Table des matières

[Résolution locale des noms 2](#_Toc59460694)

[1ère étape : Choisir le service de résolution de noms 2](#_Toc59460695)

[2ème étape: Configurer le(s) services(s) choisi(s) 2](#_Toc59460696)

[Commandes utiles 2](#_Toc59460697)

[But du DNS 3](#_Toc59460698)

[Plan du DNS 3](#_Toc59460699)

[Système de nommage 3](#_Toc59460700)

[Domaine 3](#_Toc59460701)

[Zone 4](#_Toc59460702)

[Autorité 4](#_Toc59460703)

[Délégation 5](#_Toc59460704)

[Serveurs Racine 6](#_Toc59460705)

[Redondance 7](#_Toc59460706)

[Résolution et résolution inverse 7](#_Toc59460707)

[Parcours d'une requête 8](#_Toc59460708)

[Debug DNS 9](#_Toc59460709)

[dig (Domain Information Groper) 9](#_Toc59460710)

[nslookup 9](#_Toc59460711)

[Serveur de cache 10](#_Toc59460712)

[Explication 10](#_Toc59460713)

[Avantages et inconvénients 10](#_Toc59460714)

[Configuration minimale 11](#_Toc59460715)

[Serveur autoritaire 11](#_Toc59460716)

[Bind 12](#_Toc59460717)

# Résolution locale des noms

Pour établir une correspondance compréhensible par les systèmes entre des noms de machines et leur adresse.  
La correspondance peut être connue localement (statiquement) ou être disponible sur le réseau.

Résolution locale (statique) => /etc/hosts  
 ☹ Un fichier /etc/hosts à gérer pour chacune des machines du réseau

Solution plus générale (locale + globale - internet) => système DNS   
 😊 Un serveur DNS à configurer sur une seule machine

## 1ère étape : Choisir le service de résolution de noms

/etc/nsswitch.conf[[1]](#footnote-1) (extrait / prioritaire si les 2 existent)

hosts: files dns myshostname

1. files : cherche s’il y a une association avec [www.google.be](http://www.google.be) dans le fichier /etc/hosts
2. dns : va faire intervenir le fichiers /etc/resolv.conf

name server 10.12.51.1 : @IP d’un serveur DNS

1. myhostname : ????? pas obligatoire

## 2ème étape: Configurer le(s) services(s) choisi(s)

/etc/hosts1

127.0.0.1 theti localhost.localdomain localdomain  
198.197.56.141 theti theti.isat.be papyrus  
198.197.56.9 mapasserelle  
198.197.56.67 fileserver

dns: /etc/resolv.conf1

nameserver 193.190.156.67  
nameserver 193.190.159.19

/etc/hosts était utilisé quand internet n’était pas encore « présent »

## Commandes utiles

hostnamectl pour montrer ou changer le nom de la machine hostnamectl set-hostname VM1

uname -n pour montrer le nom de la machine

# But du DNS

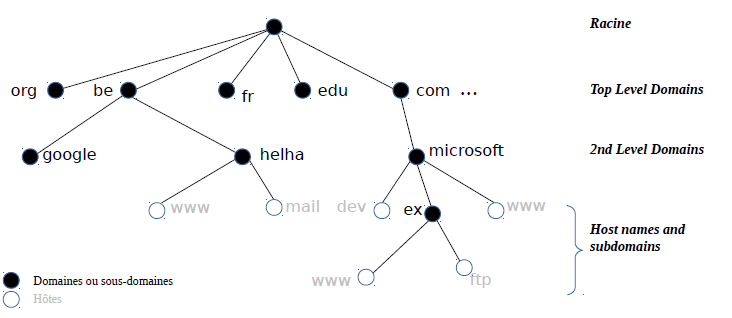
Pour traduire des noms DNS (FQDN - Fully Qualified Domain Name) en adresse IP et l ’inverse

www.helha.be → 193.190.66.18  
193.190.66.18 → www.helha.be

* Service essentiel pour tout réseau relié au monde extérieur
* Très utile aussi pour un réseau local (remplacement de /etc/hosts)
* Car le fichier /etc/hosts est très limité
  + Doit être recopié sur toutes les machines
  + Mises à jour, ajouts et suppressions synchronisées fastidieuses

# Plan du DNS

## Système de nommage

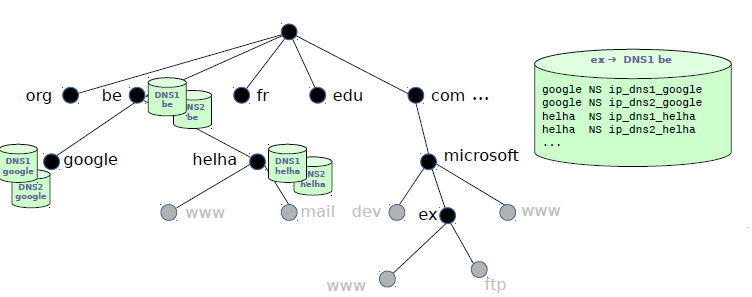


* Basé sur un modèle en arborescence similaire à celui des systèmes de fichiers.
* La dénomination d'un nom commence par le bas pour se terminer à la racine.
  + (ex. ftp.ex.microsoft.com. → le dernier point étant optionnel)
* Le DNS lit le lien à l’envers . -> .com -> google -> www

## Domaine

* Un domaine est l'ensemble d'une sous arborescence.
  + Exemple : Le domaine **"be."** rassemble toute la sous-arborescence à partir du nœud be.
* Il y a un domaine racine "**.**" et des domaines fils
  + ex. "org."
* Un nom de domaine est utilisé dans les URL et les adresses de messagerie
* ex. Soit le domaine "helha.be" → URL : <http://www.helha.be>  
   → @ : [toto@helha.be](mailto:toto@helha.be)
* En disant helha.be on parle du nœud helha

## Zone



* Une zone est la partie descriptive pour un niveau donné.
* Elle est restreinte à un nœud → une zone est constituée de la base de données décrivant un nœud.
* Chaque nœud contient une (ou plusieurs) BD (fichiers de zone) stockant des informations (les RR) dont l'adresse des BD des fil

Un RR (Ressource Record) de type NS renseigne l'adresse Ip d'un serveur Dns d'un sous-domaine.  
Pour que les RR de type NS soient propages correctement dans les TLD, il est nécessaire d'enregistrer le nom de domaine

## Autorité

* Un DNS particulier s'occupe d'un nœud sur lequel il a autorité. On dit que le serveur gère une zone d'autorité.
* C'est à dire qu'il gérera l'attribution des noms et résoudra les noms via un fichier de zone (BD) distinct pour chaque nœud.
* Chaque nœud a autorité sur la zone et contient une BD (fichiers de zone) stockant les informations nécessaires au bon fonctionnement de la zone (les RR) dont les noms de machines avec leur correspondance IP.

Un RR de type A établi une correspondance entre un nom d'host et son adresse Ip.  
Ici, on constate que les hosts www.helha.be et mail.helha.be possèdent la même adresse Ip.

Vider le cache DNS : dnf clean all

🡺 Exemple d’autorité

dnf whatprovides \*/nslookup  
dnf install bind-utils -y

nslookup [www.helha.be](http://www.helha.be)  
 Il a obtenu une réponse non-autoritaire car la réponse ne vient pas directement de helha.be

dnf install whois -y

whois helha.be | more

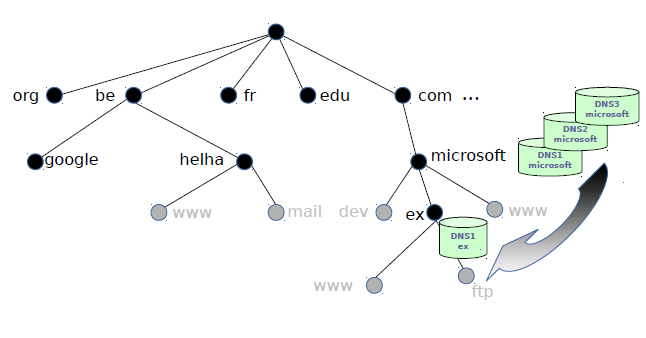
Donne toutes les infos

nslookup [www.helha.be](http://www.helha.be) 193.190.66.4

Ne spécifie pas de non-autoritative donc la réponse vient de helha.be 🡺Serveur autoritaire

Non-autoritative answer : Réponse vient d’un cache

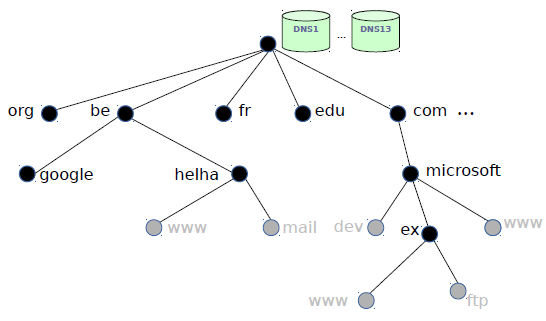
## Délégation



* Un serveur faisant autorité sur une zone peut déléguer la gestion de ses sous-domaines à d'autres serveurs de nom.
* Des fichiers de zone pour chaque sous-domaine doivent donc être créés et les fichiers de zone du domaine parent devront être modifiés en conséquence.
* Les DNS de la zone 'microsoft' délèguent leur autorité à un autre DNS en ce qui concerne la gestion de la zone 'ex'.

|  |  |
| --- | --- |
| Sans délégation | Avec délégation |
|  |  |

## Serveurs Racine



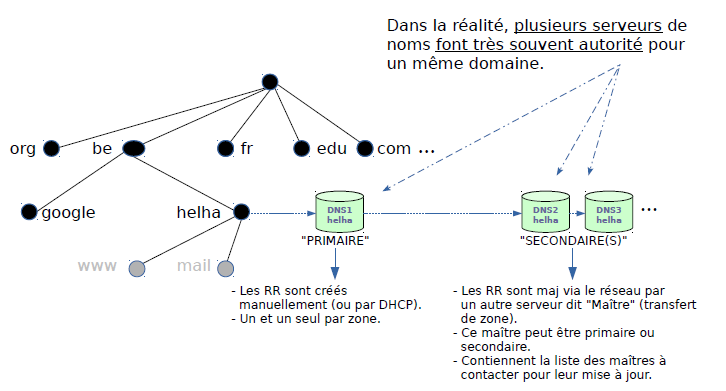
* Tout serveur DNS doit connaître les adresses IP des serveurs racines.
* 13 serveurs repartis dans le monde et gérés par 12 organisations indépendantes, chacun contenant les références de tous les serveurs de premier niveau dans une BD.
* Chacun de ces serveurs est consulte plusieurs dizaines de milliers de fois par heure.
* Hautement sécurises. Il en va de l'utilisation de l'Internet mondial.
* Ils contiennent la même information grâce à un système de réplication.
* Ils sont identifiés par les lettres de A à M et appartiennent tous au même domaine ROOT-SERVERS.NET.
* Le serveur A.ROOT-SERVERS.NET est le serveur d'origine. Les autres (B → M) sont des serveurs miroirs de celui-ci.
* Un serveur racine est en fait constitué d'un ensemble de serveurs dupliqués et configurés en 'anycast'. Autrement dit, chacun de ceux-ci possèdent la même adresse Ip mais un seul répondra à la requête DNS.
* Lorsqu'un routeur reçoit une demande pour joindre une adresse 'anycast', il la route généralement vers le serveur géographiquement le plus proche.

→ nécessité de pouvoir configurer des routeurs supportant un protocole de routage dynamique - ex. BGP (Hors cadre du cours)

root-server.org 🡺 site où sont référencés les serveurs RACINES

ping6 🡺 ping en ipv6

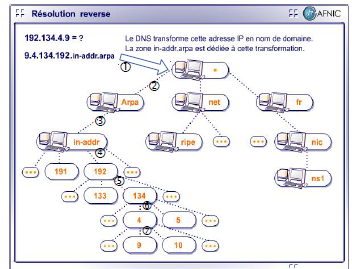
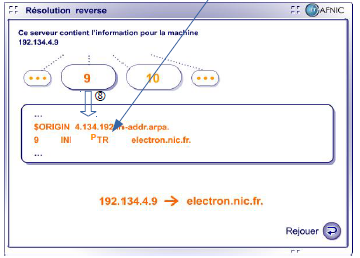
## Redondance



Backup (meilleure tolérance aux pannes)  
Loadbalancing (répartition des charges possible)

# Résolution et résolution inverse

Type de RR : PTR 🡺 Pointer – utilisé dans les recherches inversées

Utile pour restreindre l ’accès à des services Internet, permettre les règles anti-spam des serveurs de messagerie ...

- Exemple

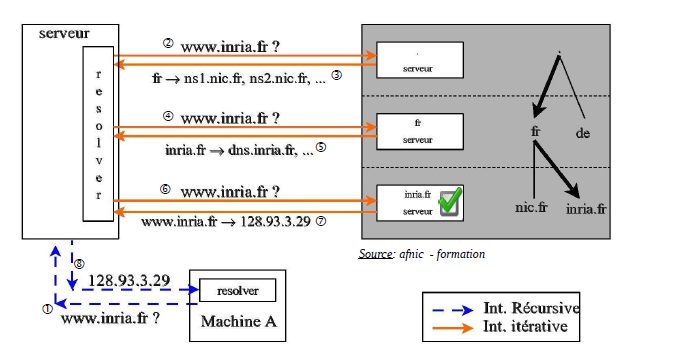
Soit un logiciel de cryptographie PGP installé sur un serveur FTP.  
FTP est configuré pour que ce logiciel ne soit téléchargeable qu ’à partir de certains pays …  
La résolution inverse sera donc sollicitée par le serveur FTP au serveur DNS.

# Parcours d'une requête

Le "resolver" permet de communiquer avec les serveurs DNS

➢ 2 modes d'interrogation :

* Récursif : Une requête récursive attend une réponse définitive à une résolution de noms.
* Itératif : Une requête itérative attend pour réponse la réponse elle-même ou bien une référence vers un autre serveur DNS. (Ne nécessite pas de réponse définitive)



* Ici, il y a eu 4 interrogations pour résoudre www.inria.fr
* Mécanisme accélérateur : le cache

Remarque: DNS recursif ouvert

* + Il est fortement conseillé de ne pas laisser votre DNS récursif ouvert.
  + C'est-à-dire ne pas permettre la récursion sur votre DNS à partir d'Internet.
  + Votre DNS n'acceptera de résoudre des noms qu'à partir votre réseau local.
* Ne pas être DNS relais.
* Accroissement de la sécurité (hors cadre du cours)

# Debug DNS

## dig (Domain Information Groper)

# dig → donne la liste des serveurs racines

# dig @server name type → donne les informations concernant une ressource (name) d'un certain type (type) d'un certain serveur Dns (@server).

|  |  |  |
| --- | --- | --- |
| 1 | dig @e.root-servers.net www.reseaucerta.org A | On demande au serveur racine E s’il sait résoudre [www.reseaucerta.org](http://www.reseaucerta.org) |
| 2 | dig @d0.org… www.reseaucerta.org A | On choisit un serveur ayant autorité sur org. |
| 3 | dig @a.dns.gandi.net www.reseaucerta.org A | On choisit un serveur ayant autorité sur  reseaucerta.org. |
|  | www.reseaucerta.org 86400 IN A 194.254.4.9 | adresse ip recherchée |
| 1 status : NO ERREUR 🡺pas d’erreur dans la question  QUERY : 1 🡺 1 question  ANSWER : 0 🡺 Pas de réponse définitive | | 3 ANSWER : 3  [www.reseaucerta.org](http://www.reseaucerta.org) -> gravelines.reseaucerta.org  -> 151.80.233.22  Le premier ->, est un CNAME , un alias. |

|  |  |  |
| --- | --- | --- |
|  | Commande | Résultat |
| 1 | dig @e.root-servers.net www.xxyyzz.be A | Pas de réponse définitive, mais il propose une liste de 6 serveurs |
| 2 | dig @brussels.ns.dns.be www.xxyyzz.be A | Le domaine xxyyzz n’existe pas |
|  | ;; ->> HEADER … status : NXDOMAIN → Non eXistant DOMAIN | |

Type de RR : MX 🡺 mail exanger

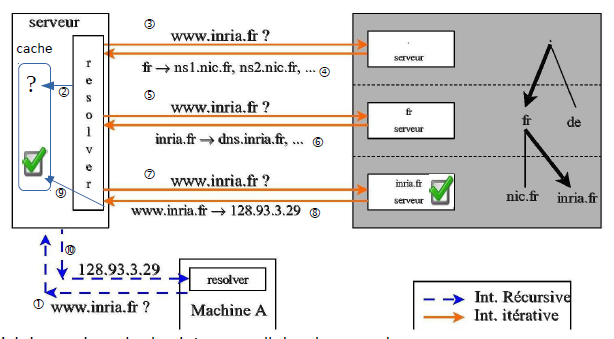
## nslookup

Cette commande peut être utilisée en mode interactif

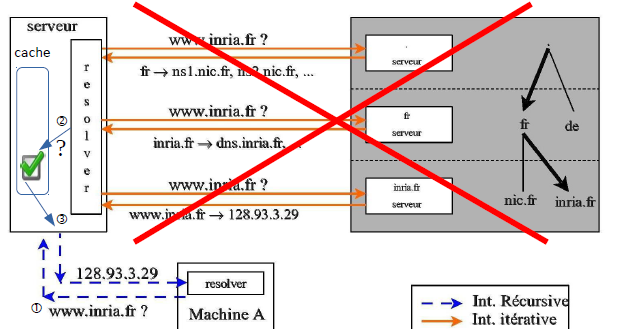
|  |  |  |
| --- | --- | --- |
|  | nslookup |  |
|  | > server e.root-servers.net | On choisit un serveur racine |
|  | > set type=NS | On s'intéresse aux records de type NS |
|  | > org. | Quels sont les dns qui gèrent org. ? |
|  | > server d0.org… | On passe sur un de ces serveurs |
|  | > reseaucerta.org. | Quels sont les dns qui gèrent reseaucerta.org. ? |
|  | > server a.dns.gandi.net | On passe sur un de ces serveurs |
|  | > set type=A | On s'intéresse aux records de type A |
|  | >www.reseaucerta.org | Quelle est l'Ip de www.reseaucerta.org ? |
|  | > set type=MX | On s'intéresse aux records de type MX |
|  | > reseaucerta.org | Quels sont les serveurs de mail de reseaucerta.org ? |
|  | > set type=A | On s'intéressé aux records de type A |
|  | > smtp.reseaucerta.org. | Quelle est l'ip du serveur smtp de reseaucerta.org ? |
|  | > set type=ANY | On s'intéresse a tout |
|  | reseaucerta.org. |  |
| server : permet de se connecter à un server DNS type A : [www.reseaucerta.org](http://www.reseaucerta.org)  Name : gravelines.reseaucerta.org Adresse : 151.80.233.22 | | Type MX reseaucerta.org  Server : ns-6-c.gandi.net  Address : 217.70.187.7 # 53  2 a strasbourg  smtp  Name : strasbourg.reseaucerta.org  Address : 194.254.4.9    strasbourg2, 51.255.170.100 |

# Serveur de cache

## Explication



* Ici, le resolver du dns interroge d'abord son cache
* Si celui-ci est vide, il interroge alors les dns extérieurs de manière itérative ou fera appel à des 'forwarders' afin de résoudre la requête (voir plus loin)
* Une fois résolue, l'association Ip/Nom est mise en cache



* Lorsque la réponse à la requête est déjà dans le cache, l'extérieur n'est pas sollicité.
* Le resolver du dns la transmet au client à partir de ce cache.
* Il s'agit d'une Non-authoritative answer.

## Avantages et inconvénients

Avantages

* Éviter la surcharge inutile du réseau
* Supprimer les délais du réseau
* Amoindrir la charge des autres serveurs
* → tout serveur possède en général au minimum un cache

Inconvénient

* Ne pas oublier de sécuriser le cache

### Configuration minimale

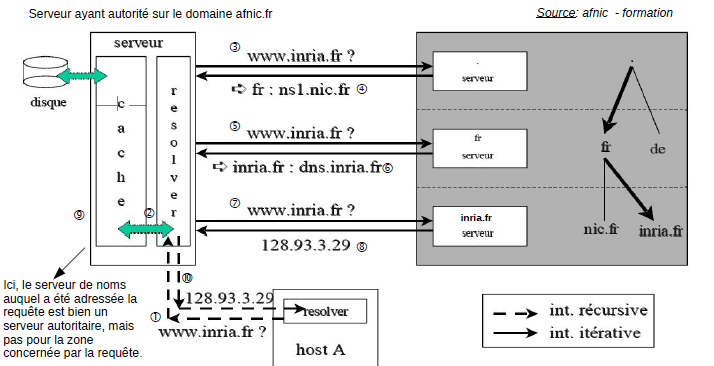
* Base de données nécessaire
  + adresses des serveurs de la racine
  + reverse du loopback 1.0.0.127.in-addr.arpa (c'est elle qui fait office de zone de cache)
* Les données du cache possèdent une durée de vie limitée (Time To Live – ttl) afin de permettre son rafraîchissement et la prise en compte des modifications.
* Il s'enrichit au fur et à mesure par les données récoltées pour résoudre les requêtes des clients.

→ une requête déjà demandée est résolue à partir du cache du serveur

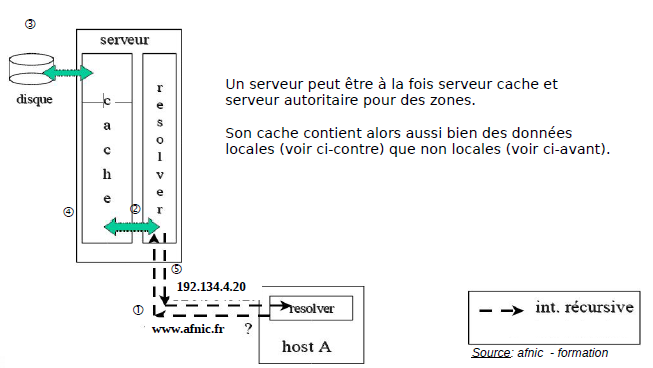
* Ce type de serveur n'a autorité sur aucune zone.

# Serveur autoritaire

Résolution d'une requête récursive par une suite de requêtes itératives envoyées vers les serveurs autoritaires des zones 'root' ('.'), 'fr' et 'inria.fr'.



Résolution d'une requête récursive envoyée directement vers le serveur autoritaire la zone concernée.



Récursif

* Le serveur résout les requêtes récursives des clients et garde les informations obtenues dans son cache
* → le cache stocke des informations pour lesquelles le serveur n'a pas nécessairement autorité
* Serveurs cache de campus par exemple

Itératif

* Il répond toujours en fonction des données qu'il possède localement

→ ne construit pas de cache pour des données non locales.

→ une machine cliente (d'utilisateur final) ne doit jamais pointer sur un serveur de ce type comme serveur par défaut.

* Mode permettant de limiter la charge d'un serveur (il ne résout pas toute la requête)

→ serveurs de la racine, serveurs ayant autorité pour un grand nombre de zones.

# Bind

Bind (Berkeley Internet Name Daemon) est le serveur de noms le plus utilisé sur Internet.

## Packages

bind – bind-utils – bind-libs

## Composants

* Le daemon named
  + C'est le service Dns → # systemctl start/stop/restart named
  + Port d'écoute (udp 53)
* Fichiers de configuration
  + /etc/named.conf → fichier de configuration principal
  + /var/named → dossier par défaut qui contient les fichiers de zones
* Outils de debuggage: dig, nslookup, host … (inclus dans le package bind-utils)
* Points d'entrée : man named, man /etc/named.conf

## Serveur cache

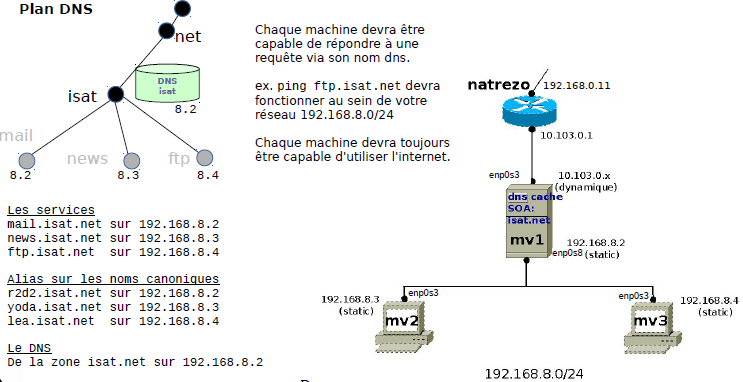
|  |  |  |
| --- | --- | --- |
| options {  listen-on port 53 {127.0.0.1 ; 192.1.0.2 ; } ; // Port d'écoute, ip admises  directory "/var/named"; // répertoire des fichiers de zones  }; | | |
| zone "." IN {  type hint;  file "named.ca"; // cache des serveurs racines  }; | | Ces 3 fichiers de zones seront automatiquement créés lors de l'installation du package 'bind'... |
| zone "1.0.0.127.in-addr.arpa" IN {  type master;  file "named.loopback"; // zone primaire du reverse loopback  }; | |
| zone "localhost" IN {  type master;  file "named.localhost";  }; | // Zone primaire du loopback.  // Facultative sauf si on veut faire résoudre le nom 'localhost' par le serveur. |

Le fichier named.ca contient le descriptif de la zone "."  
Le fichier named.loopback -> résolution de 127.0.0.1  
named.localhost : permet à named de faire de la résolution sur localhost  
 Les types "slave" sont des copies miroirs des masters.

zone "." et zone"1.0.0.27.in-addr.arpa" -> nom logique d'une zone

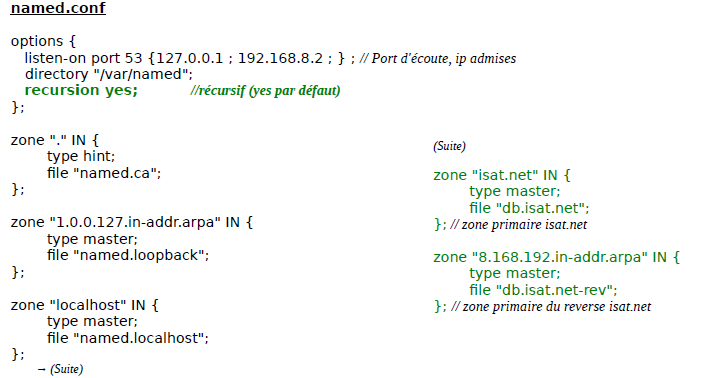
## Gérer un domaine

Soit construire un serveur dns gérant le domaine 'isat.net' suivant :

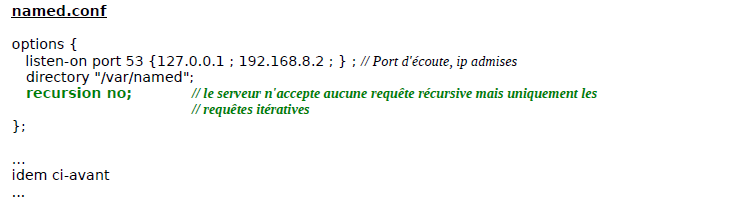


SOA : Source of authority

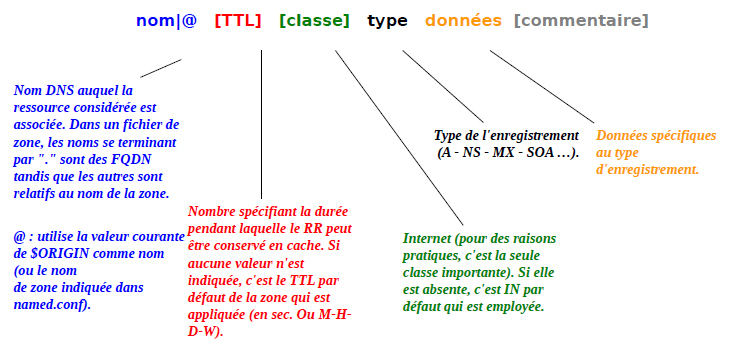
## Serveur autoritaire récursif



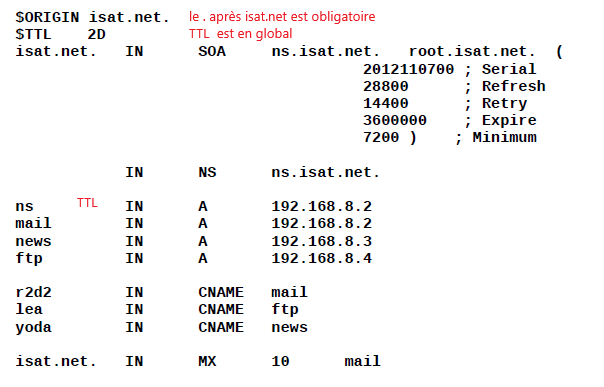
## Serveur autoritaire itératif



## Syntaxe d'un RR

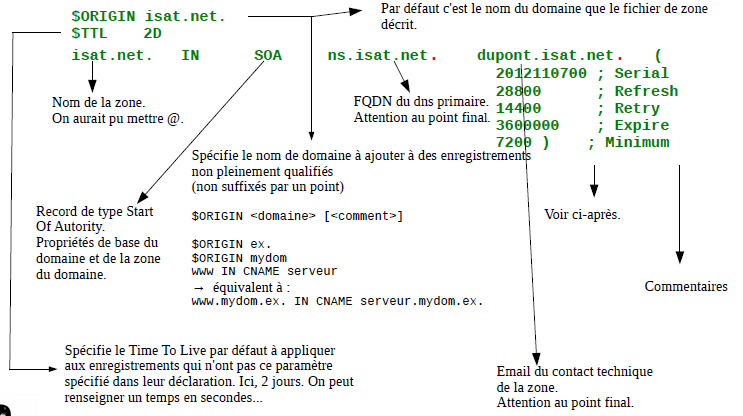


## Fichier de zone : isat.net



Le TTL s'installe après le nom, ex sur images

SOA -> obligatoire, "je suis la source d'autorité sur le srv isat"



Si on met un @ mais pas $ORIGIN qui suit, il va aller chercher dans les zones. Voir dia 42

Si on oublie le . après ns.isat.net ça va nous donner : ns.isat.net.isat.net

Un SOA a besoin d'une adresse mail de l'admin (dupont.isat.net.)

Mettre [www.mydom.net](http://www.mydom.net) revient au même que www car il va chercher le 1er $ORIGIN relatif (mydom) puis ex.

Serial : Specifie la version des donnees de la zone

Refresh : Intervalle, ici en sec., entre 2 vérifications du serial number par les secondaires.

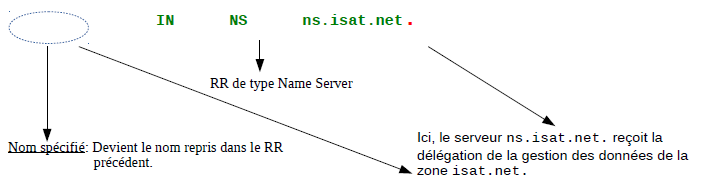
Retry : Intervalle, ici en sec., entre 2 vérifications du serial number par les secondaires si la 1ere vérification a échoué.

Expire : Temps, ici en sec., après lequel le secondaire détruit les données de la zone qu'il possède et arrête de répondre aux requêtes pour cette zone s'il ne parvient pas à contacter le serveur primaire.

Minimum : Temps que doit rester dans le cache une réponse négative suite à une question sur ce domaine.

Deux types de réponses négatives :

* NXDOMAIN : aucun RR ayant le nom demande dans la classe (IN) n'existe dans cette zone.
* NODATA : aucune donnée pour le triplet (nom, type, classe) demande n'existe ; il existe d'autres records possédant ce nom, mais de type différent.

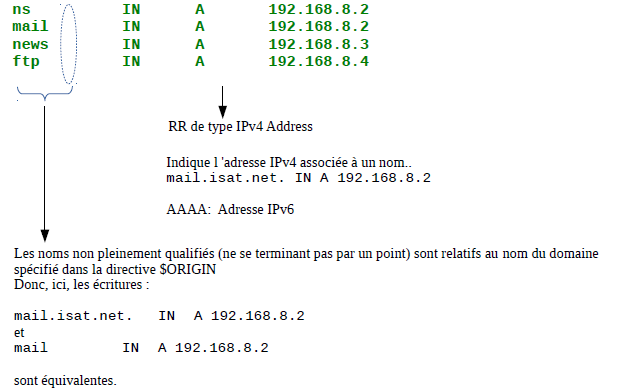


zone IN NS serveur-nom1.domaine.

IN NS serveur-nom2.domaine. → *serveur secondaire*

Il faut spécifier les serveurs de noms de la zone que l'on décrit (associée au SOA)

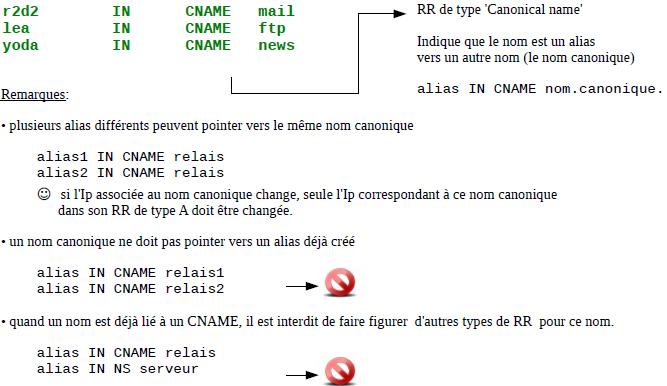
Lorsque le nom est vide, il reprend celui du champ précédent.  
On peut mettre ns sans point, il va compléter avec $ORIGIN pour faire ns.isat.net.  
Lorsqu'on a plusieurs serveurs autoritaires sur une adresse, il faut avoir plusieurs RR de type NS



On associe les "noms" à des IP

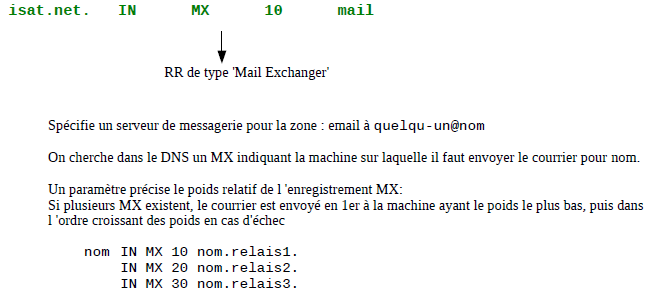
Par ex :

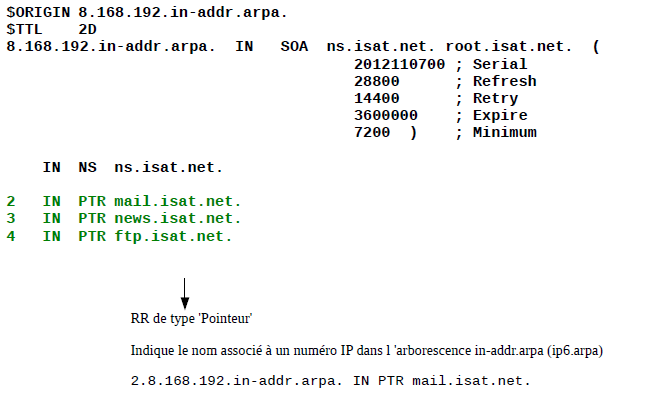
ns est l'adresse 192.168.8.2 (pas de point donc ns.isat.net.)



On ne peut avoir plusieurs alias sur une seule ligne

Cad : alias1, alias2, alias3 IN CNAME mail

10 est un niveau de priorité



On ne peut mettre mail tout court sinon il va compléter avec le $ORIGIN

## Les fichiers de zone :celui du reverse 0.0.127.in-addr.arpa

• Personne n'a la responsabilité de ce reverse pour le numéro 127.0.0.1 dans la hiérarchie in-addr.arpa.

• Doit toujours être configuré sous peine de comportement anormal du DNS.

1. Prise en compte immédiate des modifications apportées ... [↑](#footnote-ref-1)