DNS 101
Comment ça marche ?

Yazid AKANHO
Office of the CTO – ICANN
Yazid.Akanho@icann.org

Oct. 2025

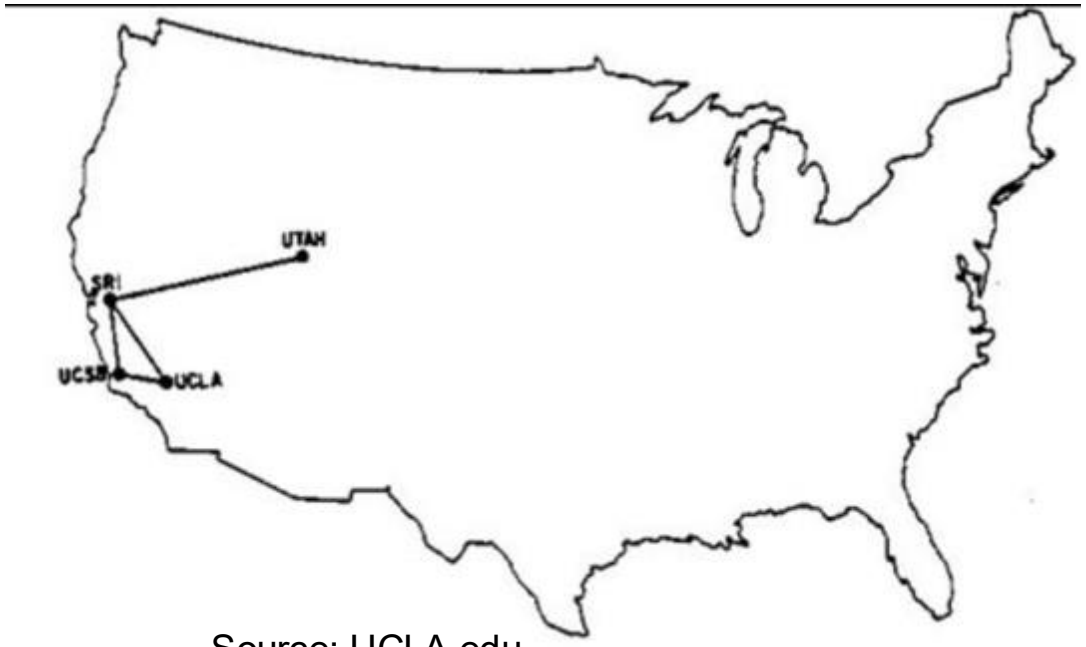
Agenda

1. Il était une fois…
2. Évolution du DNS
3. Base de données et données DNS, processus de résolution
4. Résilience, Aperçu de l'administration de la Zone Racine.

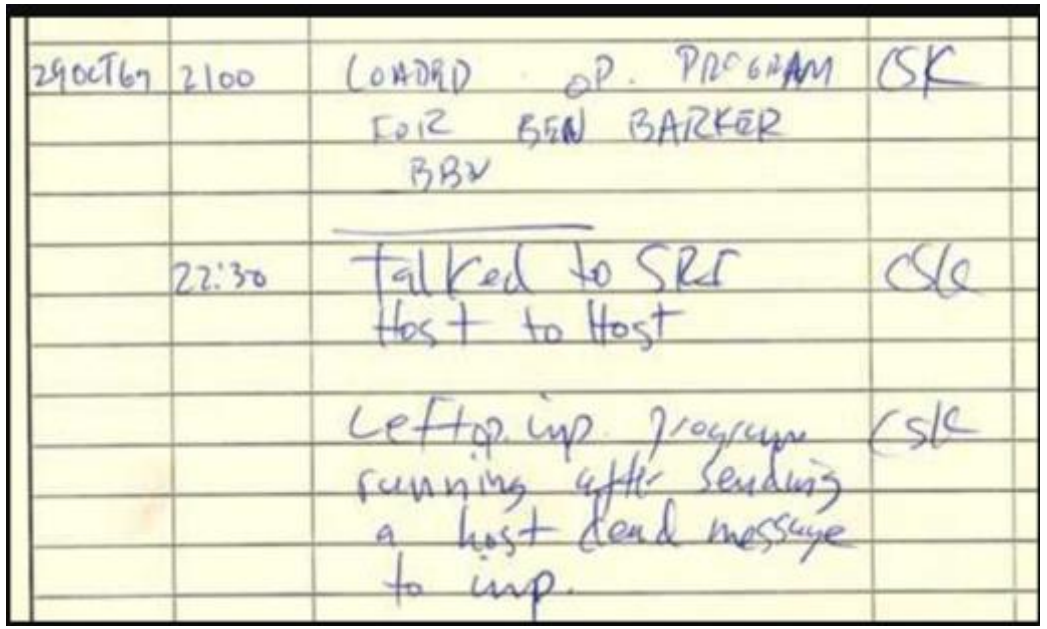
Il était une fois…

Le réseau des réseaux

- 1969 - ARPANET naissait le 29 Octobre – 04 Institutions participantes:
  - Université de Californie, Los Angeles (UCLA)
  - Stanford Research Institute (SRI)
  - Université de Californie, Santa Barbara
  - Université de l'Utah



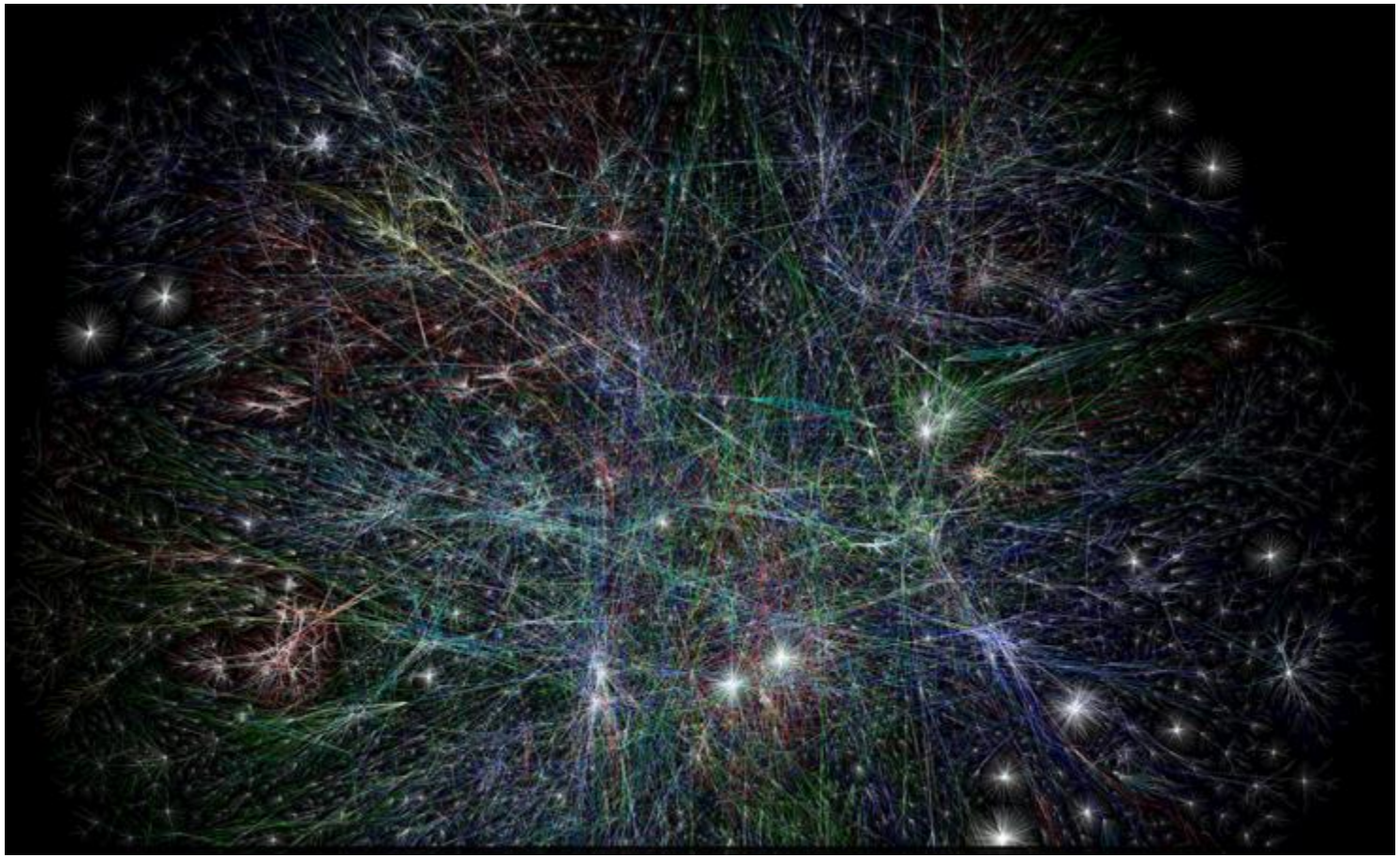
Source: UCLA.edu



Source: edn.com

Le réseau des réseaux

Source: sri.com

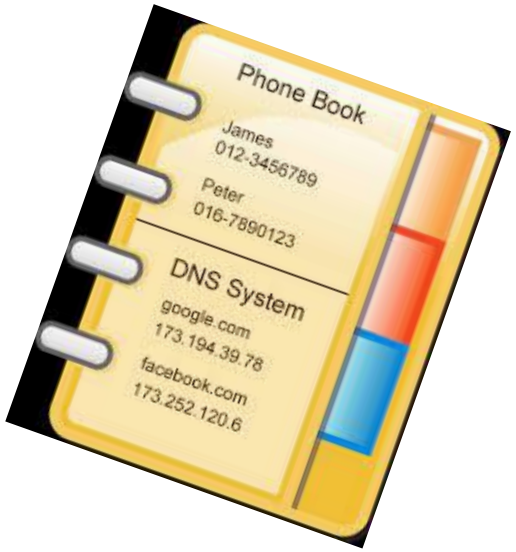


Source: Kaspersky.com

Le réseau des reseaux : +100.000 réseaux ; kirielle de services

Noms et Nombres

- Les appareils sont identifiés sur Internet à l'aide d'adresses IP.
  - IPv4: 192.0.2.7
  - IPv6: 2001:db8::7
- Les adresses IP sont faciles à utiliser pour les machines, les humains préfèrent utiliser des noms.
- Au début de l'Internet, les noms étaient au format simple
  - Il n'y avait pas encore de noms de domaine
  - « Noms d'étiquettes uniques », 24 caractères maximum
  - Appelés noms d'hôte



Résolution de nom

- Le processus permettant de déterminer l'adresse IP à partir du nom (ou le nom à partir de l'adresse IP) est appellee ***résolution de nom (ou resolution inverse).***
- Au début d'Internet, la resolution de noms était basée sur le fichier en clair appelé HOSTS.TXT
  - Même fonction mais format légèrement différent du fichier /etc/hosts
  - Maintenance centralisée par le NIC (Network Information Center) du Stanford Research Institute (SRI)
  - Les administrateurs réseau envoyaient les mises à jour par e-mail.
- Dans l'idéal, tout le monde avait la dernière version du fichier
  - Publié une fois par semaine
  - Téléchargeable via FTP

Problèmes avec HOSTS.TXT

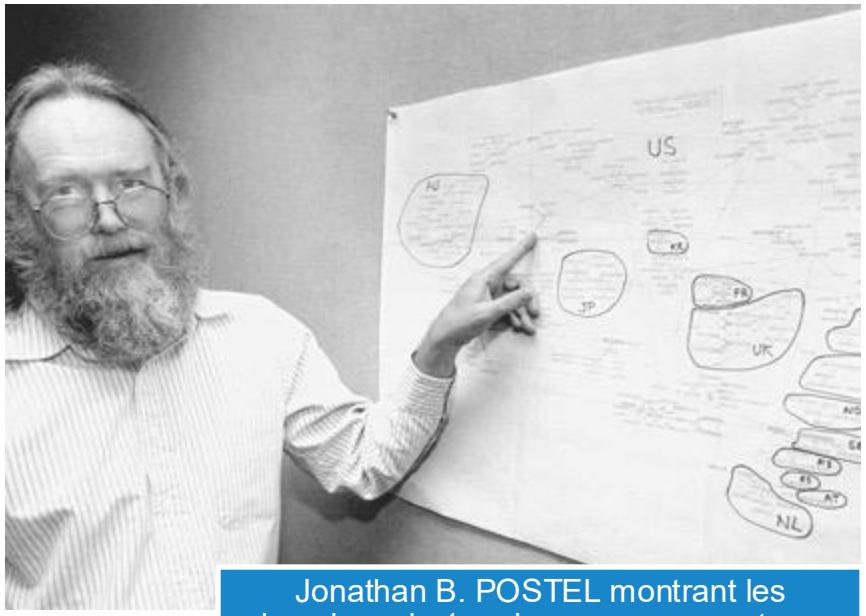
- Contention de nommage
  - Modifications effectuées à la main dans un fichier texte (pas de base de données)
  - Pas de bonne méthode pour empêcher les doublons
- Synchronisation
  - Difficile d'avoir la version à jour du fichier
- Trafic et charge
  - Bande passante importante requise pour télécharger le fichier
- **Difficile de répliquer ce fichier maintenu de manière centralisée.**

DNS à la rescousse

- Les discussions pour un remplacement ont commencé au début des années 1980
- Objectifs:
  - Résoudre la difficulté de réplication de HOST.TXT
  - Simplifier le routage des e-mails
- Résultat obtenu: le Système des Noms de Domaine ou ***Domain Name System (DNS)***
- Spécifications documentées dans plusieurs RFC:
  - RFC 799, “Internet Name Domains”
  - RFC 819, “The Domain Naming Convention for Internet User Applications”
  - RFC 882, “Domain names – concepts and facilities”

Paul MOKAPETRIS et John POSTEL

Paul MOKAPETRIS

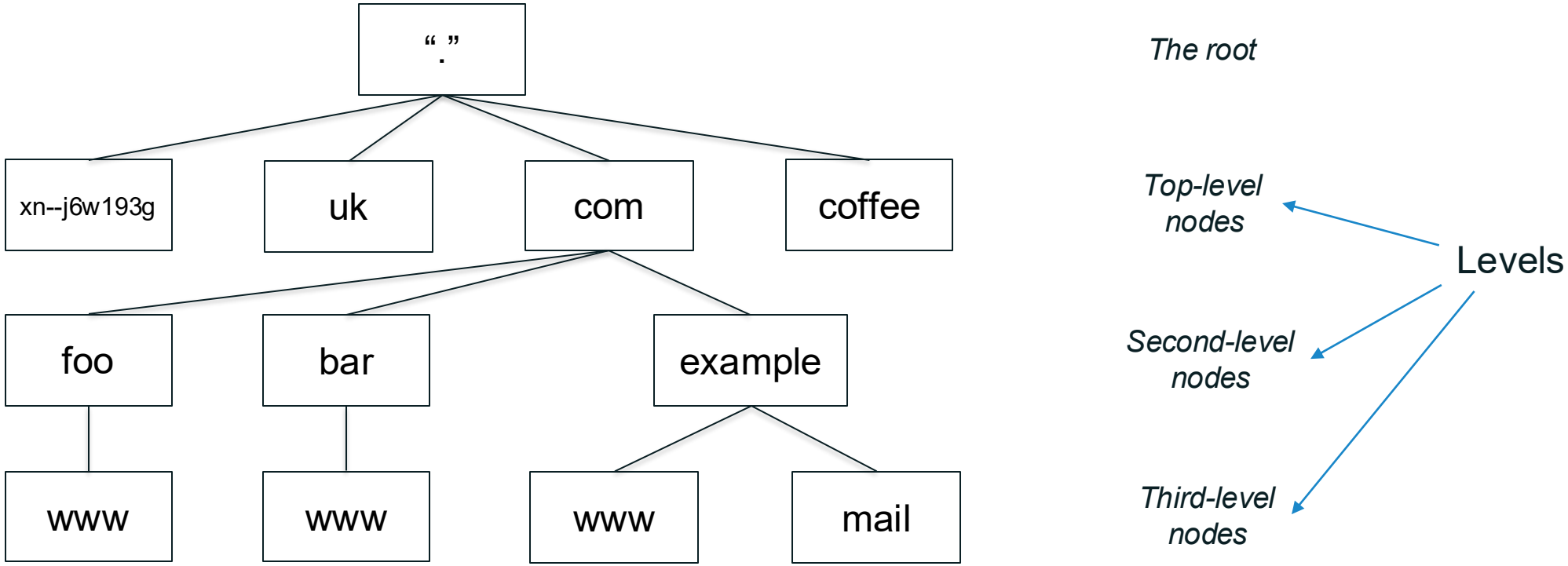


Jonathan B. POSTEL montrant les domaines de 1er niveau sur une carte en 1994

Evolution du DNS !

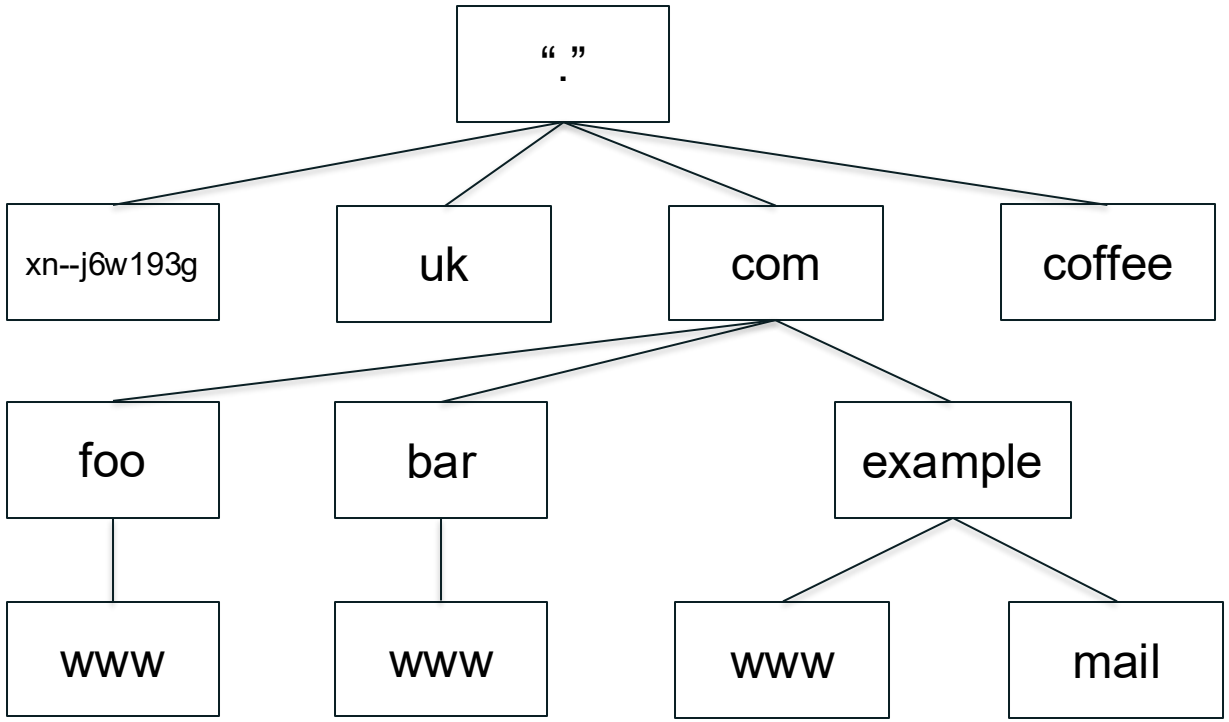
L’espace de nommage

- La structure de la base de données DNS est un **arbre inversé** appelé *l’espace de nommage*
- Chaque nœud a une étiquette
- Le nœud racine (et uniquement le nœud racine) a une étiquette null



Syntaxe de l’étiquette

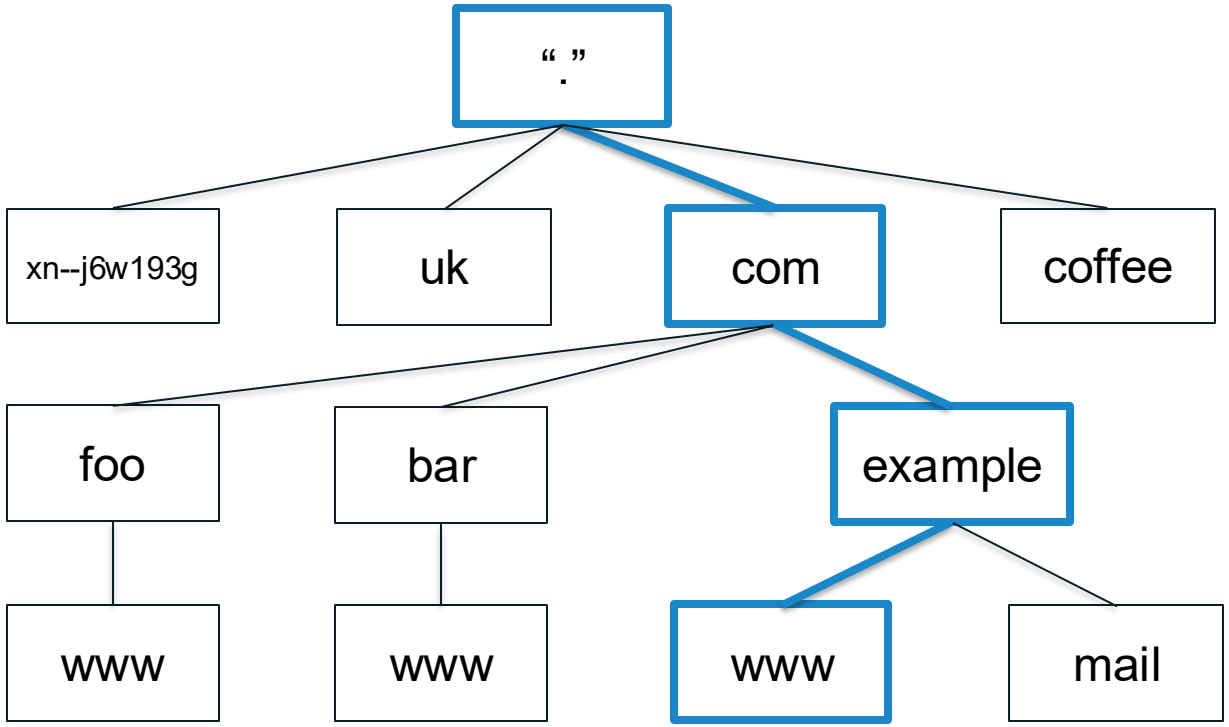
- Les caractères autorisés pour les noms sont: lettres, chiffres, trait d’union (**LDH**)
- Longueur maximale: 63 caractères
- Les comparaisons de noms ne sont pas sensibles à la case (RFC 4343)



Noms de Domaine et FQDN

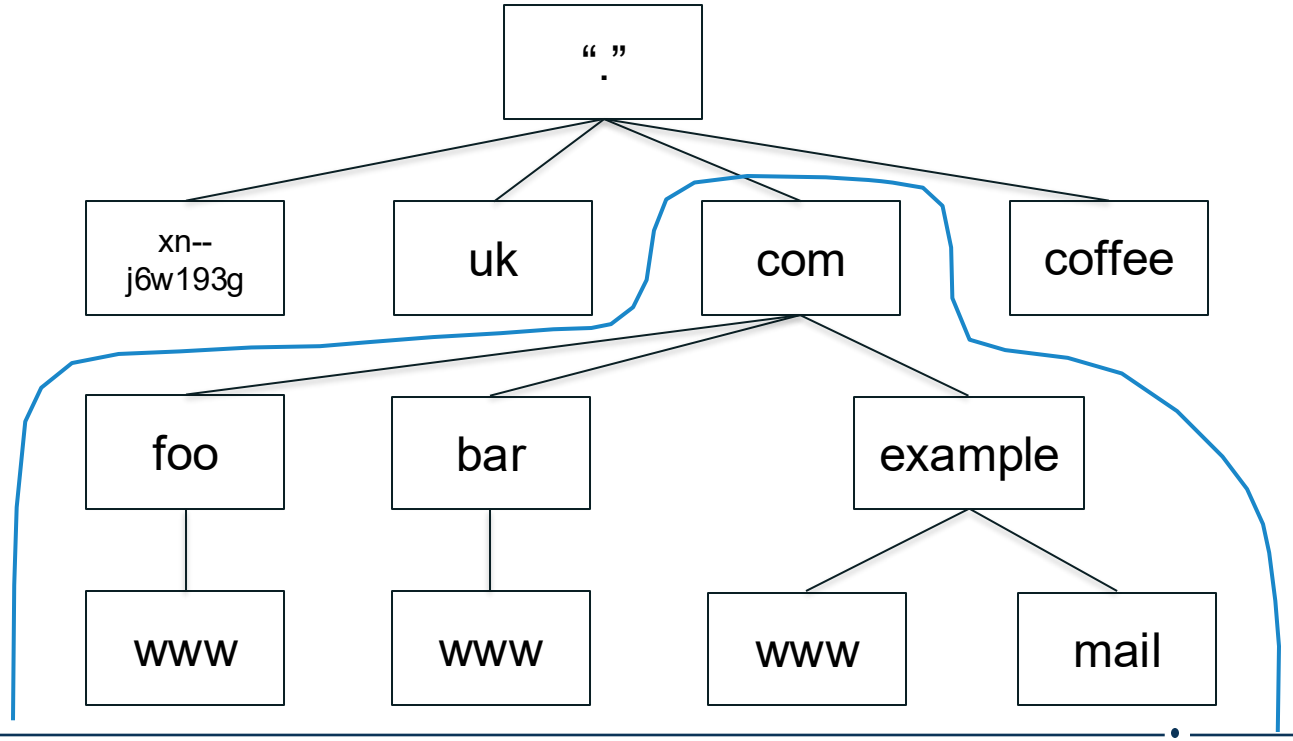
- Chaque noeud possède un ***nom (nom de domaine)***
- Obtenu en combinant du bas vers le haut les étiquettes de chaque noeud, du noeud dont il est question jusqu'à la racine, en séparant par un "."
- Exemple: *www.example.com*
- ***Fully Qualified Domain Name (FQDN)*** identifie de façon unique un noeud.

  Pas lié à un autre nom de domaine.
- Un FQDN finit par un "."
- Exemple de FQDN: *www.example.com.*

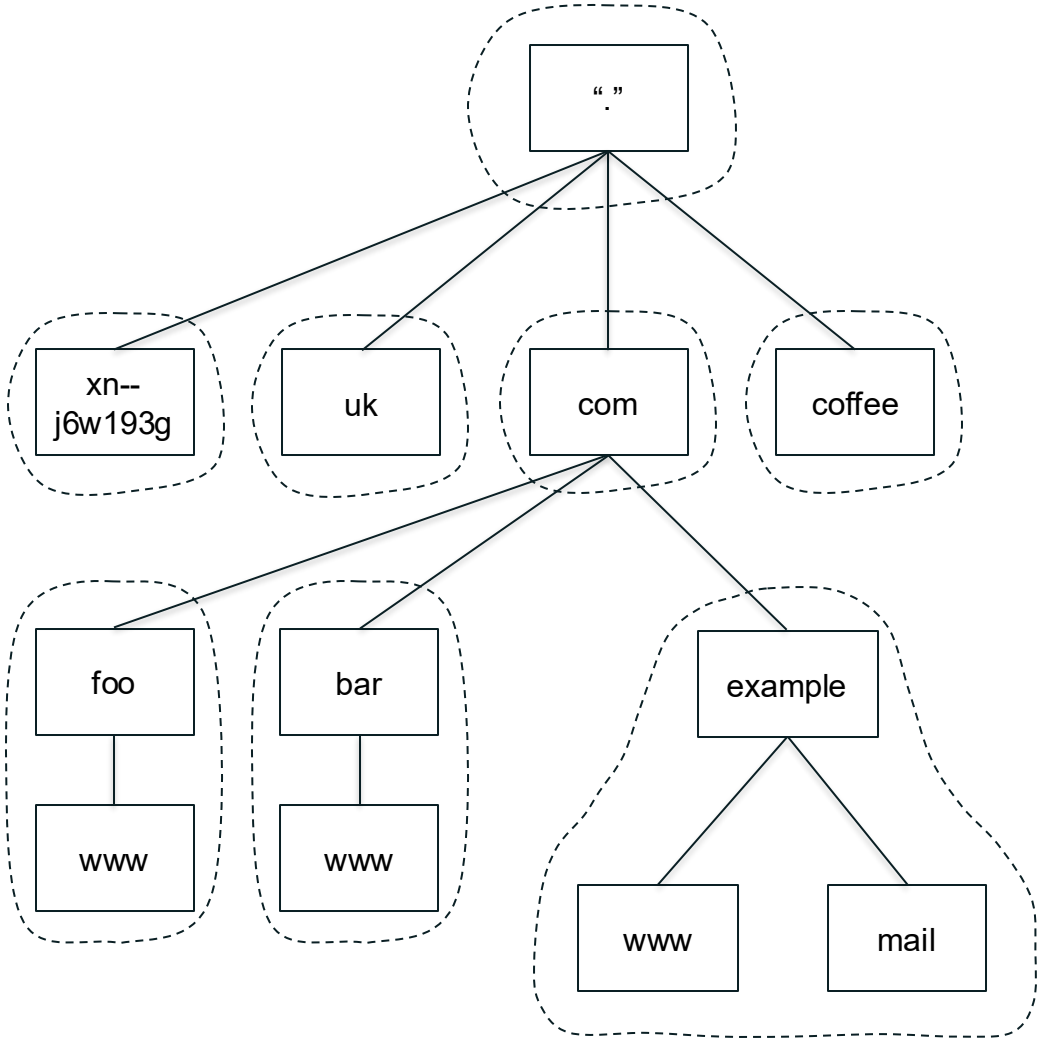


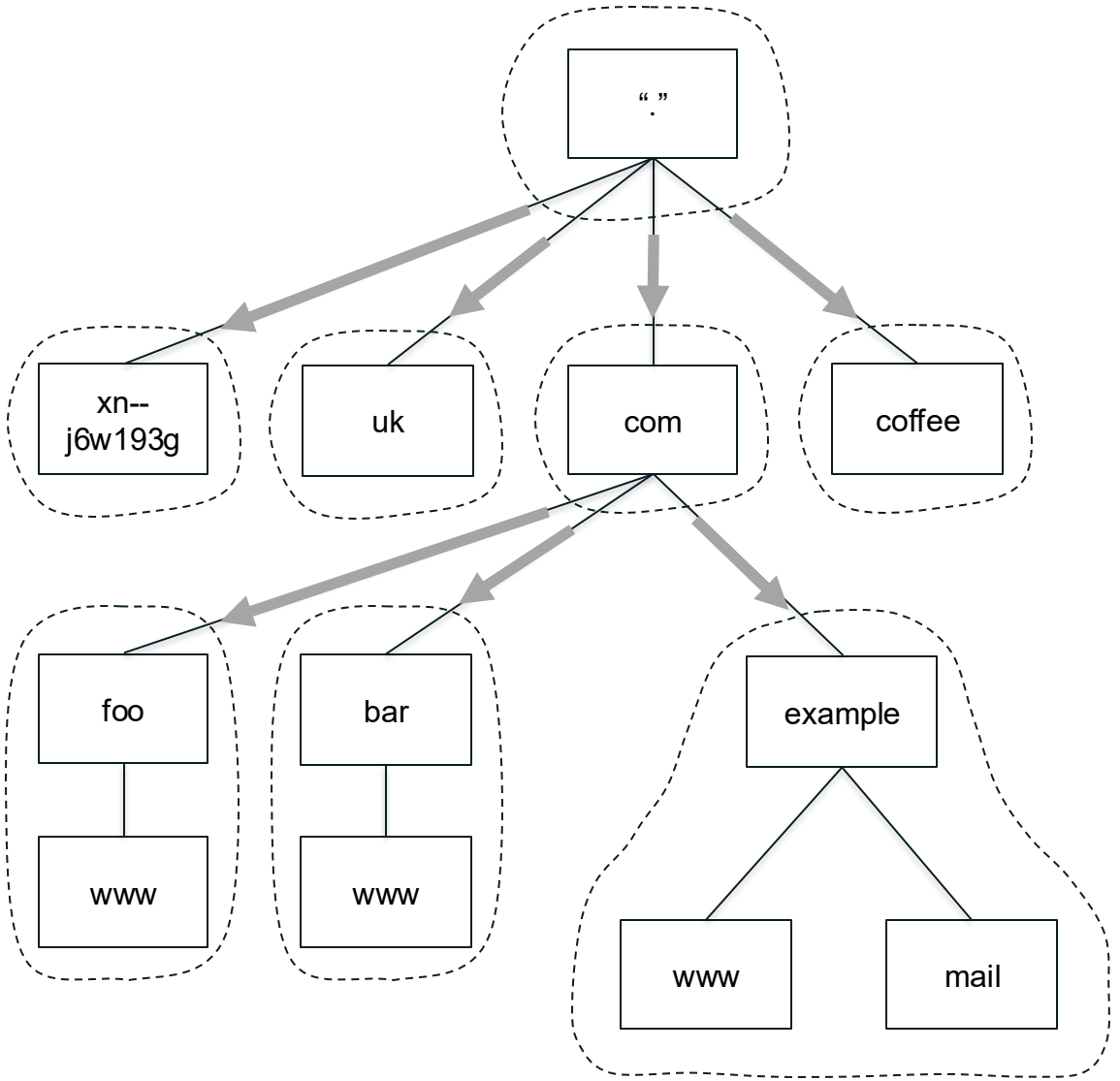
Domaines Vs Zones

- Un ***domaine*** est un noeud avec tout ce qu'il renferme en dessous de lui.
- Le noeud de tête d'un domaine est appelé ***apex*** du domaine. Exemple: le domaine *com*
- Une ***zone*** est une division administrative de l'espace de nom afin de permettre une administration distribuée.
- L'administrateur d'une zone peut librement déléguer l'administration d'une partie de cette zone, ce qui crée une nouvelle zone.
- ***Les Délégations créent des zones***
  - La zone qui délègue est apellée ***parent***
  - La zone créée est apellée ***child (enfant)***



Zones: frontières administratives et délégations





Base de données et données DNS

Données DNS

- Le standard DNS spécifie le format des données DNS transmises à travers le reseau.
- Le standard spécifie également une representation des données au format texte et appellée “master file format”, utilisé pour stocker les données (un peu comme les tables en base de données.)
- Un fichier de ***zone*** comporte toutes les données de cette zone au format master file format.

Enregistrements DNS

- Pour rappel, chaque noeud dispose d'un nom de domaine.
- Un nom de domaine peut posséder differentes sortes de données.
- Ces données sont appelées ***enregistrements de ressource,*** en anglais ***Ressource Reccord (RR)***
- Il existe plusieurs types d'enregistrements de resource correspondant chacun à un type de données.

Fichiers de zone

- Une zone se compose de plusieurs enregistrements de ressources
- Tous les enregistrements de ressources d'une zone sont stockés dans un fichier de zone
- Chaque zone a (au moins) un fichier de zone
- Les enregistrements de ressources provenant de plusieurs zones ne sont jamais rassemblés dans un même fichier.

Format des enregistrements (Resource Records)

- Un enregistrement de ressource dispose de cinq champs:
  - ***Owner (propriétaire)***: Nom de domaine auquel est associé l'enregistrement de ressource
  - ***Time to live (TTL)***: temps (en secondes) pendant lequel l'enregistrement peut être mis en cache (à étudier plus tard)
  - ***Class***: Un mécanisme d'extension très peu utilisé
  - ***Type***: type de données contenue dans l'enregistrement
  - ***RDATA***: donnée que transporte l'enregistrement (du type spécifié correspondant)

Format du Master File

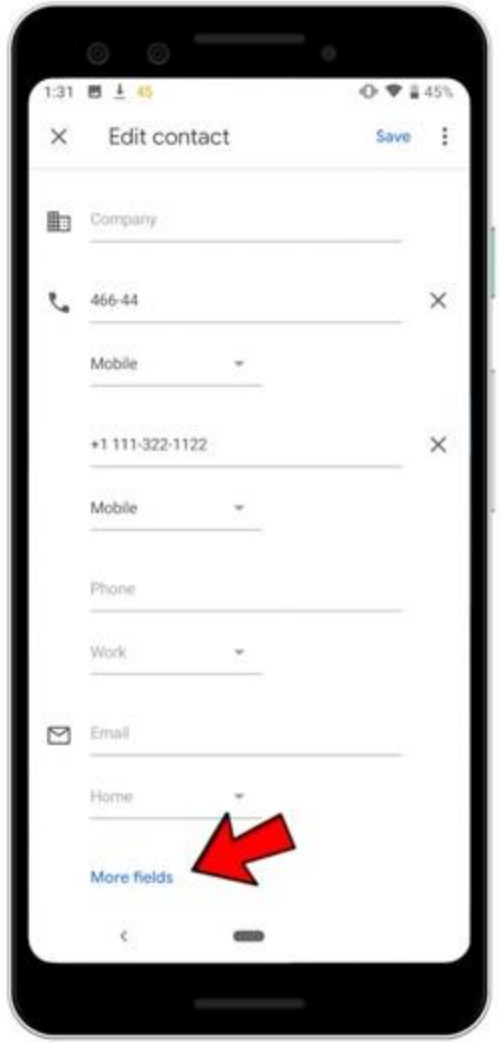
- Syntaxe d’un enregistrement de ressource dans le master file:

```
[owner]   [TTL]   [class]   <type>   <RDATA>
```

- Les champs entre crochet sont facultatifs
- Les champs Type et RDATA sont obligatoires.

Types d’enregistrements de ressources courants

- **A** adresse IPv4
- **AAAA** adresse IPv6
- **NS** Nom d’un serveur de noms faisant autorité
- **SOA** “Start of authority”, apparaît à l’apex de la zone
- **CNAME** Nom d’un alias vers un autre nom de domaine
- **MX** Nom d’un « serveur de messagerie »
- **PTR** Adresse IP codée en tant que nom de domaine (pour la resolution inverse)



Une multitude de types d’enregistrement de ressource

- Il existe de nombreux autres types d’enregistrements de ressources
- +87 types attribués: *http://www.iana.org/assignments/dns-parameters/dns-parameters.xhtml#dns-parameters-4*

Enregistrements de type adresse IP (A & AAAA)

- L'utilisation la plus courante de DNS consiste à associer des noms de domaine à des adresses IP
- Les deux principaux types d'enregistrement de resource sont:
  - Enregistrement A: fait le lien entre un nom de domaine et une adresse IP

```
example.com.            A           192.0.2.7
```

  - Enregistrement "Quad A" (AAAA): associe un nom de domaine à une adresse IPv6

```
example.com.            AAAA        2001:db8::7
```

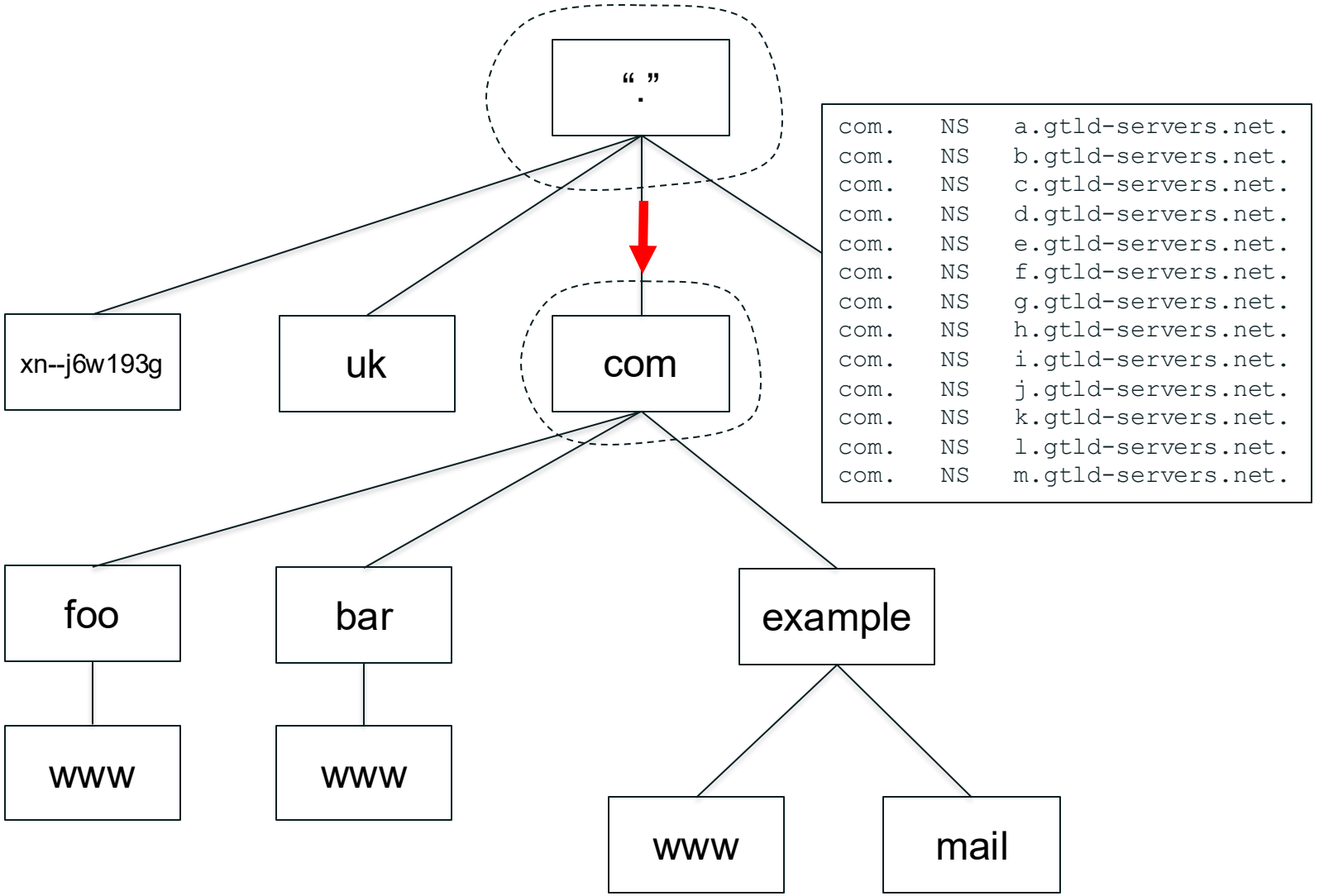
Name Server (NS)

- Spécifie un serveur de noms faisant autorité pour une zone
- Seul type d'enregistrement apparaissant à deux niveaux
  - Zones "Parent" and "enfant"

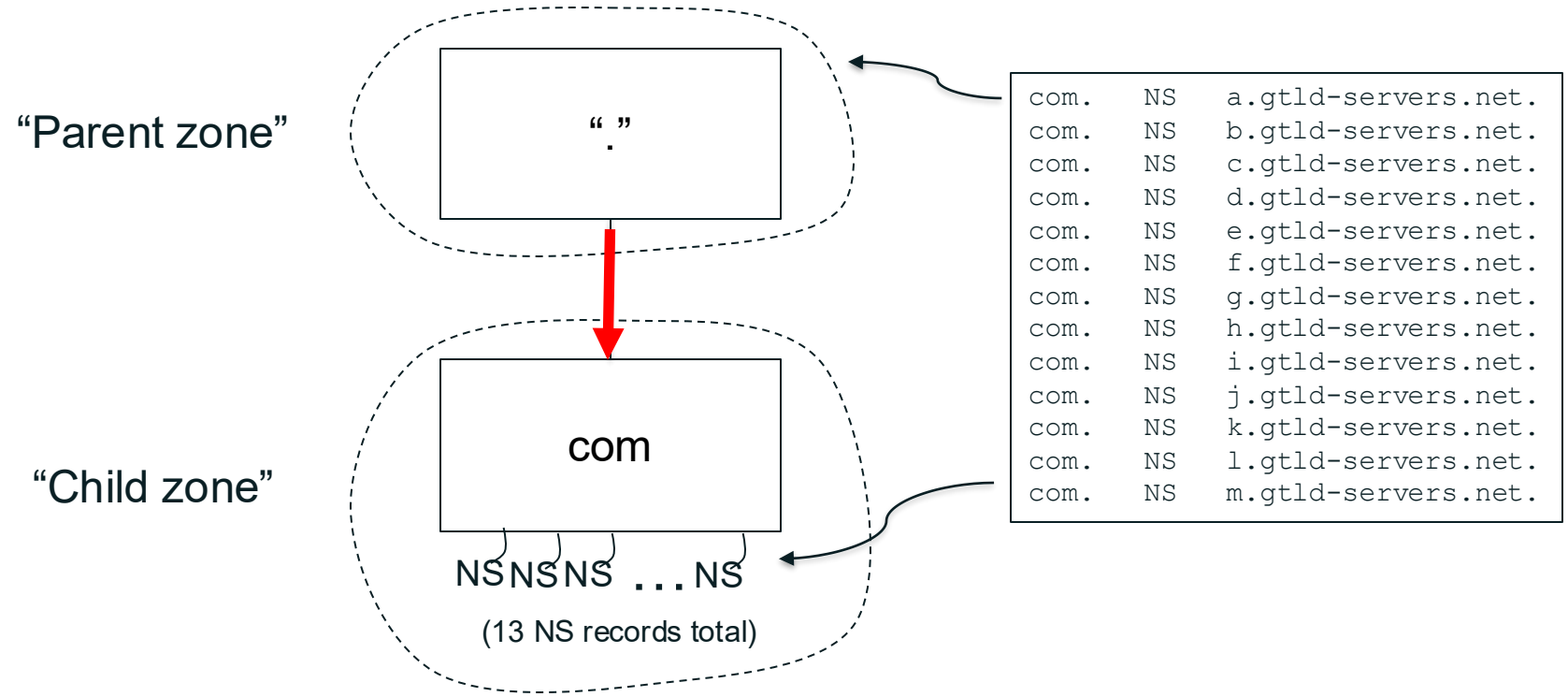
```
example.com.    NS    ns1.example.com.
example.com.    NS    ns2.example.com.
```

- A gauche, se trouve le nom de la zone
- A droite, nom du serveur de nom autoritaire (faisant autorité) sur la zone.
  - Attention: Il ne s'agit pas d'une adresse IP!

Les enregistrements de type NS représentent la délégation



Les enregistrements NS apparaissent en deux endroits

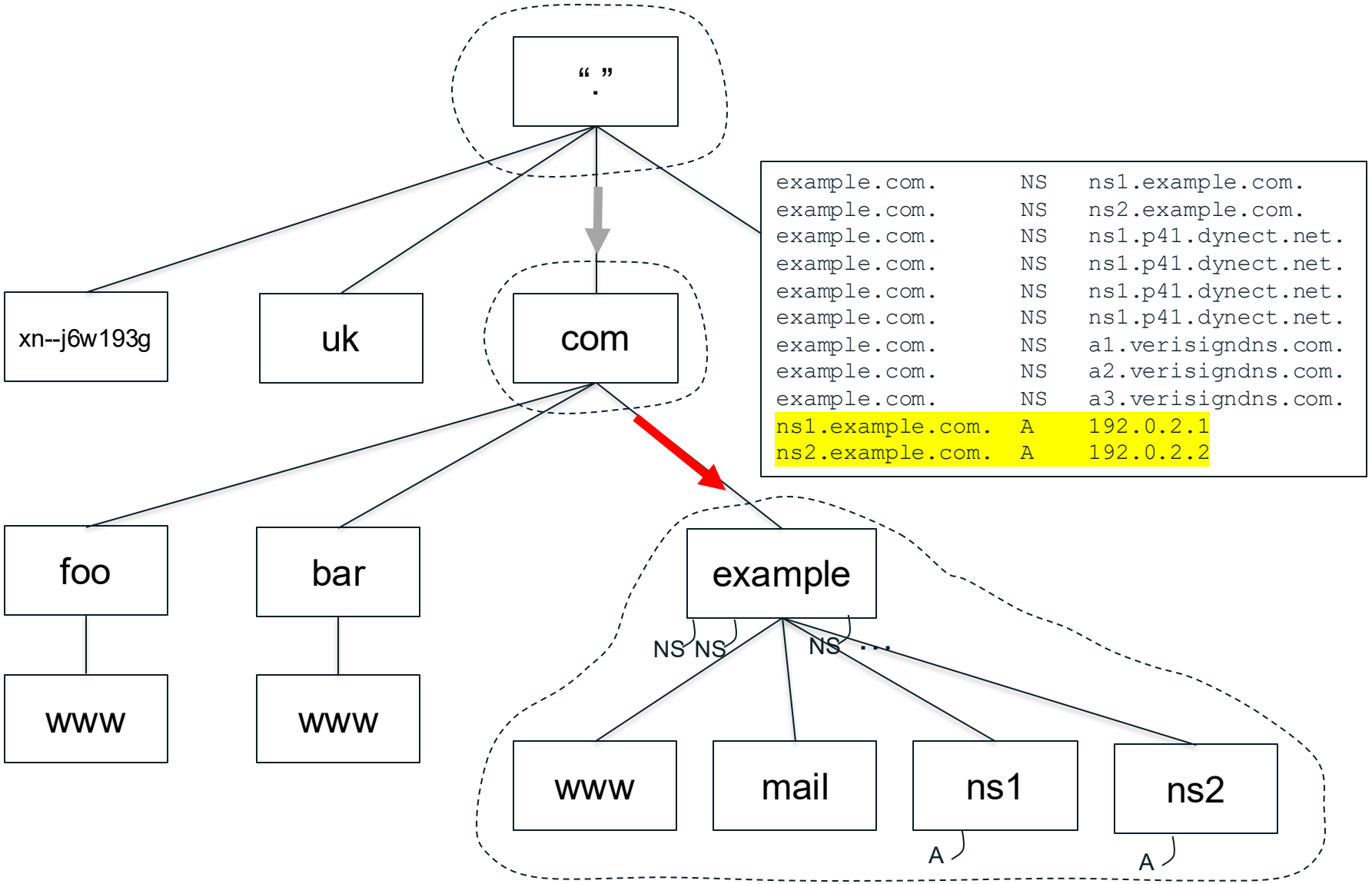


Glue Records

- Un glue record est:
  - Un enregistrement A ou AAAA associé à l'enregistrement NS dont l
  - Inclue dans la liste des données de delegation continues dans la zone parent
- utile pour rompre la dépendance circulaire lorsque le nom du serveur de noms se termine par le nom de la zone déléguée

```
example.com.    NS    ns1.example.com.
```

Exemple de glue record



Pratique

1. Identifiez les enregistrements NS de votre ccTLD
2. Identifiez l'adresse IP de ces NS
3. Identifiez les enregistrements d'adresses IP du site Web et des serveurs de messagerie de votre organisation.
4. Les TTL des enregistrements ci-dessus sont-ils les mêmes ? Veuillez utiliser la réponse faisant autorité (drapeau aa !) pour répondre.
5. Vérifiez si les informations de délégation de votre ccTLD dans la zone racine correspondent aux informations de zone.

Start of Authority (SOA)

- Contient des informations administratives à propos de la zone.
- Chaque domaine doit avoir un enregistrement de ressource Start of Authority là où la délégation lui a été faite au niveau de la zone parent.
- SOA indique qu'un serveur de noms fait autorité pour un domaine. Si nous ne recevons pas un RR SOA dans une réponse de requête à partir d'un serveur, cela indique que le serveur ne fait pas autorité pour ce domaine.
- Les serveurs de noms DNS sont normalement configurés en clusters (master et secondaires). La base de données de chaque cluster est synchronisée par le biais de transferts de zone. Les données d'un enregistrement SOA pour une zone sont utilisées pour contrôler le transfert de zone.

Start of Authority (SOA)

SOA contient les champs suivants:

- ***mname***: le principal serveur de nom pour le domaine, ou le 1er serveur de nom dans la liste des serveurs de nom pour ce domaine. Ex: *example.com*, mname *ns1.example.com*.
- ***rname***: l'adresse e-mail d'un responsible technique du domaine. Pour une adresse mail *john.doe@example.com; on aura* john\.doe.example.com .
- ***serial***: Le numéro de version de la copie originale de la zone (ne change pas Durant les transferts de zone). Si un serveur de noms secondaires asservi à celui-ci observe une augmentation de ce nombre, l'esclave supposera que la zone a été mise à jour, et il lancera un transfert de zone. Les mises à jour de zone sont indiquées par le cachet de date et d'heure (ex: si update le19 March 2020 at 15:55:00hs le serial pourrait être 20200316155500).

Start of Authority (SOA) (2)

- ***refresh***: Nombre de secondes avant qu'un NS secondaire ne vérifie les mises à jour de zone. Généralement 24hs (86400 s).

- ***retry:*** Nombre de secondes avant qu'un rafraîchissement (failed ***refresh***) qui a échoué soit repris. Valeur normalement inférieure à *refresh*. En général 2hs (7200 s).

- ***expire***: Limite supérieure en secondes avant qu'un serveur de noms secondaires ne cesse de répondre aux demandes de la zone si le maître ne répond pas. Généralement, 1000hs (360000 s).

Start of Authority (SOA) (3)

- ***minimum***: Le TTL pour des caching négatifs (temps pendant lequel le resolver gardera cette ***réponse negative*** comme valide avant une nouvelle tentative).

```
example.com.        SOA   ns1.example.com. John\.doe.example.com. (
                           20200316155500 ; serial
                           86400          ; refresh (1 day)
                           7200           ; retry (2 hours)
                           3600000        ; expire (1000 hours)
                           172800 )       ; minimum (2 days)
```

CANNONICAL NAME (CNAME)

- Le nom canonique (CNAME) est normalement utilisé pour alias un nom à un autre (mais ne le confondez pas avec un ALIAS). Dans le cas de CNAME, il ne devrait pas y avoir d'autres enregistrements sur le même nom.

- À titre d'exemple, supposons que nous voulons avoir à la fois example.com et www.example.com pointant vers le même serveur example.com, l'enregistrement devrait être:

```
www.example.com.   CNAME example.com.
```

- **UN CNAME pointe toujours vers un nom (pas une adresse IP).**

- Ailleurs, un peu plus loin, il devrait y avoir un enregistrement :

```
example.com.                A               192.0.2.7
```

CANNONICAL NAME (CNAME)

- Quelques limites:
  - Les enregistrements CNAME ne doivent pas pointer directement vers une adresse IP, mais toujours vers un autre nom de domaine.
  - Les enregistrements CNAME ne peuvent pas coexister avec un autre enregistrement pour le même nom. Il n'est pas possible d'avoir à la fois un enregistrement CNAME et TXT pour www.example.com.
  - Un CNAME peut pointer vers un autre CNAME, bien qu'il ne soit généralement pas recommandé pour des raisons de performance. Le CNAME doit pointer le plus près possible du nom de la cible afin d'éviter les problèmes de performance.
  - Il n'y a pas de corrélation directe entre un CNAME et une redirection HTTP. La configuration d'un CNAME n'entraîne pas automatiquement de redirection HTTP.
  -

Mail Exchange (MX)

- Le problème de routage du courrier : où le courrier pour user@example.com doit-il aller ?
- Dans le bon vieux temps: rechercher l'adresse de example.com et livrer via SMTP à cette adresse
  - Défaut de flexibilité: nom de domaine dans l'adresse e-mail doit être (aussi) un serveur de messagerie
  - N'était pas un souci à l'époque de HOST.TXT : les e-mails étaient au format *user@host*
  - Mais que faire si l'adresse e-mail est un hôte qui n'est pas sur Internet?
    - E.g., UUCP
  - Ou, vous voulez que le serveur de messagerie sur un serveur différent du serveur de ce domaine?
- DNS offre plus de flexibilité.

Mail Exchange (MX)

- Spécifie un serveur de messagerie et une préférence pour chacun.

```
example.com.   MX   10 mail.example.com.
example.com.   MX   20 mail-backup.example.com.
```

- Le nom du propriétaire correspond au nom de domaine dans une adresse e-mail, c'est-à-dire à la droite de l'«@»
- La preference est un nombre après le "MX", le plus bas est préféré.
- Le champ le plus à droite est le nom de domaine d'un serveur de messagerie qui accepte lee mails.

Pratique !

1. Recherchez l’enregistrement SOA pour :
2. votre ccTLD
3. le domaine de votre organisation.
4. Quelques autres ccTLD et autres noms de domaines
5. Commentez les valeurs respectives des différents champs.

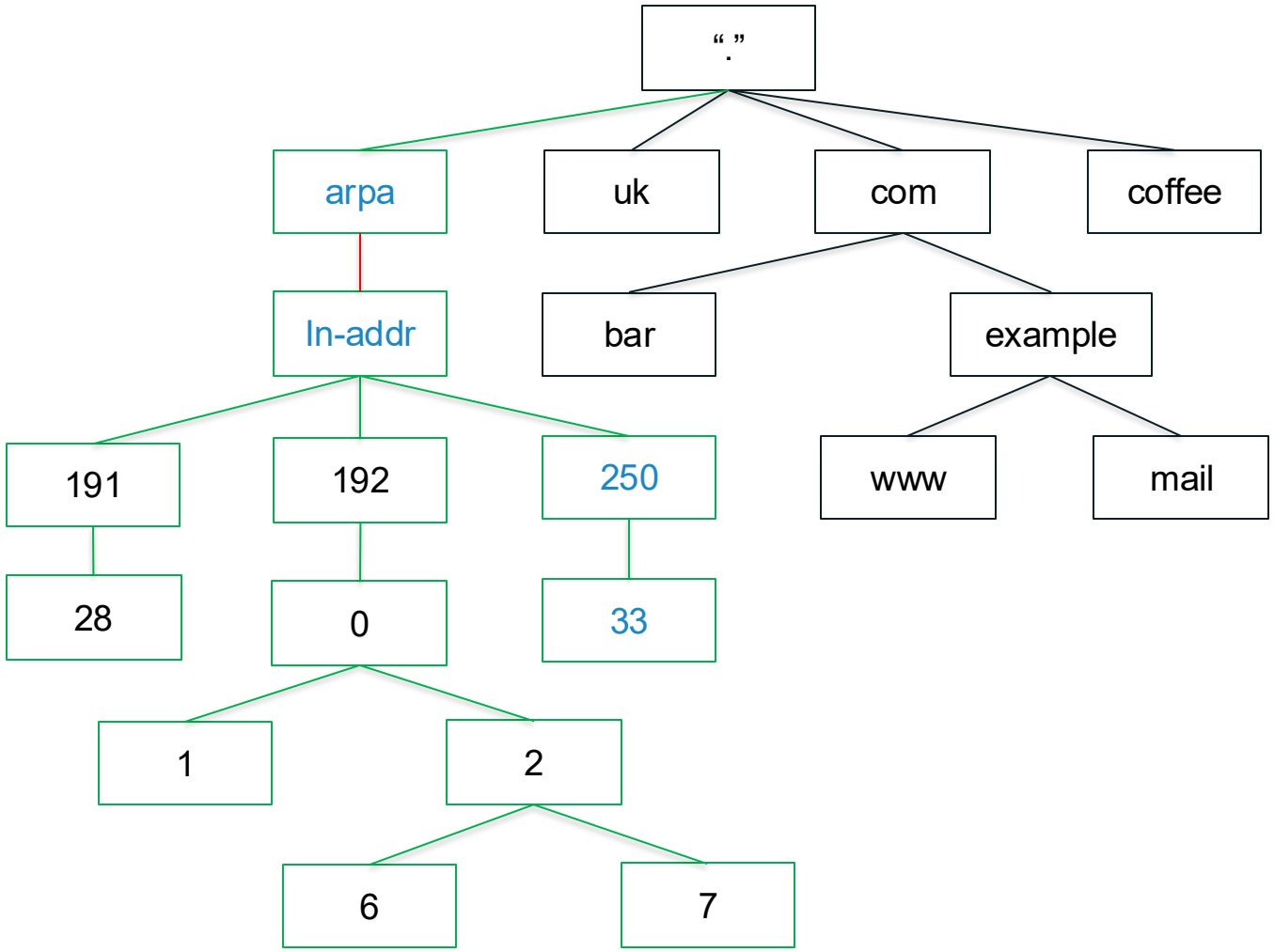
Reverse DNS (PTR)

- L'utilisation la plus courante de DNS consiste à mapper des noms de domaine à des adresses IP.
- DNS mappe également les adresses IP aux noms de domaine. C'est ce qu'on appelle le DNS inverse et il utilise le type PTR RR.
- IPv4 reverse DNS est associé à un domaine spécial (subtree) appelé ***in-addr.arpa***.
- IPv6 reverse DNS est associé à un domaine spécial (subtree) appelé ***ip6.arpa***.
- Pour représenter l'adresse IPv4 192.0.2.7 de example.com nom de domaine, nous renversons l'adresse IPv4 et ajoutons le suffixe de domaine de deuxième niveau in-addr.arpa. Résultat final:

```
7.2.0.192.in-addr.arpa.
```

Reverse DNS entries (PTR)

- résolution inverse précédente:
- `7.2.0.192.in-addr.arpa.`



Quelques autres types d’enregistrements

- **TXT**
  - Juste du texte
- **URI**, **NAPTR**
  - associe noms de domaine to URIs
- **TLSA**
  - Utilisé par DANE pour associer les certificats X.509 à un domaine.
- **CDS**, **CDNSKEY**, **CSYNC**
  - Synchronisation père-fils.
- **X25**, **ISDN**, **ATMA**
  - Adresses pour des protocols non-IP
- **LOC**, **GPOS**
  - Information de localicasion

Pratique !

1. Identifiez s'il existe des entrées DNS inverses pour les ressources suivantes de votre organisation :
   - Serveurs de messagerie
   - Serveur web
   - Serveurs de noms faisant autorité.

2. Si l'entrée DNS inversée n'existe pas, comment la rendre disponible ?

Exemple de fichier de zone: *example.com*

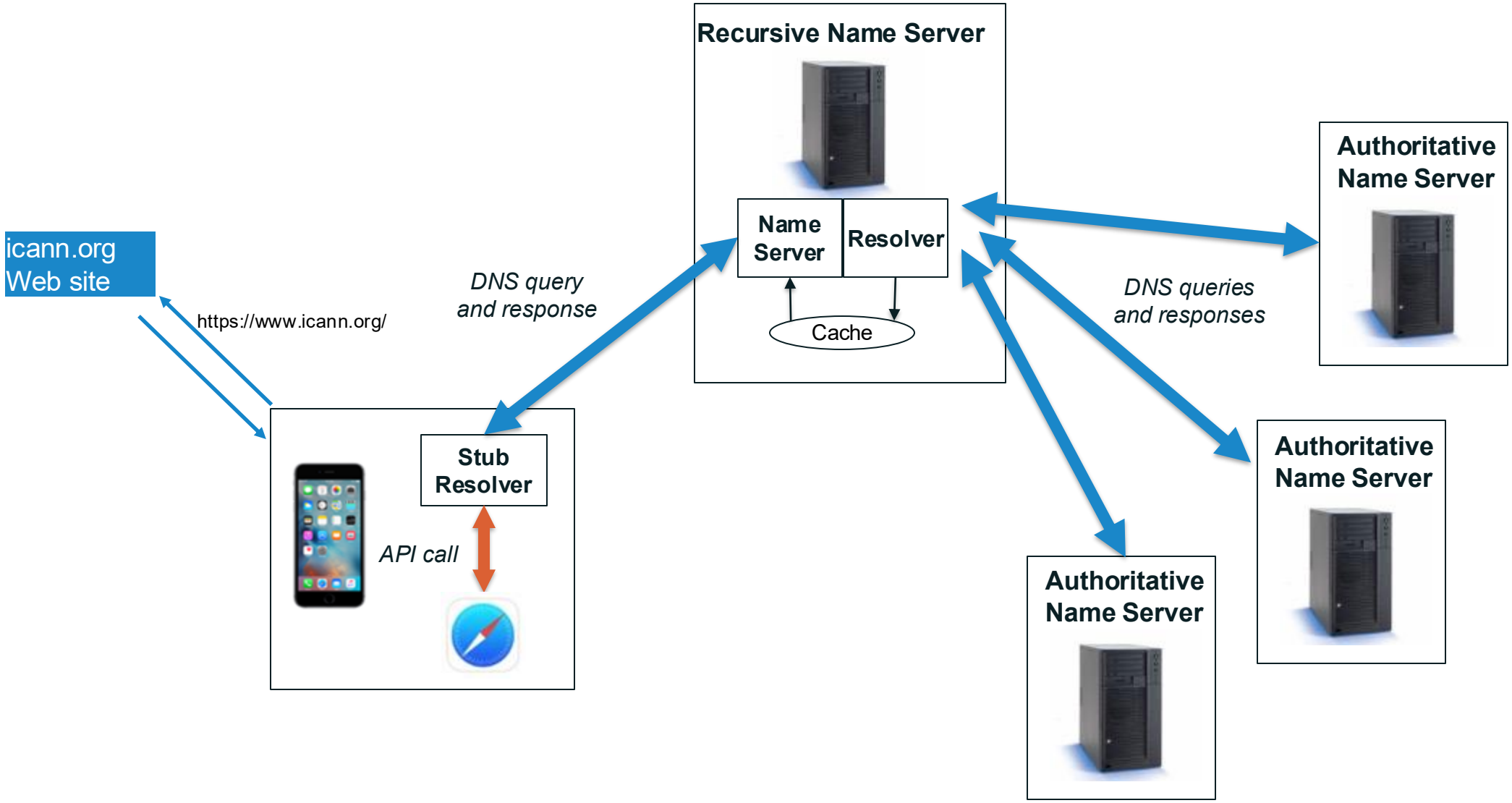
```
example.com.        SOA     ns1.example.com. hostmaster.example.com. (
                            20200316155500          ; serial
                            86400                   ; refresh (1 hour)
                            7200                    ; retry (2 hour)
                            2592000                 ; expire (4 weeks 2 days)
                            172800 )                ; minimum (2 days)
example.com.        NS      ns1.example.com.
example.com.        NS      ns2.example.com.
example.com.        NS      ns1.p41.dynect.net.
example.com.        NS      ns1.p41.dynect.net.
example.com.        NS      ns1.p41.dynect.net.
example.com.        NS      ns1.p41.dynect.net.
example.com.        NS      a1.verisigndns.com.
example.com.        NS      a2.verisigndns.com.
example.com.        NS      a3.verisigndns.com.
example.com.        A       192.0.2.7
example.com.        AAAA    2001:db8::7
example.com.        MX      10 mail.example.com.
example.com.        MX      20 mail-backup.example.com.
www.example.com.    CNAME   example.com.
ns1.example.com.    A       192.0.2.1
ns2.example.com.    A       192.0.2.2
```

Processus de résolution

DNS en bref

- DNS est une base de données distribuée
- Les données sont conservées localement mais disponibles dans le monde entier
- ***Resolvers*** envoient les requêtes
- ***Name servers*** répondent aux requêtes
- Optimisations:
  - Caching pour améliorer les performances
  - Réplication pour assurer la redondance et la distribution de charge.

Composants du DNS



Serveurs de Noms (NS) et Zones

- Les serveurs de Noms répondent aux requêtes
- Un serveur de nom **faisant autorité** (***authoritative)*** sur une zone a une connaissance complète de cette zone
  - Peut fournir une réponse définitive aux requêtes sur cette zone
- Une zone doit avoir plusieurs serveurs autoritaires (BCP16)
  - redondance
  - Répartition de charge

Processus de résolution de noms

- Le processus de résolution est la traduction d'un nom en une adresse ou de manière générique, la recherche d'une réponse à une requête DNS.
- Le stub resolver, le serveur de nom récursif et les serveurs faisant autorité collaborent ensemble pour rechercher les informations DNS dans l'espace de nommage.
- Une requête DNS comporte les paramètres ci-après:
  - Nom de domaine, classe, type
    - Ex: *www.example.com*, IN, A
- Deux categories de requêtes DNS:
  - Le Stub resolver envoit des requêtes ***recursives:*** "j'ai besoin de la réponse exacte ou d'une erreur".
  - Les serveurs récursifs envoient des requêtes ***non-récursives*** ou ***itératives:*** "je me charge de faire des recherches et accepte d'être redirigé".

Processus de résolution de noms

Le processus étape par étape

Processus de résolution de noms

Mais en fait …

- Pour un resolver qui vient d'être mis en service, il n'y a aucune donnée en local. Comment démarrer la resolution de noms?
  - Cache (si activé!) vide
  - Ne fait autorité sur aucune zone
- Seule option possible: s'adresser à la source: la racine!
  - Les serveurs racine (***root name servers)*** *sont ceux faisant autorité sur la zone racine.*
- Mais comment le resolver trouve les enregistrements NS, A/AAAA des serveurs racine?
  - Ils doivent être configures quelque part! (Ah oui, les logiciels DNS sont preconfigures avec une version à jour d'un fichier appelé ***root hint file***)
  - Il n'y a pas une autre alternative de découverte
- Le ***root hints file*** contient les nom et adresses IP des serveurs racine.
  - https://www.iana.org/domains/root/files

Liste des Serveurs Racine et fichier Root Hints

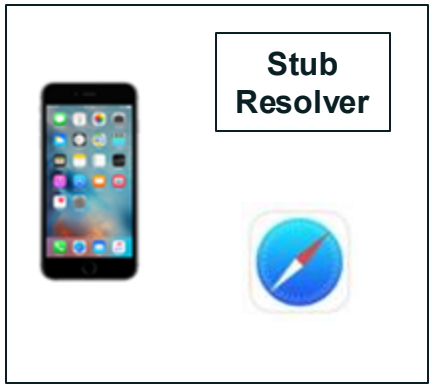
```
.                       NS      a.root-servers.net.
.                       NS      b.root-servers.net.
.                       NS      c.root-servers.net.
.                       NS      d.root-servers.net.
.                       NS      e.root-servers.net.
.                       NS      f.root-servers.net.
.                       NS      g.root-servers.net.
.                       NS      h.root-servers.net.
.                       NS      i.root-servers.net.
.                       NS      j.root-servers.net.
.                       NS      k.root-servers.net.
.                       NS      l.root-servers.net.
.                       NS      m.root-servers.net.
a.root-servers.net.     A       198.41.0.4
b.root-servers.net.     A       192.228.79.201
c.root-servers.net.     A       192.33.4.12
d.root-servers.net.     A       199.7.91.13
e.root-servers.net.     A       192.203.230.10
f.root-servers.net.     A       192.5.5.241
g.root-servers.net.     A       192.112.36.4
h.root-servers.net.     A       198.97.190.53
i.root-servers.net.     A       192.36.148.17
j.root-servers.net.     A       192.58.128.30
k.root-servers.net.     A       193.0.14.129
l.root-servers.net.     A       199.7.83.42
m.root-servers.net.     A       202.12.27.33
a.root-servers.net.     AAAA    2001:503:ba3e::2:30
b.root-servers.net.     AAAA    2001:500:84::b
c.root-servers.net.     AAAA    2001:500:2::c
d.root-servers.net.     AAAA    2001:500:2d::d
e.root-servers.net.     AAAA    2001:500:a8::e
f.root-servers.net.     AAAA    2001:500:2f::f
h.root-servers.net.     AAAA    2001:500:1::53
i.root-servers.net.     AAAA    2001:7fe::53
j.root-servers.net.     AAAA    2001:503:c27::2:30
k.root-servers.net.     AAAA    2001:7fd::1
l.root-servers.net.     AAAA    2001:500:9f::42
m.root-servers.net.     AAAA    2001:dc3::35
```

Processus de résolution de noms

Le stub resolver du téléphone est configure pour envoyer les requêtes au resolver récursif 4.2.2.2

Recursive Resolver
4.2.2.2

www.example.com
Web site

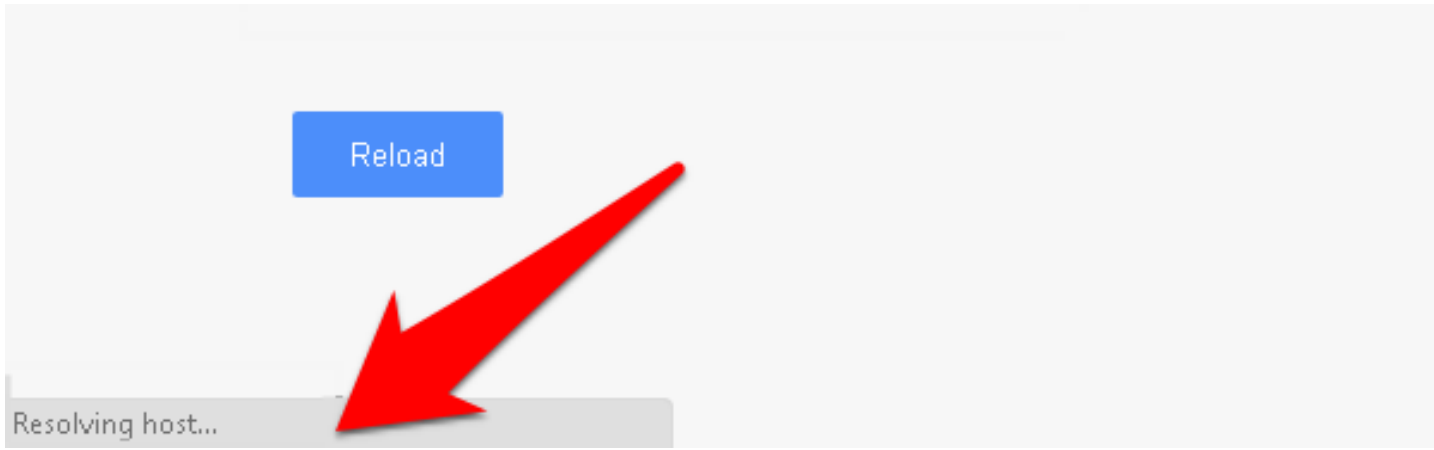


Processus de résolution de noms

L'utilisateur tape *www.example.com* dans son navigateur web par exemple; ce dernier va contacter le stub resolver local de l'équipement pour résoudre cette requête.

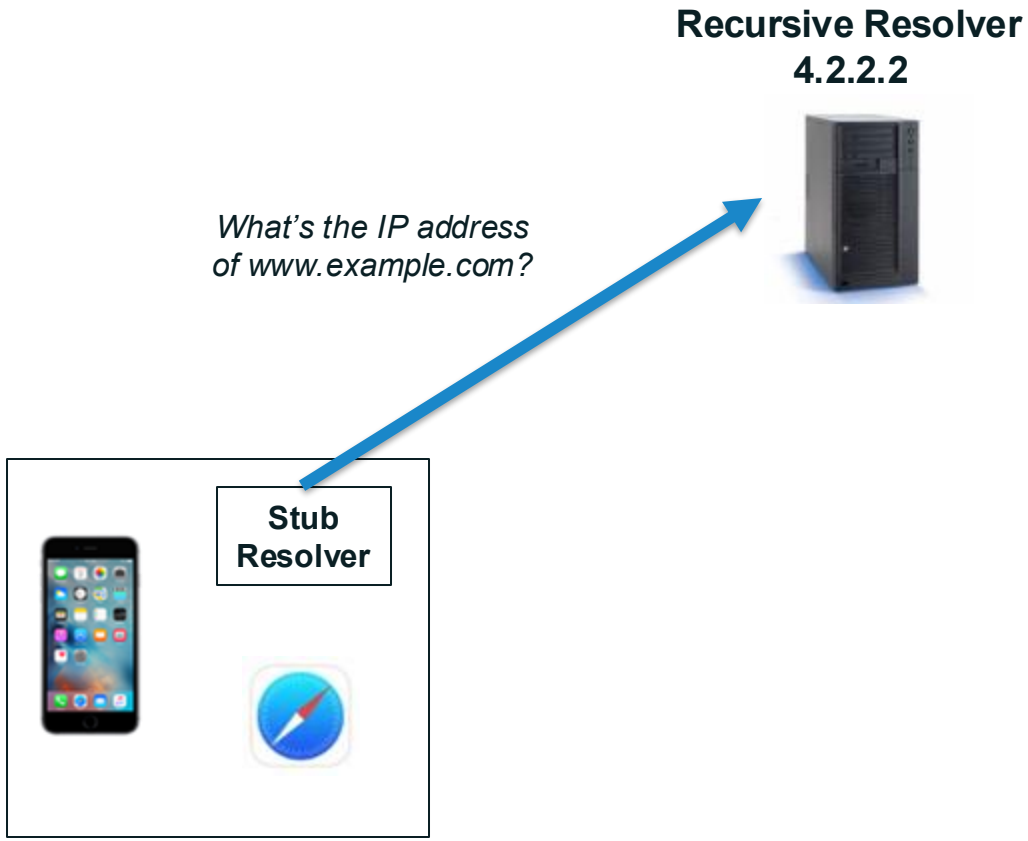
Recursive Resolver
4.2.2.2

www.example.com
Web site



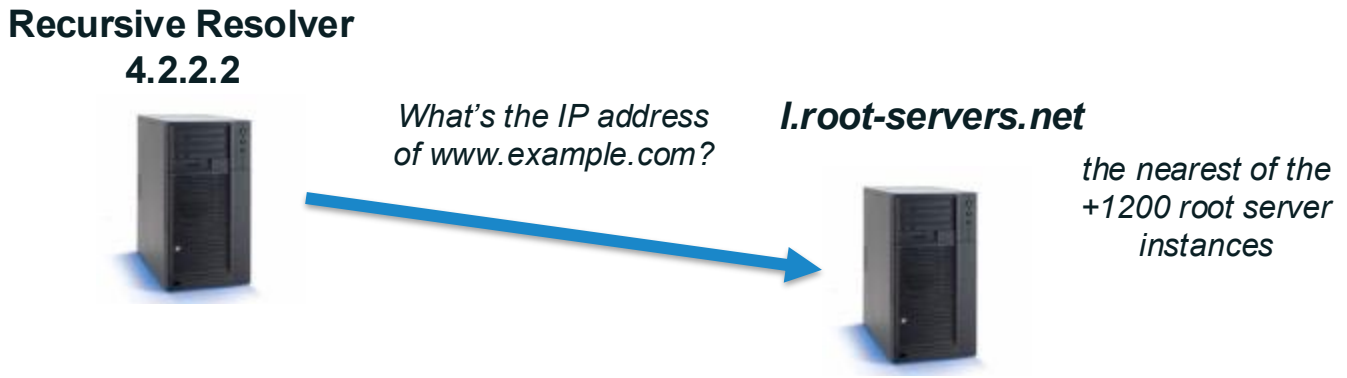
Processus de résolution de noms

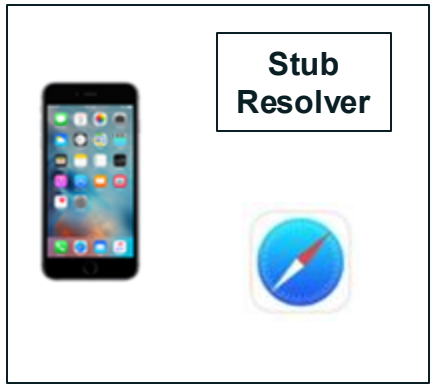
Le stub resolver du téléphone émet une requête DNS de type *www.example.com*, IN, A à destination du resolver 4.2.2.2



Processus de résolution de noms

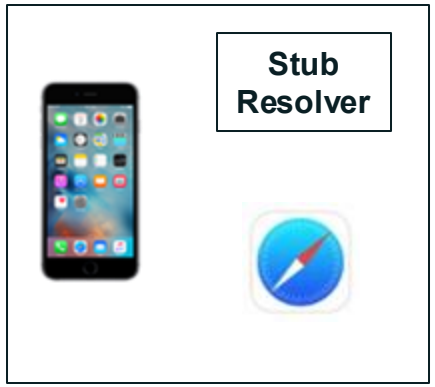
Le resolver récursif 4.2.2.2 ne possédant aucune information à propos de *www.example.com*, il va devoir interroger un serveur racine.





Processus de résolution de noms

Le serveur racine renvoit une référence vers la zone *.com*



Processus de résolution de noms

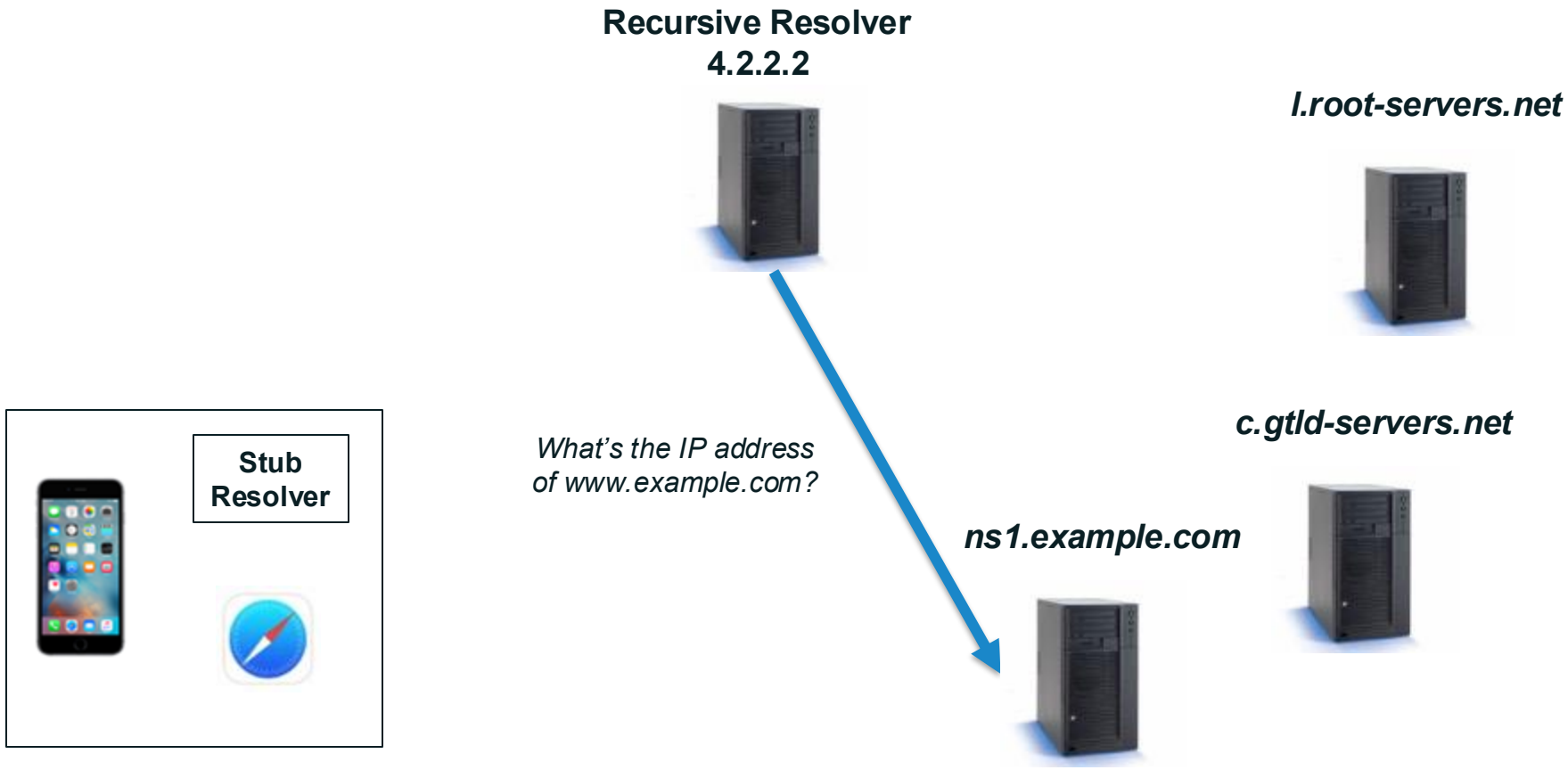
Le serveur récursif interroge ensuite un serveur autoritaire du .com

Processus de résolution de noms

Le NS autoritaire du *.com* renvoie une référence sur la zone *example.com*

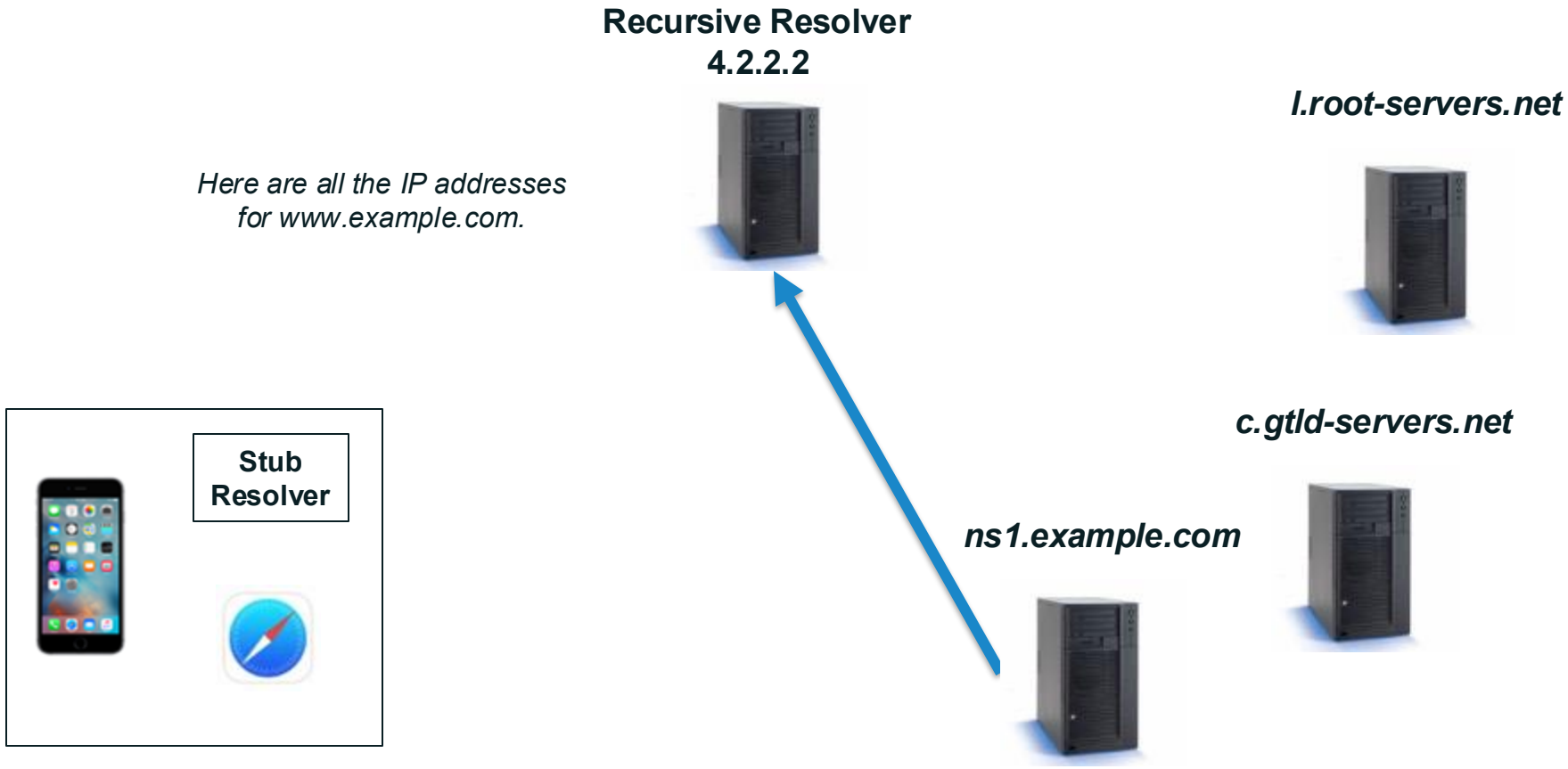
Processus de résolution de noms

Le resolver récursif interroge ensuite un serveur autoritaire de *example.com.*



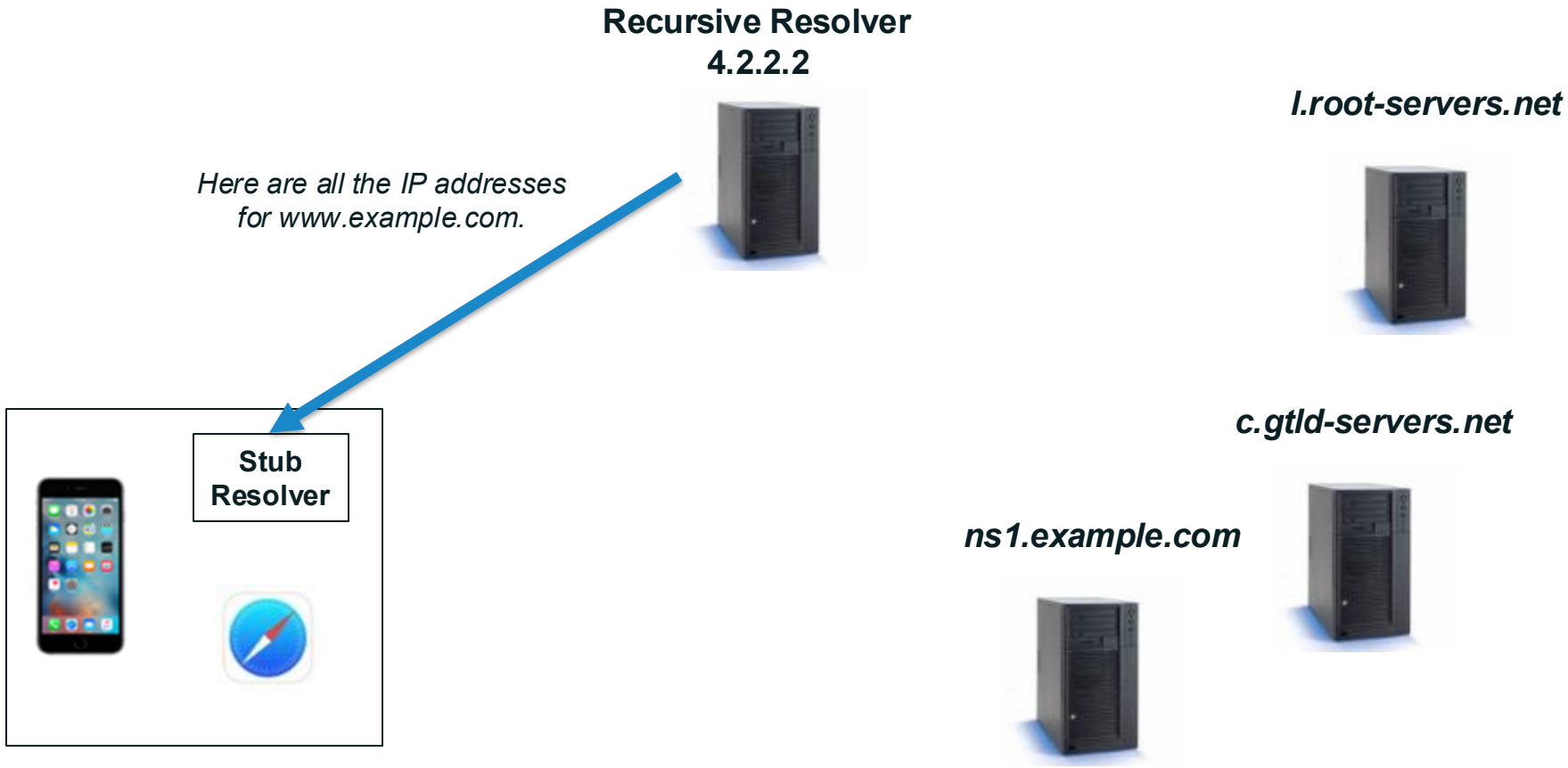
Processus de résolution de noms

Le serveur autoritaire de *example.com* renvoie la réponse car il a autorité sur la zone.



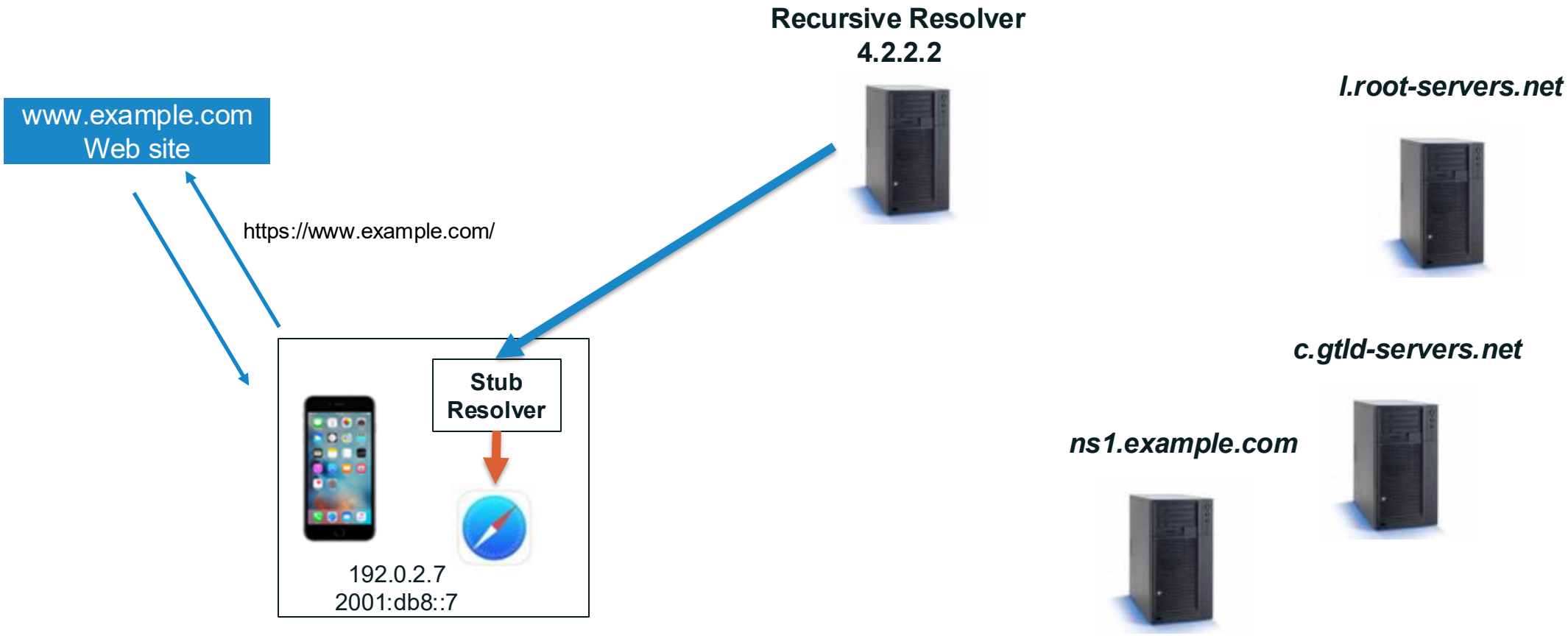
Processus de résolution de noms

Le resolver recursif peut **enfin** envoyer la réponse au stub resolver



Processus de résolution de noms

Puis le stub resolver partage l'adresse IP au navigateur qui a initialement émis la requête.



Comprendre le caching

- Lorsqu'un resolver récursif démarre, il n'a aucune donnée DNS relative aux noms de domaine (à l'exception des serveurs racine, dont les adresses IP et noms se trouvent dans ses fichiers de configuration).
- Chaque fois que le resolver récursif apprend la réponse à une requête, il met en cache les données afin de pouvoir les réutiliser pour les futures requêtes identiques.
- Il ne garde en cache la réponse que pour un temps limité: le TTL de l'enregistrement.
- Lorsque le TTL expire, le resolver efface ces données de son cache. Toute requête future donne lieu à une nouvelle recherche.
- La mise en cache accélère le processus de résolution et réduit la charge potentielle sur l'ensemble de l'infrastructure DNS.

Processus de résolution de noms

- Suite à cette première résolution, le resolver recursif 4.2.2.2 connaît désormais:
  - Les noms et addresses IP des serveurs faisant autorité sur la zone .com
  - Les noms et addresses IP des serveurs faisant autorité sur la zone example.com
  - L'adresse IP de www.example.com
- Le resolver garde en cache toutes ces données afin d'être plus rapide dans les prochaines résolutions de noms sans devoir reprendre toutes ces étapes intermédiaires.

…..

A présent, regardons ce qui se passera justement ensuite!

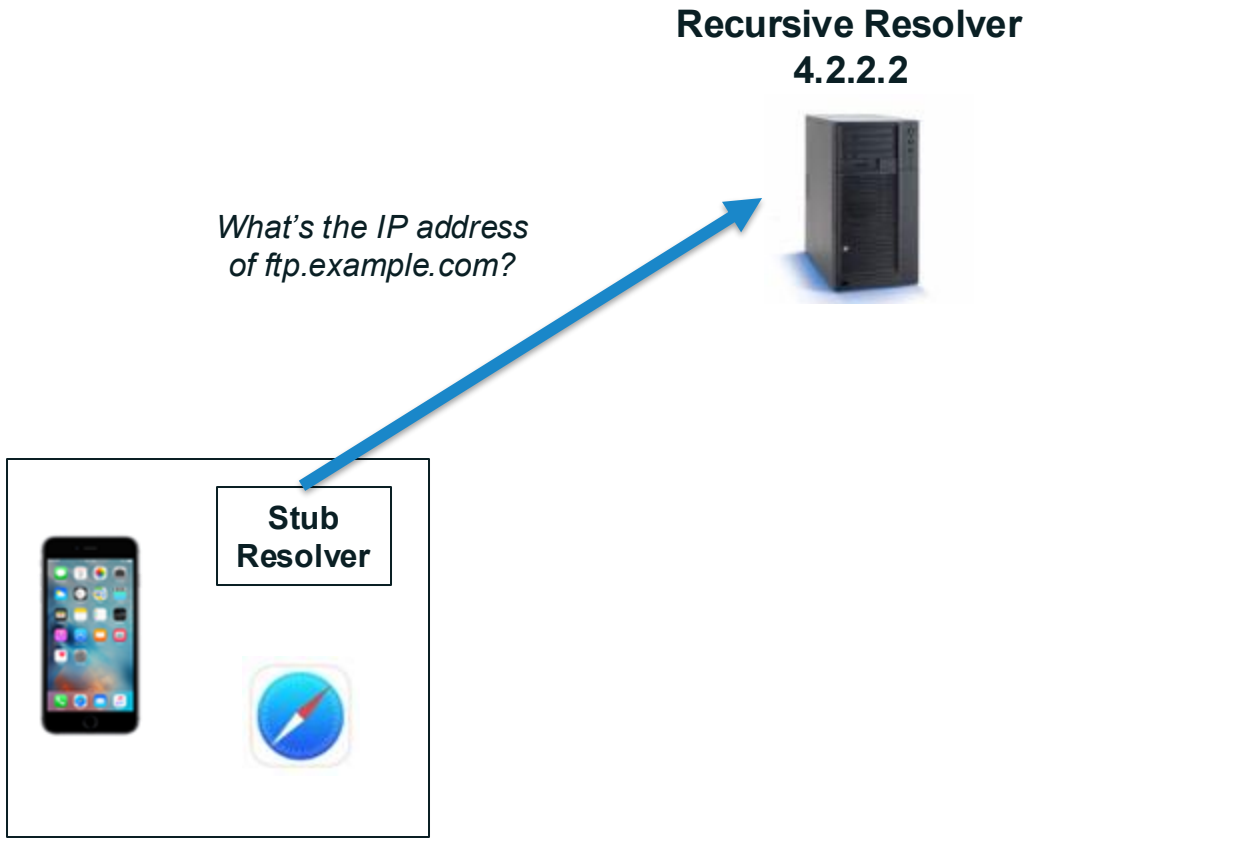
Processus de résolution de noms

Un autre utilisateur désire se rendre sur *ftp.example.com,* l'application interroge le stub resolver pour lui fournir l'adresse IP associée à ce nom

Recursive Resolver
4.2.2.2

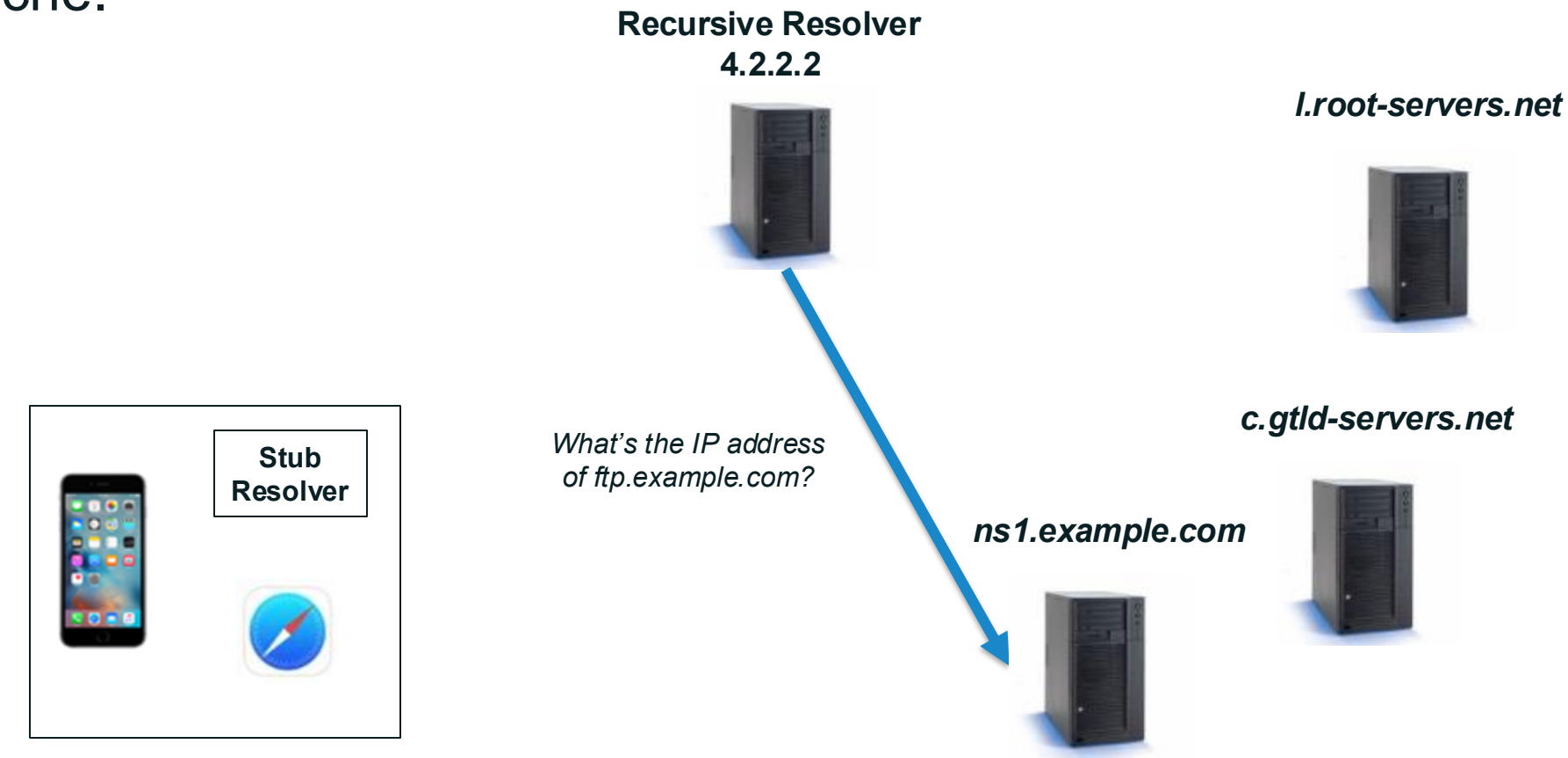
Processus de résolution de noms

Le stub resolver du téléphone envoie une requête DNS *ftp.example.com* IN A au resolver 4.2.2.2



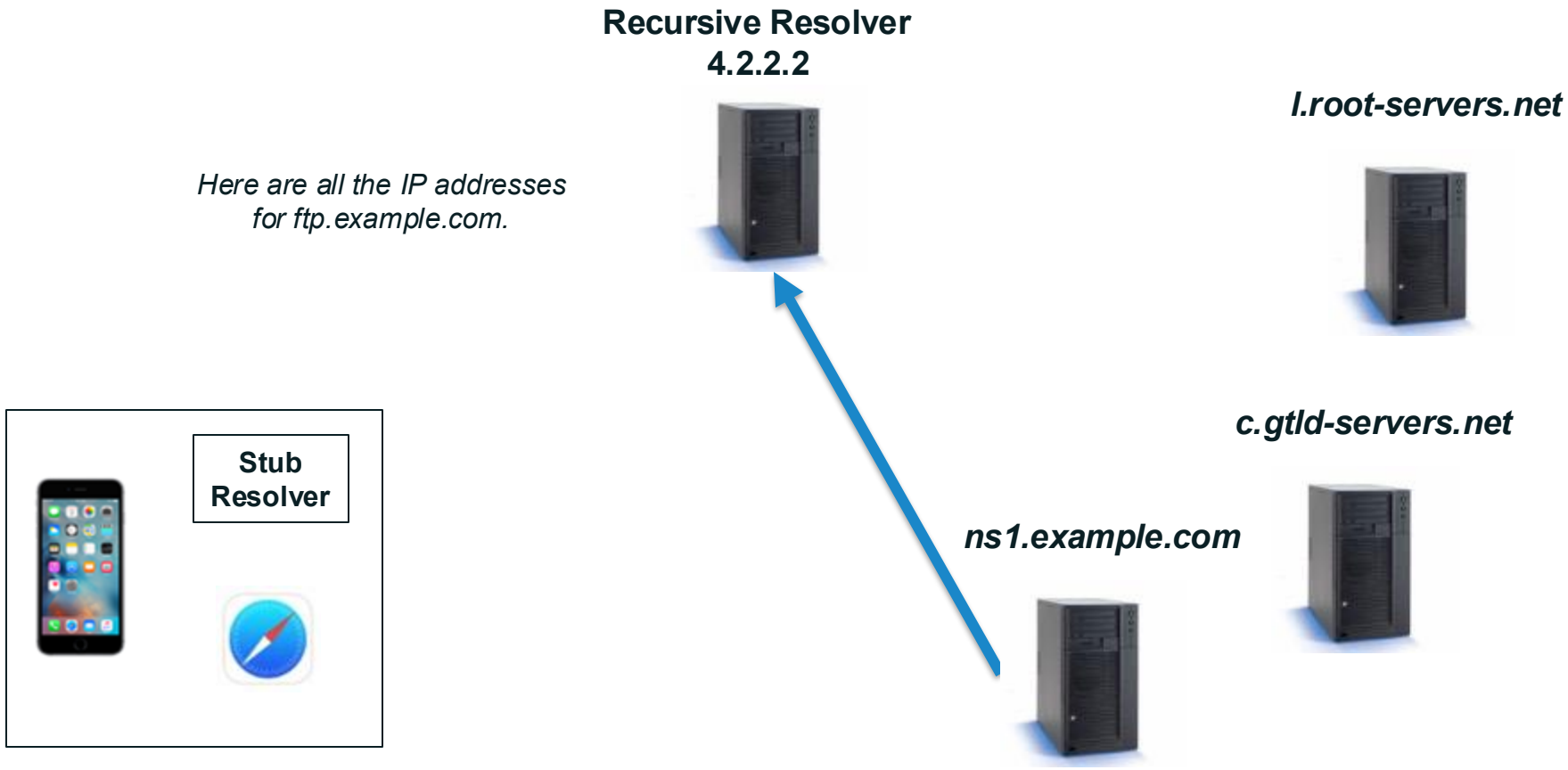
Processus de résolution de noms

Le resolver récursif interroge directement un serveur autoritaire sur la zone example.com puisqu'il a cette donnée encore présente dans son cache.



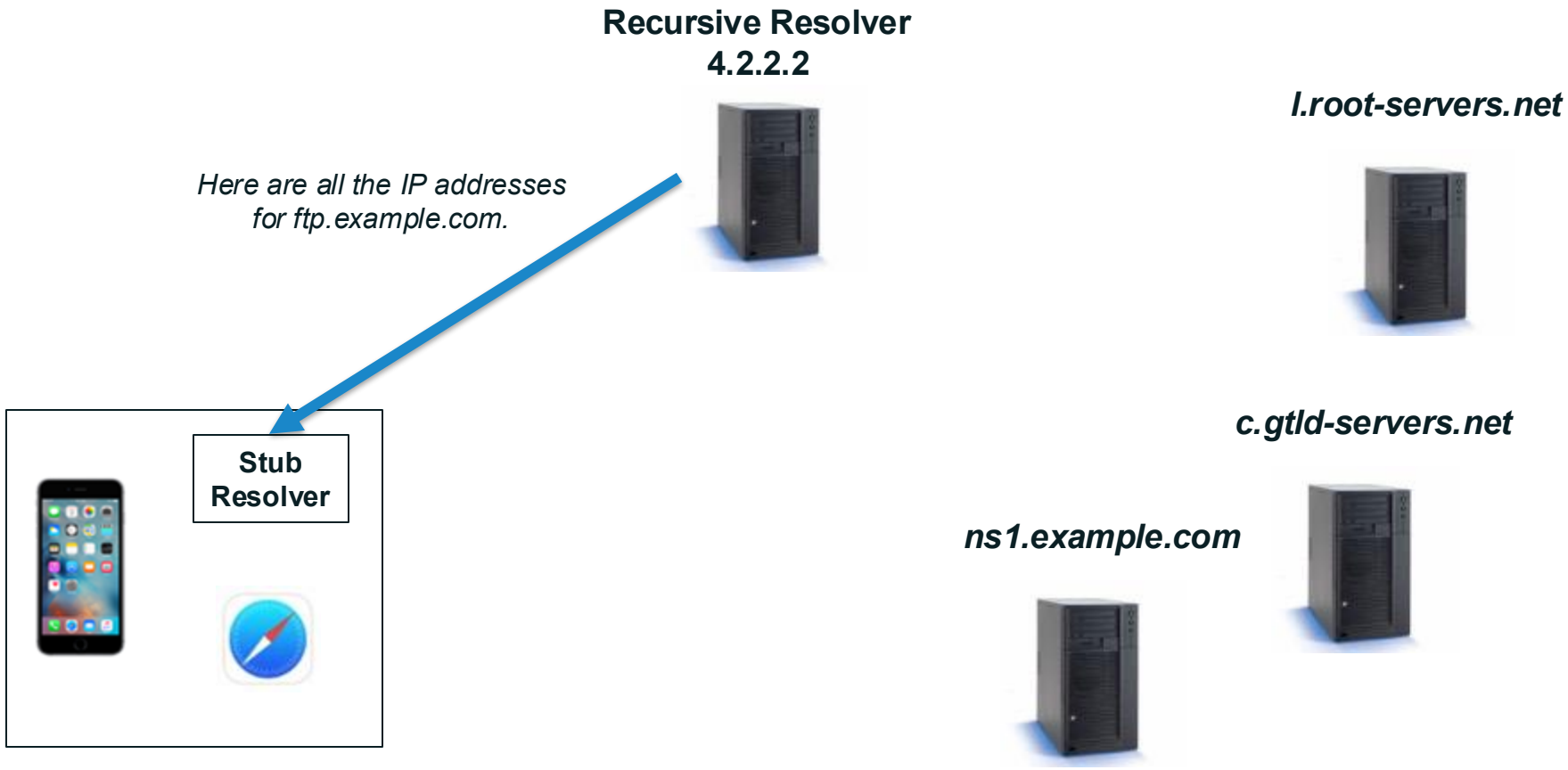
Processus de résolution de noms

Le serveur de *example.com* renvoie la réponse au resolver



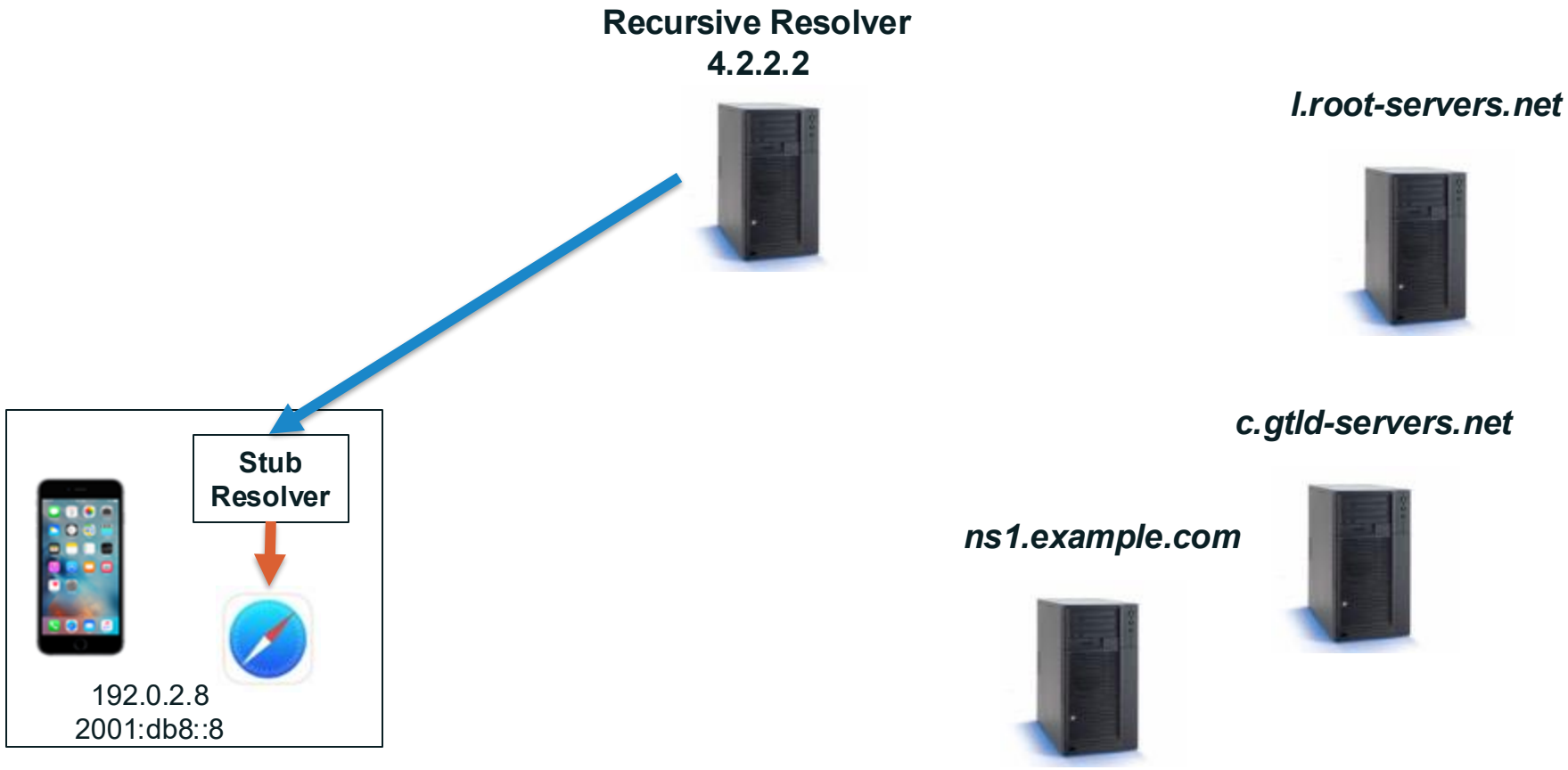
Processus de résolution de noms

Le resolver récursif revoie la réponse reçue au stub resolver



Processus de résolution de noms

Le Stub resolver renvoie la réponse à l'application



Résilience DNS #1

Résilience DNS #1

Les zones doivent disposer de plusieurs serveurs faisant autorité sur ladite zone :

- Pour assurer la redondance
- Pour répartir la charge

```
YAAK-9526:~ yazid.akanho$ dig NS icann.org @ns.icann.org.

; <<>> DiG 9.10.6 <<>> NS icann.org @ns.icann.org.
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 65026
;; flags: qr aa rd; QUERY: 1, ANSWER: 4, AUTHORITY: 0, ADDITIONAL: 3
;; WARNING: recursion requested but not available

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;icann.org.                     IN      NS

;; ANSWER SECTION:
icann.org.              86400   IN      NS      a.icann-servers.net.
icann.org.              86400   IN      NS      b.icann-servers.net.
icann.org.              86400   IN      NS      c.icann-servers.net.
icann.org.              86400   IN      NS      ns.icann.org.

;; ADDITIONAL SECTION:
ns.icann.org.           3600    IN      AAAA    2001:500:89::53
ns.icann.org.           3600    IN      A       199.4.138.53

;; Query time: 176 msec
;; SERVER: 2001:500:89::53#53(2001:500:89::53)
;; WHEN: Sat Mar 04 18:42:34 WAT 2023
;; MSG SIZE  rcvd: 164
```

Synchronisation de serveurs autoritaires

- Comment maintenir alignées les données se trouvant dans les fichiers de zone dupliquées à travers plusieurs serveurs?
- Fort heureusement, le protocole DNS résoud ce problème.
- Le serveur ***primaire*** a autorité pour répondre
  - Les changements sont donc effectués sur le NS primaire.
- Les serveurs ***secondaires*** obtiennent les données à jour de la zone à travers une opération appelée ***zone transfer*** permettant de copier le fichier de zone depuis un autre serveur autoritaire.
  - Le serveur duquel il copie s'apelle ***primary server***
- L'opération de transfert de zone est initiée par le NS secondaire.Zone transfer is initiated by the secondary
  - Chaque NS secondaire interroge le primary de façon périodique pour vérifier s'il y a une mise à jour.

Quelques outils d'analyse de configuration de zone

- Zonemaster: https://zonemaster.net/
  - programme qui teste la configuration d'une zone DNS avec différents contrôles d'intégrité configurés dans un moteur et fournit un rapport d'intégrité de zone.
- DNSviz: https://dnsviz.net/
  - fournit une analyse visuelle de la chaîne de confiance DNSSEC pour un nom de domaine et de son chemin de résolution dans l'espace de noms DNS, et répertorie les erreurs de configuration DNSSEC détectées.
- SuperTool: https://mxtoolbox.com/SuperTool.aspx
  - Un outil intégré qui peut effectuer plusieurs types de diagnostics sur un nom de domaine, une adresse IP ou un nom d'hôte. Documentation disponible: https://mxtoolbox.com/restapi.aspx
- Intodns: https://intodns.com/
  - vérifie l'intégrité et la configuration d'une zone DNS et fournit un rapport sur les serveurs de messagerie.
- Il y en a d'autres …

Aperçu de l’administration de la Zone Racine

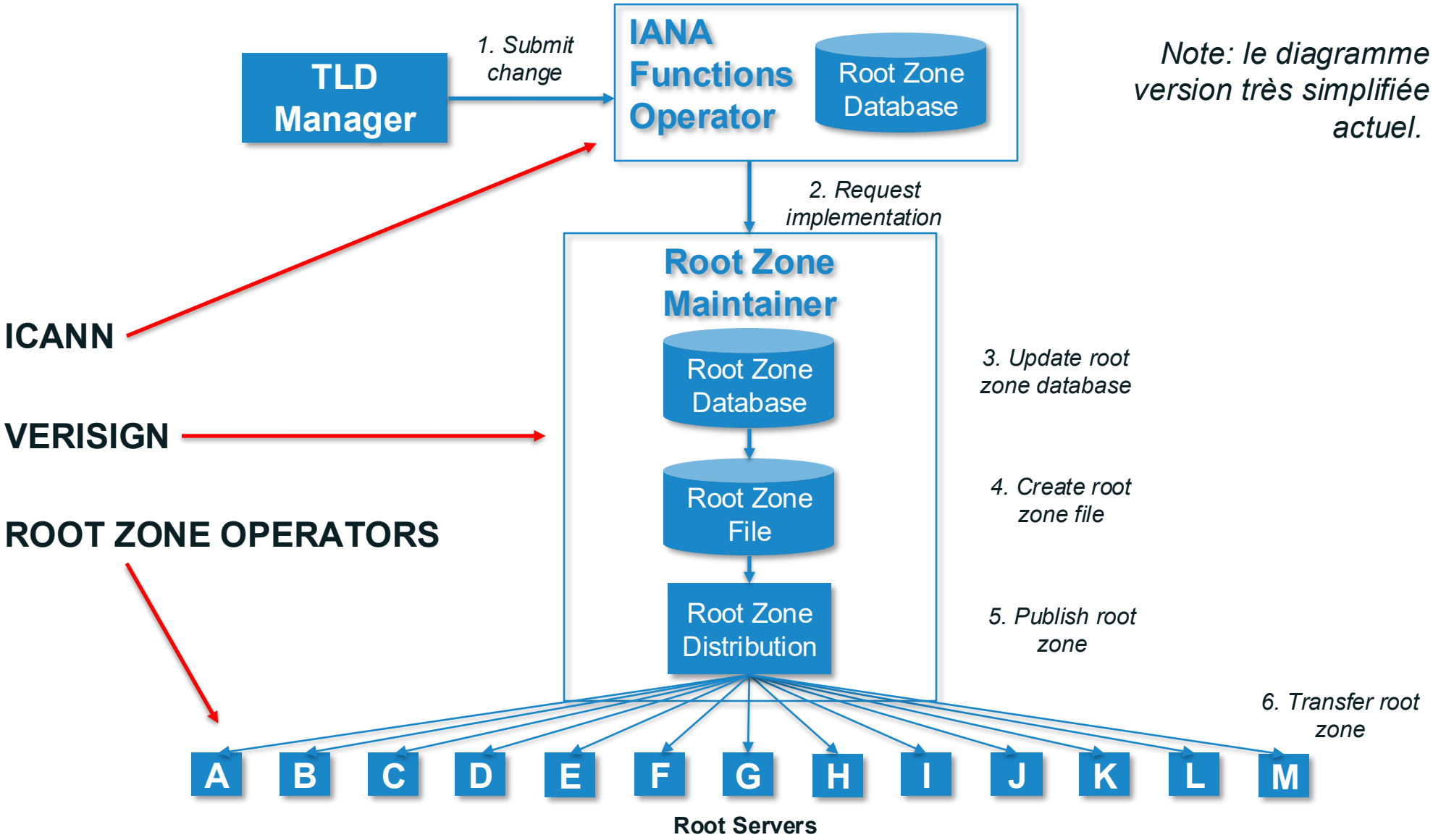
Aperçu de l’administration de la Zone Racine

- L’administration de la racine DNS n’est pas chose aisée!
- Douze organisations administrent les Treize serveurs faisant autorité sur le zone racine.

Les Opérateurs de Serveurs Root

- **A** Verisign
- **B** University of Southern California Information Sciences Institute
- **C** Cogent Communications, Inc.
- **D** University of Maryland
- **E** United States National Aeronautics and Space Administration (NASA) Ames Research Center
- **F** Information Systems Consortium (ISC)
- **G** United States Department of Defense (US DoD) Defense Information Systems Agency (DISA)
- **H** United States Army (Aberdeen Proving Ground)
- **I** Netnod Internet Exchange i Sverige
- **J** Verisign
- **K** Réseaux IP Européens Network Coordination Centre (RIPE NCC)
- **L** Internet Corporation For Assigned Names and Numbers (ICANN)
- **M** WIDE Project (Widely Integrated Distributed Environment)

Processus de changements dans la Zone Racine



Note: le diagramme montre une version très simplifiée du processus actuel.

Résilience DNS #2

Résilience DNS #2– (Résilience du Système de Serveurs Root)

- Un Opérateur de serveur racine peut déployer des copies de son serveur n'importe où dans le monde grâce à la technique ***anycast***
  - Assurer la redondance et résilience globale de l'infrastructure DNS.
  - Répartir la charge entre plusieurs serveurs.
- Chaque copie est appelée ***instance*** *du root server****.***
- Toutes les instances doivent avoir la même donnée afin de s'assurer que tous répondront de la même manière aux requêtes DNS et aussi s'assurer de la convergence d'Internet.

Instances de serveurs racine dans votre pays et sous-region

Déploiement serveur DNS:
- autoritatif
- resolver

Setup: choix du logiciel

- Logiciels resolvers connus pour faire la validation DNSSEC
  - Open Source: BIND, Unbound, Knot Resolver, PowerDNS Recursor, DNSMASQ, …
  - Commercial: Windows, Nominum Vantio (Akamai), Secure64 DNS Cache, …
- Cette liste peut être incomplète et ne privilégie pas une solution spécifique

ISC's BIND

- Authoritative server and cache all-in-one
- http://isc.org/
- Always changing, see current version on web site: https://www.isc.org/downloads/bind/
- Longest track record in DNSSEC

NLnetLab's Unbound

- a caching-only name server with DNSSEC built in
- http://www.unbound.net/
- "unbound" is a play on the word "bind"

cz.nic's Knot Resolver

- a caching-only name server with DNSSEC built in
- http://www.knot-resolver.cz/download/
- "Knot" is a play on the words "bind" and "unbound" (see a trend?)

PowerDNS Recursor

- Caching resolver
- Supports DNSSEC validation
- https://www.powerdns.com/documentation.html
- Also an authoritative server
- name is not related to BIND, unbound, Knot

DNSMASQ

- provides network infrastructure for small networks: DNS, DHCP, router advertisement and network boot
- authoritative and cache
- Supports DNSSEC (validation)
- main page: http://www.thekelleys.org.uk/dnsmasq/doc.html

Softwares DNS: aperçu

- Résolveurs récursifs populaires : BIND et Unbound. PowerDNS et Knot sont relativement récents.
- Autoritatifs populaires : BIND9 et PowerDNS. D'autres tells que NSD et Knot sont de plus en plus adoptés.
- Nous utiliserons principalement BIND, Unbound et NSD dans nos labs.

Software	Auth	Recursive	DNSSEC	DB / API
ISC BIND9	X	X	X	
PowerDNS	X		X	X
PowerDNS Recursor		X	X	
NSD	X		X	
Unbound		X	X	
Knot DNS	X		X	
Knot Resolver		X	X	

DNS Software: BIND

- Version 4 sortie avec BSD 4.3 en 1986
- Actuellement à la version 9.18
- BIND 10 était autrefois en développement, mais a été abandonné
- La plupart des implémentations DNS sont assez riches en fonctionnalités : ACL, vues, API pour integration aux base de données, DNS dynamique, signature et validation DNSSEC, etc.
- Souvent considéré comme « la référence »
  - Le format de zone BIND est la notation de facto
- More details at: https://www.isc.org/bind/
- Utilisé dans de nombreuses solutions commerciales.

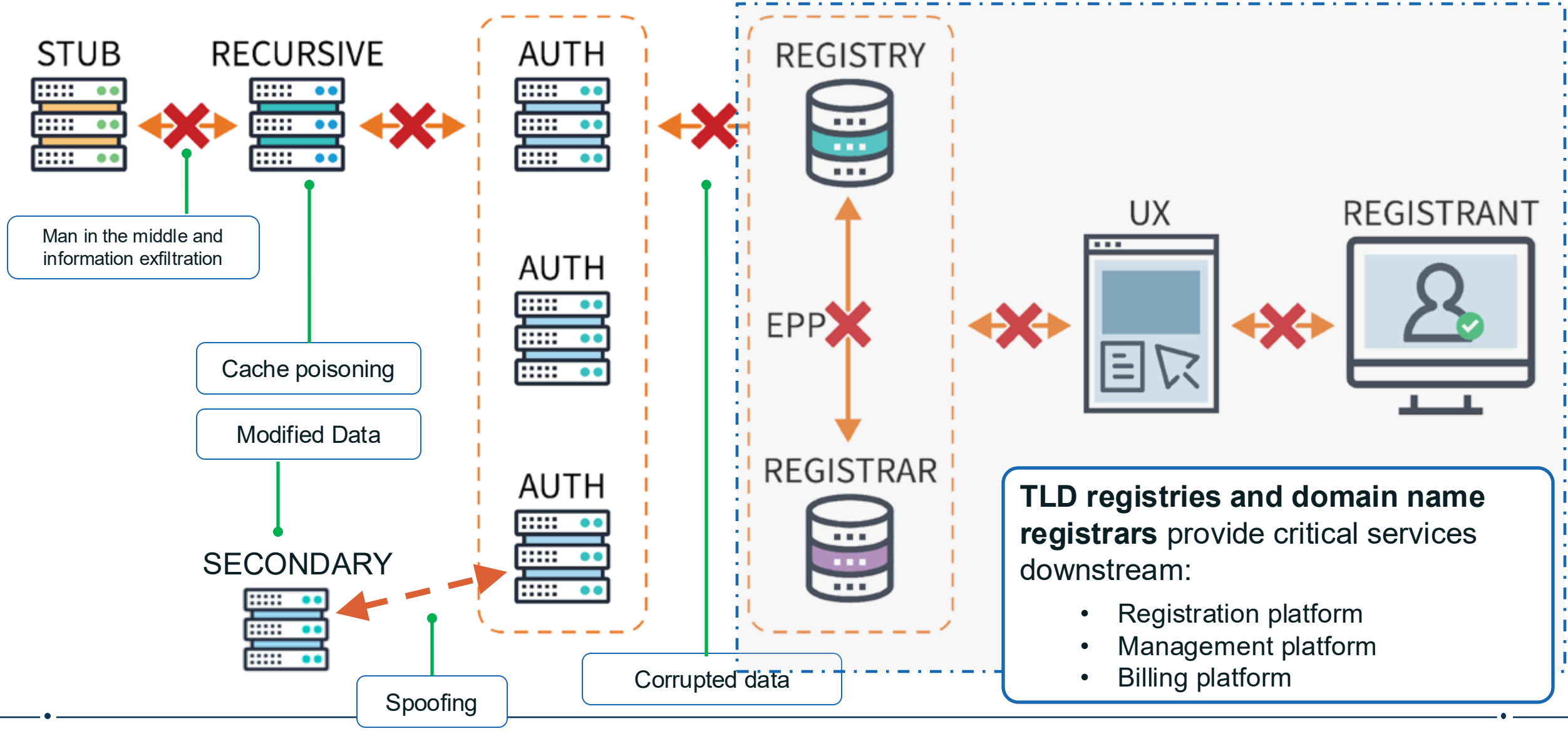
DNS Software: NSD

- Développé par NLNetLabs
- Authoritative uniquement
- Tire avantage de toutes les implementations de BIND
- Plusieurs serveurs racine utilisent NSD
- Les zones sont « compilées » dans un format précalculé « on the wire »
  - toutes les réponses possibles sont calculées, puis stockées dans une base de données binaire, prête à être envoyée
  - rapide

DNS Software: Unbound

- Développé par NLNetLabs
- Résolveur récursif uniquement
- Développé avec la performance pour objectif
- Plus léger que BIND
  - Utilisation plus efficace de la mémoire
  - Plus de fonctionnalités pour contrôler la mise en cache
  - Rapide…

Potentielles vulnérabilités et menaces de l'écosystème DNS



TLD registries and domain name registrars provide critical services downstream:

- Registration platform
- Management platform
- Billing platform

Quelques liens utiles

- TE Course Catalogue - https://www.icann.org/resources/pages/tech-engagement-training-course-catalogue-2021-04-22-en
- OCTO: https://www.icann.org/octo
- KINDNS - https://community.icann.org/display/KINDNS
- Domain Abuse Activity Reporting - https://www.icann.org/octo-ssr/daar
- ITHI - https://ithi.research.icann.org/

Pratique !

1. Configurer les NS primaire et secondaires de votre zone (assignée par le facilitateur)
2. Confirmez qu'ils sont tous synchronisés, qu'ils servent et répondent bien pour la zone.

Merci !

One World, One Internet

Visit us at **icann.org**


@icann


facebook.com/icannorg

youtube.com/icannnews


flickr.com/icann


linkedin/company/icann


slideshare/icannpresentations


soundcloud/icann