Association Lyonnaise pour le Développement de l'Informatique Libre

salle des Maison pour tous

L'auto-hébergement

Sébastien Dufromentel, Clément Février
ALDIL, Conférence « jeudi du libre »

7 février 2013

ubuntu-lyon

Internet : Réseau Libre Non Centré

Intervenants

Clément Février

- Doctorant en physique
- Président d'Ubuntu-Lyon et membre de l'ALDIL
- Serveur : tour, sous Ubuntu (desktop).

Sébastien « Elzen » Dufromentel

- Doctorant en informatique ; ancien prof d'école
- Fondateur du collectif « Internet : Réseau Libre Non-Centré »
- Serveur : portable, sous Debian.

Pourquoi l'auto-hébergement ?

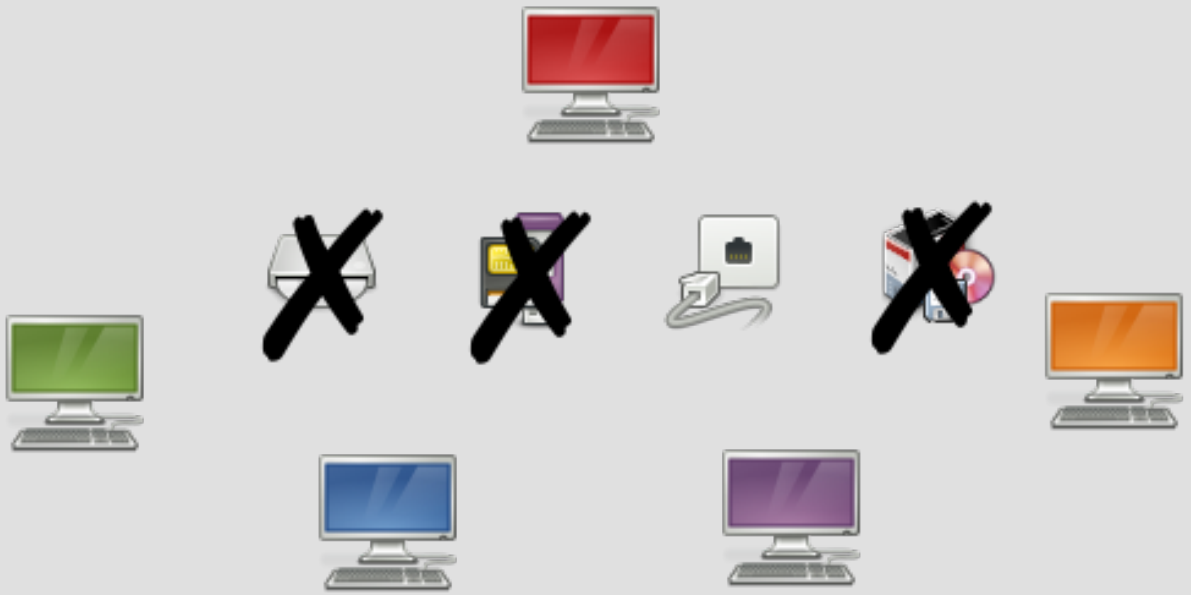
- Usagers d'*Internet*
- Militants du Logiciel Libre
- Plus pratique, tout simplement

Référence : Benjamin Bayart, « Internet Libre ou Minitel 2.0 »
(→ http ://www.fdn.fr/)
Voir aussi sur http ://fadrienn.irlnc.org

Plan

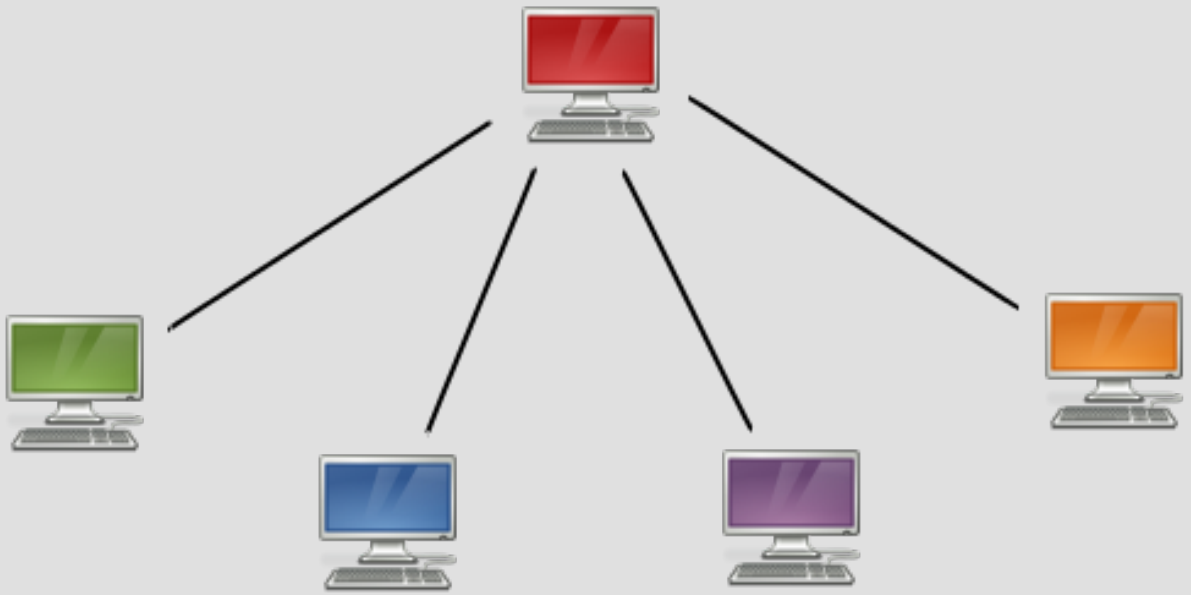
Mise en place d'un serveur Web

Échange rapide de fichiers ?



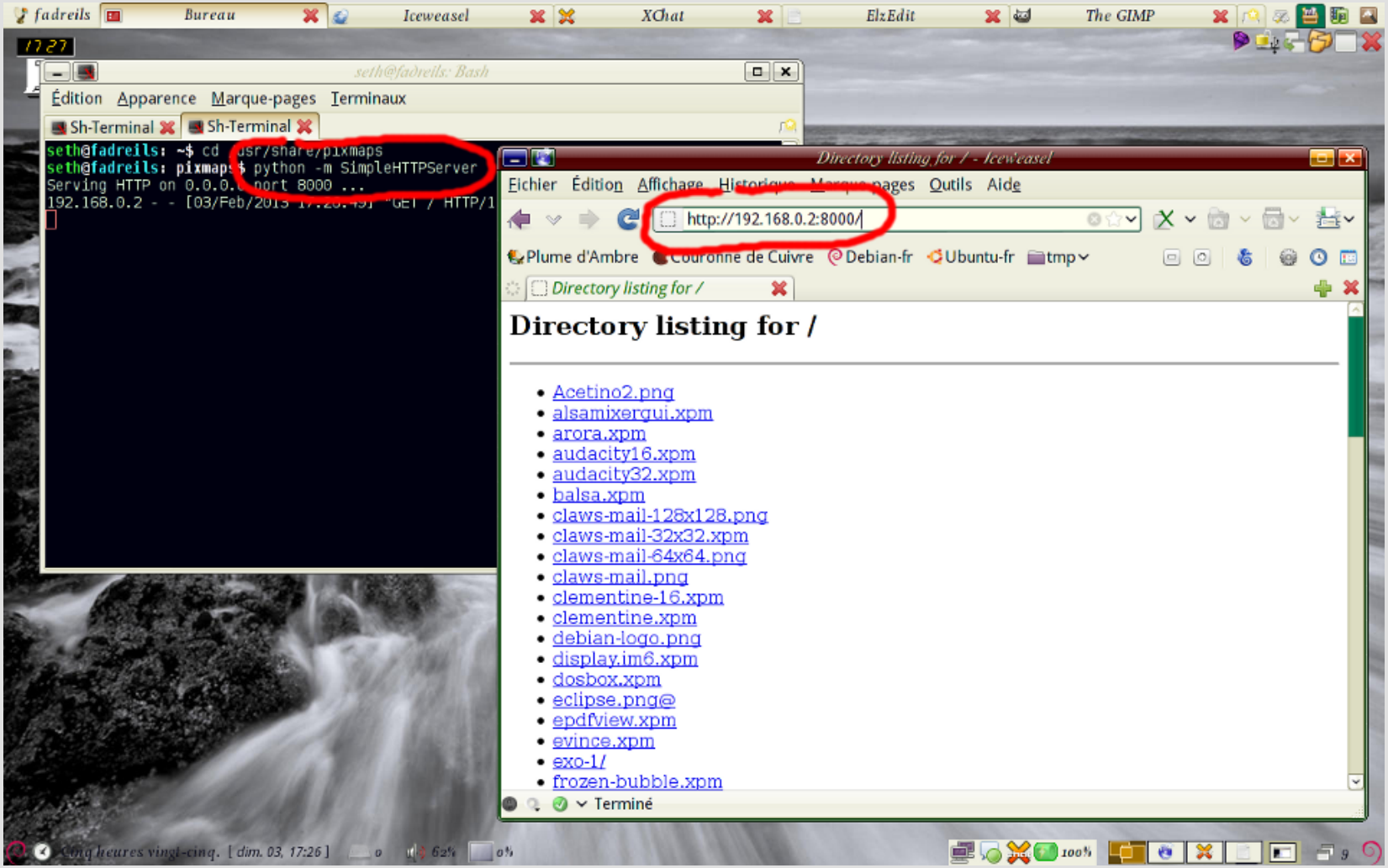
Comment transférer des fichiers par le réseau sans rien installer ?

Échange rapide de fichiers ?



Une commande : python -m SimpleHTTPServer

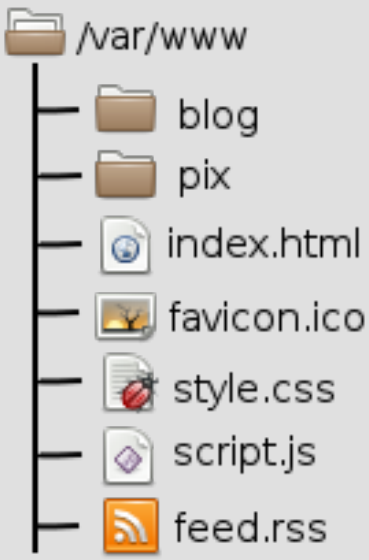
Échange rapide de fichiers ?



Un serveur en permanence

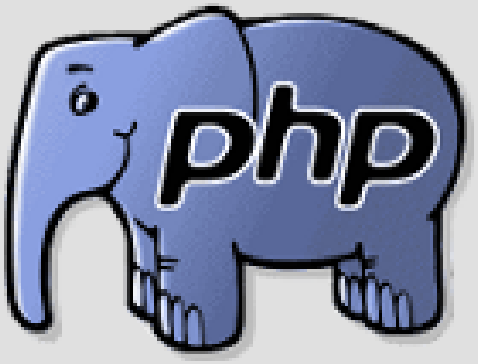
- Toujours en état de marche
- Utilisation du port par défaut
- Support TLS/Authentification
- CGI et réglages particuliers

Contenu de base d'un site



- racine du site
- page d'accueil du répertoire
- icône par défaut
- feuille de style CSS
- bibliothèque de scripts
- flux RSS

Aspects dynamiques : le CGI



- Traitements dynamiques
- Langages de programmation
- Support base de données
- Gestion de sessions

Aspects dynamiques : le SGBD

- Hors serveur Web !
- Stockage efficace

- Pas toujours nécessaire
- Utilisé par plusieurs applis

Services Web possibles

- **Blog/CMS**
  → *PluXML* (http ://www.pluxml.org/), *Joomla !*, *dotclear*. . .
- **Hébergement d'images**
  → *Pix*, utilisé sur http ://pix.toile-libre.org (archive en bas de page)
- **Échange de textes** (pastebin)
  → (https ://github.com/xanmanning/Knoxious-Open-Pastebin)
- **Documents collaboratifs**
  → *Etherpad* (voir sur http ://doc.ubuntu-fr.org/etherpad)
- **Hébergement de fichiers**
  → *Jyraphe* (http ://home.gna.org/jyraphe/)
- **Moteur de recherche**
  → *Seeks*, *YaCy* (installation depuis les dépôts - voir doc sur ubuntu-fr)
- **WebMail**
  → *RoundCube*

Authentification et sécurisation

Sessions

- Gérées par le CGI
- Intégré, pages de logins
- Utilisation de cookies
- Intégré aux applis

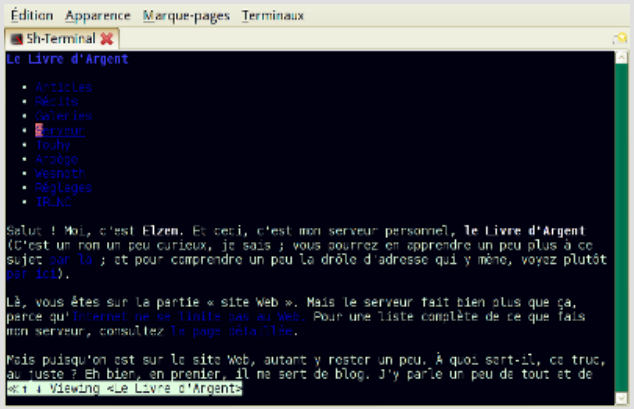
Authentification HTTP

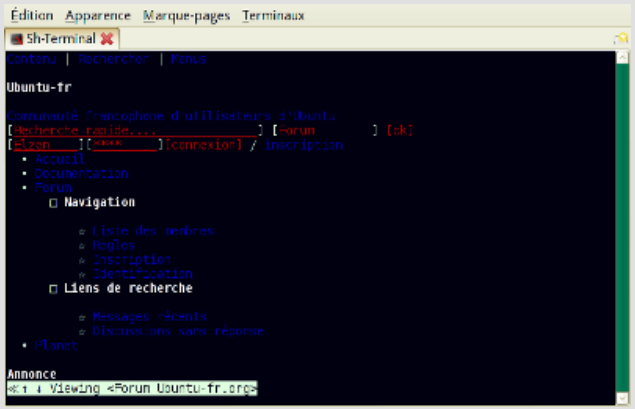
- Gérée par le serveur web
- Configuration requise
- Blocage efficace
- En fonction de l'adresse

Transmission de données sensibles : penser à sécuriser !
$\rightarrow$ Utilisation SSL/TLS (port 443, https)

Quelques éléments essentiels

- Respect des normes
  → Validateur du W3C : http ://validator.w3.org/
- Penser à l'accessibilité !
  → Images avec texte alternatif, JavaScript non-indispensable. . .





- Un moyen de vous contacter
  → Simple adresse mail ou page contenant un formulaire

Mise en place d'un serveur Mail

Les outils concernés

- Deux aspects : envoi/réception.
- Quatre concepts : MDA, MUA, MTA, SMPT.
  - MDA, Mail Delivery Agent.
  - MUA, Mail User Agent, *aka* Client de messagerie.
  - MTA, Mails Transfert Agent.
  - SMTP, Simple Mail Transfert Protocol : lien entre MTAs ou entre MTA et MUA.
- Enregistrements DNS spécifiques (MX).
- Port 25 ! mais submission 587.

Comptes mails

Plusieurs types de comptes possibles.

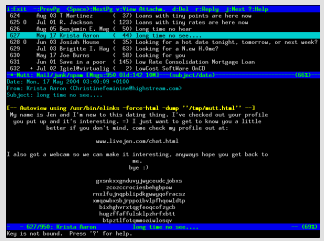
- Compte UNIX, fonctionne *out of the box.*
- Base de données, on trouve des tuto sur le web.
- LDAP, pratique et modulable, mais mise en place délicate.



Clients de messagerie (MUA)

- *Clients lourds*
  Logiciels installés en dur chez le client, usage classique

- *Clients « légers »*, ou *Webmails*
  - Client installé sur le serveur
  - Accessible depuis n'importe quel navigateur web.
  - Moins de fonctionnalités (filtres, chiffrement).

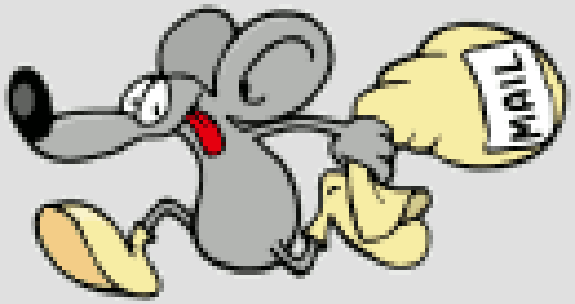


RoundCube (présent dans les dépôts)
http ://www.roundcube.net/

Services de délivrement (MDA)

- **Courier**
  - Le plus simple à installer et à configurer.
  - 4 paquets intéressants :
    - courier-pop
    - courier-pop-ssl
    - courier-imap
    - courier-imap-ssl
  - Un seul paramètre pour une configuration standard :
    le dossier où délivrer les messages, généralement ∼/Maildir.
- **Procmail**
  - Permet d'appliquer des filtres sur les messages sur le serveurs
    via un fichier de configuration dans le home (ne dépend plus du client).
  - La configuration de base, *ie* l'absence de configuration, supprime les mails.
  - Pas évident.
  - Mais performant.
- **Dovecot**.

Serveurs d'envoi (MTA)



POSTFIX SENDMAIL exim

Postfix

- Configuration de base très simple.
- Penser à prévoir quelques heures pour toute modification
  - ajout de certificats signés
  - port submission, relayhost (port 25 bloqué)
  - authentification
  - règles en fonction des domaines et plages d'ip
  - filtres anti-spam
  - anti-virus
  - ajout de nouveaux transports, ...
- Énormément de doc et tuto sur le web !

Gestion des alias

Création d'alias = Création d'adresse mail sans nouveau compte.
Pourquoi ?

- Pratique car évite de créer un autre compte système
  pour avoir une nouvelle adresse mail.
- Permet de changer le destinataire d'une adresse mails
  (exemple : predisent@aldil.org)

Comment ?

Il faut avoir les droits d'administrateur.
Dans le fichier */etc/aliases*

```
nouvelle_adresse : destinataire
postmaster : mon_compte
mon_adresse : toto@truc_machin.tld
$ sudo newaliases
```

Les messages à destinations de postmaster@ma_machine.tld
arriveront dans la boite de mail de mon_compte@ma_machine.tld

Mailing-lists

Mailman :

- **Prérequis**
  - Serveur mails (Postfix, Exim, Sendmail ou Qmail)
  - Serveur Web
- **Installation**
  Debian, Ubuntu et dérivées :
  $ sudo apt-get install mailman
- **Configuration et Utilisation**
  (en) https ://help.ubuntu.com/community/Mailman

Gestion des noms de domaines

Nom de domaine

Une machine est référencée sur le réseau par son adresse IP, exemple : 82.233.105.59
Pas évident à retenir.
Nom De Domaine : Lien entre IP et un nom explicite.

- **Architecture**
  - racine : .
  - Top Level Domain (TLD) : fr, org, com, de, ...
  - second level domain (SLD) : france, forumanalogue, irnlc, ...
  - Thrid Level Domain, généralement www.
- **Construction**
  .fr.forumanalogue.www
  .org.irlnc.fadrienn
- **second level domain**
  - Générés par les registrars, payants.
  - Certains ont des particularités, comme le .fr (AFNIC)
- **third and suivant** : géré par celui qui a acheté le Second Level Domain.

Bind9

Les registrars fournissent un serveur de nom de domaines (DNS).
DNS : **Bind9**.
Il faut une IP fixe ! ! !

Installation

$ sudo apt-get install bind9

Fonctionne out the box en *cache*.

Architecture

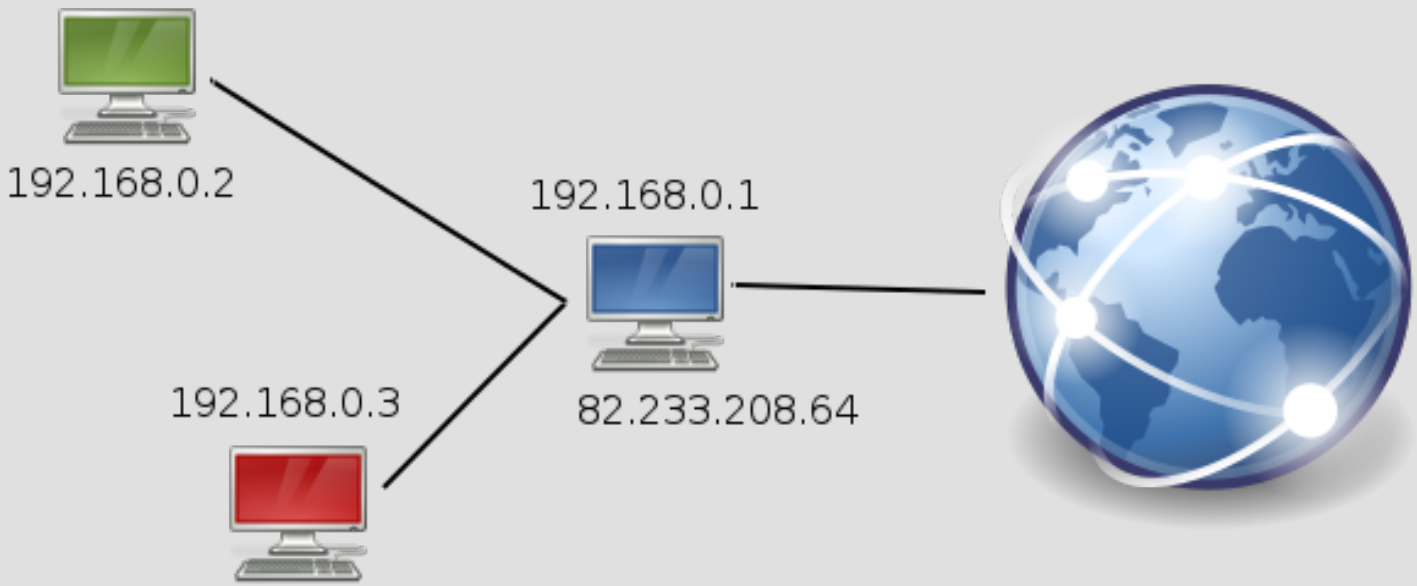
- Un fichier qui contient les serveurs racines, *db.root*
- Un fichier qui contient une zone, *db.irnlc, db.forumanalogue*
- Un fichier qui contient le reverse DNS, *db.192*

Exemples

@	3600	A	82.233.105.59
www	3600	A	82.233.105.59
univers.arciesis	3600	A	82.233.105.59
mail	3600	A	82.233.105.59
@	3600	MX	10 mail.forumanalogue.fr.
_xmpp-server._tcp	3600	SRV	5 0 5269 forumanalogue.fr.
_xmppconnect	28800	TXT	"_xmpp-client-xbosh=https ://www.forumanalo

Administration générale du serveur

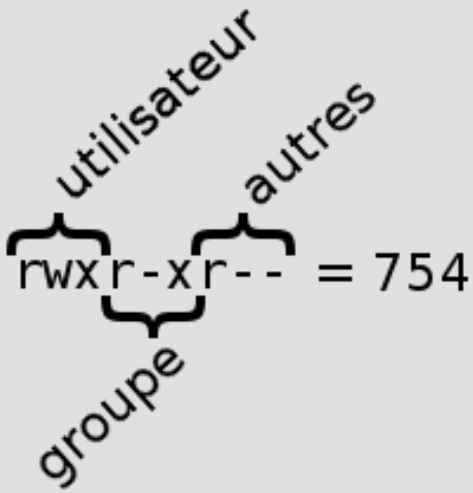
Réseau local (IPv4)



Interface unique avec l'extérieur
Routage de ports : pour que machine accessible depuis l'extérieur
Distinction réseau public/privé.

Droits d'accès : les bases

Fichiers : r = lecture ; w = écriture ; x = exécution
Répertoires : r = lecture ; w = écriture ; x = parcours

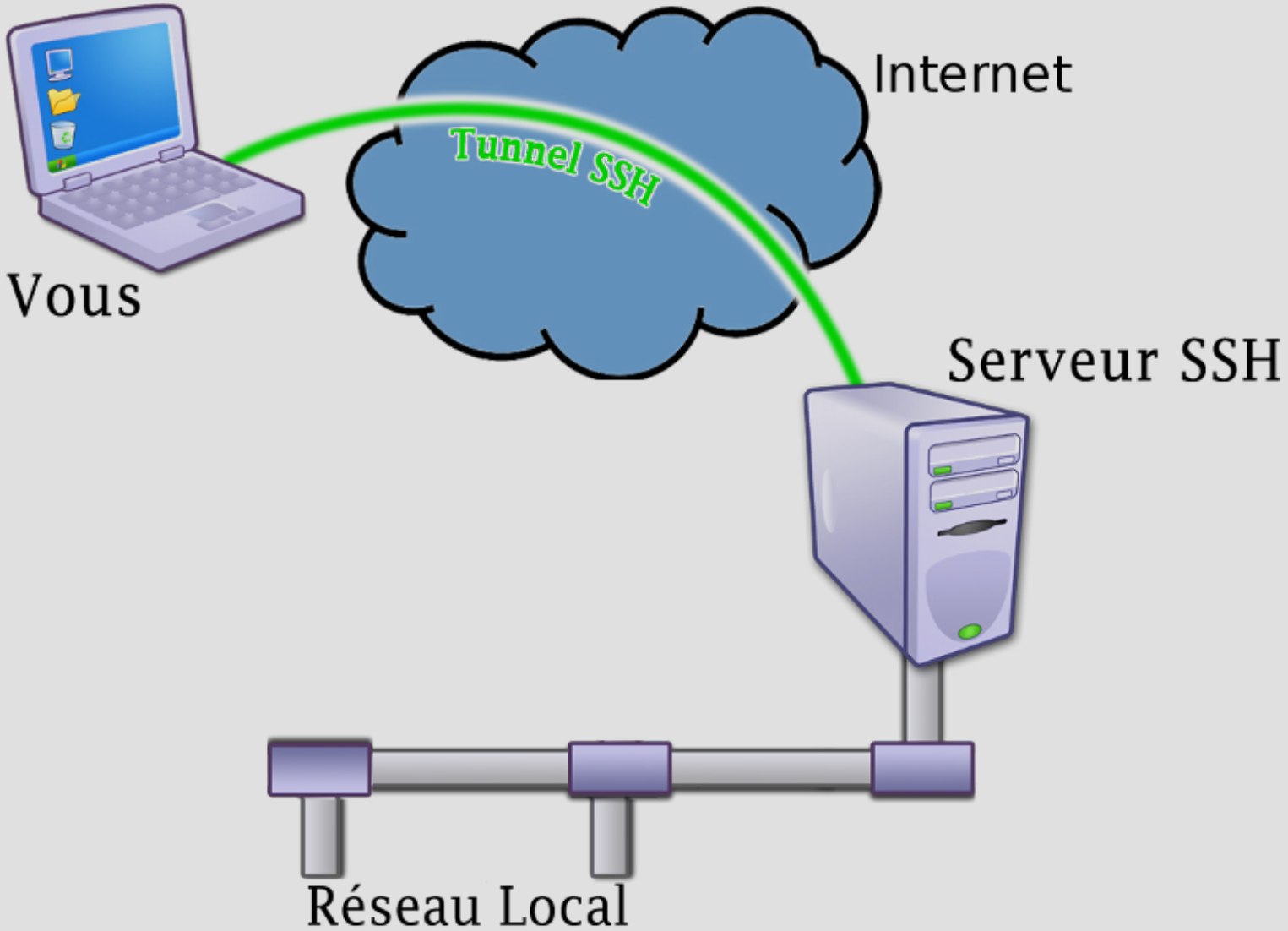


Droits d'accès : travail à plusieurs

- SGID : transmission du groupe sur les répertoires
- umask : masque de droits à *retirer* à la création

- Pour une gestion par utilisateur, utiliser les ACL : http ://lea-linux.org/documentations/Gestion_des_ACL

Accès à distance : SSh



Sauvegardes

- BDD, dump (mysql)
- Différentielle : rsync
- Incrémentielle : Copie en lien dur **cp -l**
- Machines virtuelles : xen

À chacun son propre script.

Quelques autres services possibles

Messagerie instantanée (IRC)

Messagerie instantanée (Jabber/XMPP)

- Décentralisé (serveur à serveur)
- *ejabberd*, *prosody*, ...
- Facile à installer
- Pas besoin en permanence
- Conférences possibles aussi
- Utilisé par Google Talk

http ://wiki.jabberfr.org

Serveur de jeux

Calcul scientifique (BOINC)

- Calcul partagé
- Selon disponibilité
- Utilité publique !

- Orbit, SETI, Planetquest, ...
- Climateprediction, Hydrogen, ...
- Rosetta, Malaria Control, SIMAP, ...

http ://boinc.berkeley.edu/

Dépôts versionnés

Bazaar

Mercurial

Git

Très utile pour les projets (seul ou à plusieurs)

Privilégier les outils décentrés (compatibilité. . .)

Pas plus compliqué à administrer qu'à utiliser

Échanges Pair-à-Pair (BitTorrent)

- Facilité de mise en place
- Rapidité de téléchargement
- Décharge les serveurs web

- Isos GNU/Linux ou *BSD
- Musique ou films libres
- Vidéos de conférences

http ://www.bittorrent.com/intl/fr/

Droit et sécurité

Bien choisir son FAI : « *the goods* »

FFDN ILLySE Internet Libre

Fournisseurs d'accès associatifs : le mieux

- Participation, neutralité, etc.

OVH.COM free

- IP Fixe, interface de configuration

Bien choisir son FAI : « *the bads* »

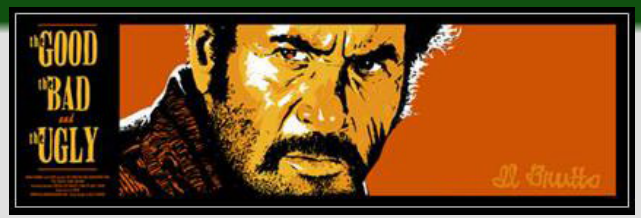
numericable
MONTEZ EN PUISSANCE

- Auto-hébergement interdit par le contrat !

DARTY BOX

- Impossibilité de rediriger les ports

Bien choisir son FAI : « *the uglies* »



Bouygues Telecom

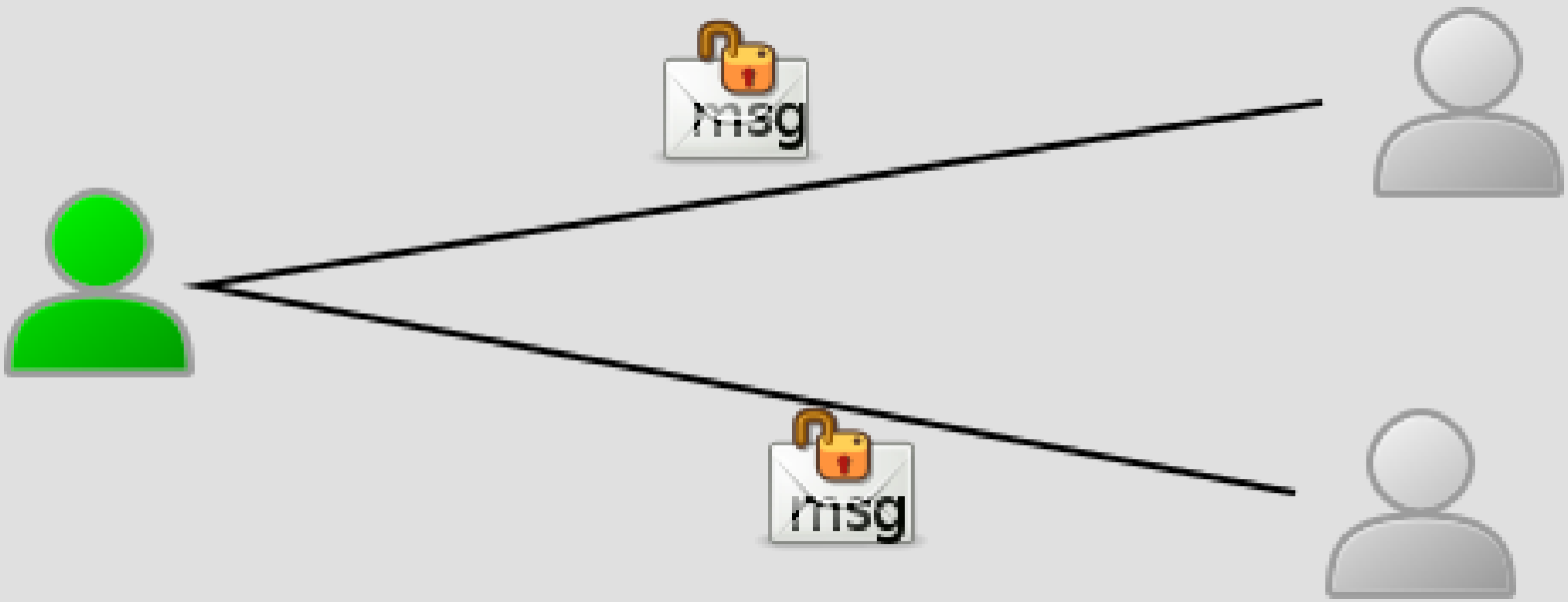
- « presque bon », mais IP pas tout-à-fait fixe

orange

orange

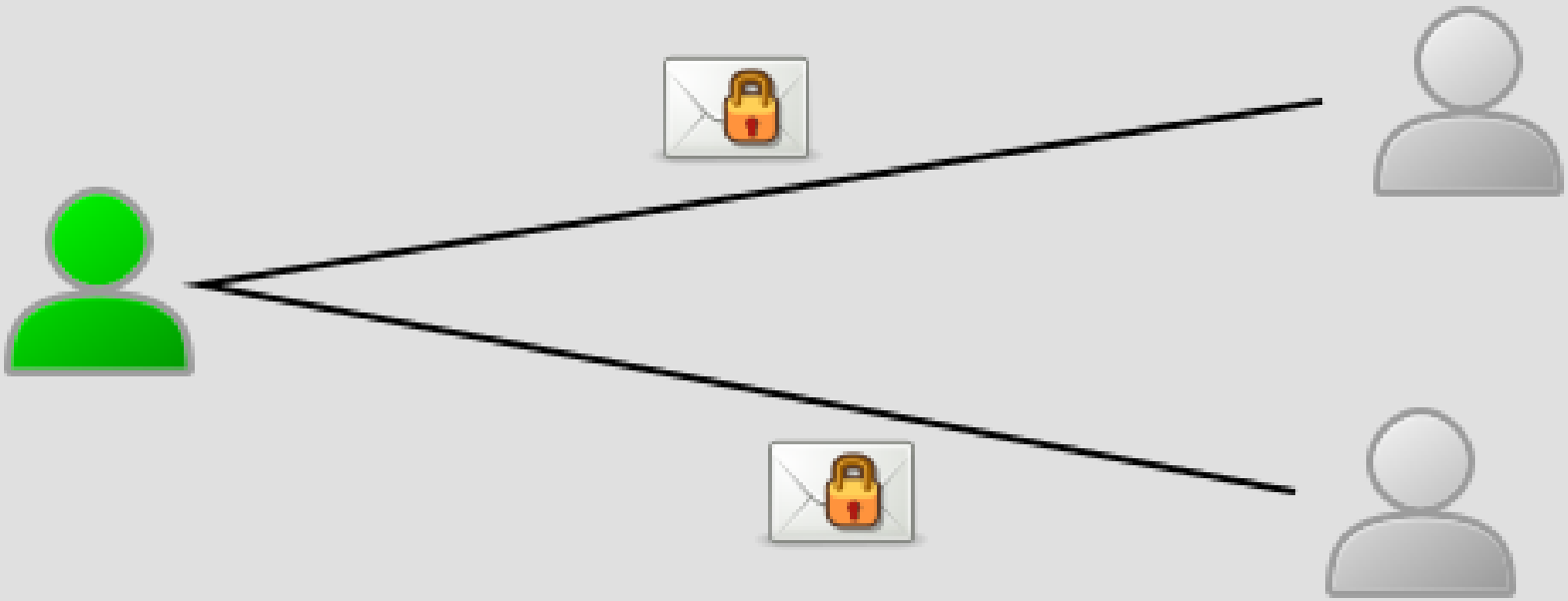
- Pas d'IP fixe, port 25 complètement bloqué

Le principe du SSL/TLS



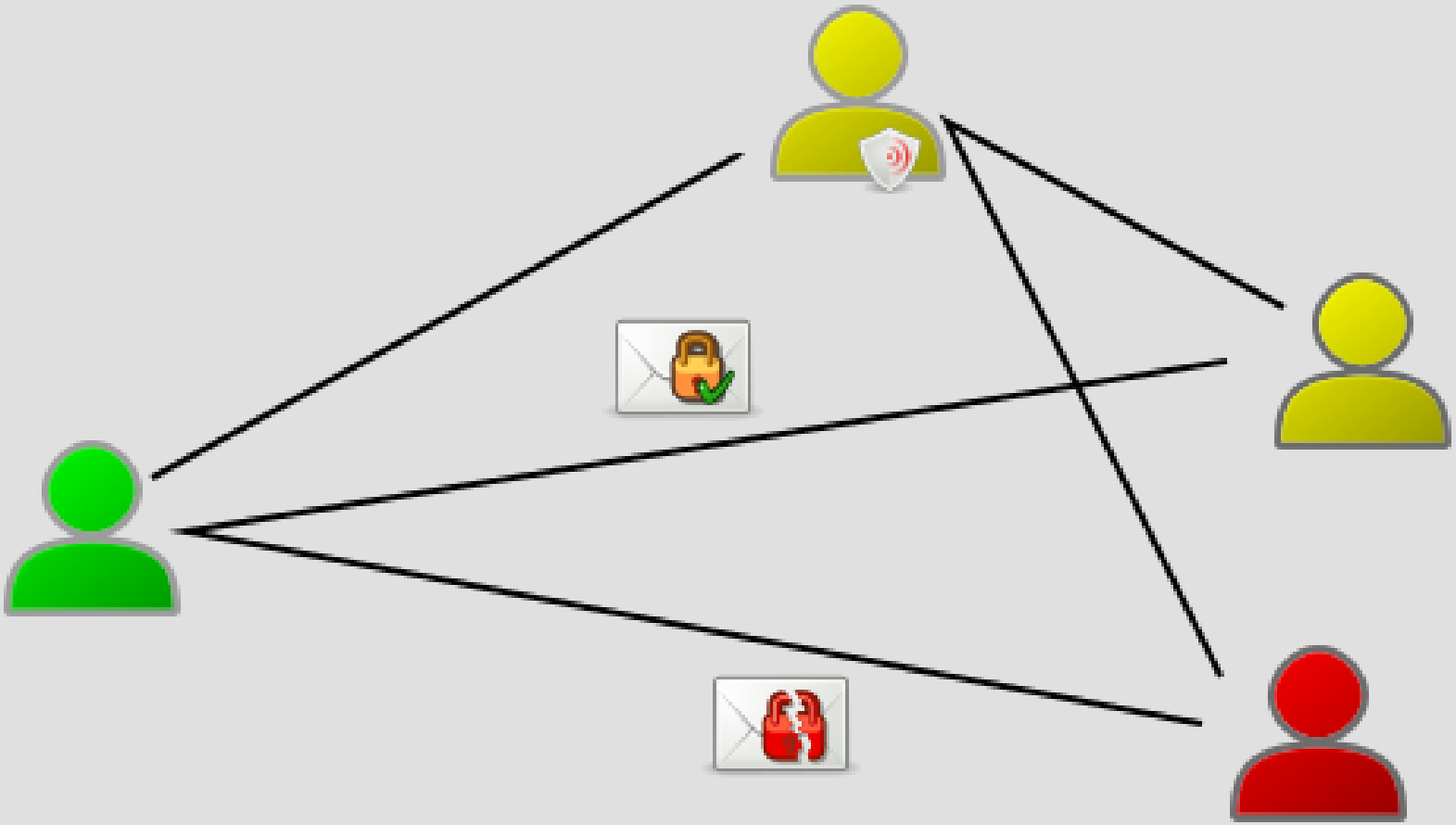
Échange standard en clair : n'importe qui peut écouter

Le principe du SSL/TLS



Échange chiffré : seul le destinataire peut lire

Le principe du SSL/TLS



Échange chiffré et authentifié : identité du destinataire confirmée

Autorités de certification

Antivirus : utile ?

GNU/Linux n'est pas concerné...

- Gestion des droits d'accès
- Mises à jour fréquentes
- Utilisation des dépôts

...mais Windows et MacOS, si !

- Sources extérieures
- Échanges de fichiers
- « porteur sain »

⇒ Un antivirus est utile sur un serveur !

Pour conclure. . .

- Beaucoup de pistes à creuser, selon ce qui **vous** intéresse.
- Encore besoin de bidouiller, prévoir du temps. . .
- Des communautés prêtes à vous aider
  (voir notamment http ://auto-hebergement.fr)
- Beaucoup de documentation disponible :
  - http ://doc.ubuntu-fr.org/serveur
  - http ://fadrienn.irlnc.org
  - . . .
- Devenir acteur d'Internet !