**COMPUTER NETWORK**

**ASSIGNMENT WEEK 3**

1.Describe Elastic and Inelastic Traffic with Applications?

Elastic traffic can adjust, over wide ranges, to changes in delay and throughput across an internet and still meet the needs of its applications. Inelastic traffic does not easily adapt, if at all, to changes in delay and throughput across an internet. The prime example is real-time traffic, such as voice and video.

We use terms like “TCP Friendly” to describe the Internet's “elastic” applications. We mean “when it encounters delay, loss, or bandwidth limitations, the application (via TCP/SCTP) adapts its rate to maximize throughput”.

Inelastic traffic is vulnerable to delay – it cannot be spread in time. This kind of traffic is associated with applications, which use RTP protocol. The main services that generate inelastic traffic are VoIP, VoD, IPTV, audio- and videoconference.

2.Explain Internet Based Applications with Diagram?

Internet-based applications are software programs that use the internet to operate successfully. [They fetch, share, and display information from server systems over the internet 1](https://www.educba.com/what-is-internet-application/). The following diagram shows a high-level representation of a web application architecture:

!Web Application Architecture Diagram

The diagram shows three main components of the process:

* **Client-side**: This is the frontend of the application that interacts with the user.
* **Server-side**: This is the backend of the application that stores business logic, processes requests, and sends responses.
* [**Database server**: This is an optional component that stores data and sends client data to the server 2](https://www.intellectsoft.net/blog/web-application-architecture/).

3.Write short notes on SMTP?

Email is emerging as one of the most valuable services on the internet today.  
Most internet systems use SMTP as a method to transfer mail from one user to  
another. SMTP is a push protocol and is used to send the mail whereas POP  
(post office protocol) or IMAP (internet message access protocol) are used to  
retrieve those emails at the receiver’s side.  
SMTP Fundamentals  
SMTP is an application layer protocol. The client who wants to send the mail  
opens a TCP connection to the SMTP server and then sends the mail across  
the connection. The SMTP server is an always-on listening mode. As soon as it  
listens for a TCP connection from any client, the SMTP process initiates a  
connection through port 25. After successfully establishing a TCP connection  
the client process sends the mail instantly.  
SMTP Protocol  
The SMTP model is of two types:  
1. End-to-end method  
2. Store-and- forward method  
The end-to-end model is used to communicate between different organizations  
whereas the store and forward method is used within an organization. An SMTP  
client who wants to send the mail will contact the destination’s host SMTP  
directly, in order to send the mail to the destination. The SMTP server will keep  
the mail to itself until it is successfully copied to the receiver’s SMTP.  
The client SMTP is the one that initiates the session so let us call it client-  
SMTP and the server SMTP is the one that responds to the session request so  
let us call it receiver-SMTP. The client- SMTP will start the session and the  
receiver-SMTP will respond to the request.  
Model of SMTP system  
In the SMTP model user deals with the user agent (UA), for example, Microsoft  
Outlook, Netscape, Mozilla, etc. In order to exchange the mail using TCP, MTA  
is used. The user sending the mail doesn’t have to deal with MTA as it is the  
responsibility of the system admin to set up a local MTA. The MTA maintains a  
small queue of mails so that it can schedule repeat delivery of mails in case the  
receiver is not available. The MTA delivers the mail to the mailboxes and the  
information can later be downloaded by the user agents.

Both the SMTP-client and SMTP-server should have 2 components:  
1. User-agent (UA)  
2. Local MTA  
Communication between sender and the receiver :  
The sender’s user agent prepares the message and sends it to the MTA. The  
MTA’s responsibility is to transfer the mail across the network to the receiver’s  
MTA. To send mails, a system must have a client MTA, and to receive mails, a  
system must have a server MTA.  
SENDING EMAIL:  
Mail is sent by a series of request and response messages between the client  
and the server. The message which is sent across consists of a header and a  
body. A null line is used to terminate the mail header and everything after the  
null line is considered as the body of the message, which is a sequence of  
ASCII characters. The message body contains the actual information read by  
the receipt.  
RECEIVING EMAIL:  
The user agent at the server-side checks the mailboxes at a particular time of  
intervals. If any information is received, it informs the user about the mail. When  
the user tries to read the mail it displays a list of emails with a short description  
of each mail in the mailbox. By selecting any of the mail users can view its  
contents on the terminal.  
Some SMTP Commands:  
• HELO – Identifies the client to the server, fully qualified domain name, only  
sent once per session  
• MAIL – Initiate a message transfer, fully qualified domain of originator

RCPT – Follows MAIL, identifies an addressee, typically the fully qualified  
name of the addressee, and for multiple addressees use one RCPT for each  
addressee  
• DATA – send data line by line

4.Difference Between telnet and FTP?

Telnet  
TELNET stands for TErminaL NETwork. It is a type of protocol that enables  
one computer to connect to local computer. It is a used as a  
standard TCP/IP protocol for virtual terminal service which is given by ISO.  
Computer which starts connection known as the local computer. Computer  
which is being connected to i.e. which accepts the connection known  
as remote computer. When the connection is established between local  
and remote computer. During telnet operation whatever that is being  
performed on the remote computer will be displayed by local  
computer.Telnet operates on client/server principle. Local computer uses  
telnet client program and the remote computers uses telnet server program.  
TELNET Commands :  
Commands of the telnet are identified by a prefix character, Interpret As  
Command (IAC) which is having code 255. IAC is followed by command and  
option codes. Basic format of the command is as shown in the following figure :  
Following are some of the important TELNET commands :  
Character Decimal Binary Meaning  
WILL 251 11111011  
1. Offering to enable.  
2. Accepting a request to enable.  
Modes of Operation :  
Most telnet implementation operates in one of the following three modes :  
Default mode  
Character mode  
Line mode  
Default Mode :

• If there is no other modes are invoked then this mode is used.  
• Echoing is performed in this mode by client.  
• In this mode, user types a character and client echoes the character on the  
screen but it does not send it until whole line is completed.  
Character Mode :  
• Each character typed in this mode is sent by client to server.  
• Server in this type of mode is normally echoes character back to be  
displayed on the client’s screen.  
Line Mode :  
• Line editing like echoing, character erasing etc. is done from the client side.  
• Client will send the whole line to the server.

TP  
File Transfer Protocol(FTP) is an application layer protocol that moves files  
between local and remote file systems. It runs on the top of TCP, like HTTP. To  
transfer a file, 2 TCP connections are used by FTP in parallel: control  
connection and data connection.

What is control connection?  
For sending control information like user identification, password, commands to  
change the remote directory, commands to retrieve and store files, etc., FTP  
makes use of control connection. The control connection is initiated on port  
number 21.

What is data connection?  
For sending the actual file, FTP makes use of a data connection. A data  
connection is initiated on port number 20.  
FTP sends the control information out-of-band as it uses a separate control  
connection. Some protocols send their request and response  
header lines and the data in the same TCP connection. For this reason, they  
are said to send their control information in-band. HTTP and SMTP are such  
examples.

FTP Session :  
When an FTP session is started between a client and a server, the client  
initiates a control TCP connection with the server-side. The client sends control  
information over this. When the server receives this, it initiates a data  
connection to the client-side. Only one file can be sent over one data  
connection. But the control connection remains active throughout the user  
session. As we know HTTP is stateless i.e. it does not have to keep  
track of any user state. But FTP needs to maintain a state about its user  
throughout the session.  
Data Structures : FTP allows three types of data structures :  
1. File Structure – In file-structure there is no internal structure and the file is  
considered to be a continuous sequence of data bytes.  
2. Record Structure – In record-structure the file is made up of sequential  
records.  
3. Page Structure – In page-structure the file is made up of independent  
indexed pages.  
4. FTP Commands – Some of the FTP commands are :  
5. USER – This command sends the user identification to the server.  
PASS – This command sends the user password to the server.  
CWD – This command allows the user to work with a different directory or  
dataset for file storage or retrieval without altering his login or accounting  
information.  
RMD – This command causes the directory specified in the path-name to  
be removed as a directory.  
MKD – This command causes the directory specified in the pathname to  
be created as a directory.  
PWD – This command causes the name of the current working directory to  
be returned in the reply.  
RETR – This command causes the remote host to initiate a data connection

and to send the requested file over the data connection.  
STOR – This command causes to store of a file into the current directory of  
the remote host.  
LIST – Sends a request to display the list of all the files present in the  
directory.  
ABOR – This command tells the server to abort the previous FTP service  
command and any associated transfer of data.  
QUIT – This command terminates a USER and if file transfer is not in  
progress, the server closes the control connection.  
FTP Replies – Some of the FTP replies are :  
200 Command okay.  
530 Not logged in.  
331 User name okay, need a password.  
225 Data connection open; no transfer in progress.  
221 Service closing control connection.  
551 Requested action aborted: page type unknown.  
502 Command not implemented.  
503 Bad sequence of commands.  
504 Command not implemented for that parameter.  
• It is good for simple file transfers, such as during boot time.  
• It uses UDP as transport layer protocols. Errors in the transmission (lost  
packets, checksum errors) must be handled by the TFTP server.  
• It uses only one connection through well-known port 69.  
• TFTP uses a simple lock-step protocol (each data packet needs to be  
• acknowledged). Thus the throughput is limited

Advantages of FTP(File Transfer Protocol):-

• speed is one of the advantages of FTP(File Transfer Protocol).  
• File sharing also comes in the category of advantages of FTP in this  
between two machines file can be shared on the network.  
• Efficiency is more in FTP.

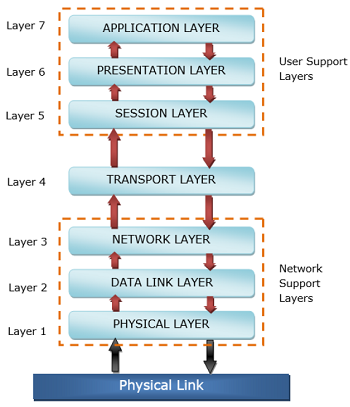
Disadvantages of FTP(File Transfer Protocol):-

• file size limit is the drawback of FTP only 2 GB size files can be  
• transferred.  
• multiple receivers are not supported by the FTP.  
• FTP does not encrypt the data this is one of the biggest drawbacks of  
FTP.

Reliable and security: FTP is both secure and unsecured we use login IDs and  
passwords making it secure but they can be attacked by hackers.

5.Explain Standardization within OSI framework with neat diagram?

OSI or [**Open System Interconnection model**](https://www.tutorialspoint.com/osi-model-in-computer-networking) was developed by International Standards Organization (ISO). It gives a layered networking framework that conceptualizes how communications should be done between heterogeneous systems. It has seven interconnected layers. The seven layers of the OSI Model are a [**physical layer**](https://www.tutorialspoint.com/data_communication_computer_network/physical_layer_introduction.htm), [**data link layer**](https://www.tutorialspoint.com/data_communication_computer_network/data_link_layer_introduction.htm), [**network layer**](https://www.tutorialspoint.com/data_communication_computer_network/network_layer_introduction.htm), [**transport layer**](https://www.tutorialspoint.com/data_communication_computer_network/transport_layer_introduction.htm), [**session layer**](https://www.tutorialspoint.com/The-Session-Layer-of-OSI-Model), [**presentation layer**](https://www.tutorialspoint.com/The-Presentation-Layer-of-OSI-Model), and [**application layer**](https://www.tutorialspoint.com/data_communication_computer_network/application_layer_introduction.htm), as shown in the following diagram −



The physical layer, data link layer and the network layer are the network support layers. The layers manage a physical transfer of data from one device to another. Session layer, presentation layer, and application layer are the user support layers. These layers allow communication among unrelated software in dissimilar environments. Transport layer links the two groups.

The main functions of each of the layers are as follows −

* **Physical Layer −** Its function is to transmit individual bits from one node to another over a physical medium.
* **Data Link Layer −** It is responsible for the reliable transfer of data frames from one node to another connected by the physical layer.
* **Network Layer −** It manages the delivery of individual data packets from source to destination through appropriate addressing and routing.
* **Transport Layer −**It is responsible for delivery of the entire message from the source host to destination host.
* **Session Layer −** It establishes sessions between users and offers services like dialog control and synchronization.
* **Presentation Layer −** It monitors syntax and semantics of transmitted information through translation, compression, and encryption.
* **Application Layer −** It provides high-level APIs (application program interface) to the users.