

mood-book



5

Application Layer

5.1 : Principles of Network Applications

Q.1 Explain communication for network application at application layer.

Ans. : Principles of Computer Applications

- Application layer provides the interface between the applications, use to communicate and underlying network.
- A process is a program in execution. When communicating processes are running on the same system, they communicate with each other using interprocess communication.
- Processes on two different end systems communicate with each other by message passing between computer networks.

• Fig. Q.1.1 shows communication for network application at application layer.

- Networking applications have application layer protocols. They decide the rules for communication along with message format.

Q.2 Explain Application Layer Protocols and addressing processes.

Ans. : Application Layer Protocols

- World Wide Web, electronic mail system and domain name system are the traditional application of the application layer network.
- Applications need their own protocols. These applications are part network protocol and part traditional application program.

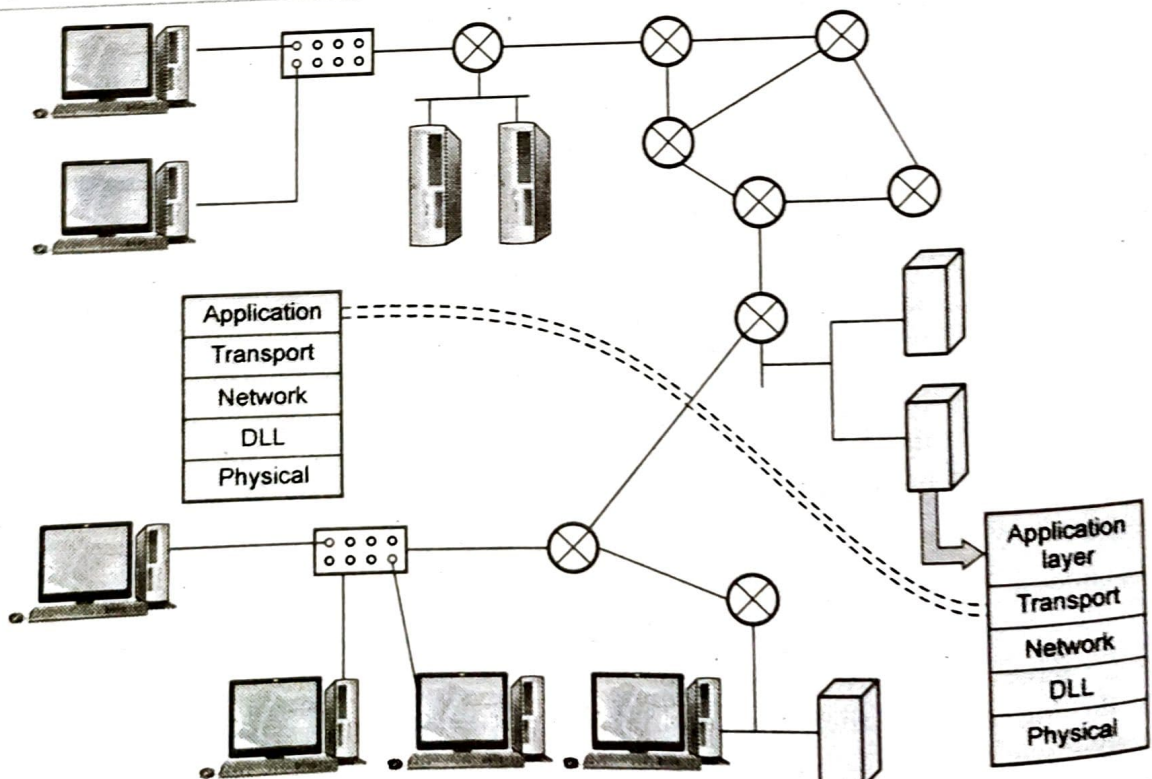


Fig. Q.1.1

- Here we study some of the most popular network applications available today. Two of the most popular applications are World Wide Web and Email system.
- Both of these applications use the request/reply method. The users send requests to servers, which then respond accordingly.
- These two application uses various protocol while exchanging the information. So it is important to distinguish between application protocols from application programs.
- Hyper Text Transport Protocol (HTTP) is an application protocol. HTTP is used to retrieve Web pages from remote servers.
- A web client uses application programs like Internet Explorer, Chrome, Firefox and Mozilla. All of them use the HTTP protocol for communication with web server.
- Widely used standardized application protocols are SMTP and HTTP
 1. Simple Mail Transfer Protocol is used to exchange electronic mail.
 2. HTTP is used to communicate between Web browsers and Web servers.

Client and Server Side Application

- Web browser is client side application of HTTP. Web server is server side application of HTTP.
- In electronic mail system, sending mail server implements the client side of SMTP and the receiving mail server implements the server side of SMTP.

Processes Communicating Across Network

- Two processes communicate with each other by sending and receiving messages. Socket is used for process communication. Socket is an interface between the application layer and transport layer within a machine.
- Socket is also referred as the application programmer's interface (API) between the application and the network. Multiple sockets might exist in each host. A port number identifies each such socket in each host.

- **Client process** : Process that initiates communication.
- **Server process** : Process that waits to be contacted.
- Application layer protocols used by both the source and destination device during a communication session. The protocols implemented on the source and destination host must match.
- The client process begins the exchange by requesting data from the server. Server responds by sending one or more streams of data to the client.

Addressing Processes

- A host (sender) uses the address of the destination host to specify where the message should sent. When data is received at the host, the port number is examined to determine which application or process is the correct destination for the data.
- Each device on a network must be uniquely defined. In Internet applications, the destination host is identified by its IP address.
- Fig. Q.2.1 shows application processes, socket and transport protocol.

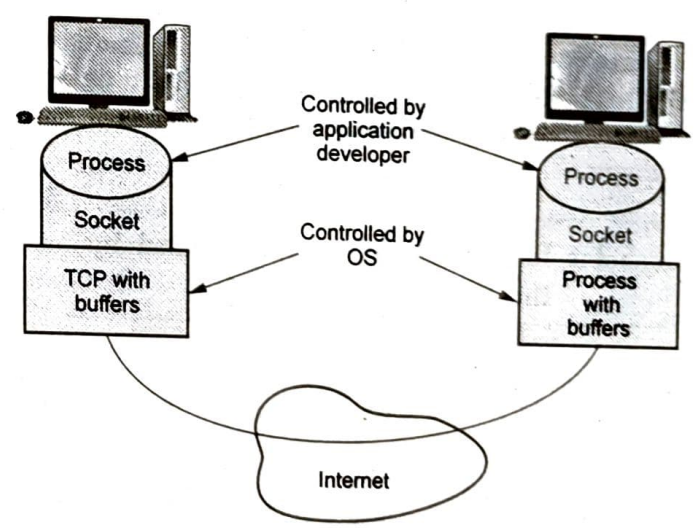


Fig. Q.2.1 Application processes, socket and transport protocol

Q.3 Types of Services Required for Application

Ans. : Types of Services Required for Application

- Application service requirements are as follows :
 1. Data Loss
 2. Bandwidth
 3. Timing

• Following application requires reliable data transfers :

- a. File transfer
- b. E-mail
- c. Remote host access
- d. Instant messaging
- e. Financial application
- f. Web document transfer

• Loss of file data creates problem. Loss of data strongly depends upon the application and coding scheme used.

Bandwidth

- Some applications like multimedia require a minimum amount of bandwidth to be effective.
- Many current multimedia applications are bandwidth sensitive.
- The application which requires little or less bandwidth, they are called *elastic applications*. Example of elastic applications are electronic mail, file transfer and remote access and web transfers.

Timing

- Some application requires low delay.
- Internet telephony, teleconferencing, multiplayer games requires tight timing constraints on data delivery.

5.2 : Transport Services Provided by the File Transfer : FTP

Q.4 Write short note on FTP.

[JNTU : Nov.-15, Marks 5]

Ans. : • File transfer is among the most frequently used TCP/IP applications and it accounts for much network traffic. File transfer software evolved into a current standard known as the File Transfer Protocol (FTP).

• FTP is designed for distributing files to a number of users. FTP uses a client-server system, in which files are stored at a central computer and transferred between that computer and other, widely distributed computers. The central computer runs FTP server software and widely distributed computer runs FTP client software.

• FTP is interactive. The FTP program accepts a sequence of commands. To interact with a remote computer, a user must identify the computer and allow FTP to establish contact.

• FTP uses TCP/IP software to contact the computer. FTP provides 58 separate commands, an average user only needs to understand the three basic commands to connect to a remote computer, retrieve a copy of a file and exit the FTP program. Fig. Q.4.1 shows working of FTP.

• The FTP server locates the file that the user requested and uses TCP to send a copy of the entire contents of the file across the Internet to the client. As the client program receives data, it writes the data into a file on the user's local disk.

• After the file transfer completes the client and server programs terminate the TCP connection used for the transfer. FTP data transfer causes more traffic on the Internet than any other application.

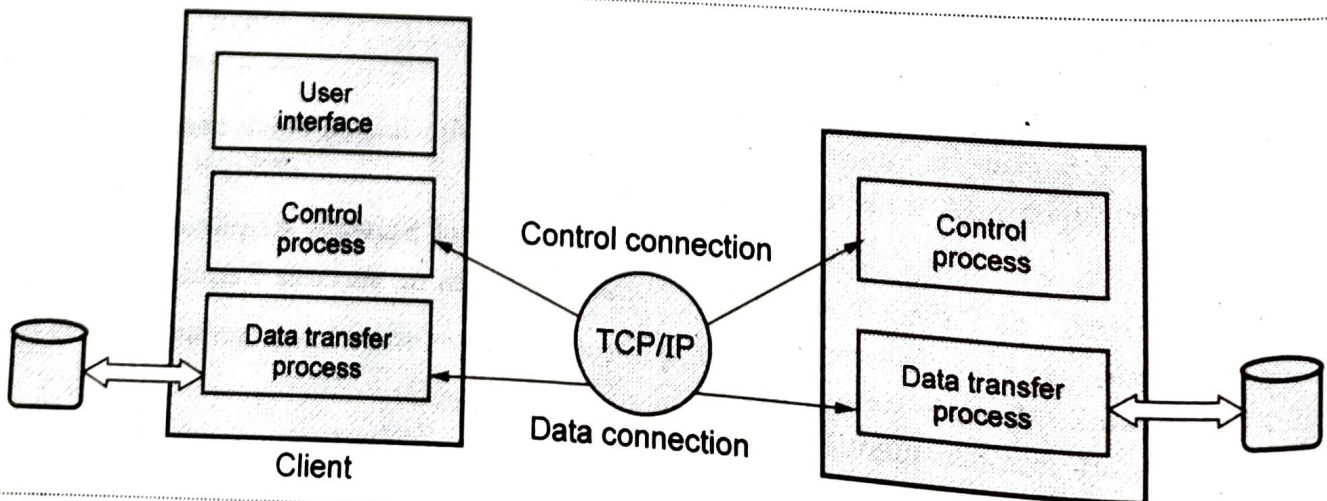


Fig. Q.4.1 FTP

Detail steps of FTP :

1. FTP client contacts FTP server at port 21 specifying TCP as transport protocol.
2. Client obtain authorization over control connection.
3. Client browse remote directory by sending commands over control connection.
4. When server receives a command for a file transfer, the server open a TCP data connection to client.
5. After transferring one file, server closes connection.
6. Server opens a second TCP data connection to transfer another file.
7. FTP server maintains state i.e. current directory, earlier authentication.

Following are the list of commands.

1. **open** : Connect to a remote computer
2. **get** : Retrieve a file from the computer
3. **bye** : Terminate the connection and leave the FTP program

When user transfer a file by either uploading or downloading-user use one of two modes. User may need to select the mode. The modes are as follows.

- 1) ASCII mode
- 2) Binary (Image) mode

• ASCII mode is used for transferring a text files including HTML files. Different computer systems use different characters to indicate the ends of lines. In ASCII mode, the FTP software automatically adjusts line endings for the system to which the file is transferred.

• In binary mode, transferring of files consists of anything but unformatted text. In this mode, the FTP software does not make any changes to the contents of the file during transfer. Use binary mode when transferring graphic files, audio files, video files, program or any other kind of file other than plain text.

• Choosing between binary and ASCII transfer can be difficult. When unsure about the content of file, enter the FTP command binary before transferring the file. FTP uses the client-server approach.

• A user invokes an FTP program on the computer, instructs it to contact a remote computer and then

requests the transfer of one or more files. The local FTP program becomes a client that uses TCP to connect on FTP server program on the remote computer.

- Each time the user requests a file transfer, the client and server programs co-operate to send copy of the data across the Internet.

Q.5 What is anonymous FTP ?

Ans. : • Many FTP servers allow "anonymous" access. Usually these servers will only allow you to download anonymously and will prohibit uploading.

- To connect with an anonymous FTP server :

1. Use "anonymous" for the login name
2. Use your email address for the password

• Anonymous FTP is a service that does not require a unique username and password to log in. Any user can log in using the username "anonymous" and typically use their email address as the password. Some anonymous FTP services allow the password field to be left blank. DreamHost allows this feature as well.

• In comparison to a standard FTP user created in the panel, an Anonymous FTP user is generally used to upload/download content to a directory on your domain defined by you when setting up the service. This service can be very useful if you require multiple users to upload/download files from your domain.

Q.6 Describe the functions of the two FTP connections.

Ans. : • FTP requires two connections for data transfer : A control connection and a data connection.

• FTP client contacts FTP server at port 21 specifying TCP as transport protocol. Client obtain authorization over control connection. Client browse remote directory by sending commands over control connection.

• The control connection is established in the normal client-server fashion. The server does a passive open on the well-known port for FTP (21) and waits for a client connection. The client does an active open to TCP port 21 to establish the control connection.

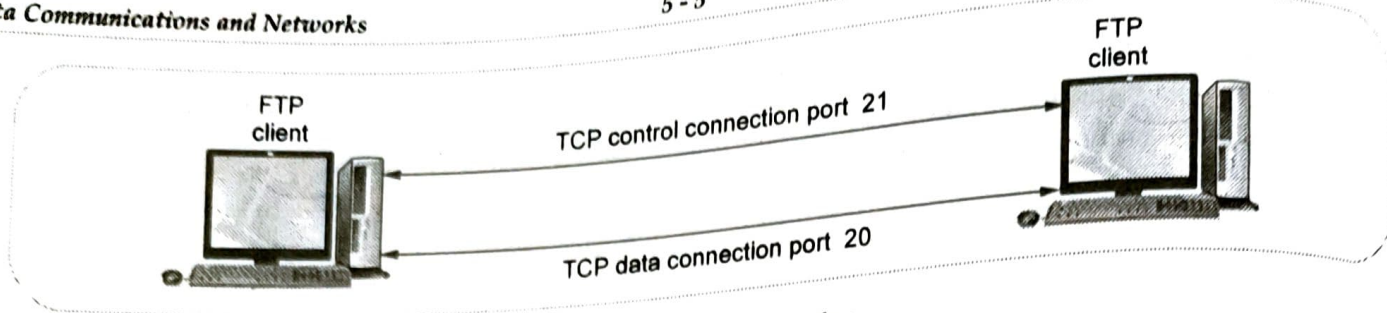


Fig. Q.6.1 Data connection

- The control connection stays up for the entire time that the client communicates with this server. This connection is used for commands from the client to the server and for the server's replies.
- A data connection is created each time a file is transferred between the client and server

Q.7 How does storing a file differ from retrieving a file? What kind of file types can FTP transfer?

Ans. : FTP transfer following types of file :

a) **ASCII file type :** The text file is transferred across the data connection in NVT ASCII. This requires the sender to convert the local text file into NVT ASCII, and the receiver to convert NVT ASCII to the local text file type. The end of each line is transferred using the NVT ASCII representation of a carriage return, followed by a linefeed. This means the receiver must scan every byte, looking for the CR, LF pair.

b) **EBCDIC file type :** An alternative way of transferring text files when both ends are EBCDIC systems.

c) **Image file type :** Also called binary file. The data is sent as a contiguous stream of bits. Normally used to transfer binary files.

d) **Local file type :** A way of transferring binary files between hosts with different byte sizes. The number of bits per byte is specified by the sender. For systems using 8-bit bytes, a local file type with a byte size of 8 is equivalent to the image file type.

Also refer Q.14.

5.3 : Electronic Mail in the Internet and SMTP

Q.8 How would you summarize the concept of E-mail, its architecture and services.

[JNTU : Dec.-16, Marks 10]

OR Describe the various parts of e-mail address and show the process of sending and receiving e-mails.

[JNTU : Dec.-18, Marks 10]

OR What is an Electronic mail? Explain the two scenarios of architecture of E-mail.

[JNTU : June-19, Marks 5]

Ans. : • E-mail is an asynchronous communication medium. Electronic mail is used for sending a single message that includes text, voice, video or graphics to one or more recipients.

- Electronic mail is fast, easy to distribute and inexpensive.
- Simple Mail Transfer Protocol (SMTP) is the standard mechanism for electronic mail in the internet. SMTP is the TCP/IP mail delivery protocol.
- E-mail is not a real-time service in that fairly large delays can be tolerated.
- It is also not connection oriented in that a network connection does not need to be setup expressly for each individual message.
- Fig. Q.8.1 shows the high-level view of the internet e-mail system.
- Mail server handles incoming and outgoing mails.
- The Post Office Protocol (POP) servers store incoming mail while SMTP servers relay outgoing mails.
- The Internet Service Provider (ISP) probably runs both an SMTP server and POP server for its customers.

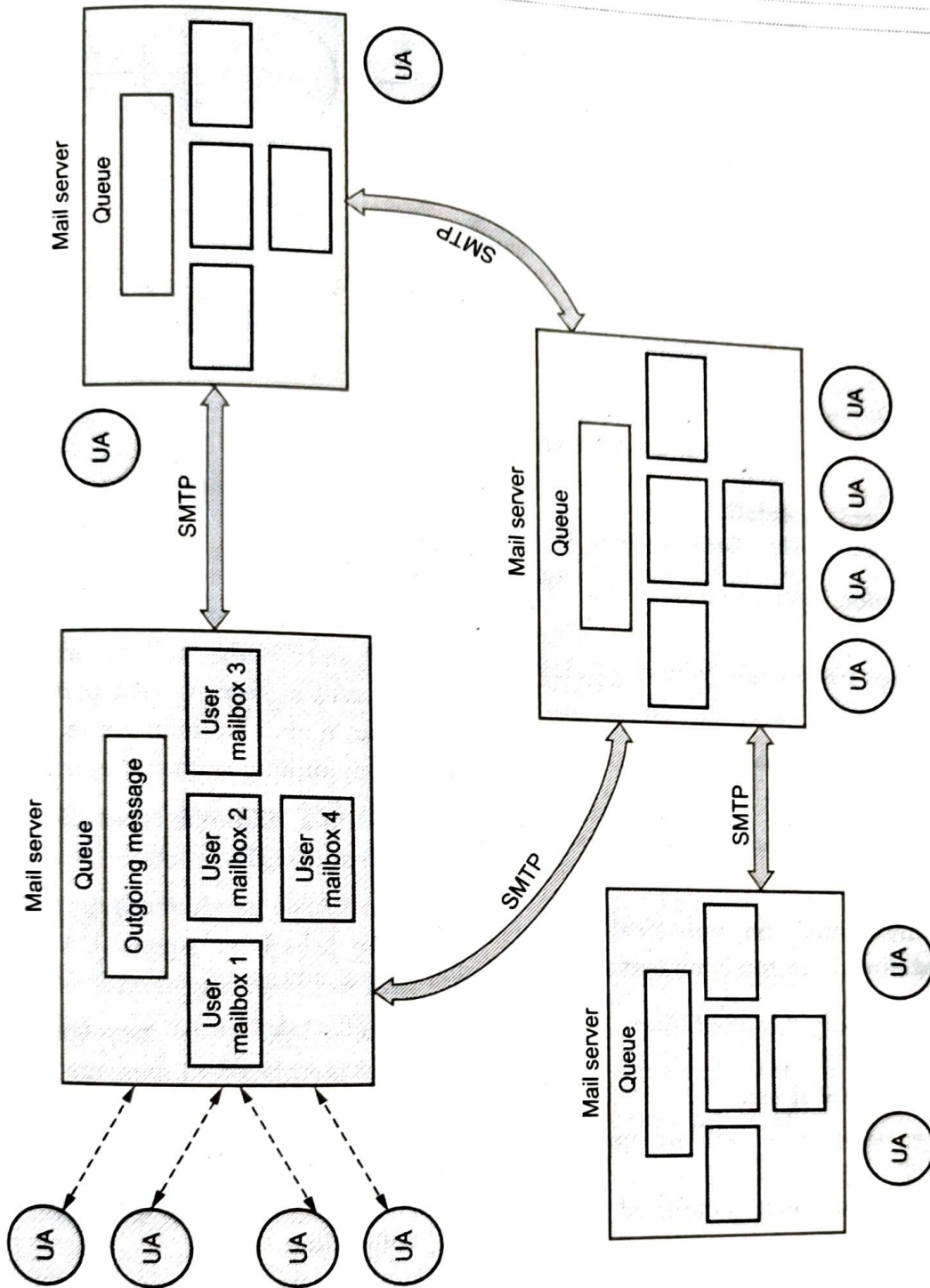


Fig. Q.8.1 View of e-mail system

Following are the ways to access the e-mail.

1. Web based e-mail service.
2. E-mail through a LAN.
3. Unix shell account.
4. Using mail client.

Components

Three major components are

1. User agents.
2. Mail servers.
3. SMTP

Fig. Q.8.2 shows the components of an e-mail system.

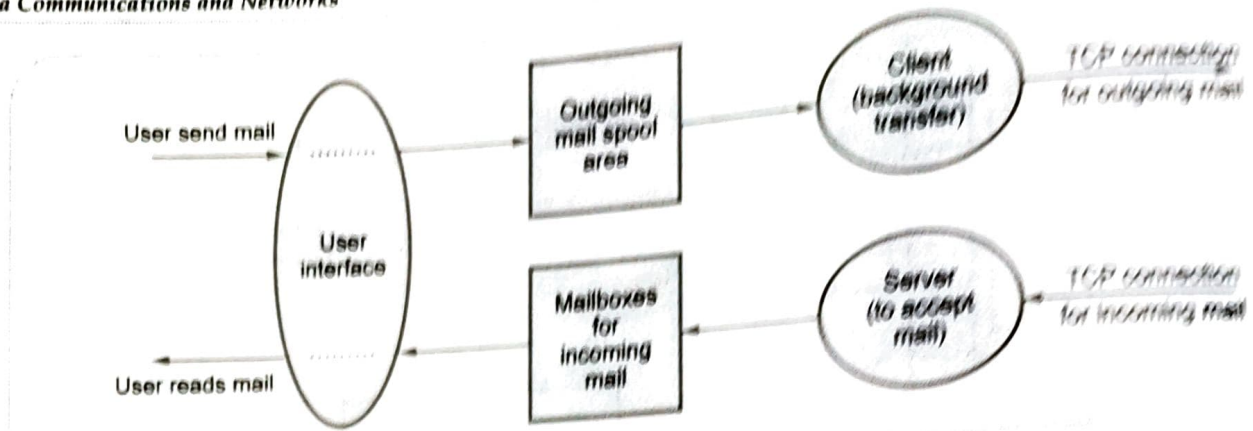


Fig. Q.8.2 Component of e-mail system

Q.9 Explain SMTP protocol in detail.

☞ [JNTU : Dec.-16, Marks 7]

Ans. : • 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 transferred directly to receiving server.
- Client/Server interaction follows a command/response 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 the 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.
 - 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.

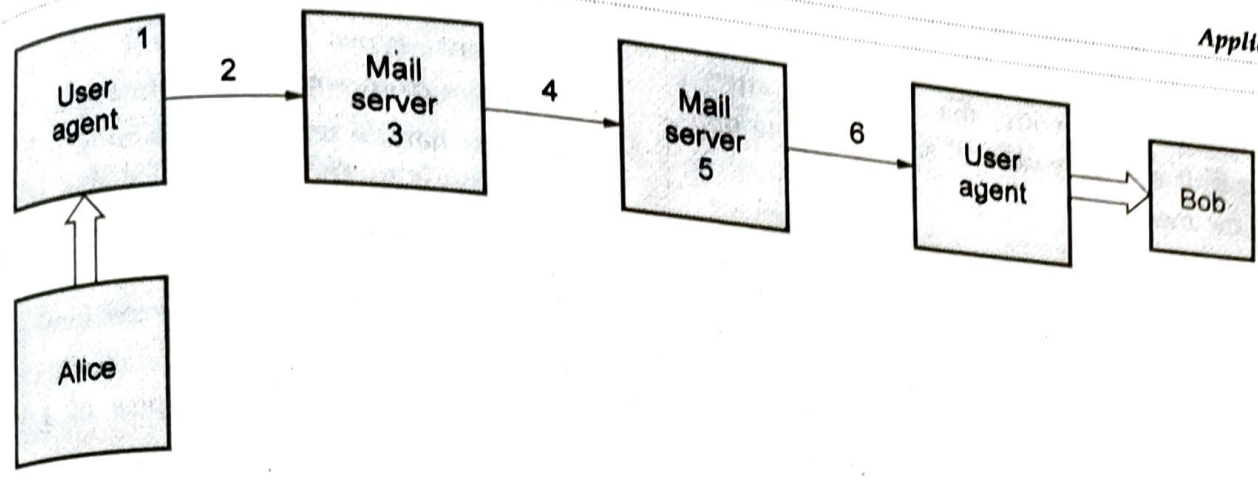


Fig. Q.9.1 Message scenario

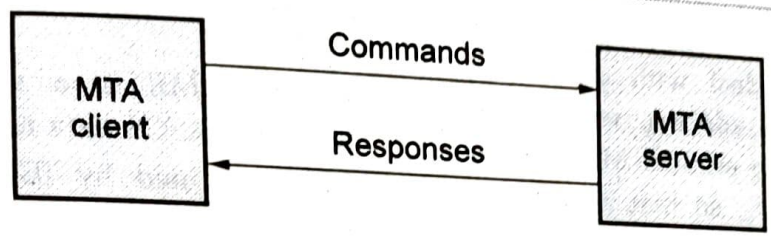


Fig. Q.9.2 Command / Response

SMTP commands consist of human readable ASCII strings.

SMTP commands are

- i) **HELO** : Initiate a mail transaction, identifying the sender to the recipient.
- ii) **MAIL FROM** : Tells the remote SMTP that a new mail transaction is beginning.
- iii) **RCPT TO** : The sending SMTP sends a RCPT command for each intended receiver.
- iv) **DATA** : If accepted, the sender transfers the actual message. End of message is indicated by sending a " • " on a line by itself.
- v) **QUIT** : Terminate the connection.

10 List and explain functions of electronic mail.

• E-mail system support five basic functions. They are as follows.

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

- 1. Composition refers to the 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 refers to moving messages from the originator to the recipient.
- 3. Reporting has to do with telling the originator what happened to the message. Whether, email is delivered or not delivered.
- 4. Displaying incoming messages is needed, so user can read their email.

Data Communications and Networks

5. Disposition is the final step and concerns what the recipient does with the message after receiving it. It may be read and save or delete or forward the message.

Q.11 Write short note on user agent and message transfer agent.

Ans. : E-mail system consists of two subsystems :

1. User agent
2. Message transfer agent.

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. Details of e-mail address, we already studied in email addressing section. 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.

Q.12 What is MIME ? Explain content type used in MIME.

Ans. : • 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 arbitrary data to be encoded in ASCII for normal transmission.
- All media types that are sent or received over the world wide web (www) 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.12.1 shows the working of MIME.

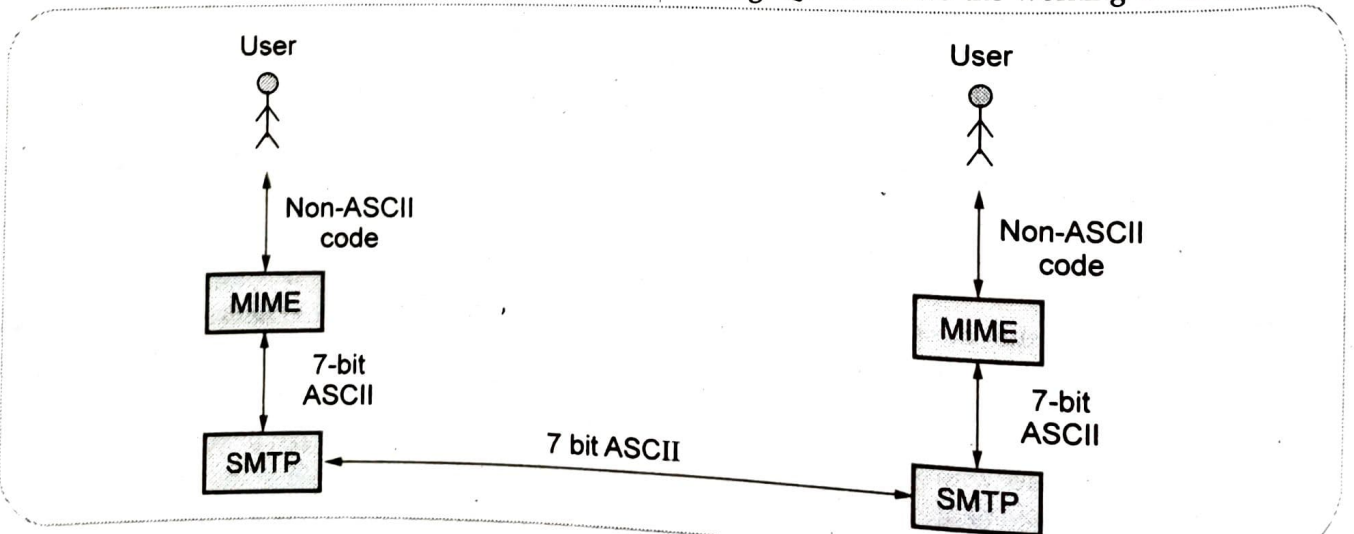


Fig. Q.12.1 MIME

• 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

• 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.

Type	Subtype	Description
Text	Plain	Unformatted text.
Multipart	Mixed	Body contains ordered parts of different data types.
	Parallel	Same as above, but no order.
	Digest	Similar to mixed, but the default is message.
	Alternative	Parts are different versions of the same message.
Video	MPEG	Video is in MPEG format.
Audio	Basic	Single channel encoding of voice at 8kHz. (Sound file)
Image	JPEG	Image is in JPGE format.
	GIF	Image is in GIF.
Message	Partial and external body	An entire e-mail message or an external reference to a message.

Application Layer

Application	Postscript	Adobe postscript.
	Octet stream	General binary data.

Content - Transfer Encoding

• This header defines the method to encode the messages into 0 and 1 for transport.

Content-Transfer-Encoding : < Type >

The five types of encoding is listed below.

Type	Description
7-bit	ASCII characters and short lines.
8-bit	Non-ASCII characters and short lines.
Binary	Non-ASCII characters with unlimited length lines.
Base 64	6-bit blocks of data are encoded into 8-bit ASCII characters.
Quoted printable	Non-ASCII characters are encoded as an equal sign followed by an ASCII code.

Q.13 Write short note on IMAP.

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

- 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
- i) **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.
- ii) **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.
- iii) **Disconnected mode** : In this mode, both offline and online modes are supported.

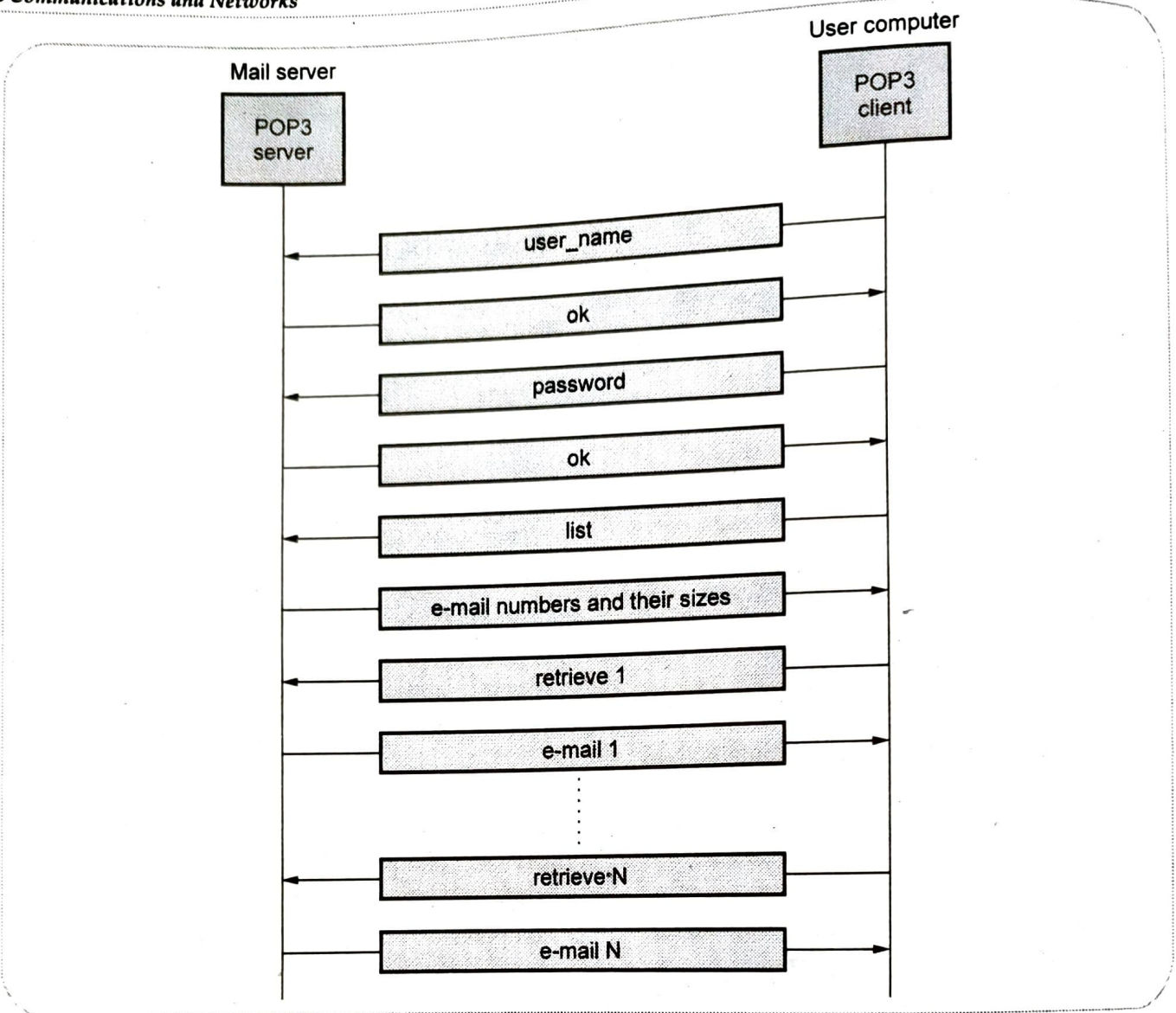


Fig. Q.13.1 POP3

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.
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.

5.4 : HTTP

Q.14 Write Short notes on : HTTP.

[JNTU : May-13, Marks 5]

OR Explain request and response messages of HTTP.

[JNTU : Dec.-16, Marks 8]

Ans. : • The standard web transfer protocol is Hyper Text Transfer Protocol (HTTP).

- The HTTP protocol consists of two fairly distinct items : The set of requests from browsers to servers and the set of responses going back the other way.
- All the newer versions of HTTP support two kinds of requests : Simple requests and full requests. A simple request is just a single GET line naming the page desired, without the protocol version. The response is just the raw page with no headers, no MIME, and no encoding.

- HTTP uses the services of TCP. HTTP is a stateless protocol.
- The client initializes the transaction by sending a request message. The server replies by sending a response.
- Request message consists of a request line, headers and a body. Fig. Q.14.1 shows request message.

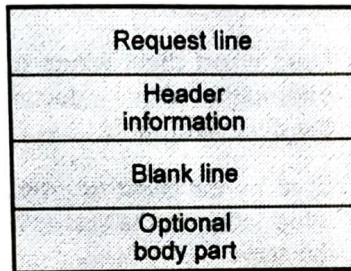


Fig. Q.14.1 Request message

- Request line defines the Request type, Resource and HTTP version.
- Request type categorizes the request message into several methods for HTTP version 1.1.
- Response Message : Fig. Q.14.2 shows the response message. It contains a status line, a header and body.

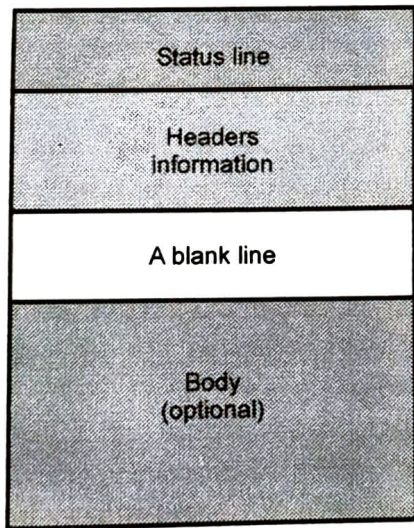


Fig. Q.14.2 Response message

- Status line defines the status of the response message. It consists of the HTTP version, Space, Status code and Status phrase.
- 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.

Q.15 Define the following :

- a) General header b) Response header
- c) Request header d) Entity header

Ans. : a) General header gives general information about the message and can be present in both a request and a response.

b) Response header can be present only in a response message. It specifies the servers configuration and special information about the request.

c) Request header can be present only in a request message. It specifies the clients configuration and the client preferred document format.

d) 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.

Q.16 Explain difference between persistent and non persistent HTTP.

Ans. : Difference between Persistent and Non-persistent

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.

Q.17 What is round trip time ? How it is calculated ?

Ans. : • RTT is the time it takes for a small packet to travel from client to server and then back to the

includes packet propagation delays, packet queuing delays in intermediate routers and switches and packet processing delays.

- Fig. Q.17.1 shows operation when user clicks on a hyperlink.
- Browser to initiate TCP connection between the browser and the web server. It requires three way handshake.
- The client sends a small TCP segment to the server. The server acknowledges and responds with a small TCP segment.
- Finally, the client acknowledges back to the server.
- The initial design HTTP 1.0 uses nonpersistent connections. The TCP connection is closed after each request/response interaction.
- Each subsequent request from the same client to the same server involves the setting up and tearing down of an additional TCP connection.

Q.18 Explain any five HTTP commands

Ans. :

Sr. No.	Method	Purposes
1.	GET	Used when the client wants to retrieve a document from the server. Server responds with the contents of the document.
2.	HEAD	Used when client wants some information about a document but not the document itself.
3.	POST	Used by the client to provide some information to the server i.e. input to the server.
4.	PUT	Used by the client to provide a new or replacement document to be stored on the server.
5.	PATCH	Similar to PUT except that the request contains a list of differences that should be implemented in the existing file.
6.	DELETE	Removes a document on the server.
7.	COPY	Copies a files to another location. URL gives the location of the source file.

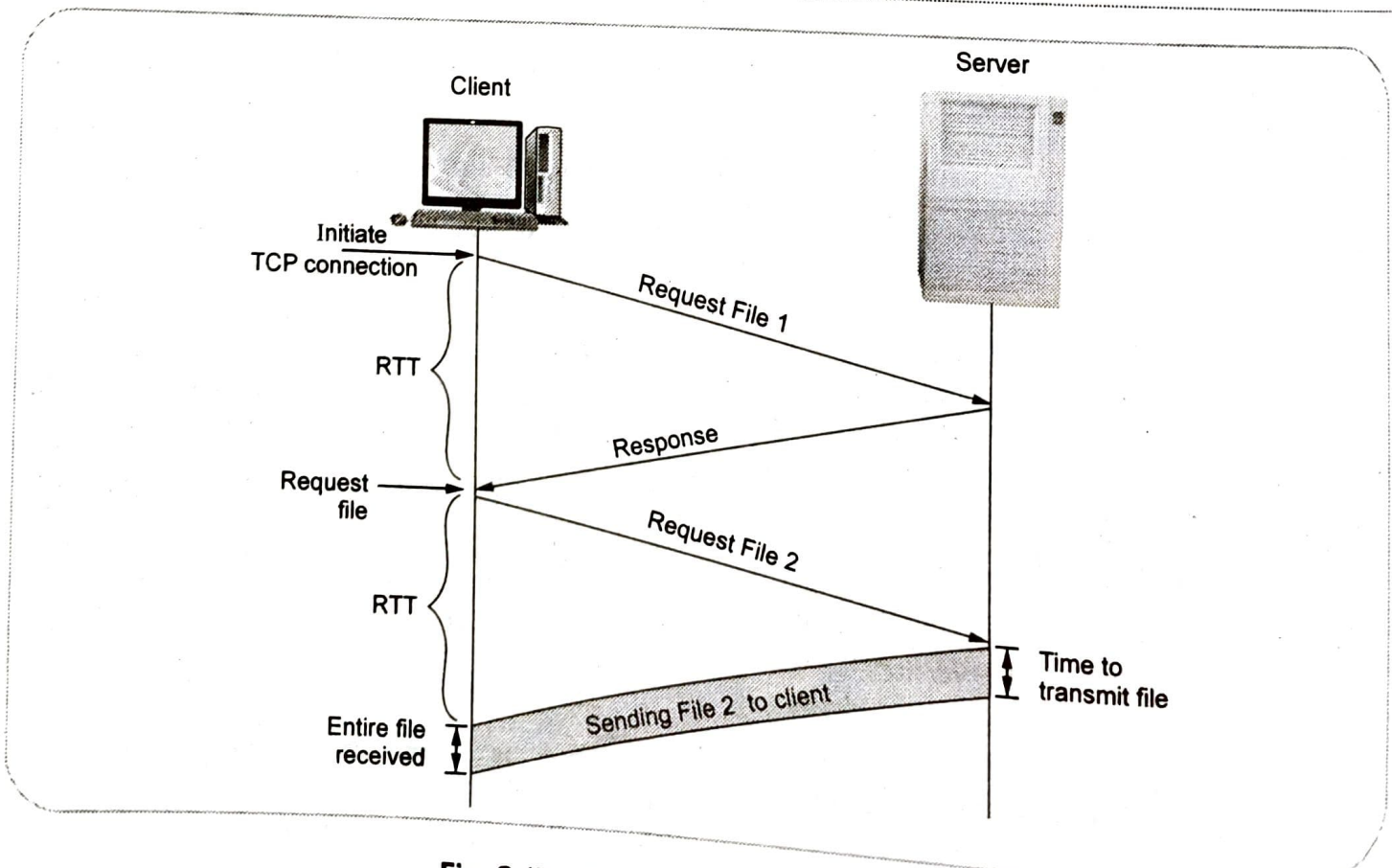


Fig. Q.17.1 Calculation for requesting file

5.5 : DNS

Q.19 Write short note on DNS.

[JNTU : Nov.-15, Marks 5]

OR What is the use of DNS ? Explain how it works ?

[JNTU : June-19, Marks 5]

Ans. : • **Goal** : Assign meaningful high-level names to a large set of machines and handle the mapping of those names to a machine's IP address.

• The DNS is a distributed database that resides on multiple machines on the internet and used to convert between names and address and to provide e-mail routing information.

• DNS provides the protocol that allows the client and servers to communicate with each other.

• Domain names are case insensitive so com and COM mean the same thing.

• The DNS protocol runs over UDP and uses port 53.

• The DNS is specified in RFC 1034 and RFC 1035.

• The DNS protocol is the application layer protocol.

• A full domain name is a sequence of labels separated by dots (.).

• The DNS name space is hierarchical and it is similar to the unix file system.

Originally, the Internet was small and mapping between names and addresses was accomplished using a centrally-maintained file called *hosts.txt*. To add a name or change an address required contacting the central administrator, updating the table, and distributing it to all the other sites. This solution worked at first because most sites had only a few machines, and the table didn't require frequent changes. **The centrally-maintained table suffered from several drawbacks :**

1. The name space was *flat*, and no two machines could use the same machine name.
2. As the Internet grew, changes to the database took days to weeks to take effect.
3. The central site became congested with the increase in the number of sites retrieving copies of the current table.
4. The Internet grew at an astonishing rate.

• The Domain Name System (DNS) is a hierarchical, distributed naming system designed to cope with the problem of explosive growth :

1. It is *hierarchical* because the name space is partitioned into *subdomains*.
2. It is distributed because management of the name space is delegated to local sites. Local sites have complete control (and responsibility) for their part of the name space. DNS queries are handled by servers called *name servers*.
3. It does more than just map machine names to internet addresses. For example, it allows a site to associate multiple machines with a single, mailbox name.

• In the DNS, the name space is structured as a tree, with *domain names* referring to nodes in the tree. The tree has a *root*, and a *fully-qualified* domain name is identified by the *components* of the path from the domain name to the root.

Services provided by DNS :

• **Host aliasing** : A host with complicated hostname can have one or more alias names. DNS can be invoked by an application to obtain the canonical hostname for a supplied alias hostname as well as the IP address of the host.

• **Mail server aliasing** : DNS can be invoked by a mail application to obtain the hostname for a supplied alias hostname as well as the IP address of the host.

• **Load distribution** : DNS is also used to perform load distribution among replicated servers.

Components of DNS

• DNS includes following components

- | | |
|----------------|------------------|
| 1. Domain | 2. Domain name |
| 3. Name server | 4. Name resolver |
| 5. Name cache | 6. Zone |

- 1) For example, vtubooks.com is the site for technical publications. Here com is the domain.
- 2) Domain name is defined by the DNS as being the sequence of names and domain. For example, vtubooks.com could be domain name.
- 3) In name server, software (program) that maps names to addresses. It does this by mapping domain names to IP addresses.

- 4) Name resolver is a software that functions as a client interacting with a name server.
- 5) Name cache is the storage used by the name resolver to store information frequently used.
- 6) Zone is a contiguous part of a domain.

Q.20 Explain the meaning of messages used in DNS.

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.20.1 shows the query and response message.

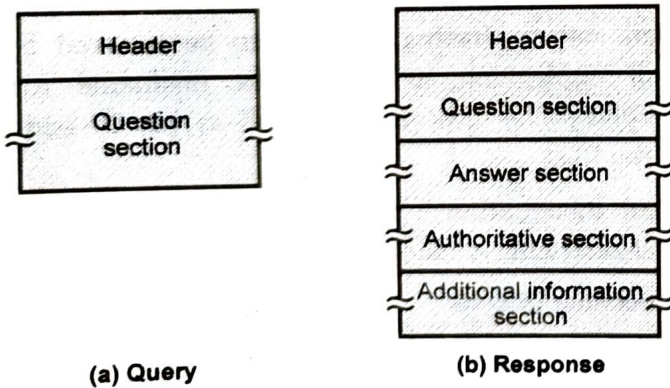


Fig. Q.20.1 Query and response message

• Fig. Q.20.2 shows the header format of the DNS.

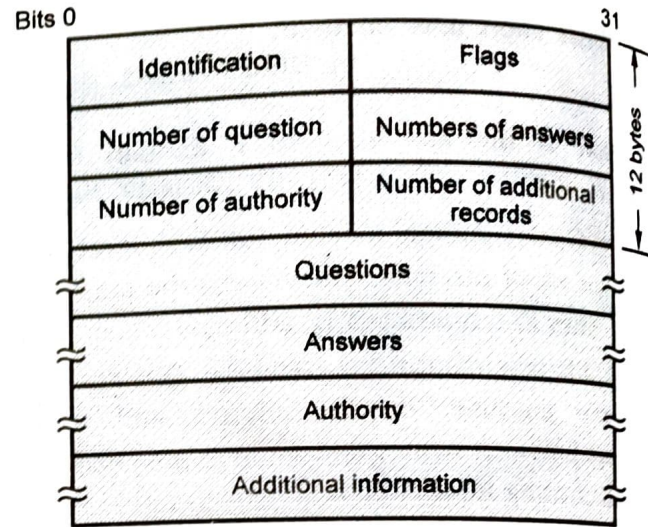


Fig. Q.20.2 Header format of DNS

- **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.
- **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.20.3 shows flags field in DNS header.

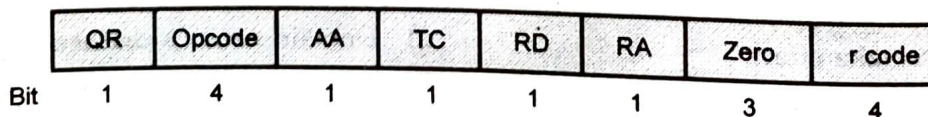


Fig. Q.20.3 Flags field in the DNS header

• 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.21 Explain the techniques recursive resolution used for name address resolution in DNS.

Ans. : • DNS is designed as a client server application. A host that needs to map an address to a name or a name to an address calls a DNS client named a resolver.

• Fig. Q.21.1 shows the recursive resolution.

• Recursive DNS queries occur when a DNS client requests information from a DNS server that is set to query subsequent DNS servers until a definitive answer is returned to the client. The queries made to subsequent DNS servers from the first DNS server are iterative queries.

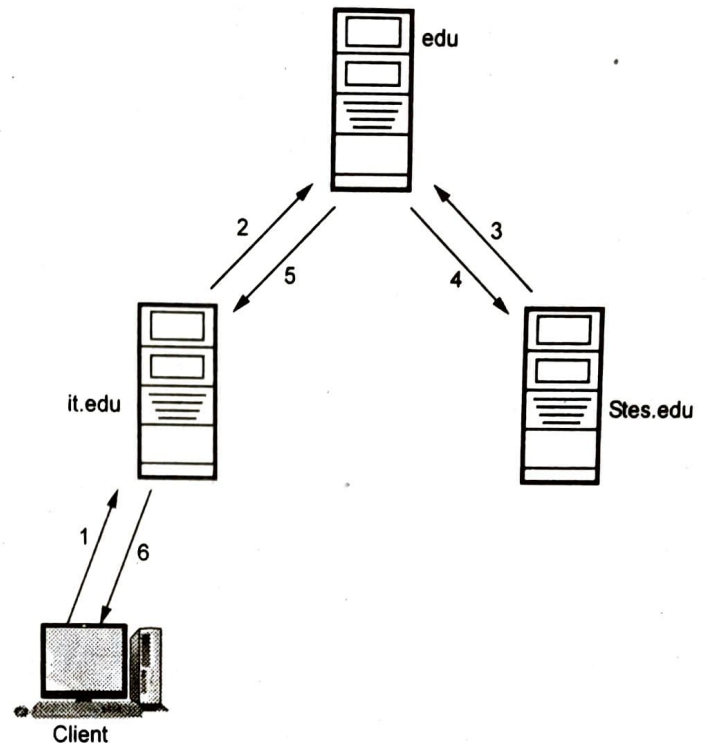


Fig. Q.21.1 Recursive resolution

- If the server is authority for the domain name, it checks its database and responds.
- If the server is not authority, it sends the request to another server and waits for the response.
- When the query is finally resolved, the response travel back until it finally reaches the requesting client. This is called recursive resolution.

Q.22 What is the difference between primary DNS server and secondary DNS server ?

Ans. : • Primary server : It stores a file about the zone for which it is an authority. It is responsible for creating, maintaining and updating the zone file.

• Secondary server : It transfers the complete information about a zone from another server and stores the files on its local disk. This server neither create nor updates the zone files.

Q.23 How does caching increase the efficiency of name resolution ?

Ans. : • Caching is designed to improve response times. A DNS server caches the queries that it resolves to improve response time and reduce network traffic.

• When performing a recursive query on behalf of a client, the DNS server caches all the information it receives from other DNS servers. Information is

kept in the cache for a specified amount of time known as the Time to Live (TTL). The TTL is set by the administrator for the primary zone.

- When the data is cached, the TTL begins to count down. After the TTL expires, the data is deleted from the cache.
- DNS clients also maintain a cache. If a DNS server resolves a query from its cache, it returns the remaining TTL for the data to the DNS client. The DNS client in turn, caches the information and uses the TTL to determine when the entry expires.

Q.24 How does recursive resolution differ from iterative resolution ?

Ans. : • In the Recursive approach, a client sends a query to the server. Assuming recursion is enabled, the server then looks for resolution first locally in its own database, then in its local cache, finally by going through the DNS tree until it finds a server that can give an authoritative answer to the query. In this model, the client is referred to as a Stub Resolver. Typically, Stub Resolvers are implemented on devices with limited resources such as embedded systems or PC.

- In the Iterative approach, the client sends a query to the server. If recursion is disabled, and the server cannot answer the query, the server will respond with a Referral answer. The client will then use that information to query another DNS server. This process will continue until a server responds with an Authoritative response.
- Recursive resolution puts more burden on a name server - global layers support only iterative resolution
- Recursive resolution makes caching more effective. Communication costs may be lower for recursive resolution

Q.25 What the advantages of a hierarchical name space over a flat name space for system of the size of the internet ?

Ans. : • Flat name spaces cannot generalize to large sets of machines because of the single set of identifiers. Single central name authority was overloaded.

Hierarchical names :

- The partitioning of a namespace must be defined in such a way that it : Supports efficient name

mapping and guarantees autonomous control of name assignment.

- Hierarchical namespaces provides a simple yet flexible naming structure. The namespace is partitioned at the top level.
- Authority for names in each partition are passed to each designated agent.
- The names are designed in an inverted-tree structure with the root at the top.
- Searching name is faster than flat name space.

Q.26 Explain the terms :

- Name space**
- Domain name space**
- Dynamic domain name system**
- DNS message**

Ans. :

- Name space :** Namespace identifies the structure of the domains that combine to form a complete domain name. Name spaces are of two types : Flat name spaces and Hierarchical names.
 - Domain name space :** The domain name space in the Internet is divided into three sections: generic domains, country domains, and inverse domains. In DNS, names are defined in an inverted tree structure with the root at the top. The tree can have only 128 levels : Level 0 to Level 127. Each node in the tree has a label, which is a string with a maximum of 63 characters. The root label is a null string , i.e. empty string.
 - Dynamic domain name system :** DDNS is a service that maps internet domain names to IP addresses. DDNS serves a similar purpose to DNS : DDNS allows anyone hosting a Web or FTP server to advertise a public name to prospective users.
- Unlike DNS that only works with static IP addresses, DDNS works with dynamic IP addresses, such as those assigned by an ISP or other DHCP server. DDNS is popular with home networkers, who typically receive dynamic, frequently-changing IP addresses from their service provider.
 - To use DDNS, one simply signs up with a provider and installs network software on their host to monitor its IP address. Compared to ordinary DNS, the disadvantage of DDNS is that additional

host software, a new potential failure point on the network, must be maintained.

iv) **DNS message** : 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.

Q.27 What do you mean by fully qualified domain name and partially qualified domain name ? Give one example for each.

Ans. : • In DNS, names are defined in an inverted tree structure with the root at the top. The tree can have only 128 levels : Level 0 to Level 127.

• Each node in the tree has a label, which is a string with a maximum of 63 characters. The root label is a null string, i.e. empty string.

• Each node in the tree has a domain name, a full domain name is a sequence of labels separated by dots(.). Fig. Q.27.1 shows the domain names and labels.

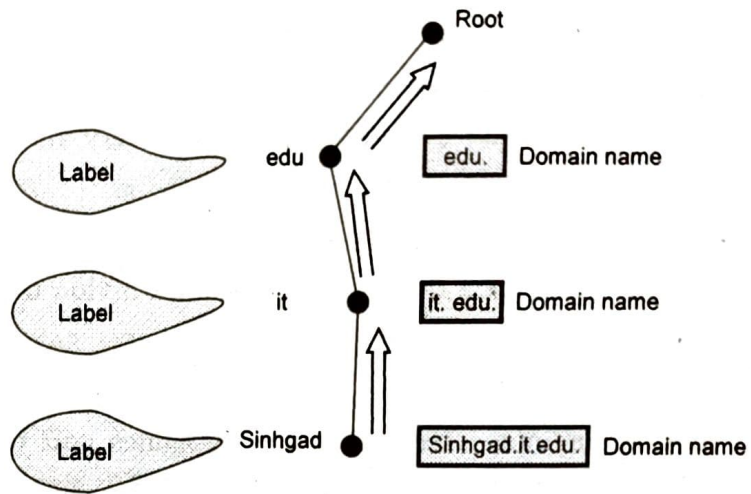


Fig. Q.27.1 Domain name and labels

- In fully qualified domain name, label is terminated by a null string. Fully qualified domain name (FQDN) contains the full name of host. For example : **sinhgad.it.edu**
- If a label is not terminated by null switch it is called a Partially Qualified Domain Name (PQDN). It starts from a node but not reach the root.
- An FQDN contains both the hostname and a domain name. It uniquely identifies a host within a DNS hierarchy. For example, **www.bayside.net** is an FQDN.

Q.28 Explain the concept of hierarchy of name servers with an example.

Ans. : • To distribute the information among many computers, DNS servers are used. Creates many domains as there are first level nodes. Fig. Q.28.1 shows hierarchy of name servers.

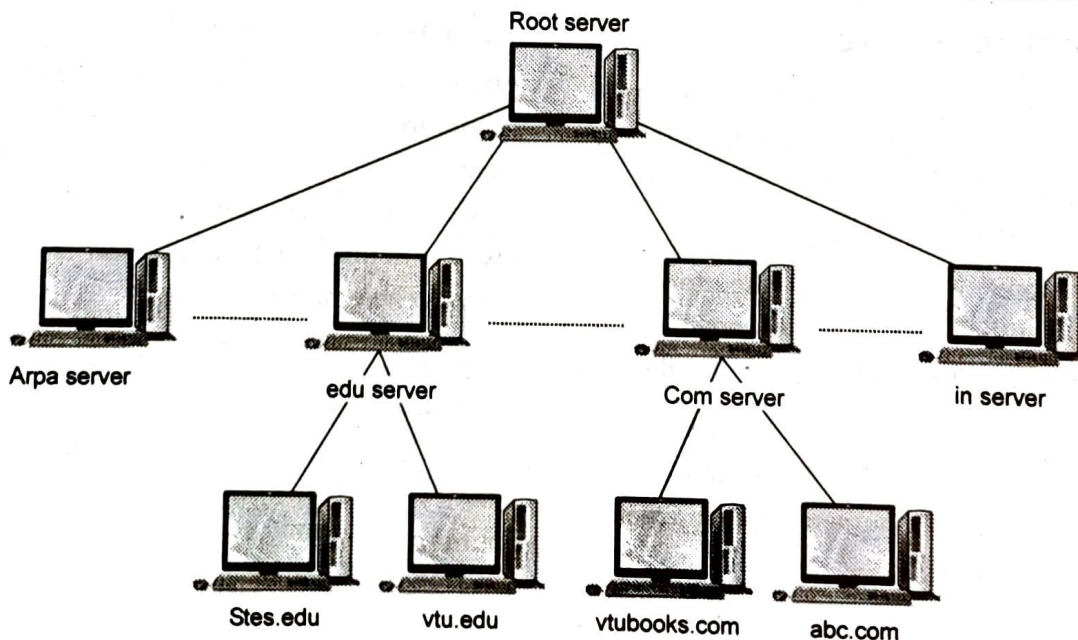


Fig. Q.28.1 Hierarchy of name server

- In zone, servers are responsible and have some authority. The server makes database called zone file and keeps all the information for every node under that domain.
- Domain and zone are same if server accepts responsibility for a domain and does not divide the domain into sub-domain.
- Domain and zone are different, if a server divides its domain into sub-domains and delegates part of its authority to other server. Fig. Q.28.2 shows zones and domains.

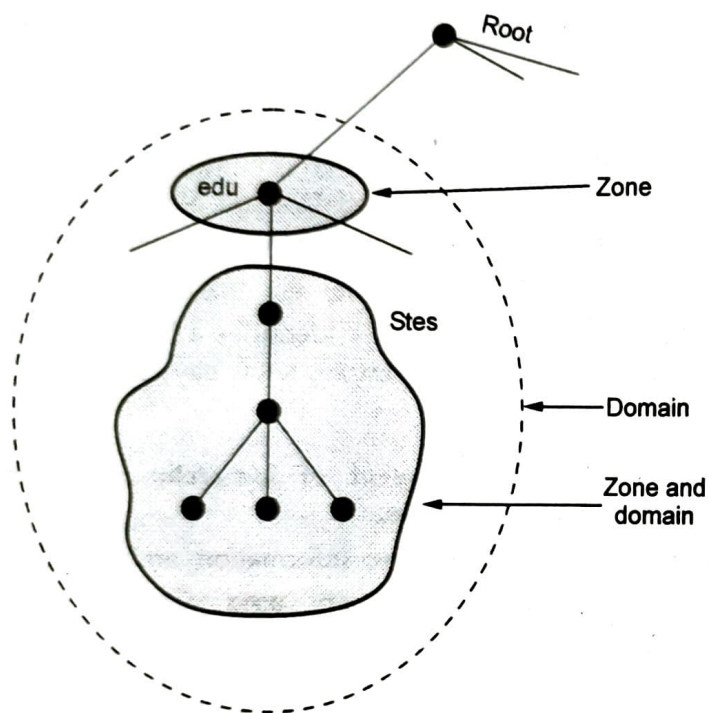


Fig. Q.28.2 Domain and zone

- A root server is a server whose zone consists of the whole tree. A root server usually does not store any information about domains but delegates its authority to other servers.
- Primary server stores a file about the zone for which it is an authority. It is responsible for creating, maintaining and updating the zone file.
- Secondary server transfers the complete information about a zone from another server and stores the files on its local disk. These servers neither create nor update the zone files.

Short Answered Questions

Q.29 What are the e-mail gateways ?

Ans. : An email gateway converts message from one mail format to another. Example : IP gateway, proxy gateways, EGP, BGP, IGP.

Q.30 What is SMTP ?

Ans. : Simple Mail Transfer Protocol is a standard and reliable host to host mail transport protocol that operates over the TCP port 25.

Q.31 State the purpose of SNMP.

Ans. : The primary purpose of SNMP is to allow the network administrator to monitor and configure devices on the network, remotely via the network. These configuration and monitoring capabilities are collectively referred to as management.

Q.32 Why email security is necessary ?

Ans. : Email security is the process of using email encryption to send messages that can only be opened by the intended recipient. Sending a message without secure email encryption is similar to dropping a post card in the mail - it can be read by almost anyone handling the postcard during its journey from sender to receiver. Secure email encryption protects both your online data and customers' sensitive information.

Q.33 Define SNMP.

Ans. : Simple network management protocol ; a standard for gathering statistical data about network traffic and the behavior of network components ; SNMP uses Management Information Bases (MIBs), which define what information is available from any manageable network device.

Q.34 What is the Domain Name System responsible for ?

Ans. : The Domain Name System converts domain names (of the form "www.vtubooks.com") into IP numbers.

Q.35 What are the four main properties of HTTP ?

Ans. : The four main properties of HTTP are :

1. Global uniform resource identifier.
2. Request-response exchange.
3. Statelessness.
4. Resource metadata.

Q.36 Describe why HTTP is designed as a stateless protocol ?

Ans. : Maintaining state across request-response connections significantly increases the initial interactions in a connection since the identity of each party needs to be established and any saved state must be retrieved. HTTP is therefore stateless to ensure that the Internet is scalable since state is not contained in the HTTP request/response pairs by default.

Q.37 What are the four groups of HTTP Headers ?

Ans. : The four groups of HTTP headers are : General headers, Entity headers, Request headers, and Response headers.

Q.38 What are the basic functions of e-mail ?

Ans. : Basic functions of e-mail are : Composition, Transfer, Reporting, Displaying, Disposition.

Q.39 What is the web browser ?

Ans. : Web browser is a software program that interprets and displays the contents of HTML web pages.

Q.40 Compare the HTTP and FTP ?

Ans. : Comparison between HTTP and FTP :

Sr. No.	FTP	HTTP
1.	FTP transfers the file from client to server and server to client.	HTTP transfer the file from server to client (i.e. web pages).
2.	It uses two different port connection. (i.e. port 20 and port 21)	HTTP use only one port connection (i.e. port 80).
3.	Uses TCP protocol.	It also use TCP protocol.

Q.41 Mention the application of FTP.

- Ans. :**
1. Used for remote login and data transfer.
 2. FTP provides good security.
 3. It is often used to upload web pages and other documents from a private development machine to a public web-hosting server.

Q.42 What are the advantages of allowing persistent TCP connections in HTTP ?

- Ans. :**
- a. HTTP requests and responses can be pipelined on a connection.
 - b. Network congestion is reduced by reducing the number of packets caused by TCP opens, and by allowing TCP sufficient time to determine the congestion state of the network.
 - c. Latency on subsequent requests is reduced since there is no time spent in TCP's connection opening handshake.

Q.43 Discuss the properties of file transfer protocol.

[JNTU : Dec.-18, Marks 3]

Ans. : Properties of File Transfer Protocol :

1. File Transfer Protocol (FTP) is used to copy files from one host to another.
2. FTP creates two processes such as Control Process and Data Transfer Process at both ends i.e. at client as well as at server.
3. FTP establishes two different connections: one is for data transfer and other is for control information.
4. FTP is a client-server protocol that relies on two communications channels between client and server.
5. FTP sessions work in passive or active modes. In active mode, after a client initiates a session via a command channel request, the server initiates a data connection back to the client and begins transferring data. In passive mode, the server instead uses the command channel to send the client the information it needs to open a data channel.

Q.44 What is the use of FTP ?

[JNTU : June-19, Marks 2]

Ans. : • File Transfer Protocol (FTP) is a standard Internet protocol for transmitting files between computers on the Internet over TCP/IP connections.

- File Transfer Protocol is a standard network protocol used for the transfer of computer files between a client and a server across a computer network.
- FTP can be used through a command-line interface such as DOS in Windows and Terminal in Linux and MacOS.
- It is possible to transfer any type of file with FTP, and in some cases, it is even faster than HTTP.
- The FTP helps to upload or download files to your website.

Q.45 What is the header format of HTTP reply message ? [JNTU : June-19, Marks 3]

Ans. : • A simple response from the server contains the following components :

1. HTTP Status Code (For example HTTP/1.1 301 Moved Permanently, means the requested resource was permanently moved and redirecting to some other resource).
2. Headers (Example - Content-Type : html)
3. An empty line.
4. A message body which is optional.

• All the lines in the server response should end with a carriage return and line feed. Similar to request, the empty line in a response also should only have carriage return and line feed without any spaces.

Q.46 What is ephemeral port number and well known port numbers ?

Ans. : • Port numbers from 0 to 65535 is used in Internet. It is 16 bits integer so the range is 0 to 65535. The client program defines itself with a port number, chosen randomly by the transport player software running on the client host. This is the ephemeral port number.

• Server also define a port number but not randomly. Internet has decided to use universal port numbers for servers, these are called well known port numbers. The port number ranging from 0 to 1023 are called well known port numbers and are restricted, which means that they are reserved for use by well known application protocols such as HTTP.

Q.47 What is DNS ?

Ans. : • The DNS is a distributed database that resides on multiple machines on the internet and used to convert between names and address and to provide e-mail routing information.

• In the DNS, the name space is structured as a tree, with domain names referring to nodes in the tree. The tree has a root, and a fully-qualified domain name is identified by the components of the path from the domain name to the root.

Q.48 What is STTP ?

Ans. : The Secure Token Transfer Protocol (STTP) provides the means for two entities to exchange a set of tokens that is needed to perform a certain task such as authentication.

**Fill in the Blanks
for Mid Term Exam**

- Q.1** _____ is the main protocol used in electronic mail (e-mail) service.
- Q.2** HTTP stands for _____
- Q.3** HTTP is a _____ protocol.
- Q.4** The DNS protocol runs over UDP and uses port _____.
- Q.5** The DNS name space is _____ and it is similar to the unix file system.
- Q.6** The 3 character domains are called the _____ domains.
- Q.7** LDAP is an _____ protocol that is implemented directly on top of TCP.
- Q.8** SMTP uses a TCP socket on port _____ to transfer e-mail reliably from client to server.
- Q.9** _____ handles incoming and outgoing mails.
- Q.10** MIME stands for _____.
- Q.11** _____ is used to transfer e-mail messages from a mail server to mail client software.
- Q.12** The _____ is the universal language of the web.
- Q.13** World wide web uses _____ interaction.

Q.14 If a time and date are supplied, the cookie is said to be _____ and is kept until it expires.

Answer Keys for Fill in the Blanks :

Q.1	SMTP	Q.2	Hyper Text Transfer Protocol
Q.3	Stateless	Q.4	53
Q.5	hierarchical	Q.6	generic
Q.7	application-level	Q.8	25
Q.9	Mail server	Q.10	Multipurpose Internet Mail Extensions
Q.11.	Post Office Protocol 3	Q.12	HTML
Q.13	client-server	Q.14	persistent

END... ✍

SOLVED MODEL QUESTION PAPER

Data Communications and Networks (As Per R - 18 Pattern)

B. Tech., IIIrd Year Sem - I [ECE]

Time : 3 Hours]

[Maximum Marks : 75

Notes : This question paper contains two parts A and B.

Part A is compulsory which carries 25 marks. Answer all questions in Part A. Part B consists of 5 units. Answer any one full question from each unit. Each question carries 10 marks and may have a, b, as sub questions.

PART - A

(25 Marks)

- Q.1**
- a) State the functions of layers of ISO-OSI model. (Refer Q.26 of Chapter - 1) [2]
 - b) List and define different network topologies. (Refer Q.31 of Chapter - 1) [2]
 - c) Difference between Pure ALOHA and Slotted ALOHA. (Refer Q.55 of Chapter - 2) [2]
 - d) What is ARQ ? List the protocol used for noiseless channel and noisy channels. (Refer Q.58 of Chapter - 2) [2]
 - e) Write down the design issue of network layers. (Refer Q.32 of Chapter - 3) [2]
 - f) What is IPv4 protocol ? (Refer Q.37 of Chapter - 3) [3]
 - g) Flow control and Error control both are properties of Transport Layer and Data Link Layer. What you think is it duplicity of properties in both layer or is it ok? Comment. (Refer Q.36 of Chapter - 4) [3]
 - h) Why three way handshake is used in TCP. (Refer Q.37 of Chapter - 4) [3]
 - i) What is the use of FTP ? (Refer Q.44 of Chapter - 5) [3]
 - j) What is the header format of HTTP reply message ? (Refer Q.45 of Chapter - 5) [3]

PART - B

(50 Marks)

- Q.2**
- a) Explain the functions of various layers in ISO-OSI reference model. (Refer Q.14 of Chapter - 1) [5]
 - b) Write short notes on : i) physical address ii) logical address iii) port address iv) specific address (Refer Q.20 of Chapter - 1) [5]

OR

- Q.3**
- a) What is IEEE 802.11 ? Explain wireless LAN in brief. (Refer Q.21 of Chapter - 1) [5]
 - b) Explain principles of IEEE standards. (Refer Q.23 of Chapter - 1) [5]
- Q.4**
- a) Describe encoding and decoding procedure used in linear block codes. (Refer Q.9 of Chapter - 2)
 - b) Explain the design of CRC encoder and decoder with a neat diagram. (Refer Q.12 of Chapter - 2) [5+5]

OR

- Q.5**
- a) Explain the algorithm for CRC method of error checking. (Refer Q.11 of Chapter - 2) [5]
 - b) Explain working of stop-and -wait ARQ protocol for noisy channel. (Refer Q.17 of Chapter - 2) [5]
- Q.6**
- a) What is logical addressing ? Give the services and header format of IPv4. (Refer Q.11 of Chapter - 3) [5]

- b) Give a comparative study of IPv4 and IPv6. (Refer Q.18 of Chapter - 3) [5]

OR

- Q.7 a) What is classful addressing ? Discuss class A, class B, class C, class D, class E address with its range in decimal dotted notation and example. (Refer Q.12 of Chapter - 3) [5]
- b) What is purpose of ICMP ? Explain its messages in detail. (Refer Q.31 of Chapter - 3) [5]
- Q.8 a) What are the services provided by transport layer to the upper layers ? (Refer Q.2 of Chapter - 4) [5]
- b) What is UDP ? What is the maximum and minimum size of a UDP datagram ? Also discuss the use of UDP. (Refer Q.8 of Chapter - 4) [5]

OR

- Q.9 a) Explain the connection establishment and release in transport layer. (Refer Q.5 of Chapter - 4) [5]
- b) Explain the real time transport protocol. (Refer Q.11 of Chapter - 4) [5]
- Q.10 a) Write short note on FTP. (Refer Q.4 of Chapter - 5) [5]
- b) Write short notes on : HTTP. (Refer Q.14 of Chapter - 5) [5]

OR

- Q.11 a) How would you summarize the concept of e-mail, its architecture and services. (Refer Q.8 of Chapter - 5) [5]
- b) Explain the concept of hierarchy of name servers with an example. (Refer Q.28 of Chapter - 5) [5]

END... ✍