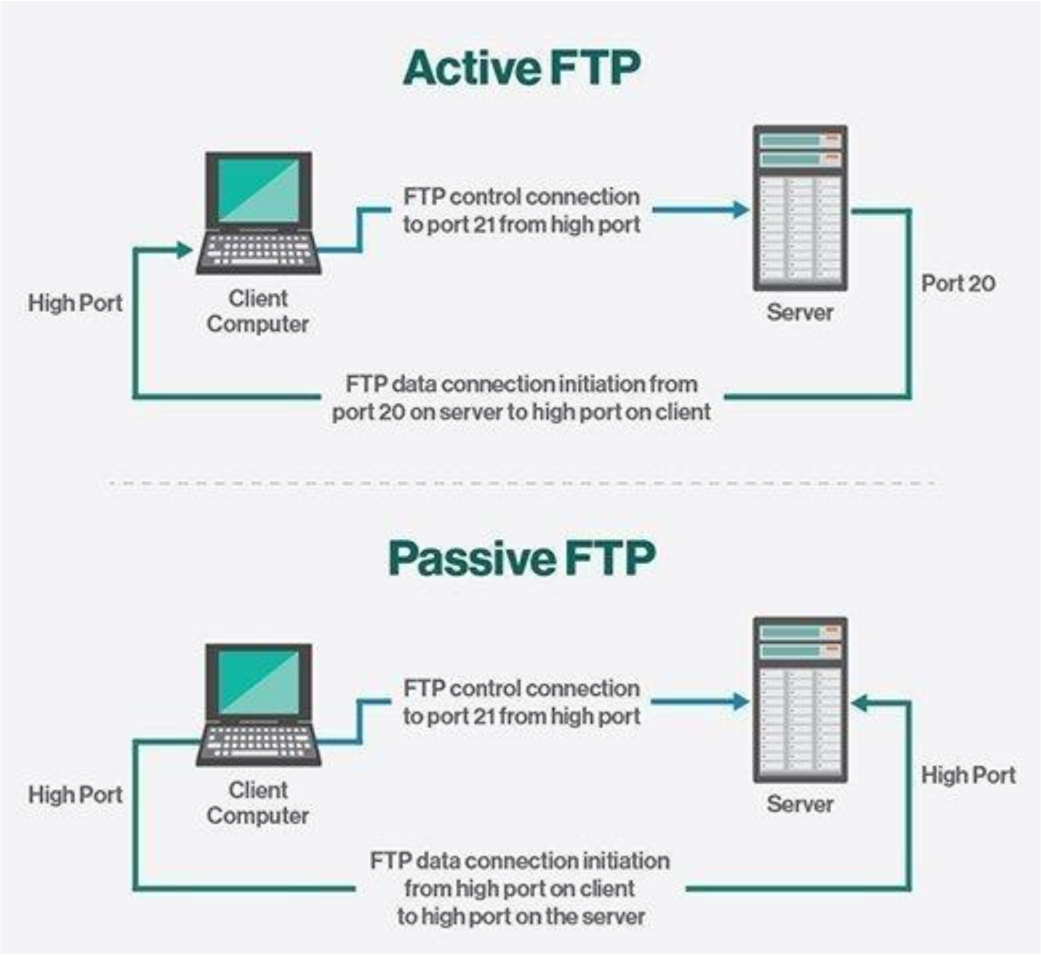
Experiment 10
File Transfer Protocol

The File Transfer Protocol or FTP is a standard application layer protocol. It runs by transmitting files between different computers that are connected to the internet via the TCP/IP protocol connection. This is a client-server protocol where clients can ask for a file, and local remote servers can provide it.

The machine of the end-user is called the local host and it is connected to the machine running the FTP service (Remote Host) via the internet.


Active FTP
FTP control connection to port 21 from high port
High Port
Client Computer
Server
Port 20
FTP data connection initiation from port 20 on server to high port on client
Passive FTP
FTP control connection to port 21 from high port
High Port
Client Computer
Server
High Port
FTP data connection initiation from high port on client to high port on the server

The sessions of FTP protocol can either be in an active mode or passive mode.

Active Mode

For active mode, the client first initiates a session with the command channel request, then the server initiates a data connection back to the client and starts to transfer the data.

Passive Mode

In passive mode, the command channel information is sent by the server to the client in order to establish a data connection. This allows it to open a data channel with the server and start the receiving of data. This works well across all firewalls and NAT gateways since the client is the one initiating the connection.

How it Works

FTP relies on two separate communication channels between the client and the server. This includes a basic command channel for the control of conversation between the client and server, and the other to transfer file content along the data channel.

Clients can initiate the conversation with the server by requesting the download of a file. With FTP, clients can even upload, delete, move, copy, rename, and download files from a server. This would require a user to log on to the FTP server first. However, some servers can make all of their content available without a login, and these are called Anonymous FTP.

Users can find working with FTP to be quite easy with the help of a basic command line interface. This includes the terminal in OS X and Linus, and the PowerShell/Command Prompt in Windows.

Security

When FTP was initially created back in 1971, the definitions of TCP and IP were not created. Since then, FTP has been redefined several times in order to adjust to the new versions of TCP/IP. It was also initially defined without any security considerations; however, this has been redefined to overcome those limits. Its extensions such as SFTP or FTPS work well with a TLS connection and ensure security of the data being transferred.

It also does not encrypt any traffic which can allow individuals to capture the packets and read them, along with the usernames and passwords in the packets. FTP can still be vulnerable to brute force attacks, spoofing, packet capture, and FTP bounce. DDoS attacks can also have a severe impact on the functioning of FTP.

FTP Clients

The clients of FTP can upload, download, and manage files on the server. Its clients include:

- WinSCP which is a Windows FTC client which supports all iterations of FTP.
- WS FTP which is another FTC client for windows with support for SSH.
- Transmit which is an FTP client for OS X with support for all FTP iterations.

Summary

FTP is an excellent application layer protocol for the transmission of files across various computers on the internet. It requires two channels for operations, and the connection is initiated by the client. It isn't a very secure protocol, but has a few extensions that help add security features to it. It relies on FTP clients to manage the data on servers.