Applications

DNS, telnet, ssh, ftp, WWW, X-Window

e-mail : SMTP, POP, IMAP

Développées au dessus des protocoles TCP et/ou UDP
Ports spécifiques (voir /etc/services sousles Unix)

Applications

- DNS
  - service de noms
- FTP
  - transfert de fichier
- telnet, ssh
  - session de terminal à distance
- X-Window :
  - Gestion de fenêtres graphiques à distance
- WWW: World Wide Web
  - Hypermédia réparti

Applications

- Echange de courrier
  - Plusieurs protocoles sous jacents (émission/réception)
- SMTP *(Simple Mail Transfer Protocol)*
  - Envoi du courrier
- Accès à distance au courrier
  - POP *(Post-Office Protocol)*
    - » Réception du courrier
  - IMAP *(Internet Mail Access Protocol)*
    - » gestion plus élaborée d'une boîte distante

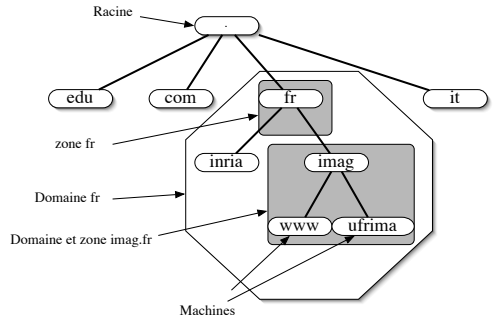
Le système de nommage d'Internet: Domain Name System

- Annuaire Adresse IP / Nom
- Au début (1970-1984) : annuaire complet dans un fichier texte (*/etc/hosts* sous Unix):
  - Adresse Nom1 Nom2 Nom3
  - Cohérence des noms par diffusion du fichier
- 1984 : mise en place du DNS
- Géré par Network Information Center (*http://www.nic.com*)
- En France Association Française pour le Nommage Internet en Coopération (*http://www.afnic.fr*)

- Information accessible grâce au DNS
  - Adresse en fonction du nom
  - Nom en fonction de l'adresse IP : résolution inverse
  - Adresse de relai de messagerie
- Système hiérarchique, redondant et distribué
  - Arborescence (comme un système de fichier)
  - Chaque site est maître de ses données
  - Dynamique: mise à jour automatique
- Documentation
  - http://www.dns.net/dnsrd (RFC, FAQ ...)
  - http://www.nic.fr/guides
  - http://www.nic.fr/formation

Structuration des noms

- Hiérarchique par domaine: www.imag.fr
  - machine www dans le domaine imag lui-même dans le domaine fr
  - Analogie nom de fichier/répertoire à l'envers avec le . à la place de /
  - On omet en général la racine (le point) : *www.imag.fr*.



Une base de données

- Une base de donnée est associée à chaque noeud
- L'ensemble de ces bases de données constitue le DNS
- Dans un noeud, on trouve
  - Les informations permettant de retrouver les noeuds fils
  - Les informations propre au noeud : liste des machines
  - Comme dans un répertoire : des sous répertoires et des fichiers
- La gestion de chaque noeud peut être effectuée par des entités différentes

Terminologie

- Domaine
  - Un domaine est la partie de l'arborescence à partir du noeud portant son nom
  - Exemple: domaine *fr*: arborescence à partir du noeud *fr*
  - Sous domaine : domaine inclus dans un autre
  - Exemple: *imag.fr* est un sous domaine du domaine *fr*
- Zone: C'est la base de donnée associée à un noeud
- Contenu des bases de donnée associées aux zones
  - Noms/Adresses des serveurs de la zone
    - » Exemples:
      - Racine: liste des serveurs des domaines de premiers niveaux
      - ***fr*: listes des adresses des serveurs des sous-domaines de *fr***
  - Noms/Adresses des machines de ce domaine

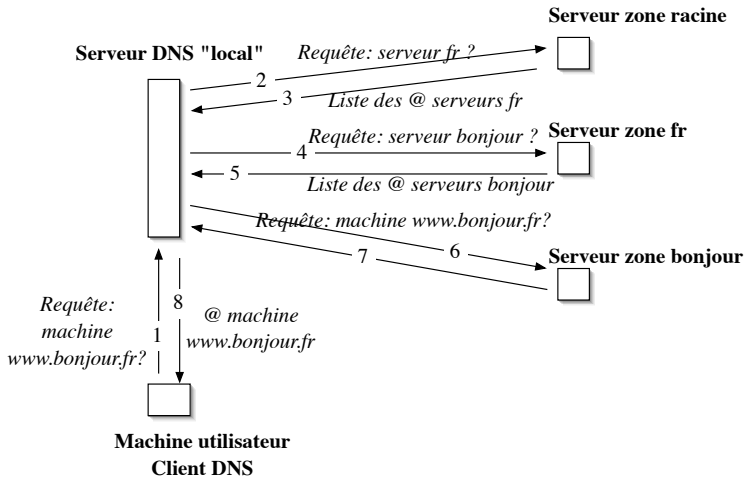
Domaines existants

- Terminologie de l'AFNIC: Domaine. Suffixe
- Suffixe ou Top Level Domain(TLD)
  - Par pays (ou Country Code, ccTLD) en deux lettres :
    - » .fr, .us, .jp, .be
    - » ICANN (Internet Corporation for Assigned Names and Number) :
      - *http://www.icann.org/cctlds/*
    - » IANA (Internet Assigned Numbers Autority) :
      - *http://www.iana.org/cctld/cctld.htm*
    - » Liste des contacts des différents ccTLD:
      - *http://www.iana.org/cctld/cctld-whois.html*
  - Génériques internationaux (gTLD) en trois lettres
    - » .com (entreprise multinationale), .org (organisation), .edu (Université)

Principe de fonctionnement

- Application client/serveur
- Serveurs DNS: il gère la base de données contenant
  - *nom*/*@IP* des machines du domaine
  - *nom*/*@IP* des serveurs d'un sous-domaine
- Système robuste par redondance: plusieurs serveurs possèdent la base de donnée d'un domaine
- Client DNS
  - Resolver: permet l'interrogation d'un serveur
  - Référence à un serveur DNS par défaut "local" (fichier sous Unix: */etc/resolv.conf*)
- Interrogation client vers serveur local
  - *Récursive*
  - Le client attend la réponse finale

Exemple d'une interrogation



Interrogation DNS

- Pour une zone : une liste d'adresse de serveurs
  - Répartition des interrogations
  - Requêtes successives si défaillance d'un serveur ou du réseau
  - Importance de la répartition géographique des serveurs d'une même zone
- Mécanisme de cache dans le serveur "local" pour limiter le nombre d'interrogations
  - Evite la surcharge du réseau
  - Diminue les délais de réponse
  - Baisse la charge des serveurs de haut niveau
- Remplissage du cache lors des requêtes des clients
- Durée de vie limitée dans le cache
  - TTL(Time To Live) spécifié dans les réponses

Serveurs

- Racine : 13 serveurs de nom répartis dans le monde
  - Connaissent tous les serveurs de premier niveau (TLD): *.fr*, *.com*, ...
  - SERVEUR “ORIGINE” (ou primaire, ou maitre) géré par IANA/ICANN
    - » *A.ROOT-SERVERS.NET*
  - SERVEURS MIROIRS (ou secondaire, ou esclave)
    - » de *B.ROOT-SERVERS.NET* à *M.ROOT-SERVERS.NET*
- Modification manuel faite sur le serveur primaire
- Echange des bases de données automatique vers les serveurs secondaires

Outils DNS

- Il existe des outils permettant d’envoyer des requêtes DNS (voir les man)
  - Host, dig, nslookup
- Possibilité d’interrogation de différents types:
  - A : nom host/adresse IPV4
  - AAAA: nom host/adresse IPV6
  - NS: liste des serveurs d’un domaine
  - MX: nom host/Adresse d’un serveur de messagerie
  - PTR: Adresse / Nom host

Outils DNS

- Exemple:
  - paros:~ sicard$ **host -t a www.google.com**
  - www.google.com is an alias for www.l.google.com.
  - www.l.google.com has address 209.85.229.104
  - www.l.google.com has address 209.85.229.105
  - www.l.google.com has address 209.85.229.106
  - www.l.google.com has address 209.85.229.147
  - www.l.google.com has address 209.85.229.99
  - www.l.google.com has address 209.85.229.103

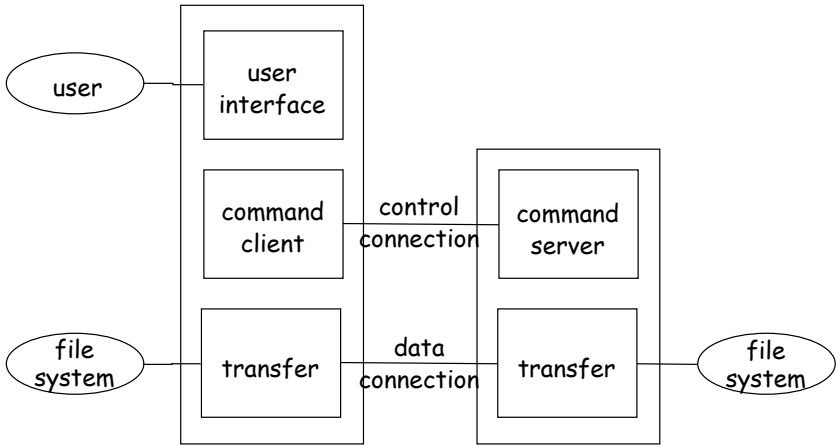
Outils DNS

- Exemple: Interrogation NS
  - paros:~ sicard$ **host -t ns imag.fr**
  - imag.fr name server dns.inria.fr.
  - imag.fr name server isis.imag.fr.
  - imag.fr name server ns2.nic.fr.
  - imag.fr name server imag.imag.fr.

FTP *(File Transfer Protocol)*

- File transfer
  - differents types de fichier
    - » text, binary
- FTP utilise deux connexions TCP
  - Transfert des commandes (port 21)
  - Transfert des données (port 20)
- Deux modes possibles (pour des problèmes de filtrage)

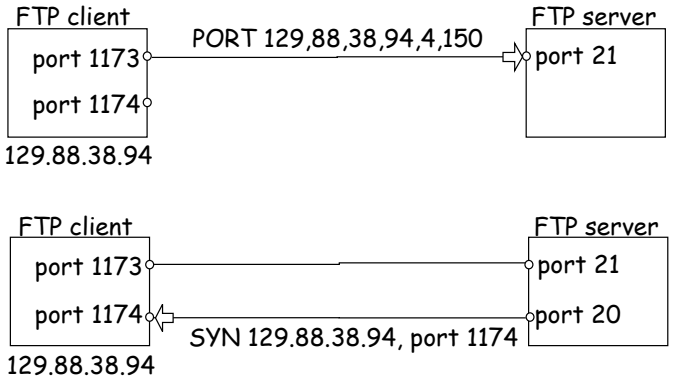
FTP



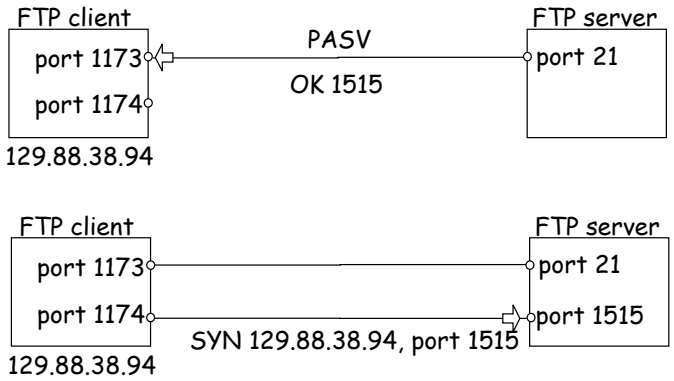
Commandes

- **open**
- **dir, ls, ls -l**
- **cd, lcd**
- **binary, ascii**
- **prompt**
- **get, mget**
- **put, mput**
- **quit, bye**
- **stat**
- **Suivant les versions les commandes sur la machine locale:**
  - **!pwd, !cd, ou lpwd, lcd**

FTP - actif mode



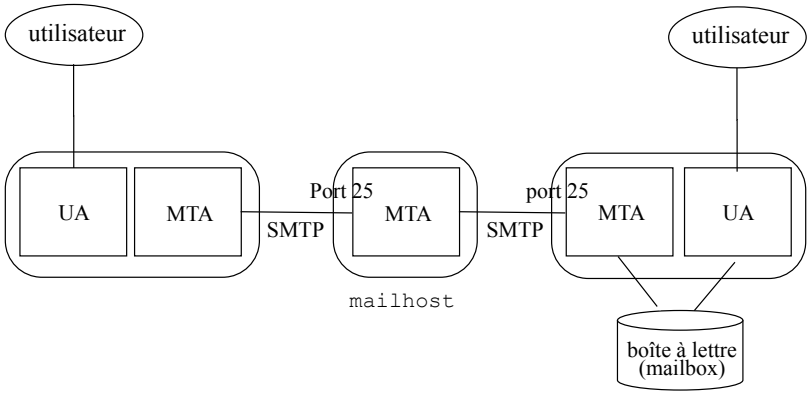
FTP - passive mode



SMTP
(Simple Mail Transfer Protocol)

- Transfert du courrier électronique
  - agent utilisateur *(User Agent - UA)*
    - » mail, Netscape, Eudora
  - agent de transfert *(Mail Transfer Agent - MTA)*
    - » sendmail, Netscape, Eudora
- Adresse - identifier un utilisateur
  - `user@domainName`
  - `domainName` est un nom de domaine (DNS)
    - » virtuel (MX)
    - » réel (A)

Principe



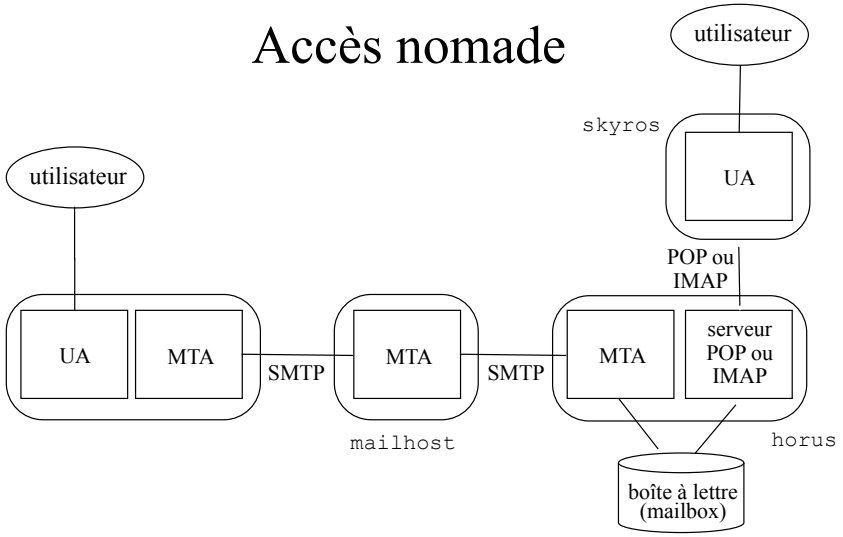
Commandes SMTP

```
HELO nom-de-site-client
MAIL From: batman@imag.fr
RCPT To:superman
DATA
ligne1
ligne2
ligne3
.
QUIT
VRFY adresse
EXPN liste
TURN
```

Enveloppe, en-tête, contenu

- Enveloppe
  - `MAIL From:`
  - `RCPT To:`
- En-tête
  - `Received:`
  - `Message-Id:`
  - `From:`
  - `Date:`
  - `Reply-To:`
  - `To:`
  - `Cc: copie`
  - `Bcc: copie secrète`
  - `Subject:`
- Contenu

Accès nomade



Accès nomade

- POP *(Post-Office Protocol)*
  - récupération de la boîte aux lettres distante
- IMAP *(Internet Mail Access Protocol)*
  - utilisateur décide quels messages récupérer
  - Gestion de la boîte à distance

Cas de pannes

- Si le MTA cible en panne
  - le MTA source stocke le message et retransmet après un intervalle (30 minutes)
  - essaie 3-4 jours

MIME

- *Multipurpose Internet Mail Extensions*
- Résolution de plusieurs problèmes du courrier
  - texte avec accents
  - texte en alphabets autres que latins
  - messages contenants d'autres média (images, audio)
  - utilisé aussi par WWW/HTTP (en-tête de la réponse)

Extensions d'en-tête

- `Mime-Version:`
- `Content-Description:`
- `Content-ID:`
- `Content-Transfer-Encoding:`
  - `ASCII` (7-bits),
  - `8-bits`,
  - `base64`
    - » 24 bits → 4 × 6 bits codé en ASCII
- `Content-Type:`
  - `type/sous-type`
  - description de la nature de données

Content-Type

```
text/     plain
text/     html
image     /gif
image     /jpeg
audio/basic
audio     /mpeg
video/mpeg
application/octet-stream
application/postcript
application/pdf
```


Content-Type

```
multipart/alternative; boundary=exemp-borne

pour mettre plusieurs styles de documents

Exemple:
--exemp-borne
content-type: text/plain
...
--exemp-borne
content-type: image/gif
...
```

Exemple MIME

From: Sherlock@homes.com
To: Pascal.Sicard@imag.fr
Subject : Enigme
MIME-Version :1.0
Content-Type :text/plain

Elementaire mon cher Watson !
.

Exemple MIME

From: sherlock@homes.com
To: Pascal.Sicard@imag.fr
Subject : Message contenant du html
MIME-Version :1.0
Content-Type :text/html

```
<html>
<head>
<title> exemple HTML </title
</head>

<h1> TITRE du document </h1>
<ul>
<li><font size="+2"><a href="repertoire/index.html">Nom associe au lien</a><font>
(commentaire sur le lien)</li>
<li><font size="+2"><a href="http://truc.com/index.html">NOM ASSOCIE AU
LIEN </a></font></li>
</ul>
</body>
</html>
```

.

Exemple Envoi faux message

[paros:~] sicard% **telnet imag.fr 25**
Trying 129.88.30.1...
Connected to imag.imag.fr.
Escape character is '^]'.
220 imag.imag.fr ESMTP ; Institut IMAG V1.2003 by LAC; Mon, 17 May 2004 11:12:07 +0200 (CEST)

500 5.5.1 Command unrecognized: ""
HELP
214-2.0.0 This is sendmail version 8.12.10
214-2.0.0 Topics:
214-2.0.0 HELO EHLO MAIL RCPT DATA
214-2.0.0 RSET NOOP QUIT HELP VRFY
214-2.0.0 EXPN VERB ETRN DSN AUTH
214-2.0.0 STARTTLS

Exemple Envoi faux message

MAIL FROM: sherlock@homes.com
250 2.1.0 sherlock@homes.com... Sender ok

RCPT TO: Pascal.Sicard@imag.fr
250 2.1.5 Pascal.Sicard@imag.fr... Recipient ok

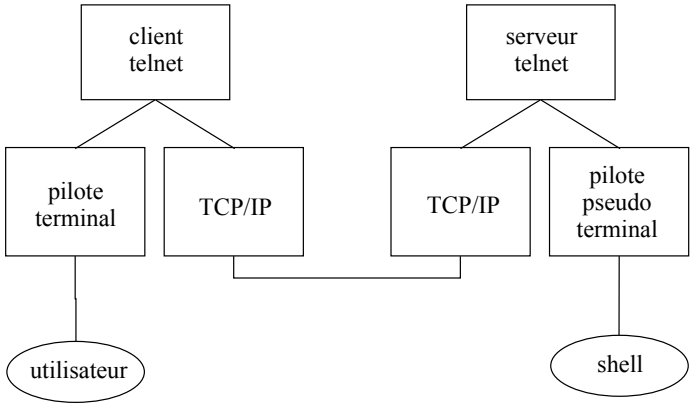
DATA
354 Enter mail, end with "." on a line by itself
From: Jacques.Dutronc@homes.com
To: Watson@imag.fr
Subject : Eureka
MIME-Version :1.0
Content-Type :text/plain

Elementaire mon cher Watson.
.
250 2.0.0 i4H9C7Gg020855 Message accepted for delivery
quit

Session de terminal à distance

- Travailler sur un système distant comme sur un système local
- Utilitaires
  - telnet
  - *R-commandes* d'Unix
    - » rlogin, rsh, rcp
  - ssh
- Principe
  - transmettre des caractères au shell distant et renvoyer des réponses

rlogin, telnet, ssh



telnet

Telnet définit :

- Le NVT (Network Virtual Terminal)
- Les règles de transfert des données
- La négociation des options

- Lors de la connexion, le client telnet et le serveur négocient le type de terminal qui sera utilisé et un certain nombre d'options
  - Type de terminaux :
    - Standards : VT100, VT220, Propriétaires : TN3270, TN5250
  - Exemples d'options : ASCII 7 bits ou 8 bits, nombre de lignes et colonnes
- Telnet permet aussi d'accéder à différent types de serveurs : mail, http (web)

SSH (Secure Shell)

- SSH: ensemble d'outils d'authentification et de chiffrements
- SSH permet de :
  - Accès sécurisé à un site distant : *ssh* remplace telnet, rlogin...
  - Copie de fichier sécurisé entre machine: *scp* au lieu de *rcp*
  - Transfert de fichier *sftp* au lieu de *ftp*
- Mais aussi permet de créer un *Tunnel* permettant le transfert de n'importe quelle application utilisant TCP

SSH

- SSH garantit:
  - L'authentification du serveur par le client par clés privée/ publique (RSA)
    - » Sur le serveur génération d'un couple de clés privé/ publique
    - » Soit le client connaît la clé publique du serveur (fichier *.ssh/Know_hosts*), soit le serveur lui envoie (message particulier de mise en garde de ssh)
    - » Pour l'authentification le client envoie une clé symétrique (appelé clé de session) et l'algorithme de chiffrement utilisé chiffrés à l'aide la clé publique du serveur
    - » Les données seront chiffrées à l'aide de cette clé symétrique
    - » Utilisation possible de certificats X509

SSH

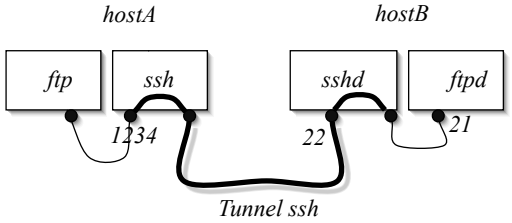
- L'authentification du client par le serveur
  - Soit par login et mot de passe classique
  - Soit par couple de clé privé/publique appartenant cette fois au client
    - » Le client génère une paire de clé privée/publique (commande *ssh-keygen*)
    - » La clé publique du client est rentrée sur le serveur (fichier *.ssh/know_hosts* contenant les noms DNS, les adresses IP , l'algo de chiffrement choisi et la clé publique*)*
    - » Le serveur génère un message chiffré à l'aide de la clé publique du client, le client doit savoir déchiffrer ce message grâce à sa clé privée
- Compression éventuelle des données

Exemple de tunnel SSH

– Sur hostA:

ssh -g -N -L 1234:hostB:21 hostB
ftp localhost 1234

On peut faire la même chose par exemple pour sécurisé un accès à un serveur WEB



Commande tunnel SSH

Résumé syntaxe:
-L définition de tunnel
-N : pas de prompt du ssh

ssh -g -N -L
port_entree_tunnel:machine_destination_tunnel:port_destination_tunnel

On peut définir plusieurs tunnels dans la même commande

Accès aux serveurs de Mail

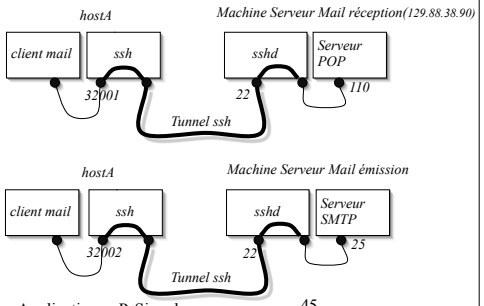
• Mise en place de deux tunnels : serveurs de d'émission (port 25) et de réception (port 110):

• *ssh -l sicard -N -L 32001:129.88.38.90:110 129.88.38.90 -L 32002:129.88.38.90:25 129.88.38.90*

• 129.88.38.90 est l'adresse de la machine sur laquelle tourne les serveurs de mail

• Il faut ensuite configurer le client mail :

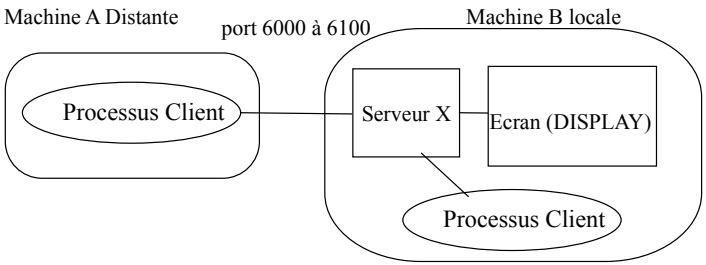
- • Réception 32001 localhost
- • Emission 32002 localhost



Serveur X_WINDOW (X11)

- Gestion de fenêtre à distance
  - Lancement d'un application sur une machine distante (Par exemple Netscape)
  - Serveur X sur la machine locale
  - Permet de renvoyer les fenêtres qui devrait s'afficher sur la machine distante sur l'écran de la locale
  - Connexion TCP
    - Chaque touche tapée génère un message de 32 octets

Principe X



Configuration X

- Sur le client
  - Définition de la machine sur laquelle les fenêtres s'afficheront (serveur X)
    - Redéfinition de la variable d'environnement DISPLAY qui spécifie la machine où se trouve l'écran d'affichage
    - setenv DISPLAY machineserveur:0.0
- Sur le serveur
  - Autorisation de recevoir des fenêtres X
  - xhost + machineclient
  - xhost + Toutes les machines autorisées
  - Connexion X à travers ssh: ssh -X

Divers

- who: liste des utilisateurs loggués; rwho idem sur les machines du réseau local
- finger
  - Information sur un utilisateur TCP port 79
  - Exemple: finger sicard@imag.fr
- whois
  - Interrogation d'une base de donnée (port 43)
    - Whois.ripe.net
    - whois.arin.net
    - whois.apnic.net
  - Nom DNS, administrateur