

**D**omain **N**ame **S**pace

**D**omain **N**ame **S**ystem

**D**omain **N**ame **S**erver



# DNS ?

Le DNS est l'**annuaire** mondial unifié de l'internet.

Il offre les services classiques d'un annuaire :

Trouver un **numéro** (@IP)  
à partir d'un **nom** (de domaine)

Mais aussi trouver des **services** pour un domaine (à qui envoyer les mails ? Où est le serveur Web ? Qui est le contrôleur du domaine ? Etc. )



# Historique

1970-1984 : un fichier unique **HOSTS.TXT**

- contenant la correspondance nom adresse IP, recopié sur chaque machine.
  - distribué par une machine unique SRI-NIC
- ⇒ Problèmes trafic et charge, conflit de noms, cohérence.

Bien que ce système ait été abandonné le fichier **hosts** est **toujours présent** dans les OS, les (quelques) informations qu'il contient sont **prioritaires** sur celles des **serveur DNS**

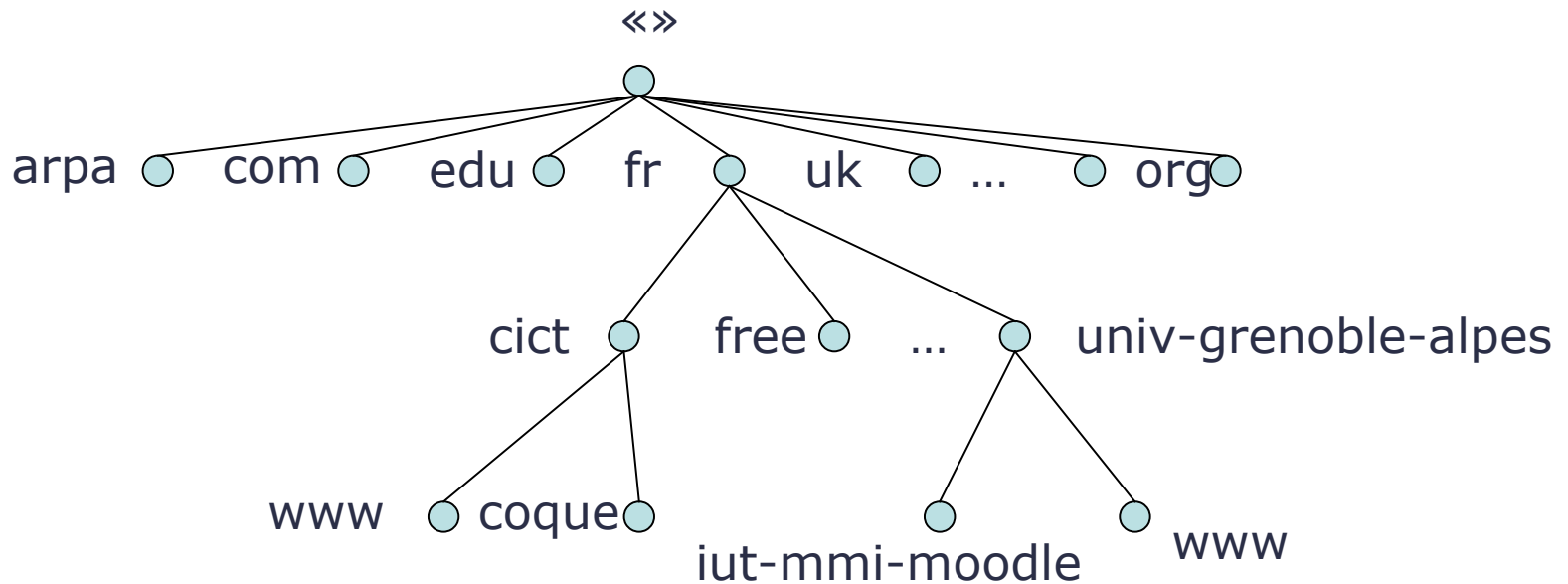
Il se trouve dans :

C:\WINDOWS\system32\drivers\etc\hosts  
ou /etc/hosts sur un OS unix (Linux / OSX)



# Structure de l'espace de noms

Structure hiérarchique en domaine et sous domaine qui forment un arbre



Racine : nom vide (chaîne de caractères vide)

**FQDN** : Nom absolu (Fully Qualified Domain Name) nom qui remonte à la racine (se termine donc par un point) : `www.univ-grenoble-alpes.fr.`

Nom associé à un nœud : 63 octets max



# DNS organisation

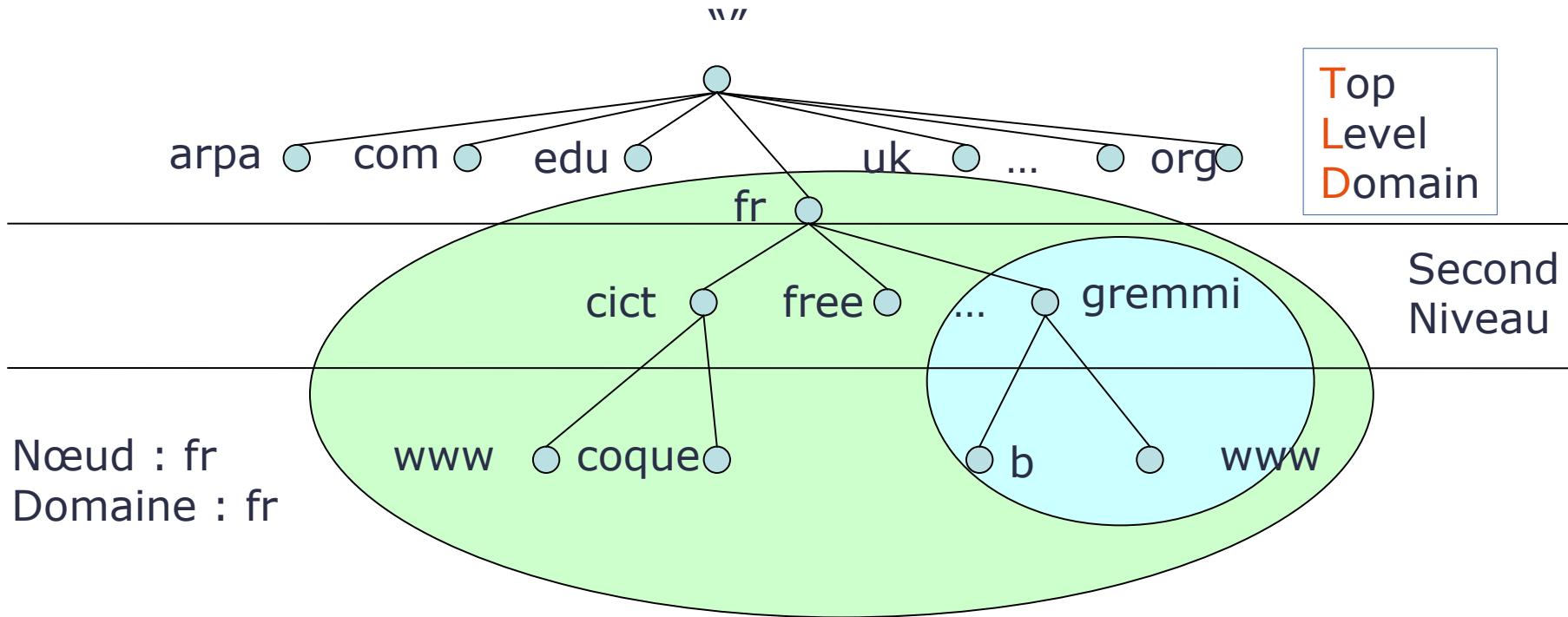
Pour résoudre les problèmes d'un serveur centralisé on a organisé une **base de données distribuée** sur un grand nombre de serveurs.

Chaque serveur prend en charge une partie de l'arborescence totale

La racine est gérée par 13 serveurs de **I'ICANN**



# Domaines



Un domaine est un sous-arbre.

Les feuilles représentent les hôtes.

Nota : Les nœuds internes peuvent aussi représenter des hôtes (avoir une adresse IP).



# Délégation

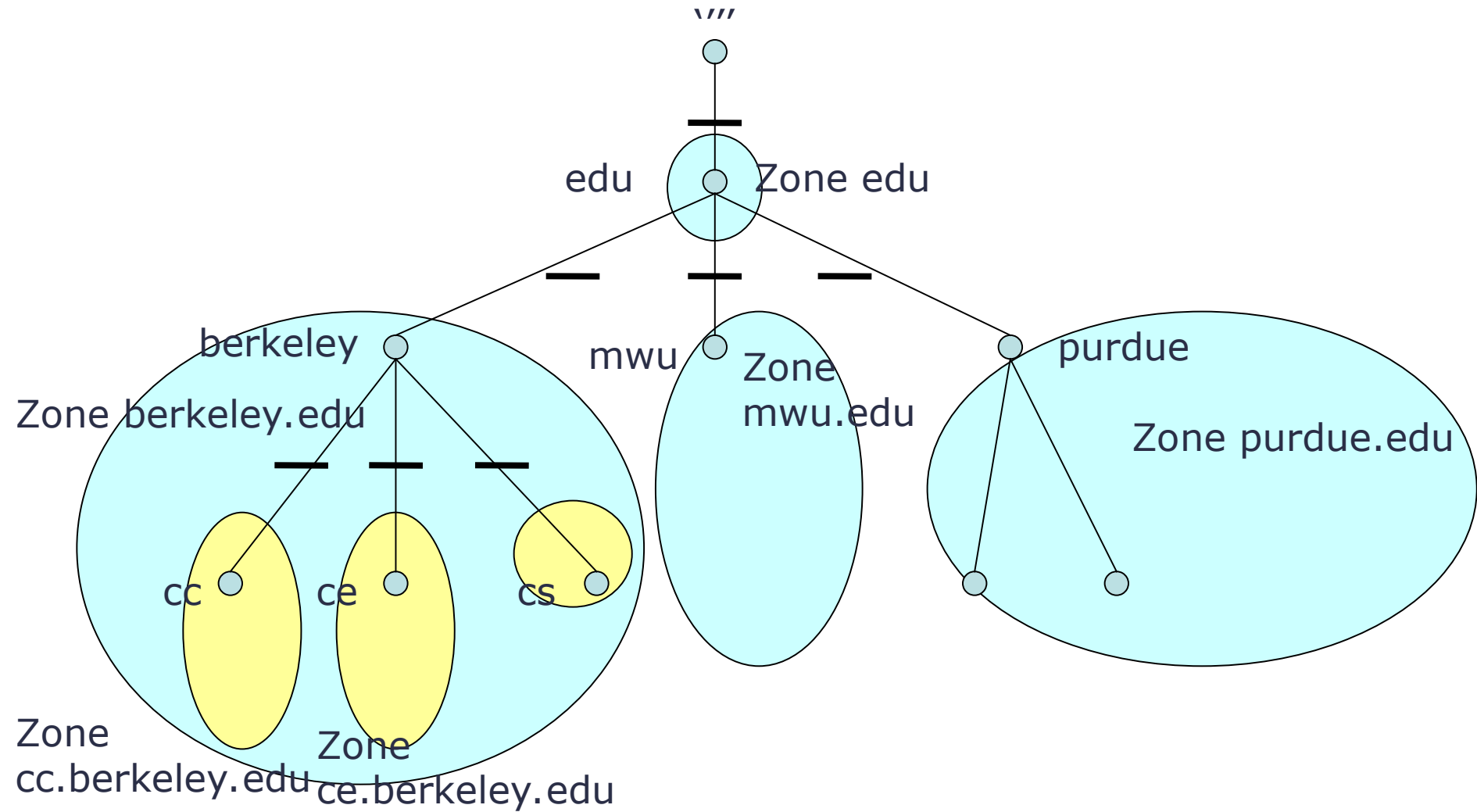
Comment décentraliser l'administration => **déléguer** l'autorité.

La **délégation** est le transfert de la responsabilité d'un sous-domaine vers une autre organisation.

- Le domaine parent contient des pointeurs vers les serveurs du sous-domaine (ses **NS**).
- L'organisme ayant la délégation peut modifier librement les données de son sous-domaine (nom, services, délégation, ...)



# Serveurs de nom et zones





# Serveurs de nom et zones

Dans un espace de nom, une **zone** est la partie de l'arbre de l'espace de nom qui est gérée par un **serveur de nom** DNS.

Un même serveur DNS peut gérer plusieurs zones dans différents domaines.

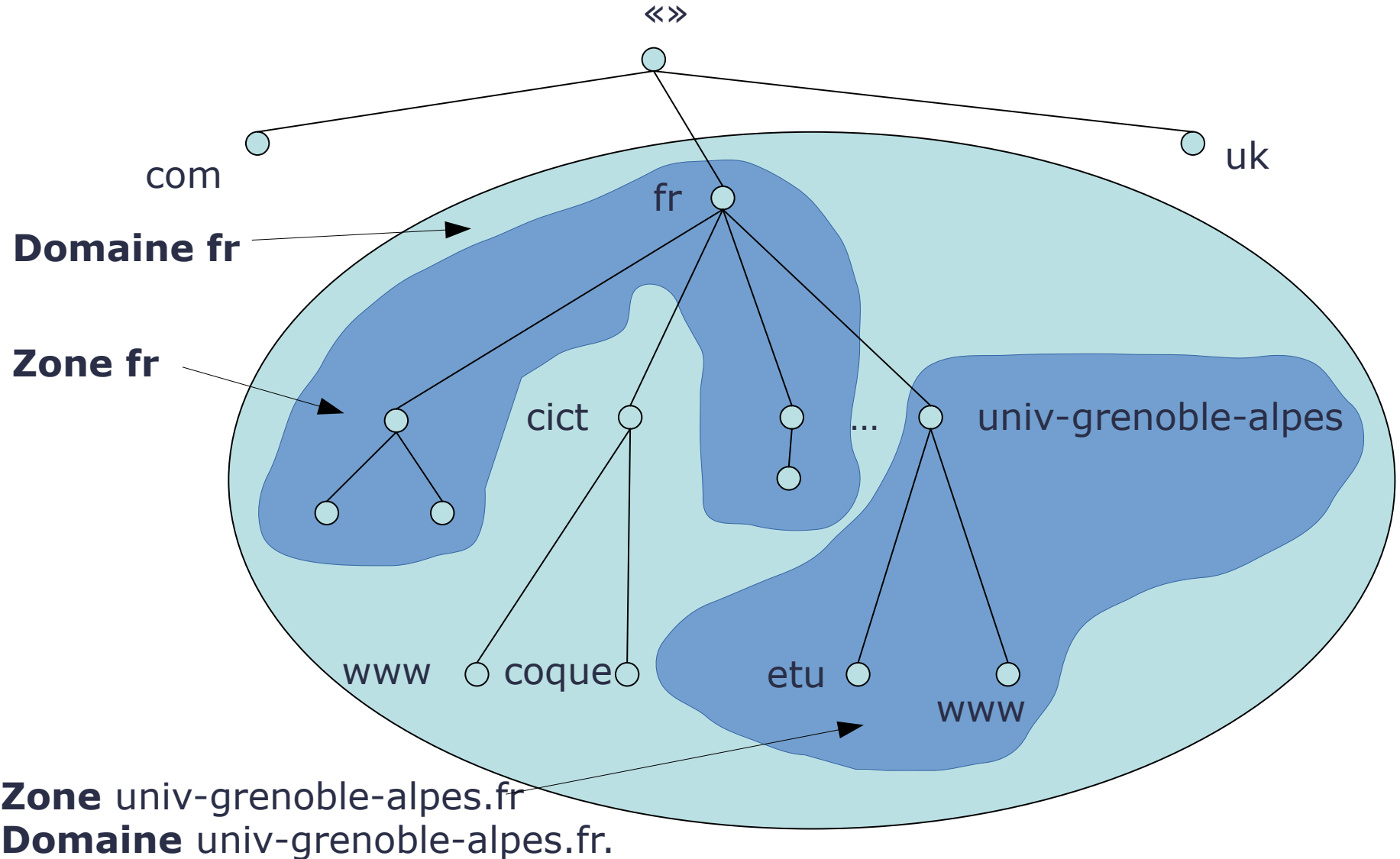
Les sous-domaines sont gérés dans la zone de leur domaine parent

ou

dans des zones séparées grâce à la **délégation**



# Serveurs de nom et zones





# Types de serveurs de nom

Pour améliorer les performances et la tolérance aux pannes les informations sont dupliquées sur plusieurs serveurs (NS).

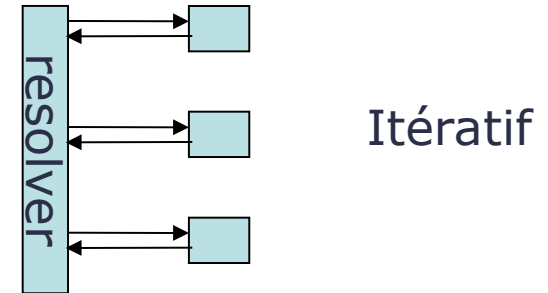
Il y a un Serveur maître ou primaire : il détient l'original du fichier de zone. On dit qu'il fait autorité sur la zone (SOA)

Plusieurs Serveurs secondaires ou esclaves : ils obtiennent une copie du fichier de zone depuis un serveur maître/primaire (transfert de zone).



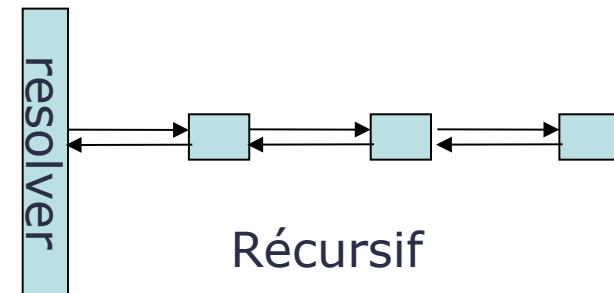
# Résolution mode Récuratif/itératif

En mode itératif, le serveur renvoie au client la référence du serveur qui sait répondre.



En mode récursif le serveur poursuit la recherche lui-même et fournit au client sa réponse.

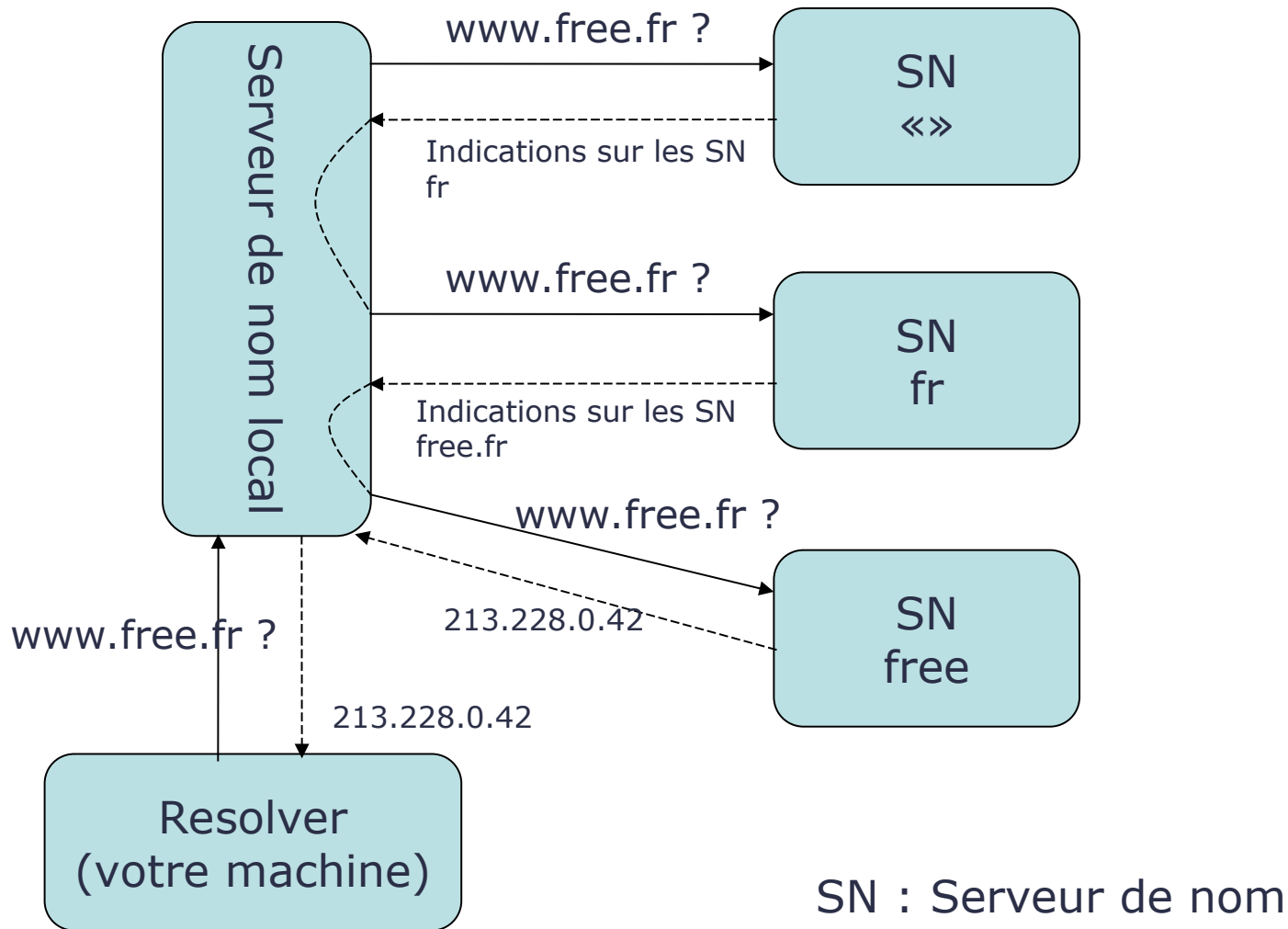
- ⇒ Le mode récursif surcharge le serveur d'origine.
- ⇒ Dans le mode récursif le serveur est obligé de répondre complètement ou d'envoyer une erreur.



Pour ne pas surcharger les serveurs le mode récursif est restreint aux clients locaux. La plupart des serveurs refuse de fonctionner en mode récursif.



# Résolution





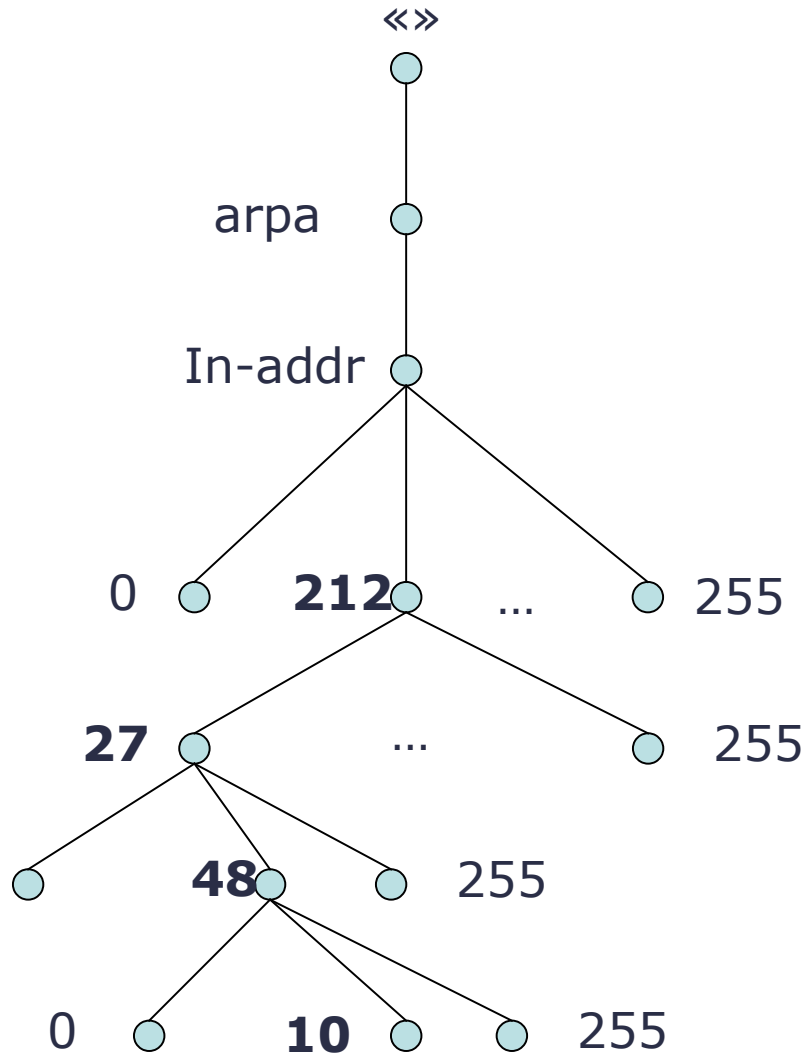
# Caches

Lors d'une requête récursive le serveur de nom voit passé le nom des serveurs faisant autorité et leurs adresses.

Dans un soucis d'optimisation, il est logique de mémoriser pour un temps donné ces informations : un cache est mis en œuvre.



# Résolution Inverse



La recherche inversée utilise un arbre différent de la recherche normale. Elle se fait dans la branche « arpa ».

**In-addr.arpa** pour IPv4 et **ip6.arpa** pour IPv6

Aucune cohérence entre les deux arbres n'est garantie.

Exemples :

**Directe :**

www.12.mmi  
⇒ 152.77.208.112

**Inversée :**

112.208.77.152.in-addr.arpa.  
⇒ iut1i-603-o12.u-ga.fr.



# Fichier de Zone

La description du contenu de la zone (hôtes, serveur de noms, etc) se fait dans un **fichier texte**.

Ce fichier contient des **directives** et des « **enregistrements** » (RR resource record).

« **( )** » permet d'écrire sur plusieurs lignes

« **;** » introduit un commentaire.

« **@** » sera automatiquement remplacé par le nom de la zone.



# Directives

Les directives permettent de définir des valeurs commune à tous les enregistrements. Elle commencent toujours par « \$ »

Exemples :

**\$TTL** : temps de vie en cache par défaut

**\$INCLUDE** : permet d'inclure un fichier

**\$GENERATE** : fabrication en série  
d'enregistrements



# Enregistrement

Les enregistrements (**RR**) définissent les informations du DNS. Ils suivent une syntaxe précise :

**nom** [**TTL**] [**IN**] **type-RR** **argument** ...

**TTL** : Time To Live (durée en cache)

**IN** : InterNet (d'autres types d'adresses étaient prévus à l'origine)

Rappel :

[] indique un élément facultatif

... veut dire un ou plusieurs



# Types d'enregistrements

**SOA** = start of authority

Indique quel serveur possède la description originelle de la zone.

c'est lui qui la distribue aux serveurs esclave/secondaire.

On dit qu'il fait **autorité sur la zone**

Syntaxe :

- domaine [TTL] [IN] **SOA** nom-du-serveur email-admin (  
    serial-number ; pour les serveurs secondaires  
    time-to-refresh ; délai entre deux synchronisation  
    time-to-retry ; délai pour refaire une tentative de synchro  
                  en cas d'échec  
    time-to-expire ; les informations ne sont plus valables car  
                  la synchro est trop ancienne  
    negative answer ) ; délai avant de refaire une requête sans  
                      réponse



# Types d'enregistrements NS

Indique le nom d'un serveur de nom pour la zone (maitre ou esclave)

il peut y avoir un ou plusieurs NS

SOA et NS servent à gérer la délégation et la redondance dans l'architecture DNS

- Syntaxe :  
domaine [TTL] [IN] NS nom-serveur



# Types d'enregistrements

## A / AAAA

Ils assurent la correspondance entre un nom d'hôte et une adresse :

IPv4 pour A

IPv6 pour AAAA

- Syntaxe :

nom [TTL] [IN] **A** adresse-IPv4

nom [TTL] [IN] **AAAA** adresse-IPv6



# Types d'enregistrements **CNAME**

Canonical Name = alias

permet de définir plusieurs nom  
ayant la même adresse IP

- Syntaxe :  
new-name [TTL] [IN] **CNAME** name



# Types d'enregistrements MX

Mail eXchange :

indique quels sont les serveurs de mail pour un domaine, avec une priorité entre eux.

- Syntaxe :  
domaine [TTL] [IN] **MX** priorité serveur-de-mail
- ... voir Wikipédia pour une (longue) liste complète



# Enregistrement de domaine

<http://www.internic.net> (Internet Network Information Centre)

En France **NIC** (**N**etwork **I**nformation **C**entre)  
= **AFNIC** (**A**ssociation **F**rançaise pour le  
**N**ommage **I**nternet en **C**oopération).

Obligation de passer par un  
intermédiaire FAI ou hébergeur.



# Configuration Serveur DNS

- Des zones par défaut

```
#serveurs racines
zone "." in {
    type hint;
    file "root.hint";
};
```

```
#local host
zone "localhost" in {
    type master;
    file "localhost.zone";
};
#local host inverse
zone "0.0.127.in-addr.arpa" in {
    type master;
    file "127.0.0.zone";
};
```

#zone propres au serveur

```
zone "mmi." in {
    file "db.mmi";
    type master;
};
```

```
zone "114.168.192.in-addr.arpa" in {
    file "db.114.168.192.in-addr.arpa";
    type master;
};
```



# Serveur DNS

- Des redirecteurs pour transférer les requêtes vers d'autres serveurs

forwarders {

192.0.2.1; 192.0.2.2;

};

- Des options pour dialoguer entre serveurs DNS



# Fichier de zone

```
$TTL 2D
@ IN SOA      serveur root (
2020020100    ; serial (date et heure en général)
3H            ; refresh
1H            ; retry
1W            ; expiry
1D )          ; minimum

@ IN NS       routeur-1
routeur-1     IN A       192.168.114.18
pop3          IN CNAME   routeur-1
smtp          IN A       192.168.114.18

poste-01 IN A       192.168.114.101
...
poste-15 IN A       192.168.114.115

@ IN MX       10 smtp
```



# Évolutions du DNS

DNS :

- transfert de zone simple
- transfert de zone comprimée
- transfert de zone incrémentielle

DDNS Dynamic DNS

DNSSEC (*Domain Name System Security Extensions*) :

DNSsec constitue une des extensions du protocole DNS. Cette extension assure, par le biais de signatures numériques, l'authentification et l'intégrité des enregistrements du DNS. Le DNS, une fois sécurisé, peut être utilisé pour stocker des certificats.



# Exemples de requête

- Utilitaires : dig, host, nslookup

Chaque zone peut contenir différents champs d'information (MX, PTR, A, SO, NS, CNAME)

Q1 : description du serveur faisant autorité pour la zone *univ-grenoble-alpes.fr*

```
dig univ-grenoble-alpes.fr soa
```

```
;; ANSWER SECTION:
```

```
univ-grenoble-alpes.fr.      IN      SOA eip1.u-ga.fr. dnsadmin.univ-grenoble-alpes.fr. 2015121897 1200  
      300 1209600 3600
```

2015121897 ; numéro de version du fichier

1200 ; temps entre deux transferts de zone

300 ; temps avant de refaire un transfert qui a échoué

1209600 ; passer ce temps (depuis le dernier transfert) la zone n'est plus valide

**3600 ; temps de mise en cache minimum (valeur par défaut même si la réponse est « pas trouvé »)**

*eip1.u-ga.fr.* : serveur maître

*dnsadmin.univ-grenoble-alpes.fr.* : email de l'administrateur : @ est remplacé par « . »



# Exemples de requête

Q2 : quels sont les serveurs de nom pour la zone univ-grenoble-alpes.fr ?

```
dig univ-grenoble-alpes.fr ns
```

```
;; ANSWER SECTION:
```

```
univ-grenoble-alpes.fr.      IN  NS  eip1.u-ga.fr.
```

```
univ-grenoble-alpes.fr.      IN  NS  eip2.u-ga.fr.
```



# Exemples de requête

Q3 : Quels sont les serveurs de Mail de univ-grenoble-alpes.fr ?

dig univ-grenoble-alpes.fr **mx**

;; ANSWER SECTION:

univ-grenoble-alpes.fr.	IN	MX	50	mxh.relay.renater.fr.
univ-grenoble-alpes.fr.	IN	MX	50	mxg.relay.renater.fr.
univ-grenoble-alpes.fr.	IN	MX	50	mxj.relay.renater.fr.
univ-grenoble-alpes.fr.	IN	MX	50	mxk.relay.renater.fr.



# Exemples de requête

Q4 Quelle est l'adresse IP de  
www.univ-grenoble-alpes.fr ?

```
dig www.univ-grenoble-alpes.fr a
```

```
;; ANSWER SECTION:
```

```
www.univ-grenoble-alpes.fr.  IN  CNAME ksup.u-ga.fr.
```

```
ksup.u-ga.fr.                IN  A   195.83.24.194
```



# Exemples de requête

Q4 Quelle est le serveur LDAP de  
iut1.local ?

```
dig _ldap._tcp.iut1.local srv
```

```
:: ANSWER SECTION:
```

```
_ldap._tcp.iut1.local.      IN  SRV    0 100 389 iut1-srv-  
ad1.iut1.local.
```

```
_ldap._tcp.iut1.local.      IN  SRV    0 100 389 iut1-srv-  
ad2.iut1.local.
```

```
_ldap._tcp.iut1.local.      IN  SRV    0 100 389 iut1-srv-  
ad3.iut1.local.
```



# Conclusion

Un service d'Internet incontournable

Une base de donnée **répartie** et **redondante**  
permettant de stocker des informations sur des  
ressources

Concepts :

- espace de noms
- domaines
- zones
- serveurs maître, serveur esclaves