

SERVEUR DE NOM DE DOMAINE

Les humains préférant les lettres aux chiffres, le service de nommage est un service qui permet d'associer les numéros INTERNET à des adresses logiques. Ainsi, 147.210.x.x identifie de manière unique le réseau u-bordeaux.fr. Le nom et le numéro doivent pouvoir être utilisés indifféremment. Le serveur de nom de domaine est attaché au port 53.

L'ensemble de ces informations est géré par un organisme basé à l'Université de Stanford, le NIC. Il est géré par trois organismes :

- Network Solutions Inc. pour l'enregistrement,
- AT&T pour les répertoires,
- General Atomics/CERFnet pour les informations.

Tout ceci se trouve sur rs.internic.net.

1 - PRINCIPE DU SERVICE DE NOMMAGE DNS

Ce service est basé sur une base de donnée répartie. L'intérêt est de s'assurer que toute l'information sera "disséminable" mais donnée seulement aux sites qui en ont besoin. Le DNS a un domaine racine qui est constitué d'un groupe de serveurs comme le montre l'arborescence figure 1.

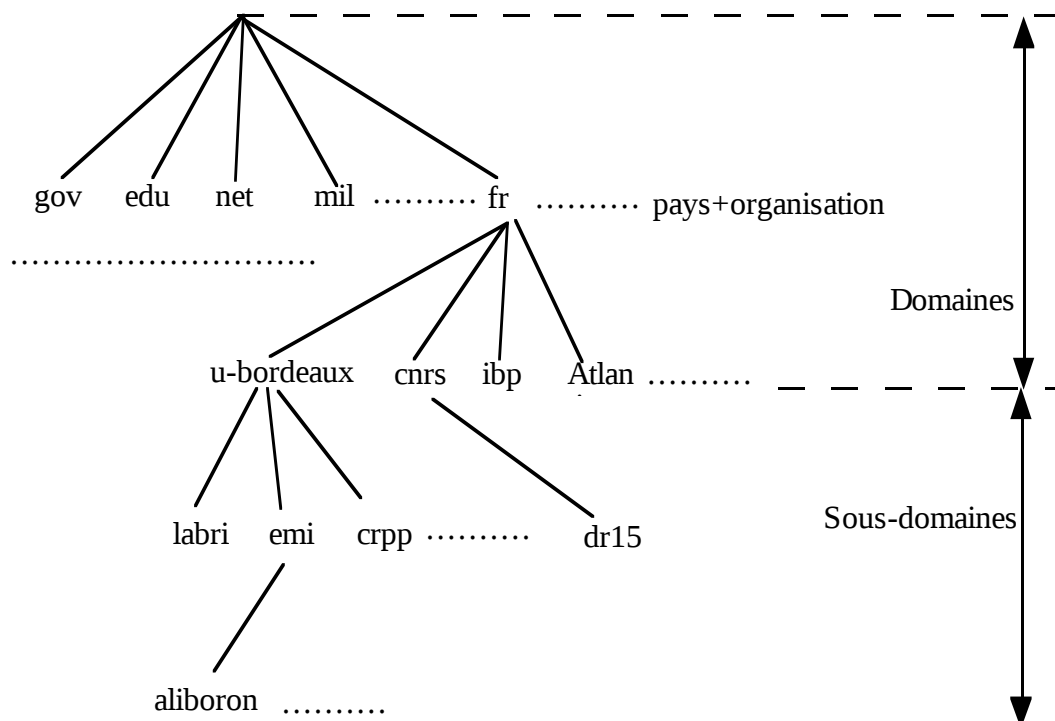


Figure 1. Les domaines INTERNET.

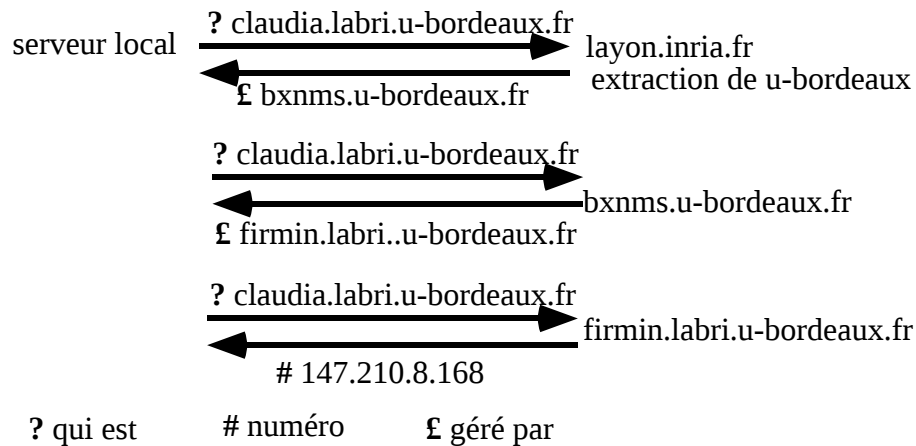


Figure 2. Diagramme temporel d'un appel à service

Chaque domaine racine a en charge des domaines qui ont eux mêmes en charge des sous-domaines. On dit qu'un domaine reçoit la délégation d'un autre lorsqu'il reçoit l'autorisation de le gérer.

Par exemple, l'INRIA a délégation pour gérer le domaine `.fr`, REAUMUR a délégation pour gérer `u-bordeaux.fr`. Cela signifie par exemple pour REAUMUR que le domaine `u-bordeaux.fr` a été enregistré auprès du NIC et que tous les sous-domaines sont attribués par REAUMUR.

Une FQDN (Fully Qualified Domain Name) est une adresse dont tous les champs sont précisés. Le fonctionnement du DNS est de type client-serveur. La partie client s'appelle le *resolver*, c'est une bibliothèque. La partie serveur s'appelle le *name server*, c'est un démon. On trouve en figure 2 son fonctionnement à partir d'un serveur local français. L'hypothèse de travail dans cet exemple est que ce serveur ne sait pas comment contacter `claudia.labri.u-bordeaux.fr` et ne se trouve pas sur le domaine `u-bordeaux.fr`.

Il existe trois types de name server :

- primaire, possède les tables à jour d'un domaine
- secondaire, possède les tables à jours provenant d'un autre serveur,
- cache, possède des tables construites à partir des informations traitées.

3 - DEMARRAGE D'UN DNS

Pour démarrer un domaine, il faut disposer au moins d'une classe C puis obtenir l'enregistrement et la délégation pour ce nom de domaine. On doit également demander la délégation pour le domaine associé `in-addr.arpa` qui est constitué par le numéro de la classe dans l'ordre inverse suivi de la mention `in-addr.arpa`. Ceci sert à constituer une arborescence de nom de numéro INTERNET conforme à l'organisation du nom de domaine afin de faciliter le travail d'archivage du DNS.

Exemple. Pour le labri le domaine est géré par `firmin.labri.u-bordeaux.fr` d'adresse `147.210.8`. La hiérarchie des numéros est l'inverse de celle des noms. On crée donc un domaine dit *reverse* `8.210.147.in-addr.arpa` qui reflète la hiérarchie des noms.

Il faut toujours deux serveurs pour un domaine si possible non situés sur le même câble physique. Le site Aquarel situé au Conseil Régional fournit par exemple un DNS secondaire pour tous les sites Aquarel qui le souhaitent.

On peut demander l'attribution d'un numéro AS (Autonomous System). Ceci peut permettre d'interconnecter des gros réseaux.

Sur le site lui-même, il faut penser à un plan d'adressage pour le domaine concerné. En effet la plupart des opérations sur les routeurs peuvent s'obtenir à partir de masques. Un plan d'adressage bien fait permettra de:

- simplifier l'administration,
- reconnaître une organisation,
- séparer le trafic,
- isoler facilement les problèmes de routages.

4 - CONFIGURATION DU RESOLVER

Le resolver est une bibliothèque qui utilise essentiellement le fichier `/etc/resolv.conf`. Il doit contenir

- l'adresse des serveurs de nom,
- le nom du domaine servi auquel appartient la machine.

Exemple. Pour le domaine emi ce fichier contient

```
domain emi.u-bordeaux.fr
nameserver 147.210.13.1      edwood.emi
```

5 - CONFIGURATION DU DEMON NAMED

Ce démon utilise cinq fichiers de configuration habituellement situés dans le répertoire `/var`. Ces fichiers sont souvent regroupés dans un répertoire, par exemple dans (cas Aquarel) ou `named` (cas emi). Il existe deux types de fichiers utilisant une syntaxe propre :

- Groupe 1
 - `named.boot` : paramètres généraux du serveur local
- Groupe 2
 - `named.ca` : pointeurs vers les domaines racine
 - `named.local` : résolution des adresses locales au serveur
 - `named.hosts` : association nom -> numéro IP
 - `named.rev` : association numéro IP -> nom

Les fichiers du groupe 1 permettent de paramétrer les adresses des fichiers utilisés par le DNS ainsi que son comportement. Les fichiers du groupe 2 contiennent la description des domaines et des hôtes. Chaque ligne est destinée à alimenter une base de donnée. On les appelle des enregistrements ressources (ici le nom utilisé sera enregistrement).

6 - ENREGISTREMENTS DU NAMED.BOOT

Ces types d'enregistrements sont au nombre de six. Il n'y a pas d'ordonancement.

directory : permet de fixer un chemin absolu, les autres chemins intervenant après cet enregistrement seront relatifs à ce point.

exemple : directory /var/named

primary : permet d'enoncer les domaines dont ce serveur est le serveur primaire et pour chaque domaine le fichier de configuration associé. Le serveur est toujours serveur primaire des domaines reverse associés aux numéros qu'il gère.

exemple : le classe C 193.51.11 est délégué à aquarel

primary	aquarel.fr	primary/aquarel
primary	11.51.193.in-addr.arpa	primary/rev.193.51.11

secondary : permet de déclarer les domaines dont ce serveur est le serveur secondaire (de secours). On déclare dans ce cas le numéro du serveur primaire du domaine à gérer et pour chaque numéro le fichier de configuration associé. Ce fichier sera alimenté par une demande au serveur primaire du domaine concerné. Le serveur est toujours serveur secondaire des domaines reverse associés aux numéros qu'il gère comme serveur secondaire.

exemple : le classe C 193.55.219 est délégué à ESC-Pau

secondary	esc-pau.fr	193.55.219.1
		secondary/esc-pau.fr
secondary	219.55.193.in-addr.arpa	193.55.219.1
		secondary/rev.193.55.219

cache : permet de définir un fichier qui sera alimenté par des couples (nom-de-domaine, numéro) obtenus à partir du trafic généré par le DNS.

exemple :

cache	.	root.cache
-------	---	------------

forwarders : permet de donner l'adresse d'un serveur qui mettra en cache systématiquement toutes les requêtes insatisfaites localement. Ce serveur sera systématiquement interrogé par le serveur en cas de non-résolution locale et c'est lui qui continuera l'exploration. Ce système prend tout son intérêt sur un gros réseau lorsqu'il y a plusieurs serveurs primaires. Cela permet de décharger le trafic DNS sur un seul système et de cumuler les caches de tous les serveurs primaires.

exemple :

```
forwarders          193.51.11.1
```

slave : est une option associée à *forwarders* qui précise que le serveur local ne doit pas continuer la recherche lui-même s'il n'a pas de réponse. Il est alors complètement dépendant du *forwarders*.

exemple :

```
forwarders          193.51.11.1
slave
```

7 - ENREGISTREMENTS DES AUTRES FICHIERS

Il n'existe que huit types d'enregistrements. L'un d'eux SOA est obligatoire en tête de fichier. Nous ne traitons ici que les cinq plus importants. Les autres transportent du texte ou ne sont pas utilisés.

SOA : C'est le premier enregistrement de chaque fichier (Start Of Authority). Il permet de préciser le nom de l'hôte sur lequel a été créé le fichier, l'adresse de la personne qui maintient ce fichier, une liste de nombre précisant le numéro de version, une liste de temps permettant d'indiquer la durée de validité des informations pour les serveurs secondaires.

exemple :

```
aquarel.fr. IN SOA dufy.aquarel.fr. rd.aquarel.fr. (94012615
                                     21600
                                     3600
                                     3600000
                                     172800)
```

NS : permet d'indiquer le serveur de nom pour un domaine donné. Il n'y a pas bijection entre serveur et nom de domaine. Un serveur peut servir plusieurs domaines, un domaine peut avoir plusieurs serveurs.

exemple :

aquarel.fr.	IN NS	dufy.aquarel.fr.
	IN NS	layon.inria.fr.

A : permet d'associer un hôte donné à un numéro IP. Ce type d'enregistrement est réservé aux fichiers de type named.local et named.hosts .

exemple :

dufy.aquarel.fr.	IN A	193.51.11.1
------------------	------	-------------

PTR : permet d'associer un numéro IP donné à un hôte. Ce type d'enregistrement est réservé aux fichiers de type named.rev.

exemple :

193.51.11.1	IN PTR	dufy.aquarel.fr.
-------------	--------	------------------

CNAME : permet de définir des alias.

exemple :

www	IN CNAME	dufy.aquarel.fr
-----	----------	-----------------