- It's possible for two applications to send a SYN to each other to start a TCP connection, although the possibility is small, because both sides have to know which port on the other side to send to. This process is called "Simultaneous Open", or "simultaneous active open on both sides".
- In a simultaneous open, both applications issue active opens.
- This is a rare situation in which there is no client or server;

		communication is between two peers that know their local port numbers. • Both TCPs go through **SYN-SENT** and **SYN-RCVD** states before going to the **ESTABLISHED** state. • Both processes act as client and server. • The two SYN+ACK segments acknowledge the SYN segments and open the connection. **OR** **Simultaneous Close:** • It's permitted in TCP for both sides to do "active close", which is called "Simultaneous Close". During "Simultaneous Close", 4 packets are exchanged, the same as in normal situations. • In this situation, both ends issue an active close. • Both TCPs go to the FIN-WAIT-1 state and send FIN segments that are in transit simultaneously. • After receiving the FIN segment, each end goes to the CLOSING state and sends an ACK segment. • The CLOSING state takes the place of FIN-WAIT-2 or CLOSE-WAIT in a common scenario.	
	(b) **Ans.**	**Explain TCP connection management with the help of TCP connection management finite state machine.** ***(Note: Any other explanation of the concept shall be considered).***  	**6M** ***3M for diagram***

To keep track of all the different events happening during connection establishment, connection termination, and data transfer, TCP is specified as the **Finite State Machine –FSM**

TCP State Machine:

- TCP uses a three way handshake to close connection
- Singled by the FIN bit in the packet header

The figure shows the two FSMs used by the TCP client and server combined in one diagram.

- Ovals/rectangle represents states.
- Transition from one state to another is shown using directed lines.
- Each line has two strings separated by a slash.
- The first string is the input, what TCP receives.
- The second is the output, what TCP sends.
- The dotted black lines in the figure represent the transition that a server normally goes through;
- The solid black lines show the transitions that a client normally goes through.
- Sometimes in some situations, a server transitions through a solid line or a client transitions through a dotted line.

State	*Description*
CLOSED	No connection exists
LI STEN	Passive open received; waiting for SYN
SYN- SENT	SYN sent; waiting for ACK
SYN- RCVD	SYN+ACK sent; waiting for ACK
ESTABLI SHED	Connection established; data transfer in progress
FI N- WAI T- 1	First FIN sent; waiting for ACK
FI N- WAI T- 2	ACK to rst FIN received; waiting for second FIN
CLOSE- WAI T	First FIN received, ACK sent; waiting for application to close
TI ME- WAI T	Second FIN received, ACK sent; waiting for 2MSL time-out
LAST- ACK	Second FIN sent; waiting for ACK
CLOSI NG	Both sides decided to close simultaneously

3M for explanation of steps

(c) **Explain the addressing scheme in IPv4 and IPv6. When IPv6 protocol is introduced, does the ARP protocol have to be changed? Explain in details.** **6M**

Ans.

An IPv4 Address:

- ✓ An IP address is a 32-bit address.
- ✓ The IP addresses are unique.

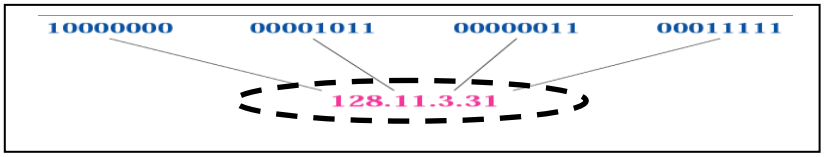
IPv4 2M

Address space rule

- ✓ The address space in a protocol That uses N-bits to define an Address is = 2^N
- ✓ ***The address space of IPv4 is 2^{32}or4,294,967,296.***

Address Space Notations:

- **Binary Notation :**
  01110101 10010101 00011101 11101010
- **Dotted-decimal notation**



Dotted-decimal notation

- **Hexadecimal Notation**

0111 0101	1001 0101	0001 1101	1110 1010
75	95	1D	EA

Hexadecimal Notation

10000001	00001011	00001011	11101111
129.11.11.239			

IPv6 2M

Example of Dotted-decimal Notation.

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 >>> ::

ARP 2M

		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 • $3.4 * 10^{38}$ possible addressable nodes • $5 * 10^{28}$ addresses per person	
6.	**(a)** **Ans.**	**Attempt any TWO of the following:** **Explain the 3 intra domain routing protocols.** ***(Note: Explanation of any other protocols shall be considered).*** **i) Distance Vector Routing:** - Require only local state (less overhead smaller footprint) - Harder to debug - Can suffer from loops • Distance vector Routing Protocol: • Here Distance vector: ✓ Current best known cost to reach a destination ✓ Idea: exchange vectors among neighbors to learn about lowest cost paths. ✓ **Distance vector protocols** advertise their routing table to all directly connected neighbors 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 neighbors, 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. - periodically (on the order of several seconds to minutes) - whenever table changes (called triggered update) • Each update is a list of pairs: - (Destination , Cost) • Update local table if receive a "better" route - smaller cost - from newly connected/available neighbor	**12** **6M** ***Any 3 protocols 2M each***

		• Refresh existing routes; delete if they time out i.e. RIP-Routing Information Protocol **ii) Link State Routing:** - Have a global view of the network - Simpler to debug - Require global state **Link State Strategy** - each router shares the information/knowledge of its neighborhood with every other router in the internetwork. - Send to all nodes (not just neighbors) - Send only information about directly connected links not entire routing table) **Link State Packet (LSP)** - ID of the node that created the LSP - Cost of link to each directly connected neighbor - Sequence number (SEQNO) Time-to-live (TTL) for this packet **i.e. OSPF-Open Shortest Path First** **iii) RIPv2:** _ Runs over UDP port 520 _ Limits networks to 15 hops (16 = 1) _ Depends on count to infinity for loops _ Supports split horizon, poison reverse _ RFC 1812 specifies what options routers should or must have. **iv) MOSPF *(*Multicast Open Shortest Path First):** • This protocol is an extension of the OSPF protocol that uses multicast link state routing to create source-based trees. • The protocol requires a new link state update packet to associate the unicast address of a host with the group address or addresses the host is sponsoring. This packet is called the group membership LSA. In this way, we can include in the tree only the hosts (using their unicast addresses) that belong to a particular group. • Thus a tree that contains all the hosts belonging to a group, but we use the unicast address of the host in the calculation. • For efficiency, the router calculates the shortest path trees on	

demand (when it receives the first multicast packet).

- In addition, the tree can be saved in cache memory for future use by the same source/group pair.
- MOSPF is a **data-driven** protocol; the first time an MOSPF router sees a datagram with a given source and group address, the router constructs the Dijkstra shortest path tree.

v) Multicast Distance Vector Routing (DVMRP):

The **Distance Vector Multicast Routing Protocol (DVMRP)** is an implementation of multicast distance vector routing. It is a source-based routing protocol, based on RIP.

- Unicast distance vector routing is very simple; extending it to support multicast routing is complicated.
- Multicast routing does not allow a router to send its routing table to its neighbors.
- The idea is to create a table from scratch using the information from the unicast distance vector tables.
- Multicast distance vector routing uses source-based trees, but the router never actually makes a routing table.
- When a router receives a multicast packet, it forwards the packet as though it is consulting a routing table.
- After its use (after a packet is forwarded) the table is destroyed.
- To accomplish this, the multicast distance vector algorithm uses a process based on four decision-making strategies.

vi) PIM-DM (Protocol Independent Multicast, Dense Mode):

- PIM-DM is used when there is a possibility that each router is involved in multicasting (dense mode).
- In this environment, the use of a protocol that broadcasts the packet is justified because almost all routers are involved in the process.
- PIM-DM is a source-based tree routing protocol that uses RPF and pruning/grafting strategies for multicasting.
- Its operation is like DVMRP; however, unlike DVMRP, it does not depend on a specific unicasting protocol.
- It assumes that the autonomous system is using a unicast protocol and each router has a table that can find the outgoing

		interface that has an optimal path to a destination. • This unicast protocol can be a distance vector protocol (RIP) or link state protocol (OSPF).	
	(b) **Ans.**	**Describe modern computer use dynamic routing. Explain with example how distance vector routing is used to route the packet & why count-to-infinity problem arises and how does it get solved?** ***(Note: Any other description of the concept shall be considered.)*** **Dynamic routing** uses a dynamic routing protocol to automatically select the best route to put into the routing table. So instead of manually entering static routes in the routing table, dynamic routing automatically receives routing updates, and dynamically decides which routes are best to go into the routing table. This intelligent and hands-off approach that makes dynamic routing so useful in modern era. Dynamic routing protocols vary in many ways and this is reflected in the various administrative distances assigned to routes learned from dynamic routing. These variations take into account differences in reliability, speed of convergence, and other similar factors. **Distance vector routing:** 1. Distance Vector Routing is one of the dynamic routing algorithm. 2. It is suitable for packet switched network. 3. In distance vector routing, each router maintains a routing table. 4. It contains one entry for each router in the subnet. 5. This entry has two parts: a. The first part shows the preferred outgoing line to be used to reach the destination. b. Second part gives an estimate of the time or distance to the destination. In distance vector routing, a node tells its neighbor about its distance to every other node in the network. **Count to infinity problem:** 1. One of the important **issue** in Distance Vector **Routing** is Count to **Infinity Problem**. 2. **Count to infinity** is just another name for a **routing** loop. 3. In distance vector **routing**, **routing** loops usually occur when an	**6M** ***2M for Dynamic routing concept*** ***2M for Distance vector routing and*** ***1M for Count to infinity problem***

interface goes down.

4. It can also occur when two **routers** send updates to each other at the same time.

1M for solution

OR

For a routing protocol to work properly, if a link is broken (cost becomes infinity), every other router should be aware of it immediately, but in distance vector routing, this takes some time.

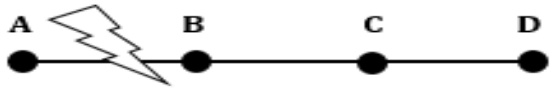
The problem is referred to as **count to infinity.** It takes several updates before the cost for a broken link is recorded as infinity by all routers.

Count to infinity problem can be solved by following methods:

1. Defining Infinity
2. Split Horizon
3. Split Horizon an Poison Reverse

Example:

Link Between A & B is Broken



	A	B	C	D
A	0, -	1, A	2, B	3, C
B	1, B	0, -	2, C	3, D
C	2, B	1, C	0, -	1, C
D	3, B	2, C	1, D	0, -

Imagine a network with a graph as shown above in figure 4.8.

- As you see in this graph, there is only one link between A and the other parts of the network.
- Now imagine that the link between A and B is cut.
- At this time, B corrects its table.
- After a specific amount of time, routers exchange their tables, and so B receives C's routing table.
- Since C doesn't know what has happened to the link between A and B, it says that it has a link to A with the weight of 2 (1 for C to B, and 1 for B to A -- it doesn't know B has no link to A).
- B receives this table and thinks there is a separate link between

C and A, so it corrects its table and changes infinity to 3 (1 for B to C, and 2 for C to A, as C said).

- Once again, routers exchange their tables.
- When C receives B's routing table, it sees that B has changed the weight of its link to A from 1 to 3, so C updates its table and changes the weight of the link to A to 4 (1 for C to B, and 3 for B to A, as B said).
- This process loops until all nodes find out that the weight of link to A is infinity.
- This situation is shown in the table below
- In this way, Distance Vector Algorithms have a slow convergence rate.
- One way to solve this problem is for routers to send information only to the neighbors that are not exclusive links to the destination.

	B	C	D
Sum of Weight to A after link cut	∞, A	2, B	3, C
Sum of Weight to A after 1st updating	3, C	2, B	3, C
Sum of Weight to A after 2nd updating	3, C	4, B	3, C
Sum of Weight to A after 3rd updating	5, C	4, B	5, C
Sum of Weight to A after 4th updating	5, C	6, B	5, C
Sum of Weight to A after 5th updating	7, C	6, B	7, C
Sum of Weight to A after nth updating	.....	....	....
∞	∞	∞	∞

(c) **Describe E-mail security over non-secure channel.** **6M**

(Note: Any other explanation on email security shall be considered.)

Ans.

- Email security describes different techniques for keeping sensitive information in email communication and accounts secure against unauthorized access, loss or compromise.

		• Email is often used to spread malware, spam and phishing attacks. Attackers use deceptive messages to entice recipients to part with sensitive information, open attachments or click on hyperlinks that install malware on the victim's device. • Email encryption involves encrypting, or disguising, the content of email messages to protect potentially sensitive information from being read by anyone other than intended recipients. Email encryption often includes authentication. • Email allows attackers to use it as a way to cause problems in attempt to profit. Whether through spam campaigns, malware and phishing attacks, sophisticated targeted attacks, or business email compromise (BEC), attackers try to take advantage of the lack of security of email to carry out their actions. • Since most organizations rely on email to do business, attackers exploit email in an attempt to steal sensitive information. • Because email is an open format, it can be viewed by anyone who can intercept it. It can be easily read and the contents of an email by intercepting it. • Email Security Policies can be established by viewing the contents of emails flowing through their email servers. It's important to understand what is in the entire email in order to act appropriately. After these baseline policies are put into effect, an organization can enact various security policies on those emails. • These email security policies can be as simple as removing all executable content from emails to more in-depth actions, like sending suspicious content to a sandboxing tool for detailed analysis. • If security incidents are detected by these policies, the organization needs to have actionable intelligence about the scope of the attack. • Enforce email encryption policies to prevent sensitive email information from falling into the wrong hands. • An email gateway scans and processes all incoming and outgoing email and makes sure that threats are not allowed in. Because attacks are increasingly sophisticated, standard security measures, such as blocking known bad file attachments, are no longer effective.	***Any 6 points 1M each***

		• Deploy a secure email gateway that uses a multi-layered approach. • It's also important to deploy an automated email encryption solution as a best practice. This solution should be able to analyze all outbound email traffic to determine whether the material is sensitive. • If the content is sensitive, it needs to be encrypted before it is emailed to the intended recipient. This will prevent attackers from viewing emails, even if they were to intercept them. • The Pretty Good Privacy (PGP) provides e-mail with privacy, integrity, and authentication can be used over non secure channel such as internet. It is used for signing, encrypting and decrypting texts, e-mails, files, directories and whole disk partitions and to increase the security of e-mail communications. • Another security service designed for electronic mail is Secure/Multipurpose Internet Mail Extension (S/MIME). The protocol is an enhancement of the Multipurpose Internet Mail Extension (MIME) protocol. This allows user to digitally sign the email to enhance privacy and data security.	