

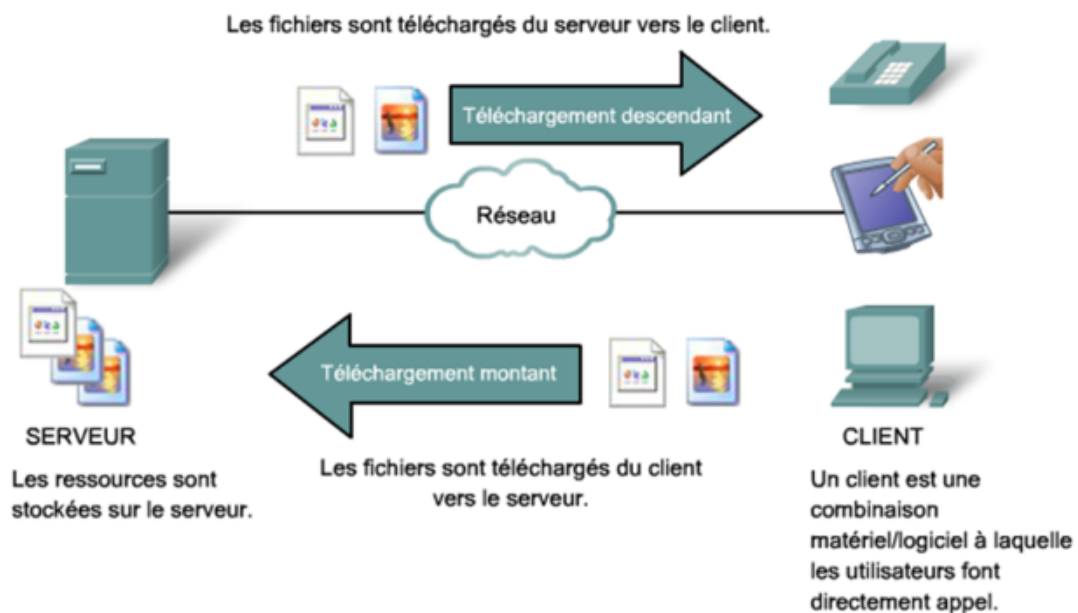
Dans ce modèle d'architecture, le périphérique qui :

- demande les informations est nommé client
- répond à la requête est nommé serveur.

Les processus client et serveur sont considérés comme faisant partie de la couche application. Le client commence l'échange en demandant des données au serveur, qui répond en envoyant un ou plusieurs flux de données au client.

Le transfert de données :

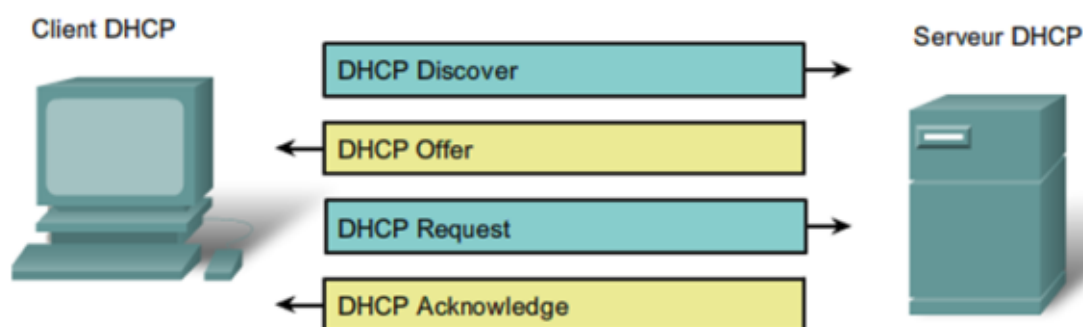
- D'un client vers un serveur est désigné par le terme téléchargement montant (upload),
- D'un serveur vers un client est désigné par le terme téléchargement descendant (download).



Protocole DHCP

Le service fourni par le protocole DHCP (Dynamic Host Configuration Protocol) permet aux périphériques d'un réseau d'obtenir d'un serveur DHCP des adresses IP et d'autres informations. Ce service automatise l'affectation des adresses IP, des masques de sous-réseau, d'une adresse IP de passerelle et d'autres paramètres de configuration de la couche réseau.

Il permet à un hôte d'obtenir une adresse IP dynamiquement lorsqu'il se connecte au réseau. Les adresses attribuées via le protocole DHCP ne sont pas affectées aux hôtes définitivement mais uniquement pour une durée spécifique (bail). Si l'hôte est mis hors tension ou retiré du réseau, l'adresse est retournée au pool pour être réutilisée.

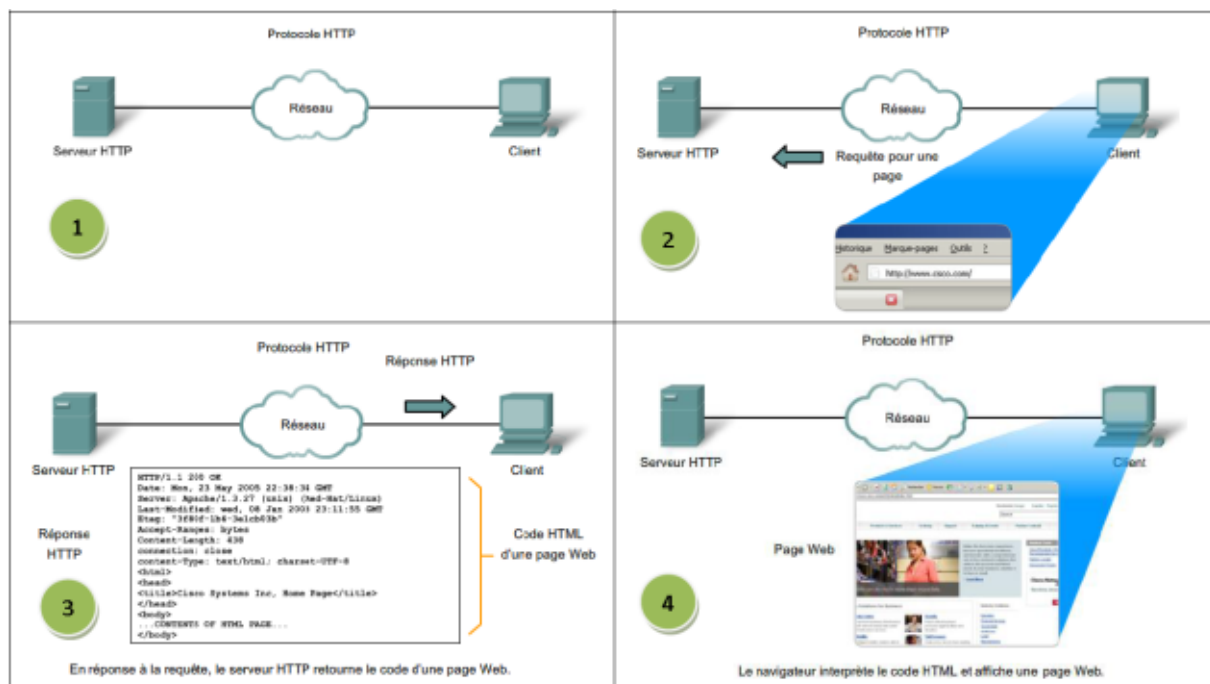


Protocole HTTP

Le protocole HTTP est utilisé à travers le Web pour le transfert des données et constitue l'un des protocoles d'application les plus utilisés.

C'est un protocole de requête/réponse. Lorsqu'un client (généralement un navigateur Web) envoie une requête à un serveur, le protocole HTTP définit les types de messages que le client utilise pour demander la page Web, ainsi que les types de messages que le serveur utilise pour répondre. Bien qu'il soit remarquablement flexible, le protocole HTTP n'est pas un protocole sécurisé. Bien qu'il soit remarquablement flexible, le protocole HTTP n'est pas un protocole sécurisé.

Pour une communication sécurisée via Internet, le protocole HTTPS (HTTP Secure) est utilisé lors de l'accès aux informations du serveur Web ou de leur publication. Le protocole HTTPS peut procéder à l'authentification et au chiffrement pour sécuriser les données pendant qu'elles circulent entre le client et le serveur. Le protocole HTTPS spécifie des règles supplémentaires de transmission de données entre la couche application et la couche transport.



Protocole FTP

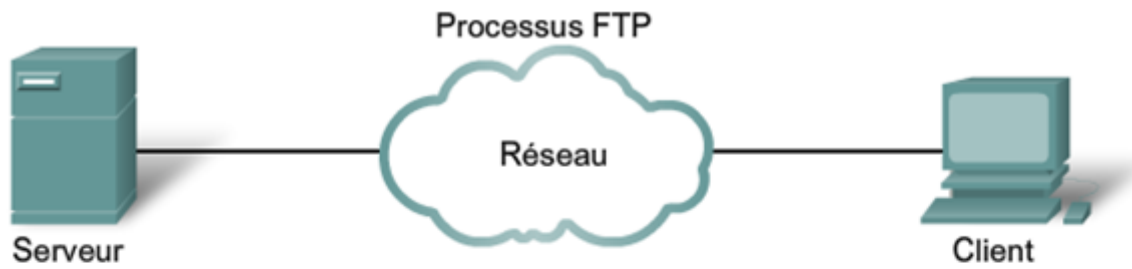
Le protocole FTP (File Transfer Protocol) a été développé pour permettre le transfert de fichiers entre un client et un serveur. Un client FTP est une application s'exécutant sur un ordinateur et utilisée pour extraire des fichiers d'un serveur exécutant le démon FTP.

Pour transférer les fichiers correctement, le protocole FTP nécessite que deux connexions soient établies entre le client et le serveur : une connexion pour les commandes et les réponses et une autre pour le transfert même des fichiers.

Le client établit la première connexion au serveur sur le port TCP 21. Cette connexion est utilisée pour le trafic de contrôle et se compose de commandes clientes et de réponses serveur.

Le client établit la seconde connexion au serveur via le port TCP 20. Cette connexion est destinée au transfert même des fichiers et est établie à chaque transfert de fichiers.

Le transfert de fichiers peut s'effectuer dans l'une des deux directions. Le client peut télécharger un fichier à partir du serveur ou en direction du serveur.



Connexion de contrôle :

le client établit une première connexion au serveur pour contrôler le trafic.



Connexion de données :

le client établit une seconde connexion pour le trafic de données.



En fonction de la commande envoyée via la connexion de contrôle, les données peuvent être téléchargées depuis le serveur ou depuis le client.