

# M1 Informatique

## Réseaux

### Applications de l'Internet

Bureau S3-354

Jean.Saquet@unicaen.fr

[http : saquet.users.greyc.fr/M1/rezo](http://saquet.users.greyc.fr/M1/rezo)

# Client / serveur (1)

Beaucoup d'applications sur ce modèle :

Le serveur est en attente de requête, y répond, se remet en attente

Le client (souvent commandé par une I.H.M) émet des requêtes et reçoit les réponses

Cas le plus simple : un dg de requête, un dg de réponse (ex : date, dns, echo ...)

# Client / serveur (2)

Nécessité d'utilisation du no de port (couche transport)

TCP ou UDP

nos de ports serveurs "bien connus"

Parfois, utilisation d'un ou plusieurs autres ports

Avec TCP, identification de la connexion par adr/port

Processus fils ou autre thread pour continuer le dialogue

Serveurs multi-clients.

# Format des messages

Les éléments du protocole doivent respecter le format prévu dans la définition (RFC)

Le format peut être binaire (champs définis en taille d'octets, de bits, éventuellement lg variable avec un champ longueur)

Le format peut être texte, plus ou moins formaté (voir POP et HTTP par exemple)

# Applications- Historique

Telnet : premières propositions en ... 1971 !

Courier électronique : 1972

FTP : RFC 114, avril 1971

SMTP : RFC 821, 1982

...

HTML(2.0), HTTP : publiés (RFC) en 1995/1996  
(en fait opérationnels un peu avant)

# Telnet (1)

But : terminal déporté (connexion à distance)

- Terminal virtuel (interface de commande des machines distantes)
- Négociation d'options

Utilise une connexion TCP

Définition "standard" des touches de contrôle, de mise en page, fin de ligne, ... : utilisée dans la communication

Adaptation à chaque système au niveau des applis serveurs et clientes

# Telnet (2)

Options négociables pour (par exemple) :

- codage des caractères
- echo local ou distant
- échange d'infos sur les possibilités de mise en page
- envoi de lignes complètes ou non  
(sinon : 1 caractère = 1 datagramme !)

Négociation d'options symétrique :

- puis-je utiliser l'option X ?
- vous pouvez ou vous ne pouvez pas

# Telnet (3)

Très utilisé au début des réseaux (avant même Internet)  
Sécurité faible : accès par login / mot de passe du système distant, données transmises en clair.  
Versions sécurisées avec SSL, mais de plus en plus remplacé par SSH;

Note : le client telnet permet une connexion TCP avec un port quelconque (par défaut port telnet=23)



# Inetd

C'est un "méta-serveur" permettant d'être à l'écoute sur plusieurs ports et d'aiguiller les requêtes vers le serveur concerné

Fichier de configuration : `/etc/inetd.conf`

Certains serveurs peuvent s'exécuter en "stand-alone" ou bien via inetd

# Transfert de fichiers

... ou plutôt copie de fichiers, via le réseau.

Utilité évidente.

Nécessite de connaître les ressources, leur emplacement

Copie fiable par FTP

Téléchargement de fichiers de config par TFTP

Comparaison avec les systèmes de fichiers en réseau  
(NFS dans le monde Unix)

# Copie de fichiers

Quelques problèmes à résoudre :

localisation des fichiers

droits d'accès

codage des fichiers

(représentation des nombres, jeux de caractères, fins de ligne, ...)

Pour la localisation, des systèmes d'indexation ont existé (avant les moteurs de recherche) : Wais, Archie, Veronica, Gopher (précurseurs du Web - 1990-1992)

# FTP (1)

Très longtemps utilisé

Interface utilisateur console très complète,  
interfaces graphiques disponibles.

S'adapte aux types de fichiers, codage de  
caractères.

Authentification par login / mot de passe ou  
serveur ftp "anonyme"

# FTP (2)

TCP, serveur sur port 21 en standard

Connexion de supervision pour commandes

Connexion de transfert de données séparée, avec des numéros de ports alloués à chaque transfert.

Le serveur peut utiliser le port 20 pour les données.

Mode passif ou actif du serveur pour l'établissement de la connexion de données

# FTP (3)

À étudier :

commandes de l'interface console ftp

comparaison avec interfaces graphiques

comparaison avec éléments de protocole

transferts en mode texte ou binaire

copie ou non des attributs du fichier (date, droits d'accès, ...)

serveurs ftp anonymes, download / upload

# TFTP

Trivial FTP. Utilise UDP, pas de sécurité  
Utilisé surtout pour télécharger des images OS  
dans des systèmes sans disques, au sein d'un  
réseau privé.

Utilisé par routeurs, terminaux X-windows, ...  
Blocs de fichiers numérotés, acquittés un à un

# Partage de fichiers en réseau

Différent de transfert de fichier : pas de copie  
(on travaille sur le fichier distant)

l'OS accède aux fichiers soit par les fonctions locales, soit en passant par client / serveur transparent pour l'utilisateur

3 réalisations concurrentes : Partage Windows (SMB), Appleshare (AFS) et Unix-Sun (NFS)



# Partage vs transfert

Partage de fichiers en réseau utilisée dans un (inter)réseau d'entreprise. Fortement déconseillé sur Internet.

Transfert de fichiers entre sites distants. Permet de conserver une copie (mais nécessité de mise à jour)

FTP encore beaucoup utilisé pour alimentation des sites Web

# HTTP

Les transferts de fichiers s'effectuent de plus en plus avec http, ou avec le client ftp inclus dans un navigateur. Toutefois :

La fonction "put" de http est peu usitée

Le client ftp des navigateurs est bien plus limité qu'un bon client ftp.

Mieux vaut utiliser les applications pour ce qu'elles savent (bien) faire !

# Courrier électronique

Très utilisé, depuis longtemps  
SMTP pour dialogue entre serveurs, ou bien  
client->serveur.

En fait SMTP utilisé pour envoyer le courrier

Simple : courrier = texte ascii (américain de préf !)

Réseaux 7 bits anciens

Nécessité de transcodage pour image, fichiers  
binaires, ...

# SMTP

Protocole très simple

HELO ou EHLO

MAIL FROM: , RCPT TO:, DATA, ...

En-tête minimal,

éléments complémentaires dans la partie données, ligne blanche pour séparer les données

==> voir un mail "brut"

Pas de sécurité ==> utilisation abusive

# Serveurs de courrier

Fonction : recevoir et envoyer le mail

Attention au relais.

Instructions de ré-écriture possible, extension des aliases, ...

Sendmail, exim, courier, ...

Fichiers de configuration complexes

Un serveur mal configuré peut se retrouver "black-listé" par les autres.

# POP

Post Office Protocol

Mis au point pour récupération du courrier par un PC.

Protocole assez simple, authentification minimale.

Interfaces graphiques (précurseur : Eudora)

A remplacé la commande-ligne "mail" d'Unix.

Possibilité de lecture, d'effacement, ...

Version actuelle : POP3. Port serveur : 110

# IMAP

Internet Message Access protocol.

Beaucoup plus complexe.

Permet de gérer son courrier sur le serveur (nombreuses commandes) : gestion des boîtes aux lettres.

Les interfaces proposent aussi en général la copie locale

version actuelle : IMAP4. Port serveur : 143

# Webmail

Accès au courrier via une interface Web (navigateur) et un programme annexe sur le serveur (liaison http-mail)

Fonctions similaires à Imap, mais pas de copie locale, utilisation exclusivement en mode connecté.

Utile pour consultation en déplacement (cyber-café, ...). certains fournisseurs ne proposent QUE ce mode d'accès.



# SSH

SSH (Secure SHell).

Utilise SSL. Système de clefs privées/publiques.

Échange de clefs publiques lors de la première connexion, utilisées pour chiffrer les mots de

passer, ou bien accès direct par autorisation

préalable et dépôt des clefs publiques.

Remplace Telnet pour l'accès à distance.

Port serveur : 22

# Sftp, scp

Versions sécurisées (utilisant une connexion ssh) de ftp et de la commande de copie (cette dernière pouvant provoquer un échange réseau en cas de partage de fichiers)

Des clients graphiques existent.

Par contre, adaptation aux types de fichiers moins évidente

# SSHFS

Systeme de partage de fichiers en réseau,  
Basé sur SSH

Permet de monter des volumes, le transfert des  
fichiers s'effectuant dans des connexions SSH

Sécurisation des transferts  
Accès aux données comme avec un filesystem

# Courrier sécurisé

Il existe des versions sécurisées de smtp, pop, imap. Les ports utilisés sont différents (resp. 465, 995, 993). La plupart des logiciels serveurs modernes peuvent dialoguer de manière sécurisée.

==> possibilité d'authentification raisonnable, donc serveurs accessibles de l'extérieur du domaine.

# MIME/S

Possibilité d'authentification forte des messages (reconnue légalement) par utilisation de certificat d'utilisateur, délivré par un organisme habilité et reconnu et authentifié par des serveurs.

Les logiciels mailers modernes reconnaissent ces certificats.

Incompatible avec Webmail.