NAME – Rahul Kumar

Student ID - 157197211

File Transfer Protocol

1. Introduction

File Transfer Protocol (FTP) is part of TCP/IP suite. It is used to transfer files reliably across different platforms. It is an application layer protocol. The main objectives of FTP are:

- Transfer of files.
- Simplification of remote terminal usage and variations in different system.

This report covers the history, basic terminology, real-life usage and finally the importance of FTP.

2. Terminology

Data Types:

- ASCII TYPE: This is the default type and is accepted by all FTP types and Clients. It's used to transfer text files but, if both sides can easily use EBCDIC type, that type is used.
- EBCDIC TYPE: This type is also used to transfer text files but, it is more efficient than ASCII representation and it contains wider range of characters.
- IMAGE TYPE: This type is also accepted by every implementation of FTP. It is used for efficient transfer of files and binary data.

Data Structures:

- File-structure: There is no structure, file is a continuous sequence of data bytes.

- Record-Structure: File is made of sequential records.
- Page-Structure: File is made up of indexed pages. Every page has a header which contains header length, page index, data length and page type.

FTP Types:

- Anonymous FTP: Most basic form of FTP. Provides support for data transfers without encryption of data or a username and password. Most commonly used for downloading material that is allowed for unrestricted distribution. Works on port 21.
- Password-protected FTP: Also a basic FTP service, but requires the use of a username and password, but the service might not be encrypted or secure. Also works on port 21.
- FTP Secure (FTPS): It is sometimes referred to as FTP Secure Sockets Layer (FTP-SSL), it enables implicit Transport Layer Security (TLS) as soon as an FTP connection is established. FTPS was initially used to transfer data more securely. It typically uses] port 990.
- FTP over explicit SSL/TLS (FTPES): It enables explicit TLS support by changing the connection on port 21 to an encrypted connection. This is commonly used by web and file sharing services to enable secure file transfers.
- Secure FTP (SFTP): Not an FTP protocol, functions similarly. It is a subset of the Secure Shell (SSH) protocol, runs over port 22. Commonly used by systems administrators to remotely and securely access systems and applications. It provides a mechanism within SSH for secure file transfer.

Clients:

- FileZilla: Free FTP client for Windows, macOS and Linux, supports FTP, FTPS and SFTP.
- Transmit: FTP client for macOS, supports FTP and SSH.
- WinSCP: A Windows FTP client that supports FTP, SSH and SFTP.
- WS_FTP. This is another Windows FTP client that supports SSH.

3. Importance

Instead of FTP, files and data can be transferred using other services such as emails and web services, but those services do not provide control and precision. Therefore, FTP is very important for businesses that wants data transfer between their networks and employees. Basically, FTP is necessary for any individual or a company that needs data sharing over the internet.

References

1. Postel, J., & Reynolds, J. (1985, October). File transfer protocol (FTP). RFC 959: File Transfer Protocol. Retrieved from https://www.w3.org/Protocols/rfc959/

2. Kerner, S. M., & Burke, J. (2021, May 6). What is FTP? file transfer protocol explained. TechTarget. Retrieved from

https://www.techtarget.com/searchnetworking/definition/File-Transfer-Protocol-FTP