SIMATS ENGINEERING

THANDALAM

ASSIGNMENT - 05

NAME	: SAMRAKSHINI.G
REGISTER NUMBER	: 192511172
COURSE CODE/NAME	: CSA0735 COMPUTER NETWORKS FOR COMMUNICATION
DEPARTMENT	: B.E. COMPUTER SCIENCE AND ENGINEERING
SUBMISSION DATE	: 01/08/2025
TOPIC	: SECURE FILE TRANSFER PROTOCOL SHARING WITH FIREWALLS

SIMATS ENGINEERING

ASSIGNMENT - 05

CSA0735 : COMPUTER NETWORKS

REGISTED NUMBER	NAME	SCENARIO
192511172	GAMRAKSHINI. G	A graphic studio shares project files over FTP with global clients

PARAMETERS :

2 GIB FILE , 100 Mbps LINK

A) ESTIMATE TRANSFER TIME OVER FTP.

STEP - 1 : CONVERT 2GB TO MEGABITS :

- 1 BYTE = 8 BITS
- 2GB = 2 x 1024 MB = 2048 MB
- 2048 MB = 2048 x 8 = 16,384 Megabits

STEP - 2 : CALCULATE TIME :

$$\text{Transfer Time} = \frac{\text{Data size}}{\text{Link speed}}$$

$$= \frac{16,384 \text{ Megabits}}{100 \text{ Mbps}} = 163.84 \text{ seconds}$$

≈ 2 minutes 44 seconds

∴ Estimated FTP transfer time is ~ 2 minutes 44 seconds under ideal conditions [without overhead or delays]

B) PROPOSE SECURE FILE SHARING ALTERNATIVES

Standard FTP lacks encryption and exposes data and credentials in plain text, making it unsuitable for sharing sensitive graphic files.

The following options are recommended for more secure file sharing:

→ **SFTP [SSH FILE TRANSFER PROTOCOL]**

i) Uses SSH [port 22] to encrypt both file data and authentication.

ii) Offers strong security, scriptable automation and detailed logging.

iii) It is widely supported and firewall-friendly

→ **FTPS [FTP SECURE]:**

i) Adds SSL/TLS encryption to standard FTP.

ii) Uses port number 21 and 990 or custom high ports (data)

iii) Can operate in both explicit or implicit mode depending on configuration.

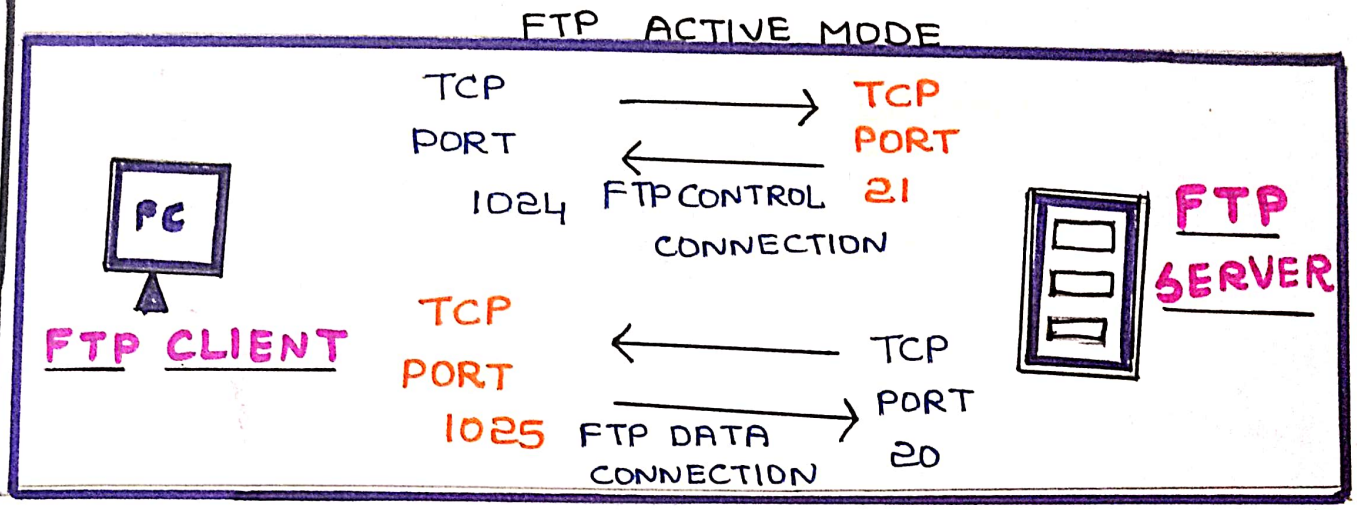
→ **HTTPS-BASED FILE SHARING [ONE-TIME SHARING]**

i) Services like WeTransfer, Smash or Firefox send [conceptually] offer link-based secure transfer over HTTPS [port 443]

ii) Example: Google Drive, Dropbox, WeTransfer

iii) Ideal for one-time or large file sharing.

c) DISCUSS FTP FIREWALL PORTS.



FTP USES TWO CHANNELS :

- COMMAND CHANNEL : Port 21 [always open for control commands]
- DATA CHANNEL :
  - * ACTIVE MODE : Server opens port 20, connects to client.
  - * PASSIVE MODE : Server opens a random high port [≥ 1024], client connects to it.

- FIREWALL ISSUE :
  - * Most firewalls / NAT routers block inbound connections [server → client], making active mode fail in many NAT environments.
  - * Server must have a range of high ports open in the firewall.
  - * Passive mode works better with NAT clients because the client always initiates both connections.
  - * For better security and fewer firewall issues, SFTP (port 22) are recommended.

D) RECOMMEND PASSIVE MODES FOR NAT CLIENTS

FEATURE	ACTIVE MODE	PASSIVE MODE
WHO INITIATES DATA CHANNEL?	Server → Client	Client → Server
IS IT NAT FRIENDLY?	NO - SERVER CAN'T REACH CLIENT	YES ☑ - CLIENT INITIATES BOTH CONNECTIONS.
IT REQUIRES PORT FORWARDING?	Often Yes	Rarely, only on server side
DOES IT WORK WITH FIREWALLS?	No (by default)	Yes [easier to configure

By considering all the above mentioned information, NAT [Network Address translation] because it avoids the primary issue faced by Active mode - inbound connections being blocked by firewalls or NAT routers.