FTP

Prepared by	Vinay B
Reviewed by	M, Ramesh Babu

File Transfer Protocol (FTP): It is the standard mechanism provided by TCP/IP for copying a file from one host to another. Although transferring files from one system to another seems simple and straightforward, some problems must be dealt with first.

For example:

- Two systems may use different file name conventions.
- Two systems may have different ways to represent text and data.
- Two systems may have different directory structures. All these problems have been solved by FTP in a very simple and elegant approach

FTP establishes two connections between the hosts:

- One connection is used for data transfer, the other for control information. The control connection uses very simple rules of communication. We need to transfer only a line of command or a line of response at a time.
- The data connection, on the other hand, needs more complex rules due to the variety of data types transferred.
- FTP uses two well-known TCP ports: **Port 21** is used for the control connection, and **port 20** is used for the data connection.

IN FTP CONNECTION HAPPENS IN TWO MODE:

- **ACTIVE MODE**
- **PASSIVE MODE**

ACTIVE MODE:

In Active Mode the control connection is initiated by client, and the data connection is initiated by the server which is explained below.

Steps for the active mode:

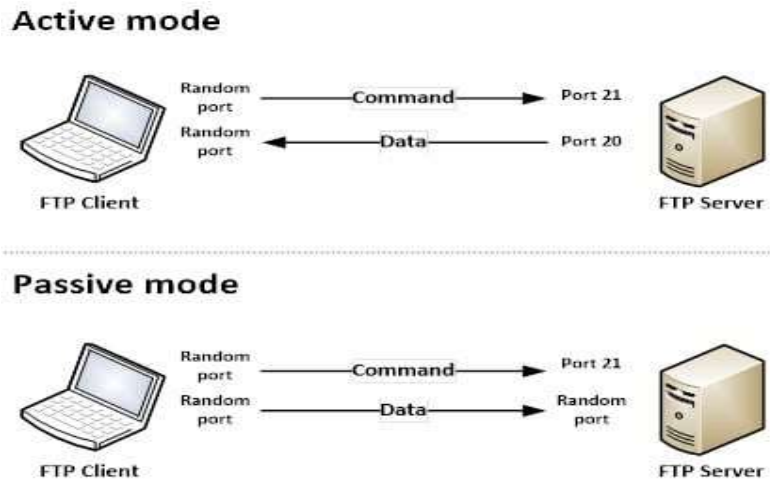
- The client sends the PORT command to an FTP server. The source port is a random, high-numbered port. The destination port is 21.
- The server responds with an ACK.
- The server initiates a connection to the client with source port 20 and the destination port specified in the client's PORT command.
- The client sends an ACK to the server. The FTP session has now been established.

PASSIVE MODE:

In passive mode the control and data connection is initiated by client only.

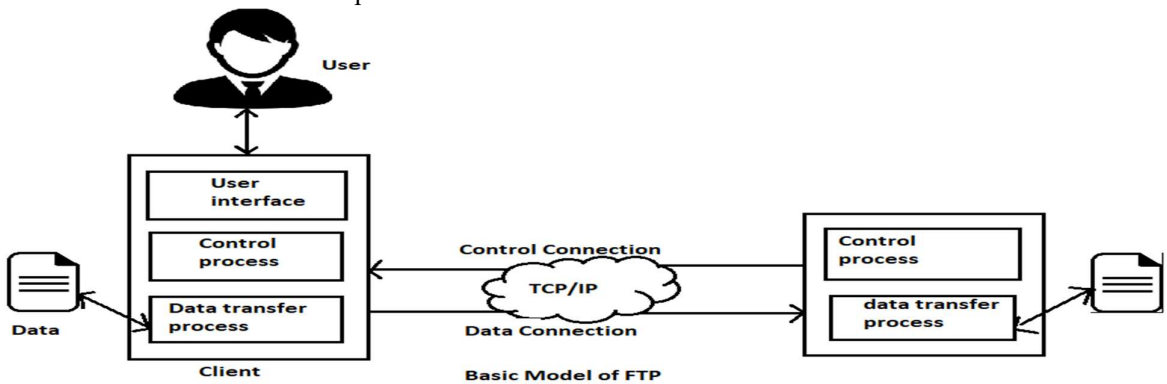
Steps given below:

1. The client sends the PASV command to an FTP server on port 21. The source port is a random, high-numbered port. The destination port is 21.
2. The server responds with the command. The port command specifies a random, high-numbered (ephemeral) port that the client can connect to.
3. The client initiates a connection to the server on this ephemeral port.
4. The server responds with an ACK. The FTP session has now been established



The basic model of FTP is shown below,

- **<u>The client has three components</u>**: **user interface**, **client control process**, and the **client data transfer process.**
- **<u>The server has two components</u>**: **the server control process** and the **server data transfer process.**
- The control connection is made between the control processes. The data connection is made between the data transfer processes



The control connection remains connected during the entire interactive FTP session. The data connection is opened and then closed for each file transferred. It opens each time commands that involve transferring files are used, and it closes when file transferred

Communication Over the Control Connection:

- The main purpose of the control connection is to transfer the files through the data connection. The file transfer occurs in the data connection with the help of control connection. The control connection controls the path and sharing files over the network using the control of the commands sent over control connection.
- Ftp uses the 7-bit ASCII Character set for the communication over the control channel.

FTP COMMANDS

Here we given some of example commands for the ftp,

GET: This command is used for getting the file from remote computer.
SEND: Used for sending the file.
USER: This command is used for user identification to the server.
OPEN: Open address.
PASS: This command is used for user password.
CLOSE: This command is used for disconnecting the ftp connection but this does not terminate user.
QUIT: This command will terminate the connection.

Communication over the Data Connection:

The purpose of the data connection is to transfer the files through the data connection.
The client must define the type of file to be transferred, the structure of data, and transmission mode.

FILE TYPE:

In ftp we can transfer the following file types,

- **An ASCII File:** The ASCII file is default form of transferring the text files, in here the text each character is encoded by using the 7-bit ASCII.
- **EBCDIC FILE:** It also encoding method developed by IBM. It uses a unique 8-bit binary code for each number and alphabets as well.
- **IMAGE FILE:** For images in ftp are transferred without any conversion just as binary form, here the bits are like continuous streams without any interpretation.

DATA STRUCTRE:

Ftp can transfer a file across the data connection using these data structures,

- **FILE STRUCTRE**: In file structure format the file is continuous stream of bits, data will be in file structure.
- **RECORD STRUCTRE:** In this the files are divided into records this is used in text files.
- **PAGE STRUCTRE:** In this the file is divided into pages which have page numbers and page header, this page can be stored, accessed randomly (or) sequentially.

TRANSMISSION MODE:

FTP Uses three types of data transmission modes for transferring the files across the network,
STREAM MODE: The stream mode is default mode here the data is delivered from FTP to TCP as a continuous stream of bytes.

- If the data is simply the stream of bytes then there is no need of **end-of-file,** In this mode the ending of the data connection is done by the sender.
- If the data is in the record structure the **End-of-record (E-O-R)** will be at the end of file.
- IF the data is in the file structure the **End-of-file(E-O-F)** will be at the end of file.

BLOCK MODE: In this mode the data is in the form of blocks, In this case each block consists of 3 bytes of header,1st byte is called block descriptor the next 2 bytes are which defines the size of block.

COMPRESSED MODE: In this mode if any big files are transferring that data can be compressed which is done by **Run Length Encoding** method

FTP DISADVANTAGES:

Ftp is not secured, here data is not encrypted will be sent as plaintext format.
We can also login as Anonymous to server.

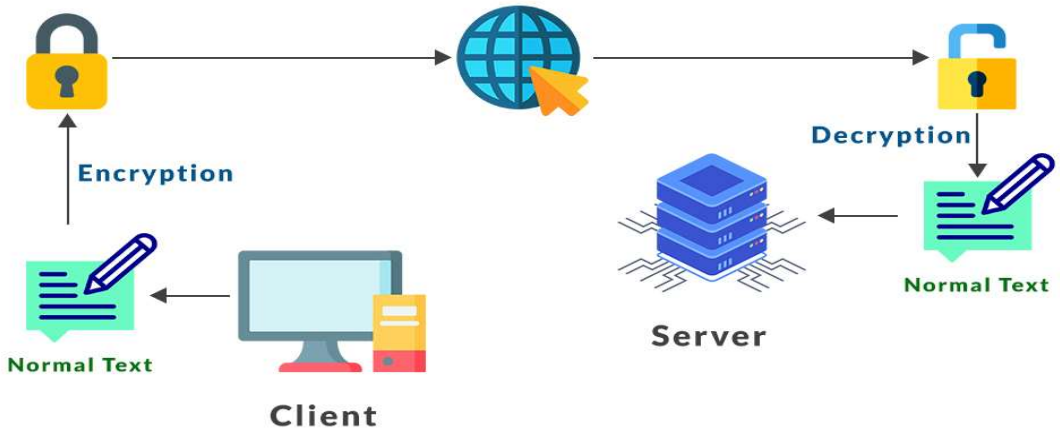
SFTP

SFTP (Secure File Transfer Protocol):

SFTP (Secure File Transfer Protocol) is the advanced version of FTP which ensures security while transferring files between the organizations/computer.
It is also known as Secure Shell (SSH). It works on **port no. 22** and uses the client server model.

The FTP was lagged in giving the security to the data which is sent by the ftp over the network so the SFTP was introduced which encrypts the files before transferring.

How SFTP Encrypts and decrypts data:



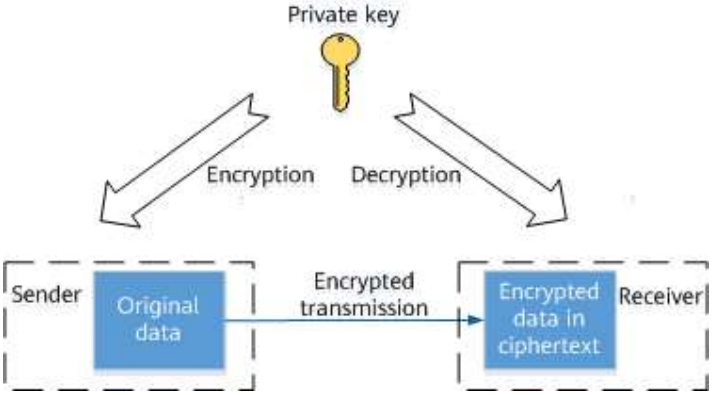
- Firstly, a safe and secure connection is established by SFTP then it provides an advanced level of protection for data transferring.
- SFTP uses the same commands as the standard File Transfer Protocol FTP, and most SFTP commands are similar or identical to the Linux shell commands.

- SFTP uses SSH for encryption and decryption of files in it , so it works as SSH
- SSH uses both symmetric and asymmetric encryption algorithms and pre-generated SSH keys to ensure data transmission security. The following figure shows the encryption and decryption processes of the two encryption algorithms.

SSH HAVE TWO TYPES ENCRYPTION:

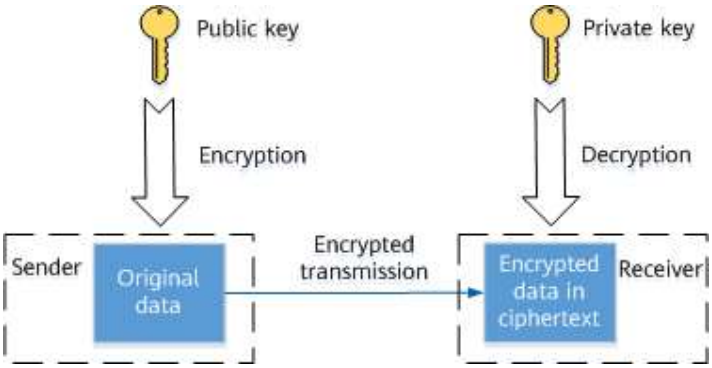
- **SYMMETRIC ENCRYPTION**
- **ASYMMETRIC ENCRYPTION**

SYMMETRIC ENCRYPTION:



- The symmetric encryption algorithm uses the same key to encrypt and decrypt data.
- During SSH connection establishment, to generate a symmetric key which is used as a session key, the client and server use a key exchange algorithm to calculate the key based on some shared information and their own private data.
- The symmetric encryption algorithm is applicable to scenarios where a large amount of data needs to be transmitted because this algorithm delivers fast encryption and decryption.

ASYMMTERIC ENCRYPTION:



- In asymmetric encryption, sending and receiving information require a pair of associated SSH keys, that is, a public key and private key, respectively.
- The private key is kept by the party that generates it, and the public key can be sent to any party that requests communication. The sender uses the received public key to encrypt communication content. Only the receiver can use the private key to decrypt the communication content. The private key for asymmetric encryption does not need to be exposed on the network, which greatly improves security. However, encryption and decryption are much slower than those in the symmetric encryption algorithm scenario.

SOME BASIC SFTP COMMANDS:

- **put** -- Upload a file
- **get** -- Download a file
- **cd** -- Change the active directory path
- **pwd** -- Display the remote working directory
- **lcd** -- Change the local system's directory path
- **lpwd** -- Display the local working directory
- **ls** -- Display contents of the remote working directory
- **lls** -- Display content of the local working directory
- **lmkdir** -- Create a local directory
- **lumask** -- Change the umask value
- **rename** -- Rename a file on the remote host
- **rm** -- Delete a file on the remote host.

DIFFERENCE BETWEEN FTP AND SFTP:

REFERRED BOOK:

Data Communications and Networking By Behrouz A. Forouzan