Le Service DNS
(Domain Name System)

M.BOUABID, 05-2015

Problématique

- Pour communiquer avec une machine, il faut connaître son adresse IP.
  - comment retenir plusieurs centaines de numéros IP ?
- Il faut un mécanisme qui associe un nom plus naturel à chaque machine
  - Solution : Domain Name System (DNS)

Nommage

- Problème : les adresses IP ne sont pas faciles a mémoriser
- Solution : faire une table de correspondance (ex : fichier /etc/hosts sous UNIX)

  193.54.113.3 L110PC3
  193.51.24.1   PCuser1
  193.51.25.192 quotaserver
  74.125.43.104 www
  195.83.118.1 ftp
  194.167.235.138 machine138
  194.167.235.139 machine139

Nommage

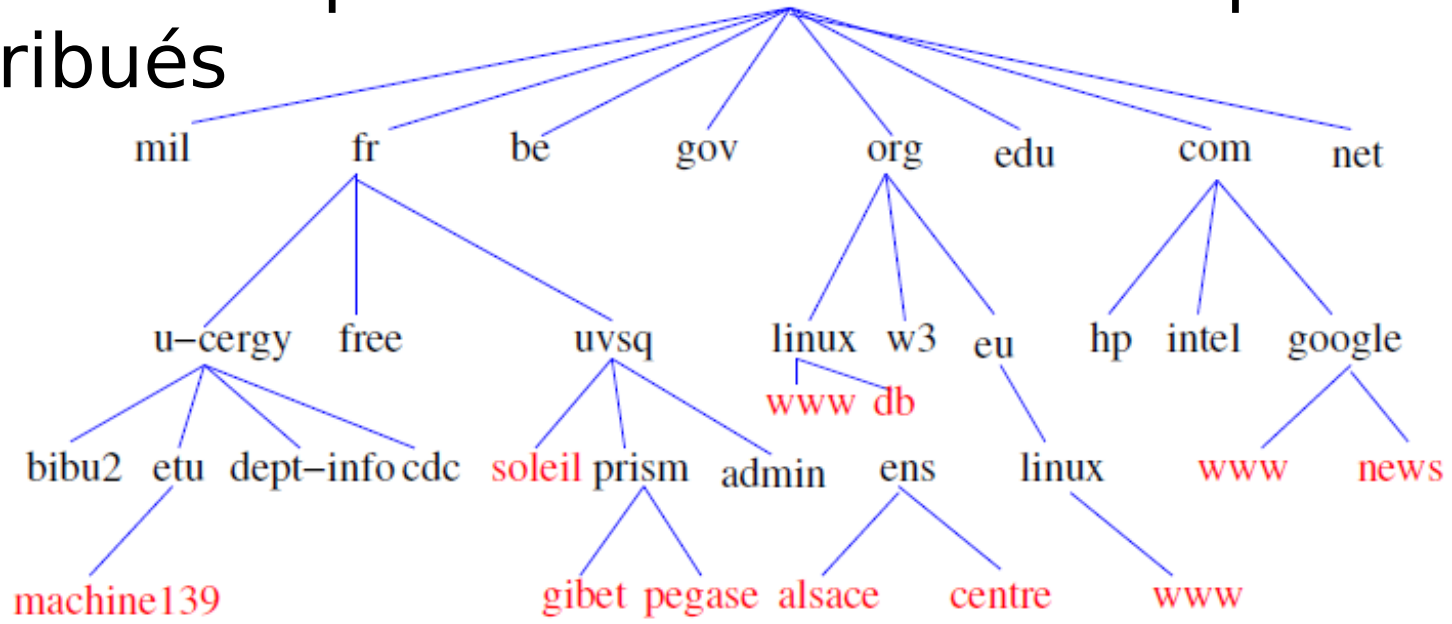
- Problème d'une table de correspondance sur plusieurs millions de machines :
  - Ambiguïté de nom inévitables
  - administration et maintenance de la table de correspondance impossible
    - une table de plusieurs millions d'entrée sur chacune des machines
    - lors d'un changement sur une table : reporter le changement sur les tables de toutes les machines !

Fonction

- Le protocole DNS permet d’associer un nom à une adresse IP et inversement
  - www.googel.com , 64.233.166.147
- Le nom complet d’une machine est décomposé en deux parties :
  - Son nom proprement dit :
    - **www**.isetmd.rnu.tn
    - **forum**.ubuntu-fr.org
    - **doc**.ubuntu-fr.org
    - **www**.google.com
  - Le domaine (ou zone) auquel la machine appartient :
    - www.**isetmd.rnu.tn**
    - forum.**ubuntu-fr.org**
    - doc.**ubuntu-fr.org**
    - www.**google.com**

Organisation

- Ambiguïté de noms
- Solution : espace de noms hiérarchique et distribués

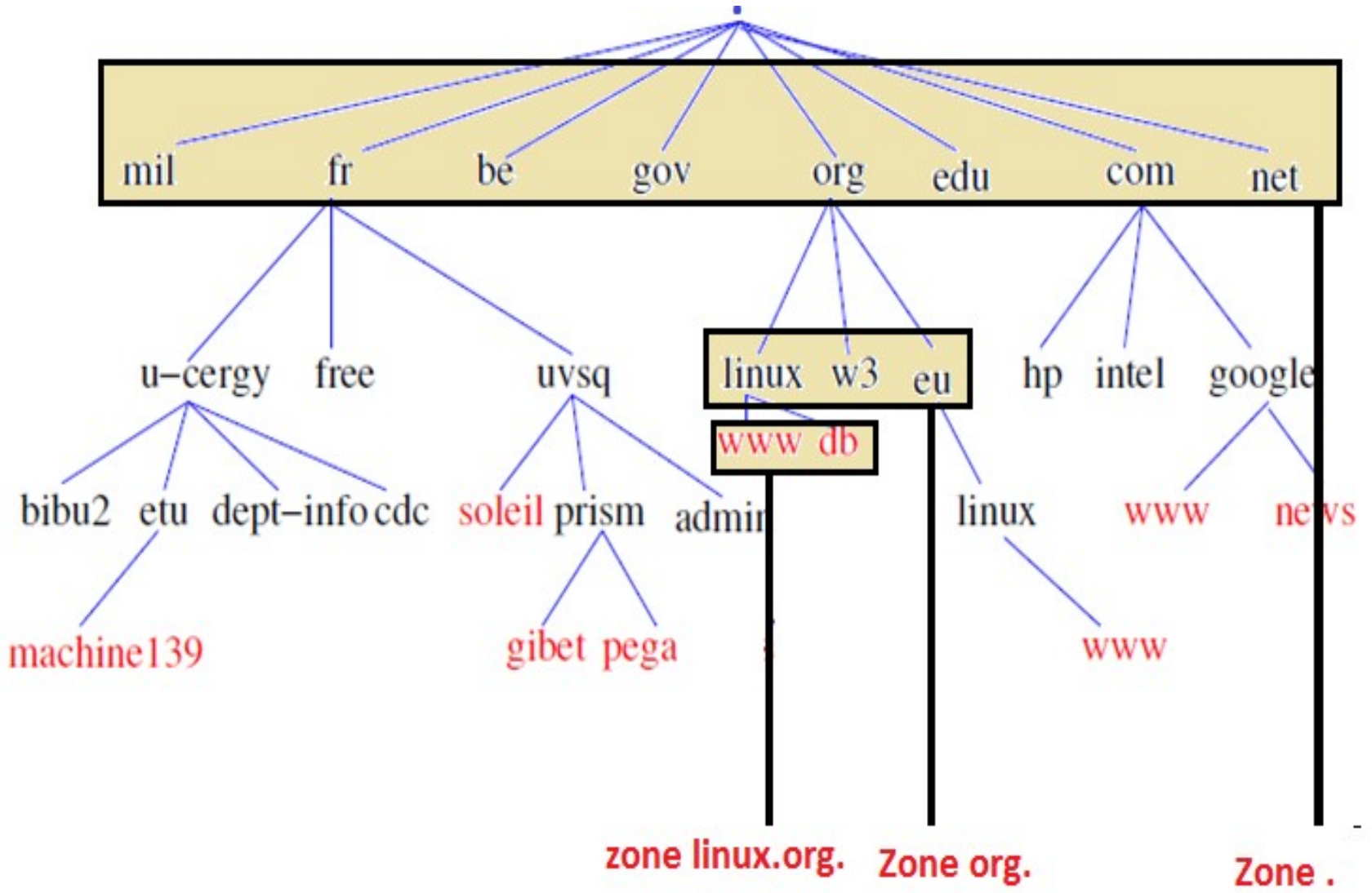


- www
- www.linux
- www.linux.org

Espace de noms hiérarchiques et distribués

- Avec le DNS, l'espace de noms est organisé en une hiérarchie au sommet de laquelle figure la racine et immédiatement en dessous les TLD (Top-Level Domain) ou domaines de niveau supérieurs.
- L'ICANN (Internet Corporation for Assigned Names and Numbers) a en charge la création des TLD et a crée notamment les TLD suivant
  - com : entreprises commerciales
  - edu : etablissements d'enseignement
  - org : organisations diverses
  - un TLD par code pays sur 2 lettres :
    - tn : tunisie
    - Fr :France

Zone


mil
fr
be
gov
org
edu
com
net
u-cergy
free
uvsq
linux
w3
eu
hp
intel
google
www
db
bibu2
etu
dept-info
cdc
soleil
prism
admin
linux
www
news
machine139
gibet
pega
www
zone linux.org.
Zone org.
Zone .

zone

- Une Zone représente une partie de l'espace de nom de Domaine, à des fins de gestion.
- Chaque zone est servie par plusieurs serveurs de noms
  - serveur primaire : source de la zone
  - Un ou plusieurs serveurs secondaires : copie (automatique) de la zone
- Un serveur peut servir plusieurs zones

Types des serveurs (1/2)

- Le serveur primaire
  - serveur d'autorité sur sa zone : il tient à jour un fichier appelé "fichier de zone", qui établit les correspondances entre les noms et les adresses IP des « hosts » de sa zone.
- Le serveur secondaire
  - obtient les données de zone via le réseau, à partir d'un serveur primaire. L'obtention des informations de zone via le réseau est appelé transfert de zone.
  - Il est capable de répondre aux requêtes de noms Ip (partage de charge), et de secourir le serveur primaire en cas de panne

Types de serveur (2/2)

- Le serveur cache
  - ne constitue sa base d'information qu'à partir des réponses des serveurs de noms. Il inscrit les correspondances nom / adresse IP dans un cache avec une durée de validité limitée (Ttl) ;
  - il n'a aucune autorité sur le domaine
  - il est capable de répondre aux requêtes des clients Dns
- Serveur racine
  - ils connaissent les serveurs de nom ayant autorité sur tous

  les domaines racine. Ils connaissent au moins les serveurs de noms pouvant résoudre le premier niveau (.com, .edu, .fr, etc.)
  - (actuellement il y en a 14), chaque serveur racine reçoit environ 100 000 requêtes par heure.

Résolution récursive/itérative

- Tout hôte doit connaitre au moins un serveur de noms
- Sur un hôte, le client DNS effectuant la résolution de noms est appelé solveur de noms
- Pour résoudre un nom (ou autre requête), le solveur s'adresse a son serveur de noms. Deux possibilités :
  - **résolution récursive** : s'il ne connait pas la réponse, il est amené à joindre d'autres serveurs de noms dans le but de trouver la réponse exacte.
  - **résolution itérative** : Lorsqu'un serveur reçoit une requête itérative, il renvoie la meilleure réponse qu'il peut donner sans contacter d'autres serveurs DNS (c'est-à-dire en consultant uniquement sa propre base de données).

Situation du DNS dans TCP/IP

- Le DNS est un protocole d'application
- DNS peut utiliser indépendamment UDP ou TCP
- Pour la quasi-totalité des requêtes DNS, c'est UDP qui est utilisé car il est rapide
- Mais certaines requêtes engendrent des réponses longues (supérieures a 512 octets) : dans ce cas, TCP est utilise (notamment pour les transferts de zone entre serveurs)
- **Les serveurs DNS ont un port réservé en UDP et TCP : le 53**

Implémentation

- L’implémentation la plus utilisée du protocole DNS est le serveur **bind9** (**B**erkeley **I**nternet **N**ame **D**omain)
  - Mais il en existe d’autres :
    - Microsoft DNS
    - PowerDNS
- Client DNS : les commandes suivantes
  - nslookup
  - dig
  - host

Configuration

- Le server DNS bind se configure à l’aide de plusieurs fichiers
- /etc/bind/named.conf
  - Fichier de configuration principal
    - Permet de définir les options globales
    - Permet de définir les zones (nom, fichier de zone, options spécifiques…)
    - Permet de définir les droits d’accès au serveur
  - Fichiers de base de données de zone
    - Correspondance IP , nom de machine ou nom de machine , IP
    - Paramètres de la zone (nom du serveur de nom, nom des serveurs de mail…)

Déclaration de zone

- La déclaration zone définit le comportement du serveur vis-à-vis d'une zone
  - zone <zone-name> <zone-class> {
    <zone-options>;
    [<zone-options>; ...]
    };
- Deux types de zones
  - Translation nom => IP
  - Translation IP => nom

Exemple

```
// Nom -> IP
zone "toto.org" {
        type master; // serveur maître
        file "toto.org"; // fichier de description de zone
};
// IP -> nom (reverse)
// réseau à l'envers suivie de in-addr.arpa
zone "139.168.192.in-addr.arpa" {
        type master;
        file "toto.org.rev"; // fichier de description de zone
};
// Serveur secondaire
Zone "tata.org" {
type slave; // serveur secondaire
file "tata.org";
masters { 134.206.10.18; }; // Adresse IP du serveur principal
};
```

Fichier de zone

- Comporte deux parties, les directives et les enregistrements :
- Les directives
  - $ORIGIN permet d'attacher un nom de domaine pour tout les noms qui n'en précisent pas (ex : $ORIGIN toto.org.)
  - $TTL valeur par défaut pour la durée de vie des information de la zone. cette valeur précise le temps qu'un autre serveur de nom peut mettre en cache les informations pour cette zone. Précisé en seconde (ex : $TTL 3600)
- Les enregistrements. Toutes les informations que peut donner un serveur sur une zone
  - translation nom => IP
  - translation IP =>nom
  - nom du serveur mail
  - nom du serveur DNS
  - Etc.
- Les commentaires sont fait à l'aide du caractère ;

Enregistrement SOA

- SOA : Start Of Authority. Donne les informations sur la zone

  @ IN SOA <ns-primaire> <mail-admin-domain> (
  <numero-de-serie>
  <time-to-refresh>
  <time-to-retry>
  <time-to-expire>
  <minimum-ttl>)
- **<ns-primaire>** : nom du serveur de nom maître pour la zone
- **<numero-de-serie>** : numéro de série du fichier de zone. DOIT être modifié à chaque modification du fichier
- **<time-to-refresh>** : Temps qu'un serveur esclave peut attendre avant de rafraîchir les informations sur la zone
- **<time-to-retry>** : Temps qu'un serveur esclave doit attendre avant de rafraîchir à nouveau la zone si un rafraîchissement précédent a échoué
- **<time-to-expire>** : Temps au bout duquel le serveur esclave se considère comme maître si le maître n'a pas répondu
- **<minimum-ttl>** : temps minimum de mise en cache des informations pour les autres serveurs de noms
- Toutes les durées sont exprimées en secondes mais on peut utiliser des abréviations pour les unités de temps (M, H, D...)

Autres enregistrements

- A : translation nom ⇒ IP
  - `<host>  IN  A  <IP>`
  - `toto  IN  A  192.168.139.128`
- CNAME : alias (donner plusieurs noms à une seule IP)
  - `<alias>  IN  CNAME  <nom-reel>`
  - `www  IN  CNAME  toto.toto.org.`
- MX : nom du serveur recevant les mails @domaine
  - `IN  MX  <priorité>  <nom>`
  - `IN  MX  10  mail.toto.org`
- NS : nom des serveurs faisant autorité pour la zone
  - `IN  NS  <nom>`
  - `IN  NS  ns1.toto.org.`
  - `IN  NS  ns2.toto.org.`
- PTR : translation IP ⇒ nom
  - `<derniers-digits-ip>  IN  PTR  <nom>`
  - `128  IN  PTR  toto.toto.org.`

Exemple : fichier de configuration de zone

```
$ORIGIN toto.org.
$TTL    604800
@       IN      SOA     toto.toto.org. root.toto.org. (
                                1           ; Serial
                               1D           ; Refresh
                               2H           ; Retry
                               7D           ; Expire
                               1H )         ; Cache TTL

        IN  NS      toto.toto.org.

toto    IN  A       192.168.139.128
tata    IN  CNAME   toto ; si $ORIGIN n'est pas précisé
                         ; il faut utiliser toto.toto.org.
```