Le protocole FTP

BTS SiO1 2022-2023 / IZAC Matthieu

-SOMMAIRE

- Introduction sur le protocole FTP

Le protocole FTP (File Transfer Protocol) est, comme son nom l'indique, un protocole de transfert de fichier.

La mise en place du protocole FTP date de 1971, date à laquelle un mécanisme de transfert de fichiers (décrit dans le RFC 141) entre les machines du MIT (Massachussetts Institute of Technology) avait été mis au point. De nombreux RFC ont ensuite apporté des améliorations au protocole de base, mais les plus grandes innovations datent de juillet 1973.

Le protocole FTP est actuellement défini par le RFC 959 (File Transfer Protocol (FTP) - Specifications).

- C’est quoi le service FTP ?

File Transfer Protocol (protocole de transfert de fichier), ou FTP, est un protocole de communication destiné au partage de fichiers sur un réseau TCP/IP. Il permet, depuis un ordinateur, de copier des fichiers vers un autre ordinateur du réseau, ou encore de supprimer ou de modifier des fichiers sur cet ordinateur. Ce mécanisme de copie est souvent utilisé pour alimenter un site web hébergé chez un tiers.

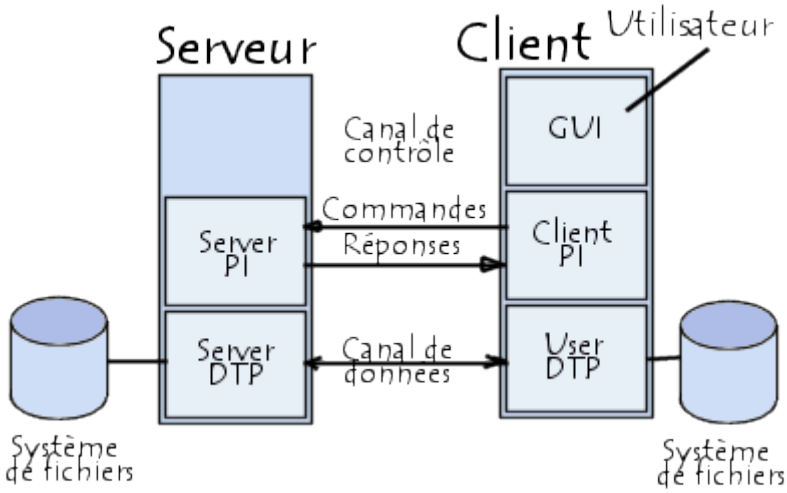
- Développement

Schéma du fonctionnement du protocole FTP

Le protocole FTP s'inscrit dans un modèle client-serveur, c'est-à-dire qu'une machine envoie des ordres (le client) et que l'autre attend des requêtes pour effectuer des actions (le serveur).

Lors d'une connexion FTP, deux canaux de transmission sont ouverts :

- Un canal pour les commandes (canal de contrôle)
- Un canal pour les données



https://web.maths.unsw.edu.au/~lafaye/CCM/internet/ftp.htm

Fonctionnement du transfert à travers ce protocole (avec le schéma page 3).

le client comme le serveur possèdent deux processus permettant de gérer ces deux types d'information :

◆le DTP (*Data Transfer Process*) est le processus chargé d'établir la connexion et

◆de gérer le canal de données. Le DTP côté serveur est appelé *SERVER-DTP*, le DTP côté client est appelé *USER-DTP*

le PI (*Protocol Interpreter*) est l'interpréteur de protocole permettant de commander le DTP à l'aide des commandes reçues sur le canal de contrôle. Il est différent sur le client et sur le serveur :

Le SERVER-PI est chargé d'écouter les commandes provenant d'un USER-PI sur le canal de contrôle sur un port donné, d'établir la connexion pour le canal de contrôle, de recevoir sur celui-ci les commandes FTP de l'USER-PI, d'y répondre et de piloter le SERVER-DTP

Le USER-PI est chargé d'établir la connexion avec le serveur FTP, d'envoyer les commandes FTP, de recevoir les réponses du SERVER-PI et de contrôler le USER-DTP si besoin

Lors de la connexion d'un client FTP à un serveur FTP, le USER-PI initie la connexion au serveur selon le protocole Telnet. Le client envoie des commandes FTP au serveur, ce dernier les interprète, pilote son DTP, puis renvoie une réponse standard. Lorsque la connexion est établie, le serveur-PI donne le port sur lequel les données seront envoyées au Client DTP. Le client DTP écoute alors sur le port spécifié les données en provenance du serveur.

Protocole

Non sécurisé (FTP)

L'inconvénient principal du protocole FTP, c'est qu'il n'est pas sécurisé. Pour cause, il a été inventé à une époque où la sécurité n'était pas aussi importante qu'aujourd'hui. Lorsque vous établissez une connexion avec un serveur FTP, l'identifiant, le mot de passe et toutes les commandes, transite en clair sur le réseau.

sécurisé (FTPS)

Le protocole FTPS n'est autre que la déclinaison sécurisée du protocole FTP. Le chiffrement SSL/TLS vient s'ajouter pour sécuriser les communications entre le client FTP et le serveur FTP. Pour le reste, c'est identique.

Néanmoins, il faut préciser que le FTPS fonctionne selon deux modes :

◆FTP explicite : dans ce cas la connexion s'établie sur le port 21 et le client FTP négocie avec le serveur FTP pour chiffrer la connexion. Des commandes FTP sont utilisées : "AUTH TLS" ou "AUTH SSL" et "PROT P"

◆ FTP implicite : le client commence directement la connexion avec le chiffrement SSL et va utiliser plutôt le port 990 que le port 21

sécurisé (SFTP)

SFTP signifie "SSH File Transfer Protocol" ou "Secure File Transfer Protocol". Nous pouvons dire les deux.

En plus du protocole FTP, il va s'appuyer sur un deuxième protocole : le SSH. Le poste client va établir un tunnel SSH avec le serveur distant, et le flux FTP passera dans ce tunnel SSH, ce qui signifie que le flux est sécurisé.

Il n'est pas nécessaire d'avoir un serveur FTP pour établir une connexion à l'aide du SFTP. Par contre il est nécessaire d’avoir un serveur SSH sur le serveur distant donc la

connexion s'effectue sur le port SSH, à savoir le port 22 par défaut. Une seule connexion à établir et ensuite tout se passe dans le tunnel SSH.

Dans quels cas a t-on besoin de transférer des fichiers ou dossiers par le biais de ce protocole?

Le protocole FTP définit la façon selon laquelle des données doivent être transférées sur un réseau TCP/IP.

de manière efficace Le protocole FTP a pour objectifs de :

- ◆permettre un partage de fichiers entre machines distantes
- ◆permettre une indépendance aux systèmes de fichiers des machines clientes et serveur
- ◆permettre de transférer des données

- Conclusion

En somme FTP est une protocole de transfert de fichiers qui est de base non sécurisé mais qui peut l'etre en utilisant les variantes SFTP ou encore FTPS. Il permet le transfert de fichier sur le port 21 (de base) entre deux machines distantes.

Pour accéder à un serveur FTP, on utilise un logiciel client FTP (possédant une interface graphique ou en ligne de commande).