

DNS / NTP / SNMP

Administration Système et Réseaux, Sécurité

DNS / NTP / SNMP

Philippe Harrand

¹Département Informatique
Pôle Sciences et Technologies

²Direction Territoriale Sud Ouest
France Télécom

29 octobre 2007

DNS

NTP

SNMP

Pourquoi DNS ?

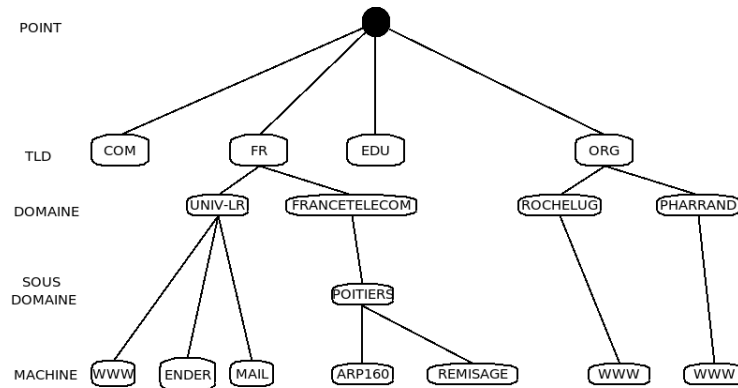
- ▶ machines accessibles par adresse IP
- ▶ Mémorisation adresses par humains
 - ▶ difficile pour IP V4
 - ▶ impossible pour IP V6
- ▶ Adressage IP "à plat"
- ▶ Pas de relation entité \Leftrightarrow adresse IP

Objectifs

- ▶ Créer une relation entité \Leftrightarrow adresse IP
- ▶ Unicité des noms de machines
- ▶ Hiérachisation des noms
- ▶ Gestion décentralisée, déléguée
- ▶ ...

Nommage des machines mis en oeuvre par l'ICANN
(Internet Corporation For Assigned Names and Numbers)

Organisation



Top Level Domain

Liste des TLD génériques		
TLD	Secteur d'activité	Organisme gestionnaire
.aero	Industrie aérienne	Dot Aero Council
.arpa	Address and Routing Parameter Area	Internet Assigned Numbers Authority
.biz	business (affaires)	Neulevel
.com	commerce, ouvert à tous	
.coop	coopération	
.edu	éducation (américaine)	EDUCAUSE
.eu	Europe	EURid
.gov	administration (américaine)	General Services Administration
.info	information	Afilias
.int	organisations internationales	Internet Assigned Numbers Authority
.mil	armée (américaine)	gouvernement (américain)
.museum	musées	Museum Domain Management Association (Muse-Doma)
.name	individus, par nom	The Global Name Registry, Ltd.
.net	organisation gérant le réseau, ouvert à tous	VeriSign
.org	organisation à but non commercial, ouvert à tous	Public Interest Registry (PIR)
.pro	professionnel	Registry Services Corporation
.jobs	Ressources humaines	société américaine Employ Media LLC (www.employmedia.com)
.travel	voyage	société américaine Tralliance Corporation (www.tralliance.info)

Domaines

- ▶ Pays reconnus par l'ONU *code iso 3166-1* ⇒ TLD
- ▶ Plus quelques particularités (îles) comme les Malouines (fk), la réunion (re)...
- ▶ Chaque TLD géré par un organisme, fr ⇒ AFNIC
 - ▶ Règles de nommage
 - ▶ Règles d'attribution
- ▶ Le propriétaire d'un domaine peut créer des sous-domaines
- ▶ L'arbre DNS est limité à 127 niveaux
- ▶ FQDN ≤ 255 caractères

Registrar

- ▶ Registrar ⇒ Organisme privé habilité à enregistrer des domaines
- ▶ Habilités par le « registre » concerné
- ▶ Peuvent avoir leurs serveurs de noms
- ▶ Peuvent déléguer l'enregistrement
- ▶ Maintiennent le *whois*

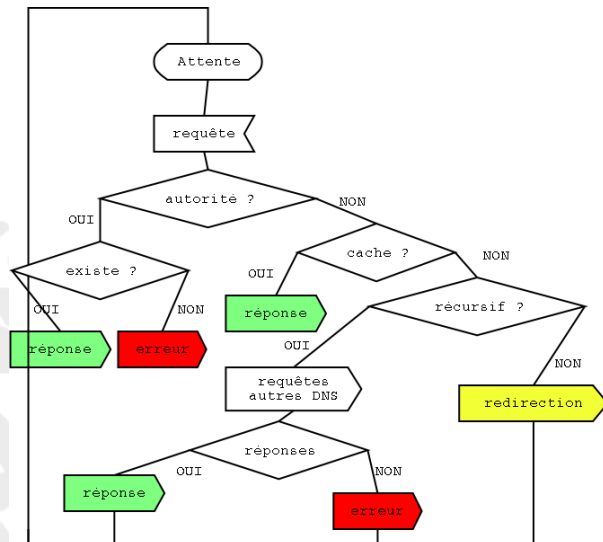
Organisation technique

- ▶ Organisation technique calquée sur organisation administrative
- ▶ 13 serveurs "point", « racine » ou « hint » entièrement redondants
- ▶ A chaque noeud correspond 1 paire de serveurs (au minimum)

Définitions

- ▶ Zone : sous-ensemble de l'espace de nommage d'Internet
- ▶ Autorité : serveur d'une zone (maître ou esclave)
- ▶ Récursivité : un serveur peut se renseigner s'il ne connaît pas la réponse
- ▶ Cache : un serveur peut conserver les données concernant les zones dont il n'est pas "autorité"
- ▶ Un serveur peut n'être qu'un cache
- ▶ Résolution directe : Nom \Rightarrow IP
- ▶ Résolution inverse : IP \Rightarrow Nom
- ▶ Trafic client \Leftrightarrow serveur : UDP 53
- ▶ Trafic serveur \Leftrightarrow serveur : TCP 53

Organisation technique



Bind

- ▶ **Berkeley Internet Name Domain** maintenu par l'**Internet Systems Consortium**
 - ▶ Serveur de noms : `named`
 - ▶ Une bibliothèque pour le résolveur (client)
 - ▶ Outils de vérification de fonctionnement : `host`, `dig`, ...
- ▶ Configuration dans `/etc/named.conf`
- ▶ **ATTENTION** au serveurs "chrootés"

named.conf

```
options {
    directory "/var/named";
};
zone "." {
    type hint;
    file "root.hints";
};
zone "0.0.127.in-addr.arpa" {
    type master;
    file "zone/127.0.0";
};
zone "land-5.com" {
    type master;
    file "zone/land-5.com";
    notify no;
};
zone "177.6.206.in-addr.arpa" {
    notify no;
    type master;
    file "zone/206.6.177";
};
```

Fichiers de zone

- ▶ Placer les fichiers de zone là où vous avez écrit qu'ils sont !
- ▶ Nommez-les comme vous l'avez écrit !
- ▶ **ATTENTION au serveurs "chrootés"**
- ▶ ATTENTION, pas de lignes vides mettez des commentaires « ; » ou « # »
- ▶ Constitués de **Ressource Records**
- ▶ Premier RR « SOA » « Start Of Authority ». indispensable et unique dans le fichier
- ▶ **FQDN** terminé par un point
- ▶ Sinon complété par le serveur...

Fichiers de zone directe

```
@ IN SOA ns.linux.bogus. hostmaster.linux.bogus (
    199802151 ; numéro de série (date+numéro)
    10800 ; refresh, seconds
    3600 ; retry, seconds
    604800 ; expire, seconds
    38400) ; minimum, seconds
;
NS ns ; Inet Address of name server
MX 10 mail.linux.bogus ; Primary Mail Exchanger
MX 20 mail.friend.bogus ; Secondary Mail Exchanger
;
localhost A 127.0.0.1
ns A 192.168.196.2
mail A 192.168.196.4
www CNAME mail
```

Fichiers de zone inverse

```
@ IN SOA ns.linux.bogus. hostmaster.linux.bogus (
    199802151 ; numéro de série (date+numéro)
    10800 ; refresh, seconds
    3600 ; retry, seconds
    604800 ; expire, seconds
    38400) ; minimum, seconds
;
NS ns.tp2.org.
1 PTR ns.tp2.org.
2 PTR happy17
```

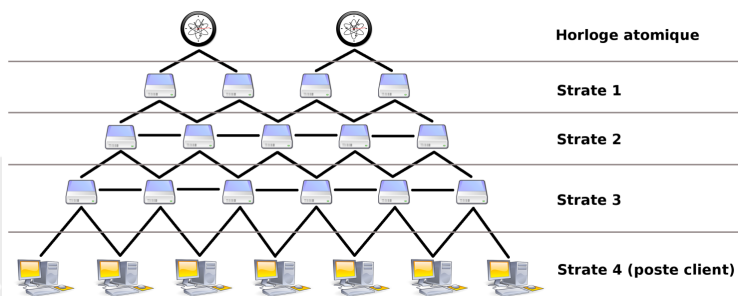
Maître / Esclave

- ▶ Un serveur DNS doit être doublé
- ▶ Serveur Maître : *type master* ;
- ▶ Serveur Esclave :
 - ▶ *type slave* ;
 - ▶ *masters {192.168.2.1 ;}* ;
 - ▶ Laisser les fichiers de zones se créer tout seuls
- ▶ Un serveur peut être maître sur certaines zones et esclave sur d'autres...
- ▶ le fichier de zone "hints" s'obtient avec *dig* sans paramètre

Network Time Protocol

- ▶ Nécessité d'être à l'heure
journalaux, BD journalisées réparties, ...
- ▶ Dérive des quartz
- ▶ NTP délivre le temps universel coordonné sur 64 bits
- ▶ Précision sur Internet $\cong 10$ ms

Organisation



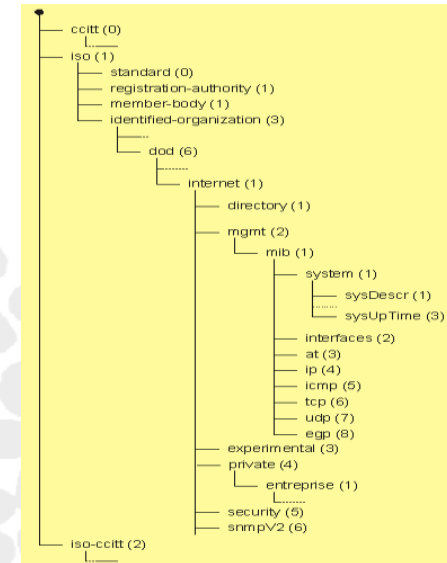
En pratique

- ▶ Un serveur NTP sur le LAN
 - ▶ Synchronisé sur un serveur de strate 3 ou plus
 - ▶ Distribue le temps pour le LAN
- ▶ Les clients utilisent *ntpdate* ou *ntpd -q*

Simple Network Management Protocol

- ▶ Gestion de matériels réseau hétérogènes
- ▶ Fonctionnement Client / ServeurS
- ▶ Serveurs : "agents SNMP"
 - ▶ Gèrent la **Management Information Base**
 - ▶ Répondent aux requêtes du Client
 - ▶ Emettent des **TRAP**
- ▶ Client : **Network Management Station**
 - ▶ Interroge les **MIB**
 - ▶ Modifie les **MIB**
 - ▶ Reçoit les **TRAP**

MIB



Utilisation

- ▶ agents SNMP plus ou moins finement paramétrables
- ▶ SNMP V1 majoritaire
- ▶ Mots de passe **EN CLAIR**
- ▶ SNMP V3 sécurisé
 - ▶ Utilisateurs authentifiés sur chaque agent par login/password MD5 ou SHA
 - ▶ Age des paquets vérifié
 - ▶ Données chiffrées
 - ▶ Vues ⇒ autorisations de lecture/écriture/trap
 - ▶ S de SNMP ?
- ▶ mais peu implémenté

Voir rapport de stage de Jean-Félix Marie (2006)