

# INTRODUCTION AU DNS

Alain Patrick AINA

[aalain@trstech.net](mailto:aalain@trstech.net)

Atelier DNS/CCTLD

Yaounde, 17-21 Decembre 2004



# Objectifs du nommage

- Les Adresses sont utilisées pour localiser des objets
- Les noms sont plus faciles à mémoriser que les nombres
- Vous aimeriez aller à une adresse ou autres objets en utilisant un nom
- **Le Système de nom de domaine (DNS) fournit une correspondance de noms en des ressources de plusieurs types**

# Noms et adresses en général

- Une adresse indique comment atteindre un point
  - Typique, hiérarchique (pour l'extension à grande échelle):
    - 867, avenue de Calais, Nyekonakpoè, Lomé, République Togolaise
- Un “nom” indique comment un point est référencé
  - Typique, pas toujours hiérarchisé
    - “Alain”, “Yaoundé”, “francophonie.org”

# Historique du nommage

- ARPANET(1970)
  - Host.txt maintenu par le SRI-NIC
  - Récupéré à partir d'une seule machine
  - Problèmes
    - trafic and charge
    - Collisions de noms
    - Cohérence
- Le DNS a été créé en 1983 par Paul Mockapetris (RFCs 1034 et 1035), modifié, mis à jour, et amélioré par une multitude de RFCs: 2181, etc.

# DNS: Domain Name System

- Un mécanisme de “correspondance” d'objet en d'autres objets
- Une base de données dynamique, globalement distribuée, cohérente, évolutive et fiable
- Composé de trois composantes
  - Un “ espace de nommage”
  - Les serveurs rendant l'espace de nommage disponible
  - Les resolvers (clients) qui questionnent les serveurs à propos de l'espace de nommage

# Caractéristiques du DNS : Distribution Globale

- Les données sont maintenues localement, mais utilisable globalement
  - Toutes les données du DNS ne sont pas maintenues par une seule machine
- N'importe quel équipement peut faire une requête DNS
- Les données DNS sont localement mis en cache pour améliorer la performance

# Caractéristiques du DNS : Cohérence

- La base de données est souvent localement cohérente
  - Chaque version d'une partie de la base (une zone) a un numéro de série
    - Le numéro de série est incrémenté à chaque changement dans la base
- Les changements à la copie principale de la base de donnée sont répliqués selon une périodicité configurée par l'administrateur de la zone
- Les données en cache expirent après un délai configuré par l'administrateur de la zone

# Caractéristiques du DNS : Extension à grande échelle

- Pas de limite à la taille de la base de données
  - Un serveur peut avoir plus de 20 000 000 de noms
    - Pas une bonne idée
- Pas de limites au nombre de requêtes
  - 24 000 requêtes par seconde gérées facilement
- Les requêtes sont distribuées entre les serveurs (maîtres, esclaves et caches)



# Caractéristiques du DNS : Fiabilité

- Les données sont répliquées
  - Les données du maître sont copiées par les esclaves
- Les clients peuvent questionner
  - Le serveur maître
  - N'importe lequel des esclaves
- Les clients questionnent généralement les caches locaux
- DNS utilise comme transport UDP ou TCP, port 53
  - Si UDP est utilisé, DNS gère les retransmissions, les séquences, etc.

# Caractéristiques du DNS : “Dynamicité”

- La base de données peut être mise à jour dynamiquement
  - ajout/suppression/modification de n'importe quel enregistrement
- La modification de la copie du maître entraîne la réplication
  - Seul le maître peut être mis à jour dynamiquement
    - Constitue un point d'échec unique

# Caractéristiques du DNS: Limites de certains objets et paramètres

Etiquettes: 63 octets ou moins

Noms: 255 octets ou moins

TTL: valeur positive de nombre sur 32 bits

Messages UDP: 512 octets ou moins

**Des extensions(EDNS0:RFC2671, etc.) proposées pour supporter de nouvelles fonctionnalités comme IPv6,DNSSEC... et peut-être plus de serveurs racine, etc.**

# Concepts DNS

- Les prochains slides parlent des concepts
- Après ces slides, vous devrez comprendre
  - Comment est bâti le DNS
  - Pourquoi est-il bâti comme cela
  - Les terminologies utilisées

# Concept: Noms DNS 1


- L'espace de nommage a besoin d'être hiérarchisé pour évoluer à grande échelle.
- L'idée est de nommer les objets sur la base de:
  - L'endroit ( au sein d' un pays, ensemble d'organisations, ensemble de sociétés, etc...)
  - L'unité dans cet endroit(société dans un ensemble de sociétés, etc)
  - objet au sein de l' unité (nom de personne dans une société)

# Concept: Noms DNS 2

## Comment les noms apparaissent dans le DNS

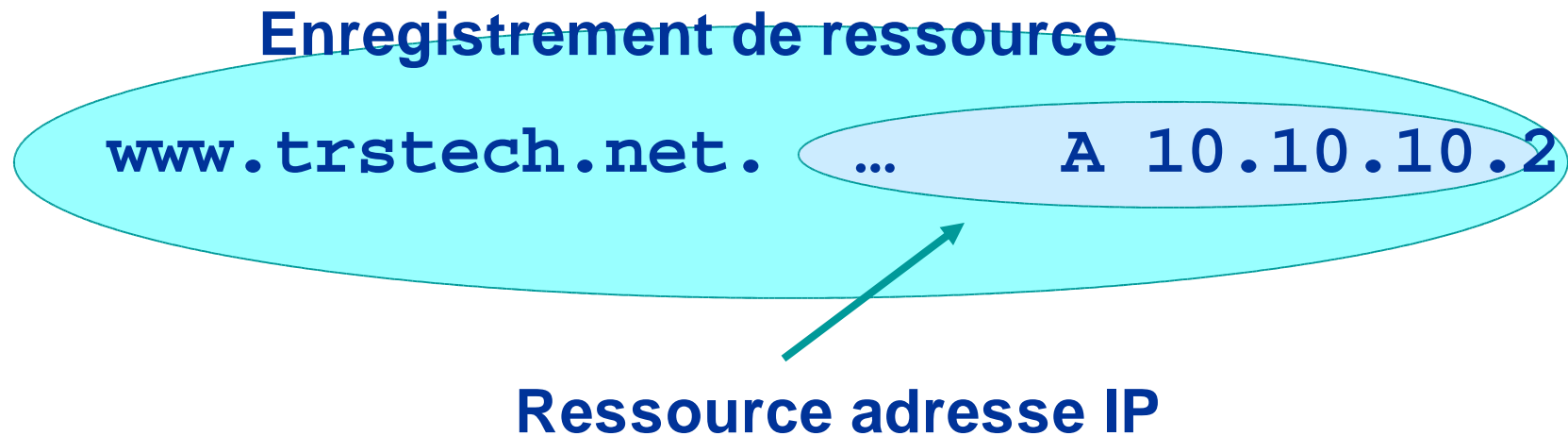
Nom de domaine complètement qualifié (FQDN)

**agence.francophonie.org.**

- Des étiquettes séparées par des points 
  - RFC 952 définit certaines contraintes
- Le DNS fournit une correspondance de “FQDN” en des ressources de plusieurs types
- Les noms sont utilisés comme clé de recherche de données dans le DNS

# Concept: Les enregistrements de ressource

- Le DNS fait correspondre à des noms, des données en utilisant les enregistrements de ressources



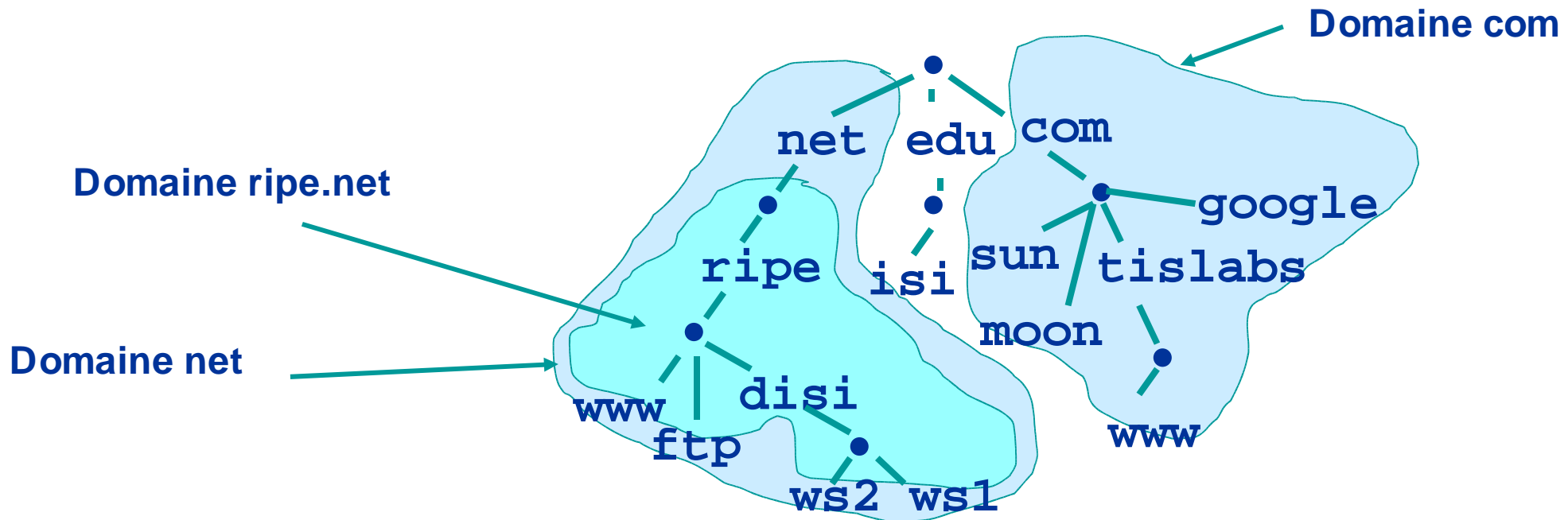
- Plus de détails plus loin





# Concept: Domaines

- Les domaines constituent “ un espace de nommage”
- Tout ce qui est au dessous de .com est dans le domaine com.
- Tout ce qui est au dessous de ripe.net est dans le domaine ripe.net et dans le domaine net.

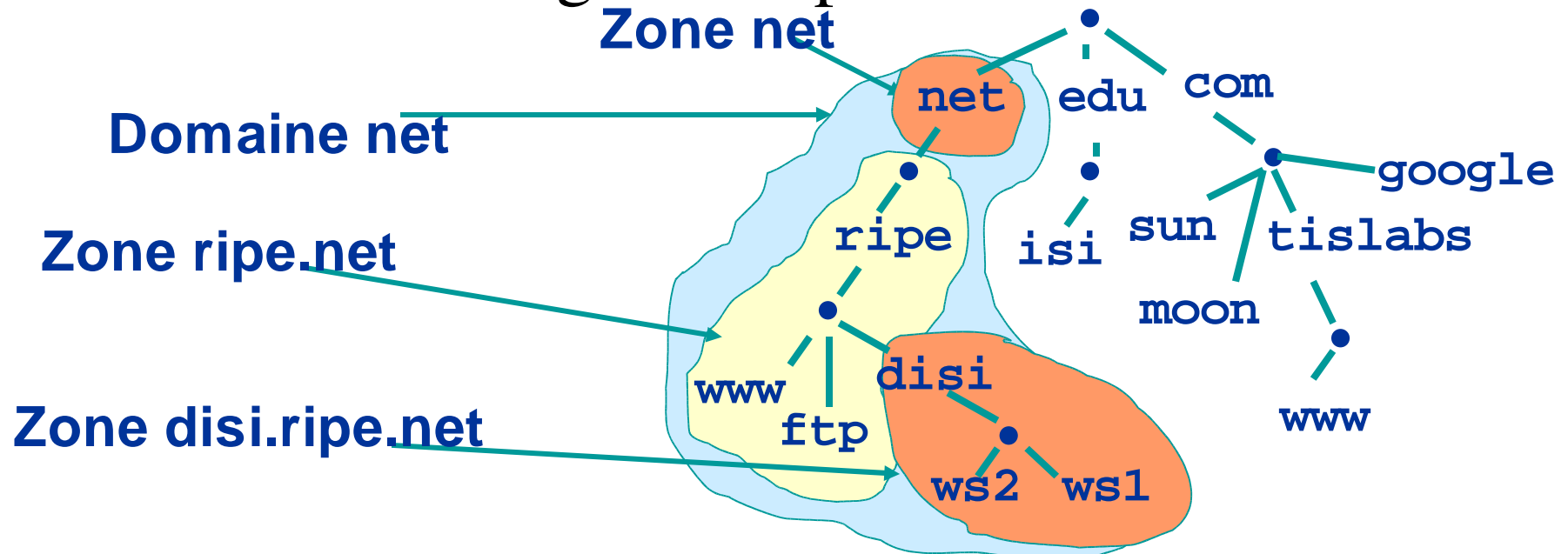


# Délégation

- Les administrateurs peuvent créer des sous-domaines pour des groupes de machines
  - Selon une affiliation géographique ou organisationnelle ou tout autre critère
- L' administrateur d'un domaine peut déléguer la responsabilité de la gestion d'un sous-domaine à quelqu'un d'autre
  - Ceci n'est pas une obligation
- Le domaine parent contient des liens vers le sous-domaine délégué
  - Le domaine parent “se souvient” de celui à qui le sous-domaine a été délégué

# Concept: Zones et Délégations

- Les zones sont des “espaces administratifs”
- Les administrateurs de zone sont responsables pour la portion de l'espace de nommage du domaine
- L'autorité est déléguée du parent et à un enfant



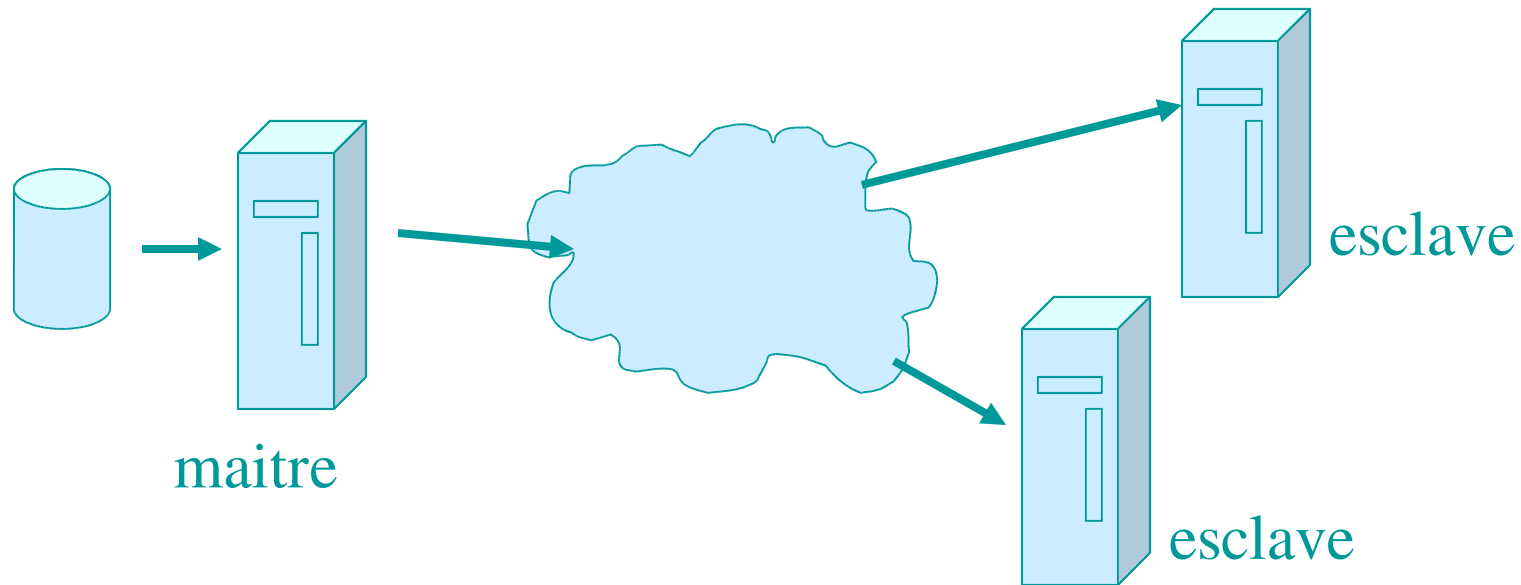
# Concept: Serveurs de noms

- Les serveurs de noms répondent aux questions DNS.
- Plusieurs types de serveurs de noms
  - Serveurs autoritaires
    - maitre (primaire)
    - esclave (secondaire)
  - Serveurs récursifs (cache)
    - Les caches "forwarders"
  - Mélange de fonctionnalités
    - Pas recommander

# Concept: Serveurs de noms

## Serveurs autoritaires

- Donnent des réponses autoritaires pour une ou plusieurs zones.
- Le serveur maître charge normalement les données à partir d'un fichier de zone
- Les esclaves copient normalement les données du maître via un transfert de zone



# Concept: Serveurs de noms

## Serveurs récursifs

- Les serveurs récursifs font les recherches courantes; Ils posent des questions au DNS en lieu en place des clients.
- Les réponses sont obtenues des serveurs autoritaires, les réponses transférées aux clients sont marquées non autoritaires
- Les réponses sont conservées pour les prochaines références dans le cache

# Concept: "Resolvers"

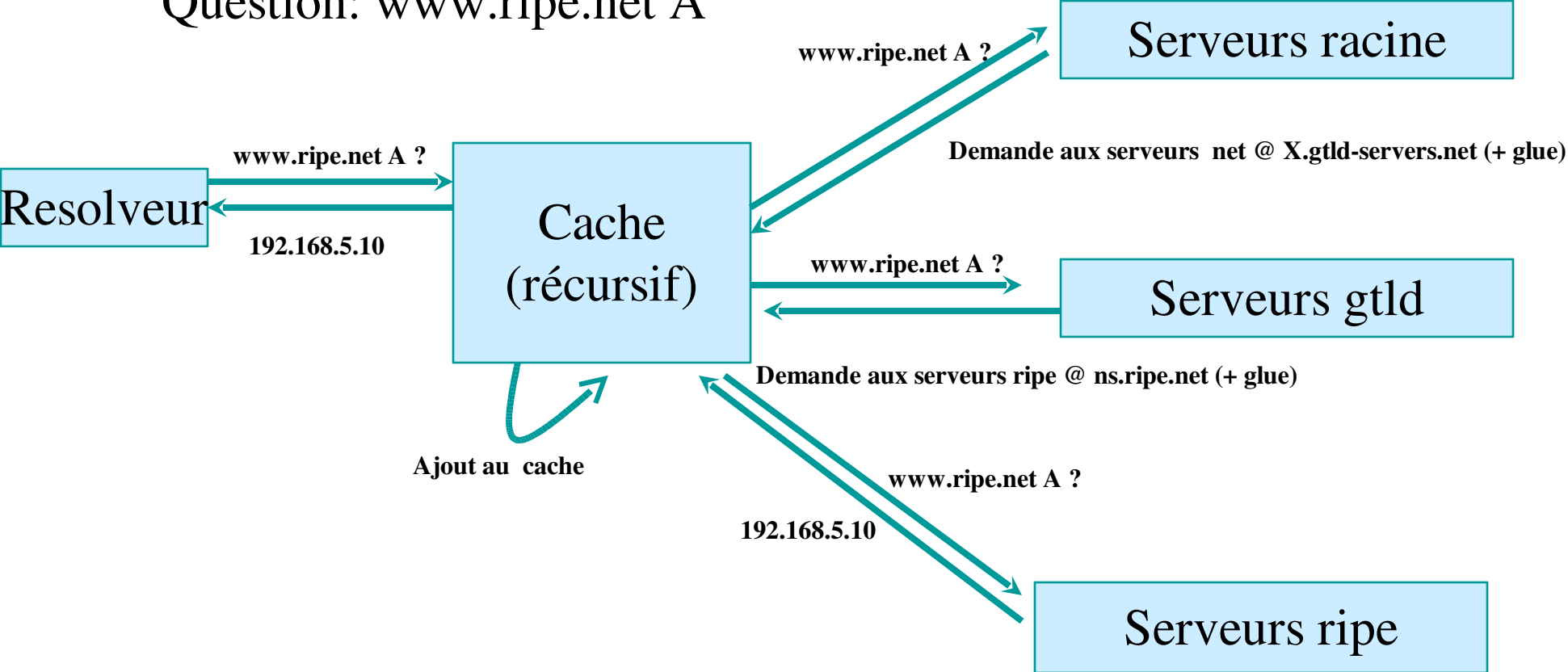
- Les “resolvers” posent des questions au DNS en lieu et place des applications.
- Normalement implémenté dans les bibliothèques systèmes ( libc etc....)

```
gethostbyname ( char *name ) ;
```

```
gethostbyaddr ( char *addr , int len ,  
type ) ;
```

# Concept: Processus de résolution & Cache

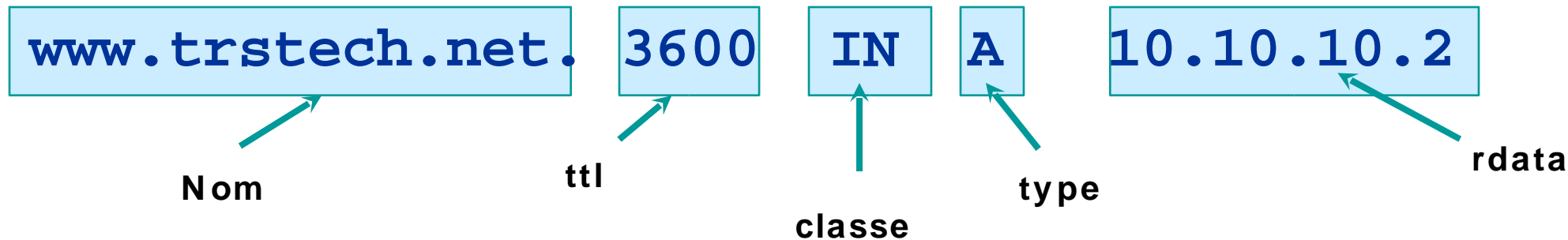
Question: www.ripe.net A





# Concept: Enregistrement de ressource(ER)

- Les enregistrements de ressources contiennent le nom propriétaire, son TTL, sa classe, son type et la donnée de la ressource
- Le TTL est un paramètre de minutage
- La classe IN( INTERNET) est la plus utilisée
- Il existe plusieurs types de ER
- Tout ce qui suit le type est appelé "donnée de ressource"



# Exemples: ERs dans un fichier de zone

```
trstech.net. 7200 IN SOA ns.trstech.net. alain.trstech.net. (  
    2001061501 ; Serial  
    43200 ; Refresh 12 hours  
    14400 ; Retry 4 hours  
    345600 ; Expire 4 days  
    7200 ; Negative cache 2 hours  
    )  
trstech.net. 7200 IN NS ns.trstech.net.  
trstech.net. 7200 IN NS rip.psg.com..
```

```
ns.trstech.net. 3600 IN A 81.199.105.10  
www.trstech.net. 3600 IN A 193.0.3.25
```

Nom ttl classe type rdata

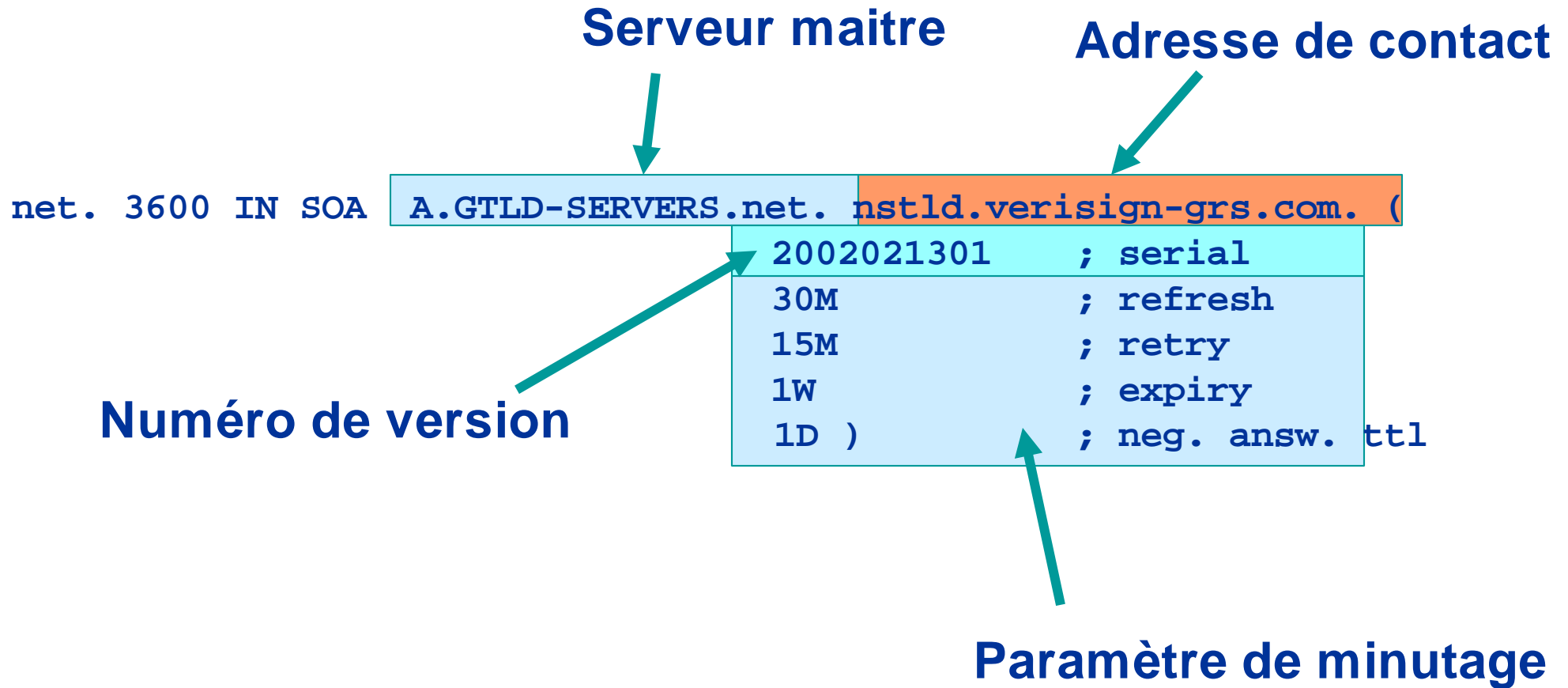
# ERs: SOA and NS

- Les enregistrements SOA et NS sont utilisés pour fournir des informations au fonctionnement du DNS.
- Les NS indiquent où trouver les informations d'une zone donnée:

```
trstech.net. 7200 IN NS ns.ripe.net.  
trstech.net. 7200 IN NS rip.psg.com.
```

- L'enregistrement SOA fournit les informations sur le début de l'autorité, i.e. le début de la zone, aussi appelé "A PEX".

# ER: SOA

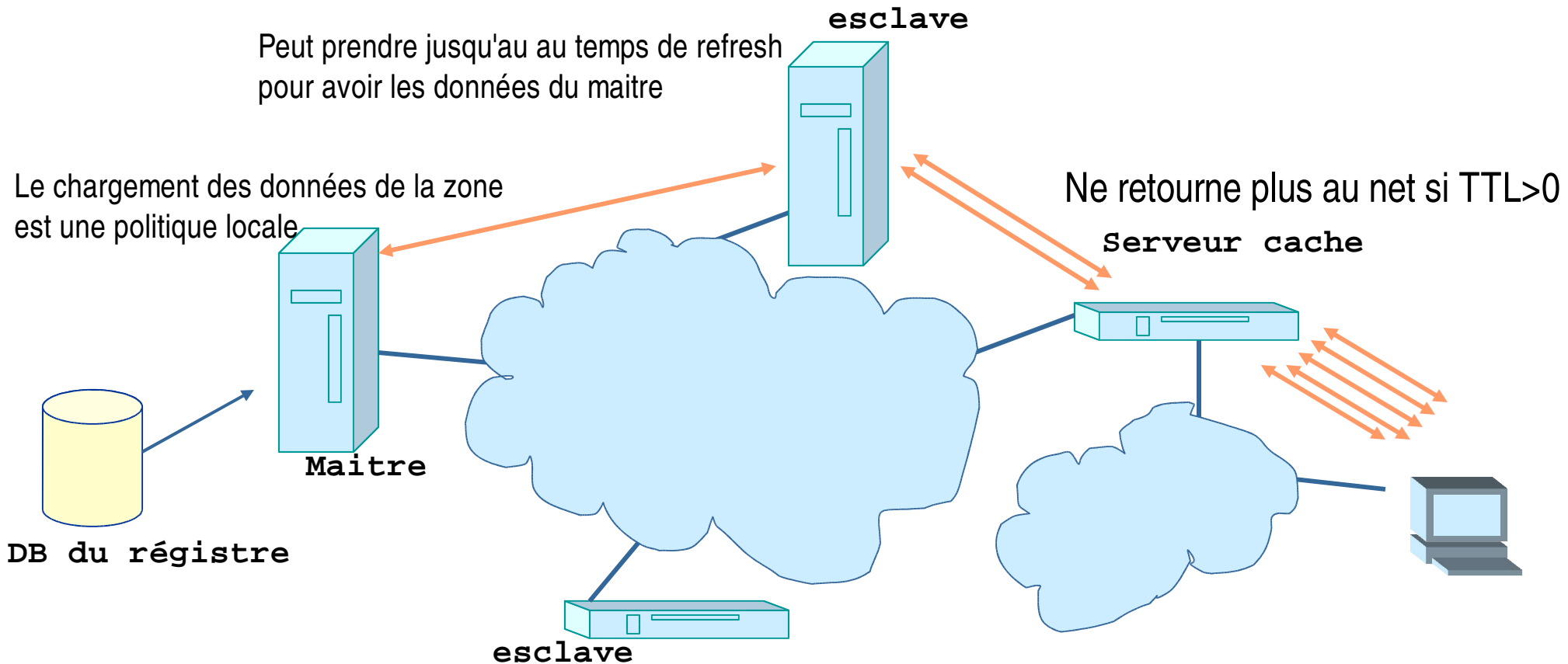


# Concept: TTL et autres minuteurs

- TTL est un minuteur utilisé dans les caches
  - Une indication de pendant combien de temps la donnée peut-être réutilisée
  - Les données supposées ‘stables’ peuvent avoir un TTL très élevé
- Les minuteurs du SOA sont utilisés pour maintenir la cohérence entre le primaire et les esclaves

# Endroits où vit la donnée DNS

Les changements dans le DNS ne se propagent pas instantanément!



# A ne pas oublier...

- Plusieurs serveurs autoritaires pour distribuer la charge et les risques:
  - **Bien choisir ses NS: RFC 2182**
- Utiliser les caches pour réduire la charge sur les serveurs autoritaires et pour réduire les temps de réponse
- Les minuteurs du SOA et le TTL ont besoin d'être réglés suivant les besoins de la zone.
  - Données stables : nombres élevés

# Qu'avons-nous appris!

## Qu'allons-nous apprendre

- Nous avons appris sur l'architecture:
  - "resolveurs",
  - Les serveurs récursifs et les forwarders,
  - Les serveurs autoritaires,
  - Les paramètres de minutage
- Nous continuons avec l'écriture des fichiers de zone



# L'écriture de fichier de zone.

- Le fichier de zone est écrit par l'administrateur de la zone
- Le fichier de zone est lu par le serveur primaire et son contenu est répliqué aux serveurs esclaves
- Le contenu du fichier de zone finira dans la base de données
- A cause des minuteurs, il pourrait s'écouler certains temps avant que la donnée ne soit visible par le client

# Premier essai

- L'entête du fichier de zone
  - Débuter avec l'enregistrement SOA
  - Inclure les serveurs de noms autoritaires et, si nécessaire, les "glue"
  - Ajouter les autres informations
- Ajouter les autres ERs
- Déléguer aux sous-zones

# L'enregistrement SOA

## Commentaires

```
secret-wg.org. 3600 IN SOA bert.secret-wg.org. (  
    olaf\.kolkman.ripe.net.  
    2002021301 ; serial  
    1h ; refresh  
    30M ; retry  
    1W ; expiry  
    3600 ) ; neg. answ. ttl
```

- Olaf.Kolkman@ripe.net → olaf\.kolkman.ripe.net
- Numéro de série: 32bits utilisant l'arithmétique circulaire
  - Les gens utilisent souvent le format date
  - A incrémenter après chaque changement dans la zone
- Les minuteurs ci-dessus sont raisonnables

# Enregistrements NS et enregistrements A relatifs

```
secret-wg.org.          3600 IN NS  bert.secret-wg.org.  
secret-wg.org.          3600 IN NS  NS2.secret-wg.org.  
bert.secret-wg.org.    3600 IN A   193.0.0.4  
NS2.secret-wg.org.     3600 IN A   193.0.0.202
```

- Enregistrements NS pour tous les serveurs autoritaires
- Enregistrements A seulement pour les NS “interne à la zone” .
  - Les NS de délégation peuvent avoir des "glue" associés.

# Autres données “APEX”

```
secret-wg.org. 3600 IN MX 50 mailhost.secret-wg.org.  
secret-wg.org. 3600 IN MX 150 mailhost2.secret-wg.org.  
  
secret-wg.org. 3600 IN LOC (  
                    52 21 23.0 N 04 57 05.5 E 0m 100m 100m 100m )  
secret-wg.org. 3600 IN TXT “zone pour le groupe de travail secret”
```

## Exemples:

- MX pour le mail  
(prochain slide)
- Enregistrements LOC
  - Situation géographique

Enregistrements TXT

Enregistrements A

Enregistrements KEY pour dnssec

# Enregistrement MX

- SMTP (simple mail transfer protocol) utilise les enregistrements MX pour trouver le serveur mail destinataire.
- Si un mail est envoyé à [aalain@trstech.net](mailto:aalain@trstech.net), l'expéditeur recherche les MX de trstech.net.
- Les enregistrements MX contiennent les relais mail avec priorité.
  - Le plus petit nombre a la plus grande priorité.
- N'ajouter pas de MX sans avoir un relai mail configuré

# Autres données dans la zone

```
localhost.secret-wg.org. 4500 IN A 127.0.0.1
```

```
bert.secret-wg.org. 3600 IN A 193.0.0.4
```

```
www.secret-wg.org. 3600 IN CNAME bert.secret-wg.org.
```

- Ajouter toutes les autres données à votre zone.
- Quelques infos sur la notation.
  - Noter les FQDN avec le point à la fin
  - Noter le TTL et la CLASSE

# Format de fichier de zone : présentation de base

```
secret-wg.org.          3600  IN SOA  bert.secret-wg.org. (
                        olaf\.kolkman.ripe.net.
                        2002021301      ; serial
                        1h              ; refresh
                        30M             ; retry
                        1W              ; expiry
                        3600 )          ; neg. answ. Ttl

secret-wg.org.          3600  IN NS   bert.secret-wg.org.
secret-wg.org.          3600  IN NS   NS2.secret-wg.org.
secret-wg.org.          3600  IN MX   50 mailhost.secret-wg.org.
secret-wg.org.          3600  IN MX   150 mailhost2.secret-wg.org.

secret-wg.org.          3600  IN LOC  ( 52 21 23.0 N 04 57 05.5 E
                        0m 100m 100m 100m )

secret-wg.org.          3600  IN TXT  "zone du groupe de travail secret"
NS2.secret-wg.org.      3600  IN A    193.0.0.202
localhost.secret-wg.org. 4500  IN A    127.0.0.1

bert.secret-wg.org.     3600  IN A    193.0.0.4
www.secret-wg.org.     3600  IN CNAME bert.secret-wg.org.
```



# Format de fichier de zone: répétition du dernier nom

```
secret-wg.org.          3600  IN SOA  bert.secret-wg.org. (
                        olaf\.kolkman.ripe.net.
                        2002021301      ; serial
                        1h              ; refresh
                        30M             ; retry
                        1W              ; expiry
                        3600 )          ; neg. answ. Ttl
                        3600 IN NS     bert.secret-wg.org.
                        3600 IN NS     NS2.secret-wg.org.
                        3600 IN MX     50 mailhost.secret-wg.org.
                        3600 IN MX     150 mailhost2.secret-wg.org.
                        3600 IN LOC    ( 52 21 23.0 N 04 57 05.5 E
                        0m 100m 100m 100m )
bert.secret-wg.org.     3600 IN TXT  "zone du groupe de travail secret"
NS2.secret-wg.org.     3600 IN A    193.0.0.4
                        3600 IN A    193.0.0.202
localhost.secret-wg.org. 4500 IN A    127.0.0.1
www.secret-wg.org.     3600 IN CNAME bert.secret-wg.org.
```

# Format de fichier de zone: TTL par défaut

```
$TTL 3600 ; directive de TTL par défaut
secret-wg.org.      IN SOA bert.secret-wg.org. (
                                olaf\.kolkman.ripe.net.
                                2002021301      ; serial
                                1h              ; refresh
                                30M             ; retry
                                1W             ; expiry
                                3600 )         ; neg. answ. Ttl

                                IN NS      bert.secret-wg.org.
                                IN NS      NS2.secret-wg.org.
                                IN MX      50 mailhost.secret-wg.org.
                                IN MX      150 mailhost2.secret-wg.org.

                                IN LOC     ( 52 21 23.0 N 04 57 05.5 E
                                                0m 100m 100m 100m )
                                IN TXT     "zone du groupe de travail secret"
bert.secret-wg.org.  IN A      193.0.0.4
NS2.secret-wg.org.  IN A      193.0.0.202

localhost.secret-wg.org. 4500 IN A      127.0.0.1

www.secret-wg.org.     IN CNAME bert.secret-wg.org.
```

# Format de fichier de zone: ORIGIN

```
$TTL      3600 ; directive de TTL par défaut
$ORIGIN  secret-wg.org.
@                IN SOA  bert (
                                olaf\.kolkman.ripe.net.
                                2002021301      ; serial
                                1h              ; refresh
                                30M             ; retry
                                1W             ; expiry
                                3600 )         ; neg. answ. Ttl

                IN NS   bert
                IN NS   NS2
                IN MX   50 mailhost
                IN MX   150 mailhost2

                IN LOC  ( 52 21 23.0 N 04 57 05.5 E
                          0m 100m 100m 100m )
                IN TXT  "zone du groupe de travail secret"

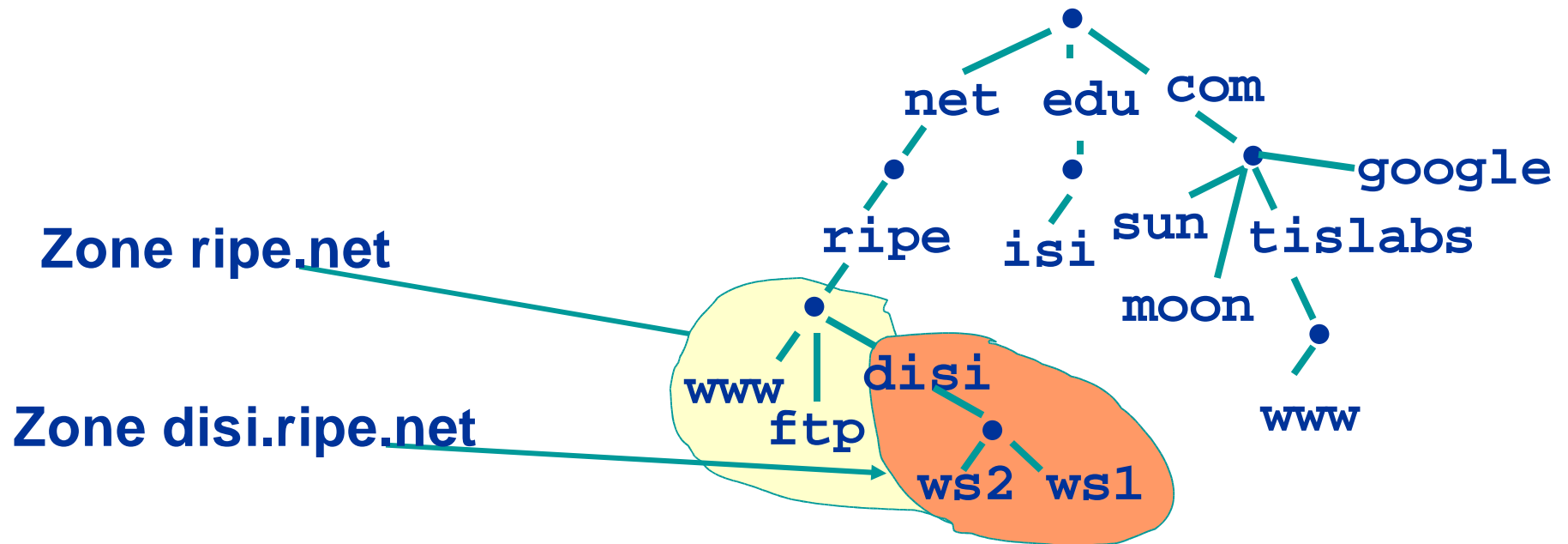
bert          IN A    193.0.0.4
NS2          IN A    193.0.0.202

localhost 4500 IN A    127.0.0.1

www         IN CNAME bert
```

# Délégation d'une sous-zone (Devenir parent)

- Délégation de l'autorité pour le sous-domaine à une autre partie (séparation de disi.ripe.net de ripe.net)



# Concept: "Glue"

- La délégation est faite en ajoutant les enregistrements NS

```
disi.ripe.net.      NS      ns1.disi.ripe.net.
```

```
disi.ripe.net.      NS      ns2.disi.ripe.net.
```

- Comment aller à ns1 et ns2. Nous avons besoin des adresses.
- Ajouter les enregistrements "glue" pour permettre aux résolveurs d'atteindre ns1 et ns2.


```
ns1.disi.ripe.net. A 10.0.0.1
```

```
ns2.disi.ripe.net. A 10.0.0.2
```

# Concept:” Glue” (suite)

- Les enregistrements “g lue” ne sont pas des données **autoritaires**
- N'ajouter pas de “glue” pour les NS qui ne sont pas dans la sous-zone

```
disi.ripe.net.      NS      ns1.disi.ripe.net.  
disi.ripe.net NS      ns2.ripe.net.  
disi.ripe.net NS      ns.bert.secret-wg.org.  
ns1.disi.ripe.net. A      10.0.0.1
```



Seul cet enregistrement a besoin de “glue”

# Délégation de disi.ripe.net. à partir de ripe.net.

## disi.ripe.net

- Configurer au moins deux servers autoritaires
- Créer le fichier de zone avec SOA et NS sur le maitre
- Ajouter toutes les données de disi.ripe.net
- S'assurer que les esclaves ont transféré la zone

## ripe.net

- Ajouter les NS et les glue
- S'assurer qu'il n'y a plus de données de la zone disi.ripe.net. dans le fichier de zone.

# Devenir enfant en général

- Acheter votre domaine avec votre régistreur/régistrare favori
- Configurer vos NS
- Enregistrer vos NS: votre régistreur communiquera les NS au régistreur qui s'assurera que les NS sont publiés.
  - Ce processus peut prendre des heures ou des jours.
- Le Régistreur/régistrare peut nécessiter des configurations spéciales