

LE SERVICE DNS

À QUOI SERT LE SERVICE DNS ?

- Définition habituellement admise :
- Le service DNS met en correspondance
 - un nom de domaine et une adresse IP
- **Abus de langage : nom de domaine**
- on distingue deux types de noms avec le système DNS :
- le **nom d'hôte** qui représente le nom d'une machine (un ordinateur, une imprimante ou bien encore un routeur).
- le **nom de domaine pleinement qualifié** ou **FQDN** (Fully Qualified Domain Name).

LE NOM NETBIOS D'UNE MACHINE

- Un nom **NetBIOS** est l'identifiant d'une machine dans un réseau utilisant le protocole **NetBIOS**.
- On peut dire : c'est le nom d'hôte.
- (terminologie utilisée également dans le monde Linux)

PROTOCOLE NETBIOS

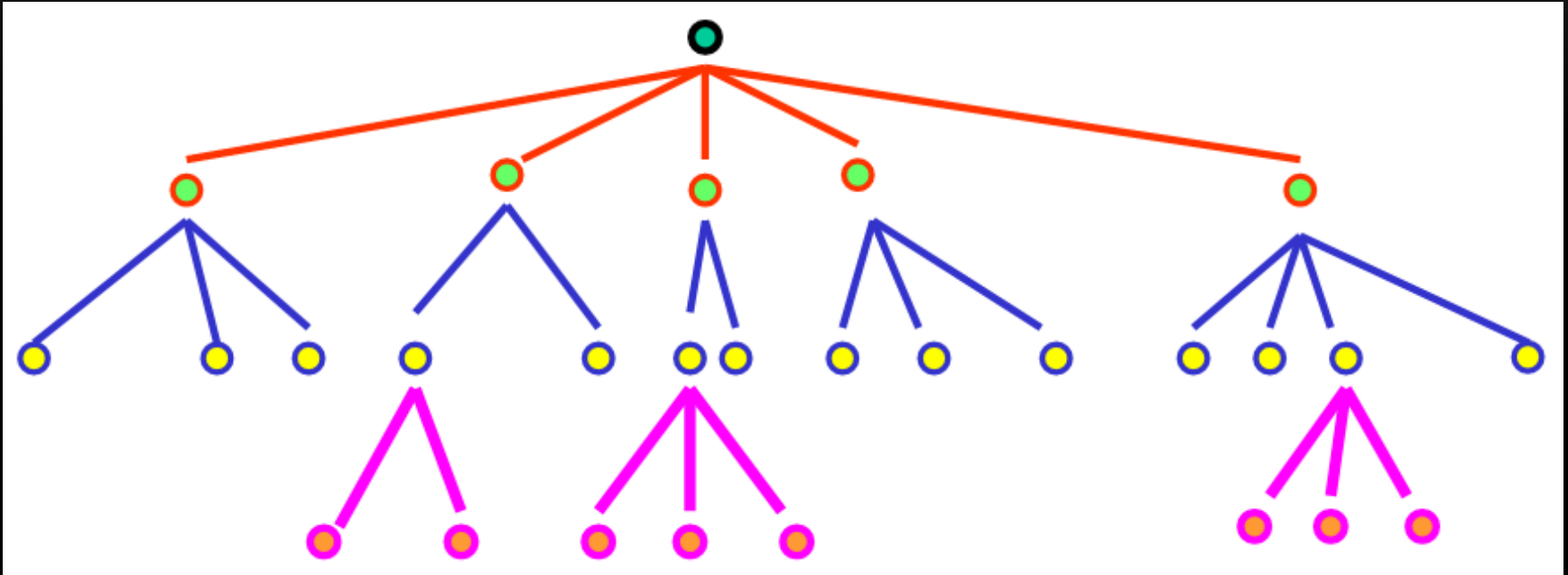
- Protocole ancien de résolution des noms en environnement Windows.
- Inconvénients :
 - Propriétaire
 - Mécanisme de résolution de noms par diffusion

POURQUOI DNS ?

- Les réseaux sont maintenant des réseaux étendus et interconnectés (Internet)
- La gestion des adresses IP est faite au niveau international
- La recherche des machines doit pouvoir être faite au niveau international
- D'où nécessité de normalisation du nommage des machines pour pouvoir les identifier.

L'ESPACE DE NOMMAGE

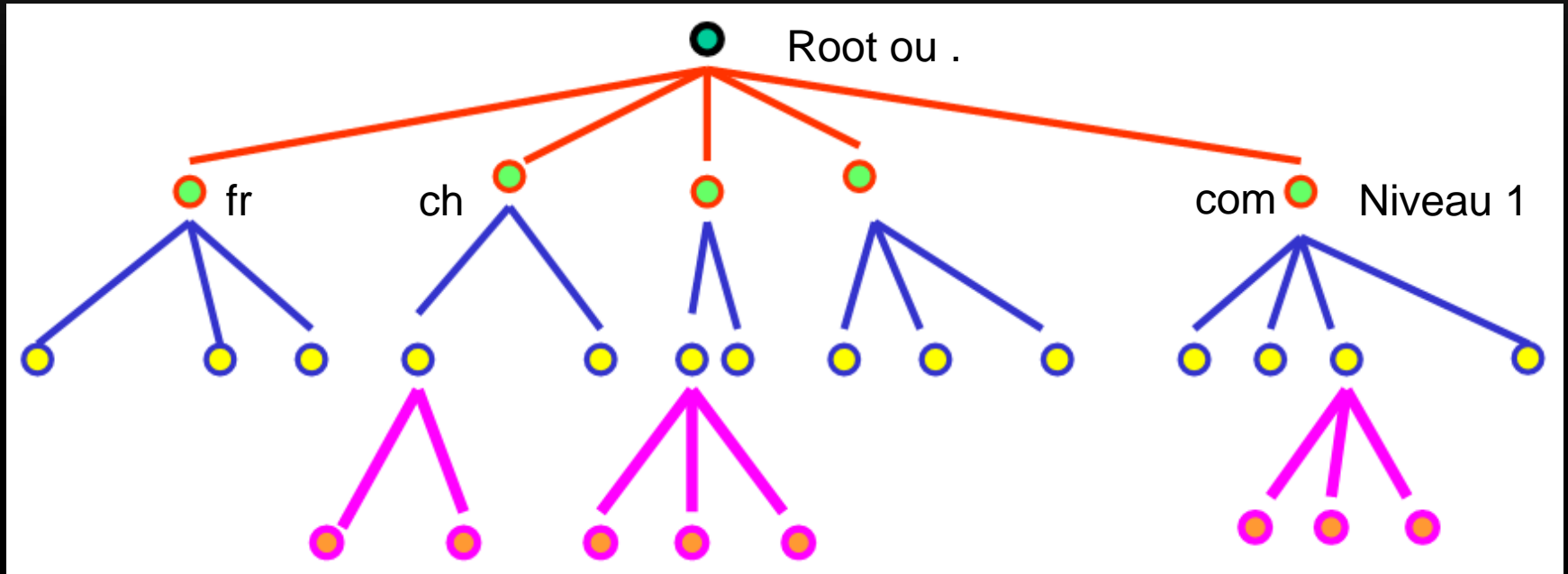
L'ESPACE DE NOMMAGE



espace de Noms de domaine : organisation arborescente

Racine appelée root, identifiée par «.»

L'ESPACE DE NOMMAGE

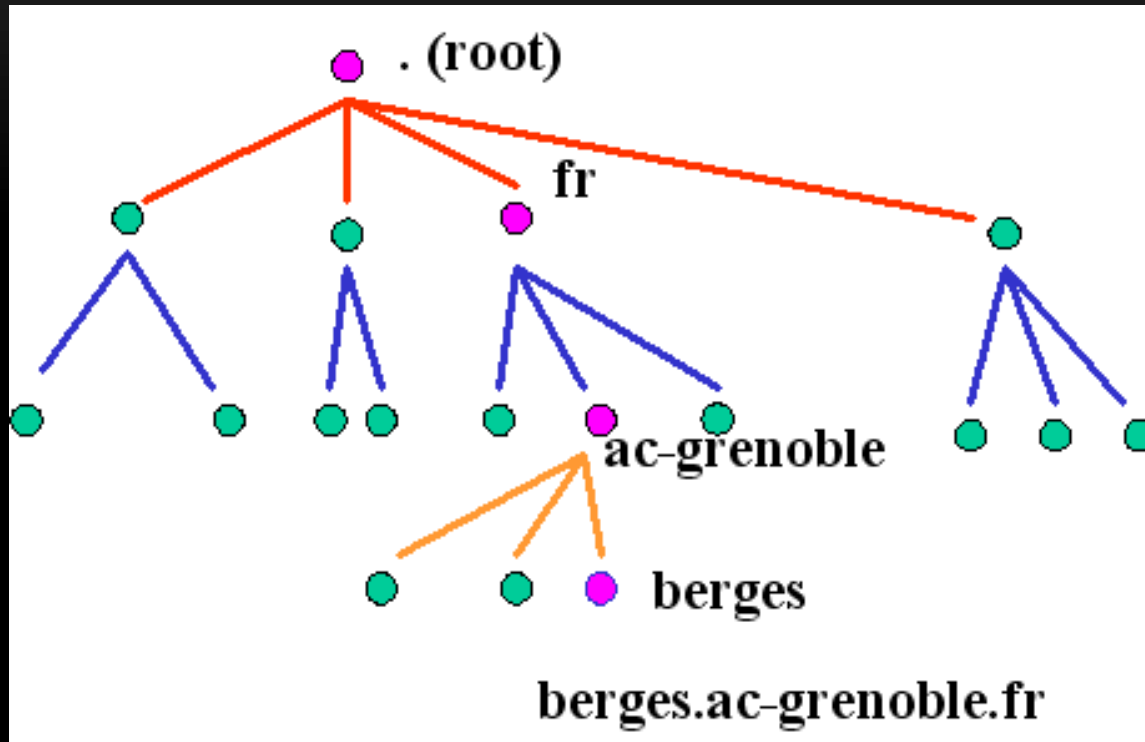


NIVEAU 1 : Top Level Domain

Codes génériques : .com, .org, .edu etc....

Codes pays : .fr, .us, .be etc....

NOM DE DOMAINE

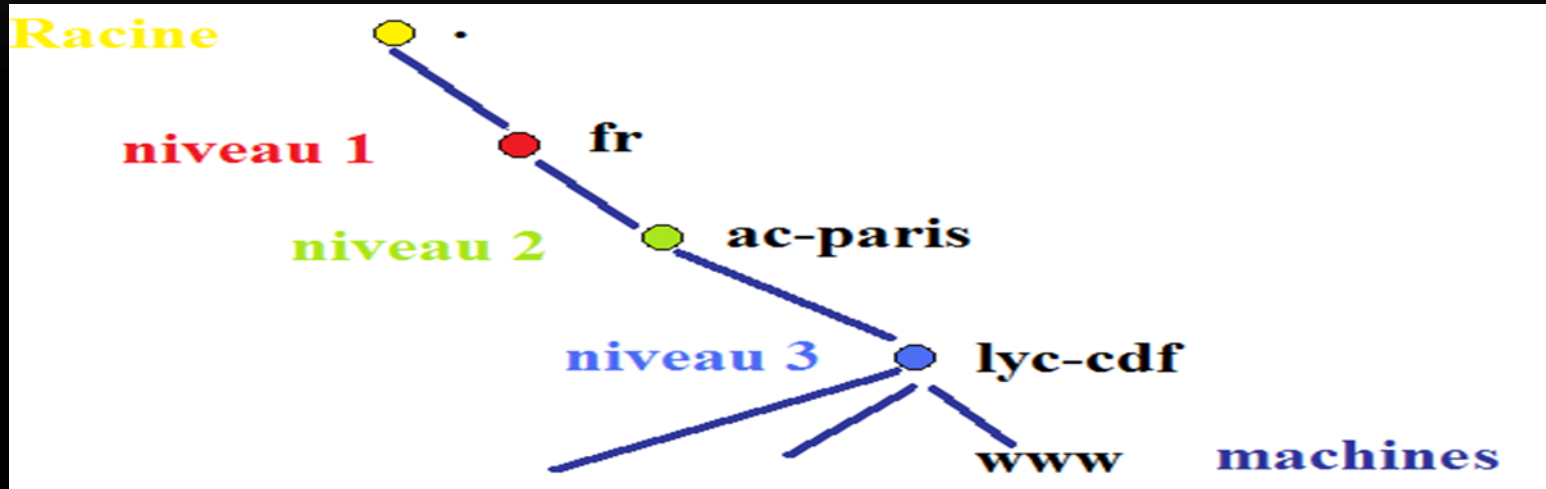


Deux nœuds fils ne peuvent avoir le même nom, on a donc unicité d'un nom de domaine au niveau mondial.

LES NOMS FQDN

- Le FQDN est en fait composé de deux parties : le nom d'hôte et le suffixe DNS.
- **Nom d'hôte** : nom de l'équipement
- **Suffixe DNS** : définit la relation entre le domaine auquel appartient la machine et le domaine racine.
- Exemple
 - **www.lyc-cdf.ac-paris.fr**

WWW.LYC-CDF.AC-PARIS.FR

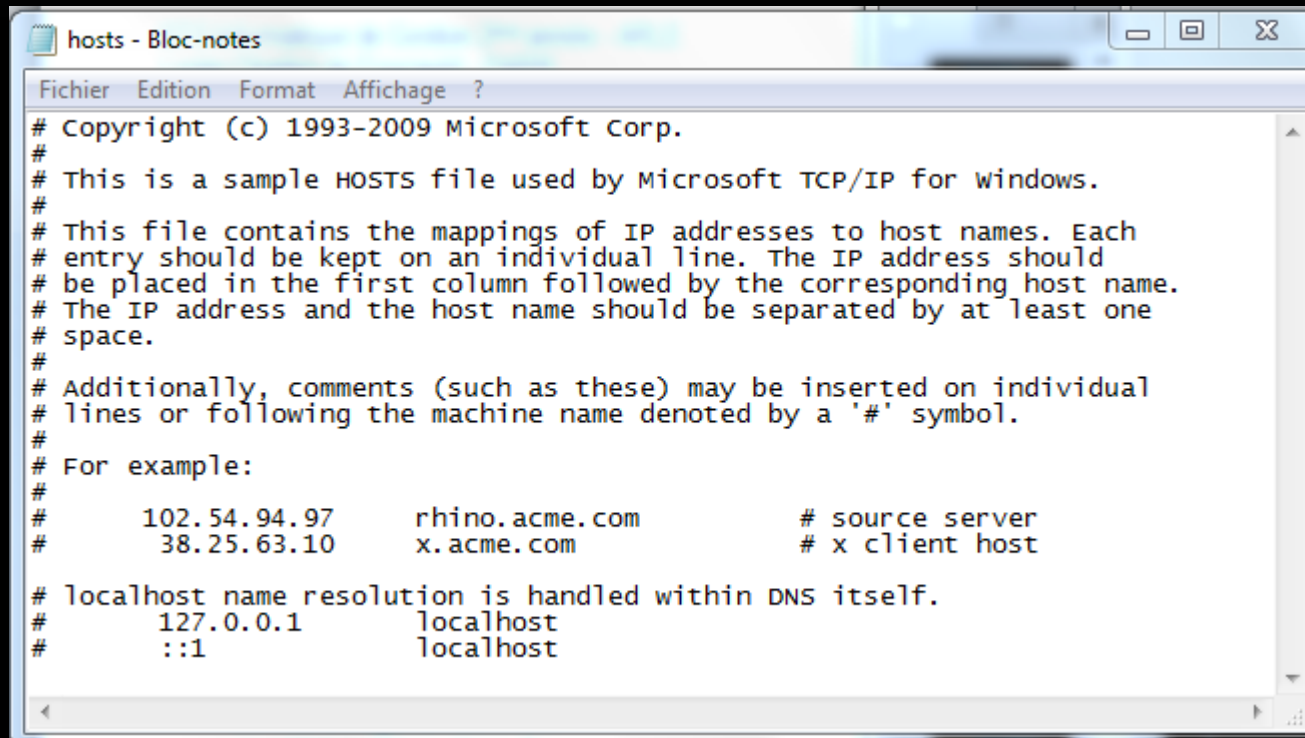


Nom d'hôte : **www**

Suffixe DNS : **lyc-cdf.ac-paris.fr**

FICHER HOSTS

- Fichier local à la machine ; répertoire de noms FQDN et adresse IP



```
hosts - Bloc-notes
Fichier  Edition  Format  Affichage  ?
# Copyright (c) 1993-2009 Microsoft Corp.
#
# This is a sample HOSTS file used by Microsoft TCP/IP for Windows.
#
# This file contains the mappings of IP addresses to host names. Each
# entry should be kept on an individual line. The IP address should
# be placed in the first column followed by the corresponding host name.
# The IP address and the host name should be separated by at least one
# space.
#
# Additionally, comments (such as these) may be inserted on individual
# lines or following the machine name denoted by a '#' symbol.
#
# For example:
#
#       102.54.94.97       rhino.acme.com           # source server
#       38.25.63.10       x.acme.com               # x client host
#
# localhost name resolution is handled within DNS itself.
#       127.0.0.1         localhost
#       ::1               localhost
```

FICHER HOSTS

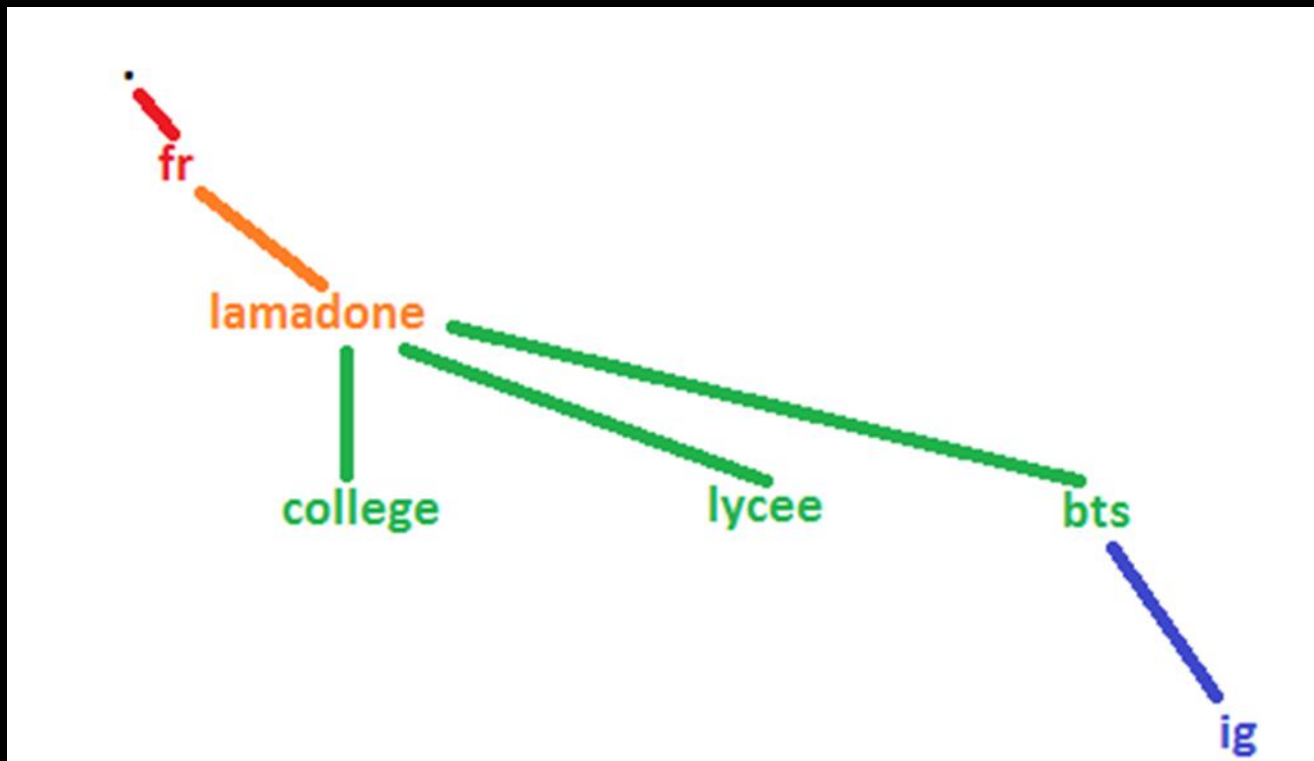
- utilité
 - Utilisé avant de faire appel au service DNS
 - Accélère les demandes de résolution
 - Éventuellement permet de mettre en place des « blacklist »
- Inconvénient
 - Local à la machine
 - Mises à jour

QUESTION 9

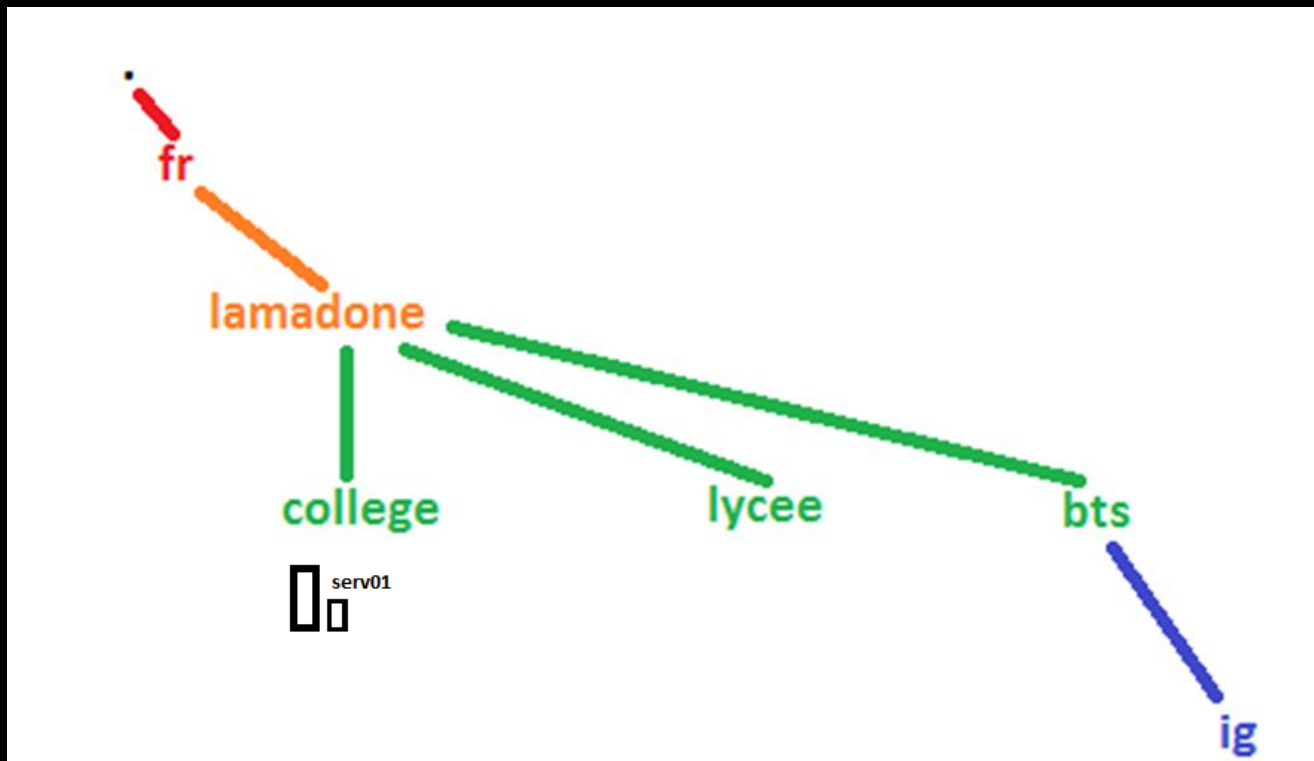
- [serv01.college.lamadone.fr](#)
- [serv02.lycee.lamadone.fr](#)
- [serv03.bts.lamadone.fr](#)
- [serv04.ig.bts.lamadone.fr](#)
- [poste1ARLE.ig.bts.lamadone.fr](#)
- [poste2ARLE.ig.bts.lamadone.fr](#)
- [poste1.bts.lamadone.fr](#)
- [www.lamadone.fr](#)

IG.BTS.LAMADONE.FR

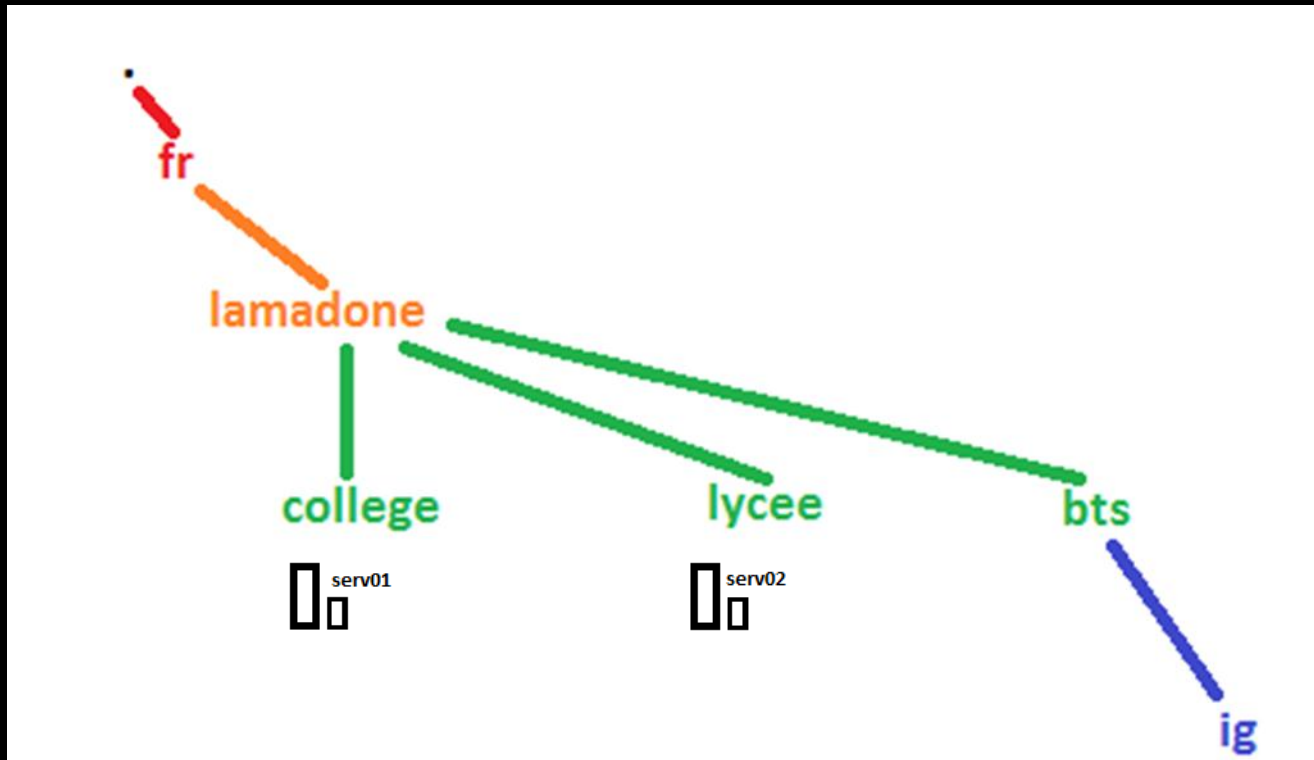
- Dessin de l'arbre



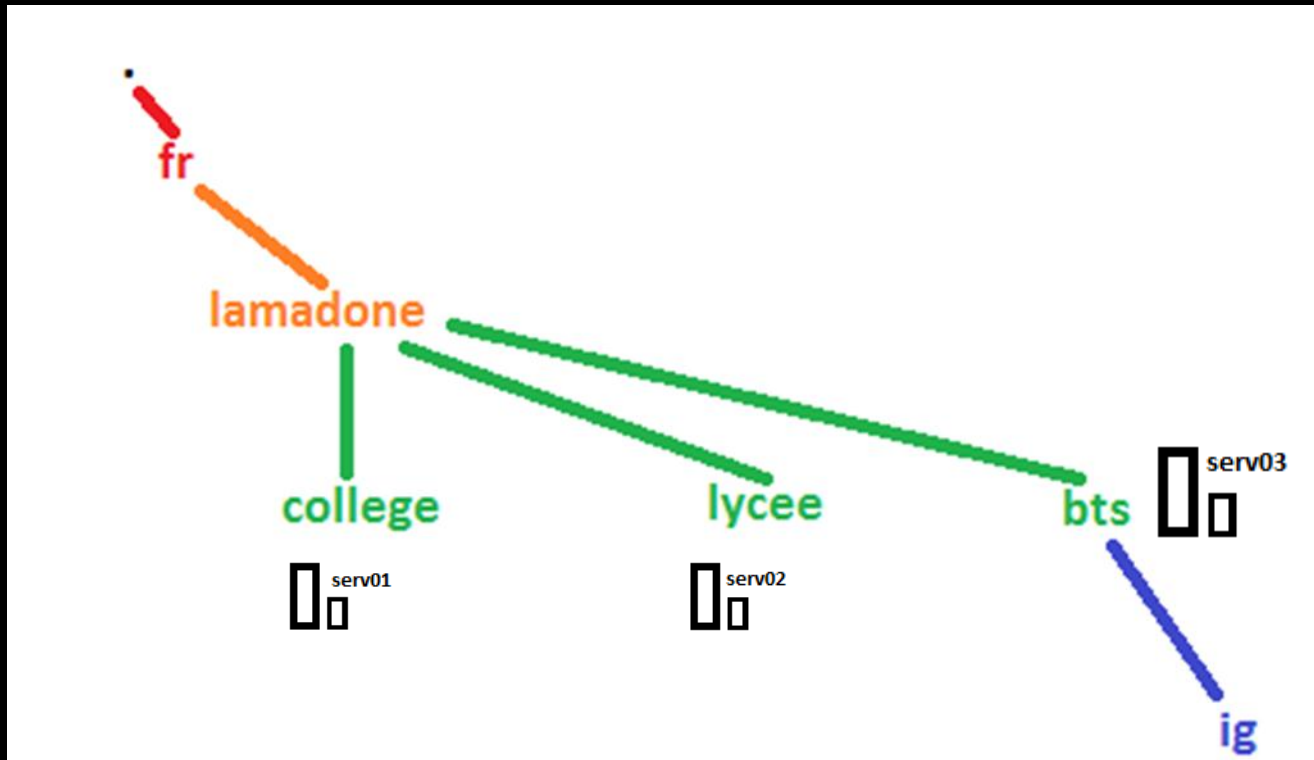
SERV01.COLLEGE.LAMADONE.FR



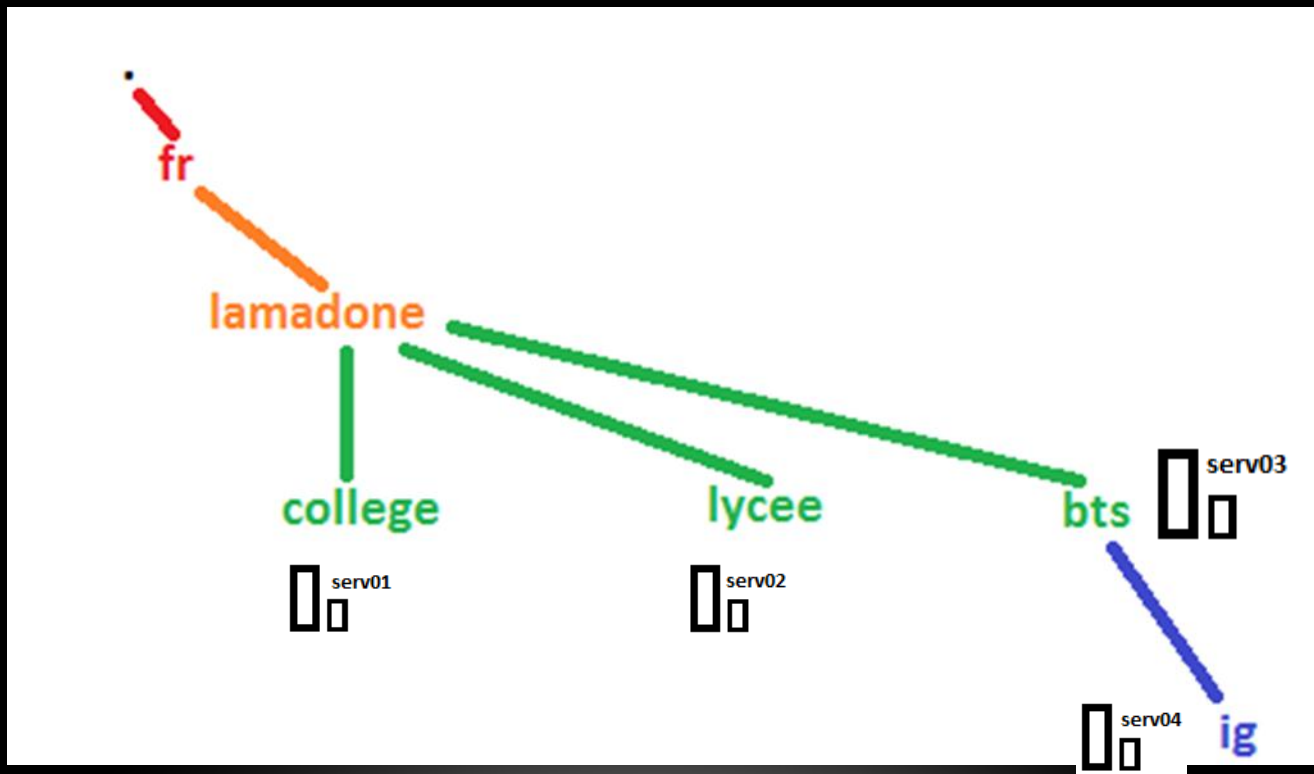
SERV02.LYCEE.LAMADONE.FR



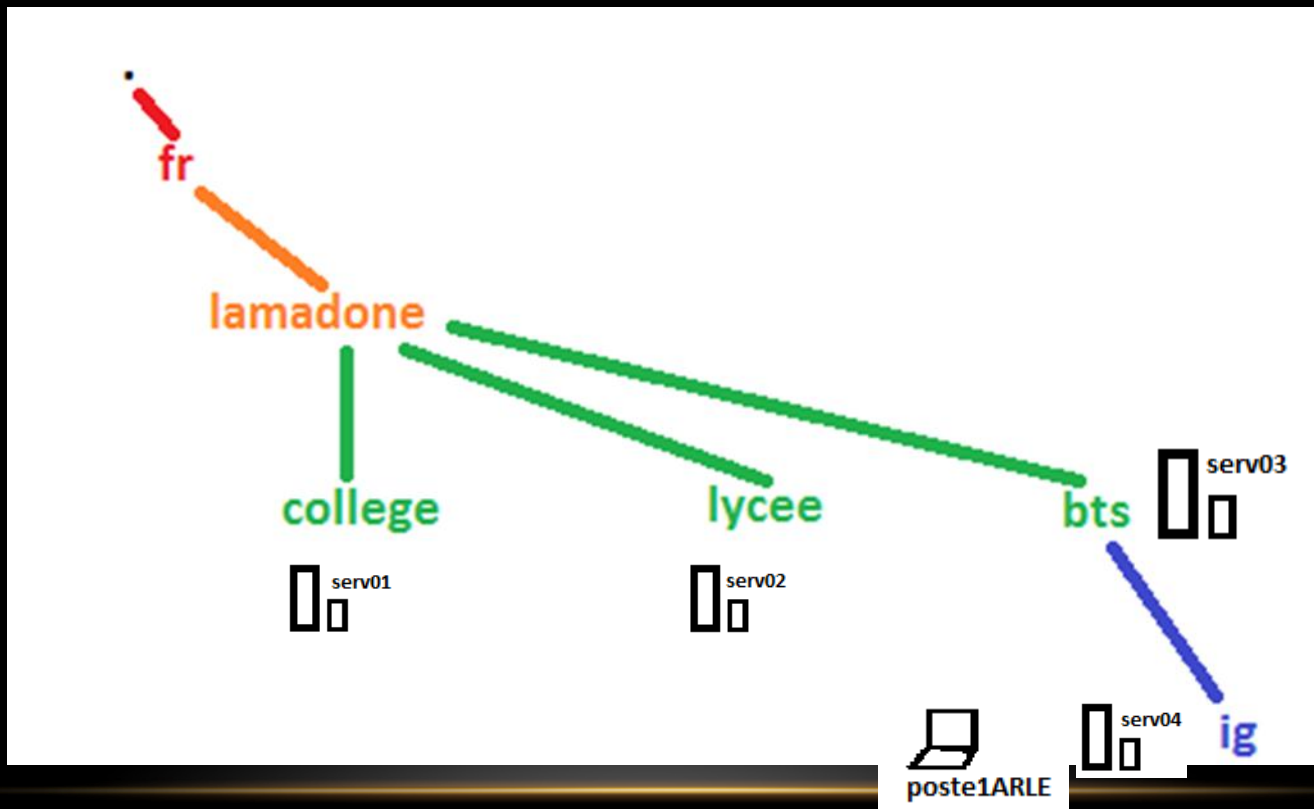
SERV03.BTS.LAMADONE.FR



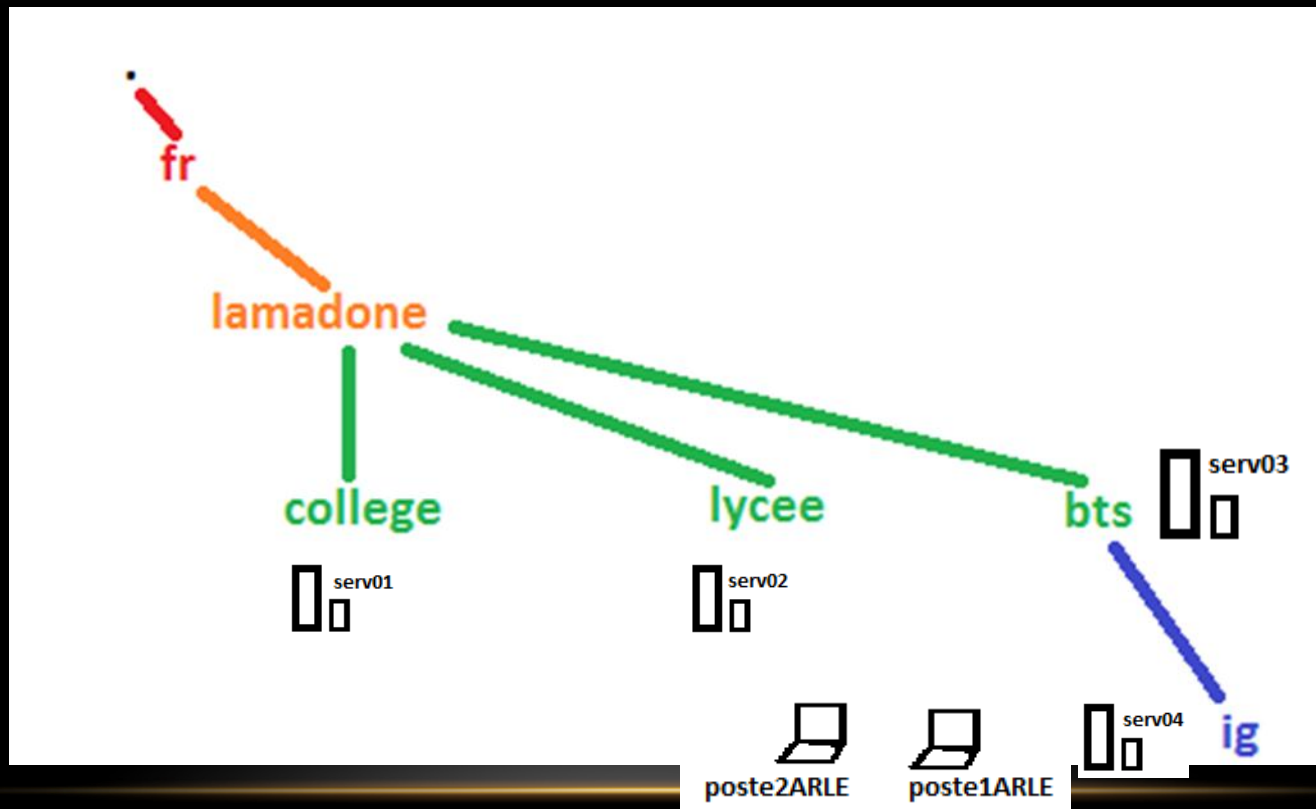
SERV04.IG.BTS.LAMADONE.FR



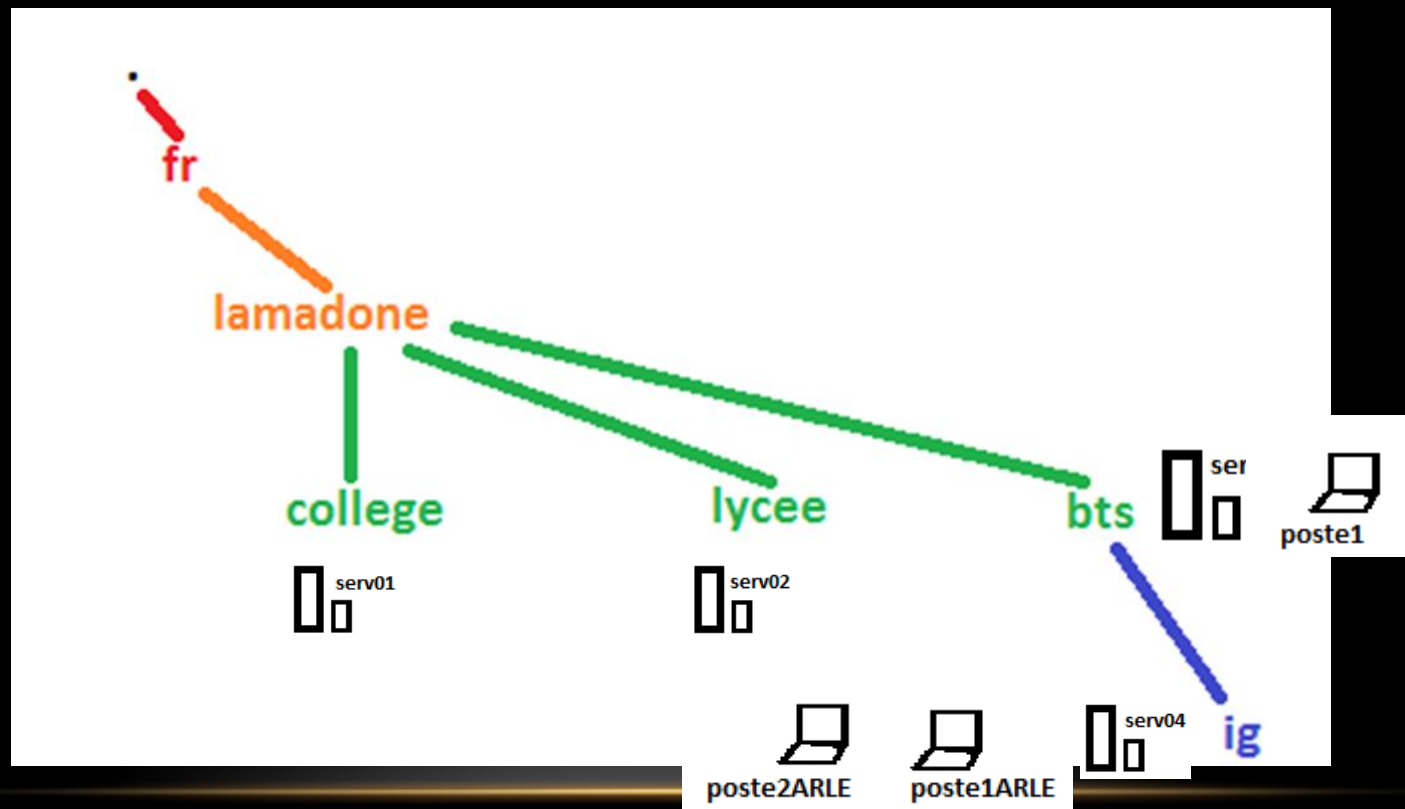
POSTE1ARLE.IG.BTS.LAMADONE.FR



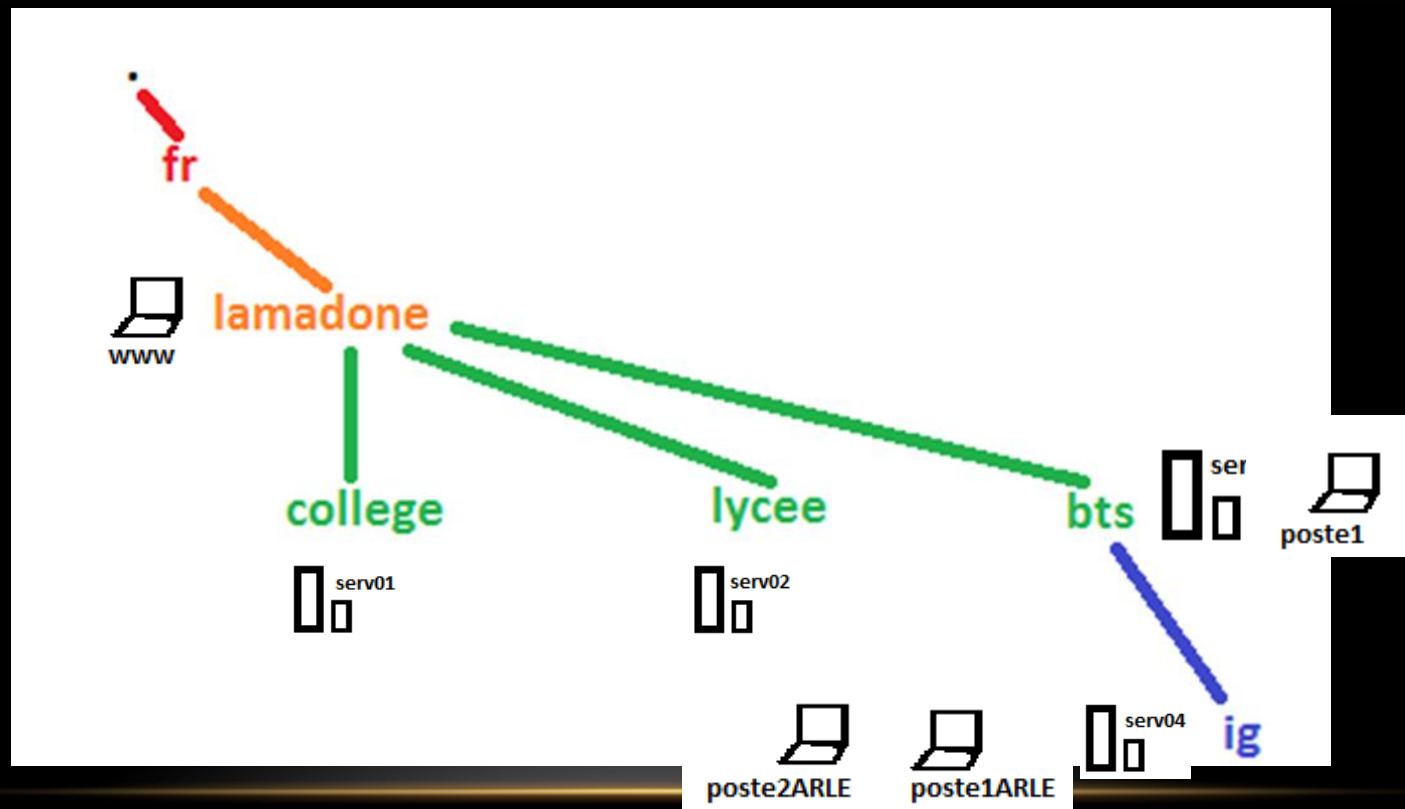
POSTE2ARLE.IG.BTS.LAMADONE.FR



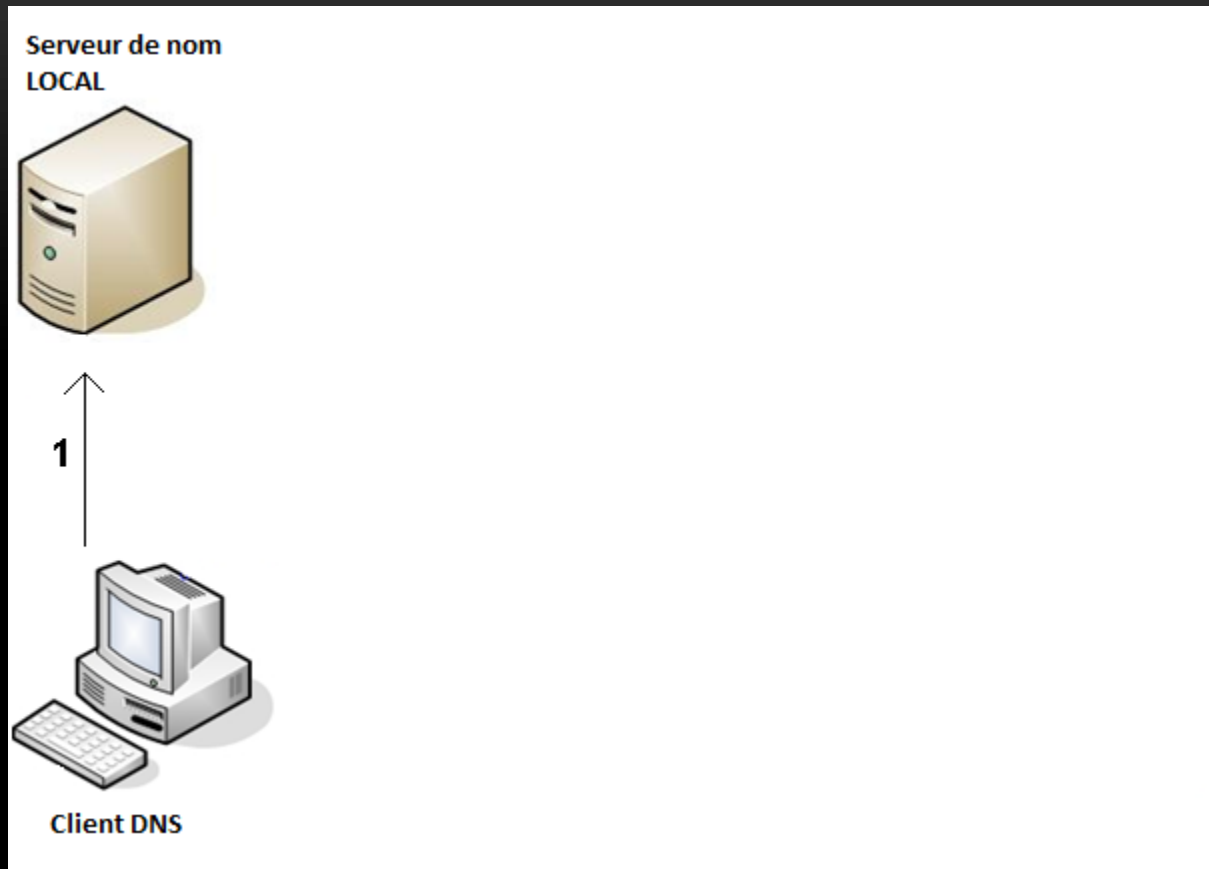
POSTE1.BTS.LAMADONE.FR



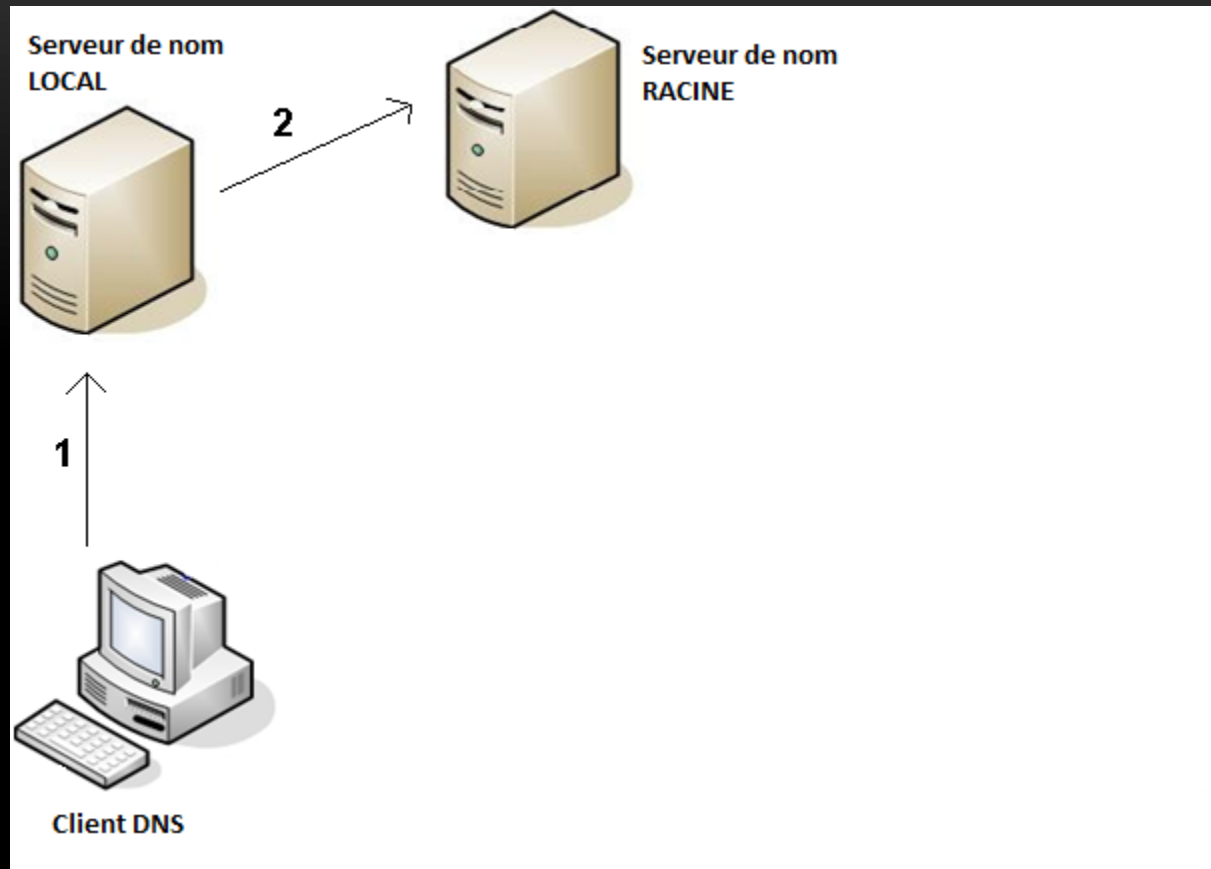
WWW.LAMADONE.FR



ET SUR INTERNET ?



Le client DNS souhaite joindre le site www.elysee.fr :
1. il envoie une requête à son serveur DNS local pour obtenir l'adresse IP de www.elysee.fr.



2. le serveur local analyse ses zones et n'en trouve aucune qui corresponde au nom de domaine demandé. Il envoie sa requête auprès du serveur de nom racine.

LES SERVEURS RACINE

CONTENU

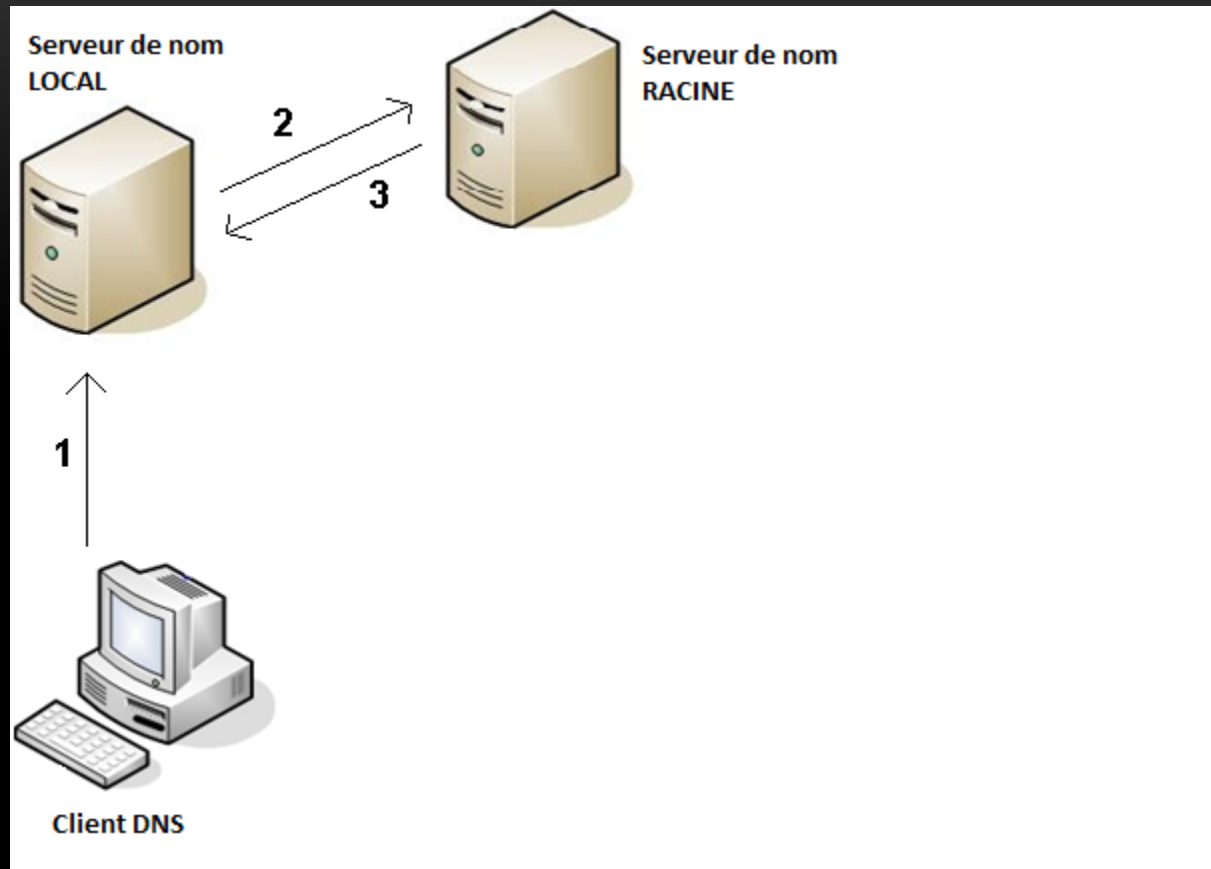
Ils référencent toutes les adresses IPV4 et IPV6 des serveurs de domaines de premier niveau.

OBSERVATIONS

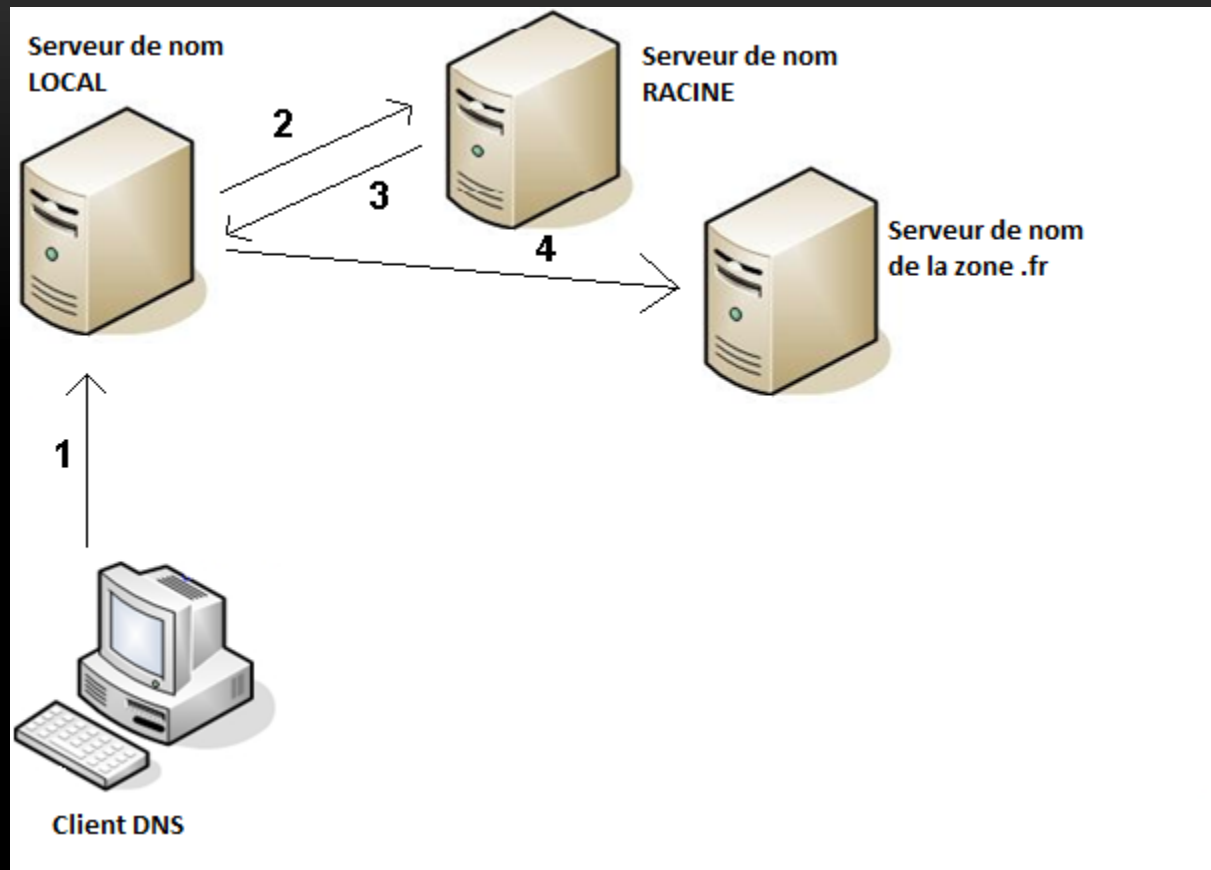
Pierre angulaire du système Internet mondial
Ils sont référencés par des lettres A, B

LOCALISATION

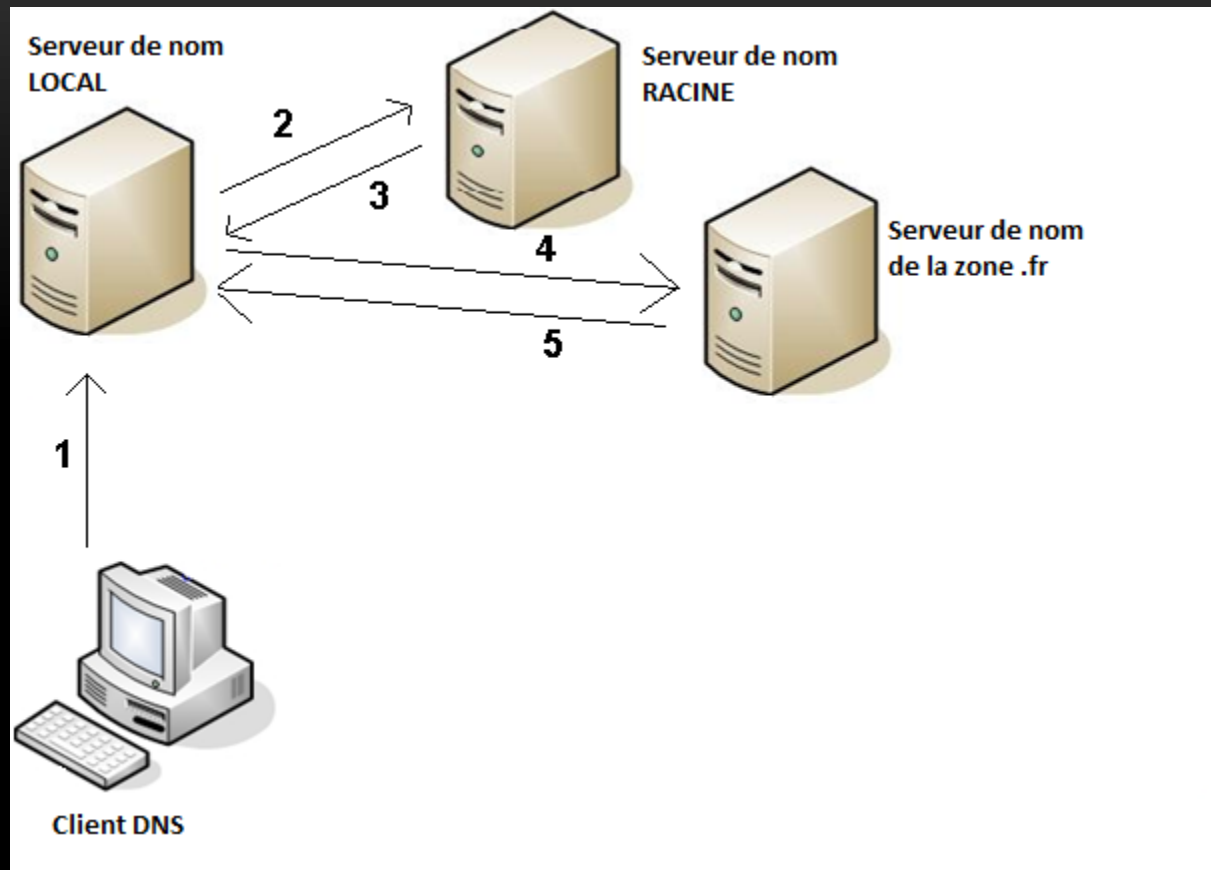
800px-Root-current.svg.png



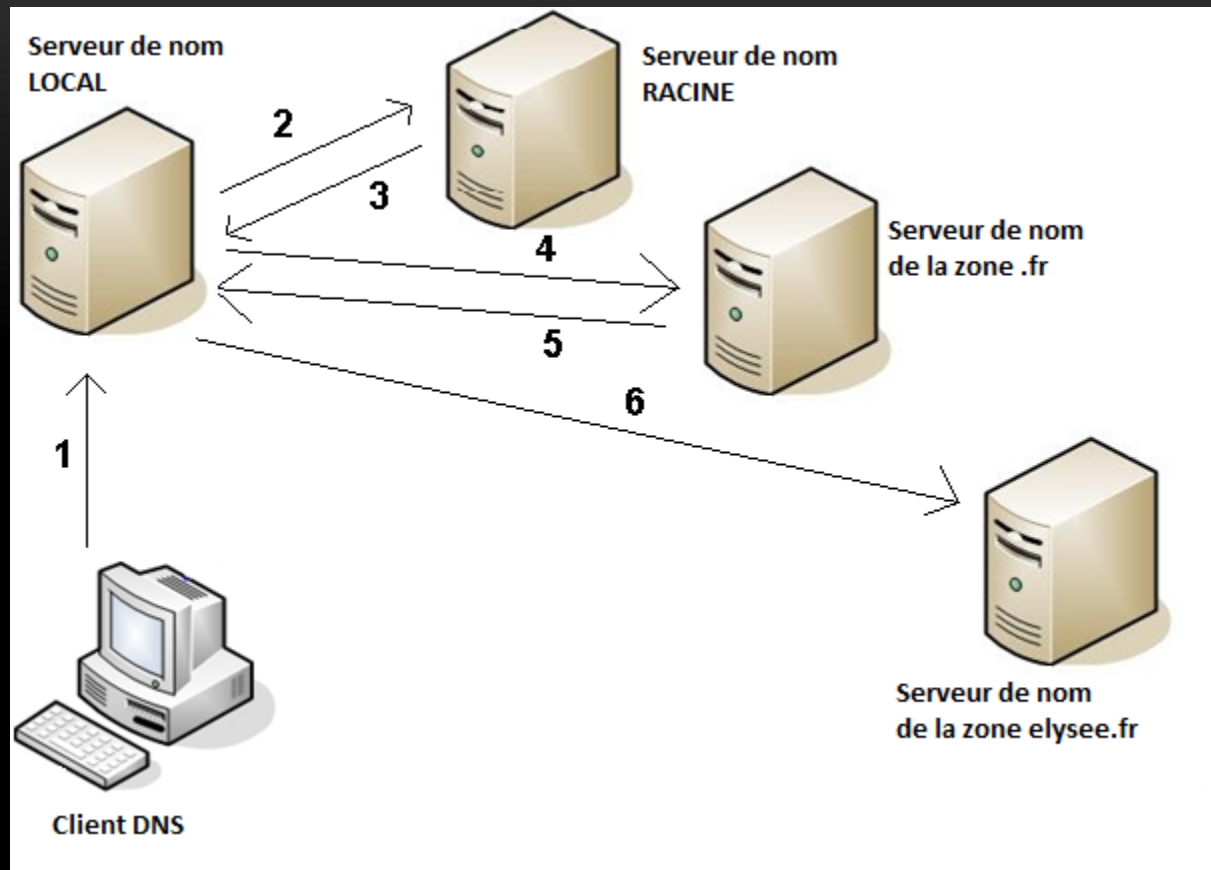
3. le serveur de nom racine va répondre en renvoyant l'adresse IP d'un serveur de nom desservant le domaine de niveau supérieur fr.



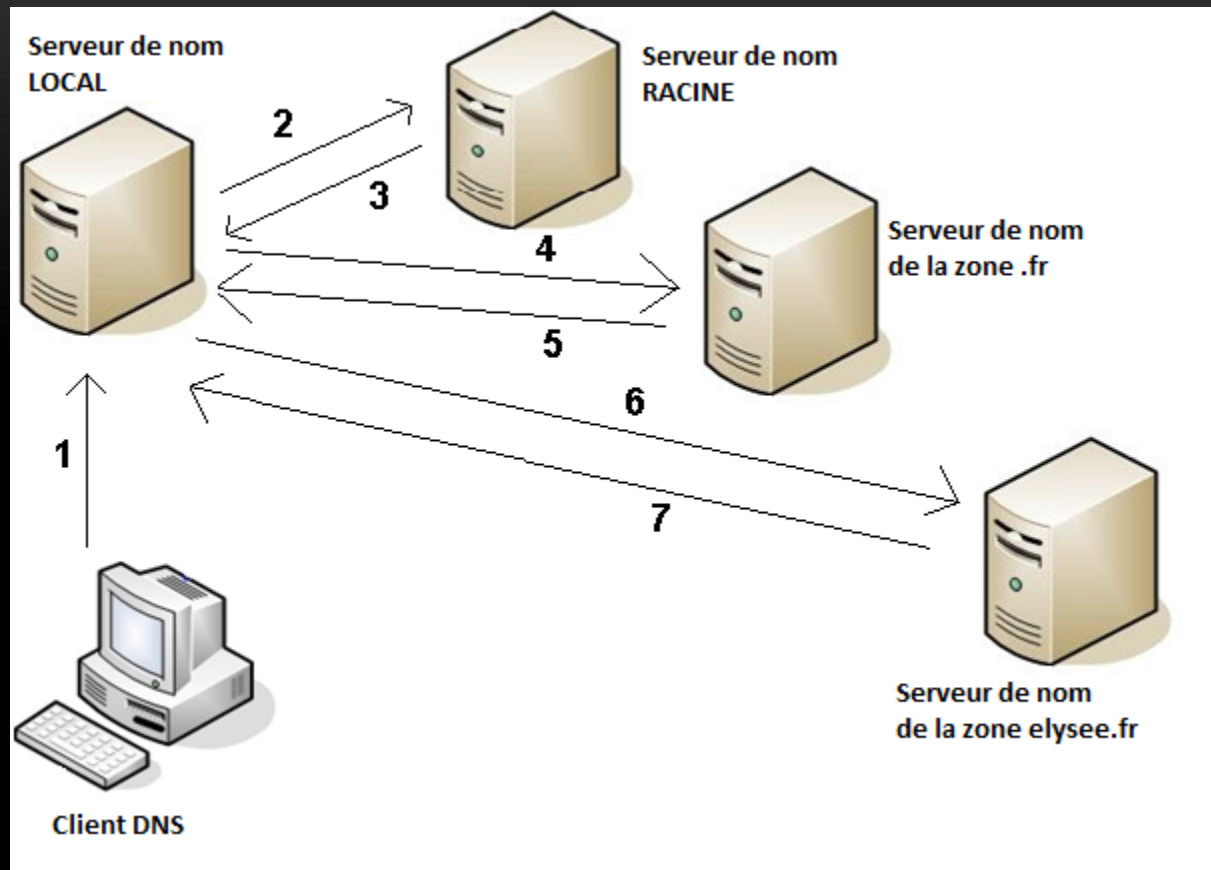
4. le serveur de nom local renvoie alors au serveur de nom gov une requête portant sur www.elysee.fr



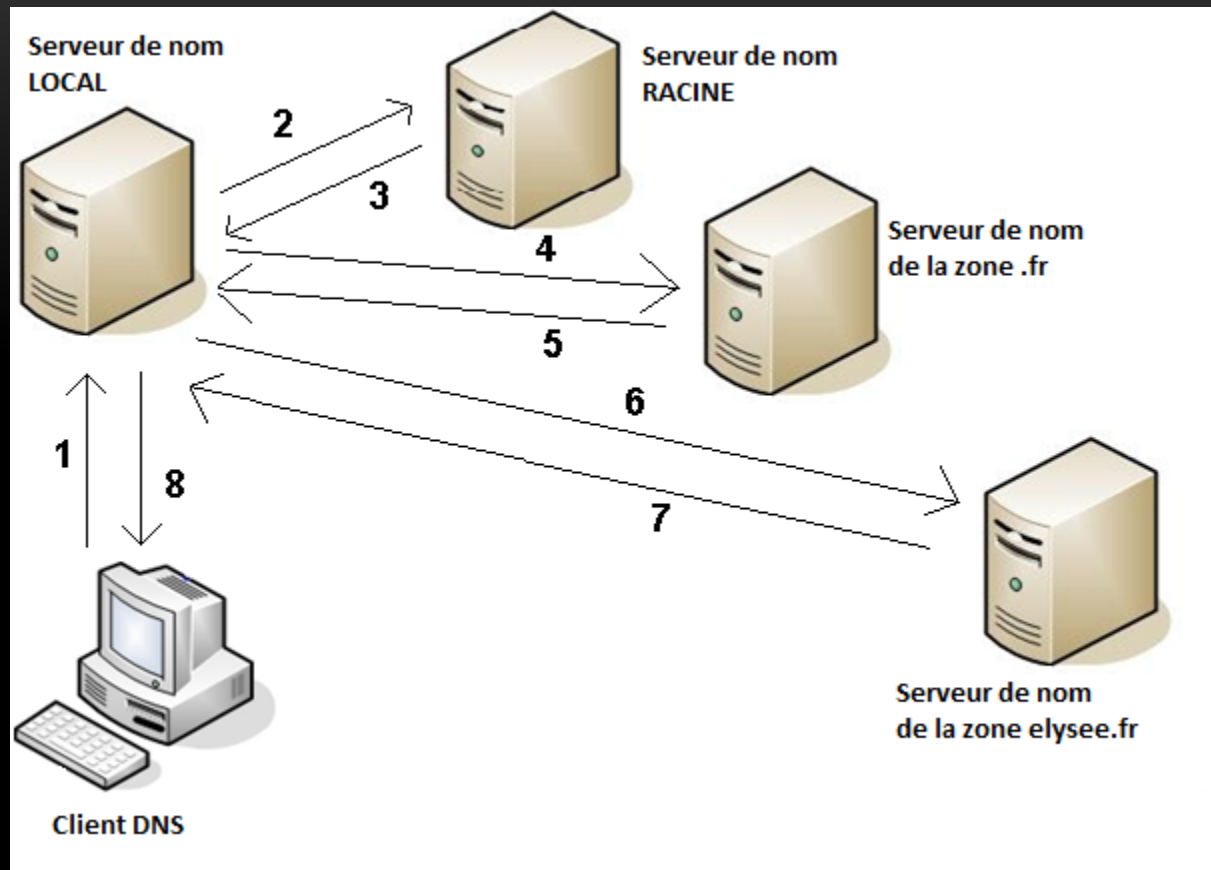
5. le serveur du nom du domaine fr répond en renvoyant l'adresse IP du serveur de noms desservant le domaine elysee.fr



6. le serveur local envoie au serveur de nom du domaine elysee.fr une requête www.elysee.fr

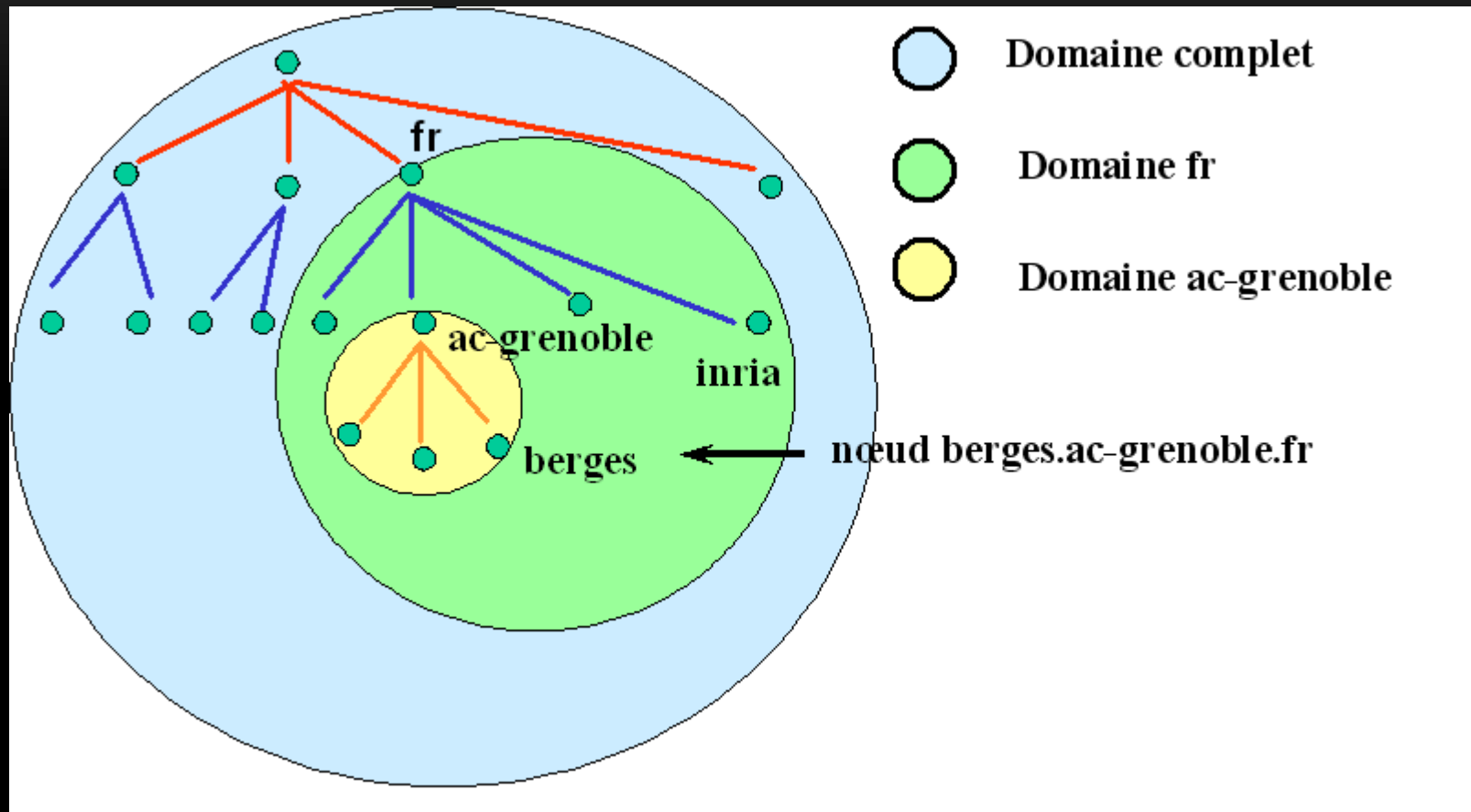


7. le serveur de nom du domaine elysee.fr répond en renvoyant l'adresse IP correspondant à www.elysee.fr



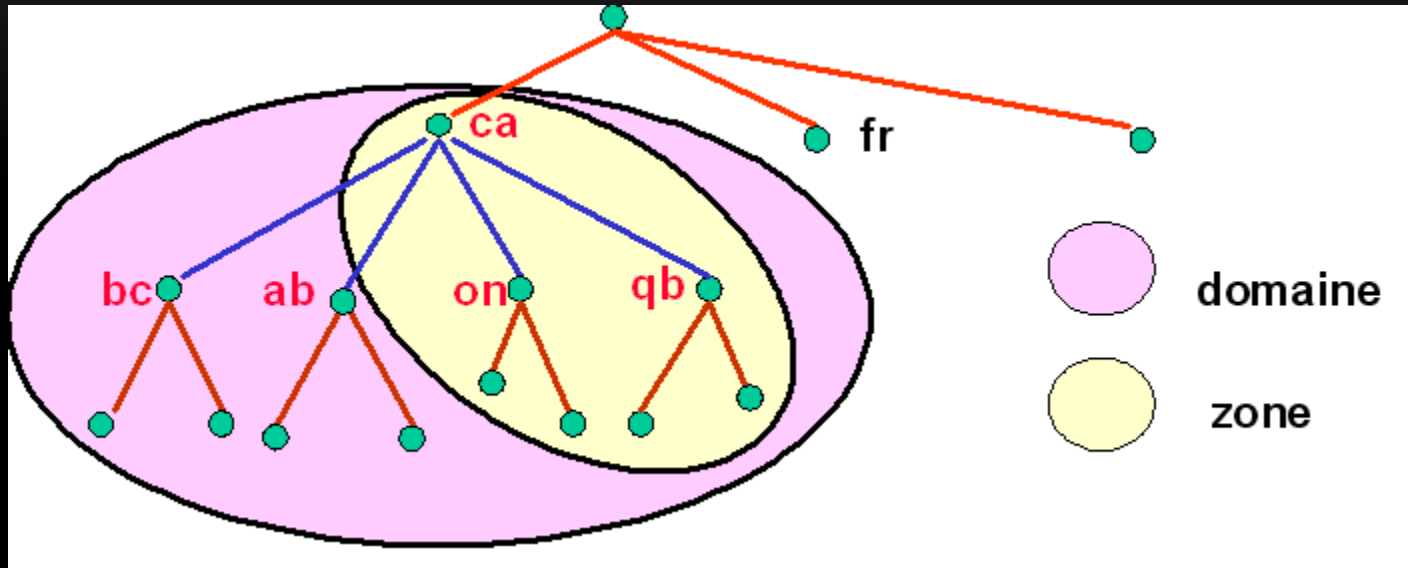
8. le serveur de nom local renvoie l'adresse IP de **www.elysee.fr** au client initial.

QU'EST-CE QU'UN DOMAINE ?



- Organisation de l'espace de nommage
- Peut être attaché à un domaine parent
- Et/ou peut avoir un ou plusieurs sous domaine enfant.

QU'EST-CE QU'UNE ZONE ?



Les zones correspondent à des organisations **logiques** (administratives) des domaines.

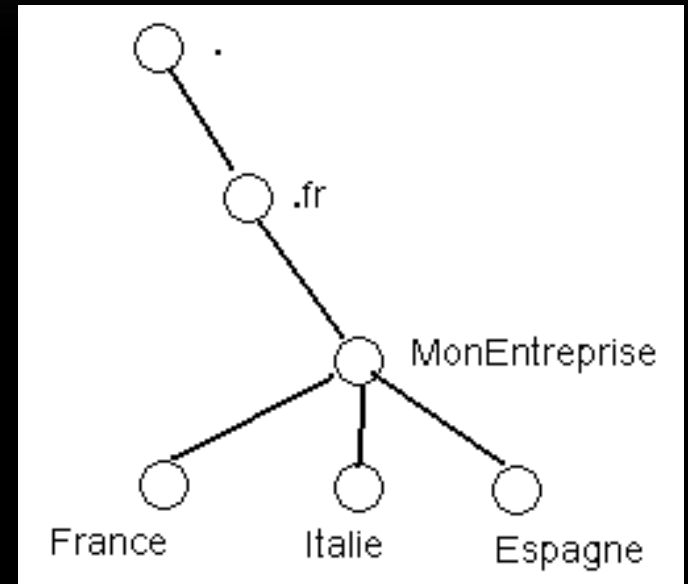
EXEMPLE

Domaine MonEntreprise.fr

- Membre de ".fr"

Trois sous domaines

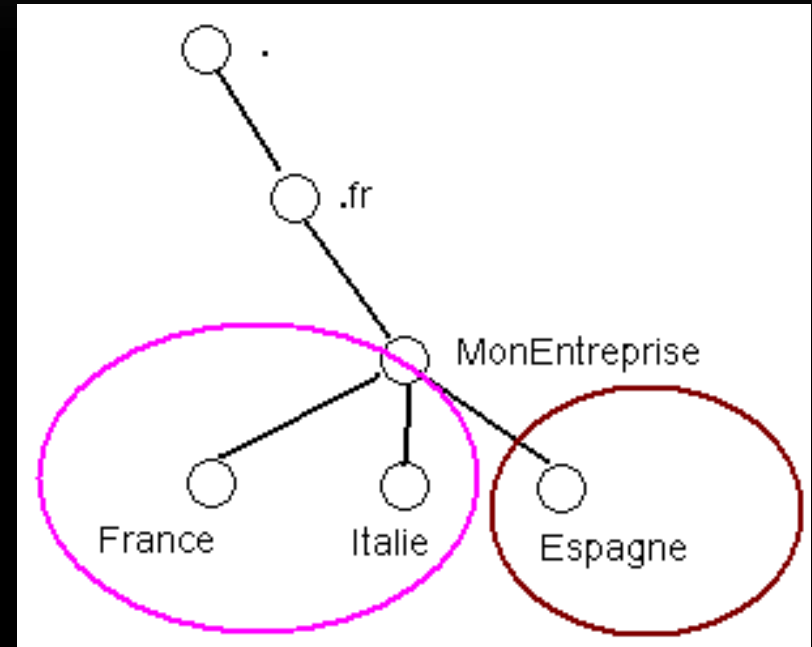
- France.MonEntreprise.fr
- Italie.MonEntreprise.fr
- Espagne.MonEntreprise.fr



EXEMPLE (SUITE)

Deux zones d'administration

- Une pour France.MonEntreprise.fr et Italie.MonEntreprise.fr
- Une pour Espagne.MonEntreprise.fr



LA RÉOLUTION DE NOM INVERSE

LA RÉOLUTION DE NOM INVERSE

- résolution de noms **directe** : un nom d'hôte est résolu en une adresse IP.
- résolution de noms **inverse** : processus inverse
 - Le processus doit fournir, pour une adresse IP, le nom correspondant.
 - Pour cela il y a une zone particulière, **in-addr.arpa**, qui permet la résolution inverse d'adresse IP.

LE DOMAINE IN-ADDR.ARPA

- Un serveur de noms peut, pratiquement, fonctionner sans la définition de cette zone tant que le réseau n'est pas relié à l'internet.
- Cependant certains utilitaires, certaines applications, des services comme la messagerie électronique, notamment à causes des règles anti-spam ont besoin d'une zone de recherche inversée pour pouvoir fonctionner correctement.
- Il faut donc prendre l'habitude de les créer.

LES SERVEURS DE NOMS

LES SERVEURS DE NOM

- Les logiciels qui gèrent les données de l'espace de noms de domaine sont appelés des **serveurs de nom** (*name servers - NS*)
- Les serveurs de noms enregistrent les données propres à une partie de l'espace de noms de domaine dans une **ZONE**.
- Le serveur de noms a autorité administrative sur cette zone.

LES SERVEURS DE NOM

- Serveur de noms primaire :

Il maintient la base de données de la zone dont il a l'autorité administrative.

LES SERVEURS DE NOMS

- Serveur de noms secondaire :
- Il obtient les données de la zone via un autre serveur de noms qui a l'autorité administrative.
- Il interroge périodiquement le serveur de nom primaire et met à jour les données.

LES SERVEURS DE NOMS

- Serveur de noms secondaire :
- Il y a un serveur primaire et généralement plusieurs secondaires.
- La redondance permet la défaillance éventuelle du primaire et du (des) secondaire(s).
- La redondance permet également la répartition de charge

- serveur cache
- Ni serveur primaire, ni serveur secondaire.
- aucune autorité et ne fait aucun transfert de zone.
- met en cache les résolutions de noms qu'il effectue en transmettant des requêtes à d'autres serveurs de noms.
- il ne contient donc que les informations qu'il a placées en cache après ses résolutions.
- son intérêt est d'éviter le transfert de zone

LE FICHER DE ZONE

LE FICHER DE ZONE DIRECTE

```
;
; Database file bisson.org.dns for bisson.org zone.
;   Zone version: 39
;
@           IN SOA dns1.bisson.org. hostmaster.bisson.org.
(
    39      ; serial number
    900     ; refresh
    600     ; retry
    86400   ; expire
    3600    ) ; default TTL
```

SOA : start of authority
décrit la zone et les mécanisme de transfert

```
;
; Database file bisson.org.dns for bisson.org zone.
;   Zone version: 39
;
@      IN SOA dns1.bisson.org. hostmaster.bisson.org.
(
    39      ; serial number
    900     ; refresh
    600     ; retry
    86400   ; expire
    3600    ) ; default TTL
```

Identification du serveur de nom primaire

```
;
; Database file bisson.org.dns for bisson.org zone.
;   Zone version: 39
;
@      IN SOA dns1.bisson.org. hostmaster.bisson.org.
(
    39      ; serial number
    900     ; refresh
    600     ; retry
    86400   ; expire
    3600    ) ; default TTL
```

Adresse mel de la personne gérant la zone

```
;
; Database file bisson.org.dns for bisson.org zone.
;   Zone version: 39
;
@           IN SOA dns1.bisson.org. hostmaster.bisson.org.
(
    39      ; serial number
    900     ; refresh
    600     ; retry
    86400   ; expire
    3600    ) ; default TTL
```

Définition des mécanismes de transfert et numéro de série

```
;
; Database file bisson.org.dns for bisson.org zone.
;   Zone version: 39
;
@           IN SOA dns1.bisson.org. hostmaster.bisson.org.
(
  39          ; serial number
  900        ; refresh
  600        ; retry
  86400      ; expire
  3600      ) ; default TTL
```

Intervalle d'actualisation (en secondes)

```
;
; Database file bisson.org.dns for bisson.org zone.
;   Zone version: 39
;
@           IN SOA dns1.bisson.org. hostmaster.bisson.org.
(
    39      ; serial number
    900     ; refresh
    600     ; retry
    86400   ; expire
    3600    ) ; default TTL
```

Adresse mel de la personne gérant la zone

```
;
; Database file bisson.org.dns for bisson.org zone.
;   Zone version: 39
;
@      IN SOA dns1.bisson.org. hostmaster.bisson.org.
(
    39      ; serial number
    900     ; refresh
    600     ; retry
    86400   ; expire
    3600    ) ; default TTL
```

Intervalle avant nouvelle tentative

```
;
; Database file bisson.org.dns for bisson.org zone.
;   Zone version: 39
;
@           IN SOA dns1.bisson.org. hostmaster.bisson.org.
(
    39      ; serial number
    900     ; refresh
    600     ; retry
    86400   ; expire
    3600    ) ; default TTL
```


Expire après : si le serveur n'a pas pu actualiser son fichier, il ne répond plus

```
;
; Database file bisson.org.dns for bisson.org zone.
;   Zone version: 39
;
@           IN SOA dns1.bisson.org. hostmaster.bisson.org.
(
    39      ; serial number
    900     ; refresh
    600     ; retry
    86400   ; expire
    3600    ) ; default TTL
```

Temps minimal de durée de durée de vie de l'information dans le cache du client

```
;
; Database file bisson.org.dns for bisson.org zone.
;   Zone version: 39
;
@           IN SOA dns1.bisson.org. hostmaster.bisson.org.
(
    39      ; serial number
    900     ; refresh
    600     ; retry
    86400   ; expire
    3600   ) ; default TTL
```

```
;  
;  
; Zone NS records  
;  
@ NS dns1.bisson.org.  
@ NS dns2.bisson.org.  
;  
;  
; Zone records  
;  
;
```

dns1	A	192.168.0.201
dns2.bisson.org	A	192.168.0.202
moi	A	192.168.0.55
toi	A	192.168.0.56
www	CNAME	Exp02.bisson.org.
xp01	A	192.168.0.101
xp02	A	192.168.0.102

LE FICHER DE ZONE INVERSE

; Database file 0.168.192.in-addr.arpa.dns for 0.168.192.in-addr.arpa zone.

; Zone version: 11

; @ IN SOA dns1.bisson.org hostmaster.bisson.org. (
11 ; serial number
900 ; refresh
600 ; retry
86400 ; expire
3600) ; default TTL

; Zone NS records

; @ NS dns1.bisson.org.

; Zone records

101 PTR xp01.bisson.org.

201 PTR dns1.bisson.org.