INSA | INSTITUT NATIONAL DES SCIENCES APPLIQUÉES CENTRE VAL DE LOIRE

Module : Réseaux

DNS : Domain Name System

INSA-CVL 4ème année
Département STI Promo 2022

Année 2020-2021

M. SZPIEG

DNS : Domain Name System

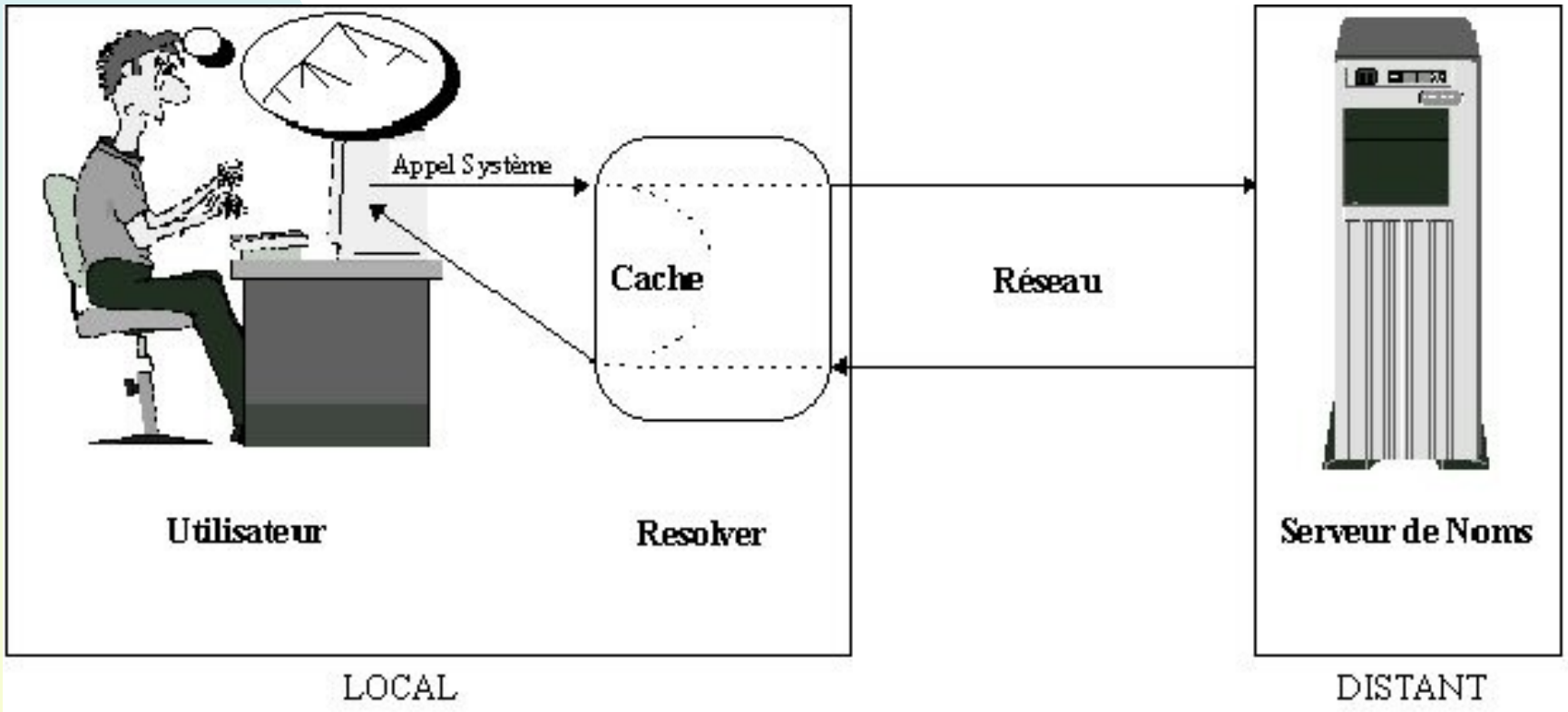
Sur Internet l'adressage se fait à l'aide d'un nombre sur 32 bits en IPv4 (Notation décimale pointée : Dotted Decimal Notation).
Ce type de notation est difficilement mémorisable pour un être humain, aussi l'emploi de nom tel que «www.insa-cvl.fr» a été mis au point.

Le nom « www.insa-cvl.fr. » est dit FQDN (Fully Qualified Domain Name).

Il est composé d'un nom de machine « www » ou « celene » complété par un nom de domaine « insa-cvl.fr. »

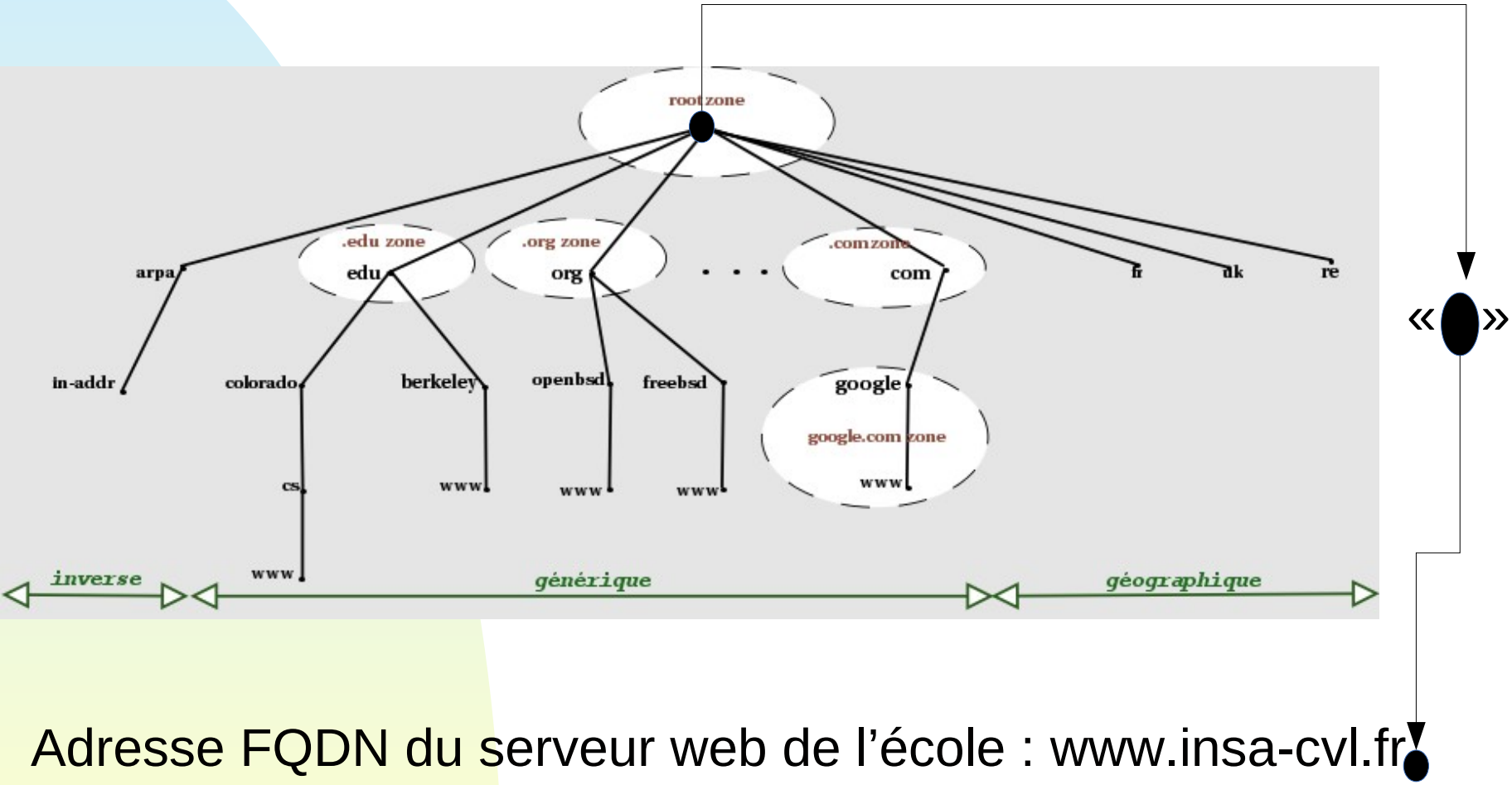
Il s'agit donc pour le système de retrouver l'adresse IP à partir de ce nom «résolution de noms». On parle aussi de «resolver» ou de « solveur » de noms.

DNS : Domain Name System



Distribution du nom par autorités

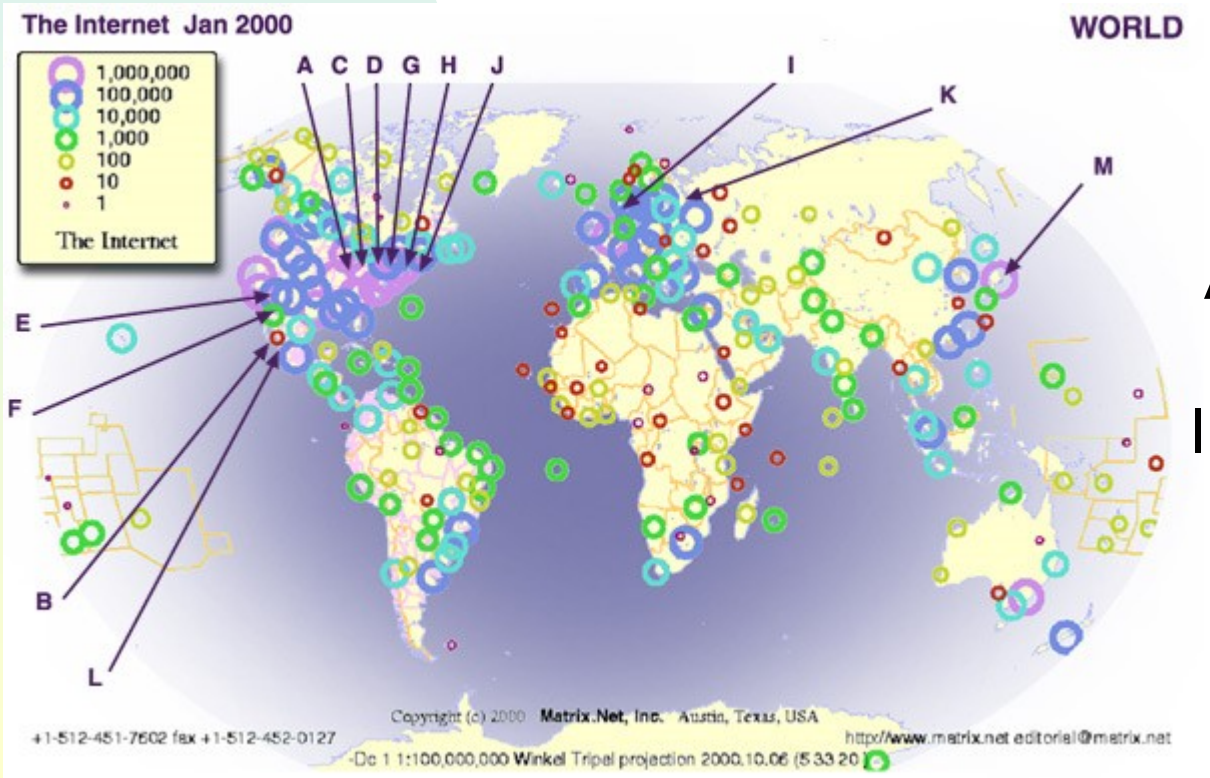
Racine de l'arborescence « root », définie par un point



Adresse FQDN du serveur web de l'école : www.insa-cvl.fr.

Les serveurs root

La **racine** (**root**), symbolisée par un « . », contient les références de tous les serveurs de domaines de niveau zéro.
Elle est constituée par 13 serveurs répartis dans le monde et qui, par un système de réplication, contiennent la même information.



Source www.afnic.fr
Association Française pour le Nommage Internet en Coopération

Les serveurs root

Les serveurs root sont identifiés par les lettres de A à M et appartiennent tous au domaine ROOT-SERVERS.NET.
Le serveur d'origine est géré par VeriSign Global Registry Services (A.ROOT-SERVERS.NET).

Les autres serveurs sont des serveurs miroirs et sont administrés par :

B.ROOT-SERVERS.NET : Information Sciences Institute USC (USA)
C.ROOT-SERVERS.NET : PSINet
D.ROOT-SERVERS.NET : University of Maryland (USA)
E.ROOT-SERVERS.NET : NASA Ames Research Center (USA)
F.ROOT-SERVERS.NET : Internet Software Consortium (USA)
G.ROOT-SERVERS.NET : U.S. DOD Network Information Center (USA) H.ROOT-SERVERS.NET : U.S. Army Research Lab (USA)
I.ROOT-SERVERS.NET : NordU (Suède)
J.ROOT-SERVERS.NET : VeriSign Global Registry Services (USA)
K.ROOT-SERVERS.NET : RIPE NCC (UK, Europe)
L.ROOT-SERVERS.NET : ICANN (USA)
M.ROOT-SERVERS.NET : WIDE Project (Japon).

Le nommage DNS

- Les noms d'hôtes sont classés en une hiérarchie de domaines.

Un domaine est un ensemble de sites qui ont une relation entre eux.

- Exemple : edu aux USA regroupe les universités de ce pays, dans les autres pays les sites sont regroupés sous un label constitué des deux lettres du code pays ISO-3166, fr France, de Allemagne etc..

- Il existe des domaines plus spécifiques. Exemple serveur dns : dns.google. Avec un domaine spécifique à « google ».

Autres domaines : garden ; arte ; etc.

Exemple : dns1.nic.garden.

Consultez : https://www.iana.org./domains/root/db

- Puis on crée des sous-domaines pour définir un peu plus précisément l'organisation

Exemples : insa-cvl.fr. ou bourges.univ-orleans.fr.

- Cette hiérarchie définit des domaines de niveau 0,1,2,3…

DNS : les Top-Level Domain TLD

Il existe deux types de domaines principaux **TLD** de premier niveau :

• Les **ccTLD** (**c**ountry-**c**ode **TLD**)
Domaines géographiques (ISO 3166) fr ; ch ; DE ; US ; etc.

• Les **gTLD** (**g**eneric **TLD**)
Domaines génériques COM: Entreprises commerciales,
edu: Établissements d'éducation,
gov: Établissements gouvernementaux américains
arte :Association Relative à la Télévision Européenne G.E.I.E.

Adresse utile : https://www.iana.org/domains/root/db

Jusqu'en 1998, la délégation de gestion d'un TLD était du ressort de l'IANA (Internet Assigned Numbers Authority).
Actuellement c'est l'ICANN (Internet Corporation for Assigned Names and Numbers).

« Top-Level Domain » particulier

Parmi les gTLD, le domaine **arpa*** (**A**ddress and **R**outing **P**arameter **A**rea), est un TLD codé sur 4 lettres et dont l'utilisation est définie dans la **RFC 3172**.

L'utilisation principale de ce domaine est la résolution inverse (adresse ip vers fqdn) .

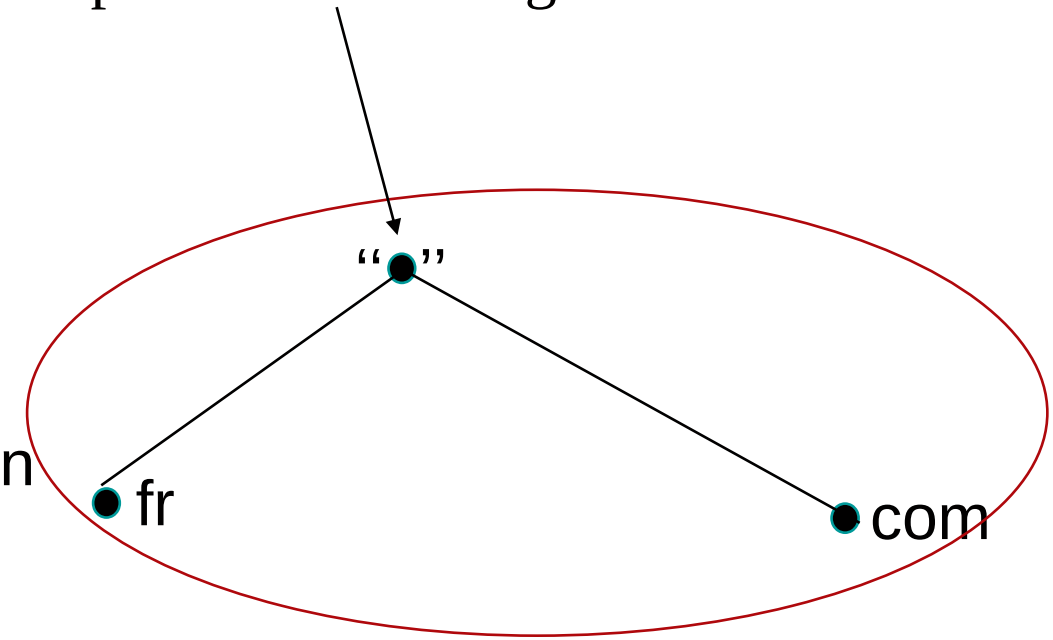
*Attention : La signification première de « **ARPA** » est **Advanced Research Project Agency**.

Distribution du nom par autorités

Géré par ICANN Internet Corporation for AssignedNames and Numbers

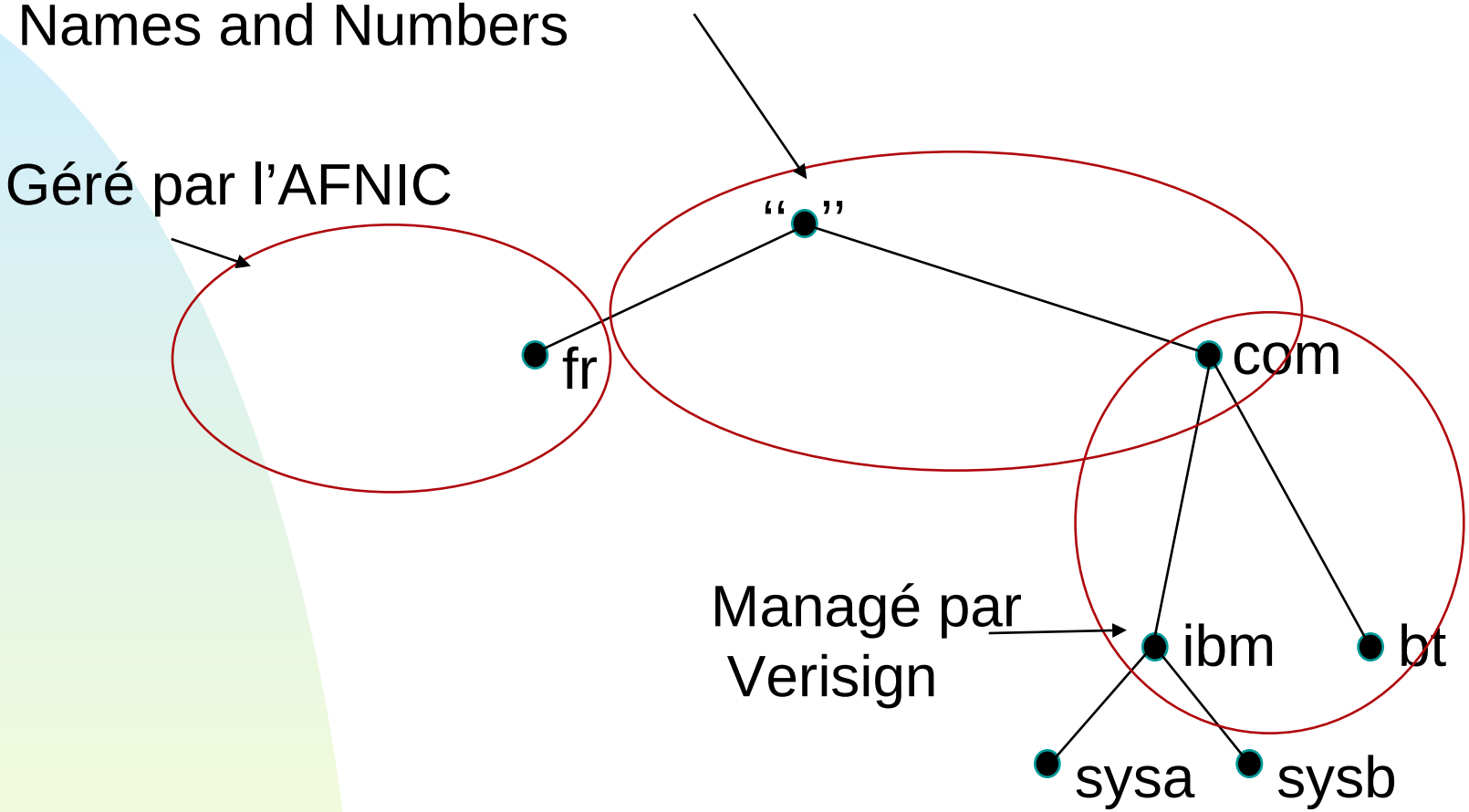
Racine
Niveau 0

Top Level Domain
Niveau 1



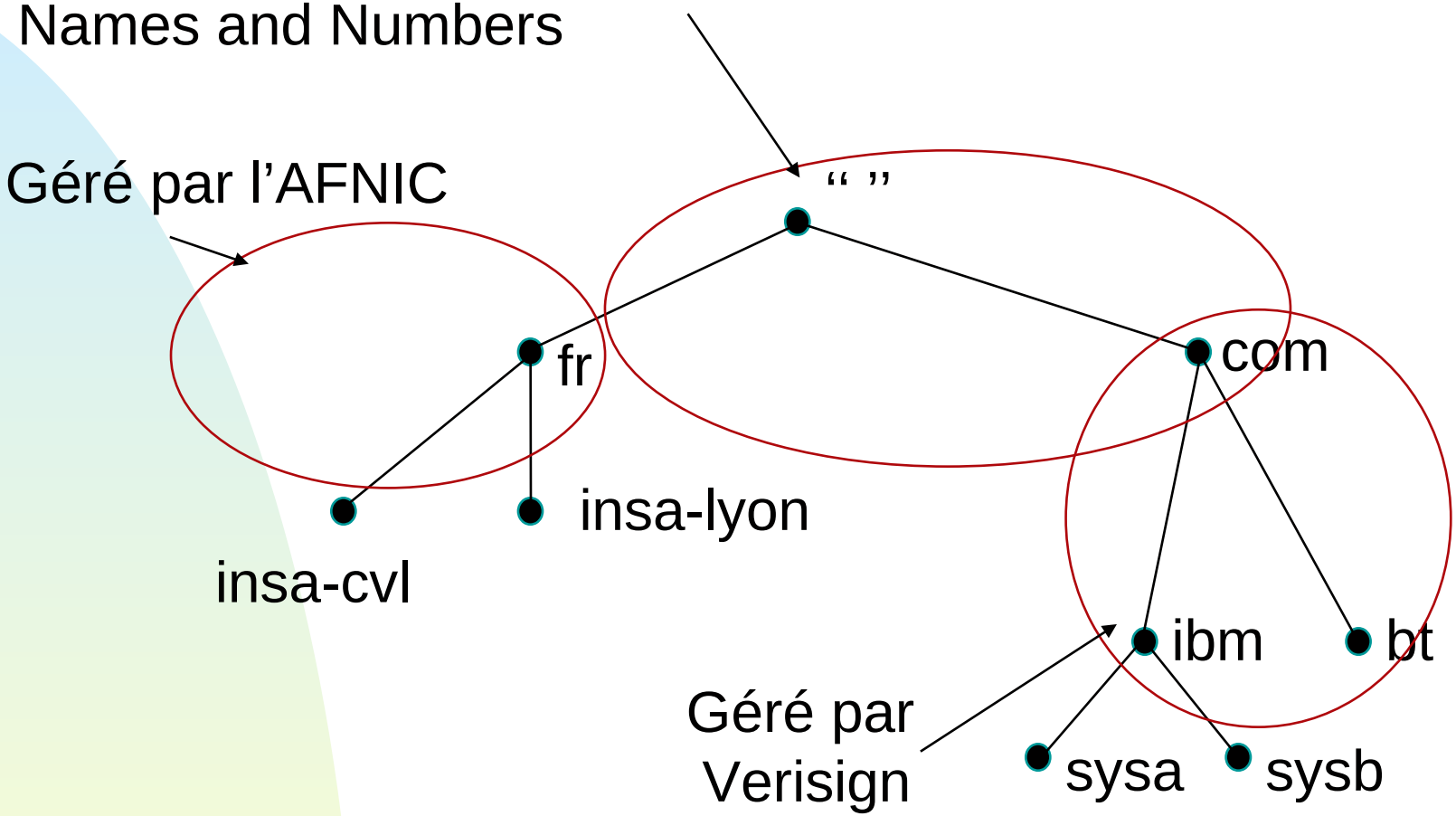
Distribution du nom par autorités

Géré par ICANN Internet Corporation for Assigned Names and Numbers



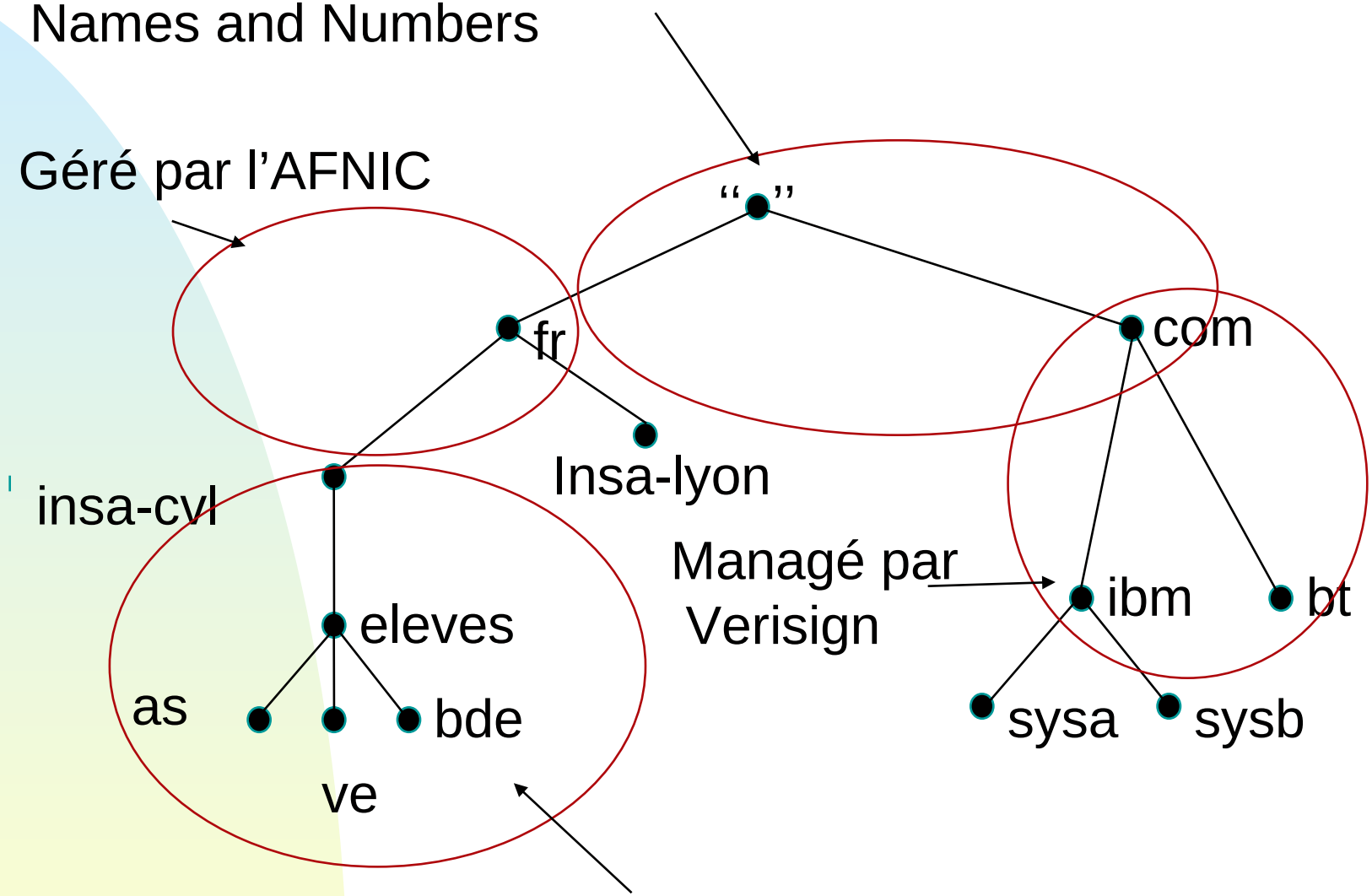
Distribution du nom par autorités

Géré par ICANN Internet Corporation for Assigned Names and Numbers



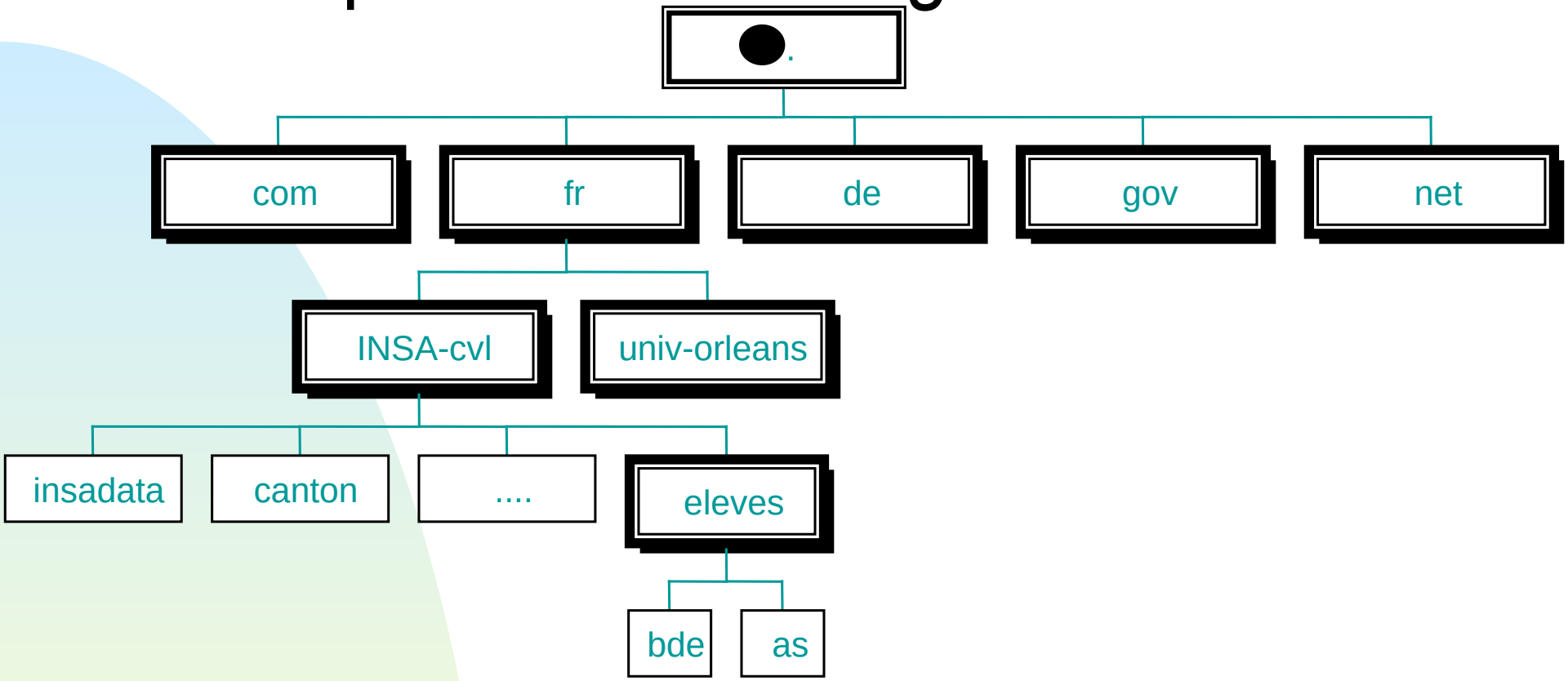
Distribution du nom par autorités

Géré par ICANN Internet Corporation for Assigned Names and Numbers



En pratique l'arborescence n'est pas aussi simple (voir td)

Extrait espace de nommage



Un domaine est constitué par toutes les machines qui ont un même suffixe DNS.

Exemples : xxxx.insa-cvl***.fr.***, yyyy.***bde.insa-cvl.fr.*** **,** www.***univ-orleans.fr*** noms de domaines parties soulignées.

Domaine et zone (différence subtile)

Pour être administré, un domaine peut-être découpé en zones, un serveur DNS différent s'occupant de chacune des zones. (Schéma diapo suivante)

L'école décide de faire une « délégation de la zone » « eleves.insa-cvl.fr » aux élèves de l'école.

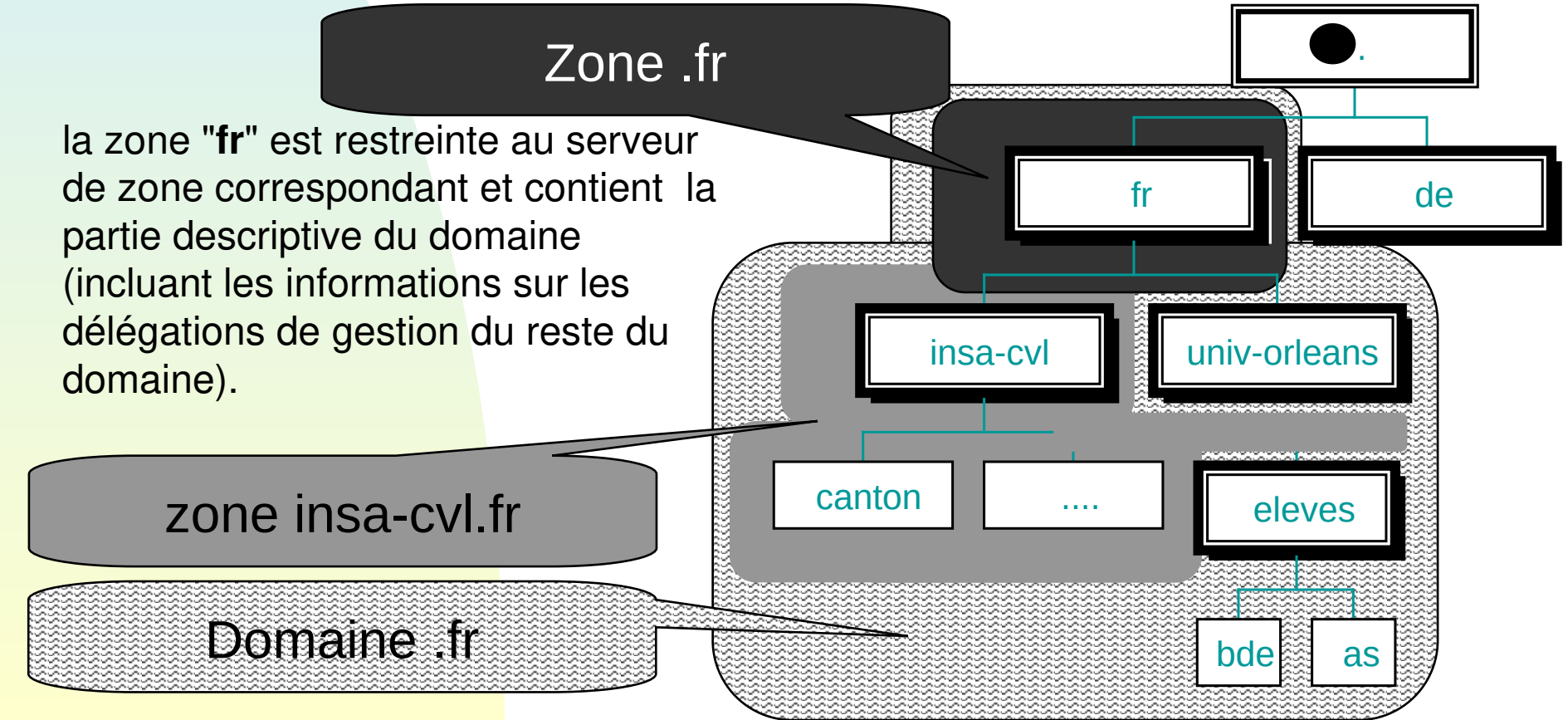
Le **domaine** « insa-cvl.fr » contient toutes les machines de l'INSA CVL.

La **zone** « insa-cvl.fr » contient les machines « insadata » « canton » … mais pas « bde » et « as ».

La zone « eleves.insa-cvl.fr contient « bde » et « as ».
« eleve.insa-cvl.fr » est aussi un domaine.

Domaine et zone

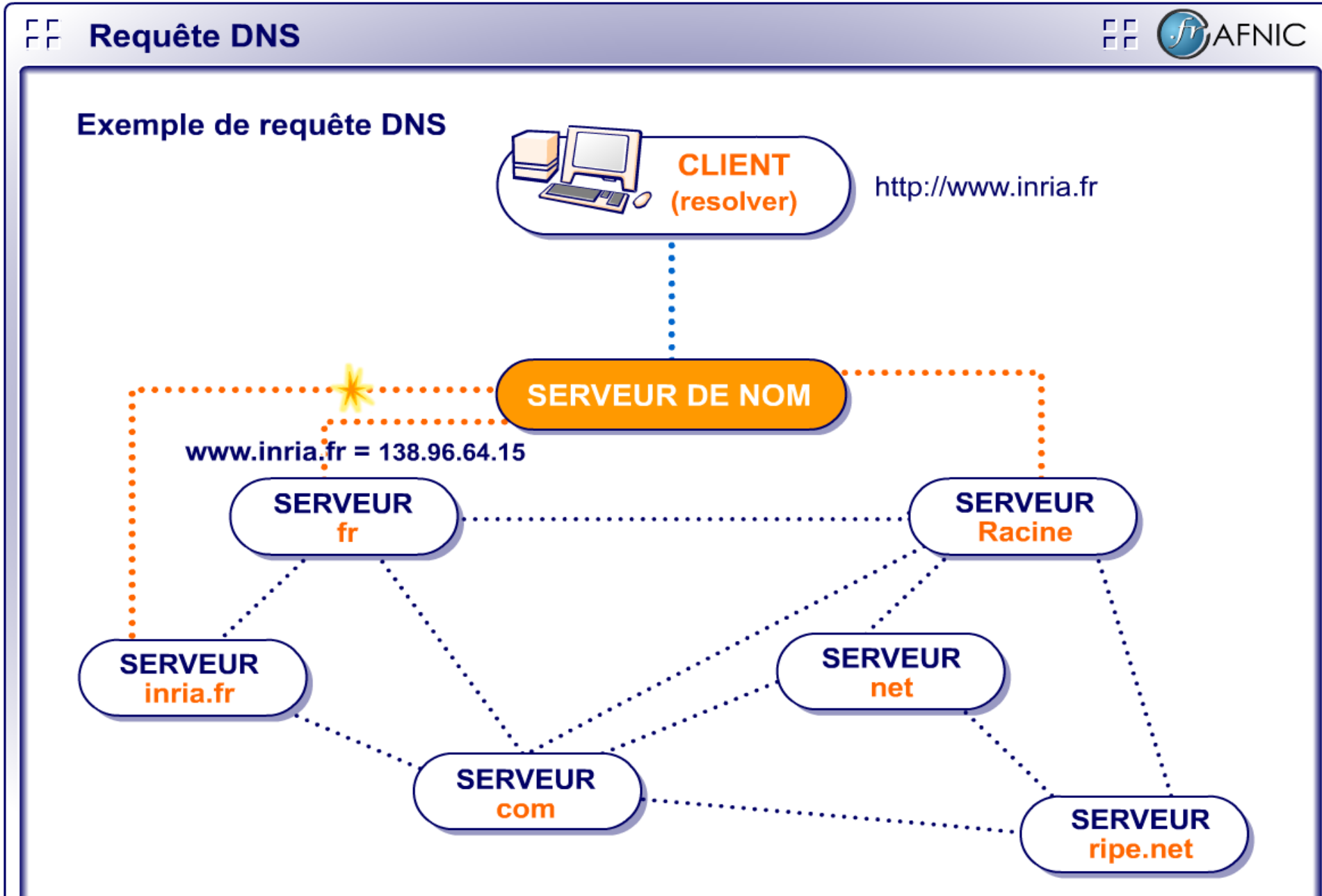
Un domaine représente l'ensemble d'une sous-arborescence à partir d'un nœud donné.
Une zone peut correspondre à un domaine, mais dans le cas général, elle englobe uniquement une partie du domaine, le reste étant délégué à d'autres serveurs de noms.



Interrogation serveurs de noms

- Pour une zone on définit généralement au moins deux serveurs de noms (pour la redondance, un maître et un esclave)
- On dit que ces serveurs ont autorité sur la zone. On parle de serveurs « autoritatifs » ou « autoritaires »
- L'un des serveurs est désigné comme maître et il y a périodiquement échange d'informations entre le serveur maître et le(s) serveur(s) esclave(s) pour une synchronisation.
- Un serveur peut gérer plusieurs zones de domaines qui peuvent être différents. Exemple : insa-cvl.fr et insa-cvl.eu
- Pour obtenir le numéro IP de bde.insa-cvl.fr, un hôte réalisera les opérations suivantes (si /etc/hosts, Wins et NIS non utilisés):
  - Envoyer sa requête à un serveur DNS
  - Si celui-ci ne connaît pas la réponse, il contacte un serveur DNS racine.
  - Puis on redescend dans la hiérarchie jusqu'à obtenir l'information désirée.

Interrogation serveurs de noms



Interrogation des serveurs de noms

- **Modes itératif, récursif**

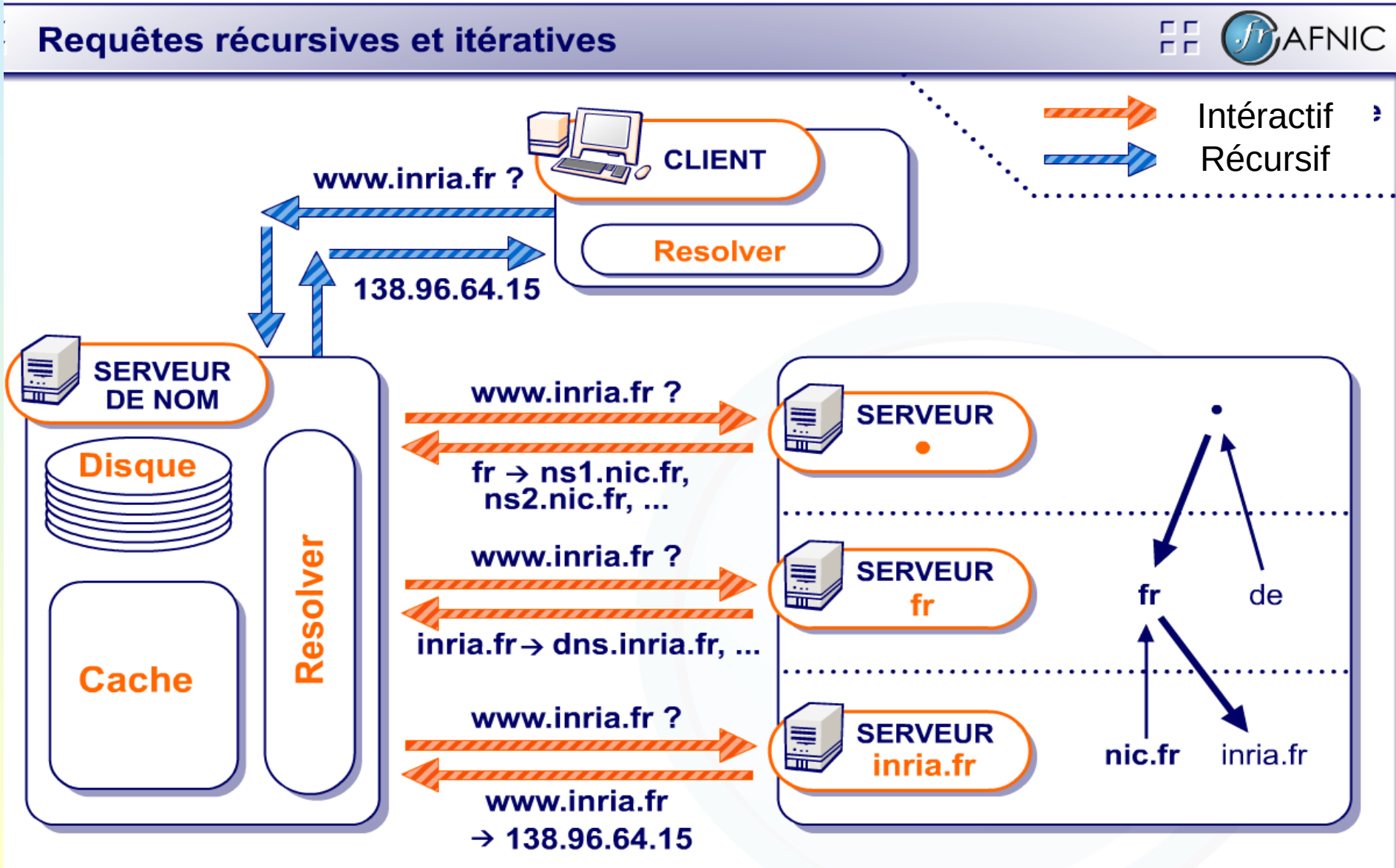
Il existe deux modes d'interrogation des serveurs.
En mode récursif, le serveur interrogé prend en charge les appels (récursifs ou itératifs) à d'autres serveurs nécessaires pour résoudre la recherche.

En mode itératif, il fournit l'information la plus détaillée dont il dispose, le programme client prenant en charge l'appel à d'autres serveurs. Un serveur de noms peut refuser d'honorer les requêtes récursives. C'est le cas des serveurs de premier niveau très sollicités.

Utilisation de caches
(noms de machines récemment utilisés et numéros IP correspondant) : lorsqu'un client demande un nom, le serveur vérifie au préalable que celui-ci n'est pas dans la mémoire cache.

Interrogation serveurs de noms

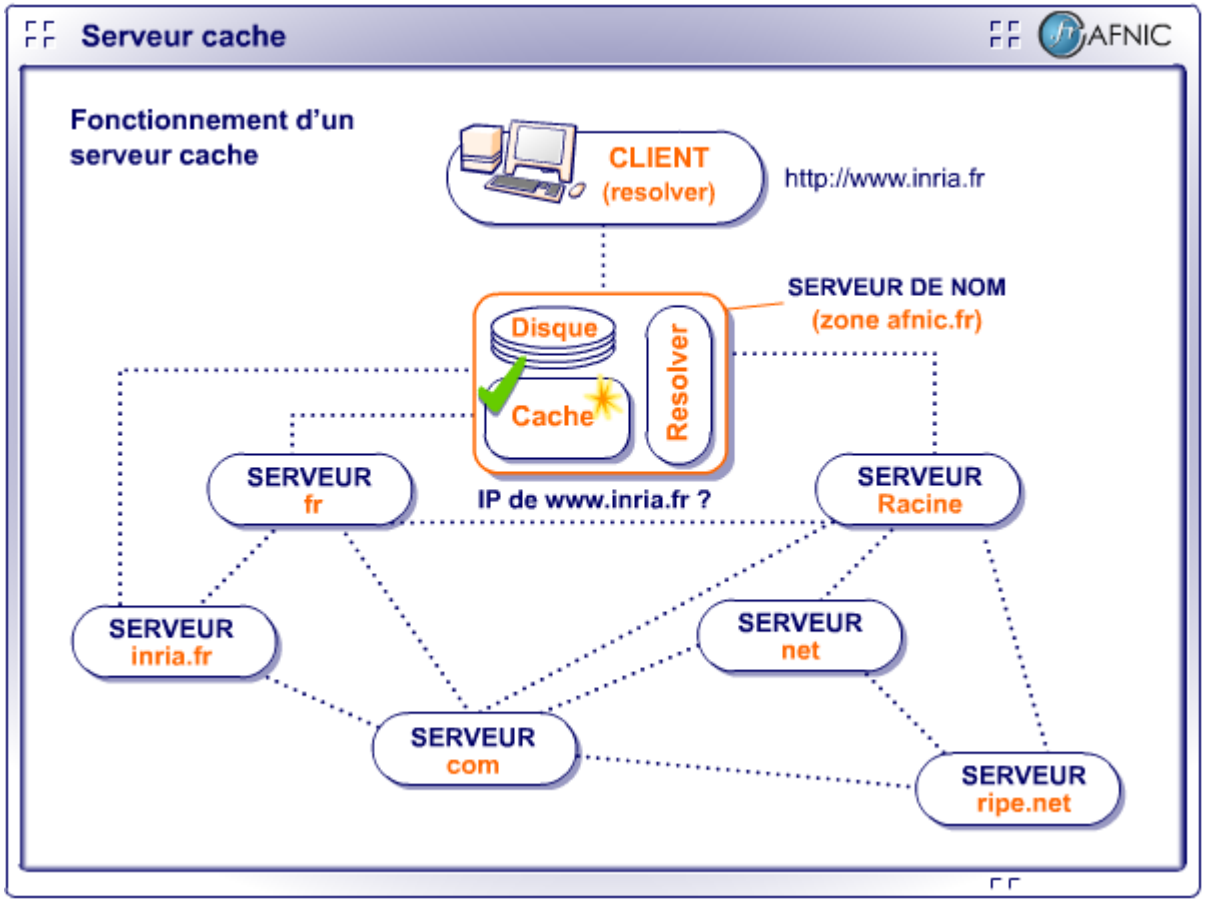
Modes itératif, récursif



Interrogation des serveurs de noms

- **Utilisation de caches**

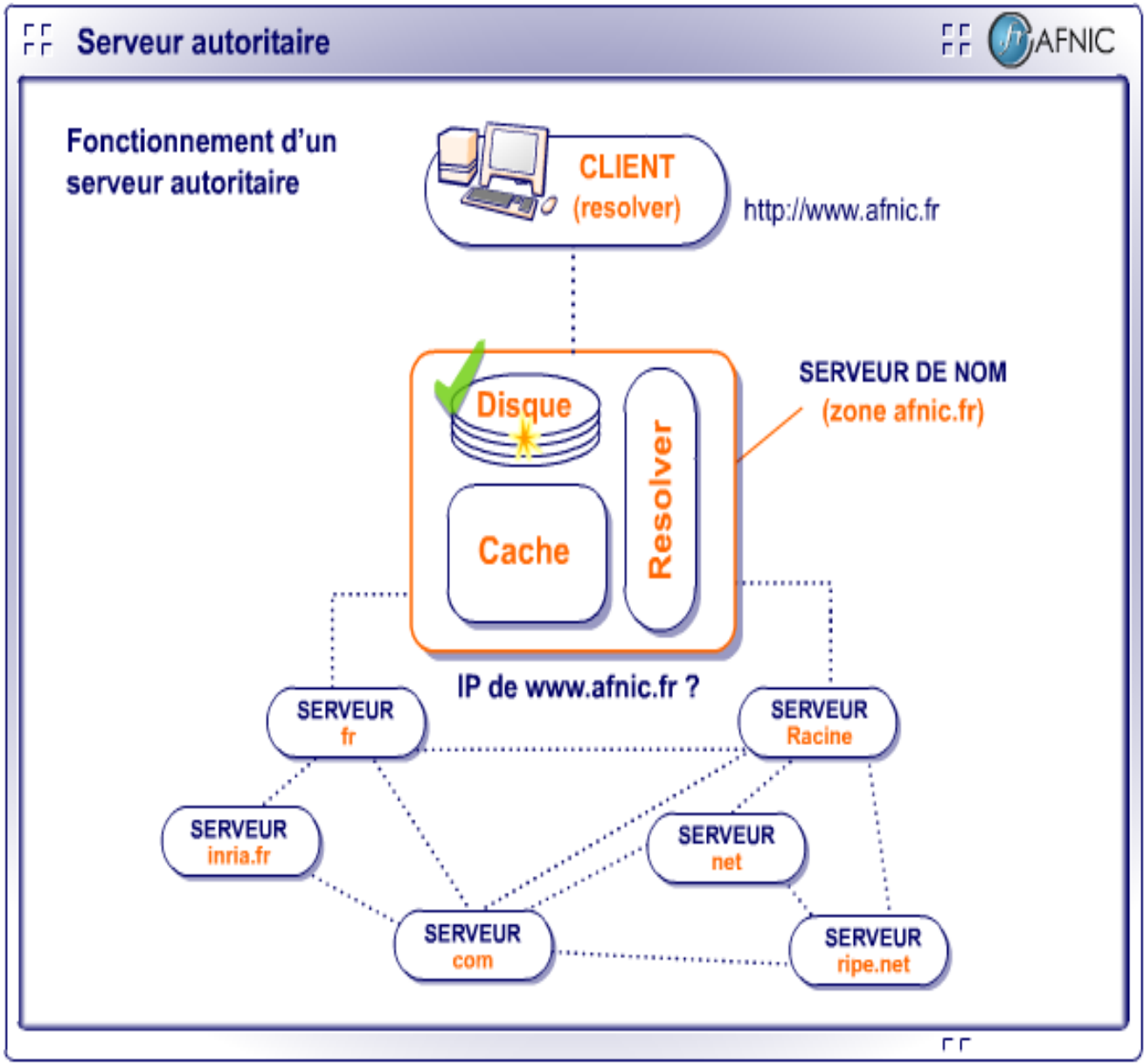
  (noms de machines récemment utilisés et numéros IP correspondant) : lorsqu'un client demande un nom, le serveur vérifie au préalable que celui-ci n'est pas dans la mémoire cache.



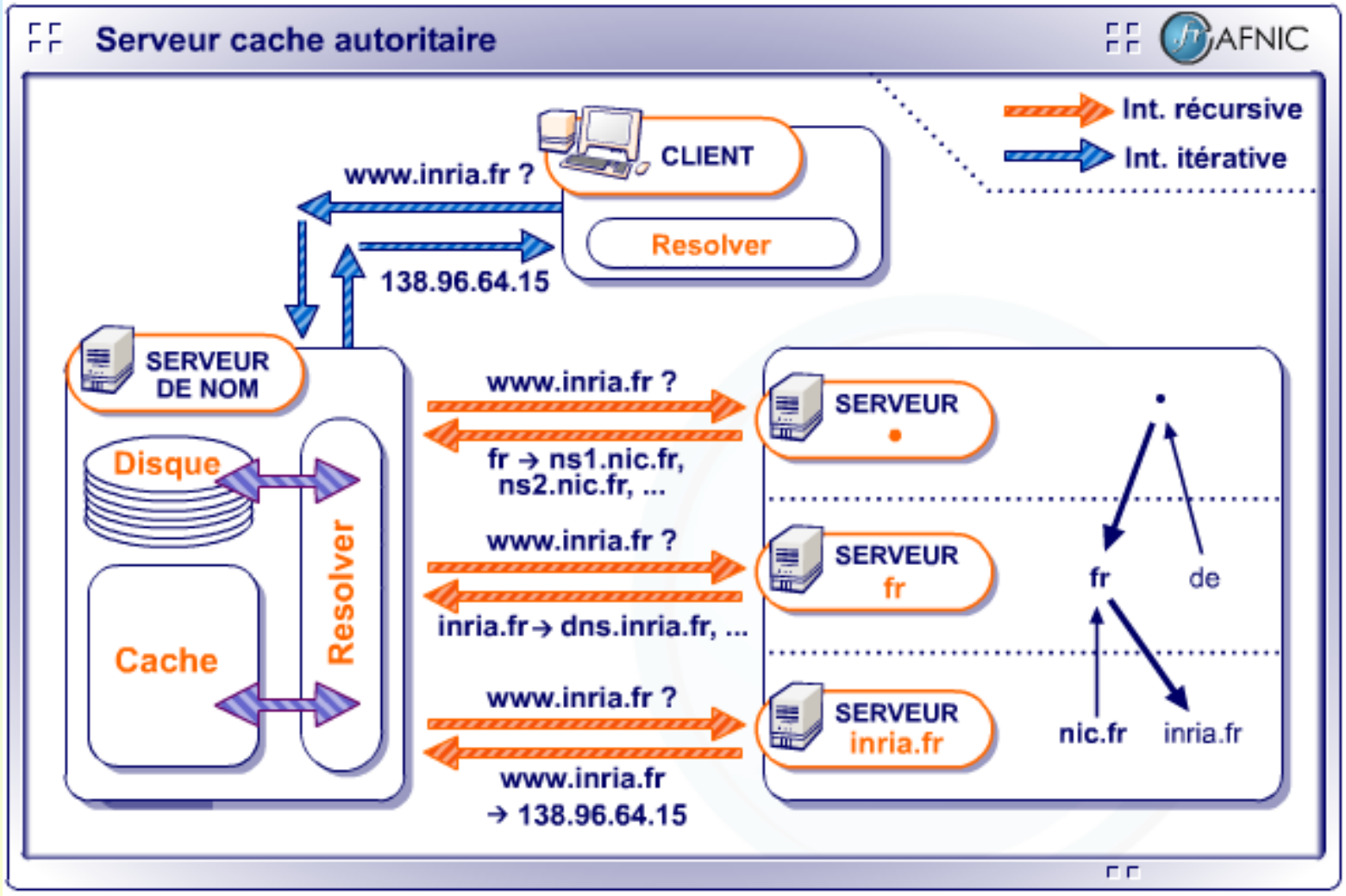
Ces données ont cependant une durée de vie limitée qui est spécifiée dans le champ TTL (Time To Live)

Serveurs qui ont autorité

Un serveur de noms ayant sur son disque dur les informations relatives à une machine est dit « autoritaire » ou « autoritatif » pour celle-ci.



Serveurs cache et autoritaires



Ressource Record

La base de données DNS ne gère pas que des adresses IP mais aussi des informations sur les serveurs de noms.
Sur UNIX on trouve ces informations dans un fichier généralement nommé named.hosts.

Chaque ligne de ce fichier est appelé RR «Ressource Record». A chaque RR est associé un type

- Ex : adresse IP est un RR de classe A (attention à la confusion avec les classes d'adresse IP) AAAA pour une adresse IPv6.
- CNAME indique un alias vers le nom canonique.
- MX (Mail Exchange), spécifie un serveur de mails (son adresse IP).

Fichier exemple :

Caractère générique contenant le nom du domaine géré ici « insa-cvl.fr. »

Fichier configuration pour la zone insa-cvl.fr

```
@       IN  SOA ns.insa-cvl.fr.   postmaster.insa-cvl.fr.
(    960900     ;numéro de série
     360000     ;  mise à jour
     3600       ;tentative après échec
     3600000    ;délai d'expiration
     3600       ;  ttl négatif RFC 2308 )
     IN NS ns ;Serveurs de noms
     IN NS ns2.insa-cvl.fr.
ns          IN    A     195.221.18.3
ns2         IN    A     195.221.18.4
serveurdenoms IN CNAME ns
```

Adresse mail du responsable de la zone

Nom du « name server » primaire de la zone

SOA Start Of Authority

Valeur incrémentée --> informer DNS secondaire de modifications

Délai entre 2 mises à jour DNS slaves

Délai abandon essais de connexion en échecs Slaves

Écriture relative

Écriture absolue

Resource Record RR de type Adresse IPv4

Resource Record RR de type alias « cname »

IN pour la gestion du réseau INTERNET

Voir URL :
https://fr.wikipedia.org/wiki/SOA_Resource_Recor

Ressource Record (suite)

Les enregistrements NS associés à un enregistrement A permettent de définir une délégation de zone. ils sont appelés Glue Record. C'est eux qui construisent l'arborescence DNS.

Exemple :

```
eleves.insa-cvl.fr.   IN  NS   nseleves.insa-cvl.fr.
nseleves.insa-cvl.fr.     IN     A     195.221.18.9
```

Ressource Record (suite)

Base de données pour les requêtes inverses (Reverse Mapping).

Il existe un domaine principal in-addr.arpa.

Ce domaine contient l'adresse des machines en notation inversée.

Exemple 195.221.2.12 devient 12.2.221.195.in-addr.arpa.

Sous unix, cette information est contenue dans named.rev

Ressource Record (suite)

Base de données pour les requêtes inverses

Exemple de fichier named.rev

le domaine 2.221.195.in-addr.arpa.

```
@IN  SOA serveur.insa-cvl.fr.
   administrateur.insa-cvl.fr. (              960925
        ;numéro de série
        360000        ; mise à jour
        3600        ;tentative après échec
        3600000      ;délai d'expiration
        3600        ; ttl par défaut  )
12        IN PTR serveur.insa-cvl.fr
```

Outil pour émettre des requêtes DNS

« nslookup » : sous OS Windows et Unix-like

Windows PowerShell

```
PS C:\Users\martial> nslookup
Serveur par dÚfaut :   UnKnown
Address:  192.168.37.2

> www.insa-cvl.fr
Serveur :   UnKnown
Address:  192.168.37.2

Réponse ne faisant pas autorité :
Nom :    www.insa-cvl.fr
Address:  91.121.44.96

> set type=ns
> insa-cvl.fr
Serveur :   UnKnown
Address:  192.168.37.2

Réponse ne faisant pas autorité :
insa-cvl.fr     nameserver = ns.insa-cvl.fr
insa-cvl.fr     nameserver = ns2.ensi-bourges.fr
> set type=mx
> insa-cvl.fr
Serveur :   UnKnown
Address:  192.168.37.2

Réponse ne faisant pas autorité :
insa-cvl.fr     MX preference = 50, mail exchanger = mxa.relay.renater.fr
insa-cvl.fr     MX preference = 50, mail exchanger = mxb.relay.renater.fr
insa-cvl.fr     MX preference = 50, mail exchanger = mxc.relay.renater.fr
insa-cvl.fr     MX preference = 50, mail exchanger = mxd.relay.renater.fr
> set type=ns
> .
Serveur :   UnKnown
Address:  192.168.37.2

Réponse ne faisant pas autorité :
(root)  nameserver = e.root-servers.net
(root)  nameserver = h.root-servers.net
(root)  nameserver = a.root-servers.net
(root)  nameserver = j.root-servers.net
(root)  nameserver = g.root-servers.net
(root)  nameserver = l.root-servers.net
(root)  nameserver = d.root-servers.net
(root)  nameserver = m.root-servers.net
(root)  nameserver = f.root-servers.net
(root)  nameserver = i.root-servers.net
(root)  nameserver = c.root-servers.net
(root)  nameserver = k.root-servers.net
(root)  nameserver = b.root-servers.net
```

```
root@debian:/home/eleve# nslookup
> www.insa-cvl.fr
Server:         192.168.1.254
Address:        192.168.1.254#53

Non-authoritative answer:
Name:   www.insa-cvl.fr
Address: 91.121.44.96
> set type=ns
> insa-cvl.fr
Server:         192.168.1.254
Address:        192.168.1.254#53

Non-authoritative answer:
insa-cvl.fr     nameserver = ns.insa-cvl.fr.
insa-cvl.fr     nameserver = ns2.ensi-bourges.fr.

Authoritative answers can be found from:
> set type=mx
> insa-cvl.fr
Server:         192.168.1.254
Address:        192.168.1.254#53

Non-authoritative answer:
insa-cvl.fr     mail exchanger = 50 mxd.relay.renater.fr.
insa-cvl.fr     mail exchanger = 50 mxa.relay.renater.fr.
insa-cvl.fr     mail exchanger = 50 mxb.relay.renater.fr.
insa-cvl.fr     mail exchanger = 50 mxc.relay.renater.fr.

Authoritative answers can be found from:
> set type=ns
> .
Server:         192.168.1.254
Address:        192.168.1.254#53

Non-authoritative answer:
.       nameserver = b.root-servers.net.
.       nameserver = l.root-servers.net.
.       nameserver = j.root-servers.net.
.       nameserver = e.root-servers.net.
.       nameserver = f.root-servers.net.
.       nameserver = d.root-servers.net.
.       nameserver = a.root-servers.net.
.       nameserver = c.root-servers.net.
.       nameserver = k.root-servers.net.
.       nameserver = m.root-servers.net.
.       nameserver = h.root-servers.net.
.       nameserver = i.root-servers.net.
.       nameserver = g.root-servers.net.
```

La commande pour quitter nslookup est : exit