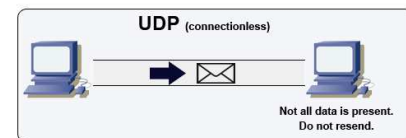
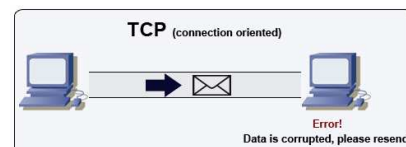
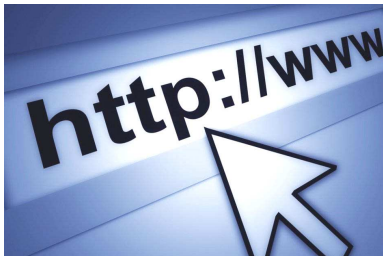
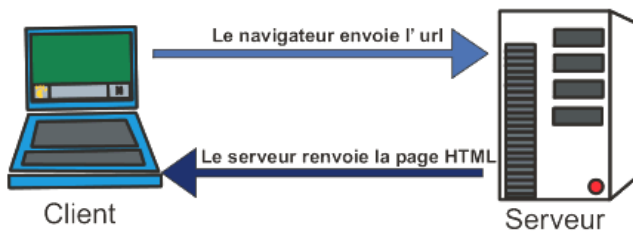


**ARCHITECTURE CLIENT/SERVEUR : PROTOCOLES
HTTP/FTP (TCP/UDP POUR LES SERVEURS P2P)****Objectifs du COURS :**

Ce cours traitera essentiellement les points suivants :

- comprendre l'architecture d'un système communicant
- évaluer les risques liés à une transmission de données sur un réseau
- les protocoles TCP et UDP pour les serveurs P2P
- le protocole HTTP (les méthodes et le dialogue)
- le protocole FTP (les modes de fonctionnement)
- exercices d'application
- avantages et inconvénients de la communication client/serveur

L'architecture client/serveur désigne un mode de communication entre plusieurs composants d'un réseau. Chaque entité est considérée comme un client ou un serveur. Chaque logiciel client peut envoyer des requêtes à un serveur. Un serveur peut être spécialisé en serveur d'applications, de fichiers, de terminaux, ou encore de messagerie électronique.

En résumé :

Le client pose une question (ou donne un ordre)... et le serveur répond à la question (ou obéit).

DIALOGUE CLIENT/SERVEUR

UN CLIENT

Les caractéristiques d'un client sont les suivantes : **il est d'abord actif (ou maître), il envoie des requêtes au serveur, il attend et reçoit les réponses du serveur.**

UN SERVEUR

Un serveur est initialement **passif**, il attend, il est à l'écoute, prêt à répondre aux requêtes envoyées par des clients. **Dès qu'une requête lui parvient, il la traite et envoie une réponse.**

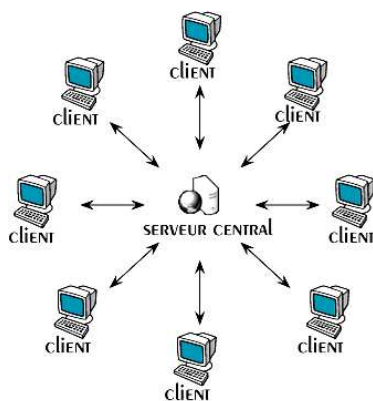
LE DIALOGUE

Le client et le serveur doivent bien sûr utiliser le même **protocole de communication**. Un serveur est généralement capable de servir plusieurs clients simultanément.

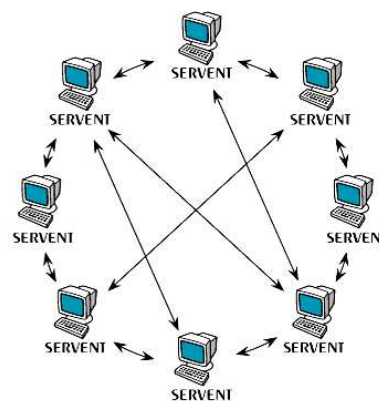
Remarques :

Une fois le client traité, le serveur peut en traiter un autre. Il existe des serveurs multiclients comme les serveurs Web/http qui sont capables de traiter plusieurs clients en même temps. Il existe aussi des serveurs « non connectés », dans ce cas il n'y a pas de connexion ou de déconnexion.

Un autre type d'architecture réseau est le pair à pair (peer to peer en anglais ou P2P), dans lequel chaque ordinateur ou logiciel est à la fois client et serveur.



Architecture Client/Serveur



Architecture P2P

Les systèmes pair-à-pair permettent à plusieurs ordinateurs de communiquer via un réseau, de partager simplement des fichiers le plus souvent, mais également des flux multimédia ou encore un service (comme la téléphonie avec Skype par exemple), ... sur internet.

L'utilisation d'un système pair-à-pair nécessite pour chaque nœud l'utilisation d'un logiciel particulier. Ce logiciel, qui remplit alors à la fois les fonctions de **client et de serveur**, est parfois

appelé **servent** (de la contraction de « serveur » et de « client »), ou plus communément mais de façon réductrice, « client ».

Une des applications la plus connue est le partage de fichiers par le biais de logiciel à la fois client et serveur comme eDonkey, eMule, FastTrack (utilisé par KaZaA) ou BitTorrent...

Les serveurs pair-à-pair fonctionnent dans la quasi-totalité des cas en mode synchrone : le transfert d'information est limité aux éléments connectés en même temps au réseau. Ils peuvent utiliser le protocole **TCP** (**T**ransmission **C**ontrol **P**rotocol ou protocole de contrôle de transmissions) comme couche de transport des données (il fonctionne en duplex, la réception des données est donc confirmée et leur intégrité est assurée).

En revanche, certaines utilisations comme le continu (streaming) nécessitent l'emploi d'un protocole plus léger et plus rapide, comme **UDP** (**U**ser **D**atagram **P**rotocol ou protocole de datagramme utilisateur), bien que moins fiable, l'UDP est aussi le protocole le plus utilisé pour transmettre des messages entre serveurs dans les systèmes en partie centralisés.

HTTP (HyperText Transfer Protocol)

La consultation des pages sur un site web a un fonctionnement basé sur une architecture client/serveur. Un internaute connecté au réseau via son ordinateur et un navigateur web est le client, le serveur est constitué par le ou les ordinateurs contenant les applications qui délivrent les pages demandées. Dans ce cas, c'est le protocole de communication **HTTP** (**H**yper**T**ext **T**ransfer **P**rotocol) qui est utilisé.

Les navigateurs sont les clients (Firefox, Internet Explorer, ...). Ces clients se connectent à des serveurs http tels qu'Apache http Server ou IIS (Internet Information Services).

Remarque :

HTTPS (avec S pour Secured ou Sécurisé) est la variante de http sécurisée par l'usage des protocoles **SSL** (**S**ecure **S**ockets **L**ayer) ou nouvellement nommé **TLS** (**T**ransport **L**ayer **S**ecurity) qui est un protocole de sécurisation des échanges sur internet.

LES MÉTHODES

Dans le protocole http, une méthode est une commande spécifiant un type de requête, c'est-à-dire qu'elle demande au serveur d'effectuer une action. En général, l'action concerne une ressource identifiée par l'URL qui suit le nom de la méthode.

Les méthodes les plus utilisées sont **GET** et **POST**.

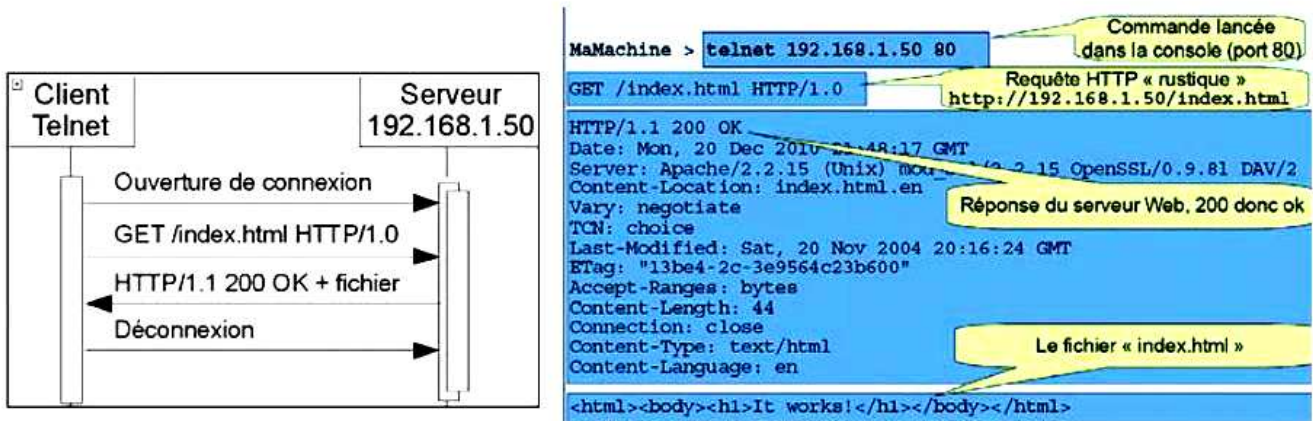
GET : c'est la méthode la plus courante pour demander une ressource. Une requête GET est sans effet sur la ressource.

POST : cette méthode doit être utilisée pour ajouter une nouvelle ressource, comme un message sur un forum, un article dans un site ou encore un login et un mot de passe.

Les autres méthodes sont : HEAD, OPTIONS, CONNECT, TRACE, PUT, DELETE. Certains serveurs autorisent des méthodes supplémentaires permettant la gestion des ressources du serveur (par exemple WebDAV ou CALDAV).

DIALOGUE HTTP

La commande **Telnet** exécutée dans un terminal permet de « simuler » un navigateur.



Lien vers les codes HTTP :

<http://www.codeshttp.com/>

La réponse du serveur contient « Content-Lengh: 44 ».

Question :

À votre avis, que représente la valeur 44 et comment peut-on vérifier cette valeur ?

44 représente la longueur des données utiles en nombre d'octets (et donc de caractères en UTF-8).

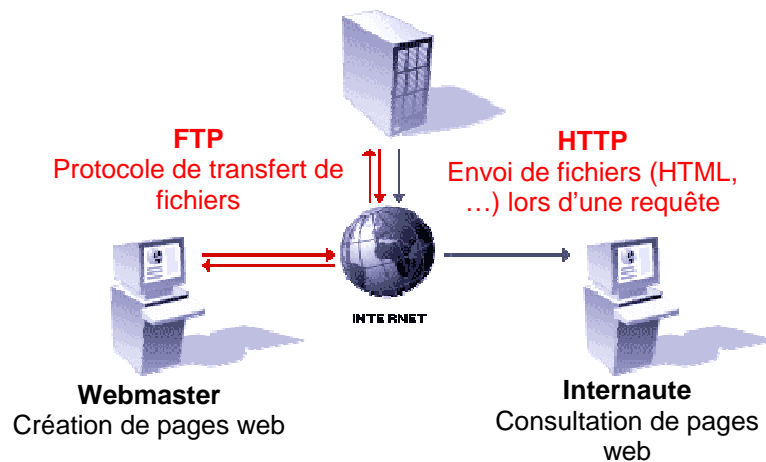
Pour vérifier il suffit de compter le nombre de caractères... depuis <html> jusqu'à </html> (marqueurs compris).

FTP (File Transfer Protocol)

Le protocole de transfert de fichiers, ou FTP (File Transfer Protocol), est un protocole de communication destiné à l'échange informatique de fichiers sur un réseau TCP/IP. Il permet, depuis un ordinateur, de copier des fichiers vers un autre ordinateur du réseau, d'alimenter un site web, ou encore de supprimer ou de modifier des fichiers sur cet ordinateur.

FTP obéit à un modèle client/serveur, c'est-à-dire qu'une des deux parties, le client, envoie des requêtes et le serveur répond.

En pratique, le serveur est un ordinateur sur lequel fonctionne un logiciel lui-même appelé serveur FTP. Pour accéder à un serveur FTP, on utilise un logiciel client FTP (possédant une interface graphique comme FileZilla par exemple ou en ligne de commande).



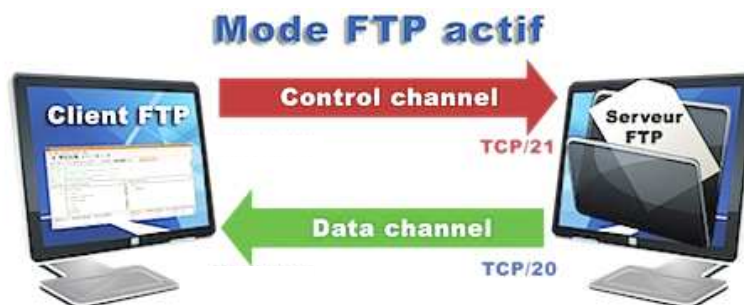
Rôle de FTP dans la publication WEB

MODES DE FONCTIONNEMENT

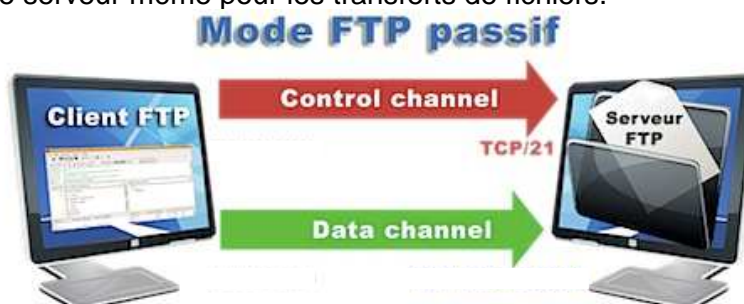
Deux ports sont standardisés pour les connexions FTP : le port 21 pour les commandes et le port 20 pour les données.

MODE ACTIF

Le client devient serveur pour recevoir un fichier, cela permet de télécharger le « serveur » FTP. Ce mode ne fonctionne pas très bien avec les « BOX » internet.

**MODE PASSIF**

Le serveur FTP reste serveur même pour les transferts de fichiers.



EXERCICES D'APPLICATION

QCM

Question :

Encadrer les bonnes réponses.

Un serveur web écoute sur le port 80...

Réponse : Vrai Faux

Vous souhaitez déposer un fichier sur un serveur,
Quel protocole utilisez-vous ?

Réponse : FTP HTTP

Vous souhaitez obtenir la liste de fichiers disponibles
sur votre serveur, quel protocole utilisez-vous ?

Réponse : FTP HTTP

Vous vous connectez sur un compte FTP, votre FAI
(Fournisseur d'Accès Internet) peut-il avoir connaissance
de votre mot de passe ?

Réponse : Oui Non

CAPTURE DE TRAME AVEC WIRESHARK

WireShark est un utilitaire permettant de capturer des trames réseau.
Un échange entre un client et un serveur a été intercepté.
En utilisant le tableau ci-dessous :

Source	Destination	Protocole	Info
192.168.1.50	192.168.1.45	FTP	Response: 220 192.168.1.50 FTP server (tnftpd 20080929) ready.
192.168.1.45	192.168.1.50	FTP	Request: USER test
192.168.1.50	192.168.1.45	FTP	Response: 331 User test accepted, provide password.
192.168.1.45	192.168.1.50	FTP	Request: PASS Chocolat2010
192.168.1.50	192.168.1.45	FTP	Response: 230 User test logged in.
192.168.1.45	192.168.1.50	FTP	Request: SYST
192.168.1.50	192.168.1.45	FTP	Response: 215 UNIX Type: L8 Version: tnftpd 20080929
192.168.1.45	192.168.1.50	FTP	Request: FEAT
192.168.1.50	192.168.1.45	FTP	Response: 211-Features supported
192.168.1.50	192.168.1.45	FTP	Response: MDTM
192.168.1.45	192.168.1.50	FTP	Request: PWD
192.168.1.50	192.168.1.45	FTP	Response: 257 "/Users/test" is the current directory.
192.168.1.45	192.168.1.50	FTP	Request: QUIT
192.168.1.50	192.168.1.45	FTP	Response: 221-
192.168.1.50	192.168.1.45	FTP	Response: Data traffic for this session was 0 bytes in 0 files.

Question 1 :

Quelle est l'adresse IP du serveur ?

192.168.1.50

Question 2 :

Quelle est l'adresse IP du client ?

192.168.1.45

Question 3 :

Quel utilisateur se connecte au serveur ?

Utilisateur connecté au serveur = test

Question 4 :

Quel est le mot de passe de l'utilisateur connecté au serveur ?

Mot de passe = Chocolat2010

Question 5 :

FTP est-il un protocole sécurisé ?

Non

ÉCHANGE HTTP

Dans l'échange HTTP suivant :

```
$> telnet www.llfnet.fr 80
POST /cgi-bin/montest.pl HTTP/1.1
Host: 192.168.1.1
Content-Length: 33
envoiest=testdenvoiestdeparametre
HTTP/1.1 200 OK
Date: Mon, 03 Dec 2012 22:45:12 GMT
Server: Apache/2.2.15 (Unix) mod_ssl/2.2.15 OpenSSL/0.9.8l DAV/2
Content-Length: 85
Connection: close
Content-Type: text/html; charset=ISO-8859-1
<HTML>
<BODY>
contenu HTML donnée = envoiest=testdenvoiestdeparametre
</BODY>
</HTML>
```

Question 1 :

Lister l'adresse IP du serveur, la version et le type de serveur web ?

Adresse IP du serveur : 192.168.1.1

Nom du serveur : www.lifnet.fr

Le serveur est de type Apache version 2.2.15

Question 2 :

Surligner les données transférées par la requête POST.

Les données reçues sont en rouge.

Question 3 :

Quel est le type des données envoyées par le serveur web ?

Le champ Content-Type: text/html, nous renseigne sur le contenu. Les données sont donc de l'html.

COMMUNICATION CLIENT/SERVEUR

Le mode client/serveur n'est pas le modèle de communication parfait, il n'y en a pas !
Connaissant les avantages et les inconvénients par rapport au mode distribué (par exemple pair à pair), vous pourrez choisir celui qui vous convient.

AVANTAGES

Toutes les données sont centralisées sur un seul serveur, on a donc « un contrôle de sécurité simplifié ».

Les technologies supportant l'architecture client/serveur sont plus matures que les autres (et plus anciennes).

L'administration se porte au niveau serveur. Toute la complexité/puissance peut être déportée sur le(s) serveur(s), les utilisateurs utilisant simplement un client léger.

Les serveurs étant centralisés, cette architecture est particulièrement adaptée et vélocité pour retrouver et comparer de vastes quantités d'information (moteur de recherche sur le web).

INCONVÉNIENTS

Si trop de client veulent communiquer sur le serveur en même temps, ce dernier risque de ne pas supporter la charge (alors que les réseaux pair à pair fonctionnent mieux en ajoutant de nouveaux participants).

Si le serveur n'est plus disponible, plus aucun des clients ne fonctionne (le réseau pair à pair continue à fonctionner, même si plusieurs participants quittent le réseau).

Les coûts de mise en place et de maintenance sont élevés.

En aucun cas les clients ne peuvent communiquer entre eux, entraînant une asymétrie de l'information au profit des serveurs.