TYPICAL QUESTIONS & ANSWERS

OBJECTIVE TYPE QUESTIONS

Each Question carries 2 marks.

Choose the correct or best alternative in the following:

Q.1   A header in CGI script can specify

   (A) format of the document.   **(B)** new location of the document.
   (C) (A) & (B) both.   **(D)** start of the document.

Ans: **A**
            A header in CGI script can specify- Format of the document & New location
            of the document.

Q.2   All exceptions in Java are subclasses of built in class called

   (A) Exception   **(B)** Error.
   (C) Throwable.   **(D)** Raise.

Ans: **C**
            All exception in Java are subclasses of built in class called Throwable.

Q.3   In 32bit IP Addressing scheme all 1's represent

   (A) this computer.   **(B)** directed broadcast.
   (C) limited broadcast.   **(D)** loop back.

Ans: **C**
            In 32 bit IP Addressing scheme all 1's represent limited broadcast.

Q.4   DMSP stands for

   (A)   Distributed Mail System Protocol
   (B)   Distributed Message System Protocol
   (C)   Distributed Message System Pool
   (D)   Distributed Mail System Pool

Ans: **A**
            DMSP stands for – Distributed Mail system Protocol.

Q.5   Which Layer is not present in TCP/IP model?

(A) Application Layer   (B) Internet Layer
(C) Transport Layer   (D) Presentation Layer

Ans: **D**
Presentation layer is not present in TCP/IP Model.

Q.6   Let most segment of a name inn DNS represents

(A) Individual Network.   (B) Individual computer.
(C) Domain name   (D) Network type.

Ans: **B**
Left Most segment of a name in DNS represents- Individual computer

Q.7   Address 192.5.48.3 belongs to

(A) class A.   (B) class B.
(C) class C.   (D) class D.

Ans: **C**
Address 192.5.48.3 belongs to class C.

Q.8   Unlike Ipv4, Ipv6 does not include the following field in thee base header

(A) Next Header field.   (B) Field for Fragmentation information
(B) Flow Label.   (D) Kind field.

Ans: **B**
Unlike Ipv4, Ipv6 does not include the Field for Fragmentation information
in the base header.

Q.9   The term byte stuffing refers to:

(A) data stuffing used with character oriented hardware.
(B) data stuffing used with bit oriented hardware.
(C) data stuffing used with both (A) & (B)
(D) data stuffing used with byte oriented hardware.

Ans: **A**
The term byte stuffing refers to data stuffing used with character-oriented
hardware.

Q.10   FDDI (Fiber Distributed Data Interconnect) is an example of

(A) token ring.   **(B)** token bus
(C) star topology   **(D)** multipoint network.

Ans: **A**
        FDDI is an example of token ring.

Q.11   Hardware that calculates CRC(Cyclic Redundancy Check) uses:

(A) Shift register   **(B)** Xor unit
(C) Both (A) & (B)   **(D)** Instruction register

Ans: **B**
        Hardware that calculates CRC uses shift register and Xor unit.

Q.12   In TCP protocol header "checksum" is of_____

(A) 8 bits   **(B)** 16 bits
(C) 32 bits   **(D)** 64 bis

Ans: **B**
        In TCP protocol header checksum is of 16 bits.

Q.13   In IP addressing scheme, class used for multicasting is:

(A) Class A   **(B)** Class B
(C) Class C   **(D)** Class D

Ans: **D**
        In IP addressing scheme, class used for multicasting is class D.

Q.14   CIDR stands for

(A) Classified Internet Domain Routing
(B) Classless Inter Domain Routing
(C) Classless Internet Domain Routing
(D) Classified Inter Domain Routing

Ans: **B**
        CIDR stands for Classless Inter Domain Routing.

Q.15   The total number of class of IP address are

(A) 3.   (B) 4.
(C) 5.   (D) 9.

Ans: **C**
The total number of class of IP addresses are 5.

Q.16   Parent class of all Java classes is

(A) java.lang.system   (B) java.lang.object
(C) java.lang.class   (D) java.lang.reflect.object

Ans: **B**
Parent class of all Java classes is java.lang.object.

Q.17   Exceptions of type error inn JAVA are handled by

(A) User program   (B) Java run time environment
(C) Operating system kerne   (D) Interrupt

Ans: **B**
Exceptions of type error in JAVA are handled by JAVA run time environment.

Q.18   Error detecting method that can detect more errors without increasing additional information in each packet is

(A) checksum   (B) even parity mechanism
(C) CRC   (D) odd parity mechanism.

Ans: **C**
Error detecting method that can detect more errors without increasing additional information in each packet is CRC.

Q.19   A Network uses a star topology if

(A) Computers are arranged in a closed loop.
(B) All computers attach to a central point.
(C) All computers attach to a single long cable.
(D) Computers attach to multiple hierarchical cables.

Ans: **B**
A Network uses a star topology if all computers attach to a central point.

Q.20   MTU is specified by

(A) IP Datagram size   **(B)** Hardware technology
(C) TCP Segment size   **(D)** None of the above.

Ans: **B**
MTU is specified by hardware technology.

Q.21   Network address prefixed by 1110 is a

(A) Class A address   **(B)** Multicast address
(C) Class B address   **(D)** Reserve address.

Ans: **B**
Network address prefixed by 1110 is a multicast address.

Q.22   FTP does not use

(A) Two transfer mode.
(B) Control connection to remote computer before file can be transferred.
(C) User Datagram Protocol.
(D) Authorization of a user through login and password verification.

Ans: **C**
FTP does not use User Datagram Protocol.

Q.23   A Header in CGI document can represent

(A) format of the document
(B) location if document used to different URL
(C) both (A) & (B)
(D) None of the above.

Ans: **B**
A header in CGI document can represent format of the document and the location if document used to different URL.

Q.24   127.0.0.1 is a

(A) limited broadcast address   **(B)** direct broadcast address
(C) multicast address   **(D)** loop-back address

Ans: **D**
127.0.0.1 is a loop-back address.

Q.25   In cyclic redundancy checking CRC is the

   (A) divisor   **(B)** quotient.
   (C) dividend   **(D)** remainder.

Ans: **D**
   In cyclic redundancy checking CRC is the remainder.

Q.26   Which one of the following uses the greatest number of layers in the OSI model?

   (A) Bridge   **(B)** Repeater.
   (C) Router.   **(D)** Gateway.

Ans: **D**
   Gateway uses the greatest number of layers in the OSI model.

Q.27   Which of the following 802 standard provides for a collision free protocol?

   (A) 802.2   **(B)** 802.3
   (C) 802.5   **(D)** 802.6

Ans: **C**
   802.5 standards provides for a collision free protocol.

Q.28   The addressing especially used by Transport Layer is

   (A) Station address   **(B)** Network address
   (B) Application port address   **(D)** Dialog address

Ans: **B**
   The addressing specially used by transport layer is application port address.

Q.29   Which one of thee following is an error reporting protocol?

   (A) ARP   **(B)** ICMP
   (C) TCP   **(D)** UDP

Ans: **B**
   ICMP is an error reporting protocol.

Q.30 Which type of web document is run at the client site

(A) Static   (B) Dynamic
(C) Active   (D) All of the above

Ans: **C**
Active web document is run at client side.

Q.31 The main function of a browser is to

(A) compile HTML   (B) interpret HTML
(C) de-compile HTML   (D) interpret CGI programs

Ans: **B**
The main function of a browser is to interpret HTML.

Q.32 Which of the following is associated with SNMP

(A) SMI   (B) BER
(C) DNS   (D) MIB

Ans: **D**
MIB is associated with SNMP.

Q.33 ATM is an example of

(A) Ring topology   (B) Star topology
(C) Bus topology   (D) None of the above.

Ans: **B**   Star topology

Q.34 The first part of the address in electronic mailbox identifies:

(A) User's mailbox   (B) Computer on which mail box resides
(C) Both (A) & (B)   (D) None of the above

Ans: **A**   User's mailnbox.

Q.35 Protocol used to monitor and control network devices operates at:

(A) Application layer   (B) Transport layer
(C) Network layer   (D) Data Link layer

Ans: **A**   Application layer.

Q.36   DHCP stands for

   (A) Dynamic Host Control Protocol
   (B) Dynamic Host Configuration Protocol.
   (C) Dynamic Host Connection Protocol.
   (D) None of the above.

Ans: **B**   Dynamic Host Configuration Protocol.

Q.37   The transport protocol used by TFTP (Trivial File Transfer Protocol) is:

   (A) FTP   **(B)** UDP
   (C) TCP   **(D)** IP

Ans: **B**   UDP.

Q.38   The Environment variable SCRIPT_NAME in CGI script specifies:

   (A) Domain name of the computer running o server
   (B) The path of URL after server name.
   (C) Name of the server
   (D) None of the above.

Ans: **B**   The path of URL after server name.

Q.39   Application layer (layer 4) in TCP/IP model corresponds to:

   (A) Layer 4 and 5 in OSI model   **(B)** Layer 5 and 6 in OSI model
   (C) Layer 6 and 7 in OSI model   **(D)** Layer 1 and 2 in OSI model

Ans: **C**   Layer 6 and 7 in OSI model.

Q.40   UDP (User Diagram Protocol) is

   (A) Connectionless   **(B)** Message Oriented
   (C) Connection oriented   **(D)** Both (A) and (B)

Ans: **D**   Both (A) and (B).

Q.41   A network address prefixed by 1000 is:

   (A) Class A address   **(B)** Class B address
   (C) Class C address   **(D)** Class D address

Ans: **B**   Class B address.

Q.42   In Java System.out is an object of type

       (A) InputStream   **(B)** PrintStream
       (C) OutputStream   **(D)** None of the above.

Ans: **B**   PrintStream.

DESCRIPTIVE TYPE QUESTIONS

Q.1 What are the various parameters inside Applet tag in a HTML file?   **(6)**

Ans:

```
<APPLET
    [CODEBASE= codebaseURL]
        CODE=applet file
        [ALT=alternate text]
        [NAME=applet instance name]
         WIDTH=pixels HEIGHT= pixels
        [ALIGN = alignment]
        [VSPACE= pixels][HSPACE = pixels]
    >
    [<PARAM NAME = Attribute name VALUE = Attribute value>]
    ……
</APPLET>
```

CODE BASE
Optional attribute used to specify the base URL of the applet code, which is the Directory that will be searched for applet's executable class file. If the applet Resides in the same directory as HTML file then this attribute is not required.

CODE
This is the requirement attribute used to specify the name of the applet class to be loaded (name of the already compiled. class file).

ALT
Optional attribute used to specify a short text message that should be displayed If browser understands the APPLET tag but can not currently run Java applets.

NAME
Optional attribute used to specify a name for applet instance so that the other applets on the page may refer to this applet.

ALIGN
Optional attribute used for alignment (LEFT, RIGHT, TOP, BOTTOM, MIDDLE)

VSPACE & HSPACE
VSPACE specifies space in pixels above and HSPACE in pixels on each side of applet.

WIDTH & HEIGHT
Required attributes that give the size of display area in pixels.

PARAM NAME & NULL
The PARAM tag allows you to specify applet specific arguments in an HTML page.

Q.2 Write an applet which accepts two integers from the user and displays their sum in the following format. **(8)**

3		2

Input a number in each box:

The sum is : 5

Ans:

```
import java .awt.*;
    import java. Applet.*;
    public class sum extends Applet
     {
            TextField text1,text2;
            Public void init()
            {
                    text1 = new TextField(8);
                    text2 = new TextField(8);
                    add(text1);
                    add(text2);
                    text1.setText ("0");
                    text2.setText ("0");
            }
        public void paint (Graphics g)
            {int x = 0, y= 0, z = 0;
              String s1, s2,s;
              g.drawstring("Input a number in each box",10,50);
              s1 = text1.getText();
              x = Integer.parseInt(s1);
              s2 = text2.getText();
              y = Integer.parseInt(s2);
              z = x+y;
```

```
                    s = String.valueOf(z);
                    g.drawString("The sum is :",10,75);
                    g.drawString(s,100,75);
                    }
            }
```

Q.3 What are the main differences between OSI and TCP/IP reference models? Explain briefly.   **(8)**

Ans:
We will be focusing only on the key differences between the two references models.
Three concepts are central to OSI model: services, interfaces and protocols. OSI model makes the clear distinction between these three concepts.
The TCP/IP model did not originally clearly distinguish between services, interface, and protocol. For example the only real services offered by the Internet layer are SEND IP packet and RECEIVE IP packet.

The OSI reference model was devised before the protocols were invented. This ordering means that model was not biased towards one particular set of protocols, which made it quite general.

With TCP/IP reverse was true: the protocol came first, and the model was really just a description of the existing protocols. So problem was model did not fit for any other protocol stack.

Another difference is in the area of connectionless versus connection-oriented communication. The OSI model supports both connectionless and connection oriented communication in network layer, but only connection oriented in the transport layer. The TCP/IP model has only connection less mode in network layer but supports both the mode in transport layer.

Q.4 Define a socket? How read and write is performed using sockets?   **(6)**

Ans:
An application program interface specifies the details of how an application program interacts with protocol software. Socket API is a defacto standard. Once a socket has been established the application can transfer information.

recv() and send() are used to read and write the data.

recv(socket, buffer, length, flags)

The socket is the descriptor of the socket, buffer specifies the address in memory where incoming message should be placed and length specifies the size of the buffer, flags allows the caller to control details.

send(socket, data, length, flags)

Here data is the address of data to be sent and other arguments are same.

Sockets also allows read() and write() to transfer data like send () and recv(). read() and write() have three arguments: a socket descriptor, the location of the buffer in the memory and the length of the memory buffer.

Q.5   How optimization is achieved in DNS?   **(7)**

Ans:
There are two primary optimizations used in DNS: replication and caching. Each root server is replicated; many copies of the server exist around the world. When a new site joins the internet, the site configures its local DNS server with a list of root server. The site server uses whichever root server is most responsive at a given point of time. In DNS caching each server maintains a cache of names. Whenever it looks up a new name, the server places a copy of the binding in its cache. Before contacting another server to request a binding , the server checks its cache, if the cache contains the answer the server uses the cached answer to generate a reply.

Q.6   How physical addressing is performed in WAN?   **(7)**

Ans:
WAN networks operate similar to a LAN. Each WAN technology defines the exact frame format a computer uses when sending and receiving data. Each computer connected to a WAN is assigned a physical address. When sending a frame to another computer, the sender must supply the destination's address.

Many WANs use a hierarchical addressing scheme that makes forwarding more efficient. Hierarchical addressing scheme divides an address into multiple parts. The simplest scheme divides address in to two parts; the first part identifies packet switch, and second part identifies computer attached to that packet switch.

Address [1,2] ———— | **Switch 1** | ——— Address [2,1]

Address [1,5] ———— | **Switch 1** | ——— Address [2,6]
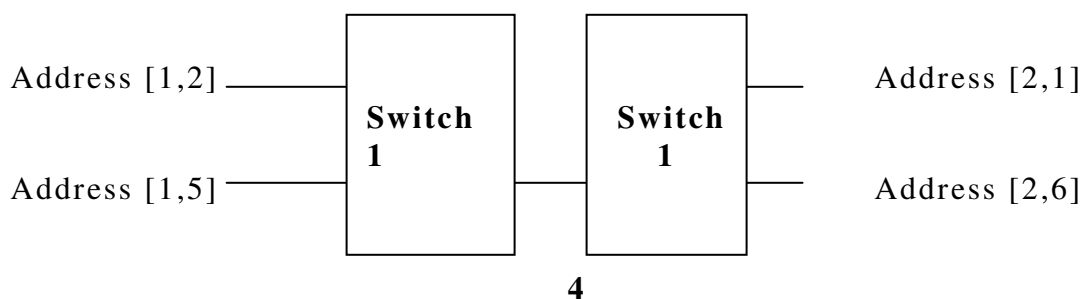
Example of Hierarchical addresses in WAN

The above figure shows each address as a pair of decimal integers. A computer connected to port 6 on packet switch 2 is assigned address [2,6].

Q.7 How do you make an image clickable in HTML? Give an example. **(6)**

Ans:
To make an image or text clickable hyperlinks are used, which use the <A> and </A> tags. This tag has various parameters, including HREF(the URL), NMAE(the hyperlink name), and METHODs(access methods).

As an example consider the following HTML fragment:

<A HREF = "http://www.foobar.com"> Foobar Home Page</A>
when a page with this fragment is displayed, following will appear on the screen:

<u>Foobar Home Page</u>

If the user clicks on this, the browser immediately fetches the page whose URL is http://www.foobar.com and displays it. Now we put a image in place of text.
<A HREF = "http://www.foobar.com"> <IMG SRC = "img1.gif" ALT = "Foobar" </A>
when displayed this page shows a picture(img1.gif). clicking on the picture switches to foobar home page just as in previous example.

Q.8 Design a form for a publishing house called foobar that allows the books to be ordered via the Internet. The form should include the customer's name, address, phone no. and Boo's title, author and edition. Payment has to be made in cash on delivery so no credit card information is needed. **(8)**

Ans:

Book Title : _____

Author : _____

Edition : _____

Customer's Name : _____

Address :

Phone Number :

SUBMIT   RESET

```
<html>

<head>
<title>New Page 1</title>
</head>
<body>
<H2 align="center"><b><u>FORM TO PURCHASE BOOK
ONLINE</u></b></H2>
<FORM METHOD ="POST" ACTION ="/cgi-bin/formmail">
<input type="hidden" NAME = "SUBJECT" VALUE = "FORM">
<INPUT TYPE="HIDDEN" NAME = "REDIRECT" VALUE ="FORM">
<p><STRONG>Book Title
:</STRONG>        &
nbsp;      
<INPUT NAME  ="NAME" TYPE = "TEXT" SIZE="50">
</p>
<p><STRONG>Author
:   </STRONG>     &
nbsp;         
   
<INPUT NAME  ="NAME" TYPE = "TEXT" SIZE="50">
</p>
<p><b>Edition
:         &nbs
p;         &nb
sp; 
</b><INPUT NAME  ="NAME1" TYPE = "TEXT" SIZE="11">
</p>
<p><b>Customer's Name :    </b><INPUT NAME
="NAME2" TYPE = "TEXT" SIZE="50">
</p>
<p><b>Address 
:         &nbs
p;        
</b><INPUT NAME  ="NAME3" TYPE = "TEXT" SIZE="50">
</p>
```

```
<p><b>Phone Number 
:        </b><INPUT NAME
="NAME4" TYPE = "TEXT" SIZE="18">
</p>

</form>

<form method="POST" action="_derived/nortbots.htm" webbot-
action="--WEBBOT-SELF--"
onSubmit="location.href='_derived/nortbots.htm';return
false;" WEBBOT-onSubmit>

<p>        &n
bsp;         &
nbsp;         
         &nbsp
;

<input type="submit" value="SUBMIT"
name="B1">        &
nbsp;
   <input type="reset" value="RESET" name="B2"></p>
</form>
<p> </p>

</body>

</html>
```

Q.9   How non-textual information is contained in a web page?   **(7)**

Ans:
Non-textual information such as a graphics image or digitized photo is not
inserted directly in a HTML document. Instead the data resides in a separate
location, and the document, and the document contains a reference to the
data. When the browser encounters such a reference, the browser goes to the
specified location, obtains a copy of the image, and inserts the image in the
specified document.

Q.10   When web pages containing emails are sent out they are prefixed by MIME
Header. Why?   **(7)**

Ans:
Initially email consisted messages containing simple text written in English
and expressed in ASCII. Now a days on world wide internet messages can be
sent in languages with accents like French and German, languages without

7

alphabet like Chinese and Japanese etc. the basic idea of MIME is to add structure to the message body and define encoding rule for non- ASCII messages.

   MIME defines five additional message headers to the RFC 822 format.

Header	Meaning
MIME Version	Identifies the MIME version
Content Description	Readable string telling about message
Content-ID	Unique Identifier
Content transfer encoding	How the body is wrapped for transmission
Content Type	Nature of the message

Q.11 What is trivial file transfer protocol. Explain briefly?   **(5)**

Ans:
Trivial File Transfer Protocol (TFTP) is useful for bootstrapping a hardware device that does not have a disk on which to store system software. All the device needs is a network connection and a small amount of read only memory (ROM) into which TFTP, UDP and IP are hardwired. Although TFTP is les powerful than FTP. TFTP does have two advantages. First, TFTP can be used in environments where UDP is available, but TCP is not. Second the code for TFTP requires less memory than the code for FTP.

Q.12 Why Gateways are used during mail transfer?   **(5)**

Ans:
Email using SMTP works best when both the sender and the receiver are on the internet and can support TCP connections between sender and receiver. However many machines that are not on the internet still want to send and receive email from internet sites. For example many companies intentionally remove themselves for security reasons.
Another problem occurs when the sender and receiver speaks different protocols so direct communication is impossible.
Both of these problems are solved using application layer email gateways.

Q.13   An SNMP integer whose value is 200 has to be transmitted. Show its representation in ASN.1 syntax.   **(4)**

Ans:
An ASN.1 transfer syntax defines how values of ASN.1 types are unambiguously converted to a sequence of bytes for transmission. Every value transmitted consists of up to four fields

a. identifier type
b. the length of data field in bytes
c. the data field
d. the end of content flag, if data length is unknown.

The last one is forbidden by SNMP, so we will assume data length is always known.

Tag	length	value
0 0 0 0 0 0 1 0	0 0 0 0 0 0 0 1	1 1 0 0 1 0 0 0

Integer 200

Q.14   Is TCP checksum necessary or could TCP allow IP to checksum the data. **(7)**

Ans:
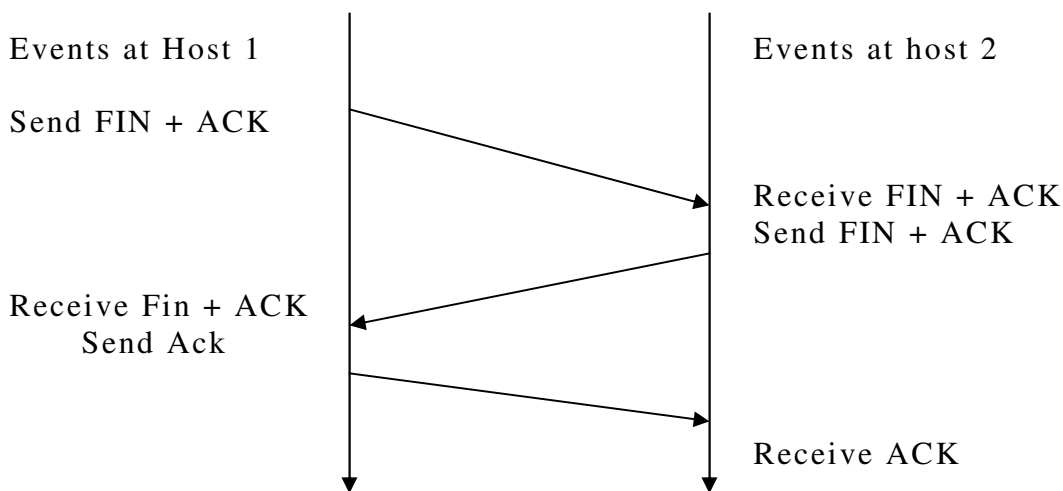Yes, TCP Checksum is necessary.
TCP layer is responsible for error detection, error control, retransmission of packets if required, reassembly of packets as well as their fragmentation. Hence for all error control and detection purposes TCP Checksum is essential.

TCP cannot allow IP to checksum data however IP has its own checksum for its header. IP layer is basically responsible for routing of IP datagrams immaterial of whether that packet is intended for TCP services or UDP services. Thus immaterial of what information is contained in data part , IP layer is only responsible for routing of packets and all the issues related to error control, error detection , flow control with regards to Routing only. Hence IP does not have a checksum for data unlike TCP.

Q.15 Explain Three-Way Handshake Mechanism used by TCP to terminate a Session reliably. **(7)**

Ans:
To guarantee that connection are established or terminated reliably, TCP uses 3-way handshake in which three messages are exchanged. TCP uses the term synchronization segment (SYN segment) to describe messages in a 3-way handshake used to create a connection , and the term FIN segment(short for finish) to describe messages in 3-way handshake to close a connection.

Events at Host 1   Events at host 2

Send FIN + ACK

                                    Receive FIN + ACK
                                    Send FIN + ACK

Receive Fin + ACK
    Send Ack

                                    Receive ACK

Threeway handshake used to close a connection

Q.16 Explain the significance of init() and destroy() methods of an applet? Also explain two ways of invoking an applet. **(7)**

Ans:
The init() method is used for basic initialization inside the applet. It is executed only once during the life time of the applet. This is the first method to be invoked when applet is started.
The destroy() method is used to clear the space from the memory when applet is stopped finally.
There are two ways to invoke an applet
• Executing the applet within a java compatible web browser or
• Using an Applet viewer

To execute an applet in a web browser a short HTML text file is written. Following is the HTML file to execute SimpleApplet:

<applet code = "SimpleApplet" width =200 height =60> </applet>

the width and height specifies the dimensions of the display area used.

To execute SimpleApplet with an applet viewer we will execute HTML file shown above. For example if preceding HTML file is called app.HTML then the following command will execute the SimpleApplet:

C:\<appletviewer app.HTML

Q.17 Why does IPV6 use separate extension headers? Explain.   **(7)**

Ans:
The extension headers in Ipv6 are used for economy and extensibility. Partitioning the datagram functionality in to separate headers is economical because it saves space. Also having separate headers in Ipv6 makes it possible to define large set of features without requiring each datagram header to have at least one field for each feature.

Extensibility comes in to existence when new features are required to be added to a protocol. A protocol like Ipv4 needs complete change, the header must be redesigned to accommodate new features. In Ipv6 however, existing protocol header remains unchanged. A new header field can be defined to accommodate new change.

Q.18 How address resolution is performed with table lookup? Explain with thee help of a suitable example.   **(7)**

Ans:
The table lookup approach to address resolution requires a data structure that contains information about address bindings. The table consists of an array. Each entry in the array contains a pair [P,H] where P is a protocol address and H is the equivalent hardware address. A separate address binding table is used for each physical network. Consequently all IP addresses in a given table have the same prefix. For example the following address binding table corresponds to a network with the class C number 197.15.3.0. therefore, each IP address in the table will begin with 197.15.3 prefix. The chief advantage of this table lookup approach is that a table can store the address bindings for an arbitrary set of computers on a given network.

IP Address	Hardware Address
197.15.3.2	0A:07:4B:12:82:36
197.15.3.3	0A:9C:28:71:32:6D
197.15.3.4	0A:11:C3:68:01:99

An example address binding table

Q.19   Write a CGI program that displays a count of how many times a browser on each computer has contacted the server. **(7)**

Ans:
```
echo Content-type: text/html
echo

N=$QUERY_STRING
Echo "<HTML>"

Case "x$N" in

x)        N = 1
Echo "This is the initial page.<BR><BR>"
;;
   X[0-9]*)   N = 'expr$n + 1'
              Echo "you have displayed this page $N times.<BR><BR>
                ;;

   *)     echo "The URL you used is invalid </HTML>"

          exit 0
          ;;
   esac
   echo "<A HREF=\http://$SERVER_NAME$SCRIPT_NAME?$N\>"
   echo " Click here to refresh the page. </ A></HTML>"
```

Q.20 Write short notes on the following: **(14)**

(i) MIB variables
Ans:
MIB (Management Information Base) variables:

MIB is a set of named items that an SNMP agent understands. To monitor or control a remote computer, a manager must fetch or store values to MIB variables. Because SNMP does not specify a set of MIB variables, the design is flexible. The separation of communication protocol from the definition of the objects permits to define MIB variable as needed. there are MIB variables that corresponds to protocols like UDP, TCP, IP and ARP, as well as MIB variables for network hardware such as Ethernet. In addition to simple variables such as integers that corresponds to counters, a MIB can include a variable that corresponds to a table or an array.

(ii) Circular Dependencies
Ans:
Circular Dependencies**:**

To understand the problem of circular dependencies consider a file server that uses a timeserver to obtain the current time whenever a file is accessed. Circular dependencies can occur if the timeserver also uses the file server. For example suppose a programmer is asked to modify the time server so it keeps a record of each request. If the programmer choose to have the time server become a client of the file server, a cycle can result; the file server becomes a client of the time server which becomes a client of the file server, and so on**.**

(iii) UDP
Ans:
UDP(User Datagram Protocol) :

UDP uses a connectionless communication paradigm. That is, an application using UDP does not need to preestablish a connection before sending data, nor does application need to terminate communication when finished. Furthermore, UDP allows an application to delay an arbitrarily long time between the transmission of two messages. UDP does not use any control messages. Communication consists only of the data messages themselves.

(iv) RPC

Ans:

RPC (Remote Procedure Call) **:**

The facility that was created to help the programmers write client-server software is known as Remote Procedure Call. In RPC instead of giving a programmer explicit communication primitives such as the socket interface, hide communication from the programmer by using a conventional programming language facility. The programming mechanism chosen is a procedure call. The RPC mechanism allows a programmer to place procedures on two or more machines, and automatically generates code that will allow a procedure call to pass from one computer to another.

(v) CGI standard

Ans:

The CGI Standard:

Technology used for building dynamic web documents is known as Common Gateway Interface (CGI). The CGI standard specifies how a server interacts with an application program that implements dynamic documents. The application is called a CGI program.
CGI provides general guidelines and allows a programmer to choose more details. For example, CGI does not specify a particular programming language. Instead the standard permits a programmer to choose an appropriate language for each dynamic document. For example a programmer can use a conventional programming language like C for documents that requires extensive computation, and use a scripting language like perl for documents that require only minor text editing.

(vi) Token Ring.

Ans:

Token Ring:

A token ring is a collection of individual point-to-point links that happen o form a circle. In a token ring a special bit pattern, called the token, circulates around the ring whenever all stations are idle. When a station wants to transmit a frame, it is required to seize the token and remove it fro the ring before transmitting. This action is done by inverting a single bit in the 3-byte token, which instantly changes it into the first 3 bytes of a normal data frame. Because there is only one token one station can transmit at a given instant.

14

Q.21 Write an applet that sets the background colour to cyan and foreground colour to red and displays a message that illustrates the order in which various applet methods are called when an applet starts up. For example : inside init()...inside start()... **(7)**

Ans:
```
import java.awt. *
 import java.applet. *

public class Method_order Extends Applet
    {
String msg;
//Sets the background and foreground color.public void init( )
{
setBackground(Color.cyan);
        setForeground(Color.red);
msg =" inside init 0- -";
}
//Initialize the string to be displayed.
 public void init( )
    {
msg =" inside startO- - ";
  }

lSets the background and foreground color.
    public void paint(Graphics g )
    {

    msg =" inside paint()-";
g.drawstring(msg, 10 , 30);
}
}
```

Q.22 How exceptions are handled in java?   /
Explain with the help of suitable example.

(7)

Ans:
Exception Handling In Java:

A java exception is an object that describes an exceptional condition that has occurred in a piece of code. When an exceptional condition arises, an object representing that exception is created and thrown in the method that causes the error. That method may choose to handle the exception itself or may pass it on. Either way, at some point exception is caught and processed.
Java exception handling is managed by five keywords: try, catch, throw, throws, and finally. The general form of an exceptional handling block is as follows:

```
try
{
//Block of code to monitor errors.

}
catch(Exception1 e)
{
//Block of code to handle Exception1.

}
catch(Exception2 e)

{
//Block of code to handle Exception2..

}

finally
{

//Block of code to be executed before try block ends.

}
```
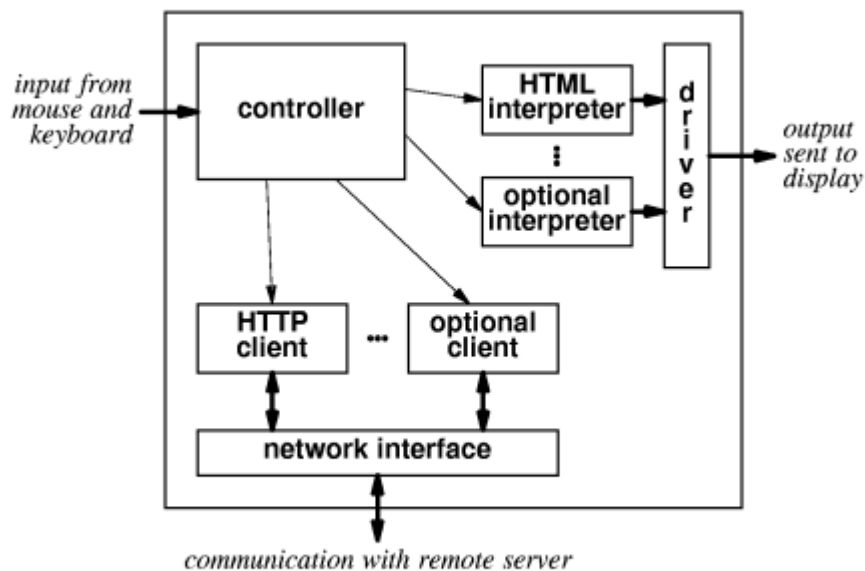
Q.23   What are the major components of a web browser? Draw a neat diagram to
explain them.   **(7)**
Ans:

The Major Component of a Web browser

16

A browser consists of a set of clients, a set of interpreters, and a controller that manages them. Each browser must contain an HTML interpreter to display the document. Other interpreters are optional. The controller forms the central piece of browser. It interprets both mouse click and key board input, and calls other components to perform operations specified by the user.

Q.24   How aliases are used in DNS? Explain.   **(7)**

Ans:
CNAME entries are analogous to a symbolic link in a file system- the entry provides an alias for another DNS entry. Foobar Corporation has two computers named hobbes.foober.com and calvin.foobar.com. further suppose that Foobar decide to run a web server and wants to follow the convention of using the name www for the computer that runs the organization's Web server. Although the organizations could choose to rename one of their computers (e.g. hobbes), a much easier solution exists: the organization can create a CNAME entry for www.foobar.com that points to hobbes. Whenever a resolver sends a request for www.foobar.com , the server returns the address of computer hobbes.

The use of aliases is especially convenient because it permits an organization to change the computer used for a particular service without changing the names or addresses of the computers. For example Foobar Corporation can move its web service from computer

hobbes to computer calvin by moving the server and changing the CNAME record in the DNS server- the two computers retain their original names and IP addresses.

Q.25   What are the three basic types of web documents? Also explain the advantages and disadvantages of each type.   **(8)**

Ans:
There are three basic types of web documents:

- static
- Dynamic
- Active

STATIC
A static web document resides in a file that is associated with a web server. The developer of static document determines the contents at. the time the document is written. Because contents do not change, each request for a static document results in exactly the same response.

DYNAMIC

A dynamic web document does not exist in predefined form: Instead a dynamic web document is created by a web server whenever a browser requests the document. When a request arrives, the web server runs an application program-that creates the dynamic document. Because a fresh document is created for each request, the contents of dynamic document can very from one request to another.

ACTIVE

An active document is not fully specified by the server. Instead, an active document consists of a computer program-that understands how to compute and display values. When a browser request an active document, the server returns a copy of the program that the browser must run locally. When it runs active documents can interact with the user and change the display continuously. Thus the contents of an active document are never fixed

ADVANTAGES AND DISADVANTAGES OF EACH DOCUMENT:

The chief advantages of a static document are simplicity, reliability and performance. A browser can display a static document quickly and place a copy in cache on a local disk to speedup the future request for the document.

The chief disadvantage of static document is inflexibility.

The advantage of an active document over a dynamic document lies in its ability to update the information continuously.

The chief disadvantages of active documents arise from the additional costs of creating and running such documents, and from a lack of security. The active document has a potential security risk because the document can export as well as can import the information.

The chief advantage of a dynamic document lies in its ability to report current information. For example a dynamic document can be used to report current stock prices, current weather conditions etc.
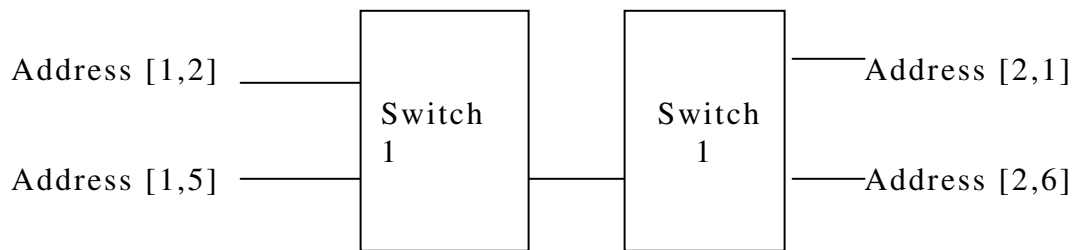
The chief disadvantages of dynamic document approach are increased cost and the inability to display changing information. A dynamic document takes slightly longer to retrieve than a static document because server requires additional time to run the application program that creates the documents.

Q.26   How physical addressing is performed in WAN?   **(6)**

Ans:
WAN networks operate similar to a LAN. Each WAN technology defines the exact frame format a computer uses when sending and receiving data. Each computer connected to a WAN is assigned a physical address. When sending a frame to another computer, the sender must supply the destination's address.

Many WANs use a hierarchical addressing scheme that makes forwarding more efficient. Hierarchical addressing scheme divides an address into multiple parts. The simplest scheme divides address in to two parts; the

first part identifies packet switch, and second part identifies computer attached to that packet switch.

Address [1,2] _____ ┌──────────┐   ┌──────────┐ ──── Address [2,1]
                        │ Switch   │   │ Switch   │
                        │ 1   │   │ 1   │
Address [1,5] ──────── └──────────┘ ────── └──────────┘ ──── Address [2,6]

Example of Hierarchical addresses in WAN

The figure shows each address as a pair of decimal integers. A computer connected to port 6 on packet switch 2 is assigned address [2,6].

Q.27   Differentiate between http and ftp.   **(5)**

Ans:
FTP and HTTP were developed to make Internet transmission better.

FTP is used to exchange files between computer accounts, to transfer files between an account and a desktop computer (upload), or to access software archives on the Internet. It's also commonly used to download programs and other files to your computer from other servers. It transfers files in two different formats ASCII for text files and Binary format for binary files. This allows a user to perform basic file and directory management operations such as deleting, copying, or renaming. Also, there is something

called Anonymous FTP used heavily today by several universities and private organizations. Anonymous FTP is a facility offered by many machines on the Internet. This permits you to log in with the user name 'anonymous' or the user name 'ftp'. When prompted for a password, type your e-mail address -- it's not necessary, but it's a courtesy for those sites that like to know who is making use of their facility. Be courteous. Some sites require a valid e-mail address, others don't.

HTTP is used primarily in today's society as a set of rules for exchanging files (text, graphic images, sound, video, and other multimedia files) on the World Wide Web. It also provides access to other protocols like FTP, SMTP, NNTP, WAIS, Gopher, Telnet, and TN3270. Essential concepts that are part of HTTP include (as its name implies) the idea that files can contain references to other files whose selection will elicit additional

transfer requests. Any web server machine contains, in addition to the HTML and other files it can serve, an HTTP daemon, a program that is designed to wait for HTTP requests and handle them when they arrive. Your Web browser is an HTTP client, sending requests to server machines. When the browser user enters file requests by either "opening" a Web file (typing

in a Uniform Resource Locator) or clicking on a hypertext link, the browser builds an HTTP request and sends it to the Internet Protocol Address indicated by the URL. The HTTP daemon in the destination server machine receives the request and, after any necessary processing, the requested file is returned.

Q.28   Write the HTML code to accomplish the web page: **(3)**

(i)   Insert the frame extending 300 pixels across the page from left side.
(ii) Insert scrollable lists that will always display four entries of the list.
(iii) Insert an image onto a page using good.gif as and image and having "welcome" as the ALT text.

Ans:
(i)

< FRAMESET COLS = " 300 , * " >
              . . .
< /FRAMESET >

(ii)

```
< SELECT SIZE  = " 4 "  >
        . . .
</SELECT>
```

(iii)

```
<IMG SRC = " good.gif "   ALT  = " Welcome"
```

Q.29 Write the HTML code for the following table: **(6)**

TEMPERATURE				
CITIES	DELHI	MUMBAI	KOLKATTA	CHENNAI
MAXIMUM	21	35	43	50
MINIMUM	5	14	28	32

Ans:
```
<html>
<head>
<title>New Page 1</title>
</head>
<body>
<div align="center">
  <center>
  <table border="1" width="441" height="106">
    <tr>
      <td width="441" height="19" colspan="5">
        <p align="center"><b>TEMPERATURE</b></td>
    </tr>
    <tr>
      <td width="60" height="23">
        <p align="center">CITIES</td>
      <td width="82" height="23">
        <p align="center">DELHI</td>
      <td width="87" height="23">
        <p align="center">MUMBAI</td>
      <td width="77" height="23">
        <p align="center">KOLKATTA</td>
      <td width="86" height="23">
        <p align="center">CHENNAI</td>
    </tr>
    <tr>
```

```
            <td width="72" height="24">
              <p align="center">MAXIMUM</td>
            <td width="82" height="24">
              <p align="center">21</td>
            <td width="87" height="24">
              <p align="center">35</td>
            <td width="77" height="24">
              <p align="center">43</td>
            <td width="86" height="24">
              <p align="center">50</td>
          </tr>

          <tr>
            <td width="72" height="21">
              <p align="center">MINIMUM</td>
            <td width="82" height="21">
              <p align="center">5</td>
            <td width="87" height="21">
              <p align="center">14</td>
            <td width="77" height="21">
              <p align="center">28</td>
            <td width="86" height="21">
              <p align="center">32</td>
          </tr>
        </table>
        </center>
    </div>
    </body>
    </html>
```

Q.30   Explain dynamic server creation briefly.   **(7)**

Ans:
Dynamic Server Creation:

If a server handles one request at a time, all clients must wait while the server fulfills the one request. In contrast, a concurrent server can handle multiple requests simultaneously. When a request arrives, the server assigns the request to a thread of control that can execute concurrently with existing thread. The server program is constructed in two parts: one that accepts request and creates a new thread for the request, and another that consists of the code to handle an individual request. When a concurrent server start executing, only the first part runs. That is the main server thread waits for a request to arrive. When a request arrives, the main thread creates a new service thread to handle the request. The service thread handles one request and then terminates.

Q.31   What is socket inheritance? Explain.   **(7)**

Ans:
Socket Inheritance:

In socket inheritance a reference count mechanism is used. When a socket is first created, the system sets the socket's reference count to 1;the socket exists as long as the reference count remains positive. When a program creates an additional thread, the system provides the thread with a list of all the sockets that program owns, and increments the reference count of each by 1. when a thread calls close for a socket, the system decrements the reference count on the socket by 1 and removes the socket from the thread's list.

The main thread of a concurrent server creates the socket that the server uses to accept incoming connections. When a connection request arrives, the system creates a new socket for the new connection. After a service thread finishes, it calls close on the new socket.

Q.32   How does a computer know whether an arriving frame contains an ARP message? Explain.   **(7)**

Ans:
The type field in the frame header specifies that the frame contain an ARP message. A sender must assign an appropriate value for the type field before transmitting the frame and a receiver must examine the type field in each incoming frame. For example, the Ethernet standard specifies that the type field in an Ethernet frame carrying an ARP message must contain the hexadecimal value Ox806.

Dest. Address   source address   frame type   data in frame

			806	complete ARP message

Illustration of type field in a Ethernet header used to specify the frame contents. A value of 0x806 informs the receiver that the frame contains an ARP message.

Q.33   What is the chief advantage of using virtual packets instead of frames? **(7)**

Ans:
The router cannot transfer a copy of a frame from one type of network to another because the frame formats differ. More importantly, the router cannot simply reformat the frame header because the two networks may use incompatible address format.

To overcome heterogeneity, Internet protocol software defines an inter packet format that is independent of the underlying hardware. This is called virtual packet and can be transferred across the underlying hardware. The underlying hardware does not understand or recognize the Internet packet format, the protocol software creates and handles Internet packets.

Q.34   "A datagram cannot be larger than the MTU of a network over which it is sent." Is the statement true or false? Explain with the help of a suitable example. **(7)**

Ans:
Each hardware technology specifies the maximum amount of data that a frame can carry. This limit is known as maximum transmission unit(MTU). There is no exception to MTU limit, the network hardware is not designed to accept or transfer frame to carry more data than the MTU allows. Thus a datagram must be smaller or equal to network MTU or it cannot be encapsulated for transmission.
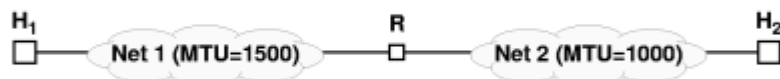
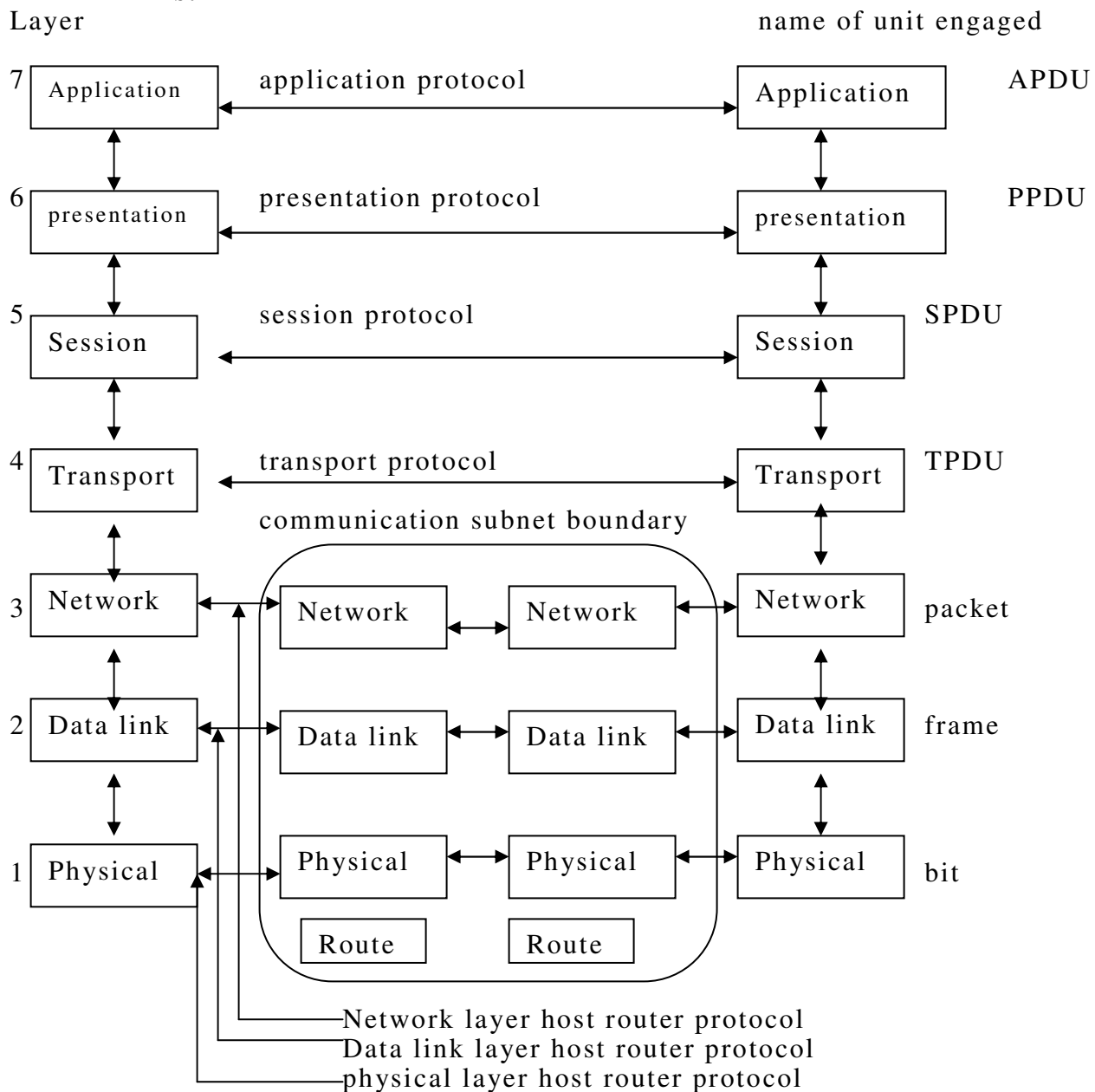An Example of a router that connects two networks with different MTU values

In the figure host H2 attaches to a network that has an MTU of 1000. Therefore each datagram that H2 transmits must be 1000 octets or less. However, because host HI attaches to a network that has an MTU of 1500 octets, HI can transmit datagrams that contains up to 1500 octets. To solve this problem IP router uses a technique called fragmentation. When a datagram is larger than the MTU of a network over which it is sent, the router divides the

datagram into smaller pieces called fragments and sends each fragment independently. To fragment a datagram for transmission across the network, a router uses the network MTU and datagram header size to calculate maximum amount of data that can be sent in each fragment and number of fragment that will be needed.

Q.35   Draw a neat labeled diagram of the OSI reference model for computer networks showing all the layers and the communication subnet boundary.

(7)

Ans:

Layer   name of unit engaged

7 | Application | ← application protocol → | Application | APDU

6 | presentation | ← presentation protocol → | presentation | PPDU

5 | Session | ← session protocol → | Session | SPDU

4 | Transport | ← transport protocol → | Transport | TPDU

communication subnet boundary

3 | Network | | Network | ↔ | Network | | Network | packet

2 | Data link | | Data link | ↔ | Data link | | Data link | frame

1 | Physical | | Physical | ↔ | Physical | | Physical | bit

| Route | | Route |

Network layer host router protocol
Data link layer host router protocol
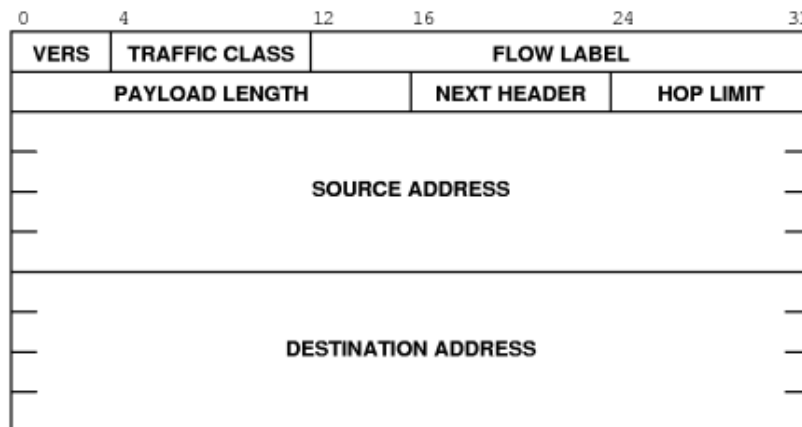physical layer host router protocol

The OSI reference Model

Q.36   Explain various fields in IPV6 base header?   **(8)**

Ans:
Although IPv6 base header is twice as large as an IPv4 header, it contains
less information. Following diagram illustrates the format:

The format of an Ipv6 base header

Most of the space in header is devoted to two fields that identify the sender and recipient.
Each address occupies sixteen octets, four times than an IPv4 address.

In addition to source and destination address, the bas header contains six fields. The VERS
field identifies the protocol as version 6. the PRIORITY field specifies the routing priority
class. The PAYLOAD LENGTH field corresponds to IPv4's datagram length field. The
HOP LIMIT corresponds to the IPv4 TIME-TO-LIVE field. IPv6 interprets the HOP
LIMIT strictly.. field FLOW LABEL is intended for use with new applications that requires
performance guarantees.

Q.37   Differentiate between adaptive and non-adaptive routing.   **(6)**

Ans:
Adaptive routing describes the capability of a system, through which routes
are characterised by their destination, to alter the path that the route takes
through the system in response to a change in conditions. The adaptation is

intended to allow as many routes as possible to remain valid (that is, have destinations that can be reached) in response to the change.

People using a transport system can display adaptive routing. For example, if a local railway station is closed, people can alight from a train at a different station and use another method, such as a bus, to reach their destination.

Systems that do not implement adaptive routing are described as using non-adapting or static routing, where routes through a network are described by fixed paths (statically). A change, such a loss of a node, or loss of a connection between nodes, is not compensated for. This means that anything that wishes to take an affected path will either have to wait for the failure to be repaired before restarting its journey, or will have to fail to reach its destination and give up the journey.

Q.38   How congestion is controlled in TCP?   **(7)**

Ans:
One of the most important aspects of TCP is a mechanism for congestion control. In most modern internets, packet loss or extreme long delays are more likely to be caused by congestion than a hardware failure. Interestingly, transport protocols that retransmit can exacerbate the problem of congestion by injecting additional copies of a message.

To avoid such a problem, TCP always uses packet loss as a measure of congestion and responds to congestion by reducing the rate at which it retransmits data.

TCP does not compute an exact transmission rate. Instead, TCP bases transmission on buffers. That is, the receiver advertises a window size and the sender can transmit data to fill the receiver's window before an ACK is received. To control the data rate, TCP imposes a restriction on the window size – by temporarily reducing the window size , the sending TCP effectively reduces the data rate.

TCP congestion control takes over when a message is lost. Instead of retransmit ting enough data to fill the receiver's buffer (the receiver's window size), TCP begins by sending a single message containing data. If the acknowledgement arrives without additional loss, TCP doubles the amount of data being sent and sends two additional messages. If acknowledgement arrive for those two , TCP sends four more and so on.

Q.39   While using FTP what is wildcard expansion in file names?   **(7)**

Ans:
To make it easy for users to specify a set of file names, FTP allows a remote computer system to perform traditional file name expansion. The user enters an abbreviation, which FTP expands to produce a valid file name. In abbreviations, a wildcard character stands for zero or more characters. Many computer systems use the asterisk _* as a wildcard. On such systems, the abbreviation   li*

Matches all file names that begin with the prefix li. Thus, if a remote computer contains the six files:

Dark light lonely crab link tuft

FTP will expand the abbreviation li* to two names: light and link. File name expansion can be especially useful with commands mget or mput because expansion makes it possible to specify a large set of files without entering each file name explicitly.

Q.40   Write short notes on the following: **(14)**

(i)   Multihomed host.

Ans:
A host computer that connects to multiple networks is called multihomed host. Multihoming is sometimes used to increase reliability. If one network fails, the host can still reach the Internet through the second connection. Alternatively multihoming is used to increase performance. Connections to multiple networks can make it possible to send traffic directly and avoid routers, which are sometimes congested. Like a router, a multihomed host has multiple protocol addresses, one for each network connection.

(ii)   Star topology.

Ans:

A network uses a star topology if all computers attach to a central point. The following figure illustrates the concept:

Computers connected

To network   hub
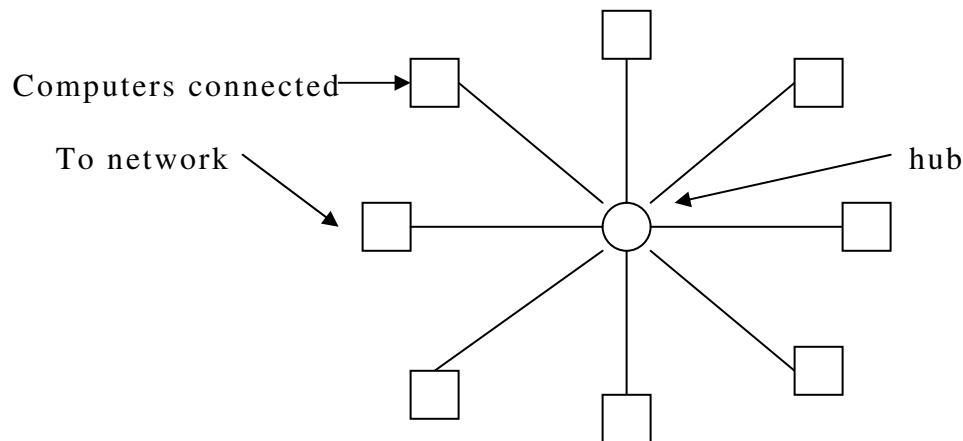
Because a star shaped network resembles the spoke of a wheel, center of a star network is often called a hub. In practice, star network seldom have a symmetric shape in which the hub is located at equal distance from all computers. Instead a hub often resides in a location separate from the computers attached to it.

(iii)   Remote Procedure Call (RPC).

Ans:

The facility that was created to help the programmers write client server software is known as Remote Procedure Call. In RPC instead of giving a programmer explicit communication primitives such as the socket interface, hide communication from the programmer by using a conventional programming language facility. The programming mechanism chosen is a procedure call. The RPC mechanism allows a programmer to place procedures on two or more machines, and automatically generates code that will allow a procedure call to pass from one computer to another.

(iv)   E-mail gateways.

Ans:

Email using SMTP works best when both the sender and the receiver are on the Internet and can support TCP connections between sender and receiver. However, many machines that are not on the internet still want to send and receive emails from internet sites.

29

Another problem occurs when the sender speaks only RFC 822 and the receiver speaks only X.400 or some vendor specific protocol. Both of these problems are solved using email gateways. Email gateways are used at application layer.

(v)   CIDR.

Ans:

CIDR is a new addressing scheme for the internet which allows for more efficient allocation of IP addresses than old class A, B, and C addressing scheme. Instead of being limited to network identifier (or prefixes) of 8, 16, or 24 bits, CIDR currently uses prefixes any where from 13 to 27 bits. Thus, block of addresses can be assigned to a network as small as 32 hosts or to those with 500,000 hosts. This allows for address assignments that much more closely fit an organization's specific need.

A CIDR address includes the standard 32- bit address and also information on how many bits are used for the network prefix. For example in CIDR address 206.13.01.48/25, the /25 indicates that the first 25 bits are used to identify unique network leaving the remaining bits to identify the specific host.

(vi)   HDLC.

Ans:

HDLC - High Level Data Link Control :

Protocol Overall Description:

Layer 2 of the OSI model is the data link layer. One of the most common layer 2 protocols is the HDLC protocol. The basic framing structure of the HDLC protocol is shown below:

HDLC uses zero insertion/deletion process (commonly known as bit stuffing) to ensure that the bit pattern of the delimiter flag does not occur in the fields between flags. The HDLC frame is synchronous and therefore relies on the physical layer to provide method of clocking and synchronizing the transmission and reception of frames.The HDLC protocol is defined by ISO for use on both point-to-point and multipoint (multidrop) data links. It supports full duplex transparent-mode operation and is now extensively used in both multipoint and computer networks.

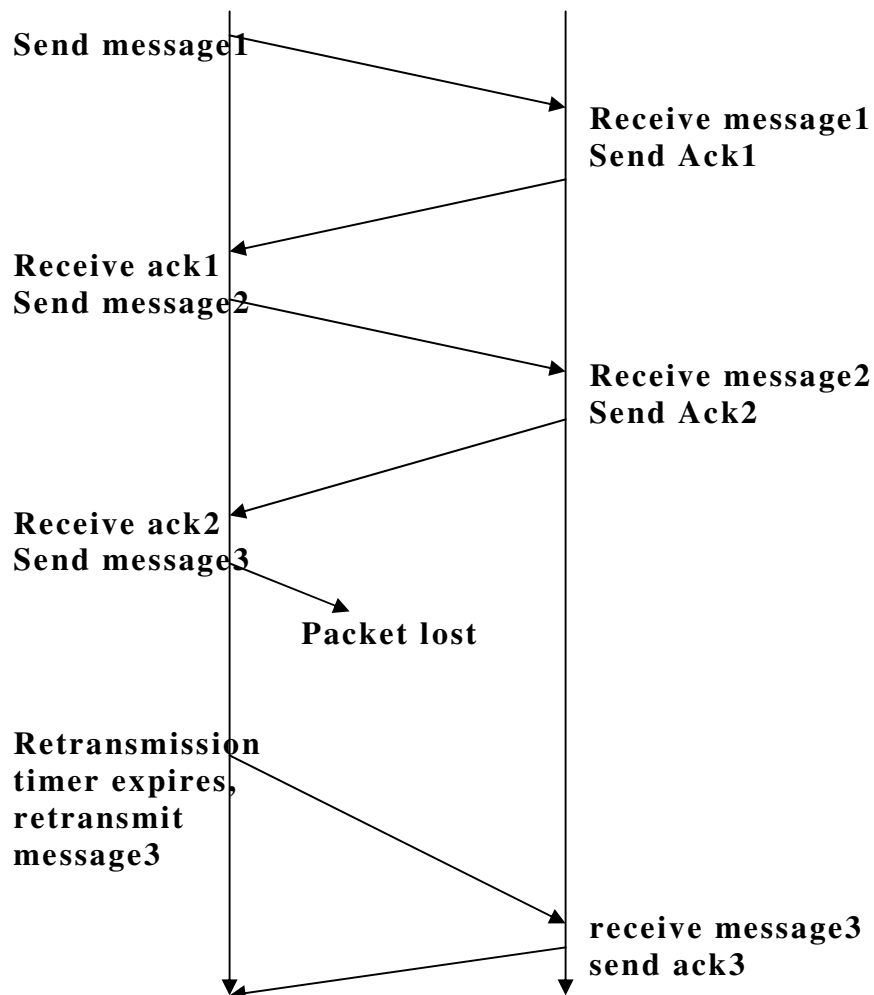**HDLC has three operational modes:**

1. Normal Response Mode (NRM)
2. Asynchronous Response Mode (ARM)
3. Asynchronous Balanced Mode (ABM)

Q.41   How does TCP achieve reliability?   **(4)**

Ans:
One of the most important technologies is retransmission. When TCP stands data the sender compensates for packet loss by implementing a retransmission scheme. Both sides of a communication participate. When TCP receives data, it sends it acknowledgements back to the sender. Whenever it sends data, TCP starts a timer . if the timer expires before an acknowledgement arrives, the sender retransmits the data. The following figure illustrates retransmission.

Send message1

                    Receive message1
                    Send Ack1

Receive ack1
Send message2

                    Receive message2
                    Send Ack2

Receive ack2
Send message3

            Packet lost

Retransmission
timer expires,
retransmit
message3

                    receive message3
   **send ack3**

TCP's retransmission scheme is the key to its success because it handles communication across an arbitrary Internet and allows multiple application programs to communicate concurrently.

Q.42 How adaptive transmission helps TCP to maximize throughput on each connection? **(5)**

Ans:
To understand how adaptive retransmission helps TCP maximize throughput on each connection, consider a case of packet loss on two connections that have different round-trip delay. For example, Figure given below illustrates traffic on two such connections.

Est1

Est2

Est1

Est2

Time out

Packet lost

Time out

packet lost
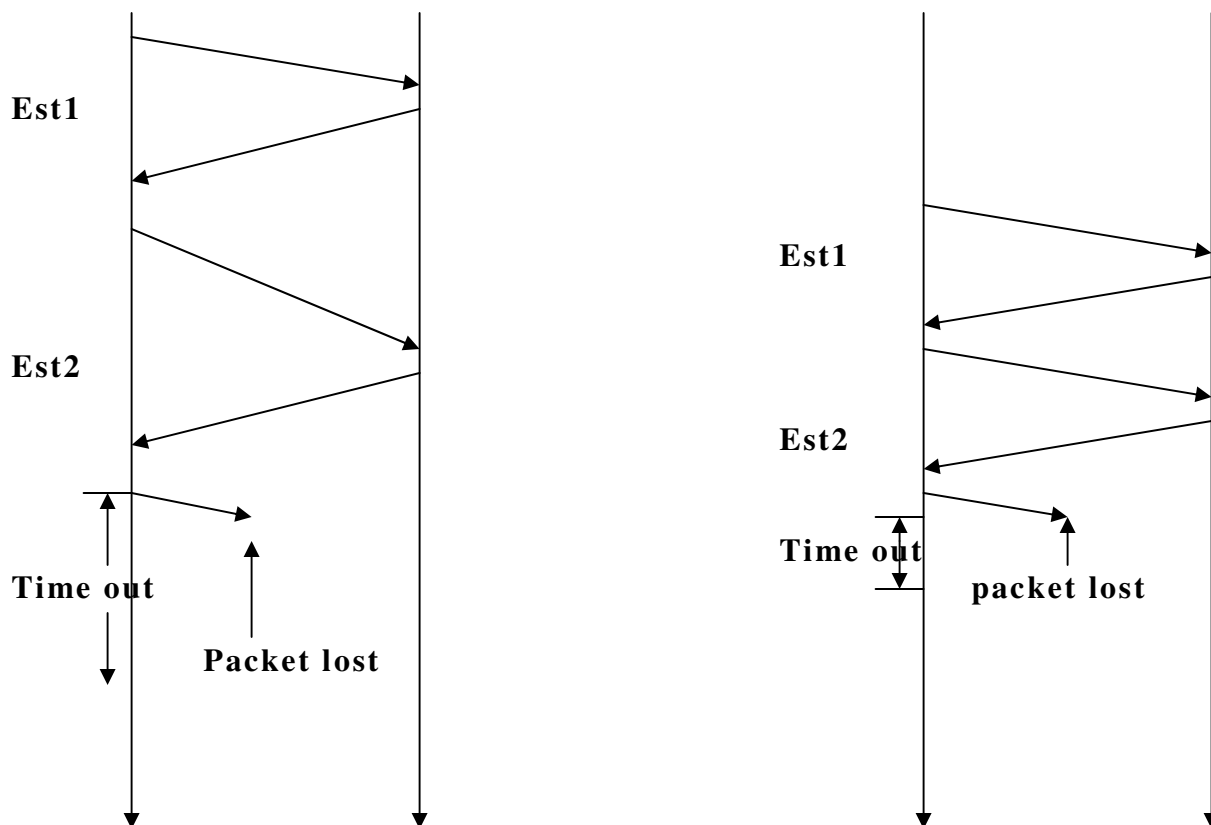
Time out and retransmission on two connections that have different round trip delays**.**

As the figure shows ,TCP sets the retransmission timeout to be slightly longer than the mean round-trip delay. If the delay is large, TCP uses a large retransmission timeout; if the delay is small, TCP uses a small time out. The goal is to wait long enough to determine that a packet was lost, without waiting longer than necessary.

Q.43   Explain that the lost acknowledgement does not necessarily enforce retransmission of the packet.   **(5)**

Ans:
To guarantee reliable transfer, protocols use positive acknowledgement with retransmission. When receiver gets the packet an acknowledgement is sent. If an acknowledgement is lost, generally packet is retransmitted. Retransmission can not succeed if a hardware failure has permanently disconnected the network or if receiving computer has crashed. Therefore, protocols retransmitting the messages bound the maximum number of transmissions. When the bound has been reached, the protocol stops retransmission of packet even if acknowledges is not received. So lost acknowledgement does not necessarily enforce retransmission of packet.

Q.44   Does it make sense for two domain servers to contain exactly the same set of names? Why or why not?   **(5)**

Ans:
Yes. It is very advantageous for two domain servers containing same set of names. If there is only one server than traffic on one server would be in tolerable, because it would be the only server to receive all the request and handle them appropriately. If there is more than one server containing same set of data then geographically closet server will respond thus reducing the load on one server. Also if one server is down due to some problem then another server containing same set of data can be used to fulfill the incoming requests.

Q.45   Reassembling of IP fragments at the ultimate destination is advantageous. Give reasons.   **(5)**

Ans:
Requiring the ultimate destination to reassemble the fragments has two main advantages. First, it reduces the amount of state information in routers. When forwarding a datagram, a router does not need to know whether a datagram is a fragment. Second, it allows routes to change dynamically. If an intermediate router reassembles fragments, all fragments would need to reach the router.

Q.46   What is the maximum number of fragments that can result from a single IP Datagram? Explain.   **(4)**

Ans:
To fragment a datagram for transmission across a network, a router uses the network MTU (Maximum Transmission Unit) and the datagram header size to calculate the maximum amount of data that can be sent in each fragment and number of fragment that will be needed. The router than creates the fragments. A datagram can not be larger than the MTU of a network over which it is sent. If a fragment eventually reaches another network that has a smaller MTU then fragment is further divided in to smaller fragments. IP does not distinguish between original fragments and sub fragments. So the maximum number of fragments from a single datagram will depend on size of datagram and MTU of the networks over which it is sent along its path.

Q.47   Does a numeric mailbox identifier have any advantage over a mnemonic identifier? Explain.   **(7)**

Ans:
Some software systems allow the system administrator to choose mailbox names, while other systems require a user's mail box identifier by concatenating a user's first name, middle initial and last name, with underscore to separate the three items. For example, the email address for employee john Quiggley Public at Foobar Corporation might be:

　　　　John_Q_Public@foober.com
On systems that require a user's login identifier to be used as a mailbox identifier, the resulting e-mail address is not nearly as readable. For example, if login accounts on a computer at nonexistent Corporation consist of two six-digit numbers separated by a period, an individual's e-mail address on that computer might be:

　　　　912743.253843@nonexist.com
Obviously mnemonic from makes the mailbox portion of an e-mail address easier to remember and enter correctly.

Q.48   What are the various address Translation schemes? Explain which scheme is used inn Internet?   **(7)**

Ans:
Translation from a computer's protocol address to an equivalent hardware address is known as address resolution. Address resolution algorithms can be grouped into three basic categories:

Table lookup-

Bindings or mapping are stored in a table in memory, which the software searches when it needs to resolve an address.

Closed Form Computation-

The protocol address assigned to a computer is chosen carefully so the computer's hardware address can be computed from the protocol address using basic boolean and arithmetic operations.

Message Exchange-

Computer exchange messages across a network to resolve an address. One computer sends a message that requests an address binding (i.e., translation), and another computer sends a reply that contains the requested information.

TCP/IP can use any of the three methods; the method chosen for a particular network depends on the addressing scheme used by underlying hardware.

Generally third scheme is used over internet. The TCP/IP suite contains a standard address   resolution protocol (ARP). ARP defines the format of the messages that computers exchange to resolve an address as well as rules for handling ARP messages.

Q.49   What are the three basic types of web documents? Discuss the advantages & disadvantages of each type.   **(5)**

Ans:

Static-

A static web document resides in a file that is associated with a Web server. The author of a static document determines the contents at the time the document is written. Because the contents do not change, each request for a static document results in exactly the same response.

Dynamic-

A dynamic web document does not exist in a predefined form. Instead a dynamic document is created by a web server whenever a browser requests the document. When a request arrives the web server runs an application program that creates the dynamic document. The server returns the output of the program as a response to the browser that requested the document.

Because a fresh document is created for each request the contents of dynamic document can very from one request to another.

Active-
An active document is not fully specified by the server. Instead an active document consists of a computer program that understands how to compute and display values. When a browser requests an active document, the server returns a copy of the program that the browser must run locally. When it runs the active document program can interact with the user and change the display continuously. Thus the contents of an active document are never fixed- they can continue to change as long as the user allows the program to run.

ADVANTAGES AND DISADVANTAGES OF EACH DOCUMENT:

The chief advantages of a static document are simplicity, reliability and performance. A browser can display a static document quickly and place a copy in cache on a local disk to speedup the future request for the document.
The chief disadvantage of static document is inflexibility.

The advantage of an active document over a dynamic document lies in its ability to update the information continuously.

The chief disadvantages of active documents arise from the additional costs of creating and running such documents, and from a lack of security. The active document has a potential security risk because the document can export as well as can import the information.

The chief advantage of a dynamic document lies in its ability to report current information. For example a dynamic document can be used to report current stock prices, current weather conditions etc.
The chief disadvantages of dynamic document approach are increased cost and the inability to display changing information. A dynamic document takes slightly longer to retrieve than a static document because server requires additional time to run the application program that creates the documents.

Q.50   What is the advantage of caching in a web browser?   **(5)**

Ans:
Like other applications browsers use a cache to improve document access. The browser places a copy of each item it retrieves in a cache on the local disk. When a user selects an item the browser checks the disk cache before retrieving a fresh copy. If the cache contains the item the browser obtains the copy from the cache without using the network.

Keeping items in a cache can improve performance dramatically- a browser can read the item from disk without waiting for network connections. For example, consider a user who connects to the Internet over a dialup telephone line. Although a high-speed modem can transfer data at 28.8 Kbps, the effective rate can be substantially lower it the connection is noisy. At such speeds, retrieving a large item from a local disk cache, in fact, local access can seem instantaneous when compared to internet access.

Q.51 **D**escribe the advantages of JAVA servlets over CGI interface. **(4)**

Ans:

The Advantage of Servlets Over "Traditional" CGI:

Java servlets are more efficient, easier to use, more powerful, more portable, and cheaper than traditional CGI and than many alternative CGI-like technologies. (More importantly, servlet developers get paid more than Perl programmers :-).

- Efficient. With traditional CGI, a new process is started for each HTTP request. If the CGI program does a relatively fast operation, the overhead of starting the process can dominate the execution time. With servlets, the Java Virtual Machine stays up, and each request is handled by a lightweight Java thread, not a heavyweight operating system process..
- Convenient. Hey, you already know Java. Why learn Perl too? Besides the convenience of being able to use a familiar language, servlets have an extensive infrastructure for automatically parsing and decoding HTML form data, reading and setting HTTP headers, handling cookies, tracking sessions, and many other such utilities.
- Powerful. Java servlets let you easily do several things that are difficult or impossible with regular CGI. For one thing, servlets can talk directly to the Web server (regular CGI programs can't). This simplifies operations that need to look up images and other data stored in standard places. Servlets can also share data among each other, making useful things like database connection pools easy to implement. They can also maintain information from request to request, simplifying things like session tracking and caching of previous computations.
- Portable. Servlets are written in Java and follow a well-standardized API. Consequently, servlets written for, say I-Planet Enterprise Server can run virtually unchanged on Apache, Microsoft IIS, or WebStar. Servlets are supported directly or via a plugin on almost every major Web server.

- Inexpensive. There are a number of free or very inexpensive Web servers available that are good for "personal" use or low-volume Web sites. However, with the major exception of Apache, which is free, most commercial-quality Web servers are relatively expensive. Nevertheless, once you have a Web server, no matter the cost of that server, adding servlet support to it (if it doesn't come preconfigured to support servlets) is generally free or cheap.

Q.52 Write short notes: **(14)**
(i) Client Server Model.

Ans:

In the client- server model, communication generally takes the form of a request message from the client to the server asking for some work to be done. The servers than does the work and sends back the reply.

A server application waits passively for contact, while a client application initiates communication actively.

A client and server must select a transport protocol that supports connectionless service or one that supports connection-oriented service. Connectionless service allows an application to send a message to an arbitrary destination at any time; the destination does not need to agree that it will accept the message before transmission occurs. In contrast, connection oriented service requires two application to establish a transport connection before data can be sent.

(ii) POP.
Ans:
POP (Post Office Protocol)
The Post Office Protocol provides remote access to an electronic mail box. The protocol allows a user's mailbox to reside on a computer that runs a mail server, and allows the user to access items in the mailbox from another computer.
This protocol requires an additional server to run on the computer with the mailbox. The additional server uses the POP protocol. A user runs email software that becomes a client of POP server to access the contents of the mailbox.

(iii) Anonymous FTP.

Ans:

Use of a login name and password helps keep file secure from unauthorized access. But sometimes such authorization can also be inconvenient. In particular, requiring each user to have a valid name and password makes it difficult to allow arbitrary access. For

example, suppose a corporation finds a bug in one of the programs it sells. The corporation might create file of changes, and make the file available to any one.

To permit arbitrary users to access a file without a specific login and password anonymous FTP is used, In which access to an FTP server is allowed using login name anonymous and password guest.

(iv)   SNMP.

Ans:

      SNMP (simple network management protocol)

      When SNMP is used the management station sends a request to an agent asking it for information or commanding it to update its state. SNMP defines seven messages that can be sent. The following six messages form an initiator.

      Get-request- requests the value of one or more variables

      Get-next-request – requests the value of next variable

      Get-bulk-request – used for large transfer like tables

      Set-request – updates one or more variables

      Inform-request – allows the manager to update an agent's variables

      SnmpV2-trap – Agent to manager trap report.

(v)   UDP.

Ans:

      UDP (User Datagram Protocol):

      UDP uses a connectionless communication paradigm. That is, an application using UDP does not need to preestablish a connection before sending data, nor does application need to terminate communication when finished. Furthermore, UDP allows an application to delay an arbitrarily long time between the transmissions of two messages. UDP does not use any control messages. Communication consists only of the data messages themselves.

    (vi)   Direct broadcast & limited broadcast.

Ans:

Broadcast is a way to send a packet to all the stations on a particular network at once. Broadcast systems allow the possibility of addressing a packet to all destinations by using a special code in the address field. When a packet with this code is transmitted, it is received and processed by every machine on the network. This is called direct broadcasting. The directed broadcast address for a network is formed by adding a suffix that consists of all 1 bits to the network prefix.

The limited broadcast refers to a broadcast on a local physical network. Limited broadcast is used during system startup by a computer that dosed not yet know the network number. The IP limited Broadcast address is found by setting all 32 bits of the IP address to a value of 1.

Q.53   Write a CGI program that keeps a list of computers that have contacted the server. If comp1 is contacting first time it will display the message: "This is the first contact from comp1" else it will display the message "Computer comp1 has requested this URL previously."   **(7)**

Ans:

```
#!/bin/sh
FILE = ipaddress

echo Content-type: text/plain
echo
# see if IP address computer appears in file ipaddress

if grep –s $REMOTE_ADDR  $FILE>/dev/null 2 >&1
then

echo Computer $REMOTE_ADDR has requested this URL previously.
else
# append browser's address to the file
 echo $REMOTE_ADDR >> $FILE
 echo This is the first contact from computer $REMOTE_ADDR.

fi
```

Q.54   Design a HTML form for a company Bookonline that allows you to order the books via internet. Form includes the following information:
   (i)   Book title, author, edition.
   (ii)   Customer's name, address, phone number.   **(7)**

   Ans:

Book Title :

Author :

Edition :

Customer's Name :

Address :

Phone Number :

SUBMIT   RESET


```html
<html>

<head>
<title>New Page 1</title>
</head>
<body>
<H2 align="center"><b><u>FORM TO PURCHASE BOOK
ONLINE</u></b></H2>
<FORM METHOD ="POST" ACTION ="/cgi-bin/formmail">
<input type="hidden" NAME = "SUBJECT" VALUE = "FORM">
<INPUT TYPE="HIDDEN" NAME = "REDIRECT" VALUE ="FORM">
<p><STRONG>Book Title
:</STRONG>        
       
<INPUT NAME  ="NAME" TYPE = "TEXT" SIZE="50">
</p>
<p><STRONG>Author
:   </STRONG>     
         &nbs
p;   
```

```
<INPUT NAME  ="NAME" TYPE = "TEXT" SIZE="50">
</p>


<p><b>Edition
:         &nb
sp;         &
nbsp; 
</b><INPUT NAME  ="NAME1" TYPE = "TEXT" SIZE="11">
</p>
<p><b>Customer's Name :    </b><INPUT NAME
="NAME2" TYPE = "TEXT" SIZE="50">
</p>
<p><b>Address 
:         &nb
sp;        
</b><INPUT NAME  ="NAME3" TYPE = "TEXT" SIZE="50">
</p>
<p><b>Phone Number 
:        </b><INPUT
NAME  ="NAME4" TYPE = "TEXT" SIZE="18">
</p>
</form>
<form method="POST" action="_derived/nortbots.htm" webbot-
action="--WEBBOT-SELF--"
onSubmit="location.href='_derived/nortbots.htm';return
false;" WEBBOT-onSubmit>
<p>         &
nbsp;        &nbsp
;         &nb
sp;         &
nbsp;
   <input type="submit" value="SUBMIT"
name="B1">        
 
   <input type="reset" value="RESET" name="B2"></p>
</form>
<p> </p>

</body>

</html>
```

Q.55   How does the Applet update its window when information changes?   **(6)**

Ans:
Whenever an applet needs to update the information displayed in its window, it simply calls repaint() method. The repaint() method is defined by AWT(abstract window toolkit). It causes the AWT run-time system to execute a call to applet's update() method, which in its default

implementation calls paint(). Thus for another part of the applet to output to its window, simply stores the output and then calls repaint(). The AWT will then execute a call to paint( ).

Q.56 Write an applet that display the directory holding the HTML file that started the applet and the directory from which, applet class file was loaded. **(8)**

Ans:
```
import java.awt.*;
import java.applet.*;
import java.net.*;

public class Base extends Applet
      {
         public void piant(Graphics g)
               {

                       String msg;
                       URL url = getCodebase();
                       Msg = "Code base:" +url.tostring();
                       g.drawstring(msg,10,20);
                       URL url = getDocumentbase();
                       Msg = "Document base: " +url.tostring();
                       g.drawstring(msg,10,40);
               }

      }
```

Q.57 How many Octets does the smallest possible IPV6 datagram contain? Explain the significance IPV6 over IPV4. **(4)**

Ans:
The maximum size of an Ipv6 datagram is 65575 bytes, including the 0 bytes Ipv6 header. Ipv6 also define a minimum reassembly buffer size: the minimum datagram size that we are guaranteed any implementation must support. The minimum size for Ipv6 datagram is 1500 bytes.

Despite retaining the basic concepts from IPv4, IPv6 changes all the details. IPv6 uses larger addresses and an entirely new datagram format. IPv6 uses a

series of fixed-length headers to handle header information. Thus, unlike IPv4, which places key information in fixed fields of the header and only appends variable-length options for less important information, the IPv6 header is always variable size.

Q.58   Suppose you have to develop an error recovery protocol for a link that is unreliable and delay sensitive, which of the following protocol would you choose?   **(6)**
(i)   Stop & wait.
(ii) Selective Repeat.
(iii) Go back.
Justify your answer.

Ans:
Selective- repeat and Go -back work well if errors are rare. But if error rate is high than a lot of bandwidth will be wasted in retransmission of frames. So both the above methods are not suitable for a link that is unreliable and delay sensitive.

For this kind of link stop and wait protocol is most suitable protocol. In this protocol sender waits after transmitting each packet. When the receiver is ready for another packet, the receiver sends a control message, usually in form of acknowledgement. Although this protocol prevents overrun, they can cause extremely inefficient use of network capacity.

Q.59   Explain the term middleware inn context of RPC.   **(4)**

Ans:
A variety of commercial tools have been developed to help the programmer in constructing client- server software. Such tools are generally called middleware because they provide software that fits between a conventional application program and the network software. Now designers are creating new middleware systems that extend method invocation across computers in the same way that remote procedure call extended procedure call. Such systems are known as distributed object systems.

Q.60   Differentiate between   **(6)**

(i)   message switching, packet switching and circuit switching

Ans:

Message switching:

Recourse computer sends data to switching office which stores the data in buffer and looks for a free link. If link is available than sends it to another switching office. This process continues until data are delivered to destination computer.

Circuit switching versus Packet switching:

In circuit switching an end-to-end path is to be established before any data can be sent. Once a connection is in its place, data can be sent across the connection. Finally when communication is complete, the connection must be terminated. Circuit switching provides connection-oriented interface.

In principle, circuit switching and packet switching both are used in high-capacity networks. In circuit-switched networks, network resources are static, set in "copper" if you will, from the sender to receiver before the start of the transfer, thus creating a "circuit". The resources remain dedicated to the circuit during the entire transfer and the entire message follows the same path. In packet-switched networks, the message is broken into packets, each of which can take a different route to the destination where the packets are recompiled into the original message.

(ii)   Bridges & Gateways.

Ans:

Gateways and Bridges:

A machine which connects a LAN to the Internet is called a *gateway*. The gateway machine is responsible for routing packets which are destined for a domain outside the local domain. These machines are called `routers`.

A *bridge* is a machine which transparently connects two segments of the LAN together. These two segments have the same domain name and behave as if part of the same LAN. In our case, we connect the Cape Town LAN and the Sutherland LAN by a PC running the public domain software called PCBRIDGE. Similarly, a PC at Sutherland, also running PCBRIDGE, connects the Sutherland LAN to the Cape Town LAN. These are soon to be replaced by CISCO bridges.

Q.61   What is the use of urgent pointer in TCP segment?   **(4)**

Ans:
To accommodate out of band signaling, TCP allows the sender to specify
data as urgent, meaning that the receiving program should be notified of its
arrival as quickly as possible, regardless of its position in the stream. For
this purpose Urgent pointer field is used. The mechanism used to mark
urgent data when transmitting it in a segment consists of URG code bit and
the URGENT POINTER field. When the URG bit is set, the urgent pointer
specifies the position in the segment where urgent data ends.

Q.62   Why does FTP use two standard ports whereas other protocols, in general
use only one port? Justify.   **(4)**

Ans:
FTP uses a control connection only to send commands and receive
responses. When it transfers a file, FTP does not send the data across the
control connection. Instead, the client and server establish a separate data
connection for each file transfer, use it to send one file, and then close the
connection. If the user requests another transfer, the client and server
establish a new data connection. To avoid conflict between control and data
connections, FTP uses a different port number for each.

Q.63   Does the use of wire-center have any influence on the performance of a
token ring? Explain.   **(4)**

Ans:
One problem with a ring network is that if the cable breaks somewhere, the
ring dies. This problem can be solved by the use of wire center.
Inside the wire center are bypass relays that are energized by current from
the stations. If the ring breaks or a station goes down, loss of drive current
will release the relay and bypass the station. The relays can also be
operated by software to permit diagnostic program to remove stations one at
a time to find faulty station and ring segments. The ring can then continue
operation with the bad segment bypassed.

Q.64 Explain the meaning of following socket primitive: **(8)**
BIND, LISTEN, ACCEPT and CONNECT.

Ans:

The bind Primitive

when created, a socket has neither a local address nor a remote address. A server uses the bind procedure to supply a protocol port number at which the server will wait for contact. Bind takes three arguments:

bind(socket, localaddr, addrlen)

Argument socket is the descriptor of a socket that has been created but not previously bound; the call is a request that the socket be assigned a particular protocol port number. Argument localaddr is a structure that specifies the local address to be assigned to socket and argument addrelen is an integer that specifies the length of the address.

The listen Primitive

After specifying a protocol port a server must instruct the operating system to place a socket in passive mode so it can be used to wait for contact from clients. To do so a server calls the listen procedure which takes to arguments:
listen(socket, queuesize)

argument socket is the descriptor of a socket that has been created and bound to a local address and argument queuesize specifies a length for the socket's request queue.

The Accept Primitive
A server that uses connection-oriented transport must call procedure accept to accept the next connection request. If a request as present in the queue, accept returns immediately; if no request have arrived the system blocks the server until a client forms a connection. The accept call has the form:
newsock= accept(socket, caddress, addresslen)

Argument socket is the descriptor of a socket the server has created and bound to a specific protocol port. Argument caddress is the address of a structure of type sockaddr and caddresslen is a pointer to an integer. Accept fills in fields of argument caddress with
the address of the client that formed the connection and sets caddresslen to the length of he address.

The connect Primitive
Clients use procedure connect to establish connection with a specific server. The form is

connect(socket, saddress, saddresslen)

Argument socket is the descriptor of a socket on the client's computer to use for the connection. Argument saddress is a sockaddr structure that specifies the server's address and protocol port number. Argument saddresslen specifies me length of the server's address measured in octets.

Q.65   What are two reasons for using layered protocol?   **(2)**

Ans:
Layered protocol means protocols used in each layer are the layer's own business i.e. they don't affect protocol of another layer.

- So each layer can use any protocol as long as it gets the gob done

- They can be replaced easily as the technology changes.

Being able to make such changes is the idea for using layered protocols.

Q.66   Give the format of Ethernet frame and explain the semantics of each field.
                                                                                (6)

Ans:
An Ethernet frame begins with a header that contains three fields. The 64-bit preamble, that precedes the frame contains alternating 1's and 0's that allows the receiver's hardware to synchronize with the incoming signal.
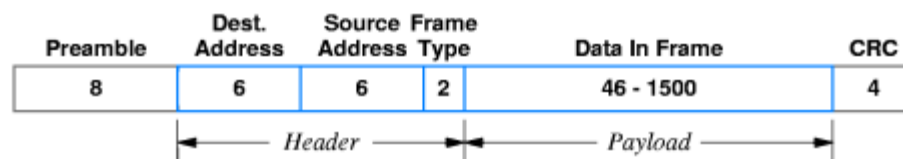
Figure 9.3 Illustration of the frame format used with Ethernet. The number in each field gives the size of the field measured in 8-bit octets.

The First two fields of the header contain the physical addresses. The third field of the header consists of a 16- bit Ethernet frame type.

Q.67   Why is packet switching important? Give at least two reasons.   **(4)**

Ans:
Packet switching is important because of the following to reasons:
1. A sender and the receiver need to coordinate transmission to ensure that data arrives correctly. Dividing the data into small blocks helps a sender and receiver determines which block arrive intact and which do not.

2. Second, because communication circuits and the associated modem hardware are expansive, multiple computers often share underlying connections and hardware. To ensure that all computers receive fair, prompt access to a shared communication facility, a network system allows one computer to deny access to others. Using small packets helps ensure fairness.

Q.68   Differentiate between Transport and Session layers of OSI model.   **(4)**

Ans:
OSI Model Transport Layer
The transport layer uses the services provided by the network layer, such as best path selection and logical addressing, to provide end-to-end communication between source and destination.

- The transport-layer data stream is a logical connection between the endpoints of a network.
- End-to-end control is provided by sliding windows and reliability in sequencing numbers and acknowledgments.
- The transport layer regulates information flow to ensure end-to-end connectivity between host applications reliably and accurately.
- The TCP/IP protocol of Layer 4 (transport layer) has two protocols. They are TCP   and UDP.

The transport layer accepts data from the session layer and segments the data for transport across the network. Generally, the transport layer is responsible for making sure that the data is delivered error-free and in the proper sequence. Flow control generally occurs at the transport layer.

OSI Model Session Layer

The session layer establishes, manages, and terminates communication sessions. Communication sessions consist of service requests and service responses that occur

between applications located in different network devices. These requests and responses are coordinated by protocols implemented at the session layer. The session layer establishes, manages, and terminates sessions between applications

- Functions of the session layer and the different processes that occur as data packets travel through this layer. More specifically, you learned that
- Communication sessions consist of mini-conversations that occur between applications located in different network devices
- Requests and responses are coordinated by protocols implemented at the session layer
- The session layer decides whether to use two-way simultaneous communication or two-way alternate communication by using dialogue control
- The session layer uses dialogue separation to initiate, terminate, and manage communication in an orderly fashion

Q.69   Describe the various characteristics of UDP protocol.   **(6)**

Ans:
The characteristics of the UDP are as follows:

- End to end: UDP is a transport protocol that can distinguish among multiple application programs running on a given computer.

- Connectionless:
  The UDP follows a connectionless paradigm.

- Message Oriented:
  An application that uses UDP sends and receives individual messages.

- Best Effort:
  UDP offers application the same best effort delivery semantics as IP.

- Arbitrary interaction:
UDP allows an application to send to many other applications, receive from many other applications, or communicate with exactly one another application.

- Operating system independent:
UDP provides a mean of identifying application programs that does not depend on Identifiers used by the local operating system.

Q.70   Why is fragmentation needed on Internet not on a typical WAN?   **(4)**

Ans:
TCP/IP protocol uses the name IP datagram to refer to an Internet packet. The amount of data carried in a datagram is not fixed. The sender chooses an amount of data that is appropriate for a particular purpose. If size of a datagram is larger than network MTU than fragmentation is performed.

When a datagram is larger than the MTU of a network over which it is sent, the router divides the datagram into smaller pieces called fragments.

Fragmentation is needed on Internet as it in connection of different networks using different LAN technologies (such as Ethernet, Token ring, etc.). Each technology has a different frame size, which is Smaller to fit an entire IP datagram.

While a typical Wan is consists of electronic devices called packet switches interconnected by communication lines. The packet switches consist of special purpose hardware. A packet switch is implemented with special purpose computer that is dedicated to the task of providing communication.

Q.71   How does TCP take of wrapping over of sequence numbers?   **(4)**

Ans:
To handle out of order deliveries, transport protocols use sequencing. The sending side attaches a sequence number to each packet. The receiving side stores both the sequence number of the last packet received in order as well as a list of additional packets that arrived out of order. When a packet arrives, the receiver examines the sequence number to determine how the packet should be handled.

TCP take care of wrapping over of sequence numbers by leaving a set of consecutive sequence numbers between initial sequence numbers of two TCP connection beginning within some specified time. This duration is known as forbidden region.

Q.72   Write notes o Frame Filtering Techniques.   **(5)**

Ans:
Frame filtering:

The most valuable function performed by bridges is frame filtering. A bridge does not forward a frame unless necessary. In particular, if a computer attached to one segment sends a frame to a computer on the same segment, the bridge does not need to forward a copy of the frame to the other segment.

To determine whether to forward a frame, a bridge uses the physical address found in the frame headers. When a frame arrives on a segment, the bridge extracts and checks the destination address. If the bridge knows that the destination computer is attached to a segment over which the frame arrived, the destination will also have received a copy of the frame, so the bridge can discard a frame without forwarding a copy.

Most bridges are called adaptive or learning bridges because they learn the location of a computer automatically. The bridge uses the source address to automatically determine the location of the computer that sent a frame, and uses the destination address to determine whether to forward a frame.

Q.73   What functions connect() and accept() call in Socket interfacing?   **(5)**

Ans:
connect() system call:
clients use procedure connect to establish connection with a specific server. The form is
            connect(socket, saddress, saaddresslen)
Argument socket is the descriptor of a socket on the client's computer to use for the connection. Argument sockaddress is a sockaddr structure that specifies the server's address and protocol port number. Argument saaddresslen specifies the length of the server's address measured in octets. The client does not have to bind a local address before calling connect(). connect() internally can call bind() to connect to a local address if not done earlier.

accept() system call:
After a connection oriented server executes the listen() system call, an actual connection from some client process is waited for by having the server execute the accept() system call. The form is:

accept(sockfd, sockaddr * peer, int* addrlen)

This system call returns up to three values: an integer return code that is either an error indication or a new socket descriptor, the address of the client process (peer), and the size of this address(addrlen).
Accept automatically creates a new socket descriptor, assuming the server is a concurrent server.
When a connection request is received, the process forks, with the child process servicing the connection and the parent process waiting for the another connection request.

Q.74   Can SMTP be used as transfer protocol for Web pages? Why?   **(4)**

Ans:
SMTP is a simple mail transfer protocol. It uses ASCII text for all communication. SMTP requires reliable delivery- the sender must keep a copy of the message until the receiver has stored a copy in nonvolatile memory.

SMTP can not be used as transfer protocol for web pages as it is not necessarily use hypertext and its header needs information of sender and receiver mail ID which is not required for web pages.

Q.75   Describe the Electronic Data Exchange (EDI) architecture in brief.   **(5)**

Ans:
Electronic Data Interchange (EDI) may be most easily understood as the replacement of paper-based purchase orders with electronic equivalents. It is actually much broader in its application than the procurement process, and its impacts are far greater than mere automation.
A more careful definition of EDI is 'the exchange of documents in standardized electronic form, between organizations, in an automated manner, directly from a computer application in one organization to an application in another'**.**
Architecture for EDI
EDI can be compared and contrasted with electronic mail (email). Email enables free-format, textual messages to be electronically transmitted from one person to another. EDI, on the other hand, supports structured business messages (those which are expressed in hard-copy, pre-printed forms or business documents), and transmits them electronically between computer applications, rather than between people.
The essential elements of EDI are:
- the use of an electronic transmission medium (originally a value-added network, but increasingly the open, public Internet) rather than the dispatch of physical storage media such as magnetic tapes and disks;
- the use of **structured, formatted messages based on agreed standards** (such that messages can be translated, interpreted and checked for compliance with an explicit set of rules);

- relatively fast delivery of electronic documents from sender to receiver (generally implying receipt within hours, or even minutes); and
- direct communication between applications (rather than merely between computers).

EDI depends on a moderately sophisticated information technology infrastructure. This must include data processing, data management and networking capabilities, to enable the efficient capture of data into electronic form.

Q.76 How do active web pages work? Describe with a small example. **(5)**
Ans:
Active Web Pages:
An active document is not fully specified by the server. Instead an active document consists of a computer program that understands how to compute and display values. When a browser requests an active document, the server returns a copy of the program that the browser must run locally. When it runs the active document program can interact with the user and change the display continuously. Thus the contents of an active document are never fixed- they can continue to change as long as the user allows the program to run. Following is the example of active document using java applets.

```
import java.applet.*;
import java.awt.*;

public class clickcount extends Applet {
  int count;
  TextField f;

  public void init() {
    count = 0;
    add(new Button("Click Here"));
    f = new TextField("The button has not been clicked at all.");
    f.setEditable(false);
    add(f);
  }

  public boolean action(Event e, Object arg) {
    if (((Button) e.target).getLabel() == "Click Here") {
      count += 1;
      f.setText("The button has been clicked " + count + " times.");
    }
    return true;
  }
}
```

Figure 37.2 An example applet that counts the number of times a user clicks a button.

Q.77   Discuss the life cycle of JSP.   **(4)**

Ans:
A JSP page services requests as a servlet. Thus, the life cycle and many of the capabilities of JSP pages (in particular the dynamic aspects) are determined by Java Servlet technology

Servlet Life Cycle

The life cycle of a servlet is controlled by the container in which the servlet has been deployed. When a request is mapped to a servlet, the container performs the following steps.

1. If an instance of the servlet does not exist, the Web container
   a. Loads the servlet class.
   b. Creates an instance of the servlet class.
   c. Initializes the servlet instance by calling the `init` method.

2. Invokes the `service` method, passing a request and response object.

If the container needs to remove the servlet, it finalizes the servlet by calling the servlet's `destroy` method.

Handling Servlet Life-Cycle Events

You can monitor and react to events in a servlet's life cycle by defining listener objects whose methods get invoked when life cycle events occur. To use these listener objects, you must define the listener class.

Q.78   Discuss the WAP stack inn brief.   **(5)**

Ans:

Wap Stack implemented the protocol stack part for the WAP research and development platform. The protocol stack will be exploited in various WAP specific system components such as WAP proxy servers and gateways
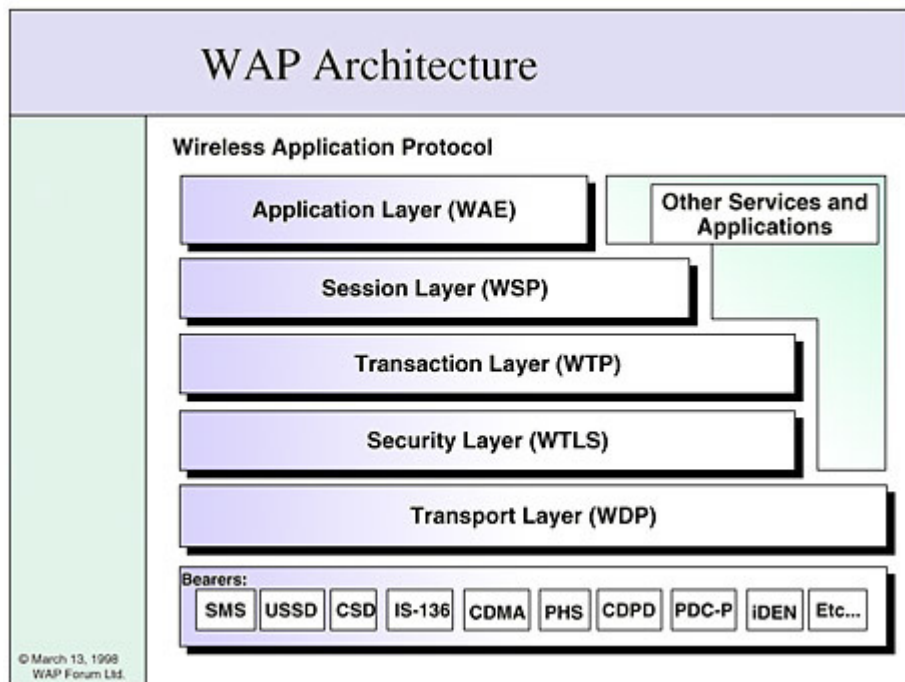
Wap Stack: WAP Architecture

WAPSTACK develops software for:

API (interface to applications/Wireless Application Environment)

WAP Forum stack layers (WSP/Session, WTP/Transaction, WTLS/Transport Layer Security, WDP/Datagram, WCMP/Control Message)

Simulation layer (simulates the behavior of an air interface and underlying communication layer protocols of a wireless data channel)

Q.79   Discuss the main tags of WML.   **(5)**

   Ans:

Tag	Definition
\<wml\> **\</wml\>**	**It defines the beginning and the ending of the page, like \<html\> \</html\>.**
\<card\> \</card\>	It defines the beginning and the ending of the card. WML pages are organized in decks and cards. A deck is a collection of cards, and cards are the basic unit of a WML page. Like a website consists of a lot of html pages and that html page is the basic unit. The id identifies this card in the deck. It has to be unique for each card in the deck. It is used to referred to this card by other cards. The next example will show you how to use it.
\<p\> \</p\>	**All text within these tags are organized in paragraph. It is required for all cards to have at least one paragraph.**
\<!--	**All text after this are comments. They are not interpreted by the browser.**
\<do\> \</do\>	This tag gives the user a general way to perform actions. It has to be defined between the card tags. It is usually placed before the first \<p\> tag. There are different actions that the user can perform as follows: The accept indicates the type of action. For this one, it is a general positive acknowledge. It's like the user clicking an Ok button.
\<go/\>	It is the action that will happen when the user performs the action. For this one, it will go the WML page that we specify. Unlike the other tags, there is no closing tag. Instead there is a slash at the end of the tag. The href indicates the destination WML page. It can be URL which will go to another deck, or for this one, another card in the same deck. An # plus the id of another card will identify that card.

<do> </do> The ontimer indicates the destination (a card or a deck) after the timer expires. Again for a card, an # is required.

<timer> This tag let you specify the value for the timer. It is an error to have two timer tags in the same card.

The value sets how much time for the timer to expire. The unit is one-tenth of a second. For the example above, the timer event will trigger after 15 seconds.

**<a> ** This tag is exactly like the <a> in HTML. It's an anchor, or a link that when the user click it, it will navigate to the next page.

The href is the place where you can set the destination. .

Q.80 Differentiate between WML-Script and Web-based scripting languages. **(4)**

Ans:
WML Script is a lightweight procedural scripting language, optimized for small-memory, low-power CPU wireless devices. It has its roots in the ECMA- Script scripting language, a standardized version of JavaScript based on core features of that language.

WML Script language constructs, syntax, flow control structures, and so on are similar to those of JavaScript because of this inheritance. It provides an optimized and extended subset of JavaScript for the narrowband wireless network-based devices like mobile phones, PDAs, and two-way pagers.

Difference between WML script and other web based languages:

o WML Script is loosely coupled with WML and can be used independently as a stand-alone tool
o The way WML Script is transferred from the WAP gateway to be executed on the wireless client is different from the way JavaScript is transferred over the Web for execution on the client browser. JavaScript is transferred in clear text, while WML Script is compiled by the WAP gateway into byte code before being transmitted to the wireless client. The advantage of this approach is that the byte code is generally much smaller in size than WML Script source code. This enables faster download of WML Script with less bandwidth consumption. It also allows low-memory capacity of the wireless device to store more application data.

o Another key difference is that the WS code isn't embedded with the WML source file but is kept as an independent module.

o WML Script doesn't support global variables; only variables declared inside functions or passed as function parameters are allowed.
o Language support for arrays is not present.
o Support for low-level binary arithmetic operations is also present in the form of bit-wise operators.

The wireless device needs a WML Script virtual machine to interpret this WS byte code. If the device doesn't contain a WS VM, it can ignore the reference to WML Script in a WML file. When the WML document interpreter comes across a reference to WML Script, it asks the WAP gateway for the referred WML Script module (compilation).

Q.81 Two computers using TDM take up turns to send 100-bytes packet over a shared channel that operates at 64000 bits per second. The hardware takes 100 microseconds after one computer stops sending before the other can begin. How long will it take for each computer to send one megabyte data file? **(5)**

Ans:
channel rate is 64000 bits/second or 8000 bytes per second.
Therefore 1000 bytes size packet will take 1000/8000 seconds that is .125 seconds.

One megabyte file will contain 1000000/1000 = 1000 packets of 1000 bytes size each. two system sending one megabyte file each means 2000 packets will be sent

Therefore, 2000 packets will take 2000 X .125 = 250.000 seconds

Hardware take 100 micro second or 0.001 seconds.

Computer send packets turn by turn between every two consecutive packets there will be 0.001 second gap for 200 packets gap is 2000 X
0.001 = 2.0 seconds.

Total time will 250 + 2 = 252 seconds a computer.

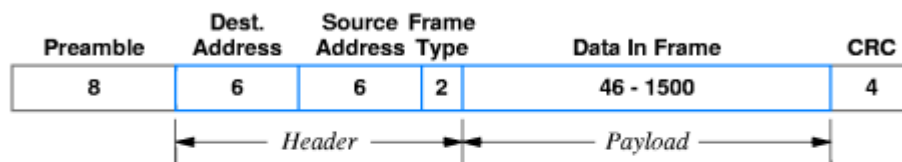**Q.82**   Compute the number of Ethernet frames formed for a data of 64 KB IP packet.   **(5)**

Ans:

Following figure illustrates the format of the Ethernet frame. Maximum data in a frame is 1500 bytes.

Number of frames formed for 64 KB IP packets is:

64*1000/1500 = 43

Preamble	Dest. Address	Source Address	Frame Type	Data In Frame	CRC
8	6	6	2	46 - 1500	4

Figure 9.3 Illustration of the frame format used with Ethernet. The number in each field gives the size of the field measured in 8-bit octets.

Q.83   Why does Ethernet specify a minimum frame size.   **(4)**

Ans:
Ethernet frame specifies a minimum frame size of 46 bytes. While a data field of zero byte is legal, it causes a problem. When a transceiver detects a collision, it truncates the current frame, which means that stray bits and pieces of frames appear on the cable all the time. To make it easier to distinguish valid frames from garbage, Ethernet specifies that valid frame must be at least 64 bytes long from destination address to checksum. If data portion of frame is less the pad field is used to fill out the frame to the minimum size.

Q.84 A router connects to at most K networks. How many routers R are required to connect to N networks? Derive an equation that gives R in terms of N and K.   **(5)**

Ans:
R = 1 if N <= K
     otherwise R = (N -1)/ (K-1) for N >K and K >=2

  it is K-1 since one network is connected to two routers. and
N- 1 is end router will also connect a network.

Q.85 How many responses does a computer expect to receive when it broadcast an ARP request? Why?   **(4)**

Ans:
An ARP request message is placed in a hardware frame and broadcast to all computer on the network. Each computer receives the request and examines the IP address. The computer mentioned in the request sends a response, all other computers process and discard the request without sending a response. So response will be obtained only from the machine for which request is being sent not fro the other machines on the network.

Q.86 Explain the technique used in the asymmetric Key Cryptography.   **(5)**

Ans:
Asymmetric or public-key cryptography differs from conventional cryptography in that key material is bound to a single user. The key material is divided into two components:

• a private key, to which only the user has access, and
• a public key, which may be published or distributed on request.

Each key generates a function used to transform text. The private key generates a private transformation function, and the public key generates a public transformation function. The functions are inversely related, i.e., if one function is used to encrypt a message, the other is used to decrypt the message. The order in which the transformation functions are invoked is irrelevant. Note that since the key material is used to generate the transformation functions, the terms *private key* and *public key* not only reference the key values, but also the transformation functions. For example, the phrase, ``*the message is encrypted using the message recipient's public key''*, means the recipient's public key transformation function is invoked using the recipient's public key value and the message as inputs, and a cipher text representation of the message is generated as output.

The advantage of a public-key system is that two users can communicate securely without exchanging secret keys. For example, assume an originator needs to send a message to a

recipient, and secrecy is required for the message. The originator encrypts the message using the recipient's public key. Only the recipient's private key can be used to decrypt the message. This is due to the computational infeasibility of inverting the public key transformation function. In other words, without the recipient's private key, it is computationally infeasible for the interceptor to transform the cipher text into its original plain text.

Q.87   Give the format of ICMP header and explain meaning of each field.   **(4)**

Ans:

Internetwork Control Message Protocol (ICMP)

Type	Code	Checksum
Data		

ICMP Header and Data

ICMP is a error reporting protocol. ICMP uses IP to transport each error message. ICMP header contains an 8-bit integer message TYPE field that identifies the message, an 8-bit CODE field that provides further information about the message type, and a 16-bit Checksum field.

Q.88   How does TCP/IP decide the size of an IP fragment? Explain.   **(4)**

Ans:
TCP/IP protocol uses the name IP datagram to refer to an Internet packet. The amount of data carried in a datagram is not fixed. The sender chooses an amount of data that is appropriate for a particular purpose. If size of a datagram is larger than network MTU than fragmentation is performed.

When a datagram is larger than the MTU of a network over whicjh it is sent, the router divides the datagram into smaller pieces called fragments and sends each fragment independently. To fragment a datagram for transmission across the network, a router uses the network MTU and datagram header size to calculate maximum amount of data that can be sent in each fragment and number of fragment that will be needed.

Q.89   Could you directly use TCP over Ethernet without using IP? Justify.   **(3)**

Ans:
Each Ethernet station has a unique, burned-in hardware address known as a Medium Access Control (MAC) address.

No matter what higher layer protocols are being used, all addressing in Ethernet must be eventually done at layer 2 as a MAC. For example, if TCP/IP is being used at layers 3 and 4, each computer will be assigned a 32-bit IP address. Before communicating, an Ethernet-attached station must resolve any IP address to a MAC address. This is done using Address Resolution Protocol, or ARP.

The address resolution protocol (ARP) is a protocol used by the Internet Protocol (IP), specifically IPv4, to map IP network address to the hardware addresses used by a data link protocol.So we cannot directly use TCP without IP over Ethernet.

Q.90   What is the largest UDP message that can fit into single Ethernet frame?
                                                                                       (3)
Ans:
UDP uses IP for delivery. Like ICMP UDP packet is encapsulated in IP datagram. So entire UDP message must fit into IP datagram, and that datagram must fit into single Ethernet frame. Maximum size of a Ethernet frame is 1500 bytes. So largest UDP message that can fit into single Ethernet frame should not be larger than 1500 bytes.
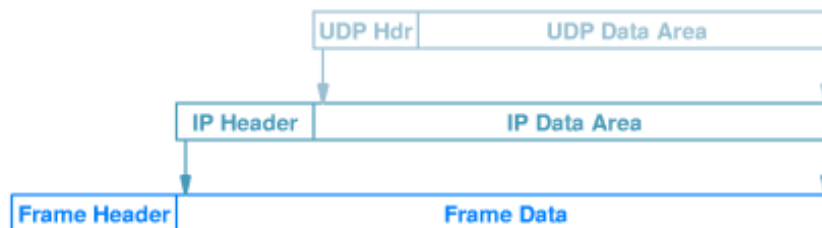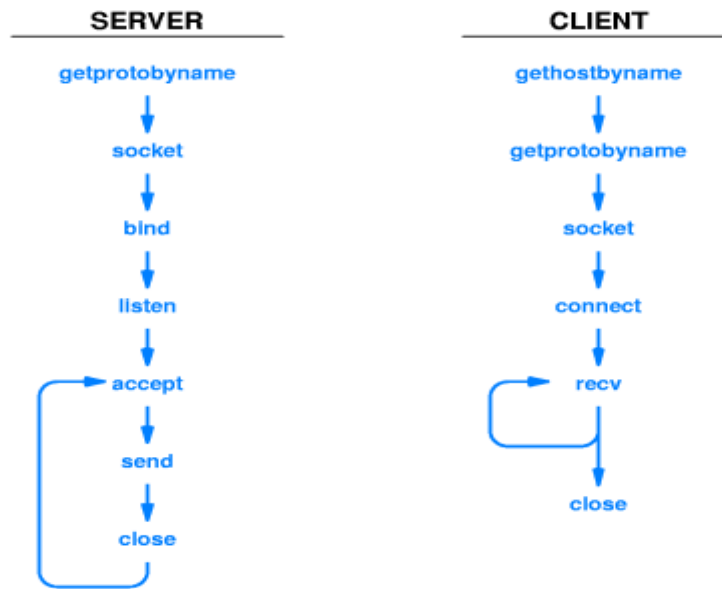

Figure 24.2 The encapsulation of a UDP message in an IP datagram. The entire UDP message, including the header and data areas resides in the data area of the IP datagram.

Q.91   Give the sequence of procedure calls for both server and client for connection-oriented application.   **(4)**

Ans:

SERVER

getprotobyname
↓
socket
↓
bind
↓
listen
↓
accept
↓
send
↓
close

CLIENT

gethostbyname
↓
getprotobyname
↓
socket
↓
connect
↓
recv
↓
close

The Sequence of Procedure calls in connection oriented communication

Q.92   Can both client and server use the same protocol port on the same computer at the same time? Explain.   **(4)**

Ans:
Client and server cannot use the same port number on the same computer at the same time. It is because two end points will be same and same port cannot be assigned to two processes. Also when a process request a port then new empty port is assigned.

Single socket bind on a remote machine can accept more than one connection from the other machine.

Q.93   Does it make sense for two domain name servers to contain exactly the same set of names? Why?   **(3)**

Ans:
Yes. It is very advantageous for two domain servers containing same set of names. If there is only one server than traffic on one server would be in tolerable, because it would be the only server to receive all the request and handle them appropriately. If there are more than one server containing same set of data then geographically closet server will respond thus reducing the load on one server. Also if one server is down due to some problem then another server containing same set of data can be used to fulfill the incoming requests.

Q.94   If voice is converted to digital form using PCM, how many bits of data will be produced in half a second?   **(3)**

Ans:
when voice is converted to digital form using PCM (Pulse Code Modulation) a device called codec (coder decoder) is used producing a 8=bit number. The codec makes 8000 samples per second. Out of 8 bits seven bits are for data and 1 bit is for control.

So data produced per second will be 7*8000=56000 bits per second and 56000/2 = 28000 bits in half a second.

Q.95   Discuss the advantages of Electronics Data Exchange (EDI).   **(4)**

Ans:
Advantages of EDI :

EDI's saves unnecessary re-capture of data. This leads to faster transfer of data, far fewer errors, less time wasted on exception-handling, and hence a more stream-lined business process. Benefits can be achieved in such areas as inventory management, transport and distribution, administration and cash management. EDI offers the prospect of easy and cheap communication of structured information throughout the government community, and between government agencies and their suppliers and clients.

EDI can be used to automate existing processes. In addition, the opportunity can be taken to rationalize procedures, and thereby reduce costs, and improve the speed and quality of services. Because EDI necessarily involves business partners, it can be used as a catalyst for gaining efficiencies across organizational boundaries. This strategic potential inherent in EDI is expected to be, in the medium term, even more significant that the short-term cost, speed and quality benefits.

Q.96   Describe architecture of WAP gateway.   **(4)**

Ans:
WAP GATEWAY :

The WAP Gateway is a very unique product providing semi-automatic redirection of HTML documents to WAP compatible mobile phones.

Wireless Application Protocol (WAP) is a global, open standard that gives mobile users access to Internet services through handheld devices. WAP Gateway, proves to be the perfect answer to the growing demand for wireless mobile services across the world.

The WAP Gateway acts as a bridge between the Internet world and the mobile world and offers services such as end-user authentication, encoding of WML pages, and WML script compiling. WAP uses the underlying web structure to render more efficient communication between content providers and mobile devices. The wireless protocol employs Wireless Markup Language (WML) for application contents instead of Hypertext Markup Language (HTML).

How WAP Gateway works
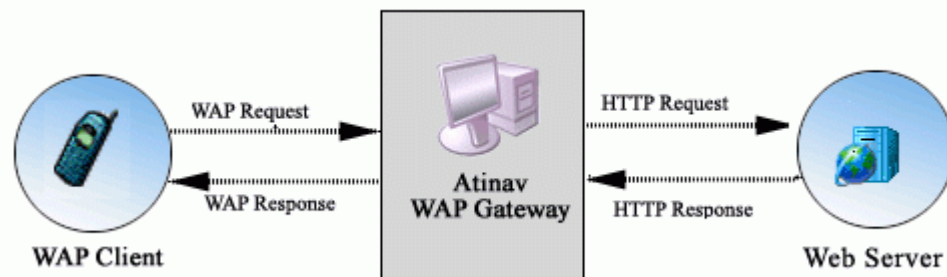
An important feature of WAP is the support of telephony service integrated with micro browsing of data. aveAccess WAP Gateway acts as a proxy between the wireless network and the Internet while encoding WAP data into byte code so as to conserve bandwidth.

Q.97   Why is XML superior to other forms of data exchange?   **(3)**

Ans:
The XML provides universal data format for integrated electronic business solutions. Relational and other database systems cannot meet all the demands of electronic business because they process data independently of its context.

Traditional databases may be well suited for data that fits into rows and columns, but cannot adequately handle rich data such as audio, video, nested data structures or complex documents, which are characteristic of typical Web content. To deal with XML, traditional databases are typically retrofitted with external conversion layers that mimic XML storage by translating it between XML and some other data format. This conversion is error-prone and results in a great deal of overhead, particularly with increasing transaction rates and document complexity.

XML databases, on the other hand, store XML data natively in its structured, hierarchical form. Queries can be resolved much faster because there is no need to map the XML data tree structure to tables. This preserves the hierarchy of the data and increases performance.

Q.98   What are the limitations of mobile devices?   **(3)**

Ans:
For mobile devices we need both PC-integrated applications and specialized mobile services rather than re purposed website content.

The latest mobile devices are agonizingly close to being practical, but still lack key usability features required for mainstream use.

Email must be reconceptualized for mobile devices. The old model of "anything sent to this address goes into this mailbox" doesn't work for mobile. We need both better filtering and a way to summarize mail that arrives at the office so you can get what you need on the road without being bogged down by a flood of non-urgent messages.

Information browsing also needs to change. Currently, the best we can hope for are websites that are basically scaled-down and redesigned to eliminate graphics and multi-column layouts. At worst, websites offer no mobile version, so you get crunched images and skinny columns that are almost impossible to read.

To cater to mobile devices, websites and services should offer

* much shorter articles,
* dramatically simplified navigation, and
* highly selective features, retaining only what's needed in a mobile setting.

Q.99   What interprets can a browser contain besides HTML and HTTP?   **(4)**

   Ans:

   Besides an HTTP client and an HTML interpreter, a browser can contain
   components that enable the browser to perform additional task. For
   example, many browsers include an FTP client that is used to access the file
   transfer services. Some browsers also contain e-mail client software that
   enables the browser to send and receive e-mail messages.

Q.100   Can we specify file transfer in a Web page? Explain with the help of
   suitable example.   **(8)**

   Ans:

   Yes, file transfer can be specified in a web page. The first field in a URL
   specifies a protocol. The URL

   ftp://ftp.cs.purdue.edu/pub/comer/netbook/client.c

   specifies that browser should use anonymous FTP to retrieve the file
   pub/comer/netbook/client.c from computer <u>ftp.cs.purdue.edu</u>.

   A URL that specifies FTP can be easily embedded I HTML consider the
   following example:

   Source code from
   <A HREF = "ftp://ftp.cs.purdue.edu/pub/comer/netbook/client.c "> an
   example client program

   </A>
   is available online.

   The program segment will be displayed as given below:

   Source code from <u>an example client program</u> is available online.

   If the user select the underlined segment, the browser uses it's FTP client to
   obtain a copy of the file client.c.

Q.101   Why is Java called Machine Independent?   **(4)**

Ans:
When a java program is compiled it is not converted into an executable code. Rather, it is converted into a byte code. Byte code is highly optimized set of instructions designed to be executed by java run time system called

java Virtual Machine (JVM). Translating a program into byte code helps make it much easier to run a program on variety of environments. Only JVM needs to be implemented for each platform. Interpreters for various platforms can interpret same byte code.

Q.102   Write an applet that can interact with both the HTTP client and HTML interpreter in a browser.   **(8)**

Ans:

```
import java.applet.*;
import java.net.*;
import java.awt.*;

public class buttons extends Applet {

   public void init() {
      add(new Button{"Yin"});
      add(new Button{"Yang"});
   }

   public Boolean action(Event e, Object arg) {
      if ((( Button) e.target).getLabel() == "Yin") {
         try {
            getAppletContext ().showDocument(new
            URL(http://www.nonexist.com/yin();
         }
         catch(Exception ex) {
         // note: code to handle the exception goes here //
         }
      }
      else if(((Button) e.target).getLabel() == "Yang") {
         try {
            getAppletContext ().showDocument(new
            URL(http://www.other.com/yang();
         }
         catch(Exception ex) {
         // note: code to handle the exception goes here //
         }
      }
```

```
        return true;
        }
}
```

Q.103   Write an HTML program segment that contains hypertext links from one
document to another.   **(8)**

Ans:

HTML allows any item to be placed as a hypertext reference. Thus a single
word, a phrase, an entire paragraph, or an image can refer to another

document. The HTML uses tags<A> and </A> for the reference. All items
between the two are the part of anchor. Consider the following example:

```
    This Article is written by
    <A HREF = http://www.ideanews.com>
    IDEA NEWS, </A>
    One of the popular newspapers worldwide.

    Contains an anchor that references the URL
        http://www.ideanews.com
    When displayed it produces the following:

    This article is written by IDEA NEWS,
    One of the popular newspapers worldwide.
```
When underlined text is selected, the document specified by the URL
http://www.ideanews.com is opened.

Q.104   Write a CGI program that prints date and time at which it was run.   **(6)**

Ans:

```
#!/bin/sh

#
# CGI script that prints the date and time at which it was run
#

# Output the document header followed by a blank line
```

```
echo Content-type: text/plain
echo

# Output the date

echo This document was created on 'date'
```

Q.105 What is the advantage of dividing an email address into two parts? **(4)**

Ans:
The division of an e-mail address into two parts is important because it achieve two goals. First, the division allows each computer system to assign mailbox identifiers independently. Second, the division permits the user on arbitrary computer systems to exchange e-mail messages. E-mail software on the sender's computer uses the second part to determine which computer to contact, and the e-mail software on the recipient computer uses the first part of the address to select a particular mailbox into which message should be placed.

**Q.106** Why can CRC detect more errors than simple Checksum? **(6)**

Ans:
There are two reasons a CRC can detect more errors than a simple Checksum. First, because an input bit is shifted through all three registers, a single bit of the message affects the resulting CRC in dramatic ways. Second, hardware uses feedback in which output from the leftmost shift register affects each exclusive or unit, the effect from a single bit of the message cycle through the shift registers more than one time.

Q.107 As IPV6 contain multiple headers, how does it know where   particular header ends and next item begins? **(7)**

Ans:
Some headers types have fixed size. For example a base header has a fixed size of exactly forty octets. To move to the item following base header, IPV6 software simply adds forty to the address of the base header. But some extension headers do not have a fixed size. In such cases, the header must contain sufficient information to allow IPV6 to determine where the header ends. The following figure illustrates the general form of an IPV6 option header.
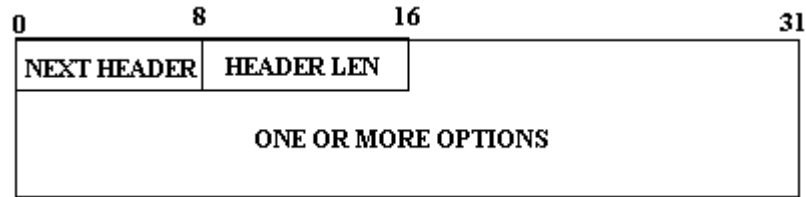
The Ipv6 option extension header. Because the size of the options header can very fro one datagram to another the HEADER LEN field specifies the exact length.

Q.108   Why is TCP called end-to-end protocol?   **(3)**

   Ans:
   TCP is called an end-to-end protocol because it provides a connection directly from an application on one computer to an application on a remote computer. The applications can request that TCP form a connection, send and receive data, and close the connection. The connections provided by TCP are called virtual connections because they are achieved in software

Q.109   IP specified that datagram can arrive in a different order than they were sent. If a fragment from one datagram arrives at a destination before all the segments from a previous datagram arrive, how does the destination know to which datagram the fragments belong?   **(6)**

   Ans:
   To solve the problem of reassembling the fragments that arrive out of order a unique identification number is placed in the IDENTIFICATION field of each outgoing datagram. When a router fragments a datagram, the router copies the identification number into each segment. A receiver uses the identification number and IP source address in an incoming fragment to determine the datagram to which the fragment belongs. In addition the fragment OFFSET field tells a receiver how to order fragments within a given datagram.

Q.110 What is the advantage of using abbreviations in DNS? **(5)**

Ans:
While using abbreviation some part of the name of the computer can be skipped. Because users tend to enter names for local computer more often, abbreviations for local names are very convenient. For example Foobar Corporation might choose to allow users to omit Foobar.com while entering a domain name.
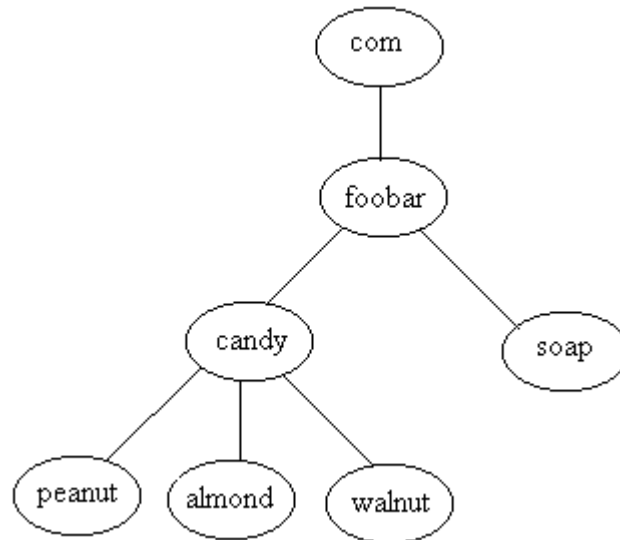
with such an abbreviation in effect, a user could enter the name venus.walnut.candy to refer to computer venus inn the walnut subdivision of the candy division in place of venus.walnut.candy.foobar.com.

Q.111 Describe ARP message format in brief. **(6)**

Ans:

0	8	16	24	31
HARDWARE ADDRESS TYPE		PROTOCOL ADDRESS TYPE		
HADDER LEN	PADDER LEN	OPERATION		
SENDER HADDER (first 4 octets)				
SENDER HADDER (last 2 octets)		SENDER PADDER (first 2 octets)		
SENDER PADDER (last 2 octets)		TARGET HADDER (first 2 octets)		
TARGET HADDER (last 4 octets)				
TARGET pADDER (all 4 octets)				

The Format of an ARP Message

The first two 16-bit fields contain values that specify the type of hardware and protocol addresses being used. For example HARDWARE ADDRESS TYPE contains 1 when ARP is used with Ethernet, and field PROTOCOL ADDRESS TYPE contains 0x0800 when ARP is used with IP. The second pair of fields HADDR LEN and PADDR LEN specify the number of octets in a hardware address and a protocol address. Field OPERATION specifies whether the message is a request or a response.

Each ARP message contains fields for two address bindings. One for the recipient and the other for the intended recipient, which ARP calls the target.

Q.112 What is the advantage or disadvantage of using INADDR_ANY instead of the IP address of the computer running on the server?   **(5)**

Ans:
Structure sockaddr_in defines the format TCP/IP uses to represent an address. Structure contains field for both an IP address and a protocol port number. Although a server can choose to fill in the IP address when specifying an IP address, doing so causes problems when a host is multi-homed because it means the server only accepts requests sent to one specific address. To allow a server to operate on a multi-homed host, the socket API includes a special symbolic constant, INADDR_ANY that allows a server to use a specific port at any of the computer's IP address.

Q.113 Is the TCP checksum necessary or could TCP allow IP to checksum thee data?   **(5)**

Ans:
Yes, TCP Checksum is necessary.
TCP layer is responsible for error detection, error control, transmission of packets if required, reassembly of packets as well as their fragmentation. Hence for all error control and detection purposes TCP Checksum is essential.

TCP cannot allow IP to checksum data however IP has its own checksum for its header. IP layer is basically responsible for routing of IP datagrams immaterial of whether that packet is intended for TCP services or UDP services. Thus immaterial of what information is contained in data part, IP layer is only responsible for routing of packets and all the issues related to error control, error detection, and flow control with regards to Routing only. Hence IP does not have a checksum for data unlike TCP.

Q.114   What is the chief advantage of CIDR over the original classful addressing scheme? **(6)**

Ans:
CIDR (Classless Inter-Domain Routing) is a new addressing scheme for the Internet, which allows for more efficient allocation of IP address than the old classful scheme.

There are a maximum number of networks and hosts that can be assigned using 32-bit classful addressing scheme. Some addresses are reserved (for broadcasting etc.), and there were a lot of wasted addresses also.

For example if you needed 100 addresses you would be assigned the smallest class addresses (class C), but that still means 154 unused addresses. The overall result was Interest was running out of unassigned addresses.

A related problem was the size of the Internet global routing tables. As the number of networks on the Internet increased, so did the number of route.

Instead of being limited to network identifiers of 8, 16 or 32 bits, CIDR currently uses prefixes any where between 13 to 27. Thus, block of addresses can be assigned to networks as small as 32 hosts or to those with over 5000,000 hosts. A CIDR address includes standard 32-bit IP address and also information on how many bits are used for the network prefix.

In the CIDR address 206.13.01.48/25, the 25 indicate the first 25 bits are used to identify the unique network leaving the remaining bits to identify the specific hosts.

CIDR addressing scheme also enables route-aggregation in which single high-level route entry can represent many lower level routes in the global routing table.
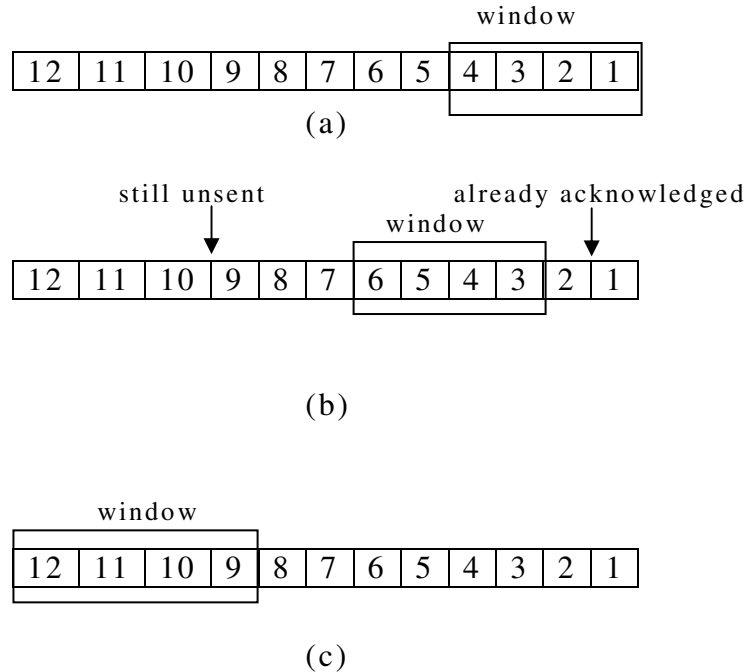
Q.115   Write short notes: **(16)**

(i)   Sliding Window Protocol.

Ans:
  To obtain high throughput rates, protocols use a flow control technique known as sliding window. The sender and receiver are programmed to use a fixed window size, which is the maximum amount of data that can

be sent before an acknowledge arrives. For example, the sender and receiver might agree on a window size of four packets.

window

| 12 | 11 | 10 | 9 | 8 | 7 | 6 | 5 | 4 | 3 | 2 | 1 |

(a)

still unsent   already acknowledged

window

| 12 | 11 | 10 | 9 | 8 | 7 | 6 | 5 | 4 | 3 | 2 | 1 |

(b)

window

| 12 | 11 | 10 | 9 | 8 | 7 | 6 | 5 | 4 | 3 | 2 | 1 |

(c)

A 4-packet window sliding through outgoing data.
(a) When transmission begins (b) after two packets has been acknowledged, and (c) after eight packets have been acknowledged.

(ii)   Digital Signature.

Ans:
This technique is used to authenticate the sender of a message. To sing a message, the sender encrypts the message using a key known only to the sender. The recipient uses the inverse function to decrypt the message. The recipient knows who sent the message because only the sender has the key needed to perform the encryption. To ensure that encrypted messages are not copied and resent later, the original message can contain date and time it was sent.

A public key system can be used to provide a digital signature.
To sign a message, a user encrypts the message using his or her own private key. To verify thee signature, thee recipient looks up thee user's public key, only the user can encrypt a message that can be encoded with the public key.

(iii)   BOOTP(Boot Strap Protocol)

Ans:
TCP/IP designer observed that many of the configuration steps could be combined into a single step if a server was able to supply more than one item of configuration information. To provide such a service BOOTP was invented.

To obtain configuration information, protocol software broadcasts a BOOTP request message. A BOOTP server that receives the request looks up several pieces of configuration information for the computer that issued the request into a single BOOTP response message, and returns the reply to the requesting computer.

(iv) Virtual Packets

Ans:
The router cannot transfer a copy of a frame from one type of network to another because the frame formats differ. More importantly, the router cannot simply reformat the frame header because the two networks may use incompatible address format.

To overcome heterogeneity, Internet protocol software defines an inter packet format that is independent of the underlying hardware. This is called virtual packet and can be transferred across the underlying hardware. The underlying hardware does not understand or recognize the Internet packet format, the protocol software creates and handles Internet packet.

Q.116   What is XML DTD (Document Type Definition)? What is the advantage of having a DTD for an XML document?   **(6)**

Ans:
DTD is a document that defines legal building blocks of an XML document. It defines the document structure with a list of legal elements. A DTD can be declared inline in your XML document, or as external reference.

Example XML document with External DTD:

```
<?xml version = "1.0"?>
<|DOCTYPE note SYSTEM "note.dtd">
<note>
<to>TOM</to>
```

```
<from>Jani</from>
<heading>Reminder</heading>
<body>Don't forget me this weekend.</body>
</note>

note.dtd
<?xml version = "1.0"?>
<|ELEMENT note (to, from, heading, body)>
<|ELEMENT to (#PCDATA)>
<|ELEMENT from (#PCDATA)>
<|ELEMENT heading (#PCDATA)>
<|ELEMENT body (#PCDATA)>
```

Why use a DTD?

XML provides an application independent way of sharing data. With a DTD, independent group of people can agree to use a common DTD for interchanging data. An application can use a standard DTD to verify that

data that an application receives from outside world is valid. An application can also use a DTD to verify it's own data.

Q.117   What is WAP? Why WAP gateways are used?   **(6)**

Ans:

Wireless Application Protocol (WAP) is a global, open standard that gives mobile users access to Internet services through handled devices. WAP Gateway proves to be the perfect answer to the growing demand for wireless mobile services across the world.

The WAP Gateway is a very unique product providing semi-automatic redirection of HTML documents to WAP compatible mobile phones.

The WAP Gateway acts as a bridge between the Internet world and the mobile world and offers services such as end-user authentication, encoding of WML script compiling. WAP uses the underlying web structure to render more efficient communication between content providers and mobile devices. The wireless protocol employs Wireless Markup Language (WML) for application contents instead of Hypertext Markup Language (HTML).

An important feature of WAP is the support of telephony service integrated with micro browsing of data. AveAccess WAP Gateway acts as a proxy between the wireless network and the Internet while encoding WAP data into byte code so as to conserve bandwidth.