Unit V

5 Application Layer

5.1 : Web

Q.1 What is web ? Explain content of web.

Ans. : • World wide web is collection of millions of files stored on thousands of servers all over the world. These files represent documents, pictures, video, sounds, programs, interactive environments.

• Following are hardware, software and protocols that make up the web.

1. A web server is a computer connected to the Internet that runs a program that takes responsibility for storing, retrieving and distributing some of the web files. A web client (web browser) is a computer that requests files from the web.
2. Well-defined set of languages and protocols that are independent of the hardware or operating system are required to run on the computers.
3. The Hyper Text Markup Language (HTML) is the universal language of the web.
4. Java is a language for sending small applications over the web. Java script is a language for extending HTML to embed small programs called scripts in web pages. The main purpose of Java and scripts is to speed up the interactivity of web pages.
5. VB script and Activex controls are microsoft system that work with IE.
6. Pictures, drawings, charts and diagrams are displayed on web using image formats such as JPEG and GIF formats.
7. The Virtual Reality Modeling Language (VRML) is the web's way of describing three-dimensional objects.

- A web page is an HTML document that is stored on a web server. A web site is a collection of web pages belonging to a particular organization.
- URL of these pages share a common prefix, which is the address of the home page of the size. Search engines are a bottom-up approach for finding your way around the web. Some search engines search only the titles of web pages. While other search every word. Keywords can be combined with Boolean operations, such as AND, OR and NOT, to produce rather complicated queries.
- Home page is the front door of a web site. When a person or organization says "My web site is at www.sangeeta.com", the URL to which they refer is the URL of the site's home page. The home page introduces the rest of the web site and provides links that leads to other pages on the site.

Q.2 Explain working of client-side and server-side of WWW.

Ans. : 1. The client side

- When a user clicks on a hyperlink, the browser carries out a series of steps in order to fetch the page pointed to.
  1. The browser determines the URL.
  2. The browser asks DNS for the IP address of www.vtubooks.com.
  3. DNS replies with 172.16.16.1.
  4. The browser makes a TCP connection to port 80 on 172.16.16.1.
  5. It then sends over a request asking for file/home/index.html.
  6. The www.vtubooks.com server sends the file/home/index.html.
  7. TCP connection is released.
  8. The browser displays all the text in home/index.html.
  9. The browser fetches and displays all images in this file.
- Fig. Q.2.1 shows the web model.

2. The server side

- The steps that the server performs.
  1. Accept a TCP connection from a client browser.

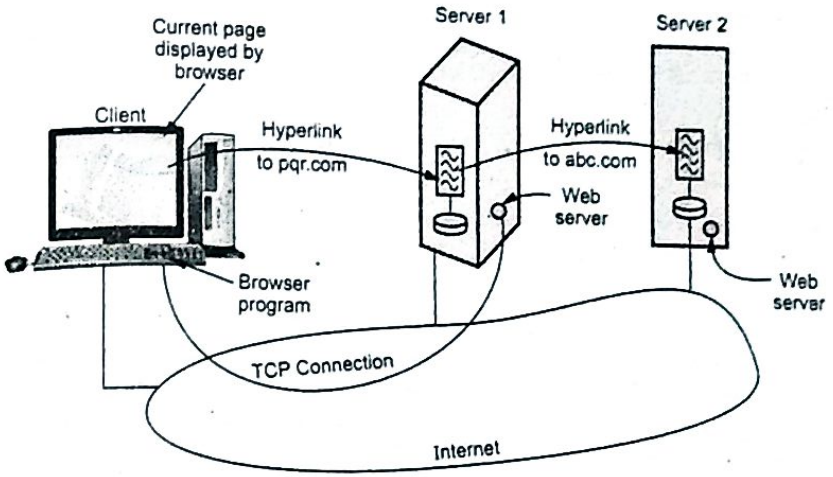


Fig. Q.2.1 Web model

2. Get the name of the file required.
3. Get the file.
4. Return the file to the client.
5. Release the TCP connection.

Q.3 What is statelessness and cookies ? Explain field used in cookies.

Ans. : • The web is basically stateless. There is no concept of a login session. The browser sends a request to a server and gets back a file. Then the server forgets that it has ever seen that particular client.

- When a client requests a web page, the server can supply additional information along with the requested page. This information may include a cookie, which is a small file. Browsers store offered cookies in a cookies directory on the client's hard disk unless the user has disabled cookies.
- Cookies are just files or strings, not executable programs. In principle, a cookie could contain a virus, but since cookies are treated as data there is no official way for the virus to actually run and do damage.
- A cookie may contain upto five fields.
  a) Domain b) Path c) Content
  d) Expires e) Secure

a) **Domain** : It tells where the cookies came from. Browsers are supposed to check that servers are not lying about their domain. Each domain may store no more than 20 cookies per client.

b) **Path** : The path is a path in the server's directory structure that identifies which parts of the server's file tree may use the cookie. It is often 1, which means the whole tree.

c) **Content** : It takes the form name = Value. Both name and value can be anything the server wants. This field is where the cookies content is stored.

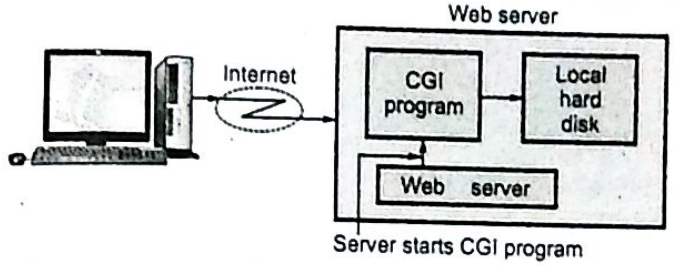
d) **Expires** : The expires field specifies when the cookies expires. If this field is absent, the browser discards the cookies when it exits. Such a cookies is called a **non-persistent cookie.** If a time and date are supplied, the cookie is said to be **persistent** and is kept until it expires.

e) **Secure** : This field can be set to indicate that the browser may only return the cookie to a secure server. This feature is used for e-commerce, banking and other secure applications.

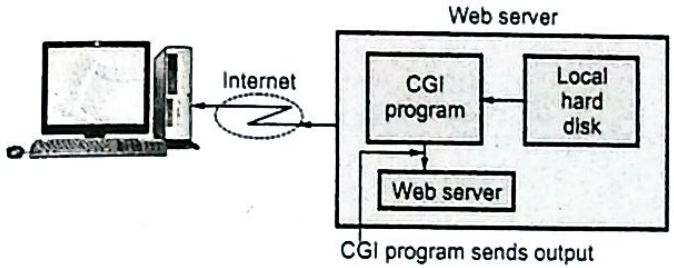
Q.4 Explain common gateway interface.

Ans. : • CGI makes dynamic computation of web pages possible. It allows a web server to associate some URLs with computer program instead of static documents on disk.

- When a browser request one of the special URLs the server runs the associated computer program and sends the output from the program back to the user. A server can have an arbitrary number of CGI programs that perform different computations.
- The server uses the URL in the incoming request to determine which CGI program to run. CGI working is as follows : CGI program is part of a web server.
- The browser sends a request to the server. If the requested URL corresponds to a CGI program, the server starts the appropriate program and passes to the program a copy of the request.
- The server then sends the output from the CGI program back to the browser in the form of reply.



(a)



(b)

Fig. Q.4.1 Illustrates the CGI concepts

- From a browser's point of view, there is no difference between a URL that corresponds to a static document and one that corresponds to a CGI program. Requests for both static documents and CGI output have the same syntatic form.

5.2 : HTTP

Q.5 Explain HTTP request and reply message format.

☞ [SPPU : May-18, Dec.-18,19, End Sem, Marks 6]

Ans. : • HTTP messages are two types

1. Request 2. Response

- Both message type used same format.
- Request **message** consists of a request line, headers and a body. Fig. Q.5.1 shows request message.

Request line

- Request line defines the

1. Request type
2. Resource
3. HTTP version

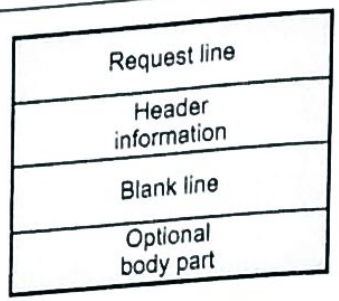


Fig. Q.5.1 Request message

- Request type categorizes the request message into several methods for HTTP version 1.1.
- Fig. Q.5.2 shows the request line.
- URL is a standard for specifying any kind of information on the internet.
- The URL define four things,

1. Method 2. Host computer 3. Port 4. Path

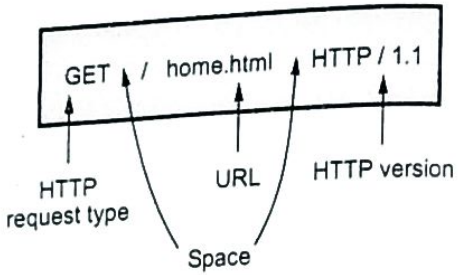


Fig. Q.5.2 Request line

- Fig. Q.5.3 shows the URL.

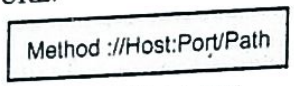


Fig. Q.5.3 (a) URL

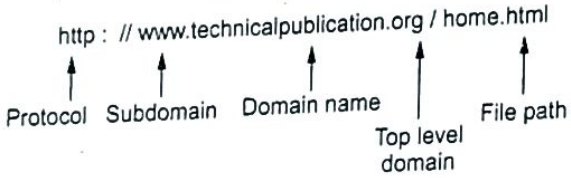


Fig. Q.5.3 (b) URL example

- The method is the prototocol used to retrieve the document. Several different protocols can retrieve a document, among them are FTP and HTTP.
- The host is the computer where the information is located, although the name of the computer can be alias. Web pages are usually stored in

computers and computers are given alias names that usually begin with the character www.

- The URL can optionally contain the port number of the server.
- Path is the path name of the file where the information is located.
- The request type field in a request message defines several kinds of messages referred to as methods.

Q.6 What is difference between persistent and non-persistent HTTP ? Explain HTTP request and reply message format.

☞ [SPPU : Dec-17, May-19, End Sem, Marks 8]

Ans. :

Sr. No.	Persistent HTTP	Non-persistent HTTP
1.	Persistent version is 1.1.	Non-persistent HTTP version is 1.0.
2.	It uses one RTT.	It uses two RTT.
3.	TCP connection is not closed.	TCP connection is closed after every request-response.
4.	Client make multiple request over the same TCP connection.	Client make multiple request over the multiple TCP connection.
5.	It is default mode.	It is not default mode.
6.	Request methods are GET, HEAD, POST, PUT, DELETE, TRACE and OPTIONS.	Request methods used are GET, POST and HEAD.

Also refer Q.5.

Q.7 Compare the salient features of HTTP and FTP.

Ans. : Comparison of salient features of HTTP and FTP

HTTP	FTP
Retrieve and view web pages	Copy files from client to server or from server to client

The "well known" TCP port for HTTP servers is port 80. Other ports can be used as well.	FTP uses TCP port 20 and port 21.
HTTP protocol is stateless.	The FTP protocol is stateful.
No built-in security mechanisms	It provides security mechanisms.
HTTP is simpler than FTP because it uses one TCP port.	FTP uses two TCP port : One data and one for control.

Q.8 I was downloading an image image1.jpg using the following URL on 2nd november, 2015 : http://www.stockphoto.com/images/image1.gif. Show HTTP request and response messages for getting the image first time.

☞ [SPPU : April-17, In Sem, Marks 5]

Ans. :

1. HTTP Request Message :

GET http://www.stockphoto.com/images/image1.gif HTTP/1.1

Host : www.someschool.edu

User-agent : Mozilla/6.0

Connection : close

2. HTTP Response Message

HTTP/1.1 200 OK

Connection close

Date : 2 November 2015 08:30:52 GMT

Server : Apache/1.3.0 (Unix)

Connection : Close

Expires : 2 November, 2015 15:31:25 GMT

Cache-Control : Max-age = 3600, public

Q.9 Browsers have a in built caching mechanism for a better user experience. How do websites indicate if a web resource needs to be cached or not ? Show HTTP messages in transit for both scenarios.

☞ [SPPU : Dec-17, May-18, End Sem, Marks 8]

Ans. : Caching or temporarily storing content from previous requests, is part of the core content delivery strategy implemented within the HTTP protocol.

- Components throughout the delivery path can all cache items to speed up subsequent requests, subject to the caching policies declared for the content.
- Caches are found at every level of a content's journey from the original server to the browser.
- Web browsers themselves maintain a small cache. Typically, the browser sets a policy that dictates the most important items to cache. This may be user-specific content or content deemed expensive to download and likely to be requested again.
- HTTP response message typically contain a last-modified header with the absolute time of the web resource e.g. an image file.
- Also optionally server may indicate an unique identifier e.g. ETag for the web resource.
- Web server's HTTP response indicates a cache-control header which will be cache-control : No-cache to indicate the browser that the web-resource cannot be cached.
- More commonly, these other headers are also added to force uniform no-caching behavior across browsers.

Q.10 Explain various header of HTTP.

Ans. : • Header can be one or more header lines. Each header line is made of a header name, a colon, a space and a header value.

- The header exchange additional information between the client and the server.
- A header line belongs to one of four categories : General header, request header, response header and entity header.
- Fig. Q.10.1 shows the header format.

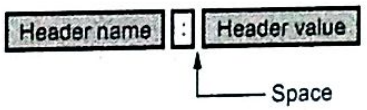


Fig. Q.10.1 Header format

- *General header* includes general information about the message. Request and a response both contains general header.
- *Response header* can be present only in a response message. It specifies the servers configuration and special information about the request.
- Request header can be present only in a request message. It specifies the clients configuration and the client preferred document format.
- *Entity header* gives information about the body of the document. It is mostly present in response messages, some request message, such as POST and PUT methods, that contain a body also use this type of header.
- Fig. Q.10.2 shows the headers.

Status line	HTTP/1.1 300 OK
General headers	Date : Wed, 8 Oct 2014 13:00:13 GMT
	Connection : Close
Response headers	Server : Apache /1.3.27
	Accept ranges : Bytes
Entity headers	Content type : Text/html
	Content length : 200
	Last modified : 2 Oct 2014 13:00:13 GMT
Blank line	
Message body	<html>
	<head>
	<title> Welcome to the India <title>
	<head>
	<body>

Fig. Q.10.2 Response message header

Q.11 Describe briefly HTTP persistent connection.

Ans. : • HTTP 1.1. made persistent connections the default mode.

- The server now keeps the TCP connection open for a certain period of time after sending a response.
- This enables the client to make multiple requests over the same TCP connection and hence avoid the inefficiency and delay of the non-persistent mode.

Types of persistent connections

- There are two versions of persistent connections :
  1. Without pipelining 2. With pipelining

Without pipelining

- The client issues a new request only when the previous response has been received.
- The client experiences one RTT in order to request and receive each of the referenced objects.
- Disadvantage : TCP connection is idle i.e. does nothing while it waits for another request to arrive. This idling wastes server resources.

With pipeling

- Default mode of HTTP 1.1. uses persistent connections with pipeling.
- Client issues a request as soon as it encounters a references. The HTTP client can make back to back requests for the referenced objects.
- It can make a new request before receiving a response to a previous request.
- When the server receives the back-to-back requests, it sends the objects back-to-back.
- It uses only one RTT.
- Pipelined TCP connection remains idle for a smaller fraction of time.
- **Persistent HTTP** connections have a number of **advantages**.
  1. By opening and closing fewer TCP connections, CPU time is saved in routers and hosts.
  2. Requests and responses can be pipelined on a connection.

3. Network congestion is reduced by reducing the number of packets caused by TCP opens.
4. Latency on subsequent requests is reduced.

Proxy server

- HTTP supports the proxy servers. A proxy server is a computer that keeps copies of responds to recent requests.
- The HTTP client sends a request to the proxy server. The proxy server checks its cache.
- If the response is not stored in the cache, the proxy server sends the request to the corresponding server.
- Incoming responses are sent to the proxy server and stored for future requests from other clients.
- The proxy server reduces the load on the original server, decreases traffic and improves latency.
- To use proxy server, the client must be configured to access the proxy instead of the target server.

5.3 : Web Caching

Q.12 What is web caching ? Explain its advantages.

Ans. : • Web caching is the activity of storing data for reuse, such as a copy of a web page served by a web server. Web caching is the storage of Web objects near the user to allow fast access, thus improving the user experience of the web surfer. Examples of some web objects are web pages, images in web pages, etc.

- Web objects can be cached locally on the user's computer or on a server on the Web. There are several types of caches for Web objects :
  1. Browser cache : Browsers' cache web objects on the user's machine. A browser first looks for objects in its cache before requesting them from the website.
  2. Proxy cache : A proxy cache is installed near the web users.

3. Transparent proxy cache : Using a "normal" proxy cache requires configuring the browser appropriately.

Advantages of web caching :

1. Faster delivery of web objects to the end user.
2. Reduces bandwidth needs and cost.
3. Reduces load on the website servers.

5.4 : DNS

Q.13 What is DNS ? Explain in brief hierarchical structure of DNS.

☞ [SPPU : Dec.-15, Marks 6]

Ans. : Domain Name System (DNS)

- The Domain Name System (DNS) is an Internet-wide distributed database that translates betweem domain names and IP addresses.
- The Domain Name System (DNS) is a hierarchical, distributed naming system designed to cope with the problem of explosive growth.
- Domain names are alphanumeric names for IP addresses e.g., www.google.com, ietf.org.

DNS hierarchy of structure

- DNS hierarchy can be represented by a tree.
- Root and top-level domains are administered by an Internet central name registration authority (ICANN)
- Below top-level domain, administration of name space is delegated to organizations.
- Each organization can delegate further.
- Domain names are hierarchical and each part of a domain name is referred to as the root, top level, second level or as a sub-domain. Different levels in DNS hierarchy are listed :

1. Top Level Domains (TLD's)
2. Second Level Domains
3. Sub-Domains
4. Host Name (a resource record)

- Fig. Q.13.1 shows DNS hierarchy.

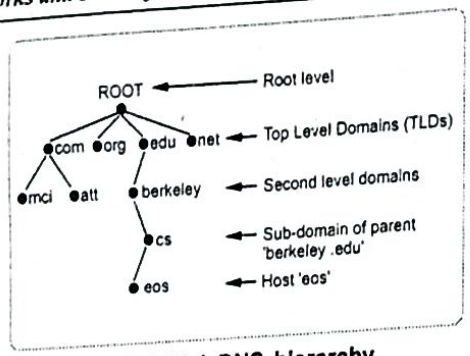


Fig. Q.13.1 DNS hierarchy

- The fully qualified domain name is split into pieces at the dots and the tree is searched starting from the root of the hierarchical tree structure.
- All resolvers start their lookups at the root, therefore the root is represented by a dot and is often assumed to be there, even when not shown.
- The resolver navigates it's way down the tree until it gets to the last, left-most part of the domain name and then looks within that location for the information it needs.
- Information about a host such as its name, its IP address and occasionally even it's function are stored in one or more zone files which together compose a larger zone often referred to as a domain.

Q.14 What is name server ? How resolver looks up a remote name ?

Ans. : • To avoid the problems associated with having only a single source of information, the DNS name space is divided into non-overlapping **zones**. When a resolver has a query about a domain name, it passes the query to one of the local name servers. If the domain being sought falls under the jurisdiction of the name server, it returns the authoritative resource records.

- An **authoritative record** is one that comes from the authority that manages the record and is thus always correct. Authoritative records are in contrast to cached records, which may be out of data.

Resolver looks up a remote name

- If the domain is remote and no information about the requested domain is available locally, the name server sends a query message to the top level name server for the domain requested.
- Consider the following example of Fig. Q.14.1. A resolver on flits.cs.vu.nl wants to know the IP address of the host india.cs.stes.edu.

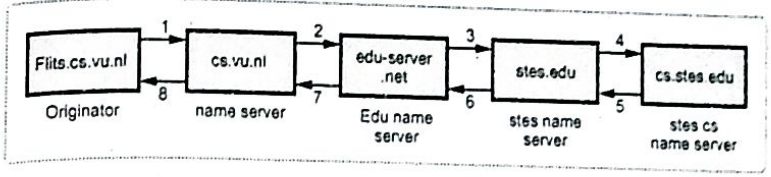


Fig. Q.14.1 Resolver looks up a remote name

Step 1 : It sends a query to the local name server, cs.vu.ne. This query contains the domain name sought, the type (A) and the class (IN).

Step 2 : The local name server has never had a query for this domain before and knows nothing about it. It may ask a few other nearby name servers, but if none of them know, it sends a UDP packet to the server for edu given in its database, edu-server.net.

Step 3 : It is unlikely that this server knows the address of india.cs.stes.edu and probably does not know cs.stes.edu either, but it must know all of its own children, so it forwards the request to the name server for stes.edu.

Step 4 : In turn, this one forwards the request to cs.stes.edu, which must have the authoritative resource records.

Step 5 - 8 : Each request is from a client to a server, the resource record requested works its way back.

- Once these records get back to the cs.vu.nl name server, they will be entered into a cache there, in case they are needed later.

Q.15 Explain DNS request and response message format.

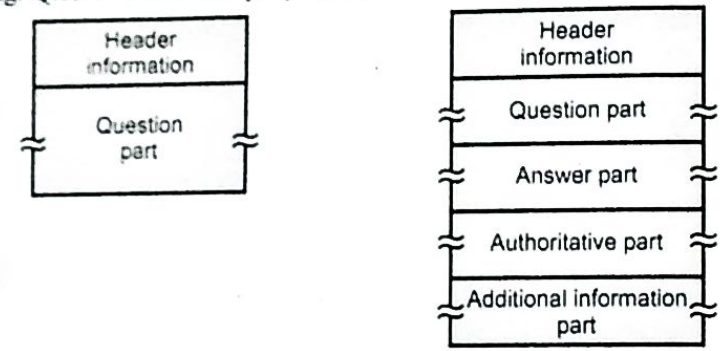
☞ [SPPU: Dec-19, End Sem, Marks 5]

OR Explain DNS message format.

☞ [SPPU : Dec-17, May-18, End Sem, Marks 4]

Ans. : • Messages are sent between domain clients and domain servers with a specific format.

- All messages of this format are used for name resolution and naming queries.
- Question sent by the client and answers provided by the server are included within different fields of the same message.
- DNS has two types of messages : Query and Response. Both types have the same format.
- The query message consists of the header and the question records, the response message consists of a header, question record, answer record, authoritative record and additional records.
- Fig. Q.15.1 shows the query and response messages.



(a) Query (b) Response

Fig. Q.15.1 Query and response message

- Fig. Q.15.2 shows the header format of the DNS. (Refer Fig. Q.15.2 on next page)
- **Identification :** It is 16 bits fields and unique value used by the client to match responses to queries.
- **Flags :** It is the collection of subfields that define the type of messages and type of the answers requested and so on.
- Number of question record contains the number of queries in the question section of the message.

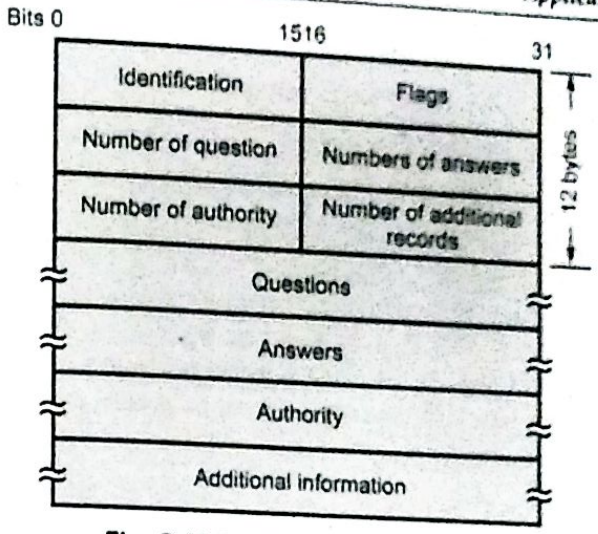


Fig. Q.15.2 General format of DNS

- Number of answer record contains the number of answer records in the answer section of the response message.
- Number of authority record contains the number of authority records in the authoritative section of the response message.
- Number of additional records contains the number of additional records in the additional section of the response message. The message has a fixed 12-byte header followed by 4 variable length fields. The identification field is set by client and returned by the server. It lets the client, match responses to requests.
- Fig. Q.15.3 shows flag fields in DNS header.

	QR	Opcode	AA	TC	RD	RA	Zero	r code
Bit	1	4	1	1	1	1	3	4

Fig. Q.15.3 Flags field in the DNS header

- The flags field is divided into 8 parts.

QR = 0 For message is a query

= 1 It is response

Opcode = 0 Standard query

= 1 Inverse query

= 2 Server status request

AA = Authoritative answer

TC = Truncated

RD = Recursive query

RA = Recursion available

r code = Return code

- RD field is 1-bit and can be set in a query and is then returned in the response. This flag tells the name server to handle the query itself, called a recursive query.
- RA is a 1-bit field and set to 1 in the response if the server support recursion. There is a 3-bit field that must be zero.
- r code is a 4-bit field. The common value are 0 for no error and 3 for name error. A name error is returned only from an authoritative name server and means the domain name specified in the query does not exist.
- The next four 16-bit fields specify the number of entries in the four variable length fields that complete the record.

Q.16 What is DNS ? Explain its various resource records with one example. ☞ [SPPU : Dec-18, May-19, End Sem, Marks 8]

Ans. : • Different types of resource records are used in DNS. An IP address has a type of A and PTR means pointer query.

- There are about 20 different types of resource records available. Some PR are listed below.

1) A = It defines an IP address. It is stored as a 32-bit binary value.
2) CNAME = "Canonical name". It is represented as a domain name.
3) HINFO = Host information, two arbitrary character strings specifying the CPU and operating system (OS).
4) MX = Mail exchange records. It provide domain willing to accept e-mail.
5) PTR = Pointer record used for pointer queries. The IP address is represented as a domain name in the in-addr.arpa domain.

6) NS = Name Server record. These specify the authoritative name server for a domain. They are represented as domain names.

Also refer Q.13.

Q.17 What is LDAP ? Explain.

Ans. : • LDAP is Lightweight Directory Access Protocol. It provides X-500 features. LDAP is an applicaion-level protocol that is implemented directly on top of TCP.

- It stores entries, which is similar to objects. Each entry must have a distinguished name, which un-equally identifies the entry. Entries can also have attributes.
- LDAP provides binary, string and time types. It allows the defination of object classes with attribute name of types. Entries are organized into a directory information tree, according to their distinguished names.
- LDAP defines a network protocol for carrying out data definition and manipulation.
- LDAP has been widely adopted, particularly for internet directory services. It provides secured access to directory data through authentication.

5.5 : Email : SMTP, MIME, POP3

Q.18 Explain email function and services in brief.

Ans. : Functions of E-mail : • E-mail system support five basic functions. They are as follows -

1. Composition 2. Transfer 3. Reporting
4. Displaying 5. Disposition

1. **Composition :** It is a process of creating messages and answers. Any text editor can be used for the body of the message. When answering a message, the e-mail system can extract the originator's address from the incoming e-mail.
2. **Transfer :** It is moving messages from the originator to the receiver.
3. **Reporting :** It inform the originator what happened to the message. Whether, email is delivered or not delivered.
4. **Displaying :** Display is required for reading the email.

5. **Disposition** is the last step and related what the receiver does with the message after receiving it. It may be read and save or delete or forward the message.

Q.19 Write short note on :
i) MIME ii) SMTP

☞ [SPPU : Dec-17,18,19, May-18, End Sem, Marks 6]

Ans. : i) MIME : Multipurpose Internet Mail Extensions : • MIME is a supplementary protocol that allows non-ASCII data to be sent through SMTP.

- MIME defined by IETF to allow transmission of non-ASCII data via e-mail.
- It allows arbitary data to be encoded in ASCII for normal transmission.
- All media types that are sent or received over the world wide web are encoded using different MIME types.
- Messages sent using MIME encoding include information that describes the type of data and the encoding that was used.
- RFC822 specifies the exact format for mail header lines as well as their semantic interpretations.
- Fig. Q.19.1 shows the working of MIME.
- MIME define five headers.
  1. MIME - Version
  2. Content - Type
  3. Content - Transfer - Encoding
  4. Content - Id
  5. Content - Description

Mail Message Header

- From : iresh@e-mail.com
- TO : rupali@sinhgad.edu
- MIME - Version : 1.0
- Content - Type : image/gif

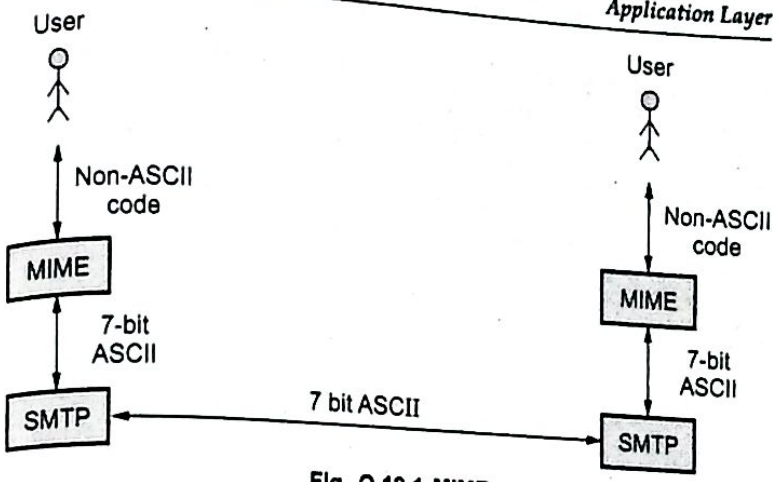


Fig. Q.19.1 MIME

- Content - Transfer - Encoding : base64

..... data for the image .....

....

....

MIME Types and SubTypes

- Each MIME content - type must contain two identifiers :
  - Content type
  - Content subtype
- There are seven standardized content-types that can appear in a MIME content - type declaration.

ii) SMTP : Simple Mail Transfer Protocol :

- SMTP is application layer protocol of TCP/IP model.
- SMTP transfers message from sender's mail servers to the recipients mail servers.
- SMTP interacts with the local mail system and not the user.
- SMTP uses a TCP socket on port 25 to transfer e-mail reliably from client to server.

- E-mail is temporarily stored on the local and eventually transfered directly to receiving server.
- Client / Server interaction follows and commond/reponse paradigm.
  a] Commands are plain ASCII text.
  b] Responses are a status code and an optional phase.
  c] Command and response lines terminated with CRLF.
- Mail client application interacts with a local SMTP server to initiate the delivery of an e-mail message.
- There is an input queue and an output queue at the interface between the local mail system and the client and the server parts of the SMTP.
- The client is concerned with initiating the transfer of mail to another system while server is concerned with receiving mail. Before the e-mail message can be transferred, the application process must be set up a TCP connection to the local SMTP server. The local mail system retains a mailbox for each user into which the user can deposit or retrieve mail. Mail handling system must use a unique addressing system.
- Addressing system used by SMTP consists of two parts : A local part and a global part. The local part is the user name and is unique only within that local mail system. Global part of the address is the domain name. Domain name is identity of the host, must be unique within the total Internet.
- SMTP uses different types of component. They are MIME and POP.

Scenario : Alice sends message to Bob

1. Alice uses User Agent (UA) to compose message and to bob@sinhgad.edu.
2. Alice's UA sends message to her mail server, message placed in message queue.
3. Client side of SMTP opens TCP connection with Bob's mail server.
4. SMTP client sends Alice's message over the TCP connection.
5. Bob's mail server places the message in Bob's mailbox.
6. Bob invokes his user agent to read message.

- SMTP uses commands and responses to transfer messages between an MTA client and an MTA server.

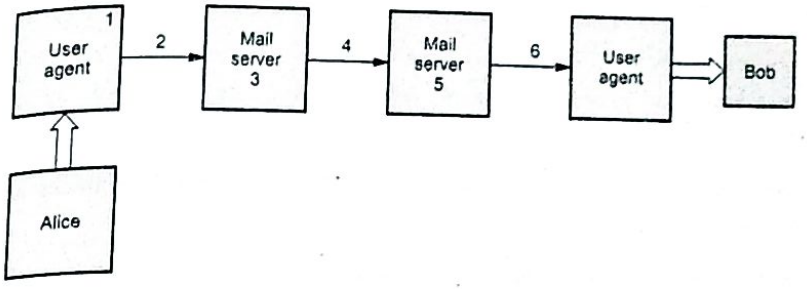


Fig. Q.19.2 Message scenario

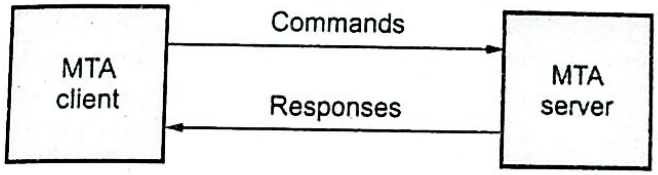


Fig. Q.19.3 Command / Response

- Each command or reply is terminated by a two character end of line token.
- Commands are sent from the client to the server. SMTP defines 14 commands. SMTP commands consist of human readable ASCII strings.

Q.20 Explain working of IMAP. ☞ **[SPPU : Dec-18, 19, End Sem, Marks 5]**

Ans. : • IMAP is the Internet Mail Access Protocol. IMAP4 is more powerful and more complex. IMAP is similar to SMTP.

- It was designed to help the user who uses multiple computers.
- IMAP does not copy e-mail to the user's personal machine because the user may have several.
- An IMAP client connects to a server by using TCP.
- IMAP supports the following modes for accessing e-mail messages :

  i) Offline mode ii) Online mode iii) Disconnected mode

Offline mode : A client periodically connects to the server to download e-mail messages. After downloading, messages are deleted from the server. POP3 support this mode.

Online mode : Client process e-mail messages on the server. The e-mail messages are stored on the server itself but are processed by an application on the client's end.

Disconnected mode : In this mode, both offline and online modes are supported.

IMAP4 provides the following extra functions :

1. User can check the e-mail header prior to downloading.
2. User can partially download e-mail.
3. A user can create, delete or rename mailboxes on the mail server.

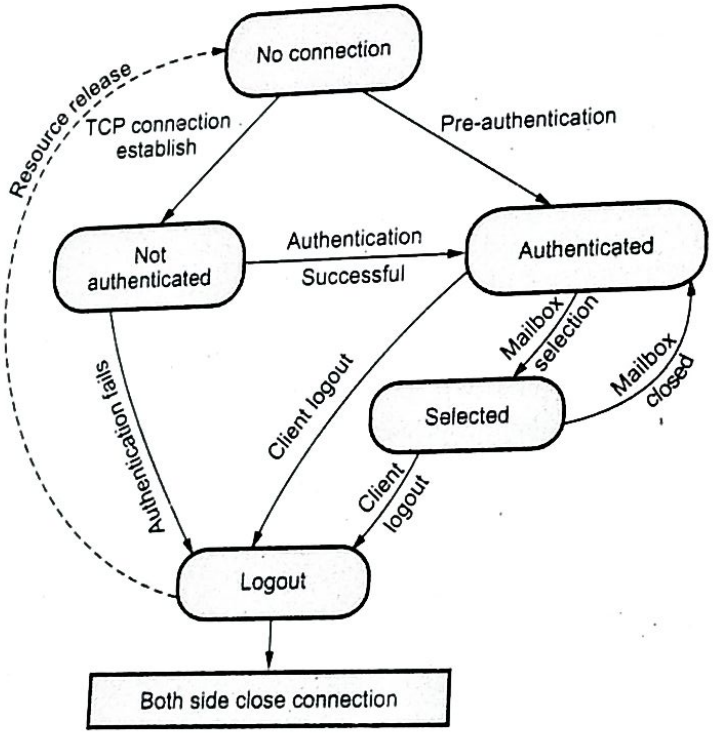


Fig. Q.20.1 IMAP state diagram

4. A user can create a hierarchy of mailboxes in a folder for e-mail storage.
5. User can search the contents of the e-mail for a specific string of characters.

- Fig. Q.20.1 shows IMAP state transition diagram. (Refer Fig. Q.20.1 on previous page)

1. **Not authenticated :** Client provides authentication information to the server.
2. **Authenticated :** Server verify the information and client is now allowed to perform operations on a mailbox.
3. **Selected :** Client is allowed to access of manipulate individual messages within the mailbox.
4. **Logout :** Client send logout command for closing IMAP session.

Q.21 State which transport layer protocol is used by following application layer protocol.
HTTP, FTP, DHCP, DNS, SMTP, TELNET.

☞ **[SPPU : April-15, (In Sem) Marks 3]**

Ans. : Application with application layer protocols is listed below.

Sr. No.	Application	Application layer protocol
1.	Email	SMTP
2.	Web	HTTP
3.	File transfer	FTP
4.	Remote Terminal Access	Telenet
5.	Remote File Server	NSF

Q.22 Compare IMAP and POP3. ☞ **[SPPU : April-15 (In Sem),Marks 4]**

Ans. : Comparison of IMAP and POP3

IMAP	POP3
In IMAP all messages from mail clients and servers are synced with each other.	There is no synchronization
IMAP uses port number 143	POP3 uses port number 110

IMAP protocol allows simultaneous access by multiple clients	POP3 protocol assumes there is only one client connected to the mailbox
The server's store is authoritative	The client's message store is considered authoritative
IMAP supports three modes : Offline mode, Online mode and disconnected mode	POP3 has two modes : Delete mode and the keep mode.

Q.23 Compare file transfer using SMTP and HTTP.

☞ [SPPU : April-15 (In Sem.), Marks 7]

Ans. : Comparison of SMTP and HTTP

SMTP	HTTP
SMTP is push protocol	HTTP is pull protocol
Multiple objects sent in multipart message	Each object encapsulated in its own response message
SMTP uses TCP port number 25	HTTP uses TCP port number 80
SMTP transfers message from sender's mail servers to the recipients mail servers	The set of requests from browsers to servers and the set of responses going back the other way
SMTP interacts with the local mail system and not the user	HTTP interact with users
SMTP is the internet protocol used to transfer electronic mail between computers	HTTP is the internet protocol used to transfer web pages between computers

Q.24 What is user agent and message transfer agent ? Explain.

Ans. : • E-mail system consists of two subsystems : User agent and MTA.

1. **User agent :** It allow user to read and send e-mail. The user agents are local program that provide a command based, menu based or graphical method for interacting with the e-mail system.

- To send an e-mail message, a user must provide the message, the destination address. The destination address should be in proper format and the user agent can deal with destination address.
- Most e-mail system support mailing lists, so that a user can send the same message to a list of people with a single command.
- For reading e-mail, the user agent will look at the user's mail box for incoming e-mail before displaying anything on the screen. It display total number of new mail.

2. **Message transfer agent :** Message Transfer Agent (MTA) move the messages from the source to the destination. MTA are system program that run in the background and move e-mail through the system. After writing the mail, user click of send icon. MTA activates at this time, MTA checks the destination address and transfer the mail to proper destination on the network.

• MTA use different types of protocol for moving the message from source to destination.

1. It must handle temporary failures, if a destination machine is temporarily unavailable, it must spool the message on the local machine for later delivery.
2. MTA must distinguish between local and remote destinations.
3. It may have to deliver copies of a message to several machines.
4. It may allow mixing text, voice and video in a message as well as appending documents and files to a message.

5.6 : FTP

Q.25 Explain FTP. Write any three FTP commands.

☞ [SPPU : May-18,19, End Sem, Marks 8, Dec.-19, End Sem, Marks 5]

Ans. : • Today, transferring files from one computer to another is one of the most common operations on internet.

• Two types of protocols needed for transferring the files on the networks : FTP and TFTP.

- File Transfer Protocol (FTP) is a standard mechanism provided by TCP/IP for copying a file from one computer to another.
- Following problems are associated with file transfer from one machine to another.
  1. Two systems may have different ways to represent text and data.
  2. Two systems may use different file name conventions.
  3. Also, these systems may have different directory structures.
- Therefore, it is necessary for the FTP to solve above mentioned problems in a very simple approach.
- For transferring a file, FTP establishes two connections between the hosts. One connection is used for data transfer and the other connection for control information (commands and responses).
- Separation of connections makes FTP more efficient.
- The data connection needs very complex rules due to the variety of data types transferred; on the other hand, the control connection uses very simple rules of communication.
- FTP uses the services of TCP as its underlying transport protocol.
- It needs two TCP connections.
- The well-known port 21 is used for the control connection and port 20 is used for the data connection.
- The following Fig. Q.25.1 shows the basic model of FTP connection. As shown in figure, the client has three components whereas the server has only two.
- It is clearly shown in Fig. Q.25.1 that the control connection is done between the control processes while the data connection is done between the data transfer processes.
- When a client starts an FTP session, the control connection remains open during the entire interactive session, while the data connection is opened when the user wants to transmit a file and it closes when the file is transferred.

Also refer Q.27.

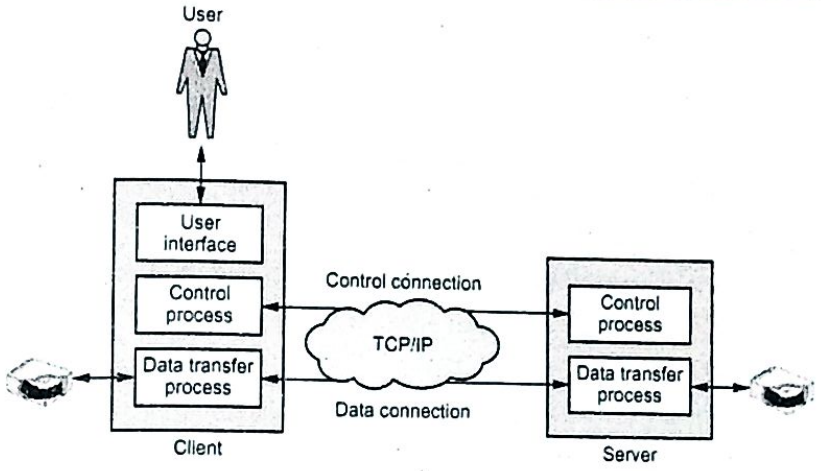


Fig. Q.25.1 FTP

Q.26 When I asked my company admin for some software he asked me to use 'anonymous FTP' and download it ? What is it ? Outline a problem scenario using it. ☞ [SPPU : April-16, (In Sem), Marks 5]

Ans. : We can configure FTP servers one of two ways :

i) Private user-only site. Allows only system users to connect via FTP and access their files.

ii) Anonymous. Allows anyone on the network to connect to it and transfer files without having an account.

- An anonymous FTP site is a computer with ftp archives permitting anyone to log on with the username : Anonymous and password : Your e-mail address.
- Assume you are required to download the file ***playgame.txt*** from *dho.cdrom.com/pub/games/*

1. At the command prompt type : ***ftp papa.cdrom.com*** (for stating ftp and connection to the site)

   The system will respond with the message

   >connected to sunsite.cnlab-switch.ch.

   >220 warchive.cdrom.com. FTP server (Version wu-2.4.2(18)

   >Thu oct 27 07:32:12 MET 2011) ready.

>Name (carchive.cdrom.com:usr) :

2. Type *ftp*

   The system will respond with something similar to.

   >331 Guest login ok, send your complete e-mail address as password

   >Password : **(type your email)**

3. After the welcome message that may look something like this.

   230 guest login ok, access restrictions apply.

   Remote system type is UNIX.

   We must now change to the directory "/pub/games"

   Type in ***cd pub*** (it will change to the directory pub), this directory contents downloadable material.

   Lets type ***dir*** to see the list of files in there we should see the directory games in the list.

   drwxr-xr-x 6 731 730 512 Nov 4 05:11 games

   The d in front of the listing tells me it is a directory. If dir does not work we can use the command : *ls-al*

4. Use 'dir' to find the file :

   Type: *dir l**

   to get a listing of all files which start with 'l'.

   You should see :

   -rw-rw-r- 1 2066 ftp-game 134868 Jun 13 2007 playgame.txt

   Because there is no 'd' at the far left, you know that it is a file, not a directory.

   The 134868 is the file size, it is 134,868 byte. It was last modified on the 13th of June 2007.

5. To download, type : *bin*

   This will make your download in 'binary' form

   This mode will always work for all files, whereas the default mode *'ascii'* will only work for text files.

Therefore always make sure you type *'bin'* before you download or you may get garbage!

6. Type : get playgame.txt

   And type 'y' when asked to confirm.

   'playgame' will now download, and will soon be on the computer you ran *'ftp'* from.

7. Alternately, if you want to download multiple files, you could type : *'mget *'*, this would download *all* files in the directory; 'mget l*' would download all files beginning with *'l'*.

8. If you do not wish to confirm each download one by one, type *'prompt'* to turn that off. If you wish to have a download indicator, type *'hash'*.

Q.27 List and explain FTP Commands.

Ans. :

Sr. No.	Command	Meaning
1.	cd	Changes the working directory on the remote host
2.	close	Closes the FTP connection
3.	quit	Quits FTP
4.	pwd	Displays the current working directory on the remote host
5.	dir or ls	Provides a directory listing of the current working directory
6.	help	Displays a list of all client FTP commands
7.	remotehelp	Displays a list of all server FTP commands
8.	type	Allows the user to specify the file type
9.	struct	Specifies the files structure

Q.28 Compare FTP with TELNET.

Ans. :

Sr. No.	FTP	TELNET
1.	FTP is a two-way system - it can be used to copy or move files from a server to a client computer as well as upload or transfer files from a client to a server.	TELNET is two –way system (with authorization) it can be used to copy or moves files from other computer.
2.	FTP systems generally encode and transmit their data in binary sets which allow for faster data transfer.	TELNET while connection client-server communication is non-coded.
3.	Commands : ASCII, Binary, Open, Del and Get.	Commands : Open, Close, Display, Status and Quit.

5.7 : TELNET

Q.29 Explain with diagram TELNET client server interaction. Also explain control characters used to control remote server.

Ans. : TELNET is a TCP applications. It provides the ability to perform remote logons to remote hosts. TELNET operates using a client and server. Fig. Q.29.1 shows TELNET client server interaction schematic.

- The client TELNET protocol is accessed through the local Operating System (OS) either by user or by a user at a terminal. It provides services to enable a user to log on to the operating system of a remote machine, to initiate the running of a program on that machine. All the commands and data entered at the user terminal are passed by the local operating system to the client TELNET process which then passes them, using the reliable stream service provided by TCP, to the correspondent server TELNET. The two TELNET protocols communicate with each other using commands that are encoded in a standard format known as network virtual terminal. The character set used for commands is

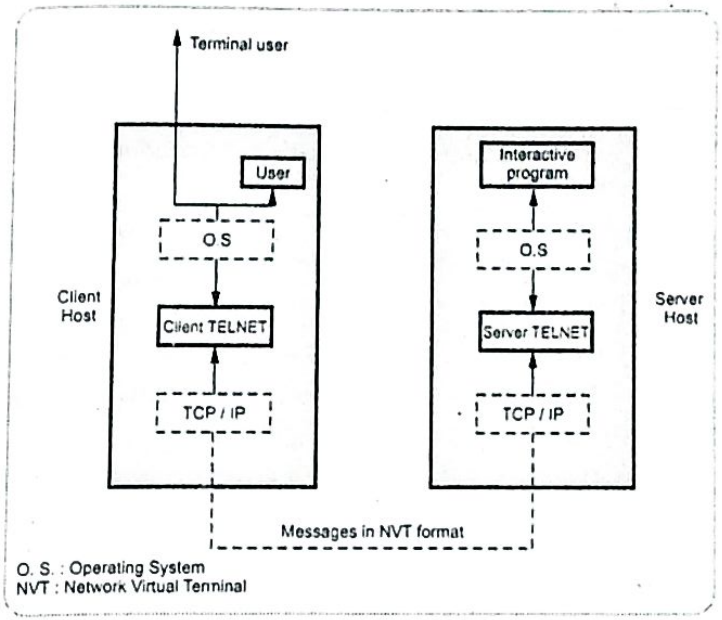


Fig. Q.29.1 TELNET client / server interaction

ASCII. All input and output data relating to an interaction is transferred as ASCII strings. If this is different from the local character set being used, the corresponding TELNET will carry out any necessary mapping functions. Thus, the two TELNET protocol entities also perform the role of the presentation layer in an OSI stack.

- Following are the Telnet commands.

Name	Code	Meaning
EOF	236	End of file
ABORT	238	Abort process
EOR	239	End of record
NOP	241	No operation
Go Ahead	249	The GA signal
IAC	255	Data byte 255

- Control characters used to control remote server in Telnet are as follows :
  1. IP : Interrupt Process which is used to interrupt the program.
  2. AO : Abort Output allows the process to continue without creating output.
  3. AYT : Are You There. It determines if the remote server is running after a long silence from server.
  4. EC : Erase Character. It is used to delete last character.
  5. EL : Erase Line. It is used to erase current line in remote host.

Q.30 What is TELNET ? Explain properties of TELNET ? What are different mode of operation used in TELNET ?

Ans. : • Client-server model can create a mechanism that allows a user to establish a session on the remote machine and then run its application. This application is known as remote login. Telnet is the example of remote login.

- TELNET (terminal network) is a protocol that provides "a general, bi-directional, eight-bit byte oriented communications facility". It is a program that supports the TELNET protocol over TCP. Many application protocols are built upon the TELNET protocol.
- A client program running on the user's machine communicates using the Telnet protocol with a server program running on the remote machine. The Telnet client program performs two important functions :
  1. Interacting with the user terminal on the local host.
  2. Exchanging messages with the Telnet server.
- The client connects to port 23 on the remote machine, which is the port number reserved for Telnet servers. The TCP connection persists for the duration of the login session. The client and the server maintain the connection, even when the user interrupts the transfer of data, for example by hitting cntl-C.
- Since Telnet is designed to work over two hosts on different platforms, the protocol assumes that the two hosts run a Network Virtual Terminal (NVT). The TCP connection is set up across these two NVT terminals.

The NVT is a very simple character device with a keyboard and a printer, data typed by the user on the keyboard is translated by the client software into NVT format and sent via its NVT terminal to the server, and data received in NVT format from the server is translated by the client into the local machine format and output to the printer.

NVT uses two types of set in TELNET :

1. Data character : It has 8 bit in which lowest bit is set as ASCII and highest order bit is 0.
2. Control character : It uses 8 bit character set in which highest order bit is set and lowest order bit is 1.

- TELNET has the following properties :
  1. Client programs are built to use the standard client/server interface without knowing the details of server programs.
  2. A client and server can negotiate data format options.
  3. Once a connection is established through TELNET, both ends of the connection are treated symmetrically.

Different modes of operation in Telnet

1. **Default mode :** It is half duplex and has become obsolete. Echoing is done by client.
2. **Character mode :** Server echoes the character back to screen and it can be delayed if transmission time is low. It also creates overhead for network.
3. **Line mode :** Line editing, Line erasing, Character erasing is done by client. It is full duplex mode.

5.8 : DHCP

Q.31 Why we need DHCP ? Explain in details.

☞ [SPPU : May-19, End Sem, Marks 8, Dec-19, End Sem, Marks 5]

Ans. : • The Bootstrap Protocol (BOOTP) is a static configuration protocol. Each client has a permanent network connection.

- When a client requests its IP address, BOOTP server checks a table that matches the physical address of the client with its IP address. The binding is predefined,

- If the client moves from one network to another then its creates a problem. BOOTP cannot handle these situations because the binding between the physical and IP addresses is static and fixed in a table until changed by the system administrator. If there is a change in a physical or IP addresses, the administrator needs to manually enter the changes.
- So, to remove the limitations of BOOTP, Dynamic Host Configuration Protocol (DHCP) is used.
- DHCP does not require an administrator to add entry for each connection to the database. DHCP provides a mechanism that allows a computer to join a new network and obtain an IP address without manual intervention. The DHCP work like plug and play networking.
- The DHCP provides static and dynamic address allocation. Static addresses are created manually whereas dynamic addresses are created automatically.
- **Static address allocation :** DHCP is backward compatible with BOOTP, which means a computer running the BOOTP client can request a static address from a DHCP server. A DHCP server has a database that statically binds physical addresses to IP addresses.
- **Dynamic address allocation :** DHCP has a pool of available IP addresses. When a DHCP client requests a temporary IP address, the DHCP server goes to the pool of available IP addresses (unused addresses) and assigns an IP address for a negotiable period of time.
- When a DHCP client sends a request to a DHCP server, the server first checks its static database. If an entry with the requested physical address exists in the static database, the permanent IP address of the client is returned. On the other hand, if the entry does not exist in the static database, the server selects an IP address from the available pool, assigns the address to the client, and adds the entry to the dynamic database.
- DHCP provides temporary IP addresses for a limited time. The addresses assigned from the pool are temporary addresses. The DHCP server issues a lease for a specific time. When the lease is expired, the

client must either stop using the IP address or renew the lease. The server has the option to agree or disagree with the renewal. If the server disagrees, the client stops using the address.

Q.32 Write short note on DHCP.

[SPPU : May-18, Dec.-17,18, End Sem, Marks 3]

Ans. : • DHCP (Dynamic Host Configuration Protocol) is a communications protocol that network administrators use to centrally manage and automate the network configuration of devices attaching to an Internet Protocol (IP) network.

- Dynamic Host Configuration Protocol (DHCP) is a client/server protocol that automatically provides an Internet Protocol (IP) host with its IP address and other related configuration information such as the subnet mask and default gateway. RFCs 2131 and 2132 define DHCP as an Internet Engineering Task Force (IETF) standard based on Bootstrap Protocol (BOOTP), a protocol with which DHCP shares many implementation details.
- DHCP allows hosts to obtain required TCP/IP configuration information from a DHCP server.
- DHCP works on a client-server model. Being a protocol, it has it's own set of messages that are exchanged between client and server.

DHCP server

- A DHCP Server assigns IP addresses to client computers. This is very often used in enterprise networks to reduce configuration efforts. All IP addresses of all computers are stored in a database that resides on a server machine.

5.9 : SNMP

Q.33 What is SNMP ? Explain management components of SNMP.

Ans. : • Network management is a technique for monitoring, testing, configuring, and troubleshooting network components so that it is used to meet a set of requirements defined by an organization.

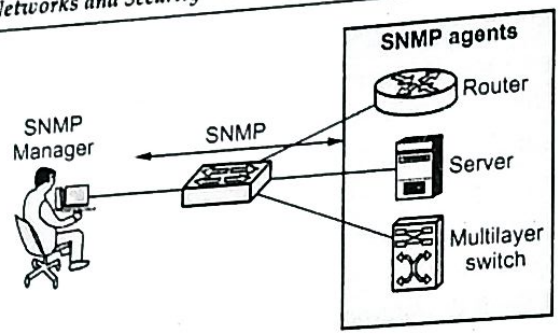


Fig. Q.33.1 SNMP concept

- The Simple Network Management Protocol (SNMP) is a framework for managing devices in an internet using the TCP/IP protocol suite. It provides a set of fundamental operations for monitoring and maintaining an internet. Devices that typically support SNMP include cable modems, routers, switches, servers, workstations, printers.
- SNMP uses the concept of manager and agent. The manager (sometimes called Network Management System) can be any machine that can send query requests to SNMP agents usually routers or servers with the correct credentials.
- SNMP is an application-level protocol in which a few manager stations control a set of agents.
- The protocol is designed at the application level so that it can monitor devices made by different manufacturers and installed on different physical networks.
- A manager is usually a host that runs the SNMP client program and an agent is usually a router that runs the SNMP server program.
- The agent keeps the information in a database such as the number of packets received and forwarded. The manager can access this database.

Management components

- To do management tasks, SNMP uses other two protocols : Structure of Management Information (SMI) and Management Information Base (MIB).

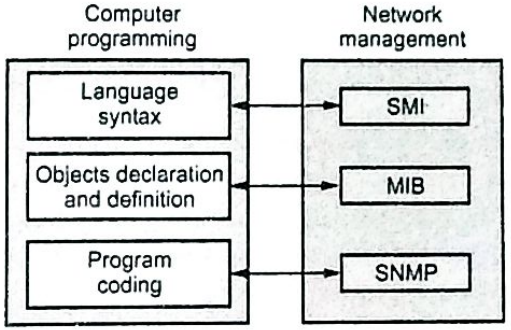


Fig. Q.33.2 Management components

- The network management components on the Internet are : SNMP, SMI, and MIB.
- **SNMP** defines the format of the packet to be sent from a manager to an agent and vice versa. It reads and changes the status of objects (values of variables) in SNMP packets.
- **SMI** defines the general rules for naming objects, defining object types (including range and length), and showing how to encode objects and values.
- **MIB** creates a collection of named objects, their types, and their relationships to each other in an entity to be managed.
- The above three network management components are exactly similar to what we need when we write a program in a computer language to solve a problem is as follows.
- Before we write a program, the syntax of the any language (such as C++ or Java) must be predefined. The language defines the structure of variables and how the variables assigned named. The language also defines the type of data to be used. In programming the rules are defined by the syntax of the language. In network management the rules are defined by SMI.
- Any computer languages require that objects be declared and defined in each specific format. For example, if a program has two variables (an integer named increment and an array named grades of type char), they

must be declared at the beginning of the program. MIB does this task in network management. MIB names each object and defines the type of the objects.

- After declaration in programming, the program needs to write statements to store values in the variables and change them whenever needed. SNMP does this task in network management. SNMP stores, changes, and interprets the values of objects already declared by MIB according to the rules defined by SMI.

Q.34 Describe SNMP messages.

Ans. :

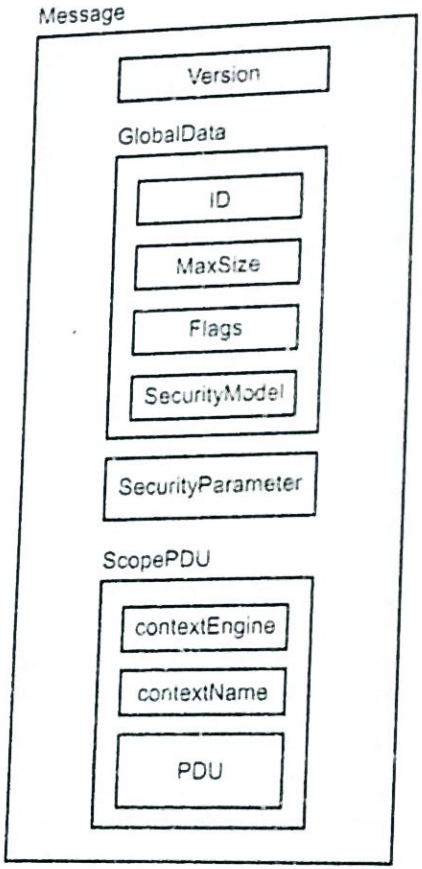


Fig. Q.34.1 SNMP messages

- SNMP does not send only a PDU but it attach the PDU in a message. SNMP message has four elements : Version, GlobalData, SecurityParameters, and ScopePDU.
- The Version field is an INTEGER data type that defines the current version.
- The GlobalData field is a sequence having four elements of simple data type : ID, Max-Size, Flags, and SecurityModel.
- Security parameter depends on the type of security used in current version3 of SNMP.
- The ScopePDU element contains two simple data type and the actual PDU.

END...