An Introduction to FTP

Author: Conrad Chung, 2BrightSparks

FTP stands for File Transfer Protocol. It is a protocol used to transfer files between an FTP host/server and an FTP client computer on the Internet. FTP is most commonly used to download files from the World Wide Web. It is an alternative choice to HTTP protocol for downloading and uploading files to FTP servers.

History of FTP

In the early days of computing, complex sets of commands had to be learned to use the Internet. FTP, invented in the early 1970s, established a standard protocol for transferring files between systems.

FTP protocols used for the Internet standard were drafted by the Internet Engineering Task Force committee as a series of RFC (Request for Comments) formal documents. In 1971 the FTP protocol RFC 114 was published. Over the years the document was revised with newer versions making changes to improve the FTP protocol. RFC 959 was published in 1985, which became the current standard specification. The RFC document is still being amended to date, with revisions to improve the security of FTP and adding support for newer technologies.

FTP is used for:

- Uploading webpages to web servers for publishing on the Internet
- Browsing and downloading files from public software sites
- Transferring large files among two parties that are too large for email attachments
- Downloading and uploading content like university's assignments via an FTP server
- Distributing the latest revisions of programs by software developers

Basics Functions and Terms of FTP

To use FTP, you will need FTP client software and an FTP server. You also need to know the server address, the username, and a password and port number. The basic information you need in order to log in successfully follows:

Login Example	Definition
site:**ftp.example.com**	This is the site address of the FTP server you're connecting to.
login:**john_doe**	Login or the USER command is the username used for logging into FTP.
pass: **GUt1KYxt**	PASS is the password.
port:**21**	PORT is the COMMAND port number you are using to connect to the server. The most common port number is port 21.

Essential FTP Terms

Below describes some of the essential FTP terms.

Anonymous FTP: Various public servers allow anonymous login. Users can log in to servers without an account to download files. Uploading is not allowed for anonymous login. Take note that your IP address is tracked even though it is an anonymous session.

Get: Also called "Download". Copy files from the FTP site to the FTP client's system.

Put: Also called "Upload". Copy files from the client's system to the FTP site. Uploading is restricted to authorized users only.

FTP Site: A hosting server that contains files for download and upload. To access the FTP site, you need to type in the address, which begins with ftp:// (instead of http://).

FTP Connection Types

An important concept to remember is that FTP connects using **two TCP ports** for all communications between the server and user.

- **COMMAND** Port: This is the main TCP port created upon a session is connected. It is used for passing commands and replies. Port 21 (unsecured) or 990 (secured) are the default command ports used.
- **DATA** Port: Each time when files or directories are transferred between server and client, a random TCP data connection is established and data transfer commences over the connection. Once data transfer is complete, the connection is closed. Subsequent data connections are established and terminated as required. Data connections are never left open.

Connection Modes – ASCII and Binary

FTP transfers files between systems by using one of these two modes – ASCII and binary. The mode is determined at the initial stage of all FTP transactions by the server. The FTP client will automatically switch to the mode.

ASCII mode is used exclusively to transfer text and HTML. Binary mode transfers zip files, images or executable files in binary form. Binary files cannot be sent via ASCII mode and vice versa as corruptions will occur.

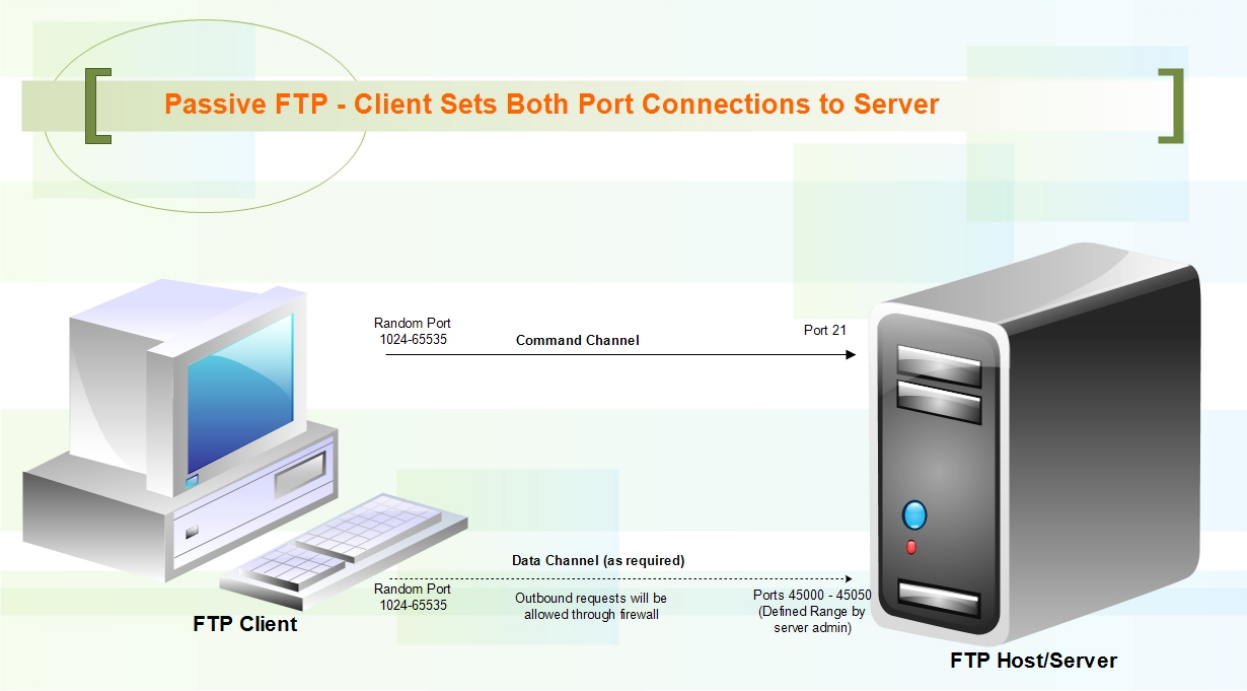
Syncback always transfers files in binary mode. This ensures that the files contents are not changed by the FTP server and that the size of the file is always the same.

Transfer Modes – Passive and Active

In passive mode connections, the FTP client initiates the connections to the command port and data port to the host server. This is the preferred mode in most FTP clients as well as the default FTP setting in SyncBackPro as the client's firewall will allow outgoing connections to the server.

The FTP client first establishes the connection by opening a port (random port, X>1023) locally and connecting to Port 21 of the server. The client then opens another port X+1 and sends out the **PASV** command to notify the server it is in passive mode.

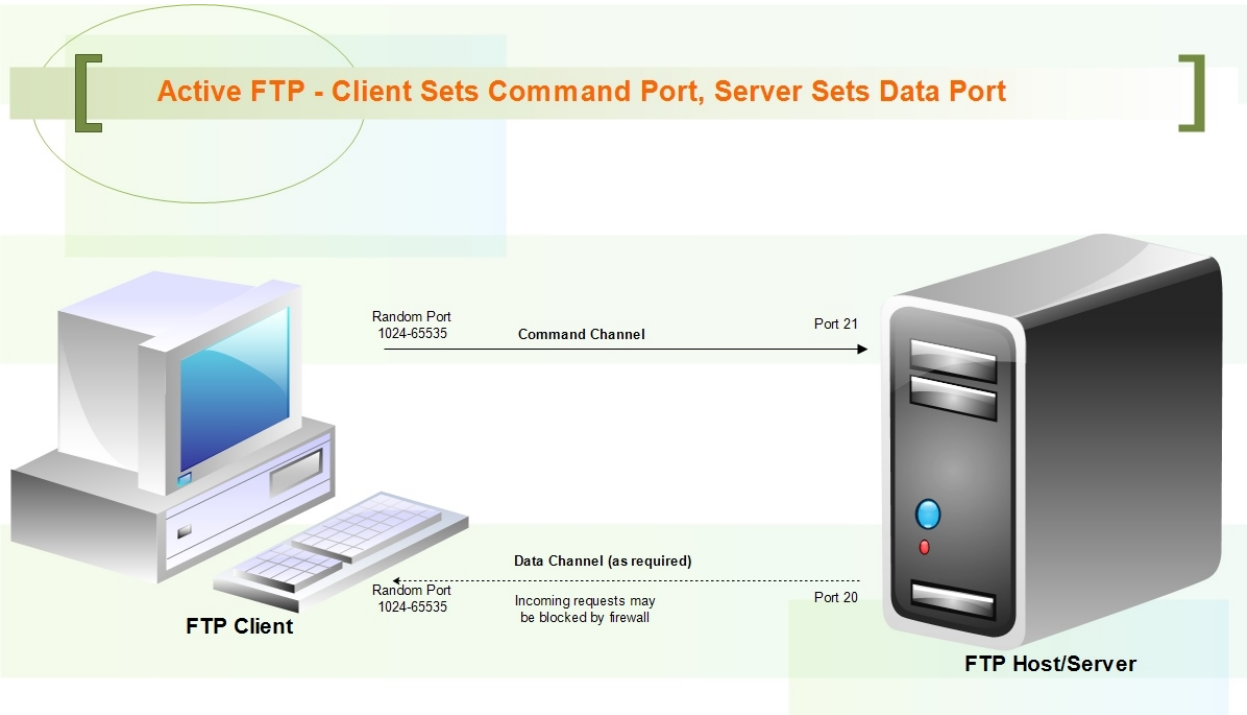
The server will respond by opening a port (predefined random port, Y>1023) and acknowledges the client by sending out **P** to it. Then the client initiates the connection from port X+1 to the server's port Y for data transferring.



In active mode, the FTP client (random port, X>1023) initiates the connection by connecting to the server's command port (Port 21). The client then opens a listening data port and sends the command **PORT** to the server. The server, using Port 20, will initiate the connection to the specified data port on the FTP client.

The problem with this is that the client simply tells the server which data port it is listening to and the server is the one making the connection to the client. Thus to the client's firewall, it appears that an external system is trying to make a connection to an internal system. This causes the firewall to block this connection unless it was configured beforehand to allow it.

For SyncBackPro users setting up an Active FTP data connection, you need to configure your firewall (if available) and SyncBackPro to allow a range of ports for the FTP server to contact SyncBackPro. They can be set on the FTP->Firewall profile settings page in SyncBackPro. Without these ports opened, files cannot be transferred.



Encryption Type

An encrypted connection secures the data while it is transferred between systems. FTP connections are usually not encrypted but some FTP servers may require or offer an encrypted connection. The types of encryption are:

- Implicit SSL – Only SSL supported clients are allowed access. Secured communication is setup from the beginning of the connection. Server and client do not transmit clear text during the session. Default SSL port is 990.
- Explicit SSL – A mix of non-secure and secure clients are allowed. Unencrypted FTP connection are established but can be upgraded to a secure connection when sensitive data are requested for sending.
- SFTP – SFTP stands for Secure FTP. It uses secure shell connection (SSH) and requires encrypted public key authentication. Files are transferred between computers over a SSH secure data stream.

Conclusion

FTP has been around for a long time and while its popularity has decreased since the introduction of cloud services, it is still commonly used by administrators for file uploads to the web server and file data transfer/backups to FTP servers. SyncBackPro developed by 2BrightSparks offers a convenient and effective way to backup or transfer files between your system and the FTP server.

In addition to this general guide about FTP, you may also be interested in reviewing more technical writing about the protocol. 2BrightSparks also features hundreds of articles in our Support Knowledge Base which you may find valuable.