Serveurs de noms (domain name servers)

- Rôle : **conversion** noms ↔ adresses IP
- Organisation hiérarchique des noms en **domaines**, s**ous-domaines** etc.
- Fonctionnement par **délégation** *:* un domaine est géré par un serveur, qui connaît les serveurs de ses **sous-domaines.**
- Serveurs **racines** : gèrent le sommet de la hiérarchie.
- Autre rôle : courrier.

Fonctionnement

- Un client adresse une **requête de résolution** à un serveur qu'il connaît
- Deux types de serveurs
  - **Récursif** : le serveur cherche la **réponse** et la transmet au client
  - **Itératif** : le serveur transmet l'adresse d'un **autre serveur** au client.

Exemple de résolution

- Un poste client du département informatique veut connaître l'adresse de **www.labri.fr.** Il interroge un serveur au département (**dns1.info.prive**)
- **dns1** interroge un serveur-racine, qui lui donne l'adresse d'un serveur pour le domaine **.fr**

(suite)

- **dns1** interroge ce serveur -> adresse du serveur pour **labri.fr**
- **dns1** interroge le dns de **.labri.fr** -> adresse de **www.labri.fr**
- **dns1** retourne l'adresse au client.

(suite)

- Dans cet exemple **dns1** agit comme **mandataire** *(proxy, relais)* pour les postes clients
- **Dns1** agit en mode **itératif**
- Il pourrait « faire suivre » la requête à un autre serveur (DNS principal de l'IUT ou du campus)

Protocoles

- Les échanges se font par **UDP** quand c'est possible, pour des raisons d'efficacité (requêtes courtes). TCP sinon.
- Port serveur **53**, port client **>1023**
- Serveur à serveur UDP : ports **53 à 53**
- Serveur à serveur TCP : **>1023 à 53**
- Remarque: les postes clients du département sont « non-routables » => passage **obligatoire** par un proxy interne

Utilisation de caches

- Pour des raisons d'efficacité, on réutilise les informations connues => Stockage dans des **caches**
- mais les informations peuvent changer
- Techniques employées :
  - Les infos ont une **durée de vie** déclarée
  - Les « fichiers » ont des **numéros de version**

Redondance

- Un serveur peut être temporairement injoignable => **plusieurs** serveurs « **autoritatifs** » pour un même domaine
- Serveur **primaire**, serveurs **secondaires**
- Le serveur primaire **notifie** les changements aux serveurs secondaires
- Organisation : de préférence sur des **réseaux éloignés**

DNS

Configuration des clients

Configuration client

- Fichier /etc/resolv.conf

```
search maison.net

nameserver 10.1.1.1
```

Serveur : déclaration de zone « maison.net »

```
@  IN  SOA wallace.maison.net. admin.maison.net. (
                 20050012       ; Serial
                   604800       ; Refresh
                    86400       ; Retry
                  2419200       ; Expire
                   604800 )     ; Negative Cache TTL
          IN       NS       wallace.maison.net.
          IN       MX       10 wallace

wallace   IN       A        10.1.1.254
          IN       MX       10 wallace

mcgraw    IN       A        10.1.1.253
          IN       MX       10 wallace

www       IN       CNAME    wallace
```

Principales déclarations

- SOA (*start of authority*) indique
  - Le serveur primaire
  - Le responsable (adresse avec « . » au lieu de « @ »)
  - Durée de vie des infos
- NS : déclaration de *serveur de nom*
- A : déclaration d'*adresse*
- MX : *échangeur de courrier*

Fichier de configuration « /etc/bind/named.conf »

```
...

zone "maison.net" {
        type master;
        file "/etc/bind/db.maison";
};
...
```

La résolution inverse

C'est
vraiment
important !

Résolution inverse : principes

- Astuce : les numéros IP sont « retournés » et mis dans le domaine spécial IN-ADDR.ARPA
- IP **1.2.3.4** => **4.3.2.1.IN-ADDR.ARPA**
- Ainsi 1.2.3.4 fait partie du domaine 1.2.3
- mêmes principes de délégation de sous-domaines, et mêmes mécanismes.
- **Mais** souvent les domaines ne correspondent pas à des « classes » d'adresses complètes...

Résolution inverse : principes

- Astuce : les numéros IP sont « retournés » et mis dans le domaine IN-ADDR.ARPA
- Ainsi IP **1.2.3.4**

  devient **4.3.2.1.IN-ADDR.ARPA**

  qui fait partie de 3.2.1.IN-ADDR.ARPA

  - Remarque : système de délégation basé sur les classes « naturelles » A,B,C.
  - Pose problème avec les réseaux « sans classe » (CIDR décrit par RFC 1519 de 1993).
  - Best current practice : RFC 2318

Déclaration de zone inverse (10.1.1.*)

```
@     IN    SOA   wallace.maison.net. admin.maison.net. (

                        4          ; Serial
                   604800          ; Refresh
                    86400          ; Retry
                  2419200          ; Expire
                   604800 )        ; Negative Cache TTL

          IN       NS       wallace.maison.net.

254       IN PTR   wallace.maison.net.
253       IN PTR   mcgraw.maison.net.
```

Déclaration zone « reverse »

- Extrait de « **/etc/bind/named.conf** »

```
zone "1.1.10.in-addr.arpa" {
        type master;
        file "/etc/bind/db.maison-rev";
};
```

DNS et courrier

- Le DNS est utilisé pour le courrier électronique
- La directive MX (***mail exchanger***) indique le serveur de courrier pour une machine/un domaine
- Possibilité de MX **multiples**

```
gromit   IN A   10.1.1.2
         IN MX 12 courrier.maison.net.
         IN MX 15 secours.maison.net.
```

Déclaration d'un sous-domaine

- Le sous-domaine peut être géré par le même serveur, ou par un autre, ou par plusieurs.
- Déclaration par NS

```
niche IN NS wallace.maison.net.
```

Travaux pratiques

- Configurer un serveur avec un domaine et quelques adresses IP. Logiciel **bind**, fichiers de config. dans **/etc/bind**
- Vérifier son fonctionnement (nslookup, dig), configurer un client, observer le trafic (tcpdump)
- Ajouter un sous-domaine avec quelques (=2) noms, géré par un autre serveur. Observer le trafic lors des interrogations.